Draft ETSI TS 1XX XXX V<m.t.e> (2006-11)

Technical Specification

Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data for digital accounting

Reference

<DTS/ESI-00047>

Keywords

< e-commerce, electronic signature, security, digital accounting, electronic invoicing, electronic signatures, trust service provider >

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

Copyright Notification

Contents

Intellectual Property Rights

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

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

Foreword

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

Introduction

Electronic records can provide a sound basis for maintaining accounting information, and with the application of good practices can prove more secure and robust than the use of paper.

The use of e-Invoicing and digital accounting is of major importance to European enterprises, because it can reduce significantly administrative costs (up to 95% of the current accounting costs). The European Directive on e-Invoicing 2001/115/EC [1] recognises the potential use of “Advanced Electronic Signatures” to protect the authenticity and integrity of electronic invoices.

Some European national governments already regulate practices for the integrity and authenticity of digital accounting data through use of electronic signatures and data formats that are not vulnerable to changes in presentation through malicious code.

In order to achieve an acceptable level of security for accounting data, practices for the use of electronic signatures need to be augmented with practices regarding storage, particularly with regards to backup regimes, and the use of appropriate data formats.

Fiscal auditing procedures can highly benefit of the availability of electronic Invoices and of digital accounting data.

The present Technical Specification is based on the findings presented in TR XXX YYY and addresses policy requirements for Trusted Service Providers (TSP) that act in name and on behalf of taxable persons that are required by the applicable law to produce and reliably keep, even beyond ten years, electronic invoices as well as other fiscally relevant documents.

1 Scope

The present document specifies security management and policy requirements applicable to Trusted Service Providers (TSP) that issue fiscally relevant electronically signed documents and/or store them on behalf of taxable persons.   This specification aims to address regulatory requirements to produce and reliably keep, even beyond ten years, signed electronic invoices as well as other fiscally relevant documents.

The presented document is directed at policies involving the use of the Advanced Electronic Signatures or Qualified Electronic Signatures. The primary aim of the application of signatures is to protect the integrity and provide data origin authentication of fiscally relevant documents in communication and storage. However, signatures may also be used, where required, to provide content commitment (i.e. non-repudiation).

This document addresses solely the Advanced Electronic Signature based solution. It is recognised that other suitable measures, not employing Advanced Electronic Signatures s and hence that are outside the scope of the present document, may be applied to assure the authenticity and integrity of digital accounting documents. It should be noted that the reliability of such alternative measures generally depend on the trustworthiness of the organisation and may require independent assessment of the technical and organisational measures applied. Advanced Electronic Signature may be used to augment existing measures to provide even higher security, or to reduce the need for other controls.

The present document may be used by competent independent bodies as the basis for confirming that a TSP is trustworthy in issuing and storing signed fiscally relevant electronic document on behalf of taxable persons.

The present document does not specify how the requirements identified may be assessed by an independent party, including requirements for information to be made available to such independent assessors, or requirements on such assessors.

Within the present document the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [18].

2 References

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

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

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

[1] CWA 14169 - Secure signature-creation devices "EAL 4+" http://www.cenorm.be/catweb/35.040.htm

[2] CWA 14167-2 - Cryptographic module for CSP signing operations with backup - Protection profile http://www.cenorm.be/catweb/35.040.htm

[3] CWA 14167-4 - Cryptographic module for CSP signing operations - Protection profile http://www.cenorm.be/catweb/35.040.htm

[4] CWA 15579 – E-invoices and digital signatures http://www.cenorm.be/isss/einv

[5] CWA 15580 – Storage of Electronic Invoices http://www.cenorm.be/isss/einv

[6] ISO/IEC 17799 – Information technology — Security techniques — Code of practice for information security management

Note: The ISO organisation will substitute ISO/IEC 17799 with ISO/IEC 27002 in 2007, so it is recommended to move from ISO/IEC 17799 to ISO/IEC 27002 when available. It is also recommended to take in the future into account the whole 2700x family, that still under development 27000 (principles and vocabulary), 27003 (ISMS implementation guidelines), 27004 (information security metrics and measurements), 27005 (risk management), and other possible future ones.

[7] ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements

[8] ISO/IEC 15408 (2005) (parts 1 to 3): "Information technology - Security techniques – Evaluation criteria for IT security"

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

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

[11] Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax

[12] ETSI TR XXX YYY: Commonly Acceptable Best Practices for handling electronic signatures and sign data relevant to accounting

[13] ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates

[14] ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates

[15] ETSI 102 176-1: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

[16] ETSI TS 102 734: Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES)

[17] ETSI TS 102 904: Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES)

[18] IETF RFC 2119: "Key words for use in RFCs to indicate Requirement Levels".

3 Definitions & Abreviations

3.1 Definitions

Advanced Electronic Signature

An electronic signature which is uniquely linked to the sender, is capable of identifying the signatory, is created using means that the signatory can maintain under his sole control, and is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable, Art. 5 No. 2 of the European Signature Directive (Directive 1999/93/EC [10]).

Commonly Acceptable Practices

Practices for Trust Service Providers signing and/or storing data relevant for accounting (i.e. fiscally relevant data) which may be recognised as acceptable by authorities in several EU nations

Electronic invoicing

Invoices sent by electronic means as defined in Directive 2001/115/EC [11]

Extended policy requirements

Extended variant of the normalised policy requirements employing a secure signature creation device and Qualified Certificate (i.e. qualified electronic signatures)

Normalised policy requirements Policy requirement which offers a quality of service equivalent to the one defined in Directive 1999/93/EC [10], in particular article 2 No 2 employing advanced electronic signatures.

Fiscally relevant data: Financial data of a taxable person or company that may need to be exhibited to a regulatory authority concerned with financial accounting (e.g. Tax Authority, Chamber of Commerce, Ministry of finance, etc.)..

Fiscally relevant document Document containing fiscally relevant data.

Maximum Identified Practices The most stringent practices identified for the signing and storage of fiscally relevant documents.

Minimum Identified Practices The least stringent practices identified for the signing and storage of fiscally relevant documents.

Qualified Electronic Signature An advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device (Directive 1999/93/EC [10]):

Qualified Certificate Certificate which meets the requirements laid down in annex I (of the Directive 1999/93/EC [10]) and is provided by a certification-service-provider who fulfils the requirements laid down in annex II (of the Directive 1999/93/EC [10])

Secure Signature Creation Device Signature-creation device which meets the requirements laid down in Annex III of Directive 1999/93/EC [10] ;

Signature Creation Data Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature (Directive 1999/93/EC [10])

Trading partner Taxable person that has trading relationships with the TSP's services user and with which invoices and/or other fiscally relevant documents are exchanged.

3.2 Abbreviations

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

AdES	Advanced Electronic Signature
CA	Certification Authority
CEN	Comité Éuropéen de Normalisation
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
ES	Electronic Signature
EUMS	European Union Member State
N	Normalised Policy Policy Requirements
N+	Extended variant of Normalised Policy Requirements
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PKI	Public Key Infrastructure
QES	Qualified Electronic Signature
SCD	Signature Creation Data
SSCD	Secure Signature Creation Device
TSA	Time Stamping Authority
TSP	Trusted Service Provider
WWW	World Wide Web
XML	eXtensible Mark-up Language

3.3 Notation

The requirements identified in the present document include:

a) mandatory requirements that must always be addressed. Such requirements are indicated by clauses without any additional marking;

b) requirements that must be addressed if applicable to the class of policy that is being applied is indicated by "[CONDITIONAL]" followed by:

"[N]" normalised policy requirements,

"[N+]" extended variant of normalized policy requirements with requirements for use of Secure Signature Creation Devices and Qualified Certificates.

c) requirements that include several choices which ought to be selected depending on the quality of the service offered under the applicable policy. Such requirements are indicated by markings by "[CHOICE]" with a subsequent indicator relating to the relative quality:

"[N]" normalised policy requirements,

"[N+]" extended variant of normalized policy requirements with requirements for use of Secure Signature Creation Devices and Qualified Certificates.

4 General concepts

4.1 Fiscally Relevant Documents

Among the number of fiscally relevant documents types addressed, across the European Union Member States, by general commercial legislation, national tax legislation, requirements for monitoring accounting in governmental organisations, this specification refers to those that specific TSPs issue, by applying them legally valid electronic signatures, and store for the required time period. These documents are currently issued according to practices that vary significantly across the European states, but there is one area where there have been some moves to provide some harmonisation of legislation, that is VAT related Invoicing. The European Directive 2001/115/EC [11], in fact, includes requirements on the use of “advanced electronic signatures” to “guarantee” “the authenticity of the origin and integrity of the contents” of invoices, even when issued across borders. This was further defined in CEN workshops on electronic invoicing which published a number of documents, among which guidelines for both the storage of electronic invoices (CWA 15580 [5]) and the application of advanced electronic signatures to electronic invoicing (CWA 15579 [4]).

The present document specifies policies for the storage and signing that may be applicable to the entire range of fiscally relevant documents that may be employed across Europe. However, the policies are particularly appropriate to the storage and signing of electronic invoices as identified in European Directive 2001/115/EC [11] as illustrated in the following diagram.

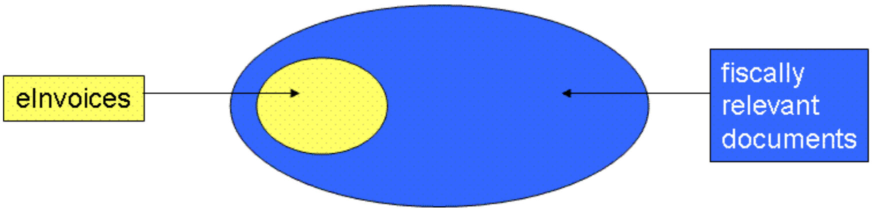

Figure 1 – eInvoices as a representative sub-class of fiscally relevant documents

4.2 Basic Model

The general application of signing and storage services to fiscally relevant documents is illustrated in the following diagram:

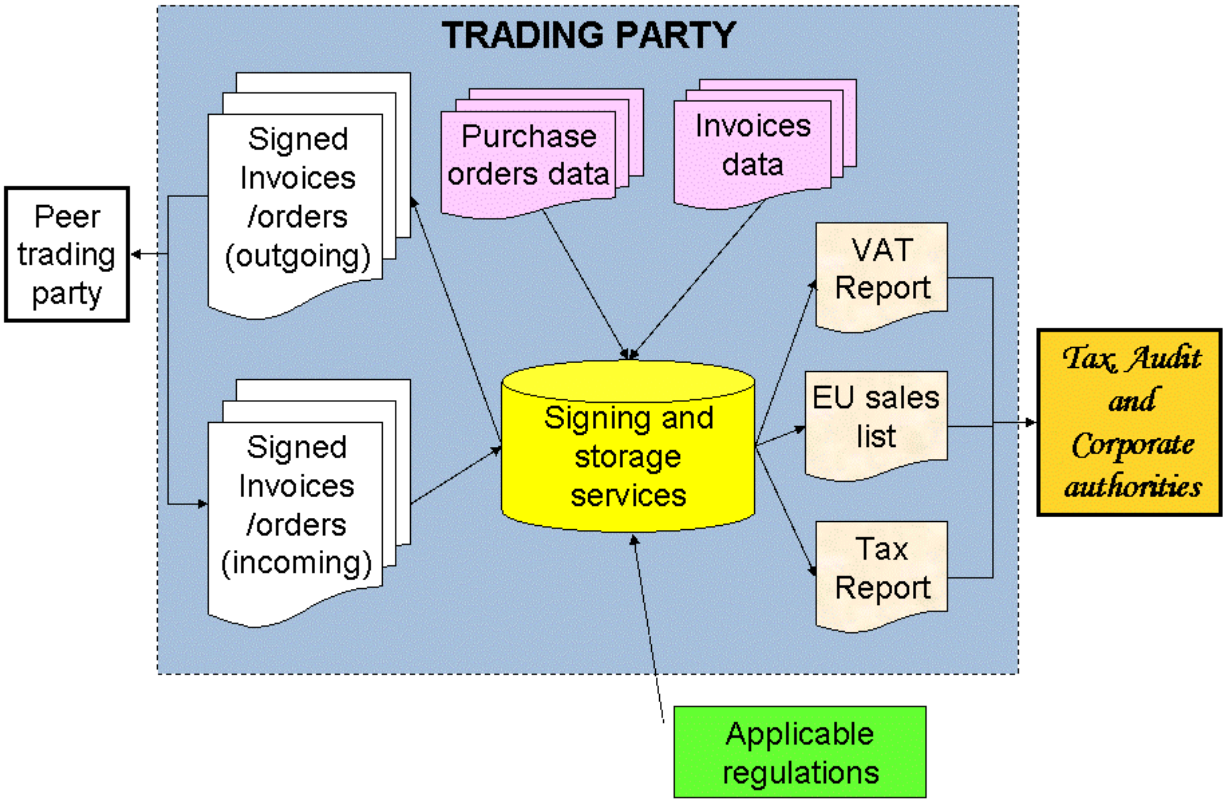
TRADING PARTY
Peer trading party
Signed Invoices /orders (outgoing)
Signed Invoices /orders (incoming)
Purchase orders data
Invoices data
Signing and storage services
VAT Report
EU sales list
Tax Report
Tax, Audit and Corporate authorities
Applicable regulations

Figure 2 - Basic Model

A range of fiscally relevant data may be input to the signing and storage services that, through appropriate procedures, produce valid fiscally relevant documents, including invoices and purchase order. Such documents would be stored for a period of time and protected using electronic signatures as required by applicable legislation or regulation. The information may be retrieved from the store when necessary and processed to provide a range of reports including VAT reports, commercial reports such as information on sales across Europe, and to provide access as needed for tax audit.

4.3 Commonly Acceptable Practices for Trusted Service Providers

In the ETSI technical report TR XXX YYY [12] the most stringent and the least stringent practices have been identified among those in effect in the five most populated EUSM for signing and storing fiscally relevant documents. Based on the same actually in use practices, the mentioned TR specifies also the "commonly acceptable practices" – CAP – for the TSPs at issue, i.e. practices which may be recognised as acceptable by authorities in several EU nations and that, therefore, may be acceptable for pan European trade.

This Technical Specification is based on the above mentioned Commonly Acceptable Practices for TSPs in a Pan European context (see figure 3).

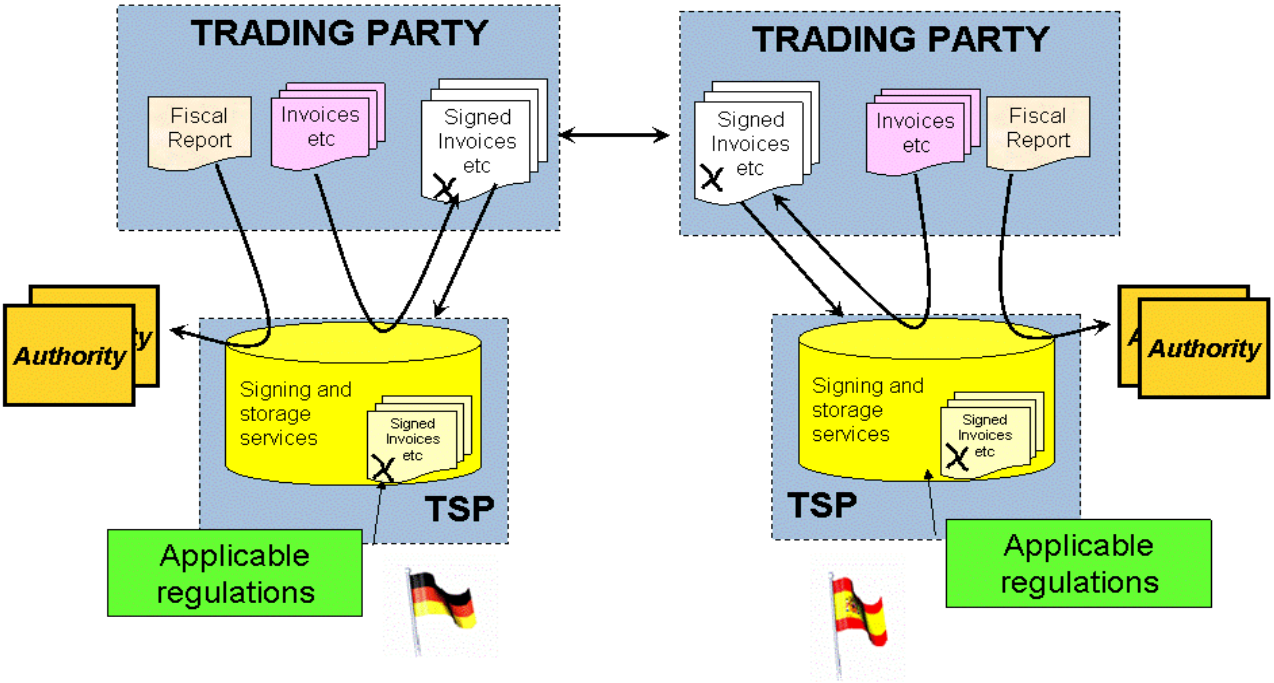

Figure 2 – Pan European Model with Trust Service Providers

4.4 Relevance to ISO/IEC 17799 to "Policy Requirements"

ISO/IEC 17799 [6] identifies the need for an information security policy to provide clear management and direction in an organisation. It is for the trust service provider to specify its information security policy. This document specifies requirements that should be addressed by the information security policy of a TSP offering signing and / or storage services for fiscally relevant documents.

The policy requirements identified in the present document are based upon the objective and control categories identified in ISO/IEC 17799 [6].

> Note: The ISO organisation is expected to substitute ISO/IEC 17799 with ISO/IEC 27002 in 2007, so it is recommended to refer to ISO/IEC 27002 when available. It is also recommended to take in the future into account the whole 2700x family, that is still under development: 27000 (principles and vocabulary), 27003 (ISMS

implementation guidelines), 27004 (information security metrics and measurements), 27005 (risk management), and other possible future ones.

This document places no requirements for the identification of a TSP's information security policy.

The information security policy of a TSP must abide by any applicable laws and regulations. In particular, a TSP shall take into account any legal requirement for the use of qualified electronic signatures employing secure signature creation devices or any legal restrictions on the holding of user's private signing key by another trusted party delegated to act on its behalf.

4.5 Normalised and Extended Policy Requirements

European Directive 1999/93/EC [10] recognises that to further strengthen Advanced Electronic Signatures "Member States may however ask for the advanced electronic signature to be based on a qualified certificate and created by a secure-signature-creation device" (i.e. Qualified Electronic Signature). Because of this, the present document identifies two classes of policy:

- one based on Advanced Electronic Signatures (referred o as "Normalised policy requirements" (N))
- the other based on "Extended Policy Requirements" (N+) extending the Normalised policy requirements the with requirements for use of Secure Signature Creation Devices and Qualified Certificates, i.e Qualified Electronic Signatures.

Where alterative choices for a particular topic these choices are indicated with paragraphs marked with [N] or [N+] as appropriate.

4.6 User Community & Applicability

These policy requirements are applicable to TSPs providing electronic signing and / or storage services applied to fiscally relevant documents including VAT invoices and reports for the purposes of VAT.

TSPs must sign documents with their own private key or, where applicable, with the taxable person's private key used by the TSP on behalf of its owner.

In addition to being applicable to independent TSPs operating in such a pan European environment these practices may also be applicable to:

- a service provider within an organisation that electronically signs and stores fiscally relevant documents on behalf of members of that organisation,
- an independent service provider serving several organisations for trade within a single country.

4.7 Conformance requirements

A TSP must demonstrate that:

a) it meets its obligations as defined in clause 5.1;

b) it has implemented controls which meet the requirements, including options applicable to the services offered by the TSP, as specified in the clauses of this Technical Specification.

Note: This may be achieved, for example, by a report from an auditor confirming also that the TSP has an Information Security Policy whose conformance to ISO/IEC 17799 [6] and to the requirements identified in the current document was verified in line with ISO/IEC 27001 [7].

5 Obligations

5.1 Trust Service Providers obligations

1. The TSP shall ensure that all the requirements as detailed in clauses 6 and 7 are implemented as applicable to the services offered.

2. The TSP has the responsibility for conformance with the procedures prescribed in this policy, even when some or all of its functionality are undertaken by sub-contractors.

3. The TSP shall provide the trust services in line with the service agreements in force offered and abiding by the applicable legislation or regulation..

4. The TSP shall obtain the necessary legal authorisations from taxable persons subscribing to its services to sign and store documents on their behalf.

   Note: this last requirement can be implemented in two different ways, that obviously depend on, and must be implemented according to, the applicable legislation or regulation:

   a) the taxable person entrusts the TSP its own signing data and the TSP will sign the fiscally relevant documents with the taxable person's signing key;

   b) the taxable person authorises the TSP to apply the TSP's signature on fiscally relevant documents in lieu of the taxable person (using a signing key assigned to the TSP) .

   The authorisation shall be drafted according to the specific case and in accordance with the applicable legislation.

5.2 Subscriber obligations

The TSP shall oblige through agreement the subscriber to address the following obligations. If the service user and subscribers are separate entities, the subscriber shall make the service user aware of these obligations applicable to the service user.

a) Ensure the accuracy and legal compliance of all fiscally relevant data or documents submitted to the TSP for subsequent issuance and/or storage of fiscally relevant documents.

b) Only submit the TSP documents in the formats which meet the requirements in the present document.

c) Submit accurate and complete information to the TSP in accordance with the requirements in its Information Security Policy, particularly with regards to registration.

d) Ensure the security of any key, security device, password or other forms of security token relating to the TSP service provision and only use them in accordance with any other limitations notified to the subscriber.

e) When accessing the TSP document storage apply security measures as notified by the TSP.

f) Take any other precautions prescribed in agreements or elsewhere.

In particular, the subscriber must agree that signatures are made with the TSP's private key or, where applicable, with the taxable person's private key used by the TSP on behalf of its owner (See item 4 of section 5.1).

5.3 Information for Trading Partner

The terms and conditions for trading partners relying on document signed by the TSP, and / or retrieving data from the TSP document storage shall include, where necessary in addition to the applicable legislation or regulation's requirements, a notice that:

a) if it is to reasonably rely upon the document, it shall verify the validity of any signed document upon delivery; this includes to:

- Verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying parties in the related CAs' Certificate Policy and /or Certificate Practice Statement; and

  NOTE 1: Depending on CA's practices and the mechanism used to provide revocation status information, there may be a delay in disseminating revocation status information. Thus, the verifier may need to await the next CRL, or even one following that, to be assured any relevant revocation request has been processed.

- Take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate itself or in the terms and conditions supplied by the certificate issuing CA;

b) it shall abide by the security measures notified by the TSP when accessing the TSP document storage.

5.4 Information for Auditor/Regulatory/Tax Authorities

Auditors, regulatory and tax authorities relying on documents signed by the TSP, and / or retrieving data from the TSP document storage, should be notified that if they are to reasonably rely upon the document, they should:

a)Verify the validity of any signed document upon delivery; this includes:

- Verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying parties in the related CA's Certificate Policy and /or Certificate Practice Statement; and

  NOTE 1: Depending on CA's practices and the mechanism used to provide revocation status information, there may be a delay in disseminating revocation status information. Thus, the verifier may need to await the next CRL, or even one following that, to be assured any relevant revocation request has been processed.

- Take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate itself or the terms and conditions supplied by the certificate issuing CA.

b) Apply security measures as notified by the TSP when accessing the TSP document storage.

6 Signature and Storage Requirements

6.1 Signature

6.1.1 Class of Electronic Signature

The TSP shall employ an electronic signature format that assures the authenticity and integrity over time of accounting data. In particular:

a) In signed fiscally relevant electronic documents the signature shall be at least an Advanced Electronic Signature, as defined in Directive 1999/93/EC [10], with the purpose of ensuring documents integrity and authenticity, as required by Directive 2001/115/EC [11].

[CONDITIONAL]

1. "[N+]" extended normalized

   The Advanced Electronic Signatures shall be created using a Secure Signature Creation Device and supported by a Qualified Certificate.

Note1: Signature formats as defined in ETSI TS 102 734 [16] and TS 102 904 [17] are recommended to maximise interoperability.

Note2: Where legally applicable, electronic signatures may also be used to provide content commitment (i.e. non repudiation).

6.1.2 Certification

The TSP shall obtain certificates from authority who can reliably certify public keys and maintain revocation status information. In particular:

b) "[CHOICE]"

1. "[N]" normalized,

   Certificates shall be issued by CAs that operate under certificate policies as per ETSI TS 102 042 [14] (NCP type) or practices that are nationally recognised as being sufficiently reliable for the purposes of signing fiscally relevant data.

2. "[N+]" extended normalized

   Qualified certificates shall be issued by CAs that operate under qualified certificate policies as per ETSI TS 101 456 [13] or practices that are nationally recognised for issuing qualified certificates.

6.1.3 Signature Creation Data

This section covers two situations :

- the TSP signs with its own key on behalf of users
- the TSP uses individual users' signing keys.

In both situations, the TSP shall ensure that the private signing key is generated and is kept secure in controlled circumstances. In particular:

a) "[CHOICE]"

1. "[N]" normalized

   Security controls shall be applied to the signing keys suitable to ensure that security is maintained over the Signature Creation Device (SCD) in line with national legal requirements. Where SCD are protected using cryptographic algorithms, this shall be in line with the guidance given in ETSI TS 102 176-1 [15] or using shared secret / secret key algorithms of equivalent strength.

2. "[N+]" extended normalized

   Where the signing key is kept in a secure signature creation device:

   a) it meets the requirements identified in one of the following CEN Workshop Agreement: CWA 14169 [1] or CWA 14167-2 / -4 [2][3], or

   b) it is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [8], or

   c) it is assured to any comparable criteria recognised in the specific EUMS.

b) Where a TSP holds keys on behalf of individual users, the TSP shall ensure that the signing key is under sole control of the owner.

c) Where a signing key held by the TSP belongs to a legal person such as a company, the TSP should ensure that signatures can be issued under control of users explicitly authorised to act for the company.

Note: Where legally allowed, signing keys may also be used by persons explicitly delegated by their owners, including the TSP

6.1.4 Certificate subject's Registration

Where TSPs apply their electronic signatures to fiscally relevant documents, they shall abide by the CA's rules that ensure the certificate holder's correct registration. In particular:

"[CHOICE]"

1. "[N]" normalized,

Subject's registration shall be performed in line with ETSI TS 102 042 [14] clause 7.3.1 or practices that are recognised as being sufficiently reliable for the purposes of signing fiscally relevant data.

2. "[N+]" extended normalized

Subject's registration shall be performed in line with ETSI TS 101 456 [13] clause 7.3.1 or practices that are recognised for issuing qualified certificate.

6.1.5 Certificate Revocation

TSP shall ensure that a certificate revocation is required by an authorised person. In particular:

a) Revocation shall be requested in a timely manner by an authorised subject, be it the certificate owner, the subscriber or another specifically authorised person, that shall also be authenticated in a manner that could encompass their electronic secure identification. The relevant CA, or its delegate, should ensure a timely requests processing and a suitable publication of the revoked certificates.

"[CHOICE]"

1. "[N]" normalized,

Certificate revocation shall be performed in line with ETSI TS 102 042 [14] clause 7.3.6 or practices that are recognised as being sufficiently reliable for the purposes of signing fiscally relevant data.

2. "[N+]" extended normalized

Subject's registration shall be performed in line with ETSI TS 101 456 [13] clause 7.3.6 or practices that are recognised for issuing qualified certificate.

6.2 Maintenance of Signature over storage period

The TSP shall ensure that the electronic signatures are maintained such that their validity can be verified for the entire storage period. In particular:

Signature verifiability shall be ensured for the entire storage period. This can be implemented by technical or organisational measures or by a combination of them as follows.

a) Technical measures

All the information required to perform the signature verification, (e.g. certificates and revocation information) and a trusted indicator (e.g. time-stamp) of the time when a valid signature existed shall be stored for the same time as the related signed document.

If the signed documents are to be stored for a period which is longer than the one for which the strength of the cryptographic algorithms employed can be assured, then additional integrity mechanisms shall be applied to the signed document and verification information. This may be achieved for example by employing archive time-stamps (such as profiled in TS 102 734 [16] or TS 101 903[17]) or maintaining the documents in write once read many (WORM) media which cannot be modified once written.

b) Organisational measures

The storage is kept by a trusted organisation, or by an organisation being recognised as applying the appropriate organisational controls, that can prove or reliably assert that before accepting the signed document its signature has been verified in accordance with generally recognised procedures,

c) Combination of technical and organisational

Where organisational measures provide an equivalent reliability, some of technical procedures might be waived.

6.3 Storage

6.3.1 Authorised Access

The TSP shall make documents securely available to the authorised parties (e.g. related Company officers, auditors, tax authority) as required by applicable legislation and practices. In particular:

a) Access shall be allowed, in addition to the related Company officials, at least to duly authorised authorities such as Tax Agency inspectors.

b) Where electronic remote access is legally required it should be implemented in a reliably secure way, so that the integrity and confidentiality of communications is protected over vulnerable networks and the parties are authenticated (e.g. user password & SSL/TLS over Internet)

6.3.2 Authenticity, Integrity and Commitment to the Content

The TSP shall maintain the authenticity of origin, integrity of content and, where applicable, commitment to the content of a set of accounting data held in storage for the legally required period. In particular :

a) An appropriate class of signature shall be used (see 6.1.1)

b) The maintenance of that signature over the storage period (see 6.2) shall be ensured.

6.3.3 Readability

The TSP shall ensure that documents remain human or machine readable over the period of storage. In particular :

a) The original document format (or, where applicable and legally valid, another suitable format reliably derived from the original) shall be ensured as readable by the storing organisation, for example by storing also the related visualising software, and where necessary the related hardware, before it becomes no more available.

b) Where there is a risk that one specific document/viewer system *is becoming* obsolete all affected documents shall be reliably copied unchanged onto another suitable document/viewer system when the older one is still available. An independent trusted assertion should attest the correspondence of the new document content to the previous one.

6.3.4 Storage media type

The TSP shall ensure that media where documents are stored can withstand the passing of time and possible support deterioration. In particular:

a) Where possible, media, as well as media readers, shall be used that can withstand the passing of the time for which storage is required. Where there is a risk that a media may become unreadable, because of technical obsolescence or physical degradation, its content shall be timely copied onto another suitable media at a frequency necessary to assure its readability.

b) Where the maintenance of signed documents depends on the integrity of the media (e.g. using WORM devices, see 6.2) any copying shall include appropriate controls to ensure the maintenance of the integrity (e.g. by employing trusted third parties) .

6.3.5 Documents Format

The TSP shall ensure that documents are kept in a format suitable to prevent changes to their presentation or to the result of automatic processing. In particular:

a) Fiscally relevant documents shall be produced in a format that prevents any change to the information represented by the document which is not detected by integrity controls, e.g. by malicious code, in macros, scripts or hidden code capable to modify the document presentation. Users should be made aware of documents that are in an unreliable format.

b) Where XML is employed it is recommended that acceptable style sheets be referenced and included in the signature calculation.

c) Fiscally relevant documents shall be stored in their original format, provided they are void of potential sources of malicious code such void of macros or hidden code.

d) Where the original format does not provide sufficient reliability in this respect, a suitable format for the same document shall be stored instead of or, optionally, in addition to the original, and a reliable assertion on the correspondence between the content of new and previous formats should be available.

6.3.6 Requirements on Separation and Confidentiality

The TSP shall ensure that electronic data from different taxable persons are stored and archived separately. In particular:

a) the storage must be clearly physically or logically separated between different owners so that the confidentiality cannot be compromised. If the storing organisation keeps fiscally relevant data related to different taxable persons the related storage or the archives must be clearly separated, e.g. by clearly marking the data with its owner and restricting access to data based on its owner, different storage areas or media, or even different storing locations.

6.4 Reporting to and Exchanges with Authorities

The TSP shall ensure that fiscally relevant documents are reported to and exchanged with authorities in such a way that their integrity and their source is secure. In particular:

a) Submission of fiscally relevant documents to Authorities should require secure channels, so that the remote user and server are authenticated, integrity and confidentiality of communications is protected over vulnerable networks.(e.g. user password & TLS over Internet).

b) To prevent subsequent corruption of the document

"[CHOICE]"

1. "[N]" normalized

   Advanced Electronic Signatures shall also be used

2. "[N+]" extended normalized

   Qualified Electronic Signatures shall also be used

c) Measures adopted in clause 6.2 shall also be provided alongside the submitted document, where possible, as a means to ensure protection against later signing certificate revocation.

6.5 Scanned Paper Originals

The TSP shall ensure that, when fiscally relevant documents originated on paper are converted into digital format, their content is preserved without any change. In particular:

a) The correspondence between paper and the derived electronic document shall be ensured as per the applicable country rules. Where these rules do not exist, a process, meeting suitable standards such as ISO/IEC 17799 [6], should ensure that the content of paper or other non-digitally encoded documents (e.g. analogic audio recordings) is not altered during their transformation to digital format.

b) Where required by the applicable country rules, or identified as necessary from the application of information security management system (e.g. ISO/IEC 17799 [6]), the copy should include an assertion (for example an electronically signed addendum to the document) on this correspondence issued by a trusted person who either carried out the scanning or later comparing the scanned version with the original. The assertion can be either explicit or implicit. The scanned document and any assertion should be signed to protect their authenticity and integrity.

7 Information Security Management

The following sections are based on ISO/IEC 17799 [6] and its certification sister standard ISO/IEC 27001 [7]. TSP's Information Security Management System shall be assessed as conformant to ISO/IEC 27001 [7] or at least be operated on the basis of ISO/IEC 17799 [6]. Information security management systems which provide equivalent assurance may be employed where allowed by applicable legislation.

7.1 Risk Analysis

Risk analysis shall be performed initially and repeated regularly to "*identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization*" (ISO/IEC 17799 [6] section 4 – Risk assessment and treatment – subsection 4.1 Assessing security risks).

7.2 Security policy

7.2.1 Information security policy

The TSP shall provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. In particular:

a) A reliable Security Policy should be in force and its knowledge and abidance should be enforced by the TSP issuing and storing fiscally relevant electronically signed documents.

b) Relevant controls specified in ISO/IEC 17799 [6] section 5.1 should be applied.

7.3 Organizing information security

7.3.1 Internal organization

The TSP shall manage information security within the organization. In particular:

a) Relevant controls specified in ISO/IEC 17799 [6] section 6.1 should be applied.

7.3.2 External Parties

The TSP shall maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties. In particular:

a) Suitable stipulations shall be in force, between service providers, that issue and store fiscally relevant electronic document on behalf of taxable persons, and the outsourcing organisation, that clearly specify the outsourcer's duties and responsibilities, covering also aspects not addressed in detail by the governing rules.

b) Relevant controls specified in ISO/IEC 17799 [6] section 6.2 should be applied.

7.4 Asset management

7.4.1 Responsibility for assets

The TSP shall achieve and maintain appropriate protection of organizational assets. In particular:

a) Relevant controls specified in ISO/IEC 17799 [6] Controls 7.1 should be applied.

7.4.2 Information classification

The TSP shall ensure that information receives an appropriate level of protection. In particular:

a) All private signing keys shall be treated as sensitive and shall be protected by special measures (see 6.1.3).

b) Fiscally relevant documents should be treated as company confidential documents unless indicated otherwise and as such only revealed to other persons as authorised by the owning company. (see also 6.3.6).

c) Relevant controls specified in ISO/IEC 17799 [6] Controls 7.2 should be applied.

7.5 Human resources security

7.5.1 Prior to employment

The TSP shall ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. In particular:

a) Personnel that will cover trusted roles should be clearly informed in writing of their duties and responsibilities and they should accept them in writing.

b) ISO/IEC 17799 [6] Controls 8.1 should be applied.

7.5.2 During employment

The TSP shall ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error. In particular:

a) Consistently with the applicable legislation and rules, TSP personnel in trusted roles, including the involved managers, shall be suitably equipped to correctly and securely perform their tasks and shall be suitably and timely educated on their task duties and informed on the consequence of their possible misbehaviour.

b) ISO/IEC 17799 [6] Controls 8.2 should be applied.

7.5.3 Termination or change of employment

The TSP shall ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner. In particular:

a) Consistently with the applicable legislation and rules, the personnel in trusted roles shall be suitably informed of their duties on confidentiality even after the termination of their working relationships, as well as on the possible consequences of non abiding by these duties.

b) For all personnel in trusted roles any Company equipment relating to this role shall be returned by the leaving employees and their privileges should be withdrawn, unless where otherwise explicitly specified.

c) ISO/IEC 17799 [6] Controls 8.3 should be applied.

7.6 Physical and environmental security

7.6.1 Secure areas

TSP shall prevent unauthorized physical access, damage, and interference to the organization’s premises and information. In particular:

a) Systems for issuing and storing fiscally relevant documents shall be located in secured areas and access to these premises should be limited to duly authorised officers, preferably in dual control regime, and logged.

b) ISO/IEC 17799 [6] Controls 9.1 should be applied.

7.6.2 Equipment

The TSP shall prevent loss, damage, theft or compromise of assets and interruption to the organization's activities. In particular:

a) Suitable measures shall be established to protect equipment relating to the TSP signing and storage services assets against equipment and information accidents and incidents, e.g. theft and damage, as well as to ensure a suitable service continuity, should be in place

b) ISO/IEC 17799 [6] Controls 9.2 should be applied.

7.7 Communications and operations management

7.7.1 Operational procedures and responsibilities

The TSP shall ensure the correct and secure operation of information processing facilities. In particular:

a) Clear and detailed procedures shall be defined for TSP trusted roles, where:

   – precise responsibilities are assigned, regarding operations and processing facilities management;

   – segregation of duties are detailed where applicable.

b) Trusted roles include at least:

   – Security Officers: Overall responsibility for administering the implementation of the security practices;

   – System Administrators: Authorized to install, configure and maintain the TSP systems relating to fiscally relevant data;

   – System Operators: Responsible for operating the TSP systems on a day to day basis. Authorized to perform system backup and recovery;

   – System Auditors: Authorized to view archives and audit logs of the TSP systems.

c) ISO/IEC 17799 [6] Controls 10.1 should be applied.

7.7.2 Third party service delivery management

The TSP shall implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements. In particular:

a) The outsourcing party shall verify that third parties providing it with services related to electronic fiscally relevant documents issuance and storage comply with all the necessary obligations. Among these measures: preliminary assessment on the provider's reliability, suitable service agreements, monitoring the provided services, on site auditing inspections, etc.

b) ISO/IEC 17799 [6] Controls 10.2 should be applied.

7.7.3 System planning and acceptance

The TSP shall minimize the risk of systems failures. In particular:

a) Fiscal electronic document issuing organisations should plan in advance their processing capacity in order to meet the peak processing periods, in particular when fiscal deadlines approach, and to keep their commitments regarding the amount of documents to keep for the expected time.

Note: Requirements relating to availability of the service would be addressed by a Service Level Agreement.

b) ISO/IEC 17799 [6] Controls 10.3 should be applied.

Note: This capacity planning could be assessed by balancing cost of system implementation, legal penalty clauses, insurance policies price, loss of image and loss of customer base.

7.7.4 Protection against malicious and mobile code

The TSP shall protect the integrity of software and information. In particular:

a) ISO/IEC 17799 [6] Controls 10.4 should be applied.

Note: See section 6.3.5 regarding requirements relating to malicious code in documents.

7.7.5 Back-up

The TSP shall maintain the integrity and availability of information and information processing facilities and fiscally relevant electronic documents exhibition requirements shall be fulfilled even in case of accidents affecting their main site(s)

In particular:

a) This should imply arranging suitably built and equipped back-up storage sites and for a recovery plan to be put into operation when necessary.

Note: The sizing of this backup management system might likely be a balance between the cost of its implementation, the fines and penalties to be applied in case of impossibility to exhibit the required documents, as well as the cost affecting intangible assets like the company image, and the related insurance policy cost and benefits.

b) ISO/IEC 17799 [6] Controls 10.5 should be applied.

7.7.6 Network security management

The TSP shall ensure the protection of information in networks and the protection of the supporting infrastructure. In particular:

a) Networks regarding fiscal documents issuance and storage shall be protected to ensure that neither unauthorised data are inserted to or deleted from the document issuing, or storing, process, nor any confidential information is disclosed.

b) ISO/IEC 17799 [6] Controls 10.6 should be applied.

7.7.7 Media handling

The TSP shall prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities. In particular:

a) Media protection shall be enforced during their entire handling process to ensure integrity and confidentiality of company data and keys up to and including their authorised disposal.

b) ISO/IEC 17799 [6] Controls 10.7 should be applied.

7.7.8 Exchange of information

The TSP shall maintain the security of information and software exchanged within an organization and with any external entity. In particular:

a) ISO/IEC 17799 [6] Controls 10.8 should be applied.

Note: See section 6.4 regarding protection of information when reporting.

7.7.9 Electronic commerce services

The TSP shall ensure the security of electronic commerce services, and their secure use. In particular:

a) ISO/IEC 17799 [6] Controls 10.9 should be applied.

Note: This clause applies when the TSP manages the electronic commerce on behalf of its customers (i.e. of the taxable persons it is acting on behalf of), and handles the electronic commerce information flow between this person and its counterparts.

7.7.10 Monitoring

The TSP shall detect unauthorized information processing activities. In particular:

a) ISO/IEC 17799 [6] Controls 10.10 should be applied.

Note: Suitable auditing/monitoring is paramount for a trusted organisation.

7.8 Access control

7.8.1 Business requirement for access control

The TSP shall control access to information. In particular:

a) ISO/IEC 17799 [6] Controls 11.1 should be applied.

7.8.2 User access management

The TSP shall ensure authorized user access and shall prevent unauthorized access to information systems. In particular:

a) ISO/IEC 17799 [6] Controls 11.2 should be applied.

Note: See 6.3.1 regarding authorised access to storage.

7.8.3 User responsibilities

The TSP shall prevent unauthorized user access, and compromise or theft of information and information processing facilities. In particular:

a) External and internal authorised users shall be made aware in writing both of their responsibilities and of the need for their cooperation to prevent unauthorized accesses. Where applicable a clean desk policy shall be carefully enforced within the TSP premises.

b) ISO/IEC 17799 [6] Controls 11.3 should be applied.

7.8.4 Network access control

The TSP shall prevent unauthorized access to networked services. In particular:

a) ISO/IEC 17799 [6] Controls 11.4 should be applied.

Note: See 6.3.1 regarding authorised access.

7.8.5 Operating system access control

The TSP shall prevent unauthorized access to operating systems. In particular:

a) Logs shall be suitably protected and inspected.

b) ISO/IEC 17799 [6] Controls 11.5 should be applied.

Note: See 6.3.1 regarding authorised access.

7.8.6 Application and information access control

The TSP shall prevent unauthorized access to information held in application systems. In particular:

a) ISO/IEC 17799 [6] Controls 11.6.1 should be applied for storage, and Controls 11.6.2 should be applied for signing keys.

7.8.7 Mobile computing and teleworking

The TPS shall ensure information security when using mobile computing and teleworking facilities. In particular:

a) ISO/IEC 17799 [6] Controls 11.7 should be applied.

7.9 Information systems acquisition, development and maintenance

7.9.1 Security requirements of information systems

The TSP shall ensure that security is an integral part of information systems. In particular:

a) ISO/IEC 17799 [6] Controls 12.1 should be applied.

7.9.2 Correct processing in applications

The TSP shall prevent errors, loss, unauthorized modification or misuse of information in applications. In particular:

a) Strict controls shall be implemented to procedures for signing and storing fiscally relevant documents, including bulk signing

Note: Severe consequence would have if such application procedures have fraudulent coding, as well as errors, that issue, or store, unexpected documents or document the presentation of which might change after their issuance.

b) ISO/IEC 17799 [6] Controls 12.2 should be applied.

7.9.3 Cryptographic controls

The TSP shall protect the confidentiality, authenticity or integrity of information by cryptographic means. In particular:

a) In countries where sensitive data protection, as addressed by Directive 95/46/EC [9], requires encryption, key management should be enforced in addition to what is usually required for signing.

b) Provisions in ISO/IEC 17799 [6] section 12.3 should be applied.

7.9.4 Security of system files

The TSP shall ensure the security of system files. In particular:

a) ISO/IEC 17799 [6] Controls in 12.4 should be applied.

7.9.5 Security in development and support processes

The TSP shall maintain the security of application system software and information. In particular:

a) The software should be developed, tested and installed under clearly defined quality assurance procedures.

b) ISO/IEC 17799 [6] Controls 12.5 should be applied.

7.9.6 Technical vulnerability management

The TSP shall reduce risks resulting from exploitation of published technical vulnerabilities. In particular:

a) ISO/IEC 17799 [6] Control 12.6 should be applied

7.10 Information security incident management

7.10.1 Reporting information security events and weaknesses

The TSP shall ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. In particular:

a) ISO/IEC 17799 [6] Controls 13.1 should be applied.

7.10.2 Management of information security incidents and improvements

The TSP shall ensure a consistent and effective approach is applied to the management of information security incidents. In particular:

a) ISO/IEC 17799 [6] Controls 13.2 should be applied.

7.11 Business continuity management

7.11.1 Information security aspects of business continuity management

The TSP shall counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. In particular:

a) ISO/IEC 17799 [6] Controls 14.1 should be applied.

Note: Requirements relating to Business Continuity of the service should be addressed by a Service Level Agreement.

7.12 Compliance

7.12.1 Compliance with legal requirements

The TSP shall avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. In particular:

a) Where cross border document validity is sought for, it may be necessary to abide by all involved countries legislation/regulations.

b) ISO/IEC 17799 [6] Controls 15.1 should be applied.

7.12.2 Compliance with security policies and standards and technical compliance

The TSP shall ensure compliance of systems with organizational security policies and standards. In particular:

a) Security Policy compliance shall be met.

b) ISO/IEC 17799 [6] Controls 15.2 should be applied.

Note: Where legislations/regulations are applicable, they prevail, but the ISO/IEC 17799 [6] provisions should be also used to fill in the possible gap.

7.12.3 Information systems audit considerations

The TSP shall maximize the effectiveness of and to minimize interference to/from the information systems audit process. In particular:

a) Even where no specific legal requirement exists in this regard, an appropriate auditing process shall be in place.

b) ISO/IEC 17799 [6] Controls 15.3.1 to 15.3.2 should be applied.

History

Document history		
V 0.0.1	November 2006	ESI Internal draft
V.0.0.2	Dec 2006	Review Draft