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

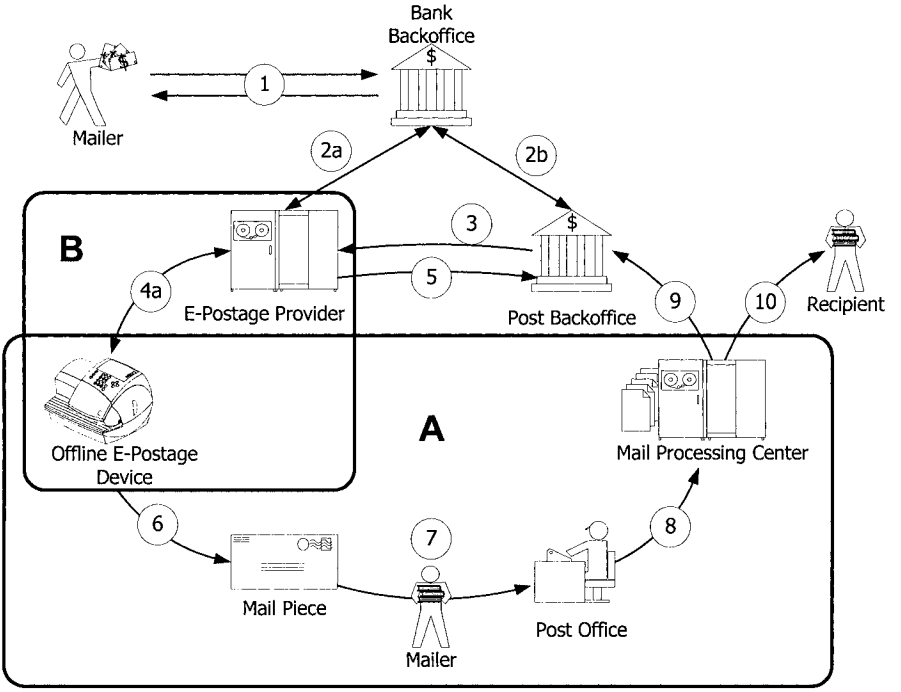

Figure 32. Offline E-Postage System Security Domains

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 verify-