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