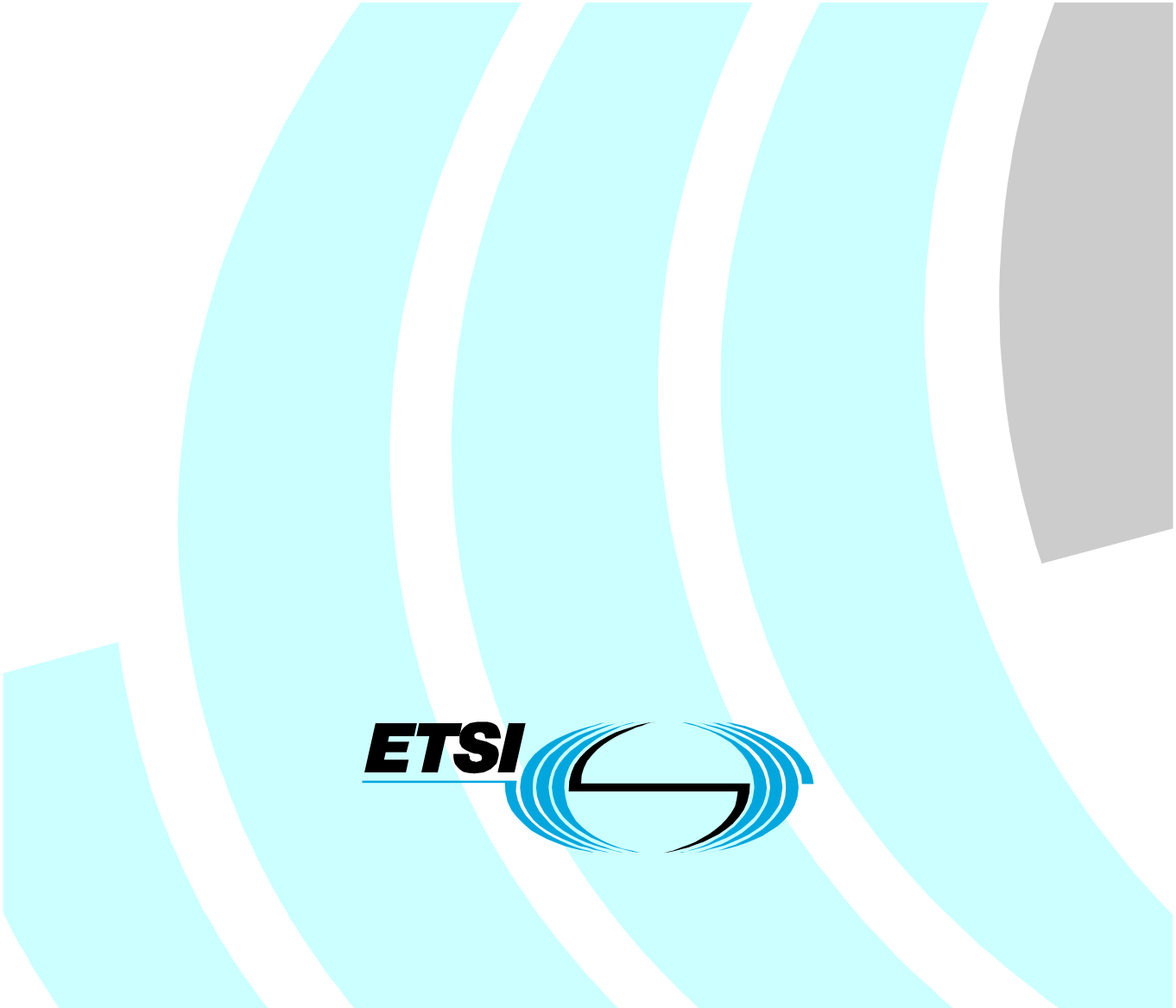
ETSI TR 102 041 V1.1.1 (2002-02)

Technical Report

Signature Policies Report



Reference
DTR/SEC-004022

Keywords
electronic signature, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - 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

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 ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

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 ETSI 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 Committee Security (SEC).

1 Scope

The present document gives guidance on the technical, organizational and legal issues related to a signature policy. The present document can best be seen in conjunction with published documents TS 101 733 [2] and ES 201 733 [1] upon which it builds.

Although the present document is recommended for all types of readers, those interested in future standardization recommendation may particularly be interested in annex B.

2 References

For the purposes of this Technical Report (TR) the following references apply:

[1] ETSI ES 201 733 (V1.1.3): "Electronic Signature Formats".

[2] ETSI TS 101 733 (V1.2.2): "Electronic signature formats".

[3] American Bar Association (1996): "Digital Signature Guidelines".

[4] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[5] Mitrakas A., Bos J. (1998): "The ICC ETERMS Repository to Support Public Key Infrastructure", Journal of Jurimetrics, Vol. 38, No. 3.

[6] IETF RFC 2459: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

[7] IETF Internet Open Trading Protocol (IOTP).

[8] ISO/IEC 17799: "Information technology - Code of practice for information security management".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

authority certificate: certificate issued to an authority (e.g. either to a certification authority or to an attribute authority)

Certification Authority (CA): authority trusted by one or more users to create and assign identity certificates

NOTE: Optionally the certification authority may create the users' keys.

Certificate Revocation List (CRL): signed list indicating a set of certificates that are no longer considered valid by the certificate issuer

digital signature: data appended to, or a cryptographic transformation 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

Online Certificate Status Protocol (OSCP): real time certificate status information resource

public key certificate: formatted piece of data that relates an identified subscriber with a public key he uses that is signed under the private key of the certification authority which issued it

signature policy: set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid

signature policy issuer: entity that defines the technical and procedural requirements for electronic signature creation and validation, in order to meet a particular business need

signature validation policy: part of the signature policy, which specifies the technical requirements on the signer in creating a signature and verifier when validating a signature

signer: entity that creates an electronic signature

time-stamping Authority (TSA): trusted third party that creates time-stamp tokens in order to indicate that a datum existed before a particular point in time

Trusted Service Provider (TSP): entity that helps to build trust relationships by making available or providing some information upon request

valid electronic signature: electronic signature, which passes validation according to a signature validation policy

verifier: entity that verifies a piece of evidence

NOTE: Within the context of the present document this is an entity that validates an electronic signature.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ARB	Authentication Response Block
ASN.1	Abstract Syntax Notation 1
CA	Certification Authority
CEO	Chief Executive Officer
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
CUG	Closed User Group
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EESSI	European Electronic Signature Standardization Initiative
EFT	Electronic Fund Transfer
ES	Electronic Signature
ICC	International Chamber of Commerce
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
OTP	Open Trading Protocol
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
SCCD	Secure Signature Creation Device
TSA	Time Stamping Authority
TSP	Trusted Service Provider
WWW	World Wide Web
XML	eXtensible Mark-up Language

4 Signature policy definition and scope

The requirement for security in business communications exacerbates the need to extend the elements of data upon which trade partners can rely upon in order to assess the validity of digital signatures. In electronic commerce, transacting parties have the capacity to determine the conditions under which an electronic signature can be deemed valid or becomes binding in a given business context. All such rules and conditions are the basis to establish the validity of an electronic signature and can be drafted in a single policy document called the signature policy.

Signature policy is a set of rules to create and validate electronic signatures, under which an electronic signature can be determined to be valid in a particular transactions context. A signature policy may be written using a formal notation like ASN.1 or in an informal free text form provided the rules of the policy are clearly identified. When two or more parties transact in an electronic business environment they may need to define the conditions under which a particular digital signature can be used. A signature policy describes the scope and the usage of such a digital signature with a view to address the conditions of a given transaction context.

Public Key Infrastructure (PKI) requires to appropriately address the various technological, organizational and legal aspects involved in the life cycle and the usage of electronic signatures. Within a PKI, a signature policy defines the conditions of usage of a digital signature within a given context. A context may include a transaction, a legal regime, a role assumed by the signing party, etc.

A signature policy can also be seen as a means to enforce trust in electronic commerce through appropriately indicated authorization levels. A signature policy can also enhance the management conditions of a PKI as it allows for more information to flow from the signer to the recipient (validating party) to ultimately add to the transparency of a transaction. Furthermore a signature policy is appropriate to address certain aspects that fall within the domain of interest of the Certification Authority regarding the various aspects of disclosing to third parties (i.e. Courts of Justice) of information such as permitted elements, conditions to disclose information, etc.

5 Signature policy context

The signature policy responds to the requirement in electronic transactions to collect as much information as possible regarding the transacting parties and the transaction in hand. The signature policy belongs to the context of a transaction formalizing certain elements of that context and putting them in the perspective of the usage of electronic signatures. To better realize the extent of usage of a signature policy it is necessary to focus on the conditions of the transaction a signature policy can be used for.

An informal private transaction is the area where an electronic signature might be mostly found useful. In private transactions there is no mandatory requirement to apply a signature in order to validate one's intention to transact. In formal transactions, such as those in which there is a legal requirement to follow a specific form, procedure, etc., a signature policy can be of use in better outlining the outer limits of such elements as the validation of a transaction and the application of electronic signatures. Signature policy users may also need to specifically determine the transactions where a signature policy might become required or mandatory.

It is practical to use one single signature policy as reference for multiple transactions. It is necessary, however, to link the need for a signature policy with the need in open electronic commerce to formalize certain information elements regarding the transaction and the usage of an electronic signature. Formalizing such information elements is necessary for the automated processing of information related to electronic signatures and to invoke trust by collecting with a view to use as evidence in case of a dispute related information elements.

5.1 Transaction context

As signature policies can represent requirements associated with transactions it is necessary to link to a particular signature policy core elements that call for such formalization. A transaction context may include commercial, administrative, private contexts or a combination of any combination of the above. The transaction context determines the general applicable rules associated with signing ceremonies. Such rules may emanate from statutes e.g. an action is to be taken by filling out a specific form, corporate conditions e.g. A, Director of company B Ltd. represents company B Ltd, contract e.g. A authorizes B to act as his agent representing him. The specific rules of the transaction context that refer to a signing right or the specific conditions of acknowledging the usage of signatures can be included in a signature policy.

5.2 Signature policy within a PKI

In a PKI environment when a signer digitally signs data he needs to indicate that the specific meaning a digital signature has. An electronic signature may commit the signer to an act related with a commitment expressed or merely be used as a challenge when authentication is needed. When the digital signature has a specific meaning the signer is required to include an indication in the signed structure that the signature is a commitment.

As such indication, a signature policy provides notice of the prevailing rules and conditions that the signer sets forth towards third parties, including relying parties, that further rely on that digital signature.

- When this indication directly determines which signature policy the signer applies an attached unique numeric value represents the signature policy and is protected under the digital signature. Upon receipt, a recipient is required to accept or reject the signature policy that the signer has indicated. If the signature policy is accepted, the verifier needs to validate the signed data using the rules prescribed in the signature policy.

- When this specific indication indirectly indicates that a signature policy is invoked by the signer, this means that some information (e.g. a document) will be made available elsewhere to allow relate the semantics of the signed data with a given signature policy. In order to be able to use this technique, the semantics of the transaction need to be clearly recognized. In practice, this technique is not adapted to free text, but to forms only. There are two ways to make such a relationship:

  - a document to indicate for a given signature policy, the forms of transactions governed under that signature policy;

  - a document to indicate for a given form of transaction the applicable signature policy.

5.2.1 Signature policy in closed environments

Although PKI is a technology better viewed in the context of open transaction and communication environments, closed PKI environments are often used in closed trade relationships. Such environments also known as Closed User Groups (CUGs) are characterized by the previous knowledge that the trade parties have about each other. PKI is used within such groups, as it is a technology that outperforms other competitive ones to meet security requirements.

As signature policies are conveyed by means of a unilateral statement from the issuer, they fit within a contractual framework. Users and parties relying on signature policies are required to indicate their consent of using or accepting a signature policy. Such consent can also be demonstrated through a prior bilateral agreement between the parties that execute a signature policy for their bilateral transactions or by any other means deemed appropriate under the transaction circumstances including a party's agreement.

In closed environments the transacting parties can maintain stringent control over the content and the conditions of acceptance of signature policies and formalize any such conditions in an agreement.

5.2.2 Signature policy in open environments

While control constraints may be less stringent in controlled transaction environments like CUGs, in open environments a signature policy may have to be further scrutinized for consistency, content and possibly fitness for the intended transaction. Unless specifically negotiated signature policies in open environments can be seen as general conditions having to conform to specific requirements mandated by law.

Signature policy controls are closely linked to the trust that trading partners can show to each other. Trust is developed among parties that are already known to each other and operate within an environment of shared norms and co-operative behaviour. In the absence of these features in open environments signature policies may face increased difficulty to be accepted by trading parties. As a result acceptance and interoperability may be ultimately limited.

Through signature policies parties in open network transactions can provide notice of the conditions of having electronic signatures assuming binding effect. A signature policy in this case provides notice of the will of issuer of a signature policy to large non-determined populations of users.

Standardizing the form and content of signature policies may contribute to their greater acceptance and interoperability in open environments.

5.3 Signature policy types

A signature policy may address such aspects as those associated with a transaction that the signatory and its counterpart are in. A signature policy may include content that relates to single signature transactions or multiple party signatures:

- signature policy for single signature transactions, i.e. transactions that include only one signer. The policy allows indicating that the individual signature is valid or not;

- signature policy for multiple party signatures. An example can be three party transactions such as those typically validated before a notary public. In notary transactions the verification of the identity of the transacting parties as well as the signed data is a requirement. Other tri-partite transactions may include transactions involving a bank, a clearinghouse, a transportation transaction involving a consigner, consignee, shipper, forwarder, etc. Given the typical complexity of electronic transactions and the actors involved therein the bulk of signature policies belong to this category.

The types of signature policies for multiple party signatures along with their verification against one signature policy are discussed in annex B.

5.4 Signature policy vs. certificate policy

As policies are a common way to express operational conditions in electronic commerce, the signature policy must be distinguished from other types of policies, like the certification policy. A signature policy contains rules that *inter alia* specify which certification policies are acceptable under that policy. This limits the certificates that can be used under the signature policy, since these certificates will need to contain information (e.g. an OID) that indicates that they comply with one the certification policies. Signature and certificate policies may reference each other like when a certificate policy supports a signature policy. Certificate policies remain distinct from signature policies at all times as they serve different purposes and have different scope.

6 Signature policy issuer

A signature policy issuer is any party describing the usage of a digital signature according to a prescribed procedure associated with a transaction. Parties that issue signature policies can be:

- legal persons i.e. organizations setting out the conditions under which an electronic signature used by their agents can bind them. Such an example might include the conditions for the procurement of goods by an organization, a tax return form, etc. Organizations may also be acting on behalf of interest groups e.g. industry or interest groups;
- natural persons acting under a professional function i.e. a notary public, a professional, etc. who sets out the conditions under which they can be bound by an electronic signature when acting in a professional capacity. Such might be the case of professionals signing a draft report that is to be used conditionally for specific purposes. Although professionals are not envisaged to be the primary users of a signature policy their professional associations may promote using them.

7 Signature policy user

Natural persons acting individually or under a professional or business role are likely to act within a transaction context and become the signers of a transaction. Verifiers of a transaction may either be some type of individuals acting directly or through an automated process.

7.1 Signer

A signer is an individual that creates an electronic signature. A signer may act as an agent of the user of the transaction or be contractually related to him. As a signer is primarily responsible for the application of an electronic signature it has an interest in a signature policy that formalizes the application of such signature in a transaction. The signer is overall responsible to provide notice of the signing conditions that apply on each specific transaction with its business counterparts.

A signer may sign under either an individual capacity or a pre-determined role. There are two types of roles envisaged for an electronic signature, i.e. a claimed role and a certified role.

- A claimed role merely contains a statement of the signatory that enters into a transaction under a certain role. This kind of role attribute might be legally important, for example, to decide on whether a signatory acted as a consumer, a trading party, etc. When the signer asserts such information, there is no proof that the signer acted under any role. If later on it can be proven that the signer did not have that role at the time of the signature, then the signer may be held responsible for providing false information.
- A certified role carries information to prove that the signer had a designated role at the time of the signature.

7.2 Verifier

A verifier is the party controlling a signed document or the beneficiary of a transaction. A verifier needs first to make sure that the policy invoked by the signer is appropriate for his specific business needs. As an acceptor of a signature policy, a verifier must perform certain actions such as validate the authenticity and content of a signature policy.

The objective for the verifier is to ensure the authenticity of the signature policy and subsequently assess whether to accept or reject the transaction.

8 Signature policy content

A signature policy specifies the technical and procedural requirements regarding signature creation and validation in order to meet specific business needs.

8.1 Signature policy format requirements

A signature policy is used at different instants in time. It must be selected by the signer to make sure that the policy is applicable to the context and the content of the transaction. At that time some human readable form has to be available.

Once selected by the signer, the signature policy must be processed, so that all the signer's conditions can be verified by the system (hardware and software) generating the signature.

When received by a verifier, the signed data should allow to directly or indirectly establish the signature policy chosen by the signer.

The signature policy can be presented to the verifier either prior to the verification of the signature or following the verification of the signature. When it is presented, the signature policy must again be available in human readable form.

When the digital signature is checked against the applicable signature policy, it must be processed, so that all conditions can be verified.

This means that a signature policy must exist in two forms:

- a form understood by humans.
- a form that can be processed by machine. This form may be internal to the machine, i.e. code embedded in the machine, or external to the machine, i.e. code that can be interpreted by the machine.

Automated validation of signature policies can be used in transactions that are based on Electronic Data Interchange (EDI) formats. EDI transactions include financial service transactions, like Electronic Fund Transfer (EFT) that are usually based on standards like the UN/EDIFACT. A more recent format for the exchange of structured data is based on the Extensible Mark-up Language (XML) format. XML is a data format for structured document interchange on the World Wide Web (WWW).

8.2 General signature policy information

A given statutory or contractual context may recognize a particular signature policy as meeting its requirements. For example, regarding the relationship between statutory requirements and a signature policy a specific signature policy may be recognized as meeting the requirements of a specific transaction such as a tax declaration or a formal sales agreement, etc.

General information includes:

A Signature Policy Issuer name: an identifier for the body responsible for issuing the signature policy. This may be used by the signer or verifier in deciding if a policy is to be trusted, in which case the signer/verifier shall authenticate the origin of the signature policy as coming from the identified issuer.

A Signature Policy Identifier: the Signature Policy shall be identifiable by an identifier, e.g. an OID (Object Identifier) whose last component (i.e. right most) is an integer that is specific to a particular version issued on the given date.

A Signing period: the start time and date, optionally with an end time and date, for the period over which the signature policy may be used to generate electronic signatures.

A Date of issue: optionally, when the Signature Policy was issued.

A Field of Application: this defines in general terms the general legal/contract/application contexts in which the signature policy is to be used and the specific purposes for which the electronic signature is to be applied.

Certain commitments that can be undertaken by the transacting parties can also be part of the signature policy. Such commitments set a transaction framework for the usage of digital signatures when signing a document. A commitment type can be the object identifier for the commitment and a qualifier. The qualifier provides more information about the commitment like for example information on the contractual/legal/application context.

8.3 Signature validation

Upon receipt of a signed document the recipient is required to validate a signature prior to taking any further action that may be required within a transaction context. The signature validating party collects elements of information that include certificate validity information and the validation of the digital signature. If the signature policy is recognized, within the legal/contractual context, as providing commitment, then the signer explicitly agrees with terms and conditions which are implicitly or explicitly part of the signed data.

The validation of a signature policy is done at the time a recipient receives the signed data and can be done through human interaction or in an automated way.

8.3.1 Signature validation policy

The technical implications of the signature policy on the electronic signature with all the validation data are called the "Signature Validation Policy". The signature validation policy specifies the rules used to validate the signature.

The signature validation policy defines for the signer, which data elements shall be present in the electronic signature he provides and for the verifier which data elements shall be present under that signature policy for an electronic signature to be potentially valid.

For the same business needs, a signer can make different types of commitments, while the same general rules still apply. Instead of defining a signature policy for each kind of commitment, it is possible to specify general rules that are valid for all the commitments types and some specific rules which are only valid for some given commitments types. In this way, a given signature policy may be used for multiple commitments types, if and only if the signer explicitly indicates in the signed data which commitment type is being invoked.

A signature policy may thus be divided into:

- rules which are common to all commitment types, i.e. Common Rules; and
- rules that are specific to some commitment types, i.e. Commitment Rules.

The signature validation policy is described in terms of:

- a set of Common Rules that define rules that is common to all commitment types. These rules are defined in terms of trust conditions for certificates, timestamps and attributes, along with any constraints on attributes that may be included in the electronic signature;
- a set of Commitment Rules for given commitment types that are defined in terms of trust conditions for certificates, timestamps and attributes, along with any constraints on attributes that may be included in the electronic signature.

8.3.2 Signature validation information

Signature validation information can be included in the common rules or in the commitment rules, but in any case they should not conflict with each other. The signature policy issuer will have to select the signature validation information items which are appropriate for a given signature validation policy. Signature validation information items include:

- rules for use of certification authorities (i.e. certification path requirements);
- rules applying to the user certificate;
- rules for making sure that the digital signature was produced while the certificate was valid (i.e. by obtaining an upper limit for the signature time (either by using time-stamping or Time-Marking);
- rules for a cautionary period;
- rules for use of Revocation Status Information (i.e. revocation requirements);
- rules for protection against Authority key compromise and weak cryptography;
- rules that relate to the environment to be used by the signer;
- signature verification data to be provided by the signer/collected by verifier;
- any constraints on signature algorithms and key lengths;
- rules for Use of Roles;
- certificate chain requirements.

The certificate requirements identify a sequence of trust anchors used to start (or end) certification path processing and the initial conditions for certification path validation as defined in IETF RFC 2459 [6].

End-certificate specific requirements

There may be requirements that apply only to the end-certificate (i.e. the certificate that is the object of the query). For example, the end-certificate must contain specific extensions with specific types or values (it does not matter whether they are critical or non critical). As an example, the end-certificate must contain information to make sure that the certificate is a Qualified Certificate, as meant by the Directive on Electronic Signatures [4]. There are currently two ways to check this property:

- the OID of the certification policy contains a specific value;
- a QC-Statement extension is present and contains a specific value.

Time-stamping or time-marking requirements

To establish the validity of a digital signature, it must be proven that the signature was applied while the end-user certificate was valid. Since it is not possible to rely on a time indicated by the signer an upper limit of that time is used instead. This upper limit may be obtained in two ways: either by using a time-stamp or a time-mark.

A time-stamp applied on a digital signature value proves that the digital signature was created before the date included in the time-stamp.

A time-mark is an audit record part of an audit trail from a third party trusted under the signature policy. A time-mark applied to a digital signature value, can prove that the digital signature was created before the time from the time-mark itself was updated.

The signature policy may include either time-stamping or time-marking requirements.

The signature is proven to have been generated while the certificate was valid, if the signature value and the hash of the signed data verify together using the public key from the certificate, but also if the two following conditions are both satisfied:

- the time-stamp or the time-mark has been applied before the end of the validity period of the certificate;
- the time-stamp or the time-mark has been applied before the revocation date of the certificate, should that certificate be revoked.

Since a certificate can in practice be revoked at any time, it is in the interest of the verifier to quickly obtain get a time-stamp or a time-mark.

Rules for a cautionary period

The following transaction scenario illustrates the timing problem in the digital signatures:

- Someone steals the signature device of the signatory, accesses the appending PIN number and sends a signed document. The signatory reports the loss to the Certificate Authority (CA) immediately, but some time may elapse before the publication of the revocation. When the certificate is revoked very shortly after a signed document is sent, the recipient who checks the revocation list, will not be able to see the revocation of the signature immediately, but only after the CA has processed the revocation.

A signature policy might state that a signature is only valid after a minimum time frame has elapsed after the signature time before the signature can be relied on as legally valid. This minimum time frame is counted from an upper limit of the signature time (obtained through a time-stamp or a time-mark) and is called the cautionary period. A signature before this time has elapsed can be considered conditionally valid. It may be deemed valid only once this time has elapsed and when the status information at the end of the cautionary period indicates that none of the certificates from the certification path is revoked. As a result this places time requirements on the instant when the revocation status information has to be fetched. In other words, the signature policy may dictate to wait for some time and thus not to use the revocation status information available at the time included in the time-stamp or the time-mark.

Revocation Requirements

Revocation information may be obtained through CRLs, delta-CRLs or OCSP responses. Certificate revocation requirements are specified both in terms of checks required on the end-certificate (i.e. the certificate for which a path is required) and on checks required on CA certificates. It can then specified if:

- full CRLs (or full authority revocation lists) have to be collected;
- OCSP responses have to be collected;
- delta-CRLs and the relevant associated full CRLs (or full authority revocation lists) are to be collected.

Revocation checks shall be carried out once the cautionary period is over.

Protection against Authority key compromise and weak cryptography

Verification of signed data takes place on the basis of validation data collected at the time of signature validation. Having successfully archived the signed data and the validation data following the transaction, there might be a need to further control this data after a period of time. Verification of signed data and the validation data occurs at time after the receipt of the signed data. If, however, advancements in encryption technology make likely the compromise of the cryptographic method applied on the signed data, more information may need to be collected to further validate such signed data. Such information may need to include additional signatures, such as time-stamp tokens, that have to protect to the signed data as well as other collected data using stronger algorithms.

Environment to be used by the signer

The signer may be required to use specific environments to produce his signature. This may come in addition to the use of a SCCD (Secure Signature Creation Device). The rules may be different whether the signature system is in a public environment or is private (e.g. a computer at home, a Laptop computer or a PDA).

Verification data to be provided by the signer/collected by verifier

The signer may be required to provide information useful for the signer, like attaching his certificate to the signed message or providing a time-stamp token.

- Constraints on signature algorithms and key lengths.
- Specific algorithms and key lengths may be required.

Rules for Use of Roles

Claimed roles or certified roles may be required.

8.4 Signature policy identifier

An identification reference is necessary to distinguish a signature policy from others in a given business context.

A signer may be given the reference of a signature policy that he shall use when signing. If only this reference was given to him, this would not be sufficient since this would not allow the signer to make sure that the description of the signature policy obtained when using this reference is the right one. Ideally the signer should be given the full description of the signature policy. However this description may be quite long. In order to avoid this, and thanks to the mathematical properties of the one-way hash functions used to compute hash values, a hash value of the signature policy is used instead.

An unambiguous reference thus consists both of an identifier of the signature policy and a hash value. The signer may use such an unambiguous reference an explicit reference of the signature policy is required to ensure that the selected policy is identical to the one being used by the verifier.

A signature policy reference may contain additional information, in particular the location where a copy of the Signature Policy can be obtained (e.g. a URL).

Using Object IDentifiers (OIDs) and Uniform Resource Locators (URLs) alone is not sufficient since they is not enough proof that the data referenced or retrieved is the correct one. Using a hash value associated with a hash algorithm is equivalent to having the full description of the signature policy. Hence, an appropriate reference is to use a signature policy identifier, a hash algorithm identifier and a hash value.

8.5 Signature policy publication

A signature policy can be made available through plain or secure WWW site publication.

Publication can be done by the Policy Issuer or by a third party through a trusted document repository service.

Third party storage can be made available for signature policy publication provided through a trusted document repository service. Such a repository can be used to generally host industry specific terms, including signature policies. An early conceptual example of such a repository is the ICC ETERMS [5] repository of the International Chamber of Commerce.

When communities of users apply signature policies, signature policies have to be published and made available to the users. The source of the information needs to be trusted and ways to authenticate the source of information have to be available. It is required to publish signature policies while they are valid, so that users can have access to their description. The role of a Signature Policy Publication Authority may be directly taken by the Signature Policy Issuer or be taken by a different organization.

8.6 Signature policy archiving

When communities of users want to verify electronic signatures generated under a given policy beyond the end of the validity of the signature policy, signature policies must be archived. Since Policy Issuer may disappear once they have issued their policies, this role should be taken by a different organization operating under conditions of independence and impartiality. A publicly accessible repository of documents can be seen as an appropriate organization to perform the function of a Signature Policy Archiving Authority.

8.7 Signature policy authentication

It is important that the signer makes sure that the signature policy he is using is the one really published by the Policy Authority.

There are various ways to achieve this. Policies may be obtained from trusted repositories or may be published in non-trusted repositories but may be signed. Once the assurance of authenticity has been obtained then the hash value maybe computed over the policy and reliably used.

9 Signature policy usage

9.1 Usage of a signature policy by a Signer

To reference a signature policy, a signer is only required to quote the identifier of the signature policy, the hash value and the hash algorithm identifier used to compute the hash value over the signature policy description. In case of a dispute a signature policy can be used to provide supportive evidence over the procedure associated with a specific signature in use.

When no explicit reference of the signature policy is used, the signer must make sure that the structure or semantics of the document that he is signing is well defined and that such semantics or structure either is referenced by a signature policy (by means of a signature policy identifier, a hash algorithm identifier and a hash value) and that such structure references a signature policy (by means of a signature policy identifier, a hash algorithm identifier and a hash value).

Signers show their consent with regard to the terms of usage of the policy by referencing explicitly a signature policy or by adding an indication that a specific security policy must be used by using some additional information provided by out-of-bands means.

9.2 Usage of the signature policy by a verifier

To verify a digital signature a verifier is required take the following steps:

- obtain the signature policy reference either from the signed data or from another document making the link between the document type and the signature policy;
- get a copy of the signature policy;
- compare the hash of the received signature policy with the hash of the signature policy to be used;
- make sure that the signature policy fits the purpose of the transaction.

Verifiers making use of signature policies show their consent with regard to the terms of usage of a signature policy when they accept a digital signature verified under that signature policy.

9.3 Conformance requirements

Both signer and validator's systems shall be able to process an electronic signature in accordance with the specification of the explicit or implicit but single signature policy.

A signature policy shall be sufficiently defined to avoid any ambiguity as to its implementation requirements. It shall be absolutely clear under which conditions an electronic signature should be accepted.

9.4 Signature policy usage in an organizational context

In organization level type of transactions, types of usage may include the following:

- Internal (within an organization):

  A typical example of a signature policy regarding the placement of a purchase order can include the roles involved by the signatory organization (e.g. Purchase Officer, Treasurer, etc.).

- External (between or among organizations):

  A typical example of a signature policy regarding the placement of a purchase order between organizations can include the roles and their attributes that are involved in both the signatory organization and the verifier organization.

9.5 Consent of usage

Users of signature policies are required to show their consent with regard to the terms of usage of the policy. Consent can be demonstrated through appropriate contractual or other arrangements, like for example a Code of Practice, or it can also be shown through a contract between the issuer and the user recognizing the binding nature of a signature policy within a specific transaction context.

9.6 Explicit reference

A reference to a certain signature policy can replace specific requirements of the contractual agreement. For example, the transacting parties can make an agreement that notices of termination may only be given electronically if certain requirements as to the creation and validation of an electronic signature are fulfilled. Referring explicitly to a certain signature policy facilitates the adherence to the formal requirements of the transaction.

Organizations that represent certain business sectors can also identify and create signature policies that comply with their specific business needs and explicitly refer to them in their business transactions. These signature policies can be published in a way that can be explicitly referred to by any member of these business sectors, and its use can be made obligatory to all parties that belong to that business sector if all parties agree.

Publication of PKI related policies could for example take place through the ICC ETERMS scheme of the ICC. The ICC offers the (additional) publication of business terms on their website. One of the advantages presented by that system is the combination of regular updates with the storage of prior versions for later reference and the fact that the user can access the information either on the server of the ICC or the server of the issuing entity.

9.7 Implicit reference

If the members of a business sector generally adhere to a specific signature policy, a transaction between the members of the sector will only be considered valid if this specific signature policy is complied with, unless stated otherwise by the contracting parties.

An implicit reference is made to a certain signature policy if a statement to the contrary is absent, and it is assumed that the transacting parties intended to require the adherence to the usual business practice for their transaction.

10 Legal aspects

10.1 Signature policy statutory aspects

In article 6, Directive 1999/93/EC [4] states that:

> "Member States and Commission (shall) work together to promote development and use of signature verification devices, in the light of the recommendations in Annex IV and in the interest of the consumer."

In the broad context of its application, the Directive mandates the usage of all digital signature support elements that can be useful to the end-user of a service. As such a signature policy can be seen as a mechanism that enhances the level of trust and support the verification of the identity of a signatory in a transaction.

A signature policy is necessary for the verification of electronic signatures that are deemed equivalent to hand-written signatures. According to article 5.1 of Directive 1999/93/EC [4]:

> "Member States shall ensure that an electronic signature is not denied legal effect, validity and enforceability solely on the grounds that the signature is in electronic form, or is not based upon a qualified certificate, or is not based upon a certificate issued by an accredited certification service provider."

By using a signature policy, transacting parties can gather sufficient evidence with regard to aspects such as the intention to sign, the bilateral formalities associated with signing, etc.

Art. 5(1): qualified electronic signatures

The same may also be suggested for qualified electronic signatures. There may be many possible signature policies the adherence to would meet the requirements for an "advanced electronic signature" as defined in article 2(2) of the directive. To be "advanced" is one of the criteria that an electronic signature has to fulfil to be considered qualified. Only qualified electronic signatures are awarded the extensive legal effects of article 5(2).

Art. 5(2): non- qualified electronic signatures

The Council Directive 1999/93/EC [4] states in its article 5(2) that electronic signatures may not be denied legal effect because they are non-qualified or because they are in an electronic form. This means that in principle all electronic signatures will have legal effect if their validity can be verified, whether they comply with certain standards or not. Thus, the European member states can generally not require usage of a specific signature policy to consider an electronic signature valid.

Accordingly, even standards that are developed by public bodies are generally not binding. Internet users are free to chose a signature policy that they like, whether it complies with a certain standard or not. Such a signature has to be given the same legal effect as an electronic signature that follows a certain standard if it can be demonstrated that it has the same security level.

10.2 Incorporation of a signature policy by reference

The American Bar Association [3] has defined incorporation by reference as "to make one message a part of another message by:

- identifying the message to be incorporated;
- providing information which enables the receiving party to access and obtain the incorporated message in its entirety;
- expressing the intention that it be part of the other message".

Incorporation of legal terms by reference is an issue that requires special attention in electronic commerce. The possibility of validly incorporating legal terms by reference has to be examined to ensure compliance with existing legal regulations. Ensuring that incorporating a signature policy by reference to existing contracts opens up new possibilities for automated transactions.

A signature policy contains the conditions under which a particular electronic signature is created and under which it can be validated. As shown previously, it can also include legal terms, such as the time frame for the validity of an electronic signature. To be valid in relation to the recipient, these terms preferably have to be incorporated in the contract between signatory and recipient. From a legal perspective, the rules of an electronic signature have to be agreed upon between the parties. They are not agreed at the same time, since the signer agrees at the time of signature generation and the verifier at the time of signature verification, but the end result is that they are agreed.

The incorporation of a signature policy into the agreement between signatory and recipient can be imagined as follows:

- by referring to a signature policy, the signatory offers an agreement to adhere to the terms of this particular signature policy;
- when the recipient accepts the signed document of the signatory, he inferentially agrees on the conditions of the underlying signature policy;
- however, to make sure that the terms of a particular signature policy are effectively agreed upon, certain rules of incorporation have to be followed.

Repositories can be used to remotely store legal terms so that they can be used by reference. By placing signature policies in repositories, trading partners can browse for the appropriate terms suitable to them select potential trading partners according to parameters that include legal terms, conditions of acceptance of certain signatures, authorization or signing requirements.

A question to be investigated in the following clauses is, how and under which conditions a particular signature policy can be incorporated into an agreement of signatory and relying party. In general, incorporation into Consumer contracts and incorporation into business contracts follow different rules. Inclusion in a business contract is comparatively easy, whereas in a consumer contract, stricter rules have to be obeyed. Moreover, especially in relation to the content of standard clauses, a distinction can also be made between civil law and common law countries. While in civil law regimes, standard terms generally have to pass a test of fairness to be considered valid by courts, the concept of reasonableness has only been introduced to English law through the Unfair Contract Terms Act of 1977 and is generally interpreted in a more liberal way than in common law jurisdictions.

10.3 Incorporation by reference in practice

In some types of contracts it is common practice to record just the essential information, and then by reference, to incorporate a more detailed set of terms like for example:

- the standard form contract of a Trade Association, for example builders, architects, law societies, etc.;
- the standard terms of one of the parties, for example bus, rail, airlines;
- the terms of another contract related to the transaction.

In electronic commerce it often occurs that the sheer size of documents does not allow for the efficient incorporation and reference of a document into another like for example in the case of Certification Policies or Certification Practice Statements.

Incorporation by Reference is not a new concept in law although its nature is still relatively elusive. Although the listing of types of usage of Incorporation by Reference in Common Law countries far exceeds that of Civil Law hereunder follow a few examples such as the following Securities regulation EU Listing Particulars Directive.

Additionally, Incorporation by Reference is quoted in the UNCITRAL Model Law on electronic commerce (1996) as well as in various standards such as those used in EDI messaging that incorporate de facto by reference interchange standards.

Civil Law at large accepts the concept of incorporation of legal terms by reference. Notable examples are the following. In Germany, Italy, Luxembourg, Spain and UK a company issuing securities may circulate a document published within the previous 12 months and approved by designated authority in lieu of a new document if note is attached to earlier document describing the characteristics of the issue and containing any updates as necessary (any material changes, accounts for the latest financial year, interim financial statements). In Belgium, France and Spain there is the concept of "shelf registration" whereby a "shelf document" containing general information on the company and financial statements is submitted to and approved by designated authority on an annual basis. When an issue is made an "issue document " is published which contains the characteristics of the offering and any applicable updating of the shelf document and which must be approved by the supervisory authority.

In a nutshell, to incorporate by reference the parties should take note of requirements that include the following:

- a unique identifier of the signature policy, together with a full description (over which a hash may be unambiguously computed);
- counterpart consent and knowledge;
- positive duty of information through express reference clause and easy access to terms;
- support by International Law through the UNCITRAL Model Law on electronic commerce, 1996;
- unambiguous publication on a document repository.

11 Conclusion

Signature policies have emerged as a necessary element that adds to the legal safety of the transaction. A signature policy can be used to identify the conditions of usage and the terms of authorization of digital signatures. A signature policy can also enhance some management conditions of a PKI as it allows for more information to flow from the signer to the receiver (validating party) to ultimately add to the transparency of a transaction.

Signature policies are demanding in drafting and editing, since appropriately structured internal processes within an organization should back up their conditions of usage. Managing and storing signature policies in the long run can also be added to the potential costs of applying them in electronic commerce practice as they demand updating to keep in pace with developments in cryptography.

Signature policies provide an additional (new) contractual instrument to outline business relationships. Organizations that represent certain business sectors can also identify and create signature policies that comply with their specific business needs and refer to them in their business transactions.

Due to the limited understanding surrounding signature policies there is a certain ambiguity surrounding their content and application. Signature policies may add to the ambiguity of PKI and compromise its chances as a widely applicable technology for any type of transactions. The usage of signature policies is likely to remain confined within large organizations where the need for backtracking authorization is more evident.

From a regulatory viewpoint signature policies can be better managed through self-regulatory initiatives that may make them applicable in certain areas of the industry or administration while they specify the content and application context of such policies.

The legal value of signature policies can be seen as a unilateral declaration of will that allows the transacting parties to declare their contractual position with respect to a transaction or signatory. As such signature policies can become an essential contractual instrument to invoke legal conditions relevant to a transaction when using digital signatures. Cautious drafting of signature policies is essential to avoid conflicting terms with other policies in support of a PKI implementation, such certificate policies.

Annex A:
Signature policy in electronic transactions

A.1 Case study I: Transactions within an organization

A transaction within an organization using digital signatures can include roles such as the purchase officer, the treasurer, the Chief Executive Officer (CEO), or the president of the board of directors.

In any purchase the initial authority to sign the transaction documents is the purchase officer. If the money requirements of this purchase are small, a single authorized party, in this case the purchase officer, is sufficient for the validity of this transaction.

Further increment in money requirements might enforce a sequential authorization of this transaction. For example, due the purchase officer's signature limitations the signed document is passed for further authorization to the treasurer. Depending on the treasurer's budget authorization limits, the transaction might be forwarded for signature all the way to the CEO.

The signature of the CEO might not be sufficient if the decision for the transaction requires the direct involvement and approval of the organization's president. In such a case where two parties are directly and simultaneously involved in a decision, a concurrent authorization should be appropriate for the validity of this transaction.

The signature policy that can be created can state that the purchase officer can sign a document for a certain amount of money. It should state that the purchase officer's signature should be valid for a certain period of time, depending on the duration of the project or the duration and agreement of the purchase officer's employment. Accordingly, it should also state the signature limitations for all parties in the hierarchy of a company, as well as the rules that apply in all of the company's transactions.

A.2 Case study II: Transactions between organizations

A transaction between organizations using digital signatures can include roles such as the purchase officer, the treasurer, the chief executive officer (CEO), or the president of the board of directors, from both the organizations. These transactions should be based on a framework that is accepted by both organizations.

Such a framework of business scenarios using digital signatures has been defined in IETF Internet Open Trading Protocol [7]. The Baseline Open Trading Protocol supports many types of OTP Transactions, like authentication, deposit, purchase, refund, withdrawal, etc. For example, in a baseline authentication between two organizations the Baseline Authentication OTP Transaction there are distinct Trading Blocks that have to be defined:

- Trading Protocol Options Block.
- Authentication Request Block.
- Authentication Response Block.

A typical authentication scenario between two organizations would include the following actions:

- first organization takes an action that requires that the organization be authenticated;
- the second organization generates an Authentication Request Block containing challenge data and the method of authentication to be used, then sends it to the first organization;
- OTP aware application is starting back on the first organization. The data received are used to generate an Authentication Response Block, which is sent back to the second organization and then stops. It optionally keeps a record of the transaction for auditing purposes;
- the second organization checks the Authentication Response Block (ARB) against the challenge data in the Authentication Request Block to check that the first organization is who they claim to be and stops.

In the above scenario a signature policy can be created to describe the conditions for the authentication of an organization. It should also describe the procedures for the authentication along with the archiving rules and the acceptance of the authentication data. Furthermore, it should include the rules of engagement in cases where the organizations involved in a transaction have conducted business before using digital signatures.

A.3 Case study III: A banking transaction

A signature policy of individual investors for signing investment orders or money transfers with a bank or financial institution might create a valid possibility of an individual or a bank issuing of a signature policy. Such a transaction framework has been defined in IETF Internet Open Trading Protocol and is described below:

- The individual decides to deposit cash electronically and sends information for example, the deposit amount, and the brand used, etc. to the Financial Institution.
- The Financial Institution sets the payment brand and decides which protocol has to be offered, generates an Authentication Request Block containing challenge data and the method of authentication and then it sends it to the individual.
- OTP aware application started. The individual selects the payment protocol to use, records selection in a Brand Selection Component, generates an Authentication Response Component and sends back to the Financial Institution.
- The Financial Institution checks the Authentication Response Block against the challenge data in the Authentication Request Block, uses the information to identify the individual, generates an Offer Response Block containing information about the deposit, and optional Signature Block and sends to the individual.
- The individual checks that the Offer is OK, combines component from the TPO Block, the TPO Selection Block and the Offer Response Block to create a Pay Request Block and sends to the Payment Handler with the Signature Block if present.

Note that the above scenario describes the general case where a Financial Institution can accept a deposit in several different types of electronic cash. In practice usually only one form of electronic cash may be accepted. However, there may be several different protocols that may be used for the same "brand" of electronic cash.

The Financial Institution may use the results of the authentication to identify not only the individual but also the account to which the payment is to be deposited. If no single account can be identified, then it must be obtained by other means. The individual could specify the account number in the initial dialogue, or the consumer could have been identified earlier, for example using a Baseline Authentication OTP Transaction, and an account selected from a list provided by the Financial Institution.

The signature policy that can be created to accommodate such a scenario can state the rules of engagement of the organization with its customers. The Financial Institution should state in the signature policy the conditions for accepting a request from its customers, along with the authentication procedures and data that will be involved in these types of transactions. The signature policy should also set the legal framework for such a transaction, that is acceptance by the customers of the rules of engagement that are set by the Financial Institution.

Annex B:
Recommendations for standardization work

B.1 Multiple signatures

In any transaction contractual agreements or statutory law may require that all the involved parties validate the transaction documents with their signatures. Even if the signatures are not required to be on the same document, in an electronic environment it can be more practical to have the signatures on one document. If electronic signatures should be able to replace hand written signatures in any context, it is necessary to create a signature standard that enables multiple signatures.

Depending on the transaction specifics, the ordering of the signatures may or may not be important, i.e. one signature may or may not need to be applied before the other. Multiple signatures fall into two general types: independent and embedded signatures. All cases of countersignatures, or double countersignatures can fall to the above two categories.

B.1.1 Multiple independent signatures

Independent signatures are parallel signatures where the ordering of the signatures is not important. Examples for independent signatures requirements can be found in the law of corporations. The signature order of the board of directors on a transaction document does not have any importance. The document is valid as long as it includes all the necessary signatures.

B.1.2 Multiple embedded signatures

Embedded signatures are applied one after the other and are used where the order the signatures are applied is important. These types of signatures are required when at least one of the functions of the second signature is to attest reception of the document with the first signature. Examples for embedded signatures requirements can be found in a notary's certification. For example, a contract for sale of land requires notary certification of the signed letters of intent of both parties. The notary has to sign his name on the document that contains the signatures of the party or parties, but the notary's signature has to be applied on the document after the signatures of the contracting parties.

Nevertheless, from a legal point of view in both cases of multiple signatures, the order in which the signatures were attached to a document must be unambiguous. One way to implement this would be to sign the second signature over the document including the first signature. However, it is not immediately visible for the recipient that the message contains another signature. A specific signature policy should be created that can be referred to inform the recipient if the signature belongs to a document with multiple signatures.

B.1.3 Multiple signature validation

To date a signature policy has been defined only to allow the validation of one single electronic signature, however there is a growing requirement to also support multiple signatures. In the description of a signature policy the signer of the document has to be clearly identified, and it suggests that more than one signer may exist, which gives support for multiple parallel signatures or for embedded signatures. The term concurrent signatures may be alternatively used to describe multiple parallel signatures while embedded signatures may better be understood by the term sequential signatures. Moreover, this description allows the signer to sign more than the hash of the data, and it also allows support for a counter signature, which gives support for multiple embedded signatures.

In the validation of multiple signatures each signer can indicate which signature policy and which commitment type under that policy is used. There should be included a set of common rules that would apply for all commitment types, and a set of commitment rules that are defined in terms of trust conditions for certificates, timestamps and attributes.

B.1.4 Multiple signature verification

Much like in the aforementioned case of the validation of multiple signatures the verification of multiple signatures is an area of further investigation. The standard is required to support the usage of multiple parallel signatures as well as embedded signatures.

B.2 Signature policy publication

Further work may be required in the direction of Signature Policy Publication Authorities. The publication of a signature policy involves many tasks. The Publication Authority must establish an infrastructure that will address issues like:

- Frequency of the publication.
- Version number.
- Updates and revision control.
- Revocation.
- Expiration date, etc.

Furthermore, roles have to be established to accommodate all of the above tasks, for example, administrator, operator, auditor, etc.

The Signature Policy Authority or the trusted third party in charge for the publication has to manage the publication process in such a manner, that the reliability of the signature policy data is ensured. To achieve this a series of administrative tasks have to be performed by the Publication Authority. Responsibilities include everyday tasks such as:

- Storage.
- Backup.
- Recovery.
- Audit.
- Access control.

The Publication Authority has to implement administrative procedures until the end of the life cycle of a signature policy. Depending upon the nature of the signature policy, it may be needed to continue to be able the verify signatures against an expired signature policy. In that case the role of maintaining available the description of that policy is transferred to a Signature Policy Archiving Authority.

The Signature Policy Publication Authority should follow security implementation guidelines that are described in numerous guides such as ISO/IEC 17799 [8].

B.3 Signature policy archiving

Further work may be required in the direction of Signature Policy Archiving Authorities. The Signature Policy Archiving Authority has to implement administrative procedures that would ensure that after the life cycle of a signature policy, certain archiving procedures take place to ensure that the expired signature policy is still accessible for re-verifying signatures from the past should a dispute arise between a verifier and a signer.

The Signature Policy Archiving Authority should follow security implementation guidelines that are described in numerous guides, such as ISO/IEC 17799 [8].

Such a publishing forum may take the work along the lines of the ICC ETERMS Repository [5]. ETERMS are discrete contract terms, groups of contract terms or complete agreements and sets of rules or practices.

The repository should be a database that contains actual data strings or codes and is maintained with an administrative infrastructure. The database needs to be up to date to ensure that the most recent as well as all the past terms of general acceptance are being referenced. A cohesive archiving policy should be established that addresses organizational and operational issues. The access policy should define maintenance procedures that will ensure the authenticity, availability and integrity of the repository's data.

The reliability of the Archiving Authority's impartiality is vital in cases where a dispute resolution is requested by a court of law, thus the Archiving Authority has to be accepted by all parties.

B.4 Accreditation schemes

Further work may be required in the direction of Accreditation Schemes for Policy Issuers.

Paragraph 11 of the 1999/93/EC Directive [4] on electronic signatures promotes the establishment of accreditation schemes.

The user can rely on a trusted accreditation scheme that examines the properties of a signature policy according to the security and legal effect of the resulting electronic signature. The recipient of an electronic signature that is based on an accredited signature policy might be more inclined to trust the validity of that signature.

Licensing schemes for signature policies can either be established by public or private entities. For example, it seems possible, that a consumer organization labels signature policies that fulfil certain criteria that protect the rights of consumers. On the other hand, public authorities might create a licensing scheme for signature policies with the effect that electronic signatures that comply with such an accredited signature policy will automatically be accepted for communication with public authorities.

B.5 Signed attribute requirement

Currently a signature policy does not include any element that allows verifying the semantics of the signed message. Since there currently exists no specific signed attribute to include an amount of money, then it is impossible using a signature policy to verify money amounts that would be authorized.

A typical example of this issue is a signature policy that deals with purchase orders. This signature policy can include the roles involved by the signatory organization (e.g. Purchase Officer, Treasurer, etc.), the amounts each role is authorized to sign for, the type of material each role is allowed to place a purchase order for, etc. Thus, adding a requirement for a new signed attribute to include an amount of money might be appropriate.

Annex C:
Signature policy in an informal free text form

A signature policy must be identifiable and include the following identity information:

- An unambiguous identifier of the **Algorithm** used to protect the signature policy Information.
- A **Hash** value of the signature policy information, which shall be re-calculated and checked whenever, the policy is passed between the issuer and signer/verifier.

In the **Signature Policy Information** section it should be specified the following information:

- The **Signature Policy Identifier** is an identifier of the signature policy that must uniquely identify the policy, and is specific to a particular version issued on the given date.
- A field that holds the **Date of Issue** for this Signature Policy.
- A field for the body responsible for issuing the Signature Policy, which is the **Signature Policy Issuer**. This may be used by the signer or verifier in deciding if a policy is to be trusted, in which case the signer/verifier shall authenticate the origin of the signature policy as coming from the identified issuer.
- A field that holds the **Field of Application** for this Signature Policy. This field holds in general terms the general legal/contract/application contexts in which the signature policy is to be used and the specific purposes for which the electronic signature is to be applied.
- It can be optionally included a **Signature Policy Extensions** section, where it can be declared any other information related to this Signature Policy.

In the **Signature Policy Information** section, it should also be included the **Signature Validation Policy** which defines for the signer, the data elements that shall be present in the electronic signature that is provided, and for the verifier, the data elements that shall be present under that signature policy for an electronic signature to be potentially valid. In more details, in the **Signature Validation Policy** information section, it should be specified the following information:

- A field that holds the **Signing Period** over which the signature policy may be used to generate electronic signatures, which defines the start time and date, and optionally the end time and date.
- A section that defines the **Common Rules**, which defines rules and conditions, that is common to all commitment types.
- A section that defines the **Commitment Rules**, which consists of the validation rules and conditions, which apply to given commitment types.
- It can be optionally included a **Signature Validation Policy Extensions** section, where it can be defined any other information related to this Signature Validation Policy.

Both **Common Rules** and **Commitment Rules** are defined in terms of rules for the signer or the verifier, and in terms of trust conditions for certificates, timestamps and attributes, along with any constraints on attributes that may be included in the electronic signature, and their sections contain the same set of information:

- A set of **Rules** for:
  - The **Signer**.
  - The **Verifier**.
- A set of **Trust Conditions** for:
  - **Signing Certificate**.
  - **Timestamping**.
  - **Attributes**.

- A set of **Algorithm Constraints** can be optionally included (if constraints are required).
- It can be optionally included an **Extensions** section where it can be defined any other information related to either Common Rules or Commitment Rules.

Both **Common Rules** and **Commitment Rules** sections may contain the same set of information, but the following rules and conditions apply:

- In the Common Rules the **Common Extensions** section holds information related to the Common Rules.
- In the Commitment Rules the **Commitment Extensions** section holds information related to the Commitment Rules.
- In the Commitment Rules it should be also specified a unique **Commitment Type Identifier**, which defines the Commitment Type.
- In the Commitment Rules it should be optionally specified the **Application Field** and the **Semantics Field**, which define the specific use and meaning of the commitment within the overall field of application, defined for the policy.
- If rules and conditions are present in Common Rules**,** then the equivalent rules and conditions shall not be present in any of the Commitment Rules.
- If the Signer Rules, the Verifier Rules, the Signing Certificates Trust Conditions, and the time-stamping Trust Conditions are not present in Common Rules, then they shall be present in each Commitment Rule.

In more details, in the **Signer Rules** and the **Verifier Rules** sections, rules should be specified to identify various information the signer or the verifier require:

- The rules should identify if the **Signed Data Hash** that is used to calculate the signature, is internal or external to CMS structure.
- A set of **Signed Attributes** that shall be present under this policy and shall be provided by the signer. It should include object identifiers for all signed attributes required by this policy.
- A set of **Unsigned Attributes** that shall be present under this policy and shall be provided by the signer. If not added by the signer, they will be added by the verifier. It should include object identifiers for all unsigned attributes required by this policy. For example, if the signer requires a signature timestamp the object identifier for this attribute shall be included.
- The **Signing Certificate** attribute that shall be provided by the signer under this policy. This should identify whether the signer shall provide just the signer's certificate, or the entire full certificate path.
- It can be optionally included an **Extensions** section where it can be defined any other information related to the Signer or the Verifier Rules.

The **Signing Certificate Trust Condition**, **Time Stamp Trust Condition** and **Attribute Trust Condition** make use of the following **Certificate Requirements**, which is used to define policy for validating the signing certificate, the TSA's certificate and attribute certificates.

The **Certificate Requirements** specify information that identifies the trust points used to start (or end) certificate path processing, e.g. using a set of self signed certificates, and the initial conditions for certificate path validation. In the **Certificate Requirements** section it should be specified the following information:

- A field for the **Trust Point**. This is the specification of the trust point for the start of processing of the certificate path that gives the self-signed certificate for the CA.
- A field for the **Certificate Path Length**. This is information about the maximum number of CA certificates that may be in a certification path following the trust point. The length of the path can specify this information.
- A field for the **Acceptable Certificate Policies**. This is information about certificate policies, any of which are acceptable under the signature policy.

- A field for the **Naming Constraints**. This is the indication of a name space within which all subject names in subsequent certificates in a certification path shall be located. Restrictions may apply to the subject-distinguished name or subject alternative names. Restrictions apply only when the specified name form is present. If no name of the type is in the certificate, the certificate is acceptable. Restrictions are defined in terms of permitted or excluded name sub trees. Any name matching a restriction in the excluded sub trees is invalid regardless of information appearing in the permitted sub trees.

- A field for the **Explicit Indication** of the certificate policy. This is specification of requirement for explicit indication of the certificate policy and/or the constraints on policy mapping.

The **Signing Certificate Trust Condition**, **Time Stamp Trust Condition** and **Attribute Trust Condition** make use of the following **Revocation Requirements**, which are used to define policy for checking the revocation status of the signing certificate, the TSA's certificate and attribute certificates. In the **Revocation Requirements** section it should be specified the following information:

- A set of information for the **End Certificate Revocation Requirements**. This is specification for checks required on the leaf certificate (i.e. the signers certificate, the attribute certificate or the timestamping authority certificate).

- A set of information for the **CA Certificate Revocation Requirements**. This is specification for checks required on CA certificates from the certification path.

- For each of the above sets of information the following fields should be included:

  - A field for the **CRL Check**. This is information for checks required whether full CRLs (or full authority revocation lists) have to be collected.

  - A field for the **OCSP Check**. This is information for OCSP responses that have to be collected.

  - A field for the **Delta CRL Check**. This is information for checks required whether delta-CRLs and the relevant associated full CRLs (or full Authority Revocation Lists) are to be collected.

  - A field for the **Other Check**. This is extension information for checks required whether any other available revocation information has to be collected.

The **Signing Certificate Trust Condition** identifies trust conditions for processing the certificate path used to validate the signing certificate. It should include the following information:

- **Certificate Requirements** and

- **Revocation Requirements**.

The **Time Stamp Trust Condition** identifies trust conditions for processing the certificate path used to authenticate the time stamping authority and constraints on the name of the time stamping authority. It should include the following information:

- A field for the **Time stamping Authorities Public Key Rules** of the time stamping authorities. This information specifies if any rules apply to the certification of the time stamping authorities public key.

- A field for the **Timestamp Revocation Requirements** that is used to check the revocation status of the time stamp. This information defines minimum requirements for revocation information and is obtained through CRLs and/or OCSP responses. This information could include the type of checks that should be carried out and whether these checks are needed or not.

- A field for any additional **Naming Constraints** on the trusted time stamping authority.

- A field for a defined **Cautionary Period**. This is the period after the signing time that it is mandated the verifier shall wait to get high assurance of the validity of the signer's key and that any relevant revocation has been notified.

- A field for the **Maximum Acceptable Time**. This is the time between the signing time and the time at which the signature timestamp is created for the verifier.

The **Attribute Trust Condition** must be present so any certified attributes can be considered to be valid under this validation policy. It should include the following information:

- A field for the **Signer Attributes**. This is information about the "claimed" or "certified" attributes of the signer.
- A field for the **Attribute Certificate Conditions**. This information specifies the certificate path conditions for any attribute certificate.
- A field for the **Attribute Revocation Requirements** that is used to check the revocation status of Attribute Certificates, if any are present. This information defines minimum requirements for revocation information and is obtained through CRLs and/or OCSP responses. This information could include the type of checks that should be carried out and whether these checks are needed or not.
- A field for the **Attribute Constraints** can be optionally included (if constraints are required). This is information about constraints on the specific attribute types and their values that may be validated under this policy.

A set of **Algorithm Constraints** can be optionally included (if constraints are required). There are different types of constraints:

- Signer Algorithm Constraints.
- Issuer of End Entity Certificates Algorithm Constraints.
- Issuer of CA Certificates Algorithm Constraints.
- Attribute Authority Algorithm Constraints.
- Time stamping Authority Algorithm Constraints.

This set of **Algorithm Constraints** are optionally included and for each type of these constraints it should be identified the following information:

- The **Signing Algorithms** (hash, public key cryptography, combined hash and public key cryptography) that may be used for specific purposes.
- A field for the **Minimum Key Length** that is required for these Signing Algorithms.
- It can be optionally included an **Extensions** section where it can be defined any other information related to the Algorithm Constraints.

Annex D: Bibliography

EESSI (2000), Mitrakas. A, Rinderle. R Signature Policies: "A Report for the ISIS Program".

ITU-T Recommendation X.209: "Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)".

Nilson H., Van Eecke P., Medina M., Pinkas D., Pope N. (1999): "Final Report of the EESSI Expert Team".

Unfair Contract Terms Act of 1977.

UNCITRAL Model Law on electronic commerce (1996).

History

Document history		
V1.1.1	February 2002	Publication