Secure Electronic Postage Stamping

Gerrit Bleumer, Francotyp-Postalia. Email: g.bleumer@francotyp.com

www.eurowired.org

The Postal Authorities of the developed countries have automated their mail processing facilities and logistics to a large extent. Potential for increasing efficiency, improving mail delivery and customer convenience and reducing the cost of Postal Authorities lies in better integrating the mail processing at the customer site with the mail processing of the Postal Authorities. Two other forces drive the Postal Authorities in this direction: the amount of postage-related fraud and the prospect of more marketing data about what customers really want. Aquiring such marketing data may conflict with legitimate privacy requirements of customers, but there are techniques supporting the former while guaranteeing strong privacy to senders[1]. Balancing these interests of Postal Authorities (and other mail carriers) and of individual customers remains a challenge in designing electronic postage systems.

Today, customers have essentially three ways of franking their mail: franking services provided by Postal Authorities, postage meters and stamps. Very roughly, each of these methods contributes about one third of the annual Postal revenue somewhat varying between different Postal markets.

Clearly, postage meters and stamps bear the biggest potential of linking the customer's mailing process closer to the Postal Authorities' processes. Also note that the fraudulent use of postage meters for example in the US, accounts for an estimated US$100 million per year. Thus the Postal Authorities have started to switch the market from mechanical postage meters towards electronic postage meters. The US Postal Authority has launched the information-based indicia-program (IBIP) in 1996 [4] and is pushing to increase the market share of electronic postage meters. Other Postal Authorities in Europe are following, driven by the liberalisation and deregulation of Postal markets. Stamps are going to be replaced gradually by PC based electronic postage, sometimes called PC-postage. Small offices and home offices just need to have a PC, a desktop printer and an Internet connection in order to produce valid indicia. Commercial products have been approved in the US since 1999. Postal Authorities in Europe are following quickly. For example, the German Postal Authority launches a PC-postage system[2] in September 2001.

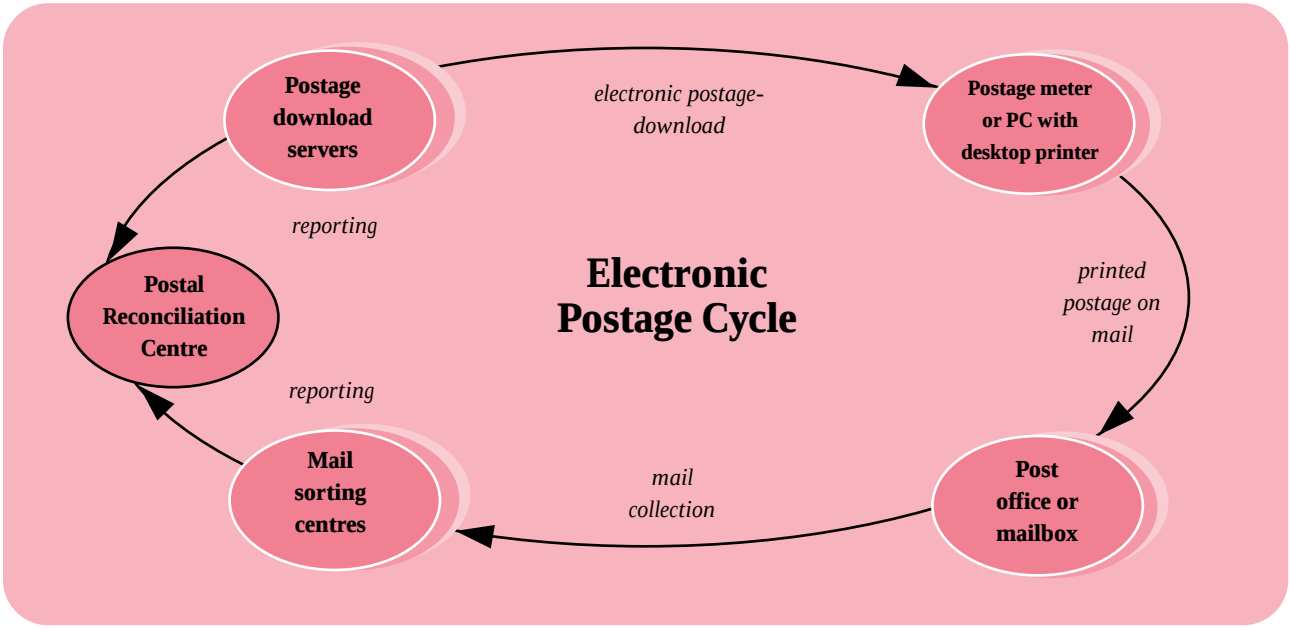
POSTAL SECURITY DEVICE

All electronic postage solutions follow the basic idea behind the IBI-Program. The customer pre-pays an amount of electronic postage and downloads it into a postal security device (PSD) at any time he likes. Each time the customer wants to print an indicium onto a letter, envelope, or postage label, the postal security device first checks if it has sufficient electronic postage available and if so produces a cryptographically secured indicium, which is then printed in the form of a two-dimensional bar code. At the same time, a corresponding amount of electronic postage is deducted automatically from the postal security device. The cryptographic portion of the indicia are either a digital signature or a message authentication code, both of which cannot be forged without breaking the postal security device. Extra measures need to be taken to discourage Xerox copies of indicia.

CUSTOMER VIEW

Whether customers use a postage meter or a PC to print their indicia, they will see a tiny machine-readable two-dimensional bar code, which contains the digital signature or message authentication code. Typically, indicia are printed onto the front of an envelope, but some PC-Postage products alternatively allow to include the indicium right in the address field of the letter head. Thus the indicium will be visible through the address window of the envelope. No separate printing of an envelope is needed.

When customers lease (US) or purchase (Europe) their postage meters, they need to register it to a post office of their choice; typically a post office close to their residence. At the same time they open a postage account with the vendor of their postage meter. After they have drawn money into that account, they can download electronic postage from their account into their postage meter. This electronic postage is used to produce indicia offline for individual mail pieces. There are postage meters for a range of offices from small law firms or travel agencies up to mail rooms of large corporations, where individual mailings are



processed at up to 12,000 pieces per hour. Mail prepared with a postage meter must be delivered to the registered post office. When customers purchase software for PC Postage, they also open an account with the respective vendor. After they have drawn money into that account, they can download electronic postage to their PC in order to later produce indicia offline (Offline PC-Postage). Or they can connect to their account each time they want to produce an indicium (Online PC-Postage). Mail prepared with a PC can be dropped into a mailbox at the curb of the road.

In general, Postal Authorities see a higher risk of fraud in PC-Postage than in postage meters. They argue that PC-Postage uses standard operating platforms, standard communication interfaces, and may use the Internet for electronic postage download. Therefore, PC Postage products typically mitigate the related risks by having in each indicium an expiration date and time as well as the recipient address. As a result, letters must be sent off no later than, say, 24 hours after their indicia are produced, and once an indicium is printed for recipient 'Smith' it cannot be used instead for recipient 'Baker'.

THE FULL POSTAGE CYCLE

Postal Authorities usually require all vendors who keep customer accounts for electronic postage to report all their transaction data for later reconciliation by the Postal Authority. This data is checked against the reports coming in from all the mail-sorting centres, where the indicia are scanned and verified.

In order to tighten the postage cycle described above, the Postal Authorities need to install high speed 2-D bar code scanning facilities in all mail sorting centres through which respective indicia can pass. A scan rate very close to 100% is required in order to sufficiently verify indicia and to reject Xerox copies of indicia. Detecting Xerox copies requires that the mail sorting centres operate a shared database in real time to keep track of all indicia that have been used and are therefore not valid any more.

SECURITY TECHNOLOGIES

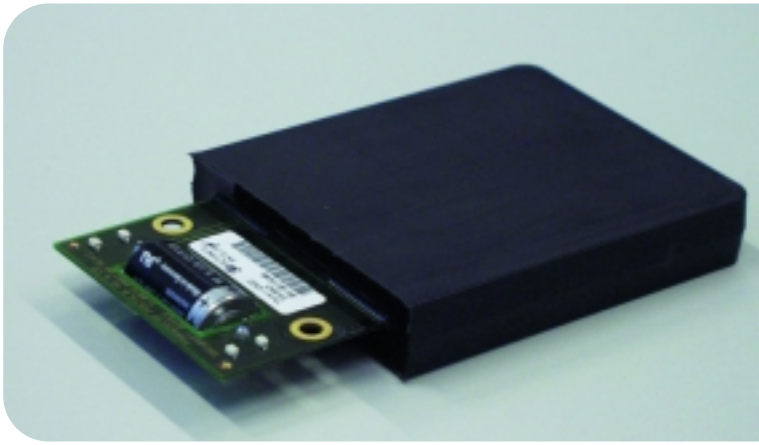
The core security technology of electronic postage solutions is a postal security device (PSD). It can be a hardware security device embedded into a postage meter or connected to a PC. This approach is also called offline electronic postage because indicia can be printed without connecting to the postage download server. Alternatively, the postal security device can be located at the remote postage download server such that a connection needs to be made to the server each time an indicium is printed. So far, this online approach has only been adopted for PC-Postage because online connections are less reliable and do not support high speed printing of indicia. The online approach might be adopted for postage meters in the future if reliable broadband connections become affordable, but there are also privacy issues related to online electronic postage.

In electronic postage systems, the postal security device has two purposes. It stores electronic postage securely and it produces valid indicia on demand. In offline electronic postage, the postal secu-rity device also protects the electronic postage download between the remote postage download server and the postage meter or PC at the customer site.

Most electronic postage systems have an inherent problem because a third party vendor:

(1) Operates the postage download server (which might include a PSD),
(2) Provides the postage meters (including PSDs), or
(3) Provides the PC software and the PSDs for the customer PCs.

FP Embedded Security Device 'Revenector'



In either case, there is a latent conflict of interests between the Postal Authority who is delivering the mail and the third party vendor who must protect the Postal Authority's revenue through proper design of the postal security device and reliable operation of the postage download server(s). The IBI Program alleviates this conflict by requiring third party vendors to have their postal security devices certified by an accredited FIPS 140 test lab. Francotyp-Postalia[3] offers a tamper resistant and responsive hardware security module called 'Revenector' that is about to receive a FIPS 140-1 L3+ certificate and is configured by certified software to work as a PSD. Equipped with a powerful cryptographic library, 'Revenector' can also be configured as a proxy for payment protocols, to authenticate databases, to protect real-time transaction logging etc., with a higher level of assurance than any smart card can. Due to its size, it is easily embedded into PCs and smaller e-commerce appliances such as POS terminals, etc.

In order to meet the strong requirements of the IBI-Program, Francotyp-Postalia has developed a B2B public key infrastructure (PKI) that identifies each PSD from the manufacturer's plant through worldwide distribution through years of life at a customer's site. This B2B PKI supports elliptic curve based digital signatures for each PSD in order to keep the footprint of indicia to a minimum. FP's PKI interoperates with the PKI of the US Postal Authority in order to deliver all the individual verifying keys that need to be accessible at the numerous US mail sorting centres.

Electronic postage stamping is an emerging area of e-commerce. Related innovations in secure interoperation between data centres and remote appliances as well as in securing paper printouts are ready to be recognised by other sectors of business and industry. ■

REFERENCES

[1] Gerrit Bleumer: Secure PC-Franking for Everyone; EC-Web 2000, LNCS 1875, Springer-Verlag, Berlin 2000, 94-109.

[2] Deutsche Post AG: http://www.deutschepost.de/stampit

[3] Francotyp-Postalia AG & Co. KG:http://www.francotyp.com

[4] US Postal Services: Information Based Indicia Program; http://www.usps.gov/ibip