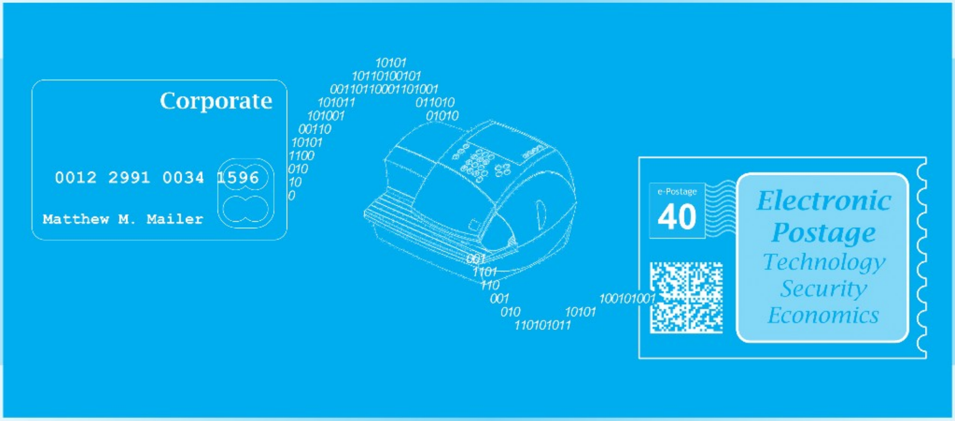
ADVANCES IN INFORMATION SECURITY

Electronic Postage Systems

Technology, Security, Economics



Gerrit Bleumer

Springer

Electronic Postage Systems

Technology, Security, Economics

Advances in Information Security

Sushil Jajodia
Consulting Editor
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
email: jajodia@gmu.edu

The goals of the Springer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers, as well as developers, are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

Additional titles in the series:

MULTIVARIATE PUBLIC KEY CRYPTOSYSTEMS by Jintai Ding, Jason E. Gower and Dieter Schmidt; ISBN-13: 978-0-378-32229-2
UNDERSTANDING INTRUSION DETECTION THROUGH VISUALIZATION by Stefan Axelsson; ISBN-10: 0-387-27634-3
QUALITY OF PROTECTION: Security Measurements and Metrics by Dieter Gollmann, Fabio Massacci and Artsiom Yautsiukhin; ISBN-10: 0-387-29016-8
COMPUTER VIRUSES AND MALWARE by John Aycock; ISBN-10: 0-387-30236-0
HOP INTEGRITY IN THE INTERNET by Chin-Tser Huang and Mohamed G. Gouda; ISBN-10: 0-387-22426-3
CRYPTOGRAPHICS: Exploiting Graphics Cards For Security by Debra Cook and Angelos Keromytis; ISBN: 0-387-34189-7
PRIVACY PRESERVING DATA MINING by Jaideep Vaidya, Chris Clifton and Michael Zhu; ISBN-10: 0-387- 25886-8
BIOMETRIC USER AUTHENTICATION FOR IT SECURITY: From Fundamentals to Handwriting by Claus Vielhauer; ISBN-10: 0-387-26194-X
IMPACTS AND RISK ASSESSMENT OF TECHNOLOGY FOR INTERNET SECURITY:Enabled Information Small-Medium Enterprises (TEISMES) by Charles A. Shoniregun; ISBN-10: 0-387-24343-7
SECURITY IN E-LEARNING by Edgar R. Weippl; ISBN: 0-387-24341-0
IMAGE AND VIDEO ENCRYPTION: From Digital Rights Management to Secured Personal Communication by Andreas Uhl and Andreas Pommer; ISBN: 0-387-23402-0

Additional information about this series can be obtained from
http://www.springer.com

Electronic Postage Systems

Technology, Security, Economics

by

Gerrit Bleumer
Francotyp-Postalia Group
Germany

Springer

Gerrit Bleumer
Francotyp-Postalia GmbH
Triftweg 21-26
16547 BIRKENWERDER
GERMANY
g.bleumer@francotyp.com

Library of Congress Control Number: 2006933129

Electronic Postage Systems: Technology, Security, Economics
by Gerrit Bleumer

ISBN-10: 0-387-29313-2
ISBN-13: 978-0-387-29313-4
e-ISBN-10: 0-387-44606-0
e-ISBN-13: 978-0-387-44606-6

Printed on acid-free paper.

9 8 7 6 5 4 3 2 1

springer.com

To Anne Christin

Contents

List of Figures

List of Tables

Foreword

My greatest appreciation to Dr. Gerrit Bleumer for taking the effort to document what, to many, may seem like a simple event in time. The technology that has emerged to produce electronic postage in postage meters and pc postage has evolved through many trial and error periods over my tenure (September 1992 – May 2005) as manager of the postage meter and pc postage programs. In order to keep the cost of metering (franking) at an acceptable level, many different technologies have evolved, and are still evolving. My grandest appreciation goes to Dr. Harald Windel, former CTO, Research, Development and Production of Francotyp-Postalia AG. It was Dr. Windel's persistence with the US Postal Service that made us realize the era for electronic digital postage had arrived. The world also owes many thanks to Dr Doug Tygar, Professor at the University of California, Berkeley. It was through his guidance and the contributions of many of his doctoral candidate students that we achieved the levels of technology and security used throughout the world posts. Dr. Tygar was reluctant to accept the consultant role in 1993, but has expressed to me, at my retirement from the United States Postal Service in June 2005, that he appreciated the association it afforded his students. This book is the first comprehensive record to present and explain the common paradigms and various approaches toward secure electronic postage to date. I don't think any of us have begun to experience the final technology that will emerge in electronic postage as a result of the foundation developed so far. I can only hope that some day someone will pick up this book and continue the next chapters of electronic postage to preserve the efforts of many who have brought this technology to reality.

WAYNE WILKERSON
Former Manager, Postage Technology Management,
United States Postal Services

Preface

Since the 1990s, the large postal operators of the world have sought for more economic and more secure forms of postage than traditional stamps and postage meters. Since the early 2000s postal liberalization gains more momentum in some markets and has created a number of private postal operators that compete with the universal postal operators. As the private postal operators grow bigger, they develop similar demands for economic and secure evidence of prepaid postage on the mail they process.

Modern technologies such as cryptography, digital signatures, hardware security devices, the Internet, sophisticated 2D bar codes, and high speed scanning equipment have come together so as to enable different flavors of electronic postage. While traditional postage meter markets are transformed into digital meter markets for enterprise mailers, new PC based electronic postage systems have come up to address the needs of small and home office mailers. Electronic postage is the enabling technology to address the needs of universal postal operators, private postal operators, enterprise mailers and mailers of small or home offices alike in the 21th century.

The topic of security in electronic postage has received remarkably little attention in the open literature about cryptography, authentication, secure protocols and system security. Peter G. Neumann, who has collected information system security incidents worldwide for decades and who has contributed to and edited the monthly column ‘Inside Risks’ inside the back cover of the ‘Communications of the ACM’, has never reported a problem related to postage meter fraud, online postage fraud, or similar. José Pastor was the first to propose cryptographically protected electronic postage in 1990 [62,63]. Doug Tygar et al [76,77] brought cryptographically enhanced postmarks to a wider audience in 1995, and Ross Anderson [1] mentioned such postmarks as a promising example “to stop the kind of frauds of greatest concern to the US

Postal Services, which involve junk mailers bribing postal employees to introduce large sacks of mail into the system." As cryptographically enhanced indicia have been rolled out at an industrial scale in countries like the United States, Canada and Germany, the time has come to take a closer look at e-postage devices and systems, their technology, security and economics.

Obviously, electronic postage systems adopt and apply a number of well-known technologies, but they are also beginning to shape a new way how mailers process, induct and trace their mail, and thus interact with the postal operators. It is conceivable that this process of system integration will proceed over the forthcoming years. The main stakeholders in e-postage systems are the mailers who pay for postal services and the postal operators who provide them. They all have legitimate security requirements, which we will unfold in detail. The material is organized as follows:

Chapter 1 presents a short history of postage and explains the advancing markets of electronic postage and their security issues.

Chapter 2 details a general model of electronic postage systems and of online and offline e-postage devices, and describes their services from a user's point of view.

Chapter 3 identifies the subsystems of an e-postage system and explains them in the standard client-server model of information technology.

Chapter 4 introduces the cryptographic mechanisms that are used in contemporary e-postage systems. Due to the small available space on paper envelopes, there is only a limited choice of cryptographic mechanisms appropriate for securing a postmark. Cryptographic mechanisms are also employed for securing the communication lines.

Chapter 5 develops a security domain framework for e-postage systems, which will be used in the following chapters to state system security requirements.

Chapters 6 and 7 provide detailed descriptions of contemporary industrial-scale electronic postage systems world-wide to support offline and online e-postage systems, respectively.

Chapter 8 exposes relevant attacker models, security risks and safeguards to electronic postage systems at various system levels. In 1995, cryptanalysts found that one of the most widely employed cryptographic mechanisms, the SHA-1 hash function is much more vulnerable to collision attacks than was supposed until 1994, and this mechanism is used exclusively in all industrial electronic postage systems in use today. Still, Chapter 8 finds that these vulnerabilities of SHA-1 hardly diminish the security of existing industrial e-postage systems. This is not meant as an excuse to stick to outdated algorithms, but it gives time to choose a reasonable successor for SHA-1 and completely replace the outdated SHA-1 within 4 to 5 years.

Privacy and anonymous mail are discussed in Chapter 9.

The process and peculiarities of getting e-postage systems approved by a postal operator are outlined in Chapter 10.

Finally, Chapter 11 looks at the major trends behind electronic postage that suggest to form its future.

This work spans a wide variety of topics from the algorithmic level and cryptographic details through hardware and software architectures all the way up to the approval process of electronic postage devices. Security and economic issues are considered at all levels, which is in line with realistic system design.

Given its variety of topics, it comes as no surprise that this work addresses a wide audience including software industry designers, developers, and testers of postage meters and other e-postage solutions, integrators connecting electronic postage to e-business systems such as eBay, security and cryptography engineers, decision makers of postal operators and postal regulators, professionals of postal standards bodies and system security testing laboratories. Students of computer science and computer security find applications of advanced cryptography in a number of real-life systems.

Acknowledgements

A number of people have encouraged and supported me to produce this work, and discussed numerous issues about the economics, technology and security of past, present and future e-postage systems. It is a pleasure for me to thank Rolf Oppliger who approached me and brought up the idea for this book in late 2000. As I was tied up in other activities at that time it took a while until the idea matured and took shape in 2005. Thanks go to the encouraging referees Ross Anderson (University of Cambridge, UK) who addressed "electronic postage security" in his own book "Security Engineering", Wayne Wilkerson and Dan Lord (US Postal Services), as well as Carsten Vullriede (Deutsche Post, Germany). Harry Whitehouse (endicia.com, US) introduced me to online e-postage in 2001, and I had extended discussions with David Chaum in 2005 about the privacy and anonymity aspects of electronic postage.

I am grateful to many of my colleagues in the Francotyp-Postalia Group for the professional and creative working environment, which sparked numerous discussions supporting this work. In particular, I thank Andreas Wagner and Manfred Schwarze for their early and continued support. Other contributors include Ludger Bornemann and Zac Moody who explained aspects of the international and US postal markets to me. Rainer Kreutzer shared his knowledge about the Canadian Postal Market. Momcilo Corovic and Andreas Witt provided the graphic images of most postal imprints. Clemens Heinrich did an excellent job in reviewing the entire manuscript.

Important feedback was given by Gerald Brose of Projectron, Germany. I thank Thierry Le Jaoudour and Jérome Modolo of Neopost Technologies, France, Douglas Clark of Pitney Bowes, Inc., and Dennis Jarrett of Dallas Semiconductor, Inc. who courteously contributed graphic images of some past and present postal security devices.

Chapter 1

Introduction

1.1 WHAT IS ELECTRONIC POSTAGE

In general, postage is a special payment instrument that is used to get access to certain postal services such as having mail pieces transported from a sender to an intended recipient. As such, postage is a special currency, which is minted by the respective *postal operator*, distributed to consumers of postal services, and eventually applied to mail pieces in order to serve as evidence of prepayment for a postal service. Unused postage, for which no postal service has been provided, is guaranteed by the respective postal operator to be converted back into cash in the amount of its face value. Certain restrictions may apply to the redemption of unused postage.

Postage has come to mailers for more than a century in the flavor of physical stamps that need to be affixed to mail envelopes. Since the 1920s, businesses have used postage meters in order to apply postage faster to their mail and to give it a more professional and customized look. Most postal operators have created additional flavors of postage, e.g. permit mail, to meet the needs of bulk mailers such as publishers, catalogue distributors and direct mailers.

Electronic postage is a contemporary flavor of postage with a variety of advantages over traditional stamps and traditional postage meter imprints: Electronic postage is distributed in electronic form from a postal operator to mailers and, before it is applied to mail pieces, it is converted into individually verifiable and printable evidence of prepayment for postal products or services. Cryptographic mechanisms are used to secure electronic postage both in its electronic and printed form. Moreover, using electronic postage can be integrated into the mailing process such that postal operators can harvest almost complete usage profiles about which of their postal products and services are used and when.

The term ‘electronic postage’ or ‘e-mail postage’ has also been used for payment instruments to prepay for electronic document or e-mail delivery and additional value-added services such as delivery notifications. The electronic evidence of such payments has been standardized as *electronic postmarks* by the Universal Postal Union (UPU) [108] and the International Post Corporation (IPC) [42]. In 2001, Microsoft went so far as to propose a universal system of mandatory electronic postage fees for sending e-mail in order to alleviate the spam problem. The proposal appears to be appealing for some reason and recurs with some frequency in usenet groups and the press. Bill Gates promoted the idea again at the world economic forum in Davos, Switzerland, in January 2004 as reported by CNN [20]. John Levine, an anti-spam advocate, considers the approach as economically unrealistic: Such an approach implies the setup of a worldwide micropayment system, which is prohibitively expensive to develop, test, deploy and maintain [49]. As Andrew Odlyzko, head of the Digital Technology Center at the University of Minnesota, pointed out, it will hardly be acceptable to users because people generally prefer flat rated over metered communication [61]. As is common in the communications industry, new services tend not to replace existing services entirely, but develop into co-existence with established ways of communication. Companies like Microsoft, America Online and Yahoo are likely to start niche markets for priority e-mail by using e-mail postage, which may gain some market share if their benefits become apparent [31]. In the following, we will focus on electronic postage to be used for physical mail delivery, not for electronic documents.

An important aspect of electronic postage are the *digital postmarks*, i.e., the secure imprints attached to envelopes or labels bearing evidence that a mailer has pre-paid for postal transportation. The significance of digital postmarks cannot be overestimated because they constitute the direct communication interface between the mailer's equipment and the postal operator's mail processing equipment. Thus, the quality of the digital postmark is key to the quality of an entire electronic postage system. This explains why digital postmarks are the subject of important standardization efforts like CEN EN 14615 [19] and UPU S36-4 [114] of more than one standards body. We shall see, however, that digital postmarks are only the tip of the iceberg, if we deal with electronic postage systems. There are many other important aspects that we need to address, among them postage meters, PC clients for online postage, background servers in different locations, hardware security modules, public key infrastructures, secure communication protocols, and cryptography.

1.2 SHORT HISTORY OF POSTAGE

The first documented use of an organized courier service for the distribution of written documents is in Egypt, where Pharaohs used couriers for the diffusion of their decrees on papyrus rolls in the territory of the State 2400 BC. One of the better known couriers in ancient Greece was the runner who in 490 BC brought the message from Marathon to Athens (42,195 km) that the Greek army had won the fight against the Persian king Daraios I. The ancient

Romans ran a well-organized network of couriers to distribute messages for military purposes. They established stations where couriers could sleep over and change horses. The latin names of these change stations (*mutatio posita*) or rest stations (*mansio posita*) became the origin of the word “Post”. In the 12th and 13th century, the knightly orders ran professional mail delivery systems for their own purposes. Over the centuries, messages were carried by couriers or salesmen going by foot or riding on horse back and later by post-coaches. In 1490, the Italian salesman Janetto von Tassis (later called Thurn und Taxis) got an exclusive license from the Habsburg emperor Maximilian I to organize a postal carrier service for military and administrative messages throughout the Habsburg territories. He organized horse change stations and professional couriers equipped with horns to guarantee a reliable letter transport service on the 1024 km distance between Innsbruck (Austria) and Mechelen (Belgium) within 5 or 6 days during summer or winter time, respectively. Around 1550, Thurn and Taxis operated a postal network throughout Western Continental Europe, and in 1615 he received the exclusive license from the Habsburg emperor Rudolf II to provide postal transport services for his government. In order to become more cost-effective, Thurn and Taxis was later allowed to also carry messages of private individuals. This license sparked the establishment of the first postal system in continental Europe.

Until the 17th century, it was common practice for mail recipients to travel to a mail delivery station to pick up their mail. The process was inconvenient and frustrating if the expected mail had not yet arrived. Around 1700, the Prussian Post introduced a mail delivery service by private servants to premium customers. The first regular letter-carrier service was mentioned in the statutes of the Prussian Post in 1710. The first street letter box in continental Europe was introduced by the Prussian Post in 1824, which came as a great relief to mail senders.

Until around 1850, it was common practice that postal transport services were paid only after successful delivery and therefore the recipient paid for the message transport. Recipients often refused to pay for mailings, in particular for unsolicited ones, thus making a fool of the couriers who had already provided the transport service. Moreover, the price for mail delivery usually depended on the particular route taken to deliver the mail. As exact maps were rarely available, the pricing for mail delivery appeared often arbitrary to mail recipients. In fact, the price asked for mail delivery was often as high as one work day’s wage, so many people looked for ways to save the postage fees altogether. There were senders and recipients who agreed on secret codes, such that the senders put certain code markings on the outside of their mail pieces and the recipients could pick them up after looking at the mail pieces without opening them. The recipients then refused to receive the mail pieces, which left the courier to decide whether to dump the mail right there or carry it back to the sender to ask the price for transport from him. The risk of recipients not willing to pay for mail delivery made mail transport an uncertain and fragile business and this in turn hampered the development of quality standards of mail delivery.

The first central, country-wide postal system in a modern sense was established in the United Kingdom in 1516. In his paper POSTAL REFORM: ITS IMPORTANCE AND PRACTICABILITY to Lord Melbourne, Sir Rowland Hill suggested in 1835 that letters up to half an English ounce (14.5 g) should be carried for a uniform fee of one penny, and the sender should pay the postage fee by affixing an adhesive stamp onto the letter. By asking the sender to pay for the letter transport, the *refusal problem* would be solved. The necessary trust by the senders would be achieved by establishing an official postal system and uniform postal rates. The effect of all measures combined would be a steep drop of postage rates compared to what senders were used to at that time. In turn, the volume of mail would increase, thereby generating revenue and profit for the postal system and thus for the Queen of England. After an appearance before a committee and further editions of his reform plan in 1839, his plans were accepted. A bill passed the British parliament and was granted by Queen Victoria on 17 August 1839.

*Figure 1.*Sir Rowland Hill (1795–1879)

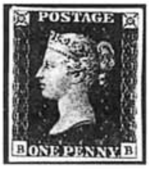


*Figure 2.*One-Penny-Black: First Stamp Ever Issued.

The first stamps were issued in 1840 in England, they were the One Penny Black and Two Pence Blue as shown in Figure 2 on page 4. Queen Victoria's portrait was taken from a medal designed by William Wyon. The pre-paid envelope was designed by William Mulready.

The postal reform proposals of Sir Rowland Hill proved to be a success story. The amount of mail sent and delivered in the UK tripled from one year to the next because of the reasonable pricing, and within the next decade many postal operators in Continental Europe and America adopted the concept of prepaid postage in the form of self-adhesive stamps. The United States issued the first stamps in 1847, and the first German stamps in the unified currency, Deutsche Mark (DM), were issued in 1872. In Japan, the first stamp was issued in 1871 and a nationwide postal system was established in 1872.

In order to harmonize postal policies and operations at an international level, the United States called for an international postal congress, which was held in 1863. Heinrich von Stephan (see Figure 3 on page 5), Prussian Minister for Posts, took the lead and founded the Universal Postal Union. It was created in 1874, under the name "General Postal Union", as a result of the Treaty of Berne signed by representatives of 22 states on October 9, 1874. On the occasion of the second world post congress in Paris, in 1878, the name was changed to "Universal Postal Union" [80]. On that congress, the UPU established that any postal matter like letters, postcards, and parcels, shall be franked by stamps and by stamps only. Furthermore, (1) there should be a more or less uniform flat rate to mail a letter anywhere in the world; (2) postal authorities should give equal treatment to foreign and domestic mail; and (3) each country should retain all monies it collected for international postage.

*Figure 3.*Heinrich von Stephan (1831–1897):
Portrayed on a Contemporary Postcard

This fundamental ruling by the UPU set the stage for practical international mail. It alleviated mailers from the burden of anticipating the physical route of each piece of mail, to determine which country would be traversed, and which stamps had to be used to pay for those traversals; the UPU provided that stamps of member nations are accepted for the whole international route and that international mailings shall employ stamps only that use letters from the latin alphabet.

Encouraged by the growing success of stamps in many countries, the UPU at the second World Postal Congress 1878 in Paris ruled that only stamps must be used as evidence of payment. The ruling turned out to be shortsighted because stamps were too inefficient to be used by large mailers. Demand increased for more automated and more convenient solutions for applying postage to mail pieces. However, it took each postal operator several years to gain confidence into stamp replacing technologies. In 1889, Josef Baumann demonstrated a first functional mechanical postage meter to the Bavarian postal authorities, which rejected the proposal. He improved the machine and was granted a patent for it on Jan. 5, 1900 at the imperial patent office (kaiserliches Patentamt). However, Baumann never got postal approval for any of his machines.

The first postage meters that applied valid imprints to a paper envelope thus indicating that the customer had paid for their postal delivery were developed by Karl Uchermann and manufactured by the Norwegian company Krag in 1903. These postage meters could imprint the fixed amount of 5 Ore and received approval by the Norwegian postal authorities on June 15, 1903. Four of these postage meters were used by post offices, three of them in private companies. However, they were soon withdrawn from operation one after another; the last one on January 2, 1905. New Zealand Post approved postage meters in 1904.

Beginning in 1902, Arthur H. Pitney constructed a series of mechanical postage meters, none of which was approved by the US Postal Services for putting postage onto first class mail. Only after joining forces with Walter H. Bowes and intense lobbying, were they successful in 1920 to get the world's first postage meter including an adjustable date stamp approved for first class mail, the Pitney Bowes Model M [67] (see Figure 4 on page 6). In the same

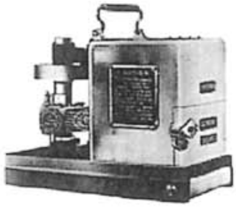


*Figure 4.*Original Pitney Bowes Model M postage meter (1920)

year, the Universal Postal Union officially recognized postage meters on their 7th world congress held in Madrid, Spain, as valid means for franking and decided that postage meters had to use red ink for their imprints.

The Model M could print only one denomination. In 1923, the German companies Bafra (Berlin) and Anker Werke (Bielefeld) founded a spin-off called Francotyp, which got approval for the first postage meter with adjustable postage amounts. Adjustable amounts were clearly necessary during the years of hyperinflation in Germany after world war I.

Unlike stamps, imprints of metered mail contain the date of mailing and are printed irreversibly onto the mail piece. A stamp can be carefully removed from one mail piece and be glued to another mail piece. To avoid the loss of postal revenues by customers who try to re-use stamps, the postal mail collection process includes a cancellation step that reliably invalidates each stamp that is used on a mail piece. Imprints of metered mail did not require a cancellation step because these imprints could not easily be removed from their original mail pieces and re-using them was easily detected by their date stamp because the date stamp was enforced to be fresh at the time of sending the mail piece. Mailers are required to deposit their metered mail at a post office on the same day that is shown as the *mailing date*. The postal clerk spot-checks if the printed mailing date matches the actual date and then feeds the metered mail into the mail collection stream behind the cancellation step for stamped mail. This convention and procedure for metered mail is similar in most countries.

Many more improvements were made to mechanical postage meters over the following decades. The mechanical postage meters used mechanical counters to keep the postal registers, i.e., the amount of remaining postage stored inside the postage meter. They used rotating printing dies into which the imprints were cut. In order to refill these meters, they had to be taken to a post office to be unsealed or unlocked to be reloaded. The locks and seals were to protect the postage meters against unauthorized manipulation, and to make sure that attempts of tampering would leave obvious forensic evidence.

It had become common practice that postage meters stored their remaining postage in four *postal registers* as follows:

1. The *ascending register* is increased every time an imprint is produced by the face value of that imprint.
2. The *descending register* is increased at every refill by the amount being refilled, and it is decreased every time an imprint is produced by the face value of that imprint.

3. The *total settings register* is increased at every refill by the amount being refilled. At any time, the total settings register represents the sum of the ascending register and the descending register.
4. The *piece count register* is increased by one every time an imprint is produced. This register maintains the total amount of all imprints produced since its initialization.

The increasing population of postage meters in many countries revealed that mailers in fact demanded for more efficient ways of franking than using stamps. Japan Post approved the first postage meters in 1958.

Propelled by growing economies, the volumes of mail grew in the developed countries, so much that postal operators had to keep automating their processes further. Germany was the first postal market where a system of *postal codes* was introduced in the early 1960's to improve the speed and quality of sorting and delivering mail. In 1963, the US Postal Services followed suit by introducing *ZIP codes* (zone improvement plan), which became the US postal codes.

In the 1970's electro-mechanical postage meters were introduced, which employed a microprocessor and maintained their postal registers in random access memory instead of using mechanical counters. The printing system was based on an electro-mechanical die, which allowed printing speeds of up to 12,000 pieces per hour. Users enjoyed to reload postage by using a regular phone. After the users had identified themselves and their postage meters they requested an amount of postage to be downloaded. They obtained an unlock code that had to be entered into the postage meter and were later debited by the respective amount. The postage meter verified the unlock code and got reloaded. This way, users of postage meters no longer had to make a trip to the post office, but could operate their postage meters without leaving their offices. The introduction of personal computers in 1982 and office printers soon after, boosted the evolution of postage meters because digital technology produced a steady stream of increasingly powerful chipsets, communication techniques, and printing systems at decreasing cost. In the late 1980's downloading postage became even more convenient by using computer modems, which were integrated into the postage meters. This way, the postage meter could access a remote postage server directly through the telephone network, thereby avoiding the inconvenience and unreliability of orally transmitting unlock codes.

The next generation of postage meters was electronic. These meters employed a digital printing technology in place of the formerly common mechanical dies. In 1991, Francotyp-Postalia introduced the first electronic postage meter, the T1000, which employed a thermal transfer print system (see Figure 5 on page 9). The digital printing technology allowed to control the content of each individual imprint by the operating software of the postage meter and to produce individual imprints at high operating speeds. As ink jet technology became more reliable and affordable in the 1990s, it was soon embraced and adopted by the postage meter industry. While market forces pulled postage meter technology to adopt more and more inexpensive PC and office printer technology, postal authorities became increasingly concerned about growing figures of counterfeit imprints that were produced by manipulated postage meters or just plain photo copying of original postage meter imprints. From the early days of postage meters, the printing system was under particular scrutiny of all postal authorities. For this reason, some postal operators required postage imprints to use a type of ink, such as fluorescent, that is hard to reproduce on a standard photo copier.

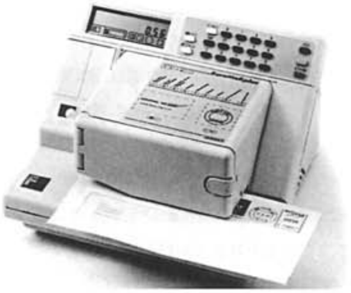


*Figure 5.*Francotyp-Postalia T1000 postage meter

1.3 FRAUD, METER MANIPULATION AND COUNTERMEASURES

Postal operators experienced the problem of counterfeit imprints because they failed to require security designs of postage meters and their imprints to stay ahead of attackers who became more knowledgeable and powerful with each generation of Xerox machines and PC digital imaging software and with every year the postage meters were left installed unchanged.

A *traditional postage meter imprint* consists of a *postmark*, a *town circle*, an optional *counter*, an optional *advertisement*, an optional *tracking number* and/or one or more *endorsements* as shown in Figure 6 on page 10. The order in which the tracking number, endorsements and advertisements may occur in an imprint depends on the requirements of the respective postal operator.

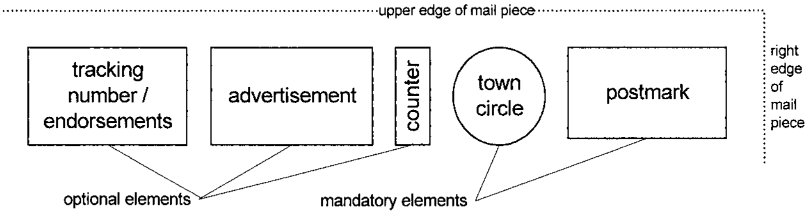


*Figure 6.*Layout of a Traditional Postage Meter Imprint

The *postmark* serves as evidence to the *depositing post office*, also called *inducting post office*, that the required amount of postage has been pre-paid. It includes a sign of the postal operator to whom the prepayment was made, the amount of postage and an identifier of the creating postage meter, e.g., its serial number.

The *town circle* approves that the mailer has inducted the mail piece at a postal operator. It includes the induction date and location, i.e., the mailing date and the town, postal code and/or post office where the mailer inducted the mail piece. Originally, town circles were introduced by postal operators who applied them at their post offices when the mail pieces were inducted. When the volume of mail increased, the postal operators allowed mailers to pre-print the town circles on behalf of their inducting post offices. Of course, the mailing date and location had to be pre-printed accurately, which means the mail had to be inducted on the printed mailing date at the printed inducting post office. Some postal operators allow a tolerance on the induction day, such that mail is accepted also one day after the printed mailing date.

The optional *counter* can be used by the mailer to index the pieces of a mass mailing in order to support the induction process. It is a helpful indicator, for example, to claim discounts for pre-sorted mail.

The optional *advertisement* promotes the mailer's business or a business event, or is just a seasonal greeting. It communicates a professional open message from the mailer to the recipient. The only postal restrictions on advertisements are not to be insulting, offending, obscene, or to look like a town circle or a postmark.

Optional *tracking numbers* are used by many postal operators to trace the mail piece through the delivery chain. Examples are tracking numbers for certified, insured or registered mail. *Endorsements* are fixed phrase indicators to inform the mail carrier about additional services ordered and pre-paid by the sender, such as address service requested, etc.

If we look at this design from a security point of view, it is obvious that traditional postage meter imprints could be easily copied onto any other mail piece that is inducted on the same day, at the same post office, and requires the same amount of postage.

Another increasingly serious threat has been the misuse of postage meters themselves. Some attackers operated mechanical or electro-mechanical postage meters, which they hid from postal inspections. Instead of resetting these meters by going to the Post Office and paying for the new load, they broke or bypassed the lead seals and manipulated the postage meter so they could reset these meters over and over again without paying the due postage fees. In fact, postal operator records showed that all major meter fraud cases involved physical tampering [81]. This type of fraud was hard to detect because the information, when each meter had been reset and by how much, was only available in paper file folders stored at respective post offices. Matching it up with usage data explored by postal inspectors was a tedious and time consuming job. An additional threat were the postal clerks handling physical meter keys, which typically allowed access to any meter of the same model, or sometimes even worse, of the same meter manufacturer. Loss and theft of these meter keys and the possibility of human error by the postal clerks posed major security risks.

Around 1990, exploits of the vulnerabilities outlined above caused the US Postal Services an estimated annual loss of revenue of at least US$100 million [83,84,53]. (This comes on top of an estimated loss of revenue of US$100 million from mail fraud caused by using ‘recycled’, insufficient or no stamps [58,68].) It got increasingly harder to prevent the misuse of postage meters and counterfeit postage imprints by only focussing on the print systems of postage meters. Clearly, a security continuum had to be enforced that linked the amount of postage downloaded into postage meters to the amount of postage imprints produced by these postage meters. And this goal was obviously far beyond securing just the printing systems of postage meters.

In 1990, José Pastor of Pitney Bowes, Inc. proposed a system to produce and verify cryptographically protected imprints, which he introduced under the name Cryptopost™ at the US Postal Services Fourth Conference on Advanced Technology in 1990 [62]. The cryptographic design was based on two layers of RSA encryption applied in non-standard ways published in 1991 [63]. Because of its proprietary approach, Cryptopost™ never became a product. However, it proved that cryptographic mechanisms in combination with tamper resistant control boxes and two-dimensional barcodes had the potential to replace traditional postmarks while limiting postage fraud much more efficiently than could be expected from existing technology at that time. It was clear that producing the new types of imprints was only one side of the deal. The other side was, of course, to upgrade all mail processing centers of the US Postal Services to respective bar code scanning and verifying technology. For the US Postal Services, the Cryptopost™ proposal was a huge financial challenge, but squarely addressed their revenue protection problems. The US Postal Services therefore concluded that the best protection for postal revenue could be achieved by

1. specifying an open security framework based on modern cryptography, which was free to be used by the US Postal Services and any manufacturer who wanted to join the market, and
2. requiring the entire market to switch to those more secure postage meter models after a transition period.

This analysis resulted in a strategic meter replacement program [80] of the US Postal Services to be implemented in six phases, which are summarized in the following Table 1 on page 12. In phase I and II, the program would retire all postage meters that can be reset manually. After completion of phase II, all postage meters in the market are reset electronically. This greatly improves the overall postal system security because all postage meters of one manufacturer download their postage through a central resetting computer system of that manufacturer, which in turn allows to request the exact amount of downloaded postage for any postage meter in any given period of time in almost real-time. The US Postal Services could then reconcile the amount of downloaded postage with the amount of printed postage on a per meter basis. If this reconciliation reveals significant imbalances, the US Postal Services would warrant investigations on the respective meters. This amounts to an "inspection" of the total settings each time the meter is reset. As a side effect, remote

Table 1. Milestones of US Postal Services Decertification Program

Phase	*Meter Type*	*Status*
I	Mechanical meters	To be off market by 1999
II	Manually reset electronic meters	To be off market by May 2005
III	Rotary print head meters	To be off market by Dec. 31, 2006
IV	Security enhanced rotary printhead meters	To be off market by Dec. 31, 2008
V	Non-IBI digital print meters	Largest installed base in 2005, no current plans to schedule retirement dates
VI	IBI digital print meter	Currently preferred technology

meter resetting eliminates the need for physical postage meter keys that were used to manually reset meters [81].

In 2001, about 92% of the 1.6 million postage meters in the US market were switched to be reset remotely through a telephone connection. Manual resets of the remaining 145,000 postage meters were supported by US Post Offices until February 2005 and had to seize operation by May 2005.

By the end of phase III, rotary print head meters without further security enhancements had to stop operation by the end of 2006. Rotary print head meters with a built-in time-out mechanism that disables their printing if the last reset is more than three months ago have to stop operation by the end of 2008 (phase IV). The goal is to switch the entire market to the next generation of postage meters, i.e., *digital postage meters*. The *Postal Technology Management* (PTM) of the US Postal Services defined the new digital postage meters in their Information Based Indicia Program (IBIP), which was prepared in co-operation with Tygar, Yee and Heintze [78] of Carnegie Mellon University. We will take a closer look at the IBI program in Section 6.3 on page 128. The term "*indicia*" described a completely new form of digital postmark that includes a 2D bar code and replaces the traditional postmark and towncircle of a postage meter imprint (Figure 7 on page 13):

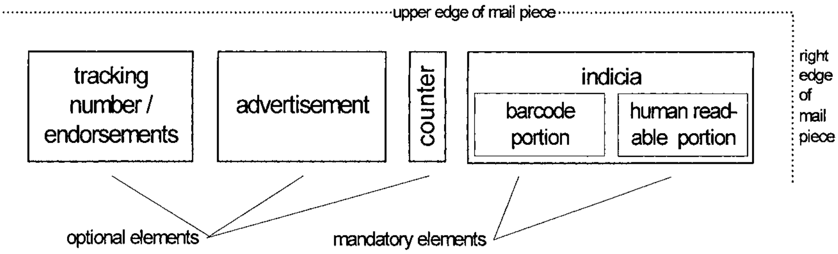


*Figure 7.*Layout of a Digital Postage Meter Imprint

The IBI Program was motivated by three key observations:

1. Computer technology provided a big potential to save manufacturing and maintenance cost of postage meters and thus mechanical postage meters would soon be on the decline.
2. Electronic postage imprints had to be authenticated by cryptographic means in order to become virtually unforgeable over the lifetime of a postage meter. The increased payload of information to be contained

in each imprint required to use sophisticated two-dimensional (2D) barcodes with small enough footprint on an envelope.

3. Digital postage meters were going to be refilled through means of telecommunications rather than through mechanical tokens from the Post Office as in the old days. It was obvious that a new generation of protection mechanisms had to be put in place because the existing locks and seals would not prevent fraud through the telephone line. Therefore, IBIP required a mandatory hardware security module complete with cryptographic engine and tamper protection and response mechanisms for each single postage meter.

The most advanced requirement in this program was that each postage metering device had to have a *hardware security module* embedded, which had essentially four tasks to fulfil: (i) Keeping the values of the postal registers in secure memory, (ii) securing the resetting process such that electronic postage can be downloaded over a telephone connection from an e-postage provider, (iii) producing unforgeable digital signatures to be included in each postage imprint to authorize its face value, (iv) ensuring digital signatures are produced only when the respective postal registers are properly updated. The hardware security module had to be tamper responsive in the following sense: If a user attempted to injure or bypass the physical housing of the hardware security module by mechanical drills, knives, sand blasting, chemical solvents, high or low pressure, or radiation, then appropriate sensors should trigger the erasure of all cryptographic keys necessary to produce valid digital signatures inside the module, while leaving the postal registers unchanged. This way, an attacker could not hope to misuse the module after an attack, while the postal inspection service had good chances to find forensic evidence of tampering at the module and possibly also the remaining amount of postage.

Since the new approach required each imprint to contain a digital signature of sufficient security, the imprints had to have an information capacity of about 90 bytes minimum. A feasible and cost-effective way of encoding this amount of information within an imprint between 1 and 2 square inches large is to use a *2D barcode symbology* such as PDF417 [37] or DataMatrix [39]. See for example Figure 8 on page 15. These 2D barcode symbologies require high precision printing technology at the mailer's side and similarly precise high-speed scanning and verification technology at the mail processing centers. Modern mail processing centers process these 2D barcodes at up to 36,000 pieces per hour. Implementing high speed bar code scanning equipment in all mail processing centers (AADC) throughout the US is a substantial investment. Moreover, each mail processing center needs to be

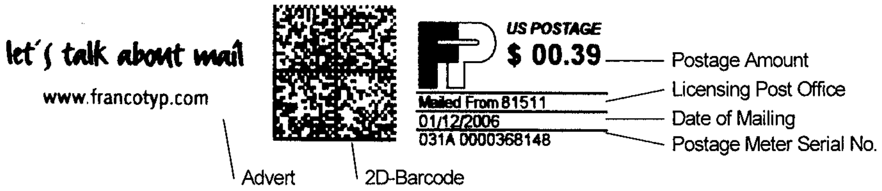


*Figure 8.*Sample Imprints for IBIP of the USPS

equipped with (i) the software to verify indicia, in particular the digital signatures, and with (ii) systematic checks for duplicate indicia and (iii) reconciliation means that check the balance between the postage volume being scanned and the postage volume being paid for. Deploying this postal verification backend and integrating it into the existing mail processing centers will take a decade or more since the IBI Program was launched.

An example that highlights how important it was to stop the operation of manually reset postage meters is the following fraud scheme of grand proportion forged by American Presort, Inc. (API), the largest pre sorter in New York City [106] in the early 1990's. The industrial facility in downtown Manhattan was processing 2.3m pieces of first class mail every day by using eight large Bell&Howell optical character sorters, each operating at 25,000 pieces per hour. In addition to pre-sorting, API offered its customers to determine for them the minimum amount of postage required and applying it. API used a few manually reset postage meters, which they had manipulated. One of the meters would print a dollar meter strip when it was set to zero meaning it did not account for any of these imprints. After some statistical analysis in 1996, postal inspectors ran a report comparing one of API's meters and found that, in the spring of 1997, one particular meter under suspicion had generated enough meter strips for roughly 120,000 pieces of mail a day over a three month period—about $30,000 worth of postage a day. Records for this meter, however, revealed it was last set on January 30, 1997, for $9,000. During the following investigation it turned out that API had manipulated some of their postage meters since the 1980's. U.S. Postal Inspection Service investigation of API concluded in July 2002 with sentences and restitution for its three owners and four of its managers, who knowingly committed more than $20 million in fraud against the US Postal Service.

Other large postal operators faced financial losses of similar proportions. in 1996, Deutsche Post was reported to have suffered a loss of DM 500m of revenue in 1995 from fraudulent activities in commercial letter shops, which was largely caused by false weighing and counting of mail pieces and to a smaller extent by postage meter manipulations [64]. One direct mailer in Dusseldorf-Lierenfeld with a daily turnover of 160 tons of mail defrauded Deutsche Post of DM 65m between 1991 and 1996 by using manipulated postage meters [121]. On top of that come revenue losses caused by re-used and counterfeited stamps. By 1995, the problem had become so significant that an internal revenue protection group (Entgeltsicherung—ESI) was installed inside Deutsche Post. In the upper 1990s, the revenue protection group at Deutsche Post designed, tested, and deployed the Frankit program (see Section 6.5 on page 151), a similar approach towards electronic postage as the IBI Program of the US Postal Services. Such fraud prevention programs will start to reduce postage meter fraud significantly when it becomes easier to identify and eliminate the manipulated meters. Given the exchange rate of postage meters of about 10% of the originally installed base every year, which has been experienced over decades in the German market, a significant decline of postage meter fraud can be expected after all bad meters have been removed from operation, because the manipulated postage meters are among the last to be replaced. The last replacements are expected around 2012-2014, i.e., 8 to 10 years after the introduction of Frankit.

1.4 THE RISE OF ELECTRONIC POSTAGE

The information-based indicia program of the US Postal Services was the beginning of secure electronic postage and it was an appropriate answer to the urgent security problems of postage meters at its time. It appeared when the underlying key technologies converged and reached industrial maturity, namely hardware security modules, efficient digital signatures and efficient 2D barcode symbologies. In 1994, the US National Institute of Standards and Technology (NIST) launched the Federal Information Processing Standard (FIPS) 140, which defined industry accepted security and testing requirements for cryptographic hardware security modules. NIST accredited the first independent test laboratories for testing modules against FIPS 140 [86,87] in 1994. In the arena of digital signatures, NIST adopted the digital signature standard DSS in 1994 [93,94], a suite of cryptographic algorithms to produce and verify digital signatures. In contrast to the then well-known RSA signature mechanism, the digital signature standard provided significantly shorter and faster to compute signatures at the same level of security, and it was not patented and therefore free to be used. The length of the digital signature is critical because it increases the footage of each indicia. The larger an imprint is, the longer it takes to compute, print, scan and verify it. The IBI Program allows two bar code symbologies, namely PDF417 and DataMatrix. The former is the long deployed standard in US Postal Services mail processing facilities, and the latter is an emerging standard so efficient in terms of error correction, information per square inch (at equal printing resolution) and recognition speed that it was in many ways the ideal choice for cryptographically secured indicia.

The IBI Program took effect in Jan. 1999 [100], and the US Postal Services approved the first electronic postage meter under the IBI Program, the Neopost IJ25, in April 2001. The IBI Program included postage meter systems, PC based postage systems and postage printing systems sharing a hardware security device over a wide area network. In each case, the underlying idea was to secure the entire cycle of electronic postage from the point of payment of the mailer up to the imprint verification at the mail processing centers. Postage meters were no longer seen as stand alone devices, which can be tested in isolation, but rather, the IBI Program looked at a postage meter or at a PC postage application as components in a larger *electronic postage system*. The IBI Program, for the first time, referred explicitly to a *server infrastructure* of the e-postage provider and required this infrastructure to be described and documented in order to apply for approval for a postage meter. According to the IBI Program, electronic postage occurs in two forms: (a) in electronic form transferred from an e-postage provider to a postage meter or PC and (b) as printed indicia containing a 2D barcode and a human readable description. The IBI Program is a large scale industrial application of public key cryptography, which will be addressed in more detail in Chapter 4 on page 91.

Propelled by a European directive towards postal liberalization in Europe, Deutsche Post started its own electronic postage program first in 2001 for PC postage systems, which is called Stampit, and in 2004 for postage meters, which is called Frankit. The first approval for a digital postage meter under Frankit was granted by Deutsche Post to the Francotyp-Postalia mymail and ultimail in April 2004. Frankit requires e-postage providers to document their server infrastructure, and imposes a detailed compliance test plan for the postage meter to be approved, its hardware security module and the supporting server infrastructure. In order to win approval for a postage meter, the entire system of the e-postage provider must be validated against these test plans. A sample imprint under the Frankit program is shown in Figure 9 on page 18.

An important feature of Frankit is motivated by the liberalization of postal markets in Europe: The complete capturing and reporting of usage data. Deutsche Post requires all postage meters under Frankit to completely record and report a statistics which postmarks it has printed to Deutsche Post. Deutsche Post thus builds up fairly accurate usage profiles for each postage meter, and thereby for each of their postal products, e.g, letters of certain weight catego-

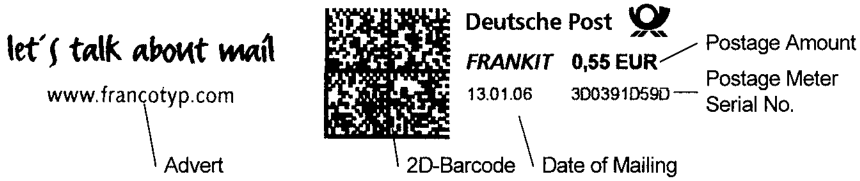


*Figure 9.*Sample Imprint for Frankit of Deutsche Post

ries, which will give them an edge in optimizing their product portfolio and pricing over competing postal operators in Europe in the future.

In 2006, there were three postal operators worldwide that had a secure electronic postage program with cryptographically secured indicia in place. They are the US Postal Services, Deutsche Post and Canada Post. Other postal operators pursue similar plans and will come out with their specific programs in the following years, for example, Netherlands Post and UK Royal Mail. Digital postage meters will gradually substitute traditional postage meters, but will hardly change the market shares of postage channels, which are quite similar throughout industrialized postal letter delivery markets. The following Table 2 on page 18 shows the typical ranges of market share per postage channel, namely postage meters, stamps, permit mail, and second class mail, such as unsolicited advertisement.

Table 2. Market share of Postage Paid Through Different Channels

Postal Market	*Postage Meters*	*Stamps*	*Permit Mail*	*Second Class*
Share of postage	45..55%	22..30%	25..30%	6..9%

The bulk of the postage paid for metered mail, permit mail, and second class mail originates from mid-size to large companies, while a smaller fraction of the postage paid for metered mail and about half of the postage paid by stamps originates from small to mid-size companies including small and home offices. The other half of the postage paid by stamps comes from consumers as summarized in Table 3 on page 18.

Table 3. Relative Mail Volumes in Industrialized Postal Markets

From	*To Consumer*	*To Business*
Consumer	5%	10%
Business	65%	20%

An additional incentive for electronic postage comes is the fact that stamped mail is hardly profitable for many postal operators if it is not a deficit business. For example, Royal Mail calculates that every stamped piece of first class mail cost them 5p and every piece of stamped second class mail cost them 9p. For this reason, Royal Mail grants a discount to customers who use electronic postage.

Secure electronic postage programs like IBIP and Frankit were the enabling framework for PC-based postage to enter postal markets. The pioneer of PC-based electronic postage was Salim Kara, co-founder of e-stamp. In March 1998, e-stamp won approval by the US Postal Services for the first product under the IBI Program that allowed to produce electronic postage using an off-the-shelf PC. Other companies launched similar PC-based electronic postage products under the IBI Program in the US. In Europe, PC postage products have been developed, branded and distributed primarily by the postal operators themselves. Actual figures show that online electronic postage is taking market share away from stamps, but not from other postage channels (see Chapter 7 on page 167).

In 2004, Los Angeles-based stamps.com received approval from the US Postal Services to distribute *customized stamps*, also called *personalized stamps*, throughout the US postal market. Customers can upload photographs of their choice to the stamps.com website and order one or more sheets of customized stamps, which show a tiny indicia and the customer's photographs and requested denomination(s). Stamps.com reviews the photos to prevent Internet pranksters from ordering stamps that feature images of controversial figures, such as Ted Kaczynski, Jimmy Hoffa and Slobodan Milosevic, which happened during an early trial.

Customers receive the ordered sheets of self adhesive stamps by mail. In contrast to PC Postage, buyers of customized stamps have no need to print anything themselves (see Figure 10 on page 19). Customized postage is likely to cut into the market share of traditional stamps, and is therefore attractive to

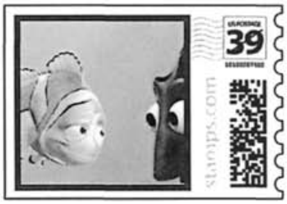


*Figure 10.*Specimen Customized Stamp (Courtesy of stamps.com)

postal operators who seek for ways to reduce the losses they make on providing traditional stamps by offering value-added services.

We summarize the terminology related to electronic postage in the following Table 3 on page 18.

Table 4. Terminology related to Electronic Postage

Printing Device	*Postage*	*Imprint / Postmark*	*First ever example*
mechanical / electro-mechanical meter	traditional	traditional postage meter imprint	Pitney-Bowes Model M
electronic meter	traditional	traditional postage meter imprint	Francotyp-Postalia T1000
digital meter PC postage client customized stamps	secure electronic also called digital	indicia	Neopost IJ25 e-stamp stamps.com

1.5 ADVANCING POSTAL MARKETS

Since the US Postal Services started their IBI Program, other postal operators adopted the approach towards secure electronic postage. In addition to preventing fraud through manipulated postage meters, postal operators have other specific motivations to move their markets in this direction.

1.5.1 Postal Security

The goal of postal security was recognized at the 20th world congress of the Universal Postal Union held 1989 in Washington D.C. Following this event, a Postal Security Action Group (PSAG) was created to aim at (a) preventing injuries to people due to dangerous goods in the mail including to combat chemical and biological warfare by terrorists (b) preventing the loss or theft of mail entrusted to postal operators, (c) preventing postal revenue or assets from being lost or stolen, and (d) preserving customer confidence in postal operators.

In the US, the terrorist attacks of Sep. 11, 2001 and a series of letters that were contaminated with anthrax spores in 2001 and 2002 resulted in the homeland security act of Nov. 2002, which called for more reliable sender identification and more secure mail transport. Clearly, metered mail contributes to these goals because meter users must get registered by the postal operator before they can meter their mail.

1.5.2 Postal Liberalization

In Europe, the postal operators are faced with a long term strategy of the European Union to liberalize the national postal markets. By 2007, the market for letter mail shall be fully opened to competition. As letter mail is the major source of revenue and profit for most if not all European postal operators, they are all working to defend their home markets against competitors, be they foreign *universal postal operators*, foreign *private postal operators* or domestic private postal operators. Secondly, European postal operators have an increased interest to optimize their portfolio of rate categories. They want to learn how frequently their rate categories are used. Thirdly, European postal operators embrace metered mail because postage meters maintain their customers' loyalty through the initial investment they make, and postage meters provide a cost efficient way of feeding the usage data directly back to the respective postal operators.

For similar reasons, many postal operators encourage Internet based electronic postage. These PC-based products target the market of small and home offices (SOHO) who find even low-cost postage meters too expensive. For some customers, Internet based electronic postage integrates nicely into their production of letters, flats or parcels.

Japan Post, holding about $3 trillion in savings, is probably the world's largest financial institute. After decades of political debate, both lower and upper house of the Japan government decided in October 2005 to privatize Japan Post in order to deal with the prospect that gigantic amounts of pensions need to be paid when the baby boomer generation is going to retire. The government approved plan is to transform Japan Post by 2008 into four separate business units under a holding company wholly owned by the state. The business units are postal services, savings services, life-insurance services, and window networks (post offices). Until 2017, the privatization shall be completed through sales of government-held shares. The new Japan postal services business unit will face a similarly competitive environment as the US and European postal operators do and is likely to protect its own home market by its own secure electronic postage program.

Worldwide, the market of postal services was US$260 billion in 2003 [109,110,111]. The industrialized countries, i.e., Australia, Canada, Israel, Japan, New Zealand, the European Union, and the United States, make up for 91% of the worldwide postal market (US$237 billion). This fraction of the worldwide postal market is segmented into

1. letter mail, which accounts for 60% of the revenue (US$142 billion),
2. parcels and express mail (25% or US$59 billion),

3. postal financial services (12% or US$29 billion) and
4. other services (3% or US$7).

The following Table 5 on page 22 compares the domestic first class letter mail market of the industrialized countries:

Table 5. Comparison of Universal Postal Operator Markets in 2003

Universal Postal Operators	*Letters delivered [billion pieces]*	*Letter revenue [billion US$]*	*# postage meters [1000 pcs]*
United States	99	37	1654
Canada	11	6	128
European Union (25 states)	90	66	969
Germany	19	16	238
United Kingdom	20	12	213
France	17	13	260
Italy	6	5	24
Netherlands	5	5	54
Remaining EU member states	23	15	180
China	28	0.6	9
Japan	25	15	25
India	9		22
Australia and New Zealand	5	3	30

1.5.3 Competitive Postal Operators

Competition among the universal operators and the *competitive postal operators* is increasing in many regions of the world. On a worldwide average, the *universal postal operators* hold 96% of the domestic letter mail market and 80% of the international letter mail market. Traditionally, the service of parcel delivery has not been reserved to universal postal operators. Here, competitive postal operators hold a 72% share in domestic parcel delivery and an 80% share in international parcel delivery [109].

Where letter mail markets are deregulated, competitive postal operators make inroads to this market segment as well. But while the letter mail delivery service of universal postal operators is usually exempt from sales taxes, that of competitive postal operators is usually not. These unjust market conditions impede many competitive postal operators to increase their market shares, even in postal markets that have been deregulated for several years. Some competitive postal operators like RIDAS in Germany (http://www.ridas.de/) issue their own stamps, and others like the DX B2B mail delivery services in the UK (http://www.thedx.co.uk/) encourage their customers to use postage meters to produce pre-paid imprints just as for letter mail sent through universal postal operators.

The larger the volume of a competitive postal operator becomes, the more similar are its economic and security requirements to those of universal postal operators. It is conceivable that growing competitive postal operators will introduce similar electronic postage technologies that we know from universal postal operators today.

1.5.4 Postal Presorters

In liberalized postal markets, the universal postal operators must open up their postal delivery network to presorted mail and deliver it to the recipients at discounted rates. Some competitive postal operators provide this *physical presorting service* of collecting mail, pre-sorting it, and bundling it into large quantities of mail with similar destination and optional calculation and application of optimized postage.

A more advanced service is *electronic presorting*, sometimes called *hybrid mail*. An electronic presorter provides a web-based service to its mailers. Instead of printing documents, mailers use this web service to send their documents in electronic form to the electronic presorter. The electronic presorter routes the electronic documents to a print center located close to the respective destinating mail processing center of the universal service provider. The print center prints the documents, folds and inserts them, applies the correct amount of postage onto the envelopes, and feeds them to the destinating mail processing center.

Some postal operators like the US Postal Services and Canada Post grant discounted rates for presorted mail. Others like Deutsche Post ask equal rates for presorted as for unsorted mail and reimburse a presort discount to the mailers on a monthly basis after the mail is delivered.

1.5.5 International Mail

The Universal Postal Union established a practical system of cross border mail delivery that was based on the weight of mail volume exchanged. In an international postal delivery network, each postal operator gets a certain amount of incoming mail from other postal operators, but it can usually not verify the validity of individual stamps and imprints on incoming international mail. The Universal Postal Union therefore ruled that the originating postal operator would compensate the destinating postal operator according to the weight of the exported mail volume. The 200 or so national post offices pay each other monthly settlements based on the relative volumes of mail in each direction. Of any two postal operators, the one who exported the greater mail volume had to compensate the difference to the other. The *terminal dues* to be paid for each ton of outgoing cross border mail were revisited and fixed by the Universal Postal Union on a regular basis and there was one clearing-house for all postal operators, the *International Post Corporation* (IPC). One of the problems of this system was that postal operators had no incentive to deliver imported international mail just as promptly as their domestic mail. The Universal Postal Union addressed the issue by tying the terminal dues of each postal operator more closely to their actual cost of mail delivery. A monitoring system run by the International Post Corporation was setup that verifies the quality of international mail delivery of the participating postal operators. Those who do not meet the quality targets get reduced terminal dues for their delivery services.

1.6 OUTLOOK

Statistics show that no significant fraction of physical mail is going to be substituted by electronic communication like facsimile or electronic mail any time soon. Although there is a slight decrease in first class letter volume since the early 2000s, there is an average increase of world-wide mail volume of about 1% per year. Some statistics indicate that households with high bandwidth connection to the Internet receive more physical mail than others. The share of metered mail is likely to remain constant, while the share of digitally metered mail and Internet based electronic postage is likely to rise.

It is conceivable that Internet-based electronic postage products and customized stamps gain market share by replacing stamps, because these products are more convenient to use for Internet-savvy mailers and more economic for postal operators.

As postal delivery networks in liberalized postal markets are opened up for growing volumes of pre-sorted mail, there is an increasing risk of misuse. Blackmailed employees of physical presorters may try to inject unpaid mail into the postal operators' networks. Electronic postage bears the potential for postal operators to detect and reject illegitimate insertion of mail into their postal delivery networks.

Chapter 2

Electronic Postage Systems

2.1 GENERAL MODEL OF E-POSTAGE SYSTEMS

Electronic postage is a special currency valid only for postal transportation of mail pieces and related additional services. The minting and printing of electronic postage is mostly regulated by national universal postal operators. The rules and regulations for using electronic postage differ from one country to another. Any electronic postage system needs an *e-postage minting system* where mailers can purchase electronic postage and pay for it. All such electronic postage can be turned into valid imprints, which can be applied to physical mailings, thus providing evidence to the postal operator that the mailer has paid for the transport of a mail piece. The postal operators in turn can reconcile the amount of electronic postage they have sold against the amount of electronic postage they have processed through their mail processing centers. This constitutes the basic cycle of electronic postage as shown in Figure 11 on page 26. We will now take a closer look at this cycle.

2.1.1 E-Postage Devices

Mailers need *e-postage devices* in order to acquire electronic postage and apply it to their mailings. An e-postage device is called *offline* if it can download an amount of electronic postage in advance, store it and then produce imprints upon request of the mailer. Offline e-postage devices connect to an *e-postage minting system* by some communication network to perform a so-called *postage value download (PVD)*. The typical example for an offline e-postage device is a digital *postage meter*, also called *postage evidencing device*. Traditionally, postage meters have connected to an e-postage minting system by modem through a telephone network or a cell phone network. Former postage meters that were not yet equipped with modems required their users to enter appropriate pass-codes that the mailers had to obtain from an operator at the e-postage minting system in the first place.

Postage devices are called *online*, if they need to contact the e-postage minting system every time they produce a postage imprint for a mail piece. Online e-postage devices do not download and store electronic postage in advance. They usually connect to the e-postage minting system through the Internet. Online e-postage devices can be convenient to use for small offices where the printing speed of imprints is not essential.

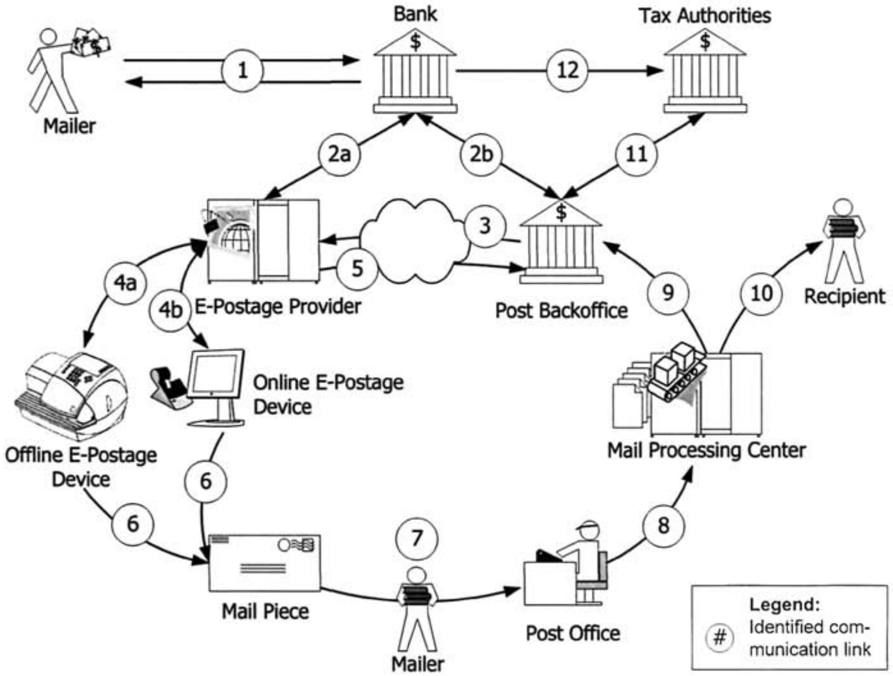


*Figure 11.*Cycle of Electronic Postage

Contemporary examples of online e-postage devices are PC postage clients and label printers, each with a broadband Internet connection.

A third type of e-postage device can be called *one-time* e-postage device because it is pre-loaded with some amount of postage by the manufacturer, can produce imprints upon request of the mailer, but cannot be refilled. Once its preloaded postage is consumed, the device is of no use to the mailer any more. It can be disposed of or returned to the vendor for example to be refurbished or recycled. One-time e-postage devices are not commercially available as of 2006.

Another common way of classifying e-postage devices is into open and closed systems [100,101,102]. An e-postage device is called *open* if it consists of standard hardware components such as a regular personal computer (PC) connected to an office printer through some standard (openly specified) communication interface such as Ethernet, USB or parallel port. A *closed* e-postage device is a system whose basic components are dedicated to the production of imprints and related functions, similar to an existing, traditional postage meter. A closed system, which may be a proprietary device used alone or in conjunction with other closely related, specialized equipment, includes its indicia print mechanism.

The above classifications of e-postage devices complete with examples is summarized in the Table 6 on page 27:

Table 6. Classification of E-Postage Devices and Examples

	special purpose hardware *closed system*	*general purpose hardware* *open system*
offline	digital postage meter [100]	• PC postage client with PC "dongle" [101]
online	not commercially available	• PC postage client with label / office printer and Internet connection [102], • Standalone label printer with Internet connection
one-time	not commercially available	• not commercially available

From the postal operators' point of view, e-postage devices are operated in a potentially unfriendly environment by per-se untrusted mailers. Thus, postal operators require e-postage devices to be given a unique identity and to maintain this identity in an unforgeable way throughout their life time. Some postal operators require the device identity to be maintained over the life-time of the e-postage device, while other postal operators require to use a new e-postage device identity every time the e-postage device is registered to a new mailer. The former approach is more common in markets where e-postage devices are leased (US, Canada), the latter approach is more common in markets where e-postage devices are purchased (Europe).

2.1.1.1 Registering an E-Postage Device

In order to hold mailers responsible for all operations of their e-postage devices including potential misuse, all postal operators require mailers to sign a contract and to register each e-postage device before they are allowed to operate their e-postage devices. During the postal registration process, the mailer's (business) name and address is recorded together with their e-postage device's model description and identity. Mailers may be denied a contract, for example, if they have a bad customer history with the postal operator or if they have an insufficient credit rating. Since offline e-postage devices are capable of franking larger amounts of mailings, mailers are required to deposit these mailings at their post office rather than in a private or public post box. (By having metered mail inducted at their post offices, the postal operators can steer metered mail past their facer canceler systems because these imprints need not be cancelled.) Mailers choose their *inducting post* *office* (also called *licensing* or *depositing post office*) when they register their e-postage devices. Mailers using an online e-postage device can deposit their mail into private or public post boxes.

In addition to the contract with the postal operator, the mailer needs to settle a service contract with the e-postage provider of the e-postage device. The service contract includes details on which conditions the e-postage device is purchased or leased and about the fees for servicing the e-postage device through the e-postage provider. Under the service contract, the mailer can usually design an individual advertisement or choose from a selection of predefined ads and have the e-postage provider produce the selected ads into a format usable by the mailer's e-postage device. Usually, the e-postage provider also manages the postal registration process for the mailer as part of the service contract.

2.1.2 E-Postage Minting System

E-postage devices are supported by an *e-postage minting system*, which consists of one or more *e-postage providers* (see link 4) in Figure 11 on page 26), a bank and the *post backoffice* of the postal operator of the respective country or market (see Figure 12 on page 28). Each e-postage provider serves as a gateway between its e-postage devices, the bank and the post backoffice. Traditionally, the manufacturers of e-postage devices serve as their own e-postage providers. Each e-postage provider receives information from the post backoffice (link 3 in Figure 11 on page 26) and passes it on to its registered e-postage devices. Likewise, the provider receives requests for e-postage from its e-postage devices and reports them to the post backoffice (link 5). In traditionally regulated postal markets, postal operators provide a

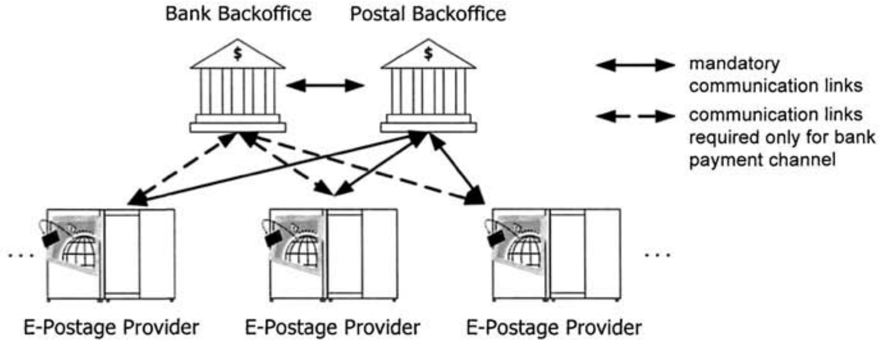


*Figure 12.*Communication Network of an E-Postage Minting System

universal and exclusive postal service. Where this situation changes due to postal liberalization, privatized postal operators develop their own postal delivery business, and mailers in that region are likely to demand for *multi-carrier e-postage devices*, i.e. e-postage devices that are registered to more than one mail carrier. This will allow mailers to choose the postal operator best fitting their requirements on price and delivery conditions.

2.1.2.1 Payment Channels with Bank and Tax Authorities

The e-postage provider system is connected to a banking system, which provides one or more payment methods through which mailers can pay for their electronic postage. Some postal operators allow the e-postage provider to be connected to the banking system directly (see link 2a). In this case we say that the system offers a *bank payment channel.* It is established by direct communication links between the bank backoffice and each e-postage provider (see the dashed communication links in Figure 12 on page 28). Other postal operators require the payment channel to be routed through their own post backoffice (see link 2b). In this case, we say the system offers a *postal payment channel.*

In either case, all e-postage providers need to report all payment related transactions of all online and offline e-postage devices to their e-postage provider in a daily transactions report. If an e-postage provider uses a bank payment channel, then the bank transfers all customer payments to the respective account of the postal operator, who utilizes the daily transaction reports received by its post backoffice to verify all payments received.

In some markets, postal services are generally exempt from sales tax (US). Other markets exempt only basic postal delivery services or postal services of universal postal operators who are obliged to serve all households, including those in rural areas (European countries), and some markets observe no tax exemption of postal services at all (Canada).

In all markets, sales tax is due by the time electronic postage is downloaded into an e-postage device. Thus, the e-postage providers need to report to their respective post backoffices the total amounts of e-postage downloaded by their e-postage devices on a daily basis. The report must indicate a total amount for each applicable sales tax. It is the postal operator's duty to forward the collected amounts of sales tax to the state and/or federal governments of its country (see link 11). Finally, the bank initiates the respective tax payments to the tax authorities (see link 12).

2.1.2.2 Methods of Payment by the Mailers

Mailers can typically choose from different payment methods for their electronic postage (see link 1). All of these payment methods make sure that the postal operator is paid for providing electronic postage either before or at most a few days after a postage value download is completed. Thus, even if mailers do their postage value downloads on the day they induct their mail, the postal operator will receive his postage fees no later than one or two days after he has delivered the mail at the recipient address. In some countries, national legislation mandates prepayment for postal delivery services in general. There are basically two types of payment methods for offline e-postage devices:

(a) *pre-download methods*, where the mailers need to transfer money into some dedicated account at a bank before they can download e-postage into their e-postage devices. Examples are by check, automatic clearing house debit (ACH-debit deducts funds from the mailer's account on the next business day). At the end of the day, the bank notifies the e-postage provider (link 2a) or the bank notifies the post backoffice (link 2b) about the mailers' payments. The respective mailer can, typically on the next business day, download any amount of electronic postage up to the paid total. Pre-download methods of payment are most appropriate for offline e-postage devices.

(b) *Post-download methods*, where mailers can download any amount of e-postage from the e-postage provider into their e-postage devices (up to a maximum amount that depends upon each mailer's credit rating). The e-postage provider generates postage download reports on a daily basis, and feeds them either directly (link 2a) or through the backoffice system of the postal operator (link 2b) to the respective bank. Upon receipt of these download reports, the bank bills or debits the respective mailers (link 1). The bank finally settles all the payments. Examples are by direct debit card, by invoicing or by automatic clearing house debit.

For either payment method, the mailers might have an option to use a credit line with their bank (e.g., credit card) or with their e-postage provider (advance payments). The fees for such advances are put on the mailers' monthly invoices or get paid by credit card.

Online e-postage devices usually have a smaller throughput of e-postage than offline e-postage devices. To mailers using online e-postage devices the postal operators are usually willing to grant some credit limit. The following types of payment methods are offered for online e-postage devices:

(c) *monthly invoice*, where the e-postage provider runs an individual account for each mailer and keeps in it a record of all online imprints produced by the respective mailer. At the end of each accounting period, the mailer is charged or billed for the sum of all postage imprints produced in the recent accounting period. Typical accounting periods are months or quarters.

2.1.2.3 Communication Interfaces

In most countries, each e-postage provider operates its data center at its own site, which is separate from the location where the postal operator runs its post backoffice. In this case, the e-postage providers usually connect their data centers to the post backoffice through the Internet (see Figure 12 on page 28). The result is a wide-area star shaped network secured under the *point-to-point security paradigm*. That is, each bilateral connection is protected individually, for example, by a virtual private network (VPN), or by application layer encryption such as Gnu Privacy Guard (GPG) [72] on top of a file transfer protocol (ftp) or other proprietary bulk transfer protocol. The respective encryption keys must be properly generated, distributed, and maintained between the post backoffice and each e-postage provider.

In postal markets where the postal operator requires a bank payment channel, the e-postage providers are also connected to the bank backoffice by a star shaped network, and the above security considerations apply to it as well.

In order to require not too much availability from the post backoffice, the bank backoffice and from the Internet connections, the backoffices are usually operated in *batch mode*: The e-postage providers collect service requests of their e-postage devices and bundle them into one batch of requests at the end of a business day or other accounting period before submitting them to the backoffices. The backoffices then return their batches of requests and responses.

This batch mode causes an inherent delay between the information available to the e-postage provider and to the backoffices. For example, an e-postage provider cannot check available balances at the backoffices online. Instead, the e-postage providers usually maintain *credit limits* for each e-postage device based on the customers' payment profile, which is obtained regularly from the post backoffice if e-postage providers run a post payment channel, or from the bank if they run a bank payment channel.

In some countries like Belgium, the postal operator contracts the e-postage providers to have their data centers hosted in the same physical location where the post backoffice is located. In this case, the e-postage providers' data centers can be connected to the post backoffice by a local area network. This local area network can be secured under the *perimeter security paradigm*. That is, the network facility has strong site security measures in place, but within that facility the communication links from each e-postage provider data center to the post backoffice are not encrypted individually, if at all.

In this setting, the post backoffice and the communication network can be assumed to be highly available which allows to operate the post backoffice in *online mode*: The e-postage providers forward their requests for electronic postage for all e-postage devices online to the post backoffice, which returns its electronic postage replies immediately. As a result the funds available at the post backoffice can be requested in real-time.

2.1.2.4 Withdrawing an E-Postage Device

When a mailer wishes to return his e-postage device, for example, to upgrade to another model, the e-postage provider terminates the respective service contract and postal registration at the next possible date.

An important part of terminating the postal contract is to withdraw the e-postage device from service by putting it into a state where it can no longer produce imprints or download electronic postage. Before an offline e-postage device is withdrawn from service, the remaining electronic postage must be refunded to the respective mailer. This can be done by a *postage value refund*, which is a 2-party transaction similar to a postage value download, but such that the e-postage provider learns the last value of the descending register of the e-postage device, and the e-postage device ends up with its descending register reset to zero, indicating that no electronic postage remains in the e-postage device. Online e-postage devices support no postage value refund because they do not store electronic postage.

Afterwards, the e-postage device is switched into a non-operational state, in which it accepts no commands other than being re-initialized to a new mailer (and a few commands for maintenance and inspection purposes). Usually, postal operators do not offer a refund option to mailers unless a mailer terminates a contract for an e-postage device.

When an e-postage provider has received a postage value refund request from an e-postage device (link 4), it feeds the request forward through the applicable payment channel. Finally, the bank credits the mailer's account or makes a check out to the mailer (link 1).

2.1.3 Indicia

Once the mailer has downloaded electronic postage, the e-postage device can start to produce postage imprints (link 6). The user enters the required input parameters and the actual weight of the mail piece, which can be determined by a scale or can be input manually by the user, the e-postage device displays the correct amount of postage, builds the postage imprint image and prints it onto the mail piece (see Figure 7 on page 13). Various rules and restrictions apply to the process, to the layout, and the content of indicia in each country. The use of a postage meter or PC postage client for managing and printing electronic postage is a security-critical process that requires profound security measures, which will be described in Chapter 4 on page 91.

Most postal operators require indicia to contain at least the following information in the 2D barcode of the indicia:

1. The location and postal code of the licensing post office,
2. the serial number of the e-postage device,
3. identification of the e-postage provider,
4. the date of mailing,
5. a reference to the respective postal operator,
6. the class of mail and presort level if applicable,
7. the postage amount, and
8. a *cryptographic checksum* over the above information (see Section 4.4 on page 98).

The human readable portion of the indicia usually displays a subset of this information and sometimes additional human readable information, for example a few keywords indicating the class of mail.

2.1.3.1 Barcode Symbology

Currently established industry e-postage systems require the indicia to contain between 14 bytes (United States) and 172 bytes (Canada) of information. Only a few barcode symbologies are efficient enough to represent this amount of information in the upper right corner of an envelope where not much more than 1 square inch of space is available. The de-facto standard barcode symbology supported by all postal operators that have established industrial scale e-postage systems by 2006 is the Data Matrix Symbology, which was invented by RVSI Acuity CiMatrix, a division of Robotic Vision Systems, Inc.

The encoding and decoding process of Data Matrix is complex and several methods have been used for error correction in the past. The postal operators prefer ECC200 from the ANSI/AIM BC11 and ISO/IEC 16022 specifications. ECC200 is the newest and most common version of data matrix error correction. It supports advanced encoding and error detection with Reed Solomon error correction algorithms. They allow to recognize barcodes that are up to 60% damaged.

Standard DataMatrix barcodes consist of solid colored and white squares, which are called *cells*, *elements*, or *cubes*. The width and height of a DataMatrix barcode can vary in defined steps from minimum 10 by 10 cubes up to maximum 144 by 144 cubes, with respective capacities of 1 byte up to 1556 bytes. Common sizes of DataMatrix barcodes used for postal indicia range from 12 by 26 cubes (14 byte capacity) to 48 by 48 cubes (172 byte capacity).

Another barcode symbology supported for indicia by some postal operators is PDF417. Each symbol consists of at least three rows of linear barcodes stacked upon each other. PDF417 symbols are the dominant symbology used by offline and online e-postage devices in the US.

2.1.4 Mail Processing and Verification

After a piece of mail has been inducted the respective postal operator is to forward, verify, sort, distribute and deliver it. Since indicia are dated and indicate the location of the source (licensing post office in case of offline e-postage devices) or the date and destination postal code (in case of online e-postage devices), they need not be canceled like stamps. At the end of the day, the mail pieces from all post offices and mail boxes in a region get collected by the *originating* mail processing facility. Stamped mail is detected and stamps are cancelled automatically. The face of each piece of mail is scanned. The recipient address and the indicia are extracted and interpreted separately. Each indicia is decoded and its cryptographic checksum is supposed to be verified. Furthermore, each indicia is checked for duplicates in order to detect attempts of postage fraud by copying. Real mail processing centers achieve verification rates between 40% and 90%.

Next, the mail pieces are sorted by their destination postal codes. All containers of mail whose respective destination postal code is less than 200 miles (US Postal Services) away from the originating mail processing center is transported directly to the destinating mail processing center. All other containers take a more complex route usually by airmail. At the destinating mail processing center, the mail pieces are automatically sorted by delivery sequence, and finally, they are delivered to their recipients (see link 8). Some postal operators have automated the entire sorting and distribution process down to delivery sequence level and achieve an automation rate of up to 90% of all letter mail. Parcel mail sorting and distribution is generally less automated, probably because of lower volumes [26].

The postal verification center archives all scanned images of indicia for some time. The postal operator runs a continuous statistical analysis on the scanned images and reconciles them with the statistics provided by the post backoffice (see link 9). In order to discover any potential loopholes in the cycle of electronic postage, the postal operator matches the amounts of postage received by the postal verification center against the respective amounts of postage produced by the post backoffice.

2.1.5 Multi-Carrier Capabilities

In liberalized postal markets, there are several postal operators (*carriers*), including private ones. For example, there are several parcel carriers worldwide such as UPS, Fedex, and DHL. The same applies to the letter post market where it is liberalized. Each postal carrier operates its own mail processing centers. If each e-postage provider supports only one postal operator, then the users of e-postage devices can use only that postal operator. This scenario applies to most e-postage devices today. Effectively, several e-postage systems as shown in Figure 11 on page 26 co-exist independently. However, e-postage providers may support more than one postal operator, thus giving their mailers the option to select the most suitable postal operator for each piece of mail. Multi-carrier e-postage devices are the natural answer to liberalized postal markets, because they allow mailers to optimize their postage total without leasing or purchasing several e-postage devices. For offline e-postage systems, it is natural to design postal security devices that can handle pre-paid e-postage for several postal carriers and produce the respective sorts of indicia.

2.2 E-POSTAGE DEVICES

Because postal operators entrust mailers and e-postage providers to handle a significant portion of their revenue, they impose strict security requirements on any e-postage devices and on the data centers of e-postage providers. Postal operators require each new model of e-postage devices to be approved before it may be distributed and used in their postal market (see Chapter 10 on page 207).

2.2.1 Interface to E-Postage Provider

The postage meter business has been and still is a highly regulated and relatively small niche market divided among a few manufacturers, which have built up considerable intellectual property portfolios over several decades. This oligopolist market has encouraged and protected proprietary communication interfaces between offline e-postage devices and their e-postage providers. Users of postage meters have no choice, there is only one e-postage provider available for each postage meter, namely its manufacturer.

Traditionally, the communication interface of closed e-postage devices has been a small bandwidth modem line. Open e-postage devices connect to their e-postage providers through the Internet. As of 2005, it is common for all vendors of e-postage devices to define and operate their own proprietary service interfaces, and so the customers of e-postage devices have exactly one e-postage provider to choose from, namely the respective vendor of their devices.

The service interface between an e-postage device and the e-postage provider is a message based communication interface supporting simple message transfer and interactive 2-party transactions. Examples for simple message transfers are the download of a new rate table from the e-postage provider into the e-postage device or the upload of a usage profile from the e-postage device to the e-postage provider. An example of an interactive 2-party transaction is a postage value download.

A simple message transfer may require *data and origin authentication* by the recipient depending on how security-critical the transferred messages are. Data and origin authentication means that the recipient, who knows the sender by some cryptographic key in the first place, can verify that the sender is in fact who he claims to be and has sent the received message. This is achieved by a cryptographic checksum. In addition, a simple message transfer may require data *confidentiality*, although this is a rare requirement in the service interface of an e-postage device. This can be achieved by using an encryption mechanism.

An interactive transaction usually requires *data and origin authentication* by either party and *semi-atomicity*. Ideally, a 2-party transaction achieves *atomicity*, meaning, it occurs either completely such that both parties reach a state in which they have acknowledged completion, or both parties reach an error state from which they reset into the same state as before they started the transaction. This ideal requirement cannot be achieved over an unreliable connection, where for example, the mailer can interrupt the communication line at any time. What can be achieved is the weaker requirement of semi-atomicity, which means whenever the e-postage provider aborts the transaction, the e-postage device must never complete it successfully. A semi-atomic transaction guarantees that the mailer keeps an interest in succeeding the transaction in order to re-synchronize the internal states of the e-postage provider and the mailer's e-postage device.

An interactive transaction may as well require confidentiality of some messages that are exchanged during the transaction, but this is a rare requirement.

2.2.2 Storing Electronic Postage

Offline and one-time e-postage devices store their electronic postage in *postal registers*. Postal registers have proved to be a simple and robust design concept, which is required by most postal operators to be used also for digital e-postage devices. There are four postal registers, the *ascending register*

(AR), the *descending register* (DR), the *total settings* register (TS), which is sometimes called *control total*, and the *piece count register* (PC). These four postal registers are the book-keeping means of each e-postage device from the day its identity is registered by the postal operator until the day its identity is unregistered.

1. The *ascending register* (AR) always represents the sum of all imprints produced by the e-postage device. Every time an imprint of face value x is produced, the ascending register is increased by x.
2. The *descending register* (DR) always represents the amount of postage remaining in the e-postage device. Every time an imprint of face value x is produced, the descending register is decreased by x, and every time a postage value download of value y is performed, the descending register is increased by y.
3. The *total settings register* (TS) always represents the sum of all postage value downloads. Every time a postage value download of value y is performed, the descending register is increased by y. At any point in time, the register of total settings must obey the following equation: $\text{TS} = \text{AR} + \text{DR}$. A violation of this equation indicates that the e-postage device has entered an inconsistent state which means it no longer manages electronic postage correctly. Postal operators require that this integrity constraint shall be checked before each imprint. If it is found to be violated, the e-postage device shall produce no more imprints and shall perform no more postage value downloads before an inspection has recovered the e-postage device from its inconsistent state.
4. The *piece count register* always represents the number of imprints produced by the e-postage device. The piece counter is increased by one every time an imprint is produced.

Online e-postage devices do not download electronic postage in advance and have no need to store electronic postage internally, because they use the concept of *virtual postal registers*, which are maintained remotely by the e-postage provider system.

2.2.3 Computing Secure Indicia

Many postal operators do not (yet) require individually secured indicia. Those who do, require a cryptographic checksum that enables the mail processing centers to verify if an indicia scanned during the sorting process has been produced by a registered e-postage device.

Offline e-postage devices that produce individually secured indicia must compute the corresponding cryptographic checksums internally with sufficient speed. To do so, they need to keep an individual cryptographic key, which we call *indicia key*. The indicia key must be kept secret inside the e-postage device. Anyone who uncovers the indicia key would be able to compute valid imprints complete with cryptographic checksums on any PC. To complete this kind of fraud, he only had to produce printouts with the right kind of ink (color, fluorescence).

Online e-postage devices that produce individually secured imprints receive a digital representation of their imprints from the e-postage provider online. The indicia key is stored and maintained by the e-postage provider, and the imprints complete with cryptographic checksum are computed in a trusted environment at the e-postage provider.

The cryptographic checksum can be a digital signature or a message authentication code. The contents of indicia are not standardized across different postal operators and neither are the cryptographic checksums used.

2.2.4 Postal Security Devices

In order to harden the security of offline e-postage devices, some of the major postal operators such as the US Postal Services, Canada Post, and Deutsche Post have started to require that each offline e-postage device must have a hardware security module embedded that implements the above three security-critical tasks, i.e., storing electronic postage (see Section 2.2.2 on page 36), securing the communication with the e-postage provider (see Section 2.2.3 on page 37) and securing the computation of indicia, i.e, storing the indicia key and computing the cryptographic checksums (see Section 2.2.4 on page 38).

This hardware security module is called a *postal security device* (*PSD*). It is physically secured against attempts of tampering and reading out private cryptographic keys such as the indicia key. Vendors of offline e-postage devices are free to use commercially available hardware security modules or develop their own ones, as long as the postal security device is security evaluated at an overall level 3 under the FIPS 140-2 standard. Some postal operators additionally require a level 4 rating in the FIPS 140 category of environmental failure protection and testing (EFP/EFT) (see Chapter 10 on page 207).

From the point of view of the postal operators, postal security devices are the secure wallets of their offline e-postage devices. As such, they require e-postage providers to uniquely identify the postal security devices such that each PSD identity can effectively serve as the main identity of its e-postage device. The e-postage device without an embedded PSD is usually called the *mail-handler*. A mail-handler can be repaired, refurbished or replaced completely, while the postal security device holding the e-postage remains unaffected. Postal operators therefore tend to associate the serial number of an e-postage device primarily with its PSD, meaning that the serial number remains unchanged even if the entire mail-handler is replaced.

The use of postal security devices in offline e-postage devices has proved so successful in postal markets that require individually secured indicia that some vendors employ them also in markets that still use conventional imprints without cryptographic checksums. In these markets, the postal security devices implement only the functions of storing electronic postage (see Section 2.2.2 on page 36) and in some cases of securing the communication with the e-postage provider (see Section 2.2.3 on page 37). Although postal security devices incur an additional cost for each e-postage device, the security evaluation of each new model of e-postage device becomes more streamlined and focused and, therefore, less expensive and time-consuming.

2.3 VALUE ADDED SERVICES

In the previous section, we described the basic model of electronic postage systems, which comprises security-critical services and functions. In addition, electronic postage systems bear a lot of potential for value-added services and functions to benefit mailers, e-postage providers and/or postal operators. These value-added services are not security-critical, but some of them are considered security-sensitive.

There are value-added services that integrate the e-postage services closer into the mailer's workflow or enhance the convenience or usability of a mailer's e-postage device. We call them *mailer's value-added services*. Implementations of mailer's value-added services usually do not require approval by the respective postal operator. Here are some examples of mailer's value-added services:

- An often requested service is the use of envelope ads or slogans to the left of the postmark. Almost every business using e-postage devices, be it online and offline, asks for such a service to differentiate its own business mail from others. Some e-postage providers allow their customers to send in their envelope ads electronically, others have them sent by conventional mail.
- Another often requested service is the option to setup a number of cost accounts and to manage electronic postage through separate cost accounts, for example, one per department.

- Connectivity of e-postage devices is a key feature. Offline e-postage devices can be connected to certain peripheral devices such as inserters, feeders, and dynamic scales that weigh while the mail pieces are travelling toward the postage meter. Static scales are a helpful add-on for any type of e-postage device. For offline e-postage devices in a company's mail room it is convenient to use a supplemental PC such that the mailing staff can use a larger display to organize the various cost accounts and manage the electronic postage per department.
- There are PC postage clients that integrate into a mailer's Internet browser in such a way that the mailer, after having sold items through eBay, can easily produce the required labels of e-postage and affix them to the parcels he is going to ship to the buyers.
- Automatic updates of the operating software or application software of e-postage devices help mailers to always work with the latest approved functions.

Other value-added services integrate the e-postage services closer into the mailing and delivery process. We call them *postal value-added services.* Implementations of postal value-added services usually do require approval by the respective postal operators. Postal value-added services are usually related to (i) the handling of e-postage, (ii) the handling of postal addresses, or (iii) logistic services. In order to signal a requested service to the postal operator, mailers print respective endorsements or postal inscriptions onto their mail, e.g., "first class", "address service requested", "return service requested", etc.

Although postal operators, at least of the industrialized countries, experience similar demand for value-added postal services, there is little standardization in their design, implementation, format, and operation. Postal operators offer different choices of postal value-added services and pursue different approaches for each of them. In the following, we describe the more common postal value-added services in general and map them into the above model of e-postage systems (see Section 2.1 on page 25). The specifics of design, implementation, format, and operation of these postal value-added services in selected industry e-postage systems are described in Chapter 6 on page 127 and Chapter 7 on page 167.

2.3.1 Postage Rate Tables

A main concern of postal operators is that mailers use the correct amount of postage for each of their mailings. As long as stamps are used, some postal operators like Deutsche Post indicate that the amount of overfranking about equals the amount of underfranking. To some extent, overfranking is caused by the fixed denominations of stamps, which make it difficult to combine standard value stamps so to achieve less common postage amounts. With electronic postage overfranking is unlikely to occur. However, electronic postage is typically used for large amounts of mail, and if the e-postage device calculates postage amounts incorrectly in a systematic way, for example, because of using an outdated postage rate table or a wrongly calibrated scale, then the missing postage easily sums up to significant amounts.

2.3.1.1 Mailing Parameters and Rate Categories

In order to specify the amount of postage required for each piece of mail, postal operators define *rate categories* also called *product codes* and assign the required amount of postage to each of them. A rate category is defined by a combination of mailing parameters such as:

- *class of mail.* As an example, the USPS classes of mail are first class mail, standard mail, express mail, priority, periodicals, package services, and international. In Canada, classes of mail are called *letter service categories*, Deutsche Post calls them *base products.*
- *subclass of mail* (e.g. letter size or flat size),
- *range of size* indicated by width, height, and thickness,
- *range of weight,*
- *origin and destination* indicated, for example, by source and destination postal code or the number of postal zones between origin and destination location,
- *presort type* indicating the depth of presorting, e.g., single piece unsorted, 3 digit ZIP code, 5 digit ZIP code, etc.
- optional *extra services* such as registered mail, certified mail, delivery confirmation, collect on delivery, and many others.

Each rate category has a unique amount of postage assigned. There may be two different rate categories with the same amount of postage, but there are no two different amounts of postage assigned to the same rate category. Different terms are in use for rate categories. Deutsche Post uses the term *product code*, the US Postal Services and Canada Post have no specific term for it, but think of it as a combination of a base price plus some fee for additional services.

Each postal operator organizes its business individually and defines its specific ranges for these mailing parameters. For example, Deutsche Post does not support a presort type in their postage rate table because they reimburse for pre-sorted mail after mail delivery, while the US Postal Services supports the presort type in their postage rate table because they support discounted prepaid postage. Postal operators also use different approaches of combining values of mailing parameters. For example, the US Postal Service supports first class mail up to 3.3 oz. per piece of mail. Heavier mail pieces can be sent as priority mail or express mail. There is no delivery confirmation available for express mail and no signature confirmation for standard mail.

Table 7 on page 42 presents a list of sample rate categories for the US in 2005 defined by combinations of mailing parameters (columns 2 through 7) and ranges for the values of these mailing parameters (see entries in respective columns 2 through 7). Each row of the table defines a rate category and is identified by a unique ID (column 1). The amount of postage due for each rate category is displayed in column 8. Some postal operators associate additional information to each rate category, for example, a short description of the category, which shall be displayed by the imprint of each mail piece of this rate category.

Table 7. Sample US Rate Categories (2005)

ID	*class of mail*	*subclass of mail*	*weight range*	*origin & destination*	*presort type*	*extra service*	*postage*
1	first class	letter size	up to 1 oz.	—	—	—	$0.37
2	first class	letter size	up to 2 oz.	—	—	certified	$0.60
3	first class	letter size	up to 2 oz.	—	3 digit	—	$0.517
4	Priority	flat size	up to 2 lbs.	zone 5	—	—	$4.90

A *postage rate table* (or simply *rate table*) of a postal operator is a complete listing of rate categories with assigned postage rate, such that each piece of mail accepted by the postal operator falls into exactly one rate category. For example, the complete list of rate categories of Deutsche Post contains about 1600 rate categories. To keep it readable for a human mailer, postal operators present their rate tables by a base table for the class of mail and a couple of auxiliary tables for optional additional services. For an e-postage device, however, one large list of all rate categories is an appropriate representation.

2.3.1.2 Updating Postage Rate Tables

Postage rate tables change frequently for various reasons. The most prominent reasons are rate changes. Other reasons are the introduction of new services or the termination of services that are no longer supported. Both types of changes may introduce new rate categories or obsolete existing ones. Postal operators may also do a complete restructuring of their rate tables in order to simplify the calculation of postage or to become more competitive.

Postage rate tables usually have a *start date* at which they take effect, but no explicit *end date* when they are going to be outdated. Instead, each rate table is implicitly outdated at the start date of the successor rate table.

In order to provide an easy and convenient way of calculating correct postage, e-postage devices should have access to the latest rate tables. Every time an offline e-postage device contacts the e-postage provider to perform a postage value download, the e-postage provider first checks if the offline e-postage device has the current rate table available. If not, it downloads the current rate table into the mailer's e-postage device. More sophisticated offline e-postage devices have more than one slot, such that they can store the current and the successor rate table (as soon as it becomes available through the e-postage provider). Such an e-postage device would pick its rate table based on the date of mailing. This approach also supports seamless pre-franking. If a mailer sets the mailing date 10 days ahead of the date of franking, and the next rate table takes effect 5 days after the date of franking, then the e-postage device could automatically use the successor rate table for calculating the amount of postage for the prefranked imprint.

For online e-postage devices, the e-postage provider usually maintains a web page, where the latest rate table can be looked up. Either the e-postage client calculates the required postage in advance and sends an indicia request for the chosen amount of postage to the e-postage provider, or the e-postage client sends an indicia request including the mailing parameters and asks the e-postage provider to calculate the required amount of postage online. There is a lot of room to further customize e-postage devices in the area of rate tables. For example, e-postage devices could show only an extraction of the actual rate table depending on which rate categories the e-postage device supports.

In the e-postage model of Figure 11 on page 26, this service affects the interaction between e-postage devices and their e-postage provider (link 4), as well as the interaction between the e-postage provider and the post backoffice (links 3 and 5).

2.3.2 Acquiring Usage Data from E-postage Devices

Some postal operators acquire *usage data* (also called *data capture*) on a monthly or quarterly basis to monitor how many first-class letters, periodicals, etc. have been processed by their postal system. The usage data helps them to accurately determine the mailers' demand for their postal products, adjust their product portfolio and optimize its pricing.

The more detailed usage data postal operators require, the better they can fine tune their product portfolio, but the more co-operation is required from the mailers. The minimum level of detail in usage data is probably the class of mail information, while the maximum level is the *rate category* information. In traditional postage meters, the mailer would just input the amount of postage to get an indicium printed (*postage amount entry*). But the amount of postage is an ambiguous and thus insufficient indication of its rate category and class of mail because, usually, there is more than one rate category with the same amount of postage associated. Thus, in order to acquire accurate usage data through an e-postage device, mailers must provide more information about their mail than just the amount of postage.

A simple approach is to make the e-postage device ask the mailer for the rate category directly (*product code entry*). The e-postage device would then look up the associated amount of postage from the rate table. Alternatively, the e-postage device asks the mailer for the mailing parameters, i.e, class of mail, format, weight, destination postal code, extra services, and then calculates the rate category and looks up the associated amount of postage (*mailing parameter entry*). To make product code entry and mailing parameter entry as easy to use for the mailer as postage amount entry ever was, many e-postage devices provide programmable hot keys that mailers can customize to their most frequently used products. E-postage devices with mailing parameter entry are convenient to use if an integrated scale is available that feeds the weight of a mail piece directly into the calculation of the rate category.

Postal operators can acquire usage data through printed indicia or electronically through the e-postage providers. In the former case, the e-postage devices fill the rate category into the respective field of the indicia, which is read by the mail processing centers directly. In the latter case, offline e-postage devices record and store the date and time stamp and usage data for each indicium until they make the next contact to the e-postage provider, typically at the next postage value download. These temporary records are sometimes called *usage profiles*. Online e-postage devices simply forward the usage data to the e-postage provider with each request for indicia. The e-postage provider then buffers, re-formats and transmits the usage data according to the postal operator's requirements. Two examples shall illustrate the tasks of the e-postage provider: (i) If e-postage devices transfer their usage profiles to the e-postage provider in compressed data format, the e-postage provider needs to expand them and usually convert them into a summary format. (ii) If the postal operators divide their business years into accounting periods, the e-postage providers are usually required to report the usage data of their e-postage devices with respect to those accounting periods. In the e-postage model of Figure 11 on page 26, this service affects either the communication links 6-8 or 3-5.

2.3.3 Preparing Traceable Mail

Many postal operators provide value-added services for business documents that should not get lost or fall into wrong hands. Such services are known in the US as certified mail and registered mail. *Certified mail* is a service that provides the sender with a mailing receipt and a unique *tracking number*. A delivery record is maintained by the postal operator and may be accessed by the mailer online, by phone, or by e-mail through the tracking number. This service is usually available for first-class mail and priority mail. *Registered mail* is a kind of certified mail with optional indemnity in case of loss or damage.

According to UPU conventions, tracking numbers are encoded using a service indicator and a one dimensional barcode such as UCC/EAN Code 128 [112]. Some postal operators like Deutsche Post, the US Postal Services and Canada Post allow the tracking number to be located to the left of the postmark. In this case, printing the tracking number can be done by an e-postage device. Some postal operators like the US Postal Services also allow the tracking number to be printed closer to the addressing field such that printing of tracking numbers can be integrated into the address printing process. For country specific integration of certified mail into electronic postage systems see Chapter 6 on page 127 and Chapter 7 on page 167.

Usually, the tracking number is generated and chosen by the e-postage device in co-operation with the e-postage provider and the post backoffice. In the e-postage model of Figure 11 on page 26, this service affects the interaction between e-postage devices and their e-postage providers (link 4). And if the postal operator provides the tracking numbers, the interaction between the e-postage provider and the post backoffice (links 3 and 5) is also affected. The service also affects the design, content and printing of indicia (link 6).

Further supplemental services related to certified mail are presented in the following subsections.

2.3.3.1 Certified Mail Statement

Some postal operators require from mailers who send certified mail to produce a *certified mail statement*, which contains the number of certified mail pieces and their individual tracking numbers. The mailer is required to deliver the certified mail together with the certified mail statement at the inducting post office. If certified mail imprints are produced by an e-postage device, it is convenient for the mailer if the e-postage device also produces the certified mail statement.

2.3.3.2 Tracking Services

Some postal operators provide web-based up-to-date tracking services for certified mail. When sending a piece of certified mail, the sender receives an individual ID for each mailing. The delivery status of each mailing is traced by the postal delivery system and can be looked up during transit by the mailer using the tracking number. Similar services have been provided by parcel carriers like UPS or FedEx.

2.3.3.3 Delivery Confirmation

This service provides the date and time of delivery or delivery attempt. Mailers who apply identifying barcodes to each piece may retrieve this information in three forms: (1) as an electronic file, or (2) through the Internet, or (3) by calling a service hotline.

2.3.3.4 Signature Confirmation

This service provides the date and time of delivery, including the recipient's signature or the date and time of the delivery attempt. This service may be obtained in two forms: (1) as an electronic file, or (2) through the Internet.

2.3.4 Postage or Date Correction

Some postal operators define special indicia for correcting human errors. If the mailer erroneously produces a printed indicia that shows an insufficient amount of postage, then he can print a *postage correction indicium* on the back of the envelope showing the missing amount of postage. Both indicia together provide evidence that the mailer has pre-paid the correct amount of postage for the mailing.

If the mailer erroneously produced a printed indicia showing a wrong date, then he can print a *data correction* or *redate indicium* on the back of the envelope. The postal operator will then accept the printed mailing date of the date correction indicium and will ignore the printed mailing date of the regular indicia. If more than one indicia is printed on a piece of mail, they must not overlap each other.

In the e-postage model of Figure 11 on page 26, this service only affects the design, content and printing of indicia (see link 6).

2.3.5 Reply Mail

Mailers seeking responses from their customers can prepare postcards or envelopes addressed to themselves and insert these prepared postcards or envelopes into the mail to their customers. Customers can fill in their answers on the prepared postcards or insert their answers into the prepared reply mail envelopes and return them.

Mailers who choose *business reply mail* pay the postage in advance for all prepared postcards and reply mail envelopes themselves. This is an incentive for the customer to return the reply mail and makes sense if almost all customers are supposed to return their reply mailings. Industrial e-postage systems offer a special type of postmark for business reply mail.

Mailers who choose *courtesy reply mail* do not pay for the reply mail. Instead their customers need to pay for the mail pieces they return. This is appropriate if a lower return rate is expected, but is still convenient for customers as they receive a ready-to-send envelope with an accurate recipient address. Courtesy reply mail can be franked by the sender with any kind of postage, electronic or stamps.

A more versatile type of reply mail is possible if the postal operator runs a lockbox account into which mailers can pre-pay the postage for their reply mail before sending them. However, the postal operator deducts the postage from the lockbox account only if and when it sees the respective reply mail pieces being inducted for their return trip. This type of reply mail is free for the customers, and the mailers pay only for those return mail pieces that are actually returned to them. An e-postage system supporting this type of reply mail must keep track of which return mail pieces have been pre-paid for in the lockbox account.

Some postal operators consider reply mail as an additional service for domestic or international first class mail. They require the mailer to indicate the reply mail service within some data field of the regular postmark. Other postal operators require the mailers to apply additional bar codes to their return mail in order to support the sorting and delivery process.

In the e-postage model of Figure 11 on page 26, this service affects the design, content and printing of india (see link 6).

2.3.6 Commercial Metering Services

Mailers can use their e-postage devices to provide commercial franking services to third parties. They can use spare e-postage devices or e-postage devices that they do not use to full capacity all the time. Commercial franking services and franking related services such as folding, inserting, addressing, etc. are provided for example by letter shops. Some postal operators, such as

Deutsche Post, require mailers who use their e-postage devices to meter mail commercially on behalf of third parties to indicate such services to the postal operator. This extra reporting is an additional security measure against fraudulent activities that have been experienced at letter shops in the past.

2.3.7 Addressing, Mail Forwarding and Return Services

One of the challenges of delivering physical mail is that the recipient address printed on a piece of mail may be printed incorrectly, may be outdated, or may be right, but the recipient refuses to receive the mail piece. The main reason for incorrect addresses is that mailers have inaccurate or outdated address data about their customers on file. Even with significant and sustained efforts, mailers can hardly achieve 100% accurate and current address data. For example, in the US, about 40m of the entire population age 1 and older (282m people) relocated their residence in 2003. The annual relocation rate ranges from 12% and 15% [79]. Many postal operators have maintained address databases on an almost real-time basis, so they can correct inaccurate or outdated addresses during postal delivery and forward the mail accordingly. Some postal operators also provide address sanitizing and validation software or online services.

Such addressing and mail forwarding services are demanded particularly by bulk mailers such as direct mailers who send catalogs, brochures and other advertising matter to a large number of recipients. Mail forwarding helps them to increase their hit rates, and addressing services help them to better keep their customer address databases up to date.

Here is an example, how an addressing and mail forwarding service works. Mailers sign a contract with the postal operator. The contract can be setup, changed, extended, or reduced at any time through a web-based service of the postal operator. The following options are available:

- *Forward Service*: If the given recipient address is inaccurate or outdated, try to figure the correct or updated recipient address, deliver the mail to that address and send the corrected or updated recipient address information back to the mailer including a reference to the respective piece(s) of mail. The feedback channel to the mailer can be by e-mail, or through a web based service.
- *Return Service*: If the given recipient address is inaccurate or outdated and the correct or updated address for the intended recipient cannot be figured or if the recipient refuses to receive the mailing, then return the mail to the mailer or discard it and send the mailer a

receipt that the mail could not be delivered and has been returned or discarded.

These options can be provided by the postal operators for specified classes of mail. Mailers who have subscribed to such services, add a tracking number to their indicia in order to identify their mailings. This tracking number will be used as a reference in case the mailing cannot be delivered to the recipient address. The tracking number could be a randomly chosen number from a large enough space. In addition to a machine readable tracking number, mailers also add a human readable mark to their imprints, which signal to the *mail-carrier* that the mailing shall be handled according to the mailer's preferences of his contract in case the mailing cannot be delivered to the intended recipient.

In the e-postage model of Figure 11 on page 26, this service affects the design, content and printing of india (see link 6) and the delivery process (see link 10).

Chapter 3

General Architecture of E-Postage Systems

3.1 E-POSTAGE DEVICES

E-postage devices help mailers to figure the correct amounts of postage for their mail pieces, compile the respective data representation of required imprints, and provide robust printing mechanisms to apply the respective imprints onto the mail pieces in the correct location. Peripheral devices such as folders, inserters, sealers, feeders, scales, sorters and stackers may be connected to e-postage devices to better integrate their core metering functions into the mailer's business processes.

The core metering functions provided by an e-postage device are listed below:

1. ***Enter Mailing Parameters***: In the simplest case, the mailer types in the required amount of postage manually. Most of the mail pieces are franked with only a few different postal rates anyway, which mailers can usually remember.

   More and more postal operators require e-postage devices to collect statistical data about which postal products they have franked (see Section 2.3.2 on page 43). These postal operators do not want mailers to enter postage amounts, but the exact rate categories or product codes. Since those may be inconvenient to remember and type, modern e-postage devices let mailers enter the characteristic mailing parameters (see Section 2.3.1.1 on page 41) and calculate the rate categories and the corresponding postage amounts automatically. This approach is called *product code entry*.

2. ***Account for Imprint***: Once the correct amount of postage is determined, an e-postage device must account for it. Accounting is the irreversible process of deducting the requested amount of postage from the prepaid amount of postage currently remaining in the mailer's e-postage device.

3. ***Apply Imprint***: Once an e-postage device has determined a rate category and accounted for its postage amount, it must produce the

respective imprint and apply it to the prepared envelope or label of the intended mail piece.

4. ***Report Activity***: After an e-postage device has performed local or remote activities, it needs to report so to its e-postage provider during the next scheduled time slot. Such reporting includes to submit its usage data if the postal operator so requires.

Ideally, the imprints should be accounted for in the exact same moment when they are applied. This would guarantee that mailers never receive unaccounted for imprints (bad for the postal operator) nor ever miss imprints that have been accounted for (bad for the mailer). Real e-postage devices must fail safe in case of failure, technical or human, by accident or intentional. Because such failure might interrupt an e-postage device's operation at any time, imprints are always accounted for *before* they are printed out. So if failure strikes, it can only lead to missing imprints that have already been accounted for. It is conceivable that such a case will be followed up by the mailer who would otherwise bear the loss.

3.1.1 Closed Offline E-Postage Devices

Closed offline e-postage devices are specialized embedded systems dedicated to download and store electronic postage and to produce imprints on demand of the user. Most postal operators require offline e-postage devices to have postal security devices embedded. A postal security device is a tamper resistant and tamper responsive hardware security module that hosts and controls all postal revenue sensitive functions of its e-postage device.

A schematic block diagram of a closed offline e-postage device is shown in Figure 13 on page 53. It contains a main processor (CPU) that is connected by a data and address bus to a number of non-volatile and random access memory components, to the postal security device, and to a co-processor. The co-processor supports the control links to a number of specialized controllers for the keypad, scale, chipcard reader, printing system, modem interface, sensors, motors, power control and to one or more serial interfaces. The chipcard reader allows customers to load and store their personal meter configuration such as adverts or cost accounts on a personal chip card. The modem links the e-postage device to the e-postage provider. The sensors and motors control the electromechanical parts of the e-postage device including the letter transport, bringing the print head to its print position and back to the rest zone, and cleaning facilities. Optional serial interfaces are useful to connect an external scale, a service PC for diagnosis and maintenance, or the user's desktop PC to facilitate the configuration of an e-postage device. Additional controllers link

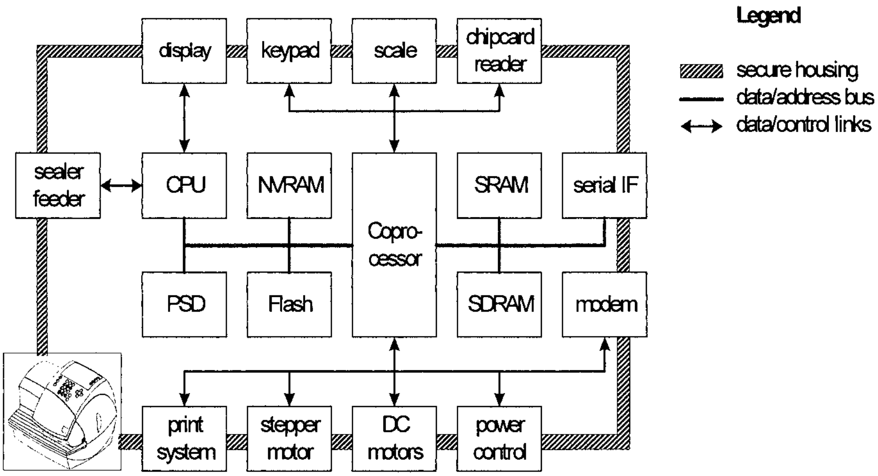


*Figure 13.*Schematic Diagram of a Postage Meter

the CPU to the display and optional peripheral devices such as a sealer, a feeder, or a dynamic scale, which weighs mail items while travelling from the feeder to the e-postage device.

3.1.1.1 Postal Security Device

The *postal security device* of an e-postage device needs to be chosen carefully so as to meet the security, performance and economic requirements. Secure indicia are unique because each indicia contains the mailing date, the value of the descending register or other non-recurring dynamic content. Therefore each imprint requires to compute an individual cryptographic checksum to be contained within the respective indicia. A high-performance e-postage device requires a high-speed postal security device that can keep up with the speed of letter processing. Such a high-speed postal security device is probably oversized to be used within an entry level e-postage device that is fed manually by the user.

Postal security devices need to be enclosed by a *tamper responsive envelope*. Unless this envelope is triggered by an attempt of tampering, for example by physical force, drilling, chemical attacks with dissolvents or acids, it protects the integrity of the values of all postal registers and of the cryptographic keys that are needed to compute the cryptographic checksums for valid indicia. If the tamper detection is triggered, it guarantees to render the postal security device inoperable, but to leave all postal registers unchanged for later inspection. This is enforced by permanently deleting only the cryptographic keys necessary to compute the cryptographic checksums for valid indicia. Furthermore, a postal security device should have suitable measures in place to discourage side-channel attacks which might otherwise give way to extract information about the cryptographic keys [27].

A schematic block diagram of a typical postal security device is shown in Figure 14 on page 54. It consists of a central processing unit (CPU) that is

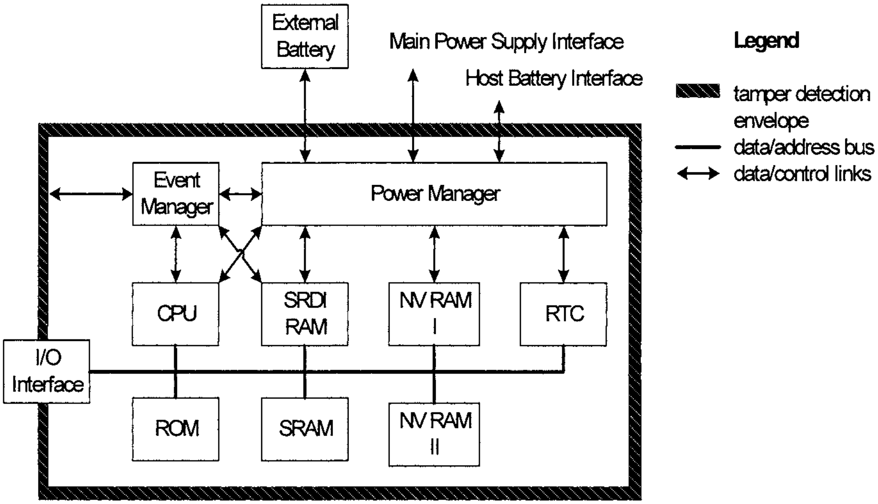


*Figure 14.*Schematic Diagram of a Postal Security Device

connected to a number of memory components such as read-only memory (ROM), static RAM, RAM that stores security relevant data items (SRDI) such as critical cryptographic keys, two redundant components of non-volatile memory that store the postal registers, to a real-time clock (RTC) and to an input/output controller that interfaces with the e-postage device into which the postal security device is embedded. The event manager monitors several environmental conditions such as the external battery voltage, host battery voltage, supply voltage, temperature and attempts of tampering such as drilling, or dissolving the physical envelope of the postal security device or disrupting the power of the external battery. When the tamper detection circuitry signals an attempt of tampering to the event manager, it triggers the SRDI-RAM immediately to actively zeroize its critical cryptographic keys. Thus the postal security device is said to have a *tamper responsive envelope.* The power manager may control several sources of supply power and backup power. A conventional design is to use the power supply of the e-postage device as the first source of power supply. During periods of transportation and power outages a backup battery of the host serves as the secondary source of power, which can be recharged as soon as the host is re-connected to power supply. A backup battery mounted onto the postal security device serves as a third source of power supply during periods of manufacturing and service when the postal security device is not yet embedded into a host or is unplugged from its host in order to be replaced or maintained otherwise.

There may be an optional hardware random number generator included within the tamper responsive envelope. However, most postal security devices import truly random input from the e-postage provider through an encrypted channel in order to seed a pseudo-random number generator. The output of the pseudo-random number generator is then used for example to generate secret or private cryptographic keys. The operating system, application software and cryptographic software libraries reside in ROM or non-volatile memory, which can retain the stored information even when not powered. Non-volatile memory, such as Flash-memory, EPROM, or EEPROM is favorable for postal security devices that can have their application software updated. Such updates must be restricted to well-defined conditions and environments.

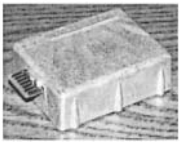
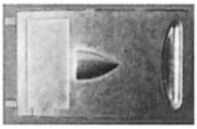
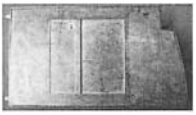
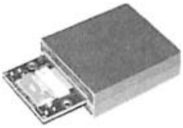
According to FIPS 140-2, postal security devices are special cases of cryptographic modules. FIPS 140-2 distinguishes the following three kinds of physical embodiments of cryptographic modules in general and thus postal security devices in particular:

Table 8. Embodiments of Cryptographic Modules (FIPS 140-2)

Embodiment	*Definition*
Single Chip Cryptographic Modules	A single integrated circuit (IC) chip is used as a standalone device or is embedded within an enclosure or a product that may not be physically protected. Examples include single IC chips or smart cards with a single IC chip.
Multi-Chip Embedded Cryptographic Modules	Two or more IC chips are interconnected and are embedded within an enclosure or a product that may not be physically protected. Examples include adapters and expansion boards.
Multi-Chip Standalone Cryptographic Modules	Two or more IC chips are interconnected and the entire component is operated within a separate physically protected host device. Examples include encrypting routers or secure radios.

The international vendors of closed e-postage devices have had a number of postal security devices certified against FIPS 140-1 or 140-2. The following Table 9 on page 56 lists those entries from the cryptographic module validation list of NIST [89].

Table 9. List of selected FIPS 140 Certified Postal Security Devices

Certificate No	*Device*	*Manufacturer*	*Type*	*Photo*	*Vendor*
#482	Cygnus X1	Mykotronx	multiple-chip standalone		[a] Pitney-Bowes
#547	CoMet 1A00	Mykotronx	multiple-chip standalone	no picture available	Pitney-Bowes
#551	N94i/155 SMM	Neopost	multiple-chip embedded		[b] Neopost
#554	Crypto iButton DS1955B #PB5 (compliant to EU-RoHS directive [28])	Dallas-Semiconductors	multiple-chip standalone	iButton®.com C2 46 0000001F1342 1-Wire® crypto m96	[c] Pitney-Bowes
#659	C20ND	Neopost	multiple-chip embedded		[b] Neopost
#665, #666	Postal Revenector	Francotyp-Postalia	multiple-chip embedded		[d] Francotyp-Postalia
#667	Postal Revenector (compliant to EU-RoHS directive [28])	Francotyp-Postalia	multiple-chip embedded		[d] Francotyp-Postalia

[a] Photograph being used courtesy of Pitney Bowes Inc.

[b] Photographs being used courtesy of Neopost Technologies.

[c] Photograph being used courtesy of Dallas Semiconductor.

d. Photographs being used courtesy of Francotyp-Postalia Group.

Protected by its tamper responsive envelope, a postal security device shall provide the three security-critical functions introduced in Section 2.2 on page 35:

1. Storing electronic postage (see Section 2.2.2 on page 36), which includes to properly initialize and manage the postal registers as well the cryptographic keys.

   The postal registers are maintained in non-volatile memory. Each time a postal register is read, their integrity constraints are verified; for example, if the values range between their minimum and maximum values and if the ascending (AR), descending (DR) and total setting (TS) registers obey the equation $TS = AR + DR$. In case any of the integrity constraints is violated, the postal security device jumps into a defect state that allows no regular operations any more, but only certain inspection services. Some postal operators require to use two different technologies of non-volatile memory and to maintain each postal register twice, one copy in one technology type of non-volatile memory, the second copy in the other technology type of non-volatile memory. Every time a postal register is read, both its copies are read and in case their values differ, the postal security device jumps into the defect state.

   In order to maintain the integrity constraints, the postal registers must be updated consistently by means of transactions. If a transaction is aborted, all postal registers are reset to the values before the transaction started. Only during such a recovery period, inconsistent values of postal registers are acceptable and do not force the postal security device into the defect state.

   The cryptographic keys are maintained in a separate portion of non-volatile memory that can be instantly zeroized without affecting the values of the postal registers. The zeroization of cryptographic keys is triggered if an attempt of tampering is detected.

2. Securing the communication with the e-postage provider (see Section 2.2.1 on page 35), which includes the proper initialization before it is put into operation, the authorization for each user to which it is associated over its life-time, the finance functions such as postage value download and postage value refund, and upon request by the e-postage provider a device audit function that reports the internal state,

postal register values, and history of the postal security device to the e-postage provider.

The communication between the postal security device and the e-postage provider is authenticated in either direction and uses encryption to transfer confidential data. Some kind of session key establishment is used, but the communication interface is a proprietary domain of each vendor and is protected by numerous patents.

3. Securing the computation of indicia, which includes to compute the cryptographic checksums (see Section 2.2.3 on page 37) that are required for all imprints of the e-postage device.

   Postal operators have established a variety of different e-postage systems (see Chapter 6 on page 127), which use very different cryptographic mechanisms and cryptographic key managements in order to produce and verify indicia. They have in common that the postal security device maintains a symmetric or asymmetric *indicia key* that is stored by the postal security device in non-volatile memory and is used to compute the *cryptographic checksum* for each indicia; hence the name of the key. Existing e-postage systems, however, vary widely with respect to

   * whether the indicia key is an asymmetric key for a digital signature mechanism such as RSA or DSA or ECDSA, or an symmetric key typically used for a (truncated) message authentication code mechanism such as HMAC SHA-1.
   * whether the indicia key is generated within the postal security device or is imported from the e-postage provider in a secure way.
   * how and how frequently the indicia keys are updated.

   Because of these differences, we use the term *cryptographic checksum* as a generic term for something that can be a digital signature, a message authentication code or truncated message authentication code (see Section 4.4 on page 98).

3.1.1.2 Life-Cycle

Because of their revenue protecting purpose, postal security devices are required to be security evaluated against the NIST standard FIPS 140-2 b (see Chapter 10 on page 207). FIPS 140-2 is organized in 11 categories of security requirements one of which is that the operating software must be specified by a finite state machine model. A generic such model that works for most postal operators in most countries is depicted in Figure 15 on page 59).

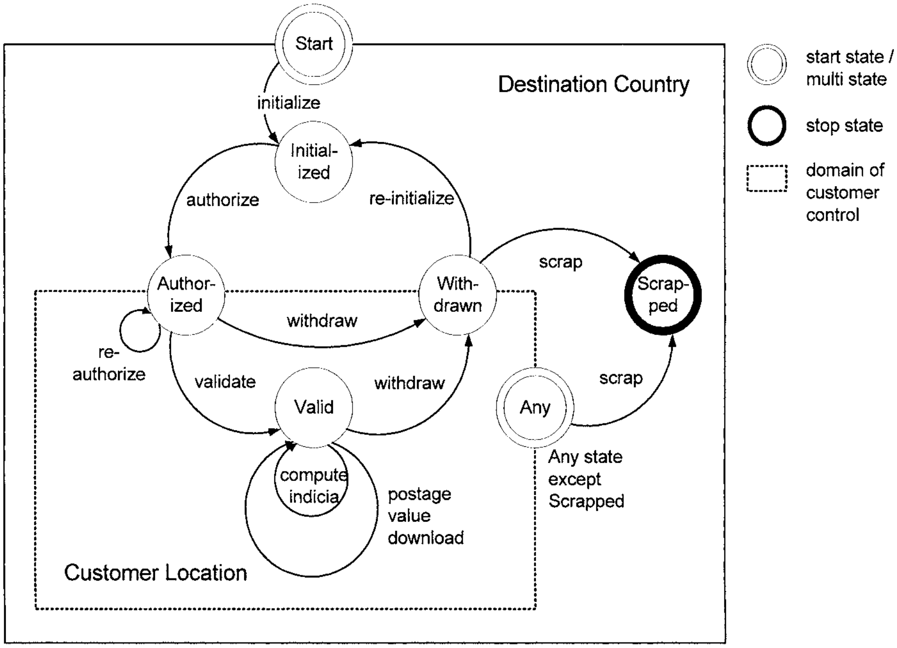


*Figure 15.*High Level Finite State Diagram of a Postal Security Device

Before e-postage devices can be distributed throughout their destination countries or postal markets, they need to be setup properly by their e-postage providers. The e-postage devices may have been manufactured at a domestic or off-shore location, but once they arrive at their respective e-postage providers, their embedded postal security devices are in state Start.

Before a postal security device can be assigned to its first user, the postal security device needs to be initialized for its destination country.

- ***Initialization*** is an online service supported by the e-postage provider. Typical actions during PSD initialization are the following:
  - * Synchronization of the *real-time clock* (RTC) with the e-postage provider
  - * Initialization of the *watchdog timer*. The postal security device shall cease regular operation in case it is not used for an extended period of time or it is disabled remotely by the e-postage pro-

vider. The watchdog timer keeps the remaining time until the maximum time unused is reached.

  - Setting all *postal registers* to their initial values, usually zero.
  - Setting all other variables of the postal security device to their initial values.
  - Assigning a unique *postal serial number* (*PSD-PSN*) to the postal security device. The postal serial number consists of a manufacturer ID, a PSD model ID and a PSD serial number.
  - Initializing all cryptographic keys of the postal security device.

  After successful initialization, the postal security device switches to state *initialized.* The e-postage device with its embedded postal security device is ready to be shipped to a customer (mailer) and be customized to the respective location and licensing post office. Alternatively, the e-postage device could be authorized at some central location and afterwards be shipped to the customer.

- ***Authorization*** is an offline service or online service supported by the e-postage provider where customer-specific information including the postal code of the licensing post office is loaded.

  After successful authorization, the postal security device switches to state *authorized.* The e-postage device with its embedded postal security device is ready for the customer (mailer) to perform the first postage value download. In case, the customer backs out of the contract at this stage, the postal security device can also be withdrawn (see transition *withdrawal* below).

- ***Validation*** is an online service supported by the e-postage provider. It is the first postage value download that sets the user up to produce imprints. Typically, this first postage value download must load a minimum amount of postage into the postal security device. The e-postage provider verifies if the user has sufficient funds on deposit or has a sufficient credit line for the requested amount of postage. After successful validation, the postal security device transitions to state *valid.*

  After successful validation, the postal security device transitions to state *valid.* The e-postage device with its embedded postal security device is ready for regular operation.

- ***Producing indicia*** is an offline service invoked each time the user requests an imprint. The descending register is decreased by the face value of the indicia, while the ascending register is increased by the same amount. The piece counter is increased by one for each indicia calculation. After the postal registers have been updated, the postal security device produces a valid cryptographic checksum over the content of the requested indicia. The indicia complete with checksum is encoded into a 2D barcode and is printed by the e-postage device.

If the computed indicia for some reason do not print successfully for example due to a paper misfeed or paper jam, then the face value is already deducted from the postal registers of the postal security device. There is no way to reverse this deduction inside the postal security device. Most postal operators support a refund of spoiled indicia after the customer has turned in physical evidence of the spoiled indicia.

After indicia are computed, the postal security device remains in state *valid*. The e-postage device with its embedded postal security device remains ready for regular operation.

- ***Postage Value Download*** is an online service supported by the e-postage provider. It is available only in state *valid* and loads the requested amount of postage into the postal security device if the user has sufficient funds on deposit or has a sufficient credit line at the e-postage provider. The descending register and the total settings register are each increased by the requested amount of postage.

  After a successful postage value download, the postal security device remains in state *valid*. The e-postage device with its embedded postal security device remains ready for regular operation.

- ***Blocking/Unblocking*** are online services that can be invoked by the e-postage provider when the e-postage device makes a connection. A blocked e-postage device cannot produce any more postage imprints unless it is unblocked. Blocking can be used, for example, if a mailer has downloaded a large amount of postage without sufficient payment.

- ***Withdrawal*** is an online service supported by the e-postage provider. The postal security device executes a postage value refund, which is like a reverse postage value download, and brings the remaining amount of postage back into the user's account at the e-postage provider. There are different ways how the postage value refund can be reflected by the postal registers. The refund can be regarded as a reversed postage value download. In this case the total settings register is decreased by the remaining amount of postage shown by the descending register and the descending register is reset to zero. Or the refund can be regarded as a large imprint. In this case the ascending register is increased by the remaining amount of postage shown by the descending register, and the descending register is afterwards reset to zero. The former approach leaves the ascending register, i.e., the sum of the face values of all imprints produced since validation, unchanged. The latter approach leaves the total settings register, i.e., the sum of all postage value downloads since validation, unchanged. Both approaches reflect a part of the truth and there are some postal operators in favor of each approach.

After a successful withdrawal, the postal security device transitions to state *withdrawn*. The e-postage device with its embedded postal security device cannot compute indicia or perform postage value downloads. It is no longer associated to the previous customer in the e-postage provider system. It is safe for the user to have the e-postage device picked up by a dealer or to return the e-postage device by mail. Some postal operators support purchase markets such that the previous user can sell his e-postage device straight to another user, for example, through eBay, and then ship the e-postage device to the new owner.

- ***Re-Initialization*** is an online service supported by the e-postage provider. Upon this service, the postal security device enters a new life-cycle in which it will be associated to a new customer.

  * Some postal operators conceive the PSD-PSN to identify the hardware of the postal security device. They require that during re-initialization the PSD-PSN and the postal registers must remain unchanged. This approach implicates that the second and every further user will recognize the postal security device to be used.
  * Other postal operators conceive the PSD-PSN to identify the respective life-cycle of the postal security device. They require the PSD-PSN to be replaced by a new one and the postal registers to be reset to zero upon re-initialization. With this approach, the postal security device looks new at the beginning of each new life-cycle.

  Otherwise, re-initialization comprises the same actions as initialization. After successful re-initialization, the postal security device transitions to state *initialized.*

- ***Re-Authorization*** is an online or offline service supported by the e-postage provider. The service is to support a mailer's relocation and change of licensing post office if the respective location data and origin postal code are required to be stored by the postal security device. Re-authorization is available in state authorized and in state valid. After successful re-authorization, the postal security device remains in the same state where it was before.

- ***Scrapping*** can be an offline or online service. It is available in any state except in state scrapped and transitions the postal security device into state *scrapped.* The transition to state scrapped is irreversible and renders the postal security device definitely inoperable. In state scrapped, the postal registers can still be inspected, but in terms of its life-cycle, the state scrapped is the terminal state. In this state, the postal security device is safe to be stored until its physical destruction.

At the beginning of each online transaction, the clock of the postal security device should be synchronized securely to the time base maintained by the e-postage provider system.

In addition to this high-level finite state machine model, every real implementation has a number of refinements to it that make sure the postal security device detects inconsistencies early, handles emergency conditions promptly and recovers from either one as smoothly as possible. Important areas where inconsistency and emergency can arise are:

- violated integrity constraints on postal registers,
- expired watch-dog timers,
- insufficient power of the postal security device's backup battery,
- interrupted transactions between the postal security device and the e-postage provider during one of the online services, most notably during postage value downloads and withdrawals,

The last type of inconsistency requires a recovery procedure that takes into account the state of the postal security device at the end of the previously interrupted transaction.

3.1.2 Open Offline E-Postage Devices

An open offline e-postage device is a standard PC that is connected to the Internet, to a postal security device, a scale for weighing mail pieces and an office printer or label printer using black ink. The PC runs some dedicated operating software to control the entire configuration. We call each software installation a *PC postage client.* A small bandwidth Internet connection such as by modem is sufficient. The postal security device works as described for closed offline postage applications (Section 3.1.1 on page 52). It is recommended to use some *address matching services* (AMS) to avoid misspelled or outdated addresses. Address matching services are available on CD-ROM or as online services. A schematic block diagram of an open offline e-postage device is shown in Figure 16 on page 64).

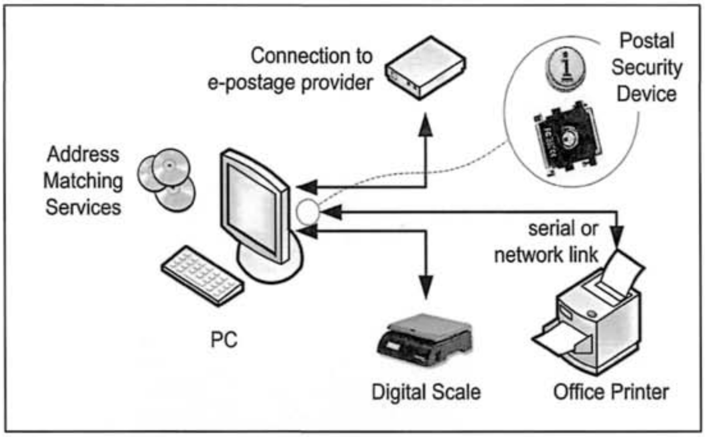


*Figure 16.*Schematic Diagram of an Open Offline E-postage Device

The US Postal Services posted the first specification of open offline e-postage devices in June 1999 [101]. It was remarkably similar to that of closed offline e-postage devices, which had been released only 6 months earlier. While the USPS kept to the concept of a hardware postal security device, it allowed for the first time to print indicia in standard black ink, which is available with any off-the shelf office printer. The specification of closed offline e-postage devices also allows imprints to be printed in black ink, but at the cost of producing and printing an extra barcode, called a *Facing Identification Mark* (FIM) left of the indicia. The FIM is a substitute for the fluorescence, which is normally used by US mail sorting centers to orient the mail pieces properly. This leaves too little space for a customer specific advertisement, and therefore, the option of printing indicia with black ink is not used by any closed offline e-postage device in the US market. As the USPS gave in to the market demands for open e-postage devices, they required an extra security feature in order to deter counterfeiters from copying indicia. The USPS required that each indicia had to include the destination ZIP code of its mail piece.

The only open offline e-postage system that has been approved by a postal operator was developed by e-Stamp, a California start-up. A first day issue produced by an e-Stamp client exhibits an IBI imprint in black ink. It is shown in Figure 17 on page 65). The IBI imprint is located in the upper right corner and consists (from right to left) the e-Stamp logo above the face value of the imprint (32c), the class of mail (First Class US Postage) and the mailing date. The lower portion of the imprint contains the location and ZIP code of the licensing Post office, a PDF417 barcode and the unique serial number of the e-Stamp client that produced the imprint. Located in the upper left corner of the IBI imprint is the Facer Identification Mark (FIM). Altogether, the footprint of the IBI indicia and FIM barcode comes to about 3 square inches. The case of E-Stamp is presented in Section 3.1.2.3 on page 67.

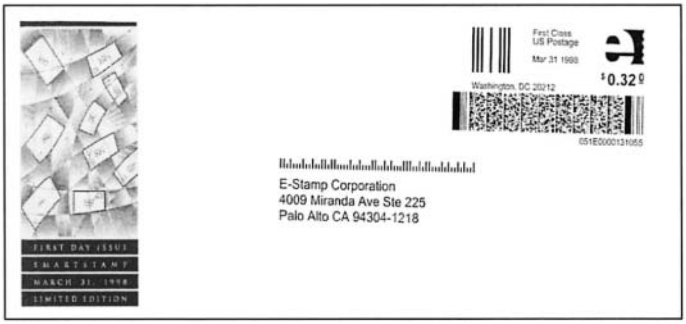


*Figure 17.*First Day Issue produced by an E-Stamp Client

3.1.2.1 Postal Security Device

The challenge of developing an open offline e-postage device is to create a low-cost postal security device that is appropriate for mass production and yet secure enough to meet the US postal security requirements, most notably FIPS 140 overall level 3 plus electronic failure protection level 4. In 1995, when e-Stamp started their system, there was little choice.

For its postal security device, the e-Stamp system used a Crypto iButton, which is a stainless steel encased 16 mm diameter hardware security module. The Crypto iButton had to be plugged into a serial or parallel adapter to be connected to the mailer's PC. Both the FIPS140 certified Crypto iButton and its adapter were available from National Semiconductor in August 1999.

It is listed in the following Table 10 on page 66, which refers to the cryptographic module validation list of NIST [89].

Table 10. List of FIPS 140-1 Certified Postal Security Devices

Certificate No	*Device*	*Manufacturer*	*Type*	*Photo*	*Vendor*
#63, #80	Crypto iButton DS1954B	Dallas-Semiconductors	multi-chip standalone	n/a	E-Stamp

The active components of the Crypto iButton consist of a lithium cell (for backup power), an energy reservoir (to provide parasitic capacitance power), a quartz timing crystal (for a real-time clock), and the single DS83C950 cryptographic chip (see Figure 18 on page 66) [22,1]. The tough stainless steel case of the Crypto iButton also defines a contiguous perimeter and provides clear visual evidence of tampering. If a Crypto iButton is pried open or exposed to extreme temperature or voltage conditions, a microswitch triggers an active zeroization of the chip's contents, destroying private keys and other sensitive information. The iButton constantly monitors the switch's contacts, and any separation of the cryptographic chip from the lithium cell switches the device to on-chip capacitor power to perform a complete zeroization as

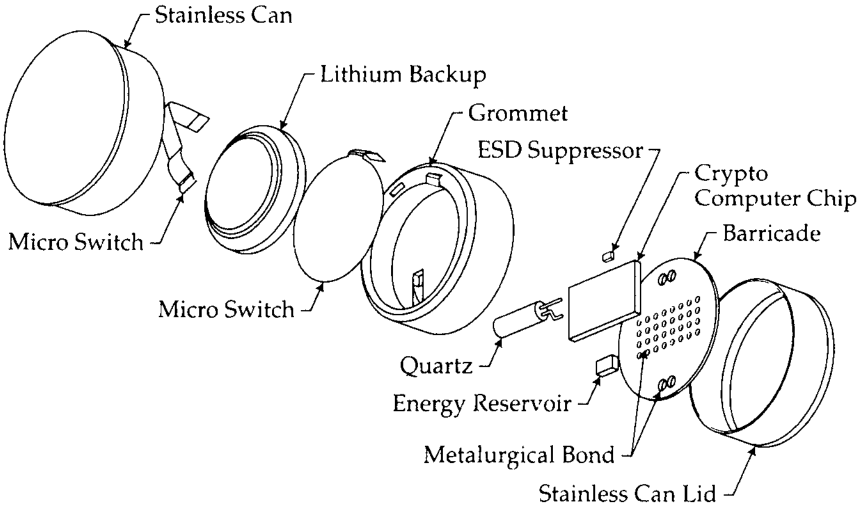


*Figure 18.*Components of the DS1954B Crypto iButton

it's last powered action. Voltages above or below maximum operating tolerances are clamped, and if excessive voltage is encountered, the I/O pin is designed to fuse and render the chip inoperable. A substrate barricade is metallurgically- and glass epoxy-bonded to the active face of the chip. Attempts to remove the barrier to get to the chip cause a tamper response that results in zeroization. If a sophisticated attacker attempts to micro-probe the chip, they will encounter a shield of sub-micron pitch metal layers fabricated into a serpentine pattern directly on the chip. The chip will detect any break in this shield and immediately zeroize the chip [22].

The next generation of Crypto-iButtons, namely the DS1955B #PB5 (see #554 in Table 9 on page 56) were used as full fledged postal security devices featuring an improved security architecture, which has not been laid open by Dallas Semiconductors.

3.1.2.2 Life-Cycle

The life-cycle of closed online e-postage devices is exactly the same as for closed offline e-postage devices as introduced in Section 3.1.1.2 on page 58.

3.1.2.3 The Case of e-Stamp

In 1994, Salim Kara founded e-Stamp, the first company engaged in providing Internet postage services and solutions. In particular, they developed an Internet postage service that allowed customers to purchase, download and print postage directly from their personal computers. On August 9, 1999, in a ceremony at Ben Franklin Hall, the US Postal Service headquarters in Washington granted postal approval to e-Stamp for a system that used a dime-sized crypto iButton by Dallas Semiconductors for its PSD. At the same ceremony, later rival stamps.com got approval for their Internet postage system, but had to delay the launch of their operations because the e-postage provider system could not scale up to customer demand at the time. To set up an e-Stamp installation on a PC, the customer had to plug a Crypto iButton into a serial or parallel adapter that had to be connected to the PC, the PC had to be connected to the Internet via modem or digital subscriber line (DSL), and the e-Stamp application software had to be installed on the PC. Customers who cancelled their contract were to return their Crypto iButtons or otherwise pay $500 fine because the US Postal Services regarded inactive Crypto iButtons remaining in the market as a security threat.

The e-Stamp product never gained a significant market share: e-Stamp had done extensive market studies throughout 1998, which suggested that most of the 7.2m home and small office customers (SOHO) in the US would prefer an open offline e-postage system because their PCs shared the modem connection with their fax machine and therefore these customers would not want to disconnect the fax every time they produced an imprint to send mail. Furthermore, customers seemed to better like the idea to have their recipient addresses verified offline rather than through the Internet, which they felt to invade their privacy. e-Stamps direct competitor Stamps.com, who launched an open online e-postage system in September 1999, just made the opposite decision. Their e-postage device was a purely web-based service and so was the address cleansing service. Despite e-Stamps market research, it turned out that in practice all of these concerns were outweighed by the convenience of a purely web-based approach. In fact, more customers disliked having a proprietary iButton adapter permanently connected to their computer and to install proprietary e-Stamp software. On top of all this, e-stamp required a substantial initial investment from each customer for their iButton with adapter and charged a 10% service surcharge on every dollar of postage sold. e-Stamp's market penetration never exceeded 97,000 small office home office customers in the US throughout 1999 and 2000. At the same time, Stamps.com attracted a customer base of 250,000. As e-Stamp profits lagged behind expectations, e-Stamp closed their Internet postage business on Nov. 28, 2000. In May 2001, e-Stamp sold its 31 Internet postage related patents to former rival stamps.com. Soon after the e-stamp product was approved in 1999, competitors entered the US Postal market providing open online e-postage systems, true Internet based products that required no additional hardware at the customer site. Their sales and distribution concept overcame e-Stamps problems at once and was much more successful in the postal market. Similar products appeared in European postal markets in 2001 and the following years.

The experience of e-Stamp was that an open offline e-postage device can achieve postal approval, but is hard to be made as convenient to use as an open online e-postage device.

3.1.3 Open Online E-postage Devices

A typical open online e-postage device consists of a PC that is connected to the Internet in order to communicate with the e-postage provider, a scale to weigh mail items, and an office printer or label printer using black ink (see Figure 16 on page 64).). The PC runs a piece of software operating the connection to the e-postage provider and the connected printer such that the mailer can request indicia and print them. It can also provide access to additional services such as the lookup of postal address databases, the lookup of postal rates, the retrieval of tracking numbers for certified, insured or registered mail, or the production of mail statements.

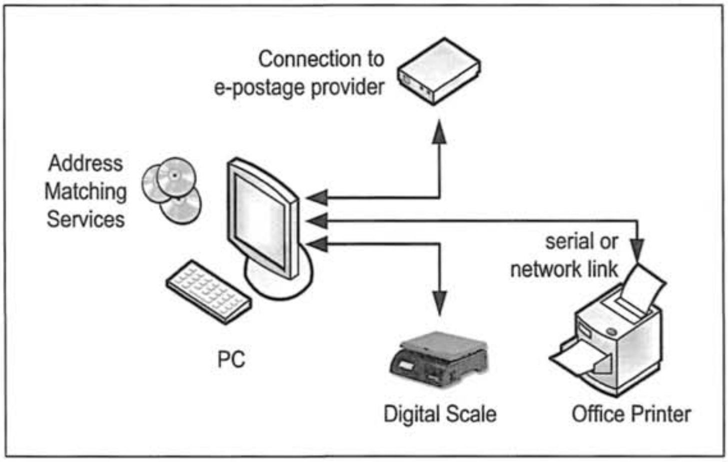


*Figure 19.*Schematic Diagram of an Open Online E-postage Device

3.1.3.1 Postal Security Device

In online e-postage systems, the e-postage provider runs a centralized repository of *virtual postal security devices*, one for each online e-postage device operated at a mailer's site. A virtual postal security device is a software instance representing a postal security device. Each online e-postage device connects to its e-postage provider in order to remotely use its virtual postal security device. This alleviates the need for mailers to maintain separate physical postal security devices at their sites.

The centralized repositories of postal security devices at the e-postage providers need to be operated within secure and controlled environments. The hardware security modules in which the virtual postal security devices are executed, fall under similar security requirements as the postal security devices of closed offline e-postage systems.

3.1.3.2 Life-Cycle

The virtual postal security devices follow the same life cycle as presented in Section 3.1.1.2 on page 58 except for the need to be re-initialized. Because virtual postal security devices are software instances of postal security devices, there is no need to re-use an already existing virtual postal security device for another customer. When a customer quits its contract, the respective virtual postal security device with the retired serial number, is archived, then reported to be scrapped, and never revived again.

From a user's standpoint, the life cycle looks a little different than that of an offline e-postage device, because online e-postage devices do not support to explicitly download postage into a virtual postal security device. Instead, every time a user deposits new funds at the e-postage provider, the e-postage provider will immediately increase the descending register of the user's virtual postal security device by the paid amount as soon as the payment transaction has been approved.

- ***User Registration***: A new user first needs to register with an e-postage provider of his choice and the e-postage provider needs to have the request for registration approved by the respective postal operator. The user must provide some payment instrument that works over the Internet, for example a credit card. In addition, the user is setup with an initial user identity such as a username and password or public key certificate such that the e-postage provider can recognize the user in all subsequent Internet transactions. After a user has been registered successfully, his virtual postal security device is created, initialized and authorized.
- ***Producing Indicia***: The user enters the mailing parameters for the mail piece he seeks to send and the registered password such that the online e-postage device can compile a corresponding indicia request message. The online e-postage device authenticates the indicia request message (for example by using a secure Internet connection via https) and sends it to the e-postage provider. If the user has sufficient postage available in the descending register of his virtual postal security device, the e-postage provider responds with an encrypted indicia confirm message. The response message is encrypted to not get used more than once for example by an eavesdropper. The online e-postage device decrypts the indicia confirm message and prints out the disclosed indicia.

- ***Logging User Activity***: The e-postage device shall have logging mechanisms in place that guarantee all user security-critical activities get logged in a persistent way that is likely to survive even catastrophic failures of the e-postage device.

3.2 E-POSTAGE PROVIDER SYSTEM

An e-postage provider system (see Figure 12 on page 28) serves the mailers' e-postage devices, either offline or online or both. Traditionally, closed offline e-postage devices have connected via modem, while open offline and online e-postage devices have connected over the Internet. These and other typical interfaces of an e-postage provider system are shown in Figure 20 on page 71. If a postal payment channel is established (Section 2.1.2.1 on page 29), the e-postage provider system maintains a communication link to a bank backoffice (see link 2a and Section 3.3 on page 84). Furthermore, the e-postage provider system maintains an e-commerce link to the post backoffice (links 3 and 5) and to the e-postage device registration system of the respective postal operator (link 13). In order to link the e-postage provider system activity with related business operations at the e-postage provider, the e-postage provider system maintains additional connections to

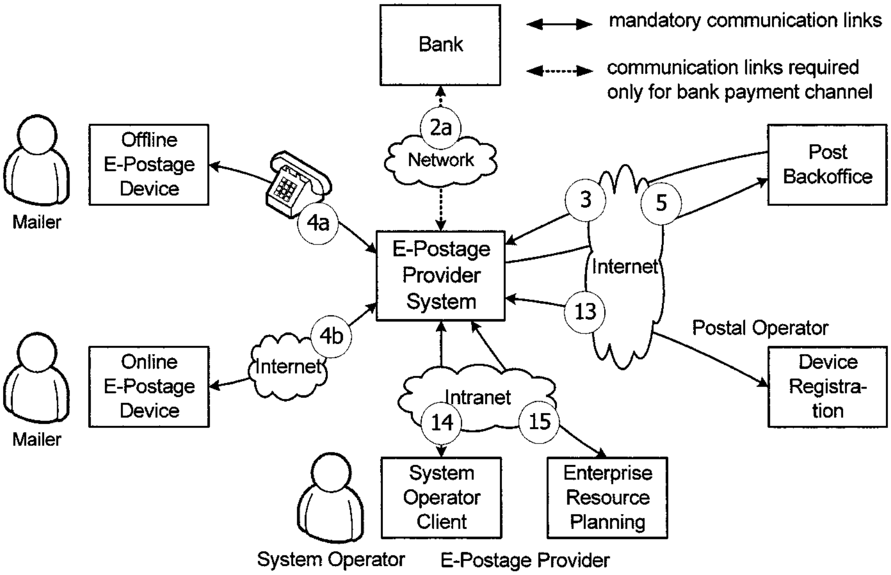


*Figure 20.*E-Postage Provider System and External Interfaces

- a system operator interface by which new records for e-postage devices can be created, assigned to customers in the ERP system, and managed over the entire life-time (see link 14).
- the enterprise resource planning (ERP) system, which controls the ordering process and subsequent delivery of e-postage devices (see link 15).

In order to look at the tasks of an e-postage provider system in more detail and to understand the interdependencies and relations between those tasks, we will focus on the software architecture of such systems [32]. We assume a client-server architecture, which allows us to separate the different concerns and requirements on the e-postage provider system, and to discuss it independently of implementation aspects, such as which implementation platform to use: Microsoft's .NET framework, Sun's Enterprise Java Beans (EJB), or the CORBA component model of the Object Management Group (OMG).

The technical architectures to be described are structured into two functional layers. The *application layer* describes the components related to certain interfaces of the system and the *common services layer* describes service components that are available to all components of the application layer. Conceptually, beneath the common services layer (but not shown in the following figures) are the operating systems, middleware, networks, and hardware architecture of the system.

Furthermore, the application layer is structured into three *distribution tiers*, which are labeled *presentation tier*, *enterprise tier* and *resource tier*, such that the components in any given tier communicate only with other components in the same or adjacent tiers. The distribution tiers describe how the components of the application layer are mapped to a distributed computing system. A logical distribution tier can be deployed over one or more systems or nodes. Conversely, several different tiers can be deployed into a single system. In this way, each tier can be replicated and the components within any one tear can be load-balanced if desired. While the distribution into tiers is necessary for the system to scale up, the concept also scales down nicely. Eventually, the decision about how to map distribution tiers to physical server systems depends on the expected load of the overall system, on the power of the physical servers available, on the degree of availability required, and other factors.

3.2.1 Local and Remote State of an E-Postage Device

We have seen in Section 3.1 on page 51 that the state of an e-postage device is kept collectively in the memory of the e-postage device itself and in the memory of its embedded postal security device if it has one. We will call this the *local state* of the e-postage device. In addition, each e-postage device is supported by a respective e-postage provider. The e-postage provider system keeps a record about each e-postage device, which follows the local state of the e-postage device. We call this record the *remote state* of the e-postage device. For offline e-postage devices, the postal security devices keeps the most part of the local state, whereas for online e-postage systems, the virtual postal security device keeps the most part of the remote state.

Note, however, that the remote state is not just a backup of the local state, which is updated every time the e-postage device connects to the e-postage provider. For example, if a mailer calls the e-postage provider to report that his e-postage device has been lost or stolen, then the operator of the e-postage provider system will set a blocking flag in the respective record, which indicates that the e-postage device should be blocked as soon as it connects to the e-postage provider the next time. This blocking flag is a part of the remote state of the e-postage device. In general, the local state and the remote state are respective views of the entire state of an e-postage device. Both, the local state and the remote state are independently updated within the e-postage device and at the e-postage provider, respectively. Each time the e-postage device connects to the e-postage provider, they synchronize their respective views such that after each connection, the local state equals the remote state.

3.2.2 Offline E-Postage Device Interface

We will look first at the technical architecture of an e-postage provider serving closed e-postage devices, i.e., postage meters (see Figure 21 on page 73)

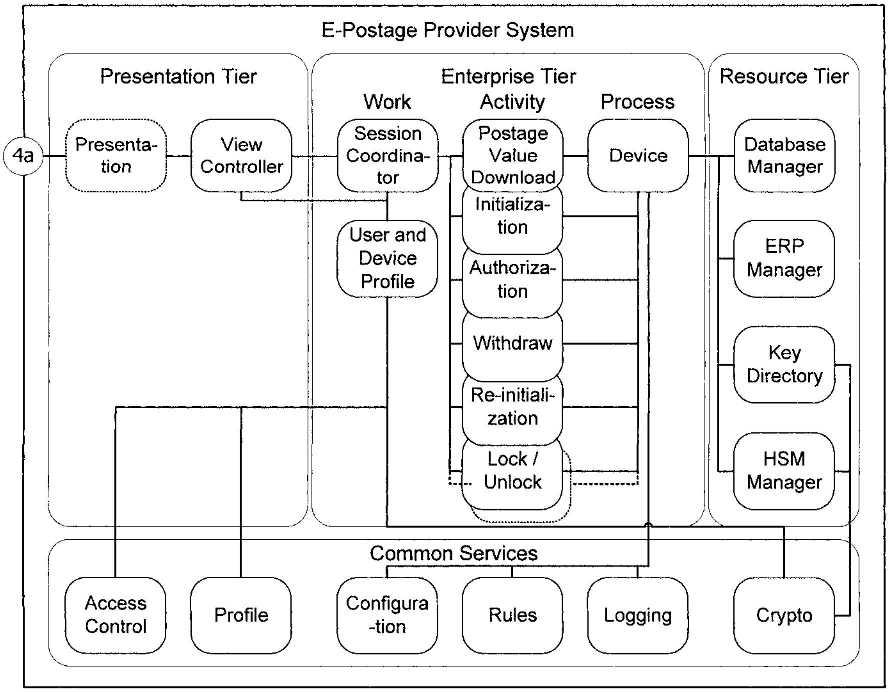


Figure 21. Offline E-Postage Device Interface: Technical Architecture

Let us follow a service request as it is processed by the e-postage provider system.

3.2.2.1 Presentation Tier

The mailer's e-postage device contacts the e-postage provider system either through a modem line (found with most postage meters) or through the Internet. If the postage meter allows the e-postage provider system to display content to the mailer and to format the content on the display, then the front-end component on the e-postage provider side is a presentation component followed by a view controller, both situated in the presentation tier. The presentation component determines the look-and-feel of the content displayed on the postage meter, and the view controller provides the right content depending on the mailer's user profile. For example, mailer's who have not paid for certain value-added services will not get displayed the respective commands or options. The user and device profile component is supported by the common services of access control, profile storage and cryptographic services. The access control component provides password establishment and verification services, the profile storage component maintains user profiles, and the cryptographic service component provides session key establishment, encryption, certificate and authentication services (see Chapter 4 on page 91).

3.2.2.2 Enterprise Tier

In the enterprise tier, the session component takes care of the entire session to serve each command of the mailer. The session component opens a communication session upon request of the mailer, and determines what kind of service the mailer requests. Then it passes the service request to the respective activity components, like 'initialization', 'authorization', 'postage value download', etc. (see Section 3.1.1.2 on page 58). Next, the session component negotiates the security attributes of the session and establishes them, exchanges the subsequent message between the respective activity component and the e-postage device, finally closes the session and reports to the activity component either success or failure. The security attributes are chosen according to the security policy, which is laid down in the *rules* common service and may also depend upon the particular mailer's user profile, which is laid down in the *user and device profile* component. How user profiles and device profiles are managed is defined by the *profile* common service. The temporary cryptographic keys used during a session are generated and maintained by the *session controller* component, which uses the *crypto* common services. Persistent cryptographic keys and public key certificates that are associated to an e-postage device are maintained within the *user and device profile* component by using the *key directory* component in the resource tier through the *crypto* common services. Certificate revocation lists are provided by the crypto common services as well. Persistent cryptographic keys that are associated to the e-postage provider are maintained by the *hardware security module* (HSM) component, which is also located in the resource tier and is accessed through the *crypto* common services. Most postal operators require this for security reasons.

There is one *device* component for each postage meter. Each *device* component maintains the remote state of its e-postage device. The *remote state* of an e-postage device is set of data representing the status of the e-postage device, as far as it is known to the e-postage provider at any one time. The remote state includes the life-cycle state, the postal registers and additional information about the e-postage device. The *device* component of each e-postage device stores its remote state persistently by using the *database* component in the resource tier. This information is updated every time a session component reports a session result for the respective postage meter. If the session was successful, the postage meter is switched to the new state. If the session was unsuccessful, the postage meter either remains in the previous state or is kept in an intermediate state. An intermediate state can occur if during a session a transaction was started, but left the postage meter and the e-postage provider system in inconsistent states, for example, because the communication line was interrupted. In this case the *device* component takes care of recovering from the intermediate state the next time it is contacted by its postage meter. *Device* components enforce the integrity of their postage meters by applying a number of rules laid down in the *rules* common service. They check if a requested service is allowed in the current state of their postage meter, they apply plausibility checks (e.g. the ascending register value must not decrease), boundary checks (e.g., the postal registers must exceed certain limits), and integrity checks to the postal register values (e.g., if the total settings register equals the sum of the ascending register value plus the descending register value).

3.2.2.3 Resource Tier

The *database* component provides database access for managing persistent data such as user profiles and e-postage device profiles.

The *ERP* component provides services to an enterprise resource planning system such as SAP or PeopleSoft, which typically maintain the customer database and customer account database. The *ERP* component also provides account related and statistical services such as managing several client accounts under one master account, increasing or reducing the credit limits of mailers, requesting account balances, producing account statements, which may include transaction statements, and doing statistical analysis of the e-postage provider system's operations.

The *key directory* component provides access to a secret key directory or public key directory (PKD) together with related public key certificate services.

The *HSM* component provides access to cryptographic services of one or more tamper resistant hardware security modules. Typical cryptographic services are encryption and decryption, computing and verifying digital signatures and message authentication codes, as well as producing and verifying public key certificates. Several RAID disk arrays or hardware security modules can be used in parallel load balanced operation in order to achieve higher availability. A popular hardware security device that has a fast cryptographic processor, integrates nicely into standard server hardware through a PCI-bus and is highly tamper resistant is the IBM crypto-coprocessor 4758-002 [35]. Table 11 on page 76 lists some examples of hardware security modules chosen by e-postage providers for use by their *HSM* components:

Table 11. List of FIPS 140-2 Certified Postal Security Devices

Certificate No	*Device*	*Manufacturer*	*Type*	*Photo*	*E-Postage Provider*
#97	Postage Server Crypto Module	n/a	multi-chip embedded	n/a	Stamps. com
#134	Postal Cryptographic Coprocessor	IBM	multi-chip embedded		PSI-Systems
#365	Neopostage PSD Module	IBM	multi-chip embedded		Neopost
#570	Secure Generic Sub-System (SGSS)	Thales e-Security	multi-chip embedded	n/a	Deutsche Post AG

3.2.3 Online E-Postage Device Interface

The online e-postage device interface is designed in a similar way as the offline interface as shown in Figure 21 on page 73). The architecture is presented in Figure 22 on page 77). Online e-postage devices connect to the e-postage provider system typically through the Internet. The layout of the web pages is controlled by the *presentation* component, the order in which web

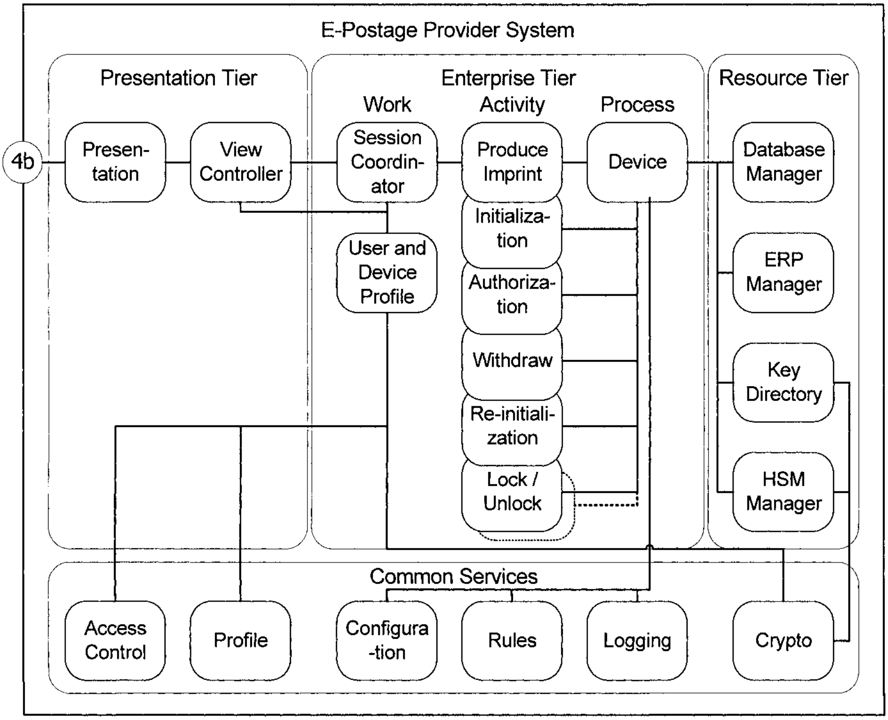


*Figure 22.*Online E-Postage Device Interface: Technical Architecture

pages are presented to the mailer is controlled by the *view controller* component. The view controller component has access to the profile of the e-postage device and its customer in order to display the options corresponding to the plan the mailer signed up for. The session component enforces proper access control and communication security during any remote service of an online e-postage device. Online e-postage devices do not carry their own local postal security devices. Instead, their PSD states (initialized, authorized, etc.) including their postal registers are only maintained by the *device* component as part of their remote state. Thus, state changes can only be triggered by the *device* component, which uses respective activity components (*initialization* component, *authorization* component, etc.) and the *database* component in order to persistently store remote states of e-postage devices. In addition, the *device* component provides the remote service of computing an imprint by using the *imprint* component. Note that this is the only PSD-related remote service available to an online e-postage device.

3.2.4 Database of Remote States

For closed e-postage devices, the communication protocol between the closed e-postage devices and the e-postage provider is usually proprietary so that the e-postage provider effectively fends off unknown e-postage devices from using its services. In open e-postage systems, however, the communication link between the open e-postage device and the e-postage provider is usually a standard Internet protocol such http or https. In order to mitigate the risks of an openly accessible service interface, some postal operators require that the database of remote states has to be cryptographically protected against unauthorized modifications (including insertions and deletions).

One way to do this is to store each remote state in encrypted form in the database and to decrypt a remote state every time it is accessed. The encryption and decryption keys for doing so, can be the same for all remote states, and should be stored in a secure place such as within the hardware security module that stores other cryptographic keys associated to the e-postage provider system anyway (*HSM*-component).

3.2.4.1 Virtual Postal Security Device

When the E-Stamp system was developed, the US Postal Services required that the e-postage provider system would have to use a cryptographic protection of the database of remote states, even though each i-Button persistently stored the PSD portion of the local state in tamper responsive memory. In the E-Stamp system, the PSD portion of the remote state was called a *virtual* PSD. The virtual PSD was updated every time the open online e-postage device performs a postage value download. During the period between two postage value downloads, the values of the local PSD and those of the virtual PSD are not synchronized and may differ.

3.2.5 System Operator Interface

Each e-postage device's record, which is maintained by its *device* component, needs to be accessible by an operator of the e-postage provider for general book keeping tasks as well as for emergency cases. Typical tasks of an operator are the following:

- creating a new e-postage device in the system,
- assigning it to a mailer's account,
- blocking its operations in case it is reported lost or stolen,
- unblocking it after it has returned to regular operation,

- inspecting its log files,
- other supplemental services.

The operator interface can be implemented by a web based service (Figure 23 on page 79). In this case there is a presentation component and a view controller to it, which work as explained in Section 3.2.2.1 on page 74. It is advisable to distinguish operators by individual user profiles the same way as mailers are distinguished. In the enterprise tier there is one component for each of the above activities. These components report to the device component of the respective postage meter, which maintains updates the state of the postage meter accordingly.

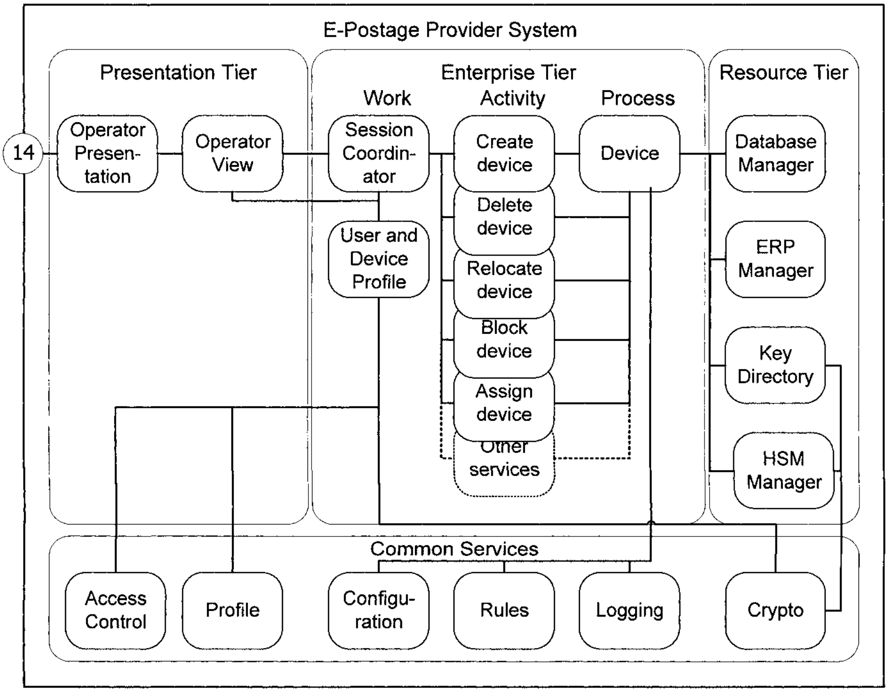


*Figure 23.*E-Postage System Operator Interface: Technical Architecture

3.2.6 Financial Interface

The optional financial interface connects the e-postage provider system to the bank through which mailers are supposed to pay for their postage (see Figure 12 on page 28, interface (2a). This option applies if the postal operator requires a bank payment channel (see Section 2.1.2.1 on page 29). The interface is a bi-directional business-to-business interface following the protocol and data formatting requirements of the respective bank (see Figure 24 on page 80). The *B2B controller* component takes care of formatting the data transferred to the bank and interpreting the data received from the bank. If the bank supports an encrypted communication channel, the *B2B controller* component manages the respective cryptographic keys and applies them to encrypt and decrypt through the *crypto* common services (this use of *crypto* common services is not shown in Figure 21 on page 73 in order to not clutter up the diagram too much). As the postal operators require electronic postage to be prepaid, the financial interface is used by the bank to inform the respective e-postage providers about the pre-payments of their customers. Usually, there is a nightly batch job in which the bank transmits the remittance files indicating which customers have paid which amount of postage. The *daily jobs* component retrieves these remittances and passes them on to the respective activity components. One of them is the *ACH* component, which handles remittance files and adjusts the credits that are maintained by the respective

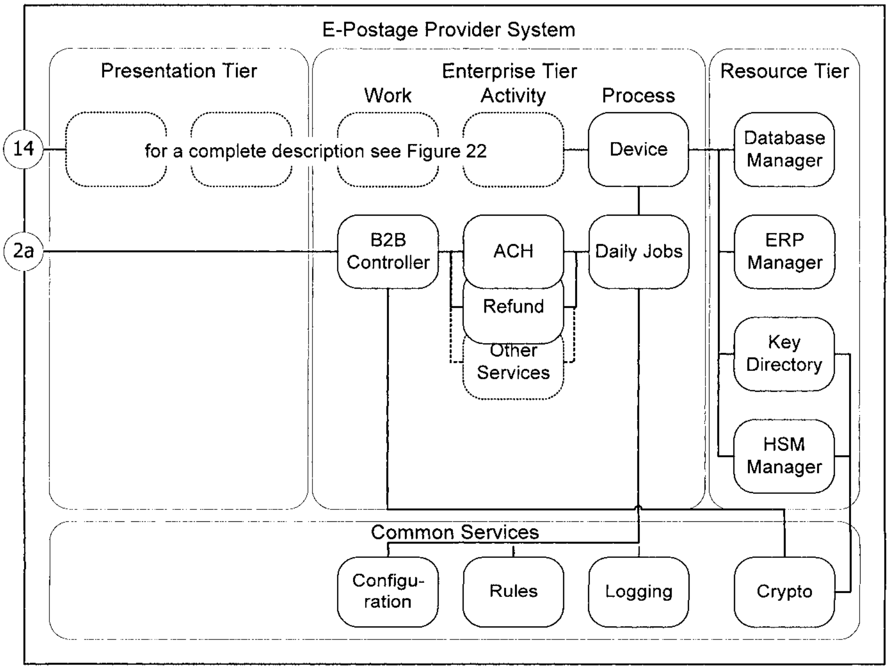


*Figure 24.*Financial Interface: Technical Architecture

device components. Once the e-postage device is brought into the state *authorized* or *valid*, the mailer can perform a postage value download up to the prepaid amount.

When an e-postage device is withdrawn, the *withdraw* component will track its new state and remaining amount of postage in its profile. Next time the *daily jobs* component comes across this profile, it will pass to the *refund* component to read out the remaining amount of postage and include the serial number and refund amount in the notification data to be sent off to the bank during the next nightly batch. Eventually, the bank is to refund the customer for example by sending him a check.

If the postal operator requires a postal payment channel (see Section 2.1.2.1 on page 29), then the financial interface of the e-postage provider system is with the postal operator backoffice instead of the bank.

3.2.7 Postal Interface

The postal interface connects the e-postage provider system to the post backoffice (see Figure 12 on page 28, links 3 and 5). It is a business-to-business interface following the protocol and data formatting requirements of the respective postal operator. The *B2B controller* component takes care of formatting the data to be exported to the post backoffice and interpreting the data imported from there. If the post backoffice supports an encrypted communication channel, the *B2B controller* component manages the respective cryptographic keys and applies them to encrypt and decrypt through the *crypto* common services (this use of *crypto* common services is not shown in Figure 25 on page 82 in order to not clutter up the diagram too much).

The postal interface is activated on a regular basis, typically at the end of each business day. Caching and/or blocking mechanisms must be in place in order to synchronize the activities at the postal interface and those at the service interface to the e-postage devices. The postal interface needs to support the following tasks:

1. Offline e-postage devices only: Report to the post backoffice all postage value downloads and all withdrawals since the previous report was sent.
2. Report to the post backoffice the usage data of all e-postage devices that have contacted the e-postage provider since the last report was sent. (This data is not requested by all postal operators.)
3. Offline e-postage devices only: Report of the refunds that were granted to customers who have withdrawn their e-postage devices.

4. Report to the post backoffice a list of all e-postage devices that have been reported lost or stolen since the last report.
5. Either export to the post backoffice the new verification keys that have been established for all e-postage devices whose keys have expired since the last report, or import from the post backoffice some new cryptographic authentication keys for those e-postage devices.
6. Import or export any other data that is required for additional services according to Section 2.3 on page 39. Examples are the import of updates of complete or partial postage rate tables, the import of *tracking numbers* (or ranges of *tracking numbers* from which e-postage devices can pick *tracking numbers*) that may be used to identify certified or registered mail or to prepare for undeliverable mail.

Each of these activities is managed by a respective activity component. Figure 25 on page 82 shows the respective part of the component architecture.

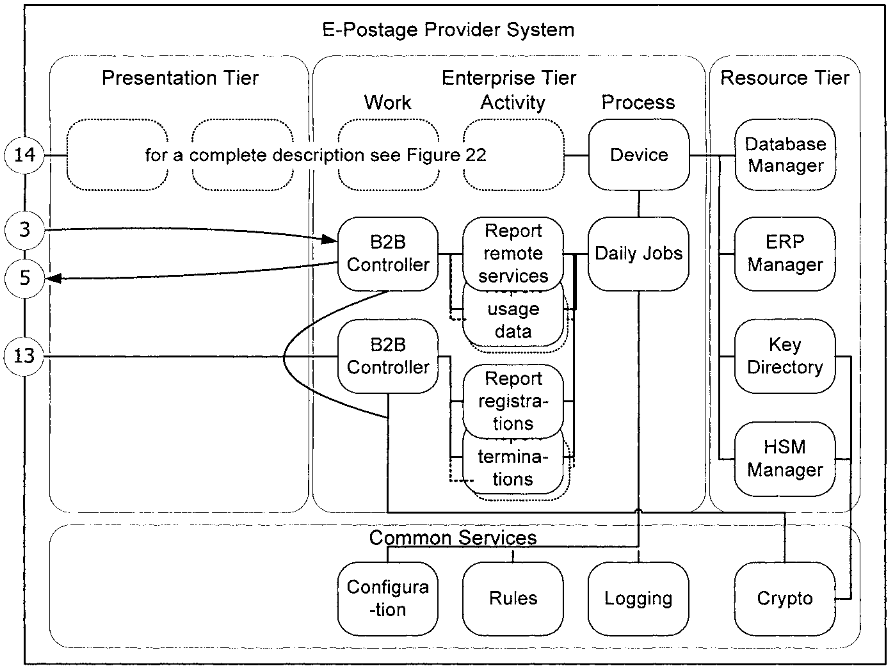


Figure 25. Postal Interface and Postal Registration Interface

The *rekey* component, which takes care of proper and timely rekeying of cryptographic keys of all e-postage devices (not shown in Figure 25 on page 82) uses the crypto common services in order to access the key directory in the resource tier.

3.2.8 Postal Registration Interface

Before an e-postage device may be delivered to a customer, most postal operators require the e-postage provider to register the new installation of an e-postage device. The minimum information required is the name and identity of the customer, the identity of the e-postage device, the location where the new e-postage device is going to be operated, the licensing Post office if it is a closed e-postage device, and the date when the new e-postage device is going to be delivered to the customer.

The identity of an e-postage device is in fact a combination of identities of its parts that are relevant to the postal operator. The following Table 12 on page 83 lists the combination of IDs for each class of e-postage device:

Table 12. Identity of an E-Postage Device

	special purpose hardware *closed system*	*general purpose hardware* *open system*
offline	• ID of the physical device (mail handler including printer) • ID of the postal security device	• Software license number of the customer installation • ID of the postal security device
online	• ID of the physical device (mail handler including printer)	• Software license number of the customer installation

Other services provided by the postal registration interface are the following:

1. Informing the postal operator which customers wish to terminate the contracts for which of their e-postage devices. More specifically, which e-postage devices have been returned by the customer (closed e-postage devices), or permanently de-activated by the e-postage provider.
2. Informing the postal operator which e-postage devices have been relocated to which new locations and to agree new licensing Post offices for those that are closed e-postage devices.

Although from a conceptual viewpoint, the postal registration interface is a part of the postal interface, the postal operators usually provide separate systems to support the registration services. In other words, the postal registration services are not necessarily integrated in the post backoffice system of a postal operator. The postal registration interface may require a different data format and communication protocol than the postal Interface, it may use other or no communication security mechanisms and it may not even be fully automated. That is why we design the postal registration interface by means of a separate *Registration B2B controller* component followed by a number of activity components for registration, termination and relocating e-postage devices (see Figure 25 on page 82). All of these activity components are connected to the *daily jobs* component, which is explained in Section 3.2.7 on page 81.

3.3 POST BACKOFFICE

The post backoffice system of a postal operator serves all e-postage provider systems participating in its e-postage minting system. Each postal operator's e-postage program is different, and so are the sets of services provided by its post backoffices. The following is a list of typical services provided by a post backoffice, not all of which must be implemented by each existing post backoffice.

3.3.1 Link to Bank

If a postal payment channel is used, the post backoffice bills or debits the mailers through the bank for purchases of e-postage (see link 2b). If a bank payment channel is used, the e-postage providers forward the funds to the postal operator, which is basically an interaction between their banks.

3.3.2 Link to E-Postage Provider

The post backoffice receives the daily transaction reports and optional usage data reports from its e-postage providers over link 5. Either the post backoffice provides the cryptographic keys needed by the e-postage provider or e-postage devices to produce valid indicia (link 3), or, otherwise, the e-postage provider sends them to the post backoffice (link 5). In order to manage each e-postage device's life cycle, various other data items are exchanged through this interface of link 3 and 5. Examples are rate tables, mail identifiers for track and trace services, information about assignments of e-postage devices to new mailers, relocations of mailers, lost and stolen e-postage devices, rekeying of cryptographic keys, and withdrawals of e-postage meters from existing mailers.

3.3.3 Link to Mail Processing Center

The post backoffice is connected to all mail processing centers through communication link 9, which is structured as follows: The post backoffice connects to a cryptographic key directory where it stores the actual cryptographic keys that will be required to verify the imprints of all e-postage devices of all e-postage providers. The post backoffice updates this key directory on a daily basis according to the key update information it receives from its e-postage providers. All mail processing centers are connected to the key directory such that they can read any cryptographic key they need to verify all indicia in the mail stream.

There is a second directory, which archives the indicia of all mail pieces processed. It is updated by each originating mail processing center, which reports all indicia it has read and their reading results. The post backoffice can access this indicia database in order to reconcile the amounts of e-postage and amounts of optional usage data reported by its e-postage providers and the amounts of indicia read by the mail processing centers. Various statistical analyses are performed taking into account the total number of indicia and their total amount of postage. If the post backoffice collects usage data from all e-postage devices, these totals can be matched down to the level of single rate categories.

An almost sharp reconciliation can be done for indicia of online e-postage devices because the e-postage providers can report the date of mailing for each indicia they provide and the delay between induction, i.e., mailing date, and reading at the originating mail processing center is well known by the postal operator.

How sharp a reconciliation is possible for indicia of offline e-postage devices, depends on how uncertain the delay is between the download of postage and the time of induction. There is unlimited uncertainty if the post backoffice collects no usage data reporting the date of mailing. In this case, it can only match up the amounts of e-postage given out in certain periods of time with the amounts of indicia processed in similar periods of time. Otherwise, if the usage data report the dates of mailing down to the level of days, weeks, months, or quarters, then the post backoffice can do a reconciliation at the same level.

3.4 MAIL PROCESSING CENTERS

Each postal operator runs a number of mail processing centers (MPC) to collect, sort and forward mail pieces. These mail processing centers are the work horses of each postal operator, and they are key to the postal operator's profitability. The higher labor costs a postal operator faces, the more optimized and automated logistics within and between mail processing centers are required.

3.4.1 Processing Mail

The goal of any network of mail processing centers is to minimize the maximum delivery time of all mailings. This goal can be achieved well in a flat network of mail processing centers, where the mail between any two centers can be exchanged in about the same time, for example, overnight. To make up for the remaining differences in delivery time, each center processes those mailings first that have left the longest time to travel. This principle suggests the following four stage schedule, which is typical for mail processing centers:

- **Cancellation**: All mailings collected from post offices, private and street mail boxes are properly cancelled if they carry stamps.
- **Outgoing**: Mail that has passed the previous stage is run through a two or three step sortation process. The recipient address is read and printed onto each mail piece by means of a *delivery point barcode.* Based on the recipient addresses, the outgoing mail is divided into three types. Type 1 contains all recipient addresses that lie within the actual mail processing center's area. Type 2 contains all addresses lying within driving distance (typically 200 to 300 miles). Type 3 contains all other addresses including international ones. All type 3 mailings are forwarded immediately to the nearest airport to be sent off as air cargo to the respective destination mail processing center or (one of) the international mail processing center(s) of the originating country. Next, type 2 mailings are forwarded by respective mail trucks. Type 1 mailings are left over for the last stage (walk sequence sortation).
- **Incoming**: Afterwards, all mail coming in from other mail processing centers (including the international ones) is collected and merged with the type 1 mailings left over from the previous stage.
- **Walk Sequence Sortation**: Type 1 mail and all mail collected in the incoming stage above are sorted automatically to the carrier level in walk sequence. The sorting is based upon the delivery point barcode that was printed on each mailing at the originating mail processing center.

Mail processing centers may differ by throughput and volume, but not by speed because they need to work in a synchronized fashion, where all of them perform the same stage in the same time window.

Next day delivery can be achieved for all mailings for which this schedule—including the transport times between the stages—can be completed overnight. The flat network and synchronous mail processing imposes about the same delivery time upon all mailings. Even a mail piece that is sent next door will only be delivered on the next day.

If the postal delivery network spans across a larger geographic area, the differences in delivery time between two mail processing centers increase up to a point where one delivery time, namely the longest, does not fit everybody's needs any more. Beyond this point, it is more appropriate to organize the mail processing centers in a two or even more layer hierarchy of mail processing center networks. Each geographic region is covered by a bottom layer subnetwork of centers, and each subnetwork has one dedicated center linking it up to the second layer network, and so on. Large national postal delivery networks and the international postal delivery network are organized in this way.

3.4.2 Postage Verification at Mail Processing Centers

Mature reading technology for recognizing typed or handwritten recipient addresses is deployed in most industrial countries. The technology for reading and recognizing 2D bar codes is following suit. Deutsche Post reported they had 2D bar code reading facilities installed nationwide in 2004. The US Postal Services reports to achieve the same for the US by 2006. To do so, the former multi-line optical character recognition (MLOCR) devices are replaced by full face CCD cameras, which pick up the entire face of each mailing. The digitized image, typically scanned at about 203 dpi, is forwarded simultaneously to an address recognizing system and a postmark recognizing system. The postmark recognizer looks for a certain graphical image, such as the keyword "US Postage" or similar, and then expects to see the 2D bar code at a specified offset from the anchor point of the recognized image. The 2D bar code is then decoded and the resulting plain data fields are checked for consistency, plausibility and replay. Finally, the integrity check code in one of the data fields is verified by using the respective cryptographic key from a key directory maintained by the postal operator.

Some e-postage programs require the postal operator to store individual cryptographic keys for each e-postage device in its key directory, others just require to maintain one cryptographic key per e-postage provider, and again others require to store just one system key for all e-postage providers. Regardless what type of key is used, these keys must be replaced by fresh ones on a regular basis. The rekeying periods are specific to each e-postage program. Mail pieces whose indicia could not be read, decoded, checked and verified successfully, are sorted out and are followed-up by special recovery procedures.

Large mail processing centers use several sorting lines each operating at about 35,000 pieces per hour. Probably the most challenging of all checks at this speed is the check for duplicates. In order to detect copies of indicia, one needs to compare each indicia read with all other indicia carrying the same mailing date, which is most likely the business day before the actual reading. An average size mail processing center running 4 sorting lines at full speed for 7.5 hours archives about 1 million indicia per day. The US Postal Services operate about 350 mail processing centers, which gives us an average volume of 350 million indicia to be archived on every business day, amounting to 100 billion indicia per year, the yearly volume of first class mail in the US (see Table 5 on page 22). One way of deciding whether an archived indicia matches an actual indicia is to compare their *cryptographic checksums* or truncated checksums because they are relatively short and unique representations of postage indicia. Only if a match is found need the other data fields be compared.

In order to compare each indicia read with all indicia of the same mailing date archived, the duplicate checker had to compare in every second 10 indicia times 4 sorting lines times 350 mail processing centers, i.e., 14,000 indicia against 350 million indicia archived every business day. The cost for such a duplicate checker that must be based on a highly available distributed database for online comparisons of indicia could not be justified given current technology.

Best practice exercised in today's mail processing centers is to verify cryptographic indicia and check for duplicates locally within every mail processing center, but not across different centers. For example, Deutsche Post AG has installed the cryptographic hardware accelerators WebSentry™ PCI of Thales e-Security [73], which are based on the Secure Generic Sub-System (see Table 11 on page 76), in all mail processing centers to verify indicia.

The approach of checking duplicates just locally at each mail processing center could be attacked by copying indicia onto two or three different mail pieces of the same class of mail and the same rate category, and inducting these mail pieces on the same day at post offices or mailboxes that feed their mail to different originating mail processing centers. This can be achieved if the fraud is organized at a geographic location close to the border between two or three mail processing districts, but appears somewhat far fetched.

A statistical analysis of how many duplicate or counterfeit postage indicia are expected to escape detection at a mail processing center under varying critical parameters such as the sampling rate (fraction of postage indicia read), fraudulent indicia rate (fraction of duplicate or counterfeit indicia), read rate (fraction of honest indicia readable), and others is provided in the UPU Standard S34-4 [114] Annex F. One of the—perhaps not surprising—conclusions is that an attacker can maximize the number of undetected duplicates or counterfeits if he produces at most one duplicate of each honest indicia.

Chapter 4

Cryptography Primer

4.1 BASIC CRYPTOGRAPHIC MECHANISMS

In modern cryptology, there are some basic mechanisms, which are essential to achieve security in distributed systems and hence in e-postage systems. We introduce these mechanisms at a conceptual level, which explains their security properties and how their cryptographic keys, if any, shall be managed. This will prepare our understanding of the existing e-postage systems in Chapter 6 on page 127, Chapter 7 on page 167 and the particular threats that apply to these systems (see Chapter 8 on page 183). Readers who are interested in a more detailed description and analysis of these mechanisms are referred to the Handbook of Applied Cryptography of Menezes, Oorschot and Vanstone [54], the Encyclopedia of Security and Cryptography of van Tilborg [74], or the reference work Applied Cryptography by Schneier [70].

The basic classes of cryptographic mechanisms include the following: Encryption mechanisms achieve message confidentiality. Message authentication codes protect the integrity of data and its originator. Digital signature mechanisms protect the integrity of data, its originator and achieve non-repudiation, i.e., provide evidence that no-one else than the claimed signer is the originator of a signed message. Until the 20th century, encryption was the primary if not the only purpose of cryptography [43]. Since the discovery of public key cryptography in the early 1970s, however, message authentication codes and digital signature mechanisms have become at least as important as encryption. In e-postage systems, for example, they are used to protect the individual indicia.

The users of a cryptographic mechanism employ individual *cryptographic keys* to establish and maintain their privileges. For example, only users whose e-postage devices hold a suitable cryptographic key can produce valid indicia. History has shown that any secret can be broken, be it an unknown cipher mechanism or an unknown cryptographic key. It is only a matter of time, effort and determination as David Kahn has shown by numerous examples in his book "The Codebreakers" [43]. The security of a cryptographic mechanism will thus be measured in terms of a minimum effort an attacker takes to break it. In order to maintain a cryptographic mechanism over a period of time it should allow for increasing its security, thus anticipating the simultaneously increasing power of potential attackers. An ideal security mechanism has a *security parameter* that determines the minimum amount of effort required to break it, and a proof that it cannot be broken with less effort. The larger security parameter is chosen, the more effort is required to break the mechanism. Such an ideal mechanism can be laid open for public review and be used as a firm security feature for everyone to use with her or his individual keys. This is the security mantra of modern cryptology: Rest the security of a cryptographic mechanism only on keeping the respective cryptographic keys secret, and do not rely on obscuring the mechanisms themselves from the prying eyes of potential attackers.

The grain of salt is, however, that all the practical and useful cryptographic mechanisms known today are just approximations of the above ideal. For the most efficient mechanisms, mathematical proofs are rare, and for the less efficient but still practical ones, all the mathematical proofs of security known today rest on more or less realistic but unproven assumptions and most of them use controversial computational abstractions, such as the random oracle model [74]. Although the situation is unsatisfactory and needs improvement, there are many cryptographic mechanisms available that have sufficient evidence of security to them, and these are subject to ongoing standardization and regular review processes.

The security problems of real systems employing standardized cryptographic mechanisms come most probably from wrong implementations [44], use of insecure random generators, or poor key management. To put it in perspective, problems at the cryptographic mechanism layer are much less frequent than the notorious security problems filling the news headlines such as ill-handled PINs and passwords, ill-configured firewalls and virus scanners, and security holes in operating systems. See all the subsections entitled "What Goes Wrong" in a large variety of real systems [1] by Anderson.

We will now look at each class of cryptographic mechanisms one by one.

4.2 CONFIDENTIALITY AND PRIVACY

Confidentiality is the security property of whether a sender can transmit a message to a recipient such that the message is intelligible only by the recipient, but not to an intelligent attacker such as an intruder and eavesdropper. In order to achieve data confidentiality, the sender must transform the plaintext into some ciphertext, such that the ciphertext reveals no information about the plaintext to an attacker. Only the intended recipient(s) of the message can transform the ciphertext back into plaintext.

One way to achieve data confidentiality is to use a conventional, also called *symmetric encryption mechanism*. Another is to use a public key, also called *asymmetric encryption mechanism*.

If a sender is to transfer a confidential message m to a recipient over an insecure channel, they employ an encryption mechanism that provides a key generation, an encryption and a decryption service. The sender and/or recipient runs the key generation service in order to achieve an encryption key e and a decryption key d, and make sure the sender obtains the encryption key over a secure *key transport channel*, while the recipient obtains the decryption key. The sender inputs the message m and the encryption key e to the encryption service in order to achieve a ciphertext c, which is sent over the insecure channel. The recipient inputs the ciphertext c and its decryption key d to the decryption service in order to recover the plaintext message $m' = m$. The concept of an encryption mechanism is depicted in Figure 26 on page 93.

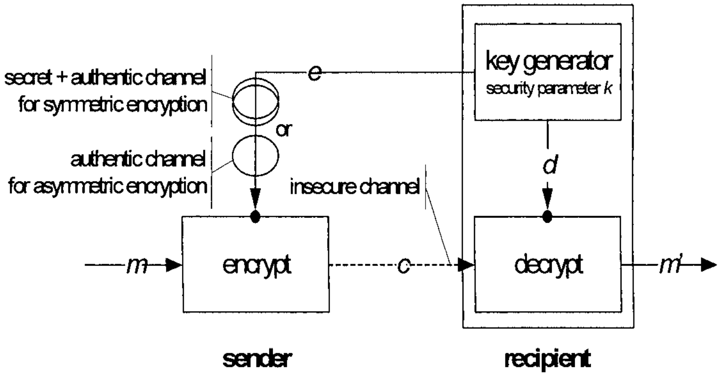


*Figure 26.*Encryption Mechanism

4.2.1 Symmetric Encryption

Symmetric encryption mechanisms use a key setup, where the encryption key equals the decryption key ($d = e$). Since the sender and recipient use this same key, it is called a *shared secret key* or *symmetric key*. Symmetric encryption mechanisms are also called *secret key encryption mechanisms*.

Secret keys must be transferred from the recipient to the sender or vice versa over a secret and authentic key transport channel, that is the secret key must neither be disclosed to nor be modified or replaced by an attacker on the key transport channel. In the data flow diagram of Figure 26 on page 93, the secret and authentic key transport channel is indicated by a line that has a double circle around it.

In order for many parties, say n, to communicate pair wise and securely, they need to establish, distribute and maintain at least $n(n+1)/2$ secret keys, which becomes a fairly large number for large n.

Examples of approved symmetric encryption mechanisms are the advanced encryption standard (AES) [87], and Triple-DES (3DES) [87,36].

4.2.2 Asymmetric Encryption

Asymmetric encryption mechanisms use a key setup, where the encryption key is different from the decryption key. The recipient generates a pair of cryptographic keys, say (d, e), such that d is infeasible to compute when only e is given. The decryption key, d, is called a *private key* because it is to be kept private by the recipient. The encryption key, e, is called a *public key.* because it is disseminated by the recipient to enable everyone to encrypt messages to him. A pair of matching private and public keys is called a *public key pair.* Asymmetric encryption mechanisms are also called *public key encryption mechanisms.*

Asymmetric encryption keys must be transferred over an authentic—not necessarily secret—key transport channel. In the data flow diagram of Figure 26 on page 93, the authentic channel property is indicated by a line that has a single circle around it. Such an authentic key transport channel can be provided by means of public key certificates (see Section 4.5.4 on page 113) managed in a public key infrastructure (PKI) or by a trusted courier. The encrypted message, i.e. the ciphertext, is transmitted over an insecure channel, which may be accessed by an attacker.

When n participants use such an *asymmetric encryption mechanism,* they need to generate, distribute and maintain only n keys, which makes key management significantly easier than by using a symmetric encryption mechanism. Examples of asymmetric encryption mechanisms are RSA and ElGamal encryption.

4.2.3 Constructions

Symmetric and asymmetric encryption mechanisms are usually constructed from symmetric and asymmetric block ciphers, respectively. A block cipher consists of a key generation service, a keyed block encryption service and a keyed block decryption service. The block encryption service maps a block of plaintext to a block of ciphertext, and the decryption service is the reverse map when keyed with the decryption key matching the encryption key. A block cipher is asymmetric if the decryption service uses a key that is infeasible to compute from its matching key, which is used by the encryption service. Otherwise, it is called a symmetric block cipher. A symmetric (asymmetric) encryption mechanism is obtained by iterating a symmetric (asymmetric) block cipher by using a proper *mode of operation* such as cipher block chaining, output feedback mode, or other. The interested reader is referred to [54].

4.2.4 Security of Encryption Mechanisms

The security of an encryption mechanism is parametrized by its security parameter, which controls the key generating service. The bigger security parameter is used, the larger encryption and decryption keys result. The security parameter specifies the decryption key length in bits which means, that an increase of the security parameter by one doubles the space an attacker needs to work through if he is trying to figure the decryption key by an exhaustive search (trial encryption).

There are three types of attacker goals, which can be pursued independently of how an actual attack proceeds. These goals are listed below in the order of increasing severity:

- *Selective cryptanalysis* aims at figuring the plaintexts for one or more ciphertexts, which are given to the attacker.
- *Universal break* aims at figuring a decryption key that is equivalent to the victim's decryption key, in the sense that it maps given plaintexts to the same ciphertexts.
- *Total break* aims at figuring the victim's decryption key.

One distinguishes active and passive attacks. *Passive attacks* allow the attacker to obtain information from the victim that the victim produces anyway. An *active attacker* is given additional power to request certain information of his choice from the victim.

For encryption mechanisms, seven types of attack are distinguished. They are listed in the following Table 13 on page 96 in the order of increasing attacker power (left column). Attacks 1 to 3a are passive, while attacks 4 to 7 are active. The victim has a secret key (in case of a symmetric encryption mechanism) or a private key (in case of an asymmetric encryption mechanism). In case of an asymmetric encryption mechanisms, the respective encryption key is known to the attacker. Each type of attack is specified by the information the attacker is allowed to request from the victim in a defined way (right column).

Table 13. Types of attack on encryption mechanisms

	Type of attack	*Allowed information or interaction*
1	key-only attack (asymmetric only)	victim's encryption key.
2	ciphertext-only attack	one or more ciphertexts.
3	known-plaintext attack	one or more pairs of matching plaintext and ciphertext.
3a	exhaustive search	a known-plaintext attack, where the attacker encrypts a given plaintext under all possible encryption keys until the result matches the given ciphertext.
4	chosen-plaintext attack (symmetric only)	ciphertexts matching the chosen plaintexts.
5	adaptive chosen plaintext attack (symmetric only)	like chosen-plaintext attack, but the plaintexts can be chosen one by one depending on previously retrieved ciphertexts.
6	chosen ciphertext attack	plaintexts matching the chosen ciphertexts.
7	adaptive chosen-ciphertext attack	like chosen-ciphertext attack, but the ciphertexts can be chosen one by one depending on previously retrieved plaintexts.

An encryption mechanism is all the stronger, the stronger attacks it can resist and the weaker goals can be achieved by attacks it cannot resist.

4.3 HASH FUNCTIONS

A cryptographic hash function or simply *hash function* is an efficiently computable compression function $h(x) = y$ that maps binary strings x of arbitrary length to binary strings y of some fixed length. The fixed length results are called *hash values*, or *hash results*. The security properties of hash functions are in order of increasing strength:

1. *Preimage resistance*: For essentially all hash values, given a value y it is practically infeasible to compute a pre-image x such that $h(x) = y$. This property is also called *one-way*.
2. *Second preimage resistance*: Given any pre-image x, it is practically infeasible to find another pre-image $x' \neq x$, such that $h(x') = h(x)$.
3. *Collision resistance*: It is practically infeasible to find any two pre-images $x' \neq x$ that map to the same image $h(x') = h(x)$.

Note that collision resistance implies second pre-image resistance because breaking an attacker who can figure second pre-images can also find collisions.

4.3.1 Constructions

Since hash functions may take arbitrarily long inputs, they need to include some iterating mechanism that can be applied to portions of the input again and again until the entire input is digested. The most prominent such iterating scheme is due to Merkle [56]. Suppose f is a compression function that maps inputs of $n + r$ bits to outputs of n bits, where r is called the *block size*. The hash function is constructed as follows. To a given input x of length b bits append a deterministic padding pattern, e.g., all zeroes, such that the padded input can be represented as t contiguous blocks x_i, each of size r. Next, append to the last block of x_t an additional block $x_{t+1} = b$ (for $b \geq 2^r$ use more than one additional block). Finally, let the hash value be $h(x) = H_{t+1}$, where

$$H_0 = \underbrace{00\ldots0}_{r\text{-times}} \text{ and } H_i = f(H_{i-1} \| x_i) \text{ for } i = 1\ldots t+1 \tag{4.1}$$

A schematic diagram of the construction is shown in Figure 26 on page 93. This construction is proven to act like an amplifier of collision resistance because if f is a collision resistant compression function for inputs of $n + r$ bits, then the hash function f is collision resistant for all inputs of lengths $b < 2^r$.

Most practically relevant hash functions follow the above construction. Three types of compression functions are in use. Block ciphers, are proven cryptographic primitives and available in many systems. Modular arithmetic performs slower than block ciphers, but is provably secure in a stricter sense than block ciphers. Customized compression functions are designed without relying on proven cryptographic primitives and aim at optimizing the perfor-

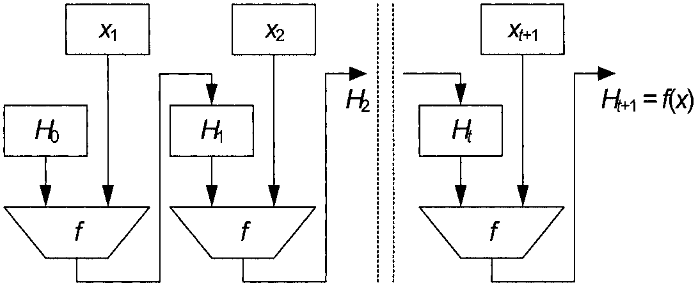


*Figure 27.*Constructing a Hash Function from a Compression Function

mance of the entire hash function. Candidates of the latter type are MD4, MD5, RIPEMD-160 and SHA-0 and SHA-1 [4,92]. All of them are no longer considered to be sufficiently collision resistant (see Section 8.3.5.1 on page 192). The FIPS 180 standard [92] was amended in 2002 by the stronger hash functions SHA-256, SHA-384, and SHA-512, where the trailing numbers indicate the bit length of the hash values produced by these mechanisms.

4.4 MESSAGE AUTHENTICATION

Message authentication is the security property of whether a recipient of a given message can decide if the alleged sender is in fact the source of the given message, even if an intelligent attacker had a chance of modifying or making up the received message. Message authentication includes *data integrity*, i.e., the assurance that a piece of data has not been modified since it was created, sent, or stored by an authorized source.

In other words, message authentication is the assurance of data integrity in the presence of intelligent attackers. Were messages only subject to statistical transmission errors, it were appropriate to use a *cyclic redundancy check code* (CRC) to detect and correct those errors. If messages are subject to intelligent attacks, cyclic redundancy check codes would not help at all because an attacker could modify or make up messages arbitrarily and then compute and attach the matching CRCs. Thus, CRCs provide no assurance of the source of a message.

In order to verify message authentication, the recipient of the message must relate to the source of the message and to some cryptographic checksum included in the message, which may either satisfy the defined authentication condition or not. When a cryptographic message authentication mechanism is used, the recipient refers to the message source by means of a cryptographic key. Message authentication mechanisms that require the sender and the recipient of a message to use a *shared secret key* are called symmetric message authentication mechanisms, or *message authentication codes*. Mechanism where the sender and recipient use different but related cryptographic keys such that the sender's key is infeasible to compute from the recipient' key, are called *asymmetric message authentication mechanisms*, or *digital signature mechanism*.

If a message authentication code is used, the cryptographic checksum included in the message is itself called a *message authentication code* or *MAC* or sometimes *integrity check value,* and the shared secret key is called the *authenticating key*. If a digital signature mechanism is used, the cryptographic checksum is called a *digital signature*, or sometimes *electronic signature*, and the respective keys are called *signing key* and *verifying key*.

If a sender is to transfer an authenticated message m to a recipient over an insecure channel, they employ a message authentication mechanism that provides a key generating, an authenticating and a verifying service. The sender runs the key generating service in order to achieve an authenticating key s and a verifying key v, and makes sure the recipient obtains the verifying key, while the sender keeps the authenticating key. The sender inputs the message m and the authenticating key s to the authenticating service in order to achieve a cryptographic checksum c, which is sent together with the message m over the insecure channel. The recipient inputs the message m, the checksum c and its verifying key v to the verifying service in order to decide if the checksum is valid for the message with respect to the verifying key. The concept of a message authentication mechanism is depicted in Figure 28 on page 99

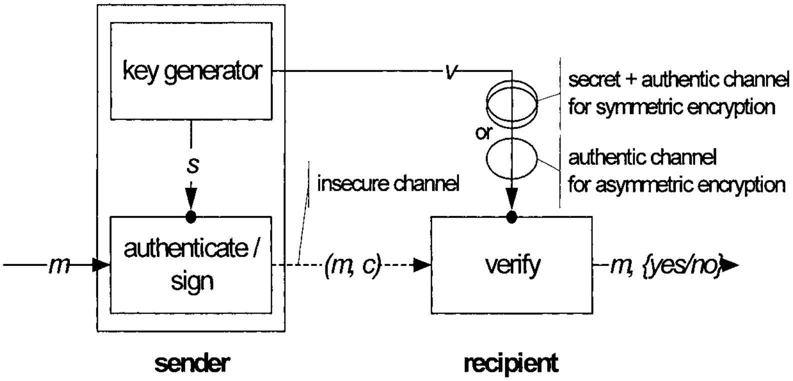


*Figure 28.*Message Authentication Mechanism

4.4.1 Message Authentication Codes

Symmetric message authentication mechanisms use a key setup, where the authenticating key equals the verifying key. This shared secret key must be transferred from the sender to the recipient or vice versa over a secret and authentic *key transport channel.* That is the secret key must neither be disclosed to nor be modified or replaced by an attacker accessing the key transport channel. In the data flow diagram of Figure 28 on page 99, the secret and authentic key transport channel is indicated by a line with a double circle around it.

In general, the recipient verifies a received message m and integrity check value c by first recomputing the integrity check code c' from the received message m and its own verification key $v = s$ and then comparing the resulting c' to the received integrity check value c. He accepts the message as originating from the alleged sender if the two values match, or otherwise rejects the message as bogus data.

A natural way of constructing message authentication codes is to choose a hash function and apply it to the message and the authentication key at the same time. The resulting hash value is used as the integrity check value. However, employing a collision-resistant hash function is no guarantee to achieve a secure message authentication code without taking further precautions. Several proposals such as secret prefix (Section 4.4.1.1 on page 100) and secret suffix (Section 4.4.1.1 on page 100) have been proposed and were found to be flawed. The state of the art in constructing message authentication codes from hash functions is the HMAC.

4.4.1.1 Secret Prefix and Secret Suffix

A simple construction is to use the authentication key s as a *secret prefix* to the message m and hash the concatenation of both in order to obtain the integrity check value $c = h(s \| m)$. Here, the symbol $\|$ denotes concatenation of two bit-strings. Alternatively, the authentication key can be appended as a *secret suffix* to the message: $c = h(m \| s)$. These simple construction designs suffer from different weaknesses outlined in [54] §9.5.2 and are not recommended for use.

4.4.1.2 HMAC

The state of the art in constructing a message authentication code from a hash function is to use the hash-based MAC called HMAC, proposed by Krawczyk, Bellare and Canetti [46] and standardized as FIPS 198 [96]. It consists of two nested applications of a chosen hash function h to the message m and the authentication key s as follows:

$$c = h(s \,\|\, \text{opad} \,\|\, h(s \,\|\, \text{ipad} \,\|\, m)) \quad . \tag{4.2}$$

The inner (outer) application of the hash function uses an inner (outer) pad, ipad (opad), in order to bring the argument of the inner (outer) hash function to a multiple of the block length of h. Krawczyk et al conclude that the strongest attack known against HMAC is based on the frequency of collisions for the underlying hash function h by means of a "birthday attack", and is totally impractical for minimally reasonable hash functions. The construction is quite efficient to compute because the argument of the outer hash function is only two blocks long independently of the length of the message m.

4.4.1.3 Truncation

It is common to truncate the output of a message authentication code in order to fit the size constraints of the application or environment. For example, the output of an HMAC-SHA1 is a 160-bit hash value. HMAC is recommended to be used with its output truncated not below half of the underlying hash function's block length, i.e. 80-bit in the above example. The truncated HMAC is denoted as HMAC-SHA1-80. Under certain conditions it can be truncated down to 32-bits. The security implications depend on the application and environment in which the MAC is applied (see Section 8.3.5.3 on page 195). Note that during the verification of a message authentication the recipient truncates its MAC outputs in the same way as the sender.

4.4.2 Digital Signatures

Asymmetric encryption mechanisms use a key setup, where the verification key is different from the authentication key. The sender generates a pair of cryptographic keys, say (s, v), such that s is infeasible to compute when only v is given. The authenticating key, s, is called a *private key* because it is to be kept private by the sender. The verification key, v, is called a *public key.* because it is disseminated by the sender to enable everyone to verify his messages. A pair of matching private and public keys is called a *public key pair.* Asymmetric message authentication mechanisms are also called *digital signature mechanisms.* The authenticating operation is called (digital) signing, and the cryptographic checksum is called a *digital signature.*

Asymmetric verification keys must be transferred over an authentic—not necessarily confidential—key transport channel. In the data flow diagram of Figure 28 on page 99, the authentic key transport channel is indicated by a line with a single circle around it. Such an authentic key transport channel can be provided by means of public key certificates (see Section 4.5.4 on page 113) managed in a public key infrastructure (PKI). The signed message is transmitted over an insecure channel, which may be accessed by an attacker.

There are two types of digital signature mechanisms: A *digital signature mechanism with appendix* requires the signer to send messages together with a respective appendix, namely the digital signature. Only if a recipient receives the message, the digital signature and the claimed signer's verifying key, he can verify if the digital signature is valid. A *digital signature mechanism with message recovery* allows the recipient of a signature to recover the message from the signature. Such a signature mechanism can be used in two ways.

- The signer can send messages and appended signatures just as he would with a signature mechanism with appendix. A recipient would recover the message from the signature and if it matches the received message, he would accept the signature as valid for the received message.
- Alternatively, the signer defines and publishes once a redundancy check for his messages. Afterwards, he only sign messages that satisfy the redundancy check and send these signatures without the corresponding messages. A recipient would recover the message from a received signature and if it satisfies the redundancy check, he would accept the signature as valid for the recovered message.

4.4.2.1 Truncation

In contrast to message authentication codes, the verifying operation is substantially different from the signing operation, which implies that truncating digital signatures is useless.

4.4.3 Security of Message Authentication Mechanisms

There are four types of attacker goals on digital signature mechanisms, which can be pursued independently of how an actual attack proceeds. These goals are listed below in the order of increasing severity:

- *Existential forgery* aims at figuring a signature for any new message, which the attacker has not asked to sign before.
- *Selective forgery* aims at figuring a signature for a new message chosen by the attacker.
- *Universal break* aims at figuring a signing key that is equivalent to the victim's signing key, in the sense that it produces signatures that are valid with respect to the victim's verifying key.
- *Total break* aims at figuring the victim's private key.

In case of a message authentication mechanism, the four goals above apply, where the terms "signature" is to be replaced by "message authentication code", and the terms "signing key" and "verifying key" or both to be replaced by "authenticating key".

For message authentication codes and digital signature mechanisms four types of attack are distinguished. They are listed in the following Table 14 on page 103 in the order of increasing attacker power (left column). Attacks 1 to 2a are passive, while attacks 3 and 4 are active. The authenticator has a secret key (message authentication code), while the signer has a private key (digital signature mechanism). In case of digital signature mechanism, the respective verifying key is known to the attacker. Each type of attack is specified by the information the attacker is allowed to request from the victim in a defined way (right column).

Table 14. Types of Attack on Message Authentication Mechanisms

	Type of attack	*Allowed information or interaction*
1	key-only attack	victim's verifying key (applies only to digital signature mechanisms)
2	known-message-attack	one or more pairs of messages and matching message authentication codes or signatures.
2a	exhaustive search	a known-message attack, where the attacker tries all possible signing/authenticating keys until he finds one for which the given message authentication code/signature matches the given message.
3	chosen-message attack	message authentication codes/signatures matching the chosen messages.
4	adaptive chosen-message attack	like chosen-message attack, but the messages can be chosen one by one depending on message authentication codes/signatures requested in between.

A message authentication mechanism or digital signature mechanism is all the more unforgeable, the stronger attacks it can resist and the weaker goals can be achieved by attacks it cannot resist.

Non-repudiation (of data origin) is an additional security property of digital signature mechanisms requiring that signers cannot repudiate their digital signatures. A digital signature mechanism is non-repudiable, if a third party, which is neither the sender nor the intended recipient of a given message can verify if the message originated from the alleged sender, even if an intelligent attacker had a chance of modifying or making up the received message.

Message authentication codes do not allow a third party to cryptographically distinguish the sender from the recipient of a message because both of them use the same shared secret key in order to authenticate and to verify messages. Either party can equally originate a message using that shared secret key. Therefore, message authentication codes cannot provide non-repudiation (of data origin). If non-repudiation is required, one can use either an online trusted third party or a digital signature mechanism.

4.4.3.1 Rivest, Shamir, Adleman (RSA) Signatures

The RSA signature mechanism was published in 1978 by Rivest, Shamir and Adleman, hence the acronym RSA. The signing and verifying operations are exponentiations modulo a composite number, which needs to be at least 1024 bits long in 2005. In order to sign a message, it is recommended to first compute a collision-resistant hash of the message, which is called a *message digest*, and then to sign the hash using the RSA exponentiation. The most widely used mode of operating RSA with a hash function is PKCS#1 v1.5 [69]. No practical attacks have come up against it, but a few special cases were found to be vulnerable. Finding more provably secure modes of operating RSA is still a subject of cryptologic research and standardization. See, for example, the more recent PKCS#1 v2.1 and the overview of the RSA Digital Signature Scheme by Kaliski [74].

4.4.3.2 Digital Signature Algorithm (DSA)

The DSA signature mechanism was announced in 1994 by the National Institute of Standards and Technology as FIPS 186 [93], and is also standardized by ANSI as X9.30-1 [3]. The signing and verifying operations are based on exponentiations modulo a prime number, which should be at least 1024 bits long. As for RSA, it is recommended to first compute a collision-resistant hash of the message and then to sign the hash using the DSA exponentiation. The proposed procedure for generating public key pairs and the proposed mode of operating DSA with a hash function such as SHA-1 is specified in FIPS 186-2 [94], which is going to be superseded by FIPS 186-3 [95] to allow larger sizes for keys and signatures. DSA is considered to be sufficiently secure against existential forgery under adaptive chosen message attacks if a plausible complexity theoretic assumption holds, SHA-1 is a one-way and collision-resistant hash function, and the signing operation employs an unpredictable random bit sequence generator (see Section 4.5.2.2 on page 110) for generating temporary keys [115].

4.4.3.3 Elliptic Curve DSA (ECDSA)

The ECDSA signature mechanisms was announced in 2000 by NIST as FIPS 186-2 [94] and was standardized as ANSI X9.62 [7]. ECDSA works like DSA, but is based on elliptic curve arithmetic instead of modular arithmetic, which allows to achieve the same level of security with shorter keys and shorter signatures. Hence, the modular exponentiations of DSA are written as integer multiples of a point on an elliptic curve. A set of recommended elliptic curves is included in the standards mentioned above.

ANSI X9.62 was adopted in 1999 and has just completed its first 5 year review. The original standard was revised in three areas. The choice of hash functions was extended from SHA-1 only to the whole SHA family including SHA-224, SHA-256, SHA-384, and SHA-512 because of the reported collision attacks on SHA-1 (see Section 8.3.5.1 on page 192). This update applies both to DSA and ECDSA. Binary fields of order 2^m for composite m are excluded to avoid certain attacks on elliptic curves, and the set of 15 elliptic curves recommended by FIPS 186-2 were included. ECDSA is sufficiently secure under similar assumptions as those for DSA [115].

4.4.3.4 Pintsov-Vanstone Signatures (ECPV)

The Nyberg-Rueppel signature mechanism, like DSA, works over finite fields or elliptic curves as an underlying arithmetic [33]. An adaptation of the elliptic curve based Nyberg-Rueppel signature scheme that provides partial message recovery was proposed by Pintsov and Vanstone [66]. It was shown by Brown and Johnson [13] to be secure against existential forgery under reasonable assumptions and has been standardized by ANSI X9.92 (draft), IEEE 1363a [34], UPU S36-4 [114], and CEN EN 14615 [19]. Nevertheless, the Pintsov-Vanstone signature mechanism is not approved for use by any postal operator in any of the existing e-postage systems also because of intellectual property reasons.

4.4.3.5 Comparison of Lengths of Digital Signatures

For postage indicia, one is interested in small footprints. The following Table 15 on page 106 lists in column 2 the digital signature mechanisms and message authentication codes that are used in industrial e-postage systems. Columns 3 to 6 indicate the lengths of (3) the public keys, (4) private/secret keys, (5) length of the message digest input and (6) length of the resulting output signature or message authentication code. Column (7) indicates the bandwidth, i.e., the number of bits to be conveyed by the signer to the recipient such that the recipient can verify the signature given he has already retrieved the verifying key of the signer. According to the NIST key management guideline [98] the parameters chosen for RSA, DSA, ECDSA, and ECPV lead to a similar level of security. The bottom line 5 refers to a truncated message authentication code MAC-SHA1-32 that is used in Frankit (see Section 6.5.1.1 on page 155). Its security has not been proven.

Table 15. Comparison of Lengths of Digital Signatures

		Length [bit]				
	Mechanism	*Public Key*	*Private Key*	*Message digest*	*Signature/ MAC*	*Bandwidth*
1	RSA	1024	1024	≤ 1024	1024	≤ 2048
2	DSA	1024	160	≤ 160	320	≤ 480
3	ECDSA	160..192	160..192	≤ 160..192	320..384	≤ 480..576
4	ECPV	160	160	160	320	320..400
5	MAC-SHA1-32	—	≥ 160	unlimited	≥ 32	unlimited

For all mechanisms except ECPV, the bandwidth is the sum of the lengths of the message and the MAC/signature. For ECPV, the bandwidth is the sum of the lengths of the non-recoverable part of the message and the signature.

4.5 KEY MANAGEMENT

The general advantage of asymmetric mechanisms is their easier key management, while the advantage of symmetric mechanisms is their faster performance—by one to two orders of magnitude faster than asymmetric mechanisms on standard processors. In order to combine and leverage both advantages, most distributed systems follow a hybrid approach towards key management, which can be described in four steps.

1. All system entities supposed to store security-critical data are supposed to have established an authentic communication channel with a dedicated public key directory service within the distributed system.
2. Each such entity establishes its own long lasting cryptographic identity by generating a public key pair of a digital signature scheme. The respective verifying keys are submitted over the assumed authentic channels to the system wide public key directory.

3. Whenever two entities need to communicate securely, they establish a shared session key between them. The protocol used to establish the session keys relies upon the ability of both entities to retrieve each other's authentic signature verification keys from the key directory.
4. The two entities finally use the established session key for encrypting their messages with a fast symmetric encryption mechanism.

This approach highlights the importance of managing long lasting cryptographic keys (see step 2.) and of establishing symmetric session keys (see step 3.). Each of these topics is addressed in the following chapters.

4.5.1 Key Management Life Cycle

Little management of cryptographic keys were necessary, if they had an infinite life time. However, the deeper reason of using cryptography and thus cryptographic keys lies in the value of resting security upon secret values that are easy to change if necessary. According to Kerckhoff's principle, the security of a system should totally rely on keeping certain cryptographic keys secret and not at all on the obscurity of the system design. Should the secret key(s) fall into an enemy's hands, all you need to do is to replace them. The most economic way to keep a system secure is to concentrate all secret keeping efforts on a small portion of information, namely, the respective cryptographic keys, and to provide graceful rekeying mechanisms for each of them. As Bruce Schneier put it: "Every secret creates a potential failure point. Secrecy, in other words, is a prime cause of brittleness—and therefore something likely to make a system prone to catastrophic collapse. Conversely, openness provides ductility" [50]. This is why cryptographic keys must be replaced on a regular basis or at least be replicas upon request, and explains why cryptographic key management is inevitable and mission critical for any system that is cryptographically secured. In other words, the goal of cryptographic protections is to reduce desirable system security requirements to key management requirements. For example, encryption mechanisms help to keep a multitude of messages confidential if only the respective decryption key is kept secret. This is why key management is of paramount importance.

More specifically, cryptographic keys should be managed according to a life-cycle, which comprises the following four stages. In case of public key pairs of asymmetric mechanisms, the private and public key may be handled differently but consistently in each stage:

- The *pre-operational stage* is entered when a cryptographic key (pair) is first generated (Section 4.5.2 on page 109), derived from a master secret or established between two or more parties by a key agreement mechanism (see Section 4.5.3 on page 112). Keys can be exported from one device for distribution or transport and imported into another device. Secret and/or authentic channels should be used for key transport depending on the type of key exported. In this stage, the public part of a public key may get registered to a registration authority, which verifies the key owner's identity. After a proper identity check of the owner, the public key is assigned a unique name, its validity period is determined and it is certified by a certification authority (see Section 4.5.4 on page 113).

- The *operational stage* is entered when a key (pair) is installed from the pre-operational stage to operational use, such as producing ciphertext, or message authentication codes or digital signatures, depending on the type of key under consideration. If the key is not compromised it remains in the operational stage until its validity is about to expire. In this stage, the key can be backed up in order to be safe stored for a short period and restored from the safe storage.
- The *post-operational stage* is entered if the key is retired from operational use either by a regular rekeying when its validity period is about to expire, or when the key must be revoked because it has been compromised or is suspected to have been so. In either case, the previously operational key is no longer accessible for normal use. A replacement key will be generated and installed and the cause of the key compromise be investigated. Post operational keys are usually archived, i.e., stored offline for extended periods of time, to be accessible only under special circumstances. For example, to verify a long lasting digital signature or to settle a dispute involving repudiation.
- The *destruction stage* is entered when the key is irreversibly deleted and all its copies are erased from the system directories and logs.

The key management life cycle is depicted in Figure 28 on page 99. All transitions of one key instance from one stage to another are depicted by solid arrows. The trigger to replace an operational key usually launches a new key-instance into pre-operational stage. This trigger is indicated by a dotted arrow.

In order to transport the very first cryptographic keys for example between each initial party and a key directory service, secure communication channels need to be used that are protected by conventional means such as trusted couriers or other trusted channels. At this bottom end, initial keys need to be safe-stored without requiring further cryptographic keys. This can be achieved by split knowledge mechanisms such as secret sharing. A good overview of most

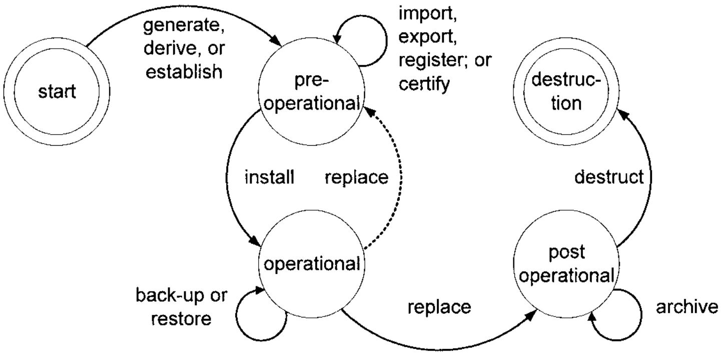


*Figure 29.*Key Management Life Cycle

practical aspects of cryptographic key management is given in the NIST key management guideline [98].

The cryptographically involved operations during the key management life cycle are considered in more detail in the following sections.

4.5.2 Random Bit Generators

The security of any cryptographic system using cryptographic keys, e.g., encryption and message authentication mechanisms, relies on the random choice of these keys. A *k*-bit string chosen truly at random requires an attacker an average effort of trying 2^{k-1} values before he figures the chosen key. Thus, the effort of an exhaustive search of a cryptographic key grows exponentially in the length of the key if it is chosen truly at random. In contrast, if a *k*-bit key is chosen by using an *l*-bit random value, which is then expanded to *k*-bits by a (deterministic) function *f*, for example a hash function or other complicated computation, then the resulting key can be figured by an average number of 2^{l-1} trials of choosing a random value for *l* and running it through *f*.

1. Truly random bits can be generated by using some physical effects such as
2. intervals of emission of particles during radioactive decay,
3. thermal noise of semiconductor diodes or resistors,
4. instabilities of the frequency of a free running oscillator, or
5. noise from microphones or video cameras.

The output of devices using physical sources of randomness is usually biased (the probability of emitting a 1-bit is not 1/2) or correlated (the probability of emitting a 1-bit depends on previously emitted bits) and should be smoothed or de-skewed before it is used as a random bit sequence. Generators based on oscillators and semiconductors can be encapsulated in hardware security devices, and thus be protected from access by active attackers. An efficient yet not provable smoothing technique is to pass the sequence of biased or correlated bits one or more times through a cryptographic hash function.

In many cases, a hardware random number generator is not available or is not efficient enough to produce enough keying material in a given time interval. In these cases, pseudo-random bit generators can be used. A *pseudo-random bit generator* is a deterministic algorithm that takes as input a random binary string of length *k*, called the *seed*, and outputs a binary string of length $l \gg k$ that looks random. Of course, the output sequences are not random, simply because only a fraction of 2^{k-l} of all possible output sequences can be produced. Note that a pseudo-random bit generator started twice on the same input seed produces exactly the same output sequence. However, good pseudo-random bit generators produce output sequences that cannot be efficiently distinguished from truly random sequences of length l.

4.5.2.1 Constructions

Pseudo-random bit generators can be constructed by iterating one-way functions as first shown by Shamir [71]. First the seed is taken to initialize the internal state of the generator. In each round, a one-way function is applied to the current value of the internal state and its output become the new internal state. Afterwards, an output function is applied to the new internal state in order to extract a fixed amount of output bits, which are appended to the output sequence of the generator. Efficient constructions of practical yet unproven security are obtained if the one-way function is instantiated by a hash function or block encryption function as is standardized by ANSI X9.17 [2], ANSI X9.82 [8], and FIPS 186-2 [94].

Less efficient construction of provable security (under a number theoretic assumption) can be obtained by instantiating the one-way function by a cryptographically secure one-way function such as RSA decryption (Micali-Schnorr [57]) or modular squaring with a secret modulus (Blum-Blum-Shub [12]).

4.5.2.2 Security

If an attacker cannot observe the output of a pseudo-random bit generator, then the classical analysis of pseudorandom numbers as outlined by Knuth

[45] Chapter 3 is appropriate and sufficient. The *entropy* of a pseudo-random bit generator is the amount of information carried by its output sequence. Because the output sequences are a deterministic map of the seeds, the entropy of each output sequence cannot exceed the length of the seed. In contrast, the entropy of the output sequence of a truly random generator is the number of bits of the output sequence itself. The seed of a pseudo-random bit generator should be chosen larger than what is tractable by an exhaustive search, that is at least 80-bit long.

Since pseudo-random bit sequence generators do in fact not produce random bit sequences, the best one can expect to prove is that their output is sufficiently close to being random. There are a number of statistical tests each of which rules out a certain class of weaknesses in the output sequence of a pseudo-random bit sequence generator. If the outcome of any of these statistical tests is negative, we can say that the pseudo-random bit sequence generator shall be rejected. Otherwise, however, we can only conclude that the given generator does not suffer from the weakness we have just tested. We may continue to investigated the given generator by applying another statistical test, or decide to stop and accept the given generator as producing "sufficiently random" output. Six of the better known statistical tests are listed below:

1. Frequency Test (monobit test): This is to verify that the output sequences contain nearly as many zeroes as ones.
2. Serial Test (two-bit test): This is to verify that the output sequences contains nearly as many two-bit sequences 00, 01, 10, and 11, where the 2-bit sequences are allowed to overlap.
3. Poker Test: This is to verify that the output sequences contain nearly as many m-bit strings of either value if the entire output is divided into non-overlapping m-bit strings, with an appropriate upper bound on m. This is a generalization of the frequency test, where $m = 1$.
4. Runs Test: This is to verify if the length of runs of either zeroes or ones in the output sequences is as expected for a random sequence.
5. Autocorrelations Test: This is to check for correlations of each output sequence with a copy of itself shifted (non-cyclically) for i bits, where i takes values from 1 to an appropriate upper bound.
6. Maurer's Universal Statistical Test [52] and Improvements by Coron [21]: This test estimates the entropy of the output sequence. The closer this measure comes to the length of the seed, the more random looking is the output sequence. This test can detect a large class of statistical defects of the output sequence.

Pseudo-random bit generators whose output sequences can be observed by an attacker must not only produce statistically random looking outputs, but these outputs must also be *unpredictable*. For example, using the binary expansion of π yields a perfectly random looking bit sequence, which passes all the statistical tests mentioned above. However, it is totally useless as a generator for cryptographic keys because it is perfectly predictable. Once the attacker has seen enough of it, he can guess to have a prefix of the binary expansion of π in front of him, and from this point on he would know exactly what the next private keys will be.

This stronger requirement of unpredictability leads up to the definition of a cryptographically secure pseudo-random number generator: After an attacker has observed l bits of an output sequence, he shall be able to predict the next bit with no better probability than 1/2 plus a negligible fraction.

Pseudo-random bit generators need not be cryptographically secure if they are encapsulated within a hardware security module such that their output bit sequences are used to generate private or secret keys that are kept within the module at all times, where an attacker cannot observe them.

4.5.3 Session Key Establishment

Key establishment is a process or protocol to establish a shared secret between two or more parties for subsequent cryptographic use. A secret can be established by having one party generate or otherwise obtain the secret and then transferring it to the other party or parties over a secret and authentic channel. This is called a *key transport protocol*. Alternatively, each participating party can contribute some input data from which a joint secret is derived by some kind of multi-party computation. Ideally, no single party can predetermine the secret outcome. This is called a *key agreement* protocol.

In general, the establishment of session keys can be secured by utilizing symmetric or asymmetric mechanisms. A good overview is given in [54] §12. With a view towards modern distributed systems as delineated in Section 4.5 on page 106, we put our focus on key establishment techniques that rely on asymmetric cryptographic mechanisms.

A simple 1-pass key transport mechanism combined with subsequent symmetric encryption is *hybrid encryption*. A sender who wants to send a confidential message encrypts the message using a freshly generated symmetric session key, e.g. for AES, and afterwards encrypts the session key under the asymmetric encryption key of the intended recipient. The encrypted message is transmitted together with the encrypted session key to the recipient. The recipient decrypts the session key first in order to finally recover the plaintext message. See RFC 2440 (openPGP) [14]. Other examples of key transport mechanisms using public key encryption and digital signatures are the X.509 (2 pass) strong authentication protocol, which uses time stamps, and the X.509 (3 pass) strong authentication protocol, which uses random nonces [38]. Recommended key transport mechanisms are standardized by ANSI X9.44 [6].

Examples of key agreement protocols using digital signatures are authenticated Diffie-Hellman key agreement and the Station-To-Station protocol (STS) [54]. Recommended key agreement mechanisms are standardized by ANSI X9.42 [5].

More efficient key agreement protocols can be achieved by using implicitly certified public keys, which effectively combining the two steps 2. and 3. of Section 4.5 on page 106 into one. Examples are the protocol MQV named after its inventors Menezes, Qu, and Vanstone [55], and HMQV proposed by Krawczyk [47], which improves and optimizes MQV.

4.5.4 Public Key Certificates

In order to distribute public keys (for encryption of messages or verification of digital signatures), authentic channels are required from the system entity generating a public key pair to potentially all users of the respective public keys. One way to establish an authentic channel from a sender to a recipient is to use digital signatures that can be verified by the recipients using their previously acquired long-term verifying keys. Suppose a sender has a long-term signing key *sig* and the intended recipients hold the corresponding verifying key *ver* in their hands, then the sender can distribute a new public key *pubkey* by using the long-term key *sig* to compute a digital signature *sign* for *pubkey* and some associated book-keeping information. The entire record of *pubkey* and its the associated book-keeping information and the digital signature *sign* is called a *public key certificate cert*. The owner of the certifying key pair (*sig*, *ver)* is called the *issuer*, the certified key *pubkey* is called the *subject key*. The book-keeping information for each public key includes, the version of the certificate, its serial number, information about the digital signature (algorithm used, formatting information, etc.), its issuer and validity period, the subject public key, the issuer's unique ID, the subject's unique ID, and optional extensions, such issuer key identifier or subject key identifier.

A public key certificate *cert* is said to be valid for the subject key *pubkey* with respect to the issuer's verifying key *ver*, if the digital signature *sign*, which is contained in *cert*, is so for the record consisting of *pubkey* and its associated book-keeping information. A valid certificate *cert* binds the book-keeping information to the subject public key *pubkey* in a verifiable way.

The certifying process can be repeated each time *pubkey* needs to be rekeyed. The concept of public key certificates and how to use them to build public key infrastructures is standardized in ISO 9594-8 alias X.509 [38]. The producer of a certificate is called an *issuer*, while the certified public key is called a *subject key*.

Issuers should provide public key certificates only after properly identifying the applicant of the subject key. Otherwise, the book keeping data of the certificates might be misleading or plain wrong. Thus, an issuer is usually considered to consist of two entities, the registration authority (RA), which is responsible for verifying each applicant's identity, and the certification authority (CA), which is responsible for protecting the issuer's cryptographic keys and providing digital certificates for subject keys that have been cleared by the registration authority. How strongly applicants must be identified by a registration authority depends on the application and the risks imposed by wrongly issued certificates. Certificate requests can be posted by the applicants themselves or by third parties acting in behalf of the applicants. Whenever, we consider certificates being issued in the following, we always assume that the respective applicants have been properly registered in the first place.

4.5.5 Security Domains

In order for system entities to communicate securely, they need reliable mechanisms (i) to identify each other and (ii) to authenticate and/or encrypt their communication data. The identity of a system entity consists of its name and an individual cryptographic key. In order to identify another system entity, one needs to recognize that entity's name and cryptographic key, which in turn requires that one has learned those in the first place. Based on the prior knowledge of other entities' cryptographic keys, one can apply respective cryptographic mechanisms to the messages exchanged with that other entity. In open environments it is more efficient, though, to establish a central trusted authority to facilitate identification of system entities and subsequent secure communication between them. This approach leads to the concept of a security domain.

A *security domain* is a collection of system entities and communication channels, each operated by a party (*operator*) that is in charge of keeping the entity or communication channel alive and working. All operators of a security domain have come to trust in a single authority, which is usually called a *trusted authority*. The trusted authority defines the *security policy* over its security domain and enforces all operators to comply to this security policy [54].

The secure communication between system entities in a security domain originates from, and is maintained through, an entity-specific shared secret key or password (in the symmetric model), or possession of the trusted authority's authentic public verifying key (in the asymmetric model). In contemporary systems, the asymmetric model is preferred wherever possible because it allows a simpler and more flexible cryptographic key management. We outline a simple yet frequently used two layer public key management.

4.5.5.1 Boot Key Layer

The trusted authority establishes a *boot key pair* consisting of a private *bootSigningKey* and a public *bootVerifyingKey*. This key pair is shown in the lower half of the box representing the Trusted Authority in Figure 30 on page 115. The relationship between a private key and its corresponding public key is denoted by a diamond. Each time a new system entity joins the security domain, the trusted authority validates the new system entity's name and identity and hands over the bootVerifyingKey in return. The trusted authority is said to provide a *name registration service*. Once the boot key layer is established, each system entity can verify messages sent by the trusted authority. A complete boot key layer for a trusted authority with two system entities is shown in Figure 30 on page 115.

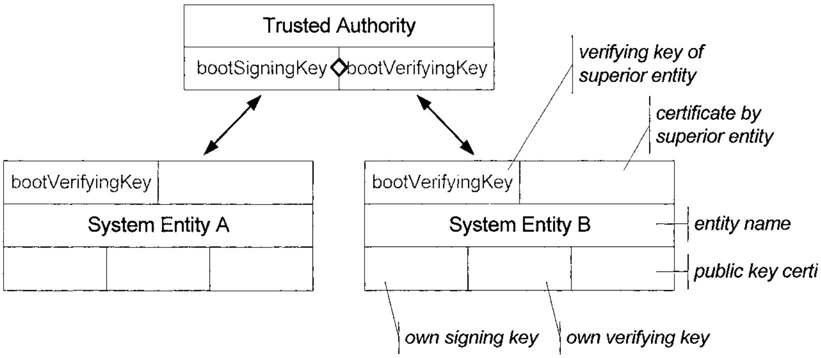


*Figure 30.*Boot Key Layer

4.5.5.2 Entity Key Layer

In order to enable system entities of the security domain to authenticate the originator and the messages of each other, they can establish an entity key layer as follows. Each system entity generates its own individual *entity key pair*, which consists of an entity signing key and an entity verifying key. Next, each entity requests a public key certificate (bootCert) for its entity verifying key from the trusted authority. If the public key certificate holds against the bootVerifyingKey, then the system entity stores the public key certificate permanently with its entity key pair. The relation between a public key and a matching public key certificate is indicated by a double diamond in Figure 31 on page 116. Once the entity key layer is established, every system entity, which holds the bootVerifyingkey can verify all signed messages sent by any other system entity. A complete entity key layer for two system entities is shown in Figure 31 on page 116.

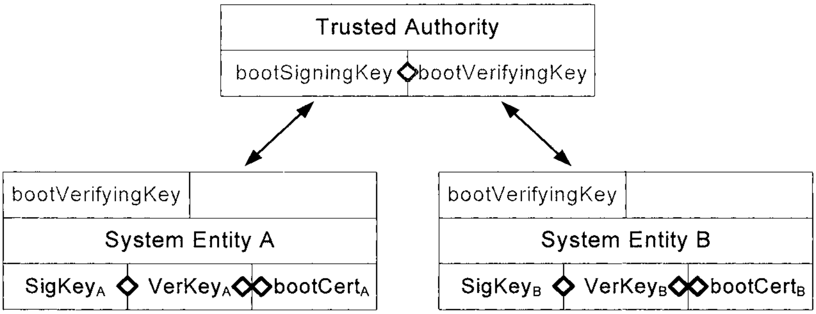


*Figure 31.*Entity Key Layer

4.5.5.3 Entity Verifying Key Directory

In more open environments where system entities need to get hold of each other's entity verifying keys in order to secure their communication without referring to a trusted authority's certificates all the time, it is useful to establish one or more entity verifying key directories [74].

4.5.5.4 Secure Communication Channels

Once two system entities have established their entity key pairs, they can establish ephemeral communication keys in the symmetric model to setup a high speed bidirectional authenticated and/or encrypted communication channel between them. Efficient mechanisms to do this are authenticated Diffie-Hellman key agreement [25], or implicitly authenticated key agreement mechanisms, first proposed by Matsumoto et al [51], later improved by Menezes, Qu, Vanstone (MQV) [55,48]. The best derivative of MQV in terms of efficiency and number of proven security features is HMQV by Krawczyk [47].

A notorious problem with cryptographic keys is to replace them by the next generation of cryptographic keys, which should be chosen stronger than the current ones in order to allow for advances in the area of cryptanalysis. Two system entities that have established entity keys can easily establish a new generation of entity keys as follows: Each system entity generates a new pair of entity keys and exports the new entity verifying key over an authenticated communication channel to the other system entity.

This setup enables to build and maintain a secret key infrastructure (in the symmetric model) or a public key infrastructure (in the asymmetric model) through which system entities can establish secure communication channels (with guaranteed authenticity and/or confidentiality) between each other and the trusted authority.

4.5.5.5 Security Policy

The security policy of a security domain clearly describes

1. who the trusted authority is and what the system entities are,
2. what the security requirements of each system entity is,
3. what security measures and cryptographic mechanisms are in place to achieve these security requirements, including a complete list of cryptographic keys complete with information when and how they are generated, imported, stored, exported, archived, rekeyed and deleted, and
4. what the established processes are to maintain these security measures and cryptographic mechanisms over time.

4.5.6 Security Architecture

The system entities of a distributed system usually have different security requirements, some diverging. other more similar, but perhaps associated with different priorities of enforcement. Some of these different requirements can co-exist, but some of them may be competing or conflicting security requirements, which must be negotiated before the system can be designed effectively. It is good practice in system design, to split all security requirements of a system into disjoint sets of coherent security requirements and to model each such set as a security domain. Security domains may be organized in an overlapping fashion such that, for example, one entity in security domain A receives a piece of electronic postage from another entity in security domain A, then switches into a sender's role in another security domain B and passes the same piece of electronic postage to another entity in security domain B. The collection and structure of all security domains is called the *security architecture* of the system.

It is good cryptographic design practice that system entities do not use any one cryptographic key in two different security domains. This separation of cryptographic keys helps a system entity to

- comply to the security policies of two security domains, even if the security policies are different, and
- achieve a fail-safe cryptographic design, where a potential security breach of a cryptographic key is confined to the respective security domain, but does not spread out into other neighboring security domains.

Despite a lot of openly available guidelines for good design practice of security architectures, see for example the Cryptographic Toolkit of NIST [85], cryptographic key management is still found to be one of the most critical areas of system security design. The collected experience of the NIST accredited FIPS 140 security testing laboratories is that the cryptographic key management is one of the hardest to get right and one those requiring most testing effort.

Chapter 5

General Security Architecture

5.1 WHAT IS A SECURITY ARCHITECTURE

We have sketched the technical architecture of e-postage systems. They are just another kind of largely distributed system comparable to flight reservation systems, or electronic banking systems. The security risks related to these servers and networks can be analyzed by standard computer security measures and tools. Lots of advice is available for comparing security measures like firewalls, intrusion detection systems, virus scanners, and so forth [93,93]. All of this must be carefully planned, installed, and reviewed and maintained on a regular basis, but it is hardly if at all specific to e-postage systems. What is highly specific to e-postage systems is their cryptographic security design. Thus, we introduce in this chapter the general *security architectures* of offline and online e-postage systems before we take a closer look at industry examples of e-postage systems in the following chapter.

The primary security goal of an e-postage system is to enforce the integrity and unforgeability of all pieces of electronic postage throughout its life-cycle in an e-postage system as shown in Figure 11 on page 26. Additional security goals are data protection of customer data and integrity of additional value-added services. Starting from the primary security goal, we derive the general security architectures for offline and online e-postage systems. Since offline e-postage systems include e-postage devices that have cryptographically active hardware security modules embedded, which are initialized, distributed and operated outside of the control of a postal operator, the resulting security architecture is more complex than that of online e-postage systems.

5.2 OFFLINE E-POSTAGE SYSTEMS

In offline e-postage systems, we distinguish two specific *security domains* as shown in Figure 32 on page 120

5.2.1 Mail Processing Domain (A)

Domain A spans across all e-postage devices (including their postal security devices) and the postal operator's entry mail processing centers with one-directional authenticated communication channels from each e-postage device

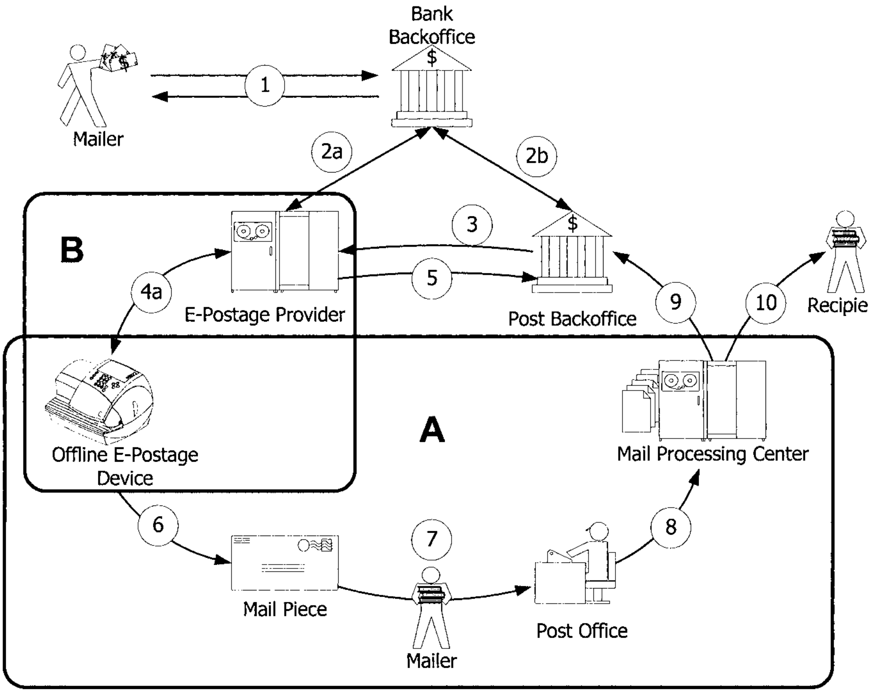


Figure 32. Offline E-Postage System Security Domains

to each entry mail processing center (links 6,7,8). Physically, the communication channels are implemented by imprints carried on physical letters, which are transported through the postal delivery network. Each e-postage device secures its imprints by using an *indicia authenticating key*, which should be kept within and never leave the e-postage device's postal security device. Entry mail processing centers verify each individual imprint by using the corresponding *indicia verifying key* of the respective e-postage device. The trust authority of this domain is the postal operator that runs the mail processing centers, because the postal operator specifies the algorithms and strengths of indicia authenticating keys to be used.

From the postal operator's point of view, the imprints should be authenticated in a non-repudiable fashion, which means that no other system entity but a legitimate e-postage device, not even the verifying mail processing centers, can produce a valid imprint. This is achieved in one blow by including in each imprint a digital signature that is computed over the imprint data. Alternatively, authentication can be achieved by including a message authentication code in each imprint, that is computed over the imprint data. In this case, each indicia authenticating key and its corresponding indicia verifying key are equal, and they are shared between the respective e-postage device and all mail processing centers, where they are needed to verify the imprints. But if such an imprint is disputed, its message authentication code cannot reveal if it has been produced by the alleged e-postage device or by one of the mail processing centers. This inherent disadvantage, however, may be outweighed by the fact that message authentication codes can be computed approximately 10 to 50 times faster and can be made about 10 times smaller than an efficient digital signature of the same level of security. An ECDSA digital signature of sufficient security level, i.e., 1024 bit modulus, requires at least 40 bytes in size, while truncated message authentication codes can be as small as 4 bytes. Some postal operators even require both, to include a digital signature and a message authentication code in each imprint.

5.2.2 Refill Domain (B)

Domain B can be instantiated many times, once for each e-postage provider. Each instance includes one e-postage provider and spans across all of its contracted e-postage devices. There are bi-directional authenticated (and optionally encrypted) communication channels between the e-postage provider and each of its contracted e-postage devices. Traditionally, the communication channels have been implemented by wired or wireless telephone lines, over which the e-postage devices can request electronic postage from their e-postage provider and receive confirmations in return. Either party can use this communication channel to transmit additional information. The trust authority of each instance of domain B is its e-postage provider, because it specifies the algorithms and key strengths to be used. In order to establish secure communication channels, the e-postage provider generates a *provider key pair*, which is a *boot key pair* according to Section 4.5.5.1 on page 115, and each e-postage device generates a *PSD key pair*, which is an *entity key pair* according to Section 4.5.5.2 on page 115. The *PSD authenticating key* of each e-postage device should be kept within and never leave its postal security device. Based on both layers of key pairs, the e-postage provider and each e-postage device establish bi-directional authenticated (and optionally encrypted) communication channels as explained in Section 4.5.5.4 on page 116.

5.3 ONLINE E-POSTAGE SYSTEMS

In online e-postage systems, we distinguish two specific *security domains* as shown in Figure 33 on page 122.

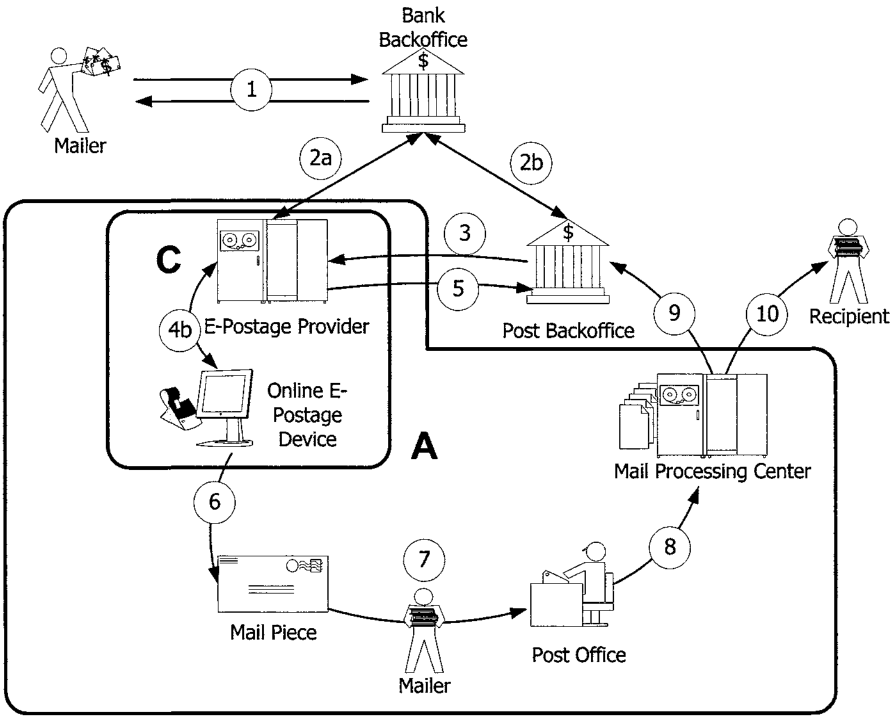


*Figure 33.*Online E-Postage System Security Domains

5.3.1 Mail Processing Domain (A)

Domain A spans across all e-postage providers, their contracted online e-postage devices and the postal operator's entry mail processing centers with one-directional authenticated communication channels from each e-postage provider to each entry mail processing center (links 4b,6,7,8). In online e-postage systems, mailers have their indicia computed by their e-postage providers and receive them into their online e-postage clients. Usually, the e-postage providers use individual indicia keys for each online e-postage client. Thus, the entire description of the mail processing domain in offline e-postage systems (see Section 5.2.1 on page 119) carries over to the mail processing domain in online e-postage systems. Essentially, both mail processing domains are equal.

5.3.2 Online E-Postage Domain (C)

Domain C can be instantiated many times, once for each e-postage provider. Each instance includes one e-postage provider and spans across all of its contracted online e-postage clients. There are bi-directional authenticated (and optionally encrypted) communication channels between the e-postage provider and each of its contracted online e-postage clients. Traditionally, the communication channels have been implemented by Internet connections, over which the e-postage clients can request suitable indicia from their e-postage provider. Either party can use this communication channel to transmit additional information. The trust authority of each instance of domain B is its e-postage provider, because it specifies the algorithms and key strengths to be used. In order to establish secure communication channels, the e-postage provider maintains a *provider key pair*, which is a *boot key pair* according to Section 4.5.5.1 on page 115, and each e-postage device maintains a *client password,* from which it can derive a symmetric *entity key* according to Section 4.5.5.2 on page 115. Users of e-postage clients should keep their *client passwords* in safe places hidden from prying eyes. Based on both layers of key pairs, the e-postage provider and each online e-postage client establish bi-directional authenticated (and optionally encrypted) communication channels as explained in Section 4.5.5.4 on page 116.

5.4 BACKOFFICE SECURITY DOMAINS

In e-postage systems, we distinguish three backoffice *security domains* as shown in Figure 32 on page 120

5.4.1 Provider Post Backoffice Domain (D)

Domain D spans across the postal operator and all approved e-postage providers. The post backoffice is connected to each e-postage provider by bi-directional authenticated (and optionally encrypted) communication channels (links 3,5). Over this B2B interface, each e-postage provider transmits on a regular basis or on request of the post backoffice one or more files of information containing all postage value downloads and all withdrawals of its e-postage devices in the preceding accounting period. Either party can use this communication channel to transmit additional information. The trust authority of domain *D* is the postal operator. As there are usually only a few e-postage providers exchanging data with the post backoffice over this file-oriented interface, the participants typically use long-term cryptographic keys in order to encrypt all their files.

Some post backoffices support static symmetric encryption keys built into pairs of special network devices, where one device of each pair must be installed at the post backoffice's end and the other at the e-postage provider's end. More contemporary systems employ asymmetric encryption software

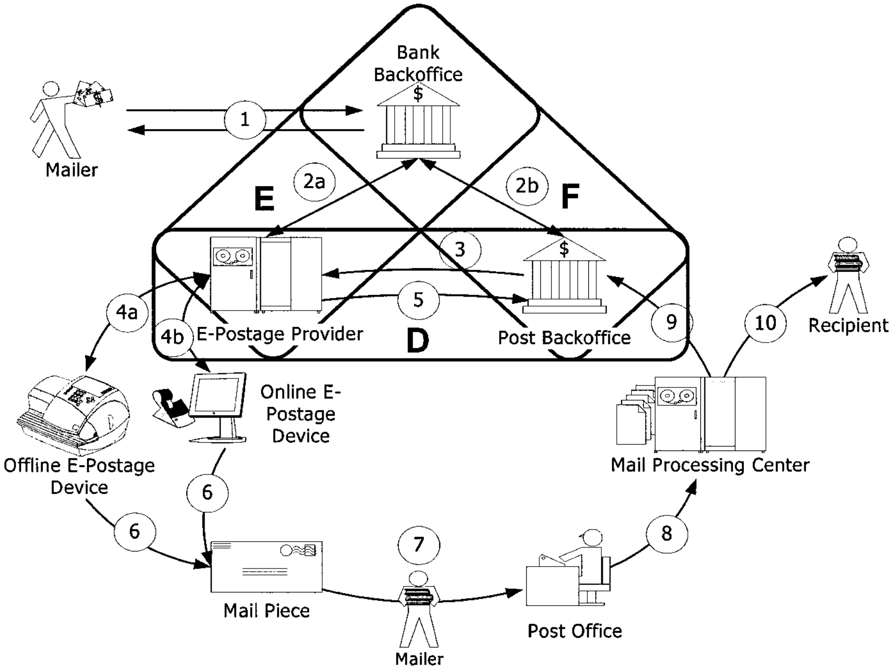


*Figure 34.*Backoffice Security Domains

engines at application layer such as Pretty Good Privacy (PGP) or GNU Privacy Guard (GPG).

5.4.2 Provider Bank Backoffice Domain (E)

If the postal operator specifies that the e-postage providers clear the postage value download requests of their customers directly through a lockbox account at a bank, then there need to be secure communication channels in place between each of the e-postage providers and this bank (link 2a). Thus, we define domain E to span across the bank's backoffice and all approved e-postage providers. The bank backoffice is connected to each e-postage provider by bi-directional encrypted communication channels. Each e-postage provider receives on a regular basis or on request of the bank backoffice one or more remittance files containing all pre-payments of customers for their postage and returns direct debit information back to the bank, such that the bank can deduct the respective amounts from the respective customer's accounts. Everything else from domain D carries over to domain E, where the bank in domain E assumes the role of the post in domain D.

5.4.3 Post Bank Backoffice Domain (F)

If the postal operator specifies that the e-postage providers clear their postage value download requests of their customers through the post backoffice, then there must be a secure communication channel in place between the two (link 2b). Domain F spans across the bank backoffice and the post backoffice, where the bank is usually the trusted authority. Everything else from domain E carries over to domain F, where the post backoffice in domain F assumes the role of an e-postage provider in domain E.

5.5 SUMMARY OF CRYPTOGRAPHIC KEYS

A summary of the system entities and typical cryptographic keys of the three security domains A, B, and C, is given in the following Table 16 on page 125. The trusted authority of each security domain is given in boldface.

Table 16. Security Domains, Entities and their Cryptographic Keys

Security Domain	*Contained System Entities*	*Cryptographic Keys*
A	post backoffice	• *indicia authenticating key*
	All approved e-postage devices	• *indicia verifying key*
B	e-postage provider	• *provider authenticating key* • *PSD verifying key*
	Each contracted e-postage device	• *PSD authenticating key* • *provider verifying key*
C	e-postage provider	• *provider authenticating key* • *mailer's password*
	Each contracted online e-postage device	• *mailer's password* • *provider verifying key*

Chapter 6

Industrial Offline E-Postage Systems

6.1 INDUSTRIAL OFFLINE E-POSTAGE

A number of postal operators have started their offline e-postage system infrastructures and encouraged e-postage providers and mailers to follow. In the following sections, we review the (cryptographically secured) offline e-postage systems that exist worldwide. Our emphasis is on industrial scale offline e-postage systems that are supported by a postal operator and at least one e-postage provider. We present these e-postage systems in terms of the general model introduced in Chapter 2 on page 25.

All offline e-postage devices approved by 2006 are some kind of digital postage meter, which are highly specialized, security-critical embedded systems. To develop and manufacture a new digital postage meter requires a number of key skills including the development and assembly of mechanical and electronic components, the development of embedded application software typically using a real-time operating system, the application and integration of printing technology, the development of new hardware security modules or application of existing ones, systematic product testing and understanding of the postal markets.

6.2 THE CLOSED OFFLINE E-POSTAGE MARKET

The market of postage meters has been an oligopoly, where a few manufacturers share the entire market. After Francotyp merged with Postalia in 1991 and Neopost acquired Ascom-Hasler in 2003, there are three manufacturers left that sell postage meters and provide e-postage on several continents, in particular in North-America, Europe and in the Asia-Pacific region. They are Pitney Bowes, Inc., based in Stamford, CT, Neopost Group based in Paris, France, and Francotyp-Postalia Group based in Birkenwerder (Berlin), Germany. Beside these international manufacturers, there are smaller manufacturers and e-postage providers who are active in regional markets.

The following table summarizes per 2005 some key facts about the international vendors of postage meters such as their annual revenue, number of employees worldwide, number of operating postage meters worldwide, market share of postage meters, and the number of active patents [29].

Table 17. International Manufacturers of Postage Meters in 2005

Manufacturer	*Annual Revenue*	*#Employees*	*Post. meters worldwide [1000 pcs]*	*Market Share Worldwide*	*Number of active patents*
Pitney Bowes, Inc.	$5,000m	32,500	1400	60%	ca. 5,000
Neopost Group	$900m	5,000	630	27%	ca. 900
Francotyp-Postalia Group	$160m	850	250	9%	ca. 850

Digital postage meters are available for different environments ranging from small offices up to large mail rooms. Entry level stand-alone devices are fed manually and can produce up to 10 pieces per minute. Mid-range devices can be connected to peripheral devices such external scales, feeders, and inserters and produce up to 10,000 pieces per hour. High-end devices can be integrated into full blown mail processing plants complete with sorting equipment operating at more than 20,000 pieces an hour. Some mid-range and high-end postage meters can automatically frank mixed mail when they are connected to a dynamic scale, which determines the format, thickness, and weight of a mail piece on the fly.

Postage meters are the workhorses when it comes to frank mail. In mature postal markets, about 15% of all businesses use a postage meter to process their outgoing mail, and their postage meters frank about 60% of all first class letters in the market. By switching the installed base of postage meters into digital postage meters using electronic postage, the large postal operators acquire more accurate marketing data, i.e., usage data, and reduce their losses resulting from meter manipulation at one blow. The following sections present the large industrial franking programs that are currently in operation in the US, Canada and Germany.

6.3 UNITED STATES POSTAL SERVICES

The US Postal Services launched the Information Based Indicia Program (IBIP) for offline closed e-postage systems in January 1999 [100], and offline open systems in June 1999 [101]. These specifications prescribed similar layouts of indicia, all of which included a 2D barcode containing machine readable information including a cryptographic digital signature. Approved

IBI compliant products available on the market include closed offline e-postage systems, i.e, postage meters, and of open online PC-based e-postage systems.

The initial draft of the Information Based Indicia Program was released by the US Postal Services on March 7, 1996, and was provided as input for developing the UPU Standard S36-4 [114].

When IBIP was launched in 1999, the US Postal Services operated 346 mail processing centers in the US and US territories, which were not equipped with 2D barcode scanners at that time. A significant investment had to be made to update the mail processing centers with wide view cameras and the supporting reading software and database infrastructure to facilitate reading of indicia. According to the annual report 2004, the US Postal Service will have the necessary scanning and verification equipment installed in almost all mail processing centers by March 2006.

During the first 5 years of IBI postage meters availability, the market of postage meters was growing at an average rate of 0.75% per year. The number of IBI compliant postage meters has more than doubled every year, and the number of traditional postage meters has dropped by about 26% over the five year period (see Figure 35 on page 129). If we extrapolate this trend, we expect to see the entire market switched to IBI compliant postage meters by around 2012.

Year	IBI	Traditional	Total
2000	0	1,604,834	1,604,834
2001	15,230	1,599,801	1,615,031
2002	35,450	1,589,515	1,624,965
2003	106,030	1,547,550	1,653,580
2004	245,940	1,415,102	1,661,042
2005	479,484	1,184,713	1,664,197

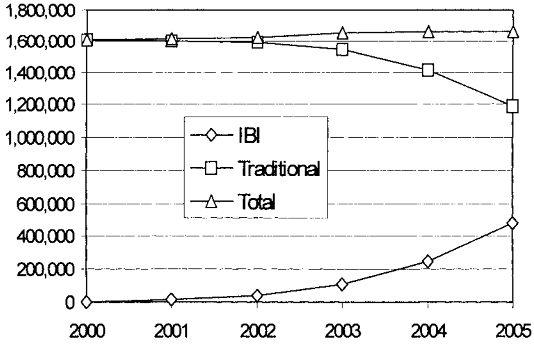


*Figure 35.*Number of postage meters operated in the US

6.3.1 IBIP for Closed Systems

Each IBI compliant postage meter has a postal security device (PSD) embedded. Both the postage meter and its postal security device have their individual identities, which are registered by the US Postal Services. The postal security device works according to the basic life-cycle described in Section 3.1.1.2 on page 58 and performs three fundamental security functions. The postal security device is the postage meter's foothold in the mail processing domain (Section 5.2.1 on page 119), where it keeps the *indicia key pair*, and in the refill domain (Section 5.2.2 on page 121), where it keeps the *PSD key pair*, and it is the link between both security domains by storing the postal register values of the postage meter.

The Post Backoffice of the US Postal Services that supports IBI compliant postage meters only acquires data from some meter operations. The main operational work load is on the e-postage providers, each of which performs the following tasks:

- When a postage meter is initialized, its first indicia key pair is established. Either the key pair is generated by the postage meter and the indicia public key is sent to the e-postage provider, or the e-postage provider generates the indicia key pair and provides the indicia authenticating key (*iak*) to the postage meter.
- When the current indicia key pair is about to expire, then the next indicia key pair is established for that postage meter as described in the previous bullet.
- The credit line for each postage meter is maintained. Direct debit customers observe a default credit line. Prepay customers observe a credit line determined by their prepayments.

The necessary action items listed above are efficiently organized in a communication schedule between a postage meter, its e-postage provider and the US Postal Services as illustrated in Figure 36 on page 131.

When a postage meter is initialized, it establishes its first indicia key pair (S1) with the e-postage provider, who, at the end of the day, forwards the indicia verifying key to the US post backoffice.

When a postage meter performs its first postage value download on business day 1, it dials up to its e-postage provider to receive a confirmation of the requested amount of postage (L1). Postage meters can perform more than one postage value download on each business day. When the current indicia key is about to expire and the postage meter asks for the next postage value download, the e-postage provider automatically establishes the next indicia key pair (S2) for the postage meter, and forwards the indicia verifying key to the US post backoffice. The US postal backoffice uses these keys to verify indicia. Each indicia key pair is valid for three years.

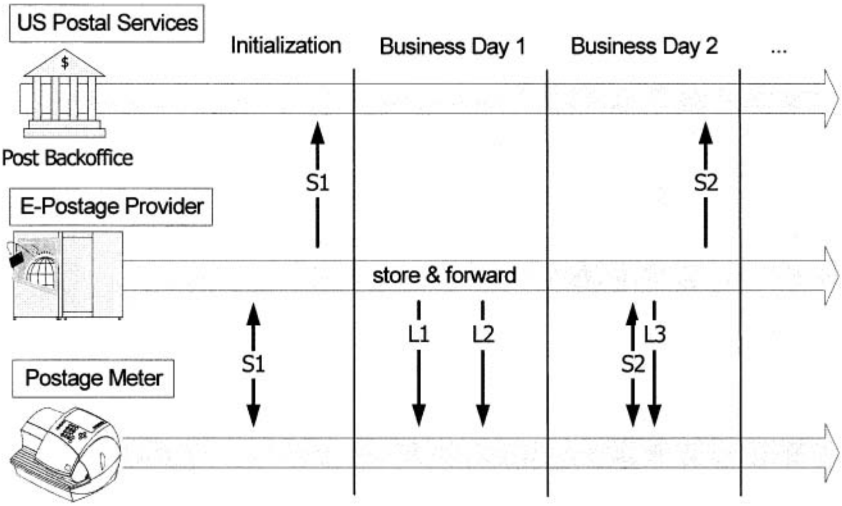


*Figure 36.*Communication Model of Postage Meters in the US Market

6.3.1.1 Indicia Layout

Indicia complying to the IBIP specification contain a 2D barcode based on either the data matrix symbology of 40 by 40 elements or the PDF417 symbology, and a human readable information as shown in Figure 37 on page 131 and with more explanations in Figure 8 on page 15. The barcode symbology must achieve a sufficient readability rate under US Postal Service reading conditions. Indicia may be printed in red fluorescent or black ink. If black ink is used, the mailer must add a facing identification mark (FIM) according to applicable USPS regulations [103]. For an example, see Figure 17 on page 65.

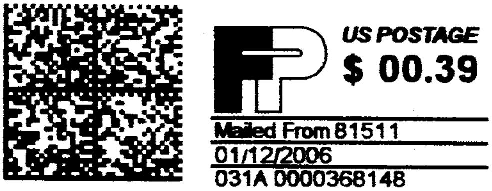


*Figure 37.*Sample IBIP Indicia

The human readable area contains the header “US POSTAGE” and an optional indication of the manufacturer of the postage meter used. It includes further the amount of postage, the class of mail, the origin ZIP code where the mailer is located, the mailing date, and the PSD-PSN. The mailing date must not be chosen prior to the printing date and no later than 30 days ahead of the printing date. Mail pieces will be accepted for induction only on the day indicated by the mailing date. The PSD-PSN consists of the manufacturer ID, which was assigned to the manufacturer of the IBIP compliant postage meter by the US Postal Service, a model ID of the postal security device embedded in the postage meter, and the serial number of the postage meter.

The data matrix barcode of 40 by 40 elements contains all of this information except for the origin ZIP code plus some book keeping, monitoring and security data. Table 18 on page 132 summarizes the data elements included in an indicium.

Table 18. Summary: IBIP Indicia Contents

No	*Data Element*	*Barcode Area*	*HR Area*	*Length [byte]*
1	Indicia Version Number	X	—	1
2	Algorithm ID	X	—	1
3	Certificate Serial Number	X	—	4
	Postal Security Device			
4	PSD Manufacturer ID	X	X	2
5	PSD Model ID	X	X	2
6	PSD Serial Number	X	X	4
7	Ascending Register	X	—	5
8	Postage	X	X	3
9	Date of Mailing	X	X	4
	Originating Address			
—	City, State, ZIP Code	—	X	—
10	Licensing ZIP Code	X	—	4
11	Reserved Field 1	X	—	5
12	Software ID	X	—	6
13	Descending Register	X	—	4
14	Rate Category	X	—	4

Table 18. Summary: IBIP Indicia Contents

No	*Data Element*	*Barcode Area*	*HR Area*	*Length [byte]*		
15	Digital Signature	X	—	DSA 40	RSA 128	ECDSA 40
16	Reserved Field 2	X	—	variable		
	Total Length			89	177	89

The largest data matrix code allowed is 40 by 40 elements, which accommodates 112 byte of information. Thus, if indicia prefer data matrix over PDF417, they have only two options left for the digital signature algorithm used: DSA or ECDSA (see Section 4.4.2 on page 101).

Field #1 gives the version number of the indicia layout, field #10 shows the origin ZIP code (of the licensing post office), field #11 reserves some space in order to keep the data layout of indicia for IBI closed systems compatible to that of IBI open systems. Field #12 indicates the version number of the certified and approved operating software of the postal security device. The remaining monitoring and security data elements are explained in the following subsections.

6.3.1.2 Security Architecture

Each IBI compliant postage meter maintains in its postal security device an individual *indicia key pair* (see mail processing domain in Section 5.2.1 on page 119). IBI allows to choose from the following digital signature mechanism: RSA, DSA or ECDSA. The actual choice of mechanism is indicated by the algorithm ID (field #2).

The *indicia authenticating key* is to be kept within the postal security device at all times, while the *indicia verifying key* is submitted to the USPS before the indicia authenticating key is put into operation. IBI allows two ways of setting up an indicia key pair. Either it is generated within a postal security device and the indicia verifying key is exported to the respective e-postage provider, or it is generated by the e-postage provider and the indicia authenticating key is imported into the postal security device. In either case, the e-postage provider manages the key transport during initialization and as an add-on service during suitable postage value downloads and re-uses the same secure communication channel with the postal security device (see refill domain in Section 5.2.2 on page 121). Afterwards, the e-postage provider computes an public key certificate according to X.509 or other proprietary format (see Section 4.5.4 on page 113) for the indicia verifying key and submits the certificate to the Post Backoffice of the US-Postal Service over a secure communication channel of the Provider Post Backoffice Domain (see Section 5.4.1 on page 123). The certificate serial number (field #3) is the ID of this public key certificate, which contains the indicia verifying key to verify the digital signature (field #15). Indicia key pairs need to be rekeyed every 3 years, while the e-postage provider is responsible to rekey all postage meters in time. The rekeying is usually done remotely at the occasion of a postage value download within a grace period before the current indicia key pair expires. This way of rekeying is mostly transparent to postage meter users.

The fields #7 and #13 contain a snapshot of the ascending and descending register values after the indicium was created. The ascending register value indicates how much postage the PSD has produced since it has been initialized to the current mailer, while the descending register indicates how much postage remains inside the postal security device.

6.3.1.3 Verification of Indicia

To verify an imprint, its 2D barcode is decoded and its data elements are extracted. First the digital signature in data field #15 is verified with respect to the indicia verifying key, which is looked up from a US Postal Services public key directory by the certificate serial number given in field #3. In addition there are a couple of plausibility checks and a check for duplicate imprints that may have surfaced at the same mail processing center before.

6.3.2 Postal Value Added Services

6.3.2.1 Postage Rate Tables

The information based indicia program does not mandate a particular way of transferring postage rate tables into IBI postage meters. In particular, it does not require postage meters to be capable of downloading new rate tables automatically as soon as they become available. Neither does an IBI indicia contain a reference to the version of the rate table that was used by the respective postage meter when the indicia was created.

6.3.2.2 Acquiring Usage Data

The US Postal Services distinguishes four classes of domestic mail. All flat size personal correspondence up to 11oz (about 312g), including handwritten material, typed media, bills, statements of accounts and carbons must be sent as *first class mail.* Other non-advertising matter including newspapers, magazines, periodicals is rated *second class mail.* Advertising mail items such as circulars, newsletters, catalogs, weighing less than 16oz (about 454g) qualifies to be sent as *third class mail.* Any other mail pieces weighing 16oz or more can be sent as *fourth class mail.*

The class of mail of the indicium is shown by field #14. The originating mail processing centers read this information and feed it into the US Postal Rate Commission's origin destination information system (ODIS). Quarterly statistical reports are available through the Postal Rate Commission's web site [99]. The US Postal Services do not capture detailed usage data down to the rate category level.

6.3.2.3 Certified and Registered Mail

The USPS provides a number of additional services for first-class, priority, express mail and parcel post such that mailers can get a proof of deposit of their mailings (receipt or certificate of mailing), a notification of delivery or attempted delivery (return receipt postcard or delivery confirmation) or a signature of the recipient at the time of delivery (signature confirmation). The requested receipts are available to mailers as postcards, by phone or online.

In order to use these services, the mailer needs to affix an adhesive label to the mail piece or custom print a similar looking face. Certified or registered mail marks contain a 16-20 digit decimal tracking number in plain text and as a linear bar code (code 128) by which they can be uniquely recognized. An example of a certified mail label positioned to the left of an IBI indicia is shown in Figure 38 on page 135. The additional fees can be pre-paid by including them in an IBI indicia. Mailers using certified or registered mail services must fill in a corresponding mail statement and deposit it together with their certified or registered mail piece at the accepting post office. Mailers using certified mail services can alternatively use Net.Post mailing online, an online hybrid mail service provided by the US Postal Services that enables mailers to send their electronic documents to a mail printing facility, have the documents printed in black and white or full color and then delivered. The

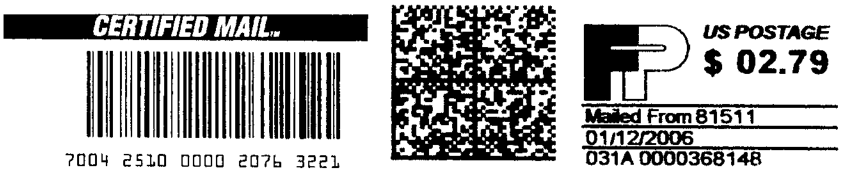


*Figure 38.*Sample Certified Mail Label

entire service is paid for online and the delivered physical mail pieces bear a special "postage paid" imprint that is unrelated to the IBI Program.

As a convenience to mailers, some e-postage devices support e-certified mail. The mailer requests a sheet of certified mail labels from the e-postage provider, and at the time of franking inputs the tracking number of the certified mail label into the e-postage device. Afterwards, the e-postage device compiles an electronic statement of mailing and sends it to the e-postage provider, who forwards it to the postal operator. The mailer can then look up the delivery status of his mailings at a web site of his e-postage provider and/or the postal operator.

For delivery and signature confirmation, mailers request special adhesive labels from the e-postage provider. They are shown in Figure 39 on page 136 and are used exactly as those for e-certified mail described above.

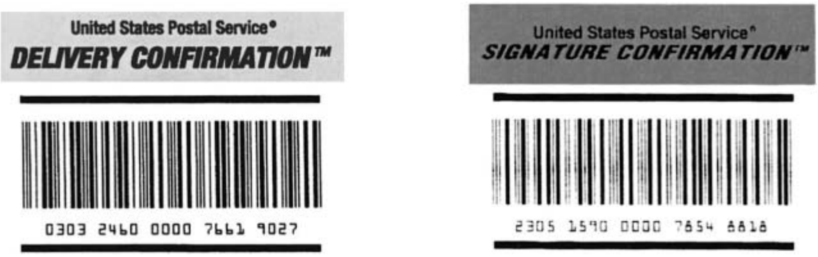


Figure 39. Sample Labels for Delivery Confirmation (left) and Signature Confirmation (right)

The workflows of certified and registered mail services are independent of how a mail piece is pre-paid. They do not particularly integrate into the workflows for IBI Indicia. For example, an IBI indicia may include the additional fee for delivery confirmation, but would make no reference to the tracking number.

6.3.2.4 Postage or Date Correction

The IBI Program supports special types of indicia that may be printed in order to correct the mailing date (redate) or a shortpaid amount of postage of a previously printed indicium [100, 104].

The redate indicium consists only of a human readable portion showing the corrected mailing date and a zero postage amount. Only one redate indicium may be applied to each piece of mail. A redate indicium is shown in Figure 40 on page 137.

The postage correction indicium consists of a 2D barcode and human readable data and looks similar to a regular indicium. A postage correction indicium must show the incremental amount of postage, in addition to the shortpaid regular IBI indicium. If more than one postage correction indicia is applied to a mail piece, the US Postal Services regards their sum of postage to be the prepaid amount of postage. A postage correction indicium is shown in Figure 40 on page 137.

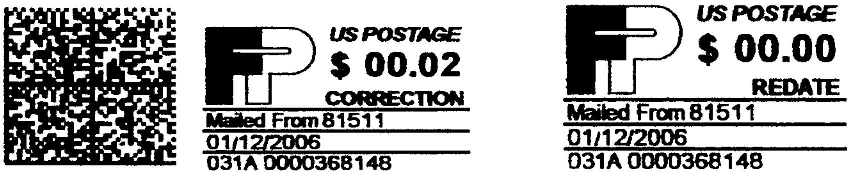


*Figure 40.*Sample IBI Indicia for Postage Correction (left) and Redate (right)

If several indicia are applied to a mail piece they must not overlap each other. This can be achieved by using labels or printing onto the back of the mail piece.

6.3.2.5 Reply Mail

Mailers can choose from three types of reply mail:

- metered reply mail, which is pre-paid by the mailer using a regular indicium with the mailing date left blank [104] Figure 41 on page 138.,
- business reply mail, which is pre-paid by the mailer, but is independent of the IBI Program, or
- courtesy reply mail, which is paid by the respondent. Mailers need to prepare reply mail envelopes using an optional pre-printed Postnet Code and an additional *facing identification mark* (FIM) code. The FIM tells a mail processing center to look up the destination address directly from the Postnet Code, rather than reading the postal address through the multi-line optical character recognition equipment (MLOCR), which is much slower.

Metered and business reply mail are expected to achieve the highest return rates because respondents neither have to provide a postcard or envelope, nor

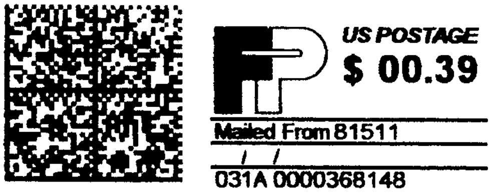


*Figure 41.*Sample IBI Indicia for Business Reply Postage

to apply an address or postage. Courtesy reply mail adds to the respondent's conveniences and improves address accuracy.

6.3.2.6 Addressing and Mail Forwarding Services

The Address Change Service (ACS) is an automated electronic enhancement to the traditional manual process for providing address corrections to mailers. The US Postal Services maintains a database of postal addresses of US residents and companies that is distributed over about 200 Computerized Forwarding System (CFS) units. Customers can get access to this postal address management system through the National Customer Support Center (NCSC) in Memphis, TN. Customers who are going to relocate can file a change of address (COA) order, or letter carriers can file such an order in behalf of their customers.

When a letter carrier receives a mail piece and it is undeliverable-as-addressed at the old address due to customer relocation, the mail piece (depending on its mail class and endorsements) is sent by the letter carrier to the CFS unit responsible for forwarding mail destined to that old address. An attempt is then made to match the name and address to a change of address on file at the CFS unit. If a match is attained from the CFS database and the mail piece bears an active ACS participant code, an electronic notification is tried to be generated. If unsuccessful, the COA notification is provided manually. Electronic ACS fulfillment notifications generated by the CFS units are transmitted daily to the NCSC, where they are consolidated and provided to ACS-participating mailers. Depending on its class of mail and endorsements, the mail piece is forwarded, disposed, or returned to sender.

In order to participate in the address change service, mailers need to enroll and get a unique ACS participant code. They need to include additional sender identifying information, such as the ACS participant code and a key-line within the address portion and respective endorsements on each piece of mail for which they request electronic COA notifications. Depending on the class of mail, the mailer may choose from four available endorsements.

- "Address Service Requested" causes the mail to be forwarded or returned if no new address could be attained and the mailer be notified in any case,
- "Return Service Requested" causes the mail to be returned with new address or reason for non-delivery if applicable.
- "Change Service Requested" causes the mail to be disposed and the mailer be notified.
- "Forwarding Service Requested" is like Address Service Requested, but the mailer is notified only if the mail is returned.

The addressing service is available for different classes of mail using the same endorsement. The applicable fees may differ by class of mail and can be included in IBI indicia.

6.3.2.7 Refunding for Spoiled Indicia

A refund procedure is in place for spoiled or otherwise damaged IBI and other indicia that have been paid for, but could not be used as postage. Mailers who return spoiled indicia need to fill in respective applications for refund of postage, fees and services, get signatures of respective witnesses and file the applications through their licensing post offices to the Scanning and Imaging Center of the US Postal Services at Sioux Falls, SD.

6.3.2.8 E-Postage Demonstration

The US Postal Services allow e-postage devices to be initialized or re-initialized in a special mode for demonstration purposes. In this specimen mode, they can print out specimen indicia only, which are not accounted for, resemble the layout of regular indicia, but are clearly marked as invalid (see Figure 42 on page 140). In specimen mode, e-postage devices generate and use a separate indicia key pair to compute their digital signatures in data field #15. The e-postage provider does not transfer the respective indicia verifying key to the US Postal Services, because the overlaying voiding mark precludes specimen indicia from being verified by US mail sorting centers anyway.

6.3.3 IBI-Lite for Closed Systems

In 2005, the USPS expanded the IBI program by a new type of indicia, dubbed *IBI-lite*, which can be produced faster and consume less ink than regular IBI indicia. IBI-lite has been approved to be printed in black ink on high speed postage meters operating at more than 20,000 pieces per hour, where each imprint must be produced in less than 180ms. IBI-lite indicia contain a data matrix bar code of 12 by 36 cubes, which has a capacity of 20 bytes and

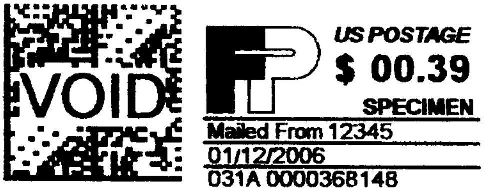


*Figure 42.*Specimen Type of Indicium

is about 27% of the size of the footprint of a regular IBI indicium (assuming cubes are of equal size). The data matrix bar code contains a truncated MAC instead of a digital signature.

IBI-lite can perform faster than regular IBI, but observes a higher security risk because it may be printed with regular non-fluorescent office inks.

6.4 CANADA POST CORPORATION

Canada Post Corporation (CPC), the universal postal operator of Canada launched their digital meter indicia program for offline closed e-postage systems in May 2003 [15] after a three year development process. By 2005, no specifications for offline or open e-postage systems have been issued. The secure digital meter indicia of CPC include a 2D barcode, which contains machine readable information including a cryptographic digital signature together with a verifying key certificate in CPC proprietary format. The first approved digital meter indicia compliant postage meters will be available on the Canadian market by 2006. Open online PC-based e-postage systems are not yet available and have not been announced.

When the digital meter indicia specification was launched in 2003, Canada Post Corporation operated 26 mail processing centers in Canada and Canadian territories. All of them will be equipped with 2D barcode scanners by 2006.

In Canada, the postal transport and delivery of letters is not exempt from sales tax. For offline e-postage systems, the mailer has to pay sales tax for the amount of electronic postage downloaded into his e-postage device at the time of the download (not at the time of franking). Applicable sales taxes are charged by the state and the province in which the mailer's business is registered. If a mailer returns a postage meter that has remaining postage in its postal security device then he is refunded the remaining postage plus the sales taxes of the state and of the province where his business registered at the time he applies for a refund.

As Canada is a bilingual country (english and french), Canada Post as a universal postal operator supports both languages in parallel. It can be seen on their website at http://www.canadapost.ca/ as well as on printed postal forms and on their indicia.

6.4.1 Digital Meter Indicia Specification (DMIS)

Each DMIS compliant postage meter must have a postal security device (PSD) embedded. Both the postage meter and its postal security device have their individual identities, which are registered by Canada Post Corporation. The postal security device works according to the basic life-cycle described in Section 3.1.1.2 on page 58 and performs three fundamental security functions similar to the IBI Program (Section 6.3.1 on page 129). The postal security device is the postage meter's foothold in the mail processing domain (Section 5.2.1 on page 119), where it keeps the *indicia key pair*, and in the refill domain (Section 5.2.2 on page 121), where it keeps the *PSD key pair*, and it is the link between both security domains by storing the postal register values of the postage meter.

The Post Backoffice of Canada Post that supports DMIS compliant postage meters acquires usage and other data from every day meter operations. The main operational work load is on the e-postage providers, which perform the following tasks:

- Retrieve indicia public keys from postage meters and return public key certificates for them.
- Maintain the credit line for each postage meter. Direct debit customers observe a default credit line. Prepay customers observe a credit line determined by their prepayments.
- Retrieve the usage data from each postage meter.
- Calculate state and provincial sales taxes for each postage value download, deduct them from the customer account and transfer them to the Canadian tax authorities.

The necessary action items listed above are efficiently organized in a communication schedule between a postage meter, its e-postage provider and Canada Post as illustrated in Figure 43 on page 142. While an e-postage provider is accredited by Canada Post to support DMIS compliant postage meters (supplier setup), it must generate a supplier key pair and transmit the supplier verifying key (S0) to Canada Post through PosteCS, a secure electronic document delivery system operated by Canada Post.

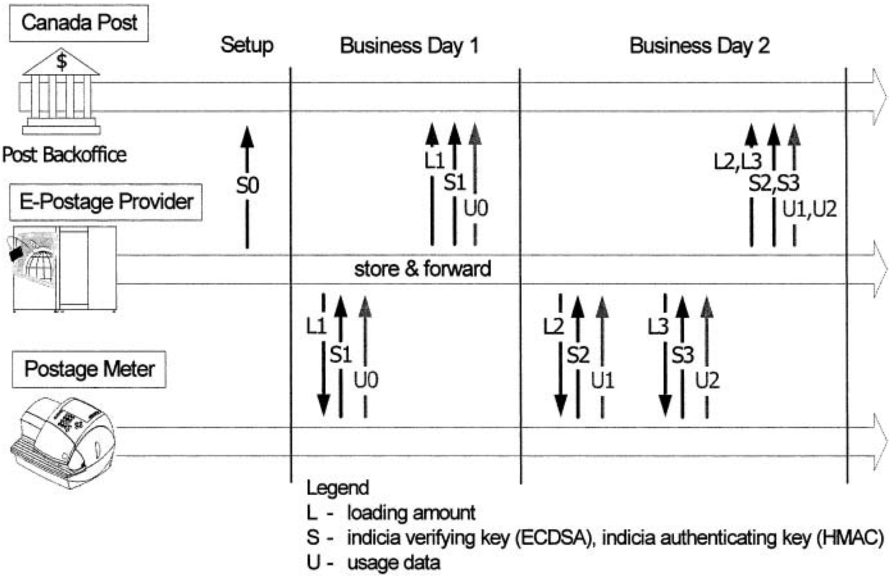


*Figure 43.*Communication Model in the Canada Market

When a postage meter performs its first postage value download on business day 1, it dials up to its e-postage provider to receive a confirmation of the requested amount of postage (L1), uploads its first security data (S1) and all the usage data (U0) that it has collected since the previous postage value download. During the first postage value download, the usage data U0 is empty. At the end of business day 1, the e-postage provider reports to Canada Post the loaded amount (L1), the security information (S1) and the usage data (U0). The security information is used by Canada Post to verify indicia that are going to be produced by the postage meter under consideration. If a postage meter performs more than one postage value download during one business day, it exchanges new security information with its e-postage provider every time. At the end of the day, the e-postage provider reports the collected download amounts (L2, L3) and usage data (U1, U2) to Canada Post.

Each indicia key pair and each indicia authenticating key (S) is valid until the respective postage meter performs the next postage value download. Although an option, it is not recommended for security reasons to re-use the indicia key pair of a preceding period.

6.4.1.1 Indicia Layout

Indicia complying to the digital meter indicia specification contain a 2D barcode based on the data matrix symbology, and a human readable information as shown in Figure 44 on page 143. The data matrix barcode must

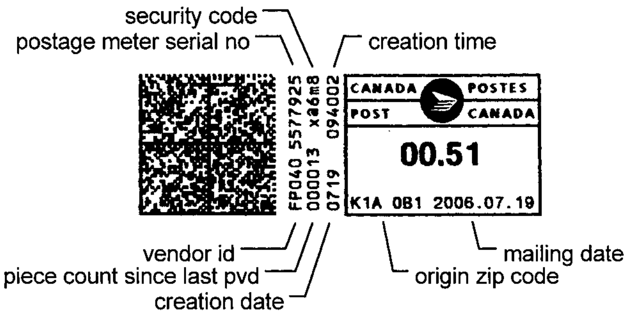


*Figure 44.*Sample Indicia of the Digital Meter Indicia Specification

achieve a readability rate between 80% and of 97% depending on the type of envelope paper under Canada Post Corporation reading conditions. Indicia must be printed in red fluorescent ink or in black ink if it is printed on special secure tape with a fluorescent marking.

The human readable area consists of the regular postage mark on the right hand side and auxiliary data printed in three vertical lines in between the data matrix barcode and the regular postage mark. The regular postage mark contains the headers "CANADA Postes" and "POST CANADA", and the Canada Post company logo. It contains further the amount of postage, the origin postal code where the mailer is located, and the mailing date in YYYY.MM.DD format, when the mailer inducted the mail piece at his post office. Neither is a reference made to the class of mail of the mail piece nor to the postal security device embedded into the postage meter.

The auxiliary data contains the vendor id and postage meter serial number (top line), the piece counter maintained by the postal security device and a security code (middle line), and the creation date in MMDD format and creation time in HHMMSS format (bottom line).

The barcode area contains a data matrix barcode of 48 by 48 elements. It contains all of the human readable information except for the creation time, origin postal code and the supplier identification, but, in addition, it contains some book keeping, monitoring and security data. Table 19 on page 144 summarizes the data elements included in a Canadian digital meter indicium.

Table 19. Summary: Canada Post Digital Meter Indicia Contents

No	*Data Element*	*Barcode Area*	*HR Area*	*Length [byte]*		
1	Country Code = ’CA’	X	—	2		
2	Indicium Code	X	—	1		
3	Algorithm ID	X	—	1		
4	Piece Count since last pvd	X	X	3		
5	Creation Date	X	X	2		
	Creation Time		X	—		
6	Mailing Date	X	X	1		
	origin postal Code		X	—		
7	Ascending Register	X	—	5		
8	Descending Register	X	—	4		
9	Service Code	X	—	2		
10	Postage	X	X	2		
11	Meter Serial Number	X	X	4		
12	Meter Key Expiry Date	X	—	2		
13	Security Code	X	X	4		
	Supplier Identification		X	—		
14	Digital Signature	X	—	42	48	42
15	Meter Public Key	X	—	41	49	41
16	Supplier Signature	X	—	42	42	48
	Total Length			158	172	164

The total length of the Canadian indicia is 172 byte maximum, which fits tightly into a data matrix bar code of 48 by 48 elements.

Field #1 is set to “CA”, the ISO 3166 abbreviation for Canada, indicating its use for Canada Post domestic applications. Field #2 indicates the type of indicium, i.e., regular postage, or return postage prepaid (see Section 6.4.2.5 on page 149).

Field #9 displays the service code, which indicates any additional services chosen and paid for with the respective indicia. The dictionary for this field is given in the Postage Server Product Information Handling Requirements [17] Appendix A. Field #10 shows the origin postal code (of the licensing post office), field #11 reserves some space in order to keep the data layout of indicia for IBI closed systems compatible to that of IBI open systems. Field #12 indicates the version number of the certified and approved operating software of the postal security device. The remaining monitoring and security data elements are explained in the following subsections.

6.4.1.2 Security Architecture

Each digital meter approved by Canada Post maintains in its postal security device an individual *indicia key pair* (see mail processing domain in Section 5.2.1 on page 119), which must be an ECDSA key pair using either one of the elliptic curves secp160r1 backed by Certicom or P-192 backed by NIST (see Section 4.4.3.3 on page 105). The actual choice of elliptic curve is indicated by the 4 least significant bits of the algorithm ID (field #3). The indicia key pairs are rekeyed during each postage value download, and thus are short-term cryptographic keys with an average life time of about 6 weeks. Although the DMIS specification allows to re-use the indicia key pair of the previous period, it is recommended for security reasons to establish a new key pair during each postage value download.

The *indicia authenticating key* is to be kept within the postal security device at all times, while the *indicia verifying key* is transmitted to Canada Post by including it in each indicia that is produced by using the respective *indicia authenticating key*. In other words, Canadian postage meters transmit their indicia verifying keys through the mail processing domain (Section 5.2.1 on page 119) to Canada Post.

The transmission of indicia verifying keys through the mail processing domain is authenticated by respective public key certificates valid with respect to long-term supplier verifying keys. Each e-postage provider generates an individual *supplier key pair*, transmits the supplier verifying key to Canada Post and keeps the supplier signing key secret at its e-postage vendor site. (This process is denoted by transmitting security information S0 in Figure 43 on page 142). The supplier key pair is an ECDSA key pair using either one of the elliptic curves secp160r1 or P-192 (see Section 4.4.3.3 on page 105). The life-time of a supplier key pair depends on the actual elliptic curve chosen. E-Postage providers transmit their supplier verifying keys to

Canada Post through their Provider Post Backoffice Domain D (Section 5.4.1 on page 123).

Each time, a postage meter performs a postage value download, its postal security device generates a new indicia key pair, replaces the current indicia key pair by the new one, requests a public key certificate for the new indicia verifying key and respective book-keeping data from its e-postage provider. It stores the received public key certificate together with its indicia verifying key until the next postage value download is performed. In addition, the postage meter has its postal security device generate a *indicia authenticating key* for backup purposes and transmits it in encrypted form to the e-postage provider. (This process is denoted as an exchange of security information in Figure 43 on page 142.) The e-postage provider forwards all received indicia authentication keys to Canada Post on a daily basis. The transmission of indicia authentication keys from the e-postage provider to Canada Post is through the Provider Post Backoffice Domain D (Section 5.4.1 on page 123).

In each imprint produced after the current and before the next postage value download, the book-keeping data is repeated unchanged in the data fields #2, #3, #7, #11, #12, the indicia verifying key, which is called meter public key, is represented by data field #15, and the certificate signature, which is called supplier signature, is represented by data field #16 (Table 19 on page 144). For each imprint, the postage meter computes the remaining data fields #4, #5, #6, #8, #9, #10, and #13 individually and has the postal security device compute an ECDSA signature over the data sequence #1 through #13 and puts the signature in data field #14. This signature shall be valid with respect to the indicia verifying key (field #15).

In effect, each indicium contains two ECDSA signatures, each of length 42 or 48 byte. As the overall capacity of the barcode is limited to 172 byte, the space left for the two signatures and the corresponding indicia verifying key is limited to 139 byte. This excludes to choose both signatures of length 48 byte, which would induce an indicia verifying key length of 49 byte, which sums up to 145 byte. The remaining three options of combining signature lengths are specified in Table 19 on page 144 fields #14, #15, and #16.

As a backup authentication method, each indicium includes a message authentication code in the human readable area. It is computed by using the indicia authenticating key generated by the postal security device during the previous postage value download. The message authentication code is computed over all data fields in the human readable area (excluding the security code) by using the HMAC-SHA1-30 algorithm (Section 4.4.1.2 on page 100) and truncating the result to the most significant 30 bits (Section 4.4.1.3 on page 101). The result is then encoded into five 6-bit ASCII characters in a way avoiding visual misinterpretations.

6.4.1.3 Verification of Indicia

To verify an imprint, its 2D barcode is decoded and its data elements are extracted. First the supplier signature in data field #16 is verified with respect to the supplier public key, which is looked up from a Canada Post public key directory by the vendor ID given in the human readable portion of the imprint. If that verification holds, then the meter ECDSA signature in data field #14 is verified with respect to the indicia verifying key in data field #15. In addition to these signature verifications, there are a couple of plausibility checks and a check for duplicate imprints that may have surfaced at the same mail processing center before.

If the barcode cannot be read successfully or any of the signature verifications or checks fail, the mail piece is sorted out to be investigated further. These out-of-band checks resort to the security code. By looking up the creation date and meter serial number, the mail processing center can look up the indicia authenticating key that was used to compute the security code. This secret indicia code is used together with all human readable data fields to verify the HMAC-SHA1-30 message authentication code (Section 4.4.1.2 on page 100).

6.4.2 Postal Value Added Services

6.4.2.1 Postage Rate Tables

The digital meter indicia specification mandates that postage meters shall load any updated postage rate tables automatically and as soon as possible after they have been released by Canada Post. The preferred method of data transfer is remote electronic download. However, digital meter indicia do not contain a reference to the version of the rate table that was actually used by the respective postage meter at the time when the indicia was created (see data field #5 in Table 19 on page 144).

6.4.2.2 Acquiring Usage Data

Postage meters convey their usage data to Canada Post electronically through their e-postage providers every time they request a postage value download. Canada Post promotes the common failure control strategy that requires a postage meter to successfully upload its usage data before it receives the requested amount of postage (see the Postage Meter Product Information Requirements [16]).

Digital indicia do not contain class of mail information, just some information about additional services (service code). The service code is read and interpreted during postal delivery, but is not used for collecting usage data.

Instead, the e-postage providers collect and consolidate all usage data received from all postage meters on any one business day. At the end of each business day, each e-postage provider compiles a number of files containing the usage data for its contracted postage meters that performed a postage value download on that day. All usage data is organized and reported according to Canada Post accounting periods. For each accounting period there is a file showing for each rate category the number of indicia created within that period and the sum of their face values. The usage data files are uploaded through the Provider Post Backoffice Domain to an SAP based database system of Canada Post as explained in the Postage Server Product Information Handling Requirements [17].

6.4.2.3 Registered Mail

Mailers requiring a proof of mailing and/or a proof of delivery can use the additional service of registered mail, which is available for domestic and international letter mail, document mail and domestic letters containing valuables. The additional service fee can be included in a regular digital indicia, but a registered mail envelope must carry an extra barcode label showing a unique mail piece ID.

The service provides the sender with a mailing receipt and secures the signature of the addressee, a print of the signature and the date upon delivery of the item. Registered Mail provides confirmation that the item has arrived at its destination. Upon delivery, or attempted delivery, the mail piece ID is scanned and the date captured. If no one is available at the recipient location, a delivery notice card is left in the mailbox. The date of delivery is available the next business day after delivery, upon request by phone or the Canada Post website.

6.4.2.4 Postage or Date Correction

When a mailer happens to produce a digital indicium that shortpays the intended piece of mail, he can print a postage correction indicium to the back of the envelope. A postage correction type indicium (see Figure 45 on page 149) is a regular postage indicium except for an additional keyword "correction" printed in the human readable area right below the amount of postage. It shows the missing amount of postage and carries the service code 62200.

When a mailer fails to induct a piece of mail within the control period of the mailing date indicated in the indicia, an additional redate indicium must be printed to the back of the envelope in order to extend the validity of the original digital indicia. A re-date indicia is a regular indicia showing a postage value of $00.00 in the Postage field, uses the service code 62300 and shows

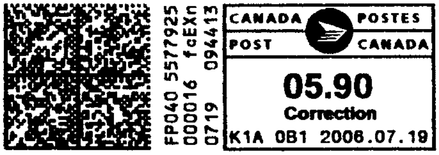


*Figure 45.*Postage Correction Type of Indicium

the last numeric value in the counter before the re-date (see Figure 45 on page 149). The indicia counter (Section 4.2.4) is not ascended when a re-date message is created. Instead, a separate counter is provided to track the number of re-date messages for data capture.

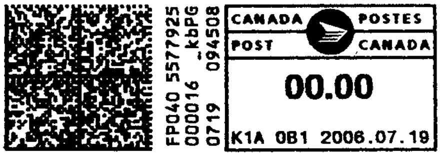


*Figure 46.*Redate Type of Indicium

6.4.2.5 Business Reply Mail

Business Reply Mail is a direct response vehicle used by businesses, publishers, government departments, fund raisers and other organizations. Mailers need to enroll in the business reply program and pay an annual fee in order to be eligible to use the service. Business reply mail is available in two pre-addressed and postage-paid formats: envelope and card. Both formats can be produced through a special kind of digital indicia called *Return Postage Prepaid* (see Figure 47 on page 149). Senders pay for all items including those that are not returned by their recipients. A return postage paid indicium

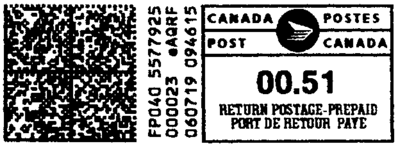


*Figure 47.*Return Postage Paid Type of Indicium

looks like a regular indicium (Figure 44 on page 143) except for three data items: (i) In the clear text box on the right hand side, the bottom lines display the fixed phrase "Return Postage Prepaid" (in english and french language) instead of the origin postal code and mailing date of a regular indicium. (ii) The auxiliary data presents the creation date in YYMMDD format. (iii) In the data matrix barcode, the indicium code (field #2 in Table 19 on page 144) is set to value 2 in order to distinguish return postage prepaid from regular postage.

6.4.2.6 Sharing E-Postage Devices

Canada Post does not support services that allow several mailers to share one e-postage device equally. Each e-postage device is registered to exactly one customer, and this is the one who has to prepay for all of the resulting digital indicia.

6.4.2.7 Addressing, Mail Forwarding and Return Services

Canada Post does not provide an address correction service for undeliverable mail. If the recipient is not found to reside at the given postal address no attempt is made to figure the correct postal address of the given recipient. Such mail pieces are usually returned to the sender.

Canada post provides no address validation services, neither offline through an address database on CD-ROM nor through an online service.

6.4.2.8 Refunding for Spoiled Indicia

Mailers who find indicia spoiled by their e-postage devices may turn them in at certain postal outlets. If the requested value is less than $200, postal outlets reimburse the respective customers directly. For requested values of $200 or more, the postal outlet forwards the request to Canada Post Headquarters for individual approval. Once approved, Canada Post Headquarter notifies the e-postage provider of the respective e-postage device to reimburse the mailer accordingly.

6.4.2.9 E-Postage Demonstration

Canada Post allows e-postage devices that are once and for all setup up for demonstration purposes. They can print out specimen indicia only, which are not accounted for, resemble the layout of regular indicia, but are clearly marked as invalid (see Figure 48 on page 151). Such e-postage devices generate their individual indicia key pairs during each postage value download just regular e-postage devices do. However, the e-postage provider uses a separate supplier signing key to certify the indicia verifying keys. The mail sorting centers distinguish unaccounted for specimen indicia from regular indicia by the supplier signature they carry in data field #16.

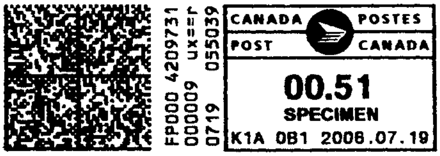


*Figure 48.*Specimen Type of Indicium

6.5 DEUTSCHE POST

Like other large postal operators in the early 1990s, Deutsche Post began to look into possible improvements of postage marks indicating prepaid postage. In order to validate different approaches, among them the draft information based indicia program by the US Postal Service, Deutsche Post participated in a project led by the International Postal Corporation (IPC) about re-engineering the mail—postal interface (REMPI). Other participants were Pitney-Bowes, Neopost, Royal Mail, and the pilot customer Lufthansa Air Plus. The project objectives were to develop and evaluate a new electronic interface between mailers and postal operators supporting item identifiers to be included in the indicia or elsewhere on an envelope, data capture to be reported to the postal operator, electronic accounting and evidence of payment, and proof of posting and customer information access. A system was piloted that assumed a high volume mailer using electronic statements of mailing and operated in a controlled bulk acceptance environment. The digital indicia were based on the data matrix barcode symbology. The resulting experience was partially fed back into CEN TC 331 and into the UPU working groups that were elaborating the specification of digital postmarks S36-4.

In the second half of the 1990s, online postage solutions were developed and marketed first by E-Stamp, then by Stamps.com and others. In 1998, Deutsche Post acquired a 1% share in online postage pioneer E-Stamp. Using the collected experiences from both initiatives, Deutsche Post developed an independent franking program that supports open online e-postage clients and closed offline e-postage devices alike. The former is called Stampit and was launched in September 2001. The latter is called Frankit, its first specification was published September 2002 [24] and the first products were launched in April 2004.

In 2004, Deutsche Post operated 82 mail processing centers ("Briefzentren") in Germany, most of which were equipped with 2D barcode scanners at that time. By the end of 2005, Deutsche Post was reading about 40% of all Stampit and Frankit indicia, but is still in the process of optimizing the reading quality. At the same time, about 243,000 postage meters are installed in the German market of which about 20,000 are Frankit compatible.

During the first 2 years of Frankit postage meters availability, the market of postage meters has been flat. The number of traditional postage meters has dropped by about 10% over the two year period (see Figure 49 on page 152).

Year	FRANKIT	Traditional	Total
2003	0	239,000	239,000
2004	6,000	234,000	240,000
2005	24,000	217,000	241,000

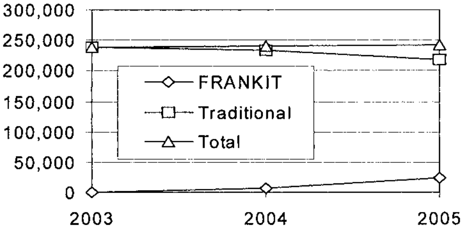


*Figure 49.*Number of postage meters operated in Germany

If we extrapolate this trend, we expect to see the entire market switched to Frankit compliant postage meters by around 2015.

6.5.1 Frankit

Each Frankit compliant postage meter has a postal security device (PSD) embedded. Both the postage meter and its postal security device have their individual identities, which are registered by Deutsche Post before the postage meter may be operated. The postal security device works according to the basic life-cycle described in Section 3.1.1.2 on page 58 and performs three fundamental security functions. The postal security device is the postage meter's foothold in the mail processing domain (Section 5.2.1 on page 119), where it keeps the *indicia authenticating key*, and in the refill domain (Section 5.2.2 on page 121), where it keeps the *PSD key pair*, and it is the link between both security domains by storing the postal register values of the postage meter.

Frankit mandates that indicia are secured by a message authentication code based on SHA-1. Indicia authenticating keys are valid for exactly 90 days, which means they should be rekeyed during each postage value download. To facilitate this rekeying, each postal security device generates during its first initialization an individual RSA public key encryption key pair. We call it the DPAG key pair of the postal security device under consideration. Each DPAG key pair is valid for 8 years. The postal security device further exports its DPAG encryption key, and its postage meter transmits it through the refill domain (B) to the e-postage provider. The e-postage provider forwards the DPAG encryption key to Deutsche Post together with all other administrative data necessary to have the new postage meter registered with Deutsche Post. To manage the registration of postage meters, Deutsche Post provides a postage meter registration link that is called "DigForms". It is separate from the Provider Post Backoffice Domain and uses a separate layer of cryptographic keys to protect the communication over this link. After a postage meter is properly registered, its postal security device is initialized, has generated its DPAG key pair and is thus capable of receiving new indicia authenticating keys from Deutsche Post encrypted under its DPAG encryption key.

The Post Backoffice of Deutsche Post that supports Frankit compliant postage meters (and online postage clients alike) is called the *Postage Point.* Its main purposes are

- Generate and provide indicia authenticating keys to each postage meter.
- Maintain the credit line for each postage meter. Direct debit customers observe a default credit line that cannot be exceeded in any three day period. Prepay customers observe exactly the credit line determined by their prepayments.
- Retrieve the usage data from each postage meter. Each block of usage data carries a message authentication code of the originating postage meter.

All operating manufacturers of postage meters act as e-postage providers for their own postage meters. Therefore, postage meters talk online to their e-postage providers, and the e-postage providers run nightly batch jobs of interaction with the Postage Point, but postage meters never talk directly to the Postage Point. Because the indicia authenticating keys are valid for 90 days only, but can be downloaded into a postage meter only when its user connects to the e-postage provider, some synchronization is necessary between the e-postage providers and the Postage Point.

In fact, the Postage Point can talk directly to postage meters, if they support the communication interface P-Talk defined by Deutsche Post. However, the e-postage providers would experience cuts into their service fees, if they supported this approach. As of 2005, no single postage meter in the German postal market is refilled directly through the Postage Point.

The necessary action items listed above are efficiently organized in a communication schedule between a postage meter, its e-postage provider and the Postage Point as illustrated in Figure 50 on page 154. When a new postage meter is registered with Deutsche Post, the Postage Point has received the

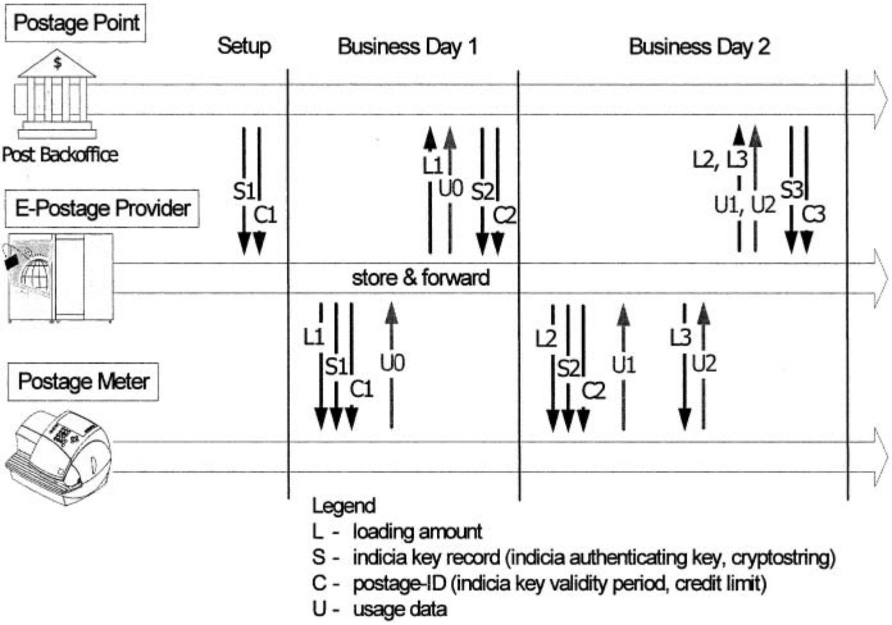


*Figure 50.*Communication Model under Frankit

DPAG encryption key of that postage meter such that it can provide to the respective e-postage provider in a setup stage a first *indicia key record* (S1) and a *postage-ID* (C1). The indicia key record consists of an indicia authenticating key encrypted under the DPAG encryption key of the respective postage meter and a corresponding *cryptostring*, which is the indicia authenticating key encrypted under a Frankit system key, which will be required to verify indicia later on. The postage-ID contains the validity period of the indicia authenticating key contained in (S1) and a corresponding credit limit, which will be set to a default value for new customers. When a postage meter performs its first postage value download on business day 1, it dials up to its e-postage provider to receive a confirmation of the requested amount of postage (L1), the first indicia key record (S1) and the actual postage-ID (C1). In return, the postage meter transmits all the usage data (U0) that it has collected since the previous postage value download. During the first postage value download, the usage data (U0) is empty. At the end of business day 1, the e-postage provider reports the loaded amount (L1) and the usage data (U0) to the Postage Point. After the Postage Point has completed its validation checks on the received data, it provides a new indicia key record (S2), and postage-ID (C2) for the postage meter based on the payment history of the corresponding customer, and sends S2 and C2 back to the e-postage provider. During the next postage value download, the postage meter will receive a confirmation (L2) of the requested amount of postage (if it is within the limits of the current credit limit), the new indicia key record (S2) and the new postage-ID (C2) and it will report its usage data (U1) collected since the previous postage value download. If a postage meter performs a second postage value download during one business day, its e-postage provider provides no new indicia key record and postage-ID. At the end of the day, the e-postage provider reports the collected download amounts (L2, L3) and usage data (U1, U2) to the Postage Point.

Clearly, the indicia authenticating keys age as they reside with the e-postage provider. Thus all postage meters are required to perform at least one postage value download every month. A download amount of zero is acceptable if the postage meter user so wishes. With this approach, indicia authenticating keys are expected to be 30 days old when they are downloaded and to have another 60 days of validity left, which is considered a sufficient validity margin.

6.5.1.1 Indicia Layout

Indicia complying to the Frankit specification contain a 2D barcode based on the data matrix symbology of 36 by 36 elements, and a human readable information as shown in Figure 51 on page 155 and with more explanations in Figure 9 on page 18. The data matrix barcode must achieve a readability rate of 99.5% under Deutsche Post reading conditions. Indicia must be printed in blue non-fluorescent ink.

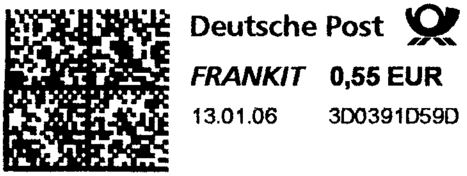


*Figure 51.*Sample Frankit Indicia

The human readable area consists of the regular postage mark on the right hand side contains the header "Deutsche Post" and the Deutsche Post company logo. It contains further the keyword "Frankit", the amount of postage, the mailing date in DD.MM.YY format, when the mailer inducted the mail piece at his post office, the postage meter serial number and a verbal description of the class of mail.

The barcode area contains all of this information plus some book keeping, monitoring and security data. Table 20 on page 156 summarizes the data elements included in a Frankit indicium. Even on a high speed postage meter where two indicia are produced during the same second for two consecutive mail pieces of the same class of mail and the same postage amount the two indicia differ by the content of their 2-D bar codes.

Table 20. Summary: Frankit Indicia Contents

No	*Data Element*	*Barcode Area*	*HR Area*	*Length [byte]*
1	Postal operator	X	X	3
2	Indicia version no	X	—	1
3	Rate Table version no.	X	—	1
4	Postage meter serial no.	X	X	5
5	Postage	X	X	2
6	Date of mailing	X	X	2
7	Postal product code	X	—[a]	2
8	Key phase indicator	X	—	1
9	Currency indicator	X	X	1
10	Piece counter	X	—	4
11	CryptoString	X	—	32
12	Reserved for future use	X	—	2
13	Item counter (resettable)	X	—	3
14	Service indicator	X	—	1
15	Service data	X	—	20
16	Message Authentication Code (MAC)	X	—	4
	Total Length			84

a. The human readable area contains a clear text description of the postal product.

The total length of the Frankit indicia is 84 byte maximum, which fits tightly into a data matrix bar code of 36 by 36 elements. Field #1 contains the fixed string "DEA" in ASCII for Deutsche Post. Field #2 indicates the version number of the indicia layout, currently 1.0. Field #3 contains the version number of the rate table that is currently used by the postage meter to calculate the postage of for a given mail piece. Field #4 contains the postage meter serial number, which is composed of a 1 byte vendor identification, 1 byte model identification, and 3 byte model device serial number. For example 3D0391D59D (Figure 51 on page 155). Field #5 presents the amount of postage, and field #6 the date of mailing, at which the mail piece is to be inducted. Field #7 shows the postal product code, which describes exactly the combination of class of mail, weight, thickness, format, and additional services chosen for the mail piece at hand. Field #8 depicts the key phase indicator, which is used for verifying the indicia within any of the mail processing centers. Field #9 tells in which currency the postage is given (typically EUR). Field #10 contains an the piece counter maintained by the postal security device. The piece counter is reset to zero only when the postage meter is withdrawn from service, for example to be refurbished and sold to another customer. It is helpful to prepare large amounts of mail ready for claiming a discount for presorting. Field #11 bears the cryptostring, another data item solely used for indicia verification by a mail processing center. Field #12 is reserved for future use. Field #13 contains an item counter that can be resetted by the user. It is helpful to prepare large amounts of mail ready for claiming a discount for presorting. Fields #14 and #15 serve to carry indication flags and data required by additional services to be described in Section 6.5.2 on page 160. Field #16 contains a message authentication code (MAC) that protects the indicia content of byte 1 to 80 against unauthorized modifications.

The truncated MAC of an indicium is computed by forming a message of the first 80 bytes of the indicium appended by the postage-ID appended by the 16-byte indicia authenticating key (*iak*). This message is input to the hash function SHA-1 and the result is truncated to the first 4-byte as follows:

$$h = \text{SHA-1}_{1..4}(\text{indicia}_{1..80} \,||\, \text{postage-ID} \,||\, \mathit{iak}) \tag{6.1}$$

6.5.1.2 Security Architecture

The Postage Point maintains a Frankit system encryption key, whose counterpart, the system decryption key, is available to all mail processing centers.

When an e-postage device is initialized, it generates a DPAG encryption key pair, and exports the DPAG encryption key to the Postage Point, while the DPAG decryption key remains within the e-postage device at all times. The transmission and rekeying of the DPAG encryption key is managed over the postage meter registration link of Deutsche Post (DigForms) as outlined in Section 6.5.1 on page 152.

The Postage Point keeps generating fresh *indicia authenticating keys* with corresponding postage-IDs for each initialized e-postage device; one key and postage-ID each time the e-postage provider reports activity for an e-postage device (loaded amount L and usage data U in Figure 50 on page 154). In return, the Postage Point encrypts the new indicia authenticating key twice, once under the DPAG encryption key and a second time under the Frankit system key. The second encryption produces the *cryptostring* associated to the new indicia authenticating key. The resulting pair (S in Figure 50 on page 154) of encrypted items and the associated postage-ID (C in Figure 50 on page 154) are transmitted to the e-postage provider, who relays them to the requesting e-postage device when it posts the next postage value download request. The e-postage device passes S and C along to its postal security device, which decrypts the new indicia authenticating key using its DPAG decryption key and stores it together with the new cryptostring and the postage-ID, thus replacing the previous indicia authenticating key, cryptostring and postage-ID. (Note that the postal security device cannot decrypt the cryptostring, because it cannot access the Frankit system decryption key.)

Next, the postage meter compiles its usage data in the form of a usage profile, i.e., a detailed list of all frankings produced since the previous postage value download, and an account franking, i.e., an 84-byte usage summary containing the total amount of the usage profile. The account franking contains a 4-byte truncated MAC that is computed exactly like a MAC for an indicia as denoted by equation (6.1) above.

The e-postage device is now ready to produce indicia with the new indicia authenticating key according to equation (6.1). The flow of data up to this stage is depicted in the upper half of Figure 52 on page 159.

6.5.1.3 Verification of Indicia

To verify an imprint, its 2D barcode is decoded and its data elements are extracted. First the message authentication code in data field #16 is verified. The verification of the message authentication code in data field #16 requires to have access to the corresponding *indicia authenticating key* that the postage meter used when it produced the indicium. However, Frankit avoids to maintain a large directory of indicia authenticating keys at some trusted site. Instead each indicium bears its indicia authenticating key encrypted under a Frankit system key, namely under the hood of the cryptostring contained in data field #11 (see Table 20 on page 156). In effect, the indicia authenticating keys are distributed through the mail processing security domain (Section 5.2.1 on page 119) to the mail processing centers.

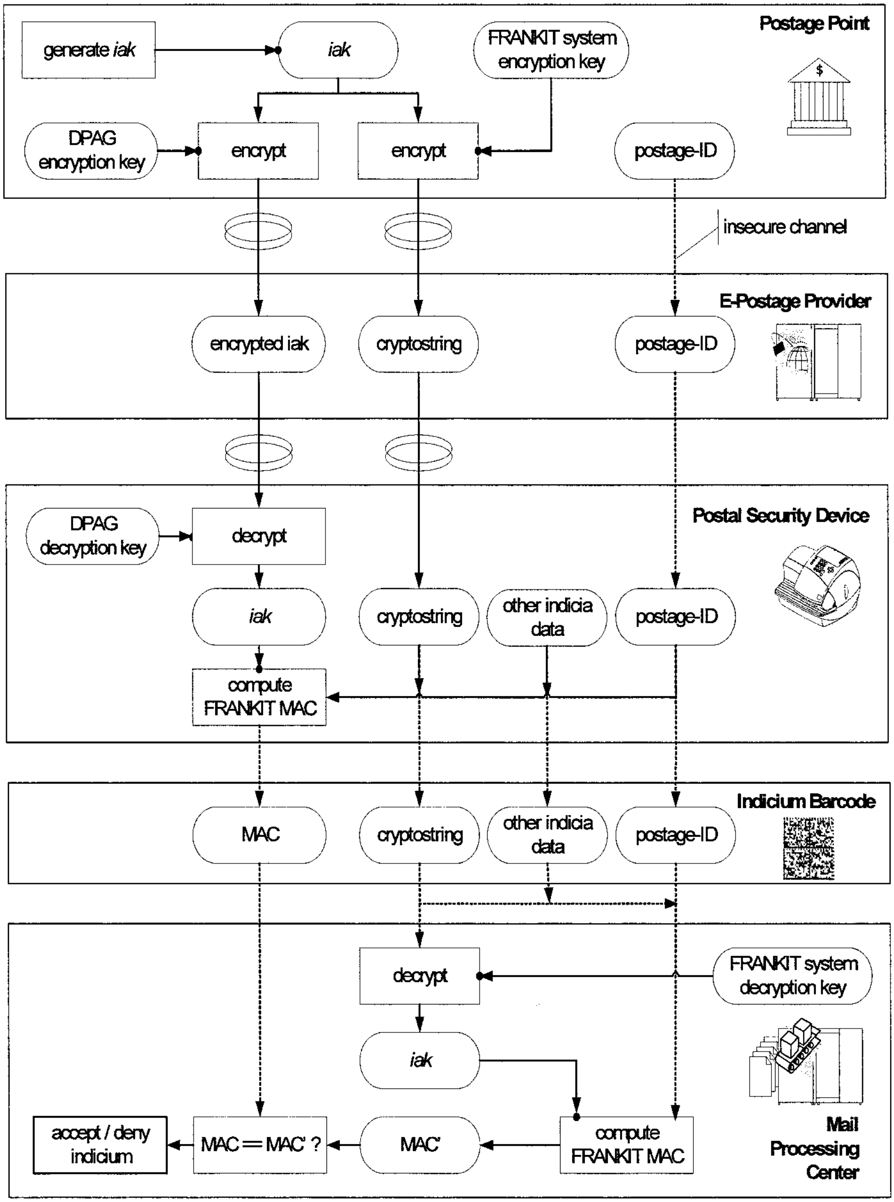


*Figure 52.*Key Flow to Produce and Verify Frankit Indicia

The indicia verifying unit at the mail processing center verifies an indicium according to the following steps (see the bottom half of Figure 52 on page 159):

1. Use the Frankit system decrypting key to recover the indicia authenticating key from the cryptostring.
2. Use these results together with other data from the imprint to compute a message authentication code MAC' according to equation (6.1).
3. Compare this MAC' against the MAC read from the imprint data field #16. If the verification succeeds, accept the imprint, otherwise reject it.

The Frankit system key is a triple-DES key that is updated every 3 months and is distributed to all mail processing centers. The mail processing centers learn which version of the Frankit system key to use for each indicia from the key phase indicator in data field #8 (see Table 20 on page 156).

In addition there are a couple of plausibility checks and a check for duplicate imprints that may have surfaced at the same mail processing center before.

6.5.2 Postal Value Added Services

6.5.2.1 Postage Rate Tables

The Frankit specification [24] mandates that postage meters shall load any updated postage rate tables automatically and as soon as possible after they have been released by Deutsche Post. The preferred method of data transfer is remote electronic download. Each indicium carries a reference to the version of the rate table that was actually used by the respective postage meter at the time when the indicia was created (see data field #3 in Table 20 on page 156).

6.5.2.2 Acquiring Usage Data

Postage meters convey their usage data to Deutsche Post electronically through their e-postage providers every time they request a postage value download. Deutsche Post promotes the same failure control strategy as Canada Post that requires a postage meter to successfully upload its usage data before it receives the requested amount of postage.

Frankit indicia contain detailed class of mail information down to the level of rate categories, the highest level of detail. In addition, each postage meter collects all the rate category information of its imprints and transmits it to its e-postage provider during the next postage value download. At the end of each business day, each e-postage provider compiles a number of files containing the usage data for its contracted postage meters that performed a postage value download on that day. The usage data file contains an entry for each month, for each product code (rate category) and for each user that was reported by the postage meters on that day. Each entry shows the number of indicia and their total amount of postage. The usage data files are uploaded through the Provider Post Backoffice Security Domain to the Postage Server as explained in the Frankit Specification [24].

6.5.2.3 Registered Mail

Producing imprints for domestic and international registered mail is more integrated into Frankit than it is into IBIP of the USPS or DMIS of Canada Post. A certified or registered mail imprint under Frankit consists of a human readable portion and a linear barcode. The human readable area shows the keyword "Deutsche Post" and its logo, a short description of the type of registered mail, and an tracking number (*identcode)*, i.e., a 14 character (domestic) or 11 character (international) string to identify the mail piece uniquely. The linear barcode is a code 128 containing the identcode. The additional fees for registered mail are reflected by the product code (rate category), and the corresponding postage amount of the accompanying Frankit indicia. In addition,

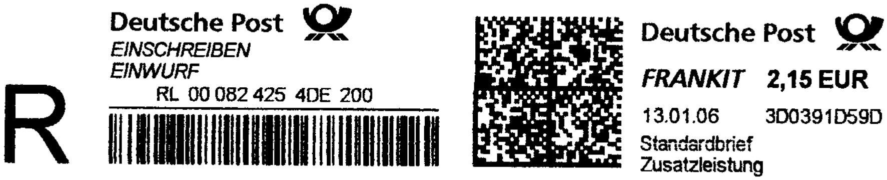


*Figure 53.*Sample Frankit Indicia for domestic certified mail

the identcode is included in the service data field #15 of the indicia barcode (Table 20 on page 156). An example of a Frankit indicia with accompanying imprint for domestic registered mail is shown in Figure 53 on page 161. Customers can request up-to-date tracking information about their certified and registered mail pieces, both domestic and international, from the Deutsche Post Internet homepage. Foreign postal operators feed their mail delivery statuses into the Deutsche Post registered mail tracking system.

6.5.2.4 Postage or Date Correction

There are no special indicia available to correct the amount of postage or the mailing date of a printed indicia.

6.5.2.5 Reply Mail

Mailers can choose metered reply mail, which is pre-paid by the mailer. It is called "return answer letter" [24]. The reply mail imprint looks exactly as a regular imprint, but carries the intended recipient's postal code in the service data field #15 of the barcode (Table 20 on page 156). A sample is shown in Figure 54 on page 162.

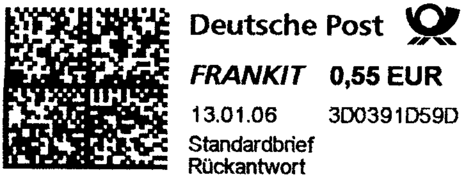


Figure 54. Sample Frankit Indicia with business reply service

6.5.2.6 Order Management

Frankit allows owners of postage meters to meter mail in behalf of third parties or to let third parties frank mail by themselves as a kind of self service. This service is called "order management". For all frankings done in behalf of or by a third party, the third party's own customer number with Deutsche Post (7-digit EKP-Number) or a one-time job number (14-digits) provided by Deutsche Post is entered into the e-postage device and gets included in each indicia. These indicia look exactly like regular indicia, but carry the third party's customer number or the one-time job number in the service data field #15 of the barcode (Table 20 on page 156).

6.5.2.7 Addressing, Mail Forwarding and Return Services

Deutsche Post runs an addressing service database system, the addressing service being called "Premiumadress". Typical customers for Premiumadress are large mailers such as direct marketing companies. They can enroll in Premiumadress by opening a Premiumadress account. In their accounts, customers can create subordinate accounts with separate bank account information, separate contact persons to which change of address notifications shall be sent and separate postal addresses to which return mail shall be delivered. This supports mailers to send out a mailing to a large number of target customers from a central mail production site while the customers are assigned to different customer service agents. Mailers can maintain their Premiumadress accounts online through a web interface provided by Deutsche Post, and the mailer's agents can maintain their own subordinate accounts online in order to take care of their respective customers directly.

Premiumadress is available only in combination with order management (Section 6.5.2.6 on page 162), which causes the customer ID (EKP) to be included in service data field #15 of the barcode (Table 20 on page 156). Each subordinate account is then identified by a Premiumadress-ID, which must also be included in the service data field #15 of each barcode (Table 20 on page 156) that requests addressing service. In order to use an addressing service, the mailer needs to add an extra imprint showing the keyword Premiumadress (Figure 53 on page 161). This extra imprint informs the mail carrier how to handle the mail piece if it cannot be delivered at the destined address.

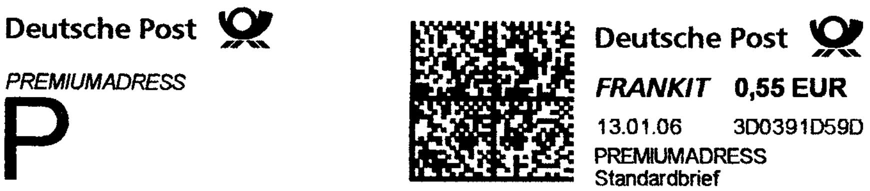


*Figure 55.*Sample Frankit Indicia with Premiumadress service

Depending on the class of mail, the mailer may choose from five available types of Premiumadress, which is reflected by the rate category (product code) included in the indicia barcode. The type of Premiumadress is not visible in human readable form because the mail carrier handles them all in the same way, namely by sorting them out into a return mail bag.

- "Standard" (Standardvariante) causes the mail to be forwarded to the corrected or new address or disposed of if no valid address could be attained and the mailer be notified in any case,
- "Forward or Return Service Requested" (UZ-Retoure) causes the mail to be forwarded to the corrected or new address or returned if no valid address could be attained and the mailer be notified in any case,
- "Return Service Requested" (Umzug- und UZ Retoure) causes the mail to be returned with new address or reason for non-delivery if applicable.
- "Forward or Return Service Requested without notification" (UZ-Retoure statt Info) is like "Forward or Return Service Requested but without notifying the sender.
- "Standard without notification" (UZ-Info ohne Retoure) is like "Standard", but the mailer is notified only if the mail could not be delivered

and was disposed of. Mailers demand this kind of notification to support their claims against commercial sellers of customer addresses.

6.5.2.8 Refunding for Spoiled Indicia

A refund procedure is in place for spoiled or otherwise damaged Frankit and conventional indicia that have been paid for, but could not be used as postage. Mailers who return spoiled indicia need to fill in respective applications for refund of postage including their bank account details and sign it. All applications must be sent to Deutsche Post Service Management in Bielefeld Germany and get reimbursed directly, without involving the respective e-postage provider.

6.5.2.9 Demonstrating E-Postage

Deutsche Post allows e-postage devices to be initialized or re-initialized in a special mode for demonstration purposes. In this specimen mode, they can print out specimen indicia only, which are not accounted for, resemble the layout of regular indicia, but are clearly marked as invalid (see Figure 56 on page 164). In specimen mode, e-postage devices use the indicia authenticating keys provided by the Postage Point just as they do in regular mode to compute their message authentication codes in data field #16. However, the mail sorting centers shall be unable to recover the data of the 2D barcode because a voiding mark covers the center of the 2D barcode and the clear text postage amount is crossed out.

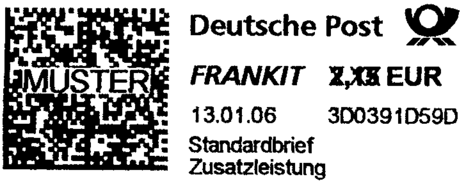


*Figure 56.*Specimen Type of Indicium

6.6 NETHERLANDS POST (TPG POST)

The Netherlands Post, TPG Post, has an offline electronic postage program (NetSet 1) in place [75]. It supports all NetSet 1 compliant postage meters to report their usage data on a timely basis. NetSet 1 indicia are not cryptographically secured, and NetSet 1 supports only postal rates that are not subject to sales tax or any other taxes. The liberalization of the European Postal markets will further harmonize the inconsistent taxation requirements on different postal products, most notably that letter delivery is exempt from sales tax, while parcel delivery is fully subject to sales tax. It is conceivable, that the liberalized European postal markets will demand sales tax, for example, for value-added services beyond the basic postal mail transportation.

TPG Post is preparing to roll out a new electronic postage program called NetSet 2, which shall support postal rates that are partially subject to sales tax and mandates cryptographically secured indicia using data matrix barcodes of 16 by 48 elements. In order to fit within the limited capacity (47 byte) of such barcodes, their integrity checks shall be based on a truncated message authentication code that employs the hash function SHA-256.

6.7 OTHER POSTAL MARKETS

Many postal operators have embraced the data matrix symbology to automate the mail sorting and processing, among them the universal postal operators of Australia, Canada, Germany, New Zealand, Norway, Switzerland, and the United States. As of 2005, only the postal markets of Canada, Germany, and the United States mandate cryptographically secured indicia for offline electronic postage systems. Some postal operators have designed their electronic postage programs such that they can acquire usage data for marketing reasons.

6.8 PRELIMINARY APPRAISAL

The specifications of the existing industrial offline e-postage systems have been around for less than a decade and practical experience with operating such systems is limited to a couple of years only. Hence, the following conclusions must be understood as preliminary and may have to be revised based on the next couple of years of experience.

The common experience of the US Postal Service and Deutsche Post is that scanning and analyzing information rich indicia at about 9 to 10 mail pieces per second is a challenge. The US Postal Services, Deutsche Post and Canada Post are ramping up their scanning rates gradually. By March 2006 the US Postal Service intends to scan 97% of IBIP indicia, while Deutsche Post scans about 50%, and Canada Post is just beginning to see the first fully compliant indicia in its mail stream. This approach appears to be appropriate because the rate of information rich indicia among all mail pieces is starts out low with an expected annual increase of about 5% if no incentives or regulative measures motivate customers to exchange their existing postage meters by new ones.

Given current wide view cameras and imaging equipment, it appears unlikely to achieve readability rates of more than 95% for information rich indicia under real-life operating conditions. One of the limiting factors is the indicia color. IBIP and DMIS indicia are printed in fluorescent red, Deutsche Post and TPG have adopted postal blue ink. Neither color achieves optimal contrast nor was it chosen to optimize the readability rate.

The footage of US Postal Service has recognized that IBI indicia of 112 byte capacity have too large a footprint for high speed postage meters. Thus, the US Postal Service has developed the IBI Program further. IBIP-Lite promotes indicia that are based on a data matrix barcode of 12 by 36 elements. These indicia use a 4-byte truncated message authentication code in place of the digital signature of IBIP indicia in order to fit into the limited space of 20 bytes.

The offline electronic postage systems seem to achieve the security they claimed in the first place. No significant security breaches have been reported by the US Postal Services, Canada Post or Deutsche Post. Postage meter fraud is on the decline for the new generation of postage meters. In some cases, however, this increase of security is achieved by large cryptographic checksums, which in turn blow up the indicia. The relative size of the cryptographic checksums are compared in Table 21 on page 166. If we relate the number of content bytes to the number of integrity check code bytes and take it as a measure of security space efficiency, then we get a ranking as displayed in the right most column of Table 21 on page 166. Practical experience will tell if large integrity check codes and therefore large indicia have enough benefits in certain applications to justify their size.

Table 21. Summary: Relative Size of Integrity Checksums

Country	*E-Postage Program*	*Indicia Capacity*	*Relative Size of Checksum*	*Bytes of Content per Byte of Checksum*
US	IBIP	112	36.0%	2.1 byte
US	IBIP-Lite	20	20%	4 byte
CA	DMIS	158..172	79..81%	0.23..0.27 byte
DE	Frankit	84	4.8%	20 byte
NL	NetSet 2	47	8.5%	10.8 byte

Chapter 7

Industrial Online E-Postage Systems

7.1 INDUSTRIAL ONLINE E-POSTAGE

A few postal operators have started their online e-postage system infrastructures and encouraged e-postage providers and mailers to follow. In the following sections, we review the (cryptographically secured) online e-postage systems that exist worldwide. Our emphasis is on industrial scale online e-postage systems that are supported by a postal operator and at least one e-postage provider. We present these e-postage systems in terms of the general model introduced in Chapter 2 on page 25.

7.2 THE ONLINE E-POSTAGE MARKET

Worldwide, there are two postal operators who invite e-postage providers to sell (cryptographically secured) online electronic postage. The US Postal Services announced their IBI Program for centralized systems [102] in August 2000, while Deutsche Post launched their Internet postage service [23] in August 2001. Both programs are good for franking letters and parcels. As of 2005, the US Postal Services supports IBIP for centralized systems in the US and US territories, while Deutsche Post supports Stampit for first class mail in Germany and for parcels and higher value letters throughout Europe.

The IBI Program for centralized systems has attracted 5 e-postage providers in the US offering online postage through their respective web sites. The US Postal Service lists them online at http://www.usps.com/onlinepostage/.

1. *Stamps.com* got approval for their online postage service in 1999 and for their NetStamps service in 2002. They have more than 300,000 active customers, mostly small offices and home offices.
2. *Endicia.com* got approval for their Internet postage service in 2000. It supports printing indicia for certified mail including delivery confirmation, and also for insured mail, international mail, parcel post, media mail, bound printed matter and library mail.
3. *Click'n'ship* is the online postage service of the US Postal Services. It supports most classes of mail and asks no monthly fee.

4. *eBay* offers an Internet postage service that integrates into the eBay Client application. Sellers can pay their postage and monthly fees through PayPal, eBay's Internet payment instrument.
5. *Shipstream Manager* is an Internet postage service of Pitney Bowes. Mailers can produce shipping labels for parcels, packages, and oversized envelopes.

The PC franking program of Deutsche Post attracted considerable interest when it was announced in 2000, but until 2005, only one e-postage provider has launched its service: Deutsche Post itself started a product called *Stampit* in September 2001. Stampit is available in three flavors: Two PC software applications, *Stampit Home* and *Stampit Business*, and one web application, called *Stampit Web*. Stampit Home and Stampit Business integrate into Microsoft Word and Open Office such that indicia can be printed also in the upper right corner of the address window of a letter. This saves a separate print of the indicia onto an envelope or label. StampitWeb integrates into the eBay web client and addresses eBay sellers throughout the European Union who ship their goods through Deutsche Post. Deutsche Post has licensed several customized versions of Stampit Home and Stampit Business to other European postal operators to support their domestic postal network.

1. Swiss Post has offered *WebStamp* in Switzerland since 2002.
2. Royal Mail started *SmartStamp* in the United Kingdom in 2004.
3. Estland Post started a trial of a customized version of Stampit Home in 2005.

IBI for online e-postage devices is an open standard of the US Postal Services that is supported by several private e-postage providers in the US with respective products.

Stampit is a proprietary standard of Deutsche Post. Documentation for Stampit is available only under a confidentiality agreement. E-postage providers for Stampit are Deutsche Post and a couple of universal postal operators who have licensed the Stampit system from Deutsche Post. Stampit Client software is available for Microsoft Windows. An open source project 'GNU-Stamp' was launched in August 2005 to develop Stampit Clients for other operating system platforms such as Linux or Mac OS X [60]. It remains an open question if Deutsche Post will support such approaches to develop Stampit towards an open standard.

7.3 UNITED STATES POSTAL SERVICES

The US Postal Services launched the Information Based Indicia Program (IBIP) for online open e-postage devices in August 2000 [102]. The US Postal Services reports an installed base of online e-postage devices of more than 450,000 in the year 2000. This high figure resulted from the competing race of the two online postage pioneers, namely e-stamp and stamps.com, who both won postal approval in 1999. After the dot com bubble had burst in 2000, the number of online e-postage clients dipped slightly and came out after the first 5 years of IBI online postage availability about 1% above the figure in year 2000. Figure 57 on page 169 shows that online postage has established an additional market in the US, which has not cut into the traditional market of postage meters, but probably took its market share away from stamps.

Year	Online	Offline	Total
2000	450564	1,604,834	2,055,398
2001	376307	1,615,031	1,991,338
2002	404048	1,624,965	2,029,013
2003	419158	1,653,580	2,072,738
2004	461694	1,661,042	2,122,736
2005	553751	1,664,197	2,217,948

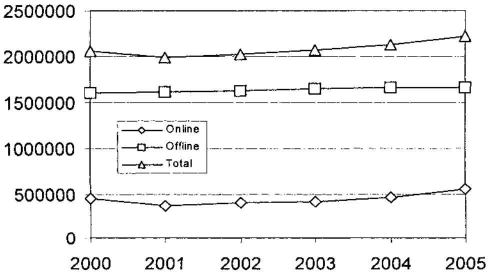


*Figure 57.*Number of installed online e-postage devices in the US

All IBI Online Clients are required to support at least Express Mail, Priority Mail, International Express Mail, Global Priority Mail, and Priority Mail.

7.3.1 IBIP for Open Online E-Postage Systems

According to the Information Based Indicia Program, each online e-postage device needs to have its own postal security device. For online e-postage devices, these postal security device are data records located, protected and concentrated at the e-postage provider site. They are thus called *virtual postal security devices*.

When an IBI Online Client is setup, it is assigned a fresh virtual postal security device at its e-postage provider. During the setup, the mailer is assigned a unique user ID and password, and a hash of the password is imported into the corresponding virtual PSD. Second, the IBI Online Client generates two long term public key pairs, one for encryption and one for doing signatures and transmits both public keys to its virtual PSD at its e-postage provider. Third, the virtual PSD generates an indicia key pair, requests a public key certificate for the indicia verifying key from the USPS Certificate Authority and returns the indicia verifying key together with the serial number of the retrieved public key certificate to the IBI Online Client. Fourth, the virtual PSD initializes its postal registers to zero.

The IBI Online Client is now ready to download a first amount of postage. The message flow is depicted in Figure 58 on page 170. The mailer inputs his

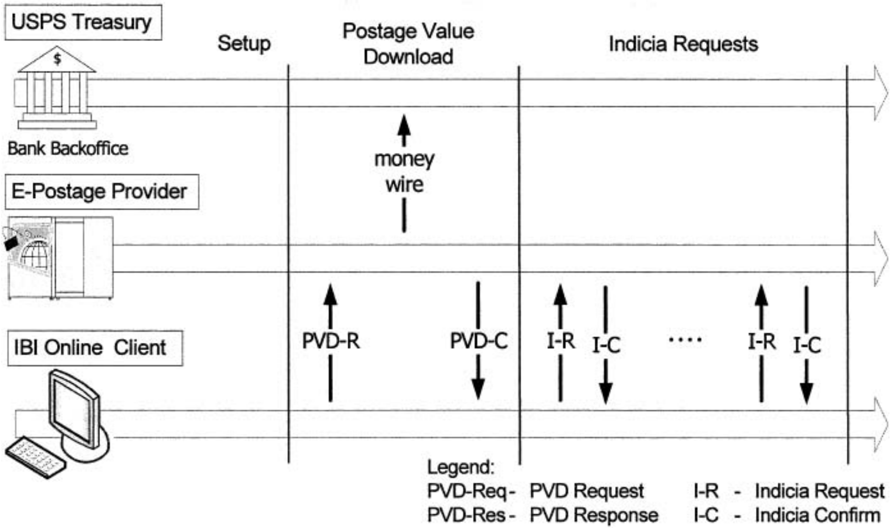


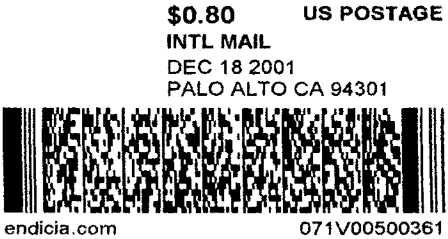
*Figure 58.*Communication Model of IBI Online

password and sends to the e-postage provider a postage value download request (PVD-R), which contains the requested amount of postage and a hash of the password. The e-postage provider routes the request to the corresponding virtual PSD. If the password is verified, the e-postage provider charges mailer's credit card account by the requested amount of postage and, if successful, increases the ascending register of the virtual PSD and confirms the postage value download to the IBI Online Client.

When the mailer wants to send a piece of mail, he inputs the respective mailing parameters such that the e-postage device can look up the rate category and required amount of postage from its postage rate table or he inputs those values manually. The mailer further enters his password and sends an indicia request (I-R) to the e-postage provider. The indicia request contains a hash of the password and at least the unique user ID, required amount of postage, its currency, the mailing date, the destination ZIP code, and rate category. The e-postage provider forwards the indicia request to the respective virtual PSD, which verifies the password, reduces its descending register by the required amount of postage, and returns an indicia confirm message back to the IBI Online Client. Finally, the IBI Online Client composes the indicia content, computes the barcode symbology and prints it onto the actual mail piece.

7.3.1.1 Indicia Layout

Indicia complying to the IBIP specification contain a 2D barcode based on either the data matrix symbology of 40 by 40 elements or the PDF417 symbology, and a human readable information as shown in Figure 59 on page 171. The barcode symbology must achieve a sufficient readability rate under US Postal Service reading conditions. Indicia may be printed in standard black ink. A facing identification mark (FIM) must be added to indicia for domestic mail according to applicable USPS regulations [103]. Mail pieces carrying online e-postage may be deposited in street letter boxes.



$0.80 US POSTAGE
INTL MAIL
DEC 18 2001
PALO ALTO CA 94301
endicia.com 071V00500361

*Figure 59.*Sample IBI Indicia of an Open Online E-Postage Device

Indicia of open online e-postage devices meet the same requirements as those of closed e-postage devices as described in Section 6.3.1.1 on page 131. Each virtual postal security device has a serial number, which is used in just the same way as the serial number for postal security devices in offline e-postage systems. Online indicia differ from offline indicia in one important respect: The reserved data field #11 indicates the ZIP+4 code of the recipient for domestic mail and the ISO country code plus the length of the recipient address for international mail. The US Postal Service requires to include the recipient ZIP code as a deterrence from copying indicia in return for allowing online e-postage to be printed in black ink.

7.3.1.2 Security Architecture

The security architecture described for offline e-postage IBI systems (Section 6.3.1.1 on page 131) basically carries over to online e-postage IBI systems if we consider the virtual postal security devices hosted at the e-postage providers central repository to take the place of the physical postal security devices in offline e-postage devices. This configuration simplifies the postage value download operations because they can be handled entirely in the provider post backoffice security domain and all postal security devices may be regarded as virtually always available and properly working. However, sending requests for depositing funds (including postage value downloads), new indicia, register status, account balance report, or postage value refunds from the online e-postage device to the e-postage provider requires a cryptographic protection in the refill security domain. Since the e-postage device is stateless with respect to postal registers, there is no need for transaction security, for example, 2-phase commit protocols.

Upon initialization of a virtual PSD, it generates an indicia key pair (*iak*, *ivk*) and requests a public key certificate for *ivk* from the USPS certificate authority. The virtual PSD keeps the certificate and forwards the certificate serial number to its IBI Online Client, which includes the certificate serial number in all its subsequent indicia. The public keys and certificates involved are shown in the upper part of Figure 64 on page 181

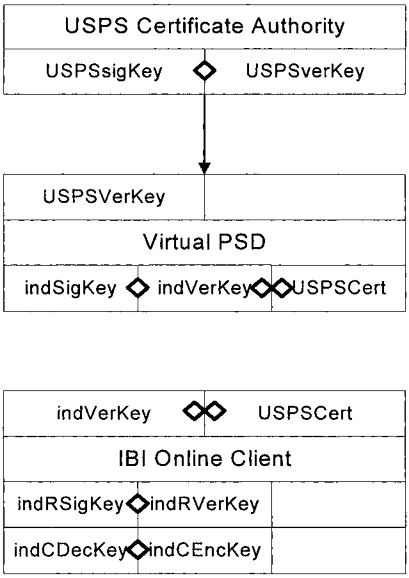


*Figure 60.*Public Keys and Related Certificates

Also during initialization of a virtual PSD, its IBI Online Client generates an indicia request key pair (*indRSigKey*, *indRVerKey*) and an indicia confirm key pair (*indCDecKey*, *indCEncKey*), and the public parts of both key pairs are imported into the virtual PSD. These public keys are not required to be certified, but an extra key transport key layer, such as the Secure Socket Layer (SSL) or the Transport Layer Security (TLS) [74], should be provided to facilitate the transfer of either key pair over an authentic channel for the first time and for rekeying it later on.

If an IBI Online Client requests an indicium, it composes the data fields #1..#14 (Table 18 on page 132) in exactly the format they occur in the indicium, signs the message using its *indRSigKey* and sends it to the e-postage provider. After receiving the indicia request, the virtual postal security device verifies the message signature using the *indRVerKey*, computes the digital signature *sign* for the transmitted message using its *iak* and encrypts the result under the *indCEncKey*. When the online e-postage device receives the response, it recovers the signature *sign* by using its *indCDecKey* and inserts the signature in data field #15, which completes the indicium.

If the centralized virtual PSD repository keeps the actual data of the postal security devices within a database, then it must have strong cryptographic integrity protection at record level and the indicia authenticating key *iak* of each postal security device must be encrypted.

7.3.1.3 Verification of Indicia

Indicia of open online e-postage devices are verified at mail sorting centers exactly as those originating from offline e-postage devices (see Section 6.3.1.3 on page 134). Thus, the mail processing centers run a uniform verification algorithm for all IBI indicia.

7.3.2 Postal Value Added Services

7.3.2.1 Postage Rate Tables

The US Postal Services provides new postage rate tables online and mandates that online e-postage devices use new rate tables when they become valid.

7.3.2.2 Acquiring Usage Data

The US Postal Services is not acquiring usage data through an electronic channel from e-postage devices, neither online nor offline.

7.3.2.3 Certified and Registered Mail

Online e-postage devices shall support certified, registered, and insured mail by handling and printing tracking numbers as outlined in Section 6.3.2.3 on page 135.

7.3.2.4 Postage or Date Correction

Online e-postage devices shall support postage and date correction indicia. Producing postage correction indicia works interactively like producing regular indicia. Date correction indicia are produced offline by online e-postage devices.

7.3.2.5 Reply Mail

Online e-postage devices shall not support business reply mail.

7.3.3 IBI-Lite for Online E-Postage Systems

The US Postal Services actively promotes new forms of online electronic postage, such as customized stamps or photo stamps by commercial providers (see Figure 10 on page 19) in order to eliminate capital investment while providing opportunities for cost savings, cost avoidance, revenue generation, and mail security (see also Section 6.3.3 on page 139). A one year market test was launched in May 2005.

IBI-lite indicia produced by online e-postage devices resemble the looks of traditional stamps much more than regular IBI indicia. The better part of these IBI-lite indicia shows some graphics or photograph of the mailer's choice, and only a small fraction of the footprint is reserved for the data matrix barcode and some human readable information such as the face value of the indicia.

7.4 DEUTSCHE POST

Deutsche Post launched their Internet postage service Stampit in August 2001. In Germany, Stampit has more than 80,000 registered users. As Deutsche Post started to market their parcel delivery service throughout Europe, Stampit can be used by all World Net shippers in Europe to pre-pay for their parcels. There is only one approved e-postage provider for Stampit, namely Deutsche Post, and they provide three types of Stampit Clients: Stampit Home is for home use, Stampit Business is for small offices, and Stampit-Web, a web application, is customized for eBay sellers. PCs running any kind of

Stampit Client are open online e-postage devices that connect over the Internet to the e-postage provider, which supplies the actual postage rate table and downloadable postage, and collects usage data. Stampit Clients must support all postal products listed by the rate table of Deutsche Post. The actual rate table shall be downloaded by a Stampit Client automatically on the next occasion after it has been activated by the e-postage provider. The e-postage provider system operated by Deutsche Post is called *Postage Point*. The Postage Point employs a cryptographic accelerator called SafeBox, which is a customized WebSentry Ethernet device [73] employing a Secure Generic Sub-System, both by Thales e-Security (Table 11 on page 76).

7.4.1 Stampit for Open Online E-Postage Systems

When a Stampit Client is setup, it is assigned a fresh virtual postal security device at the e-postage provider. During the setup, the customer is assigned a username and password, and a hash of the password is configured inside the corresponding virtual PSD, such that the customer can later identify his Stampit Client to its virtual PSD over the Internet. Second, the virtual PSD generates two long term public key pairs, one for encryption and one for doing signatures and, third, requests public key certificates from the e-postage provider for both its public keys. In return, the virtual PSD receives the public key certificates and the public verifying key of the Postage Point. Fourth, the virtual PSD initializes its postal registers to zero. The cryptographic engine inside the Postage Point is an array of cryptographic accelerator cards by Thales e-Security [73].

The Stampit Client is now ready to download a first amount of postage. The message flow is depicted in Figure 61 on page 176. The mailer inputs his password and sends to the e-postage provider a postage value download request (PVD-R), which contains the requested amount of postage and a hash of the password. If applicable, the e-postage provider downloads a new rate table to the e-postage device and, afterwards, routes the request to the corresponding virtual PSD, which verifies the password hash. If successful, the virtual PSD establishes a session encryption key with the Postage Point by employing the long term public keys that were exchanged during its initialization. Stampit uses a proprietary key transport protocol (see Section 4.5.3 on page 112), and the following messages are exchanged in encrypted form under the resulting session keys. The virtual PSD generates a fresh indicia authenticating key (*iak*) and sends it along with the loading amount (L) and the usage data (U) collected since the previous postage value download request to the Postage Point. (During the initial postage value download request, the usage data message is empty.) Finally, the virtual PSD increases its ascending register by the requested amount of postage. The Postage Point,

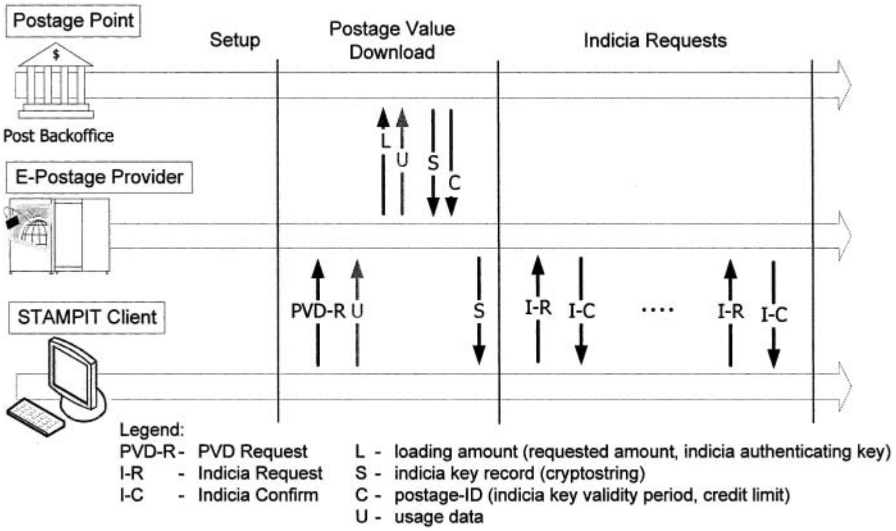


*Figure 61.*Communication Model of Stampit

in turn, contacts the bank backoffice in an offline batch job to debit the mailer's bank account for the requested amount of postage.

The Postage Point returns an indicia key record containing a cryptostring (S) and a postage-ID (C). The cryptostring is the indicia authenticating key encrypted under a Stampit system key, which will be required to verify indicia later on. The postage-ID contains the validity period of the indicia authenticating key contained in (L) and a corresponding credit limit, which is set to a default value for new customers. To confirm the postage value download, the e-postage provider returns the new cryptostring (S) to the Stampit Client, which needs to use it in all subsequent indicia until the next postage value download.

When the mailer wants to send a piece of mail, he inputs the respective mailing parameters such that the e-postage device can look up the product code and required amount of postage from its rate table. The mailer inputs his password and sends an indicia request (I-R) to the e-postage provider. The indicia request contains a hash of the password and at least the required amount of postage, its currency, the product code, the mailing date and the destination postal code. The e-postage provider forwards the indicia request to the respective virtual PSD, which decreases the descending register by the postage amount, computes the matching hash value and returns it to the Stampit Client. Finally, the Stampit Client composes the indicia content, computes the data matrix symbology and prints it to the actual mail piece.

7.4.1.1 Indicia Layout

Indicia complying to the Stampit specification contain a 2D barcode based on the data matrix symbology of 32 by 32 elements, and a human readable information as shown in Figure 62 on page 177. The barcode symbology must achieve a sufficient readability rate under Deutsche Post reading conditions. Indicia may be printed in standard office (black) ink. Mail pieces carrying online e-postage may be deposited at post offices and in street letter boxes on the date shown as the mailing date or the next day.

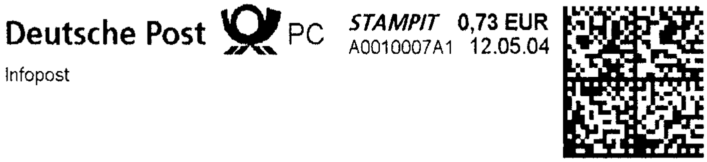


*Figure 62.*Sample Stampit Indicia

Stampit indicia meet similar requirements as Frankit indicia described in Section 6.5.1.1 on page 155. Each virtual postal security device has a serial number, which is used in just the same way as the serial number for postal security devices in offline e-postage systems. The information contained in Stampit indicia is summarized in Table 22 on page 177.

Table 22. Summary: Stampit Indicia Contents

No	*Data Element*	*Barcode Area*	*HR Area*	*Length [byte]*
1	Postal operator	X	X	3
2	Indicia version no	X	—	1
3	Rate Table version no.	X	—	1
4	Serial No.	X	—	5
5	Piece counter	X	—	3
6	Key Phase Indicator	X	—	1
7	CryptoString	X	—	24
8	Postal product code	X	—[a]	2
9	Postage	X	X	2
10	Date of mailing	X	X	2

Table 22. Summary: Stampit Indicia Contents

No	*Data Element*	*Barcode Area*	*HR Area*	*Length [byte]*
11	Recipient postal code	X	—	3
12	Recipient Postal Address	X	—	6
13	Truncated MAC	X	—	4
	Total Length			57

a. The human readable area contains a clear text description of the postal product.

Online indicia differ from offline indicia of Frankit in one important respect: The reserved data field #11 indicates the recipient postal code for domestic mail or a condensed description of the postal address for international mail. Deutsche Post requires to include the recipient postal code as a deterrence from copying indicia.

The truncated MAC of an indicium is computed by forming a message of the first 53 bytes of the indicium appended by the 12-byte postage-ID appended by the 12-byte indicia authenticating key (*iak*). This message is input to the hash function SHA-1 and the 20-byte result is truncated to the first 4-byte as follows:

$$h = \text{SHA-1}_{1..4}(\text{indicia}_{1..53} \,\|\, \text{postage-ID} \,\|\, iak) \tag{7.1}$$

7.4.1.2 Security Architecture

The e-postage provider runs a hardware security module hosting a multitude of virtual postal security devices (Safe Box), one for each Stampit Client. The Postage Point runs a hardware security module (Postage Point Box) that maintains and distributes the electronic postage from the postal operator to the e-postage providers upon postage value download requests.

Technically, the postage value download is a transaction protocol that is cryptographically secured and based upon certified public key pairs for encryption and digital signatures maintained by each virtual PSD and by the Postage Point Box. More specifically, a simplified setup of keys and certificates is shown in Figure 64 on page 181:

Each e-postage provider maintains an individual certifying public key pair. To keep the notation simpler, we consider only one e-postage provider and denote its certifying public key pair as (*eppSigKey*, *eppVerKey*). Likewise, the Postage Point maintains a certifying public key pair (*ppSigKey*, *ppVerKey*). The Postage Point Box maintains one public key pair for encryption (*ppbDecKey*, *ppbEncKey*) and one for digital signatures (*ppbSigKey*,

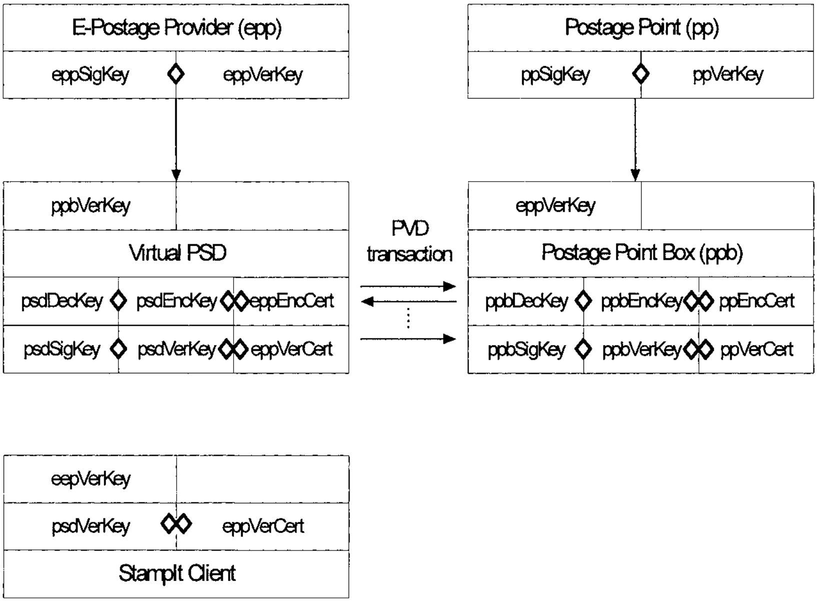


*Figure 63.*Public Keys and Related Certificates

ppbVerKey). In addition, the Postage Point Box downloads the verifying key (*eppVerKey*) of the e-postage provider.

Conversely, during their initialization (see Figure 61 on page 176), each virtual PSD downloads the verifying key of the Postage Point and generates one public key pair for encryption and one for digital signatures. To keep it simple, we consider only one virtual PSD and denote its respective public key pairs as (*psdDecKey*, *psdEncKey*) and (*psdSigKey*, *psdVerKey*). Furthermore, the virtual PSD requests one public key certificate for its encryption key and one for its verifying key from its e-postage provider. As a result the virtual PSD receives and stores two certificates (*eppVerCert*) and (*eppEncCert*), which are valid for the keys (*psdEncKey*) and (*psdVerKey*) with respect to the e-postage provider's public key (*eppVerKey*).

When the mailer requests a postage value download, then his virtual PSD and the Postage Point Box run a proprietary session key establishment protocol by using their respective signing and encrypting key pairs. Afterwards, they transmit all the data items according to Section 7.4.1 on page 175 encrypted by the so established session keys.

If an online e-postage device requests an indicium, it composes a message of the data fields #1..#12 (Table 22 on page 177) in exactly the format they occur in the indicium and sends the message to the e-postage provider. After receiving the indicia request, the virtual PSD computes the 20-byte SHA-1 hash value for the transmitted message appended by a freshly generated 12-byte postage-ID, appended by the 12-byte indicia authenticating key (*iak*) that it generated upon the most recent postage value download request. It signs the hash value with its *psdSigKey* and returns the hash value together with the signature to the Stampit Client. The Stampit Client verifies the signature by using the verification key *psdVerKey* of its virtual PSD and, if successful, inserts the 4-byte truncated hash value in data field #13, which completes the indicium. Note that the Stampit Client cannot verify the hash value directly because it would not know the actual postage-ID nor the indicia authenticating key, which are kept secret by the virtual PSD.

Clearly, the Stampit Client must have been supplied with the verification key *psdVerKey* of its virtual PSD in the first place. Stampit leaves the solution and other design of the interface between a Stampit Client and its virtual PSD to each vendor applying for a Stampit license. An obvious solution as shown in Figure 64 on page 181 is to implant the e-postage provider's verifying key (*eppVerKey*) within the software binary of each Stampit Client. During its initialization, the freshly created virtual PSD provides its verifying key *psdVerKey* together with its certificate *eppSigCert* to the Stampit Client. If it finds the *eppSigCert* valid for *psdVerKey* with respect to the implanted *eppVerKey*, then the Stampit Client accepts the *psdVerKey* and stores it persistently, e.g., in the MS-Windows Registry.

7.4.1.3 Verification of Indicia

Stampit indicia are verified by the mail processing centers of Deutsche Post in the same way as Frankit indicia are verified (see Section 6.5.1.3 on page 158) by using a separate Stampit system key in place of the Frankit system key.

7.4.2 Postal Value Added Services

The Stampit Home and Stampit Web Clients provide a minimal functionality, while Stampit Business provides some of the additional functions that are also available under the Frankit program. In particular, the mailer can integrate a customized advert into the Stampit imprint as shown in Figure 64 on page 181.

7.4.2.1 Postage Rate Tables

The Postage Point of Deutsche Post provides new postage rate tables online and mandates that all online e-postage devices use new rate tables when they become valid.

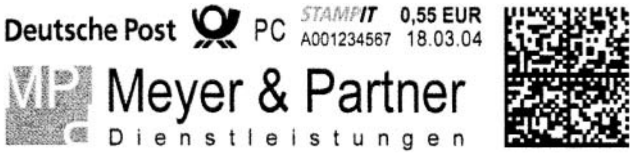


*Figure 64.*Sample Stampit Indicia with Advertisement

7.4.2.2 Acquiring Usage Data

The Postage Point of Deutsche Post acquires usage data through an electronic channel from all e-postage devices, online and offline.

7.4.2.3 Certified and Registered Mail

Stampit Business supports certified and registered mail by handling and printing tracking numbers as an additional service outlined in Section 6.5.2.3 on page 161.

7.4.2.4 Postage or Date Correction

Stampit does not support the correction of an amount of postage or the date of a printed indicia.

7.4.2.5 Reply Mail

Stampit Business supports metered reply mail as outline in Section 6.5.2.5 on page 162

Chapter 8

Security Risks in E-Postage Systems

8.1 RISK MANAGEMENT

The primary goal of e-postage systems is to enable mailers to use the services of postal operators (universal and competitive), to determine the correct amount of postage for each service used, and to transfer the corresponding funds from the mailer to the postal operator in a secure and timely manner. Secondary goals are to provide the postal operators with accurate usage data, to supply mailers with accurate track and trace information and to protect the mailers' and recipients' privacy.

Important assets of an electronic postage system are the postal revenues, the related taxes such as sales tax, the service fees of the e-postage providers, the usage data of all mailers, the track and trace information for the mailers, and the payment information of mailers such as bank account and credit card information.

In order to design and operate secure e-postage systems through their entire system life-cycle, it is important during the design stage to anticipate the security threats to which the e-postage system will be exposed during the system lifetime and after the system's deployment to re-evaluate its residual risks on a regular basis. For any e-postage system under consideration, all this must be planned, organized and performed through an ongoing process called *risk management*. It is an iterative cycle of assessing risks, taking steps to reduce the identified risks to an acceptable level and maintaining that level of risk.

- During the *risk assessment stage* one needs to identify the relevant *assets* of the system and value them. Next, one identifies the possible *threats* that may harm the identified assets. Threats include unintentional disaster or malfunction as well as intelligent attacks. In order to understand the system exposure to intelligent attacks realistically, it is helpful to develop an *attacker model* describing which parts of the system are assumed to be accessible by an attacker in which ways and how strong in terms of resources the attacker is assumed to be. An example of a classification of attacker strength is given by Weingart et al [120] of IBM, which is reproduced in Section 10.3.1 on page 213.

Unintentional threats can be valued by their likelihood. Intelligent attacks can be valued by the expected cost they incur on the perpetrator. Threats can exploit *vulnerabilities* of the e-postage system thereby imposing a *security risk* on the system. A security risk is all the bigger, the more valuable the targeted asset is, the more likely or the cheaper the threat is to incur, and the more severe or critical the expected compromise of or damage to the respective asset will be. This is illustrated by Figure 65 on page 184.

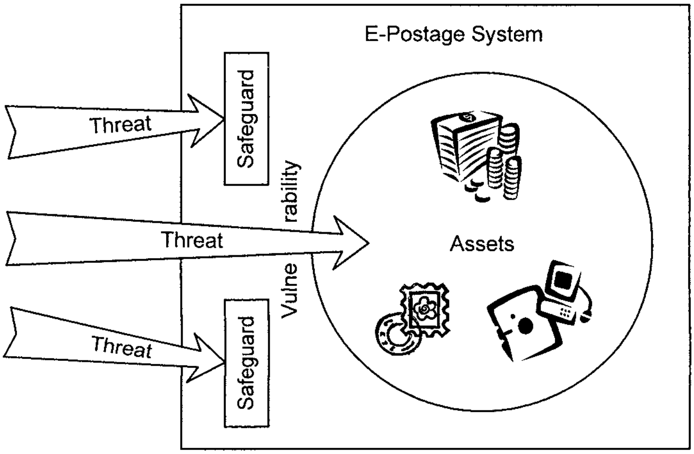


*Figure 65.*Illustration of Risk Management

- During the *risk reduction stage*, one needs to eliminate or reduce vulnerabilities by strengthening existing safeguards and controls or introducing additional ones. All changes to the system are reflected by the system documentation.
- The *risk maintenance stage* usually consists of a system security audit in which all security-critical subsystems and security safeguards are inspected to be in effect and working. The resulting system security report provides the basis on which the current system security level can be determined and compared to the level of system security that was achieved during the previous system security audit or when the e-postage system was first deployed. If new threats or new vulnerabilities are discovered, or existing safeguards are found to be no longer effective, then a new risk reduction stage is entered where appropriate

replacement or additional safeguards are identified and installed and the system documentation is updated accordingly.

General methodologies for risk management have been established by the US National Institute of Standards and Technology (NIST) [93] and the International Standards Organization (ISO) [40] and others.

To facilitate the risk management of e-postage systems, it is helpful to begin with a catalog of common threats on e-postage systems. For each type of e-postage system, e.g., open, closed, online, offline, and combinations thereof, and for each particular system instance, this catalog of threats must be reviewed and needs most likely to be refined. This threat analysis falls into the early stages of the security evaluation of an e-postage system as explained in Chapter 10 on page 207. The results of the threat analysis are to be reflected in the e-postage system design stages and by the security test plan, which is the master document directing and supporting the final security evaluation of an e-postage system.

In this chapter we look at e-postage systems from the point of view of a postal operator, whose primary security requirement is to protect its legitimate revenue. In addition, the mailers may have privacy requirements, whose main concern is to protect their identities against the postal operators and/or the recipients. These privacy requirements will be addressed in Chapter 9 on page 201.

In the following, we develop a catalog of security threats that are common to most e-postage systems and give examples, which sometimes refer back to mechanical and electro-mechanical postage meters. The catalog takes into account the reports of the US General Accounting Office [83,84], and the standards UPU S36-4 [114] Annex C and CEN EN 14615 [19].

8.2 ATTACKER MODEL

For (distributed) business transaction systems in the commercial sector, Weingart et al [120] of IBM proposed to distinguish 3 classes of attackers in the commercial sector:

- Class 1 attackers are considered as clever outsiders, often very intelligent but may have insufficient knowledge of the system. They may have access to only moderately sophisticated equipment. They often try to take advantage of an existing weakness in the system, rather than try to create one.

- Class 2 attackers are considered as knowledgeable insiders, having substantial specialized technical education and experience. They have varying degrees of understanding of parts of the system but potential access to most of it. They often have highly sophisticated tools and instruments for analysis.
- Class 3 attackers are considered funded organizations able to assemble teams of specialists with related and complementary skills backed by great funding resources. They are capable of in-depth analysis of the system, designing sophisticated attacks, and using the most advanced analysis tools. They may use class 2 adversaries as part of the attack team.

In e-postage systems, we need to distinguish the mail delivery domain and the backoffice domains as two areas of potential attacks that are operated in environments under very different control regimes.

8.2.1 Backoffice Domains

The backoffice systems at the e-postage provider, the postal operator and the bank also provide opportunities for cheating system operators and administrators to manipulate data files, transaction data or data base entries in order to "generate" postage that has not been paid for, or redirect funds onto illegitimate accounts, or subvert the system. These system personnel are usually full-time employees working in a controlled environment, and thus may be regarded at most class 2 attackers. Typical examples are greedy, dishonest or disgruntled employees who take advantage of system vulnerabilities they happen to know about.

8.2.2 Refill, Online E-Postage and Mail Delivery Domain

Mailers are identified when their e-postage devices are registered, and companies using closed e-postage devices may face postal inspections under certain circumstances. Otherwise, the mail refill, online e-postage and the delivery domains are effectively uncontrolled from a postal operator's point of view, which creates a variety of opportunities for attack.

In traditional postal mail transport and processing systems, where mail pieces are not cryptographically secured, attackers may get direct access to the mail transport system by bribing or blackmailing postal employees who work at mail processing centers. This way, attackers could illegitimately induct sacks of unpaid mail pieces into the postal transport and delivery system after the stamp cancellation stage and before the address recognition stage without running a big risk of being detected. These avenues of attack can be assumed to be taken by class 1 attackers.

In e-postage systems, the mail processing centers are designed such that the address verification process includes to take a snapshot of the entire face of each mail piece. The resulting digital image is then split into a lower portion carrying the recipient address and an upper portion containing the postage and related information. If the verification of postage fails, then the mail piece is automatically sorted out and delivered to the recipient if he pays a penalty fee, or, otherwise, it is returned to the sender. This higher degree of automation and system integration effectively prevents class 1 attackers from accessing the postal delivery system by bribing or blackmailing postal employees. However, an attacker may try to mis-use e-postage devices to produce valid indicia, which will smoothly pass the mail transport and processing facilities. Since e-postage devices are operated in uncontrolled environments, postal operators assume class 2 or even class 3 attackers, who have all kinds of manipulation and access possibilities to e-postage devices. Attackers can probe one or more e-postage devices to learn about their security design before they mount an informed and sophisticated attack on a new e-postage device.

8.3 THREATS TO E-POSTAGE SYSTEMS

Social engineering can be used to achieve fraudulent goals in each security domain. Threats specific to certain security domains are considered afterwards. Each security domain can come under attack at the level of cryptographic mechanisms. Since 2004, some hash functions that are employed in many e-postage systems have been found to be less secure than expected. We evaluate the implications of these cryptographic weaknesses in the last subsection.

8.3.1 Social Engineering

- *Collusion* is an intentional cooperation between several cheating parties pursuing a fraudulent goal. Parties can collude across security domain boundaries such as mailers collaborating with corrupt employees of the e-postage provider and/or postal operator and/or the bank. An example was described in Section 8.2.2 on page 186. Another type of collusion is if the attacker “hires” a former employee of the manufacturer of an e-postage device to get access to insider knowledge and tools to manipulate an e-postage device and to get hold of replacement lead seals or replacement plastic covers, which would cover up the manipulation,

8.3.2 Backoffice Domains

- *System infiltration* is a general term for any kind of attack impeding the integrity or accountability of financial transaction systems. Most of them are still administrated according to a perimeter security concept, which basically grants little access rights to outsiders on a need-to-know basis and root access rights to insiders. Thus, insiders can misuse their access privileges to database or application servers in order to create hidden accounts and implant Trojan Horses to redirect funds into these accounts. They can cover up such illegitimate action by "cleaning up" the system audit trail after the fact. As a result, outsiders can become privileged insiders once they have figured the passwords or otherwise hijacked one of the privileged user accounts.

System infiltration is not specific to e-postage systems and has been reported to have occurred in grand proportions by many banks [59].

8.3.3 Refill Domain and Online E-Postage Domain

- *Impersonation* is a cheat that results in indicia showing a mailer's ID that is not the originator's. It can be achieved by altering indicia, by manipulating e-postage devices, operating lost or stolen e-postage devices without re-registering them to the new operator's name. For example, in the US market alone, about 0.6% of all registered postage meters were reported lost or stolen in 1996 [77]. Impersonation is usually combined with inappropriate induction.
- *Subverted payments* are an attempt to lead an e-postage provider into providing e-postage for a payment that is later subverted by the mailer, for example, by a bounced check or a rejected direct debit. The attacker tries to download the e-postage into his offline e-postage device before the e-postage provider can detect that in fact the payment was unsuccessful.
- *Repudiation* is the false denial of having participated in a transaction such as a postage value download of an offline e-postage device. If the e-postage provider keeps insufficient evidence about the identity of the e-postage devices connecting, attackers can use repudiation in order to falsely claim their money back.

8.3.3.1 E-Postage Device

- *Manipulation* is the illegitimate modification of e-postage devices. In mechanical postage meters, the key locks and lead seals were circumvented in order to replace the printing dies by others, which, for example, were taken from lost or stolen postage meters of the same or a similar meter model. Another threat was to bypass the lockout mechanism that was to prevent franking after the remaining amount of postage on the descending register had been consumed. Such "jack-pot" meters (also called "roll-over" meters) could reset themselves for the maximum amount of postage available, which in some cases was up to US$99,999,999 [83].
- *Hijacking the print mechanism* is achieved by replacing the print mechanism control of the e-postage device by a PC program of his own making. This attack can theoretically produce any indicia and print it out in postal ink.
- *Print multiplexing* is an attack where the print control unit of a legitimate e-postage device is connected to the printing units of two or more e-postage devices. As a result, the attacker harvests one or more free copies of each legitimate indicia, all of which are printed in postal (fluorescent) ink. This attack can produce indicia duplicates more efficiently and more perfectly than Xeroxing can.

8.3.3.2 Postal Security Device

- *Physical attacks* include drilling, cutting, sawing, sand blasting, exposure to heat or cold or to certain chemical substances such as acids or solvents. These attacks aim at revealing certain electrical access points that are usually protected by the postal security device [87].
- *Side channel attacks* include simple and differential timing attacks, power attacks, tempest and fault induction [74]. These attacks aim at extracting the cryptographic private keys from a postal security device that are necessary to produce valid indicia.
- *Subversion of key management* is the replacement of legitimate cryptographic keys by fake keys of the attacker's own choice or making ("man-in-the-middle" attacks), or the insertion of fake keys into a postal security device. This attack can lead to impersonation, for example, if the attacker employs the cryptographic keys of other customers.

- *Message replay attacks* try to repeat a remote transaction without paying for it a second time. If messages are authenticated by cryptographic means, an attacker may be unable to compute a valid cryptographic checksum for an arbitrarily chosen message, but he can re-use an intercepted message together with its checksum and replay it to the e-postage provider.
- *Bogus postal security devices* behave somehow in favor of an attacker while leaving minimal evidence of their fraudulent behavior. For example, a bogus postal security device might work exactly as the real postal security devices, but continues to produce valid indicia even if the descending register is close or equal to zero. An attacker may fabricate bogus postal security devices by reverse engineering a real postal security device or by colluding with an employee working at the manufacturing site of the postal security devices.

8.3.4 Mail Processing Domain

- *Alteration* is the modification of intercepted indicia such that the postage amount, or sender ID or other data contained in the indicium is changed.
- *Copying* is the illegitimate reproduction of printed indicia by using, for example, photo copying machines or color laser printers [77]. For e-postage systems using cryptographically secured indicia, any indicia occurring twice is invalid by definition. This, however, would not deter perpetrators too much from copying because all "electronic tracks" available to an investigative body would only lead back to the authorized postal security device of the original indicia. Another risk for postal operators stems from attackers using high-speed copying machines to swamp the postal delivery network with mass copies of indicia.
- *Counterfeiting* is the production of valid or valid-looking indicia by anything else than a registered e-postage device, for example, rubber stamps, bitmap processors on a personal computers, or manipulated e-postage devices. Quality counterfeit impressions can usually be detected only through laboratory analysis. It is one of the most common ways of defrauding postal operators.
- *Miss-application* is the act of applying an indicia to a mail piece such that the face value of the indicia does not match the mail piece. If it happens accidentally, it can result in an overpayment or an underpay-

ment. If it happens deliberately, it almost certainly leads to an underpayment.

- *Obliteration* is the defacing of an indicia such that it cannot be read and verified successfully, in the hope to get the mail piece delivered anyway. It can be achieved by folding, spindling, mutilating, smudging, and may be hard to detect because all of these effects can also have unintended causes.
- *Substitution* is the deliberate interception and replacement of a mail piece by another in order to have the latter mail piece delivered by reusing the postage of the former. It has no immediate adverse effect on the postal operator who is paid once and delivers once. However, complaints of the legitimate mailers may degrade the reputation and the business of the postal operator.
- *Inappropriate induction* is a way to induct usually large amounts of mail pieces into the postal delivery system while bypassing the normal induction controls, for example by colluding with an employee at a local mail processing center or at an office of exchange, where foreign mail pieces enter the national postal delivery system.

8.3.5 Algorithmic Level

- *Cryptanalysis* is a general term for any kind of attack against a cryptographic mechanism as outlined in Chapter 4 on page 91.

Each postal operator reserves the right to specify, which cryptographic algorithms are authorized to be used in its e-postage systems. This regulatory authority works as a strong protection of a few species against a number of others that are not allowed to live and prosper. Even if the postal operators review their recommendations for cryptographic algorithms regularly, former recommendations have a lasting effect in real systems. Their average life time from deployment to retirement should be expected to last at least 10 years. The benefit of these regulations is that flawed algorithm are unlikely to be employed in approved e-postage systems. On the other hand, if a flawed algorithm is already employed and turns out to be flawed afterwards or is otherwise broken by cryptanalytic advances, the entire e-postage system and potentially all of the e-postage devices and mailers were put at risk.

A professional way of managing this dilemma is to continue approving only matured cryptographic algorithms, but additionally require the manufacturers of e-postage devices and of e-postage provider systems to also deploy an instant key upgrade method for each cryptographic mechanism to take effect in an emergency case.

8.3.5.1 Cryptanalysis of Common Hash Functions

It is widely accepted that a representative benchmark of an effort that is beyond computational feasibility is 2^{80} operations. That means for a hash function in order to be second pre-image resistant (one-way), it must produce an output of length 80-bit or more. In order to be collision resistant, its hash values must be at least 160-bit long. Shorter outputs are not recommended, because finding second pre-images or collisions can be done offline and such attacks can be highly parallelized.

Hash functions are an example of how too narrow regulations can put all e-postage systems at risk. Since the original Secure Hash Algorithm SHA-0 [90] was revised in 1995 [91], the resulting SHA-1 has become the de-facto standard for hash functions in cryptographic systems and applications. Although alternatives existed, many standards including the ANSI X9.30-1 [3] (DSA), ANSI X9.62 (ECDSA) [7] and the FIPS 186-2 (ECDSA) [94]) adopted SHA-1 as their preferred (and besides a DES based variant often their only) hash function. Even less excusable, the standards recommended that SHA-1 produced a fixed length hash value of 160-bit. This was a striking violation of good cryptologic practice demanding that cryptographic mechanisms should always have a security parameter in order to keep their strength adaptable to progress in available computing power and cryptanalysis.

It comes as no surprise that most if not all existing e-postage systems (and many other cryptographic systems) in 2005 use SHA-1 where ever they employ a hash function, most prominently for (a) preprocessing messages before they get digitally signed or (b) authenticated by using a message authentication code, (c) for deriving the secret keys in session key agreement, and (d) in pseudo-random bit generation according to FIPS 186-2 [94].

As the output length of SHA-1 added some extra margin to the minimum recommended output length for collision resistant hash functions, SHA-1 was believed to be sufficiently collision resistant. That started to change when Biham and Chen [10] demonstrated new ways to find near collisions in SHA-0 and SHA-1 in 2004. At the same time, Wang et al presented collision finding ways for MD4, MD5, Haval128 and RIPEMD160 in a series of papers [116,117]. In 2005, Wang, Yin and Yu published a paper claiming to find collisions with effort less than 2^{69} [119] and later reduced that upper bound to 2^{63} [118], which is in the realm of dedicated practical attacks using parallelization.

All of these attacks aim at the lowest hanging fruit still, i.e., finding collisions, where the attacker is to come up with any two pre-images that map to the same hash value under SHA-1. None of the above research papers reports progress in faster methods of finding second pre-images under SHA-1 or inverting it (see Section 4.4.2 on page 101). In order to evaluate the risks inverting it (see Section 4.4.2 on page 101). In order to evaluate the risks imposed on existing e-postage system by the weaknesses of SHA-1 described above, one must certainly look at each particular system in detail. However, a few general considerations are in order.

8.3.5.2 Exploits of SHA-1 Weaknesses

While we focus on weaknesses of the hash function, we assume the attacker cannot figure out the private signing keys or secret message authentication keys of any postal security device (including his own ones). Such an attacker could try to come up with two or more indicia contents that map to the same hash value under SHA-1, one of which the attacker needs to sign by sending it through a regular postal security device in order to obtain a valid signature. This attack ends up with two or more valid indicia only one of which is paid for (*two-for-one-attack*). Alternatively, such an attacker could capture any given indicia complete with a valid signature and try to come up with a colliding message, for which the given signature were also valid. This attack would come up with one or more valid indicia, none of which is paid for (*one-for-nothing-attack*). The hunt for one or more colliding messages could be performed offline in both types of attack.

How do these attacks apply to the industrial e-postage systems and how likely are they to succeed? In general, the data fields of indicia contents fall into two categories: (a) system constants and data that is specific to a customer or e-postage device, and (b) data that is specific to each individual indicia. Since customers and their e-postage devices are generally registered by the postal operators, the category (a) data fields of an indicium must match a record registered by the postal operator in order to be accepted as valid. The category (b) data fields may vary more widely, but usually must adhere to additional integrity constraints. For example, the data field holding the amount of postage is usually related if not determined by the data field holding the rate category (Section 2.3.1.1 on page 41) or service category.

We first consider the case where SHA-1 is used in combination with a digital signature algorithm such that the indicia content (the message) is first hashed to a fixed length value and then signed by using, for example, RSA, DSA or ECDSA (Section 4.4 on page 98). Afterwards, we consider the case where SHA-1 is used in combination with a message authentication code such as in Frankit (Section 6.5.1 on page 152).

Consider an IBIP indicia that shall be used for a mailing deposited on a specified day. How many valid IBIP indicia contents exist for that day? By analyzing Table 18 on page 132 we find that 8 out of the 14 data fields fall into category (a) namely fields #1-6, 10, and 12. This subset of data can take the values of any of 1.6 million records of registered postage meters in the US (if the market had entirely migrated to IBIP). The remaining data fields fall into category (b). Of those, the date of mailing (field #9) is fixed by the specified date of deposit, and, usually, the rate category (field #4) is uniquely determined by the amount of postage (field #8). Assuming that the unused field #11 may take any possible value, there are 17 bytes of category (b) data left that lead to a valid indicia contents. Factoring in both categories of data, there are at most $1.6 \times 10^6 \times 256^{17} \approx 256^{19.58}$ valid indicia contents. Any formatting restrictions on the data fields under consideration would further reduce this amount.

Because the space of valid indicia contents is about the same order as the space of all SHA-1 hash values, namely, 256^{20}, we conclude that in the context of IBIP indicia, SHA-1 is about a one-to-one mapping. If any, there exist only few collisions, and it is highly unlikely that those could be found by an attacker. This is in line with the results of Wang, Yin and Yu [119], who have found pairs of messages to collide under SHA-1 that are at least 64 byte long. Thus, their attack requires that for each message at least $256^{64-20} = 256^{44}$ collisions exist to be successful. A closer analysis of the Canadian indicia leads to similar results under the assumption that breaking ECDSA over one of the approved elliptic curves mentioned in Section 6.4.1.2 on page 145 is infeasible. One-for-nothing and two-for-one attacks therefore have a negligible chance of success.

If SHA-1 is used in combination with a (truncated) message authentication code, the above attacks can only exploit collisions on the indicia contents of the input to SHA-1, but not on the secret authentication key part, which is neither known nor controlled by the attacker. Frankit indicia are a particularly simple example of using SHA-1 as a message authentication code as shown in Section 6.5.1.1 on page 155. The 80-byte indicia content ($\text{indicia}_{1..80}$) can be regarded as a message, whereas the 16-byte postage-ID appended by the 16-byte integrity authentication key ($\text{postage-ID} \,\|\, iak$) can be regarded as a secret authentication key. The hash value is calculated by applying SHA-1 to the indicia content and the secret authentication key in secret suffix mode: $\text{SHA1}(\text{indicia}_{1..80} \,\|\, \text{postage-ID} \,\|\, iak)$ (see Section 4.4.1.1 on page 100 and Equation 6.1 on page 157). The total length of the SHA-1 input is $80 + 16 + 16 = 112$ byte, which is extended to 128 bytes by using SHA-1 padding, split up into 2 SHA-1 blocks of 64 bytes each and processed according to SHA-1. Since the secret authentication key $\text{postage-ID} \,\|\, iak$ in the second block is neither known nor controlled by the attacker, a two-for-one-attack or a one-for-nothing attack is limited to find a collision in the first block, i.e., ($\text{indicia}_{1..64}$). If the same second block were appended to either of two colliding first blocks, then the resulting complete indicia contents will collide themselves under SHA-1 due to the Merkle-Damgard Iteration (Section 4.3.1 on page 97).

Consider a Frankit indicia that shall be used for a mailing deposited on a specified day. How many valid Frankit indicia contents exist for that day? By analyzing Table 20 on page 156 we find that 6 out of the 15 data fields fall into category (a) namely fields #1-2, 4, 8, 9 and 11. This subset of data can take the values of any of 250 thousand records of registered postage meters in Germany (if the market had entirely migrated to Frankit). The remaining data fields fall into category (b). Of those, the date of mailing (field #6) and the rate table version (field #3) are fixed by the specified date of deposit, and, usually, the amount of postage (field #5) is uniquely determined by the rate category, i.e., postal product code (field #7). Assuming that the 4 bytes of service data (field #15) contained in the first block may take any possible value, there are 16 bytes of category (b) data left that lead to a valid indicia contents. Factoring in both categories of data, there are at most $2.5\times10^{3}\times256^{16}\approx256^{18.24}$ valid indicia contents. Since Frankit uses a truncated MAC with output length 4 bytes, each indicia contents is expected to have an average of $256^{14.24}$ colliding indicia contents. This is still far less than the number of 256^{44} collisions required by the attack of Wang et al, to be successful.

Secondly, we consider the use of SHA-1 in pseudo-random bit generators (Section 4.5.2 on page 109) and in session key agreement protocols (Section 4.5.3 on page 112). In both of these applications, the SHA-1 function is iterated over several rounds. In the first round, SHA-1 is applied to a secret initial value that is not known to the attacker, and from each round the SHA-1 output is fed forward as an input to SHA-1 of the next round. This application of SHA-1 is different from the message preparation of digital signatures and message authentication codes because the honest parties are in control of running the pseudo-bit generator or the session key derivation. The attacker has no way of re-starting the process from scratch while using his own input data.

In the case of pseudo-random bit generation, the attacker observes a fraction of the SHA-1 output of each round and tries to forecast the SHA-1 output of the next round. Finding a pair of just any two colliding inputs would not help him in solving this task for any given secret initial value. In the case of session key agreement, the attacker observes the cipher text or message authentication codes that result from the honest parties using the secret session key(s) for a symmetric encryption mechanism or a message authentication code and tries to figure out that session key. Again, finding a pair of any two colliding input to SHA-1 would not help the attacker to figure out any given instance of a secret session key.

Although SHA-1 is not an immediate weakness in postage indicia, ongoing cryptanalysis on hash functions strongly suggests that existing systems should use stronger hash functions and use proven constructions for message authentication codes, such as HMAC (Section 4.4.1.3 on page 101).

8.3.5.3 Cryptanalysis of Message Authentication Codes

For most applications, a key length of 64 to 80-bit and an output length of 64-bit are sufficient. For a proper message authentication code, pre-image resistance, second pre-image resistance and collision resistance follow from lack of knowledge of the secret key, and hence depend primarily on the secret key length. Given certain controls, such as frequent updates of the secret key, facilitate to use outputs as short as 32 bits, which can be achieved by truncating the regular output of the message authentication code. This option is of particular interest for use in postal indicia whose available space is limited. It is used by Frankit (Section 6.5.1 on page 152) and Stampit (Section 7.4.1 on page 175).

Output lengths b much shorter than 32 bits are not recommended because the probability of guessing a MAC output correctly without any knowledge about the message or the authentication key is 2^{-b}. If $b < 32$, this probability is at least 2.3×10^{-10}.

8.4 SECURITY SAFEGUARDS

We have seen a number of different e-postage systems in Chapter 6 on page 127 and Chapter 7 on page 167. They use similar kinds of safeguards, which we will explore for each security domain. In general, there are monitoring and preventive safeguards, aiming at the detection and the preclusion of attacks and fraud, respectively. As we all know, monitoring safeguards can have a preventive effect as well, because perpetrators who know that certain kinds of attack will be revealed by monitoring and observing measures, are likely to be deterred and try to accomplish their fraudulent goals via less exposed avenues of attack. Which kind of safeguard is appropriate for a given e-postage system needs to be concluded from a detailed risk analysis, which is beyond the scope of this work.

8.4.1 Revenue Reconciliation

A postal operator's primary security requirement is that the amount of payments received in exchange for electronic postage, equals the sum of all postage fees due for the mail pieces that are inducted and delivered in the same period of time. Because of the natural delay between the time of payment and the time of delivery of each mail piece, it is important to acquire the data about payments and that about induction and delivery as quickly and comprehensively as possible. Otherwise, the data about payments and the data about induction and delivery are too diffused over time and can hardly be matched up with each other in any reasonable time intervals. It is thus an important safeguard to provide electronic postage to e-postage devices through a centralized electronic communication channel rather than through decentralized manual procedures, which was the traditional resetting method for mechanical postage meters.

- *Payment/volume reconciliation*: In existing e-postage systems, each indicia carries a serial number of the e-postage device it originated from. Likewise, each payment for e-postage is associated to a unique e-postage device. Therefore, the sum of all payments and the sum of all postage fees can be reconciled with each other down to the e-postage device level in each time interval.
- *Postal register reconciliation*: If the indicia contain information about the postal register values at the time of indicia creation, and e-postage devices report their postal register values at the time of postage value download or indicia request, then the postal operator can reconcile both data about postal register values at the e-postage device level.
- *Mailing behavior monitoring*: The postal operator can create mailing profiles of certain mailers based on the volume and distribution of their mailing behavior. If a mailer's actual mailing behavior deviates significantly from the mailer's mailing profile, the mailer's account can be investigated.
- *Volume analysis*: Postal operators keep records of the mail volume of bulk mailers and reconcile the payments with the volume of processed mail of these mailers

8.4.2 Backoffice Domains

The bank backoffice, post backoffice, e-postage provider systems and mail processing center systems are data centers which must be protected against system infiltration (Section 8.3.2 on page 188), namely, fraud and theft, malicious hackers, employee sabotage, loss of physical and infrastructure support, industrial espionage, malicious code, and the disclosure of personal information. Comprehensive lists of appropriate safeguards for security-critical data centers can be found for example in the encyclopedic work of Pfleeger [65].

The electronic communication between the above mentioned data centers in the backoffice domains is batch oriented, typically one transfer of a couple of files in XML or EDI format at the end of each business day, for example, using the file transfer protocol (ftp).

The files can be secured against eavesdropping and illegitimate modification in transit by employing secure ftp (ftps), application layer encryption and digital signatures using for example the open-PGP compliant Gnu Privacy Guard (GPG) [72] or by out-of-band methods such as printed or fax reports containing relevant checksums.

If cryptographic mechanisms are used, long-term encryption keys and signing keys are generated and exchanged between the data centers and should be updated on a regular basis before they expire. An emergency update option should be in place by which cryptographic keys can be replaced by fresh key material immediately if they have been compromised or have been suspected to be compromised.

8.4.3 Refill Domain and Online E-Postage Domain

- *Disabling lost or stolen e-postage devices*: Offline e-postage devices that are lost or stolen or online e-postage devices whose access codes have been lost, compromised or stolen shall be reported immediately to the respective e-postage provider such that they can set blocking flags for these e-postage device. The next time, a lost or stolen e-postage device connects to its e-postage provider, it will be disabled based on the blocking flag. Disabled e-postage devices cannot create indicia any more.

  E-postage providers are held to forward reports of lost and stolen e-postage devices to the respective postal operator, which maintains up-to-date black lists of such devices and may reject mail pieces that carry indicia originating from a lost or stolen e-postage device.

- *Putting e-postage devices on hold*: Offline e-postage devices using e-postage that has not been paid for are flagged by their e-postage providers to be put on hold. This case occurs if the mailer's check bounces or a direct debit to the mailer's account is rejected by the mailer's bank. The next time such an e-postage device connects to the e-postage provider, it will not be allowed to download postage unless the mailer has paid any outstanding amounts.

8.4.3.1 E-Postage Device Level

An important safeguard against fraudulent manipulation of offline e-postage devices is the use of embedded tamper protected postal security devices. Their purpose is to secure the communication channel to the e-postage provider, the correct management of postal registers, including the link between printing and accounting, the management of watchdog timers, and the proper creation of a unique cryptographic checksum for each indicia.

Safeguards against attackers who try to spy out the security-critical cryptographic keys maintained by a postal security device. Such safeguards include shields to absorb compromising emanations of spurious electromagnetic radiation (tempest), sensors detecting various environmental parameters such as temperature, humidity, pressure, vibration, shock, voltage, current, frequency, and tamper detection meshes that trigger a signal if they are damaged by physical drilling, chemical solvents, sandblasting, etc. The sensors trigger a shutdown circuit that stops the postal security device from operating as soon as the environmental conditions fall outside of the specified range of tolerance. If the tamper detection mesh is triggered, it actively zeroizes the critical cryptographic parameters or otherwise guarantees that they will never become readable again. Other safeguards are available against side channel attacks such as timing and power analysis and fault induction. Effective safeguards against timing and power analysis are blinding and masking techniques. A good overview of results of this active research area in applied cryptography is given by the Side Channel Cryptanalysis Lounge [65] of ECRYPT.

An important safeguard against the use of copied indicia originating from open e-postage devices is the inclusion of origin and/or destination location information within each indicia, e.g., the origin/destination postal code.

Another safeguard against outdated indicia is the inclusion of a controlled mailing date within each indicia, which must equal the date of induction. The mailing date is required to be set no sooner than the creation date of the indicia, and no later than a specified offset from the creation date, e.g., 30 days.

8.4.3.2 Protection of Data Exchange

The communication channel between an e-postage device and its e-postage provider can be secured by cryptographic communication protocols. An efficient safeguard against eavesdropping and illegitimate modification of messages (including insertion and deletion) is to employ a key establishment mechanism (see Section 4.5.3 on page 112), and to use the resulting session keys for a message authentication code (Section 4.4.1 on page 100), and—if required—a symmetric encryption mechanism (Section 4.2.1 on page 93).

8.4.4 Mail Processing Domain

As a safeguard against illegitimate modification and counterfeiting of indicia, the existing e-postage systems require an individual digital signature or a (truncated) message authentication code for each indicia.

8.4.4.1 Induction Control

If a mailer inducts a large amount of mail over a post office counter, he is to fill in a *statement of induction* describing the number and type of mail pieces handed over. The post office staff can validate the accuracy of the statement of induction and thus establish an induction rating for certain mailers. Future mail inductions will be validated based on the mailer's induction ratings. The higher a mailer's induction rating is, the smaller sample of mail might be chosen to validate the accuracy of an actual mail induction.

8.4.4.2 Mail Piece Validation

At a mail processing center, each indicia is picked up and can be validated with respect to a number of criteria. How large a fraction of all processed indicia are validated and how many checks are applied to them varies from one postal operator to another and may also depend on the mail processing center, the calender season, the day of the week, the time of the day and other conditions. The following checks can be applied:

- *Indicia barcode symbol readability* determines if the readability rate of indicia barcodes passes a high quality threshold of at least 97% to counter deliberate obliteration of indicia.
- *Internal data consistency* checks determine if the data fields of a decoded indicia match up with each other.
- *External data consistency* checks determine if the data fields of a decoded indicia match up with external data about the originating e-postage device and its mailer that are available to the mail processing center. These checks include a validation of the date of mailing, the device registration status, the method and location of induction, the authorization of the mailer, the verification of the cryptographic checksum, and the uniqueness of the indicium.
- *Lost and stolen e-postage device management*: E-postage devices that are lost or stolen are reported to the respective e-postage provider and from there to the postal operator, which maintains up-to-date black lists of these devices. Mail pieces carrying indicia that originate from blacklisted e-postage devices may be rejected or investigated otherwise.
- *Incidence analysis*: Investigation of significant signs of fraud detected during the mail processing stages at a mail processing center.

Chapter 9

Privacy in E-Postage Systems

9.1 ANONYMOUS MAIL

Privacy of the post, or secrecy of correspondence, as it is sometimes called is a human right respected and guaranteed in many democratic countries. Sending mail anonymously, however, is not. It is easy to send personal letters anonymously simply by using stamps and omitting the sender's name and address. The postal operators do not recommend sending mail anonymously for various reasons. An obvious one is that they find it difficult to return such mail to the sender if it is not deliverable.

Another reason is that anonymous mail imposes significant risks on the postal operator, the recipient and other third parties. In fact, anonymous mail has been used as a weapon against the intended recipients, for example, by sending explosives (mail bombs), chemical poisons or biological germs (anthrax spores). These substances may also inflict serious injury or even death upon postal workers or bystanders or damage upon property. Another risk of anonymous mail is that senders can construct false images of individuals, organizations or political parties or spread other pieces misinformation while keeping their identities secret.

On the other hand there is a good thing in anonymous mail as well. It can be used to cast votes in an election. It is a way of revealing a true story behind a plot to the law enforcement agencies or the press without risking one's life. It is a way to give witness testimony to a lawyer without putting oneself in danger. It is sometimes the only way of communicating a legitimate standpoint that happens to oppose the current political or economic majority opinion.

In most of today's mail processing systems, anonymous mail is a service that is readily available through the payment instrument of stamps. Although sending mail anonymously is not promoted, it is also not discouraged, because stamps cost the same whether it is used for anonymous or for identified mail. Preventing the processing of anonymous mail is hardly economic, because reading the sender's address, verifying it and rejecting mail pieces whose sender's address cannot be verified requires significant investments into the postal operators mail processing centers if the performance shall not be degraded.

In today's electronic postage systems, sending mail anonymously is not an available service, because all postal operators requires each online or offline e-postage device to be registered to them before it is enabled to print postage. Interestingly, this security requirement of the postal operators easily aligns with the advertisement interests of most mailers. Business mailers want to advertise their products and services and make their corporate identity known to their correspondents and to the public in every way possible and efficient, which includes to use the envelopes of their mail. Even many private mailers demand for individual e-postage, showing their personal preferences or achievements. This can be seen from the popularity of customized stamps, which show photographs of the mailers, their children, pets, quilts, or any other pursuit one can think of.

So what are the data items found on anonymous mail? We distinguish three types of anonymous mail according to the overview presented in Table 23 on page 202.

Table 23. Types of Anonymous Mail

Mail	*Anonymous to*	
	postal operator	*recipient*
r-anonymous	no	yes
p-anonymous	yes	no
fully anonymous	yes	yes

9.1.1 R-Anonymous Mail

R-anonymous mail is anonymous to the recipient, but not to the postal operator. This can be achieved by using a pseudonym for the mailer's identity whose owner is known to the postal operator only. If the mailer uses one-time (transaction) pseudonyms, none of his mailings can be linked by the respective recipients, i.e., be recognized as originating from the same mailer.

The recipient addresses can be given in the clear because the postal operator needs to know them anyway and the recipients already know their addresses before the mail is sent.

9.1.2 P-Anonymous Mail

P-anonymous mail is anonymous to the postal operator, but not to the recipient. This can be achieved by using a pseudonym for the mailer's identity whose owner is known to the recipient only. If the mailer uses one-time (transaction) pseudonyms, none of his mailings can be linked by the postal operator. Alternatively, mailers can omit to give their identity altogether, but include it for the recipient within the enveloped mail.

Again, the recipient address can be given in the clear with the same reasoning as above for r-anonymous mail.

In addition, the postmark must be anonymous. They must not reveal any information about the mailer's identity. This rules out all of the e-postage systems covered in previous chapters, because all of them include a unique serial number of the e-postage device by which they were created and printed. A perfect solution for an anonymous postmark is a conventional stamp.

9.1.3 Fully-Anonymous Mail

Fully anonymous mail is anonymous both to the postal operator and to the recipient. This can be achieved by mailers printing no senders identity and using anonymous postmarks, such as conventional stamps.

9.2 ANONYMOUS POSTMARKS

In the previous section we have not exactly defined what we mean by anonymity. In this section we will distinguish two degrees of anonymity. The weaker degree is called pseudonymity, the stronger is called unlinkability.

9.2.1 Pseudonymity and Unlinkability

We say that the postmarks of an e-postage system are pseudonymous, if each postmark is equally likely to have originated from any given e-postage device. Thus anonymous postmarks cannot carry a registered ID of their originating e-postage device, nor an ID or postal address of their mailer, nor an origin ZIP code.

The postmarks of an e-postage system are called *unlinkable*, if any two postmarks are equally likely to have originated from the same e-postage device as any other two postmarks. The privacy property of unlinkability is strictly stronger than that of unlinkability. We can see by contradiction, that if the postmarks of an e-postage system are unlinkable, then they are also pseudonymous:

Suppose the postmarks of an e-postage system are not pseudonymous, that means there exist an e-postage device *d* and three postmarks m_1, m_2 and m_3 that have originated from *d* with respective probabilities p_1, p_2, and p_3 such that $p_1 \neq p_2$. Then, the probability that m_1 and m_3 have both originated from *d* is $p_1 p_3$, while the probability that m_2 and m_3 have both originated from *d* is $p_2 p_3$. Thus, the pairs (p_1, p_2) and (p_1, p_3) of postmarks have originated from *d* with different probabilities $p_1p_3 \neq p_2p_3$, which implies by definition that the postmarks are not unlinkable.

Second, we can see by example, that there are e-postage systems with pseudonymous postmarks, which are NOT unlinkable: Suppose that each e-postage device has a unique pseudonym, but the mapping of pseudonyms to e-postage devices is NOT known to the postal operator. If each postmark includes the pseudonym of its originating e-postage device, then these postmarks are pseudonymous (to the postal operator), but not unlinkable, because any two postmarks showing the same pseudonym can be easily recognized as originating from the same e-postage device.

9.2.2 Anonymous Electronic Postmarks

The problem of making anonymous electronic postmarks, is to enforce their unforgeability. If the originator of a postmark remains anonymous, what would prevent him from using each electronic postmark two or more times?

An efficient solution to this problem was proposed by Brands [74] who presented unlinkable electronic coins, which could be issued and spent over the Internet. If the customer's wallet contains a tamper resistant security module, the payment system can prevent that coins are spent twice. Without employing tamper resistant security modules, it can detect any double spending after the fact and recover the identity of the double spender from the two transcripts that the merchants received who were paid with the two copies of the same electronic coin.

This approach can be applied to implement anonymous postmarks, which can be obtained online from an e-postage provider and printed offline onto envelopes [11]. If the offline e-postage devices are equipped with tamper resistant postal security devices, the system can prevent multiple uses of postage coins. Without employing postal security devices, it can accurately detect multiple use and identify the respective perpetrators.

The basic idea is as follows. During a postage value download, a mailer receives a number of requested electronic postage coins, which may have different denominations and are stored by his offline e-postage device. At the time of franking, the e-postage device chooses an electronic postage coin of sufficient denomination and transforms it into an electronic postmark. The transformation depends upon the date and time of mailing and the recipient ZIP code, which are also included in plaintext in the resulting postmark. If the an electronic postage coin is transformed twice using the same date and time of mailing and recipient ZIP code, the result is two exact copies of an indicium. Using copies of such individualized postmarks is as unattractive as for all the postmarks discussed in Chapter 7 on page 167.

The mail processing centers look for exact copies of indicia and reject any second or further occurrence of such copies. Furthermore, the mail processing centers look for indicia that contain the same data elements as previous indicia. These matches are evidence for double uses of the same electronic postage coin. If two indicia with matching data elements are input to a certain recovery procedure, it will reveal the identity of the e-postage device and thus of the double user.

An e-postage system based on this concept can produce unlinkable electronic indicia, which can be used to achieve p-anonymous as well as fully anonymous mail.

9.3 AVAILABILITY

Efficient fully anonymous and secure electronic indicia are technically feasible, but the service of anonymous mail is not supported in any of the existing industrial e-postage systems. Sending mail anonymously is probably not demanded for mass mailings, but typically for selected individual mail pieces only. As such, conventional stamps are the payment instrument of choice for p-anonymous and fully anonymous mail. However, if a time comes where conventional stamps, or other stamps bearing no indication about the mailer, are no longer available, then anonymous indicia might be worthwhile to consider in certain situations and applications.

Chapter 10

Evaluation, Assurance and Postal Approval

10.1 TERMINOLOGY

Before a computerized system is applied to the real world, for example by representing real money by bits and bytes, the stakeholders demand to convince themselves of the security and reliability of the system. This is called *system security assurance*. It is achieved by good and bad case *testing* and *evaluating* the actual system at hand over an extended period of time by a team of experts knowledgeable of the system. A full scale business of system security assurance consulting has been developed since the early 1990's, when the orange book was retired and overcome by a more flexible assurance methodology called the Common Criteria [41]. For e-postage systems, the postal operators are the primary stakeholders, so they have established a mandatory *postal approval process* that any e-postage provider's system must pass before his system is allowed to be operated in the respective postal market. Major updates and bug fixes of an e-postage system are usually required to be approved by the respective postal operator, in particular if they might affect the financial integrity of the whole or a part of the e-postage system.

Each e-postage system comprises a data center at the e-postage provider, which manages potentially large amounts of e-postage. These data centers not only need to run correct software, they must also be operated correctly and be protected against system infiltration by disgruntled internal employees and external perpetrators (Section 8.3.2 on page 188). Some postal operators require a *site security audit* to be conducted on a regular basis in order to validate the sufficiency and effectiveness of the safeguards (Section 8.4.2 on page 196) installed by the e-postage provider.

10.2 THE POSTAL APPROVAL PROCESS

E-postage devices are advanced computerized systems, which download, store and apply prepaid electronic postage. Operating thousands of such e-postage devices in a postal market poses a security risk on the revenue of the respective postal operator(s). In order to manage this risk, postal operators have been given the authority to enforce an appropriate level of security for each new model of e-postage device through some kind of approval process.

Manufacturers of e-postage devices need to get new models approved by the respective postal operator, and customers who want to operate such e-postage devices need to get registered by the postal operator. This way, postal operators enforce an appropriate level of security in all e-postage devices operated in their market, keep track of their whereabouts and who is responsible for operating them.

The postal approval process for an e-postage system supporting online or offline devices includes the following areas of compliance testing:

1. *Regular use testing* of an e-postage device includes to try out its basic functions and to produce a number of different postmarks. This test is done by the postal operator when it receives a new model of e-postage device for approval. It is more a kind of spot check testing rather than a comprehensive walk through all functionality and may take into consideration past experience that the postal operator had with other e-postage devices.
2. *Security compliance testing* of the e-postage device addresses its printing mechanism, access controls, postage calculation and accounting mechanisms and its interface to the e-postage provider. The testing includes a thorough review of the hardware (if applicable) and software, and accompanying documentation such as its security policy, concept of operation, hardware layout, software interface descriptions and operating manuals.
3. *Integration testing* of the e-postage provider system includes its interface to the postal operator's backoffice and/or to the respective banking backoffice. The test includes registration and revocation of the proposed e-postage device, initialization, authorization, postage value download, producing postmarks of various rate categories and types of indicia, updating the postage rate table, relocating the user's office, refund of remaining postage, withdrawing the e-postage device from service, cash management transactions and daily reporting of financial transactions. The test determines if all these operations comply to the life cycle of the e-postage device and result in correct interactions with the bank's and the postal operator's backoffices.
4. *Site security audit* of the e-postage provider system sites includes the physical and logical access controls of key storage, customer and account databases as well as physical and organizational site security. The e-postage provider system site may be distributed over several data centers including supplementary data centers such as a trust center for the public key infrastructure. It is advisable to first review how

security relevant each data center site is and then set up an audit plan for each data center accordingly.

5. *Readability testing* evaluates the readability of printed postmarks under near production conditions of a mail processing center. A quantity of 200 up to 1000 envelopes of specified types is franked and inducted into the postmark reading and mail sorting machines of the postal operator in order to determine how many pieces of mail are readable at production speed and whether the read postmarks can be decoded and verified successfully.

For traditional offline e-postage devices such as mechanical and electromechanical postage meters, the security conformance testing was restricted to the postage meter itself and its mechanical locks and seals. Postal operators performed the approval of new products by their own personnel. When cryptographically secured indicia came up, the testing of e-postage systems became more complex and demanded too much from postal operators, who thus looked for alternative, systematic and standardized methodologies of security testing and approval. In the early 1990s, the banking industry had developed approval methodologies for ATMs and financial backoffices that were based on hardware security modules. In 1994, the US National Institute of Standards and Technology (NIST) released the first version of the FIPS 140 standard [86,87], titled Security Requirements for Cryptographic Modules, which specified four security levels of hardware security modules complete with a comprehensive yet practical testing methodology. NIST established the national voluntary laboratory accreditation program (NVLAP) in order to accredit, train and audit cryptographic module testing laboratories. Accredited testing laboratories are authorized to perform security compliance testing according to FIPS 140 and its derived test requirements (DTR) [88]. When the US Postal Services started to develop their Information Based Indicia Program in 1995, it was natural to leverage on this established standard and related testing industry, which had gained considerable acceptance throughout the banking industry. Independent testing is a growing business. By the end of 2005, the NVLAP had accredited 12 test laboratories, nine of them in the US and Canada, the other three in Europe.

To be specific, we describe the approval process that the US Postal Services has established for IBI compliant e-postage devices [105]. (Other Postal operators reveal their approval requirements only to applicants.)

1. The applicant must choose an NVLAP accredited FIPS testing laboratory.
2. The applicant must provide a letter of intent to the US Postal Services identifying the applicant, its business qualification, its staff involved

in managing, designing, developing, testing, and manufacturing the proposed product, its suppliers involved in developing components that may be critical to postal revenue, and the FIPS testing laboratory chosen.

3. The applicant must sign a non disclosure agreement with any third party that the US Postal Services assigns to support the product security review. The non disclosure agreement may be extended to third party suppliers identified in the letter of intent.
4. The applicant must submit a complete set of system documentation including the security policy, concept of operation, hardware layout, software interface descriptions, cryptographic key management plan, operating manuals, financial system design, e-postage provider infrastructure plan, configuration management, etc. as itemized in [105].
5. The applicant must submit a complete production grade product with postal security device to the chosen FIPS testing laboratory and, upon request, a second sample to the US Postal Services.

   The FIPS testing laboratory performs the security compliance testing as outlined in Section 10.2 on page 207 compliance test area no. 2. In particular, the postal security device is tested to comply to the postal security requirements of IBIP and to the cryptographic security requirements of FIPS 140. Upon successful completion of all required testing, the FIPS testing laboratory produces a letter of recommendation for FIPS 140 certification to NIST. The FIPS testing laboratory must provide a copy of this letter and a copy of the resulting FIPS 140 certificate (if any) to the US Postal Services.

   The US Postal Service may use the product sample to conduct some regular use testing and readability testing according to Section 10.2 on page 207 compliance test areas no. 1 and 5.
6. The applicant must demonstrate IBI compliance of the entire e-postage system including the proposed product by performing an integration test as outlined in Section 10.2 on page 207 compliance test area no. 3.
7. The applicant must perform a limited distribution field test in order to demonstrate the entire system's utility, security, audit and control, functionality, and compatibility with other systems, including mail entry, acceptance, and processing when in use. Mailers engaged in the field testing may need to be approved by the US Postal Services and may be required to sign a non-disclosure agreement before they are allowed to report about system security issues, audit and control

issues, deficiencies, or failures to the e-postage provider and to the US Postal Service.

8. The USPS postal technology management will grant an approval letter if the above tests have been completed and reported successfully by the applicant. Approval may be subject to certain conditions based on the findings during the various testing stages.
9. The applicant is responsible for obtaining all intellectual property rights that may be required to market the proposed product and to allow the US Postal Service to process mail bearing the indicia produced by these products.

The US Postal Services was the first postal operator to delineate an approval process for offline e-postage devices. As other postal operators like Deutsche Post and Canada Post followed suit they did not publish their approval procedures, but they too required an NVLAP accredited FIPS testing laboratory, and it became common practice to assign the testing areas between the FIPS test laboratory and the postal operator as outlined in Table 24 on page 211.

Table 24. Assignments of Testing Tasks

	Test Area	*Postal Operator*	*Security Test Lab*
1	Regular use testing	perform	—
2	Security compliance testing	—	perform
3	Integration testing	perform / validate	perform
4	Site security audit	supervise / validate	perform
5	Readability testing	perform	—

For the integration testing and the site security audit, no common practice has been established yet, thus the multiple entries in the above table. The e-postage provider integration testing is all the more complex the more information is conveyed through the interface between the e-postage provider and the postal operator backoffice, for example, class of mail information and cryptographic keys. At a minimum, the integration testing should verify that, at all times, the postal backoffice holds valid indicia verifying keys that are necessary to verify the indicia of all e-postage devices. Some postal operators provide detailed integration test plans themselves. Other postal operators request the applicants to have an integrations test plan setup by an accredited test laboratory. Some postal operators require to do the integration testing in co-operation with the e-postage provider. Other postal operators require the applicant to do the testing in co-operation with an accredited test laboratory.

Site security audits should, from an IT security standpoint, be conducted under the supervision of a certified information system security professional (CISSP), who is familiar with national and international security audit methodologies such as the German baseline protection manual [30], US NIST handbook [97] the ISO Information Security Standard 17799 [40] and others. There is growing consensus among postal operators to require independent and professional audit and advisory services to perform the site security audits according to established methodologies as mentioned above. Some require a positive audit report by a test laboratory. some retain a supervisory role in the test laboratories audit process. The most comprehensive and in-depth of approaches toward site security audits is pursued by the Netherlands Post TPG under their NetSet program [75].

At the end of the day, the postal operator receives all test reports from the engaged test laboratory, the professional auditor, and from its own business units involved in the testing. If all these test reports are sufficiently successful, the postal operator will grant approval for distribution and operation of the new model of e-postage device.

10.2.1 The Security Evaluation Process

The security testing and evaluation process promoted by FIPS 140 is that a government agency such as NIST in the US accredits test laboratories and that vendors engage a test laboratory and pay the laboratory for security testing and evaluation of their product. The general problem with this kind of approach is that there is a wicked economic incentive for vendors to watch out for test laboratories that charge less or test less rigidly than other test laboratories. This economic incentive of the vendors works against the security interest of the postal operators because the former have to pay for the security testing, while the latter pay for the consequences of lack of testing. In order to alleviate this dilemma, all test laboratories are audited by the accreditation body, e.g., by NIST, on a regular basis and need to have their test reports validated by NIST before releasing them to their customers. Moreover, a strict division of security design and security testing is propagated and enforced by NVLAP. All test laboratories are held to refrain from designing or optimizing security measures in the products of their customers. This division of duties is maintained to prevent a tying up of security vendors, consultants and test laboratories, which would be the end of independent testing. If the accreditation body finds test laboratories not to follow these rules or to produce doubtful test reports, it may seize the accreditation.

Next, we will look at some of the testing areas in more detail.

10.3 SECURITY COMPLIANCE TESTING

Under the auspices of the UPU, the Postal Meter Group (PMG), a subgroup of the Postal Security Action Group (PSAG), developed a framework for testing the security of offline e-postage devices. A part of their work has been approved by the UPU in 2001 and was published as the International Postage Meter Approval Requirements (IPMAR) Standard S30-4 [113]. The main goal of the IPMAR standard is to enforce the predominant common interest of all postal operators, namely to protect their legitimate revenues. IPMAR has gained wide acceptance among postal operators because it is based on the well established security testing methodology FIPS-140.

10.3.1 FIPS 140

The FIPS 140 standard is a framework in which the level of security of cryptographic modules (hardware and/or software) can be defined. In the sense of FIPS 140, a cryptographic module is a means to protect security-critical data by using cryptographic mechanisms. The cryptographic module is encapsulated within a *cryptographic boundary*, which protects the internal mechanisms and cryptographic keys of the module against manipulation. FIPS 140 addresses only the cryptographic means and how to manage them securely, it is not about the application data to be protected and not about how the cryptographic means are applied to the application data. The FIPS 140 standard defines four levels of security, with level 4 being the highest, in eleven security-critical areas of cryptographic modules, namely:

1. Cryptographic Module Specification
2. Cryptographic Module Ports, Interfaces
3. Roles, Services, and Authentication
4. Finite State Machine Model
5. Physical Security
6. Operational Environment
7. Cryptographic Key Management
8. Electromagnetic Interference and Compliance (EMI / EMC)
9. Self-Tests
10. Design Assurance
11. Mitigation of other attacks such as side-channel attacks.

To illustrate the security levels, we consider the area of physical security. The physical security requirements of FIPS 140-2 [87] do not apply to cryptographic modules that are implemented completely in software such that their physical security rests solely on the host platform. Any other cryptographic module is classified as either single ship, multiple-chip embedded or multiple chip standalone cryptographic modules as defined in Table 8 on page 55. The physical security requirements for each class of embodiments are summarized in Table 25 on page 214. The security requirements of level *n* are defined by the table entries of the general requirements column and the respective embodiments column including the cells from security level 1 up to level *n*.

Table 25. Physical Security Requirements according to FIPS 140-2

Level	*General Requirements*	*Single Chip*	*Multi-Chip Embedded*	*Multi-Chip Standalone*
1	Production-grade components (with standard passivation).	No additional requirements.	If applicable, production-grade enclosure or removable cover.	Production-grade enclosure.
2	Evidence of tampering (e.g., cover, enclosure, or seal).	Opaque tamper-evident coating on chip or enclosure.	Opaque tamper-evident encapsulating material or enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.	Opaque enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.
3	Automatic zeroization when accessing the maintenance access interface. Tamper response and zeroization circuitry. Protected vents.	Hard opaque tamper-evident coating on chip or strong removal-resistant and penetration resistant enclosure.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or applicable Multiple-Chip Standalone Security Level 3 requirements.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or strong enclosure with removal/penetration attempts causing serious damage.
4	Environmental Failure Protection (EFP) or Testing (EFT) for temperature and voltage.	Hard opaque removal-resistant coating on chip.	Tamper detection envelope with tamper response and zeroization circuitry.	Tamper detection/response envelope with tamper response and zeroization circuitry.

When FIPS 140 was under development, Weingart et al [120] of IBM proposed the 3 classes of attackers outlined in Section 8.2 on page 185. They further proposed six levels of physical security for computing systems, level 1-3 aiming at class 1 attackers, levels 4 and 5 aiming at class 2 attackers and level 6 aiming at class 3 attackers. The FIPS 140 standard finally adopted the proposed security levels 1 to 3 and the proposed level 6 as its level 4. This selection is oblivious to class 2 attackers and explains why there is a big gap between FIPS 140 security level 3 and level 4. The better commercially available cryptographic modules aim at something that is informally called 'level 3.5' in order to provide affordable security against class 2 attackers. Such a security 'level 3.5' is also desirable for postal security devices. Stronger attackers than class 3 are not considered by FIPS 140, which is geared towards commercially available systems, not military systems.

The FIPS 140 level of security of a cryptographic module is specified by selecting a security level between 1 and 4 for each security-critical area listed above. For example, a cryptographic module that is specified as FIPS 140 security level 3 for each security-critical area is called *level 3 overall*. The rules for testing each level in each of the above areas are laid down in the FIPS 140 Derived Test Requirements (DTR) [88]. These rules must be interpreted and applied by NIST accredited test laboratories only. If all tests are successful, the test laboratory sends a respective test report to the Cryptographic Module Validation Program (CMVP) [89] of NIST and asks for validation. If the manufacturer so wishes, he can order a FIPS 140 certificate signed off by CMVP, which automatically produces an entry in the list of published certified cryptographic modules in the CMVP.

Many cryptographic modules provide a cryptographic application programming interface, such that the application can provide arbitrary data to the cryptographic module in order to have certain cryptographic mechanisms applied to it. An example of such a cryptographic API is PKCS#11. In a sense, a cryptographic module provides its cryptographic services for free, because the application can apply them to arbitrary application data. For postal security devices, this approach is inappropriate, because it shall also enforce that whenever a valid indicia is produced, it shall be accounted for by way of the postal registers.

The FIPS 140-1 standard was established by the US National Institute of Standards and Technology (NIST) under the cryptographic module validation program (CMVP) in 1994 as a successor of the former Federal Standard 1027. NIST is required to review the FIPS standard every 5 years to take into account the experiences of accredited test laboratories and other security evaluation methodologies such as Common Criteria, comments from the general public and research results in the fields of computer security, applied cryptography. FIPS 140-2 took effect in May 2001, and FIPS 140-3 is scheduled to take effect in 2006.

10.3.2 International Postage Meter Approval Requirements

According to IPMAR, postal security devices are called *revenue sensitive modules (RSM)* and include at least the following components:

- a cryptographic module,
- a set of postal registers plus some additional application data,
- a control logic enforcing at least that every time when a valid indicia is produced by the cryptographic module, the values of the postal registers are updated accordingly, and
- a *revenue sensitive boundary* encapsulating the above three components.

IPMAR re-uses the framework of FIPS 140 in order to define a postal security device. It augments each of the eleven security-critical areas of FIPS 140 to include the additional components of a revenue sensitive module and specifies a FIPS 140-2 'level 3.5' by requiring that each security-critical area must be tested FIPS 140 level 3 or higher and that physical security must be strong enough such that

1. environmental failure protection or testing (EFP/EFT) is enabled with respect to temperature, voltage, exposure to chemicals and contaminants, electromagnetic interference and a number of other environmental conditions.
2. any unauthorized attempt of accessing, using, or modifying will be detected with high probability after the attempt by leaving visible signs (tamper evident) and during the attempt (tamper detection) so that appropriate actions can be taken by the revenue sensitive module to protect itself (tamper response). Generally speaking, physical security requires the use of strong enclosures with tamper detection and tamper response (counter measures) (see [113] §4.5).

Extending the concept of the FIPS 140 derived test requirements, the Postal Meter Group in co-operation with the manufacturers of e-postage devices has established a set of IPMAR derived test requirements, which refer the tester of FIPS 140 security requirements to the FIPS 140 derived test requirements and outline specific derived test requirements for the postal security requirements. The IPMAR derived test requirements will be included as a non-normative Annex in the IPMAR standard UPU S30-4 [113].

Some postal operators, like the US Postal Services, leave it to the security test laboratory to setup appropriate operational test plans directly from the IPMAR DTR, while others, like Deutsche Post, worked out specific (non-public) admission requirements and require the FIPS test laboratory to derive their operational test plans from the admission requirements.

This half-common-half-product specific approach toward security compliance testing has proved to be successful and efficient in practice. In the approval process, the test laboratory serves as a mutually trusted intermediary between the postal operator and the e-postage device manufacturer. Postal operators decide individually, which test laboratories they accept, but it is common practice that they are chosen from the list of NVLAP accredited FIPS 140 test laboratories. Effectively, manufacturers have a choice, which test laboratory they want to work with.

When a manufacturer requests approval for a new offline e-postage device, the postal operator will ask for an IPMAR or equivalent test report supporting the new product. As a first step, the manufacturer discloses his new product to an accredited test laboratory by providing several key documents such as a system operating manual, a concept of operation, a security policy, the complete source code listing, mechanical and electronic design documents, and one or more pre-production samples of the actual product. The test laboratory verifies the documentation and sets up an operational test plan, which resembles the approval requirements of IPMAR and describes in detail how the new product is going to be tested for security compliance. The manufacturer can assist in setting up the operational test plan and later supports the test lab in performing the testing. When the test laboratory has verified the documentation and finished the operational testing, it prepares a test report, which may be reviewed by the manufacturer, and sends the final test report to the postal operator.

10.3.3 Security Model of Digital Postage Meters

In traditional franking systems, which used non-cryptographic indicia, the postal operators focussed their security requirements on the postage meter housing, which encloses the franking engine, i.e., the operating hardware and software as well as the printing subsystem. Important issues were secure housings, locks and seals to avoid unauthorized and undetected access to the franking engine. The housing had to avoid any openings, such as for air fans, through which a dedicated attacker could poke some wire in order to manipulate the franking engine.

This approach of a security perimeter around a monolithic franking engine was partly obsoleted by IPMAR. Here, the revenue protection mainly rests upon the cryptographic mechanisms and how they are implemented and how the cryptographic keys are managed. IPMAR reduces the housing of a franking engine to just a first level of defense, which shall ensure *tamper evidence.*

The second level of defense is the postal security device, which is a hardware security device embedded within an offline e-postage device. A postal security device hosts the revenue sensitive application data such as the postal registers, related cryptographic keys, and the computing circuitry necessary to control the revenue sensitive application data and cryptographic keys securely and consistently. Compared to the franking engine, the postal security device is much smaller, has no moving parts and no fans, and can thus be protected much more effectively than a franking engine could.

The third level of defense is the cryptographic module, which is a component enclosed within the postal security device. The cryptographic module hosts and manages all the cryptographic keys necessary for the operation of the postal security device. This three layer model is shown in Figure 66 on page 218.

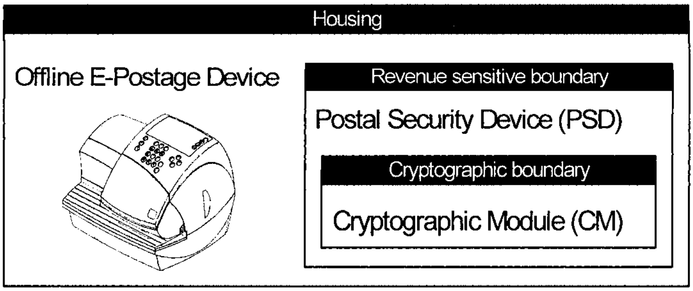

Housing
Offline E-Postage Device
Revenue sensitive boundary
Postal Security Device (PSD)
Cryptographic boundary
Cryptographic Module (CM)

*Figure 66.*Boundaries of an Offline E-Postage Device

10.3.3.1 Offline E-Postage Device

The offline e-postage device keeps all the data that is not revenue sensitive, such as the operating system and application software of the e-postage device, the device drivers for the letter transport and printing subsystems, the modem, keyboard, display, integrated scale and postal security device. Other data kept by the e-postage device is the usage data (optional) and system log files for after the fact investigations.

10.3.3.2 Postal Security Device

The postal security device keeps all postal revenue sensitive data required by its host, including the postal registers, the watchdog timers, the postal application software that enforces its life cycle, and a cryptographic module. The postal security device may further include separate communication protocol stacks in order to securely talk to the e-postage provider. The postal security device is protected against various environmental threats (Section 8.3.3.2 on page 189) by a perimeter called the *revenue sensitive boundary* according to IPMAR.

10.3.3.3 Cryptographic Module

The cryptographic module keeps all cryptographic keys, supplementary cryptographic parameters such as initialization vectors, seed values, and a cryptographic engine including certain cryptographic mechanisms. The cryptographic module is protected from certain environmental threats by a perimeter called its *cryptographic boundary* according to FIPS 140.

10.3.4 FIPS 140 vs. Common Criteria

We have seen that the international postage meter approval requirements have been expressed in the framework of FIPS 140, although they do not fit into the boundary of a cryptographic module. Are there other frameworks available that are capable to accommodate all the security requirements of a postal security device at one blow?

The classical security requirement frameworks of the US (orange book), Canada (TCPSEC) and Europe (ITSEC) have been harmonized into one framework, the ISO Common Criteria Standard [41], which is designed to be applicable to commercial and military systems alike. It is complete with a fully developed testing methodology and an accreditation program for test laboratories. If FIPS 140 were a cheetah, then the Common Criteria were an 800 pound Gorilla both in terms of expressiveness and formality. The Common Criteria framework supports to express the security requirements of a given class of products in a *protection profile* (PP). There is a library of predefined security requirements one can choose from, and more specialized security requirements can be defined and added. The security requirements of a particular product are delineated in a security target (ST), which inherits its security requirements from a protection profile and may refine or add to them. The real product to be tested is called the *target of evaluation* (ToE). The Common Criteria define 7 *evaluation assurance levels* (EAL), where levels 1 to 5 aim at commercial products. Test laboratories can be accredited by the accreditation authorities of each country participating in the *Common Criteria*

Recognition Arrangement, which also regulates the mutual recognition of Common Criteria certificates. Similar to the FIPS 140 Derived Test Requirements, Common Criteria establish the *Common Evaluation Methodology* (CEM), which defines the scope, depth and rigor of testing required for each evaluation assurance level.

Compared to FIPS 140, the Common Criteria are more expressive because one can combine any set of security requirements specified in a protection profile or security target with any evaluation assurance level. Although many such combinations make no sense, or are outright misleading, they are perfectly valid in the Common Criteria framework. For example, one can define a protection profile for a postal security device that misses one or more important security requirements such as to decrease the descending postal register each time the postal security device produces an integrity check code for a postmark. In spite of this security gap, one can demand and achieve a high level of evaluation assurance such as EAL 4. Finally, there may be products, suffering from the security defect described above, which carry a CC EAL 4 certificate. Bottom line: The evaluation assurance level of a CC certificate alone does not tell you anything about the level of security of the real product. It is just an indication of how likely the real product will satisfy the security requirements described by the respective security target or protection profile.

Using an example, the CC allow you to specify a flawed architecture (defect in protection profile) and once the house is built to use excessive rigor to prove that the real house indeed observes the specified flaws (high evaluation assurance). Likewise, the Common Criteria allow you to specify a rock solid architecture (perfect protection profile) and once the house is built to use only minimal effort to prove that it conforms to the specification (low evaluation assurance). In either case, the efforts put in the specification and in the evaluation do not match, which will waste resources. To be on the safe side, customers of security products should ask for a security review or certificate for the protection profile or security target, before drawing any conclusions from the evaluation assurance level of a CC certificate.

In FIPS 140, the security levels indicate both, security specifications of increasing strength AND testing requirements of increasing strength. In terms of the Common Criteria, the FIPS 140 standard defines 4 protection profiles for cryptographic modules of security levels 1 to 4, while the derived test requirements define one particular evaluation assurance level for each of the four cryptographic module protection profiles. This approach keeps a balance between the strength of security specification and the rigidness of the related security evaluation.

In 2001, the UK Royal Mail made an attempt, to use the Common Criteria in the postal approval process for postage meters. Supported by the UK based test laboratory Logica, they wrote a protection profile for postal security devices and had it certified [9] for EAL 4+. Although the approach was technically sound, the postage meter vendors refused to undergo the bureaucratic Common Testing Methodology for as simple a component as a postal security device. The lesson learned was that the FIPS 140 and IPMAR security testing process and effort is economically more appropriate for an embedded system component such as a postal security device.

10.4 INTEGRATION TESTING OF E-POSTAGE PROVIDER SYSTEM

The postal operators who demand to retrieve usage data from the e-postage providers through their postal operators backoffice systems usually require assurance that they receive accurate data and that the data they forward to the e-postage providers is used correctly. These postal operators set up integration test plans that describe a sequence of actions that a couple of postage meters shall perform over the course of 4 to 6 business days. For example, if a postal operator requires the usage data to be reported within certain accounting periods, then the test schedule would likely cross the border between one accounting period and the next. Other typical integration test cases include

- the reporting of daily transactions, lost and stolen postage meters and cryptographic keys.
- the relocation of an e-postage device when the origin postal code is changed.
- the automatic remote download of postal rate tables that have been made available by the e-postage providers and their timely activation inside an e-postage device.
- the proper functioning of recovery procedures from various error conditions that may result from input errors at the operator or administrator console of the e-postage providers systems, the compromise of certain cryptographic keys, network outages, database failures,

If an e-postage provider needs to maintain an interface to a bank backoffice, then the remittances of customer payments and the refunds of remaining postage back to customers are additional areas of integrations testing.

10.5 READABILITY TESTING

The postal operator will finally perform the reading tests of the postmarks produced by the new product in a close to production environment. These tests reveal if the fraction of unreadable postmarks is sufficiently small, and if the layout, content, color and fluorescence (if required) of the printed postmarks comply to the postal operator's specifications. These tests can take several iterations and can last an extended period of time because the optical systems, reading equipment and subsequent postmark analyzing and verification tools is highly specialized machinery. On the one hand the reading characteristics, critical parameters and tolerances are often not fully available from the postal operator using it, and on the other hand the approval applicant can usually not reproduce the machinery at his own site because it is expensive and requires a lot of manual maintenance to keep it in a condition that is close to the production environment inside a mail processing center of the postal operator.

To get the full picture, we also need to look at the printing process used by the e-postage device. The accuracy of the printing result depends on the following important parameters:

- speed and rippling characteristics of the letter transport,
- temperature of the print head,
- chemical composition of the ink used,
- quality of paper, and
- print growth, i.e., the dispersion of ink before it dries up.

Some of these parameters may be interdependent and all of them together determine the variance of the print accuracy from the specified mean that can be achieved by the given e-postage device. In order to get a high acceptance rate in bar code reading, the tolerances of the scanner equipment should not be too restrictive and the variance of the printing accuracy should not be too high. In general, the problem of matching the scanner's tolerances with the given variance of the printing accuracy is all the bigger the smaller elements or cubes the required barcode consists of.

As a simple example, consider a data matrix barcode of 1 square inch that has 40 by 40 cubes. Given a hypothetical printing resolution of 280 dots per inch, each cube is 7 dots wide. The print growth, i.e., the extent of ink dispersion before drying up, may vary between 3.4 and 10.2 mil, which equals 1 to 3 dots, for certain qualities of envelope paper. The print growth of average 2 dots can be compensated by printing each element only 5 dots wide. In effect, the width of elements then varies between 6 and 8 dots. In order to read the resulting bar codes reliably, the scanning machinery must have a tolerance of at least ±1 dot plus some safety margin. Relative to the width of 7 dots per element, this is a tolerance of at least ±14% without safety margin. Clearly, the relative tolerance required from the reading scanners increases if the width of elements decreases.

This simple example reveals the inevitable limitations set by physics, which must be respected by any printing mechanism. The tolerances of the reading equipment at the mail sorting centers are usually found to be carved in concrete at least as much as the laws of physics, which could lead up to a challenge getting a high speed printing mechanism to match up reliably with a high speed scanning machinery. At the bottom line, a manufacturer would be better off to expect the more testing time and effort the smaller tolerances are allowed by the scanning machinery, and the wider variance of printing accuracy the e-postage device observes.

If the test report of the test laboratory and the mail processing tests by the postal operators are successful, the postal operator grants approval by returning an approval letter to the applicant. If not all the tests were successful, the postal operator may grant approval under certain conditions, or refuse approval for this e-postage device.

10.6 POSTAL STANDARDIZATION BODIES

Most of the standardization work for the postal industry is done under the auspices of the Universal Postal Union (UPU). Some initiative is taken also by CEN TC 331.

10.6.1 CEN TC 331 Postal Services

In 1996, the CEN Technical Board (TB) approved the recommendation of CEN Programme Committee 8 to create the technical committee (TC) 331 "Postal Service" [18]. Its main objective is to increase the interoperability of postal networks and to improve the quality of service by aiming at the following topics:

1. measurement of quality of service
2. hybrid mail
3. tracing, identification, encoding and physical characteristics of mail
4. address data and forms.

Working group one on quality of service in co-operation with the Universal Postal Union worked out a comprehensive proposal on digital postmarks CEN EN 14615 [19]. The document has little binding character because the bulk of work is declared to be informative rather than normative.

10.6.2 Universal Postal Union (UPU)

Within the Universal Postal Union, there are two bodies related to e-postage devices. The Postal Security Action Group (PSAG) developed the IPMAR Standard S30-4 [113]. The Postage Meter Group (PMG) developed the Digital Postmark Standard S36-4 [114].

Chapter 11

Outlook

11.1 THE FUTURE OF ELECTRONIC POSTAGE

Under the continued forces of globalization, many companies face a broader and stronger competitive environment, which forces them to streamline their processes, cut costs and focus on their respective fields of excellence. The political strategy of many democratic countries is to shape this globalization by liberalizing the markets such that monopolies are reduced or avoided, in order to keep consumer prices in check.

Postal liberalization means to reduce the traditional postal monopolies of universal postal operators, who hold exclusive licenses to deliver letters up to a certain weight and to have these services exempt from sales tax. Such postal deregulation opens postal markets to competitive postal operators, who collect, presort, consolidate, transport and/or deliver letters.

Postal privatization is often the second step following postal liberalization. The goal is to transform universal service providers into efficient and profitable companies that are fit to survive in a liberalized postal market. A key strategy of postal operators in a competitive environment is to rationalize the business processes, including those to collect prepayments for postal products and services and of course for processing mail.

For postal operators, expansion is the next logical step in order to achieve a bigger return on their investment into rationalized and streamlined processes. If the forces of globalization continue, the smaller postal systems are likely to be acquired or merged to give way to a world of only a few large postal systems or *alliances* of postal systems, which span across multiple national borders. While universal postal operators recognize each other as competitors in the globalized markets, they are less likely to merge than to acquire upcoming successful private postal operators. This transformation process has been going on in other liberalized transport and logistic markets as well as in the parcel delivery and airline business.

The expanding postal markets and increasing use of electronic postage also create common interests of postal operators and electronic postage operators, for example in the area of postal rate tables. Traditionally, each postal operator has defined its specific portfolio of basic postal services and optional additional services. In each postal market, a multitude of dependencies between basic and optional services has applied and changed once or twice per year on short notice. The postal rate tables have been released on traditional media such as paper documents and faxes. An international standard for the specification and transmission of postal rate tables would enable the automation of related processes within postal operators, the e-postage providers and the data exchange between them. It would not come as a surprise to see such standardization activity by the Universal Postal Union within the next five years. As more postal operators turn to collect usage data of e-postage devices, an international standard for the specification and transmission of class of mail data could further streamline the postage related processes.

Electronic postage is a means to manage, distribute and reconcile pre-paid postage in a secure, efficient and decentralized way. The larger the mail volume of a postal operator is, the stronger becomes the demand for electronic postage because it helps to stay focused on the main business of collecting, sorting and distributing mail.

Without electronic postage, a postal operator is partly but constantly tied up in minting and distributing conventional forms of postage such as stamps, monitoring its use, deterring counterfeiters, and investigating in 'successful' schemes of forgery. Secure electronic postage has the potential to bring this kind of arms race to a halt at least for the foreseeable future.

Clearly, a postal operator can only switch to electronic postage step by step because it will not be fully acceptable to all mailers at once, but the larger a postal operator's business is, the larger fraction of his postage will be electronic.

References

[1] Anderson R: Security Engineering: A Guide to Building Dependable, Distributed Systems; John Wiley & Sons, 2001.
http://www.cl.cam.ac.uk/users/rja14/

[2] ANSI X9.17: Financial institution key management (wholesale), ASC X9 Secretariat American Bankers Association, 1985.

[3] ANSI X9.30–1: Public key cryptography for the Financial Services Industry – Part 1: The Digital Signature Algorithm (DSA); 1997.

[4] ANSI X9.30–2: Public key cryptography for the Financial Services Industry – Part 2: The Secure Hash Algorithm 1 (SHA–1); 1997.

[5] ANSI X9.42: Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography; 2001.

[6] ANSI X9.44: Public Key Cryptography Using Reversible Transport of Symmetric Algorithm Keys Using RSA.

[7] ANSI X9.62: Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA); 1998.

[8] ANSI X9.82 Part 3: Deterministic Random Bit Generators, ASC X9 Secretariat American Bankers Association.

[9] Appleford K, Hill S: Postage Meter Approval Protection Profile; Consignia PLC, Logica UK Ltd, 30-Apr-2001
http://www.commoncriteriaportal.org/public/files/ppfiles/IPMAR_pp.pdf

[10] Biham E, Chen R: Near collisions of SHA-0; Advances in Cryptology, Crypto 04, Springer-Verlag, Berlin 2004, pp290-305.

[11] Gerrit Bleumer: Secure PC-Franking for Everyone; Kurt Bauknecht, Sanjay Kumar Madria, Günther Pernul (Eds.): Electronic Commerce and Web Technologies (EC-Web 2000), LNCS 1875, Springer-Verlag, Berlin 2000, 94-109.

[12] Blum L, Blum M, Shub M: A simple unpredictable pseudorandom number generator; SIAM Journal on Computing, 15 (1986), 364- 383.

[13] Brown D, Johnson D: Formal Security Proofs for a Signature Scheme with Partial Message Recovery; Topics in Cryptology, RSA 2001, Springer Verlag, Berlin 2001,
http://grouper.ieee.org/groups/1363/Research/contributions/PVSigSec.pdf

[14] Callas J, Donnerhacke L, Finney H, Thayer R: Open PGP; Request for Comments 2440, Nov 1998.
http://www.ietf.org/rfc/rfc2440.txt

[15] Canada Post Corporation: Digital Meter Indicia Specification (DMIS); Version 1.2, May 2003.

[16] Canada Post Corporation: Postage Meter Product Information Handling Requirement; Version 2.0, May 15, 2003.

[17] Canada Post Corporation: Postage Server Product Information Handling Requirement; Version 2.02, Dec 2005.

[18] CEN TC 331 Postal Service
http://www.nen.nl/cen331/

[19] CEN EN 14615: Digital postage marks - Applications, Security & Design, 2005.

[20] CNN: Gates: Buy stamps to send e-mail; CNN Technology; March 5, 2004.
http://www.cnn.com/2004/TECH/internet/03/05/spam.charge.ap/index.html

[21] Coron JS: On the Security of Random Sources; in (Imai H and Zheng Y, Eds.), Public-Key Cryptography, LNCS 1560, Springer-Verlag, Berlin 1999, 29–42.

[22] Dallas Semiconductors: DS1954B Crypto iButton™, FIPS 140-1 Non-Proprietary, Cryptographic Module Security Policy, Level 3 Validation, August 16, 1999.

[23] Deutsche Post AG Zentrale: Voraussetzung zur Einführung von Systemen zur PC-Frankierung; Version 1.2, Nov 2001.

[24] Deutsche Post AG Headquarters: FRANKIT New Generation Digital Franking; Version 1.3, May 2003

[25] Diffie W., van Oorschot P.C., Wiener M.: Authentication and Authenticated Key Exchanges; Designs, Codes and Cryptography, vol 2, 1992, pp 107-125.

[26] European Commission, DG Internal Market: Main Developments in the European Postal Sector; WIK Consult, Final Report, July 2004.
http://europa.eu.int/comm/internal_market/post/doc/studies/2004-wik-final_en.pdf

[27] European Network of Excellence (ECRYPT): The Side Channel Cryptanalysis Lounge; Ruhr Universität Bochum.
http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html

[28] European Parliament: Directive on the restriction of the use of certain hazardous substances in electrical and electronic equipment; Directive 2002/95/EC of the European Parliament and of the Council of 27 January 2003.
http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_037/l_03720030213en00190023.pdf

[29] Fisher D.: Companies, People, Ideas, Delivery Problems; in Forbes Feb 28, 2005
http://www.forbes.com/global/2005/0228/046.html

[30] German Federal Office for Information Security (BSI): IT Baseline Protection Manual; 2003
http://www.bsi.de/english/gshb/manual/download/index.html

[31] Saul Hansell: Postage Is Due for Companies Sending E-Mail; New York Times, Feb 5, 2006.
http://www.nytimes.com/2006/02/05/technology/05AOL.html?_r=1&oref=slogin.

[32] Harmon P., Rosen M., Guttman M.: Developing E-Business Systems and Architecture; Morgan Kaufmann Publishers, San Francisco, 2001.

[33] IEEE Standard 1363: Specifications for Public-Key Cryptography; 2000.

[34] IEEE Standard 1363a: Specifications for Public-Key Cryptography—Amendment 1: Additional Techniques; 2004.

[35] International Business Machines (IBM): IBM 4758 Models 2 and 23 PCI Cryptographic Coprocessor; Specification Sheet (G221-9091-04) (04/2004)
http://www-1.ibm.com/servers/eserver/zseries/library/specsheets/pdf/g2219091.pdf

[36] International Standards Organization (ISO): Information Technology—Security Techniques, Modes of Operation for an n-bit block cipher; ISO/IEC 10116, 1997.

[37] International Standards Organization (ISO): "Information Technology AIDC Techniques Bar code symbology specification - PDF417"; ISO/IEC 15438.

[38] International Standards Organization (ISO): The Directory Authentication Framework; ISO/IEC/ITU 9594-8, 1988.

[39] International Standards Organization (ISO), "Information Technology AIDC Techniques Bar code symbology specification - Data Matrix"; ISO/IEC 16022.
http://www.idautomation.com/datamatrixfaq.html

[40] International Standards Organization (ISO): The Information Security Standard; ISO/IEC 17799, 2005
http://www.iso17799software.com/

[41] International Standards Organization (ISO): Common Criteria for Information Technology Security Evaluation, Version 2, May 1998, ISO/IEC JTC 1 15408
http://www.commoncriteriaportal.org/

[42] International Post Corporation: Global Electronic Postmark (EPM)
http://www.ptc.upu.int/ps/ebusi.shtml.

[43] Kahn D: The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet; Scribner 1996.

[44] Klima V, Rosa T: Attack on Private Signature Keys of the OpenPGP Format; Research Report 2001;
http://eprint.iacr.org/2002/076.pdf.

[45] Knuth D: The Art of Computer Programming — Seminumerical Algorithms, Vol 2, Addison-Wesley, Reading MA, 2nd edition 1973.

[46] Krawczyk H, Bellare M, Canetti R, *HMAC: Keyed-Hashing for Message Authentication*, Internet Engineering Task Force, Request for Comments (RFC) 2104, February 1997.
http://www.faqs.org/rfcs/rfc2104.html

[47] Krawczyk H.: HMQV: A High-Performance Secure Diffie-Hellman Protocol; in V. Shoup (Ed.): Crypto 2005, LNCS 3621, Springer-Verlag August 2005, pp 546-566.

[48] Law L., Menezes A.J., Qu M., Solinas J., Vanstone S.: An efficient Protocol for Authenticated Key Management; Designs, Codes and Cryptography, vol 28, 119-134, 2003.

[49] Levine, J.R.: An Overview of E-Postage; Feb 2004.
http://www.taugh.com/epostage.pdf

[50] Mann CC: Homeland Insecurity; The Atlantic Monthly, Sep 2002
http://www.theatlantic.com/doc/200209/mann

[51] Matsumoto, T., Takashima, Y., Imai, H.: On seeking smart public-key distribution systems; Transactions IECE of Japan, 1986, E69(2), pp 99-106.

[52] Maurer UM: A universal statistical test for random bit generators; Journal of Cryptology, vol 5, no 2 (1992), 89-105.

[53] Mayer M.: USPS will use a PKI to manage electronic postage; Government Computer News (GCN), Sep 7, 1998, Vol 7, No 24.
http://www.gcn.com/17_24/news/33918-1.html

[54] Menezes A..J., van Oorschot P.C., Vanstone S.A.: Handbook of Applied Cryptography; CRC-Press, August 2001.
http://www.cacr.math.uwaterloo.ca/hac/

[55] Menezes A.J., Qu M., Vanstone S.: Some new key agreement protocols providing mutual implicit authentication; Second Workshop on Selected Areas in Cryptography (SAC), pp 22–32, 1995.

[56] Merkle RC: A fast software one-way hash function; Journal of Cryptology, issue 3, 1990.

[57] Micali S, Schnorr C.P.: Efficient, perfect random number generators; Advances in Cryptology, Crypto 88, Springer Verlag, Berlin 1990, 173-198.

[58] Mr. Unzip: How to Screw the Post Office; Loompanics Unlimited, Washington 2000.

[59] Neumann PG: Computer Related Risks; ACM Press, New York, Addison-Wesley, Reading Massachusetts, 1995.
http://www.csl.sri.com/users/neumann/insiderisks.html

[60] Niehaus S.: GNU Stamp, http://gnustamp.sourceforge.net/

[61] Odlyzko A.: *The Case Against Micropayments;*
http://www.dtc.umn.edu/˜odlyzko/doc/case.against.micropayments.pdf

[62] Pastor J: CRYPTOPOST (TM): A universal information-based franking system for automated mail processing. *US Postal Services Fourth Advanced Technology Conference, Washington, D.C.*, Nov 5-7, 1990, pp 429–442.

[63] Pastor J: CRYPTOPOST (TM) - A Cryptographic Application to Mail Processing; Journal of Cryptology, vol 3, no 2, Springer Verlag, Berlin 1991, 137–146.

[64] Paul H. (Hg.): Abschlußbericht der Mensch – Maschine – Kommunikation 1995 – Irritation und Komplexität; Institut Arbeit und Technik, Gelsenkirchen, 1996
http://www.iatge.de/aktuell/veroeff/ps/paul96b.pdf

[65] Pfleeger C: Security in Computing (3rd ed); Prentice Hall PTR, Dec 2002.

[66] Pintsov L, Vanstone S: Postal Revenue Collection in the Digital Age; Financial Cryptography 2000, Springer Verlag, Berlin 2001,
http://www.postinsight.pb.com/files/POST_REV.pdf

[67] American Society of Mechanical Engineers: Pitney Bowes Model M Postage Meter 1920, An International Historic Mechanical Engineering Landmark, September 1986.
http://www.asme.org/Communities/History/Landmarks/
PitneyBowes_Model_M_Postage.cfm

[68] Rowe C.: Mail Fraud; Chip's Closet Cleaner Issue 13
http://www.chiprowe.com/articles/mail.html

[69] RSA Laboratories: Public Key Crypto Systems, PKCS#1, Version 1.5; Nov 1993.
http://www.rsasecurity.com/rsalabs/

[70] Schneier B: Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition; John Wiley, 1996.

[71] Shamir A: On the generation of cryptographically strong pseudoyrandom sequences; ACM Trasnactions on Computer Systems, 1 (1983), 38-44.

[72] Skala M, Roth M, Hernaeus N, Guyomarch R, Koch W: Gnu Privacy Guard; 2005.
http://www.gnupg.org/

[73] Thales e-Security Inc.: WebSentry™ Secures the First Live Electronic Stamping System; http://www.thales-esecurity.com/CaseStudies/Documents/Stampit_Case_Study.pdf

[74] Tilborg Hv: Encyclopedia of Cryptography and Security; Springer Verlag, New York 2005.

[75] TPG: NetSet™: de nieuwe standaard http://www.tpgpost.nl/business/post_versturen/frankeren/frankeermachines/net-set.jsp

[76] Tygar JD, Yee BS: Secure Coprocessors in Electronic Commerce Applications; Proceedings of USENIX Electronic Commerce Workshop, New York 1995, 155–170. http://citeseer.ist.psu.edu/yee95secure.html

[77] Tygar JD., Yee BS., Heintze N.: Cryptographic Postage Indicia; in Concurrency, and Parallelism, Programming, Networking, and Security, ASIAN '96; LNCS 1179, Springer-Verlag, Berlin 1996, pp378-391. ftp://www.cs.ucsd.edu/pub/bsy/pub/asian-96.ps

[78] Tygar JD., Yee BS., Heintze N.: Cryptographic Postage Indicia; Research Report CMU-CS-96-113. http://www.cs.berkeley.edu/~tygar/papers/Cryptographic_Postage_Indicia/CMU-CS-96-113.pdf.

[79] United States Census Bureau: The Current Population Survey; 2006, http://www.census.gov/population/www/socdemo/migrate.html

[80] United States Federal Register, "Postal Service Retirement Plan for manually set postage meters", vol 65, no 84, May 1, 2000, pp 25399–25400. http://ribbs.usps.gov/files/fedreg/usps2000/00-10812.PDF

[81] United States Federal Register, "Retirement Plan for Manually Set Postage Meters", vol 65, no 240, December 13, 2000, pp 77934–77938, . http://www.gpoaccess.gov/fr/index.html

[82] United States Federal Register, "Manufacture, Distribution, and Use of Postage Meters—Final Rule", vol 60, no 111, June 9, 1995, pp 30713–30742. http://www.gpoaccess.gov/fr/index.html

[83] United States General Accounting Office: "Report to the Chairman, Subcommittee on Federal Services, Post Office and Civil Service, Committee on Governmental Affairs, U.S. Senate: Postage Meters, Risk of significant financial loss but controls are being strengthened", May, 1994. http://archive.gao.gov/t2pbat3/151880.pdf

[84] United States General Accounting Office, "Letter to Senator David Pryor Ranking Minority Member Subcommittee on Post Office and Civil Service United States Senate", Sep 26, 1996. http://www.gao.gov/cgi-bin/getrpt?GGD-96-194R

[85] United States National Institute of Standards and Technology (NIST): Cryptographic Toolkit. http://csrc.nist.gov/CryptoToolkit/index.html

[86] United States National Institute of Standards and Technology (NIST): Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140-1, Jan. 11, 1994. http://www.itl.nist.gov/fipspubs/fip140-1.htm

[87] United States National Institute of Standards and Technology (NIST): Security Requirements for Cryptographic Modules; *Federal Information Processing Standards Publication* 140-2, May 25, 2001.
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[88] United States National Institute of Standards and Technology (NIST): Derived Test Requirements for FIPS 140 (Draft); Mar 24, 2004
http://csrc.nist.gov/cryptval

[89] United States National Institute of Standards and Technology (NIST): Cryptographic Module Validation Program (CMVP);
http://csrc.nist.gov/cryptval

[90] United States National Institute of Standards and Technology (NIST): Secure Hash Standard, *Federal Information Processing Standards Publication* 180, May, 1993.

[91] United States National Institute of Standards and Technology (NIST): Secure Hash Standard, *Federal Information Processing Standards Publication* 180, April, 1995.
http://www.itl.nist.gov/fipspubs/fip180-1.htm

[92] United States National Institute of Standards and Technology (NIST): Secure Hash Standard, *Federal Information Processing Standards Publication* 180-2, Aug 1, 2002.
http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

[93] United States National Institute of Standards and Technology (NIST), "Digital Signature Standard (DSS)"; Federal Information Processing Standards Publication 186, May 19, 1994.
http://csrc.nist.gov/cryptval/dss.htm

[94] United States National Institute of Standards and Technology (NIST): Digital Signature Standard (DSS), *Federal Information Processing Standards Publication* 186-2, Jan 27, 2000.
http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

[95] United States National Institute of Standards and Technology (NIST): Digital Signature Standard (DSS), *Federal Information Processing Standards Publication* 186-3, Jan 27, 2000.
http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

[96] United States National Institute of Standards and Technology (NIST), The Keyed-Hash Message Authentication Code (HMAC); *Federal Information Processing Standards Publication* 198, Apr 8, 2002.
http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf

[97] United States National Institute of Standards and Technology (NIST): An Introduction to Computer Security - The NIST Handbook; Special Publication 800-12, October 1995
http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/index.html

[98] United States National Institute of Standards and Technology (NIST): Recommendation for Key Management; NIST Special Publication 800-57, Aug 2005.
http://csrc.nist.gov/publications/nistpubs/

[99] United States Postal Rate Commission,
http://www.prc.gov

[100] United States Postal Services (USPS): Information Based Indicia Program; Performance Criteria for Information-Based Indicia and Security Architecture for Closed IBI Postage Metering Systems (PCIBI-C); January 12, 1999.

[101] United States Postal Services (USPS): Information Based Indicia Program; Performance Criteria for Information-Based Indicia and Security Architecture for Open IBI Postage Metering Systems (PCIBI-O); June 25, 1999.
http://www.usps.com/postagesolutions/programdoc.html

[102] United States Postal Services (USPS): Information Based Indicia Program; Performance Criteria for Information-Based Indicia Program Systems Employing Centralized Postal Security Devices (PCIBI-WAN); August 17, 2000.

[103] United States Postal Services: Postal Explorer
http://pe.usps.gov

[104] United States Postal Services: Domestic Mail Manual, Chapter 604, §4.4

[105] United States Postal Services: Postage Evidencing Product Submission Procedures (Correction); Federal Register, vol 67, no 232, Dec 3, 2002.
http://ribbs.usps.gov/files/fedreg/usps2002/02-30649.pdf

[106] United States Postal Services Postal Inspection Service: "The Story of American Presort, Inc",
http://www.usps.com/postalinspectors/ar02/ar02nsrt.htm

[107] Universal Postal Union: Electronic Postmark (EPM) Interface; Standard S43-2, Nov 20, 2003.

[108] Universal Postal Union, http://www.upu.int

[109] Universal Postal Union, "Postal Market 2004, Review and Outlook".
http://www.upu.org/statistics/en/postal_market_2004_review_and_outlook_en.pdf

[110] Universal Postal Union: Development of Postal Services in 2004.
http://www.upu.int/statistics/en/development_of_postal_services_in_2004_en.ppt

[111] Universal Postal Union: The Worldwide Postal Network in Figures.
http://www.upu.int/news_centre/documents/en/
brochure_the_worldwide_postal_network_in_figures_en.pdf

[112] Universal Postal Union: Identification of postal items - Part C: 13 character identifier for special letter products; UPU Standard S10c, Approved 19-Apr-2005.

[113] Universal Postal Union: International Postage Meter Approval Requirements (IPMAR); UPU Standard S30-4, Approved 17-Oct-2000.

[114] Universal Postal Union: Digital postage marks (DPM) — Applications, Security and Design; UPU Standard S36-4, Approved 06-Oct-2004.

[115] Vaudenay S: The Security of DSA and ECDSA, Bypassing the Standard Elliptic Curve Certification Scheme; Y.G. Desmedt (Ed.): PKC 2003, LNCS 2567, Springer-Verlag, Berlin Heidelberg 2003, pp. 309–323.

[116] Wang XY, Feng DG, Yu HB: How to Break MD5 and other Hash Function; Advances in Cryptology, Eurocrypt 04, Springer-Verlag, Berlin 2005, pp19-35.

[117] Wang XY, Lai XJ, Feng DG, Chen H, Yu XY: Cryptanalysis for Hash Functions MD4 and RIPEMD, Advances in Cryptology, Eurocrypt 05, Springer-Verlag, Berlin 2005, pp1-18.

[118] Wang XY, Yao A, Yao F: New collision search for SHA-1; Rump Session of Crypto 05.

[119] Wang XY, Yin YL, Yu HB: Finding Collisions in the Full SHA-1; Advances in Cryptology, Crypto 05, Springer-Verlag, Berlin 2005, pp17-36.

[120] Weingart S.H., White S.R., Arnold W.C., Double G.P., An Evaluation System for the Physical Security of Computing Systems, IEEE Sixth Annual Computer Security Applications Conference, Dec 3-7, 1990, Tucson AZ, pp. 232-243.

[121] Westdeutscher Rundfunk: Betrug mit Frankiermaschine; WDR Aktuell, June 18, 2001.
http://www.wdr.de/online/news/postbetrug/index.phtml

Appendix A

List of Acronyms

Keyword	*Explanation*
3DES	Tiple-DES
AADC	Automated Area Distribution Center, i.e., a USPS mail processing center
ACH	Automatic Clearing House
ACS	Address Change Service of the US Postal Service
AES	Advanced Encryption Standard
AMS	Address matching service
ANSI	American National Standards Institute
AR	Ascending Register
CA	Two letter abbreviation for Canada (ISO 3166)
CA	Certification Authority
CC	Common Criteria
CCD	Charge Coupled Device, technology used for digital photography
CEM	Common evaluation methodology
CEN	Comité Européen de Normalisation, European Committee for Standardization
CFS	Computerized Forwarding System of the US Postal Services
CISSP	Certified information system security professional

Keyword	*Explanation*
CMVP	Cryptographic Module Validation Program of NIST
COA	Change of Address (of the US Postal Service)
CORBA	Common Object Request Broker Architecture of the OMG
CPC	Canada Post Corporation
CPU	Central processing unit, main processor
CRC	Cyclic Redundancy Code
CRL	Certificate Revokation List
DES	Data Encryption Standard
DMIS	Digital Meter Indicia Specification of the Canada Post Corporation
DPAG	Deutsche Post AG
DR	Descending Register
DSA	Digital Signature Algorithm
DSL	Digital subscriber line
DSS	Digital Signature Standard
DTR	Derived Test Requirements under FIPS 140
EAL	Evaluation Assurance Level (under Common Criteria)
ECDSA	Elliptic Curve DSA
EDI	Electronic document interchange
EEPROM	Electrically Erasable PROM
EFP / EFT	Environmental failure protection / testing
EJB	Enterprise Java Beans
EKP	Customer number provided by Deutsche Post
EMI / EMC	Electromagnetic interference / compliance
EPROM	Erasable PROM
EPV	Elliptic curve PV
ERP	Enterprise Resource Planning
ESI	"Entgeltsicherung", German for revenue protection group

Keyword	*Explanation*
EUR	European currency
FIM	Facing identification mark
FIPS	Federal Information Processing Standard of NIST
FTP	File Transfer Protocol
GPG	GNU Privacy Guard
HMAC	message authentication code mechanism based on a hash function
HMQV	Hash enhanced MQV
HSM	Hardware Security Module
IBI	Information Based Indicia
IBIP	IBI Program
IC	Integrated Circuit
IEEE	Institute of Electrical and Electronic Engineers, Inc.
IPC	International Post Corporation
IPMAR	International Postage Meter Approval Requirements
ISO	International Standards Organization
ITSEC	Information Technology Security Evaluation Criteria
MAC	Message authentication code, message authentication code mechanism
MD	Message Digest
MLOCR	Multi-line optical character recognition
MQV	Menezes, Qu, Vanstone
NCSC	National Customer Support Center (of the US Postal Service)
NIST	National Institute of Standards and Technology of the United States
NVLAP	National voluntary laboratory accreditation program of NIST
ODIS	Origin destination information system (of the US Postal Service)
OMG	Open Management Group
PC	Personal Computer
PC	Piece Count Register

Keyword	*Explanation*
PGP	Pretty Good Privacy
PKCS	Public Key Crypto System Standard
PKD	Public Key Directory
PKI	Public Key Infrastructure
PP	Protection Profile (Common Criteria)
PROM	Programmable ROM
PSAG	Postal Security Action Group
PSD	Postal security device
PSD-PSN	Postal Serial Number of a PSD
PTM	Postal Technology Management of the US Postal Services
PV	Pintsov-Vanstone digital signature mechanism
PVD	Postage value download
PVD-R	PVD request
PVR	Postage value refund
RA	Registration Authority
RAID	Redundant Array of Independent Disks
RAM	Random access memory
REMPI	Re-engineering the mail—Postal Interface
RFC	Request for Comment
RIPE	RACE Integrity Primitives Evaluation
ROM	Read only memory
RSA	Rivest-Shamir-Adleman digital signature mechanism
RSM	Revenue Sensitive Module
RTC	Real time clock
SHA	Secure Hash Algorithm
SOHO	Small office / home office
SRDI	Security relevant data item

Keyword	*Explanation*
SSL	Secure Socket Layer
ST	Security Target (Common Criteria)
STS	Station-to-station protocol
TCPSEC	Trusted Computer Product Security Evaluation Criteria
TLS	Transport Layer Security
TPG	Netherlands Post
TS	Total Settings Register
UK	United Kingdom
UPU	Universal Postal Union
USPS	United States Postal Services
UZ	"Unzustellbar", German for mail item not-deliverable
XML	extendible markup language
ZIP	Zone Improvement Program (of the US Postal Service)

Appendix B

About the Author

As senior cryptography architect, Gerrit Bleumer lead the design and development of the global cryptographic architecture of Francotyp-Postalia Group (FP), which controls the transport and delivery of cryptographic modules worldwide and supports postage meters from their initialization to removal from market. Since 2004, he has headed the department of innovation projects and product quality of the research and development division of FP. He has served on the advisory board of the Encyclopedia of Cryptography and Security published by Springer.

In 1991, he received a diploma in computer science from the University of Karlsruhe, Germany. From 1992 to 1996, he worked as research associate in several research projects in security of health care informatics funded by the Commission of the European Union. From 1997 to 1999, he worked as senior technical staff member at AT&T Labs-Research in Florham Park, NJ. In 2001 he received a Doctorate in computer science from the University of Dortmund, Germany.

Index

Printed in the United States