December 1999

Towards A Unique World-wide Digital Certificate

Michael Fritscher
Vienna University of Economics and Business Administration, Austria

Towards A Unique World-wide Digital Certificate

Michael Fritscher

Vienna University of Economics and Business Administration, Austria
Department of Management Information Systems, A-1090 Wien, Augasse 2-6, Austria
Tel.: +43/1/313 36/4467, Fax: +43/1/313 36/746, E-mail: Michael.Fritscher@wu-wien.ac.at

Abstract

This paper discusses the importance of a unique digital certificate for the world wide use of public-key infrastructure and the impact such a unique digital certificate will have on the players. First, the basic concepts of public-key infrastructure are presented. Special interest is put on the concepts important for the use of identity-based digital certificates. Then, an overview of the Austrian situation in the international context is given and the key factors for the success of digital certificates are presented.

Digital certificates

There is a broad range of applications for digital certificates: electronic banking, electronic payment systems, e-mail communication, identification in communication with public authorities (e.g. tax declaration, court documents, electronic passports, public health service, etc.), electronic contracts, selective web access, selective database access, etc. In this context, several questions come up:

- Which players will provide the future infrastructure for digital certificates (governmental institutions, financial service providers, IT companies or others)?
- What are the key-factors for a successful provider of digital certificates?
- How should governments regulate the emerging market of digital certificates?
- Can nationally isolated solutions successfully survive?
- Is the combination of access-control, encryption and signature in one ”product” important for the success?

To get the answers to the above questions it is first necessary to understand the concepts of public-key infrastructure and then examine the behaviour of the players in this market.

Public-key cryptography

Public-key cryptography is a key-factor for the solution of the transaction security problems arising with the commercial use of the internet: *authenticity*, *integrity*, *confidentiality* and *non-repudiation* (Bhimani, 1996). Public-key algorithms are mainly used in two ways:

- **Encryption and decryption**
  Messages which are encrypted with the public key of the recipient can only be decrypted with the respective private key. In this way, only the possessor of the recipient’s private key can read the message which can be encrypted by any person, provided that the key management guarantees the correct distribution of the public key to the potential senders. In reality the message is first encrypted with a symmetric algorithm, and then the symmetric key is encrypted with the public key of the recipient. This is called a *digital envelope* (PKCS, 1993), (Kaliski and Kingdon, 1997). With public-key-encryption, the authenticity of the recipient and the confidentiality can be guaranteed.

- **Digital signatures**
  Messages can be signed encrypting a *message digest* (created by a hash function) with the private key of the sender. Any person in possession of the public key of the sender is in grade of verifying the signature by decrypting the message digest with the public key of the sender and comparing the result to the message digest of the received message created by the same hash function. Digital signatures guarantee the integrity of the message and the authenticity of the sender. Additionally, non-repudiation can be realised by the signing of both sender and recipient.

Key and certificate management

In the procedures described above, the distribution and management of the public key is the crucial point. It must be guaranteed that the key really belongs to the respective person (or e-mail address or authorisation role).

A means to guarantee this, is the use of digital certificates. They are digital documents containing the public key, the name of the possessor, the digital signature of the *certification authority* (CA) that issued the certificate and the certificate validity period. In this way the problem of key management is reduced to the public key of the CA. Once in possession of the trustworthy public key, the end user is able to verify all certificates issued by the certification authority. The function of a CA is therefore the verification of the identity of the certificate holder. This process follows the *certification practice statement* (CPS) of the CA (Chokhani and Ford, 1998).

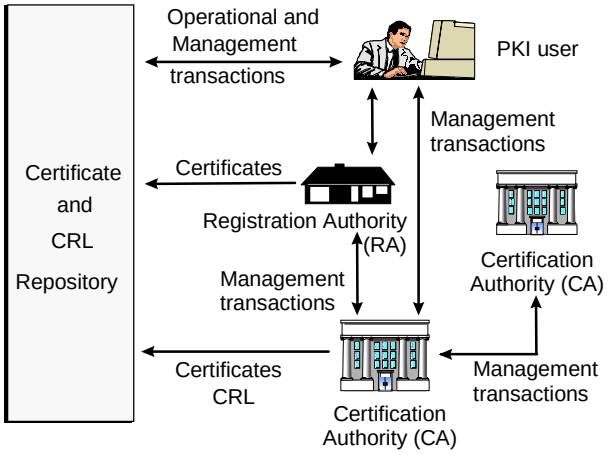

Figure 1. Certification and registration authorities
(Hously et al., 1998)

In the architectural model of the PKIX Working Group (see Figure 1) there is an additional optional system called *registration authority* (RA). The CA delegates certain management functions to the RA. Unexpired certificates can be revoked using a periodically-issued *certificate revocation list* (CRL). In recent research there are considerations to eliminate the CRL, because its handling has its drawbacks and there are other methods to verify the validity of a presented certificate (Rivest, 1998).

The certification of identity is only the simplest form of a certificate. With version 3 the digital certificates following the ISO X.509 standard are provided with extensions for the certification of attributes (ITU-T, 1993). Similar extensions are provided with role-based systems as the Simple Public Key Infrastructure (SPKI) (Ellison et al., 1997). With the use of application-specific extensions, the function of the certification authority is extended to the verification of the respective attributes of the certificate holders.

Trusted third parties and cross certification

The world-wide use of certificates causes the emerging of a large number of certificate issuers. One cause for this is that a certificate issuer needs a certain regional presence in order to verify the identity of a person. From this point of view, it makes sense that an organisation issuing certificates consists of a large number of locally operating entities, independent from each other. For the end users, the management of different trustworthy public keys is not applicable, because each of these would have to be transmitted in a secure way.

This problem can be solved by the use of *cross certificates* (ITU-T, 1993), (Nusser, 1998). These are certificates issued by a CA certifying another CA. In this way, an end user is able to verify a certificate issued by a CA whose public key was not directly transmitted to the end user. For the verification, there must only be a link via cross certificates to the CA whose trustworthy public key is with the end user. This link is also called *certification path* or *chain of trust*. The CA whose trustworthy public key is provided is called *trusted third party* (Rüppel and Wildhaber, 1995).

Using these mechanisms, a system can be built that consists of several certification authorities issuing certificates for individuals but also building links between each other using cross certificates. In an ideal situation, each end user is able to verify the certificates of any other person using only one trusted third party in this system. The combination of certification authorities linked to each other via cross certificates and the end users is called *public-key infrastructure* (Schneier, 1996).

The Austrian situation in the international context

In Austria, there are several institutions trying to be the first in providing a nation-wide infrastructure for digital signatures. There are activities in three fields:

1. Certification authorities offering certificates for clients, servers and developers: GlobalSign by Innovation Systems, AD-Cert by ARGE Daten and A-Sign by datakom Austria.
2. Public authorities are preparing for the use of digital signatures and certificates for the communication with the citizens. So, the ”Bundesrechenzentrum” (federal computing centre) takes steps to provide the necessary infrastructure.
3. Europay Austria, operator of the Austrian cash-dispensers, a very important player in the credit card business and the operator of the ”Quick” electronic wallet, plans to issue a signature card especially for financial services and uses the SET standard (SET, 1997) for credit card payment on the internet.

The co-operation with some of these key players in Austria helps to identify the key factors and to test the research results in practice.

On the juridical side there is a model law on electronic commerce issued by the United Nations Commission on International Trade Law (UNCITRAL, 1996), there are cryptography guidelines issued by the OECD (OECD, 1997), some US states have their own laws on cryptography or digital certification, there is a directive of the EU concerning a common framework for electronic signatures and in some member countries of the EU there are laws on digital certification. In Austria there is a draft (Mayer-Schönberger et al., 1999) for a law on digital signatures which is very near to the German law and decree. This draft provides a licensing authority that is with the Austrian Telekom-Control commission.

Key factors for the use of digital certificates

The different players (end users, public authorities, financial service providers, etc.) have different utility functions. The following are some examples of key factors for the players:

1. For end users the cost of the certificate, the simplicity of use, the variety of applications (interoperability) and the number of potential partners are key factors.
2. For public authorities a high security level for identity certification is important (e.g. electronic passport).
3. For financial service providers the cost of the system, the number of potential customers and the attributes certified by a certificate are important key factors.

With the utility functions of the players a model of the ”game of certification” with the adequate payoff matrices can be built to show different scenarios of the development of public-key infrastructure use.

Conclusions

As we have seen, the success of digital certificates does not only depend on the technical process of certification or on the key length (even if there are very important issues in these fields) but mainly on the ease of use and the variety of applications for the user and the service provider. So, it seems to be very important that the mass of the users (the typical consumers) is provided with a unique digital certificate to carry out all standard functions (secure e-mail, tax declaration, banking, payment, etc.). This way, the use of digital certificates can reach a critical level. To enable the interoperability of digital certificates cross certification between the different CAs is a crucial point. The client of a bank provided with a digital certificate issued by her bank has additional utility using this certificate also for other applications, e.g. private or official e-mail. For the service providers a world-wide public-key infrastructure implies new opportunities, new customers and new business fields.

References

Bhimani, A. "Securing the Commercial Internet". *Communications of the ACM*, 39(6)**,** pp. 29-35 1996.

Chokhani, S. and Ford, W. *Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework.* In http://www.ietf.org/html.charters/pkix-charter.html 1998.

Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B. and Ylonen, T. *Simple Public Key Certificate.* In http://www.clark.net/pub/cme/html/spki.html 1997.

Hously, R., Ford, W., Polk, W. and Solo, D. *Internet Public Key Infrastructure - Part 1: Certificate and CRL Profile. Internet-Draft.* In http://www.imc.org/draft-ietf-pkix-ipki-part1-11.txt 1998.

ITU-T *ITU-T Recommendation X.509: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework*. ITU, 1993 and ISO/IEC 9594-8 1993.

Kaliski, B. S. and Kingdon, K. W. *Extensions and Revisions to PKCS #7*. RSA Laboratories 1997.

Mayer-Schönberger, V., Pilz, M., Reiser, C. and Schmölzer, G. *Entwurf eines Gesetzes über den elektronischen Geschäftsverkehr und die digitalen Signaturen.* In http://www.medien-recht.com/digitale_signaturen.html 1999.

Nusser, S. *Sicherheitskonzepte für WWW-Informationssysteme*. Springer Verlag, Heidelberg 1998.

OECD *Cryptography Policy: The Guidelines And The Issues*. OECD 1997.

PKCS *Cryptographic Message Syntax Standard. Version 1.5*. RSA Laboratories 1993.

Rivest, R. L. "Can We Eliminate Certificate Revocation Lists?". In *Financial Cryptography, Second International Conference*(Ed, Hirschfeld, R.) Springer , Berlin, Anguilla, British West Indies, pp. 178-183 1998.

Rüppel, R. A. and Wildhaber, B. "Public Key Infrastructure - Survey and Issues". In *Trust Center - Grundlagen, rechtliche Aspekte, Standardisierung und Realisierung*(Ed, Horster, P.) Vieweg Verlag, Wiesbaden, pp. 197-212 1995.

Schneier, B. *Applied Cryptography - Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, Inc., New York 1996.

SET *Secure Electronic Transactions: Book 2: Programmer's Guide. Version 1.0.* In http://www.setco.org/set_specifications.html 1997.

UNCITRAL *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment.* In http://www.un.or.at/uncitral/english/texts/electcom/ml-ec.htm 1996.