J. Lopez, R. Oppliger, and G. Pernul, "Classifying Public Key Certificates", *2nd European PKI Workshop: Research and Applications (EuroPKI05)*, LNCS vol. 3545, pp. 135-143, 2005.
NICS Lab. Publications: `https://www.nics.uma.es/publications`

Classifying Public Key Certificates

Javier Lopez[1], Rolf Oppliger[2], and Günther Pernul[3]

[1]Computer Science Dept., University of Malaga, Malaga, Spain
e-mail: jlm@lcc.uma.es
[2]eSECURITY Technologies Rolf Oppliger, Gümligen, Switzerland
e-mail: rolf.oppliger@esecurity.ch
[3]University of Regensburg, Germany
e-mail: guenther.pernul@wiwi.uni-regensburg.de

Abstract. In spite of the fact that there are several companies that (try to) sell public key certificates, there is still no unified or standardized classification scheme that can be used to compare and put into perspective the various offerings. In this paper, we try to start filling this gap and propose a four-dimensional scheme that can be used to uniformly describe and classify public key certificates. The scheme distinguishes between (i) who owns a certificate, (ii) how the certificate owner is registered, (iii) on what medium the certificate (or the private key, respectively) is stored, and (iv) what type of functionality the certificate is intended to be used for. We think that using these or similar criteria to define and come up with unified or even standardized classes of public key certificate is useful and urgently needed in practice.

1 Introduction

It is commonly agreed that security is an important prerequisite for Internet-based electronic commerce. The term security, in turn, means different things to different people, and there are many security services one may think of. According to the OSI security architecture specified in ISO/IEC 7498-2, there are at least authentication, authorization, data confidentiality, data integrity, and non-repudiation services to distinguish [9].

Public key cryptography as originally proposed by Diffie and Hellman [7] provides an important technology to provide security services. Some of the services, such as non-repudiation services, cannot easily be provided without public key cryptography, whereas other services can be provided more efficiently with public key cryptography (as compared to secret key cryptography). This is particularly true for (entity or data origin) authentication services and the key establishment for data confidentiality and integrity services (see, for example, [14]).

With respect to its practical deployment, the Achilles heel of public key cryptography is public key certification, meaning that the authenticity of the public keys in use must be guaranteed, that is, certified by some trusted party (see, for example, Chapter 7 of [13]). This certification is usually done by *Certification*

Authorities (CAs) or—more generally— *Certification Service Providers* (CSPs [1]).

In short, a CSP authenticates a public key by digitally signing it together with some identification or naming information about the key owner (and some other attributes). The result is a digital or *public key certificate*. A set of mutually trusting and cooperating CSPs forms a *Public Key Infrastructure* (PKI).

Public key cryptography can only be used in an efficient and effective way, if a PKI exists and is operated in some trusted way. Unfortunately, the establishment and successful commercial deployment has not really taken off so far (see, for example, [12] for a corresponding analysis).

There are many companies that (try to) act as CSPs and market public key certificates and corresponding services on a national or international level [2]. They all use policies and terminologies of their own, and it is getting increasingly difficult to tell their offerings apart and to put them into perspective.

Additionally, several standardization organizations are working on public key certificates and PKIs (e.g., ANSI, NIST, IETF, OASIS, ...). However, they work neither on a unified or even standardized terminology and set of policies, nor on interoperability issues. This is unfortunate, because it makes everything more involved from the user's perspective. An old proverb saying that every cat is black at night also applies to public key certificates, and hence it may be difficult to tell the various offerings of CSPs apart. Against this background, we believe that a unified or even standardized classification scheme is urgently needed to compare and put into perspective the offerings of the CSPs.

In this paper, we propose a classification scheme for public key certificates. The scheme distinguishes between (i) who owns a certificate, (ii) how the certificate owner is registered, (iii) on what medium the certificate (or the private key, respectively) is stored, and (iv) what type of functionality the certificate is intended to be used for. It goes without saying that the resulting four-dimensional classification scheme can be used as a starting point for further standardization activities. In fact, a classification scheme is only useful if many CSPs support it and specify their offerings according to this scheme. The rest of the paper is organized as follows. The related work is addressed in Section 2. The four classification criteria mentioned above are introduced and discussed in Section 3. A notation is proposed in Section 4, and a few major classes are overviewed and discussed in the same section. Finally, conclusions are drawn in Section 5.

2 Related Work

Each CSP has to specify a set of policies— *certificate policies* (CPs) and/or *certification practice statements* (CPSs)—to specify and nail down its offerings (see informational RFC3647 [6] for a corresponding framework). Unfortunately, most policies are written in a terminology of their own. This, in turn, makes it

[1] Note that the acronym CSP is sometimes also used to refer to a cryptographic service provider.

[2] http://www.openvalidation.org/en/service/calist.html

difficult to compare directly the various offerings of different CSPs, and to tell the sometimes subtle difference(s) between them.

To the best of our knowledge, there is no international standardization effort to define unified classes for public key certificates (in fact, the major goal of this paper is to initiate such an effort). In some countries, there are CSPs that work together in defining some unified classes of public key certificates. For example, in Switzerland, the Certification Service Providers Forum [3] has proposed five classes of public key certificates (i.e., *Bronze*, *Silver*, *Gold*, *Platinum*, and *Qualified*).

From a user's point of view, this classification is advantageous and allows them to better compare the offerings of various CSPs. Unfortunately, there are only two small CSPs that together form the Swiss CSP Forum [4], and hence the classification scheme is not widely deployed and used by all CSPs (even in Switzerland). To be really successful, a classification scheme needs to be agreed upon on an international level.

3 Classification Criteria

The initial classification scheme proposed in this paper distinguishes between the following four criteria:

Certificate owner: Who is the owner of the certificate and the corresponding private key?

Registration: How is the certificate owner registered? More specifically, how is the certificate owner identified and authenticated before the certificate is issued?

Storage medium: On what medium is the certificate (or the corresponding private key, respectively) stored?

Functionality: What type of functionality can the certificate and the corresponding private key be used for?

Note that the storage medium is not an inherent property of a public key certificate. In fact, it is possible and technically feasible to provide a certificate on different media. Nevertheless, we think that it is appropriate to take the storage medium into account, mainly because the certificate is coupled with a way to store the private key. So it is more a property of the private key (than the certificate).

There are other criteria one may think of. For example, one can distinguish whether a public key pair is generated by the user, generated by the CSP, or imported (from a potentially unknown source). For the purpose of this paper, however, we do not use key generation as a criterion for certificate classification.

[3] http://www.csp-forum.ch

[4] The companies are SwissSign and SwissCERT.

Instead, we argue that from the CSP's viewpoint, it does not really matter how a key pair is generated. The only thing that matters for the CSP (and for which the CSP can be held accountable) is that the certificate owner is registered as claimed in the CSP's policies. If the CSP offers complementary key generation services, then these services can be treated independently from the certification services (like many other trusted services, such as time-stamping services).

3.1 Certificate Owner

As its name suggests, the criterion "certificate owner" specifies who owns the certificate and the corresponding private key. We distinguish basically three possibilities:

- *Natural person:* The certificate is owned by a natural person. These are the certificates one usually has in mind when one elaborates on digital signature laws. In fact, in most legislations it is ultimately required that the certificate owner (i.e., the entity that is specified in the subject field) is a natural person. Furthermore, certificates for natural persons are used and widely deployed in the realm of secure messaging and secure authentication (i.e., single sign-on and secure firewall traversal).

- *Legal entity:* The certificate is owned by a legal entity, such as a company, an administrative entity, or a non-profit organization. From a business point of view, it is often argued that public key certificates owned by legal entities are ultimately required. In fact, many digital signature legislations have to struggle with the question whether it is possible to have legal entities issue legally-binding signatures (in addition to natural persons). There is, for example, an ongoing controversy on this topic in Germany and Switzerland. There are pros and cons on either side, and we are not going to get into this discussion in this paper.

- *Machine:* The certificate is owned by a computer system, device, or service. Examples include certificates for devices that implement the IP security (IPsec) protocol suite and certificates for Web servers that implement the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol. So far, certificates for machines have been the only certificates that have been able to be successfully deployed in the marketplace.

In some classification schemes, it is also possible to distinguish between certificates that are owned by CAs, root CAs, or software publishers. We think that the distinguishing feature in these cases is not who owns the certificate, but for what purpose is it actually to be used for. For example, a certificate owned by a (root) CA is used to issue other certificates, whereas a certificate owned by a software publisher is used to digitally sign software. In either case, the (root) CA or software publisher may be a natural person, a legal entity, or a machine. There are mainly commercial and/or legal reasons for CSPs to market software publisher certificates separately. Again, this point is not further addressed in this paper.

3.2 Registration

The criterion "registration" specifies how the certificate owner is registered, or—more specifically—who registers the certificate owner before the certificate is issued (i.e., is registration part of the service or not). There are basically three possibilities (and several sub-possibilities in the last case) to distinguish between.

- *No registration:* The certificate owner is not registered at all. The corresponding certificates are typically used for test purposes only. In fact, a certificate without registration does not make a lot of sense for all practical purposes.

- *Customer registration:* The certificate owner is registered by the customer organization. This type of registration is usually used if a CSP is providing virtual CA services. In this case, the CSP "only" offers its certificate issuing capabilities, whereas the actual work related to user registration is done by the customer organization.

- *Registration:* The certificate owner is registered by the CSP, or a registration authority (RA) working on behalf of the CSP, respectively. There are a number of possibilities to register the owner.
  - The certificate owner may be registered using some form of e-mail based identification and authentication (EBIA) as, for example, discussed in [8].

  - The certificate owner may be registered by a trusted organization acting as registration authority and using some existing identification and authentication mechanism (e.g., username and password). For example, if an organization already has a customer relationship, it can use this relationship to identify and authenticate certificate applicants. It goes without saying that the authentication information must be transmitted over some secure channel (e.g., an SSL/TLS connection).

  - The certificate owner may be registered personally by a trusted organization using strong identification and authentication mechanisms (using, for example, a photo ID).

  - The certificate owner may be registered personally by a trusted organization using some official identification and authentication document, such as a national ID card or a passport.

  In either case, registration services can be provided by the CSP or delegated to partner companies acting as RAs, such as postal service providers or banks. In search of business plans to allow the successful marketing of certification services, many potential CSPs have been talking (and are still talking) to postal service providers and banks.

It goes without saying that a certification service without registration (i.e., no registration or customer registration) is substantially simpler to provide, and that the resulting business risks for the corresponding CSP can be made very small.

3.3 Storage Medium

There are several possibilities to store the certificate, or the private key, respectively. On a high level of abstraction, there are three possibilities to distinguish between.

- *Hardware:* The certificates employ special hardware devices to store private keys and corresponding certificates. Most of the time, it is assumed that all cryptographic computations with the private key are performed on the hardware device. Examples of hardware devices include smartcards and USB tokens.

- *Software:* The certificates do not employ hardware devices to store private keys and corresponding certificates. Instead, the private keys are stored in the application software that is going to use them. Most importantly, the Windows operating system can store the private keys of the registered users and make them available to all applications that can make use of it.

- *Server:* The private keys are stored on a server. They either never leave the server or are downloaded only temporarily and with special security precautions. Server-based certificates have many advantages for practical deployment, especially if one considers the mobility of users as an important criterion (see, for example, [15]).

From a security viewpoint, the use of special hardware and hardware-based certificates are certainly the preferred choice. It must also be said, however, that the security advantage of hardware certificates is frequently overemphasized, and that there are many possibilities to attack smartcards and other hardware tokens (cf. [3], [1], [11], [2], [4], [5], [10]).

Also, security is not always the main decision criterion and there are many situations in which the use of hardware-based certificates is prohibitively expensive. In these cases, the use of software-based certificates or server-based certificates provides a reasonable alternative. This is particularly true for software-based certificates that are frequently used in Windows operating systems. Using the auto-enrollment feature of the Windows 2003 PKI server, for example, certificates can be easily deployed in a corporate environment. The security of the corresponding certificates is directly coupled to the security of the user accounts for the Windows domains.

3.4 Functionality

There are basically three types of functionality a certificate and the corresponding private key can be used to provide.

– *Authentication:* The certificate can be used for authentication, meaning that its owner can use the private key to authenticate himself or herself to a (peer) entity.

– *Digital signatures:* The certificate can be used for digital signatures, meaning that its owner can use the private key to digitally sign documents (or public key certificates, respectively) and protect the authenticity and integrity of these documents accordingly.

– *Encryption:* The certificate can be used for encryption, meaning that its owner can use the private key to decrypt documents.

If a certificate and the corresponding private key are used to agree on a shared secret key (using, for example, a Diffie-Hellman key exchange [7]), then we consider encryption to be the functionality that is actually provided. Consequently, we do not consider key agreement to be a functionality of its own. Note that this is a simplification, because the secret key can also be used to protect the authenticity and integrity of a document (using, for example, a message authentication code).

4 Notation and Major Classes

Because our classification approach comprises four different criteria, it is necessary to use a four-dimensional notation to refer to public key certificates. More specifically, the term [⟨O⟩-⟨R⟩-⟨M⟩-⟨F⟩]-certificate refers to a certificate with owner ⟨O⟩, registration ⟨R⟩, storage medium ⟨M⟩, and functionality ⟨F⟩.

– Possible values for owner ⟨O⟩:
  - NP: Natural person
  - LE: Legal entity
  - M: Machine

– Possible values for registration ⟨R⟩:
  - NR: No registration
  - CR: Customer registration
  - R1: EBIA
  - R2: Authentication based on some existing identification and authentication mechanism
  - R3: Personal authentication based on a strong identification and authentication mechanism
  - R4: Personal authentication based on an official identification and authentication document, such as a national ID card or a passport

– Possible values for storage medium ⟨M⟩:
  - HW: Hardware
  - SW: Software

- S: Server

– Possible values for functionality $\langle F \rangle$:
  - A: Authentication
  - E: Encryption
  - S: Digital signatures

  These values can be combined, i.e., AE refers to authentication and encryption.

The classification scheme yields $3 \cdot 6 \cdot 3 \cdot 3 = 162$ certificate classes, and the criteria can even be further refined at will. Consequently, there are many certificate classes that are not used, and that do not make a lot of sense in practice. For example, if we use very strong registration mechanisms but employ server-based certificates, then the overall security is somehow difficult to evaluate.

In practice, it is possible and likely that we see only a small fraction of all possible certificate classes being offered by CSPs. As an example, only a few of these classes are overviewed and discussed:

– [NP-R4-HW-S]: Certificates from this class are issued for natural persons. Registration is as strong as possible and the private key is stored on a hardware device. Furthermore, the certificates can be used for digital signatures. Certificates from this class play a major role in digital signature legislations and discussions about electronic ID cards (comprising public key certificates).

– [NP-CR-SW-A]: Certificates from this class are issued for natural persons that are registered by the customer organization(s). The private key is stored in software, and the certificates can be used for authentication purposes. Certificates from this class are frequently used for single sign-on and secure firewall traversal.

– [M-CR-SW-AES]: Certificates from this class are issued for machines that are registered by the customer organization(s). The private key is stored in software, and the certificates can be used for authentication, encryption, and digital signatures.

It goes without saying that many other classes may be used and play an important role in practice.

5 Conclusions

In this paper we have argued that a unified (or even standardized) classification scheme is urgently needed to compare and put into perspective the various offerings of commercially operating CSPs (without having users read and compare all CPSs). This is particularly true if CSPs are to become successful. Against

this background, we proposed a four-dimensional classification scheme that can be used to briefly describe and characterize the offerings of CSPs. The scheme distinguishes between (i) who owns a certificate, (ii) how the certificate owner is registered, (iii) on what medium the certificate (or the private key, respectively) is stored, and (iv) what type of functionality the certificate is intended to be used for. There is a total of 162 possible certificate classes in the scheme, and some exemplary classes are briefly mentioned. If there is concensus about the look and feel of the major classes, one may introduce abreviations to refer to them (e.g., A, B, C, ... or 1, 2, 3, ...). In either case, it will be interesting to see what classes are actually populated and supported by commercially-operating CSPs.

References

1. Anderson, R., and M. Kuhn, Tamper Resistance — A Cautionary Note, Proceedings of the 2nd USENIX Workshop on Electronic Commerce, November 1996, pp. 1–11.
2. Anderson, R., and M. Kuhn, "Low Cost Attacks on Tamper Resistant Devices," *Proceedings of the 5th International Workshop on Security Protocols*, Springer-Verlag, LNCS 1361, 1997, pp. 125–136.
3. Anderson, R., "Why Cryptosystems Fail," *Communications of the ACM*, Vol. 37, No. 11, November 1994, pp.32–40.
4. Boneh, D., R. DeMillo, and R. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults," *Proceedings of EUROCRYPT '97*, Springer-Verlag, LNCS 1233, 1997, pp. 37–51.
5. Biham, E., and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," *Proceedings of CRYPTO '97*, Springer-Verlag, LNCS 1294, 1997, pp. 513–525.
6. Chokhani, S., et al., Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, RFC 3647, November 2003.
7. Diffie, W., and M.E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, IT-22(6), 1976, pp. 644–654.
8. Garfinkel, S.L., "Email-Based Identification and Authentication: An Alternative to PKI?" *IEEE Security & Privacy*, Vol. 1, No. 6, November-December 2003, pp. 20–26.
9. ISO/IEC 7498-2, Information Processing Systems—Open Systems Interconnection Reference Model—Part 2: Security Architecture, 1989.
10. Kocher, P., J. Jaffe, and B. Jun, "Differential Power Analysis," *Proceedings of CRYPTO '99*, Springer-Verlag,LNCS 1666, 1999, pp. 388–397.
11. Kocher, P., "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," *Proceedings of CRYPTO '96*, Springer-Verlag, LNCS 1109, 1996, pp. 104–113.
12. Lopez, J., R. Oppliger, and G. Pernul, "Why have public key infrastructures failed so far?," work in progress.
13. Oppliger, R., *Security Technologies for the World Wide Web, Second Edition*, Artech House Publishers, Norwood, MA, 2003.
14. Oppliger, R., *Contemporary Cryptography*, Artech House Publishers, Norwood, MA, 2005.
15. Oppliger, R., "Server-based Signatures: A Different Approach," work in progress.