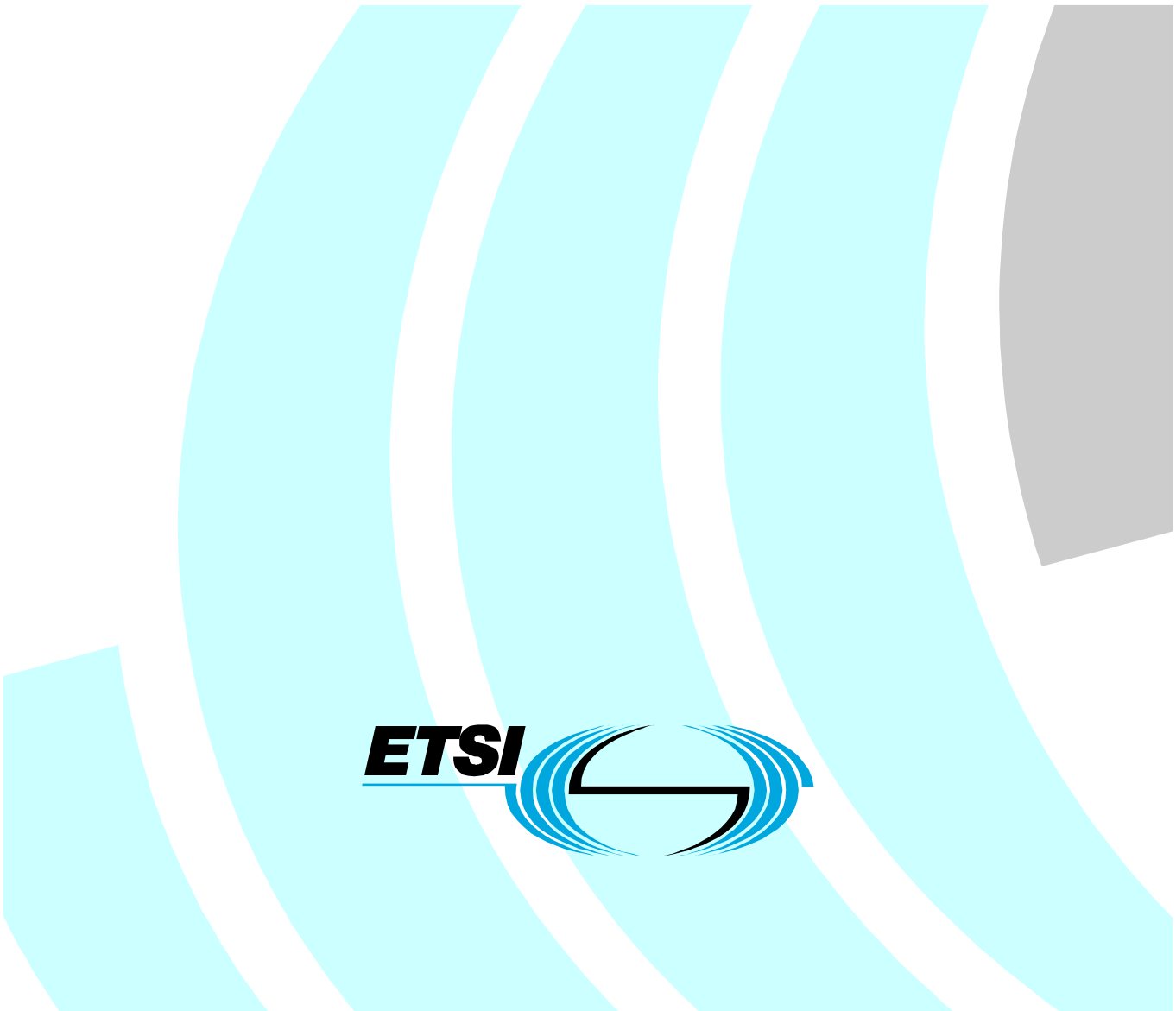
ETSI TS 102 231 V1.1.1 (2003-10)

Technical Specification

Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust Service Provider status information



Reference
DTS/ESI-000010

Keywords
e-commerce, electronic signature, security,
trust services

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

Contents

Intellectual Property Rights

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

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

Foreword

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

Introduction

The purpose of a Trust-service Status List (TSL), and hence of the present document, is to provide a harmonized way in which schemes having an oversight role with regards to trust services and their providers (trust service providers - TSPs) can publish information about the services and TSPs which they currently oversee, or indeed (through the provision of historical information) have overseen.

The present document is based upon the reasoning that it will enhance the confidence of parties relying on certificates or other services related to electronic signatures if they had access to information that would allow them to know whether a given TSP was operating under the approval of any recognized at the time of providing their services and of any dependent transaction that took place.

The information should be available for a wide range of services and schemes, including the use of Qualified Certificates. The importance of this information is especially significant for cross-domain and international transactions. This information should preferably be accessible using an on-line protocol, although accessibility both off-line and on-line should be possible.

Entities having such an oversight role could be supervisory systems or voluntary approval schemes as defined in Directive 1999/93/EC (see bibliography), similar schemes established by other sovereign states or economies (e.g. certain government e-authentication frameworks), and those established by specific industry sectors or for international promotion of trust services.

1 Scope

The present document specifies a standard for a Trust-service Status List making available trust service status information. In addition, it gives guidelines for access to and the use of such status information.

The present document is applicable to scheme operators responsible for the approval of trust services and to those who wish to rely on such information.

2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ISO 639-1: "Codes for the representation of names of languages - Part 1: Alpha-2 code".

[2] IETF RFC 1766: "Tags for the Identification of Languages".

[3] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes".

[4] IETF RFC 2396: "Uniform Resource Identifiers (URI): Generic Syntax".

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

[6] IETF RFC 2253: "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names".

[7] IETF RFC 2141: "URN Syntax".

[8] ITU-R Recommendation TF.460-5: "Standard-Frequency and Time-Signal Emissions".

[9] IETF RFC 3280: " Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

3 Definitions and abbreviations

3.1 Definitions

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

approval: assertion that a(n electronic trust) service, falling within the oversight of a particular scheme, has been either positively endorsed (active approval) or has received no explicit restriction since the time at which the scheme was aware of the existence of the said service (passive approval)

(electronic) trust service: service which enhances trust and confidence in electronic transactions (typically but not necessarily using cryptographic techniques or involving confidential material)

scheme: any organized process of supervision, monitoring, approval or such practices that are intended to apply oversight with the objective of ensuring adherence to specific criteria in order to maintain confidence in the services under the scope of the scheme

scheme operator: body responsible for the operation and/or management of any kind of scheme, whether they be governmental, industry or private, etc.

Trust Service Provider (TSP): body operating one or more (electronic) trust services

NOTE: This embraces a wide range of services which may relate to electronic signatures and is broader than the provision of certification services alone, and hence is used in preference to and with a broader application than, the term certification-service-provider used in Directive 1999/93/EC.

3.2 Abbreviations

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

ASN	Abstract Syntax Notation
CA	Certification Authority
CRL	Certificate Revocation List
EU	European Union
OCSP	Online Certificate Status Protocol
PKC	Public Key Certificate
PKI	Public Key Infrastructure
TSL	Trust-service Status List
TSP	Trust Service Provider
URI	Uniform Resource Identifier
URN	Uniform Resource Name
UTC	Coordinated Universal Time
WWW	World Wide Web
XML	eXtensible Markup Language

4 TSP status information

The present document specifies a standard for the provision of trust service status information. In recognition of the selection of a form of signed list as the basis for presentation of this information, the term Trust-service Status List (TSL) is adopted. Each scheme which maintains a TSL in accordance with the present document must comply with the format and semantics specified in clause 5. Each such scheme must operate against specific criteria for determining the status of TSPs and trust services which it recognizes: a scheme operator could, therefore, operate more than one discrete scheme.

It should be noted that the present document addresses only the type, format and meaning of information which may be presented in a TSL and does not define how that information should be sourced. Nor does it specify the criteria which schemes should use to determine the status of any trust services falling within their remit - such criteria remain the responsibility of the scheme operators. Furthermore, it does not specify how any status or scheme-related information should be presented outside the context of a TSL, e.g. on schemes' websites.

Each scheme adopting this TSL standard must be able to support the provision of status information in each of the following forms:

- Human readable in hard-copy form;
- Human readable in a format readily down-loadable and printable;
- Machine processable to allow automatic verification of status information.

The TSL specified by the present document accommodates the requirement as to "*whether the provider of a trust service is **or was** operating under the approval of any recognized scheme at either the time the service was provided, or **the time at which a transaction reliant on that service took place***". In order to fulfil this requirement, Trust-service Status Lists must necessarily contain information from which it can be established whether the TSP's service was, at the time of the transaction, known by the scheme operator and if so the status of the service, i.e. whether it was approved, suspended, cancelled, revoked, etc. The Trust-service Status List must therefore contain not only the service's current status, but also the history of its status. The TSL must therefore, because of this requirement upon it, be a combination of "white list" and "black list", including historical information.

The TSL specified by the present document therefore has four major components, in a structured relationship. These components:

- provide information on the issuing scheme;
- identify the TSPs recognized by the scheme;
- indicate the service(s) provided by these TSPs and the current status of the service(s);
- indicate for each service the status history of that service.

The logic of the list is that, once the scheme operator has become aware of the existence of the TSP (whether by some pro-active action on the part of the TSP or by the scheme's own supervision of the marketplace), the particular status as determined according to the scheme rules is either the present status of the TSP's service (i.e. only current status, no history) or is seamlessly followed by a sequence of one or more statuses (current status and history). Note that if a trust service was approved until a certain date/time and there was a period in between the expiry of the approval and the start of the re-approval, then a status identifier would provide the information for that interim period. The "interim status" would either be cancelled (voluntarily, by the TSP) or revoked (by the scheme, with reasons).

5 Trust-service Status List structure

This clause specifies the Trust-service Status List structure. Each of the fields within the TSL is described to a level of detail sufficient to permit any scheme operator to implement a standardized TSL, consistent with any other TSL conformant to the present document, with specified values, meanings and interpretations given for each field. Whether the inclusion of a field is mandatory or optional is indicated. The rationale for requiring each field and specifying it as given is explained in annex E.

5.1 Structure of the Trust-service Status List

The logical model of the Trust-service Status List is shown in figure 1. It has four logical component parts, all but the first of which may be replicated as required.

The list commences with key information about the list itself and the nature of the scheme which has determined the information found in, and through, the list (component 1). The specified set of information must include a pointer (URN) to details of the scheme and how its operator may be contacted. Whilst the objective has been to keep the size of the TSL to the minimum consistent with its purpose and the requirements placed upon it, certain key information which one would expect to be found in the scheme details must be provided directly within the TSL itself so as to facilitate either easy recognition and contact with the scheme or machine processing.

Following this scheme-related information there comes information relating to the Trust Service Providers (TSPs) whose services are within the scope of the scheme (component 2), and for each of those TSPs, the details of their specific trust services whose current status is recorded within the TSL (component 3). For each service, any available historical status information is recorded (component 4). The number of TSPs, of services per TSP, and of history sections per service is unbounded.

The TSL is a signed list for authentication purposes and is tagged to facilitate identification for electronic searches. The structure of the TSL is described in the following clauses by each component part and its fields.

5.1.1 Trust-service Status List information

Description: This field represents all the structured information and shall contain the following:

a) Scheme information, as specified in clause 5.2;

b) A sequence of fields containing information on the TSPs that the scheme oversees. This sequence is mandatory. The contents of the TSP information field are specified in clause 5.3;

c) For each TSP, a sequence of fields containing information on the service(s) provided by that TSP. This sequence is optional. The contents of the service information field are specified in clause 5.4;

d) For each service, a sequence of fields containing information on the status history of that service. This sequence is optional. The contents of the history information field are specified in clause 5.5;

e) A signature computed over all fields of the TSL except the signature value specified in clause 5.6.4. The contents of the signature field are specified in clause 5.6.

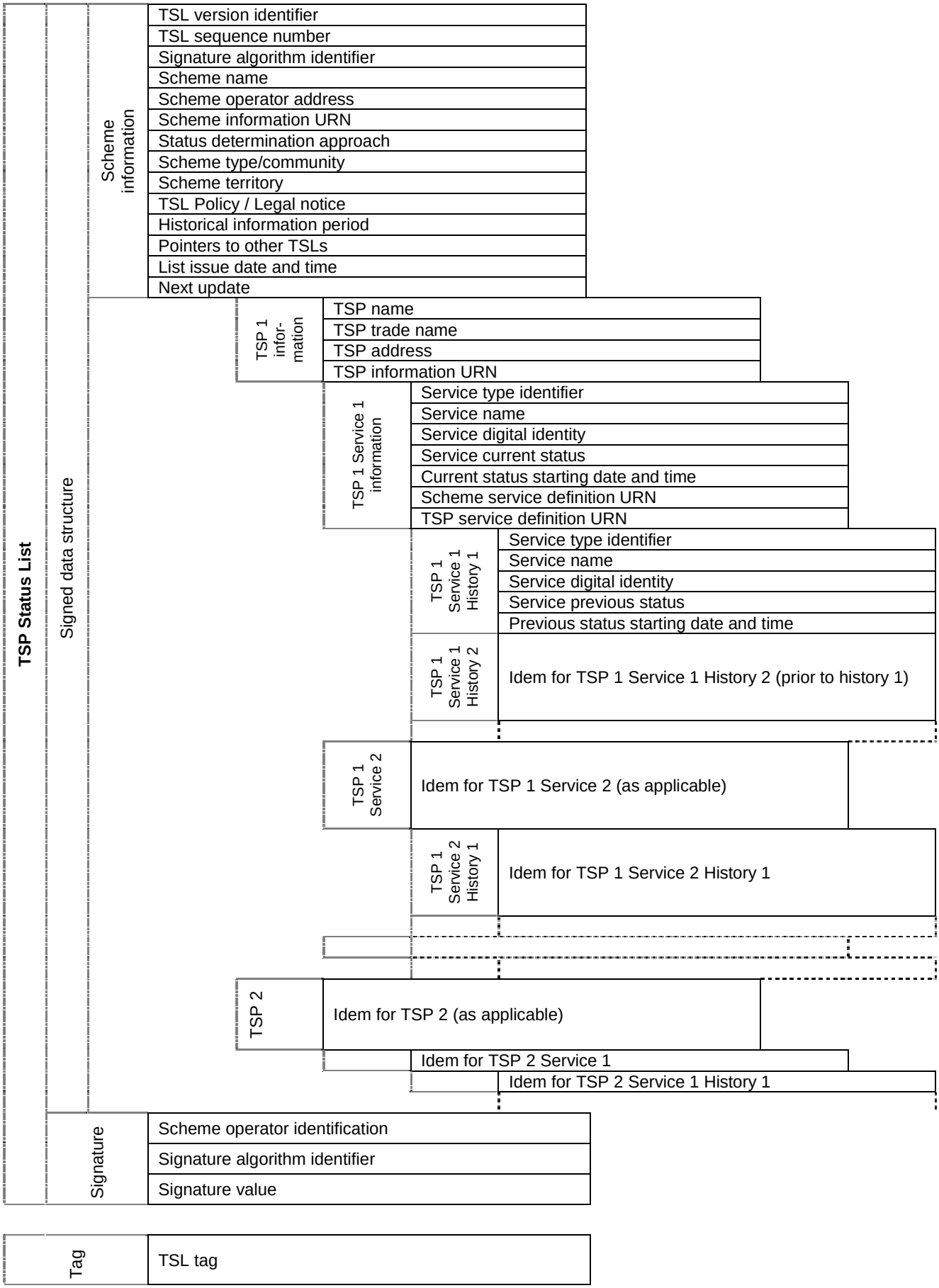


Figure 1: Logical model of the TSP Status List

f) A Trust-service Status List tag to facilitate identification of the TSL for electronic searches. The contents of the tag are specified in clause 5.7.

NOTE: Dependent on the implementation, the tag location could be at the front of the TSL, at the end of the TSL or completely disconnected from the TSL. The logical model in Figure 1 shows the tag disconnected from the TSL. See annexes A and B for tag specifications using ASN.1 and XML implementations respectively.

5.2 Scheme information

5.2.1 TSL version identifier

Description: This field is mandatory. It shall specify the version of the TSL format.

Format: Integer.

Value: The value of the identifier for TSLs conforming to this version of the present document shall be 1.

5.2.2 TSL sequence number

Description: This field is mandatory. It shall specify the sequence number of the TSL.

Format: Integer.

Value: At the first release of the TSL, the value of the sequence number shall be 1. The value shall be increased by 1 at each subsequent release of the TSL.

5.2.3 Signature algorithm identifier

Description: This field is mandatory. It shall specify the cryptographic algorithm that has been used to create the signature. This field provides a copy of the signature algorithm identifier specified in clause 5.6.3 and the two fields must be identical.

Format: Representation format dependent: character string or bit string.

Meaning: The information in this field is depending on the signature format used (see clause 5.6).

5.2.4 Scheme name

Description: This field is mandatory. It shall specify the name under which the scheme operates.

Format: Unicode character string or a sequence of Unicode character strings encoded in UTF-8, specifying the language used in accordance with ISO 639-1 Alpha 2 code [1] for the representation of names of languages. Where multiple languages are used, their representation shall be conformant with RFC 1766 [2].

Meaning: The name of the scheme must be the name which is used in formal legal registrations and to which any formal communication, whether physical or electronic, should be addressed.
Local language and cross-border (international) trading considerations may require that this information be provided both in a national language (and script) and in a commonly accepted internationally-used language.

5.2.5 Scheme operator address

Description: This field is mandatory. It shall specify the address of the legal identity identified in clause 5.2.4, for both postal and electronic communications. Users (subscribers, relying parties) should use this address as the contact point for enquiries, complaints, etc. to the scheme operator.

This is a multi-part field consisting of the scheme operator physical address specified in clause 5.2.5.1 and the scheme operator electronic address specified in clause 5.2.5.2.

5.2.5.1 Scheme operator postal address

Description: This field is mandatory. It shall specify the postal address of the legal entity identified in clause 5.2.4, with the provision for the inclusion of the address in multiple languages.

Format: Sequence of Unicode character strings or multiple sequences of Unicode character strings encoded in UTF-8, each specifying the language used for each sequence of strings in accordance with ISO 639-1 Alpha 2 code [1] for the representation of names of languages. Where multiple languages are used, their representation shall be conformant with IETF RFC 1766 [2].

Each sequence of character strings shall give the following attributes pertaining to the legal entity:

- Street address (delineated with ";" within)
- Locality (town/city)
- If applicable, State or Province name
- Postal code
- Country name as a two-character code in accordance with ISO 3166-1 [3].

Meaning: This must be a postal address at which the scheme operator provides a regularly serviced capability for conventional (physical) mail.

5.2.5.2 Scheme operator electronic address

Description: This field is mandatory. It shall specify the address of the legal entity identified in clause 5.2.4 for electronic communications.

Format: Sequence of character strings giving: e-mail address; web-site URI [4].
At least one of these must be present.

Meaning: In the case of an e-mail address, this must be an address at which the scheme operator provides a regularly serviced help line capability. In the case of a web-site URI, this must lead to a capability whereby the user may communicate with a regularly serviced help line capability.

5.2.6 Scheme information URN

Description: This field is mandatory. It shall specify the URN [4] where users (subscribers, relying parties) can obtain scheme-specific information.

Format: Character string. The syntax must follow the rules of RFC 2141 [7].

Meaning: The referenced URN must provide a path to information describing the general terms and conditions of the scheme, its criteria for TSP and service approval and other generic information which applies to the scheme operations.

NOTE: The URN could differ from the URI provided in clause 5.2.5.2, e.g. if the scheme operator wanted to have a different service or facility for handling e-mails.

5.2.7 Status determination approach

Description: This field is mandatory. It shall specify the identifier of the status determination approach.

Format: Integer.

Meaning: The identifier shall have one of the following values:

1) services listed have their status determined after assessment by or on behalf of the scheme operator against the scheme's criteria (active approval);

2) services listed have been nominated by their provider or are known to be operating in the marketplace, but have not undergone assessment by or on behalf of the scheme operator for initial approval (passive approval);

3) services listed have been deemed to be non-compliant with scheme criteria.

In the case of meanings 1 and 2, the scheme could include in the TSL both services whose current status is approved (either actively or passively) and those which have failed to meet the criteria. In the case of meaning 3, the TSL would list only those services which had explicitly failed to fulfil the criteria of the scheme.

5.2.8 Scheme type/community

Description: This field is optional. If present, it shall contain a registered URN [4].

Format: URN.

Meaning: This field may be used by any community of users which establishes and registers a URN by which to denote participation within that community. Such communities may be legislative, inter-governmental, industry or other, which have registered a URN for the purposes of identifying themselves.

5.2.9 Scheme territory

Description: This field is optional. If present, it shall specify the country in which the scheme is established.

Format: Character string giving a Country name, as a two-character code in accordance with ISO 3166-1 Alpha-2 code [3].

Meaning: A two-letter code which specifies the country in which the scheme is established.

5.2.10 TSL policy/legal notice

Description: This field is optional. If present, it shall specify the scheme's policy or provide a notice concerning the legal status of the scheme or legal requirements met by the scheme for the jurisdiction in which the scheme is established and/or any constraints and conditions under which the TSL is maintained and offered.

Format: Either:

a) a URN [4] which has been registered for the specific use as a pointer to the policy or notice; or

b) the actual text of any such policy or notice, as a Unicode character string or multiple Unicode character strings, encoded in UTF-8, each specifying the language used for each string in accordance with ISO 639-1 Alpha 2 code [1] for the representation of names of languages. Where multiple languages are used, their representation shall be conformant with RFC 1766 [2].

Meaning: Any referenced URN must provide a path to information describing the policy under which the TSP operates or any relevant legal notices with which users of the TSL should be aware. If plain text is provided, this must serve the same purpose.

In either case, local language and cross-border (international) trading considerations may require that this information be provided both in a national language and in a commonly accepted internationally-used language.

5.2.11 Historical information period

Description: This field is mandatory. It shall specify the duration over which historical information in the TSL is provided.

Format: Integer.

Meaning: a) 0 (zero) shall signify no history retained;

b) 1 through 65 534 shall signify the number of days over which historical information in the TSL is provided;

c) 65 535 or greater shall signify an indefinite duration.

NOTE: The period chosen should take due account of the legal requirements for data retention in the host jurisdiction.

5.2.12 Pointers to other TSLs

Description: This field is optional. It may be used to indicate TSLs maintained by other scheme operators.

Format: Sequence of one or more pairs of character strings, each pair giving:
a) a URI to another scheme operator's TSL, and;
b) additional data in an implementation-specific format.

Meaning: A series of pointers to the location of other TSLs with additional information whose meaning is implementation specific.

5.2.13 List issue date and time

Description: This field is mandatory. It shall specify the date and time on which the list was issued.

Format: Character string.

Meaning: UTC time.

5.2.14 Next update

Description: This field is mandatory. It shall specify the latest date and time by which the next TSL will be issued.

Format: Character string.

Meaning: UTC time.

5.2.15 List of Trust Service Providers

Description: This field is mandatory. In the case where no TSPs are or were recognized by the scheme (according to the scheme type and criteria), this field shall be empty. If one or more TSPs are or were recognized by the scheme then the field shall contain a sequence identifying each TSP, providing details on the approval status and history of each of the TSP's services.

Format: Sequence of TSP information (see clause 5.3).

Meaning: The presence or absence of TSPs within this list can only have meaning when taken in the context of the scheme's status determination approach (see clause 5.2.7). E.g. no TSPs under a scheme working solely on a black-list principle suggests that there are no known TSPs which are known to be not operating within the permissible or acknowledged bounds, whereas a similar absence of TSPs in a white-list driven scheme would suggest that no TSPs are approved by the scheme.

5.3 TSP information

5.3.1 TSP name

Description: This field is mandatory. It shall specify the name of the legal entity responsible for the TSP's services that are or were recognized by the scheme.

Format: Unicode character string or multiple Unicode character strings encoded in UTF-8, each specifying the language used in accordance with ISO 639-1 Alpha 2 code [1] for the representation of names of languages. Where multiple languages are used, their representation shall be conformant with RFC 1766 [2].

Meaning: The name of the legal entity responsible for the TSP must be the name which is used in formal legal registrations and to which any formal communication, whether physical or electronic, should be addressed.

Local language and cross-border (international) trading considerations may require that this information be provided both in a national language (and script) and in a commonly accepted internationally-used language.

5.3.2 TSP trade name

Description: This field is optional. If present, it shall specify an alternative name under which the TSP identifies itself in the provision of its services.

Format: Unicode character string or multiple Unicode character strings encoded in UTF-8, specifying the language used in accordance with ISO 639-1 Alpha 2 code [1] for the representation of names of languages. Where multiple languages are used, their representation shall be conformant with RFC 1766 [2].

Meaning: Any name under which the legal entity responsible for the TSP operates, in the specific context of the delivery of those of its services which are to be found in this TSL.

Local language and cross-border (international) trading considerations may require that this information be provided both in a national language (and script) and in a commonly accepted internationally-used language.

5.3.3 TSP address

Description: This field is mandatory. It shall specify the address of the legal entity identified in clause 5.3.1, for both physical and electronic communications. Users (subscribers, relying parties) should use this address as the single contact point for enquiries, complaints, etc. to the TSP.

This is a multi-part field consisting of the TSP physical address specified in clause 5.3.3.1 and the TSP electronic address specified in clause 5.3.3.2.

5.3.3.1 TSP postal address

Description: This field is mandatory. It shall specify the postal address of the legal entity identified in clause 5.3.1, with the provision for the inclusion of the address in multiple languages.

Format: The format shall be the same as that specified in clause 5.2.5.1.

Meaning: This must be an address at which the TSP provides a regularly serviced capability for conventional (physical) mail.

5.3.3.2 TSP electronic address

Description: This field is mandatory. It shall specify the address of the legal entity identified in clause 5.31, to be used for electronic communications.

Format: Sequence of character strings giving: e-mail address; web-site URI [4].
At least one of these must be present.

Meaning: In the case of an e-mail address, this must be an address at which the TSP provides a regularly serviced customer care or help line capability. In the case of a web-site URI, this must lead to a capability whereby the user may communicate with a regularly serviced customer care or help line capability.

5.3.4 TSP information URN

Description: This field is mandatory. It shall specify the URN [4] where users (subscribers, relying parties) can obtain TSP-specific information.

Format: Character string.

Meaning: The referenced URN must provide a path to information describing the general terms and conditions of the TSP, its customer care policies and other generic information which applies to all of its services.

NOTE: The URN could differ from the URI provided in clause 5.3.3.2, e.g. if the scheme operator wanted to have a different service or facility for handling e-mails.

5.3.5 List of services

Description: This field is optional. If present, it shall contain a sequence identifying each of the TSP's recognized services and the approval status of that service.

Format: Sequence of service information (see clause 5.4).

Meaning: The presence or absence of services within this list can only have meaning when taken in the context of the scheme's status determination approach (see clause 5.2.7). E.g. no services under a scheme working solely on a black-list principle suggests that there are no known services which are not operating within the permissible or acknowledged bounds, whereas a similar absence of services in a white-list driven scheme would suggest that no services meet the scheme's criteria.

5.4 Service information

5.4.1 Service type identifier

Description: This field is mandatory. It shall specify the identifier of the service type.

Format: Integer.

Meaning: The identifier shall have one of the following values:
0 (zero) Unspecified;
1 Certification authority issuing public key certificates;
2 Certification authority issuing Qualified Certificates;
3 Time stamping authority;
4 Certificate status provider (also known as OCSP-server or CRL distribution point);
5 Registration authority;
6 Identity verification;
7 Certificate generation;
8 Attribute certification authority;
9 Archive;
10 Key escrow.

NOTE: The above list cannot be regarded as being exhaustive at the time of issue of the present document since further eligible services can be expected to evolve. Should the service type not be adequately specified by any of the above meanings a value of "0" (zero) shall be used.

5.4.2 Service name

Description: This field is mandatory. It shall specify the name under which the TSP provides the service identified in clause 5.4.1.

Format: Unicode character string or multiple Unicode character strings encoded in UTF-8, each specifying the language used in accordance with ISO 639-1 Alpha 2 code [1] for the representation of names of languages. Where multiple languages are used, their representation shall be conformant with RFC 1766 [2].

Meaning: The name under which the TSP provides the service.
Local language and cross-border (international) trading considerations may require that this information be provided both in a mother language (and script) and in a commonly accepted internationally-used language.

5.4.3 Service digital identity

Description: This field is mandatory. It shall specify at least one representation of a digital identifier unique to the service specified in clause 5.4.1 by which the service can be unambiguously identified. The digital identifier may be present more than once and in different formats. If the digital identifier is present more than once, all variants must refer to the same identity.

Format: Character string or Bit string or data structure specifying for each occurrence of the digital identifier the type of format and the data representing the digital identity. Implementation dependent - see annexes A and B.

Meaning: The digital identifier can be of different types depending on the service. It could be a certificate which can be used to verify electronic signatures of the service provider or a subject key identifier.

5.4.4 Service current status

Description: This field is mandatory. It shall specify the identifier of the status of the service.

Format: Integer.

Meaning: The identifier shall have one of the following values:

1) in accordance with the scheme's status determination criteria;

2) expired, e.g. due to non-renewal or withdrawal by the TSP or cessation of the scheme's operations;

3) suspended by the scheme;

4) revoked/not in accordance with the scheme's status determination criteria.

NOTE: Interpretation of service status:

In actual use of the information within a TSL, the status of a service needs to be fully determined and understood with reference to both the service's status as indicated and the status determination approach of the scheme. Table 1 is intended to assist in that understanding. The meanings given apply to a status given in either the current or historical part of the TSL, for a scheme which is known still to be operational.

Should the scheme no longer be operational (which may be determined by all the current statuses indicating "expired", or implied by the "next update" time having been exceeded) only the historic information should be relied upon. This is because either the status will have been set to "expired" when the scheme ceased operations and hence no subsequent status information will have been maintained, or the scheme ceased operations before it could effect a re-issue of the TSL in which case it could be uncertain the extent to which the indicated current status remained valid after the publication of the list.

Table 1: Meaning of Service status in relation to the Status determination approach

		Status determination approach		
		1 positive assessment (active approval)	**2 nomination/observation (passive approval)**	**3 non-compliant**
Service current or previous status	**1 in accordance**	An assessment has been performed on behalf of the scheme operator and the TSP and its service found to be in compliance.	The service is known to be operational and has not been found to be non-compliant with the scheme's criteria.	This combination cannot exist (since only those non-compliant with the scheme's criteria are listed).
	2 expired, not renewed	The validity of the assessment has lapsed without the service being re-assessed.	Unlikely to exist under these kind of scheme criteria.	This combination cannot exist (since only those TSPs and services non-compliant with the scheme's criteria are listed).
	3 suspended	No specific conclusion should be drawn - it could be because the service's validity is being verified (for reasons which are likely to be specific to the scheme) or there could be a delay in renewal, e.g.	Although no explicit approval is granted under these schemes, such a status could be used if a scheme's possible non-compliance was under investigation.	This combination unlikely to exist (since only those which are non-compliant are listed), although a scheme could, at its own discretion, use such a status if it was investigating a scheme's possible flagging as "non-compliant".
	4 revoked	Having once been found to be in conformance with the scheme's criteria, the TSP and/or the service have failed to continue to fulfil the criteria set by the scheme.	The TSP and/or the service have been found to be non-compliant with the criteria required by the scheme.	The TSP and/or the service have been found to be non-compliant with the criteria required by the scheme for the TSPs/services listed.

It should be understood that few schemes could state with absolute certitude that all services which potentially fall within their scope are actually listed within the TSL, irrespective of their status determination approach.

5.4.5 Current status starting date and time

Description: This field is mandatory. It shall specify the date and time on which the current approval status became effective.

Format: Character string.

Meaning: UTC time, expressed to the following accuracy: CCYY-MM-DD-HH-MM-SS.999 999 9 as specified in Coordinated Universal Time (UTC): Time scale based on the second as defined in ITU-R Recommendation TF.460-5 [8].

5.4.6 Scheme service definition URN

Description: This field is optional. If present, it shall specify the URN [4] where users (subscribers, relying parties) can obtain service-specific information provided by the scheme operator.

Format: Character string.

Meaning: The referenced URN must provide a path to information describing the service as specified by the scheme.

5.4.7 TSP service definition URN

Description: This field is optional. If present, it shall specify the URN [4] where users (subscribers, relying parties) can obtain service-specific information provided by the TSP.

Format: Character string.

Meaning: The referenced URN must provide a path to information describing the service as specified by the TSP.

5.4.8 Service approval history

Description: In the case where the service has no history prior to the current status (i.e. a first recorded status or history information not retained by the scheme operator) this field shall be empty. Otherwise, for each change in TSP service approval status which occurred within in the historical information period as specified in clause 5.2.11, information on the now previous approval status shall be provided in descending order of status change date and time (i.e. the date and time on which the subsequent approval status became effective).

Format: Sequence of History information (see clause 5.5).

5.5 History information

5.5.1 Service type identifier

Description: This field is mandatory. It shall specify the identifier of the service type.

Format: Integer.

Meaning: The identifier shall have one of the values specified in clause 5.4.1.

5.5.2 Service name

Description: This field is mandatory. It shall specify the name under which the TSP provided the service identified in clause 5.5.1.

Format: Unicode character string or multiple Unicode character strings encoded in UTF-8, each specifying the language used in accordance with ISO 639-1 Alpha 2 code [1] for the representation of names of languages. Where multiple languages are used, their representation shall be conformant with RFC 1766 [2].

Meaning: The name under which the TSP provided the service identified in clause 5.5.1 from the date and time given in clause 5.5.5 up to the date and time of the next status value.
Local language and cross-border (international) trading considerations may require that this information be provided both in a national language (and script) and in a commonly accepted internationally-used language.

5.5.3 Service digital identity

Description: This field is mandatory. It shall specify at least one representation of a digital identifier unique to the service specified in clause 5.5.1 by which the service can be unambiguously identified. The digital identifier may be present more than once and in different formats. If the digital identifier is present more than once, all variants must refer to the same identity.

Format: Character string or bit string or data structure specifying for each occurrence of the digital identifier the type of format and the data representing the digital identity. Implementation dependent - see annexes A and B.

Meaning: The digital identifier can be of different types depending on the service. It could be a certificate which can be used to verify electronic signatures of the service provider or a subject key identifier.

5.5.4 Service previous status

Description: This field is mandatory. It shall specify the identifier of the previous status of the service.

Format: Integer.

Meaning: The identifier shall have one of the values specified in clause 5.4.4.

5.5.5 Previous status starting date and time

Description: This field is mandatory. It shall specify the date and time on which the previous status in question became effective.

Format: Character string.

Meaning: UTC time.

5.6 Signature

5.6.1 Signed TSL

The TSP status list shall be signed by the scheme operator to ensure its authenticity and integrity. This clause does not prescribe the format of the signature but refers to clauses 6 and 7 for implementations using ASN.1 and XML respectively. Only general requirements regarding the signature are stated in this present clause.

5.6.2 Scheme operator identification

Description: This field is mandatory. It shall specify a reference uniquely identifying the scheme operator responsible for this TSL.

Format: Character string or Bit string.

Meaning: This shall either be an X.509-certificate [5], a value of an X.509v3 SubjectKeyIdentifier extension, a distinguished name [6], an issuer/serial number pair or a public key itself.

5.6.3 Signature algorithm identifier

Description: This field is mandatory. It shall specify the cryptographic algorithm that has been used to create the signature.

Format: Character string or Bit string, depending on format used.

Meaning: Depending on the algorithm used, this field may require additional parameters.

5.6.4 Signature value

Description: This field is mandatory. It shall contain the actual value of the digital signature. The calculation of the digital signature shall cover all fields described in clauses 5.2 to 5.5 as well as 5.6.2 and 5.6.3.

Format: Implementation dependent - see annexes A and B.

Meaning: Contains the actual value of the digital signature.

5.7 Trust-service Status List tag

5.7.1 Tagged TSL

The TSP shall be tagged to facilitate the identification of a TSL for electronic searches. This clause does not prescribe the format of the tag but refers to clauses 6 and 7 for implementations using ASN.1 and XML respectively. Therefore, only general requirements regarding the tag are stated in this present clause.

5.7.2 TSL tag

Description: This field is mandatory.

Format: Implementation dependent - see annexes A and B.

Value: A uniquely implementation dependent value enabling a web-searching tool to establish during a WWW-wide search for TSLs that a resource it has located is indeed a TSL conformant with the present document - see annexes A and B.

Annex A (normative): Implementation in ASN.1

This clause specifies the ASN.1 structures to be used when implementing an ASN.1-version of the present document. The field names used reflect those assigned to fields in clause 5.

```
TSL ::=SEQUENCE {
           ToBeSignedTSL     ToBeSignedTSL,
           tslSignature      TSLSignature }

ToBeSignedTSL ::=SEQUENCE {
           version                      Version,
           sequence                     SequenceNumber,
           algorithm                    AlgorithmIdentifier,
           schemeName                   SchemeName,
           schemeOperatorAddress        SchemeOperatorAddress,
           schemeInformationURN         SchemeInformationURN,
           statusDetermination          StatusDeterminationApproach,
           schemeType                   SchemeType OPTIONAL,
           schemeTerritory              SchemeTerritory OPTIONAL,
           tSL-Policy                   TSL-Policy OPTIONAL,
           historicalInformationPeriod  HistoricalInformationPeriod,
           pointersToOtherTSLs          PointersToOtherTSLs OPTIONAL,
           issuedAt                     IssuedAt,
           nextUpdate                   NextUpdate,
           tSPlist                      TSPlist }
```

A.1 Trust-service Status List tag

This field is mandatory. It shall facilitate the identification of the TSL as such, when electronic searches are conducted across the Internet. It shall be placed immediately before the ASN.1 implementation of the TSL structure specified in clause 5. The tag is implemented as an object identifier specified similar to the OID for CRLs.

```
id-trustServiceStatusListIdentifier OBJECT IDENTIFIER ::=
         { itu-t(0) identified-organization(4)
                    etsi(0) tsl-specification (2231) attributes (1) 0 }
```

A.2 Scheme information

A.2.1 TSL version identifier

This mandatory field specifies the version of the TSL format. In this version of the TSL it must have the value "1".

```
Version  ::=  INTEGER
```

A.2.2 TSL sequence number

This mandatory field specifies the sequence number of the TSL. At the first release of the TSL, the value of the sequence number shall be "1". The value shall be increased by "1" at each subsequent release of the TSL.

```
SequenceNumber  ::=  INTEGER
```

A.2.3 Signature algorithm identifier

This mandatory field contains the algorithm identifier for the algorithm used to sign the TSL. It must be the same algorithm identifier as in signature field of the TSL.

```
AlgorithmIdentifier  ::=  SEQUENCE  {
          algorithm               OBJECT IDENTIFIER,
          parameters              ANY DEFINED BY algorithm OPTIONAL  }
```

A.2.4 Scheme name

This mandatory field specifies the name(s) under which the scheme operates.

```
-- UNIVERSAL Types defined in 1993 and 1998 ASN.1
-- and required by this specification

UniversalString ::= [UNIVERSAL 28] IMPLICIT OCTET STRING
        -- UniversalString is defined in ASN.1:1993

UTF8String ::= [UNIVERSAL 12] IMPLICIT OCTET STRING
        -- The content of this type conforms to RFC 2279

TSLschemename ::= CHOICE {
          universalString   UniversalString ,
          utf8String        UTF8String }
```

A.2.5 Scheme operator address

This mandatory field includes the scheme operator postal address (see clause 5.2.5.1) and the scheme operator electronic address (see clause 5.2.5.2).

```
SchemeOperatorAddress ::= SEQUENCE {
          physicalDeliveryAddress  ORAddress,     -- imported X.400 address syntax
          emailAddress             IA5String }
```

A.2.6 Scheme information URN

This mandatory field specifies the URN where users can obtain scheme-specific information.

```
SchemeInformationURN  ::= IA5String
```

A.2.7 Status determination approach

This mandatory field specifies the status determination approach.

```
StatusDeterminationApproach  ::= ENUMERATED {
          active               (1),
          passive              (2),
          non-compliant        (3) }
```

A.2.8 Scheme type/community

This optional field is a registered Uniform Resource Name (URN), used when required to indicate a specific type of scheme.

```
SchemeType  ::= IA5String
```

A.2.9 Scheme territory

This optional field specifies the country in which the scheme is established.

```
SchemeTerritory ::=     PrintableString (SIZE (2))
```

A.2.10 TSL policy/legal notice

This optional field can be used to specify the scheme's policy or provide a notice concerning the legal status of the scheme or legal requirements met by the scheme for the jurisdiction in which the scheme is established and/or any constraints and conditions under which the TSL is maintained and offered. It can be provided in multiple languages. This string is either recognized as a registered URN or represents the textual form of the legal notice.

```
TSL-Policy  ::= UTF8String
```

A.2.11 Historical information period

This mandatory field contains the duration over which historical information in this TSL is provided (see clause 5.2.11).

```
HistoricalInformationPeriod  ::=  INTEGER
```

A.2.12 Pointers to other TSLs

This optional field specifies the URI where TSLs maintained by other scheme operators can be found.

```
PointersToOtherTSLs  ::= SEQUENCE OF
           OtherTSLPointer

OtherTSLPointer  ::= SEQUENCE {
           tSLLocation            IA5String,
           additionalInformation  IA5String  }
```

A.2.13 List issue date and time

This mandatory field gives date and time of the issuance of the TSL.

```
IssuedAt     ::= UTCTime
```

A.2.14 Next update

This mandatory field specifies the latest date and time by which the next TSL will be issued.

```
NextUpdate   ::= UTCTime
```

A.2.15 List of Trust Service Providers

This is the list of all TSP information. For each service provider a name field, an alternative trading name, an address, and a pointer to a web page are mandatory. The list of services offered is optional. If it is present it must contain at least one service.

```
TSPlist       ::=SEQUENCE OF
           TrustServiceProviderInformation

TrustServiceProviderInformation ::= SEQUENCE {
           tspname            TSPname,
           tradename      [0] TSPtradename OPTIONAL,
           tspaddress         TSPaddress,
           informationurn     IA5String,
           listofservices [1] ListofServices OPTIONAL }

TSPname ::= CHOICE {
           universalString    UniversalString ,
           utf8String         UTF8String }
TSPtradename ::= CHOICE {
           universalString    UniversalString ,
           utf8String         UTF8String }
TSPaddress ::= SEQUENCE {
           physicalDeliveryAddress  ORAddress,     -- imported X.400 address syntax
           emailAddress             IA5String }
ListofServices ::= SEQUENCE OF
           TSPserviceinformation
```

A.3 TSP service information

This is the description of one service.

```
TSPserviceinformation ::= SEQUENCE {
           type             ServiceType,
           name             ServiceName,
           digitalidentity  ServiceDigitalIdentity,
           currentstatus    ServiceStatus,
           start            UTCTime,
           schemeURN        IA5String OPTIONAL,
           tspURN           IA5String OPTIONAL,
           history          ServiceApprovalHistory }

ServiceType  ::= ENUMERATED {
           unspecified               (0),
           issuingcertificates       (1),
           issuingqcertificates      (2),
           timestamping              (3),
           certificatestatusprovision (4),
           registrationauthority     (5),
           identityverification      (6),
           certificategeneration     (7),
           attributeauthority        (8),
           archive                   (9),
           keyescrow                 (10) }

ServiceName  ::= CHOICE {
           universalString   UniversalString ,
           utf8String        UTF8String }
ServiceStatus  ::= ENUMERATED {
           inaccordance              (1),
           expired                   (2),
           suspended                 (3),
           revoked                   (4) }
```

A.3.1 Service digital identity

This is a mandatory field. The service digital identity can be realized in a number of different ways, depending on the service offered. It could be a certificate which can be used to verify electronic signatures of the service provider or a subject key identifier or a collection of these types. Each of the included attributes can be used for the identification of the service. How many have to be considered for a complete identification is beyond the scope of the present document, it being dependent on the policy of the TSP as well as that of the user/relying party.

```
ServiceDigitalIdentity ::= SET SIZE (1..MAX) OF IdentityAttributeTypeAndValue
IdentityAttributeTypeAndValue ::= SEQUENCE {
          type     IdentityAttributeType,
          value    IdentityAttributeValue }
IdentityAttributeType ::= OBJECT IDENTIFIER
IdentityAttributeValue ::= ANY DEFINED BY IdentityAttributeType
```

A.4 History information

The history information replicates the current status information.

```
ServiceApprovalHistory  ::= SEQUENCE OF
          TSPhistoryinformation

TSPhistoryinformation ::= SEQUENCE {
          type             ServiceType,
          name             ServiceName,
          digitalidentity  ServiceDigitalIdentity,
          previousstatus   ServiceStatus,
          start            UTCTime }
```

A.5 Signature

This mandatory field contains the signature value and the signing key information.

```
TSLSignature  ::= SEQUENCE {
          operatorIdentifier      OperatorIdentitifier,
          signatureAlgorithm      AlgorithmIdentifier,
          signaturevalue          BIT STRING  }

OperatorIdentitifier  ::= CHOICE {
          x509Certificate,
          SchemeKeyIdentifier }

SchemeKeyIdentifier  ::= SEQUENCE {
          keyIdentifier             [0] KeyIdentifier           OPTIONAL,
          authorityCertIssuer       [1] GeneralNames            OPTIONAL,
          authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL  }
KeyIdentifier ::= OCTET STRING  -- SHA-1 hash value of the public key
AlgorithmIdentifier  ::=  SEQUENCE  {
          algorithm            OBJECT IDENTIFIER,
          parameters           ANY DEFINED BY algorithm OPTIONAL  }
```

Annex B (normative): Implementation in XML

This clause specifies an XML schema to be used when implementing an XML-version of the present document. The field names used reflect those assigned to fields in clause 5.

B.1 XML-namespace and basic types

The XML namespace URI that must be used by implementations of the present document is:
http://uri.etsi.org/02231/v1.1.1.

The following namespace declarations apply for the XML Schema definitions throughout the present document:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema  targetNamespace='http://uri.etsi.org/02231/v1.1.1#'
             xmlns:tsl='http://uri.etsi.org/02231/v1.1.1#'
             xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
             xmlns:xsd="http://www.w3.org/2001/XMLSchema"
             xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
             elementFormDefault="qualified"
             attributeFormDefault="unqualified">
```

Several types are better specified separately. These types are specified in the clauses B.1.1 through B.1.6.

B.1.1 The InternationalNames Type

The `InternationalNamesType` specifies a format for giving alternative names in different languages and scripts.

```
  <xsd:complexType name="InternationalNamesType">
     <xsd:sequence maxOccurs="unbounded">
        <xsd:element name="Name">
           <xsd:complexType>
              <xsd:simpleContent>
                 <xsd:extension base="xsd:string">
                    <xsd:attribute ref="xml:lang" use="optional"/>
                 </xsd:extension>
              </xsd:simpleContent>
           </xsd:complexType>
        </xsd:element>
     </xsd:sequence>
  </xsd:complexType>
```

B.1.2 The AddressType Type

This type is used for addresses containing postal addresses and electronic addresses.

```
<xsd:complexType name="AddressType">
   <xsd:sequence>
      <xsd:element name="PostalAddresses" type="tsl:PostalAddressListType"/>
      <xsd:element name="ElectronicAddress" type="tsl:ElectronicAddressType"/>
   </xsd:sequence>
</xsd:complexType>
```

B.1.3 The PostalAddressListType Type

The PostalAddressListType Type allows specifying lists of postal addresses in different languages and scripts.

```
<xsd:complexType name="PostalAddressListType">
   <xsd:sequence>
      <xsd:element name="PostalAddress"
         type="tsl:PostalAddressType" maxOccurs="unbounded"/>
   </xsd:sequence>
</xsd:complexType>
```

B.1.4 The PostalAddress Type

The PostalAddress Type allows specifying one postal address.

```
<xsd:complexType name="PostalAddressType">
   <xsd:choice>
      <xsd:element name="StreetAdress" type="xsd:string" minOccurs="0"/>
      <xsd:element name="Locality" type="xsd:string" minOccurs="0"/>
      <xsd:element name="StateOrProvince" type="xsd:string" minOccurs="0"/>
      <xsd:element name="PostalCode" type="xsd:string" minOccurs="0"/>
      <xsd:element name="CountryName" type="xsd:string" minOccurs="0"/>
   </xsd:choice>
   <xsd:attribute ref="xml:lang" use="optional"/>
</xsd:complexType>
```

B.1.5 The ElectronicAddressType Type

The ElectronicAddressType Type allows specifying one electronic address.

```
<xsd:complexType name="ElectronicAddressType">
   <xsd:sequence maxOccurs="unbounded">
      <xsd:element name="URN" type="xsd:anyURI"/>
   </xsd:sequence>
</xsd:complexType>
```

B.2 The TrustserviceStatusList element

The `TrustserviceStatusList` element is the root element of an XML TSL. An implementation must generate *laxly schema valid* [XML-schema] `TrustserviceStatusList` elements as specified by the following schema.

```
<xsd:complexType name="TrustStatusListType">
   <xsd:sequence>
      <xsd:element  ref="tsl:TSLTag"/>
      <xsd:element  ref="tsl:SchemeInformation"/>
      <xsd:element  ref="tsl:TrustServiceProvider"
                    minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element  ref="ds:Signature"/>
   </xsd:sequence>
</xsd:complexType>
```

B.3 The SchemeInformation element

The SchemeInformation element is a container structure for all the elements giving detailed information about the scheme.

```
<xsd:element name="SchemeInformation" type="tsl:TSLSchemeInformationType"/>

<xsd:complexType name="TSLSchemeInformationType">
   <xsd:sequence>
      <xsd:element name="TSLVersionIdentifier" type="xsd:integer" fixed="1"/>
      <xsd:element name="TSLSequenceNumber" type="xsd:integer"/>
      <xsd:element name="SchemeName" type="tsl:InternationalNamesType"/>
      <xsd:element name="SchemeOperatorAddress" type="tsl:AddressType"/>
      <xsd:element name="SchemeInformationURN" type="xsd:anyURI"/>
      <xsd:element name="StatusDeterminationApproach" type="xsd:integer"/>
      <xsd:element name="SchemeType" type="xsd:anyURI" minOccurs="0"/>
      <xsd:element name="SchemeTerritory" type="xsd:string" minOccurs="0"/>
      <xsd:element name="PolicyOrLegalNotice" type="tsl:PolicyOrLegalnoticeType"
         minOccurs="0"/>
      <xsd:element name="HistoricalInformationPeriod" type="xsd:integer"/>
      <xsd:element name="PointersToOtherTSL" type="xsd:anyURI" minOccurs="0"/>
      <xsd:element name="ListIssueDateTime" type="xsd:dateTime"/>
      <xsd:element name="NextUpdate" type="xsd:dateTime"/>
   </xsd:sequence>
</xsd:complexType>
```

B.3.1 The TSLVersionIdentifier element

This mandatory element specifies the version of the TSL format. In this version of the TSL it must have the value "1".

```
<xsd:element name="TSLVersionIdentifier" type="xsd:integer" fixed= "1" />
```

B.3.2 The TSLSequenceNumber element

This mandatory element specifies the sequence number of the TSL. At the first release of the TSL, the value of the sequence number shall be "1". The value shall be increased by "1" at each subsequent release of the TSL.

```
<xsd:element name="TSLSequenceNumber" type="xsd:integer"/>
```

B.3.3 The SignatureAlgorithmIdentifier element

This mandatory element is part of the Signature Element described in clause B.7.

B.3.4 The SchemeName element

The mandatory element specifies the name(s) under which the scheme operates.

```
<xsd:element name="SchemeName" type="tsl:InternationalNamesType"/>
```

B.3.5 The SchemeOperatorAddress element

This mandatory element specifies the format for representing the address details of the scheme operator.

```
<xsd:element name="SchemeOperatorAddress" type="tsl:AddressType"/>
```

B.3.6 The SchemeInformationURN element

This mandatory element specifies the URN where users can obtain scheme-specific information.

```
<xsd:element name="SchemeInformationURN" type="xsd:anyURI"/>
```

B.3.7 The StatusDeterminationApproach element

This mandatory element specifies the status determination approach (see clause 5.2.7).

```
<xsd:element name="StatusDeterminationApproach" type="xsd:integer"/>
```

B.3.8 The SchemeType element

This optional element is used to indicate a specific type of scheme or community in which the scheme is used.

```
<xsd:element name="SchemeType" type="xsd:anyURI" minOccurs="0"/>
```

B.3.9 The SchemeTerritory element

This optional element specifies the country in which the scheme is established.

```
<xsd:element name="SchemeTerritory" type="xsd:string" minOccurs="0"/>
```

B.3.10 The PolicyOrLegalNotice element

This optional element can be used to specify the scheme's policy or provide a notice concerning the legal status of the scheme or legal requirements met by the scheme for the jurisdiction in which the scheme is established and/or any constraints and conditions under which the TSL is maintained and offered. It can be provided in multiple languages.

```
<xsd:element name="PolicyOrLegalNotice" type="tsl:PolicyOrLegalnoticeType"
   minOccurs="0" />
```

The PolicyAndLegalNotice Type allows specification of the language used.

```
<xsd:complexType name="PolicyOrLegalnoticeType">
   <xsd:choice>
      <xsd:element name="TSLPolicy" type="xsd:anyURI"/>
      <xsd:element name="TSLLegalNotice" type="xsd:string"/>
   </xsd:choice>
   <xsd:attribute ref="xml:lang" use="optional"/>
</xsd:complexType>
```

B.3.11 The HistoricalInformationPeriod element

This mandatory element contains the duration over which historical information in this TSL is provided (see clause 5.2.11).

```
<xsd:element name="HistoricalInformationPeriod" type="xsd:integer"/>
```

B.3.12 The PointersToOtherTSL element

This optional element specifies URIs where users can obtain other TSLs. The OtherTSLPointersType specifies a list of tupels containing a URI pointing to the TSL and additional information about that TSL which is implementation-specific.

```
<xsd:element name="PointersToOtherTSL" type="tsl:OtherTSLPointersType "
     minOccurs="0"/>
```

```
<xsd:complexType name="OtherTSLPointersType">
   <xsd:sequence>
      <xsd:element name="OtherTSLPointer" type="tsl:OtherTSLPointer"/>
   </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="OtherTSLPointer">
   <xsd:sequence>
      <xsd:element name="TSLLocation" type="xsd:anyURI"/>
      <xsd:element name="AdditionalInformation" type="xsd:string"/>
   </xsd:sequence>
</xsd:complexType>
```

B.3.13 The `ListIssueDateTime` element

This mandatory element specifies the date and time of the issuance of the TSL.

```
<xsd:element name="ListIssueDateTime" type="xsd:dateTime"/>>
```

B.3.14 The `NextUpdate` element

This mandatory element specifies the latest date and time by which the next TSL will be issued.

```
<xsd:element name="NextUpdate" type="xsd:dateTime"/>
```

B.3.15 The `TrustServiceProvider` element

This element contains all information related to one TSP. It is of type `TSPType` whose content is described in clause B.4.

```
<xsd:element name="TrustServiceProvider" type="tsl:TSPType"/>

<xsd:complexType name="TSPType">
   <xsd:sequence>
      <xsd:element name="TSPInformation" type="tsl:TSPInformationType"/>
      <xsd:sequence>
         <xsd:element ref="tsl:TSPServices" maxOccurs="unbounded"/>
      </xsd:sequence>
   </xsd:sequence>
</xsd:complexType>
```

B.4 The TSPInformation element

The TSPInformation element has the following structure.

```
<xsd:complexType name="TSPInformationType">
   <xsd:sequence>
      <xsd:element name="TSPName" type="tsl:InternationalNamesType"/>
      <xsd:element name="TSPTradeName" type="tsl:InternationalNamesType"
         minOccurs="0"/>
      <xsd:element name="TSPAddress" type="tsl:AddressType"/>
      <xsd:element name="TSPInformationURI" type="xsd:anyURI"/>
   </xsd:sequence>
</xsd:complexType>
```

B.4.1 The TSPName element

This mandatory element contains the name of the TSP.

```
<xsd:element name="TSPName" type="tsl:InternationalNamesType"/>
```

B.4.2 The TSPTradeName element

This optional element contains alternative trading names of the TSP.

```
<xsd:element name="TSPTradeName" type="tsl:InternationalNamesType" minOccurs="0"/>
```

B.4.3 The TSPAddress element

This mandatory element contains the address of the TSP.

```
<xsd:element name="TSPAddress" type="tsl:AddressType"/>
```

B.4.4 The TSPInformationURI element

This mandatory element contains a pointer to a web page containing service-specific information.

```
<xsd:element name="TSPInformationURI" type="xsd:anyURI"/>
```

B.4.5 The TSPServices element

The TSPServices element is a list of Trust-Services the TSP offers. The elements of that structure are specified in clause B.5.

```
<xsd:element name="TSPServices" type="tsl:TSPServicesType"/>

<xsd:complexType name="TSPServicesType">
   <xsd:sequence>
      <xsd:element ref="tsl:ServiceInformation"/>
      <xsd:element name="ServiceHistory" type="tsl:ServiceHistoryType"/>
   </xsd:sequence>
</xsd:complexType>
```

B.5 The ServiceInformation element

The ServiceInformation element is a container element containing information about a service.

```
<xsd:element name="ServiceInformation" type="tsl:TSPServiceInformationType"/>
<xsd:complexType name="tsl:TSPServiceInformationType">
   <xsd:sequence>
      <xsd:element ref="tsl:ServiceStatusInformation"/>
      <xsd:element name="SchemeServiceDefinitionURI" type="xsd:anyURI" minOccurs="0"/>
      <xsd:element name="TSPServiceDefinitionURI" type="xsd:anyURI" minOccurs="0"/>
   </xsd:sequence>
</xsd:complexType>>
```

The information that is part of the current status information as well as the ServiceHistory has been specified as one special type (as follows) useable in both places. It also allows implementations to easily transfer a ServiceStatus element into the ServiceHistory element.

```
<xsd:element name="ServiceStatusInformation" type="tsl:ServiceStatusInformationType"/>

<xsd:complexType name="ServiceStatusInformationType">
   <xsd:sequence>
      <xsd:element name="ServiceTypeIdentifier" type="xsd:integer"/>
      <xsd:element name="ServiceName" type="tsl:InternationalNamesType"/>
      <xsd:element name="ServiceDigitalIdentity" type="tsl:digitalIdentityListType"/>
      <xsd:element name="ServiceStatus" type="xsd:integer"/>
      <xsd:element name="StatusStartingTime" type="xsd:dateTime"/>
   </xsd:sequence>
</xsd:complexType>
```

B.5.1 The ServiceTypeIdentifier element

This mandatory element specifies the identifier of the service type.

```
<xsd:element name="ServiceTypeIdentifier" type="xsd:integer"/>
```

B.5.2 The ServiceName element

This mandatory element specifies the name under which the service is provided.

```
<xsd:element name="ServiceName" type="tsl:InternationalNamesType"/>
```

B.5.3 The ServiceDigitalIdentity element

This is a mandatory field. The ServiceDigitalIdentity element borrows from XMLDSig's specification. It allows two representations for key: keyvalue, as specified in XMLDSig, and X509Certificate. The latter is not directly referable to, since it is a base64-encoded binary element and not a type. Implementations must implement the X509Certificate-element exactly as specified in XMLDSig.

```
<xsd:element name="ServiceDigitalIdentity" type="tsl:digitalIdentityListType"/>

<xsd:complexType name="digitalIdentityListType">
   <xsd:sequence maxOccurs='unbounded'>
      <xsd:element name="digitalId" type="tsl:digitalIdentityType"/>
   </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="digitalIdentityType">
   <xsd:choice>
      <xsd:element name="X509Certificate" type="xsd:base64Binary"/>
      <xsd:element name="keyValue" type="ds:KeyValueType"/>
      <xsd:sequence>
         <xsd:element name="digitalIdType" type="xsd:string"/>
         <xsd:element name="digitalIdValue" type="xsd:anyType"/>
      </xsd:sequence>
   </xsd:choice>
</xsd:complexType>
```

B.5.4 The ServiceStatus element

This mandatory element specifies the identifier of the status of the service (see clause 5.4.4).

```
<xsd:element name="ServiceStatus" type="xsd:integer"/>
```

B.5.5 The StatusStartingTime element

This mandatory element specifies the date and time on which the current status became effective.

```
<xsd:element name="StatusStartingTime" type="xsd:dateTime"/>
```

B.5.6 The SchemeServiceDefinitionURI element

This optional element specifies the URN where users can obtain service-specific information provided by the scheme operator.

```
<xsd:element name="SchemeServiceDefinitionURI" type="xsd:anyURI" minOccurs="0"/>
```

B.5.7 The TSPServiceDefinitionURI element

This optional field specifies the URN where users can obtain service-specific information provided by the TSP.

```
<xsd:element name="TSPServiceDefinitionURI" type="xsd:anyURI" minOccurs="0"/>
```

B.5.8 The `ServiceHistory` element

This optional field provides any historical status information.

```
<xsd:element name="ServiceHistory" type="tsl:ServiceHistoryType"/>
```

B.6 The `ServiceHistory` type

The service history structure as specified in clause 5.5 is equivalent to the information contained in clause 5.4. For XML, the relevant fields have been specified in clauses B.5.1 through B.5.5 representing clauses 5.4.1 through 5.4.5 as well as 5.5.1 through 5.5.5. Clause B.6 therefore does not need to specify additional XML schemas.

```
<xsd:complexType name="ServiceHistoryType">
   <xsd:sequence>
      <xsd:element ref="tsl:ServiceStatusInformation" minOccurs="0"
          maxOccurs="unbounded"/>
   </xsd:sequence>
</xsd:complexType>
```

B.7 The Signature element

The present document uses the XMLDSig-Standard for signing a TSL. The TSL-structure contains a Signature element that represents an enveloped signature-type.

B.8 The TSLTag element

The TSLTag is not required as a special element in this XML-specification. It only makes sense to have structural compatibility to ASN.1 or by providing the same value as the ASN.1 version or as an element useable by other XML-schemes for TSLs that are similar but different.

NOTE: Any future developments which lead to new ways in which to implement the TSL should have any implementation-specific aspects described in additional dedicated clauses, to be included hereafter.

Annex C (informative): Implementation considerations

C.1 General

This informative annex describes implementation considerations which are beyond the normative scope of the present document. The parties affected by these considerations will be the various scheme operators, TSPs which may want to participate within or may be the subjects of schemes which adopt the TSL, and developers and vendors of proprietary products and services which support users engaging in electronic transactions and which may want to access information within a TSL. Access to a TSL may be either to retrieve information in human-readable form or for the purposes of automated processing, which may include determining what level of reliance can be placed upon the status information which a TSL provides.

Annex E also provides implementation guidance in the form of an explanatory rationale for each TSL field.

C.2 What is a Service?

It is the expectation, from understanding of the schemes presently existing, that a trust-service whose service status is reported within a TSL is dealt with "in its own right", i.e. it is solely the status of **that** service which is given. It may be expected that, in establishing the status of a trust service, a scheme's rules will require examination and assessment of secondary services (which could be independent trust services in their own right) on which that trust service relies. The extent to which this is applied must be determined by each scheme according to its own principles, and could range from examining contractual arrangements to in-depth assessment of the secondary service, or perhaps the acceptance of that service's independent approval under the same or another scheme.

However, it is not expected that the TSL will support directly a chain of trust dependencies where secondary services are used. It is the responsibility of the relying party to determine whether such relationships exist, if that is of significance for them, and to make separate checks within available TSLs for any status information they may require. They may expect to find this information on the TSP's or the service's web site, pointers to which are provided from within a TSL.

C.3 TSL publication

These guidelines recommend that, given the circumstances and processes described in the following clauses, a sufficiently reliable method for publication of a TSL is to have it published on the scheme operator's web-site, and then replicated on additional sites, supported by an equally distributed self-signed certificate for the signing key used for signing that TSL.

C.3.1 Scoping the TSL population

TSLs are intended to play a valuable role in the process when deciding what level of assurance to have in a trust service and its provider. However, TSLs are unlikely to be considered to be essential, nor to be a pivotal point of trust. It is likely that they will deliver broad confidence to business and personal users as much as adding assurance on a discrete transactional level.

It is considered unlikely that, in WWW terms, there will be a large number of TSLs. Certainly in the short term we might envisage: two per EU Member State (allowing for imminent expansion of the EU, and both a supervision and a voluntary scheme per country, this would amount to fifty); one from each of another twenty nations worldwide (possibly being promoted through regional economic communities other than the European Economic Community, e.g. the Asia-Pacific Economic Community); five industry/international schemes not territorially limited (e.g. WebTrust for CAs, Identrus...). This amounts, globally, to seventy-five TSLs foreseeable within the period up until the end of 2006. It is considered unlikely that the average number of services and TSPs across all these TSLs will rise above ten during this period. Up to 750 services are therefore considered a reasonable figure, possibly up to 1 500.

C.3.2 Publication guidelines

TSLs then, will be relatively few in number, with only moderate numbers of service statuses described within them and furthermore, since it is unlikely that services will come and go with great rapidity (in terms of internet-speed), they will have a low frequency of information change (Low-FIC).

For this reason, this annex suggests a low-complexity approach to the publication of TSLs and to control over their authenticity, based upon safety in numbers (of copies of each TSL) rather than management within tightly controlled hierarchies, highly secure infrastructures and complex cryptography (although positive use of cryptographic functions are proposed).

C.3.2.1 Provision of the scheme operator's public (verification) key

As defined by the present document, a TSL is a signed electronic document. To verify the signature, relying parties need to be able to access the applicable public key. Since the scheme issuing the TSL is effectively positioned "above" the TSPs approved by that scheme, the authenticity of the public key cannot be certified by any TSP inside or outside the scheme. Therefore, the acceptance of the public key and its installation by the user in his/her computer system cannot be fully automated in the general case. How users accomplish this is dealt with in a following clause.

At an appropriate point in time, e.g. when first becoming operational, or subsequently for any other good reason, a TSL-operating scheme generates a key-pair for the purposes of signing its TSL and issues a self-signed Public Key Certificate (PKC) relating to these keys. The keys could alternatively pre-exist, for the purposes of signing any formal documents relating to formal approval of the TSPs and the trust services referenced by the TSL. Furthermore, the scheme could operate within an hierarchical trust model, and the PKC could be signed by some recognized authority. The present document recommends self-signed certificates.

The scheme operator then publishes this certificate, ensuring that there are a number of ways to verify the authenticity of it, e.g. by publishing the fingerprint in an official publication and on its own web page. The certificate may also be published by any TSP operating under that scheme, perhaps also by other TSPs outside the scheme, or through other sources which are considered to be stable and reliable, such as other schemes or industry and governmental bodies.

Naturally, appropriate measures need to be taken when generating, storing and distributing the scheme operator's signing keys, akin to the steps employed by any reliable trust-service provider issuing PKCs.

C.3.2.2 Publication of the TSL

Whenever a new or revised (or possibly simply re-issued) TSL is published by a scheme operator it should be immediately made available through the scheme operator's own web site and at the same time securely distributed to the other locations where it is normally hosted. As for the distribution of the scheme's TSL-signing PKC, such bodies will be TSPs operating under that scheme, perhaps also other TSPs outside the scheme, or other sources which are considered to be stable and reliable, such as other schemes or industry and governmental bodies.

Thus, both the TSL and the PKC for the keys used to sign it will be distributed across multiple sites, and the typical Low-FIC will make it a stable entity, subjected to infrequent change which, when change does occur, should be updated rapidly across those sites.

C.3.2.3 Security issues

It is recognized that a part of the security of this approach relies upon there being a reasonable number of TSPs and services, on the web sites of which could be published the TSL and the related scheme's PKC, to ensure that complete replacement of these sources is a complex and difficult task. However, some specific considerations need to be made.

Where the number of services covered by any one scheme is small the low number of replications increases the vulnerability of the system. This can be overcome by encouraging the publication of the TSL and related PKC on other sites, such as those of government and industry bodies, and co-operating schemes.

Additionally, the public key corresponding to the scheme operator's signing key could be bound into a certificate by each participating TSP, and these certificates published as widely as is the list and the scheme operator's self-signed certificate. Thus, the level of complexity required of any agent intending to corrupt the TSL is increased quite significantly.

Although the idea of a harmonized TSL is to bring all scheme representations up to a consistent level of robustness, early implementations which exercise the "opt-out" implementation of a TSL may find themselves unable to publish their TSL a sufficient number of times. Taking for example a scheme operating only on a "black list" principle, it could be naïve to expect to find willing those TSPs whose services have been indicated as being in default according to the scheme's criteria - there is absolutely no incentive for them to display their own failure! A solution to this could be for such schemes to actually include within their list all TSPs falling within the scope of the scheme and making a distinct separation between those schemes who continue to operate in conformance with the "failure" criteria as well as those who fall into the "black list" zone. This could readily be accomplished by using the appropriate "status" indicators in the standard.

Additionally, some schemes may find comfort in existing within a hierarchical trust model, the wider implications of which could compensate for a small number of published copies of their TSL.

This decision process may be a manual one where a person assesses TSP-related information, or an automated one. It is beyond the scope of the present document to consider the complexities of how subjective manual decisions based upon TSL-derived information can be reached, whether published as a web page or printed on paper. This clause therefore focuses on the automated case only, where a signed TSL is handled by some piece of software which needs to make an automated decision.

C.3.2.4 Identifying TSPs

Whenever a scheme operator adds a TSP to a TSL, it is important to users of the TSL to be able to unambiguously identify if an entry is related to the TSP he is interested in. While name and address may be highly relevant and therefore very important, the digital identity-field is the only option that can provide for a secure link to the TSP. When using public key technology, this will be one representation of the public key(s) the TSP uses for providing its services; e.g. the key used for signing certificates or OCSP responses. The *service digital identity*-field does not, however, prescribe a specific format for this identifier, since the TSL is intended to be applicable to services based on technologies other than PKI.

For PKI-applications, applications also have choices as to how to present the digital identifier. For creating or parsing TSLs, applications should support two formats for the *service digital identity*:

- one of the two methods defined in RFC 3280 [9], section 4.2.1.2, on how to calculate subject key identifiers for CA certificates;
- X.509-certificates.

C.4 Locating a TSL

TSLs serve at least three distinct purposes. In the first instance, they act as a directory of the TSPs and the trust services which fall within a particular scheme, in accordance with the selection criteria established by the scheme. It is anticipated (and is the primary rationale behind the TSL defined in the present document) that such schemes would apply positive criteria, compliance with which would admit trust services into the TSL. In such a case, the TSL acts as a directory of the services which have succeeded in gaining entry to the scheme. This leads to their second purpose, which is to enable interested parties to review the TSL to see which organizations are offering services, what range of services are available and, ideally, what status history they have enjoyed.

It is clear that, at least in the interim period, some schemes will exist, and could implement a TSL, which apply criteria which highlight services which fall short of certain expectations. In such a case the second potential use of TSLs becomes a kind of warning mechanism, which can only contribute to mistrust, rather than trust.

The third potential use of a TSL, and one which presents the most difficulties, is as a means of adding assurance to a relying party who receives a form of e-communication signed by a party whom she does not know (Unknown Party - UP) and supported by a trust-service provider of whom she has never heard (Unheard-of TSP - UTSP). In this case, the relying party would want to interrogate any TSL which has information about UTSP.

NOTE: Any TSL - there may be more than one within whose scope falls the indicated TSP.

This draws the question "How is the relying party to find this information which some TSL may be able to offer?" - in other words, how can the, or any, TSL(s) be located?

C.4.1 TSL location models

Three models by which TSL location information can be provided can be considered. They are: Bound, Linked, and De-coupled. Each is explained and their comparative merits considered.

In the present document the idea of a "trust service" is broad, and in the following clauses the use of the generic term "trust service token" is intended to mean any token provided by a TSP in respect of the service it rendered. The "usual suspect" would be a certificate issued by a certification authority, but it could be any other indication or attestation concerning a trust service, such as a statement that private keys are held in escrow, that someone's identity has been verified against specific criteria, that insurance cover or a bond has been issued, etc. Furthermore, it need not necessarily be a PKI service, simply a trust service.

C.4.1.1 Bound information

In this model, information about a TSL (or possibly more than one) is intimately bound into the trust service token. In other words, the TSP advertises the fact that its service fulfils the criteria of the indicated scheme. The user initiating the communication (i.e. the sender) need not be aware of the inclusion of this information.

Such a solution is easy in terms of the need to locate a TSL - the work is done - but it is "dirty" in that it renders the token a victim of the continued fulfilment of the scheme's criteria, and indeed the stability of the scheme itself. In the event that the status of the trust service changes, or the scheme's PKC itself is revoked, or the scheme substantially changes its criteria, or even ceases to exist in its recognized state, the trust service token would most probably need to be revoked. This has the implication that a TSP issuing large volumes of tokens would have to revoke and re-issue them in the case of any of these failures originating largely outside its control (of course it may well be that in the change in its status is the result of some action (or inaction) on the part of the TSP itself.

In the case of "black list" principle TSLs, it is manifestly unlikely that a TSP will bind in information of a negative nature, and so here the Bound model most probably does not apply. By the same token, even schemes applying positive criteria may find TSPs unwilling to bind in a pointer to information which may put them in a bad light if, for example, they have suffered a degradation in their approval status.

The bound model therefore suffers from its sensitivity to changes from a number of other sources and from circumstances where the TSP may feel jeopardized by inclusion of a reference to its present status. Nevertheless, if used this model obviates the need to search for a TSL (although there may be other TSLs not referenced which might have useful information about the trust service).

C.4.1.2 Linked information

In this model, information about any relevant TSL(s) is included within the transaction but not in a way which binds it intimately to the service token. The TSL location could be included by an application, possibly configured by either the user or their service provider; the user may not need to know about it, but transparency may not always be so clear as with the Bound model. The Linked model has the obvious advantage that status information is provided separately from the trust service token and hence could change without having any impact on the trust service token (although according to the nature of the scheme, this may not always be so).

Most of the arguments about the willingness of TSPs to include this information apply as they do to the Bound model. However, it is clearly less sensitive to status changes and also makes it unnecessary to search for TSL information, with the same caveat that there may be other TSLs not referenced which might have useful information about the trust service.

C.4.1.3 De-coupled information

In the De-coupled model there is no TSP location information provided with the transaction - it is up to the relying party to find it herself. This has the distinct advantage of there being no dependency on the TSP to provide the information, no need for the sender to have any knowledge of this information either. Furthermore, this model is effectively the default value and is therefore by default backward compatible.

This is therefore much cleaner than either of the preceding models, but it carries a potential penalty: the relying party's system has to search for the TSL, and the search may have no initial clues as to where to look.

C.4.2 Searching for a TSL

It becomes necessary to search for a TSL particularly in the case of the De-coupled model, but it may also be necessary where the information provided through the Bound and Un-Linked cases is inadequate for some reason. Note that a search may also be appropriate simply when an interested party seeks information about a particular TSP and/or its services but does not know where to find an associated TSL.

Searching can be broken down into three potential stages which can be regarded as offering decremental ease of searching. These are described below, starting with the simplest.

C.4.2.1 Same-scheme searching

In this case the relying party is able to use the TSL belonging to any scheme(s) within which fall any TSPs with whom he himself has a relationship (and presumably, therefore, in which he has some assurance) - we will use the term "relying-party's scheme/TSL" as a convenience, although strictly speaking there is no direct relationship between the relying party as a subscriber to a service and any scheme under which that service operates. Such an approach would work where the counter-party's TSP lies within the same, or one of the, relying party's schemes. Each of the TSLs associated with those schemes could be searched for the presence of status information relating to the counter-party's TSP.

C.4.2.2 Known scheme searching

In this case there are three possible options, each dependent upon the relying party being a subscriber to at least one trust service which is within a TSL-issuing scheme, i.e. that there is a "relying-party scheme" as explained above. These options may exist in any combination.

In the first case, if the relying-party's scheme operates under a Root Key Authority (RKA) then it may be possible to derive from that RKA the location of other schemes which provide TSLs and which could be assumed to have the same degree of assurance as the relying-party's scheme.

In the second case, the relying-party's TSL could contain within it a pointer or pointers to other TSLs (see clause 5.2.12) which the relying-party's scheme operators feel worthy of some degree of recognition. How one scheme operator determines that another TSL is sufficiently reliable to merit inclusion in their own is not defined by the present document. The scheme operator would be expected to make publicly accessible their policy for doing so.

In the third case, the relying party may have built up their own list of TSLs which they regard as reliable and could search any of those.

Thus by any combination of the above options, the relying party could have identified TSLs within which they could search for the presence of status information relating to the counter-party's TSP.

If none of the options in this and the preceding part are successful, then a "blind" search may be conducted, as described in clause C.4.2.3.

C.4.2.3 "Blind" (unknown) scheme searching

These guidelines suggest that standard Internet search engines are used for this purpose, with a supporting front-end to construct an appropriate query. The basic search mechanism would be to take the unique service-related information from the trust service token (i.e. a unique service name which could be matched to the TSL field "Service digital identity"), include the "Trust-service Status List tag" and use these to construct a query for available search engines. Although the tag is used, one would expect a certain degree of "junk" finds to be reported by these generic engines. The front-end application would then need to sort them according to specific criteria, leading to a list which was only TSLs which had a reference to the uniquely identified trust service. Further refinement could separate multiple occurrences of the same TSL (on different sites) from distinct alternative TSLs.

There may be an alternative to the need to perform such a search, if there is available some trusted source of pointers to (or possibly reliable copies of) TSLs. These could be from the user's own TSP(s) or from some other established resource. In such cases a search across the Internet may not be required.

At this stage it could be possible to formulate a response to the query, depending on how it was expressed (e.g. if no TSLs are found and the question was "Does this service appear in any TSLs?" then one might conclude a negative response.

At the time of publication of the present document, no search engines have been found capable of parsing, and then indexing, WWW-pages whose MIME-Type they do not understand. Therefore, searching for TSLs at this moment would yield no results. Putting a searchable string into the TSL data structure is, therefore, only for future use, when search engines fully index any XML-page they find or alternatively find TSLs important enough to understand the format directly. Until then, we can only recommend TSL operators to edit a webpage in HTML, which can and will be indexed by search engines, which contains standard hyperlinks to the TSLs themselves. The front-end application then can try to follow these hyperlinks and check whether they locate a TSL that way.
Using Mimetypes Application/TSL-ASN.1 and Application/TSL-XML would help these applications to locate TSLs.

Assuming that at least one TSL having reference to the specific service is located, by any of the means described in this annex, there is now a need to verify the TSL.

C.5 Verifying a TSL

The proposed implementation of a Verification relates to the manner of publication described in clause 6.1. For each TSL located the following tests should be applied.

Starting with the TSL's host site (i.e. the web-site of the scheme which maintains this TSL), ensure that the published PKC authenticates the signature on the TSL. It is also necessary to ensure that the validity period of the TSL has not expired (see "Latest next update"). If either of these checks fails, the TSL verification fails overall.

If there are multiple occurrences of the TSL perform the same check on each of them, taking the same action if any one signature authentication fails.

NOTE: It may be tempting to also verify that each replication of the TSL stems from an explicit reference to a TSP or service from within the TSL, but additional replication is permissible and may indeed add to the overall strength of the TSL model, and hence "second generation" replication is to be encouraged so long as it is always included in verifications.

If all located multiple occurrences of the TSL are successfully authenticated then internal checks are required. These checks assume that service providers mentioned in lists will replicate the TSL, and since this is unlikely to be the case for "black list" TSLs, this check should not be conducted in such a case. When these checks are to be made, a sufficient number of cross checks are performed, from the choice of service providers in the list, to ensure that the TSL replicated on the site of the TSP and the corresponding TSL PKC found there are indeed the same. This check should not be undertaken for the TSP whose service is being claimed in the transaction, since this may serve only to demonstrate the same information as is being verified - it is the other sites whose responses are required. If any one of these authentications fails, the whole verification should be considered to have failed.

Whenever the verification fails overall a response to the query has to be constructed. If the verification succeeds then a query can be processed after parsing and interpreting the information within the TSL.

The process as so far described is the default verification of any TSLs which are located. However, additional verification measures could be undertaken to determine whether a TSL should be trusted.

C.5.1 Further verification issues

The process to be followed by any user that wants to use a TSL is very similar to the steps that need to be taken when deciding about trust in a certification authority. If public key certificates are used in this process, the relying parties' software should be able to distinguish between certificates trusted for issuing certificates and certificates trusted for issuing TSLs.

Having identified, located and verified a TSL, the user could then carry out any further steps to establish trust in the scheme/TSL as required by their own policy. Consequently the user decides whether or not to trust the scheme and the TSLs it operates. Only if these further checks are positive is the information within the TSL relied upon.

The user can then take steps to ensure that on future searches this TSL is automatically accepted as being reliable. A typical procedure might therefore look like the following:

1) User imports the TSL's public key certificate into the software.

2) User sets the status of the imported certificate to something like "*trusted for issuing TSLs"*.

3) User subsequently uses the certificate to verify TSLs maintained by the specified scheme.

This procedure can be performed by each user, but will in many cases be carried out on the level of an organization according to their own policy. In this case, the software environment of each user's machine would typically be pre-configured by the system administration or by the security officer. In time it is likely and certainly possible that such certificates could also be pre-installed in browsers, so enabling personal users to gain advantage from this approach.

In the case of compromise of the scheme's private key, the user must be informed in the same manner as in the case of a key compromise of a TSP's self-certified key. Such key compromise will get broad attention, since there will only be a limited number of schemes operational, they will be widely known, and furthermore their certificates (and therefore notification of their certificates' revocation) will be widely available, ensuring that such events will not remain unnoticed.

A scheme operator may also provide mechanisms compatible with the standard way of handling revocation information: add a CRL distribution point extension into the self-signed certificate and provide a CRL at that point. A compliant client implementation could then also automatically check that CRL to detect any revocation.

C.6 Management and performance of TSL provision

The TSL is a mechanism which is supporting of electronic transactions but not essential for them. There remains a variety of different models on which schemes operate and a variance in how information from TSLs can be interpreted. Because of this lesser degree of dependence upon the TSL, the need to keep up to date information within a TSL is less urgent than that for, e.g. a CRL.

Scheme operators should publish their specific criteria for the provision of revisions to TSL information. These revisions will fall into the following categories.

C.6.1 Change of scheme administrative information

This category includes any changes to information concerning the scheme and which is embedded within the TSL. Such changes could include, inter alia, change of scheme addresses, revisions to acceptance criteria, scheme policy. When these change the TSL should be re-issued.

If there are material changes to information directly referenced through the TSL but the reference itself doesn't change then there will be no need to amend the TSL.

Any changes in this category should not affect the status information concerning any trust services mentioned within the TSL.

If the changes were the result of a change of ownership of the entity operating the scheme then the scheme could continue to operate without change or the scheme could cease operations and re-establish itself as a new scheme. It would be for the operators to determine how they wanted to handle this and how they would deal with the handling of services recognized under the scheme.

C.6.2 Change of TSP administrative information

This category includes any changes to the information pertaining to a TSP and/or its service(s) which is/are referenced within the TSL. Such changes could include, inter alia, change of TSP addresses, location of specific information referenced by a URN. When any of these change the TSL should be re-issued without any change to the status information pertaining to services operated by the TSP concerned.

When any administrative change occurs the TSL should be re-issued with the previous "Service information" (see clause 5.4) becoming the most recent "History information" (see clause 5.5) and a new "Service information" entry being updated to reflect the new administrative information (without any change to the status itself).

A change to the "Service digital identity" (see clause 5.4.3) should be considered as a change to the service status - see clause C.6.3.

C.6.3 Change of trust-service status

These changes are those directly affecting the inclusion, exclusion or reported status of any trust service within the TSL (and possibly also information concerning their provider) and whether the information is current or historical (e.g. the introduction of a new TSP and service; the revocation of a service).

When any such change occurs the TSL should be re-issued with the previous current status becoming the most recent historical status and current status being amended to reflect the situation.

Where a service changes its "Service digital identity" (see clause 5.4.3), e.g. as a result of a take-over or a re-branding or a renewal of associated digital data for security reasons, the situation should be handled effectively as if the service using the old identity had ceased to operate and the service using the new identity had come into being.

The service which is effectively stopping should have its "Service current status" (see clause 5.4.4) revised to meaning 2 (ceased operations) and the previous status information placed into the "History information" (see clause 5.5) of the TSL. This should then be retained for the published retention period (since there may be requirements to check on services rendered during it period of activity - no ceased service's "Historical information" should be discarded.

The service under the new digital identity should be given its own new entry, which at this initial stage would have no "History information" which required recording.

C.6.4 Amendment response times

Changes to any TSL information should be provided in a timely fashion, which as a minimum should be the following (the response times taking account of the format of the information's presentation):

a) Within two working days of the decision to change status, where the information is made available in hard-copy form.

b) Within four working hours and anyway within the same working day as the decision to change status, where the information is either made available in electronic format, i.e. machine processable or readily down-loadable and printable.

c) Where each TSL revision is disseminated electronically to those parties who are obliged by the scheme operator to maintain copy of the TSL for their own clients, whether in hard-copy or electronic form, response times as defined in (b) should be met. Such parties would typically be TSPs whose services are listed in the TSL, and should themselves undertake to post the revised TSL within the same response criteria.

Status information may optionally be periodically refreshed, in accordance with the information provided in clause 5.2.14.

C.6.5 On-going verification of authenticity

The Low-FIC characteristic of a TSL could give a determined hacker sufficient time to replicate and replace all instances of a TSL, *IF* they were able to replace all examples of the TSL itself and a surrogate PKC for the TSL operator. This should be protected against by the scheme operator itself making frequent verification of its own TSL and all authorized and recognized replications of it. In addition, the regular re-issuing of the TSL, even when there is no change to any statuses within it, will also ensure that, at the least, the signature value changes periodically. This clause has already discussed some security measures which would reduce significantly the likelihood of this being achievable.

C.6.6 Upon a scheme's cessation of operations

Owing to the dependence which users may place upon the TSL, schemes which operate a TSL should have in place appropriate mechanisms for any cessation of their operations, be it temporary or permanent. The normative parts of the present document provide for the provision of a "Latest next update" date and time. Whilst this may allow for a natural expiry of the validity of a TSL's contents, a scheme operator should be able to take more positive actions towards notifying users of their TSL that it is no longer supported.

As a minimum, the scheme should revoke the keys used for signing and verification of its TSL and make a public announcement of its cessation of operations, indicating (if known) whether this is temporary or permanent.

If time permits and circumstances warrant, a new TSL should be issued which relegates all status records to the history components as of a specific date after which the scheme no longer accepted responsibility for status determination and produces an archive for long-term reference. It is recommended that in such a circumstance the field "Service current status" is set to indicate "Expired". Whilst the issues of the long-term validity of this archived TSL may be something for consideration it is beyond the scope of the present document to deal with them in depth. Suffice to say that, where there is a decision or obligation to hold available the final TSL status for an extended period, appropriate measures (already widely known and discussed in this field) should be taken to protect signatures against the decay of the strength of crypto algorithms.

C.6.7 User reference to TSL

When and how often a user/relying party should reference to a TSL for status information is not an issue within the scope of the present document. Such a decision lies with the user and should be a determination made according to a variety of factors reflecting their own circumstances, *inter alia*, the degree of reliance they place in a TSL status indication, how often they deal with the other party, the nature of the business relationship and the value of the business or the transaction in question. These are factors only they can determine after conducting their own risk analysis. They may have such infrequent recourse to a TSL that they will always check for any TSL records of status.

Scheme operator's could assist in this by offering additional services to notify when a new TSL is issued, or to guarantee frequent re-issue of a TSL at a frequency which may mean numerous re-issue without change of any services' status. However, the mechanisms proposed for having multiple copies of TSLs existing contemporaneously are designed to cater for the Low-FIC already discussed, and these may not be suitable for frequent TSL re-issue.

C.6.8 Reliance upon hard-copy TSL information

Whilst it is a requirement that scheme operators make available information which is "human-readable in printable, hard-copy form" there is no requirement, nor expectation, that hard copy should be provided in a manner which can be authenticated by any printable means. Users should expect that authenticated information presented on-screen by an application accessing a TSL will faithfully reproduce that information when it is printed and should take the trouble to cross-check the information with that on-screen where they have any doubts.

Scheme operators might choose to make paper copy available by surface post if that seems desirable.

Annex D (informative): Example queries and responses

D.1 General

This informative annex uses some possible queries to show how the structure of the TSL can be used to resolve them. It uses alternative scheme scenarios to show how certain queries may be answered differently according to the nature of the schemes whose TSLs are located and used. It is assumed that the query process is performed automatically. The examples have been written in as open a way as possible, in the hope of showing how broader queries could be managed.

The examples given demonstrate the ability of the information provided in, and through, a TSL conformant to the present document, to enable a range of queries to be answered by automated processing. The examples are expressed in natural language rather than any Boolean type of presentation as might be the case for genuine implementations.

It is clear that the potential range of questions which might be posed is varied and rich, and these examples can only make suggestions as to how the TSL as defined is able to fulfil the needs of both simple and more complex queries. For example, these examples make no check to ensure that the status does not suggest that the scheme is no longer operating, although this would need to be a practical check in reality. Nevertheless, these examples illustrate clearly the feasibility of using a TSL for automated processing.

D.2 Example 1

D.2.1 Scenario

The sender has attached their Qualified Certificate to a signed communication. Simple authentication of the signature with respect to the certificate has been successful. We assume that a TSL has been located and verified (see annex C) - otherwise the response has to be "*unknown*" since no definitive status has been found (e.g. the EU Member State concerned may choose not to adopt the TSL model).

Assuming that a scheme is found, let us further assume that the scheme is operated by an EU Member State as a "supervision system". The scheme works on a "white list" basis, either through monitoring the marketplace and identifying TSPs which claim to be issuing QCs and have no claims against them upheld, or through requiring positive tests to establish compliance with specified criteria, failure of which will lead to the TSP's status showing their non-compliance. This TSL therefore shows all known TSPs established in the particular EU Member State, and indicates whether they comply to the criteria of the scheme or not.

D.2.2 Query

In natural language, we can express the relying party's query as: "*Is the TSP which issued the Qualified Certificate compliant with the supervision scheme of the country in which the TSP is established?*"

D.2.3 TSL interpretation and query response

1) Verify that the TSL is for an EU Member State Supervision System by determining whether the value of the field "Scheme type/community" (see clause 5.2.8) is a URN which indicates that the scheme was established as an EU Member State Supervision System (in accordance with Directive 1999/93/EC). For the purposes of this scenario we will assume that this is a positive result: if this could not be verified then the response would have to be "*unknown*" - no further action required.

2) Verify that the EU Member State to which this TSL refers is the same as the Country Name in the Qualified Certificate: if it is present, does "Scheme territory" (see clause 5.29) match the Country Name? In this scenario this works: if this could not be verified then the response would have to be "*unknown*" - no further action required.

3) If "Status determination approach" (see clause 5.2.7) is 1 or 2 and "Service current status" (see clause 5.4.4) is 1 then the response must be "*Yes*". (i.e. the scheme applies a positive approach and the status is the specified "conformant" value).

4) In any other case the response must be "*No*".

D.3 Example 2

D.3.1 Scenario

This scenario is the same as that in clause D.2, except that the scheme is operated by an EU Member State as a "supervision system". The scheme works on a "black list" basis, identifying only TSPs which fail to meet the scheme criteria. This TSL therefore shows only TSPs established in the particular EU Member State known not to comply to the criteria of the scheme.

D.3.2 Query

This is the same as in clause D.2: expressed in natural language, the relying party's query as: "*Is the TSP which issued the Qualified Certificate compliant with the supervision scheme of the country in which the TSP is established?*"

D.3.3 TSL interpretation and query response

Steps (1) and (2) are the same as in clause D.2.

3) If "Status determination approach" (see clause 5.2.7) is 3 and the specified service cannot be found in the TSL then the response must be "*Yes*" (i.e. the scheme applies a negative approach and absence of the TSP leads to an assumed compliance).

4) In any other case the response must be "*No*".

D.4 Example 3

D.4.1 Scenario

The sender has attached their Qualified Certificate to a signed communication. Simple authentication of the signature with respect to the certificate has been successful. We assume that at least one TSL has been located and verified (see annex C) - otherwise the response has to be "*No*" since no definitive status has been found (i.e. it has not been possible to locate a TSL which refers to this TSP).

Assuming that a referencing TSL is found, let us further assume that the scheme works on a "white list" basis, requiring positive tests to establish compliance with specified criteria, failure of which will lead to the TSP's status showing their non-compliance (the idea of a voluntary scheme working on the "black list" principal requires some stretch of the imagination). This TSL therefore shows all TSPs which have volunteered to be subjected to the scheme's criteria, and for those which have initially satisfied those criteria, the TSL indicates the TSPs" current status.

D.4.2 Query

In natural language, we can express the relying party's query as: "*Is the TSP which issued the Qualified Certificate recognized by any voluntary approval scheme?*" Note that the query as expressed is concerned only with whether the TSP is "recognized" - not necessarily approved, not necessarily approved for issuing Qualified Certificates.

We could therefore imagine two levels of refinement of this query:
"*Is the TSP which issued the Qualified Certificate currently **approved by** any voluntary approval scheme?*"
"*Is the TSP which issued the Qualified Certificate currently **approved by** any voluntary approval scheme **for issuing QCs**?*"

D.4.3 TSL interpretation and query response

1) For the basic query posed, the mere fact that there is at least one TSL which references the service would make it possible to respond positively, without further action. The user would of course still need to make further discovery to know the manner of recognition, i.e. whether the service was approved or not.

2) To answer the first refinement of the question we have first to check, in each TSL located, for the service corresponding to "Service digital identity" (see clause 5.4.3): In each case, if "Status determination approach" (see clause 5.2.7) is 1 or 2 and "Service current status" (see clause 5.4.4) is 1 then the service is presently approved. (i.e. the scheme applies a positive approval approach and the status is one of the two specified approved values). However this does not yet fully answer either of the refinements of the query.

NOTE: In each of the above cases, and indeed in the examples D.2 and D.3, there has been no check on the type of service, since this is implicit in the fact that the trust service token provided is (or claims to be) a Qualified Certificate. However, an additional explicit check to confirm that "Service type identifier" (see clause 5.4.1) was 2 could add further assurance.

3) The refined queries both ask whether the service is approved by "*any voluntary approval scheme*". The TSL does not include a field with a meaning which indicates this directly. Two possibilities exist: the first is that the field "Scheme type/community" (see clause 5.2.8) is a URN which indicates that the scheme is an approval scheme. The provision of such a URN is beyond the scope of the present document, but any interest group which wished to establish itself for the purposes of supporting voluntary schemes could register such a URN. The alternative possibility is that, using the pointer to scheme information, the user would need to extract this information from the scheme operator's web site. If neither of these options can indicate that it is a voluntary approval scheme which is providing the information, then the query has to conclude with either a negative or an indeterminate response.

4) To answer the second refinement of the question, concerning the specific nature of the service's approval, we have to perform the checks described in (2) and (3) and additionally to check whether "Service type identifier" (see clause 5.4.1) is 2, in which case the response must be "*Yes*". (i.e. the scheme applies a positive approach, the status is one of the two specified approved values, the scheme is a voluntary approval type, and the service is explicitly declared as a CA issuing QCs).

5) In any other cases the response must be "*No*".

Strictly, to answer the question, only one positive search need be determined, although specific applications could provide the location of the TSL holding the status information, and could therefore examine all TSLs if more than one was found, and report on all which held a reference to the specific service.

D.5 Example 4

D.5.1 Scenario

In the preceding three examples the query has implicitly concerned with a contemporaneous check, i.e. "now". However, one of the scoping terms for the TSL is that it be possible to check status at a previous point in time. This scenario could be any of the preceding ones, with an additional requirement that a specific time be quoted.

D.5.2 Query

To take two of the example queries already used, we could modify them as follows (in bold):

*"**Was** the TSP which issued the Qualified Certificate compliant with the supervision scheme of the country in which the TSP is established **on date ccyy-mm-dd hh:mm**?*
"***Was** the TSP which issued the Qualified Certificate approved by any voluntary approval scheme for issuing QCs **on date ccyy-mm-dd hh:mm**?*"

D.5.3 TSL interpretation and query response

The tests so far described in preceding examples would still be necessary according to the construction of the query. However, in order to determine the result on the basis of the specific dates quoted, we now need to check additional fields as follows:

1) If ccyy-mm-dd hh:mm is at or after the "Current status starting date and time" (see clause 5.4.5) then the current status (as determined in preceding examples) is the one required, and the response is generated accordingly.

2) If the "Current status starting date and time" is after the required status time then ccyy-mm-dd hh:mm should be compared with "Historical information period". If ccyy-mm-dd hh:mm is before this time then no status information for the required date is available, and so a response "*unknown*" is appropriate. Otherwise, the "History information" (see clause 5.5) for the specified trust-service must be examined.

3) In the "History information" block for the specific trust-service, the "Previous approval status starting date and time" must be checked: if it is after ccyy-mm-dd hh:mm then the previous entry must be checked. If the end of the list is reached (NB - the list could be empty) then the response must again be "*unknown*".

4) When an historical status is found then, for the relevant historical status set of information, the contents of "Service previous status" (see clause 5.5.4) should be used instead of the current status used in the preceding examples, when determining the final response.

Annex E (informative): Rationales for TSL fields

This informative annex records the rationale for the inclusion of each field within the TSL as supportive information for those wishing to implement or understand better the TSL.

The TSL has been constructed so as to be as "lean" as possible and to contain the minimum information necessary consistent with the requirements for developing the present document and the need to machine-process a TSL to establish the status of a specific TSP service within that TSL. The inclusion of each field has therefore been carefully considered and the case for each is set out below in the order of the clause where the field is defined.

Clause	Field name	Rationale
5.2.1	TSL version identifier	The field provides for identification of the TSL structure and format in case of possible future TSL format enhancements. Knowledge of the version will enable selective parsing or manual interpretation of the TSL.
5.2.2	TSL sequence number	The field provides for tracking the subsequent releases of the TSL.
5.2.3	Signature algorithm identifier	By placing a copy of the signature algorithm identifier in the beginning of the TSL, the computation on the list for verification against the signature value specified in clause 5.6.4 could start from the moment of beginning to receive the TSL string.
5.2.4	Scheme name	For general communications and specifically in the event of any dispute, especially one which involves any extent of litigation, correctly titling/naming the responsible legal entity will be a necessity in most jurisdictions. There are no explicit requirements for the scheme name - it need be simply a decision of the scheme operator's and it is expected that they will take due care in ensuring that it is not in breach of any copyright or trademark issues. Provision of multiple language representations makes the information accessible to local communities as well as to the international community.
5.2.5.1	Scheme operator postal address	For general communications and specifically in the event of any dispute, especially one which involves any extent of litigation, correctly addressing communications with the responsible legal entity will be a necessity in most jurisdictions. For the foreseeable future, many organizations, administrations and indeed the public, even those involved in electronic commerce, will be reluctant to rely exclusively upon electronic communications or may even be prohibited from doing so by law. under certain circumstances. Local language and cross-border (international) trading considerations may require that this information be provided both in a national language (and script) and in a commonly accepted internationally-used language.
5.2.5.2	Scheme operator electronic address	For general communications and specifically in the event of any dispute, especially one which involves any extent of litigation, correctly addressing communications with the responsible legal entity will be a necessity in most jurisdictions. This field provides for that communication to be effected electronically rather than through physical means. The use of a URI instead of a URN recognizes the potential volatility of commercial websites, and does not introduce any implication of "institutional commitment to persistence, availability" which the use of a URN would require by definition.
5.2.6	Scheme information URN	There may be information regarding the scheme which is sought by users and which is not available through the TSL (nor should it be, since it duplicates and makes difficult the maintenance of such information). By providing a URN either manual or automated access to further information is enabled. The information regarding the scheme could include information concerning the legal status of the scheme or legal requirements met by the scheme for the jurisdiction in which the scheme is established.
5.2.7	Status determination approach	This information will enable adoption of the TSL format by schemes of differing types of operation whilst there remain schemes which are unable to fully comply with the harmonized TSL structure and implied processes.

Clause	Field name	Rationale
5.2.8	Scheme type/community	Significance may be placed upon the fact that a scheme complies with a specific set of criteria, code or legislative requirement, having a significant effect upon the trustworthiness of the trust service in question. This could, e.g. indicate that the scheme was established as an EU Member State Supervision System (in accordance with Directive 1999/93/EC) by adoption of a URN registered by, e.g. ETSI. Although it would be expected to find this information within the details of a specific scheme's web-site (located through the field "Scheme information URN") by providing for it within the TSL structure the location and format of its presentation can be standardized and hence the determination of this information (when provided) readily performed, including by automated means. The field is optional since for some schemes this information may be of no significance.
5.2.9	Scheme territory	Some users, especially relying parties, may place significance on where a scheme is based. Although it would be expected to find this information within the details of a specific scheme's web-site (located through the field "Scheme information URN"), by providing for it within the TSL structure the location and format of its presentation can be standardized and hence the determination of this information (when provided) readily performed, including by automated means. The field is optional since for some schemes this information may be of no significance.
5.2.10	TSL Policy / Legal Notice	Although this kind of information could be expected to be found within the scheme information pointed to by clause 5.2.6, it is advisable that, by making plain the policy and/or legislation under which their TSL is maintained and operated, scheme operators do not encourage users of their TSL to hold any unreasonable expectations or reliance upon the information within the TSL. By providing this information within the TSL itself a scheme operator can make this clear to those using its TSL.
5.2.11	Historical information period	This information could be compared with the date and time of e.g. a certificate or time stamp being verified for trustworthiness (the trust service token). If the date and time of the trust service token fall outside the range given by the number of days and the TSL issue date and time (see clause 5.2.13), then further investigation of the information in the TSL would not provide an answer. Note that the value 1 through 65534 allows for stating a specific duration of up to at least 179 years.
5.2.12	Pointers to other TSLs	Provision of this information could facilitate the location of a TSL when a search is required and provide, on an implementation-specific basis, additional trustworthy information, such as authentication information or other trust-related support data.
5.2.13	List issue date and time	This field will assist users in determining the relevance of this TSL's information to their needs.
5.2.14	Next update	This field limits the validity of the current TSL to the latest date and time that the next TSL is intended to be issued. Any conformant application parsing an expired TSL shall get the latest issue of the TSL. For the TSL to provide useful and up-to-date information, it must be re-issued whenever a change in status of a TSP or service occurs and, furthermore, within the declared time-constraints for publication of changes, once determined as being required. In the event of no interim status changes to any TSP or service covered by the scheme, the TSL must be re-issued by the time of expiration of the last TSL issued.
5.2.15	List of Trust Service Providers	The present document could have ordered information according to service type. However, information about the service status alone will in some circumstances be insufficient for the establishment of trust. Inclusion of all services relating to a specific service provider is a more favourable structuring.
5.3.1	TSP name	For general communications and specifically in the event of any dispute, especially one which involves any extent of litigation, correctly titling/naming the responsible legal entity will be a necessity in most jurisdictions. Provision of multiple language representations makes the information accessible to local communities as well as to the international community.
5.3.2	TSP trade name	Where a service is offered under a product or brand name, for general communications and specifically in the event of any dispute, especially one which involves any extent of litigation, correctly identifying the trade or brand name of the TSP will be advisable in most jurisdictions. Provision of multiple language representation makes the information accessible to local communities as well as to the international community.

Clause	Field name	Rationale
5.3.3.1	TSP postal address	For general communications and specifically in the event of any dispute, especially one which involves any extent of litigation, correctly addressing communications with the responsible legal entity will be a necessity in most jurisdictions. For the foreseeable future, many organizations, administrations and indeed the public, even those involved in electronic commerce, may be reluctant to rely exclusively upon electronic communications or may even be prohibited from doing so by law under certain circumstances.
5.3.3.2	TSP electronic address	For general communications and specifically in the event of any dispute, especially one which involves any extent of litigation, correctly addressing communications with the responsible legal entity will be a necessity in most jurisdictions. This field provides for that communication to be effected electronically rather than through physical means. The use of a URI instead of a URN recognizes the potential volatility of commercial websites, and does not introduce any implication of "institutional commitment to persistence, availability" which the use of a URN would, by definition, require.
5.3.4	TSP information URN	There may be information regarding the TSP which is sought by users and which is not available through the TSL (nor should it be, since it duplicates and makes difficult the maintenance of such information). By providing a URN either manual or automated access to further information is enabled. The information regarding the TSP could include information concerning the legal requirements met by the TSP for the jurisdiction in which the TSP is established.
5.4.1	Service type identifier	Through the service type identifier, the specific type of TSP service can be determined. Provision is made for the introduction and approval of services which do not fit into the specified list, pending possible revision to the standard.
5.4.2	Service name	For general communications and specifically in the event of any dispute, especially one which involves any extent of litigation, correctly titling/naming the service will be a necessity in most jurisdictions. Provision of multiple language representation makes the information accessible to local communities as well as to the international community.
5.4.3	Service digital identity	The service digital identity could be used by relying parties to authenticate a service and thereby the TSP offering the service as being the one referred to in this TSL.
5.4.4	Service current status	This is the fundamental aspect of the TSL - i.e. the service's status. That status, whilst having four distinct values as specified, needs to be interpreted with regard to the scheme's status determination approach (see clause 5.2.7) which indicates the general types of criteria being applied. This will allow a richer understanding of the actual status. Guidance on this is given in annex D. The history and current status together provide full information from the date on which the TSP service was recognized for the first time by the scheme (according to the scheme's "status determination approach"). The current status can be determined from the field specified in clause 5.4.4. The date on which the current status became effective is given in the field specified in clause 5.4.5. Any previous status with its starting date would be found in the history. Even if the scheme had a fixed approval period followed by re-approval, this would show in the history (current status is "approved"; previous status is also "approved"). The same status identifier values are used in the service approval history (see clause 5.5.4).
5.4.5	Current status starting date and time	The user (subscribers, relying parties) could apply this information by comparing it with other available information, e.g. the date and time on which a certificate or a time stamp was issued. From the comparison, the user could determine whether the specific service of the TSP had the desired approval status under the scheme at the date and time of provision of the service.
5.4.6	Scheme service definition URN	There may be information regarding the service which is sought by users to determine the nature of the approval. By providing a URN either manual or automated access to further information is enabled. The information regarding the service could include information concerning the legal requirements to be met by TSPs concerning the service for the jurisdiction in which the scheme is established.

Clause	Field name	Rationale
5.4.7	TSP service definition URN	There may be information regarding the service which is sought by the user to determine the nature of the TSP's offering. By providing a URN either manual or automated access to further information is enabled. The information regarding the service could include information concerning the legal requirements met by the TSP concerning the service for the jurisdiction in which the TSP is established.
5.5.1	Service type identifier	Through the service identifier, the specific type of TSP service can be determined.
5.5.2	Service name	For general communications and specifically in the event of any dispute, especially one which involves any extent of litigation, correctly titling/naming the service will be a necessity in most jurisdictions. Provision of multiple language representations makes the information accessible to local communities as well as to the international community.
5.5.3	Service digital identity	The service digital identity could be used by relying parties to authenticate a service and thereby the TSP offering the service as being the one referred to in this TSL.
5.5.4	Service previous status	The same status values are used in the service information (see clause 5.4.4). The history and current status together provide information from the date on which the TSP service was recognized for the first time by the scheme. The current status can be determined from the field specified in clause 5.4.4; the date on which the current status became effective is given in field specified in clause 5.4.5. Any previous status with its starting date could be found in the history. Even if the scheme had a fixed approval period followed by re-approval, this would show in the history (current status is "approved"; previous status is also "approved").
5.5.5	Previous status starting date and time	The user (subscriber, relying party) could apply this information by comparing it with other available information, e.g. the date and time on which a certificate or a time stamp was issued. From the comparison, the user could determine whether the specific service of the TSP had the desired approval status under the scheme at the date and time of issue of the certificate or time stamp.
5.6.2	Scheme operator identification	This field identifies the scheme operator responsible for the TSL. Since the verifier of a TSL is assumed to already be in possession of all public keys that can be used for verification, he only needs some information to distinguish which key to use. Most likely he will have it in the form of a self-signed certificate.
5.6.3	Signature algorithm identifier	In order to know how to authenticate the TSL, the user must know the identity of the signature algorithm used when the list was signed. The signature algorithm must be specified and protected by the signature. The field is duplicated at the beginning of the TSL to allow for increasing the speed of signature verification (see clause 5.2.3).
5.6.4	Signature value	Since the signature protects the signed information from undetected manipulation, all fields of the TSL except the signature value itself must be included in the calculation of the signature.
5.7.2	TSL tag	When attempting to establish the status of a trust service it may be necessary to search the Internet to locate any TSLs which have information relating to that specific service. The TSL tag will enable search-engines and/or parsing applications to quickly determine that a resource which has been located is a TSL conformant with the present document.

Annex F (normative): XML schema

The XML schema is contained in the file TS102231 v1-1-1.xsd which is in archive ts_102231v010101p0.zip which accompanies the present document.

Annex G (informative): Bibliography

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

ETSI TR 102 030 (2002-03): "Provision of harmonized Trust Service Provider status information".

ETSI TS 101 456: "Policy requirements for certification authorities issuing qualified certificates".

ETSI TS 101 733: "Electronic signature formats".

ETSI TS 101 862: "Qualified certificate profile".

ITU-T Recommendation X.501: "Information Technology - Open Systems Interconnection - The Directory: Models".

XML-Signature Syntax and Processing, W3C Recommendation, February 2002.

XML Schema Part 1: Structures, W3C Recommendation, May 2001.

XML Schema Part 2: Datatypes, W3C Recommendation, May 2001.

History

Document history		
V1.1.1	October 2003	Publication