

## 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.

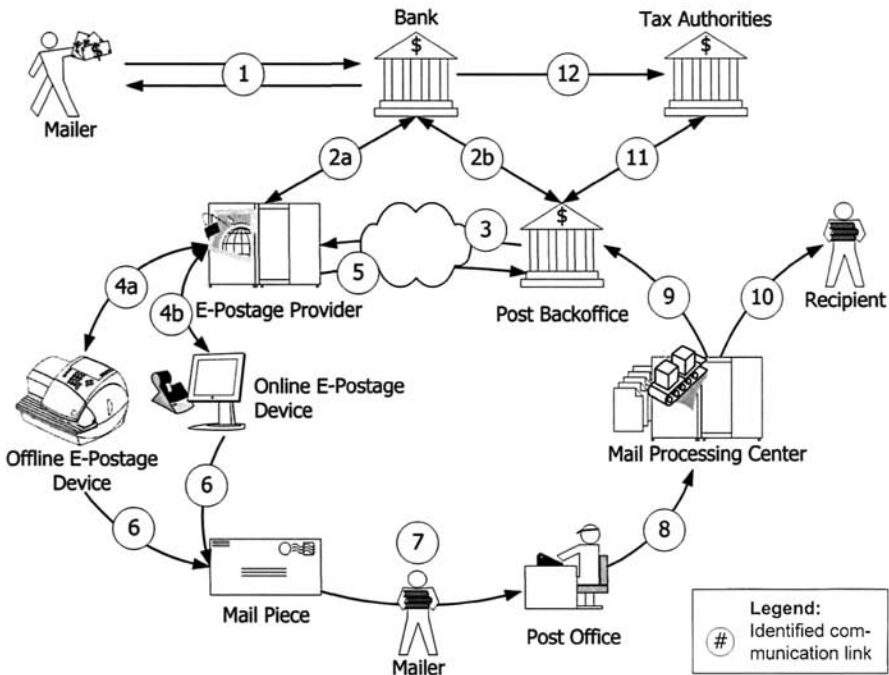


Figure 11. Cycle of Electronic Postage

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

|                 | <i>special purpose hardware<br/>closed system</i> | <i>general purpose hardware<br/>open system</i>  |
|-----------------|---|--|
| <i>offline</i>  | digital postage meter [100]                       | <ul style="list-style-type: none"><li>• PC postage client with PC “dongle” [101]</li></ul>   |
| <i>online</i>   | not commercially available                        | <ul style="list-style-type: none"><li>• PC postage client with label / office printer and Internet connection [102],</li><li>• Standalone label printer with Internet connection</li></ul> |
| <i>one-time</i> | not commercially available                        | <ul style="list-style-type: none"><li>• not commercially available</li></ul>   |

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 pre-defined 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

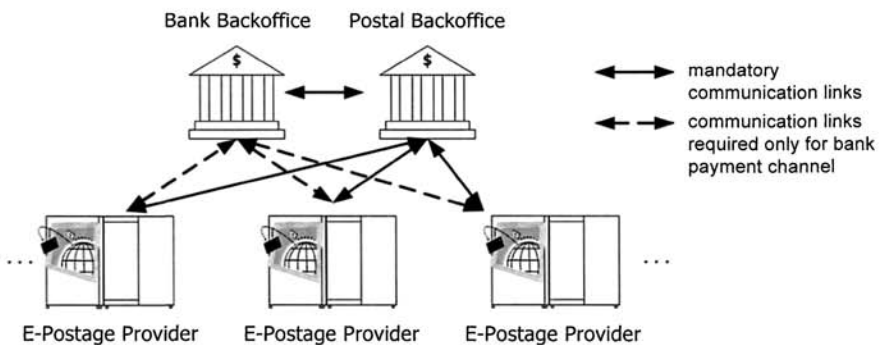


Figure 12. Communication Network of an E-Postage Minting System

serves as a gateway between its e-postage devices, the bank and the post back-office. 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

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 Symbolology

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:  $TS = AR + DR$ . 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 reim-

burse 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

Table 7. Sample US Rate Categories (2005)

| <i>ID</i> | <i>class of mail</i> | <i>subclass of mail</i> | <i>weight range</i> | <i>origin &amp; destination</i> | <i>presort type</i> | <i>extra service</i> | <i>postage</i> |
|-----------|----------------------|-------------------------|---------------------|---------------------------------|---------------------|----------------------|----------------|
| 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         |

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.

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-post-

age 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).



<http://www.springer.com/978-0-387-29313-4>

Electronic Postage Systems  
Technology, Security, Economics  
Bleumer, G.  
2007, XXIII, 248 p., Hardcover  
ISBN: 978-0-387-29313-4