In Chap. 3 we explain the hierarchical trust model for PKIs. In this trust model, certification authorities that issue certificates play an important role. However, issuing certificates is not sufficient. The certificates must be maintained and additional information must be provided during the entire life cycle. The entity that is responsible for certificate life cycle management is called the certification service provider (CSP). A CA is only one component of a CSP. Another component is the registration authority (RA), which registers certificate applicants and collects all information relevant for issuing certificates. Other possible components of a CSP are, for example, a directory service, which publishes information concerning certificates, and a revocation service, which issues revocation information. Sometimes, certification service providers are also called trust centers. In this chapter, we start by explaining the life cycle of a certificate. Then, we describe the CSP components. In the next chapter, we discuss certificate policies that govern the operation of CSPs in a PKI.

7.1 Certificate Life Cycle

Certificate life cycles may vary according to the organization of a PKI and the certificate usage. Here, we describe a typical certificate life cycle. It can be divided into three phases.

7.1.1 Certificate Generation Phase

The certificate life cycle starts with a certificate application by some entity. This entity may be the intended owner of the certificate or some other authorized entity, for example, someone who is responsible for IT security in some institution of which the intended certificate owner is an employee. The application is followed by the
registration of the intended certificate holder. In the registration, the information relevant for issuing the certificate is collected and verified. This information typically includes the name of the intended certificate owner and some contact information such as an email address. It may also include the public key to be contained in the certificate if the corresponding key pair is generated by the intended user. After application and registration, the certificate is issued. If the key pair is not generated by the certificate applicant, the key pair is generated by a trusted third party such as the card manufacturer or the CSP while issuing the certificate. The CSP creates the certificate and signs it digitally. The CSP may also back up the private key corresponding to the public key in the certificate. For example, this is useful for decryption keys. For such keys, a backup prevents encrypted data from becoming inaccessible in the case where the private key owner loses the private decryption key. However, key backup opens security risks since the CSP has knowledge of private keys and with this knowledge the power to decrypt information of its users. Once a certificate is issued, it is delivered to and accepted by its owner. Without owner acceptance the certificate must not be used since it may contain incorrect information. The final step of the generation phase is publication of the certificate since it is intended to be used by many entities for establishing trust in the public key in the certificate belonging to the certificate owner.

7.1.2 Certificate Validity Phase

The main purpose of a certificate is to prove that the public key contained in the certificate belongs to the certificate owner. To this end, the certificate is retrieved from some directory. This may be a local directory of the user or a directory operated by some directory service. The certificate user validates the certificate, which includes verifying the certificate signature and checking the validity period of the certificate and its revocation status. But certificate validation may be much more involved. For example, if the certificate is an element of a certificate chain, the validity of the full chain must be checked. This is explained in Chap. 9.

When a certificate expires, the subject in the certificate may want to continue using the public key, for example, if he or she wants the smart card containing the corresponding private key to remain usable. In such a case, the certificate may be reissued before it expires. The re-issued certificate has the same content as the original certificate and a new expiration date.

7.1.3 Certificate Invalidity Phase

Typically, certificates have a limited validity period. For example, the validity of an X.509 certificate ends on the notAfter date in the certificate. Another way of invalidating certificates is to revoke them before they expire. Revocation is discussed in Chap. 5.