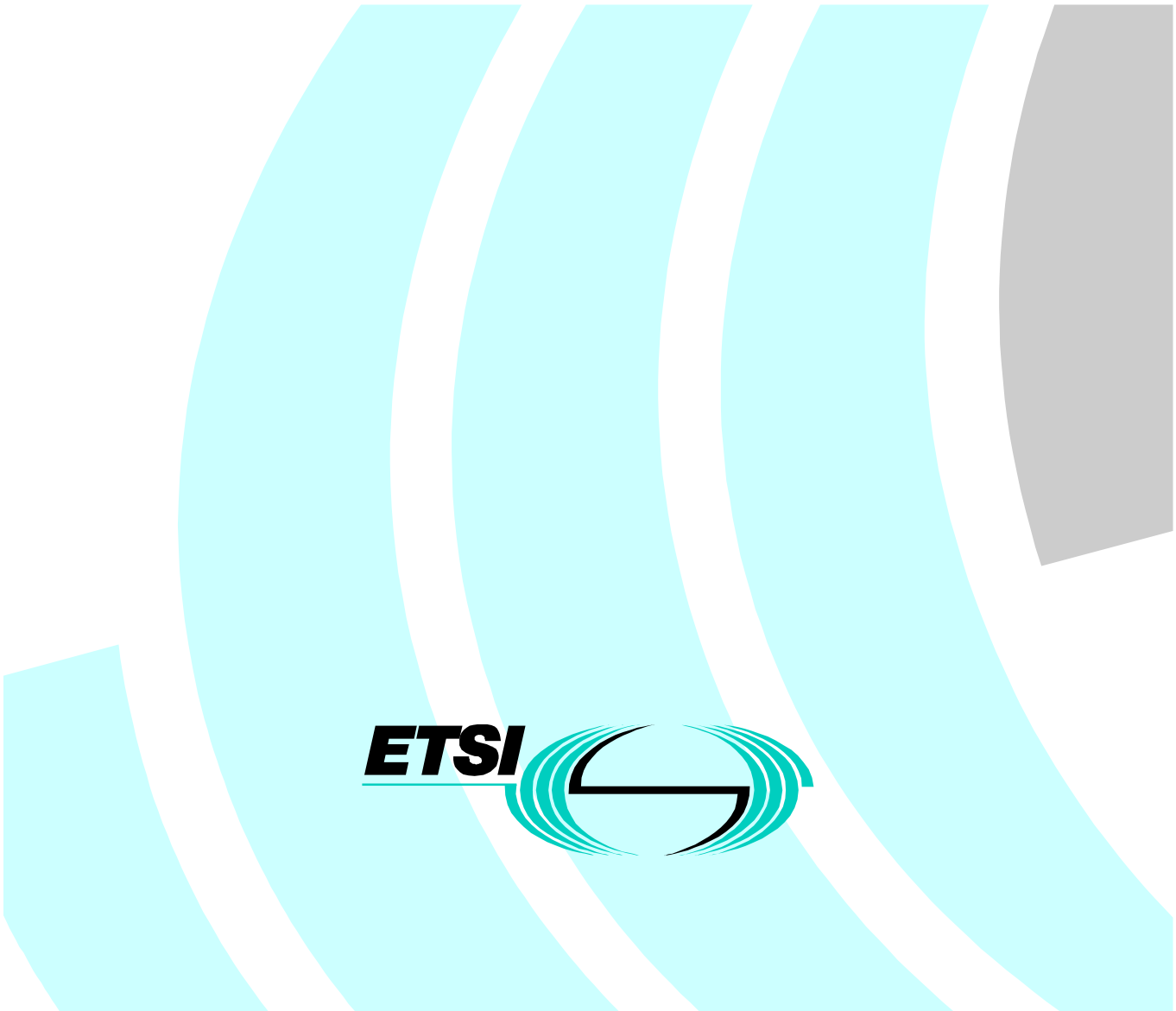
Draft TR 101 xxx V0.4.2 (1998-11)

Technical Report

Telecommunications Security; Electronic signature standardization report



Reference
<Workitem> (draft.PDF)

Keywords
<Security, Electronic signature>

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet
secretariat@etsi.fr
http://www.etsi.org

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical CommitteeSecurity (SEC) and provides the results of a study carried out by TC Security on Electronic Signature Standardization.

Introduction

Electronic Signatures – background

Open networks such as the Internet are of increasing importance for world-wide communication. They offer the possibility of interactive communication between parties who may not have pre-established relationships. They offer new business opportunities by creating tools to strengthen productivity and reduce costs, as well as new methods of reaching customers. Networks are being exploited by companies that wish to take advantage of new ways of doing business and new means of working, such as telework and shared virtual environments. Government departments are also using these networks in their interactions with companies and with citizens. Electronic commerce presents the European Union with an excellent opportunity to advance its economic integration.

In order to make best use of these opportunities, a secure environment with respect to electronic signature is needed. Several different methods exist to sign documents electronically varying from very simple methods (e.g. inserting a scanned image of a hand-written signature in a word processing documents) to very advanced methods (e.g. digital signatures using ‘public-key cryptography’). The term "Electronic Signature" is currently being used, but there is currently no agreed definition for it. It is thus very likely that different interpretations may exist behind this wording. Without considering the following as a formal definition, the following intuitive definition is given: an electronic signature is the electronic equivalent of a manual signature placed over a document. See the annex A: "What is an electronic signature ?" for a discussion of a possible more formal definition.

When digital signatures are used, the verification of the authenticity and integrity of data not necessarily prove the identity of the signer that created the electronic signature. How does for instance the recipient of a signed document know without ambiguity who the signer is or make sure that it is the one that he claims to be ? The recipient may therefore wish to obtain more reliable information on the identity of the signer. Such information can be given by the signer himself, issuing the recipient with satisfactory proof. Another way is to have it confirmed by a trust service provider (e.g. an authority trusted by one or more parties)."

1 Scope

The scope of this study considers the area of standardisation for electronic signatures. This concentrates on the requirements of the different European Member States and the emerging electronic commerce market taking account of the proposed Directive from the European Commission entitled ‘Framework for Electronic Commerce’.

The result of this study is to identify a prioritised list on electronic signature standardisation and a subsequent work programme for ETSI.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1]

[2]

3 Definitions and abbreviations

3.1 Definitions

3.2 Abbreviations

4 Electronic Signature related definitions

Today exist many sources of definition from ISO/IEC/ITU-T, UNICTRAL, European Commission, IETF and various other bodies. There is a need to have an agreed set of definitions to ensure a common conceptual basis can be established. Definitions for the following concepts need to be produced and/or universally accepted:

- **Electronic signature** (see the annex A);
- **Non-repudiation policy.** A set of criteria for the provision of non-repudiation services. More specifically, a set of rules to be applied for the generation and verification of evidence and for adjudication [ISO/IEC 13888-1: 1997];
- **Evidence**. Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action. NOTE - Evidence does not necessarily prove truth or existence of something (see proof) but contributes to establish proof [ISO/IEC 13888-1: 1997].

5 Technology dependent / independent aspects

This study covers both technology dependent and technology independent requirements for electronic signature standardisation. This includes those requirements necessary to achieve interoperability taking account of legal, trust and technical aspects.

6 Global Aspect

This study recognises the requirements for international inter-working and takes account of available results and on-going activities on electronic signatures, in particular in support of global electronic commerce. Standardisation in the area of electronic signatures should not be limited to just regional developments but must include international initiatives and standardisation activities e.g. within ABA, OECD, Open Group, ECMA, IEEE, IETF, ISO/IEC/ITU-T, UNCITRAL.

7 Standardisation requirements and existing work

7.1 Technology independent requirements and work

7.1.1 Non-repudiation policies

There seems to be no work being done in this area. A non-repudiation policy is necessary to successfully process electronic signatures. A major goal of non-repudiation is to solve disputes. The non-repudiation policy should identify the following issues:

- the various trust relationships and conditions that are applicable;
- the arbitrator that is able to settle disputes;
- the security mechanisms to be used;
- the conditions under which an electronic signature will be considered as being valid.

Current situation: The various constituents of a non-repudiation policy are not well identified. Once a security policy is defined, it needs to be referenced unambiguously and any user must be able to make sure that the content of the non-repudiation policy reflects what the issuer of that policy initially stated. How and where to retrieve such non-repudiation policies is not defined.

7.1.2 Types of actions or events recognized by the signer

The types of actions and events are unlimited. The following types of non-repudiation have already been identified in various committees:

- Non-repudiation of creation

  This service is intended to protect against an entity's false denial of having created the content of a message (i.e., being responsible for the content of a message). [ISO/IEC 13888-1: 1997]

- Non-repudiation of delivery

  This service is intended to protect against a recipient's false denial of having received the message and recognised the content of a message. [ISO/IEC 13888-1: 1997]

- Non-repudiation of knowledge

  This service is intended to protect against a recipient's false denial of having taken notice of the content of a received message. [ISO/IEC 13888-1: 1997]

- Non-repudiation of origin

  This service is intended to protect against the originator's false denial of having created the content of a message and of having sent a message. [ISO/IEC 13888-1: 1997]

- Non-repudiation of receipt

This service is intended to protect against a recipient's false denial of having received a message. [ISO/IEC 13888-1: 1997]

- Non-repudiation of sending

  This service is intended to protect against the sender's false denial of having sent a message. [ISO/IEC 13888-1: 1997]

- Non-repudiation of submission

  This service is intended to provide evidence that a delivery authority has accepted the message for transmission. [ISO/IEC 13888-1: 1997]

- Non-repudiation of transport

  This service is intended to provide evidence for the message originator that a delivery authority has delivered the message to the intended recipient. [ISO/IEC 13888-1: 1997]

Requirements: Other useful types of actions or events could be defined.

7.1.3 Role and / or name of the signer

7.1.3.1 Role

When signing a contract the role of the signer, e.g. Financial Director from the Delta Company, is more relevant than its name.

The concept of a role appears in the document IDUP which describes an API to handle evidences. There is also some work being done by ANSI and ISO in the area of attribute certificates able to handle the concept of role. This work is however not directly related to non repudiation policies.

Requirements: It needs to be explored when non repudiation policies may require the concept of role and how they can support it.

7.1.3.2 Name

At the moment, no naming scheme is specified for electronic signatures. That leads to the following key question: which technique should be used to point unambiguously to a person (or entity) that can be easily recognised and traced?

Let us illustrate the case with an example. The name 123456.789@compuserve.com is a unique and non-ambiguous name. A CA may respect the rule that it will never issue two certificates for two different persons with the same name. However, how can a verifier know who was indeed the signer when having access only to that information?

Unique and unambiguous names are a necessary condition to address the problem but not a sufficient condition.

At least, two directions may be taken:

a) The electronic signature contains the **full-distinguished name** of the signer, including the address, phone number, employment. This approach does not respect privacy but allows one to directly distinguish one signer from another signer;

b) The electronic signature contains a **pseudonym** in order to respect privacy. In such a case using the pseudonym and some look-up mechanism, it becomes possible to obtain additional attributes from a Trust Service Provider (TSP) about the signer such as his/her picture, date of birth that may allow to make sure that the pseudonym belongs to the "right" individual.

Requirements : A naming scheme for electronic signatures should be defined. When pseudonyms are used, mechanisms, procedures and legislation issues need to be defined which point unambiguously to a person (or entity) that can easily be recognised and located.

7.1.4 Time the recognition was made

The time a signature was made needs to be known securely to allow to settle disputes which are arising after this signature was made, e.g. in the case of a trust relationship being compromised or revoked.

Current situation: The problem has been addressed in general by ISO [Non repudiation Framework] by introducing the concept of a Time Stamping Authority. The IETF is currently defining a protocol to obtain a time stamping token from a Time Stamping Authority (TSA). However, the way non repudiation policies make use of the Time Stamping information has been left undefined.

Requirements: Non repudiation policies should specify when they require the use of Time Stamping Authorities and which accuracy is expected for the time of the electronic signature.

7.2 Technology Dependent Requirements

7.2.1 Policy and Practice Statements for TSPs

A Trust Service Provider (TSP) can be defined as:

- *An entity, which can be used by other entities as a trusted intermediary in a communication or verification process, or as a trusted information service provider.*

The TSPs discussed in the following subsections are relevant for electronic signature.

A draft document from the IETF PKIX Group [http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part4-03.txt] currently defines a certificate policy and certification practices framework for Certification Authorities but no document from the IETF exists today for the other TSPs.

There is also work done in the European Commission (COM (1998) 297/2) and UNCITRAL which is considering the circumstances under which an electronic signature is ‘secure’ and can be legally recognised. This work includes policies and practices for CAs and other TSPs mentioned below and should be taken into account in this area.

7.2.1.1 Certification Authorities

Certification Authorities (CAs), when used in the context of electronic signature, certify public verification keys by issuing "User Certificates".

No document exists today to cover only CAs generating signature certificates.

7.2.1.2 Registration Authorities

Registration Authorities act as intermediaries between users and CAs. They receive requests from users and transmit them to the CAs in an appropriate form.

7.2.1.3 Time Stamping Authorities

Time Stamping Authorities are mandatory for non-repudiation in case of key loss or key compromise. In practice, they provide a counter-signature to anyone, including a reliable time, over a hash and a hash identifier.

7.2.1.4 Certificate Repositories

Certificate Repositories (e.g. an X.500 Directory) hold User Certificates and Certificate Revocation Lists (CRLs). They are trusted to make that information accessible but are not responsible for the content or accuracy of the information they receive from the CAs or the RAs.

7.2.1.5 On-line Certificate Status Providers

The On-line Certificate Status Protocol (OCSP) (http://www.ietf.org/internet-drafts/draft-ietf-pkix-ocsp-05.txt] enables applications to determine the revocation state of an identified certificate. OCSP may be used to satisfy some of the

operational requirements of providing revocation information in a more timely way than is possible with CRLs. On-line certificate status providers can be seen as an alternative to the use of off-line CRLs. Examples include high-value funds transfer or the compromise of a highly sensitive key.

7.2.1.6 Privilege Attribute Authorities

The concept of Privilege Attribute Authority is coming from ECMA. A PAC (Privilege Attribute Certificate) is generated by an Authority that directly vouches the attributes of the user. It is a short-lived certificate (at most, valid a day) so that revocation of it is not needed. It may contain either a non repudiation identity or a public key to be used for the verification of digital signatures generated under the corresponding private key. The use of Privilege Attribute Authorities in the context of electronic signatures would need to be explored.

7.2.1.7 Attribute Authorities

The concept of Attribute Authorities is still being discussed. An attribute certificate is linked to a user certificate and contains some attributes relative to the user. It may be a short-lived certificate (at most, valid a day) so that revocation of it is not needed.

7.2.1.8 Data Certification Authorities

A Data Certification Authority verifies the correctness of specific data submitted to it (see draft document: ftp://ds.internic.net/internet-drafts/draft-adams-dcs-00.txt). It may support one or more of the following services:

- verify a digital signature together with a certification path, at a given time, against a trusted point and then provide back a Data Certification Token that contains the verification time and assurance that the submitted data was valid at that given time;
- verify a certification path, at a given time, against a trusted point and then provide back a Data Certification Token that contains the verification time and assurance that the submitted data was valid at that given time.

Requirements: Policies and practice statements should be developed for each kind of TSP. This would ease voluntary accreditation schemes.

7.2.2 Interoperability between users and TSPs

7.2.2.1 Certification Authorities

The interactions are defined by the PKIX group from the IETF in several documents, mainly:

- draft-ietf-pkix-ipki3cmp PKIX Certificate Management Protocols (CMP)
- draft-ietf-pkix-cmc PKIX Certificate Management Messages over CMS
- draft-ietf-pkix-cmmf PKIX Certificate Management Message Formats
- draft-ietf-pkix-crmf PKIX Certificate Request Message Format (CRMF)

Current situation: Work is in progress at the IETF (PKIX working group). This work is expected to fulfill the various needs.

Requirements: Standardised protocols are needed to allow interoperability between users and CAs. The work of the IETF should be monitored to make sure that the output documents are covering the needs. The document should be used as a basis to build a new document taking into consideration what is relevant to Electronic Signature only.

7.2.2.2 Registration Authorities

Current situation: The work of the IETF about the RAs is included in the set of documents mentioned above in subclause 7.2.2.1 about CAs.

Requirements: Standardised protocols are needed to allow interoperability between users and RAs. These IETF documents should be used as a basis to build a new document taking into consideration what is only relevant to RAs.

7.2.2.3 Time Stamping Authorities

Time Stamping Authorities are mandatory for non-repudiation in case of key loss or key compromise. In practice, they provide a counter-signature to anyone, including a reliable time, over a hash and a hash identifier. The IETF PKIX group defines the interactions with a TSA in the following document draft-adams-time-stamp-02.txt on the site:

- ftp://ds.internic.net/internet-drafts/

The name of the document is Time Stamp Protocols. It describes the format of the data returned by a **Time Stamp Authority** and the protocols to be used when communicating with it. The time stamping service can be considered as a Trust Service Provider (TSP), i.e. as one of the components that are necessary in building reliable non-repudiation services (see ISO/IEC 10181-5: Security Frameworks in Open Systems 'Non-Repudiation Framework'). An example of how to place a signature at a particular point in time, from which the appropriate certificate status information (e.g. CRLs), may be checked is given in the annex B.

7.2.2.4 Certificate Repositories

The interactions with certificate repositories are defined by the IETF PKIX group in the documents:

- draft-ietf-pkix-ipki2opp PKIX Operational Protocols - LDAPv2
- draft-ietf-pkix-ldapv2-schema PKIX LDAPv2 Schema
- draft-ietf-pkix-opp-ftp-http Operational Protocols: FTP and HTTP

Current situation: Work is in progress at the IETF (PKIX working group). This work is expected to fulfill the various needs.

Requirements: Standardised protocols are needed to allow interoperability between users and Certificate Repositories. The work of the IETF should be monitored to make sure that the output documents are covering the needs.

7.2.2.5 On-line Certificate Status Providers

The interactions with an OCSP are defined by the IETF PKIX group in the document: ftp://ds.internic.net/internet-drafts/draft-ietf-pkix-ocsp-03.txt.

Current situation: Work is in progress at the IETF (PKIX working group). This work is expected to fulfill the various needs.

Requirements: Standardised protocols are needed to allow interoperability between users and OCSPs. The work of the IETF should be monitored to make sure that the output documents are covering the needs.

7.2.2.6 Privilege Attribute Authorities

A protocol to interface with a PAA in order to obtain a PAC that contains specific attributes is defined in ECMA 219 (section 6.1). The format of the request would need to be transformed so that a PAC can be used for electronic signatures.

Requirements: There exists different ways to support the concept of roles, like the generation of ACs (Attribute Certificates) by Attribute Authorities. These various ways should be investigated and the protocols to obtain the adequate data structures should be defined.

7.2.2.7. Attribute Authorities

Drafts document are available from ANSI and ISO. The ISO document can be obtained from:

- ftp://ftp.bull.com/pub/OSIdirectory/Phoenix98Output/AttCertWD.doc

Current situation: The use of attribute certificates is one out of several ways being investigated to support the concept of roles for electronic signature.

Requirements: There exists different ways to support the concept of roles, like the generation of PACs (Privilege Attribute Certificates) by Privilege Attribute Authorities. These various ways should be investigated and the protocols to obtain the adequate data structures should be defined.

7.2.2.8 Data Certification Authorities

Current situation: A draft from the PKIX working group from the IETF is available [ftp://ds.internic.net/internet-drafts/draft-adams-dcs-00.txt]. It is unclear at this time whether the various services that are supported through the protocol are needed.

Requirements: An observer position should be taken for the time being.

7.2.3 Interoperability between TSPs

From the list of the seven TSPs identified above, only a few of them need to inter-operate between each other. There is no need for a RA to interact with another RA. In the same way, there is no need for a TSA to interact with a TSA. The two remaining cases to be considered are given in subclauses 7.2.3.1 and 7.2.3.2.

7.2.3.1 CA to CA

Cross-certificates may be established between CAs. A cross-certificate is a certificate issued by one CA to another CA, which contains a CA signature key used for issuing certificates. Two different aspects must be considered:

1) the protocol for a CA to obtain a *single* cross-certificate from another CA;

2) the trust conditions that are necessary for the issuance of a cross-certificate.

A CA may issue a certificate for another CA without any obligation for the other CA to reciprocate.

Current situation: The protocol for a CA to obtain a *single* cross-certificate from another CA is defined by the IETF PKIX group in the document:

- ftp://ds.internic.net/internet-drafts/draft-ietf-pkix-ipk3cmp-08.txt.

The conditions for the issuance of a cross certificate are not presently well defined.

Requirements: Standardised protocols for cross-certification between CAs should be developed. The work of the IETF should be monitored to make sure that the output document is covering the needs.

The conditions for the issuance of a cross certificate should be clarified, in particular:

- the rules that CAs will have to obey; and

- the way to handle information about the name forms that each CAs will be trusted to certify.

7.2.3.2 Certificate Repository to Certificate Repository

These protocols are dependent upon the type of repository, e.g. an X.500 Directory or a database from a vendor. Therefore the standardisation of these protocols is not security specific.

7.2.4 Portability

IDUP-GSS-API (Independent Data Unit Protection Generic Security Service Application Program Interface) specifies programmatic interfaces that allows to place and extract various data elements within a piece of evidence. Evidence is a data structure that can be used to support the concept of electronic signature (see subclause 7.2.2.3). The current draft is available at: ftp://ds.internic.net/internet-drafts/draft-ietf-cat-idup-gss-11.txt.

IDUP provides a level of abstraction that is independent from the underlying mechanism. The internal format of the evidence is NOT specified in the document. Therefore various security mechanisms can be used.

Evidence is encapsulated in a token that must include at its beginning a mechanism type (OID). This allows to know whether the following data structure which is mechanism specific can or cannot be understood.

When used for generating evidence, the evidence security policy (specified using an OID) is always specified either implicitly or explicitly. This means that the caller explicitly refers to a security policy that will have to be used by the verifier. This may, for example, refer to the terms of a contract.

The security policy itself may be used by an adjudicator when resolving a dispute. For example, the adjudicator may refer to the policy to determine whether the rules for generation of the evidence have been followed.

It is fundamental to be able to know when evidence was generated, so that it becomes then possible to know what were the security policy selected and which certificates were or were not revoked *at that time*. Since it is not possible to rely only on the date/time indicated by the signer, in practice **Time Stamping Authorities** will be used.

The APIs allow a verifier to extract not only the name of the signer but also the **role of the signer**, e.g. Financial Director from the Delta Company.

Requirements: The implementation of security mechanisms (e.g. as described above) should be supported by standardisation of object identifiers and concrete language bindings.

7.2.5 Interoperability between users

The use of *digital signatures* (not to be confused with *electronic signatures*) in order to support *off-line* electronic signatures is anticipated as the generic mechanism. The use of public key certificates is also anticipated.

In order to be able to verify a digital signature when public key certificates are used, it is necessary to be in the possession of a public key value from a CA, and also in the possession of its validity and its associated naming constraints. All that information may be carried in a structure called "self-signed certificate". That information may be considered as one of many components of the non-repudiation policy.

The implication of this is important: the non-repudiation policy specifies which CAs are adequate to be used. Those CAs which are not listed or do not belong to a chain of trust through the chaining of certificates, is therefore inadequate. This means that all those CAs will not be usable under a given security policy. Furthermore, nothing mandates a CA to establish a cross certificate with another CA.

In order to settle disputes, an Arbitrator will need the appropriate software or hardware to state whether a given electronic signature was valid or not at the time it was generated. It would be inappropriate to mandate a specific software for every category of evidence - therefore a standard verification engine able to use non repudiation security policy templates would be more appropriate.

Currently there exists no technique to allow a standard "verification engine" to take as initial inputs both the non repudiation security policy and an electronic signature and states whether or not that electronic signature was valid or not at the time it was generated.

Current situation: Presently, there is no mechanism defined to support electronic signature.

Requirements: Without the definition of a few mechanisms, interoperability cannot be achieved. Concrete token formats must be defined for candidate IDUP mechanisms.

7.2.5.1 Public key certificates

Electronic Signatures must be verifiable off-line, but may be generated off-line and/or on-line. The general accepted technique is to use *off-line public key certificates* issued by Certification Authorities (CAs) conforming to the standard X.509 v3 and/or the IETF draft document: ftp://ds.internic.net/internet-drafts/draft-ietf-pkix-ipki-part1-09.txt

A public key certificate may point to a *certificate policy*. This policy has often been misunderstood. It indicates the policy under which the certificate has been issued and the purposes for which the certificate may be used. It is possible to distinguish two cases:

- the certificate policy limits the use of the certificate to specific applications. An example is the SET example where a certificate issued by a bank shall be used to support the SET protocol but should not be used for another application;
- the certificate policy does not specify anything about applications that can use the certificate.

In the first case, the *usage is restricted by the CA to specific applications.* The conditions of use of the certificates by the applications are under the responsibility of the CA. It should be observed that such applications are not *CA neutral*.

In the later case, CAs are not aware of the applications making use of the certificates and thus the usage is *not* restricted to specific applications.

There are no guidelines available to handle the two cases, i.e. certificate policies limiting or not limiting the applications that can use a certificate.

Another problem to address is whether or not a CA with a given name is really trusted to certify a user name with a similar or different name form. "Naming constraints" are mandated by the standards but their use is not straightforward.

Requirements: Profiles in the above areas should be standardised to allow interoperability.

7.2.5.2 Unilateral / bilateral / multilateral electronic signatures

The basic definition of electronic signature implies only one signer. In the real world a contract is signed by, at least two persons, one or both of them being a company representative instead of an individual.

When two electronic signatures are involved, should these signatures be embedded or concatenated. If embedded, in which ordering ? When more than two electronic signatures are involved, how should that case be handled ?

There is no work to cover the case of bilateral/multilateral electronic signatures over the same contract.

Requirements: The case of bilateral/multilateral electronic signatures over the same contract should be specified.

7.2.5.3 Use of smart cards

In the draft paper from the European Commission COM (1998) 297/2 the terms "signature creation device" and "signature verification device" are used. A smart card could be such a device.

A signature creation device should carry signature key pairs: private keys and possibly the associated public key certificates.

A signature verification device as well as signature creation device should be able to carry ways to point securely to non-repudiation policies. Some of the information included in the non-repudiation policies will be "trust points", e.g. self-signed certificates from trusted root CAs.

Current situation: Some low-level APIs have been defined by RSA Inc. in the PKCS series to interface with a « security token ». Such a token may be a smart card. The format of the storage of data relevant to Electronic Signature verification within a smart card has not been addressed.

Requirements: Investigate if the PKCS # 11 document covers the needs of electronic signature and consider if work done in ISO/IEC SC 17 in this area should be taken into account.

7.2.6 Cryptographic functions

Two categories of cryptographic functions are relevant to Electronic Signature:

1) One way collision resistant hash function;

2) Asymmetric cryptographic algorithm.

In order to allow for interoperability it is important to support the same crypto functions. There exists many standards in this area (see the annex B). The set of cryptographic functions to use is dependent upon the purpose for which there are being used. Therefore no uniform choice can be made and that choice will be reflected in the other various documents identified in this report.

Current situation: At present and in the first category the use of SHA-1 seems to be dominant whereas in the second category the use of the DSA algorithm and the RSA algorithm is to be considered. In the near future the use of Elliptic Curves is likely to be important.

Requirements: Define which algorithms should be used from a European prospective and provide some rational for the choice (e.g. patents, performance for signature generation, performance for signature verification, size of the code, sizes of the keys). Consider whether the use of Elliptic Curves is mature enough and define which algorithm combinations will be relevant.

8 What needs to be done?

This section identifies some of the standardization efforts that would need to be undertaken in the area of Electronic Signatures. No assumption is made whether all, some or none of the items that are identified should be addressed by the ETSI or other standardization groups, e.g. within CEN or CENELEC.

8.1 Technology Neutral Requirements

8.1.1 The non repudiation policy

Work needs to be done to define the constituents of a non repudiation policy and to unambiguously reference a non-repudiation policy. The use of object identifiers (OIDs) is anticipated.

Work needs to be done to make sure that the content of the non-repudiation policy reflects what the issuer of that policy initially stated. The use of off-line digital signatures is anticipated.

Work needs to be done to say how/where to retrieve such non-repudiation policies. The use of URLs is anticipated as one of the various means.

8.1.2 Types of actions or events recognized by the signer

Work needs to be done to define useful types of actions or events where repudiation is not possible.

8.1.3 Role and/or name of the signer

8.1.3.1 Role

Work needs to be done to define when and how non repudiation policies will support the concept of roles.

8.1.3.2 Name

Work needs to be done to specify the naming schemes to be used.

When pseudonyms are used, the mechanisms, procedures and legislation issues to point unambiguously to a person (or entity) that can be easily recognized and located need to be defined.

8.1.4 Time the recognition was made

The use of time stamping information for securing electronic signatures needs to be specified for each electronic signature mechanism. This topic needs to be addressed in subclause 8.5.1.

8.2 Technology Dependent Requirements

8.2.1 Policy and Practice Statements for TSPs

It is important to produce Policy and Practice Statements for each kind of TSP. This would ease voluntary accreditation schemes.

8.2.1.1 Certification Authorities

Develop a profile for CAs providing digital signature keys only using the framework document from the IETF that covers all kinds of keys. In particular, define the conditions for the issuance of a cross-certificate.

8.2.1.2 Registration Authorities

Develop Policy and Practice Statements for Registration Authorities

8.2.1.3 Time Stamping Authorities

Develop Policy and Practice Statements for Time Stamping Authorities

8.2.1.4 Certificate Repositories

Develop Policy and Practice Statements for Certificate Repositories

8.2.1.5 On-line Certificate Status Providers

Develop Policy and Practice Statements for On-line Certificate Status Providers

8.2.1.6 Privilege Attribute Authorities

It may be too early to develop Policy and Practice Statements for Privilege Attribute Authorities. Some technical work on this topic will be necessary before being able to address this topic which is considered as a longer-term issue.

8.2.1.7 Attribute Authorities

It may be too early to develop Policy and Practice Statements for Attribute Authorities. Some technical work on this topic will be necessary before being able to address this topic which is considered as a longer-term issue.

8.2.1.8 Electronic Notaries

It may be too early to develop Policy and Practice Statements for Electronic Notaries. Some technical work on this topic will be necessary before being able to address this topic which is considered as a longer-term issue.

8.2.2 Interoperability between users and TSPs

Users will need to use standardized protocols to communicate with the various TSPs that have been identified. The case of each TSP is addressed hereafter.

8.2.2.1 Certification Authorities

Provide a profile of the IETF protocols. Provide additional information about the issuance of a cross-certificate

8.2.2.2 Registration Authorities

Provide a profile of the IETF protocols.

8.2.2.3 Time Stamping Authorities

No action to be done.

8.2.2.4 Certificate Repositories

Provide a profile of the IETF protocols.

Define new protocols with a finer granularity than LDAP allowing appropriate certificates to be obtained according to search criteria like certificate validity, key usage.

8.2.2.5 On-line Certificate Status Providers

Provide a profile of the IETF protocols.

8.2.2.6 Privilege Attribute Authorities

When the concept will be stabilized, protocols to interface with Privilege Attribute Authorities should be defined.

8.2.2.7 Attribute Authorities

When the concept will be stabilized, protocols to interface with Attribute Authorities should be defined.

8.2.2.8 Electronic Notaries

When the concepts will be stabilized, protocols to interface with various kinds of 'Electronic Notaries » should be defined.

8.2.3 Interoperability between TSPs

Only a few TSPs need to inter-operate between each other using a specific protocol. The two cases to be considered are: CA to CA and Certificate Repository to Certificate Repository.

8.2.3.1 CA to CA

A profiling of the IETF document might need to be considered.

8.2.3.2 Certificate Repository to Certificate Repository

This topic is not security specific. However, replication and addressing through referrals using various communication means has to be considered. A selection of mechanisms and protocols would need to be considered.

8.2.4 Portability

In order to implement the IDUP-GSS-API atop existing, emerging, and future security mechanisms, the following is necessary:

- object identifiers must be assigned to candidate IDUP-GSS-API mechanisms and the name types which they support; and
- Concrete language bindings (e.g. C-bindings) are required for the programming environments in which the IDUP-GSS-API is to be employed. [This work is likely to be done within the IETF PKIX WG].
- a minor addition would be to allow knowing which IDUP mechanisms are locally supported and their characteristics in order to load the appropriate software. [This work could be done within the IETF PKIX WG].

8.2.5 Interoperability between users

Define IDUP mechanisms, i.e. electronic signature token formats, to support the generation and verification of evidences.

8.2.5.1 Public key certificate and CRLs formats

A profiling of public key certificates containing keys dedicated to non-repudiation only, (i.e. with the key usage non-repudiation bit set) would need to be considered. The documents from the IETF should be used as an initial start.

A profiling of CRLs might also need to be considered. The documents from the IETF should be used as an initial start.

A selection of the mandatory cryptographic algorithms and hash functions to be used for public key certificates and CRLs should be made. Candidate algorithms include RSA, DSA, EC-DSA, SHA-1 and MD5.

Some guidelines to handle the cases of certificate policies limiting and not limiting the applications that can use a certificate should be provided.

More work on naming constraints needs to be considered. The issue to address is whether or not a CA with a given name can be trusted to certify a user name with a similar or different name form. "Naming constraints" are mandated by the standards but their use is not straightforward.

8.2.5.2 Unilateral / bilateral / multilateral electronic signatures

The case of bilateral/multilateral electronic signatures over the same contract needs to be specified.

8.2.5.3 Use of smart cards

Work needs to be done to specify the use of smart cards in combination with both a PKI (Public Key Infrastructure) and electronic signatures. More precisely, smart cards may need to be loaded with private key(s), public key certificates and some ways to point securely to non-repudiation policies. The loading procedure and the data formats need to be specified.

The use of standardized low-level APIs, such as PKCS # 11, is to be considered. The work done in ISO/IEC SC 17 should be investigated to check whether it is relevant to be used in the context of electronic signatures.

8.2.6 Cryptographic-functions

The combinations of the one-way collision-resistant hash algorithms and asymmetric signature algorithms that should be used from a European prospective should be identified. Some rational for the choice (e.g. patents, performance for signature generation, performance for signature verification, size of the code, sizes of the keys) should be given. The use of Elliptic Curves should also be considered. Such choices should be reflected in the various other documents.

9 Recommendations and conclusions

9.1 Major areas of standardisation where work needs to be carried out

The following list of seven topics has been identified by the ETSI TC Security as needing particular attention and prompt actions from the ICTSB.

- Naming conventions and constraints;
- Format of public key certificates and CRLs;
- Format of Electronic Signature tokens;
- Selection of protocols to inter-operate with TSPs;
- Non repudiation policy;
- Security Policy Practice statements for TSPs;
- Use of smart cards for Electronic Signature.

9.1.1 Naming conventions and constraints

Procedures and legislation issues need to be defined in order to unambiguously identify a signer. A naming scheme for electronic signatures should be defined. That scheme must support the use of pseudonyms as well as of hierarchical names. The forms of such hierarchical name forms need to be specified. The identification must finally allow to point unambiguously to a person (or entity) that can be held responsible for its electronic signature, easily recognised (e.g. by looking at its public or private attributes) and located (e.g. by obtaining its private address or the name of its company).

NOTE: This topic affects the format of public key certificates and format of electronic signature tokens topics.

More work on naming constraints needs to be considered. The issue is whether or not a CA with a given name can be trusted to certify a user name with a similar or different name form.

NOTE: This topic is strongly related to trust relationships.

9.1.2 Format of public key certificates and CRLs

A profiling of public key certificates and CRLs containing keys dedicated to non-repudiation only would need to be considered. The documents from the IETF may be used as an initial start. A selection of the mandatory cryptographic algorithms and hash functions to be used for public key certificates and CRLs should be made.

Some guidelines to handle the cases of certificate policies limiting and not limiting the applications that can use a public key certificate should be provided.

9.1.3 Format of Electronic signature tokens

Electronic signature token formats need to be defined to support the concept of evidence. The case of bilateral / multilateral electronic signatures over the same contract needs to be specified. A selection of the mandatory cryptographic algorithms and hash functions to be used for Electronic signature tokens needs to be made.

9.1.4 Selection of protocols to inter-operate with TSPs

Standardised protocols are needed to allow interoperability between users and TSPs. A particular attention should be made on interoperability with Certificate Repositories.

9.1.5 Non repudiation policy

The various constituents of a non repudiation policy need to be identified. Unambiguous references pointing to well defined non-repudiation policies have to be defined. How and where to retrieve such non-repudiation policies should be defined. Finally, once such a reference is being obtained, it is important to specify how to make sure the data reflect what the issuer of the policy initially stated.

NOTE: This topic is strongly related to trust relationships.

9.1.6 Security Policy Practice statements for TSPs

It is important to produce Policy and Practice Statements for each kind of TSP. This would ease voluntary accreditation schemes. Since no work is currently available for Time Stamping Authorities (TSAs), the definition of Policy and Practice Statements for a TSA would need to be considered with a high priority. The subset applicable to Registration Authorities (RAs) should also be specified.

NOTE: This topic is strongly related to trust relationships.

9.1.7 Use of smart cards for Electronic Signature

Smart cards are expected to be used for electronic signatures. It is therefore important to specify their use in combination with a PKI (Public Key Infrastructure).

Smart cards need to be loaded with private key(s), public key certificates and some ways to point securely to non-repudiation policies. The loading procedure and the data formats need to be specified.

The use of standardized low-level APIs to allow electronic signature enabled applications to interface with any kind of smart card is to be considered.

9.2 Specific work items relevant to the work of ETSI

9.2.1 Overview

Following, the different work items considered in subclause 9.1 (and before in the document) are discussed in relation to ETSI, and what work ETSI and especially ETSI TC Security could do in these areas:

Naming Conventions and Constraints, Format of Public Key Certificates and CRLs, and Format of Electronic Signature Tokens

A lot of the work that is currently done in these areas for TCP/IP applications (as stated in subclauses 7.2.4, 7.2.5.1, 8.2.4 and 8.2.5.1 of this report) is done by IETF. The work in these three areas is closely related (as already stated in subclause 9.1.3), and it seems appropriate to use the TCP/IP related work carried out by IETF, with appropriate amendments to ETSI needs since IETF is not carrying out telecommunication related work. The work setting general conventions for applications involving any communications (and any protocols), as being carried out by ITU-T Study Group 7[1] and the ITU-T group dealing with electronic commerce should be taken into account.

Selection of Protocols to Inter-operate with TSPs

The existing work being done related to the interoperability between users and TSPs for TCP/IP applications is described in subclauses 7.2.2 and 8.2.2. It is:

- either done by IETF, as it is the case for CAs (subclause 7.2.2.1), RAs (subclause 7.2.2.2), TSAs (subclause 7.2.2.3), Certificate Repositories (subclause 7.2.2.4), and On-line Certificate Status Providers (subclause 7.2.2.5);
- or the concepts are fairly new and need to be stabilised, as stated in subclauses 8.2.2.6, 8.2.2.7 and 8.2.2.8 for the Privilege Attribute Authorities, Attribute Authorities and Electronic Notaries.

Again, it should be noted that IETF is not doing telecommunications related work, so the work being done by ITU-T in its relevant subgroups should be considered. It should also be noted that any work that is done with the aim to achieve interoperability cannot be done within one single group but should take into account the work being carried out in the different groups like ISO/IEC which is covering electronic commerce, GII, security techniques, management standards, and IETF and ITU-T, as mentioned above.

Non-Repudiation Policy and Security Policy Practice Statements for TSPs

Both topics are important for the widespread use of electronic signatures, but there is very little scope for standardisation work in the areas of non-repudiation or security policies for the following reasons:

All policies dealt with on a high level, which are aimed at giving conditions for non-repudiation or being valid for a large group of TSPs, need as a basis some agreements in the various activities taking place nationally and internationally. This includes the consideration of national laws (e.g. the laws in operation in Germany, Italy, and soon in other countries like UK), the European directive, the OECD Cryptographic Policy Guidelines, the UNCITRAL activities, etc. It will be very difficult for ETSI to achieve harmonised solutions for the trust in and recognition of electronic signatures as long as the various national and international activities are not harmonised.

All non-repudiation or security policies developed on a lower level (for one or more organisations) are specific for the organisation or group of organisations that is developing it. Standards cannot set policies - the most standards could do is to generally list the topics a non-repudiation or security policy should cover.

Use of Smart Cards for Electronic Signatures

---

[1] Collaborative work in done in ITU-T SG 7 and ISO/IEC SC27 WG 1on labels and security identification objects.

Smart cards are dealt with in several groups, like in ETSI (SMG 10), in CEN (TC 224) and in ISO/IEC SC 17. There is also TC 251 in CEN (Healthcare), where a digital signature algorithm was standardised and work on smart cards in combination with that is carried out. Therefore, it is recommended that the status of the various standardisation activities in the area of smart cards for electronic signatures of these groups is checked; according to the results of this check, these groups could take up the work of specifying the use of smart cards in combination with PKI and electronic signatures.

9.2.2 Conclusions

The results of the study has identified the following major areas of standardisation, harmonisation and policy development that need to be considered:

- naming conventions and constraints;
- format of public key certificates and CRLs;
- format of electronic signature tokens;
- selection of protocols to inter-operate with TSPs;
- non-repudiation policy;
- security policy practice statements for TSPs;
- use of smart cards for electronic signature.

The study concludes that the following is a specific work item relevant to the work of ETSI which can be dealt with in the short term:

- electronic signature standardisation for electronic commerce in particular for business to business transactions, focusing on the application of signatures for purchasing requisition, contracts, and invoices.
- areas to be covered include the first four topics from the list above, namely:

    1) Naming conventions and constraints;
    2) Format of public key certificates and CRLs;
    3) Format of Electronic Signature tokens;
    4) Selection of protocols to inter-operate with TSPs.

The other items in the list above are either for further study and consideration or will be dealt with in other fora.

Annex A: What is an electronic signature?

It appears fundamental to agree on a definition of "electronic signature". The difficulty of this task should not be under estimated. The following definition is considered to be a start, but more discussions would be needed.

Electronic signature: evidence in a digital form that can be processed to get confidence that some event or action has been explicitly endorsed under a non repudiation security policy, at a given time, by a signer under a name and/or a role.

This definition is addressing four fundamental elements that need to be considered:

- the non repudiation policy;
- the type of action or event that is recognised by the signer;
- the role of the signer (its name is not always needed) and;
- most of all, the time this recognition was made.

1) The non repudiation policy

Unless the non repudiation security policy is known, an electronic signature cannot be processed. A major goal of non repudiation is to solve disputes. So that an arbitrator is able to settle the disputes must be identified in the non repudiation security policy. Then after the mechanisms allowed to be used in accordance with the security policy must be identified. The next step is to indicate the conditions able to state that the electronic signature will or will not be considered as valid, many of them being mechanism dependent.

2) The types of actions or events recognised by the signer

The types of actions and events are unlimited. Under the same security policy different kinds of events or actions may be recognised: they must be clearly identified.

3) The role and/or name of the signer

When the employee from a company is signing a contract their role as a signer, e.g. Financial Director from the Delta Company, is more important than their name. When an individual is signing a document, the key issue is to unambiguously identify that person (or entity) that can be easily recognised and traced.

4) The time this recognition was made

Unless the signature time may be securely known, it would be impossible to settle a dispute should the private signature keying information be compromised and revoked.

Other definitions

European Commission: The document COM (1998) 297/2 ("Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. Proposal for a European Parliament and Council Directive on a common framework for electronic signatures") proposes a definition which attempts to make a difference between an "electronic signature" and a "digital signature".

A "digital signature" is defined in of ISO 7498-2, section 3.3.26 as:

> *"Data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient."*

"Electronic signature" has not been defined up to now and should not be confused with *digital signature* . The proposed definition contained in the document COM (1998) 297/2 is as follows:

1) **"~~electronic signature~~"** ~~means a signature in digital form in, or attached to, or logically associated with, data~~ and used by a signatory to indicate that signatory's approval of the content of that data and which meets the following requirements:

a) is uniquely linked to the signatory;

b is capable of identifying the signatory;

c is created using means that the signatory can maintain under his sole control; and

d is linked to the data to which it relates in such a manner that it is revealed if the data is subsequently altered.

2) **"Signatory"** means a person who creates an electronic signature.

3) **"Signature creation device"** means unique data, such as codes or private cryptographic keys, or a uniquely configured physical device, which is used in creating an electronic signature.

4) **"Signature verification device"** means unique data, such as codes or private cryptographic keys, or a uniquely configured physical device, which is used in verifying the electronic signature.

5) **"Qualified certificate"** means a digital attestation which links a signature verification device to a person, confirms the identity of that person and meets the requirements laid down in Annex I of COM (1998) 297/2.

6) **"Certification service provider"** means a person who or entity which issues certificates or provides other services related to electronic signatures to the public.

7) **"Electronic signature product"** means hardware or software, or relevant components thereof, which are intended to be used by a certification service provider for the provision of electronic signature services.

The current proposed definition has several problems:

1) it does not follow the general rule that a definition should be contained in one or two sentences at most;

2) some statements are not appropriate;

3) it is missing some key concepts.

From the first sentence *"a signature in digital form"* seems equivalent to *"a digital signature"*. This could lead to confusion.

A language point: the word *"signatory"* has rather an official political meaning in English. The Oxford Shorter English Dictionary defines it as: *"A party or especially a State that had signed an agreement or especially a treaty"*. It would be better to say *"signer"*, which is a perfectly good English word meaning exactly what it seems to mean.

The *"approval of the content of that data"* is one of the numerous recognition that can be accomplished by a signer. Another example would be an acknowledge of receipt of a letter (without looking at its content). That case would not be covered by the proposed definition.

The item b) would not be applicable when pseudonyms are used.

The item c) would not be practical in the real world, since it would be impractical to mandate to each signatory to maintain a full computer under its sole control.

An *"electronic signature"* definition should be trying to define what a verifier can assume, independent of signing mechanism, rather than define what the signing process is. This is a useful approach for two reasons:

1) it can then form a rational basis for the legal commitment that can be associated with something that is signed;

2) it's all that can be done anyway, since the definition must be technology independent and no assumptions can be made about the circumstances under which the signature was made.

This proposed definition is lacking to address the four following fundamental elements, i.e. the non repudiation policy, the type of action or event that is recognized by the signer, the role of the signer (its name is not always needed) and most of all, the time this recognition was made.

UNCITRAL

UNCITRAL also differentiates between an *"electronic signature"*, an *"Enhanced Secure electronic signature"* and a *"digital signature"*:

Article 1. Definitions

For the purposes of these Rules:

(a) "**Electronic signature**" means data in electronic form in, affixed to, or logically associated with, a data message, and [that may be] used to [identify the signer of the data message and indicate the signer's approval of the information contained in the data message][satisfy the conditions set forth in article 7(1)(a) of the UNCITRAL Model Law on Electronic Commerce];

(b) "**[Enhanced][Secure] electronic signature**" means an electronic signature which [is created and][as of the time it was made] can be verified through the application of a security procedure or combination of security procedures that ensures that such electronic signature:

(i) is unique to the signer [for the purpose for][within the context in] which it is used;

(ii) can be used to identify objectively the signer of the data message;

(iii) was created and affixed to the data message by the signer or using a means under the sole control of the signer; [and]

[(iv) was created and is linked to the data message to which it relates in a manner such that any change in the data message would be revealed].

(c) **Digital signature**

Variant A:

"Digital signature" means an electronic signature created by transforming a data message using a message digest function, and encrypting the resulting transformation with an asymmetric cryptosystem using the signer's private key, such that any person having the initial untransformed data message, the encrypted transformation, and the signer's corresponding public key can [accurately] determine:

(i) whether the transformation was created using the private key that corresponds to the signer's public key; and

(ii) whether the initial data message has been altered since the transformation was made.

Variant B:

"Digital signature" is a cryptographic transformation (using an asymmetric cryptographic technique) of the numerical representation of a data message, such that any person having the data message and the relevant public key can determine:

(i) that the transformation was created using the private key corresponding to the relevant public key; and

(ii) that the data message has not been altered since the cryptographic transformation.

Annex B: Existing standards

B.1 Cryptographic-algorithms: hash-functions

The following work has been done in the area of hash functions:

1) ISO/IEC 10118-1 (1994): Hash-functions – Part 1: General. ISO/IEC 10118-1 contains definitions and describes basic concepts.

2) ISO/IEC 10118-2 (1994): Hash-functions – Part 2: Hash-functions using an n-bit block cipher algorithm. ISO/IEC 10118-2 specifies two ways to construct a hash-function from a block cipher.

3) ISO/IEC 10118-3 (1997): Hash-functions – Part 3: Dedicated Hash-functions. ISO/IEC 10118-3 specifies the following dedicated hash-functions:

   - SHA-1 (→ FIPS 180-1)
   - RIPEMD-128
   - RIPEMD-160.

4) ISO/IEC FCD 10118-4: Hash-functions – Part 4: Hash-functions using modular arithmetic. Status: Final Committee Draft; Expected publication date: 1998 ISO/IEC 10118-4 specifies ways to construct a hash-function from a modular multiplication.

5) Internet RFC 1320 (PS 199?): The MD4 Message Digest Algorithm. RFC 1320 specifies the hash-function MD4. Today, MD4 is considered out-dated.

6) Internet RFC 1321 (I 1992): The MD5 Message Digest Algorithm. RFC 1321 (informational) specifies the hash-function MD5.

7) FIPS Publication 180-1 (1995): Secure Hash Standard. FIPS 180-1 specifies the Secure Hash Algorithm (SHA), dedicated hash-function developed for use with the DSA. The original SHA published in 1993 was slightly revised in 1995 and renamed SHA-1.

8) ANS X9.30-2 (1997): Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry – Part 2: The Secure Hash Algorithm (SHA-1). X9.30-2 specifies the ANSI-Version of SHA-1.

9) ANS X9.31-2 (draft): Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry – Part 2: Hash Algorithms. X9.31-2 specifies ??? - to be added.

B.2 Cryptographic-algorithms: digital signature algorithms

The following work has been done in the area of digital signature mechanisms:

1) FIPS Publication 186 (1994): Digital Signature Standard. NIST's *Digital Signature Algorithm* (DSA) is a variant of ElGamal's Discrete Logarithm based digital signature mechanism. The DSA requires a 160-bit hash-function and mandates SHA-1.

2) IEEE P1363 - Standard Specifications for Public-Key Cryptography. Status: Draft, Expected publication date: 1999. The current draft contains mechanisms for digital signatures, key establishment, and encipherment based on three families of public-key schemes:

   - "Conventional" Discrete Logarithm (DL) based techniques, i.e., Diffie-Hellman (DH) key agreement, Menezes-Qu-Vanstone (MQV) key agreement, the *Digital Signature Algorithm* (DSA), and Nyberg-Rueppel (NR) digital signatures.

- Elliptic Curve (EC) based variants of the DL-mechanisms specified above, i.e., EC-DH, EC-MQV, EC-DSA, and EC-NR. For elliptic curves, implementation options include mod p and characteristic 2 with polynomial or normal basis representation.

- Integer Factoring (IF) based techniques including RSA encryption, RSA digital signatures, and RSA-based key transport.

3) ISO/IEC 9796 (1991): Digital signature scheme giving message recovery. ISO/IEC 9796 specifies a digital signature mechanism based on the RSA public-key technique and a specifically designed redundancy function.

4) ISO/IEC 9796-2 (1997): Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash-function. ISO/IEC 9796-2 specifies digital signature mechanisms with partial message recovery that are also based on the RSA technique but make use of a hash-function.

5) ISO/IEC CD 9796-4: Digital signature schemes giving message recovery – Part 4: Discrete logarithm based mechanisms. Status: Committee Draft; Expected publication date: 2000. ISO/IEC 9796-4 specifies digital signature mechanisms with partial message recovery that are based on Discrete Logarithm techniques. The current draft includes the Nyberg-Rueppel scheme.

6) ISO/IEC FCD 14888-1: Digital signatures with appendix – Part 1: General. Status: Final Committee Draft; Expected publication date: 1999. ISO/IEC 14888-1 contains definitions and describes the basic concepts of digital signatures with appendix.

7) ISO/IEC FCD 14888-2: Digital signatures with appendix – Part 2: Identity-based mechanisms. Status: Final Committee Draft; Expected publication date: 1999. ISO/IEC 14888-2 specifies digital signature schemes with appendix that make use of identity-based keying material. The current draft includes the zero-knowledge techniques of Fiat-Shamir and Guillou-Quisquater.

8) ISO/IEC FCD 14888-3: Digital signatures with appendix – Part 3: Certificate-based mechanisms. Status: Final Committee Draft; Expected publication date: 1999. ISO/IEC 14888-3 specifies digital signature schemes with appendix that make use of certificate-based keying material. The current draft includes five schemes:

   - DSA;

   - EC-DSA, an elliptic curve based analog of NIST's Digital Signature Algorithm;

   - Pointcheval-Vaudeney signatures;

   - RSA signatures;

   - ESIGN.

9) ISO/IEC WD 15946-2: Cryptographic techniques based on elliptic curves - Part 2: Digital signatures. Status: Working Draft; Expected publication date: 2000. ISO/IEC 15946-3 specifies digital signature schemes with appendix using elliptic curves. The current draft includes two schemes:

   - EC-DSA, an elliptic curve based analog of NIST's Digital Signature Algorithm;

   - EC-AMV, an elliptic curve based analog of the Agnew-Muller-Vanstone signature algorithm.

10) ANS X9.31-1 (draft): Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry – Part 1: The RSA Signature Algorithm. ANSI X9.31-1 specifies a digital signature mechanism with appendix using the RSA public-key technique.

11) ANS X9.30-1 (1997): Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry – Part 1: The Digital Signature Algorithm (DSA). ANSI X9.30-1 specifies the DSA, NIST's *Digital Signature Algorithm*.

12) ANS X9.62 (draft): Public Key Cryptography for the Financial Services Industry – The Elliptic Curve Digital Signature Algorithm (ECDSA). The ANSI X9.62 draft standard specifies the *Elliptic Curve Digital Signature Algorithm*, an analog of NIST's *Digital Signature Algorithm* (DSA) using elliptic curves. The appendices provide tutorial information on the underlying mathematics for elliptic curve cryptography and many examples.

B.3 Supporting TSP infrastructure

The following work has been done in the area of TSP's infrastructures:

1) ISO/IEC 14516 (WD): Guidelines on the use and management of Trusted Third Party services. Status: Working Draft; Expected publication date: 1999. ISO/IEC 14516 contains guidelines on the use and management of Trusted Third Party services.

2) ISO/IEC 15945 (WD): Specification of TTP services to support the application of digital signatures. Status: Working Draft; Expected publication date: 2000. ISO/IEC 15945 specifies TTP services to support the application of digital signatures.

3) ANS X9.31-3 (draft): Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry – Part 3: Certificate Management for RSA. Status.

4) ANS X9.30-3 (draft): Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry – Part 3: Certificate Management for DSA. Status.

5) ANS X9.57 (1997): Public Key Cryptography for the Financial Services Industry – Certificate Management. This standard specifies the content of public-key certificates and techniques for the generation, validation and revocation of certificates. The document focuses on DSA public-key certificates and attribute certificates.

6) ANS X9.55 (1997): Public Key Cryptography for the Financial Services Industry – Extensions to Public Key Certificates and Certificate Revocation Lists. Meant to be used in conjunction with X9.57, X9.55 broadens and provides greater flexibility for certificate use by adding fields for additional information about public keys, alternative names for a certificate subject, and constraint specifications. X9.55 covers the specifications of the extension fields, descriptions of the underlying requirements, and descriptions of their intended use.

Annex C: Glossary

ABA
IETF
ISO/IEC/ITU-T
OECD
SOGITS
UNCITRAL

History

Document history		
V0.4.2	November 1998	Draft produced from draft report 4.1 for update and approval by TC Security