ETSI TS 102 573 V2.1.1 (2012-04)

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

Reference
RTS/ESI-00124

Keywords
data preservation, e-commerce, electronic signature, provider, 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

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://ipr.etsi.org).

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 data object.

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 data object, and with the application of good practices can prove more secure and robust than the use of paper. The key issue is ensuring integrity, authenticity and legibility to preserved data objects throughout the entire storage period.

This issue is particularly relevant to the case where the data object owner resorts to a Data Preservation Service Provider (DPSP) since, especially when fiscal accounts are involved, the owner is in any case responsible towards the law of the preserved data, regardless that the actual preservation is in charge of a service provider. Therefore for the owner choosing a reliable Service Provider is of paramount importance.

Within the scope of the EU Community legislation on consumer protection, EU Services Directive 2006/123/EC [i.1], article 26 requires EUMS to "take accompanying measures to encourage providers to take action on a voluntary basis in order to ensure the quality of service provision". This will be accomplished through certification, independent assessment or compliance with quality charters.

It is to be noted too that, if a DPSP bases its services on electronic signatures, its certification/assessment is also consistent with Directive 1999/93/EC [8] that, at art. 3(2), allows Member States to "introduce or maintain voluntary accreditation schemes aiming at enhanced levels of **certification-service provision**". Art. 2(11) of this Directive defines: ""certification-service-provider" means an entity or a legal or natural person who issues certificates **or provides other services related to electronic signatures**". What these services are, is clarified in Whereas (9) that reads: "…the definition of such … services … ***should also encompass any other service and product using, or ancillary to, electronic signatures***…". Therefore DPSPs, providing services based on electronic signatures, are Certification Service Providers.

The present document, consistently with the Services Directive goals, specifies policy requirements that anyone who archives data objects, on his own account or as a provision of services to his customers, may comply with. Such policy requirements complement the number of archival related standards and specifications with provisions on Information Security Management related to Storage Systems. These requirements apply to fiscally relevant data objects storage.

The technical format of the data to be preserved as well as the process of the signature creation are of importance for ensuring authenticity and integrity to the data object, therefore some European national governments regulate practices for achieving this goal through use of electronic signatures and of data formats that are not vulnerable to changes in presentation through malicious code. It would be welcome if these EU Member States also adopt a common policy for data objects storage, based for example on matching the policy requirements specified in the present document, thus facilitating the development of a EU-wide market for this kind of services.

The present document is based on the findings presented in TR 102 572 [i.2] and addresses policy requirements by both natural/legal persons that perform data objects storage on their own behalf as well as on behalf of other natural/legal persons.

1 Scope

The present document specifies policy requirements applicable to Trusted Service Providers (TSP) that electronically sign and/or store data objects on behalf of their customers. These policy requirements may also be complied with by persons that store data objects on their own. The present document aims to address regulatory requirements to produce and reliably keep, even indefinitely, electronic data objects, where applicable also signed. The practices identified in the present document are independent of the type of data object being preserved, although peculiar requirements for fiscally relevant ones are also specified.

The present 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 assure the integrity and the authenticity of origin of data objects in communication and storage. However, signatures may also be used, where required, to provide content commitment (i.e. non-repudiation).

The present document addresses solely the Advanced Electronic Signature based solutions. It is recognized that other suitable measures, not employing Advanced Electronic Signatures, and hence that are outside the scope of the present document, may be applied to assure the authenticity and integrity of digital data objects. It should be noted that the reliability of such alternative measures generally depend on the trustworthiness of the organization, on the exhaustiveness of the adopted practices and procedures and may require independent assessment of the technical and organizational measures applied. Advanced Electronic Signatures may be used to augment existing measures to provide even higher security, or to reduce the need for other controls. This fits particularly art. 233 of EU VAT Directive 2006/112/EC [9] as amended by 2010/45/EU.

The present document may be used by competent independent bodies as the basis for confirming that an organization is trustworthy in issuing and storing signed electronic data object on behalf of other persons or on its own behalf.

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

Within the present document the key words "should" indicates that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications need to be understood and carefully weighed before choosing a different course.

Guidance on implementing a trustworthy Data object Preservation System can be found in TS 101 533-1 [i.3]. Guidance on assessing Data object Preservation Systems can be found in TR 101 533-2 [i.4].

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

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

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] CEN CWA 14169: "Secure signature-creation devices "EAL 4+"".

NOTE: http://www.cenorm.be/catweb/35.040.htm.

[2] CEN CWA 15579: "E-invoices and digital signatures".

NOTE: http://www.cenorm.be/isss/einv.

[3] CEN CWA 15580: "Storage of Electronic Invoices".

NOTE: http://www.cenorm.be/isss/einv.

[4] ISO/IEC 27002: "Information technology - Security techniques - Code of practice for information security management".

[5] ISO/IEC 27001: "Information technology - Security techniques - Information security management systems - Requirements".

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

[7] 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.

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

[9] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax, as amended by Council Directive 2010/45/EU of 13 July 2010.

[10] 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.

[11] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[12] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

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

[14] ETSI TS 102 734: "Electronic Signatures and Infrastructures; Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES)".

[15] ETSI TS 102 904: "Electronic Signatures and Infrastructures; Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES)".

[16] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[17] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[18] CEN CWA 14170: "Security requirements for signature creation applications".

[19] ETSI TS 102 778: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles".

[20] ETSI TS 102 918: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

[i.2] ETSI TR 102 572: "Best Practices for handling electronic signatures and signed data for digital accounting".

[i.3] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".

[i.4] ETSI TR 101 533-2: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 2: Guidelines for Assessors".

3 Definitions and abbreviations

3.1 Definitions

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

advanced electronic signature: 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 [8])

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

electronic invoices: invoices sent by electronic means as defined in Directive 2006/112/EC [9]

extended policy requirements: extended variant of the normalized policy requirements employing a secure signature creation device and Qualified Certificate (i.e. qualified 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 data object: data object or record containing fiscally relevant data

normalized policy requirements: policy requirement which offers a quality of service equivalent to the one defined in Directive 1999/93/EC [8], in particular employing advanced electronic signatures as defined in article 2 No 2 of this Directive

qualified electronic signature: advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device (Directive 1999/93/EC [8])

qualified certificate: certificate which meets the requirements laid down in annex I (of the Directive 1999/93/EC [8]) and is provided by a certification-service-provider who fulfils the requirements laid down in annex II (of the Directive 1999/93/EC [8])

secure signature creation device: signature-creation device which meets the requirements laid down in annex III of Directive 1999/93/EC [8]

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 [8])

statement of applicability: data objected statement describing the control objectives and controls that are relevant and applicable to the TSP's ISMS (ISO/IEC 27001 [5])

trading partner: taxable person that has trading relationships with the TSP's services user and with which legally relevant data objects, including fiscally relevant ones, are exchanged

3.2 Abbreviations

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

AdES	Advanced Electronic Signature
CA	Certification Authority
CAP	Commonly Acceptable Practices
CEN	Comité Européen de Normalisation
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
CWA	CEN Workshop Agreement
DPSP	Data Preservation Service Provider
EAL	Evaluation Assurance Level
EU	European Union
EUMS	European Union Member State
ISMS	Information Security Management System
ISO	International Organization for Standardization
N	Normalized policy requirements
NCP	Normalized Certificate Policy
QES	Qualified Electronic Signature
TLS	Transport Layer Security
TSP	Trusted Service Provider
VAT	Value Added Tax
WORM	Write Once Read Many
WWW	World Wide Web
XBRL	eXtensible Business Reporting Language
XML	eXtensible Mark-up Language

4 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]" normalized 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 marking them with "[CHOICE]" with a subsequent indicator relating to the relative quality:

   "[N]" normalized policy requirements;

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

5 General concepts

5.1 ISO/IEC 27001 ISMS and "Policy Requirements"

The present document specifies requirements on the information security policy in terms of security objectives and controls as specified in ISO/IEC 27002 [4] and ISO/IEC 27001 [5], annex A, for a Trust Service Provider (TSP) supporting signing and storing data objects. The present document also identifies additional objectives and controls specifically meeting the potential risks associated with signing and/or storing fiscally relevant data objects. These controls are applied by the TSP as identified through a risk analysis as being relevant and applicable to that TSP.

ISO/IEC 27001 [5] specifies requirements on an Information Security Management System that can be used to apply the controls as appropriate. The present document requires that an ISO/IEC 27001 [5] conformant ISMS or recognized alternative be used to ensure that the appropriate controls are applied (see clause 4.7).

The present 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.

5.2 Fiscally Relevant Provisions

5.2.1 Fiscally Relevant Data objects

Among the number of fiscally relevant data objects types addressed, across the European Union Member States, by general commercial legislation, national tax legislation, requirements for monitoring accounting in governmental organizations, the present data object refers to those that specific TSPs issue, by applying them legally valid electronic signatures, and store for the required time period. These data objects 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 harmonization of legislation, that is VAT related Invoicing. The amended European Directive 2006/112/EC [9], in fact, envisages the possibility, among others, to use "advanced electronic signatures", be they AdES or QES, to ensure "the authenticity of the origin, the integrity of the content and the legibility of an invoice", even when issued across borders. This was further defined in CEN workshops on electronic invoicing which published a number of data objects, among which guidelines for both the storage of electronic invoices (CWA 15580 [3]) and the application of advanced electronic signatures to electronic invoicing (CWA 15579 [2]).

The present document specifies policies for the storage and signing that may be applicable to the entire range of data objects, including fiscally relevant ones, that may be employed across Europe. These policies apply to the storage and signing of electronic invoices too as identified in European Directive 2006/112/EC [9] as illustrated in figure 1.

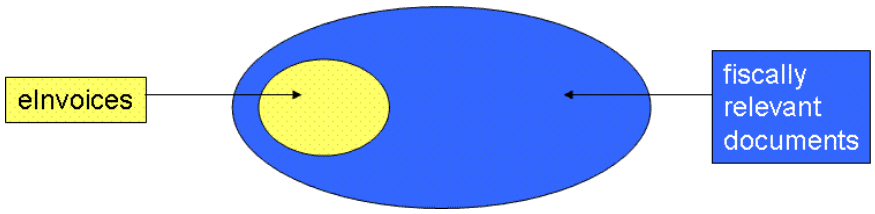

Figure 1: E-invoices as a representative sub-class of fiscally relevant data objects

5.2.2 Basic Model for Fiscally Relevant Data Objects

The general application of signing and storage services also to fiscally relevant data objects is illustrated in figure 2.

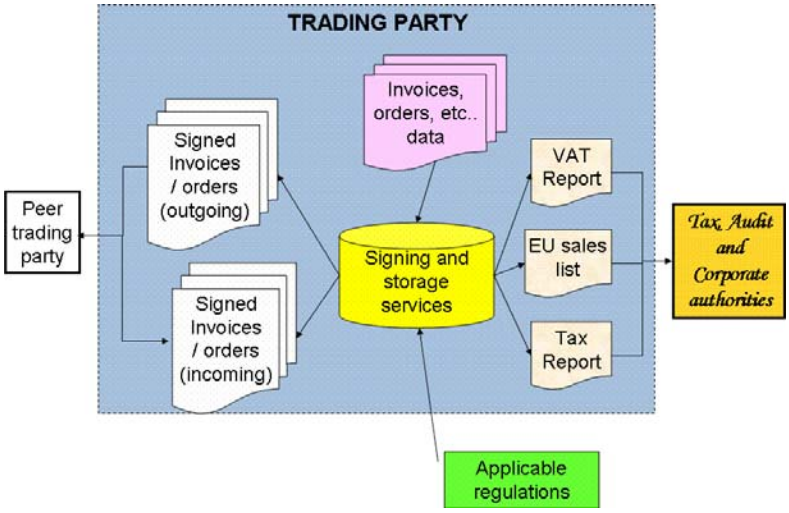

Figure 2: Basic Model

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

5.2.3 Commonly Acceptable Practices for Trusted Service Providers

In TR 102 572 [i.2] the most stringent and the least stringent practices have been identified among those in effect under then in force Directive 2001/115/EC [10] in the five most populated EUMS for signing and storing fiscally relevant data objects. 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 recognized as acceptable by authorities in several EU nations and that, therefore, may be acceptable for pan European trade.

The present document, whilst addressing all kind of documents and not only fiscally relevant ones, is based on the above mentioned Commonly Acceptable Practices for TSPs in a Pan European context (see figure 3).

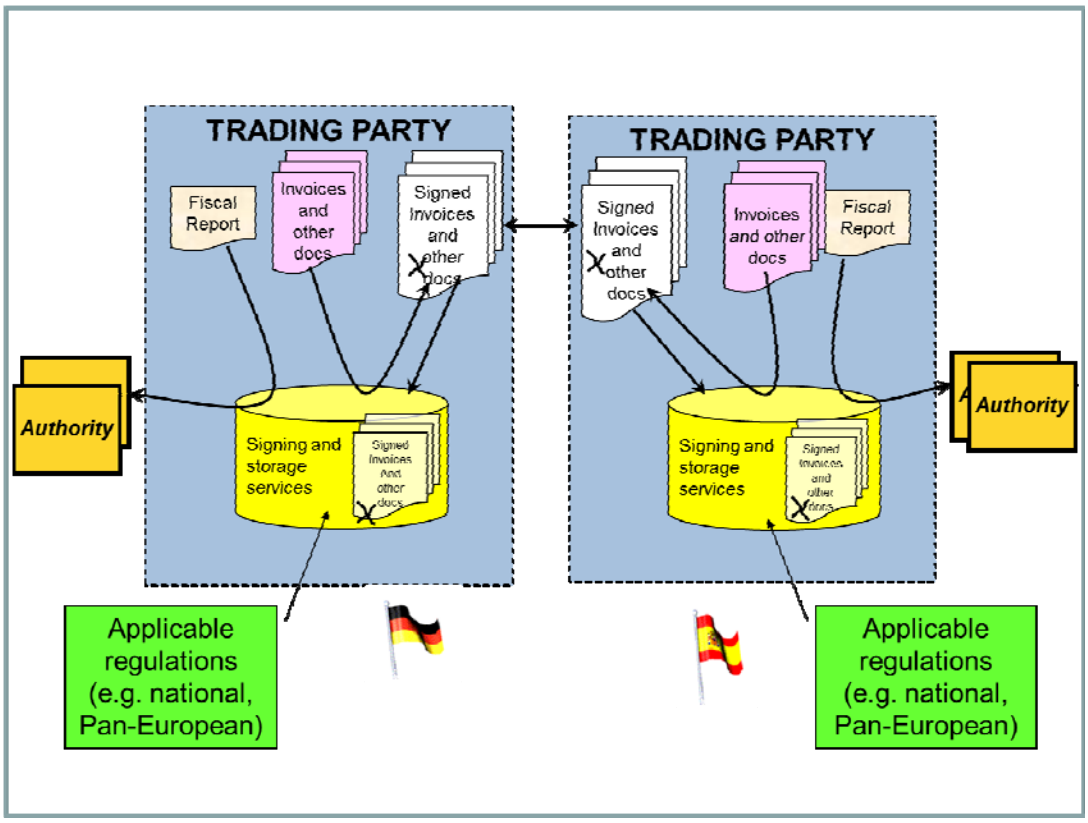

Figure 3: Pan European Model with Trust Service Providers

European Directive 2006/112/EC as amended by Directive 2010/45/EU [9] states at art. 233 that "Each taxable person shall determine the way to ensure the authenticity of the origin, the integrity of the content and the legibility of the invoice", and specifies, just as an example of "technologies that ensure the authenticity of the origin and the integrity of the content of an electronic invoice", the usage of "an advanced electronic signature" "based on a qualified certificate and created by a secure signature creation device". More: art. 273 of such Directive denies EUMS the right to "impose additional invoicing obligations over and above those laid down in chapter 3 [of Title XI: Obligations of Taxable Persons and certain Nontaxable Persons]". It is worth clarifying that art. 233 belongs to the mentioned chapter 3. In other words: no EUMS cannot impose that E-invoices must abide solely by certain requirements, having the taxable person full freedom of choice.

As a consequence no EUMS may impose electronic signatures as the sole mechanism accepted to ensure authenticity and integrity to electronic invoices.

5.3 Normalized and Extended Policy Requirements

The present document identifies two classes of policy related to adoption of AdES:

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

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

5.4 User Community and Applicability

These policy requirements are applicable to TSPs providing electronic signing and/or storage services. Although the practices identified in this report are independent of the type of data object being protected, they apply also to services supporting fiscally relevant data objects including VAT invoices and reports for the purposes of VAT.

TSPs must sign data objects with their own private key or, where applicable, with its customer'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:

- an organization that electronically signs and stores data objects for itself;
- an independent service provider serving several organizations.

5.5 Conformance requirements

A TSP must demonstrate, in line with its statement of applicability and with the legal requirements, that:

a) it meets its obligations as defined in clause 6.1;

b) it meets the organizational requirements defined in clause 6.2;

c) it provided its trading partners and Auditor/Regulatory/Tax Authorities with the data object respectively specified in clauses 6.4 and 6.5, where applicable;

d) it has implemented controls which meet the requirements as specified in annexes A and B.

This shall be demonstrated through the implementation of an ISMS that meets the requirements of ISO/IEC 27001 [5] or a system recognized (legally or through accepted best practice) as providing sufficient assurance for the purposes of signing and storing fiscally relevant data objects.

The TSP shall prepare a Statement of Applicability that includes the following:

a) the control objectives and controls and the reasons for their selection;

b) the control objectives and controls currently implemented; and

c) the exclusion of any control objectives and controls identified in the current document and the justification for their exclusion.

6 Obligations

6.1 Trust service providers obligations

1) The TSP shall ensure that all the requirements as detailed in annexes A and B 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 functionalities 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 authorizations from persons subscribing to its services to sign and/or store data objects on their behalf.

NOTE: This last requirement can be implemented in two different ways, that obviously depend on applicable legislation or regulation:

a) persons entrust the TSP their own signing data and the TSP will sign the data objects with one person's signing key;

b) persons authorize the TSP to apply the TSP's signature on data objects in lieu of the persons themselves (using a signing key assigned to the TSP).

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

This may not be applicable where one organization signs and/or stores fiscal data object for itself.

6.2 Trust service providers organizational requirements

The TSP shall ensure that its organization is reliable, i.e. that it will meet the provisions of the agreement(s) it has in force with specific taxable persons, in compliance the present document, regarding:

a) issuing in the name and on behalf of such taxable persons all the data objects as specified in such agreement(s);

b) electronically keep the issued data objects as specified in such agreement(s).

In particular that:

TSP general

1) the TSP is a legal entity according to the applicable law;

2) the TSP has adequate arrangements to cover liabilities arising from its operations and/or activities;

3) the TSP has the financial stability and resources required to provide the services as specified in the present document;

4) the TSP has the financial stability and resources required to seamlessly pass, directly or through the data objects owners, the provisioning of the service as specified in the present document to other suitably reliable TSPs, in case of discontinuation of the agreement(s) with the related customer, whatever is the reason of such discontinuation;

5) the TSP has policies and procedures for the resolution of complaints and disputes received from customers or other parties about the provisioning of the services, specified in the present data object, defined in the agreement(s) it has in force with specific customer;

6) the TSP has a properly data objected agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements;

7) where the TSP subcontracts or outsources the services, as specified in the present document, addressed in the agreement(s) with specific customers, these agreements shall clearly indicate what, and how, services are totally or partly subcontracted or outsourced and to which organization.

Issuance and storage of digitally signed fiscally relevant data objects

8) the parts of the TSP concerned with issuance and storage of electronically signed data objects shall be independent of other organizations, or of other parts of the same organization, for their decisions relating to the establishing, provisioning and maintaining and suspending of services; in particular its senior executive, senior staff and staff in trusted roles, must be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides;

9) the parts of the TSP concerned with issuance and storage of electronically signed data objects shall have a documented structure which safeguards impartiality of operations.

6.3 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 data objects submitted to the TSP for subsequent issuance and/or storage of data objects.

b) Only submit the TSP data objects in the formats which meet the requirements in the present document (refer to SS.3.5 in table A.1 of annex A).

c) Submit accurate and complete data object 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 data object 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 service user's private key used by the TSP on behalf of its owner (see item 4 of clause 5.1).

6.4 Information for trading partner

The terms and conditions for trading partners relying on data object signed by the TSP, and/or retrieving data from the TSP data object 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 data object, it shall verify the validity of any signed data object 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: 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 data object storage.

6.5 Information for auditor/regulatory/tax authorities

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

a) verify the validity of any signed data object 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: 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 data object storage.

Annex A (normative): Objectives and controls - signature and storage

Table A.1

SS.1. Signature

SS.1.1. Class of Electronic Signature

Objective: To employ a class of electronic signature that assures the authenticity and integrity, and where applicable commitment to content, over the lifetime of individual fiscally relevant data objects.

SS.1.1.1 If electronic data objects are signed, the signature shall be at least an Advanced Electronic Signature, as defined in Directive 1999/93/EC [8], with the purpose of ensuring data objects integrity and authenticity, as required by Directive 2006/112/EC [9].

[CONDITIONAL]

1) "[N+]" extended normalized

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

NOTE 1: Signature formats as defined in TS 102 734 [14] (which profiles TS 101 733 [16]) and TS 102 904 [15] (which profiles TS 101 903 [17]) are recommended to maximize interoperability. Should these profiles not fully satisfy specific application requirements, use of more general formats defined in TS 101 733 [16] and TS 101 903 [17] is recommended. Alternative signature formats can be used such as in TS 102 778 [19] (PDF signatures) or in TS 102 918 (Associated Signature Containers) [20].

NOTE 2: Where applicable, electronic signatures may also be used to provide content commitment (i.e. non repudiation).

SS.1.2. Certification

Objective: To obtain certificates from authority who can reliably certify public keys and maintain revocation status data object.

SS.1.2.1 Electronically signed fiscally relevant data objects shall be supported by:

"[CHOICE]"

1) "[N]" normalized

Certificates issued by CAs that operate under certificate policies as per TS 102 042 [12] (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 issued by CAs that operate under qualified certificate policies as per TS 101 456 [11] or practices that are nationally recognized for issuing qualified certificates.

SS.1.3. Signature Creation Data

Objective: To ensure that the private signing key is generated and is kept secure in controlled circumstances in the two following situations:

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

SS.1.3.1 "[CHOICE]"

1) "[N]" normalized

   Security controls shall be applied to the signing keys suitable to ensure that security is maintained over the private signing key in line with national legal requirements. Where signing keys are protected using cryptographic algorithms, this shall be in line with the guidance given in TS 102 176-1 [13] 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 the CWA 14169 [1]; or

   b) it is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [6]; or

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

SS.1.3.2 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.

SS.1.3.3 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 only under control of users explicitly authorized 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.

SS.1.4. Certificate subject's Registration

Objective: To ensure the certificate holder's correct registration.

SS.1.4.1 "[CHOICE]"

1) "[N]" normalized

   Subject's registration shall be performed in line with TS 102 042 [12], clause 7.3.1 or practices that are recognized 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 TS 101 456 [11], clause 7.3.1 or practices that are recognized for issuing qualified certificate.

SS.1.5. Certificate Revocation

Objective: To ensure that when required only authorized persons can request revocation of a certificate and that this revocation is carried out in a timely manner.

SS.1.5.1 Revocation shall be requested in a timely manner by an authorized subject, be it the certificate owner, the subscriber or another specifically authorized person, that should 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 status of revoked certificates (e.g. CRL).

"[CHOICE]"

1) "[N]" normalized

   Certificate revocation shall be performed in line with TS 102 042 [12], clause 7.3.6 or practices that are recognized as being sufficiently reliable for the purposes of signing data objects.

2) "[N+]" extended normalized

   Certificate revocation shall be performed in line with TS 101 456 [11], clause 7.3.6 or practices that are recognized for issuing qualified certificate.

SS.2. Maintenance of Signature over storage period

Objective: To ensure that the electronic signatures are maintained such that their validity can be verified for the entire storage period.

SS.2.1 Signature verifiability shall be ensured for the entire storage period. This can be implemented by technical or organizational measures or by a combination of them as follows.

a) Technical measures

   All the information required to perform the signature verification, (e.g. certificate path from a known trust point, e.g. root CA and revocation information), and a trusted indicator (e.g. time-stamp) of the time when that signature existed and was valid shall be stored for the same time as the related signed data object and in a manner that preserves the integrity of this set of information as required in SS.3.2.

   If the signed data objects 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 data object and verification information. This may be achieved for example by employing archive time-stamps (such as profiled in TS 102 734 [14] or TS 102 904 [15]) or maintaining the data objects in write once read many (WORM) media which cannot be modified once written, provided they are properly managed to prevent damages and to ensure data recovery.

b) Organizational measures

   The storage is kept by a trusted organization, or by an organization being recognized as applying the appropriate organizational controls, that can prove or reliably assert that before accepting the signed data object its signature has been verified in accordance with generally recognized procedures.

c) Combination of technical and organizational

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

SS.3. Storage

SS.3.1. Authorized Access

Objective: To make data objects securely available to the authorized parties (e.g. related Company officers, auditors, tax authority) as required by applicable legislation and practices.

SS.3.1.1 Access shall be allowed, in addition to the related Company officials, at least to duly authorized authorities such as Tax Agency inspectors.

SS.3.1.2 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). Where the applicable legislation lays down the electronic remote access characteristics, they shall be complied with.

SS.3.2. Authenticity and Integrity

Objective: To maintain the authenticity of origin and integrity of a set of data objects, also preventing loss or surreptitious addition of data objects, held in storage for the legally required period.

SS.3.2.1 An appropriate class of signature shall be used (see SS.1.1.).

SS.3.2.2 The maintenance of that signature over the storage period (see SS.2.) shall be ensured.

SS.3.2.3 Mechanisms to detect loss or surreptitious addition of data objects shall be used.

SS.3.3. Readability

Objective: To ensure that data objects remain human or machine readable over the period of storage.

SS.3.3.1 The original data object format (or, where applicable and legally valid, another suitable format reliably derived from the original) shall be ensured as readable by the storing organization, for example by storing also the related visualising software, and where necessary the related hardware, before it becomes no more available.

SS.3.3.2 Where there is a risk that one specific data object/viewer system *is becoming* obsolete all affected data objects shall be reliably copied keeping their semantics unchanged onto another suitable data object/viewer system while the older one is still available. An independent trusted assertion should attest the correspondence of the new data object content and semantics to the previous one.

SS.3.4. Storage media type

Objective: To ensure that media where data objects are stored can withstand the passing of time and possible support deterioration.

SS.3.4.1 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.

Where the maintenance of signed data objects depends on the integrity of the media (e.g. using WORM devices, see SS.2.1) any copying shall include appropriate controls to ensure the maintenance of the integrity (e.g. by employing trusted third parties).

SS.3.5. Data objects Format

Objective: To ensure that data objects are kept in a format suitable to prevent changes to their presentation or to the result of automatic processing.

SS.3.5.1 Data objects shall be produced in a format that prevents any change to their presentation which is not detected by integrity controls (as described in SS.3.2), e.g. by malicious code, in macros, scripts or hidden code capable to modify the data object presentation. Users should be notified when data objects that are in an unreliable format (please refer to section 8.6 of CWA 14170 [18]).

SS.3.5.2 Where XML is employed either acceptable style sheets shall be referenced and included in the signature calculation, or a standard syntax with fully defined semantics (e.g. XBRL) shall be employed.

SS.3.5.3 Data objects shall be stored in their original format, provided they are void of potential sources of malicious code such as macros or hidden code.

SS.3.5.4 Where the original format does not provide sufficient reliability in this respect, the data object shall be stored in a suitable format 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.

SS.3.6. Requirements on Separation and Confidentiality

Objective: To ensure that electronic data objects related to different owner organizations are stored and archived separately.

SS.3.6.1 The storage must be clearly physically or logically separated between different owners so that the confidentiality cannot be compromised. If the storing organization keeps data objects related to different persons the related storage or the archives must be clearly separated, e.g. by clearly marking the data with its owner's identifier and restricting access to data based on its owner, different storage areas or media, or even different storing locations.

SS.4. Reporting to and Exchanges with Authorities

Objective: To ensure that data objects are reported to and exchanged with authorities in such a way that their integrity and their source is secure.

NOTE: In accordance with the applicable law, any submission is generally the responsibility of the data object owner and so any submission should be authorized by such person.

SS.4.1 Submission of data objects 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). Where the applicable legislation specifies ways to secure these channels, these ways shall be complied with.

SS.4.2 To prevent subsequent corruption of the data object to go unnoticed:

"[CHOICE]"

1) "[N]" normalized

   Advanced Electronic Signatures shall also be used.

2) "[N+]" extended normalized

   Qualified Electronic Signatures shall also be used.

SS.4.3 Controls identified in objective SS.2. shall also be provided alongside the submitted data object, where possible and necessary, as a means to ensure protection against later signing certificate revocation or certificate expiry inappropriately making old signatures invalid.

NOTE: This is not necessary if the certificate revocation authority does not remove information on revoked certificates upon certificates expiration and the data object storage period does not exceed the validity period of the algorithms used by this authority. In the latter case alternative measures should be adopted to create a seamless verification path.

SS.5. Conversion of Analog Originals to Digital Formats

Objective: To ensure that, when data objects originally in analog, i.e. non-digitally encoded, formats (e.g. paper, audio, microfiche) are converted into digital format, their content is preserved without any change.

SS.5.1 The correspondence between data objects in non-digital formats and their corresponding digital image (e.g. scanned copies) should be ensured. Where these rules do not exist, a process, in line with best practice such as ISO/IEC 27002 [4] or, where applicable, assessed per ISO/IEC 27001 [5], should ensure that the content of non-digitally encoded data objects (e.g. analog audio recordings) matches the corresponding digital image.

SS.5.2 Where identified as necessary from the application of information security management system (e.g. ISO/IEC 27002 [4] or ISO/IEC 27001 [5]), the digital version of non-digitally encoded data object should be physically or logically associated with an assertion (for example an electronically signed addendum to the data object) on this correspondence issued by a trusted person who, for example, either carried out the scanning or later compared the consistently matched by their corresponding with the original. The assertion can be either explicit (see note below) or implicit. The paper or other non-digitally encoded data object digital image and any assertion should be signed to protect their authenticity and integrity.

NOTE: An explicit statement may just certify the outcome of the digitalization process (i.e. the conformity of the digital file to the non-digitally encoded originals); or it may also provide details of the digitalization process, for example:

i) an inventory of the data objects delivered for digitalization;

ii) the verification of their physical integrity and readability;

iii) the description of the files generated by the digitalization process and their relation to the analog data objects;

iv) the description of the outcome of the signature creation process of the files generated by the digitalization process;

v) a description of the delivery and/or storage technique of such digital files.

The description of the digitalization process should be given in a way that enables the relying parties to identify the weaknesses of the process, instead of disguising them.

Annex B (normative): Objectives and controls - information security management

The objectives and controls as stated in ISO/IEC 27001 [5], annex A apply with the following additions.

NOTE: The objectives listed in this annex are copied from ISO/IEC 27001 [5], annex A by kind permission of ISO - International Organization for Standardization.

Table B.1

A.5. Security Policy

A.5.1. Information security policy

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

A.5.1.SS1 A reliable Security Policy should be in force and its knowledge and abidance should be enforced by the TSP issuing and storing electronic data object.

A.6. Organizing information security

A.6.1. Internal organization

Objective: To manage information security within the organization.

A.6.1.SS1 No additional controls

A.6.2. External Parties

Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

A.6.2.SS1 Suitable stipulations shall be in force, between service providers, that issue and store electronic data object 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.

A.7. Asset management

A.7.1. Responsibility for assets

Objective: To achieve and maintain appropriate protection of organizational assets.

A.7.1.SS1 No additional controls.

A.7.2. Information classification

Objective: To ensure that information receives an appropriate level of protection.

A.7.2.SS1 All private signing keys shall be treated as sensitive and shall be protected by special measures (see SS.1.3.).

A.7.2.SS2 Data objects should be treated as company confidential data objects unless indicated otherwise and as such only revealed to other persons as authorised by the owning company (see also SS.3.6.).

A.8. Human resources security

A.8.1. Prior to employment

Objective: To 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.

A.8.1.SS1 Personnel that will cover trusted roles should be clearly informed in writing of their duties and responsibilities and they should accept them in writing.

A.8.2. During employment

Objective: To ensure that employees, contractors and third party users are aware of data object 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.

A.8.2.SS1 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.

A.8.3. Termination or change of employment

Objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

A.8.3.SS1 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.

A.8.3.SS2 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.

A.9. Physical and environmental security

A.9.1. Secure areas

Objective: To prevent unauthorized physical access, damage, and interference to the organization's premises and information.

A.9.1.SS1 Systems for issuing and storing data objects shall be located in secured areas and access to these premises shall be limited to duly authorised officers, preferably in dual control regime, and logged.

A.9.2. Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

A.9.2.SS1 Suitable measures shall be established to protect equipment relating to the TSP signing and storage services assets against equipment and data object accidents and incidents, e.g. theft and damage, as well as to ensure a suitable service continuity, should be in place.

A.10. Communications and operations management

A.10.1. Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.

A.10.1.SS1 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.

A.10.1.SS2 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 data objects issue and/or storage;
- 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.

A.10.2. Third party service delivery management

Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

A.10.2.SS1 The outsourcing party shall verify that third parties providing it with services related to electronic data objects 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.

A.10.3. System planning and acceptance

Objective: To minimize the risk of systems failures.

A.10.3.SS1 Electronic data object issuing organisations should plan in advance their processing capacity in order to meet the peak processing periods, for example when fiscal deadlines approach, and to keep their commitments regarding the amount of data objects to keep for the expected time.

NOTE 1: Requirements relating to availability of the service would be addressed by a Service Level Agreement.

NOTE 2: 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.

A.10.4. Protection against malicious and mobile code

Objective: To protect the integrity of software and information.

A.10.4.SS1 No additional controls.

NOTE: See objective SS.3.5. regarding requirements relating to malicious code in data objects.

A.10.5. Back-up

Objective: To maintain the integrity and availability of information and information processing facilities and electronic data objects exhibition requirements shall be fulfilled even in case of accidents affecting their main site(s).

A.10.5.SS1 This should imply arranging suitably built and equipped back-up storage sites and 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 data objects, as well as the cost affecting intangible assets like the company image, and the related insurance policy cost and benefits.

A.10.6. Network security management

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

A.10.6.SS1 Networks regarding data objects issuance and storage shall be protected to ensure that neither unauthorised data are inserted to or deleted from the data object issuing, or storing, process, nor any confidential data object is disclosed.

A.10.7. Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

A.10.7.SS1 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.

A.10.8. Exchange of information

Objective: To maintain the security of information and software exchanged within an organization and with any external entity.

A.10.8.SS1 Wherever applicable, data object should be securely exchanged between all systems components and whatever parties. This addresses all communications facilities.

A.10.9. Electronic commerce services

Objective: To ensure the security of electronic commerce services, and their secure use.

A.10.9.SS1 No additional controls.

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.

A.10.10. Monitoring

Objective: To detect unauthorized information processing activities.

A.10.10.SS1 No additional controls.

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

A.11. Access control

A.11.1. Business requirement for access control

Objective: To control access to information.

A.11.1.SS1 No additional controls.

A.11.2. User access management

Objective: To ensure authorized user access and shall prevent unauthorized access to information systems.

A.11.2.SS1 Rigid measures shall be implemented to duly manage the users' authorisation to access the processed data, from the users' registration to their deregistration, also addressing suitable authentication management procedures. See also SS.3.1. regarding authorised access to storage.

A.11.3. User responsibilities

Objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

A.11.3.SS1 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.

A.11.4. Network access control

Objective: To prevent unauthorized access to networked services.

A.11.4.SS1 Organisations that issue and store data objects, that implement on line connections with their customers and with their customers' counterparts, shall have in place and enforce processes that duly manage and monitor access authorisations to their networked services. See also SS.3.1. regarding authorised access.

A.11.5. Operating system access control

Objective: To prevent unauthorized access to operating systems.

A.11.5.SS1 Logs shall be suitably protected and inspected.

A.11.5.SS2 Access control to operating systems should be carefully implemented, to prevent unauthorised access to key resources. See also SS.3.1. regarding authorised access.

A.11.6. Application and information access control

Objective: To prevent unauthorized access to information held in application systems.

A.11.6.SS1 ISO/IEC 27001 [5], annex A, Controls A.11.6.1 should be applied for storage, and Controls A.11.6.2 should be applied for signing keys, or alternative systems providing a similarly reliable control.

A.11.7. Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

A.11.7.SS1 No additional controls.

A.12. Information systems acquisition, development and maintenance

A.12.1. Security requirements of information systems

Objective: To ensure that security is an integral part of information systems.

A.12.1.SS1 No additional controls.

A.12.2. Correct processing in applications

Objective: To prevent errors, loss, unauthorized modification or misuse of information in applications.

A.12.2.SS1 Strict controls shall be implemented to procedures for signing and storing data objects, including bulk signing.

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

A.12.3. Cryptographic controls

Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.

A.12.3.SS1 In countries where sensitive data protection, as addressed by Directive 95/46/EC [7], requires encryption, key management shall be enforced in addition to what is usually required for signing.

A.12.4. Security of system files

Objective: To ensure the security of system files.

A.12.4.SS1 No additional controls.

A.12.5. Security in development and support processes

Objective: To maintain the security of application system software and information.

A.12.5.SS1 Applications shall be developed, tested and installed under clearly defined quality assurance procedures.

A.12.6. Technical vulnerability management

Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

A.12.6.SS1 No additional controls.

A.13. Information security incident management

A.13.1. Reporting information security events and weaknesses

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

A.13.1.SS1 No additional controls.

A.13.2. Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.

A.13.2.SS1 No additional controls.

A.14. Business continuity management

A.14.1. Information security aspects of business continuity management

Objective: To 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.

A.14.1.SS1 The requirements for Continuity of the TSP services shall be specified in a Service Level Agreement.

A.15. Compliance

A.15.1. Compliance with legal requirements

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

A.15.1.SS1 Where cross border data object validity is sought for, it may be necessary to abide by all involved countries legislation/regulations.

A.15.2. Compliance with security policies and standards and technical compliance

Objective: To ensure compliance of systems with organizational security policies and standards.

A.15.2.SS1 Security Policy compliance shall be met.

A.15.2.SS2 No additional controls.

NOTE: Where legislations/regulations are applicable, they prevail, but the ISO/IEC 27001 [5] provisions should be also used to fill in the possible gap.

A.15.3. Information systems audit considerations

Objective: To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

A.15.3.SS1 Even where no specific legal requirement exists in this regard, an appropriate auditing process shall be in place.

Annex C (informative): Change history

From version 1.1.1 to 2.1.1

1) Typos, internal reference errors and linguistic corrections applied.

2) Terms "document" and "information", when referred to archiving, changed in "data object".

3) Scope broadened to encompass all kinds of data objects, not only fiscally relevant ones that become just one of the possible data objects addressed by the present document; consistent corrections have been applied throughout the whole specification.

4) Scope broadened also to non-electronically signed data objects.

5) Added PDF Signatures and Associated Signature to the signatures types and to Reference clause.

6) Redrafted Introduction and Requirements as the first clause and grouping fiscally data objects related clauses in one clause.

7) Added to the Scope clause a reference to the recently published TS 101 533-1 [i.3] and TR 101 533-2 [i.4].

History

Document history		
V1.1.1	July 2007	Publication
V2.1.1	April 2012	Publication