ETSI TR 102 030 V1.1.1 (2002-03)

Technical Report

Provision of harmonized
Trust Service Provider status information

Reference

DTR/SEC-004010

Keywords

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.fr

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 Report (TR) has been produced by ETSI Technical Committee Security (SEC).

Introduction

It would enhance the confidence of relying parties if they had access to information that would allow them to know whether a given Trust Service Provider (TSP) was operating under the approval of any recognized scheme (supervision system, voluntary "accreditation" (approval) scheme, or otherwise) at the time of providing their services and of any dependent transaction that takes place. This information should preferably be accessible using an on-line protocol, although accessibility both off-line and on-line should be possible.

The information should be available for a wide range of services and schemes, including the use of Qualified Certificates. The importance of this inform

ation is especially significant for cross-domain and international transactions.

In this regard, some schemes have already included procedures and facilities for the provision of status information about TSPs. However, the frameworks are not harmonized, neither are the protocols and formats used for retrieving such information by the relying party.

In order to avoid the proliferation of numerous and different protocols and formats, the present document has been prepared to present the features of existing approaches and the rationale for harmonized requirements plus recommendations for further implementation and actions.

1 Scope

The present document defines minimum requirements for the provision of harmonized status information on certification-service-providers and other Trust Service Providers (TSPs) and for the means to provide such information. The requirements can be used as the starting point for the development of technical norms and agreed procedures.

1.1 Intended audience

The present document is intended to be of interest to at least the following audiences:

Those having responsibility for the specification, management or operation of schemes which oversee the trust services provided by TSPs and those who may have a role in the drafting and passing of legislation governing the provision of such services. Many of these parties will have contributed to the requirements extraction phase of this task.

Secondly, the task will be of interest to parties who may seek status information prior to deciding whether to rely upon a trust service offered by one of the overseen TSPs and perhaps also to those who are contemplating subscribing to one of these trust services.

Lastly, the present document will be the primary input to those undertaking any normative actions to establish standards addressing the processes, procedures, formats etc. necessary to support implementation of these harmonized requirements.

1.2 Status of the requirements herein

The present document is an ETSI Technical Report. It conveys informative material which has been prepared by a team of experts who have drawn input from a wide range of sources concerned with specification, management, operation or legislation in connection with schemes which provide status information about trust services.

The report delivers a set of harmonized requirements which takes fully into account these inputs. It accommodates all of the reviewed types of status information in a harmonized structure which satisfies the broadest range of status information. It is the intention that the resultant Trust Status List defined in clause 7 can accommodate any of the differing current means of managing schemes and set a target for more harmonized representation for the future.

It is recognized that the harmonized requirements herein exceed the current extent of status information provision, but because of the very disparity of existing schemes, there is no current basis for harmonization. Furthermore, the objectives of the present document (see clause 4.1) cannot presently be satisfied fully by any of the schemes surveyed - these harmonized requirements offer a means to achieve that.

1.3 Notice to readership

It is important that the readership of the present document is fully aware of the fact that it is ***not*** the intention of the present document to impose upon any form of, or specific, approval scheme the freedom to operate in a manner of its own choosing. Adoption of these harmonized requirements is entirely voluntary and nothing in the present document is intended to require otherwise. The requirements herein are constructed so as to accommodate the various existing mechanisms and to provide an attainment target which will result in the delivery of enhanced quality of status information to users, both relying parties and subscribers.

2 References

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

[1] PKI Forum Technology Working Group White Paper on CA-CA interoperability (March 2001).

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

[3] ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8: "Information Technology - Open Systems Interconnection - The Directory: authentication framework".

[4] ETSI TS 101 456 (V1.1.1): "Policy requirements for certification authorities issuing qualified certificates".

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

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

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)

cross-domain transaction: transaction where the relying party has no relationship with the provider of services used by their counter-party and (i.e. they do not share a common TSP) therefore potentially has no knowledge of the service providers' status and hence no explicit basis on which to establish confidence their service and in the transaction

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

scheme: generic term applied to 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 are governmental, industry or private, etc.

Trust Service Provider (TSP): provider of any **electronic trust service**

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 (CSP) used in the Directive 1999/93/EC [2].

In addition to the terms above-defined, the present document takes great care to effect correct use of the terms Accreditation, Certification and Approval. The presentd document uses the term "**Accreditation**" in its strict sense and not to imply "**Approval**", as is often the case elsewhere. Where reference is made to other sources which have used "Accreditation" where "Approval" is actually the function intended, the present document will use the original term followed by a qualifying "(Approval)".

3.2 Abbreviations

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

CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
CWA	CEN Workshop Agreement
EC	European Commission
EEA	European Economic Area
EESSI	European Electronic Signature Standardization Initiative
EFTA	European Free Trade Association
ESI	ETSI Electronic Signature and Infrastructure Working Group
EU	European Union
HTML	Hyper-Text Mark-up Language
HTTP	Hyper-Text Transfer Protocol
LDAP	Lightweight Directory Access Protocol
OID	Object IDentifier
PKI	Public Key Infrastructure
STF	Specialist Task Force
TSP	Trust Service Provider
URL	Uniform Resource Location
XML	Extendable Mark-up Language

4 Objectives and methods of investigation

This clause describes the objectives for the task set by the STF178-5 team and the methods used for performing the investigation. It refers to the briefing document and questionnaire prepared for interviewing the interested parties (those responsible for supervision systems and voluntary approval schemes, as well as relying party representatives).

4.1 Task objectives

In January 2001, the ETSI Electronic Signature and Infrastructure Working Group established a work program supported by a Specialist Task Force (STF 178) as part of the European Electronic Signature Standardization Initiative (EESSI), Phase 3.

STF 178 Task 5 was charged with establishing requirements for the provision of harmonized status information on Trust Service Providers. The subject of consideration was how users could determine whether the provider of a trust service is or was operating under the approval of any recognized scheme at either:

a) the time the service was provided, or

b) the time at which a transaction reliant on that service took place.

The objectives of the task were to establish minimum common requirements for the provision of this status information and for the means to provide it. Such requirements could be used as the starting point for the development of technical norms and agreed procedures. The present document describes how the task was performed, what input was obtained and which requirements were established.

4.2 Task rationale

4.2.1 The need for status information

Among the most easily identified situations in which status information is needed, one such case is when a relying party who is in possession of the other party's Public Key Certificate wishes to rely upon that Certificate for the purpose of conducting some form of transaction. Another one is when, subsequent to a transaction being concluded, a relying party needs to know whether at the time the transaction was enacted, the service provided by the TSP was to be trusted. In such cases, in addition to verifying the Certificate, the relying party wants to establish the status of the TSP that issued the Certificate, at any one or all of: the time that the TSP issued the certificate; the time that the relying party wishes to enter into a transaction, or; the time the relying party verifies the transaction validity.

Other examples do not necessarily involve reference to a certificate, e.g. when a Time Stamping service is provided. For this reason, in the present document the broad generic term Trust Service Provider (TSP) is used rather than certification-service-provider (CSP), used by the EC Directive on electronic signatures [2].

Organizations best placed for providing status information are those responsible for the governance (management) and operation of schemes for approving TSPs. Such a scheme could be one operated as a voluntary scheme by industry and consumers, one established under national regulation to oversee the provision of trust services (such as a scheme operated by a state not a member of the EEA) or, more specifically, one established as a supervision system by a State which is subject to Directive 1999/93/EC [2].

It would be useful for relying parties to have access to status information, preferably on-line, especially when conducting cross-domain and international transactions. In open electronic transaction (e.g. e-commerce) environments the relying party may well have no established trust relationship with the provider of services used by their counter-party and therefore potentially has no knowledge of the service provider's status, and hence no explicit basis on which to establish confidence in the transaction.

The provision of status information could include reference to the criteria that the TSP has had to satisfy in order to be recognized under the relevant scheme. Examples of such criteria are, *inter alia*, financial liability, maintenance of Certificate Revocation Lists (CRLs), date last audit passed. It is worth noting that the usual check of the validity of a user's public key certificate does not provide this kind of information. Furthermore, the validation of Certificate Authority (CA) certificate chains is only feasible in hierarchical CA-schemes, where the trust in the top CA still remains an open issue, in accordance with the above examples.

4.2.2 The need for harmonization

Some schemes have already established procedures and facilities for the provision of status information about TSPs. However, these schemes are not being harmonized and neither are the protocols and formats used for retrieving such information by the relying party. In order for a user's system to do business with actors under different schemes, it will have to support the specific protocols, formats, etc. of each of the targeted schemes, about some of which they may have no prior knowledge. Neither are they fully automated, nor even possible to automate fully in their present form.

Input has been sought from those responsible for running any of the possible types of approval schemes or regimes, in order to try to avoid the proliferation of numerous and different protocols and formats.

In particular, the focus has been on input from those responsible for implementing national schemes fulfilling the provisions of Directive 1999/93/EC [2]. By taking into account this input, the developed requirements will provide a harmonized basis for the necessary status information being made available from each scheme to relying parties. Some implementers of these schemes have already expressed their wish to have access to such requirements to assist in the full implementation of national schemes. This will in turn support the widespread adoption of e-commerce under the umbrella of Directive 1999/93/EC's [2] provisions.

By addressing a broad range of trust services the developed requirements can facilitate the provision of harmonized approaches to accessing status information across a wide range of approval schemes.

4.3 Requirements determination process

The STF 178-5 team has, in the first instance, taken input from those individuals responsible for the operation or implementation of approval schemes. The team wished to see how such schemes are working and what kind of information they might either wish to provide or would expect to be provided to relying parties. Of special significance in this, because of the importance given to Directive 1999/93/EC [2], was the need to ensure that each EU body responsible for establishing their national supervision system was invited to have the chance to express their views. The geographic scope of the task was therefore primarily the fifteen states of the European Union.

The team also sought input from other schemes operating within geographic Europe, e.g. national schemes from other states and any voluntary schemes that have become established, such as *tScheme* in the UK and TTP.NL in the Netherlands, or international schemes such as Identrus, GTA, WebTrust, etc. Additionally, the team took input from other interested parties, e.g. Australia and the Asia Pacific Economic Co-operation, Telecommunications and Information Working Group (APEC TEL), Canada and the USA, where EESSI has already established liaison. Input from other territories and groups has been pursued actively.

Milestones of the task, being the release of progressive drafts of the developing Technical Report, have been co-ordinated with ETSI ESI WG meetings, which took place:

2001:

- 13-14 March in Stockholm, Sweden.
- 15-16 May in Hamburg, Germany.
- 26-27 June in Sophia Antipolis, France.
- 2-3 October in Milano, Italy.
- 27-28 November in Wien, Austria. (Draft D4 for ESI review.)

2002:

- 23-24 January in Barcelona, Spain. (Final draft report submitted for ETSI ESI approval.)

Two documents were developed for collecting input:

- Task briefing - To establish requirements for the provision of harmonized status information on CSPs and other Trust Service Providers (ETSI ESI STF178-5 Ref. Z02 vn. 2.00 dated 2001-04-19);
- Requirements capture questionnaire (ETSI ESI STF178-5 Ref. Z03 vn. 2.02 dated 2001-05-05). See annex A.

The Task Briefing, a general information document on the objectives of the project, was distributed to those individuals who were identified as connected to a particular scheme in a particular country. In case they were not directly responsible, these persons were requested to indicate the person responsible for or involved in the implementation of the scheme. This resulted in a list of contact persons who were subsequently approached for a face-to-face interview. In some cases the questionnaire was provided beforehand to the person interviewed.

The questionnaire was the principal means by which the STF 178-5 team gained its external inputs. The process is referred to as "Requirements Capture". The objective was to capture the actual intentions, practices or the expectations of the respondents. These findings were then used as key input material when establishing minimum common requirements for the provision of TSP status information and for the means to provide it.

The questionnaire consisted of three parts as follows:

Part A was intended for those who participate in the management or operation of a scheme. It addresses the identification of the scheme, its general characteristics and development status. It then addresses the items that make up the essential targets of investigation. These are the critical components to maintain TSP status information and to make it available and useful to users in an open environment. Some of the important items and components to be defined and agreed are:

- The contents of information to be provided and its format;
- Policies and rules how to distribute, store and manage the information;
- Definition of the user community;
- Framework and mechanisms to maintain user confidence;
- Technical means (e.g. pointers, protocols, etc) to find, access and validate the information.

Part B was intended for relying parties who will want to gain access to status information, e.g. consumers, government agencies, tax authorities, banks, chambers of commerce, etc. It seeks their views on how that information should be made available and what it should cover.

Part C of the Questionnaire dealt with follow-up and contact details.

The Questionnaire is shown in annex A of the present document.

The results of the requirements determination process are discussed in clause 5 of the present document. Clause 6 provides an overview of alternative solutions and the reasons for selection of one of the alternatives. Clause 7 defines the requirements for TSP Status Lists, while clause 8 discusses implementation options. Clause 9 provides recommendations for further actions.

5 Results of investigation

This clause describes the results of the requirements capture process undertaken to establish the harmonized requirements expressed in clause 6 of the present document. It provides background about the extent of input received by the authors, which provides helpful context for the harmonized requirements.

It should be noted that the large majority of investigations were conducted in the period 2001-05 to 2001-07, and it is these results on which the bulk of the present document's analysis has been based. Since that time there has been progress on the development of plans and implementations of the various schemes visited. Subsequently, during review of the report, some revised inputs have been offered by those persons responsible for the schemes, and this had lead to revisions in the analysis. Where possible we have indicated that the information given has been subject to revision.

5.1 Introduction

Input was received from two distinct perspectives: firstly, and primarily, from that of being involved in the operation and management of a "scheme"; secondly from being one who might be a relying party wishing to use such a scheme.

Clause 5.2 provides an overview of the countries from which input on schemes has been received. Clause 5.3 summarizes the responses received from supervision systems in EU and EFTA Member States to the questions dealing with operation and management aspects (Part A of the questionnaire - see annex A). This is by far the largest proportion of responses (19 out of a total 26).

Clause 5.4 describes the responses received from voluntary schemes, likewise to the questions concerning operation and management aspects (Part A of the questionnaire). This covers a smaller part of the responses (6 out of a total of 26).

Clause 5.5 deals with technical aspects emerging from the responses of supervision systems and voluntary schemes.

Clause 5.6 describes the responses to Part B of the questionnaire, dealing with the viewpoint of relying parties who would seek and apply the requirements information (1 response received).

Annex B provides a list of the contacts that provided input to the preparation of the present document.

5.2 Overview of countries and schemes types

The table in this clause indicates for each country that contributed to the input the kind of scheme(s) that are in operation or for which there are concrete implementation or development plans. The scheme types are classified here as "Regulatory scheme" (e.g. supervision system in EU/EFTA countries in accordance with Directive 1999/93/EC [2] article 3.3) and "Voluntary scheme" (e.g. according to article 3.2 of Directive 1999/93/EC [2]).

A Regulatory scheme is set-up by a national government in order to maintain the observance of legal requirements and regulations. Directive 1999/93/EC [2] requires that each Member State ensures the establishment of an appropriate system that allows for the supervision of certification-service-providers that are established on its territory and issue qualified certificates to the public. EU Member State supervision systems as well as comparable supervision systems in other countries are designated in the present document as "Regulatory schemes". Such a scheme is usually operated by a governmental body; however a government could also subcontract the scheme operation to one or more market parties.

Voluntary schemes, as the name implies, are set-up and operated by market parties. Note that a government can operate as market party and establish or participate in establishing and operating a voluntary scheme. A voluntary scheme can assist in controlling legal and regulatory requirements, but need not necessarily do so. Voluntary schemes have been subdivided into "Public body" and "Private body" schemes. Schemes operated by national accreditation bodies have been listed here as "Private body" since industry participates in national accreditation bodies although governmental influence could be substantial. Note that the classification for the EU and EFTA countries relates to issuing qualified certificates to the public. The scheme types are discussed in the next clauses.

Area	**Country name**	**Country code (ISO 3166-1)**	**Regulatory scheme**	**Voluntary scheme**	
				Public body	**Private body**
EU	Austria	AT	✔	✔	
	Belgium	BE	✔	✔	
	Germany	DE	✔	✔	
	Denmark	DK	✔		
	Spain	ES	✔	✔	
	Finland	FI	✔		
	France	FR	✔		
	United Kingdom	GB	✔		*tScheme*
	Greece	GR	✔	✔	
	Ireland	IE	✔		NAB
	Italy	IT	✔		
	Netherlands	NL	✔		TTP.NL
	Portugal	PT	✔		
	Sweden	SE	✔		
EFTA	Switzerland	CH	✔		
	Norway	NO	✔		NA
Other Europe	Hungary	HU	✔		
Other regions	Australia	AU	✔		
	Australia/New Zealand	AU/NZ			CFA
	Canada	CA			
	United States	US			WebTrust for CAs Identrus

5.3 Summary of regulatory scheme types

Although the overall objectives for the present document were to encompass a wider set of schemes than simply those that might fall under the scope of Directive 1999/93/EC [2], the reality is that of the 16 identified regulatory schemes, 15 are established in Europe. Note that these schemes may exist only on paper or may be fully operational.

5.3.1 Supervision systems

Of the 16 responding supervision systems in Europe, 10 have been created directly as a result of the mandatory implementation of Directive 1999/93/EC [2]. In 3 other EU countries, electronic signature legislations and the systems for implementing and maintaining electronic signature regulations existed prior to the publication of Directive 1999/93/EC [2].

Two EFTA countries and one non-EU/EFTA country have set up (or are in the process of setting-up) similar supervision systems. The systems are those meant in article 3, clause 3 of Directive 1999/93/EC [2] and allow for supervision of TSPs.

Countries having schemes considered within this category are shown in the table in clause 5.2 for the areas EU, EFTA, and "other Europe".

From outside Europe, input has been received from the regulatory scheme in Australia. This scheme is meant for the use of public key technology by all levels of Australian federal, state and territorial government.

5.3.2 Scope and process of supervision

The scope of supervision by the various systems differs widely. In some countries all TSPs, irrespective of the kind of services offered, fall under the supervision system (AT, DE and ES); in other countries the scope is limited to those TSPs that issue qualified certificates to the public (BE, CH, DK, FI, FR, GB, HU, IE, IT, NL, NO, and PT). The following main characteristics of supervision have been found:

- **Reactive:** TSPs are not required to notify the supervision system of their activities. Action (investigation) by the supervision system will arise only in the case of the supervision system receiving information that a TSP might be non-compliant. (GB).

- **Notification with publication:** TSPs must notify the supervision system and will be registered. There is neither verification of the TSP's documentation nor assessment of the operations. Action (investigation) by the supervision system is only taken in case of receiving information that a TSP might be non-compliant. Proven non-compliance results in publication of the fact by the supervision system. (FR).

- **Notification with prohibition:** TSPs must notify the supervision system and will be registered. There is neither verification of the TSP's documentation nor assessment of the operations. Action (investigation) by the supervision system is only taken in case of receiving any information that a TSP might be non-compliant. Proven non-compliance can lead to de-registration and prohibition of continuing the TSP services. (ES, NO).

- **Notification and verification of documentation:** TSPs must notify the supervision system and provide documented evidence of complying with the regulations. Registration will follow once the documented system is considered compliant. Note that the depth of verification differs from cursory evaluation under some schemes to extensive verification of TSP procedures and records under other schemes. Once registered, TSPs must provide information on changes in the CPS, organization, management, etc. Complaints will be investigated; proven non-compliance and failure to correct will lead to de-registration and formal prohibition of operations. (AT, BE, DE, FI, IE, NL).

- **Assessment and approval:** TSPs must be assessed and approved prior to starting operations. (CH, HU, IT).
  In some countries assessment is done by the state agency responsible for the supervision system; in others by accredited certification bodies. The assessment varies from extensive evaluation of documentation and records (IT) to a full assessment procedure including evaluation of documentation and implementation audit (CH, HU).

5.3.3 Provision of status information

Three countries have implemented systems for providing status information regarding TSPs that fall under the supervision system. The supervision system in Austria issues public key certificates to registered TSPs. The supervision system in Italy provides a signed list containing information on all registered TSPs. The supervision system in France lists the CAs that are found to be non-compliant with the rules for issuing Qualified Certificates. Many supervisory systems have expressed their expectation or intention to make status information available using normal web-based browsers and tools. Other supervision systems have not yet decided on the method of providing status information other than publication of TSP approval or suspension/cancellation/withdrawal of approval in the relevant national administration notifications.

In Germany, the supervision system does not issue public key certificates to supervised TSPs, only to those within the voluntary scheme (see clause 5.4.3).

5.4 Summary of voluntary schemes

Article 3.2 of Directive 1999/93/EC [2] allows Member States to introduce or maintain "voluntary accreditation (approval) schemes" aiming at enhanced levels of TSP service provision. "Voluntary accreditation (approval)" is defined in the Directive as "any permission, setting out rights and obligations to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise rights stemming from the permission until it has received the decision by the body." In practice this means that a TSP can apply for a certificate of recognition issued under the rules of a voluntary scheme, will undergo an assessment, is granted the certificate of recognition if found compliant, may than announce publicly that it is approved, and will subsequently be subject to periodic surveillance.

The responses received from the European countries show that so far 5 voluntary schemes have been set up. Interviews with respondents in different European countries indicate that plans are being worked out to develop and implement voluntary schemes in at least 6 other countries.

Outside Europe, private body schemes have been set-up or are being set-up/considered in Australia-New Zealand, Canada and the USA. No studies have yet been performed comparing similarities/differences of these schemes and their requirements with the schemes and standards developed in Europe.

5.4.1 Public and private body schemes

The definition of "voluntary accreditation (approval)" in the Directive refers to "public or private" bodies that could be charged with conformity assessment of TSPs in a voluntary scheme. The responses received indicate that 2 countries (AT, DE) have, on the basis of regulations adopted before Directive 1999/93/EC [2] came into force, implemented voluntary schemes operated by the public body that is responsible for the regulatory scheme. Private body schemes exist, in different stages of development and implementation, in 5 countries (GB, IE, NL, NO, US). Four private body schemes emerged from industry initiatives (GB, NL and two originating from the US); the two other schemes identified have been developed by the national accreditation body (IE, NO).

5.4.2 Scope of voluntary schemes

Voluntary schemes may be operated by either national administrations or by private/industry bodies.

In the first case, the same national bodies that are responsible for the regulatory schemes may operate the public body voluntary schemes identified in the table in clause 5.2 above. However, the actual assessment activities can be subcontracted to private bodies recognized by the regulator. The standards used for the assessment of TSPs may be defined in regulations derived from legal requirements. There is much emphasis on the use of "trustworthy systems" by the TSP. The scope differs: in one country all TSPs can apply for voluntary approval, in another this is only possible for TSPs issuing qualified certificates.

Alternatively, some European private body voluntary schemes (initially at least) are only aiming at TSPs issuing qualified certificates to the public; others embrace all services from the beginning. Likewise some are limited to the territory where they are established, while others could accept TSPs from outside their territory.

The European private body voluntary schemes from which input has been received all indicate that certification bodies recognized by the scheme perform conformity assessment of TSPs. In 3 countries the recognition is based upon accreditation of the certification bodies by the national accreditation body. All schemes require ISO/IEC 17799/BS 7799 [3] based assessment competence as the basis for recognition of the certification bodies. Some schemes explicitly define [4] as the standard against which TSPs issuing qualified certificates must be assessed. In other schemes the notion "conformity to the requirements of Directive 1999/93/EC [2]" is used.

Only one of the European voluntary schemes is yet operational (DE). Under some schemes trial assessments of TSPs have been conducted. The other schemes all expected to be operational before the end of 2001.

The private sector scheme in Australia/New Zealand operates under the joint accreditation body JAS-ANZ. The scheme is accessible for open and closed (i.e. public and non-public) CAs and will use recognized international standards and established accreditation/certification processes.

The "WebTrust for CAs" scheme is developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). The criteria used in the scheme (AICPA/CICA WebTrust Program for Certification Authorities, August 25, 2000, Version 1.0) have been developed from PKI documents and standards such as BS 7799 and were subjected to a process of public comment. Approved practitioners of chartered accountancy institutions perform assessment of CAs. The scheme has been in operation since August 2000. Up to July 2001, two CAs in the USA and one in Canada have been awarded the "WebTrust Seal".

Also registered in the US, but in fact initiated by an international group of nine banks (of which six were European), is Identrus, which operates exclusively within the banking sector. It aims to be global in its coverage and all approvals are based upon criteria set out in its Minimum Operating Requirements. However, it acts as a closed service rather than a truly public one and therefore detail information as to what criteria it employs and what status information is provided was not made available. Identrus has been operational since April 2000, and had eight participating organizations in July 2001.

5.4.3 Provision of status information

The input received indicates that the public body voluntary schemes have decided on provision of status information: the schemes in Austria and Germany issue public key certificates to accredited TSPs.

Within European private voluntary schemes, the ideas of *tScheme* in the UK can be called well established indeed, with a comprehensive set of information proposed for publication, but no implementation has been achieved yet. Other private body voluntary schemes in Europe are working on ideas for the provision of status information.

The voluntary sector scheme in Australia-New Zealand also is in the phase of developing ideas and is proposing to use an electronic accreditation (approval) certificate. WebTrust already publish a list of approved TSPs and recognized assessors.

5.5 Technical issues

None of the responses indicates that technical issues have been considered so far. In interviews, the scheme operators expressed generally that standard web-based tools should be doing the job. Most scheme operators foresee that textual information, i.e. information to be read and interpreted by relying parties, would be supplied initially. Ultimately, the information would be provided in such a format that verification could be automated.

Platform issues (Windows NT, UNIX, Linux, etc.) have not yet been considered by any of the scheme operators.

5.6 Relying party issues

In formulating the questionnaire, and in keeping with the scope of the task, the focus has been on scheme operators as the sources that should provide status information on TSPs. The relying parties were included in the questionnaire at a late stage, as a potential source of "added value" information. It proved difficult to identify parties that could express viewpoints of relying parties. Only one response from a relying party was received; this response cannot be considered statistically significant.

In interviews with scheme operators, the question of relying party issues was raised. The responses received indicate that there is general consensus on keeping the verification of TSP status simple such that minimum bandwidth and connection time would be required.

6 A trust model and the need for status information

This clause defines a Trust Model for the open environment (in clause 6.1) and explains the various verification processes that go on within it. Various existing options for trust domain interoperability are then discussed, addressing their suitability in regard to fulfilling the requirements for providing TSP status information and the manner in which this could be realized.

6.1 Introduction

The focus of the present investigation is on trust services, made available to the public at large in an open, non-discriminatory manner. These principles apply to both service providers and users, and the term "open environment" is used in this sense. Although much of the analysis is based on existing knowledge and proposals concerning the issuance of public key certificates, the conclusions and resulting requirements are intended to be applicable easy to a wide range of schemes addressing other types of Trust Service Providers (TSP).

6.2 Trust model in the open environment

It will be easier for users to compare and accept service providers and their products, e.g. certificates, if the service is governed by:

- A widely agreed and published set of requirements for the service;
- Harmonized approval criteria applied by evaluators/auditors;
- Harmonized means for providing information about the status of the service provider.

Trust in the open environment is built on these factors. Figure 1 shows this, using a model based upon public key certificates: the principles are the same in the general case.

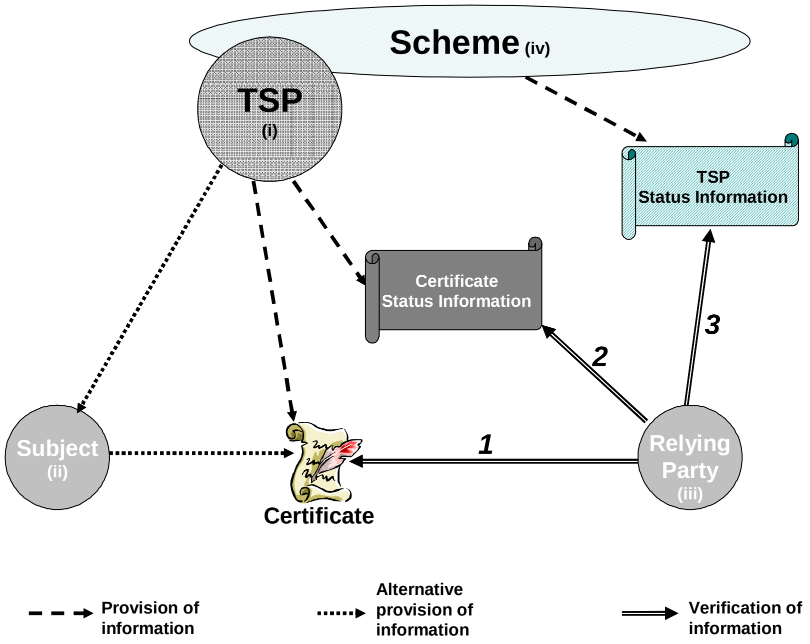

Figure 1: Trust model in the open environment

The entities involved are (i) the TSP, (ii) the subject who has a certificate issued by the TSP, (iii) a Relying Party and (iv***) a scheme***. The information sources available are (1) the certificate issued by the TSP, (2) the status of certificates issued by the TSP and (3) ***information about the TSP (and the scheme) issued by the scheme***. It is these ***emphasized components*** that are the focus of this present report and this model.

The diagram shows the three available stages of verification and acceptance that may be used by a relying party during a transaction. Those numbered "1" and "2" are already well established and presented here as reference and a basis of comparison for a more detailed discussion of the third verification option, "3".

6.2.1 Verification of service identity and policy

This is indicated in the verification of information path "1" in figure 1. The certificate provides information about the identity of the key pair holder. It also provides, by an OID or by a statement, a reference to the policy under which the certificate was issued. Thus, the relying party can make a judgement as to whether they wish to accept the terms of the policy. The referenced policy should be available to users and preferably be published as a standard. For example, in the case of a qualified certificate issued by a CA complying with the Qualified Certificate Policy [4], the corresponding identifier (OID) is carried in the certificate.

This first stage of declaration/verification is covered by widely recognized standards for policy requirements, including the verification of identity, and for format and encoding of the information provided in the certificate.

6.2.2 Verification of certificate status

This is indicated in the verification of information "2" in figure 1. The relying party may inspect status information that tells them whether or not the certificate remains valid at the time of checking. This stage is well covered by standardized certificate management protocols, formats and encoding in the standards.

The standards are widely adopted and implemented and most of the corresponding services are available or in the process of being implemented.

6.2.3 Verification of approval and current status of the service

This is indicated in the verification of information path "3" in figure 1, and represents the specific added value for which the present document seeks to define requirements. Any TSP that falls under the oversight of a scheme (whether that be by obligation or choice) may have information about its status provided by the scheme for public verification.

The static part of the information is either based upon both the initial evaluation and the following approval of the service, or simple recognition under the scheme, as appropriate.

The dynamic part of the status information should be based on (a) results of regular audits and on (b) any other events reported by the processes of a specific scheme e.g. based upon an assessment carried out after a report of non-compliance. Examples of such events are changes of the financial standing of the service provider affecting liability, report of a security incident, etc.

A positive result of this verification will ensure the relying party that the service, within the limitations of the given framework, was deemed as reliable at a specific time and compliant with the commitments stated by the service provider. It is important to recognize that the verification steps 1-3 do not explicitly cover any business relationship existing between signer and relying party. In order to cover such aspects, further information exchange is necessary, either on-line or off-line. Contractual relationships and signature policy are examples of how to deal with the business context. Such enhanced relationships can benefit from the quality assurance provided by the open environment.

Given the alternative means for reporting TSP status which are currently in use or planned, the absence of a statement about a specific service cannot be assumed to imply anything about the actual status of the service without an understanding of the form of status reporting employed.

In many cases there is also a requirement for the information, or part of it, to be machine-readable by the relying party.

Management and harmonized provision of status information in the open environment implies the fulfilment of some essential requirements:

- Harmonized minimum criteria agreed for approval of TSPs and for alarm reports (static + dynamic info);
- Agreed formats and protocols to provide status information to relying parties;
- Trustworthiness of the information and its management.

These requirements are yet to be developed.

6.3 Comparison of different policy mapping concepts

This clause examines different mechanisms for policy mapping, and identifies where they may have any valuable contribution to the issue of the provision of status information.

Significant work has been undertaken to examine how different trust domains can inter-operate. To some extent this inter-operation is the issue when a relying party receives a transaction supported by a public key certificate. However, the approach to inter-operability has been through establishing some kind of policy mapping, which should not be confused with the needs of TSP status information management. In the former the purpose is to allow interoperability between two (or more) domains supported by a Certificate Authority, and in general the intended beneficiaries are the operators of those domains. Assessment is usually based on the Certificate Policy and Certificate Practice Statement of the TSP and can be mutual or one-way. The PKI Forum's Technology Working Group has produced a valuable paper summarizing these interoperability issues [1]. In the latter case, the intended beneficiary is the relying party, whose confidence in relying upon the attestation of a certificate could be enhance by having a widely-recognized body confirm certain status-related characteristics of the issuer. Therefore, trust establishment in an open environment is not identical with interoperability between trust domains.

Each of the inter-operability models has differences from our trust establishment model, due to the verification path 3, in figure 1. Bearing in mind the requirements for verifying the TSP's status, we can consider the potential contribution of the most noteworthy models as follows:

- **Cross-certification:** in this case one TSP issues a certificate to another, or they may mutually exchange certificates. The scope of recognition may be fully inclusive (symmetric) or it may differ (asymmetric). In such a case, each TSP has a significant amount of knowledge about the other, in order to take the decision to cross-certify. There is also the presumption that the parties involved are of peer status (generally speaking). When a relying party is trying to determine whether to trust the issuing TSP, they may have no idea as to who or where that TSP is, and they cannot expect to find that their own service provider has entered into a cross-certification arrangement with the originator's TSP. The purpose of having an approval scheme is to allow the issuer to provide a reference to a scheme which holds information about it. It is desirable that that scheme can contain some unique reference to the TSP in question, e.g. their public key, but this is not contained within a certificate - it is merely included within the status information as an authenticating reference.

- **Bridge-CA:** because this is a "hubbing" version of cross-certification, it has the same characteristics with regard to trust status information as does the cross-certification model. Where this concept may help in the area of TSP status information might be to provide some kind of connectivity between schemes, to aid with the cross-recognition of assessment criteria.

- **Cross-recognition:** this relies upon the ability to use authentication information across domains. The parallel model for TSP status information is the ability for the relying party to have confidence in the trust information it is presented with, and there could be a parallel application in this regard. Indeed, the cross recognition approach proposed by APEC was developed to use accreditation (approval) status information to allow a user to decide whether to accept a transaction or not. As such it went to trust as well as authentication.

- **Trust hierarchy:** The principle feature of a trust hierarchy is that it has a single point of trust. Interpreting this in terms of a model for TSP status information has a number of difficulties, principal amongst which are: it is not the intention of this task to suggest any form of hierarchy between schemes, nor it seems would it be sensible to do so, and hence there is no obvious point of "root" trust (although some projects such as EMERITUS have proposed such approaches); since schemes may operate with a range of available approvals according to different types of services and hence have different sets of criteria used in granting approval, there might be no simple, single, relationship between schemes.

- **Accreditation (Approval) Certificate:** in this approach a recognized body issues a signed certificate bearing the subject TSP's public key, as a confirmation of their approval within a particular scheme. It is, however, unclear how to include this certificate into the verification process by the relying party (e.g. "must" the signing party forward their TSP's accreditation (approval) certificate? Should it be embedded within the certificate issued by the TSP?) and how to manage it for dynamic changes in a visible way.

- **Certificate Trust Lists:** this is a list, signed by the issuer, which could contain (amongst other information) the identities of TSPs whom the issuer regards as being "trusted". Normally, in an inter-operability context, some specific criteria would be established in order for a TSP to be eligible for inclusion of the list - this would normally be policy-related. The requirements for status information differ from certificate trust lists in at least the following three ways: firstly, in a trust list that might be published by an approval scheme, the degree of commonality of the members of the trust list (i.e. those named within it) would differ according to the type of service being offered; secondly, inclusion within such a list may not denote "trustworthiness" - the status may actually record their failure to gain approved (i.e. trusted) status; thirdly, the beneficiaries of the status information are relying parties, rather than peer CAs. Nevertheless, Trust Lists have some helpful qualities, not least the notion of the list being signed, hence allowing its provenance to be authenticated.

6.4 Existing approval scheme mechanisms

The known mechanisms already in use or proposed by existing schemes are described below, with an analysis as to their ability to support the requirements of this task.

- **Signed List:** This approach is used by the Italian supervision system, the list and the issuing authority's public key being widely available from the scheme's own website and from each of the member TSP's web sites. It also provides for the supervisory authority's public key to be issued with a certificate by each of the trusted CAs within the scheme. This mechanism ensures that it is widely recognized and difficult to "spoof". The voluntary approval scheme *tScheme* intends following a similar path, publishing a signed list of approved TSPs including their historical status within the scheme. *tScheme*'s public key will be made widely available on a variety of reputable web sites. This list too will be available from *tScheme*'s own website and through those of its approved TSPs. In each of these cases, the list is widely available and freely accessible by any relying (or other interested) party. Such a list has the ability to provide a solution to the requirements of this task, given that a suitable format and syntax can be developed.

  Webtrust also publishes a list of approved TSPs but this is not signed (as yet).

- **Accreditation (Approval) Certificates:** *tScheme* will issue a mark of approval, the "*tScheme* Mark", linked to a "grant of approval" for each approved service, which takes the form of a signed statement describing the service and the conditions of approval. These statements may also include a hyper-link to the full-signed status list. Although such attestations could be used to establish the current status of a service, there is no capacity to record historical status (nor incentive for a TSP to display it when it is not in their interests to do so), and in this sense an Accreditation (Approval) Certificate (or a set of them) is rather like an un-linked "white list" (see below). WebTrust has a similar "WebTrust Seal" linked to a detailed statement of what has been approved.

- **Root Certificates:** Some schemes use this principle to issue a root point of trust through which a chain of trust may be parsed to determine membership of the scheme. In general, several of the characteristics of the Trust Hierarchy apply (refer to clause 6.3). This approach could suffer from a lengthy chain back to the root. In addition, this approach may be unable to include historical status information, and thus, under these circumstances, specific measures may need to be deployed to retain knowledge of the status at the time of a transaction or service.

- **Black/White lists:** Some schemes opt for these approaches which have the shared characteristic of capturing primarily only the up-to-date status, neglecting the historical aspect, at the time of the transaction or service, required for this task. Black lists in particular rely upon an assumption that absence from the list indicates compliance with whatever criteria are set, whereas the scheme operator may potentially be unaware of a particular TSP who fails to comply. These mechanisms do not fulfil the requirements of this task as described above without additional supporting information relating to historical status.

6.5 The way forward

On the basis of the foregoing discussion of the requirements for relying party verification of trust, and the available inter-operability mechanisms and their comparison with those requirements, the present document concludes that a form of signed list is the best-suited mechanism by which status information can be provided for the capture and presentation of TSP status information. Additionally, careful regard to the overall mission of the task, i.e. to be as fully inclusive as possible and to ensure that relying parties can determine the status of the TSP at the time a transaction took place, confirms that a form of signed trust list is the best-suited form of structure by which status information can be provided.

This selection is reinforced by the choice of this approach by two existing schemes of quite differing nature (the Italian supervisory scheme and the industry voluntary approval scheme *tScheme*), each of which wishes to publicize their approved TSPs status widely and openly. The next clause will consider the form of harmonized requirements for TSP status information based upon a signed list structure.

7 Harmonized requirements for TSP status information

This clause addresses the requirements for harmonized provision of TSP status information. In recognition of the selection of a form of signed list as the basis for presentation of this information, the term "TSP Status List (TSL)" is adopted. Each scheme would maintain its own TSL in as close a fashion to the eventual standard as its own procedures enabled. Each scheme would operate against specific (i.e. fixed) criteria for determining the status of TSPs which it recognized: a scheme operator could, therefore, operate more than one discrete scheme.

The intention of the present document is that, whilst this structure is unlikely to be immediately achievable by any existing schemes, it represents a future attainment target, fulfilment of which would allow the exchange, and possibly in time the integration, of status information giving users comprehensive information about the schemes and the services provided by TSPs falling under the scope of the respective schemes. Development of a standard for implementation of the TSL would address further details such as encoding, interpretation, etc.

These requirements are drawn from the input of the various schemes which responded to the questionnaire (see clause 5). It is ***not*** the intention of the present document to impose upon any form of, or specific, approval scheme any restrictions on its freedom to operate in a manner of its own choosing. Adoption of these harmonized requirements is entirely voluntary and nothing in the present document is intended to require otherwise. The requirements herein are constructed so as to accommodate the various existing mechanisms and to provide an attainment target which will result in the delivery of enhanced quality of status information to users, both relying parties and subscribers.

7.1 Information provision

Within each scheme's TSL, status information should be provided in each of the following forms:

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

The manner in which the status information should be provided is discussed in clause 7.2. The specified format is meant to allow automatic verification, but could be used as a specification of the minimum human readable information that should be provided.

Due to the nature of the question to be answered - i.e. "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**" (see clause 4.1) - the TSP Status List must necessarily contain information from which it can be established whether the TSP's service at the time of the transaction was known by the scheme operator and if so the status of the service, i.e. whether it was approved, suspended, cancelled, revoked, etc. The TSP Status List must therefore contain not only the service's current status, but also the history of its status. The TSP Status List must therefore, because of the requirements upon it, be a combination of "white list" and "black list", including historical information.

7.2 TSP Status List

As described in clause 6, the objective of the TSP Status List (TSL) is to enhance the confidence of relying parties by providing access to information that allows them to know whether a given Trust Service Provider (TSP) was operating under the approval of that scheme (be it a supervision system, a voluntary approval scheme, or otherwise) at the time of providing the TSP services or other times specified by the relying party. The TSL identifies all TSPs that are or were previously approved by the scheme. It provides for each of the TSP services that are or were previously approved under the scheme, information on their current status (approved/not-approved) as well as historic information on approval, suspension, cancellation and withdrawal. The TSL therefore provides "white list" as well as "black list" information which relates not only to the status at the time at which the TSL was published, but retrospectively as well.

The status list should therefore have three major components, in a structured relationship. These should:

- provide information on the issuing scheme;
- identify the TSPs recognized by the scheme; and
- indicate the service(s) provided by these TSPs. For each service, the current status should be given as well as the status history of the service.

To achieve this goal, requirements for the nature of information included in the TSL are specified in this clause.

TSLs may be used in a wide range of applications and environments covering a broad spectrum of interoperability goals and an even broader spectrum of operational and assurance requirements. The requirements for the TSL profile define a baseline set of information that should be expected in every TSL.

In defining the following TSL profile consideration has been given to the X.509 v2 CRL syntax [3], which has been used as an input to the abstraction of a requirements model.

7.2.1 TSL general structure

The TSL should be a signed list. The scheme operator issuing the TSL is responsible for signing the list. The manner of signing should be the same as for a CA signing a CRL.

The TSL should consist of the following fields:

a) Status list to be signed.
This field is a sequence containing the identification of the issuing scheme, the issue date of the list, the issue date of the next list, and the list of TSPs (if any). Each TSP entry defines the identity and address (postal and e-mail) of the TSP and information on their current status as well as status history. The status list structure is defined in clause 7.2.2.

b) Identifier of the algorithm used for signing the status list.
This field contains the identifier for the algorithm used by the issuing scheme to sign the status list.

c) Signature value.
This field contains the signature computed on the status list. The scheme issuing the TSL should sign the list.

7.2.2 Status list structure

The status list to be signed should be a sequence of fields identifying the version of the list format, the TSL issuer (the scheme), and the date and time the TSL was issued.

The status list to be signed should contain the following fields:

a) Version identifier of the TSL.
This (optional) field describes the version of the list format. The field provides for identification of possible future format enhancements.

b) Scheme identity, name or other formal title/reference.
The scheme identity specifies the name of the scheme.

c) Name and address of the scheme operator, including the country in which it is established.
Full address details of the scheme operator identified in clause 7.2.2 b) are provided in this field, for both physical and electronic communications.

d) Scheme information URL.
This field provides the URL where users (subscribers, relying parties, other interested parties) can obtain any scheme-specific information. This information should include, *inter alia*, details about the specific classes of service which the scheme oversees (see clause 7.2.4 a).

e) Status determination approach
E.g. fully compliant with the TSL or based on a partially-compliant process, such as a white list, a black list, a certification path or any other basis (this information will enable adoption of the TSL format whilst the means to be fully compliant with its requirements do not yet exist).

f) The duration over which historical information is maintained, as appropriate.

g) Date and time of this update.
This field specifies the date and time on which the list was issued.

h) Date and time of the next update.
This (optional) field specifies the latest date and time by which the next list will be issued.

NOTE: Requirements for timeliness may necessitate re-issuance of the list prior to this time owing to any significant change requiring notification, e.g. a new service becoming approved, a revocation occurring, etc.

i) List of Trust Service Providers.
Depending on the Status Determination Approach (see (e) above) the list of TSPs may be either mandatory or optional. E.g. in the case where no TSPs are or were previously recognized by the scheme, this field should be empty. If one or more TSPs are or were previously recognized by the scheme then the field should contain a sequence identifying each TSP and providing details on the approval status of each of the TSP's services.

Item i) is expanded in clause 7.2.3.

7.2.3 List of Trust Service Providers

For each TSP the following information should be provided:

a) TSP identity, name or other title/reference.
This field specifies the name of the legal entity responsible for the TSP services that are or were recognized by the scheme.

b) Brand/trading/marketing name under which the TSP operates.
This (optional) field specifies an alternative name under which the TSP identifies itself in the provision of its services.

c) Address and contact details of the legal entity responsible for the TSP services, including the country in which it is established.
This field provides full address details of the legal entity identified in clause 7.2.3 a), 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.

d) TSP information URL.
This field provides the URL where users (subscribers, relying parties) can obtain TSP-specific information.

e) List of Approved Services.
This field contains a sequence identifying each of the TSP's recognized services and the approval status of that service.

Item e) is expanded in clause 7.2.4.

7.2.4 List of approved services

For each of the TSP's services recognized by the scheme the following information should be provided:

a) Identifier of the service.
This field contains the identifier of the service type. A list of service types and their identifiers should be defined and agreed (refer to clause 8).

b) Service identity, name or other formal title/reference.
This field contains the name of the service as used by the TSP in the provision of that service.

c) Service digital identity
This field contains a digital identifier unique to the service which can 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.

d) Identifier of the current approval status of the service.
This field contains the identifier of the approval status of the service. A list of approval status types and their identifiers should be defined and agreed. The status types should comprise the following:

- approved (active approval)/not subject to notices (passive approval);
- expired (due to non-renewal);
- suspended (by the scheme, with reasons);
- cancelled (voluntarily, by the TSP);
- revoked (by the scheme, with reasons).

The same status types are used in the Service Approval history (refer to clause 7.2.5). 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. The current status can be determined from clause 7.2.4 d); the date on which the current status became effective is specified in clause 7.2.4 e). Any previous status with its starting date can 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").

e) Starting date and time of the current status.
This field specifies the date and time on which the current approval status became effective.

f) Scheme service definition URL.
This (optional) field provides the URL where users (subscribers, relying parties) can obtain information on any scheme-information specific to the service that will help understanding the significance of the approval status.

g) TSP service definition URL.
This (optional) field provides the URL where users (subscribers, relying parties) can obtain information on the specific TSP service, e.g. the Service Definition, PKI Disclosure Statement, etc.

h) Service approval history.
In the case where the service has no history prior to the current status (i.e. first time approved status) this field would be empty. The field must otherwise record any change in the status of the service and must then contain a sequence of one or more service approval history details.

Item h) is expanded in clause 7.2.5.

7.2.5 Service approval history

For each change in TSP service approval status the following information on the previous approval status should 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):

a) Identifier of the service.
This field contains the identifier of the service type; refer to clause 7.2.4 a).

b) Service identity, name or other formal title/reference.
This field contains the name of the service as used by the TSP in the provision of that service; refer to clause 7.2.4 b).

c) Service digital identity
This field contains the service's unique digital identifier applicable at the time of the referred approval status; refer to clause 7.2.4 c).

NOTE: The above three fields are repeated with respect to the current status shown in clause 7.2.4 in order that any historical changes are recorded.

d) Identifier of previous approval status of the service.
This field contains the identifier of the previous approval status of the service; refer to clause 7.2.4 d).

e) Starting date and time of previous approval status.
This field specifies the date and time on which the previous approval status in question became effective.

The logic of the list is that, once the scheme operator was aware of the existence of the TSP, the particular beginning status either remained unchanged during the lifetime of the TSP (only current status, no history) or is seamlessly followed by a sequence of one or more statuses (current status and history). E.g. if a TSP 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, than 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).

7.2.6 Summary of TSL profile

The following is a representation, using informally an ASN.1-like syntax, of the proposed TSL profile (clauses 7.2.1 to 7.2.5 inclusive). It should be noted that this representation is merely a demonstration of the logic of the TSL and not meant as prescription for possible standardization work. Although the preceding text suggests that some components could be optional, this representation deliberately avoids use of the keyword "OPTIONAL" since the intention is to show the structure. Determination of actual optional inclusion or not is left for any follow-on work to establish definitively.

```
TSPStatusList       : :=    SEQUENCE            {
        tbsStatusList               TBSStatusList,
        signatureAlgorithm          AlgorithmIdentifier,
        signatureValue              BIT STRING      }

TBSStatusList       : :=    SEQUENCE            {
        version                     VersionTSL,
        schemeIssuing               Name,
        schemeOperator              SchemeOperatorNameAddress,
        schemeInfo                  SchemeURL,
        statusDetermination         StatusDeterminationBasis,
        historicalRetention         Duration,
        thisUpdate                  UTCtime,
        nextUpdate                  UTCtime,
        tspList                     SEQUENCE OF SEQUENCE
                                    DEFAULT "None"              {
                tspName                     TspName,
                tspMktName                  TspMktName,
                tspAddress                  TspAddress,
                tspInfo                     TspInfoURL,
                tspSvList                   TspServiceList      }
                                                    }

TspServiceList      : :=    SEQUENCE            {
        serviceId                   ServiceIdentifier,
        serviceName                 ServiceName,
        serviceDigitalId            ServiceAuthenticationData,
        statusId                    ApprovalStatusIdentifier,
        statusTime                  UTCtime,
        schemeServiceInfo           SchemeServiceURL,
        tspServiceInfo              TspServiceURL,
        svApprHistory               SEQUENCE OF SEQUENCE
                                    DEFAULT "None"              {
                serviceId                   ServiceIdentifier,
                serviceName                 ServiceName,
                serviceDigitalId            ServiceAuthenticationData,
                statusId                    ApprovalStatusIdentifier,
                statusTime                  UTCtime             }
                                                    }
```

7.3 Performance characteristics

Changes to status information should be provided in a timely fashion according to the following, the response times being dependent upon 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 a format readily down-loadable and printable or is machine readable.

Status information may optionally be periodically refreshed, in accordance with the information provided in clause 7.2.2 h).

8 Implementation options

This clause deals with possible implementation aspects of the provision of status information in electronic form, through a TSL as defined in clause 7, both for automated access and processing by relying-party clients, and also in human-readable form. The clause starts with an overview of the major stages that make up the complete process of the provision of status information to relying parties. The overview also includes interoperability requirements to be met by basic functions in an open environment. Next, some of scenarios are presented, intended as examples of implementation of the process.

An important conclusion of the analysis is that transparency among different schemes calls for harmonization of more than the technological aspects alone.

The purpose of this clause is twofold. First, to suggest a suitable scope for a tangible idea about the contents of the forthcoming activity on selection and, where necessary, development of standards for formats, protocols and interfaces. Second, to provide some useful initial input to that work. Early comments and discussions on the requirements and examples presented in this clause will facilitate the next phase of the work, as outlined in clause 9.

8.1 Automated processing

8.1.1 Process overview and interoperability requirements

Each stage contains some necessary interoperability requirements, to be met in an open environment. A basic assumption is that the relying party, specifically its client software, has to be able to validate the TSP in question on-line, without suspending the transaction. The intention with these requirements is to contribute with guidance and rationale to the selection and/or specification of the necessary minimum set of standards.

Some high-level requirements for trust are given below, but the more detailed security analysis, including inter-operability aspects, is beyond the scope of this task and must hence be addressed by future work.

- **Decision by the scheme** to accept and publish a TSP/Service according to prevailing criteria. The decision by the scheme operator, resulting in approval, non-approval or other determination regarding approved status, has to be based on widely publicized harmonized criteria agreed for approval of TSPs. Such harmonization across different schemes will allow the relying party client software to interpret the status information and make a decision based on it. That is, the relying party's system can make an automated decision in real-time without the need of a detailed study of the regulations and criteria applied by the scheme in question.

- **Creation or update of status information**. This stage shall conform to standard format and syntax in order for the relying party client to successfully read and interpret the information and present it to the user or to the decision-making software. The electronically provided status information shall be signed by the scheme operator and properly time stamped.

- **Distribution and storage of status information** for retrieval by relying parties. The scheme operator is responsible for this stage. From a relying party's perspective it is indifferent whether protocols and interfaces for this stage are standardized. In principle, it may or may not be left as a local implementation matter. However, the following implementation scenarios will show that most of the involved functionality is covered by at least industrial standards.

- **Access to and retrieval** of status information by relying parties. The client software shall be provided with a pointer, i.e. an electronically processable address, to the site where the status information can be retrieved. One way is to carry this information in the certificate attached to the transaction. Interoperability requires, that the protocol and interfaces for information retrieval are standardized across the different schemes.

- **Interpretation of the retrieved information** and the status determination by the relying party. In order to decide whether or not to accept the product of the TSP (certificate, time stamp, etc.), the relying party client has to read and understand the status information (standard format and syntax) that supports the decision-making process. Interpretation of the actual TSP status also requires harmonization of the approval criteria, as already explained under the first bullet of this list.

8.1.2 Scenarios

The scenarios presented in this clause are examples of possible, and what the authors believe likely, implementation options for the provision of TSP status information. Emphasis is on components for information storage and provision by the scheme and for access and evaluation by relying parties.

Both of the presented examples offer scalability and the potential of wide availability of products and operational platforms.

8.1.2.1 Scenario based on X.500 Directory

In this scenario the X.500 Directory is used to make the status information available. Most of the interoperability requirements, with the possible exception of some security features, can be met by applying relevant parts of the X.500 specifications. This includes the LDAP protocol for posting and retrieving information.

Signing operations may conform to CMS as specified in S-MIME or to TS 101 733 [5] format if additional features are required.

It is important to keep in mind that the interpretation of the information contained in the TSL differs from that of a common CRL.

8.1.2.2 Scenario based on Web server

A significant number of questionnaire responses suggested that a Web-based solution may become their preferred means of providing status information. Web technology has reached a high degree of maturity; its main functions and formats are standardized (HTTP, HTML) and it is widely deployed and used. User-friendliness is among its major strengths.

An extra benefit offered by an XML-based Web-scenario is that automatic processing and human-readable presentation can be combined with almost no additional effort. Hence, e.g. a TSL-parser should be able to interrogate the list to establish status at a specific desired time. Another feature is support to declare the privacy policy of the information service.

Signing operations are specified in the proposed W3C standard "XML Signature Syntax and Processing" and for more advanced functionality by the evolving ETSI XML signature format standard.

Although it is possible to display on a Web interface information that has been specified in ASN.1, the assumption in the present document is that each of the two scenarios has its "native" encoding, i.e. encoding based upon ASN.1 for the Directory and XML for the Web. Annex C provides a very preliminary draft of an XML schema definition of the TSL.

8.2 Human-readable presentation

The requirement that TSP status information be accessible in human-readable form leads to requirements of varying simplicity and style. The present document describes two alternative ways to provide access - static and dynamic. In either case, human readable form may be entirely natural language or in some mildly encoded form, so long as the encoding (abbreviated) notation is clearly explained. The preparation of a common syntax could be considered but is likely to limit the accessibility of the information and may defeat the purpose of human-readable status information. Whilst English may be the more universally useful natural language to choose, the present document expresses no preference as to the natural language that should be used.

Although human readable presentation will include all major steps of the process as presented in clause 8.1.1, requirements for human readable presentation standardization will be limited in comparison with the case of automated processing. Widely used platforms and protocols are available for storage and retrieval of text files, either in word processing format or HTML. Agreed mechanisms may, however, still be needed, for example to localize the information and to authenticate its origin.

8.2.1 Static presentation

This would effectively require the provision of the whole of a scheme's status information, i.e. its complete TSL expressed in natural language. This would be a direct report of all fields of the TSL, appropriately structured and presented to allow easy understanding of the information, by service provider, their services and the full status history for each service. The user need not be provided with the ability to manipulate or search this information other than in terms of their own sequencing through it (the only explicit requirement being that the information is sensibly ordered, probably alphabetically).

Static presentation may be provided off-line, although the currency of the information may become an issue, and the user needs to be made aware of this.

8.2.2 Dynamic presentation

It should not be forgotten that, apart from the obvious and primary needs of parties trying to determine whether they should rely upon a particular certificate's contents, parties seeking status information may be doing so as part of a process of selecting a service provider, and hence their needs should be facilitated. These joint needs can be accomplished by providing dynamic presentation.

Dynamic presentation should therefore permit user-generated enquiries, searching by specific (named) service, by type(s) of service, by provider and other useful criteria. At all times, the user must be able to access the historical status information for any service's details they are provided with.

This form of presentation is much more likely to require an on-line service, rather than off-line, although a package to manipulate downloaded status information could be useful, if demand justifies its creation.

8.3 Transition scenario

A further aspect of implementation is how existing schemes might be able to express their status information within the framework of the TSL. As noted previously in the present document, the full scope of the TSL represents the combination of the qualities of the various schemes addressed during the requirements capture phase of the task, whilst also fulfilling the requirements of the task for the provision of historical information. This clause sets out how the various fields can be provided from existing schemes. Some of this content can be readily provided from current schemes. Some might require changes to current operating policy (i.e. the retention of historic information which might otherwise not be publicly available). Some may require changes to how the schemes collect, collate and classify information prior to its provision before substantial compliance with the requirements can be claimed. Each scheme is completely free to determine its own plan for doing this, if it chooses.

To consider the components of the TSL in turn:

8.3.1 Basic TSL information

Field	Provision
Version identifier	Readily built-in and maintained. Proposed normative work should specify a particular format governed by a process for maintaining the standard(s).
Scheme identity	Text of the scheme operator's choosing.
Address	These will pre-exist in both physical and electronic form.
Scheme information URL	Very unlikely not to pre-exist.
Status determination approach	To be defined by proposed normative work - this process must ensure that each existing scheme can be suitably identified.
Period of historical retention	Determined by the scheme's own policy - normative work need only specify a means of expression.
Date/time of this update	Self evident - normative work need only specify a means of expression.
Date/time of next update	Self evident - normative work need only specify a means of expression.

8.3.2 Trust Service Provider information

Field	Provision
TSP identity	Text of the TSP's choosing.
TSP Brand name	Text of the TSP's choosing.
Address	These will pre-exist in both physical and electronic form.
TSP information URL	Very unlikely not to pre-exist.

8.3.3 Approved service information

Field	Provision
Service identifier	To be defined by proposed normative work - this process must ensure that each type of service can be suitably identified, with scope for extension. This could be by generic type (e.g. CA) with specific qualifiers (e.g. issuing QCs to the public) - to be encoded.
Service identity	Text of the TSP's choosing.
Service digital identity	This would typically be the public counterpart to the key used by the TSP when delivering the specific service, e.g. signing certificates, time stamp tokens, etc. Other digital "finger prints" may be required according to the type of service.
Current approval status	Normative work is required to ensure that a range of statuses can be conveyed. Their interpretation may need to take into account the "Status determination approach" field from the Basic TSL information - this also should be left to normative work. Thus this field will permit the use of a range of status indicators, e.g. "approved", "suspended", "revoked" - for many schemes these would fulfil the needs of those employing a white list approach or a trust list approach; "revoked", "notified (of failure to comply with requirements" or "prohibited" might also be required, especially by schemes employing a black list approach.
Starting date and time	Time at which the declared status took effect - normative work need only specify a means of expression.
Scheme service definition URL	Very unlikely not to pre-exist.
TSP service definition URL	Very unlikely not to pre-exist.

8.3.4 Approval history information

The basis of this information is simply the Approved Service information referred to in the preceding clause, removed to a different part of the TSL and thereby adopting a change of significance (i.e. it is no longer the current status). Existing schemes, which do not currently protect this information for continued accessibility, need only put in place a process to retain this information and place it elsewhere within the TSL. No new information need be captured, and the interpretation of the information relies upon the same principles and Basic TSL information as the main status information.

Thus, the TSL presents not a threat to existing schemes but an opportunity to enhance the information they provide in a consistent and structured form. They need only establish a transition strategy at a time when it suits them, and the process for doing so, given that normative work has been concluded, does not require complex processes.

9 Recommendations for future actions

This clause recommends actions that should be taken to further development of the requirements.

9.1 Development of a supporting TSL standard

The preparation of a TSL standard is the principal recommendation of the present document, and supports closely the "Task 5" description for the proposed ETSI ESI SI 2002 work programme. Such a standard will harmonize the content and format of Trust Status Lists in a manner that facilitates their exchange and interpretation both by humans and machines.

The recommended normative tasks are the following:

- Resolution of additional requirements issues (see clause 9.2);
- Refinement of the TSL structure, agreed by all parties to the task;
- Drafting and, ultimately, agreement of an ETSI Technical Specification for a TSL, including:
    - (normative) Structure,
    - (normative) Format and interpretation,
    - (normative) Implementable form (e.g. XML),
    - (informative) recommendation of preferred scenarios, including baseline protocols and interfaces to be used (with additional profiling if interoperability so requires) and recommendations for measures ensuring trust,
    - (informative) plan for pilot implementation, based on commitment of the wider task participants.

The specification and implementation of such a standard should be undertaken against the following objective criteria:

- Participation of a representative number of scheme operators, both governmental and private, both supervisory and voluntary (in the terms of [2]) and from both Europe and further afield;
- Provision of open workshops at which the interested parties can discuss and contribute to the development of the task. One interest group in this context is the community of relying parties; another may be developers of trust-based applications.

9.2 Requirement issues deserving further attention

During the latter stages of the preparation of the present document a small number of important issues have arisen which could not be adequately addressed in the available time-frame. These are itemized below and it is recommended that, prior to the refinement of the TSL structure and the drafting of a technical standard, these requirements issues are resolved, since they could influence the TSL structure. The points to be addressed are:

- In certain jurisdictions there are legislative requirements for the approval of TSPs before their services (e.g. issuing public key certificates to support electronic signatures, issuing time stamps) can have legal effect. Indeed, Directive 99/93/EC [2] gives specific legal presumptions for qualified certificates. This issue should be assessed to see to what extent the TSL could and should address this issue as well as simply a "trust status";
- In the present document the description of the TSL has suggested that some components could be optional, and for others has suggested a default value (e.g. when lists are empty). During the course of producing the technical standard these aspects need to be firmly established and defined accordingly.

9.3 Necessary complementary action

Development of equivalent criteria for the process and methods of conducting approvals of TSPs. The rationale for such criteria is presented in clauses 6.2.3 and 8.1.1 of the present document.

The task needs co-operation among the different schemes and between the representatives of the schemes and the standardization group, responsible for the execution of the normative tasks described above in clause 9.1.

9.4 Potential complementary actions

The following potential complementary actions have been identified:

- Development of guidance for application software verifying TSLs and presenting status information to users (subscribers, relying parties). An option would be to extend the document CWA 14171 [6] (E-Sign WA-G2) with specifications of functional and quality requirements for products verifying TSLs. An alternative would be to prepare a completely separate CWA, leaving CWA 14171 [6] to address its specific Directive 99/93/EC [2]-derived subject;

- Development of a prototype system of interoperable TSLs supported by real-world schemes of differing sorts. Such work could be carried out as a funded project in which scheme operators would participate.

Annex A: Specimen requirements capture questionnaire

A.1 Introduction

This questionnaire is the principal means by which the ETSI task STF 178-5 "**Provision of harmonized status information on CSPs and other Trust Service Providers (TSP)**" is gaining its external inputs, in a process referred to as "Requirements Capture". The task has the objective to establish minimum common requirements for the provision of TSP status information and for the means to provide it. This is explained in greater depth in an accompanying document, STF178-5/Z02 "Task Briefing", copy of which will have been made available in advance to all respondents to this questionnaire.

This questionnaire consists of three parts.

Part A is for those who participate in the operation of a scheme. It addresses the identification of the scheme, its general characteristics and development status. It then addresses the items, which make up the essential targets of the present task. These are the critical components to maintain Trust Service Provider (TSP) status information and to make it available and useful to users in an open environment. Some of the important items and components to be defined and agreed are:

- The contents of information to be provided and its format;
- Policies and rules how to distribute, store and manage the information;
- Definition of the user community;
- Framework and mechanisms to maintain user confidence.

Technical means (e.g. pointers, protocols, etc) to find, access and validate the information

Part B is intended for those who will want to gain access to status information. It seeks their views on how that information should be made available and what it should cover.

Part C deals with follow up and contact details.

A.2 For scheme managers/implementors

A.2.1 Details of the scheme

This clause covers general characteristics of the scheme for which the respondent has responsibility/participation. Please provide the following information:

The **country** (code) in which the scheme is based and the **name or reference** by which the scheme is known:

What is the **legal basis/mandate** for the scheme? (E.g. Directive 1999/93/EC Supervisory System, any specific national/international law/regulation requiring it, international treaty or agreement, trade organizations, co-regulatory, industry-consumer):

Which body is responsible for **governance of the scheme**, i.e. has the authority over it?:

Which body is responsible for the **operation of the scheme** and **granting recognition/approval** (or whatever word is preferred)?:

What is its **geographic coverage**, i.e. in which countries might participants operate from?:

Who may participate or is/will be subject to or become a member? (E.g. voluntary/mandatory, who are those eligible):

Is it for **public or closed** Trust Services?:

What is it about this scheme that makes it **trustworthy**, i.e. what is the basic characteristic that enables third parties to rely upon it?:

What is its present **implementation/operational status**? (E.g. paper definition/being "built"/in operation - please give key dates):

Any other comments on the scope/objectives/specific **characteristics** of the scheme?:

A.2.2 Status information

What specific status info is made available? (specify classes of data and where practical, meaning and ranges - e.g. the "approving" scheme identity, standards/criteria against which TSPs are assessed, financial liability, maintenance of CRLs, date last audit passed):

How is status info made available? (E.g. Approval/Revocation List, Trust list, Black-list/White-list):

What is the **intended user community**? (E.g. all potential relying parties (from other countries, etc), closed group only, defined by contract or other means, other):

What technical and/or other means guarantee that the provided information can be **trusted**?

How is the information and its location **referenced and accessed**? (E.g. is it published by the scheme and/or communicated by the party who initiated the transaction):

What **requirements are there on users** and their systems? (E.g. clients, so as to access, retrieve, validate and use the information, client software, authentication, etc.):

A.2.3 Technical Aspects

What is the **basis of assessing** those TSPs which are monitored/approved - what standards/criteria are applied?:

Who can cause/what events could lead to **changes in the status information** the scheme holds?:

How do you **share information** - is there any agreed method of policy/approval mapping with other schemes?:

What is the **method of dissemination/publication** of this status information? (E.g. mechanisms, protocols, formats, etc.):

What are your **timeliness criteria** for publication of status information?:

Are there any technology or other specific **requirements or constraints**?:

What do you believe would be the **minimum characteristics of a harmonized approach** to providing status information for general (public) use?:

A.3 For relying parties/verifiers (e.g. consumers/government/tax authorities/banks/chambers of commerce)

This part is to be completed by those who would want to access status information.

From which specific/generic schemes would you want to have status information?:

What **specific information** would you be seeking (please list)?:

How would you want or expect this **information to be provided**?:

What **timeliness expectations** would you have on its provision?:

What do you believe would be the **minimum characteristics of a harmonized approach** to providing status information for general (public) use?:

What would you expect to be given to demonstrate the **trustworthiness of the information** and its source?:

A.4 Follow-up and Contact Details (all respondents)

Principal Respondent's details:

Name:

Organization:

Rôle/Position:

Address:

Email:

Tel:

Other participants' details: (duplicate as necessary):

Name:

Organization:

Rôle/Position:

Address:

Email:

Tel:

Nature of participation (contributor/observer):

Would you be willing to receive drafts of our Technical Report as it is developed and to submit comments on it (either your own and/or from within your organization)?: *(Delete the inapplicable answer)*

Yes ✓ No ✗

May we contact you to follow-up on points of clarification or additional questions which might arise during our synthesis of comments?: *(Delete the inapplicable answer)*

Yes ✓ No ✗

Date, location and manner of completion

Annex B: Contact list

B.1 Introduction and legend

In the following tables, broken into geo-political groups, the general quality of the input received is recorded.

We have graded the responses according to how the input was collected - the manner of collection is shown in the following tables listing our sources. The sources used were those made known to us during the preparation of the task as the responsible person(s) for the scheme or system under consideration, or their representative(s).

By far the highest quality came from face-to-face situations, where the authors were able to explain in greater detail their objectives and discuss their respondent's responses with them. Although some of these activities also included receipt of e-mailed responses, the face-to-face contact always ensured the best level of understanding and quality of input. The following symbol is used to denote this form of requirements capture: 👥.
In some circumstances, a lengthy telephone conversation was conducted during the course of which the questionnaire was completed; these are also included in the 👥 classification.

In other cases, although the authors did not discuss face-to-face with the respondent, a completed questionnaire was made available to the authors, and this was frequently backed-up by some preliminary discussion by telephone. In these cases the quality of input was considered to be good, but substantially lower than the face-face situations. The following symbol is used to denote this form of requirements capture: 🗁.

In a small number of cases a telephone conversation determined that the respondent did not really have sufficiently-well developed plans to make completion of a questionnaire practically feasible. The following symbol is used to denote this form of requirements capture: ☎.

Where the authors were unable to establish any appropriate contact, arrange a meeting, or no timely response was forthcoming (or had not been at the time of the present draft) the following symbol is used: ⌛.

B.2 EU/EEA States

Country	Contact(s)	Organization	
AT	Dieter KRONEGGER	Rundfunk und Telekom Regulierungs-GmbH (RTR)	👥
BE	Philippe DEGAVRE	Administration de la Qualité et de la Sécurité Division Accréditation Service de la Signature électronique, Ministère des Affaires économiques	👥
CH	Peter STADLIN	Bundesambt für Metrologie und Akkreditierung (METAS)	👥
DE	Friedrich KÖNIG, Assistant Head of Clause Digital Signature	Regulierungsbehörde für Telekommunikation und Post (RegTP)	👥
DK	Birgitte HAGELSKJÆR NIELSEN, Legal Adviser	Telestyrelsen DK, National Telecom Agency	🗁
FI	Kirsi SUNILA-PUTILIN, Legal Counsel/Telenetwork security	Telecommunications Administration Centre (TAC), National Post & Telecom Agency	🗁
	Timo LEHTIMÄKI, Senior Adviser/Telenetwork security	Telecommunications Administration Centre (TAC), National Post & Telecom Agency	🗁
FR	Laurent PERDIOLAT	Direction Générale de l'Industrie, des Technologies de l'Information et des Postes - Ministère de l'Économie, des Finances et de l'Industrie	👥
GB	Geoff SMITH	Information Security Policy Unit, Department of Trade & Industry	👥
	Tom PARKER	*tScheme*	👥

Country	Contact(s)	Organization	
GR	Eleni VYTOGIANI	EϑNIKH ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΤΑΧΥΔΡΟΜΕΙΩΝ (Ethniki Epitropi Tilepikinonion Kai Tachydromion - National Telecommunications and Post Commission)	📂
IE	Úna NÍ FHAIRCHEALLAIGH, Assistant Principal,	Communications Development Division, Department of Enterprise, Trade and Employment, Irish Govt.	👥
	Michael CLARKE, Assistant Principal	e-Business Unit, Department of Enterprise, Trade and Employment, Irish Government	
	John HUSSEY	National Accreditation Board, Ireland (NAB)	👥
IS	Arsaell DORSTEINSSON, Technical Director	Löggildingarstofa, National Accreditation Agency	⌛
IT	Giovanni MANCA	Autorità per l'informatica nella Pubblica Amministrazione (AIPA)	👥
LU	Carlo WIRTH	Commerce électronique, Accréditation, Promotion de la Qualité Ministère de l'Économie	⌛
NL	Réné van den ASSEM, Consultant	Ministry of Transport, DG Telecommunications & Post	👥
	Rob van EIJL	OPTA (Independent Post and Telecommunication Authority)	👥
	Anton PRONK	TTP.NL	👥
NO	Øyvind HAUGEN, Legal Adviser/Market Regulation	Post- og teletilsynet (PT), Norwegian Post and Telecommunications Authority	📂
	Leif HALBO	Justervesenet	📂
PT	Manuel PEDROSA DE BARROS, Director	Direcção de Equipamentos e Normalização	👥
	Pedro VEIGA, Manager	Programa Operacional Sociedado da Informacão, Ministério da Ciéncia e da Tecnologia	👥
	Carlos GONÇALVES, Vogal	Instituto das Tecnologias de Informacão ba Justiça, Ministério da Justiça	👥
SE	Kenneth OLOFSSON	Post & Telestyrelsen (PTS), National Post & Telecom Agency	👥
SP	Gema CAMPILLOS, Legal Advisor	Dirección General para el Desarrollo de la Sociedad de la Información	👥
	Fernando FAZIO FERNÁNDEZ de MIRANDA	Dirección General para el Desarrollo de la Sociedad de la Información	👥
EC	Joep VAN DER VEER	EC DG Int Mrkt	⌛
	Claire SION		⌛

B.3 Other European States

Country	Contact(s)	Organization	
HU	Istvan RENYI	Hungarian Communication Authority	👥

B.4 North America

Country	Contact(s)	Organization	
CA	E. Jane HAMILTON	E-Com Policy, Industry Canada	👥
	Andrew STEPHENS	Director, IT Architecture, Industry Canada	
US	Mark LUNDIN	KPMG/WebTrust	👥

B.5 Asia/Pacific

Country	Contact(s)	Organization	
AUS	Steve ORLOWSKI	Independent	👥

Annex C: XML schema definition for the Trust Status List

This annex presents a very preliminary draft schema definition for the `TBSStatusList`, following the general structure explained in clause 7. It is expected to be the basis for extension and enhancement once work is commenced on the recommended normative tasks.

It should be noted that, at this stage, no details on signature algorithms have been included and that the definition contains only the structure of the document that has to be signed, i.e. the TSL.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2000/10/XMLSchema"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns="http://www.etsi.org/names/TR/CAs-Status#"
  targetNamespace="http://www.etsi.org/names/TR/ CAs-Status#"
  xmlns:xades="http://www.etsi.org/names/TS/101903/v.0.0.9"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig"
  xmlns:p3p=http://www.w3.org/2001/09/P3Pv1
  elementFormDefault="qualified">

   <xsd:element name="TBSStatusList" type="TBSStatusListType"/>
   <xsd:complexType name="TBSStatusListType">
      <xsd:sequence>
         <xsd:element name="Version" type="xsd:anyURI"/>
         <xsd:element name="SchemeName" type="xsd:string"/>
         <xsd:element ref="p3p:ENTITY"/>
         <xsd:element name="SchemeInfo" type="xsd:anyURI"/>
         <xsd:element name="StatusDetermination" type="xsd:string"/>
         <xsd:element name="HistoricalRetention" type="xsd:timeValue"/>
         <xsd:element name="ThisUpdate" type="xsd:timeInstant"/>
         <xsd:element name="NextUpdate" type="xsd:timeInstant"/>
         <xsd:element name="Tsp" type="TspType"
                 maxOccurs="unbounded"/>
      </xsd:sequence>
   </xsd:complexType>
   <xsd:complexType name="TspType">
      <xsd:sequence>
         <xsd:element ref="p3p:ENTITY"/>
         <xsd:element name="TspMkt" type="xsd:string"/>
         <xsd:element name="TspInfo" type="xsd:anyURI"/>
         <xsd:element name="TspSvList"
                 type="TspServiceListType"/>
      </xsd:sequence>
   </xsd:complexType>
   <xsd:complexType name="TspServiceListType">
      <xsd:sequence>
         <xsd:element name="ServiceId"
                 type="xsd:string"/>
         <xsd:element name="ServiceName" type="xsd:string"/>
         <xsd:element name="ServiceDigitalId"
type="etsi:EnhancedIdentifierType"/>
         <xsd:element name="StatusId" type="xsd:string"/>
         <xsd:element name="StatusTime" type="xsd:timeInstant"/>
         <xsd:element name="SchemeServiceInfo"
                 type="xsd:anyURI"/>
         <xsd:element name="TspServiceInfo" type="xsd:anyURI"/>
         <xsd:element name="SvApprHistoryItem"
                 type="ServiceApprovalHistoryItemType"
                 maxOccurs="unbounded"/>
      </xsd:sequence>
   </xsd:complexType>
   <xsd:complexType name="ServiceApprovalHistoryItemType">
      <xsd:sequence>
         <xsd:element name="ServiceId"
                type="xsd:string"/>
         <xsd:element name="ServiceName" type="xsd:string"/>
         <xsd:element name="ServiceDigitalId"
type="etsi:EnhancedIdentifierType"/>
         <xsd:element name="StatusId" type="xsd:string"/>
         <xsd:element name="StatusTime" type="xsd:timeInstant"/>
      </xsd:sequence>
   </xsd:complexType>
</xsd:schema>
```

History

Document history		
V1.1.1	March 2002	Publication