An Infrastructure For Support Of Digital Signatures

Tomaž Klobučar and Borka Jerman-Blažič
Jožef Stefan Institute, Jamova 39, Ljubljana, Slovenia
Phone: +386 61 1773 900, Fax: +386 61 1232 118
E-mail: klobucar@e5.ijs.si

Keywords: digital signature, public-key infrastructure, technical framework, legal framework

Edited by: Cene Bavec and Matjaž Gams
Received: October 10, 1999 **Revised:** November 5, 1999 **Accepted:** December 14, 1999

In this paper, we present an infrastructure for support of digital signatures in the Information society. Technical aspects are briefly described and a short overview of several existing legal frameworks is given. Certification authorities, certificate policies, signature policies and certification practice statements are identified as important parts of the infrastructure.

1 Introduction

Provision of security is one of the most important issues in the Information society. Several security aspects should be taken care of when communicating on global computer networks. Confidential information must not be made available or disclosed to unauthorised subjects, and users must be able to authenticate other users or check that the source of data is as claimed. In addition, unauthorised data modification must be detectable, methods for the prevention of unathorised use of resources, including the prevention of use of a resource in an unauthorised manner must exist, and falsely denying of participation in certain activities should be prevented. These security requirements are characterised with the following concepts, known as security services: confidentiality, authentication, integrity, access control and non-repudiation. There exist several security mechanisms and structures for security provision, one of them being digital signatures, which are used to provide authentication, data integrity and non-repudiation.

A digital signature means data in electronic form which are attached to, or logically associated with, an electronic message and which serve to ascertain both the originator of the message and the fact that the message has not been modified since it left the originator. Digital signatures are used in various places in the Information society, for example in communication with public institutions (e.g. calls for tenders, exchange of application forms, tax declarations, transmission of legal documents), electronic buying and selling, electronic financial transactions, as well as for personal purposes, such as personal electronic mail, or for identification in the Internet. In order to use these signatures with equivalent legal effect as hand-written signatures in non-electronic documents, certain conditions have to be met. In the next two Sections, technical and legal aspects of digital signatures, and current activities in this field are briefly described. Conclusions are given at the end.

2 Technical framework

A technical framework describes a set of security mechanisms, technologies and technical standards that are used to support digital signatures. Management requirements for supporting those mechanisms are also included. Digital signature methods are based on a public-key technology, which has been widely recognised as a fundamental technology for providing secured Information society. Although the definition of digital signatures is technology neutral, public-key cryptosystems are in practice almost always used for signature creation and validation of signed data.

Two distinct keys are used in public-key cryptosystems - one for encryption and the other for decryption. Anything encrypted with the first key can only be decrypted with the second key. Although both keys are mathematically related, it is computationally unfeasible to derive one key from the other without additional (secret) information. One of the keys (public key) can thus be published, allowing everyone to perform encryption or signature validation with this key, while only a user knowing the corresponding private key can decrypt or sign a message.

There exist several different methods for generating digital signatures, most often being used DSS (Digital Signature Standard) [14] and RSA [17] in combination with one of the one-way hash functions, such as SHA-1 [15], RIPEMD-160 or MD5 [16]. Digital signatures are generally produced in a two step process. Firstly, the message is compressed using a one-way hash function which transforms the information into a string of fixed length, then this so-called message digest is encrypted with the user's private key. As the private key is known only to the originator then no one else could forge its signature. Every slightest change of the document after it being signed produces changes in the digital signature that make the signature not anymore valuable. The recipients verify the signature with the originator's public key.

In order to verify the signature, the recipient must first authenticate the originator's public key. The identity of the public key owner and public key integrity are guaranteed with public-key certificates. A public-key certificate is a digitally-signed data structure which securely binds a public key to the entity's identity. A digital signature is produced with the private key of a trusted entity, called a certification authority (CA), which vouches for the correctness of the information included in the certificate. The de-facto standard public-key certificate format is defined in ITU-T Recommendation X.509 [11]. The first two versions of this document, published in 1988 and 1993, described the version 1 (v1) and version 2 (v2) formats. Since then, several deficiencies have been found and new security requirements identified. As a result, optional extension fields were added into the version 3 format [9, 10], which was standardised in 1997. Besides a public-key and the name of its owner, an X.509 public-key certificate also contains the name of the issuer of the certificate, validity period, serial number and algorithm identifiers. Standard extensions in version 3 certificates define additional key and policy information, subject and issuer attributes, certification path constraints, and information about certificate revocation lists (CRLs). Supported extensions and their semantics for particular use are defined in certificate and CRL profiles. Two important profiles for the use of public-key certificates for digital signatures are "Internet X.509 PKI Certificate and CRL profile" [6] and "Internet X.509 PKI Qualified Certificates" [18]. The first document profiles the X.509 certificates and CRLs for the use in the Internet, while the second describes certificates which are qualified to support digital signatures in a context which is considered to be functional equivalent with hand-written signatures.

2.1 Public-key infrastructure

Certification authorities are an essential part of the infrastructure for the use of digital signatures. A system of certification authorities with supporting registration authorities (RAs) and other agents and servers that provide services that are needed if public-key-based technologies are to be used on a wide scale is called a public-key infrastructure (PKI). The core services of a PKI are registration and identification of users, issuance of certificates, directory services, certificate distribution, archiving services, revocation of certificates, publishing of CRLs, and time-stamping services.

Public keys can be used for different purposes and in different environments, such as military, commercial, research or educational. Since these environments do not have the same security requirements, there will certainly not exist a single public-key infrastructure for the whole Internet. At the moment, there are several, generally isolated and hierarchically structured public-key infrastructures in the world [1]. Most of them are governmental, such as the Government of Canada Public Key Infrastructure, or commercial and consisting only of a few certification authorities, e.g. Verisign or Thawte. A common world PKI for a business-to-business electronic commerce, named Identrus, is also in the process of building-up by several global financial institutions. In Europe, an ICE-TEL public-key infrastructure was established a few years ago with the aim to provide a large-scale public key certification infrastructure in a number of European countries for the use of security services based on public keys. The ICE-TEL (Interworking Public Key Certification Infrastructure for Europe) project was part of the 4th Framework Programme of European Community activities in the field of Research and Technological Development. Tools for the provision of the infrastructure, security toolkits and user tools (e.g. secured e-mail programs) were also developed during the project, which ended in February 1998.

The successor to this project, the ICE-CAR project (Interworking Public Key Certification Infrastructure for Commerce, Administration and Research) [8] from the same 4th EU Framework Programme, was launched in 1999 to foster the development of European-based security technology for the purpose of securing the growing applications of the Internet for administration, electronic commerce, intra-organisation communication, health care applications and research. Solutions to the problem of authenticity, integrity and privacy on the Internet are offered through the tools for secure communication, the provision of the public key infrastructure and the support of users of the PKI. One of ICE-CAR activities is also the transfer of security technologies and services to Central and Eastern European countries through the Security Technology Competence Centre for Central and Eastern European Countries (SETCCE). ICE-CAR is continually improving and enlarging the European PKI set up within the ICE-TEL through integration of public key based security services into applications which make use of the PKI.

A part of this infrastructure, which connects CAs from different European countries, is Slovenian certification authority SI-CA [13]. SI-CA, which has been certified by the ICE-CAR top-level certification authority, certifies individuals and other CAs in Slovenian academic, research, governmental and commercial organisation. Issued certificates for Web clients and servers can be used to secure Web transactions, while public-key certificates for e-mail help users to provide authenticity, integrity and confidentiality of their e-mail messages. Adopted ICE-TEL certificate policy, which has been assigned the unique object identifier 1.3.6.1.4.1.2712.10, specifies that the identity of the certificate applicants must be verified with official documents only, e.g. passports or personal id-cards, and that a personal presence of the applicant is required during verification. This part of the ICE-TEL certificate policy is very important, because it assures verifiers of digital signatures and other certificate users that the owners of the keys have been properly identified and authenticated before the certificate issuance.

2.2 Certificate policies and certification practice statements

Certificate policies are crucial for the operation of global public-key infrastructures since they define where, when and how the public-key certificates and public keys are used. In the X.509 Recommendation, a certificate policy is defined as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements." Certificate policies generally include basic information about the policy authority that defined the policy, community and certificate applicability, as well as certificate and CRL profiles, security requirements, requirements for subject identification and authentication, and obligations for CAs, RAs, owners of certificates and relying parties. A certificate policy may, for example, state that the keys for digital signatures must be stored on smart cards and can only be generated by the users themselves. Types of documents which are allowed to be signed can also be specified. Operational procedures of a CA are described in more detail in a CPS that is defined as "a statement of the practices which a certification authority employs in issuing certificates" [3]. Unfortunately, there is still no clear distinction between certificate policies and CPSs. Both will generally contain similar information - only that in policies this information will be less detailed. Each CPS is also specific to one CA, while certificate policies are widely supported by more than one CA. High-level topics which need to be part of certificate policies and certification practice statements are informally described in RFC 2527.

Applied certificate policies are identified in public-key certificates by unique, registered object identifiers. Knowledge about the policies is necessary during digital signature validation in order for users to evaluate the binding of a public key and the originator's identity, and to decide whether the key was meant to be used for a particular purpose or by a particular application. A user may, for example, not completely trust a certificate for the use in a financial transaction knowing that the CA that issued this certificate accepts no liability for its services and does not verify the identity of a certificate applicant with official documents. Certificate policies thus need to be evaluated by the users and compared against their personal requirements or local security policies. Unfortunately, policies are still written in natural language in different forms, which do not allow automatic processing. A format for a formal presentation of certificate policies was proposed in [12] to facilitate their comparison and evaluation. This format:

- Helps users in to decide more easily which policies satisfy their requirements, and which certificates can thus be accepted by their applications, e.g. secure e-mail programs or electronic commerce applications.

- Helps to modify applications to support accepted certificate policies, i.e. recognise them and conform to the semantics of the policies.

- Helps CAs in policy development. By selecting different explicit policy elements from a template they can prepare their policies in a more efficient way.

- Helps CAs to decide which certificate policies from other security domains can be considered equivalent.

- Helps CAs to decide whether the applicant CA's policy is in accordance with their policies.

The proposed specification of a formal certificate policy in ASN.1 is as follows:

```
CertificatePolicy      ::=  SEQUENCE{
 version                    Version DE-
FAULT v1,
 policyId                   OBJECT IDENTI-
FIER,
 policyDescription          DisplayText,
 generalInfo                GeneralInfo,
 issuerCAPolicy             Subpoli-
cyRules,
 subordinateCAPolicy [0]    SubpolicyRules
                              OPTIONAL,
 rAPolicy            [1]    SubpolicyRules
                              OPTIONAL,
 userPolicy          [2]    SubpolicyRules
                              OPTIONAL
}
```

A detailed description of the elements, their order relations and an algorithm for comparison of policies are omitted from this paper. Policies are distinguished on the basis of different levels of security control, different levels of thoroughness of applicant authentication, the complexity of operational procedures, and restrictions on certificate usage and applicability.

Certificate policies are therefore used to specify conditions which have to be met during the use of public-key certificates and public keys for digital signatures. There exist other rules which are specific to digital signatures and are not contained in the certificate policies. These rules are part of signature policies, which define the technical requirements on signature creation and validation. An ASN.1 specification of the signature policy is described in the document, prepared by ETSI TC Security [4]. This formal specification allows an electronic signature to be automatically verified against the signature policy to which it refers.

2.3 Technical standards

High level requirements for legally valid signatures will be defined by legal frameworks, which are briefly described in the next Section. There still needs a lot of work to be done in the area of standardisation before the exact technical rules, that will fulfill those high level requirements, can be specified. A report prepared by the EESSI (European Electronic Signature Standardisation Initiative) Expert Team [5] has identified several missing functional and quality standards, that are needed for the use of digital signatures. One of the required standards is a standard for trusted systems and products for digital signatures (signature creation and verification products). In addition, there is a need for standards for interoperability, that will for example define a standard syntax and encoding format for electronic signatures or a protocol to interoperate with a time stamping authority, and for standards for secure management of CAs and other service providers. When standards already exist, minimal security requirements need to be defined, e.g. algorithms and key lengths that are strong enough to resist calculation of the private signature key from the public signature key, or from the signature itself. Minimal security requirements generation and protection of private keys can be based on the FIPS PUB 140-1 (Security Requirements for Cryptographic Modules) standard, or one of existing security evaluation criteria, e.g. ITSEC (Information Technology Security Evaluation Criteria), TCSEC (Trusted Computer System Evaluation Criteria), CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) or a Common Criteria (CC). German regulation on digital signatures, for example, requires ITSEC E4 HIGH level for key generation and private key protection in the smart card.

3 Legal framework

Before the legal framework is discussed, we should first explain the difference between digital signatures and electronic signatures. The term electronic signature, which is widely used in several legislations, generally means any data in electronic form which serves as a method of authentication. Message Authentication Codes (MAC) or electronic pens are examples of electronic signatures methods. With this definition, digital signatures can be regarded as electronic signatures which meet additional requirements, i.e. they are capable of providing data integrity and uniquely identifying the subject that created a signature.

Several countries are in a process of updating their legal frameworks in order to regulate and incorporate recognition of signatures in electronic form. First legal frameworks for electronic or digital signatures were established in the U.S. a few years ago. The state of Utah was the first jurisdiction to enact the digital signature legislation in 1995, and many other states followed thereafter. On an international level, UNCITRAL (United Nations Commission on International Trade Law) adopted its Model Law on Electronic Commerce in 1996. Although it is not digital signature legislation, the Law influenced a number of national and international initiatives. In Europe, several countries, such as Germany with its Digital Signature Law and Digital Signature Ordinance, Italy or Austria, have already passed their digital signature legislation. Detailed summaries and comparisons of other existing and draft laws have been prepared by different institutions, for example by the Interdisciplinary Centre for Law and Information Technology at University of Leuven [7].

To facilitate the use of electronic signatures and to contribute to their legal recognition in EU member countries, European Commission published last year a proposal for a Directive on a community framework for electronic signatures. The Directive, which has been adopted by the European Parliament and the Council of the European Union in November 1999, establishes a legal framework for electronic signatures and certain certification services in order to ensure the proper functioning of the internal market. Although it tries to be technology neutral and covers all forms of electronic signatures, not only digital signatures, public key cryptography and certification authorities are mandated for so-called "qualified electronic signatures" (i.e. digital signatures) with legal equivalence to hand-written signatures. Only certificates called qualified certificates, which meet requirements defined in the Directive, can be used for qualified electronic signatures. The Directive also defines basic requirements for certification service providers issuing these certificates, requirements for secure signature-creation devices, and recommendations for secure signature verification. Certificate profile for qualified certificates is being specified in the IETF draft [18], that was already mentioned in Section 2. An importance of the use of digital signatures in electronic commerce to the EU Commission is also reflected in the V. Framework Programme of the European Community for research, technological development and demonstration (RTD). One of the key actions of the Programme is "New methods of work and Electronic Commerce" with the following prioritised areas: identification and authentication, secure electronic financial transactions and digital object transfer.

What about Slovenia? In Slovenia, we are still in the preparatory phase with a Draft law on electronic commerce and electronic signatures. It is expected that a legislation that is in accordance with the EU Directive will be enacted in a few years. However, it should be noted that the absence of legislation does not preclude parties from using digital signatures in bilateral communication. The parties are free to agree among themselves the terms and conditions under which they accept digitally signed data.

4 Conclusion

Digital signatures are one of the most important security mechanisms and structures in a secured Information society. There exist various types of signatures in electronic form, that can be used to provide authentication, data integrity or non-repudiation. However, it seems that at this time only digital signatures that are based on public-key cryptography can have, under certain technical and legal conditions, equivalent legal effect as hand-written signatures. In this paper, we have briefly described a technical framework required for support of digital signatures, that consists of a set of security mechanisms, technologies and technical standards. An emphasis was given on public-key infrastructures, certification authorities and certificate policies. We have also presented current activities for the standardisation of a legal framework.

References

[1] Anderson R., Crispo B., Lee J.H., Manifavas C., Matyas V. Jr., Petitcolas F.A.P., The Global Internet Trust Register 1999, MIT Press, Cambridge, MA, 1999.

[2] Baum M.S., Ford W., Secure electronic commerce: building the infrastructure for digital signatures and encryption, Prentice-Hall, 1997.

[3] Chokhani S., Ford W., Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527, 1999.

[4] European Telecommunications Standards Institute (ETSI), Electronic Signature Format, draft ETSI ES 201 733 v1.1.4, 1999.

[5] European Electronic Signature Standardization Initiative (EESSI), Final Draft of the EESSI Expert Team Report, 1999.

[6] Housley R., Ford W., Polk W., Solo D., Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, 1999.

[7] Interdisciplinary Centre for Law and Information Technology, K.U.University, The legal aspects of digital signatures, http://www.law.kuleuven.ac.be, 1998.

[8] ICE-CAR (Interworking Public-Key Certification Infrastructure for Commerce, Administration and Research) project, http://ice-car.darmstadt.gmd.de, 1999.

[9] ISO/IEC, Draft Amendment DAM 1 to ISO/IEC 9594-8 on Certificate Extensions, 1997.

[10] ISO/IEC, Final Proposed Draft Amendment on Certificate Extensions, 1999.

[11] ITU-T Recommendation X.509 (1993) | ISO/IEC 9594-8:1994, Information technology - Open Systems Interconnection - The Directory: Authentication framework.

[12] Klobučar T., Jerman-Blažič B., A formalisation and evaluation of certificate policies, Computer Communications 22 (1999), 12, pp. 1104-1110.

[13] Klobučar T., Jerman-Blažič B., SI-CA: agencija za certificiranje javnih ključev v Sloveniji, Varnost in zaščita v telekomunikacijskih omrežjih, Peta delavnica o telekomunikacijah, Brdo pri Kranju, 1997, Marko Jagodic, ur., Sašo Tomažič, ur., Ljubljana, Elektrotehniška zveza Slovenije, 1997 (In Slovene).

[14] National Institute of Standards and Technology (NIST), Digital Signature Standard, Federal Information Processing Standards Publication 186-1, 1998.

[15] National Institute of Standards and Technology (NIST), Secure Hash Standard (SHS), Federal Information Processing Standards Publication 180-1, 1995.

[16] Rivest R., The MD5 Message Digest Algorithm, RFC 1321, MIT in RSA Data Security, Inc., 1992.

[17] Rivest R., Shamir A., Adleman L., A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM, Vol. 21, No. 2, pp. 120-126, 1978.

[18] Santesson S., Polk T., Gloeckner P., Internet X.509 Public Key Infrastructure Qualified Certificates, Internet Draft, 1999.