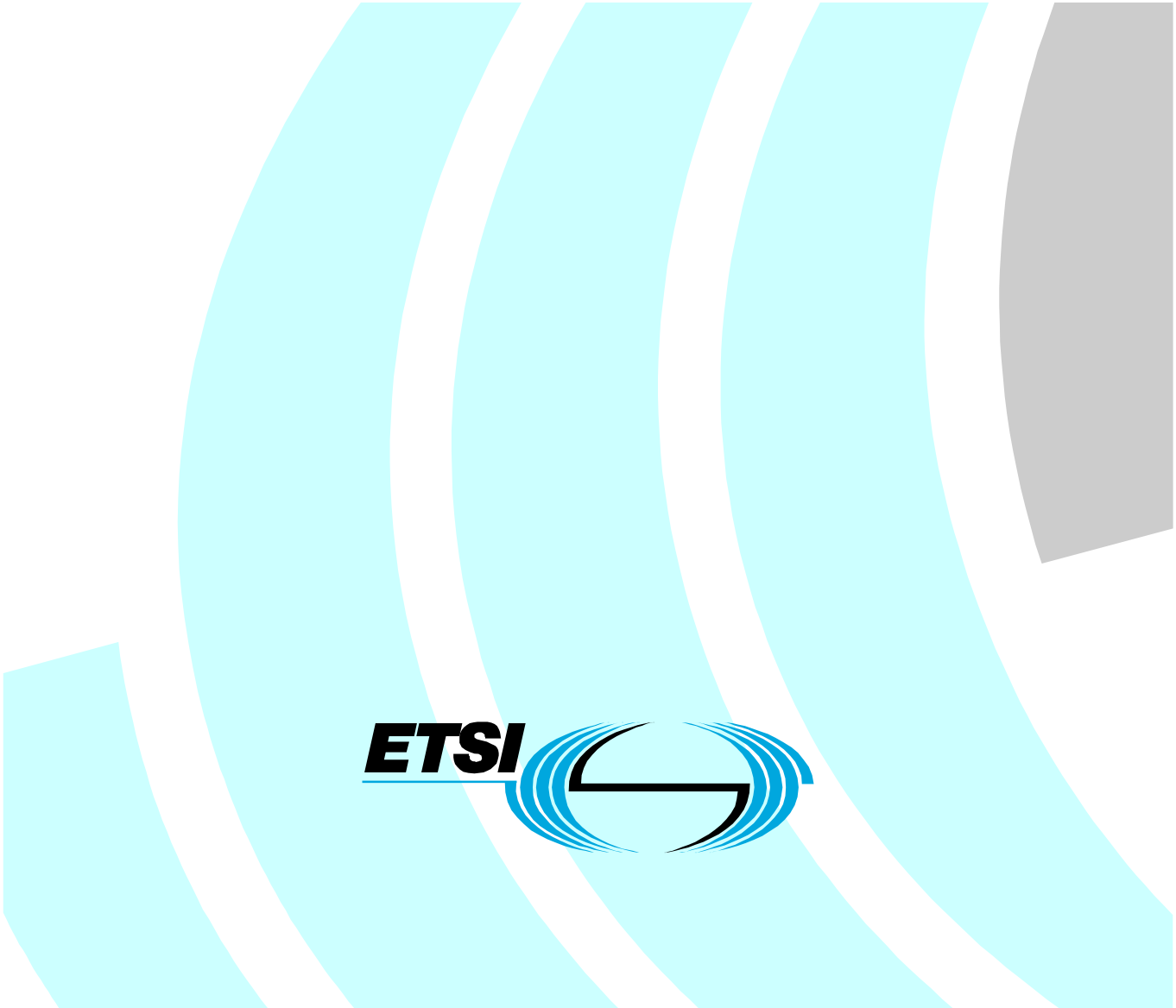
ETSI TR 102 045 V1.1.1 (2003-03)

Technical Report

Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model



Reference
DTR/ESI-000006

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2003.
All rights reserved.

DECT™, **PLUGTESTS**™ and **UMTS**™ are Trade Marks of ETSI registered for the benefit of its Members.
TIPHON™ and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

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).

All published ETSI deliverables shall include information which directs the reader to the above source of information.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Introduction

The work of the ETSI-TC ESI and CEN/ISSS has already addressed issues relating to single signatures, but very often documents require more than one signature to give it legal validity or to make a transaction effective. These may be parallel independent signatures, such as those of a buyer and seller on a contract; or embedded, countersignatures, where the countersignature is applied on top of a primary signature, such as a witness's signature, or the signature of a superior validating the signature of a subordinate. To date, a signature policy has been defined only to allow the validation of one single electronic signature (TS 101 733 [1]), however, as more paper-based processes are being transposed into the electronic environment, there is a growing business need to extend this policy to support multiple signatures. This is evidenced by the slow progress being made in relation to more complex business transactions, such as those requiring notarization, or those which, in the paper world have more stringent requirements for form. These include consumer finance or credit transactions, transactions with structured payment/delivery terms. For this to happen there needs to be some way of communicating/expressing the purpose for and the context in which a signature(s) has been applied so that it will be legally enforceable in any Member State (and ideally in any other jurisdiction).

The present document is intended to supplement TS 101 733 [1] and TR 102 038 [2] by investigating business needs and by providing a foundation for further work in relation to the technical implementation of a signature policy governing multiple signatures. It aims to provide general guidance on a methodology for the validation of multiple signatures. It assumes that each signature will be validated under a signature policy for single signatures such as TS 101 733 [1] or TR 102 038 [2]. It therefore remains to validate the relationship of each required signature against the others. The present document provides a framework for specifying high level requirements for the acceptance by a business of electronic signatures. It then considers a set of signature usage rules for a number of aspects of the business requirements which could be used to inform an implementation of a signature policy. The rules are not organized into a model policy in the present document. The present document provides a framework for the development of such rules.

There is a business need to transpose all the features of a handwritten signature into the virtual world, and to develop an equivalent trust in electronic signatures, particularly where they indicate a legally binding commitment. Directive 1999/93/EC [5] provides for the equivalence to handwritten signatures where an electronic signature is supported by enhanced technical security measures (article 5.1). However, there are many aspects of "real world" characteristics of signatures which are not provided for in the Directive. These could conveniently be covered by a signature policy.

The meaning of a signature is implicit in the signature itself, and yet it is readily understood even by a lay person. Usually that understanding is drawn from the context in which the signature was made. The present document attempts to analyse the meaning and implied consequences of a "real" world signature in a number of different business contexts. What commitment does a signature imply? What are the business purposes for which signatures are used? What are the consequences of a signature? What is its evidential value in legal proceedings? What are the relevant factors in relation to the creation of a signature? How can these factors be transposed into the virtual world? In many business situations, more than one signature is required to give effect to a document or transaction. The most obvious example is in relation to a contract where both buyer and seller sign to indicate their acceptance of the terms of the contract and their will or intention to be legally bound by them. In this case, the commitment implied by the signature, and the consequences of its creation it are straightforward. More complex to analyse are scenarios where counter signatures are required, i.e. where the signature of one person is countersigned by another. The meaning of such signatures, and the commitment being assumed by the countersigner, often is unclear without a careful study of the underlying business process. Even then, in the scenarios examined, there remains a great deal of ambiguity surrounding counter signatures.

The present document, therefore, assumes a broad interpretation of a signature policy and therefore, a signature policy may be a useful tool for specifying the means for the creation and verification of ***all*** the typical qualities of a handwritten signature. A signature policy could include the means for reproducing the "real world" ceremony, or formalities of signing. It could also include who may sign, in what capacity, what should be signed and in what circumstances. By defining the domain and/or the application to which the signature policy will apply, it is possible to reproduce some of the contextual information which is relevant to interpreting the signature commitment, as in the paper world. As these factors will vary according to the circumstances in which a signature is to be used, it follows that it is not possible to define a single, model policy to cover all scenarios. The present document analyses some of the factors common to many situations, and aims to provide "building blocks" which can be assembled ("Lego™"-style) to make a signature policy which is relevant to a particular business need.

A signature policy can (indeed, perhaps should) be drafted by reference to a specific business application.. It does not ignore the fact that there is probably an existing business need for guidance or a set of rules which could be specified by two parties with no previous relationship who want to sign a once only contract electronically. However, it is unlikely that they will have the technical expertise to implement a signature policy developed under the present document and/or that such an implementation will be cost effective on a one-off basis. It is also unlikely that signature policies will be read or understood in depth by potential signers. It is perceived that the principle use of signature policies is to communicate a business requirement and signature context to aide system/application interoperability between different developers of an Enterprise application (such as modules developed by JD Edwards and SAP) or other XML-based developers such as Sterling Commerce, Documentum, Webmethods, Tibco and BEA Systems. Signature usage rules need to take into account an interface between human operators and a computer system. Only a person can make the decision to apply a signature. This is true even when the signature is on behalf of an organization or entity. Even where signatures are created as a part of an automated process, at some stage a person must have made a decision to configure a system to perform that task. On the other hand, it is feasible that a person may be guided through a signature policy through an application interface.

The present document provides a framework for specifying high level requirements for the acceptance by a business of electronic signatures. It then considers a set of signature usage rules for a number of aspects of the business requirements which could be used to inform an implementation of a signature policy. The rules are not organized into a model policy in the present document, rather clause 10 provides a framework for such rules.

1 Scope

The present document addresses signature policies to be used in the management of multiple signatures within extended business models. The concept of a signature policy is an important element for the establishment of a common basis for electronic signatures. However, there are many assumptions made regarding the application of signatures as well as concerns as to the use of signature policies by Relying Parties. TS 101 733 [1] already addresses certain aspects of electronic signatures for the establishment of a common basis for a signature policy. It already contains specification tools for the definition of signature policies but it is recognized that it still has to address other signature policy concerns such as multiple signatures, referred to as an extended business model.

The present document on signature policies elaborates on the signature policy concept (defining the meaning of the signature e.g. what the signature is meant to endorse), addresses certain aspects of multiple signatures (especially with respect to their current application in the paper world) whilst recognizing their applicability in all EC countries and for global trade, and if necessary propose extensions of the standard.

The objective of the first part of the deliverable, following an analysis of signature issues, is to identify the business requirements, while the second part is to make proposals to extend of TS 101 733 [1] Electronic Signature Formats, and TR 102 038 [2] XML Format for Signature Policies (and the corresponding RFC) to satisfy those requirements.

The work has been done in co-ordination with other bodies in the domain of electronic signatures, particularly in Europe; however, liaison with other organizations outside Europe has also been taken into consideration, such as European Forum for Electronic Business (EEMA), Internation Chamber of Commmer (International Chamber of Commerce), Asia Pacific ecomonic Community (APEC), the Information Security Committee of the American Bar Association, Radicchio, amongst others.

2 References

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

[1] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats".

[2] ETSI TR 102 038: "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies".

[3] CEN CWA 14171: "Procedures for Electronic Signature Verification".

[4] ETSI TR 102 041: "Signature Policies Report".

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

[6] Concise Oxford English Dictionary, Fifth Edition 1974.

[7] ITU-T Recommendation X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[8] IETF RFC 2630: "Cryptographic Message Syntax".

[9] ETSI TS 101 862: "Qualified certificate profile".

[10] ETSI TR 102 044: "Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates".

3 Definitions and abbreviations

3.1 Definitions

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

attribute: information bounded to an entity that specifies a characteristic of an entity, such as group membership or a role, or other authorization information associated with the Attribute Certificate holder

NOTE: An attribute may be further defined as an inherent characteristic or set of qualities closely associated with (bounded to) an object (person or entity).

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

NOTE: Optionally the certification authority may create the users' keys (ITU-T Recommendation X.509 [7]).

contractual signature policy: set of rules for the creation and validation of multiple signatures under which signatures on a contract can be determined to be valid

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 (ISO 7498-2)

public key certificate: public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it (ITU-T Recommendation X.509)

role: part played in a transaction or protocol; one's function, what one is appointed or expected or has undertaken to do

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 (IETF RFC 3126)

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

signer: person or entity that creates an (electronic) signature

signing role: role specified in a signature policy, allocated to or adopted by a signer, which defines the relationship between its signature and any other signatures as required by the signature policy

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

transactional signature policy: set of rules for the creation and validation of multiple signatures, under which signatures giving effect to a transaction can be determined to be valid

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

verifier: entity that verifies an evidence (ISO/IEC 13888-1) within the context of TR 102 045

NOTE: This is an entity that validates an electronic signature or signatures.

3.2 Abbreviations

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

ASN.1	Abstract Syntax Notation 1
CA	Certification Authority
OCSP	On-line Certificate Status Provider
OED	Oxford English Dictionary
OID	Object Identifier
TSA	TimeStamping Authority
XML	eXtended Mark up Language

4 Overview

4.1 Background research

The goal of the present document is to define a signature policy which would handle the validation of multiple signatures within a wide range of business models. The starting point for the research is to identify use cases for multiple signatures which were representative of business processes in the paper world. If possible, a use case for each type of multiple signatures should be identified: that is for stand alone independent signatures (parallel), countersignatures (embedded) and sequential signatures (primary) for example on a data flow or transaction chain. The focus was first on real world scenarios, and secondly on transpositions into the virtual world.

Sources:

A number of sources were used to gather real life experiences of the use of signatures, their use and meaning in the paper world, and experience of the transposition of signing processes into the virtual world. Information was gathered on an informal basis: the available resources for this project did not permit a structured comprehensive survey.

- Legal research, including case law, where available, and the personal experience of the author(s) as to judicial approaches to interpreting signatures in legal proceedings.
- Business experience of signature usage in a range of business scenarios, both "real world" and "virtual".
- Information from businesses included a number of jurisdictions: this focused on the European Economic Area, but also drew on business experiences and developments from third countries; the reason being that business needs, as regards electronic signatures, are universal and not particular to one jurisdiction.
- Information from a range of experts in information security and particularly electronic signatures: this included, but was not restricted to members of ETSI - ESI and CEN/ISSS E-Sign. It also included informal discussions with representatives from organizations which are regarded as leaders in this field.
- Authoritative literature from ETSI, CEN/ISSS, IETF, ebXML, OASIS, etc.

Results:

It became apparent at a relatively early stage that it would not be possible to write one generic "model" signature policy which would be capable of meeting the needs of diverse business models. Secondly, it was apparent that although handwritten signatures are traditionally required in almost any transaction of more than nominal value, many of those asked were not able to describe why a signature was required, what its commitment type was intended to be, how (or if) signatures were validated at any stage of the transaction, nor how such signatures added to the security of the transaction concerned. In fact, this confirmed the authors" expectations reinforced an existing impression, and lead the authors to investigate how real world business applications requiring signatures were being transposed into the virtual world. General information was relatively easy to obtain, however, more specific information such as how or for what purpose electronic signatures were used, proved difficult to obtain. There may have been two main reasons: the business application was at a relatively early state of development, and/or it was a proprietary product and protected by confidentiality and non-disclosure agreements.

The final source was from publicly available material, including recognized standardization work. Where the present document suggests new material, it has been subject to discussion with interested parties, particularly those working on similar issues.

4.2 Implications of the Electronic Signatures Directive 1999/93/EC

The recitals within the Directive [5] establish certain fundamental principles, in that the Directive:

- preserves party autonomy, i.e. that it does not restrict the right of organizations or individuals to contractually agree conditions under which they will accept an electronic signature;
- does not interfere with the rights of government agencies to determine the conditions under which they will accept electronic signatures;
- does not affect national rules of evidence and requirements for form;
- is intended to promote the development of the internal market and harmonization of signature practices.

The term "electronic signature" as used in the Directive is intended to convey technical neutrality. It is noteworthy that in the early stages of its drafting, the directive made reference to "digital" rather than "electronic" signatures. This changed in response to arguments that the Directive should not discriminate or inhibit the development of technologies capable of producing the equivalent of a handwritten signature, but which were not based on public key cryptography. The present document refers to "electronic signature" (article5.2), "advanced electronic signature" (article 2.2), and "qualified electronic signature" (as defined in article 5.1), but makes the assumption that these signatures are created using public key cryptography.

The Directive creates effectively three categories of electronic signatures:

- "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and ***which serve as a method of authentication*** (article 5.2);
- "advanced electronic signature" means an electronic signature which is:

    a) uniquely linked to the signatory;

    b) capable of identifying the signatory;

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

    d) linked to the data to which it relates in such a manner that any subsequent change of the data is detectable (article 2.2);

  NOTE 1: Recital 20 makes it clear that it is anticipated that an advanced electronic signature may be based on a qualified certificate.

- an electronic signature under article 5.1 which is an advanced electronic signature, which is based on a qualified certificate and created on a secure signature creation device, usually known as a "qualified electronic signature."

A qualified certificate, as defined in annex I must be issued by a Certificate Authority complying with annex II.

Secure signature creation devices are specified in annex III. Signature validation recommendations are in annex IV

Under article 5.1, Member States ***must*** ensure that qualified electronic signatures are given the equivalent status as handwritten signatures in legal proceedings. However, article1, recitals 20 and 21, which clearly preserve national rules relating to signatures and form, as well as judicial discretion in relation to the treatment of electronic signatures as evidence; substantially reduce the impact of article 5.1, so that it will not necessarily apply in all circumstances.

The definition in article 2.2 effectively reproduces the de facto criteria applicable to paper-based signatures. The effect of article 5.1 should ***not*** be interpreted as meaning that non-qualified electronic signatures cannot (or must not) be given similar recognition. It should also be noted that the Directive does not define what it means by a handwritten signature, and national laws as to what forms of signature have been accepted as handwritten remain intact. Therefore, the signature need not be formal; a signature may be a mark, initial, in pencil, or even (in England and Wales) a rubber stamp, providing it has been applied by the signer himself. It is also a logical conclusion that the Directive does not restrict itself to any particular commitment type which might be inferred from a signature. Therefore it should not be assumed that the Directive only applies to signatures which are intended to indicate a will or intention to be bound by the content of the document or data to which it is applied. The actual commitment implied by a signature can vary greatly, and cover a wide range of scenarios. (See clause 8.)

There is no requirement in the Directive in respect of any electronic signature, that the signer must have ***an intention to create the signature***. This is the case even for qualified electronic signatures which ***must*** be given equivalent effectiveness to hand written signatures in legal proceedings. This element, which is often present in similar laws in other jurisdictions dealing with the legal effectiveness of electronic signatures, is missing, even from the definition of an advanced electronic signature in article 2.2.

NOTE 2: This clause of the present document seeks to draw attention to the fact that a simple compliance with the elements of a qualified electronic signature, as specified in the Directive, may not be sufficient to enforce, through legal proceedings, even an article 5.1 qualified signature, in some circumstances.
It is noted that there is considerable scope for the interpretation of the Directive, both in its implementation into national laws and where it falls for consideration in legal proceedings. When article 5.1 is read in conjunction with the recitals (in particular recital 20), it is apparent that a broad rather than narrow view should be taken as to the meaning of a "handwritten" signature, which is probably capable of encompassing the full range of what has been considered to be a handwritten signature in national jurisprudence. It probably is also capable of incorporating a range of commitment types for electronic signatures from data origin authentication to an expression of intention to be legally bound by the data (document) to which it is attached.

In order for a Court to find that an article 5.1 electronic signature has legal equivalence to, or the same legal effect as, a handwritten signature, it is necessary for it to be satisfied that the signer intended to create such a signature. This is particularly true where the signature is intended to show an acceptance of responsibility or a legal commitment to be bound. The intention could be expressed directly or indirectly, i.e. the signer created the electronic signature by a direct action, or by an application, or an automated process, under his control, which was intended to create a binding signature. This is very likely to be the legal position in both civil and common law jurisdictions.

In fact, electronic signatures created using public key cryptography, i.e. digital signatures, are ***not*** (unless there is other evidence) capable of demonstrating the signer's intentions. However, ***intent*** is an essential element of signing.

Signatures in the paper world perform two main functions:

a) they indicate a will or intention by the signer, which is ambiguous except by reference to the document to which it is applied, or to some other evidence; and

b) a signature is ***evidence*** of itself, i.e. of the act of signing.

Therefore, there are two elements which electronic signatures, as currently defined under the Directive, by themselves, cannot prove:

a) the ***intention*** to express a commitment; and

b) the ***intention*** to create the signature.

b) is also often referred to as the formality or ceremony of signing. These elements need to be incorporated into an electronic signature, which is intended to be the equivalent of a handwritten signature. (See clause 5.5.)

There is also no guidance under the Directive as to how an electronic signature created solely for data origin authentication purposes, is to be distinguished from one which is intended to have legal equivalence to a handwritten signature, which may (or must, if it complies with article 5.1) be recognized as such in legal proceedings. Signature policies may provide a method of making such distinctions.

NOTE 3: One should not ignore the possibility that signature policies may have relevance in situations in the paper world, where a document is not signed as such but where there are non-repudiatory factors, which can be inferred from context. In these situations, a simple (article5.2) electronic signature accompanied by a signature policy might be appropriate. (This may be particularly true in England and Wales, where common law precedents have eroded the intrinsic qualities of a hand written signature and where, in the business context, there is an inherent reluctance to change business practices which often ignore signature formalities.)

4.3 Extended business model

In the present document the concept of an extended business model has been taken to mean a business or commercial transaction, which may involve several actors/participants and/or multiple actions in its process and which may require multiple signatures to give it effect.

The approach is to look at the transaction context in which signatures are used, and then to conduct a more detailed analysis, from those observations of the essential elements of signature creation and validation. The document has looked at scenarios from the paper world, but also used experience in the electronic environment to provide information and guidance. The scenarios considered are the purchase of life insurance in Italy, a supply chain containing linked service level agreements, and the conclusion of a land purchase agreement (within the UK) These examples are included at annex A.

4.4 Signature scenarios

Variations in signature scenarios may be extremely varied. Therefore the attempt has been to focus on scenarios which may be typical to many jurisdictions and applications and have drawn on specific examples which demonstrate the essential issues which deserve special attention. The analysis has not been restricted to consideration of real world signatures which are created personally, in handwriting, by the signer. Therefore the ambit of real world signatures which are considered take into account the use of facsimile signature methods (typewritten, rubber stamps, fax, copies etc), signatures in the name of an entity (rather than that of an individual), official seals, rubber stamps which are not signatures per se, but which are often used to process documents or to denote official validation or approval.

The present document considers a number of scenarios common to business scenarios where signatures are used:

- two (or more) primary signatures, such as buyer and seller on a contract;
- a countersignature as "authorization" or witnessing of a primary signature;
- signatures which are applied as part of a document flow, i.e. which assume a responsibility for a defined part of a document or transactional process;
- a combination of signatures all of which may be signed by another party, e.g. a notarial signature.

4.5 Introduction to signature policies

A signature policy is a set of rules to create and validate electronic signatures, under which an electronic signature can be determined to be valid [1]. A given legal/contractual context may recognize a particular signature policy as meeting its requirements. In some circumstances, the signature policy may be negotiated between the parties for a proposed course of business dealings. A signature policy may also be issued by a party relying on the electronic signatures and selected by the signer for use with that relying party. The terms will be applicable to both parties, as to how they apply and rely upon signatures, and may be determined by one party and imposed on the other. For example, the case where a large organization deals with a number of players, e.g. public procurement, or a business dealing with a number of suppliers/deliverers or customers. Alternatively, a signature policy may be established through an electronic trading association for use amongst its members. Both the signer and verifier use the same signature policy.

4.5.1 Signature policies in the "paper" world

In the paper world the meaning of a signature is usually inferred from the context in which it is created and/or from the text it is applied. Implied signature policies are also prevalent in the paper world, and it is not uncommon for one or both parties to a transaction to specify that a document be signed by a person with apparent authority, or that it be witnessed or notarized. Frequently, these practices have their origins in statute, but have been copied to provide additional security in business transactions, where laws are not mandatory. They have become established by custom and are implied rather than explicitly agreed as a "policy" between parties. The signing of a personal cheque is probably one of the most commonly used examples. The meaning of the signature, i.e. to authorize a payment is well understood and no-one would realistically seek to claim that his signature on a cheque means anything else. The signature must be dated, and (in some jurisdictions) the signer writes on the cheque the place where it was signed. In some circumstances, a cheque guarantee card must be presented with the cheque; or some documentary proof of identity of the signer is required.

4.5.1.1 Statutory signature policies

There are numerous examples in the laws of all jurisdictions of legal conditions surrounding the creation of a signature in order for it to be valid:

- requirements that the signature be created by writing, or under the hand of the signatory;
- that the signature is countersigned or witnessed;
- that the transaction is notarized.

These most usually apply in:

- wills;
- family affairs;
- transactions involving land;
- consumer protection and/or financial services;
- contracts for guarantee or surety;
- requirements under company laws.

4.5.1.2 Customary signature policies

Very often, business has copied statutory requirements for signature creation and imposed similar requirements by agreement. Counter signatures are often required in the internal administrative processes of large organizations. Its purpose is to ensure that employees work within their authority, and to provide checks against error of fraud.

Witnessing or notarization is often agreed where the proposed transaction is particularly valuable. The only sanction for failure to comply is that one party may refuse to accept that a valid agreement exists. Challenges against the voluntary imposition of such conditions are rare.

In electronic commerce, there are few examples of laws where existing statutory requirements for signatures have been translated to meet the needs of the electronic environment. (The Directive [5], article 5.1 provides that an electronic signature which fulfils the requirements of that article must be recognized as the legal equivalent of a hand written signature, but does not deal with aspects of the meaning or commitment type implied by an article 5.1 signature, nor the intention, or absence of intention, by the purported signer, to create the signature.) There are even fewer examples (if any) where customs and procedures relating to electronic signing have become established.

Outside formally regulated business protocols, transacting parties have the freedom to determine under which conditions an electronic signature can be deemed to be valid or becomes binding in their business context. All such rules and conditions are the basis for establishing the validity of an electronic signature and can be drafted in a single policy document called the signature policy. A signature policy describes the scope and the usage of an electronic signature with a view to address the conditions of a given transaction context. A signature policy may be written using a formal notation like ASN.1 or XML or in an informal free text form provided the rules of the policy are clearly identified. TS 101 733 [1] was developed around the scenario of being able to verify one single signature against one signature policy. If a document bears two signatures, each signature is verified independently from the other. Within TS 101 733 [1], there is no defined means to validate the relationship of each signature to the other.

Signature policies may be implied from the context, but may be useful where the requirements surrounding the creation of a signature are more complex, e.g. because:

- the formalities of signing are an important part of the signing process;
- the document or transaction requires multiple signatures;
- the transaction is of high value, and the electronic signatures must be robust.

It is desirable that signature policies should be machine processable, however, they may also need to be human readable (either as a business need, because of value or complexity or specific need e.g. laws of a specific jurisdiction, or because it must be capable of being processed by the man in the street).

4.5.2 "Real world" signature policy example - Banking

Based on the conclusions drawn from the analysis of real world business processes and the use of signatures, it is highly likely, in some cases, that signature policies will be created to support electronic signatures in the electronic environment. As in the paper world, these may be created by statute, by the establishment of technical standards, business custom, or by agreement between contracting parties.

The most obvious "real world" example of an implicit signature policy is a personal cheque. Cheques are an instruction to the issuing bank to transfer funds to a payee; the issued form of cheque must be used and it must be completed correctly or it will not be accepted by banks. The signature creation policy is defined within the cheque itself. The validation policy is described in the bank's cheque processing procedures which are outlined below.

The document:

A cheque usually contains a distinctive background, making it unique to the issuing bank; it has printed on it the account holder's name, account number and identifying information about the issuing bank. Account holders are also aware of their responsibility to keep the cheque book secure, to report any stolen cheques immediately so that the bank can stop any unauthorized payment.

NOTE: This is no longer the case in Italy: for privacy reasons not even the account number is printed on the cheques. The issuing bank retrieves the account from the bank code and the cheque number.

The signer:

Cheques are usually personal to the signer, who is the only person authorized to use them. Their name is usually printed on the cheque, and a copy of their signature is held by the bank for comparison with cheques signed by them.

In some circumstances, cheques may be issued to a specified entity, usually one which has a legal persona. Officers of the company may be nominated to draw cheques and to sign them. Again the issuing bank will store copies of their signatures. A mandate will be given to the bank, specifying the persons with authority to write cheques and the conditions under which they may do so, e.g. cheques should only be accepted where they are signed by two authorized persons. In the case of larger organizations, cheques and the authorizing signature may be printed as part of a computerized process: again the rules relating to the drawing and payment of cheques will be agreed in advance between the account holder and the issuing bank.

There are other standard banking rules for situations, for example, where a counter cheque is issued, or where an account is opened on behalf of an organization which has no recognized legal persona.

Signature commitment type:

A cheque is the authorization of the account holder to the issuing bank to transfer the sum of money specified on the cheque to the nominated payee.

Timing:

A date must be written on the cheque. There is no means of verifying that the stated date is accurate, but an issuing bank will normally return to the payee, any cheque which is presented more than six months after the date written on it.

Location:

In some jurisdictions, the payer must write the location where the cheque was signed. Again there is no means of verifying that this is truthful information, but information which is unusual may alert the payee or issuing bank of a potential problem. The information about where the signature is created could have relevance to jurisdiction in the event of a dispute. Even if the information about location is inaccurate, providing the payee and the issuing bank accept the information, it could, in most circumstances, be argued that they have waived their rights to argue about the point at a later time.

Formalities:

In relation to personal cheques, there are generally no particular formalities associated with signing. If an account is held in joint names or is a corporate account, then signing formalities will be specified in the bank mandate and must be observed in order for the cheque to be processed.

Technical and security considerations:

- the signature(s) on the cheque must match the specimen signatures held by the issuing bank;
- the rules set out in a bank mandate as to who and in what circumstances someone may sign must be strictly adhered to;
- the cheque must be completed in full, and errors on its face must be de minimis and initialled by the signer;
- the amount of the sum of money to be paid must be written in words and figures and must match;
- banks must comply with banking regulations as to the validation of signatures;
- banks have a duty to comply with money laundering regulations as to verifying the identities of their customers and reporting to the appropriate authority any suspicious transactions.

4.5.3 Electronic signature policies

Notwithstanding that the development and use of electronic signatures is still in its infancy, there are already examples of electronic signature policies available. article 5.1 of the Electronic Signatures Directive [5] is effectively a high level signature policy created by statute to specify conditions under which an electronic signature must be accepted as the equivalent of a handwritten signature in all member states. The German Digital Signature Regulations (Framework for Electronic Signatures, Amendment of Further Regulations Act (Signaturgesetz – SigG) of 22 May 2001) (Electronic Signature Ordinance (Signaturverordnung - SigV) (http://www.regtp.de) of 22 November 2001 implies a signature policy implementing article 5.1. The Italian Framework for Electronic Signatures,(Presidential Decree No. 513 (Regulations implementing Italian Law No. 59) 10 November 1997. (http://www.aipa.it/english[4/law[3/pdecree51397.asp) now supersede by the Presidential Decree 445/2000. Decree of the President of the Council of Ministers 8/2/2002 http://www.interlex.com/testi/regtecn.htm (Italian only)) has general application but also sets out the requirements of the Italian Public Administration under which it will accept electronic signatures as being valid.

It is likely that, in time, "guidance" provided by national laws and examples set by government administrations will be adopted on a voluntary basis by business, ultimately forming a set of customary rules establishing standard business practices for electronic signatures. This would mirror what has happened over the centuries in the paper world.

It is perceived that the principle use of signature policies is to communicate a business requirement and signature context to aide system/application interoperability between different vendors" enterprise applications or other solutions. Signature usage rules need to take into account an interface between human operators and a computer system. Only a person can make the decision to apply a signature. This is true even when the signature is on behalf of an organization or entity. Even where signatures are created as a part of an automated process, at some stage a person must have made a decision to configure a system to perform that task. On the other hand, it is feasible that a person may be guided through a signature policy through an application interface.

5 Analysis of signature issues

As a preliminary step to formulating a signature policy, it is necessary to understand the role and meaning of signatures as used in the paper world. Signatures are so much a part of everyday life that they are taken for granted. Very few jurisdictions provide legal definitions of a signature, the notable exception being France, where a definition is contained within the Code Civil (see Bibliography). Rules for signing, both statutory and customary, have evolved over centuries, so that an analysis of their legal base is complex. This is further complicated by the fact that such rules have evolved with marginal differences across the European Union member states. A detailed comparison of the evolutionary process is beyond the scope of the present document, which confines itself to observations of how signatures are used in business transactions today.

Looking retrospectively, it is clear that "real world" signatures were not restricted to manuscript signatures representing the name of the signer. Other forms of acknowledging a commitment have been acknowledged by Courts to be valid forms of expressing a commitment: such as engraved stamps, rubber stamps, and seals. Even a tick or cross can amount to a signature in some circumstances.

In England and Wales (and the USA) there is a body of legal precedent which considers the legal validity of non-manuscript signatures, intended by the signer, to have the same validity as a handwritten signature. This is not within scope of the present document. What however, does need to be considered, in the present document, is the commitment indicated by the application of such signature forms, which are in common everyday use. Examples include the imprint of a stamp which might be made by a bank clerk on a cheque stub, indicating receipt by the bank of that instrument. Typically, the stamp indicates a date, the name of the recipient bank and is often accompanied by a squiggle purporting to be a signature or initial of the clerk. An application for a grant of license or some other privilege might also go through a process, where authority/approval is signified by a rubber stamp impression on the original application form. Official court documents also often authenticate themselves by the application of a recognized official stamp. In the virtual world, these could all be managed by the use of an electronic signature, or even a qualified electronic signature.

It is also relevant to note that the evidential weight attached to some alternative signature forms may vary from jurisdiction to jurisdiction. Seals are rarely required by law in the UK, their value having been undermined by an eighteenth century fashion, where common seals became a fashion accessory. The intrinsic value of a seal, namely that it was recognizable and unique to the holder was seriously undermined. Since then, common law precedents and general custom have eroded the necessity for strict adherence to traditional requirements for seals, until finally, virtually all statutory requirements have been repealed. By contrast, in other European jurisdictions, seals have retained their status as an important adjunct to a signature. Notaries' governments' and companies' seals are obvious examples.

5.1 Transactional context/field of application

It became apparent from analysis of business scenarios that the signature role, meaning, and ancillary formalities of signing were often context specific. For example, signatures on a contract are not usually accompanied by explanatory text. Their position on the paper at the end of the contract is usually sufficient for a reader to understand that the signer intended to be bound by the terms contained in the document. A draft document may be recognizable in that it is annotated in such a way that it is (contextually) evident that no commitment to its terms was intended by the signer, e.g. by the inclusion of the words "Draft", "Proposed", or "For Comment". In such a case, the signature form may also be distinguishable: it may be written in the margin, or in pencil or represented by initials rather than a full signature.

The transaction context may also imply a set of signature requirements. In most instances, this understanding or interpretation is so much engrained in our everyday understanding of what a signature is, that it is easy to miss the subtleties. This has significant implications for the focus of the present document in relation to specifying signature policies.

5.2 Formalities of signing/intention to sign

One of the most important characteristics of a signature is the manner of its creation. Handwritten signatures are not simply the writing of one's name, but a stylized and often complex piece of calligraphy. Often referred to as the "ceremony of signing", it is the act of signing which draws the signer's attention to the significance of the commitment he is undertaking. The written mark or signature stands as evidence of that act. In the paper world, a signature is something more than just writing one's name, and it is well understood that the act of signing carries with it some commitment or legal consequence. The creation of a hand written signature is a conscious act and it is fanciful to suggest that a person can pick up a pen and make a signature without knowing that he is doing so. (This may be different from realizing what he is signing or what the consequences may be.) There are many degrees of formality to signing in the paper world, e.g.:

- simple signature;
- a printed declaration next to the signature space;
- witnessing;
- notarization;
- signature ceremony.

In some circumstances, little or no formalities for the process of attaching a signature may be required or desired. For example, where a purchasing manager raises dozens of repetitive purchase orders in a single day, to attach undue formalities may unnecessarily increase his burden and waste time. Repetitive funds transfers or trade on a stock exchange are conducted by skilled professionals; compliance with signature formalities wastes valuable time, in an environment where time may be of critical importance. Although the significance and value of each transaction may be high, nonetheless excessive signature formalities may be unduly burdensome to traders.

A good example of the effectiveness of such formalities in the consumer environment is the French custom of requiring the signer to write, "lu et approuvé", "bon pour accord", or "certifie sur l'honneur" immediately preceding the signature, which unambiguously draws the commitment type to the signer's attention. The requirement that the signer writes the words himself, minimizes the potential for future dispute about the significance of the signature. In other jurisdictions, printed text in close proximity to the space in which the signature is to be placed, performs a similar function.
E.g. "I ... declare that the information above is true" or "I agree to the terms and conditions…".

For significant transactions, a business meeting may be called where the parties formally sign and exchange documents at the conclusion of negotiations.

It is noteworthy that the Directive [5] does not make any provision for this element. In contrast with the laws of some other jurisdictions which have made provision for the legal recognition and equivalence of electronic signatures, it does not specifically require evidence of the will or intention to sign, either in respect of an advanced electronic signature, or for a qualified electronic signature.

5.3 Identity of signer

In most cases, a signature is worthless if it cannot be attributed to the purported signer. It is therefore necessary to ensure that a signature is that of a specified individual, e.g. where a contract names an individual as a party to be bound by its terms. In the paper world this is often achieved by printing one's name under the signature. In some business scenarios, the role or attributes of a signer are at least as important as his identity, if not more so (see below). It should also be noted that the function of a signature historically was not as a means of identifying the signer, but to impress upon him the significance of the commitment he was about to undertake. (The origin of the concept of signing was to make the sign of a cross, not to write one's name: a scribe then wrote the signer's name next to the cross as a means of identification. This also reveals the early root of the concept of witnessing.)

5.4 Roles and attributes of signer

In many business scenarios it is enough that the signer has "apparent authority" to act on behalf of the organization he purports to represent. Contracting parties, in most commercial situations, are not required to verify the status and authority of the individual they are negotiating with. This applies to employees and agents, and is well established in the laws of most jurisdictions. There are obviously some exceptions: transactions for the sale of land, filing company financial returns, and other types of significant or high value transactions may require the signature(s) of designated company officers in order to be effective. In practice, there appears to be a demand from business that in the electronic environment, an apparent (or claimed) authority to act should be supported by some verifiable evidence. This could be in the form of a public key certificate, an attribute certificate, or by some other certified information. Given the desirability that this type of information should be capable of timely verification, preferably by an automated process, it would enhance business processes, if standard business roles could be categorized and referenced for example by an OID.

5.5 Signature commitment types

In the "real" world the meaning, or more specifically, the precise nature of the responsibility assumed by signing, often has to be inferred from the circumstances surrounding the creation of the signature. In many instances, this is so well understood that the subtleties of the responsibility which is undertaken by the act of signing is implied and inferred from the context without further analysis. Some of these subtleties may well translate effortlessly into the electronic environment, e.g. receipts for e-mail, others less so, e.g. click wrapped contracts. This latter example continues to trouble website designers and lawyers alike. It is precisely because the commitment which is to be inferred from this method of "signing", i.e. evidencing an intention to be bound contractually, is ambiguous, that difficulties arise and contracts may be unenforceable.

Common types of commitment are:

- signing a draft (e.g. a contract) to identify the status/integrity of the draft under discussion, but no intention to be legally bound by the draft contract;
- signing a contract (i.e. with an intention to be legally bound);
- an acknowledgement (proof) of receipt.

5.6 Timing and sequence

It is well understood that the sequence in which signatures should be appended to a document has real life meaning. For example where the signature of a superior company officer is required to authorize or "sign off" a piece of work, it is obvious that that signature should come after the primary signature of the employee who has performed the work. There are other examples, e.g. where a claim is made (signed by the claimant); later countersigned by an authorizing officer to avoid inappropriate or fraudulent claims. The latter may or may not also approve the reimbursement of the claim.

A witness must sign after the primary signer. This is also a good example of a situation where the timing of both signatures may be critical. A witness must see the signer actually make the signature; it therefore follows that one would reasonably expect his signature to be close in time to that of the primary signer.

Timing and sequence may also play a significant role as evidence in the signature validation process, e.g. if the signatures of a primary signer and his witness take place within a short time period and are in the correct sequence, there is a reasonable chance that the witness did actually see the signer making his signature. Without additional evidence, this does not prove conclusively, that the two people were actually in each other's physical presence, but it increases the possibility that they were. A substantial delay would raise questions as to whether the formalities had been adhered to. It perhaps should be remembered that there is nothing in a handwritten signature to indicate location or proximity and in many instances, where signatures are required; one trusts to the honesty of the witness, that he actually fulfilled his duties as such.

Timing and sequence may have relevance within the business scenario or transaction, in that one action must take place in a certain sequence or time frame in order to be legally enforceable.

In some business scenarios, sequence and timing may not just relate to the signatures on a single document, but on multiple documents which may all form part of a single process or transaction. In some circumstances, the validity or acceptance of an agreement/authorization etc may be contingent upon certain steps or approvals having been taken within given timeframes for example,

Italian life insurance scenario - the signature (or date) on a medical report should be recent, denoting that the information contained therein is recent and therefore relevant.

Trade: health certificate for an export should predate the shipping and be within a timescale that it relevant to its intended purpose. The same may be true for export/import licenses and letters of credit etc.

5.7 Location

Conventional handwritten signatures, in common law jurisdictions, may not require or provide evidence as to the geographic location of where the signature was appended. Nonetheless, the location, or jurisdiction, in which the signature was made, may have legal consequences in the event of a dispute, in determining where the dispute should be heard/subject to the laws of which jurisdiction.

In France, Germany, Italy as well as numerous other jurisdictions, writing a personal cheque requires the inclusion of the geographic location where the cheque was signed. This may only be a claimed fact, but it serves the valuable function of binding the signer to his assertion in the event of a future dispute.

Location as evidence: What is also important, in both civil and common law jurisdictions, is in whose presence was the document signed? In common law jurisdictions there may be requirements (which have the force of law or more often are imposed by agreement between the parties, or by custom) that documents should be witnessed by another person or by a notary. In civil law jurisdictions documents may need to be notarized. It should also be noted that the concept of the role of a notary (both US and European/Latin America) is being extended and developed to fit the needs of the electronic environment. In this sense, one should have regard to new business practices which are emerging.

It is almost impossible to build a verification mechanism/policy for physical location into a signature policy. Where signatures are made in front of a witness or notary, it is possible for that fact to be attested to by the witness or notary. It may be possible for a notary to keep a publicly accessible repository of notarial acts, but this imposes an unreasonable burden on the notary, and ignores the fact that many such acts should attract confidentiality. Private witnesses do not have the means to provide this service. At present, in the absence of a solution, it would seem that location is something which can be claimed but cannot be easily verified without extraneous evidence which would only be undertaken in the event of a dispute.

A notarized document may, in itself, provide trusted evidence of physical presence.

5.8 Longevity

The facility to reverify a signature after the event is taken for granted in the paper world. The durability of paper and ink means that the integrity of a signature is verifiable at least within the lifetime of the signer, and perhaps also, long after his death. The same may not be true in the case of an electronic signature.

The optimum time to verify an electronic signature is at or shortly after the time of its creation. This may ***not*** be at the time of reliance, and research for the present document indicates that the party best able to conduct the verification process may not be the relying party. However, there are circumstances in which it may become necessary to reverify the signature, for example in the event of litigation, or allegations of fraud or compromise of the electronic signature itself. There are two means of addressing longevity issues: firstly by building robustness and longevity into the electronic signature itself - this could include further (newer, more robust electronic signatures to the original to prolong evidence of its integrity); secondly by verifying the signature at an early stage, capturing the verification data and maintaining a secure archive and audit trail of that data. The approach which should be taken may depend on the purpose for which the signature is being used. For example, signatures which give effect to a contract which may not be performed for a considerable period of time, possibly years in the future. Or a signature on a will which may not be relied upon for decades after it was created.

NOTE: IETF RFC 3126 (September 2001) and TS 101 733 [1] allow for a "grace" period in the verification process to allow for certificate revocation requests to be published.

5.9 Technical and security considerations

These play an essential role in relation to "real" and electronic signatures, increasing trust and confidence that an electronic signature or the data to which it is attached has not been altered or compromised.

Paper world security considerations:

- requiring a handwritten signature (i.e. in writing, under the hand of … etc.);
- requiring a cheque card, with a specimen signature;
- maintaining a specimen signature on a database;
- requiring identification, or personal attendance e.g. witnessing/countersignatures/notarization.

Electronic world security considerations: equivalents in the electronic world have focused on technical considerations, such as certificates which offer higher levels of quality:

- as to the identity of the holder, and/or restrictions on the permitted use of the certificate, as well as quality, e.g. the issue of a qualified certificate under the Directive [5] (or in USA certificates intended for non-repudiation purposes);
- the development of secure signature creations devices.

Under the Directive [5], it is possible to identify some broad categories of electronic signature type:

- simple e-signature (article 5.2);
- advanced electronic signature (article 2.2);
- advanced electronic signature + qualified certificate;
- advanced electronic signature + PK certificate + scd (or sscd);
- advanced electronic signature + qualified certificate + scd;
- qualified e-signature (article 5.1);
- qualified e-signature + CA accreditation.

5.10 Multiple signatures

Some documents may only require one signature to give it effect. These are comparatively rare in a business context: usually they are restricted to claims, such as an insurance claim or an application form, or declarations, such as a tax return. Most types of documents require more than one signature before they are "effective" and binding. It is almost taken for granted that a contract must contain signatures from all the parties to it, e.g. buyer and seller. One without the other will not bind either party: the contract will be unenforceable and the transaction potentially ineffective. Similarly, where custom, legal requirements or business agreements dictate that more than one signature is required to give validity to a document or transaction, failure to comply may result in the unenforceability of terms. Other types of document, such as a deed which are signed unilaterally by the party making the commitment, usually require the primary signature, to be witnessed, or notarized. Legal rules may exist as to how those signatures should be created. For example, where there is a requirement (statutory or agreed) that a signature on a document must be witnessed, the signer must sign in the presence of the witness; the witness must sign after he has seen the testator make his signature; the signatures must be on the same document. The same applies to the notarial act: there is a legal set of procedures which the notary must perform. Many of these legal rules are common to most jurisdictions; some, however, may have only national relevance.

In a business transaction, signatures on more than one document may be required in order to give effect to the transaction. Examples are:

- an export licence, bill of health etc. before a contract to export/import goods can be effected;
- the signed release of a mortgage, by a mortgagee or other party holding a beneficial interest in land, before the land can be transferred or sold.

For simplicity, the present document restricts itself to the concept of multiple signatures on a single document, but it should be noted that the concept of a discreet document has less relevance in the virtual world, where data can be manipulated (processed) without the physical restraints of piles of paper. There are many examples where the elimination of paper has produced a more stream-lined data flow with increased efficiency and cost savings. There is no reason that business transactions could not be approached in a similar manner, with signatures being applied within a defined electronic protocol.

Sequence and timing of signatures may have critical significance to the business transaction, i.e. one signature may or may not need to be applied before the other. In the paper world, it is conventional to date a signature. The date is a separate element, but so closely connected to the signature, that it is impossible to ignore its significance in the context of considering signature policies. Additionally, in the electronic environment where real world where the context in which a signature is created, may be lost, sequence and timing have significance in providing evidence which might replicate some of that context, e.g. demonstrating physical presence where a signature is required to be witnessed (not fool-proof, but helpful?).

5.10.1 Countersignatures

Countersignatures are used where the signature of another is required to give effect to, or activate a primary signature. Examples are where a signature must be witnessed either as a result of a legal requirement or an agreement between the parties; or where an employee's signature must be countersigned by a superior or another person in order for it to be binding. Again, there may be requirements as to how the countersignature is made. A witness must sign in the presence of the primary signer - therefore time, sequence and location are critical factors. A countersignature may have no such requirements save that it is applied over the primary signature.

It is difficult to specify general commitments for a countersignature. The term is most frequently used to denote the process of a superior or other person with a supervisory role "signing off" or authorizing the actions or proposed actions of another. For example, within a corporate entity, it could relate to a supervisor, approving or validating the exercise of authority of a subordinate, by countersigning the subordinate's signature. In some circumstances, a counter-signer does have a responsibility to check/validate both the primary signature and the data to which it is attached, e.g. manager counter signing an expenses claim. This is implied by the context. It may be that in other cases, the responsibility is only to add to existing data, as a transaction progresses or as a document goes through a process. General rules as to what a countersignature implies cannot be laid down. They will be constructed from an analysis of the business application to which the countersignature relates. The particular responsibility/commitment of the countersigner will vary from scenario to scenario and is likely to be determined by the procedures required by the specific transaction.

Often, it is the countersigner's signature that really matters, since it is the one that endorses the document. He can even choose to sign a document without a previous claimant's signature. Needless to say that in this case the countersigner is exposed to the risk the claimant denies having written the document.

It may also apply where a document goes through a specified or well-understood process, where each person or officer concerned in that process, is required to perform his functions and add a signature to the document to indicate that he has done so.

This process of counter signing may also have relevance within the context of signature validation. In many scenarios, a counter signature implied a checking of the identity of the primary signer and his authority to act. It therefore validates (potentially):

- the validity of the signature (it is recognized as being that of the purported signer);
- the identity of the signer;
- his authority to make the commitment indicated by the signature;
- by implication, his business role in making the signature.

These are matters which will have to be reflected in validating an electronic signature under a signature policy, although need not necessarily affect the way in which countersignatures are handled from a technical perspective. There needs to make a clear distinction between a countersignature in the technical sense and one which implements the business need. Decisions have to be made at the signature policy rules level as to ***what*** is being signed, ***and*** from a business/legal perspective, ***why*** it is being signed (i.e. what are the consequences).

NOTE: Although the term "countersignature" has been defined in technical standards (see RFC 2630 [8], clause 11).4to mean a signature which is applied to another signature only, it often has a meaning in a business context, which may be inconsistent with the technical meaning. It is important that it is recognized that the present document is considering the business use of counter signature, not the pure technical use, and this clause emphasizes the difference in meaning. The technical definition where the countersignature is nothing else than one among other unsigned attributes of some signature applies to a "policyless" straightforward electronic signature creation application. However, the purpose and scope of the present document is to suggest a means, i.e. in a signature policy, which will reflect the ***business*** concept of a countersignature. One signature creation application abiding by a signature policy (implied or explicit, it's meaningless) might require the countersigner to add an additional document to the pack and sign the whole of it, why not, after having zipped them all together to have a unique object.

5.10.2 Witnesses

The concept of witnessing a signature is a very old concept dating back to the Middle Ages. In those days, to sign meant to make the sign of the cross, not to write one's name. It was a mark of solemnity, to draw the signer's attention to the importance of the commitment he was making. The witness, usually a scribe wrote the name of the signer next to the cross (signature). From this developed the concept of witnessing. However, in modern law, and contrary to popular opinion, a witness is not required to validate the identity of the signer, only to attest to the fact that he saw a person whom he recognizes as having made the signature in question. He also has no interest in the semantics of the data to which the primary signature is attached.

In the virtual world, the role of the witness could be to ensure that the person applying the signature is indeed the right one. This mandates that the witness is able to verify that the name included in the certificate (that is itself included in the signed data) indeed corresponds to the person applying the signature. However, it should be observed that the physical presence of both the signer and the witness ***at the time of the signature*** may not be mandatory. The witnessing could be done after the signature has been applied. This is a major difference with the paper world situation, where the witness must actually ***see*** the person signing.

5.10.3 Notarial signatures

Notarial signatures are to be distinguished from counter signatures or witnessing in that they imply a specific function. We have therefore categorized them separately from any other signature model. The only exception which may be included in this category is that of commissioners for oaths (UK), i.e. persons who are entitled to witness the swearing of an affidavit. The reason is that such persons perform strikingly similar functions to those of a notary, although their powers are restricted to a very limited event.

The notarial act goes beyond mere witnessing of a signature, or consideration of documents and their form or legal validity. Notarization provides virtually incontrovertible evidence of the intentions of the parties to a transaction, their legal capacity to act, their authority to act, the legality of the transaction, its documentation, etc.

Notaries hold a position of trust, and notarization is rarely challenged. To this extent, we have taken the view that in terms of electronic signature validation, there should be no additional requirement to validate the notarial process, only that the purported notarial signature is valid. Once the notarial signature has been verified (or validated?) then there should be no reason to go behind it to verify the signatures of the parties to the notarized document or transaction. Notary is a trusted officer. It makes no sense to challenge their trustworthiness.

Specifically excluded from this category are e-notaries (see later) and USA-style notaries.

NOTE: Transposing notarial services, per se, into the electronic environment is entirely a different issue and far beyond the scope of the present document. There are technical issues associated with a notarial signature which is to be applied over multiple other signatures, as well as legal and ethical obstacles to be overcome. See also clause 10.5.4.

6 Formalities of signing

The physical act of writing his signature draws the signer's attention to the significance of the commitment he is undertaking. This "warning" mechanism may be lost where electronic signatures are used, unless there are additional steps which provide a similar context and meaning. This may not be achievable through purely technical means. The selection by the signer of a PIN to activate a key dedicated to article 5.1 signatures is, by itself, insufficient to prove that the signer intended to create a legally binding electronic signature. Permitting or compelling a signer to choose a commitment type from a drop down list provides no greater safeguards or certainty. In both cases, the signer can later deny that he intended the legal consequences implied by his signature, e.g. that he intended to choose another option, or not to choose one at all. Mistake, even unilateral mistake, i.e. where the fault is entirely that of the signer can lead to a signature being unenforceable against him. Additionally, both solutions have the potential to cause more confusion, where genuine mistakes are made by the signer.

Better solutions may be to require the signer to add some text, e.g. "lu et approuvé", (providing he can spell) or type his name; alternatively to cause warnings to appear about the consequences of signing. One of the most succinct methods of drawing the signer's attention to the fact that he is about to create the equivalent of a hand written signature could be to cause a picture of his actual signature to appear on screen as part of the process of creating the electronic signature. If this (or a hash value) is also incorporated into the data actually signed, it may provide evidence of the signer's awareness that he was creating an electronic signature intended to be the equivalent of a handwritten one.

7 Roles and attributes

7.1 Meaning of "role" "attribute" and "privilege"

The concepts of roles and attributes are frequently misunderstood and confused. The most common mistake is to take a role out of context, for example, taking a business role such a purchasing manager and inappropriately labelling it as a transactional or signing role. What may be a role in one context becomes an attribute in another, e.g. purchasing manager may be a person's business role, but that role becomes an attribute in a transactional context, where the role is that of a buyer. The purchasing manager's signing role may be that of a counter signer when he "signs off" the purchase orders of his subordinates.

In fact, the application of everyday definitions taken from the Concise Oxford Dictionary [6] is sufficient to explain the differences.

Role:

"actor's part; one's function, what one is appointed or expected or has undertaken to do".

Therefore, a role is part to be played in a particular operation or process or protocol. The role remains stable although different persons may take on the role. In a transaction, each role describes the acts which the role is expected to perform, and the responsibilities or commitments implied by that role.

Attribute:

"quality ascribed to anything; material object recognized as appropriate to person or office; characteristic quality"

An attribute may be further defined as an inherent characteristic or set of qualities closely associated with (bounded to) an object (person or entity). Therefore the business role, i.e. the set of authorities (privileges) and responsibilities which are associated with it, becomes an attribute of the transactional role.

Privilege:

"right, advantage, immunity, belonging to person, class, or office; …… special advantage or benefit, ...".

The privilege may be access rights, or authority to sign etc. In some circumstances, a privilege, i.e. often a right to take some kind of action, or perform some function such a signing, can also amount to an attribute.

From the above, it can be concluded that a ***role*** is a "*relatively stable"* behaviour pattern based on a set of qualities, i.e. ***attributes***, and/or ***privileges***. The person holding the role may leave and be replaced by another, without affecting the role itself. Similarly, the role may be up-dated or changed, without necessarily impacting on the identity of the person associated with it. In a business environment, each role has a set of attributes and privileges associated with it. These attributes result in authority to act, or access privileges (for example). Within the context of a signature policy, the business or transactional roles become the attributes of the role of the "signer".

7.2 Claimed versus certified business roles or attributes

In the paper world, business relationships are built on trust accumulated over a course of business dealings. It is the exception rather than the rule that a signer's role or authority be verified at (or shortly before) the time of signing, e.g. whether he holds certain office, or authority. An individual's business card or company letterhead is usually accepted at face value as evidence of the validity of claimed authority to act. The reason for this practice can be explained by laws which are almost universal: i.e. that an organization is ultimately responsible for the actions of its employees or agents and that an "apparent" authority to act, should be sufficient for a contracting party to rely upon in its business dealings with that organization. Therefore, in many cases, the veracity of a claimed business role or status or authority to enter into a transaction is taken on trust.

Where persons are conducting the transaction are at considerable geographic distance from each other, it may not be possible to assess the reliability of such claims face to face. Trust in such claims may be drawn from prior knowledge, or a consistent pattern of conduct etc. In some circumstances, there may be no good reason to deflect from this manner of doing business simply because the transaction is to be signed electronically: in others the electronic environment may contribute an added element of uncertainty such that the parties may not be satisfied with claimed attributes and require reliable certification in support.

7.3 Authority as an attribute

A business role, e.g. purchasing or sales manager, may imply an authority to perform certain functions on behalf of an organization. Professional roles may also fulfil these functions, e.g. a medical doctor having authority to prescribe drugs. However, additional information may be required as to the extent of the value of the authority, e.g. authority to enter into contracts the value of which is below a specified amount, or the scope of the authority, e.g. the doctor may only be permitted to write prescriptions drawn on a hospital pharmacy within the course of his employment. This is an internal limit set by the organization and may not be obvious to a contracting party. There appears to be a growing concern that for the purposes of electronic commerce, a certification of that authority by the relevant organization may be a required trust component. Proof of authority may be required as part of a business agreement. In other cases, laws may require that only persons holding certain authority or status may perform certain functions, e.g. under English law, sale of land by a company requires the signatures of two company directors; annual company accounts must be signed by the financial director or company secretary.

7.3.1 Delegated authority

Delegated authority is an attribute of the signer which is relevant to the validity of the signature. Delegation, in the business world, may be expressly bestowed or merely inferred by the signer. E.g. someone signing on behalf of a superior may know from previous experience that in certain circumstances, authorization to sign would have been forthcoming had the principal been aware and available. Therefore where a signature policy allows for a delegated signature, it is important to specify whether ***actual authorization*** is required or whether ***claimed authorization*** (which may include inferred authorization) is sufficient.

Three situations in which authority to sign is commonly delegated are set out below. In this clause, consideration should be given to the circumstances in which persons acting under a delegated authority may be permitted to sign and subject to what conditions (if any).

Agency:

The acts of agents, save in unusual circumstances, bind the principals on whose behalf they are operating. When an agent acts for another organization, his representations and actions are usually binding on that organization even if they are not precisely in accordance with his instructions or his authority. This is to protect parties who rely on his ***apparent*** authority to act. There is not an automatic obligation on parties to check the validity or extent of his authority. The authority of an agent to act may be both express (as specified in the terms of his engagement) and inferred (by the agent) from his instructions and perhaps from a course of dealing with his principal.

Powers of Attorney:

Powers of Attorney may be intended to be very short lived, or irrevocable or unlikely to be revoked, e.g. a P/A for a day or so to cover a very specific function such as signing a contract, whilst the primary signatory is on holiday. P/A with longer time frames and broader delegated powers, such as enduring P/A for the elderly or persons under a disability need special consideration. This must always be actual authority and holders of a power of attorney have a duty to act only within the bounds of the delegated powers.

signing per proxy, p.p.; p.o.:

In most business scenarios, the issue of authority to sign is more relevant than whether a subordinate within a company purports to sign on behalf of his superior. If the signer is the employee of a company bound to a contract as a result of his signature, then in many cases the company will remain bound regardless of whether the employee acted properly. It would appear that most often this is a claimed authority rather than something which is specifically delegated. It is an essential part of everyday business life and appears to be utilized very often where a crisis demands immediate action and where the person with actual or primary authority is unavailable. It is also likely to be the most difficult to define rules for, as the circumstances in which it is likely to be used are often the most difficult to predict. Without this flexibility, many transactions may be frustrated.

Actual delegated authority, such as that granted to an agent or by way of a power of attorney may best be dealt with by the issue of a public key certificate, which contains attribute information as a certificate extension. The certificate should also contain a pointer, OID or other reference to the "document" which is the source of the authority. The validity period of the certificate should correspond to the intended duration of the delegated authority. Special considerations may apply to enduring powers of attorney. A revocation of an authority to act could therefore be dealt with conveniently by a revocation of the certificate.

Managing claimed or inferred delegated authority such as that represented by signing per proxy may be more difficult to manage in the virtual world. An approach to drafting a signature policy to manage claimed delegated authority is contained in clause 10.

7.3.2 Restricted authority

Usually, an employee or person acting in a similar capacity on behalf of an organization knows the limitations of the authority vested in them. Employers are bound by the actions of an employee in the course of his employment even if he exceeds his authority. There appears to be a perception for electronic commerce that some reliable method is needed to allow a trading partner to know the limits of an employees authority, particularly where his ability to enter into transactions above a certain value is restricted. There may equally be a desire on the part of corporate entities to develop some means of monitoring and inhibiting an employee from acting beyond his given authority. Restricted authority is effectively a negative attribute and may be particularly problematic to manage unless the relying party has an interest in ensuring that the positive aspects of the authority (i.e. authority to enter into transactions up to a specified value) is capable of verification. From a legal perspective, there seems to be little to encourage such an attitude where the relying party is protected by the principles of vicarious liability (i.e. the employer is liable for the actions of his employee undertaken in the course of his employment). It may be possible for an employer to make it infeasible for the employee to enter into any transactions through normal business communication channels without a valid certificate (including this certified authority), and after a period of business dealings, trading partners may be put on notice of a potential problem if the certified authority attribute is absent.

7.4 Categorization of roles

7.4.1 Business roles

On analysis, it is clear that there is insufficient consistency across the business community to be able to categorize business roles, save in a few exceptional cases. The reason is that roles, or more specifically job descriptions carry wide variations in authority and responsibility depending on the size and organizational structure of the business. There is a further problem in respect of professional roles or qualifications: for example, a lawyer qualified in France may fulfil the same functions as a lawyer in Germany and hold the same professional status, but the two qualifications are not recognized as being equivalent, in that the French qualification will not, on its own, permit the French lawyer to practise in Germany.

Categorizing business roles is beyond the scope (and resources) of this project. However, the following recommendations are made as to how this task might be undertaken.

Each role must be carefully defined, in terms of its title (in various languages and jurisdictions); its authority, privileges and responsibilities. Where two such definitions match, they can be placed in the same category. As a starting point, the present document recommends that this can only be achieved by reference to clearly defined, well established and understood existing definitions. Only reliable sources for this should be used, such as the laws of member states. In the company laws of most jurisdictions there are specific definitions of the roles of certain company officers, e.g. a director, financial director, shareholders etc. A detailed analysis should be made, and roles should not be placed together in the same category unless there is substantial similarity in all relevant aspects.

It is desirable and will promote the interests of businesses within the Internal market, if substantially similar business roles in member states can be identified and categorized. The advantages of categorizing certain business roles and allocating an OID (or other identifier) to each category are twofold:

1) it will enhance certainty;

2) promote harmonization in the internal market;

3) provide a "standard" against which businesses can define and allocate roles within their own organizations.

In order for them to be useful, they should not conflict with existing statutory definitions and concepts; AND must be capable of recognition and adoption in all member states.

7.4.2 Transactional roles in international trade

In TR 102 044 [10], annex B, there has been included an extract of the Italian Assocertificatori document on role certification. This is a real example on how roles can be classified and identified by an OID-like code.

7.4.3 Signing roles

Signing roles exist as a means of managing multiple signatures creation and validation under a signature policy. They may be described as either business or transaction roles within a signature policy. They are always allocated or claimed roles, as within a protocol. Where there is a perceived need for a role to be certified, this becomes an attribute of the signing role and should be managed as such. Signing roles are discussed in greater detail at clause 9.4.1.

8 Commitment types in electronic signatures

This clause should be read in conjunction with clause 6.

In the paper world, the meaning or commitment type of a signature is implied from the context (including reference to the document on which it is made. It is not usual for a signer to have to specify which of them he intends at the time of signing. It is likely that in the majority of cases, that this will not be necessary in the electronic environment. To provide an electronic signer with a lengthy list of options for commitment types and ask him to select one may create confusion and is not likely to be of benefit to a relying party. It is likely that degree of ambiguity around the meaning of real world signatures has developed as the most efficient method of using and interpreting signatures. It is capable of addressing a situation where the stated intention behind a signature (probably after the event) is inconsistent with the circumstantial evidence which can be derived from the actions of the parties concerned. Because electronic signatures are capable of addressing a wider range of applications than handwritten ones, there is a growing need to provide a recognized method by which a signer can demonstrate the purpose for which it is to be used. In particular, there is a need to be able to distinguish between electronic signatures intended for authentication purposes only and those which are evidence of an intention to assume a legal commitment. There is also a need, where the contextual information which would support an accurate interpretation of a signature in the paper world but is missing in the virtual world, to provide an alternative means of providing that information. Finally a commitment type (better described as signature type attribute) may assist in the management and validation of multiple signatures under a signature policy.

8.1 Real world commitment types

The following list provides a useful summary of the purposes for which signatures are used in the paper world. Subject to a few notable exceptions, it is *not* the recommendation of the present document that these commitment types be categorized for use in an electronic signature application or policy document.

The purpose of a handwritten signature may be to:

1) indicate an intention to be legally bound by the content of the document to which it is attached:

   - commitment as a buyer/seller;
   - commitment to an offer (e.g. offer open for a period of time);
   - or to accept (e.g. to accept terms and conditions);

     a) "lu et approuvé" (French);

     b) "bon pour accord" (French);

     c) "certifié sur l''honneur" (French).

   NOTE: a) and c) are all means of emphasizing approval and actually form part of the formality or "ceremony" of signing, although they may also emphasize a commitment type.

2) indicate approval of a document, e.g. of a draft (to be distinguished from signing a contract);

3) authorize or validate a document, i.e. bring it into force or distinguish it from earlier drafts e.g. a contract or legislation;

4) certify that a document is an authentic copy:

   - certify a copy of an official/public record, birth certificate, court order, extract from a register etc.;

5) "sign off" a document, i.e. approve and assume responsibility for its content, e.g.:

   - sign off drawings etc for safety in construction projects;
   - issue a company financial statement;
   - issue company accounts;
   - authorize information provided to shareholders.

6) attest to the validity/accuracy of a document, e.g.:

   - a tax, VAT return;
   - an affidavit;
   - an insurance claim;
   - Note "certifié exact sur l''honneur" (also correct for any individual claim for social security - certify the information is correct) is actually part of the "ceremony" of signing.

   NOTE: In respect of a tax return, the person on whose behalf the return is being filed signs to assume legal responsibility for the contents; and accountant may sign for his compiling the return, but on the basis of the evidence provided by the person on whose behalf he is filing the forms. Also, it should be noted that, in some jurisdictions, the accountant or financial person compiling the return may also have a responsibility for the return's accuracy, i.e. to the extent that he has correctly indicated all income and deductions as required by the rules, and in accordance with his client's instructions.

7) authorize a past and/or future action

   - sign a time/expenses sheet or authorization for a payment to be made;
   - a doctor signing a prescription;
   - a pharmacist filling the prescription;
   - authorization for surgery or treatment.

8) witness another person's signature;

9) notarize a document (cf. a commissioner for oaths - UK);

10) acknowledge receipt of something e.g. of a registered letter, (read, not read - does not indicate consent);

    - or sign a delivery note.

11) establish a claim or ownership, e.g. signing a painting,
or acknowledge a transfer of rights or ownership, e.g. sign a deed for a transfer of land;

12) sign a marriage certificate;

13) make a declaration, e.g. a will;

14) make a declaration according to a rule of law e.g. a statutory declaration (UK);

15) indicate a document has been through a process, e.g. checking that its form or content is correct, such as a clerk checking the form of a document is correct and all relevant clauses have been completed and/or signed without actually making a judgement on the quality of the content;

16) signing or initialling a document, perhaps on each page to indicate that the contents have not been tampered with, and are complete. Signatures or initials are also often used to show the authenticity of alternations to a draft. These types of signature are easily replicated by simple electronic signatures;

17) test signatures, i.e. signatures which are not intended to have any legal effect or commitment, but are created in order to test a system;

18) signatures which have no meaning or intent, such as those created in the course of a game or play acting, or autographs. (These, although valid signature forms are not so significant as to fall within the scope of the present document.)

8.2 Electronic commitment types

Electronic signatures present their own unique problems. Much of the contextual information surrounding documents and the associated signatures is missing in the virtual world. It is from the contextual information, that inferences could be drawn about the status of a document and any signatures; such as whether the document was a draft or a final contract, whether the signatures intended to indicate a legally binding commitment or just an approval of its contents. The type of paper, handwritten amendments, the use of different pens or pencil markings, the presence of a full signature or initials all provide relevant information. Electronic signatures cannot provide equivalent contextual information which can lead to uncertainty about the signer's intention.

There are three main areas of potential ambiguity. For the purposes of this discussion, it can be assumed that the signer had knowledge of the data to be signed, and intended to create an electronic signature. However, his intention could be:

- to apply the signature for data origin authentication only;

- to create the equivalent of a handwritten signature but not to indicate a will or intention to be legally bound by the content of the data which is signed (this could be an intention to sign a draft, an acknowledgement of receipt, or to indicate authorship or responsibility for a document);

- to express a will or intention to be legally bound by the content of the data which is signed.

There is perhaps a fourth possible category: that of a signature which is intended for testing purposes only.

It is important to define a means by which a signer can indicate the intended meaning of his electronic signature.

There is, therefore, a need to specify commitment types which will distinguish between an electronic signature as data origin authentication and an electronic signature as the equivalent of a handwritten signature.

Where the signature is intended as a handwritten equivalent, there is also a need to distinguish between:

- a signature on a draft, where there is knowledge and perhaps authorship of the content;

- a signature as an acknowledgement of receipt; and

- a signature intended as a legal commitment.

These are commitment types which should be expressly selected or approved by the (primary) signer at the time of signing.

Current methods distinguish between signatures used for data origin and those used for signing purposes through the use of pre-selected of key usage bits or key usage OIDs, as indicated in a public key certificate. However, this method should be relied upon with caution, unless it can also be demonstrated that the signer must have realized the implications of using such a certificate, and could not reasonably have made a mistake.

NOTE: This is precisely because the key usage bit or key usage OID is pre-set within the certificate. Even where the signer has agreed to a set of contractual terms governing the permitted use of the certificate, it should not necessarily be assumed that a Court will enforce his signature against him. A Court is likely to look at the signer"s intention at the time he created the signature. Providing the signer can establish that he did not intend to assume the consequences of his signature, a Court may not enforce it, even if he has misused the certificate, and is in breach of his contractual obligations. The key usage as defined in a certificate and the associated contractual terms may be used as evidence by a relying party, but they may not amount to conclusive evidence.

Countersignatures (where the countersigner signs a previous signature):

- authorization;
- witness;
- notary.

These commitment types are also likely to be expressly selected by the signer.

Administrative e-signatures:

- e-notary or administrative signature (record keeping).

In the paper world, the meaning of a signature is implied from contextual evidence, such as the document on which the signature is written or the circumstances in which it was created. Interpreting the signer's intentions is not a precise science. There is no established body of law or business practice which deals with how signatures should be interpreted. It is arguable that a degree of ambiguity is actually beneficial, and probably helps to avoid unnecessary disputes. This clause recognizes that some definitions of signature commitment types will be beneficial in the electronic environment. However, the present document recommends that such definitions are defined only where there is a clear and obvious business need to do so; also that any definition is made as broad as is reasonably possible.

A set of definitions for electronic signatures are set out at annex B.

8.2.1 E-notary signatures

Electronic notary services are increasingly becoming a part of the "trust" infrastructure supporting electronic business application. They encompass a broad range of subordinate services, largely associated with the administrative requirements involved in running a business. The term "notary" or "electronic notary" has acquired a particular meaning in this context. It does not refer to an electronic equivalent of traditional civil law notarial services, nor the US concept of a notary. It is generally used to mean a trusted third party service which validates authenticity and integrity of data at a given point (e.g. receipt or storage); and archives evidence of the validation for future reference. When the data is retrieved, and providing the trustworthiness of e-notary remains reliable, validation of authenticity and integrity of the data can be proved as at the time of "notarization". This concept often forms part of a broader "trust" service. Where electronic signatures are used as part of this service, it may be useful to select a commitment type which reflects this. Although the service is not directly concerned with data content, it does potentially give rise to responsibility for the data which is the subject of the service. That responsibility is evidenced by e-notarial signatures.

8.2.2 Electronic signatures as part of a validation process

In some circumstances, this concept of a trusted service may be useful to perform signature validations, particularly where relying parties may not have the capability to do this for themselves. It might also form part of an application which handles multiple signatures. The e-notary (verifier) performs the validation of signatures at an appropriate time after their creation, captures and signs and timestamps the validation data and/or result. That then stands as evidence for future reference.

8.2.3 Simple administrative e-signature

This is probably a form of e-notarial signature, but one which does not imply any review or consideration of what is being signed. It may relevant for archiving or record keeping purposes where the signer has no interest in reviewing either the documents or the signatures. This replicates what is now a legal fiction in the paper world that a record is created by a person, who potentially is capable of being identified (and remembering that he/she created the record!!!).

There are many instances where business transactions do not depend on a sole document, but require a number of properly signed documents to be gathered together before the transaction can be finalized. In this case the signing role is simply to electronically "staple" or join documents together, to signify that the transaction is complete or so that the next stage of the transaction can proceed.

EXAMPLE 1: An exchange of contracts: where each party to a contract signs his copy of a final agreed document, but the signed copies are not send to the other party until an agreed time, at which the contract becomes "accepted". It should not be assumed that a single copy of a contract will be signed by all parties. The binding of the copy contracts and associated signatures may be performed formally by a third party or by one party undertaking to perform the task on behalf of both parties; or simply by each party ensuring that the two copies are kept together as a single file as part of their records management system.

EXAMPLE 2: An export of goods may require a shipping contract, documents of title, insurance, export license and bill of health, before a ship can put to sea with the goods on board. If this process is to be conducted electronically, there needs to be a means of ensuring all relevant documents and signatures have been collected and validated. A simple administrative signature might be used to indicate the presence of the relevant material, although not the validity of it.

9 Multiple signatures

In the paper world, a relatively brief inspection of a document will be sufficient to give an indication that all the required signatures are in place and will provide a reasonable level of confidence in the effectiveness of the document. The same is not so easy to achieve in respect of signed electronic data where multiple signatures are needed. This clause addresses the means by which multiple signatures can be managed and therefore validated under a signature policy.

"Multiple" signatures can be arranged into various sub categories, each with a different purpose.

9.1 Parallel signatures

Parallel signatures are mutually independent signatures where the ordering of the signatures is not important. They "stand alone" and may be created independently of each other. Independent signatures are applies only to a hash of the data to which they are relevant, i.e. they are not applied to another electronic signature.

The signatures have an interrelationship only to the extent that all required signatures must be present (and valid) to give effect to the document to which they are attached, or to the transaction to which they relate. The most obvious example is the requirement for signatures by both a buyer and a seller on a contract.

NOTE: It has been argued that as a matter of technical security, this scenario should be handled by embedded signatures. If a contract is signed by the buyer and the seller independently, one could peel off a signature and add another (fraudulent) one. So would the original contract still be valid? The response to this is likely to be that the contract as between the parties who intended to make the contract would still be valid and enforceable. A legal commitment was entered into at the time both parties made the agreement and created their signatures. It is a question of proof or evidence as to whether the signatures were tampered with later. That proof is unlikely just to depend on technical evidence; circumstantial or contextual evidence will also be relevant. Also, for general commercial transactions, there is no rule of law or custom, which says that one signature *must* be applied before/after another. Sometimes the signatures may not even be on the same (physical, or electronic) document. If the contracting parties are concerned that their signatures may be tampered with, then they need to agree a procedure which a) provides an adequate level of security and b) will allow the production of evidence, if needed later. In the paper world this might currently be a requirement for a witness or notarization. For the future, parties may agree a technical solution such as embedded signatures. This can be included in the signature policy. However, it is not within the scope of the present document (and would be contrary to the principles of the Electronic Signatures Directive) to try to mandate methods of contract formation, or to change ordinary business practices.

Other examples for independent signatures requirements can be found in the law of corporations. Where a law requires the signatures of two (or more) directors of a company, the sequence of signatures on a document does not have any importance. The document is valid as long as it includes all the necessary signatures.

9.2 Sequential (parallel) signatures

Sequential signatures are of variation parallel signatures, but where the ordering of the signatures is significant. Sequential signatures also may or may not be applied to the same data content. This may include other signatures, but only as part of the data content; it is not a substitute for a counter signature or embedded signature as described below. It is useful to define this form of signatures in order to manage multiple signatures in a data flow or transactional context.

NOTE: Parallel and embedded signatures have been described in previous literature: sequential signatures are not a well-recognized entity.

9.3 Embedded signatures

Embedded signatures describe a scenario where one signature is applied to another, i.e. one is embedded in another. The sequence in which the signatures are applied is important and there is a strong interrelationship, i.e. the validity of the first signature is dependant on another. For example, where there exists a requirement that a signature be witnessed by another person: the primary signature is countersigned, i.e. the countersignature is applied directly to the primary: (an embedded signature). These types of signatures are required when at least one of the functions of the second signature is to attest to the reception of the document with the first signature. In addition, a countersignature may also attest to the following, either in isolation or in combination:

- verification or approval of the semantics of the data originally signed;
- verification of the identity of the primary signature;
- verification of the validity of the primary signature (perhaps by verifying the validity of a certificate, or in accordance with a signature policy).

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. In this case the notary's signature attaches not just to the electronic signatures of the parties but also to the document to which they themselves are attached. In some scenarios, for example where a person witnesses the signature of another, he has no interest in the document only in the signature which is being countersigned.

9.4 Multiple signature management

A signature policy, or more precisely rules developed under a signature policy can provide a framework for managing multiple signatures. The rules should provide for both the creation and the validation of signatures under the policy: however, depending on the business application concerned there may be greater or lesser emphasis on one rather than the other. For example, where the policy governs signatures to be applied as part of an in-house application, the emphasis may be on signature creation: i.e. if the signature creation rules are such that it is unlikely that a false signature could be created, validation rules may be a safeguard for quality control procedures and random checks rather than the norm. By contrast, where a signature is to be relied upon by a trading partner, the emphasis may be on generating sufficient validation data by which the reliability of a signature can be established.

As a starting point to managing multiple signatures, it is necessary to describe and specify the method of creation of each of the signatures required to give effect to the document or transaction in question. Each signature may then be validated according to the signature policy, e.g. TS 101 733 [1].

The second step is to define the relationships between the signatures. This can actually be done in two steps: firstly to allocate a "signing" role to each signature; secondly to associate some attribute data with each signature, which describes its purpose in the context of the signing procedure or protocol.

9.4.1 Signing roles

A signing role is a role specified in a signature policy, allocated to or adopted by a signer, which defines the relationship between its signature and any other signatures required by the signature policy. The purpose of a signing role is to enable the management of multiple signatures. It does not have any greater relevance within a transaction. A signing role is to be distinguished from a signature role as defined in TS 101 733 [1]. A signature role in that document means a role such as sales director, which may be either claimed or certified, but which implies some attribute(s) associated with the signer. A signing role does not, in itself, imply any attribute(s) associated with the signer, even when the role is described as, e.g. buyer/seller or employee/supervisor. This does not prevent attributes being associated with the signer.

In essence, the signing roles are:

- Primary signatures (PS): these are signatures applied in parallel, although there may be requirements that a primary signature (or signatures) must be countersigned (witnessed, authorized, notarized etc); there may also be requirements that primary signatures be applied sequentially.

- Countersignatures (CS): these are applied to one or more parallel signatures and other sequential countersignatures.

A signature creation policy specifies the number and relationships of signatures required to give effect to a document, data flow or transaction.

Thus, on a contract where a single buyer and seller are involved, the required signing roles would be:

- PS/1 = buyer;

- PS/2 = seller.

In principle, there is no limit to the number of roles that can be allocated, providing the basic framework for managing their relationships is maintained. In a more complex transaction, where, for example a sale of land may require the signatures on each side of two persons having an interest in the land, there would be addition primary signing roles. They would be:

- PS/1 and PS/2 = Buyer 1 and 2;

- PS/3 and PS/4 = Seller 1 and 2.

If the transaction takes place in a jurisdiction where the transaction is to be notarized, the notarial signature would be CS/1 (or for ASN.1, CS/1-4).

The signing roles may also be expressed by using a notional transactional or business role, but this remains a claimed role within the signing process. Buyer and seller are (of course) transactional roles. In respect of an expenses claim, the required signing roles may be:

- PS/1 = employee;
- CS/1 = manager;
- CS/2 = accounts' clerk.

These role descriptions should be viewed as transactional roles allocated to the signing roles. Certification of these roles as attributes or business roles falls outside the scope of this clause, although the signature policy may specify some means of ensuring that the employee does not, for example, sign as CS/1, i.e. as his manager. One method of preventing this may be to mandate that CS/1 signature be supported by an attribute and/or identity certificate.

There are also various methods by which the signing role can be handled within a signature policy. In an XML specification, it may be sufficient to define the signing role as it relates to each required signature within a "signing" protocol. Alternatively, the signing role may form part of the signed attribute data (see note) which is itself signed. Another method may be to specify the signing role (which is perhaps described as a transactional role: buyer/seller etc) as a claimed attribute of the signer. These latter methods may be preferred for specifications in ASN.1, as all relevant data is closely associated with each electronic signature, and could form part of an extension to a single signature policy (such as TS 101 733 [1]).

NOTE: As defined in TS 101 733 [1] (this equates to signed properties in TS 101 862 [9]).

9.4.2 Commitment types for electronic signatures

Commitment types can play a useful role in the validation of relationships between multiple signatures

The commitment type is a set of information which describes the purpose of the signature. Commitment types provide information to a relying party about the signer's intention in making the signature. They may be express, i.e. the signer consciously selects or approves a commitment type when he signs, or implicit, in that the commitment type field may be empty or its value is not drawn to the attention of the signer at the time of signing.

Commitment types for primary signatures are:

- final (legal) commitment;
- approval of data content;
- authentication;
- proof/acknowledgement of receipt.

Final (legal) commitment and approval of draft content should always include a notice to the signer and be expressly selected, or approved by him. Applications which do not provide this, and which cannot capture reliable evidence of the signer's intention, may result in the signature being unenforceable in legal proceedings. (This is regardless of whether the signature is proved to be "valid" under the signature policy and/or equivalent to a hand written signature.) Signatures for authentication may or may not need to be expressly selected by the signer and could be transparent to the signer, depending on the circumstances.

Commitment types for countersignatures are:

- authorization;
- witnessing;
- notarial.

Therefore, in the expenses claim scenario, a supervisor countersigning a primary signature of an employee, will show the commitment type as being "authorization".

There may be situations where a superior needs to override or assume the functions of a subordinate, e.g. a supervisor signing in the absence of a signature from an employee. In these circumstances, the commitment type may remain as "authorization" with a corresponding allowance being made in validation rules under the signature policy. Alternatively, a countersigner could adopt any of the commitment types (except "authentication") relating to primary signatures.

In addition to the above, a commitment type equivalent to the paper world practice of signing per proxy could be selected and added to indicate that the signer is claiming delegated authority to sign. However, it would never be appropriate for a per proxy commitment type to be selected with authentication witnessing or notarial signature types. Issues related to managing delegated authority within a signature policy are discussed further in clause 7.3.2.

Administrative signature type attributes:

- administrative (simple);
- administrative (e-notary);
- e-signature validation.

See clause 7.

9.5 Multiple signature validation

Each piece of information associated with a signature is capable of providing evidence of whether a signature policy has been complied with. By predicting a set of validation results from the signature creation rules, it is possible to make a comparison of the actual results to assess the reliability of the relevant signatures. Therefore, multiple signature validation involves three stages:

1) ensuring the creation and collection of relevant signature validation data;
2) predicting a set of validation results based on that data;
3) comparing actual results with the predicted results.

Firstly, each single signature must be validated according to a (single) signature policy. The relationships between the signatures must then be validated. This can be achieved by:

- checking that each required signature is present;
- checking that the role attributes correspond to each of the specified signing roles;
- checking that the signature commitment types correspond to the requirements of the signature policy and are appropriate to their respective signing roles;
- checking that each signature has signed the required data (e.g. that a countersignature has signed the relevant preceding signature).
- where sequence and timing are significant, that all timestamps are consistent with expected results.

The following example is intended to be illustrative only, and demonstrates how a requirement for witnessing might be validated under a signature policy. Similar principles may be applied to other signature scenarios.

EXAMPLE: Purchase/sale on an offer/acceptance basis, i.e. this is not a negotiated contract. The seller does not wish to leave his offer open for an indefinite period of time. For the sake of this example, the contract is to be signed by 2 parties (buyer and seller), each party's signature to be witnessed.

Logical association with data: i.e. what data is signed?

Signature creation rules:

- Buyer's witness (B/W) must sign Buyer's signature (B);
- Seller's witness (S/W) must sign Seller's signature (S);
- Timing and sequence;

- When was it signed?;
- What is the sequence in which the signatures were created?;
- Compare the results against a table of rules provided in the signature policy.

Signature creation rule:

All signatures must be time stamped by a TSA or using a trusted time source (optional, but to be specified in the signature policy).

Seller: time = Stime
Witness: S/W time must = Stime + not more than 5 minutes

Buyer: time = Btime
(Btime must = Stime + not more than 24 hours)
Witness: B/W time must = Btime + not more than 5 minutes

From this, it may be concluded that there is a predictable sequence of signatures, if the process has been concluded properly, i.e. S => S/W => B =>B/W

However, the following could also be correct, e.g.:

S => B => S/W => B/W providing that B, S/W, B/W signatures are created within 5 min of Stime.

If the actual signed data and the timestamps match one of the acceptable results' profiles, there is evidence that the multiple signatures have been applied correctly.

Other methods of validation of multiple signatures under a signature policy:

Comparison of identities contained in certificates:

Signature creation rules:

- The identity of the seller must not be that of the buyer;
- The identity of the seller's witness must not be the same as the seller;
- The identity of the buyer's witness must not be the same as the buyer;
- Optional: the identity of the seller's witness must not be that of the buyer's witness.

Comparison of attributes:

The validation of relevant attributes of a signer should be considered first of all within the validation under a single signature policy. However, there could relevance in comparing the information about attributes as part of the validation of signature relationships. For example, where a countersignature of a supervisor is required under the signature policy, it may be relevant to compare the attribute information of both the primary and countersignature to ensure that they both belong to the same organization. Where a specific role is allocated to a signing role, e.g. a manager, the signature creation rules could specify that a business role or other attributes must be certified and associated with the signature.

10 Signature policies

The signature policy [1] is a set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid. A signature policy, therefore, needs to state the conditions under which parties to a transaction agree to accept electronic signatures, and rules as to their creation and verification It is generally accepted that a signature policy consists of two halves: a signature creation policy, and a signature validation policy. The one should correspond to the other. The specification of signature creation processes allows for the construction of efficient and effective verification/validation processes. In the case of multiple signatures, the policy should also set out the rules governing the relationships between the required signatures, and for the validation of those relationships. A legal/contractual context may recognize a particular signature policy as meeting its requirements. A signature policy may be issued, for example, by a party relying on the electronic signatures and selected by the signer for use with that relying party. Alternatively, a signature policy may be established through an electronic trading association for use amongst its members. Both the signer and verifier must use the same signature policy.

A signature policy could potentially serve two business purposes:

- a statement of the procedures used by an organization or entity in the creation, validation and use of electronic signatures on its own behalf (i.e. to be relied upon by others); and
- a statement of the conditions under which an electronic signature will be accepted as valid by that organization (i.e. to be applied by others).

A signature policy may relate to the validation of a single signature (e.g. TS 101 733 [1]) or to multiple signatures on a single document, e.g. a contract; on the other hand they may potentially be very complex, managing signatures which are required at multiple stages of a transaction and which are necessary to give effect to the transaction, e.g. international trade transaction involving export/import controls. These policies may be distinguished from each other by naming them *transactional signature policy, or contract signature policy.*

It is also recognized (although it is out of the scope of the present document) that a signature policy may be useful in applications which do not necessarily rely on conventional handwritten signature. Procedures for safety testing, e.g. aircraft maintenance, lifting equipment could be recorded electronically and a safety inspection report produced. The safety "check list" may be completed (in the paper world by a series of ticks or crosses) by the mechanic, and is likely to be countersigned by a number of other persons, before the final approval is given. Each tick or cross may be created using an electronic signature which needs to be attributable to the mechanic or inspector concerned. A signature policy governing this process and the rules concerning the validation of the signatures could be a useful tool.

10.1 Legal effect of signature policies

The requirement to read a signature policy and its legal effect on a signature, in itself raises complex legal issues. Failure to read or follow a signature policy may ***not*** be treated in legal proceedings in the same manner as a failure to read or comply with terms and conditions of a contract. In relation to a contract, there is an established body of law, which is common to many jurisdictions, which deals with the enforceability of standard ***contract*** terms or "small print" which may not necessarily be read by the party to be bound by them. Providing the terms are reasonable and the party wishing to rely on the terms draws them to the intention to the party to be bound by them (in the present document, the signer) and makes them readily available to read, than they will be binding regardless of whether the signer actually read them. In relation to the enforceability of a signature against a signer, there is another, established body of law which requires the will or understanding of the signer to follow the signature if it is to be enforceable against him. That is, the signer must have understood that he was making a signature and, in general terms, why he was doing so. It follows logically, that a distinction needs to be made between the "small print" scenario and a signature policy: in the former case, the signer has demonstrated his consent (by a signature) to be bound by terms and conditions which he then seeks to retract; in the latter, there may be no consent at all (i.e. no valid signature) if the signer did not read or understand the signature policy.

10.2 Implicit or express signature polices

A signature policy may be express or implied. That is, it may be in the form of a detailed set of rules, or implied by applicable law or custom, or implied by the structure of a document. However, a signature policy might also be implicit in the sense that is built into a technical implementation, so that it is transparent to the user. This is analogous to the example of the personal cheque in the paper world.

There may be no need for an express signature policy, which is therefore to be assumed as implicit, when, for example:

1) the signing process is defined by well-established rules that do not need to be translated in an express signature policy; e.g. signing a bank cheque;
2) the signing context is uniquely identified by the application; e.g. tax filing;
3) the signature scope and the signers' roles are clearly stated inside the signed document; e.g.: notarized documents.

In cases 1) and 2), not only in 3), it is advisable to make explicit reference, within the document to the signature governing rules (e.g. "signature applied in conformance with Directive 1999/93/EC [5] article 5.1").

As a general principle, combining technical signature policies with human intervention appears inadvisable. Technology cannot cope with ambiguity and the risk of error and hence an inaccurate result is increased when there is human intervention introduced into a technical process. However, there must be an element of human intervention if signature policies are to be used to define rules around signatures which are intended to have the legal effect of handwritten signatures. Signature policies which are to be used by humans, need to be high level if they are to be understood and adopted, e.g. signatures will conform to the requirements of article 5.1; the issuing CA will be accredited; signatures will be countersigned by a person holding such an office, etc. They may be expressed or incorporated into a contract, as part of an organization's standard business terms. Where there is no need to allocate responsibility to another party to conduct signature validations, all that is required to be specified is the means of signature creation (e.g. where the relying party writes the signature policy). In the paper world, customers are often guided through a signature creation process as part of completing a document. The same could be achieved by electronic means. Signature policies could be conveyed using a standard form e.g. expressed in an XML document. Assistance to the signer could be "built in", for example, in signing an electronic document, a customer may be prompted to send a valid certificate, and the process would stall/fail if he did not do so. Examples of signature policies may include detailed technical specifications of how signatures are to be verified, they are likely to be transparent to the user, as part of an application, simply displaying a result to the user of the validation process.

10.3 Drafting a signature policy

The aim of this clause is to provide guidance for the drafting of a signature policy, which can be adapted to fit different business needs. Not all the options may be required, but where an option is chosen from the business rules, they should be supplemented by corresponding rules from the signature policy rules (both management and operational, and technical rules). Therefore, if the signature policy specifies that a countersignature is required, the high level statement may be supplemented by a subordinate set of signature policy rules. The present document provides guidelines for drafting such rules.

General principles:

Policies are high level plans which describe goals of the underlying procedures. They are a blue-print for an overall process. Subordinate to a policy are rules or procedures which state how the policy goals are to be achieved and/or implemented.

Policy must meet a business need and be devised from a careful analysis of the relevant business application. It should be capable of technical implementation.

The objective of a signature policy is to provide a set of conditions for the creation and validation of electronic signatures which will generate confidence in their reliability.

Where electronic signatures are to be relied upon by trading partners or third parties, a signature policy should provide an efficient and effective method of validating signatures. Therefore, it is signature validation which informs the creation requirements in the policy.

Claimed facts:

In principle, in the business world there are factors which may be claimed, but cannot be easily verified, and those which are capable of timely verification. The fact that some factors are not capable of verification should not necessarily mean that they should be disregarded. A statement of fact, capable of being produced in evidence, may be relevant regardless of the fact that its veracity cannot be proved or disproved. The maker of the statement has made an assertion by which he will be bound, potentially to his detriment if circumstances change. The recipient of the statement should then be entitled to rely upon it. To this extent, it may still be relevant to include in a signature policy requirements that the signer makes certain types of statement, such as where the signature was created.

Signature validation:

In the paper world, the factors surrounding a signature must be true at the time the signature was created. In rare circumstances, defects may be corrected, with the consent of the relevant affected parties, at a later date. Therefore the validation of a signature must relate to the time of creation, not the time of receipt, nor the time of reliance on either the signature or the data to which the signature is attached. E.g. if a signature policy requires that the signature should be created by the CEO of a corporation, then the person signing, must have been a CEO at the time, the signature is not made good by the fact that he may later have become CEO, neither is it invalidated by the fact that he ceases to be CEO shortly after its creation. Validation, itself, may take place at a later date, such as at the time of receipt, reliance or following a dispute, but the validation still relates back to the time the signature was made and the circumstances surrounding its creation. In some cases, the purpose for which the signature is required may not justify extensive and costly validation procedures. Many aspects of business transactions are taken on trust. It is for the parties agreeing to use a signature policy, or a party intending to rely on a signature to determine which signature policy will fit their business needs. Signature validation can take place in a number of ways:

- Validation by a relying party:
  Where a transaction depends on the presence of multiple signatures, this may an onerous undertaking, even though, in some circumstances, it may be unavoidable;

- Validation as part of the transaction process:
  In some transactions, the relying party may not be readily identifiable, or may not be playing an active part in the transactional process. Conventional safeguards such as witnessing, counter signatures and notarization are all real world forms of signature validation. Some transactions, e.g. involving a data flow, may be made more efficient by incorporating provisions for signature validation as part of that process. By making use of signing roles, the relationship of each signature on a single document can be defined and validated one against the others. The advantages of this method is that signatures can be validated close to the time of their creation, by a person well placed to detect error or fraud: the disadvantage is that the validation must be performed by a "trusted" entity (this need not be a third party) and that evidence of the validation and results may need to be captured and stored for future reference.

- Validation as part of the completion of an electronic document:
  Just as the form of a paper document and its completion may form a signature policy in the paper world (c.f. a personal cheque), electronic "documents"/applications could potentially fulfil a similar function. Indeed the functionality could be greatly extended to incorporate aspects which could not be achieved in the paper world.

10.4 Significant elements of a signature policy

A single written policy document is unlikely to be sufficient for most business applications and a technical implementation supplemented by human readable policy documents is likely to provide the most effective solution. It is envisaged, therefore, that a signature policy is likely to be designed at three levels, with each subordinate level drawing its parameters from the higher one. The levels are:

- business (corporate-wide) rules, describing at high level the conditions under which electronic signatures will be used within a business and/or the conditions under which they will be accepted as valid (i.e. where the signer is outside the organization);

- signature usage rules, consisting both of management and operational procedures, and technical rules, addressing the specific processes within the business (internal and/or external) and which describe how electronic signatures will be created and validated; and

- technical specifications.

By using this "umbrella" type of approach, a signature policy may incorporate a number of a subordinate signature policies (signature usage rules and/or technical specifications). These may be developed "in-house" or be drawn from external sources: it may be expedient to adopt a signature policy, standard, or protocol which has already become established in general business use. These subordinate signature policies may relate to single or multiple signatures. They may relate to different trust models (e.g. certification authority domain) and/or to different business models, however, they must all conform to the governing business rules, and adhere to the same levels of technical security, in order for trust to be maintained throughout the transaction. The "umbrella" approach allows scope for a signer to select from a number of acceptable alternatives. This also maximizes the potential for interoperability with other organizations which may have developed their own signature policies.

10.4.1 Business rules

At the highest level is a set of business rules. The may be applicable to internal processes as well as governing the terms to be agreed between trading parties at a contractual level. Between trading partners, they may be negotiated and agreed within a substantive contract, or be referenced as an entity's standard business terms or policy relating to electronic signatures. An organization may have more than one set of such rules depending on the context in which the electronic signatures are to be used. For the purist, these rules may be the signature policy in that they should state the requirements of the parties in order for an electronic signature to be accepted as valid. However, they may incorporate by reference or include matters which, for the purposes of the present document, have been included in the "signature usage rules". In some cases, the business rules may specify the use of an existing technical implementation.

It is suggested that the business rules include the following information.

- **Title/identification of signature policy:**
  Information about where the signature policy is available, for example a URL or by e-mail; and how a paper/hard copy may be obtained. This clause may also contain an OID of the signature policy.

- **Signature policy issuer:**
  There should be information as to the name and contact details of the signature policy issuer.

- **Business application domain:**
  This clause should outline the business domain in which the signature policy is suitable for use, e.g.:
  sale of goods/international trade transactions;
  B:B, B:C, G:B contract;
  transactions in land;
  consumer transactions;
  financial services;
  government taxation services;
  medical/health services;
  e-notary service.

- **Transactional context:**
  This clause should providing additional information about the transactional context, e.g:.
  RFP (request for proposal);
  offer letter (or other form of offer);
  exchange of design documents;
  draft of contract;
  acknowledgement of receipt;
  contracts requiring specific authorizations (e.g. because of value).

- **Consent to accept electronic signatures:**
  This clause should record the parties" actual or deemed consent to accept electronic signatures. Consent is required by the laws of some jurisdictions, and may be revoked on notice to the other party.

- **Proposed signers:**
  This clause may identify the proposed signers. Alternatively, it may specify the business role or attributes required in order for a signature to be accepted as valid. It should also state whether a counter signature, witnessing or notarization is required. (Effectively, this clause can be used to identify signing roles within a signature policy.)

- **Proof of authority:**
  This clause should state the type of proof of authority to sign which is acceptable. Where the parties have already established communications, and there is ostensible authority to enter into the proposed transaction, an identity certificate may be considered sufficient. In some cases, additional proof may be appropriate, an attribute certificate, or certified attribute information from a reliable source, such as a companies" registration office, professional body, or employer. This may include proof that an employee or representative is authorized to enter into transactions over a specified value. This clause may also include a statement about whether authority to sign may be delegated.

Where the document or transaction is to be notarized, this clause may be superfluous.

- **Signature commitment type:**
  Where appropriate, a signature commitment type may be used. See clause 8.

- **Formalities of signing:**
  The formality or ceremony of signing in the paper world is not easily transposed into the electronic one. However, there remains a business need, for some formalities to be in place, particularly where the transaction is of high value, involves consumers, or sensitive information. This clause facilitates a statement of such requirements, although the implementation may be governed by more specific details in the signature usage rules. (See clause 5.5)

- **Timing constraints:**
  - not before/not after.
  It is not anticipated that this clause will contain detailed technical requirements relating to the timing of signatures. However, at this level, it may be appropriate to express constraints on the timing of signatures, e.g. where an offer is made, which will expire after a given period of time, if it is not accepted. Details of how that should be implemented could be clarified in the signature usage rules.

- **Specifications of any security considerations:**
  This section deals (at high level) with requirements relating to technical or "trust" issues.

  - **The "trust" model:**
    It could simply in broad terms indicate a requirement for an article 5.1 signature, and or/specify that certificates must be qualified certificates and/or issued by an accredited certification authority etc.

  - **Longevity of electronic signatures/archiving**:
    This section may contain a requirement that signatures must remain trustworthy, and capable of validation for a given period of time: this might be appropriate where the performance of contract obligations may not take place perhaps for some years in the future.

  - **Archiving validation data:**
    There may also be requirements for the archiving of essential validation data.

- **Allocation of responsibility for signature verification/validation:**
  It should not be assumed that in every instance, it will be the party relying on a signature who will be responsible for its validation. Indeed in some cases, this may be impractical. It is possible that one the parties to a transaction may be nominated to perform this task, or that it will be undertaken by a trusted independent party. Alternatively, signatures may be validated by counter signers as part of a data flow. This section may also include an obligation to capture and archive validation data.

- **Audience conditions:**
  This section states the conditions under which a signature may be relied upon. e.g. the signature only valid in a specified jurisdiction, where laws exist which recognize the legal validity of signatures created under conditions as specified in the policy. Conditions relating to jurisdiction/governing laws should probably be used in this way with caution, as they could potentially have the effect of depriving the signer of benefits if his signature is not effective. However, this section could include provisions relating to the intended effectiveness of signatures, where multiple signatures are required, e.g. the signature of X may not be relied upon unless it is countersigned by Y.

- **Access control management:**
  This section provides rules about who may access data, and under what circumstances. This is not the same as a privacy or data collection notice, but may, for example, provide rules for controlling access to, and use of data which is protected by law, business custom or contractual obligations.

- **Dispute resolution procedures:**
  It is difficult to predict with any degree of certainty how effective rules created under this section might be. Signatures usually go to the root of any agreement, and a dispute over the validity or acceptance/refusal to accept a signature may well result in a larger dispute which would fall to be determined by a means beyond the scope of a signature policy. It is conceivable that in some circumstances the parties may elect to determine any dispute relating to an electronic signature as a preliminary issue under this section, but where there are substantial other areas of dispute, whether or not they arise directly from a disputed signature, it is more likely that all matters will be tried together in some other forum (e.g. arbitration or court.) On the other hand, provision for a cost effective dispute resolution procedure may be beneficial for example in the following areas:
    - customer (consumer) relations and complaints;
    - internal corporate affairs;
    - business transactions with longstanding trading partners, suppliers, distributors etc.
- **Boilerplate terms:**
  This business rules may form part of a contract or stand alone as terms and conditions of electronic signature use. They may be used to qualify a person or entities consent to accept electronic signatures. In such circumstances, it is appropriate to include some standard contractual terms, e.g. governing laws clause, rights of third parties, limitation and exclusion clauses.

An example of these rules may be drafted is set out at annex C. It relates to a simple offer/acceptance scenario, where the offeror is a bank or other lender making a mortgage offer to a potential borrower. It does not require the signature of the borrower to make it effective as long as it has been brought to his attention. It is also informative to a business application developer, without being unduly restrictive.

10.4.2 Signature policy rules

These rules should implement the business rules. If the business rules are roughly analogous to a policy statement, i.e. what is to be achieved; then this clause might be considered roughly equivalent to a practice statement, in that it should set out how (multiple) signatures are to be created and validated under the policy.

This clause is divided into two subclauses: management practices and procedures, and technical rules. These should be correspond to each other, and provide mutual support. That means that the management practices and procedures should provide guidance to operators (signers, verifiers and relying parties); and rules as to how any application implementing the signature policy should be used. Within, design of an application, it is desirable that a series of prompts and error messages could be incorporated so as to guide the human user through the signature creation and verification/validation process. Consideration should be given to constraints which would prevent the creation of an invalid signature (i.e. one which does not conform to the agreed conditions of signature acceptance as set out in the business rules); or reliance on a failed signature verification. Parameters may need to be set so as to allow some flexibility in circumstances where business needs may justify overriding strict adherence to the rules:

- management practices and procedures.

These are the procedures to be followed by the parties in the creation/verification of signatures, i.e. the human element. For example, it would include consideration of rules for:

- allocation of attributes and signing privileges to business roles;
- management and use of identity and attribute certificates;
- use of signature creation tokens, smartcards etc.;
- safekeeping of tokens, smartcards etc.;
- signature creation procedures (authorization, formalities of signing etc.);
- verification, and validation of countersignatures;
- attesting to, and archiving electronic signature validation data (where appropriate);
- disciplinary procedures.

Technical rules:

These are the technical rules which will inform an implementation. They should provide a greater level of granularity than would usually be expected in the business rules, which may have been negotiated by non-technical personnel. However, it is possible that these rules may be incorporated by reference into the business rules, particularly where they pre-exist as an organization/entity's standard terms for the use of electronic signatures. They may include consideration of rules relating to the following matters:

- identification and allocation of signing roles:
  - to business or transactional roles;
  - to an individual.
- use of and reliance upon certificates:
  - issuing CA/accredited/non-accredited;
  - other trust marks;
  - qualified/non-qualified certificate;
  - algorithms/key length;
  - sscd/token - evaluations/certifications;
  - use of OCSP etc services;
  - registration requirements;
  - conformance with ETSI policies/technical specifications.
- certification of signer attribute information:
  - use of public key/attribute certificates;
  - delegated/restricted authority (permitted/not permitted);
  - attribute certifier.
- time stamping:
  - time stamping authority/in-house time source;
  - use of trusted time source.
- signature attributes:
  - commitment type;
  - delegated/non delegated;
  - parallel/embedded/sequential.

10.5 Illustrations for signature policy rules

10.5.1 Countersignatures for authorization

In order to devise appropriate rules, some preliminary consideration of the purpose of the counter signature with the specific business/transactional context is required. Why is a counter signature required? What actions does the counter signer perform prior to creating the signature? What does the counter signature actually signify, i.e. what should be inferred from it? For example, does the counter signature:

a) indicate an action performed by a signer as part of a transactional process;

b) confirm a prior signer's actions and/or authority;

c) confirm the validity of another's signature?

Even where the technical meaning of a counter signature is used (i.e. that a countersignature signs data which is only the equivalent of the primary signature), it may still necessary to identify whether the intended meaning is b) or c).

In case a), the signer is indicating an assumption of responsibility for data which is relevant to his role in a process. It may be part of a series of actions, or stages of a transaction performed by a number of persons. Where each signature stands alone, (i.e. is not dependant on any other for its validity), these are parallel signatures, but the sequence and timing of their creation may be relevant to the validity/effectiveness of the transaction as a whole. In the paper world this may involve multiple signatures on a single document, or a signature(s) on more than one document, each of which is required to give effect to the transaction.

In case b), the countersigner "recognizes" or confirms a prior signature and the authority of that signer to perform certain actions, for example a senior officer "signs off"/authorizes the preparation of a subordinate. The countersigner may therefore be assuming responsibility for the data "content" and the primary signature appended to it. In this case it is necessary to devise rules which provide for the verification/validation of the primary signature. If responsibility is to be assigned to the countersigner for signature verification and/or validation under a signature policy, consideration should also be given to capturing and preserving for future reference evidence of the process and the results. It may be that the counter signer signs only the primary signature or he may sign the signature, plus the existing data "content". He also may add data which may be signed.

In the last case c), the countersigner only signs the primary signature, but he may add text which potentially has legal relevant as evidence of that action, e.g. his name and address, a statement to the effect that he has witnessed the signature.

Although, this detailed analysis of countersignatures is not usually conducted in the paper world, it is likely necessary to do so in order to draft the technical rules from which an implementation may be derived. Decisions have to be made as to what data is to be signed. Thereafter, the fact that data is or is not signed may become an issue in legal proceedings (in the event of a dispute) if a court or tribunal is called upon to interpret the intended meaning of the electronic signature and the liabilities and consequences which flow from that.

For the purposes of the present document the function in case (b) is assumed as an example which has been used to form the basis of a signature policy. The business rules may simply require a countersignature.

Business rule: Specifies the requirement for a countersignature as one of the conditions for the acceptance of electronic signatures.

NOTE: Authorization implies that the countersigner should validate the primary signature he is signing. It may also imply that there is some check, in a supervisory capacity, of the data with which the primary signature is associated.

1) Verification of time stamp;

2) Verification/validation of the "primary" signature;

   What should be checked?

   - the identity of the signer;

   - that the identity matches that contained in the certificate;

- the validity and status of the certificate;
- the signer's authority to make the commitment indicated by the signature; (by implication) his business role.

3) What other data must be checked?

- data which has been signed by the primary signer;
- any claimed attributes;
- the occurrence of preceding steps in the business application;
- previous validation results of preceding signatures

4) Archiving validation results

- what validation data must be captured (rule set)?
- are there applicable laws?
- should the validation data be signed by C/S?
- timestamped?

In addition, there should be a set of rules for the archiving of validation results. For example:

- where will the data be stored?
- who has responsibility for the archive?
- for what time period should the validation be stored?
- what security measures are required?
- what are the arrangements for backing up data?
- who has access rights, what are they?
- rules for retrieval of data.

Creation of the countersignature:

- identity (type of certificate required)
- role/attributes (proof)
- delegated authority (actual/claimed);
- declaration by C/S;
- commitment type (authorization);
- formalities of signing;
- time stamp.

What must be signed?

- primary signature +
- existing data which is signed by the primary signer;
- additional data (optional);
- declaration(s) by C/S (optional).

Validation of the underlying primary signature?

- by implication, i.e. by reliance on the validated counter signature;
- by checking the validation result signed by the countersigner;
- by repeating the entire validation process.

10.5.2 Countersignatures in a document flow

This assumes that the countersigner does not have an interest in the preceding signatures or data, except to note that they exist. (Parallel signatures) This scenario would cover circumstances where data is being processed and each signer adds data or performs a function within a business application. In this case the signatures would be in parallel, but the sequence and timing may be important. The management and operation rules would be similar to those relating to single signatures. The technical rules would cover matters relating to time stamps and validation of the ordering of the countersignatures.

10.5.3 Delegated authority

There is a need to state in the policy (if relevant) whether a signature created under delegated authority is acceptable or not. If yes, then the signature policy rules should state under what conditions it will be accepted, i.e.:

- must there be ***actual*** authorization (how should this be proved/verified?); or
- may there be ***claimed*** authorization (how can this be managed?).

Where the need to delegate authority is predictable, ***actual*** authorization can be certified in a public key or attribute certificate. The question which arises is how any restrictions on the use of delegated authority are to be defined and managed under a signature policy? If it is specified that a subordinate may sign in the absence of his superior, but the signature of his superior is preferred, how is this to be managed from a relying party's perspective? Even worse, how does one specify a verification method for ensuring compliance? The reality is probably that a decision has to be made as to who (or what role) may sign and specify all persons/roles which are acceptable.

In respect of ***claimed*** authorization, this usually occurs as a matter of expediency: someone is ill, or out of the office and a document must be signed urgently. Therefore, an appropriate person (who does not have actual authority in the normal course of events) takes the responsibility of signing in the hope (usually well-founded) that the signature will be effective and that he will not get into trouble for doing so. Sometimes, of course, it may be the absent person's superior who signs, which is less of a problem because this falls into the category of ***actual*** authorization, by default. The solution may be to state in the signature policy that delegated authority is acceptable (under exceptional circumstances), and then to specify a range of results in the validation process, which will not cause the validation process to fail, or which will allow the verifier to make a decision whether or not to accept a result and proceed with the transaction.

10.5.4 Notarial signatures

In this clause, a notary is taken to be a civil law (European/Latin American) notary, not the North American type of notary which is essentially a professional witness. It is recognized that there may be subtle national variations in the requirements of notaries and the notarial act. For this reason, any signature policy, requiring a notarial signature, may have to specify a country or jurisdiction (?)

In general terms a notary's duties can be summarized as follows:

- he must ensure that the data (document) has legal validity;
- that the signers have authority to sign;
- that they are aware of and understand the commitments they are undertaking,
- that they are mentally and legally capable of making those commitments; and
- that they do so of their own free will.

The present document does not attempt to write a signature policy for notarial signatures. There are two basic requirements of a notarial function which inhibit its being developed as an entirely "virtual" service. The first is the requirement of personal attendance before the notary. It seems unlikely (with current technology) that the assessment of the capacity, understand and willingness to sign, which the notary must perform can be properly executed without the signer appearing before him. This appears to be the view of many notaries. Therefore, the notary function cannot be conducted "virtually" for at least for the time being. The second requirement is that notarized documents must be archived in paper form by the notary. This may be less of a problem, since electronic archiving could be adequate for many types of notarized document, e.g. general commercial documents which do not require an extensive lifetime. In other situations, there may still be a need to require paper documents signed in manuscript by the notary and relevant parties.

NOTE: There are already legal and technical initiatives to transpose notarial services into the virtual environment underway in Austria, Germany, France and Italy.

It should, however, be recognized that transposing at least some of the notarial process could be efficient and useful to many businesses which engage in electronic commerce. For example, documents to be notarized could be sent to the notary in electronic form for his initial consideration. The parties could attend before the notary to sign. This could be by creating an electronic signature; similarly the notary could sign by electronic means.

What needs to be investigated, before a signature policy for notarization can be structured, is the security requirements and procedures which surround the process. This can only be done effectively if there is extensive consultation with notaries, any professional bodies and their governing bodies, e.g. the national ministry of justice. Topics which should be covered include:

- secure communication of documents to/from the notary;
- secure system of the notary;
- security relating to the notarial signature;
- secure archiving;
- longevity of the notarial signature;
- longevity of the archive.

11 Conclusions

In summary, a number of conclusions can be drawn:

1) Signature policies can cover a wide range of aspects related to signatures, both legal and technical: in particular, a signature policy can be used to specify the conditions under which electronic signatures will be accepted by or on behalf of a relying party, and the means by which the "formality" of signing may be accomplished.

2) The Directive [5] gives no direct consideration to the intention by the signer to make a signature: the steps which create the formality of signing; and the technical and procedural means for minimizing opportunities for a signer to attempt falsely to deny that he created a signature can be incorporated into a signature policy.

3) A signature policy may relate to a single signature; to a document; or to a transaction.

4) It is not possible to write a single (generic) signature policy which is capable of applying to all types of business models, nor for handling all situations in which multiple signatures may be used.

5) A signature policy may relate to the validation of a single signature (e.g. TS 101 733 [1]) or to multiple signatures on a single document, e.g. a contract; on the other hand they may potentially be very complex, managing signatures which are required at multiple stages of a transaction and which are necessary to give effect to the transaction, e.g. international trade transaction involving export/import controls. These policies may be distinguished from each other by naming them *transactional signature policy, or contract signature policy.*

6) A signature policy consists of business rules, under which a number of subordinate signature policies may co-exist.

7) Until business rules relating to electronic signatures are established by custom and endorsed by law it is likely to be necessary for trading partners to agree the terms of a signature policy as a preamble to their course of business dealings.

8) Legal aspects: signature policies should not be viewed as the equivalent of normal (contractual) terms and conditions of business: they may be enforceable against a signer who has no ***actual*** knowledge or understanding of their content.

9) Signature policies are, therefore, likely to be most effective when they are implemented by automated means within a business application.

11.1 Recommended changes to the signature policy formats

The present document is intended to supplement TS 101 733 [1] Electronic Signature Formats, TR 102 038 [2] XML Format for Signature Policies and by investigating business needs and, if possible, by providing a foundation for further work in relation to the technical implementation of a signature policy governing multiple signatures. It is apparent that in some respects, the present document does not endorse some aspects of the previous documents. However, it may be that some of those differences may be capable of reconciliation as a result of future projects, and it may, therefore, be premature to suggest changes or modifications at this stage.

11.2 Recommendations for future work

The present document focuses on electronic signatures that are intended to be legally enforceable; it identifies business issues around the use of signatures. A further piece of work is needed to provide solutions in an electronic format. It is recommended that further work should take the form of the development of a protocol, which will enable businesses:

- to manage multiple signature; and
- to publish in a recognized interoperable format, the conditions under which they accept, and/or provide electronic signatures.

This future task should be "XML-orientated" and should exercise caution that the work focuses on electronic signatures and their management and is not simply related to a transactional protocol.

It should strive to be generic. (Given budget constraints, the further work will use a single business scenario as an illustrative example and should encourage participation by other organizations to conduct parallel work on an unfunded basis.)

The work should ideally complement initiatives in OASIS, which are developing a protocol by which businesses can publish the terms under which they conduct electronic commerce. This will give the ETSI deliverable the widest possible international exposure.

No attempt has been made in the present document to draft detailed technical rules relating to a signature policy. It is evident that there could be several different approaches, each based on the guidance provided in clause 9, and each of which may have validity. Equally, the approach may depend on the business application for which the technical rules are being developed. Whereas this may indicate that it is not possible to develop a technical specification for the validation of multiple signatures, applicable across multiple business applications, it is suggested that a technical specification focussing on one, widely used, business model would provide a valuable extension to the present document. It would provide an illustration of how the principles described in the present document may be applied, and provide a tool for managing multiple signatures in at least one business scenario.

In order to achieve this, there must be detailed information available about the business application in question, and clear rules or understanding about the commonly understood meaning/interpretation of the signatures involved. It should be one of wide applicability. Suggestions are: a purchasing model, contract formation, e-government, and notarization. A signature policy governing contract formation is problematic, in that it is almost impossible to mandate how parties evidence their intention to make an agreement. There is, for example, already a body of case law about so-called "click wrapped" contracts where the parties "sign" by a click of a mouse. Contracts may also be concluded by email with no enhanced forms of security. Signature policies require an agreement to use them: it is infeasible that parties to a transaction would agree to use a signature policy in order to sign a one-off contract unless the value of the contract were exceptionally high, or the subject matter of exceptional importance. E-government and notarization would both provide excellent material for a technical specification, but probably involve complex considerations which would place them outside the funding limits of the proposed project. On balance, the purchasing example is probably the most feasible. It is relatively simple and has wide applicability.

The present document has international significance for e-commerce. Given that there is work of a similar (complementary) nature on-going in OASIS and ebXML, it is important that the present document and EESSI's focus in this area should not become marginalized. Consideration should be given to ways in which co-operation could be achieved with these groups.

Annex A:
Business scenario descriptions

A.1 General

This clause outlines a series of Use Cases which illustrate how signatures may be used. They will fall into a range:

- Single;
- Multiple parallel;
- Counter signatures;
- Sequential;
- Combination of the above.

It is emphasized that the Use Cases included below are not fully described. They are produced using the Unified Modelling Language (UML) as a standard notation and to provide continuity into the development and use of electronic signatures. However, the Use Cases focuses on the signature aspects and only provide a contextual overview of the whole scenario. In order to emphasize the signing point in the sequence diagrams, the UML message call is (mis)used.

NOTE: Reviewers are requested to provide comments/additions etc to the use cases. The Team are particularly interested in alternative mechanisms/methods in different jurisdictions. Each Use case will be expanded where necessary to support the signature usage discussion following the structure of the tabulation in clause A.4.

A.2 Purchase of life insurance

This outline reflects the Italian approach to the purchase of Health Insurance.

A.2.1 Use Case

There are a number of actors involved in the use case below:

Client: the individual who wishes to manage an element of health risk by purchasing insurance cover.

Procurer: the organization/individual who obtains health insurance for the Client from the Agent.

Agent: the organization/individual who is authorized by the Insurance Company to sell its insurance products.

Insurance Company: the organization who owns the insurance product, sets the premium and rules for purchase.

Doctor: who may be called upon to undertake a medical examination at the request of the Insurance Company.

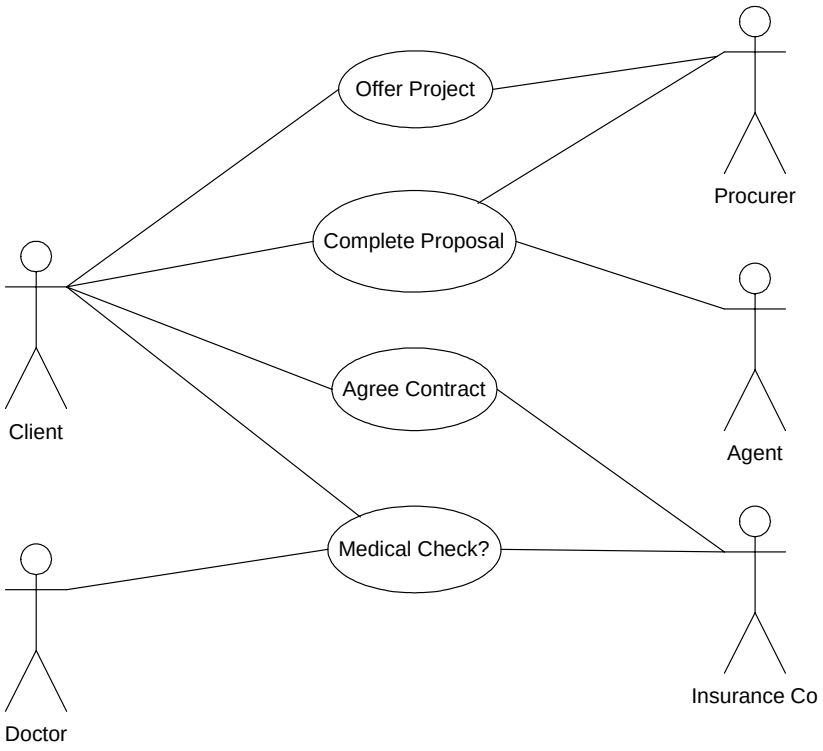


Figure A.1: Life Insurance Use Case

A.2.2 Sequence Diagram

Procurer offers Health Insurance to prospective Client.

Client signs proposal form and forwards it to Procurer.

Procurer forwards proposal form to Agent who forms and forwards it to the Company.

Insurance Company, after processing the request, signs and issues a contract to the Client, via Agent and Procurer.

Insurance Company may require a medical examination. Client visits Doctor, who undertakes and examination, sends a signed health declaration to the Insurance Company in compliance with privacy rules, and also sends a copy of the report to the Client.

Client signs and returns the contract to the Insurance Company, via the Agent and the Procurer.

If no examination is required, the policy becomes effective after a latency period (e.g., 6 months.)

If the Company deems the contract unacceptable, one clause entitles it to refuse to accept it.

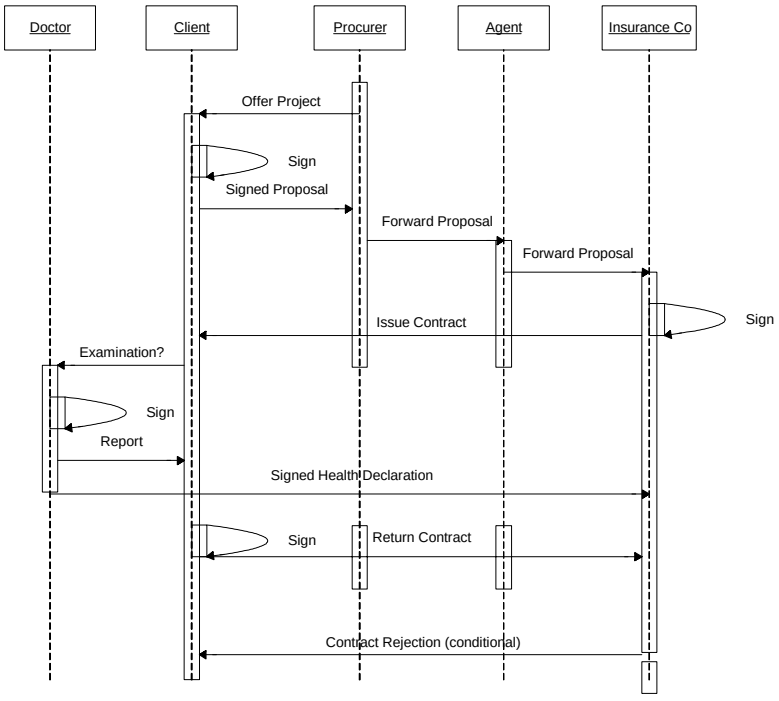


Figure A.2: Life Insurance Sequence Diagram

A.3 Supply chain (illustrated via linked service level agreements)

The scenario is where an agent is reselling services to his customers. These services are managed services and are, therefore, not operated by the agent. In addition, 1st line customer support has been outsourced. Service development is carried out by a separate organization to the one providing the service to the Agent and, finally the service development team required support from the original product manufacturer of the platform and operating system.

The result is illustrated below:

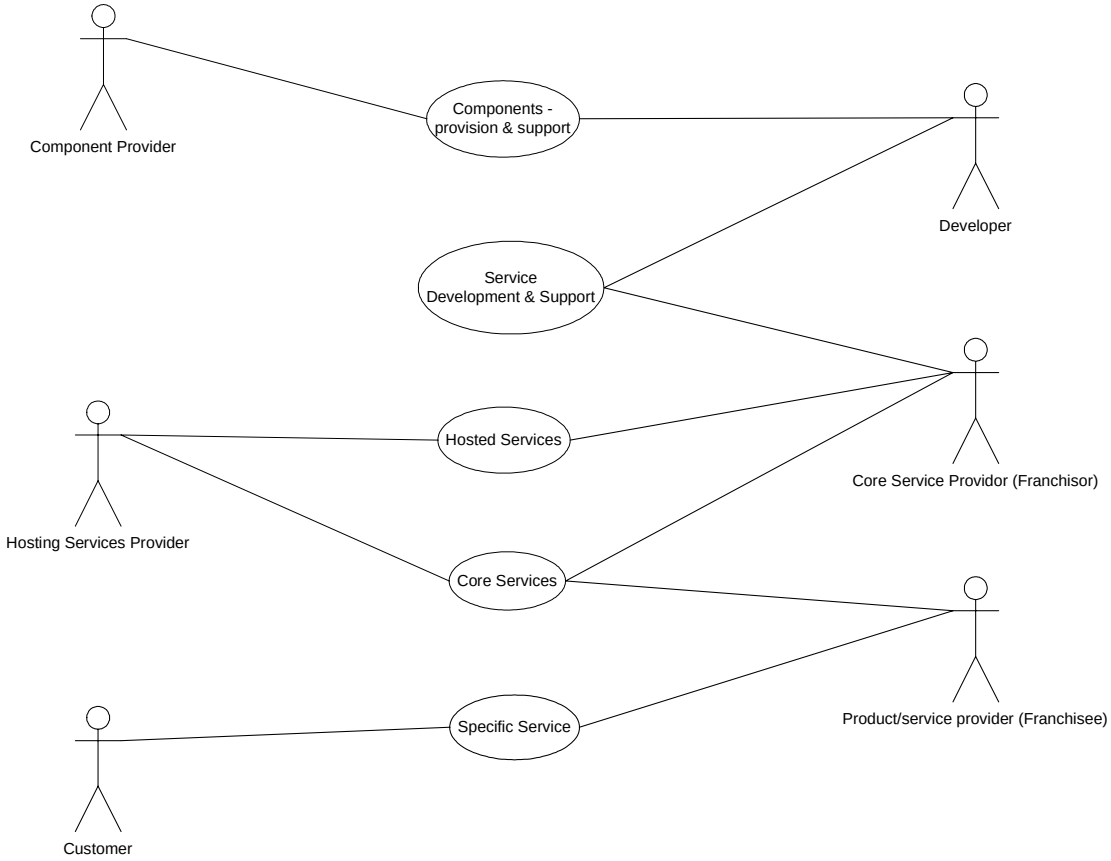


Figure A.3: Supply chain use case

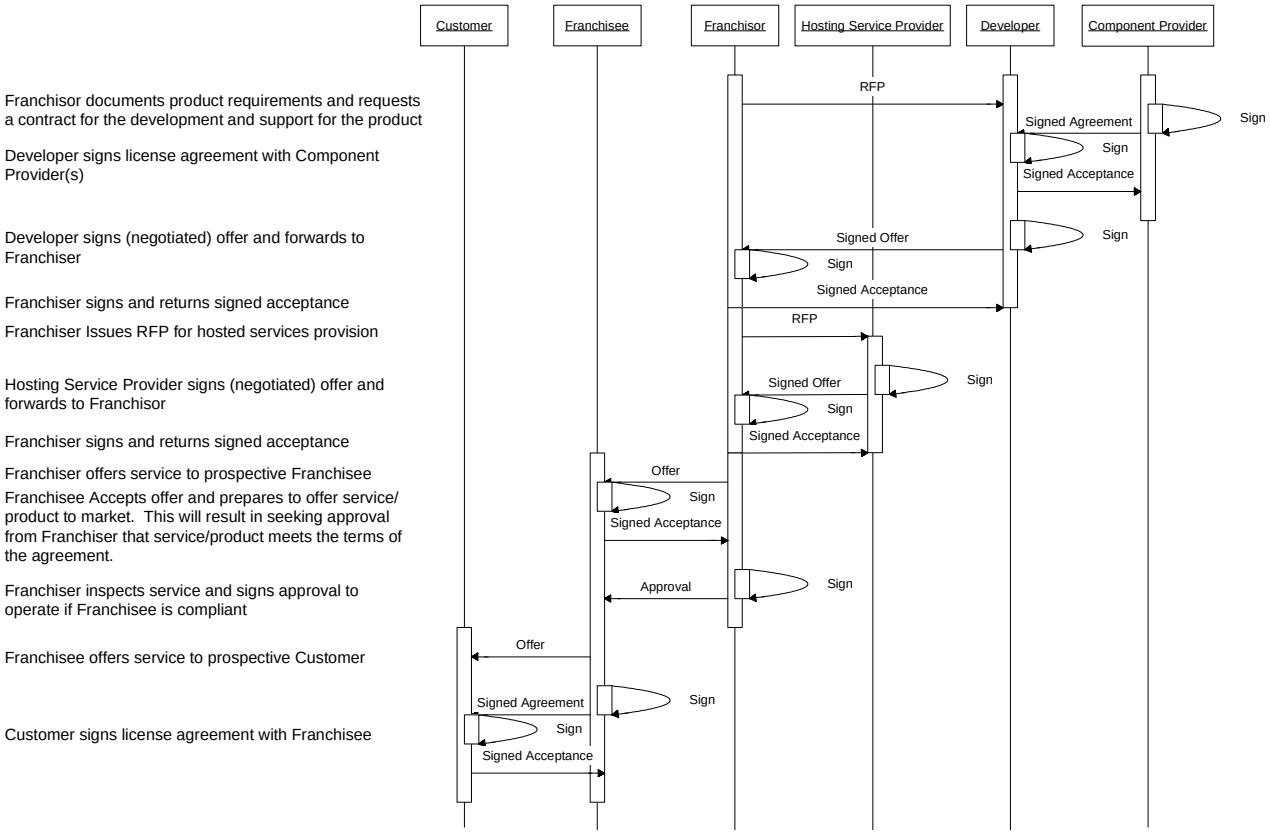


Figure A.4: Supply chain sequence diagram

The important element to be brought out I this Use Case is that when the Franchisee offer a service to the customer, he knows all the previous agreements are in place and signatures are valid.

A.4 Land purchase

This scenario excludes the selection of estate agents, selection of property, or contract negotiation element. It is assumed that production of the contract is deemed to be by the Vendor's lawyer. The use of Use Cases here is further abused in that there is no "system" for exchange and completion of contracts, which would be core to the Use Case. We have also assumed that in this case, the property is being traded between organizations where countersignatures are required to authorize transactions.

A.4.1 Use case

There are three major classes of user; Buyer, Seller and Adviser and (in the UK)one minor user; the Land Registry. The user "Buyer" includes both representatives in the organization buying the property and any witnesses; whereas "Seller" includes both representatives in the organization selling the property, again including any witnesses. "Advisor" includes the buyer and seller lawyers, the Valuation Agent and the Financial Adviser/Mortgage Company. The first diagram below illustrates the system level context of the use case. It is followed by the use case hierarchy which shows the various use cases involved.

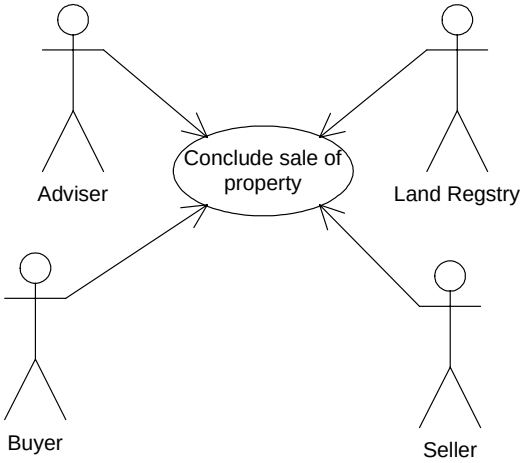


Figure A.5: Conclude Sale of Property

Use Case Name:	Conclude Sale of Property.
Iteration:	Filled.
Summary:	System context Use Case. The price has been agreed and the parties have agreed to the purchase. All that remains is the terms to be agreed, loan to be procured, contracts to be signed and exchanged and completion reached.
Basic course of events:	1) The Seller's Lawyer produces the contract and distributes it to the Seller and the Buyer's Lawyer. 2) The Buyers and Sellers sign the contract. 3) The Buyers negotiate a mortgage on the property. 4) Contracts are exchanged. 5) Completion occurs on the agreed date. 6) Documents are collated and required documents forwarded to the Land Registry.
Alternative Paths:	Civil Law processes ……..
Exception Paths:	N/A
Extension Points:	N/A
Trigger:	N/A
Assumptions:	This reflects the UK perspective of Land (property) purchase.
Preconditions:	N/A
Postconditions:	N/A
Related Business Rules:	N/A
Author:	Jeremy Hilton/Jane Hill.
Date:	August 19, 2002 - Façade; August 20, 2002 - Filled.

The following diagram illustrates how the "Conclude Sale of Property" Use Cases is made up of a number of other discrete Use Cases.

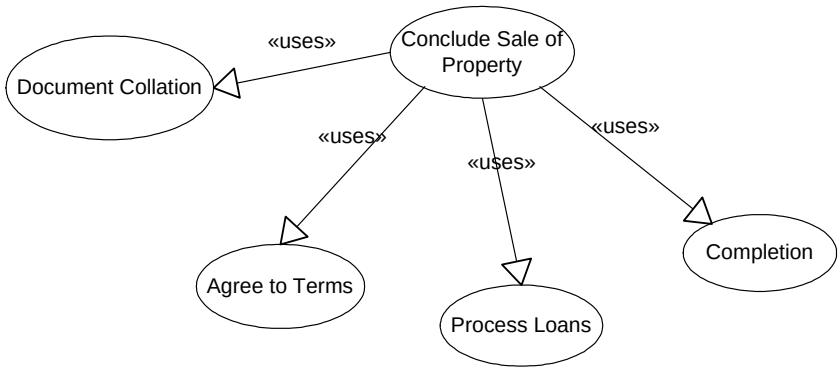


Figure A.6: Conclude sale of property Use Case hierarchy

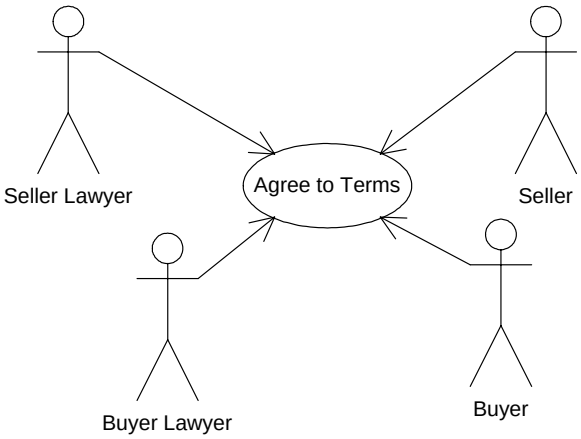


Figure A.7: Agree to terms Use Case

Use Case Name:	Agree to Terms.
Iteration:	Filled.
Summary:	The Buyer and Seller agree to the terms of the sale, including any changes to the existing property, the items included with the property, the date of possession, the financing and any other conditions of the sale.
Basic course of events:	1) This use case begins when the Buyer and Seller indicate to their Lawyers that an agreement is possible. 2) The Sellers" Lawyer then prepares the contract, sends one copy to the Sellers and another copy to the Buyers Lawyer. 3) The Buyers'Lawyer forwards the contract to the Buyers. 4) Seller 1 signs the contract, has it countersigned by a witness, and forwards it to Seller 2. 5) Seller 2 signs the contract, has it countersigned by a witness, and returns it to the Seller's Lawyer. 6) Buyer 1 signs the contract, has it countersigned by a witness, and forwards it to Buyer2. 7) Buyer 2 signs the contract, has it countersigned by a witness, and returns it to the Buyers" Lawyer. 8) This use case ends when the Buyers' Lawyer notifies the Sellers' Lawyer of Contract agreement.
Alternative Paths:	In Step 2, the Buyers Lawyer could initiate the contract on behalf of the Buyer.
Exception Paths:	If at Steps 3 the Buyer does not agree to any of the terms of the contract, then there may be negotiation between the Lawyers on behalf of their clients. Once a modified contract is agreed, then the process continues at Step 4.
Extension Points:	None.
Trigger:	Buyer and Seller indicate that agreement to terms can begin.
Assumptions:	None.
Preconditions:	An offer has been made and accepted.
Postconditions:	Contract is agreed by the Buyer and Seller.
Related Business Rules:	None.
Author:	Jeremy Hilton/Jane Hill.
Date:	August 19, 2002 - Façade; August 20, 2002 - Filled.

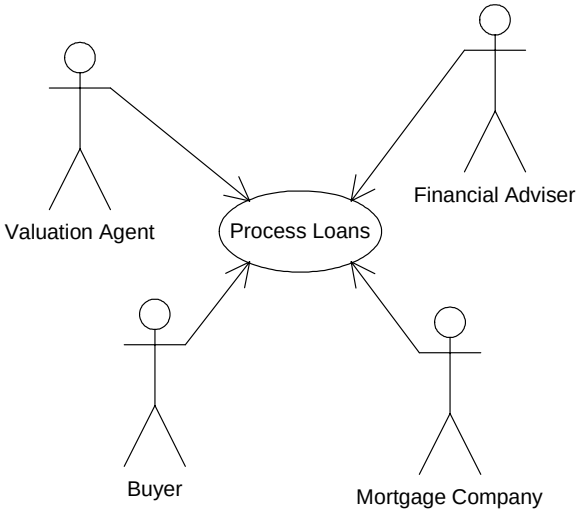


Figure A.8: Process loans Use Case

Use Case Name:	Process Loans.
Iteration:	Filled.
Summary:	The Financial Adviser/Mortgage Company and the Buyer work out the terms of the loan if the Buyer requires one. Terms include the interest rates, term, insurance etc.
Basic course of events:	1) This use case begins when the Buyer and the Seller have agreed to terms. 2) The Buyer seeks a valuation on the property from a Valuation Agent. 3) The Valuation Agent provides a signed valuation of the property to the Buyer. 4) The Buyer requests a loan from a Financial Adviser, outlining the property details, funding available, funding required and terms preferred. 5) The Financial Adviser recommends a Mortgage Company and related Loan Proposal. 6) The Buyer negotiates with the Mortgage Company through the Financial Adviser. 7) The Mortgage Company indicates their acceptance to the Buyer of the final offer. 8) The Buyer indicates acceptance of the loan.
Alternative Paths:	If, in Step 6 the Buyer accepts the initial proposal, then go to Step 8.
Exception Paths:	If, at Step 5, there is no acceptable Loan proposal, the Buyer can return to Step 4 and seek an alternative Financial Adviser, seek an alternative Mortgage Company or cancel the offer.
Extension Points:	None.
Trigger:	The Buyer requires financing and initiates a loan search.
Assumptions:	None.
Preconditions:	Buyer requires financing.
Postconditions:	The loan is approved and recorded.
Related Business Rules:	None.
Author:	Jeremy Hilton/Jane Hill.
Date:	19 August, 2002, Façade; 20 August, 2002, Filled.

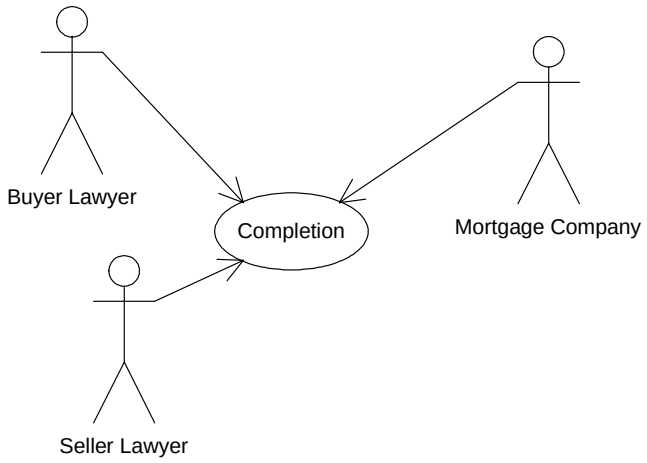


Figure A.9: Completion Use Case

Use Case Name:	Completion.
Iteration:	Filled.
Summary	The Buyers' Lawyer and Sellers' Lawyer agree that contracts are complete, funding is transferred. The Buyers" Lawyer forwards a transfer deed to the Sellers" Lawyer which is signed and witnessed by both Sellers, then returned to the Buyer. Completion date is set at mutual convenience to Buyer and Seller.
Basic course of events	1) Lawyers of both parties check contracts are completed and signed. 2) Sellers' Lawyer confirms funding is available. 3) Exchange is agreed between the Lawyers and communicated to Buyer and Seller. 4) Date for completion is agreed by Buyer and Seller. 5) Transfer Deed is prepared by Buyers" Lawyer and sent to Sellers" Lawyer who forwards it to Seller. 6) Sellers sign Transfer Deed with witnesses signatures and return to Buyers Lawyer via Sellers' Lawyer. 7) At due date, Completion occurs, appropriate documents sent to the Land registry and deeds to the property sent to the Mortgage Company.
Alternative Paths:	None.
Exception Paths:	If, in Step 3, exchange is not agreed by either the Buyers' Lawyer or Sellers' Lawyer, both parties are notified, and the sale is aborted.
Extension Points:	None.
Trigger:	The Buyer and Seller indicate a closing can occur.
Assumptions:	None.
Preconditions:	The Buyer and Seller have agreed to terms. The Buyers" source of payment has been secured.
Postconditions:	The completion has occurred and ownership has been transferred.
Related Business Rules:	None.
Author:	Jeremy Hilton/Jane Hill.
Date:	19 August, 2002 - Façade; 20 August, 2002 - Filled.

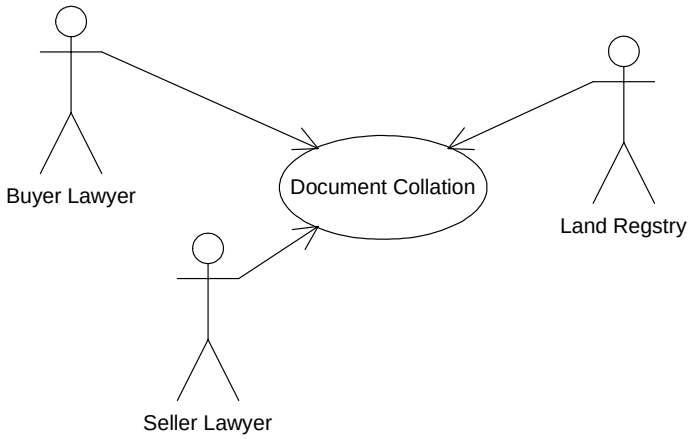
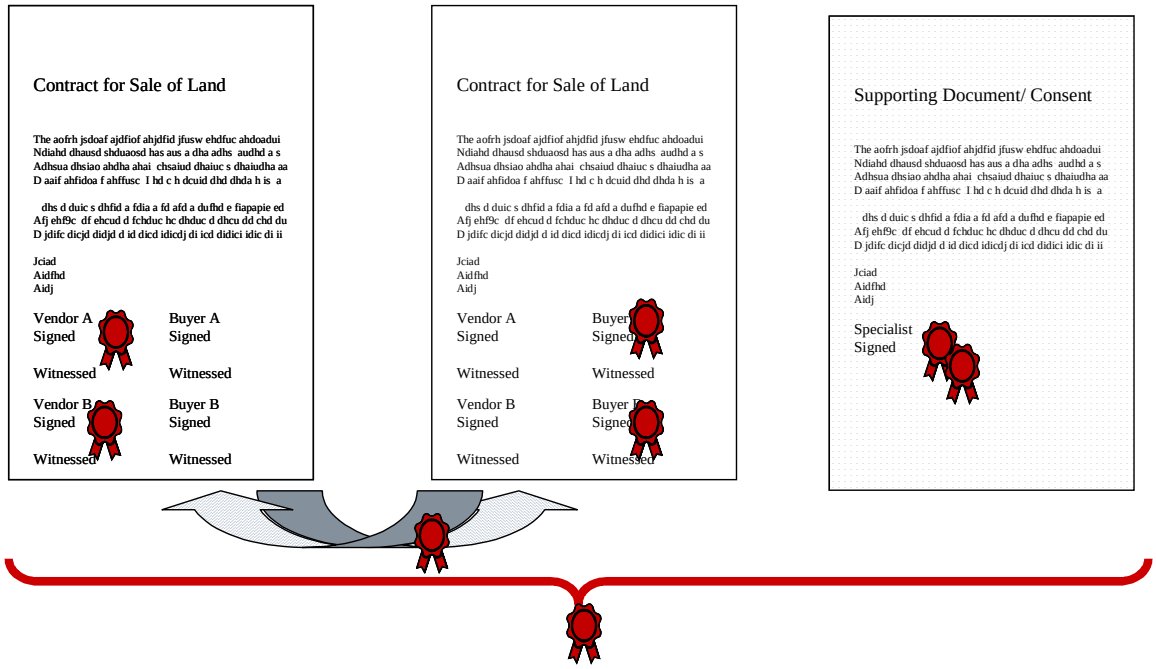


Figure A.10: Document collation Use Case

Use Case Name:	Document Collation.
Iteration:	Filled.
Summary:	Documents are collected together and stored with an indication of completeness.
Basic course of events:	1) The Sellers' Lawyer collects together the copy of the contract signed by the Sellers, the copy of the contract signed by the Buyers and any other related documents. 2) The Sellers document set is signed to indicate completeness and stored (as shown below). 3) The Buyers" lawyer collects together the copy of the contract signed by the Sellers, the copy of the contract signed by the Buyers the Valuation Statement together with the loan agreement and any other related documents. 4) The Buyers document set is signed to indicate completeness and stored.
Alternative Paths:	None.
Exception Paths:	None.
Extension Points:	None.
Trigger:	Completion has occurred.
Assumptions:	None.
Preconditions:	Completion has occurred.
Postconditions:	The transaction is complete.
Related Business Rules:	None.
Author:	Jeremy Hilton/Jane Hill.
Date:	19 August, 2002 - Façade; 20 August, 2002 - Filled.

A.4.2 Illustrative document set



Annex B:
Signature commitment categories

1) Positive assertion of a will or intention to make a legal commitment.

2) Authentication purposes only.

3) Acknowledgement of receipt only.

4) "authorship" or "attribution" where the signer assumes a responsibility for data, including its accuracy, but does not intend to make a legal commitment, e.g. signing a draft contract in the course of negotiations.

NOTE 1: Signing off design drawings, signing a tax return would involve making a legal commitment and therefore are included in 1). (See clause 7.)

5) Countersignature for authorization.

6) Witnessing.

7) Notarization

8) Administrative signature, where the signature indicates only the integrity of data e.g. for record-keeping, or archiving purposes.e-notary signature

9) E-notarial signature, where the signature indicates the performance of a "trusted" service.

10) E-validation signature, where the signature indicates that a previous signature or signatures have been validated in accordance with a signature policy.

11) Claimed delegated authority ("per proxy")

NOTE 2: This must ***not*** be used in conjunction with 2), 6), 7) above.

Annex C:
Model/specimen policy document

This model policy document is intended to demonstrate an offer/acceptance.

Title/identification of signature policy:

ABC plc Signature Policy

for use in the provision of financial services to consumers

Version No:

Date:

Business application domain:
This policy covers the provision of financial services to consumers by ABC plc.

Transactional context:
Offer/acceptance in relation to a private mortgage/loan agreement between ABC plc and a client of ABC plc.

Consent to accept electronic signatures:
ABC plc and ……. agree that they will accept signatures in electronic form, and which are created in accordance with this policy.

Proposed signers:

On behalf of ABC plc

The persons authorized to sign a mortgage/loan offer on behalf of ABC plc are **A** (insert business role); and

Counter signed by B: (insert business role)

On behalf of the client

Client ……

Witness (a professional person) ……

Proof of authority:
It shall be deemed sufficient proof of authority if signatures created by ABC plc employees or agents are accompanied by a certificate issued by XYZ, certification authority containing information as to their identity and job title, providing the latter corresponds to the required authority specified in this policy.

Signature commitment type:
1. Legal commitment

Timing constraints:
The mortgage/loan offer shall expire 28 days after the time at which the offer is signed (countersigned) on behalf of ABC plc.; a signature created by the client after that time period will not be accepted by ABC plc as a valid signature.

Specifications (at high level) of any security considerations:
E.g. All signatures shall conform to article 5.1. Electronic Signatures Directive; and/or
certificates shall be issued by an accredited certification authority.
All signatures shall be timestamped by a TSA.

Allocation of responsibility for signature verification/validation:
N/A

NOTE: In these circumstances, it is reasonable to assume that each relying party will wish to verify the other's signatures.

Audience conditions:
The mortgage/loan offer shall not be valid or binding upon ABC plc unless it is signed and countersigned by the specified officers in accordance with this policy.

Access control management:
A mortgage/loan agreement is protected by banking confidentiality; and data protection laws. Only authorized banking personnel at ABC plc may access such agreements; disclosure to third parties is prohibited except with the consent of the client, or in accordance with a Court order.

Dispute resolution procedures:
Any disputes arising under this policy shall be referred to …… a suitably qualified expert, whose decision shall be final and binding upon the parties…….

Misc

Governing laws clause etc….

Annex D: Bibliography

- "Business Process and Business Information Analysis Overview" V1.0 Business Process Team 11th May 2001. http://www.ebxml.org
- "Business Process Specification Schema" V1.01 - Business Process Team 11th May 2001 http://www.ebxml.org
- "Catalog of Common Business Processes" V1.0 Business process Team 11th May 2001 http://www.ebxml.org
- "Chitty on Contracts" 28th Edition - Sweet & Maxwell.
- "Collaboration-Protocol Profile and Agreement Specification" Version 2.0 OASIS ebXML, Collaboration Protocol Profile and Agreement Technical Committee, September 23, 2002, www.oasis-open.org.
- "Core Component Overview" V1.05 Core Component Team 10th May 2001 http://www.ebxml.org
- "Core Component Discovery and Analysis" V1.04 Core Component team 10th May 2001 http://www.ebxml.org
- "Context and Re-Usability of Core Components" V1.04 Core Component Team 2001 http://www.ebxml.org
- "E-Commerce Patterns" V1.0 - Business Process Team 11th May 2001 http://www.ebxml.org
- "E-Commerce, Security & Privacy Law Resources" Baker & McKensie http://www.bakernet.com/ecommerce/.
- "Internet Open Trading Protocol" David Budett, Donald E. Eastlake III, Marcus Goncalves McGraw Hill ISBN: 0-07-135501-4
- "International Trade Transaction Model" (http://www.unece.org/trade/itt/uk/intro.htm)
- Booch, Rumbaugh and Jacobson: "The Unified Modelling Language User Guide";1999, Addison Wesley, ISBN 0201571684.
- Kulak and Guiney: "Use Cases: Requirements in Context"; 2001, ACM Press, ISBN 0201657678.
- ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".
- IETF RFC 3126: "Electronic Signature Formats for long term electronic signatures".
- ISO/IEC 13888-1: "Information technology - Security techniques - Non-repudiation - Part 1: General".
- http://www.legifrance.gouv.fr.

History

Document history		
V1.1.1	March 2003	Publication