ETSI TR 102 572 V1.1.1 (2007-07)

Technical Report

Best Practices for handling electronic signatures and signed data for digital accounting

Reference

DTR/ESI-000046

Keywords

e-commerce, electronic signature, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

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

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

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

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee 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. The European Directive on e-invoicing 2001/115/EC [6] recognizes 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.

It has become clear that the technical format of the data to be signed and the process of the signature creation are of importance for data authentication.

Also auditing procedures can highly benefit from the availability of electronic invoices and of digital accounting data.

ETSI has launched a project to identify security management and policy requirements for a specific type of Trusted Service Providers (TSP) that act in name and on behalf of taxable persons. This takes into account legal requirements to produce and reliably keep for up to ten years, and sometime longer, electronic invoices as well as other fiscally relevant documents

As a preliminary stage, in order to identify the existing practices for the handling of accounting data, a survey has been carried out across the five major European countries. This report, based on the findings of this survey, presents minimum, maximum and commonly acceptable practices for the above specified TSPs.

1 Scope

The present document has the purpose to propose a set of practices applicable to the various security related aspects of signing fiscally relevant documents when issued and storing them for the legally required time. It is based on the results of a survey carried out on what practices are actually in place in the five most populated European Union Member States (France, Germany, Italy, Spain, UK).

The present document specifically addresses trust service providers supporting signing and storage services for fiscally relevant documents, regarding business accounting for corporate entities in several European Member States. In particular it is suitable for Value Added Tax (VAT) purposes although it is applicable also to other fiscally relevant documents.

The present document does not directly address requirements for accounting for individuals. The practices identified in the present document are independent of the type of document or information being protected.

The present document addresses solely the Advanced Electronic Signature based solution. It is recognized that other suitable measures, not employing Advanced Electronic Signatures, and hence 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 organization and may require independent assessment of the technical and organizational 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.

In the present document three practices categories are provided, that are defined in clause 3.1:

- Maximum Identified Practices.
- Minimum Identified Practices.
- Commonly Acceptable Practices for Trust Service Providers.

All identified practices do not replace specific national legislation in the area of fiscally relevant documents and care should be taken when implementing them that the national legal requirements are complied with.

In the present document guidance is provided on:

- How accounting data and documents can be securely handled and protected to maintain their authenticity and integrity.
- How this security is achieved by enacting measures ensuring:
    - Authentication of persons accessing processing related assets like systems, facilities, networks, storage media.
    - Integrity of data.
    - Integrity of documents, including integrity of the set or sequence of documents, for the time they are to be kept as per the applicable law; this addresses, in addition to electronic signatures, both their format (that should be void of malicious code and other features capable of changing the documents presentation or the result of automatic processing without affecting the integrity controls) and their storage media handling.
    - Reliable processing.
    - Documents readability; this relates to the documents formats, their viewers, the related hardware and operating systems, etc.
    - Documents availability; this implies implementation of some form of Business Continuity Plan, at least envisaging backup copy sites, if not disaster recovery sites.
- How electronic signature may be used to guarantee "the authenticity of the origin and integrity of the contents" of e-invoices, as per Directive 2001/115/EC [6], and, where applicable, other fiscally relevant documents.
- Storage for the legally required period.

The present document is structured in security objectives and controls clauses and categories, based on annex A of ISO/IEC 27001 [4] with the addition of controls specific to signing and storing. Guidance on the implementation of the controls in ISO/IEC 27001 [4] annex A is given in ISO/IEC17799 [3]. These controls may be applied through an information security management system as defined in ISO/IEC 27001 [4].

2 References

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

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

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

NOTE: Available at http://www.cen.eu/isss/einv.

[2] CWA 15580: "Storage of Electronic Invoices".

NOTE: Available at http://www.cen.eu/isss/einv.

[3] ISO/IEC 17799: "Information technology - Security techniques - Code of practice for information security management".

NOTE: The ISO organization will substitute ISO/IEC 17799 with ISO/IEC 27002 by mid 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.

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

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

[6] 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.

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

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

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

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

NOTE: Available at http://www.cen.eu/catweb/35.040.htm.

[11] 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 movement of such data. .

[12] ISO/IEC 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security".

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

[14] ETSI TS 101 903: "XML Advanced Electronic Signatures (XAdES)".

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

NOTE: Available at ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eInvoicing/CWA15579_2006.pdf

[16] ETSI TS 101 862: "Qualified Certificate profile".

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

2.1 France

PRIS V1 Template of certification policy.

PRIS V2 Template of certification policy, http://www.adele.gouv.fr/spip/article.php3?id_article=547.

Art 1316-3 of Civil Code Article of civil code concerning juridical value about electronic proof.

http://www.legifrance.gouv.fr/WAspad/UnCode?code=CCIVILL0.rcv (French document).

Art 1348 of Civil Code Article of civil code concerning copy for juridical value.

http://www.legifrance.gouv.fr/WAspad/UnCode?code=CCIVILL0.rcv (French document).

AFNOR NF Z 42-013 Electronic archival storage - Specifications relative to the design and operation of information processing systems in view of ensuring the storage and integrity of the recordings stored in these systems.

http://www.afnor.fr/portail.asp

AFNOR NF Z 43-400 Archival of electronic data - COM/COLD.

http://www.afnor.fr/portail.asp

Law 80-525 12 July1980. Law about civil code-contract, obligation - proof - testimonial proof - action copy - registration - order to pay - mortgage - relative to juridical actions proof.

http://www.legifrance.gouv.fr/WAspad/UnDocument?base=LEX_SIMPLE_AV90&nod=1LX980525 (French document).

Law 2000-230 13 March 2000. Law about adaptation of proof concerning information technology and relative to electronic signature. http://www.legifrance.gouv.fr/texteconsolide/AREBV.htm (French document).

Law 2004-801 6 August 2004. Law about protection of natural people for data treatment containing personal data.

http://www.legifrance.gouv.fr/texteconsolide/PPEAU.htm (French document).

B.O 136 Official document for taxes n° 136. 7 August 2003. Value Added Tax. Obligations for companies concerning invoices.

http://alize.finances.gouv.fr/dgiboi/boi2003/3capub/cadre3ca.htm (French document).

2.2 Germany

IT Grundschutz Manual 2004: IT Baseline Protection Manual.

http://www.bsi.de/english/gshb/index.htm.

Abgabenordnung German General Tax Code.

http://bundesrecht.juris.de/bundesrecht/BMF_index.html.

Umsatzsteuergesetz 2003 German Turnover Tax Act/VAT legislation, 29th January 2004.

http://bundesrecht.juris.de/bundesrecht/BMF_index.html.

Umsatzsteuerrichtlinien 2004 Administrative Guidelines for Corporate Tax, Issue 2005 ("Umsatzsteuerricht-linien").

Guidelines for Computerized Accounting GoBS 1995; Generally Accepted Principles of Computer-assisted Accounting Systems. Letter from the German Federal Ministry of Finance (BMF) dated 07 November 1995 (in German, *GoBS*).

http://bundesrecht.juris.de/bundesrecht/BMF_index.html .

Guidelines for Access of Tax Authorities to Digital Documents

Principles of Data Access and Auditing of Digital Documents. Letter from the German Federal Ministry of Finance (BMF) dated 16 July 2001.

http://bundesrecht.juris.de/bundesrecht/BMF_index.html).

Guidelines on Electronic Invoicing in Germany (English Version)

AWV 2006, www.awv-net.de.

Signaturgesetz German Digital Signature Act, www.bundesnetzagentur.de.

2.3 Italy

Dlgs 196/2003. Decreto legislativo 30 June 2003. Code in the matter of personal data protection

http://www.garanteprivacy.it/garante/document?ID=727068 (in English).

NOTE: All the following rules are available from the specified URLs only in Italian.

Dlgs 82/2005 amended by Dlgs 159/2006: Legislative Decree 7 March 2005 No 82, amended by Legislative Decree 4 April 2006 No 159; "Code for the Digital Administration". http://www.cnipa.gov.it/site/_files/Opuscolo%2013.pdf

Dlgs 52/2004 Legislative Decree 20 February 2004 No 52; "Implementation of Directive 2001/115/EC on simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax". http://www.camera.it/parlam/leggi/deleghe/testi/04052dl.htm

DMEF 23/1/2004 Decree by the Minister of Economy and Finance 23 January 2004; "Manners to accomplish fiscal obligations relevant to electronic documents and to their copy on various media". http://www.cnipa.gov.it/site/_files/DECRETO%2023%20gennaio%202004.pdf

DPCM 13/1/2004 Decree by the President of Council of Ministers 13 January 2004; "Technical rules for forming, transmitting, keeping, duplicating, reproducing, and validating, also time validating, electronic documents". http://www.cnipa.gov.it/site/_files/DPCM%20040113_v2.pdf

CNIPA Deliberation 11/2004

CNIPA Deliberation 19 February 2004; "Technical rules for reproducing and keeping documents on optical media suitable to guarantee conformity to original documents". http://www.cnipa.gov.it/site/_files/DELIBERAZIONE%2019%20febbraio%202004_v1.pdf

NOTE: Despite its title, this Deliberation allows for any media type to be used.

CNIPA Deliberation 4/2005

CNIPA Deliberation 17 February 2005; "Rules for recognition and verification of the electronic document". http://www.cnipa.gov.it/site/_files/Deliberazione%2042005%2017%20febbraio%202005.pdf

2.4 Spain

AEAT

Spanish Tax Agency portal on e-invoice. http://www.aeat.es/wps/portal/Listado?url=Campa%C3%B1as/e-factura&channel=cab69588beb99010VgnVCM1000004ef01e0a____&ver=L&site=56d8237c0bc1ff00VgnVCM100000d7005a80____&idioma=es_ES&menu=0&img=0

A MISI/2007

ANTEPROYECTO de Ley de Medidas de Impulso de la Sociedad de la Información.

CCI

Centro de Cooperación Interbancaria portal on e-invoice. http://www.asociacioncci.es/Paginas/eFactura_AEAT-CCI.aspx

I 138/1999

INSTRUCCIÓN de 26 de mayo de 1999, de la Dirección General de los Registros y del Notariado, sobre presentación de las cuentas anuales en los Registros Mercantiles mediante soporte informático y sobre recuperación de sus archivos.

I 7/2000 PRES

INSTRUCCIÓN de 30 de diciembre de 1999, de la Dirección General de los Registros y del Notariado, sobre presentación de las cuentas anuales en los Registros Mercantiles a través de procedimientos telemáticos.

I 7/2000 LEG

INSTRUCCIÓN de 31 de diciembre de 1999, de la Dirección General de los Registros y del Notariado, sobre legalización de libros en los Registros Mercantiles a través de procedimientos telemáticos.

I 158/2003

INSTRUCCIÓN de 13 de junio de 2003, de la Dirección General de los Registros y del Notariado, complementaria de la Instrucción de 30 de diciembre de 1999, sobre presentación de las cuentas anuales en los Registros Mercantiles mediante procedimientos telemáticos.

L 30/192

LEY 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones Públicas y del procedimiento administrativo común.

L 59/2003

LEY 59/2003 de 19 e diciembre 2003 de firma electrónica.

O 311/2000

ORDEN de 21 de diciembre de 2000 en el que se establecen las condiciones generales y el procedimiento para la presentación telemática por Internet de las declaraciones correspondientes a los modelos 117, 123, 124, 126, 128, 216, 131, 310, 311, 193, 198, 296 y 345.

O 298/2002

ORDEN HAC/3134/2002, de 5 de diciembre, sobre un nuevo desarrollo del régimen de facturación telemática previsto en el artículo 88 de la Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido, y en el artículo 9 bis del Real Decreto 2402/1985, de 18 de diciembre.

O 116/2003

ORDEN HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria.

PL 2006 PROYECTO DE LEY para el acceso electrónico de los ciudadanos a las Administraciones Públicas.

R 51/2003 RESOLUCIÓN 2/2003, de 14 de febrero, de la Dirección General de la Agencia Estatal de Administración Tributaria, sobre determinados aspectos relacionados con la facturación telemática.

R 286/2003 RESOLUCIÓN de 24 de mayo de 2005, de la Secretaría de Estado de Hacienda y Presupuestos, de control de accesos a las bases de datos de la Secretaría General de Presupuestos y Gastos y de la Intervención General de la Administración del Estado.

R 298/2005 FILE RESOLUCIÓN de 28 de noviembre de 2005, de la Intervención General de la Administración del Estado, por la que se regulan los procedimientos para la tramitación de los documentos contables en soporte fichero.

R 298/2005 IRIS RESOLUCIÓN de 28 de noviembre de 2005, de la Intervención General de la Administración del Estado, por la que se aprueba la aplicación IRIS.

RD 1496/2003 REAL DECRETO 1496/2003, de 28 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación, y se modifica el Reglamento del Impuesto sobre el Valor Añadido.

RD 2188/1995 REAL DECRETO 2188/1995, de 28 de diciembre, por el que se desarrolla el régimen del control interno ejercido por la Intervención General de la Administración del Estado.

RD 263/1996 REAL DECRETO 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

RD 772/1999 REAL DECRETO 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro.

RD 1377/2002 REAL DECRETO 1377/2002 por el que se desarrolla la colaboración social en la gestión de tributos para la presentación telemática de declaraciones, comunicaciones y otros documentos tributarios.

RD 209/2003 REAL DECRETO 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

RD 686/2005 REAL DECRETO 686/2005, de 10 de junio, por el que se modifica el Real Decreto 2188/1995, de 28 de diciembre, por el que se desarrolla el régimen de control interno ejercido por la Intervención General de la Administración del Estado.

2.5 United Kingdom

UK Legislation Companies Act 1989 requirements on record keeping:

http://www.opsi.gov.uk/ACTS/acts1989/Ukpga_19890040_en_2.htm

Finance Act 1998 requirements on company tax returns.

Her Majesties Revenue and Customs http://www.hmrc.gov.uk

HM Customs and Excise (now HMRC) Notice 700/21 Keeping records and accounts.

HM Customs and Excise (now HMRC) Notice 700/62 self-billing.

HM Customs and Excise (now HMRC) Notice 700/63 Electronic Invoicing.

HM Customs and Excise (now HMRC) Notice 725 Single markets.

Companies House.

Guidance documents http://www.companieshouse.gov.uk/about/guidance.shtml

Policy on document signatures

http://www.companieshouse.gov.uk/about/policyDocuments/documentSignatures.shtml

Institute of Chartered Accountants for England and Wales.

http://www.icaew.co.uk/

Guidance regarding assurance of internal controls of a service organization.

http://www.icaew.co.uk/index.cfm?route=136450

British Standards Institute.

Code of Practice for legal admissibility and evidential weight of information stored electronically.

http://www.bsi-global.com/ICT/Legal/bip0008.xalter

PAS 76 Accounting software - Value Added Tax in the UK - Specification.

http://www.bsi-global.com/ICT/SoftwareQuality/PAS76.xalter

Business Application Software Developers Association (BASDA).

2.6 International Organisations

OECD Guidance for Developers of Business and Accounting Software Concerning Tax Audit Requirements.

http://www.oecd.org/document/57/0,2340,en_2649_33749_34910329_1_1_1_1,00.html

3 Definitions and abbreviations

3.1 Definitions

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

Advanced Electronic Signature (AdES): 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, Article 2 No. 2 of the European Electronic Signature Directive (Directive 1999/93/EC [5])

Commonly Acceptable Practices (CAS): 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 2001/115/EC [6]

fiscally relevant data: data relevant to financial accounting related to the taxable person or company, i.e. data on book-keeping, invoicing, payroll, investment, etc.

NOTE: They are subject to exhibition to the regulatory authority concerned with financial accounting. (e.g. Tax Authority, Chamber of Commerce, Ministry of finance, etc.).

fiscally relevant document: document or record containing fiscally relevant data

Maximum Identified Practices (MaxIP): most stringent practices identified for the signing and storage of fiscally relevant documents.

Minimum Identified Practices (MinIP): least stringent practices identified for the signing and storage of fiscally relevant documents

Qualified Electronic Signature (QES): advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device (Directive 1999/93/EC [5])

Secure Signature Creation Device (SSCD): signature-creation device which meets the requirements laid down in Annex III of (Directive 1999/93/EC [5])

Signature Creation Data (SCD): unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature (Directive 1999/93/EC [5])

statement of applicability: documented statement describing the control objectives and controls that are relevant and applicable to the TSP's ISMS (ISO/IEC 27001 [4])

3.2 Abbreviations

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

AdES	Advanced Electronic Signature
AFNOR	Association Français de NORmalisation
BOE	Boletín Oficial del Estado
BPR	Business Process Reengineering
CA	Certification Authority
CAP	Commonly Acceptable Practices
CAP-TSP	Commonly Acceptable Practices-Trusted Service Provider
CC	Common Criteria
CNIPA	Centro Nazionale per Informatica nella Pubblica Amministrazione
CRL	Certificate Revocation List
EDI	Electronic Data Interchange
EUMS	European Union Member States
FAT	File Allocation Table
HSM	Hardware Security Module
IGAE	Intervención General de la Administración del Estado
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
MaxIP	Maximum Identified Practices
MINEFI	MINEstry of Finance
MinIP	Minimum Identified Practices
QES	Qualified Electronic Signature
SCD	Signature Creation Data
SSCD	Secure Signature Creation Device
SSL	Secure Socket Layer
TIFF	Tagged Image File Format
TLS	Transport Layer Security
TSP	Trusted Service Providers
VAT	Value Added Tax
WORM	Write Once Read Many
XBRL	eXtensible Business Reporting Language
XML	eXtended Markup Language

4 General concepts

4.1 Basic Model

The general application of signing and storage services to fiscally relevant documents is illustrated in figure 1.

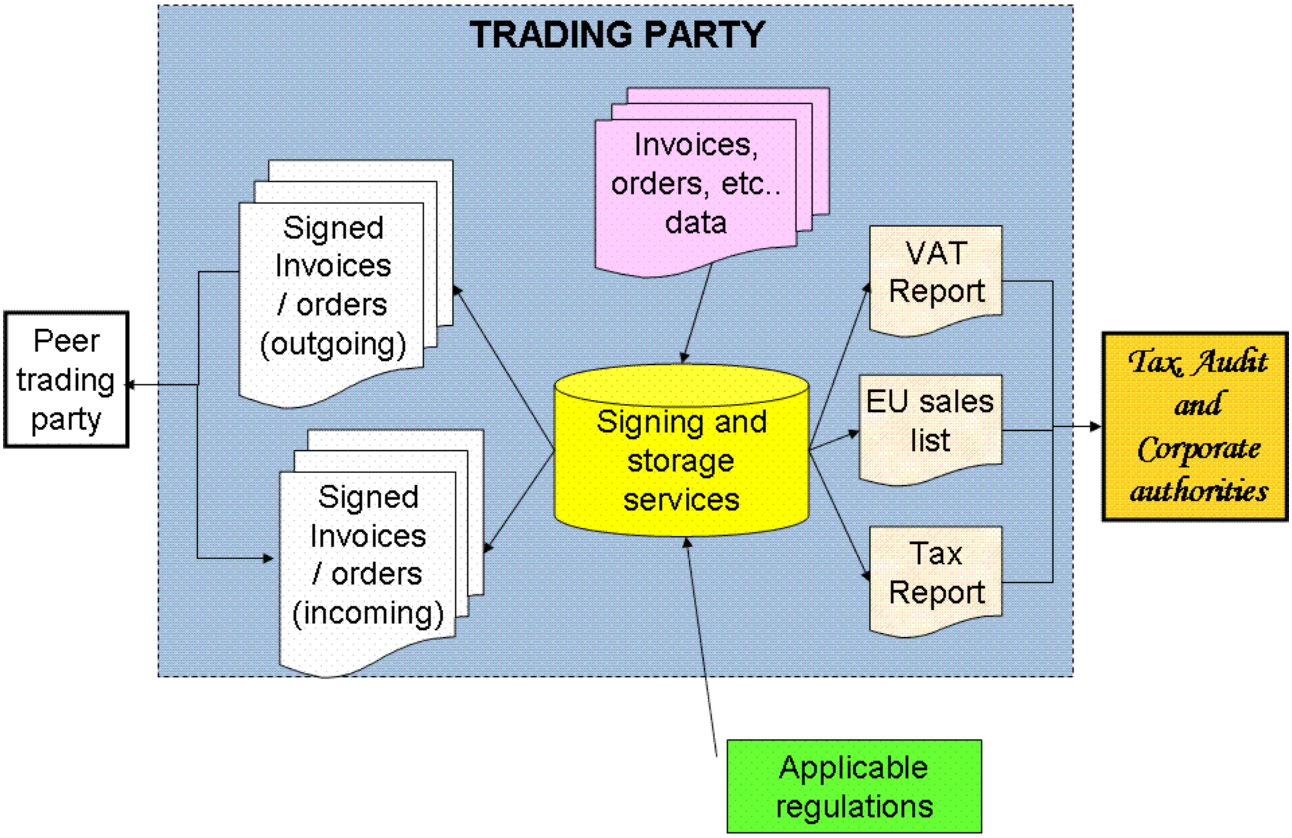
TRADING PARTY
Invoices, orders, etc.. data
Signed Invoices / orders (outgoing)
Peer trading party
Signing and storage services
VAT Report
EU sales list
Tax Report
Tax Audit and Corporate authorities
Signed Invoices / orders (incoming)
Applicable regulations

Figure 1: Basic Model

A trading party (e.g. limited company) uses the services to sign and store invoices, purchase orders and other fiscally relevant documents, which then are passed to its trading partners. The information may be retrieved from the store and processed to provide a range of reports including VAT and other tax reports, commercial reports such as information on sales figures across Europe, and to provide general information as needed for audit purposes. This information would be stored for a period of time and protected using electronic signatures as required by national regulations (legislation and rules established by tax and other authorities).

4.2 VAT invoices and other fiscally relevant socuments

The study, on which the present document is based, considered the practices across the range of applications involving fiscally relevant documents (invoices, orders, pay roll, accounting documents, etc). This included not only VAT invoicing but requirements for record keeping and reporting for other areas of tax as well as corporate accounting and auditing of public expenditure. The practices for signing and storage of general accounting data in the different countries for these areas were widely varying.

There is, however, one area where there have been some moves towards harmonization. That is in VAT related invoicing. The European Council Directive 2001/115/EC [6] of 20 December 2001 on modernising and harmonizing the conditions laid down for invoicing in respect of value added tax, includes requirements for the use of "Advanced Electronic Signatures". There is also a general requirement to maintain records of VAT invoices sent and received, although the period of time for such records to be kept varies. These requirements have been further refined in the CEN workshop agreements on "E-invoices and Digital Signatures" CWA 15579 [1] and "storage of electronic invoices" CWA 15580 [2].

Thus, the aim of the present document is to identify harmonized practices for storage and signing across the range of areas of fiscal document handling. However, given the more advanced state of work on harmonization of e-invoicing, this is the area where there is the strongest basis for harmonization and hence the present document is most applicable.

4.3 Minimum and maximum identified practices

The practices described in the present document are based upon a survey of the practices in 5 major European states for handling fiscally relevant documents including VAT invoices as well as other business accounting practices.

This survey has shown two fundamental differences in the five countries considered:

1) The status of implementation of electronic signatures for fiscally relevant documents in all five countries is different as regards:

    - integration into the regulatory framework in general; and
    - integration of electronic signature standards in accounting specifically.

2) The status of the regulatory framework as regards fiscally relevant documents, regardless of electronic signature usage, is different:

    - few countries regulatory framework cover the whole spectrum of regulation for the handling of fiscally relevant documents aspects in any detail;
    - most countries are covering only very specific areas, e.g. electronic invoices.

As a result it was not possible to identify a single set of practices for the signing and storage of fiscally relevant documents which would be fit within all the regulatory frameworks that exist across Europe.

The present document, instead, identifies the range of practices that could be applied to the signing and storage of fiscally relevant documents as they might fit within the range of existing accounting practices across the European countries studied and is aimed not to conflict with the regulatory frameworks so they should be acceptable across Europe. Moreover, the report only addresses those practices where the use of "Advanced Electronic Signatures" is considered necessary for the handling of fiscally relevant documents.

The range of practices for signing and storage of fiscally relevant documents is expressed in the present document in terms of:

- Minimum Identified Practices (MinIP): The least stringent practices identified for the signing and storage of fiscally relevant documents.

NOTE 1: This minimum level was aimed to provide a level of reliability that might be acceptable across Europe and meets the basic legal provisions for the free circulation of goods and services within the European Union.

- Maximum Identified Practices (MaxIP): The most stringent practices identified for the signing and storage of fiscally relevant documents.

NOTE 2: This maximum level should be acceptable across Europe as, according to the free circulation of goods and services within the European Union, no receiving country should object on accepting one document abiding by these requirements, provided it is created in one EU member state.

Clause 4.6 addresses practices which may be recognized as acceptable by authorities in several EU nations. Moreover, these practices are specifically targeted at TSPs supporting signing and storage services for accounting. Clause 5 outlines minimum and maximum identified practices, as well as commonly acceptable practices for TSPs.

Annex A to the present document details the practices of 5 European states on which these minimum and maximum practices are based.

4.4 Pan European model

To expand the basic model to pan European trade the requirements of national regulations need to be extended to take into account the requirements of pan European trade. Where two parties trade, each will operate under its own regulations but have to take account of the pan European requirements as illustrated in figure 2.

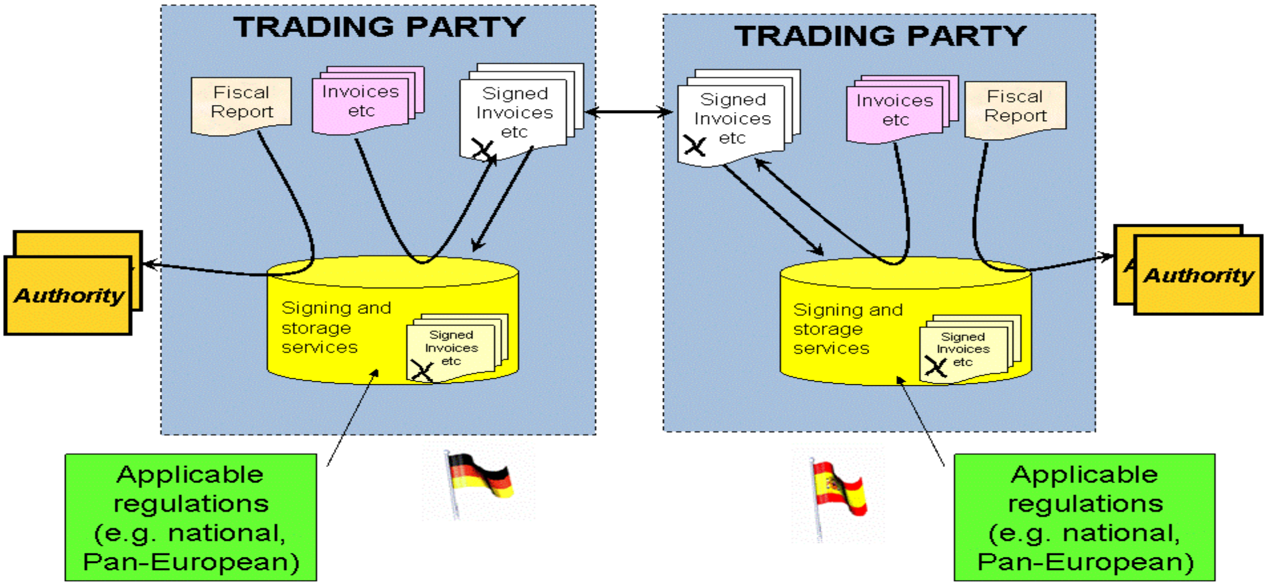

Figure 2: Pan European Model4.5 Trusted Service Providers (TSPs)

The pan European model described above can be further refined where the signing and storage service is provided by Trusted Service Providers (TSP) who can support several trading parties operating in a single country. This is illustrated in figure 3.

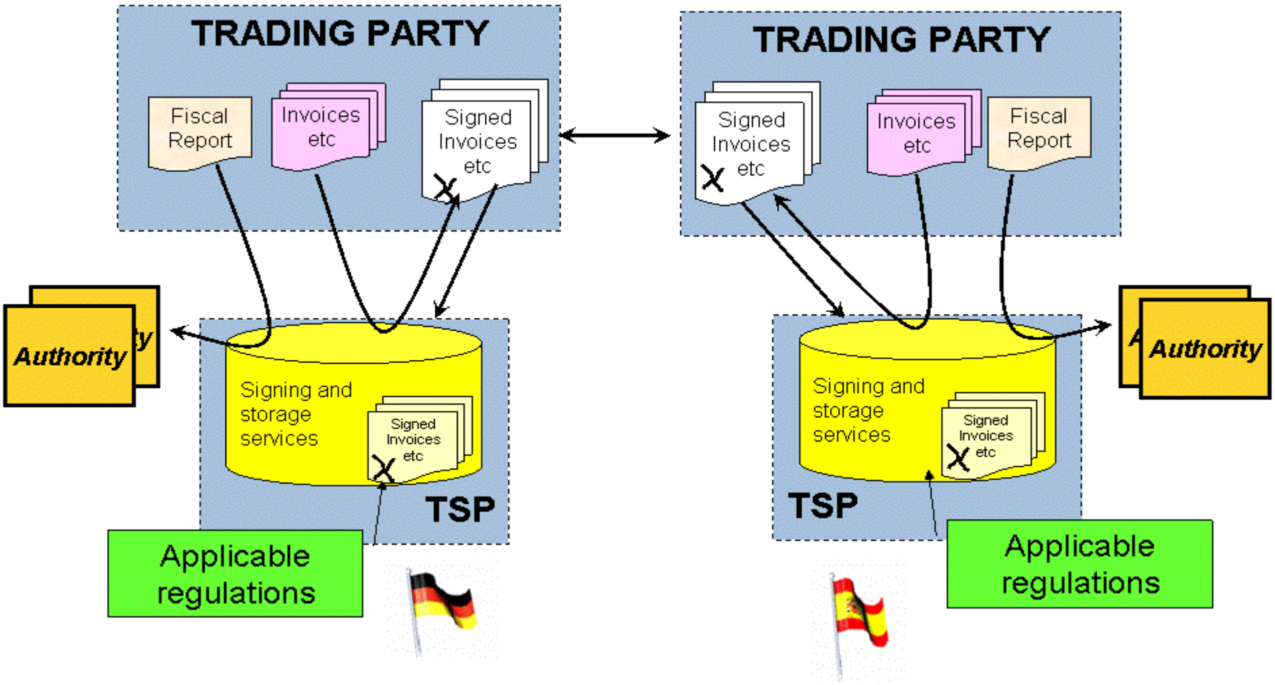

Figure 3: Pan European model with Trusted Service Providers

In this scenario trading documents of each trading party are signed and/or stored by an external trusted service provider (TSP) but the production of reports from the stored information remains the responsibility of the trading parties. The information is exchanged directly between trading parties, unlike the case of EDI supported by value added network service, and the trading parties are responsible for providing the necessary reports to the tax authorities, etc.

4.6 Commonly Acceptable Practices (CAP) for TSPs

As discussed above (see clause 4.3) the current document sets out the minimum and maximum for the range of identified practices for the European nations studied. One particular usage scenario, pan European trade supported by Trusted Service Providers (TSPs) has been recognized as being of importance and particularly requiring standardization. Such a trust service may be used by trading parties persons (individuals or organizational entities) in one European state for signing and/or storage services for trade with taxable persons in another state.

The present document identifies "Commonly Acceptable Practices" for trust services providers operating in such an environment. These commonly acceptable practices further refine and identify a set of practices that may be acceptable for pan European trade.

Whilst the Commonly Acceptable Practices defined in the present document are directed at this pan European scenario, they may also be used:

- as the basis for practices for TSPs supporting trade within a single nation that may be defined, for example, by a national authority or by the TSP itself;
- as the basis for practices for an organization that electronically signs and stores fiscally relevant documents for itself.

5 Practices identified

5.1 Signature and storage requirements

5.1.1 Signature

5.1.1.1 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 documents.

MaxIP Fiscally relevant documents, when electronically signed, should be signed with a Qualified Electronic Signature.

MinIP Invoices, where electronically signed, should be signed by an Advanced Electronic Signature (see Directive 2001/115/EC [6] Article 2.2).

Similarly, where other fiscally relevant documents are signed they may be signed by an Advanced Electronic Signature.

CAP-TSP If fiscally relevant electronic documents are signed the signature should be at least an Advanced Electronic Signature, as defined in Directive 1999/93/EC [5], with the purpose of ensuring documents integrity and authenticity, as required by Directive 2001/115/EC [6].

Signature formats that maximize interoperability are recommended, such as those defined in TS 102 734 [8] (which profiles TS 101 733 [13]) or TS 102 904 [9] (which profiles TS 101 903 [14]). Should these profiles not fully satisfy specific application requirements, use of more general formats defined in TS 101 733 [13] or in TS 101 903 [14] is recommended.

5.1.1.2 Certification

Objective: To obtain certificate from authority who can reliably certify public key and maintain revocation status information.

MaxIP Fiscally relevant documents, when electronically signed, should be supported by a qualified certificate. The CA issuing the qualified certificate may be accredited.

MinIP Fiscally relevant documents, when electronically signed, should be supported by a certificate issued by a CA that, if not qualified as per Directive 1999/93/EC [5], should at least meet some recognized policy requirements (e.g. TS 102 042 [7]) or be approved by some nationally recognized scheme.

CAP-TSP Electronically signed fiscally relevant documents should be supported by:

1) a qualified certificate issued by a CA which may be accredited as per Article 3(2) of Directive 1999/93/EC [5]; or

2) a certificate issued by a CA that should operate under certificate policies as per TS 102 042 [7] (NCP type) or practices that are nationally recognized as being sufficiently reliable for the purposes of signing fiscally relevant data.

5.1.1.3 Signature creation data

Objective: To ensure that the private signing key is kept secure.

MaxIP To sign fiscally relevant documents, signing keys should be kept in an SSCD certified per CWA 14169 [10].

MinIP Security controls are applied to signing keys suitable to ensure that the signatory can maintain them under his sole control.

CAP-TSP

1) Where a Qualified Electronic Signature is required, and in all cases where a hardware signature creation device is used, the signing key should be held in a SSCD certified per CWA 14169 [10], or in a high security module certified to CC EAL4 or ITSEC E3, or to any comparable criteria recognized in a EUMS.

2) Where an Advanced Electronic Signature is used, security controls should be applied to the signing keys suitable to ensure that the signatory can maintain them under his sole control. In particular:

   a) where a TSP holds keys on behalf of its users, the TSP should ensure that signing keys can be only used by their owners.

   b) 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 with that key only by users explicitly authorized to act for the company.

NOTE: Where legally allowed, signing keys can also be used by persons explicitly delegated by their owners, including the TSP.

5.1.1.4 Certificate subject's registration

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

MaxIP Subjects' registration should be based on their secure identification, where applicable via legally valid or commonly accepted identity documents (e.g. passports, identity cards, driving licences, etc.) and supported by documentation specifying their roles and signing powers (e.g. maximum transaction values) as well as authorization to act for the taxable person.

MinIP Where a qualified certificate is used, its subjects' registration management should be deemed as acceptable by the other EUMS countries.

Where non qualified certificates are used, an agreement on their usage, and in particular on their subjects' registration procedures, should exist between the countries where the issuing CA is established and the receiving organization is located.

CAP-TSP Subjects' registration should be based on their secure identification, where applicable via legally valid or commonly accepted identity documents (e.g. passports, identity cards, driving licences, etc.) and supported by documentation specifying their roles and signing powers (e.g. maximum transaction values) as well as authorization to act for the taxable person.

5.1.1.5 Certificate revocation

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

MaxIP Revocation should 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).

MinIP Where a qualified certificate is used, its revocation management should be deemed as acceptable by the other EUMS countries.

Where non qualified certificates are used, an agreement on their usage, and in particular on their revocation procedures, should exist between the countries where the issuing CA is established and the receiving organization is located.

CAP-TSP Revocation should 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).

5.1.2 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.

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

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 should be stored for the same time as the related signed document and in a manner that preserves the integrity of this set of information as required in clause 5.1.3.2.

If the signed documents are to be stored for a significant period which is longer than the strength of the cryptographic algorithms employed can be assured, then additional integrity mechanisms should be applied to the signed document and verification information. This may be achieved for example by employing archive time-stamps (such as specified in TS 101 733 [13] or TS 101 903 [14]) or maintaining the documents in Write Once Read Many (WORM) media which cannot be modified once written.

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 document its signature has been verified in accordance with generally recognized procedures,

Combination of technical and organizational measures

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

MinIP If a signed document is kept for the required period in conformity with the regulations in force in the EUMS where the latter is located, this document storage should be accepted in any other EUMS.

CAP-TSP Signature verifiability should be ensured for the entire storage period. This can be implemented by technical or organizational measures or by a combination of them as follows:

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 that signature existed and was valid should be stored for the same time as the related signed document and in a manner that preserves the integrity of this set of information as required in clause 5.1.3.2.

If the signed documents are to be stored for a significant period which is longer than the one for which the strength of the cryptographic algorithms employed can be assured, then additional integrity mechanisms should be applied to the signed document and verification information. This may be achieved for example by employing archive time-stamps (such as specified in TS 101 733 [13] or TS 101 903 [14]) or maintaining the documents in Write Once Read Many (WORM) media which cannot be modified once written.

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 document its signature has been verified in accordance with generally recognized procedures,

Combination of technical and organizational

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

5.1.3 Storage

5.1.3.1 Authorized access

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

MaxIP Access should be allowed, in addition to the related company officials, at least to tax authority inspectors and to other legally authorized authorities. Where electronic remote access is legally required it should be implemented in a secure way, so that the remote user and server are authenticated, and the integrity and confidentiality of communications is protected over vulnerable networks.(e.g. user password and TLS over Internet)

MinIP Access to fiscally relevant documents is to be allowed at least to duly authorized company officers and equally duly authorized authorities such as tax agency inspectors.

No remote access should be required.

CAP-TSP Access should be allowed, in addition to the related company officials, at least to duly authorized authorities such as tax agency inspectors. 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 and SSL/TLS over Internet).

5.1.3.2 Authenticity and integrity

Objective: To maintain the authenticity of origin and integrity of a set of fiscally relevant data, also detecting loss or unauthorized addition of documents, held in storage for the legally required period.

MaxIP Authenticity of origin and integrity of electronically signed documents should be ensured by:

use of appropriate class of signature (see clause 5.1.1.1); and

maintenance of that signature over the storage period (see clause 5.1.2);

mechanisms to detect loss or unauthorized addition of documents.

MinIP The authenticity of origin and integrity of fiscally relevant electronic documents, where signed, should be ensured by technical measures recognized as valid in the country where the Company on behalf of which the documents are kept is established (e.g. compliance with ISO/IEC 17799 [3]).

Where electronically signed e-invoices are stored, their storage is to abide by the country rules that apply to the specific document, that "*may require that when invoices are stored by electronic means, the data guaranteeing the authenticity of the origin and integrity of the content also be stored*". (Directive 2001/115/EC [6]).

CAP-TSP Authenticity of origin and integrity of electronically signed documents should be ensured by:

use of appropriate class of signature (see clause 5.1.1.1); and

maintenance of that signature over the storage period (see clause 5.1.2);

mechanisms to detect loss or unauthorized addition of documents.

5.1.3.3 Readability

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

MaxIP The original document format (or, where applicable and legally valid, another suitable format the content of which is derived from the original under supervision by a trusted body) should be ensured as readable by the storing organization, for example by also storing the related visualising software before it becomes no longer available.

Where necessary, also the required hardware and environmental software should be stored as well.

Where there is a risk that one specific document/viewer system *is* becoming obsolete all affected documents should be reliably copied, keeping its semantics 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.

MinIP No specific requirement. However, the storing organization is liable for any lack of readability.

Documents should be exhibited both on paper and/or electronically.

CAP-TSP The original document format (or, where applicable and legally valid, another suitable format reliably derived from the original) should be ensured as readable by the storing organization, for example by also storing the related visualising software, and where necessary the related hardware, before it becomes no longer available.

Where there is a risk that one specific document/viewer system is becoming obsolete all affected documents should be reliably copied keeping its semantics 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.

5.1.3.4 Storage media type

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

MaxIP Media, as well as media readers, should 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 should be timely copied onto another suitable media at a frequency necessary to assure its readability. Where the maintenance of signed documents depends on the integrity of the media (e.g. using WORM devices, see clause 5.1.2) any copying is to include appropriate controls to ensure the maintenance of the integrity (e.g. by employing trusted third parties) .

MinIP No specific requirement: however the storing organization may be liable for any document loss due to media deterioration.

No specific media type should be required, provided that organizational measures are in place to timely copy the content of a no longer reliable media onto a new one, with the assurance that the copied documents content is not changed.

CAP-TSP Where possible, media, as well as media readers, should 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 should be timely copied onto another suitable media at a frequency necessary to assure its readability. Where the maintenance of signed documents depends on the integrity of the media (e.g. using WORM devices, see clause 5.1.2) any copying is to include appropriate controls to ensure the maintenance of the integrity (e.g. by employing trusted third parties).

5.1.3.5 Documents format

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

MaxIP Fiscally relevant documents should be produced in a format that prevents any change to the information represented by the document which is not detected by integrity controls (as described in clause 5.1.3.2), 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 (please refer to clause 8.6 of CWA 14170 [15]).

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

Fiscally relevant documents should be stored in their original format, provided they are void of potential sources of malicious code in macros, scripts or hidden code capable to modify the document presentation. Where the original format does not provide sufficient reliability in this respect, a suitable format for the same document should 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.

MinIP No specific requirement: however the issuing organization may be liable for any future change in the document presentation.

CAP-TSP Fiscally relevant documents should 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 (please refer to clause 8.6 of CWA 14170 [15]).

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

Fiscally relevant documents should be stored in their original format, provided they are void of potential sources of malicious code in macros, scripts or hidden code capable to modify the document presentation. Where the original format does not provide sufficient reliability in this respect, a suitable format for the same document should 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.

5.1.3.6 Requirements on separation and confidentiality

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

MaxIP The storage of data is to provide clear separation of data between different owners so that confidentiality of information stored cannot be compromised. If the storing organization keeps fiscally relevant data related to different taxable persons the related storage or the archives is to 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.

MinIP The storage of each owner's information should ensure the confidentiality of the data.

CAP-TSP The storage is to be clearly physically or logically separated between different owners so that the confidentiality cannot be compromised. If the storing organization keeps fiscally relevant data related to different taxable persons the related storage or the archives is to 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.

5.1.4 Reporting to and exchanges with authorities

Objective: To ensure that Fiscally relevant documents 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 taxable person and so any submission should be authorized by the taxable person.

MaxIP Fiscally relevant documents, including reports, should be submitted to authorities by secure electronic means, signed at least with an Advanced Electronic Signatures or, where required, a Qualified Electronic Signature Measures adopted in clause 5.1.2 should also be provided alongside the reported document, where possible, as a means to ensure protection against later signing certificate revocation or certificate expiry inappropriately making old signatures invalid.

Secure channels such as TLS should additionally be used.

MinIP Secure submission of electronically signed fiscally relevant reports 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. password and TLS over Internet).

CAP-TSP 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 and TLS over Internet).

To prevent subsequent corruption of the document, Advanced Electronic Signatures (or Qualified Electronic Signature) should also be used. Controls identified in clause 5.1.2 should also be provided alongside the submitted document, where possible, as a means to ensure protection against later signing certificate revocation or certificate expiry inappropriately making old signatures invalid.

5.1.5 Conversion of paper originals to digital formats

Objective: To ensure that, when fiscally relevant documents originally in paper, or other non-digitally encoded formats(e.g. audio, microfiche) are converted into digital format, their content is preserved without any change.

MaxIP The correspondence between paper documents (or other non-digital formats) and their corresponding digital image (e.g. scanned copies) should be ensured. This requires an assertion (even electronic) by a trusted person, that either carries out the conversion or later compares the paper or other non-digitally encoded documents with the original. The assertion can be either explicit or implicit. The digital image of the document and any assertion should be signed to protect their authenticity and integrity.

MinIP The correspondence between paper document (or other non-digital format) and their corresponding digital image (e.g. scanned copies) should be ensured. Where these rules do not exist, a process, meeting suitable standards such as ISO/IEC 17799 [3], should ensure that the content of paper or other non-digitally encoded documents (e.g. audio recordings) is not altered during their transformation to electronic format.

CAP-TSP The correspondence between a paper document (or other non digital format) and the 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 17799 [3] or, where applicable, assessed per ISO/IEC 27001 [4], should ensure that the content of paper or other non-digitally encoded documents (e.g. analogic audio recordings) matches the corresponding digital image.

Where required by the applicable country rules, or identified as necessary from the application of information security management system (e.g. ISO/IEC 17799 [3], ISO/IEC 27001 [4]), the digital version of the paper or other non-digitally encoded document should be physically or logically associated with an assertion (for example an electronically signed addendum to the document) on this correspondence issued by a trusted person who, for example, either carried out the scanning or later compared the scanned version with the original. The assertion can be either explicit or implicit. The paper or other non-digitally encoded document digital image and any assertion should be signed to protect their authenticity and integrity.

5.2 Information security management

The following clauses are based on annex A of ISO/IEC 27001 [4] and its code of practice sister standard ISO/IEC 17799 [3], therefore, in general, the organization's ISMS should be assessed as conformant to ISO/IEC 27001 [4] or at least be operated on the basis of ISO/IEC 17799 [3] or equivalent guidance. Information security management systems which provide equivalent assurance may be employed where allowed by applicable legislation.

The following applies to all aspects of Information Security Management.

MaxIP IT systems of organizations issuing and storing fiscally relevant electronic documents should incorporate controls complying with ISO 27001 [4] annex A as identified in its statement of applicability. Conformance assessment/certification of the organizations ISMS per ISO/IEC 27001 [4] is also recommended, unless the applicable regulations ensure achieving an analogue trust level.

MinIP No special provision is specified in addition to what is required by the applicable regulations and legislation.

However it is wished that any organization implementing an ISMS develops and maintains it, based on the ISO/IEC 27001 [4], the ISO/IEC 2700x series, among which the practices indicated in ISO/IEC 17799 [3], or a nationally developed guidance.

CAP-TSP Unless applicable regulations specifies requirements on the definition and implementation of an Information Security Management System, and in their default, IT systems of organizations issuing and storing fiscally relevant electronic documents should implement an Information Security Management System in line with ISO/IEC 27001 [4], for example according to the practices indicated in ISO/IEC 17799 [3]. Conformance assessment/certification per ISO/IEC 27001 [4] is also recommended, unless the applicable regulations ensure achieving an equivalent trust level.

5.2.1 Risk analysis

Risk analysis is a process to 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 [3] clause 4 "Risk assessment and treatment" and clause 4.1 "Assessing security risks").

5.2.2 Security policy

5.2.2.1 Information security policy

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

MaxIP Reliable security policy should be in force and their knowledge and abidance should be enforced by the company issuing and storing fiscally relevant electronically signed documents.

MinIP No special provisions.

CAP-TSP 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.

5.2.3 Organizing information security

5.2.3.1 Internal organization

Objective: To manage information security within the organization.

MaxIP ISO/IEC 17799 [3] controls in clause 6.1 should be implemented.

MinIP No special provisions.

CAP-TSP ISO/IEC 17799 [3] controls in clause 6.1 should be implemented.

5.2.3.2 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.

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

ISO/IEC 17799 [3] controls in clause 6.2 should be implemented.

MinIP No special provisions.

CAP-TSP Suitable stipulations should be in force, between service providers, that issue and store fiscally relevant electronic document on behalf of taxable persons, and the outsourcing organization, that clearly specify the outsourcer's duties and responsibilities, covering also aspects not addressed in detail by the governing rules, where necessary.

ISO/IEC 17799 [3] controls in clause 6.2 should be implemented.

5.2.4 Asset management

5.2.4.1 Responsibility for assets

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

MaxIP All sensitive assets should have a specific accountable owner.

ISO/IEC 17799 [3] controls in clause 7.1 should be implemented.

MinIP No special provisions.

CAP-TSP ISO/IEC 17799 [3] controls in clause 7.1 should be implemented.

5.2.4.2 Information classification

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

MaxIP Signing material should be treated as addressed by Directive 1999/93/EC [5] and by its implementations in the various EUMS that specify their confidentiality requirement. This regards the signing private keys and, at times only implicitly, also SSCD/HSM and private key activation data.

These fiscal electronic documents issuance and storage related assets, as well as additional ones including personal data, should be inventoried and classified according to their secrecy level even when no specific classification is legally required.

Fiscally relevant documents should be treated as company confidential documents unless indicated otherwise.

In particular, regarding information classification, ISO/IEC 17799 [3] controls in clause 7.2 should be implemented.

MinIP No special provisions.

CAP-TSP All private signing keys should be treated as sensitive and should be protected by special measures (see clause 5.1.1.3).

Fiscally relevant documents should be treated as company confidential documents unless indicated otherwise (see also clause 5.1.3.6).

ISO/IEC 17799 [3] controls in clause 7.2 should be implemented.

5.2.5 Human resources security

5.2.5.1 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.

MaxIP A candidate screening during the hiring phase should be performed, in abidance by the applicable legislation or regulations, capable to help assess his/her suitability to the specific job, also regarding its sensitivity. In any case personnel that will cover sensitive roles should be clearly informed in writing of their duties and responsibilities and they should accept them in writing.

In particular, regarding human resource security prior to employment, ISO/IEC 17799 [3] controls in clause 8.1 should be implemented.

MinIP No special provisions.

CAP-TSP A candidate screening during the hiring phase should be performed, in abidance by the applicable legislation or regulations, capable to help assess his/her suitability to the specific job, also regarding its sensitivity. In any case personnel that will cover sensitive roles should be clearly informed in writing of their duties and responsibilities and they should accept them in writing.

ISO/IEC 17799 [3] controls in clause 8.1 should be implemented.

5.2.5.2 During employment

Objective: To 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.

MaxIP Consistently with the applicable legislation and rules, the personnel at issue, including the involved managers, should be suitably equipped to correctly and securely perform their tasks and should be suitably and timely educated on their task duties and informed on the consequence of their possible misbehaviour.

In particular, regarding human resource security during employment, ISO/IEC 17799 [3] controls in clause 8.2 should be implemented.

MinIP No special provisions.

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

ISO/IEC 17799 [3] controls in clause 8.2 should be implemented.

5.2.5.3 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.

MaxIP Consistently with the applicable legislation and rules, the involved personnel should 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.

All the company equipment should be returned by the leaving employees and their privileges should be withdrawn, unless where otherwise explicitly specified.

ISO/IEC 17799 [3] controls in clause 8.3 should be implemented.

MinIP No special provisions.

CAP-TSP a) Consistently with the applicable legislation and rules, the personnel in trusted roles are to 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 is to be returned by the leaving employees and their privileges should be withdrawn, unless where otherwise explicitly specified.

ISO/IEC 17799 [3] controls in clause 8.3 should be implemented.

5.2.6 Physical and environmental security

5.2.6.1 Secure areas

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

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

ISO/IEC 17799 [3] controls in clause 9.1 should be implemented.

MinIP No special provisions.

CAP-TSP Systems for issuing and storing fiscally relevant documents should be located in secured areas and access to these premises should be limited to duly authorized officers, preferably in dual control regime, and logged.

ISO/IEC 17799 [3] controls in clause 9.1 should be implemented.

5.2.6.2 Equipment

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

MaxIP The equipment should be protected to prevent compromise of confidential information, insertion of arbitrary information in the document production process and denial of service in critical moments, e.g. when tax inspections are performed. Information and data that are to be kept for the time required by force of law should not be kept in unique copy, to avoid that accidents, security incidents, media degradation, obsolescence of reading applications, etc. may affect compliance to the legal requirements. Suitable measures to protect assets against accidents and incidents, e.g. equipment and information theft and damage, as well as to ensure a suitable service continuity, should be in place.

ISO/IEC 17799 [3] controls in clause 9.2 should be implemented.

MinIP No special provisions.

CAP-TSP Suitable measures should 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.

ISO/IEC 17799 [3] controls in clause 9.2 should be implemented.

5.2.7 Communications and operations management

5.2.7.1 Operational procedures and responsibilities

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

MaxIP

NOTE: A correct and secure operation of information processing facilities is even more important where third parties act on behalf of tax payers and in all cases where automated processing is performed.

Precise responsibilities should be assigned and clear procedures defined for the operations management and for managing all information processing facilities. Segregation of duties regarding at least the key activities are also paramount, to prevent introduction of fake documents in the production pipeline or incorrect operations management.

ISO/IEC 17799 [3] controls in clause 10.1 should be implemented, such as change management, separation between development, test, operational environment, and segregation of duties.

MinIP

No special provisions.

CAP-TSP

a) Clear and detailed procedures should 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.

ISO/IEC 17799 [3] controls in clause 10.1 should be implemented.

5.2.7.2 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.

MaxIP

Having outsourced part or the whole of the fiscally relevant electronic document provision service does not relieve the principal party from their responsibility, hence it should be their duty to ensure that their outsourcers comply with all the necessary obligations.

ISO/IEC 17799 [3] controls in clause 10.2 should be implemented.

MinIP

No special provisions.

CAP-TSP

The outsourcing party should 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.

ISO/IEC 17799 [3] controls in clause 10.2 should be implemented.

5.2.7.3 System planning and acceptance

Objective: To minimize the risk of systems failures.

MaxIP Fiscal electronic document issuing organizations 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.

ISO/IEC 17799 [3] controls in clause 10.3 should be implemented.

MinIP No special provisions.

CAP-TSP Fiscal electronic document issuing organizations 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 should be addresses by a Service Level Agreement.

ISO/IEC 17799 [3] controls in clause 10.3 should be implemented.

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.

5.2.7.4 Protection against malicious and mobile code

Objective: To protect the integrity of software and information.

MaxIP Macros and hidden code, capable to surreptitiously change the fiscally relevant documents presentation, should be absent from fiscally relevant electronic documents. Where users have no reliable way to ascertain that no such kind of malicious code is present, all macros and hidden code should be removed from these documents.

ISO/IEC 17799 [3] controls in clause 10.4 should be implemented.

MinIP No special provisions.

CAP-TSP See clause 5.1.3.5. as regards malicious code in documents.

ISO/IEC 17799 [3] controls in clause 10.4 should be implemented.

5.2.7.5 Back-up

Objective: To maintain the integrity and availability of information and information processing facilities.

MaxIP Organizations should arrange their physical, processing, personnel structure in order to meet the requirements of exhibiting fiscally relevant electronic documents even in case of accidents affecting their main site(s). This should imply arranging suitable back-up storage sites and a recovery plan to be put into operation when necessary.

Controls in clause 10.5 of ISO/IEC 17799 [3] should be implemented.

MinIP No special provisions.

CAP-TSP Fiscally relevant electronic documents exhibition requirements should be fulfilled even in case of accidents affecting their main site(s). This should imply arranging suitably built and equipped back-up storage sites and a recovery plan to be put into operation when necessary.

Controls in clause 10.5 of ISO/IEC 17799 [3] should be implemented.

However, 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.

5.2.7.6 Network security management

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

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

Controls in clause 10.6 of ISO/IEC 17799 [3] should be implemented.

MinIP No special provisions.

CAP-TSP Networks regarding fiscal documents issuance and storage should be protected to ensure that neither unauthorized data are inserted to or deleted from the document issuing, or storing, process, nor any confidential information is disclosed.

Controls in clause 10.6 of ISO/IEC 17799 [3] should be implemented.

5.2.7.7 Media handling

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

MaxIP Media protection should be enforced during their entire handling process to ensure integrity of their content, prevention of hidden codes insertion and possible compromise of their content confidentiality, starting from their purchase/delivery, through their storage and installation (where applicable), up to their disposal.

ISO/IEC 17799 [3] controls in clause 10.7 should be implemented.

MinIP No special provisions.

CAP-TSP Media protection should be enforced during their entire handling process to ensure integrity and confidentiality of company data and keys up to and including their authorized disposal.

ISO/IEC 17799 [3] controls in clause 10.7 should be implemented.

5.2.7.8 Exchange of information

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

MaxIP Wherever applicable, information should be securely exchanged between different issuing or storing system components, between the document issuer and its customers (i.e. the taxable persons it is acting on behalf of), as well as with its customers' counterparts (e.g. invoice recipients, Chamber of Commerce, etc.). This addresses all communications facilities.

ISO/IEC 17799 [3] controls in clause 10.8 should be implemented.

MinIP No special provisions.

CAP-TSP Wherever applicable, fiscally relevant information should be securely exchanged between all systems components and whatever parties. This addresses all communications facilities.

ISO/IEC 17799 [3] controls in clause 10.8 should be implemented.

5.2.7.9 Electronic commerce services

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

MaxIP ISO/IEC 17799 [3] controls in clause 10.9 should be implemented.

MinIP No special provisions.

CAP-TSP When the electronic commerce is managed by the organization on behalf of its customers (i.e. the taxable persons it is acting on behalf of), the electronic commerce information flow between this person and its counterparts is managed by the organization in secure mode.

In particular ISO/IEC 17799 [3] controls in clause 10.9 should be implemented.

5.2.7.10 Monitoring

Objective: To detect unauthorized information processing activities.

MaxIP NOTE: Even when non explicitly mandated by the applicable legislation, auditing/monitoring is paramount for a trusted organization.
ISO/IEC 17799 [3] controls in clause 10.10 should be implemented.

MinIP No special provisions.

CAP-TSP Suitable auditing/monitoring is paramount for a trusted organization.

ISO/IEC 17799 [3] controls in clause 10.10 should be implemented.

5.2.8 Access control

5.2.8.1 Business Requirement for Access Control

Objective: To control access to information

MaxIP ISO/IEC 17799 [3] controls in clause 11.1 should be implemented.

MinIP No special provisions.

CAP-TSP ISO/IEC 17799 [3] controls in clause 11.1 should be implemented.

5.2.8.2 User access management

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

MaxIP Organizations issuing and storing fiscal documents on behalf of customers should implement, even where not required by legislation or regulations in force or, where necessary, in addition to such requirements, rigid measures to duly manage the entire process of authorising users to access the processed data, from the users' registration to their deregistration, also addressing suitable authentication management procedures.

ISO/IEC 17799 [3] controls in clause 11.2 should be implemented.

MinIP No special provisions.

CAP-TSP Rigid measures should be implemented to duly manage the users' authorization to access the processed data, from the users' registration to their deregistration, also addressing suitable authentication management procedures.

ISO/IEC 17799 [3] controls in clause 11.2 should be implemented.

5.2.8.3 User responsibilities

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

MaxIP External and internal authorized users should be made aware in writing both of their responsibilities in meeting the security measures in force (e.g. password secrecy) and of the need for their cooperation to prevent unauthorized accesses, for example by reporting identified security weaknesses. Where applicable a clean desk policy should be carefully enforced.

ISO/IEC 17799 [3] controls in clause 11.3 should be implemented.

MinIP No special provisions.

CAP-TSP External and internal authorized users should 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 should be carefully enforced.

ISO/IEC 17799 [3] controls in clause 11.3 should be implemented.

5.2.8.4 Network access control

Objective: To prevent unauthorized access to networked services.

MaxIP Organizations that issue and store fiscal documents, that implement on line connections with their customers and with their customers' counterparts, should have in place and enforce processes that duly manage and monitor access authorizations to their networked services.

ISO/IEC 17799 [3] controls in clause 11.4 should be implemented.

MinIP No special provisions.

CAP-TSP Organizations that issue and store fiscal documents, that implement on line connections with their customers and with their customers' counterparts, should have in place and enforce processes that duly manage and monitor access authorizations to their networked services.

ISO/IEC 17799 [3] controls in clause 11.4 should be implemented.

5.2.8.5 Operating system access control

Objective: To prevent unauthorized access to operating systems.

MaxIP Access control to operating systems should be carefully implemented, to prevent unauthorized access to key resources. Where possible operating systems verified as conformant to a suitable level of commonly accepted security criteria like ISO/IEC 15408 [12] should be adopted. Logs should be carefully inspected.

ISO/IEC 17799 [3] controls in clause 11.5 should be implemented.

MinIP No special provisions.

CAP-TSP Access control to operating systems should be carefully implemented, to prevent unauthorized access to key resources.

Logs should be carefully protected and inspected.

ISO/IEC 17799 [3] controls in clause 11.5 should be implemented.

5.2.8.6 Application and information access control

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

MaxIP An organization handling and processing business and fiscally relevant document on behalf of third parties should have in operation a process to manage the entire cycle of strongly authenticating users that access information and their handling applications.

ISO/IEC 17799 [3] controls in clause 11.6.1 should be implemented in relation to storage. Controls in clause 11.6.2 should be implemented in relation to signing keys.

MinIP No special provisions.

CAP-TSP An organization handling and processing business and fiscally relevant document on behalf of third parties should have in operation a process to manage the entire cycle of authenticating users accessing information and related handling applications.

ISO/IEC 17799 [3] controls in clause 11.6.1 should be implemented in relation to storage. Controls in clause 11.6.2 should be implemented in relation to signing keys.

5.2.8.7 Mobile computing and teleworking

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

MaxIP It is to be taken into account that mobile computing is highly prone to attacks of many kinds, from the theft of notebooks to wireless eavesdropping. Therefore should the involved organization adopt these methods, ISO/IEC 17799 [3] controls in clause 11.7 should be implemented.

MinIP No special provisions.

CAP-TSP If mobile computing is adopted, its intrinsically related risks should be carefully evaluated and properly countered.

ISO/IEC 17799 [3] controls in clause 11.7 should be implemented.

5.2.9 Information systems acquisition, development and maintenance

5.2.9.1 Security requirements of information systems

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

MaxIP Security requirements of information systems operated by organizations performing fiscally relevant documents issuance and storage, should be identified and agreed prior to the their development and/or implementation.

ISO/IEC 17799 [3] controls in clause 12.1 should be implemented.

MinIP No special provisions.

CAP-TSP Security requirements of information systems operated by organizations performing fiscally relevant documents issuance and storage, should be identified and agreed prior to the their development and/or implementation.

ISO/IEC 17799 [3] controls in clause 12.1 should be implemented.

5.2.9.2 Correct processing in applications

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

MaxIP Strict controls should be implemented to procedures issuing, especially in bulk, fiscal documents and storing them.

NOTE: In fact there would be severe consequences 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.

ISO/IEC 17799 [3] controls in clause 12.2 should be implemented.

MinIP No special provisions.

CAP-TSP Strict controls should be implemented for signing and storing fiscally relevant documents including bulk signing.

ISO/IEC 17799 [3] controls in clause 12.2 should be implemented.

5.2.9.3 Cryptographic controls

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

MaxIP In countries where sensitive data protection, as addressed by Directive 95/46/EC [11], requires encryption, key management is necessary in addition to what is usually required for signing.

ISO/IEC 17799 [3] clause 12.3 should be implemented.

MinIP No special provisions.

CAP-TSP In countries where sensitive data protection, as addressed by Directive 95/46/EC [11], requires encryption, key management is necessary in addition to what is usually required for signing.

ISO/IEC 17799 [3] controls in clause 12.3 should be implemented.

5.2.9.4 Security of system files

Objective: To ensure the security of system files.

MaxIP ISO/IEC 17799 [3] controls in clause 12.4 should be implemented.

MinIP No special provisions.

CAP-TSP ISO/IEC 17799 [3] controls in clause 12.4 should be implemented.

5.2.9.5 Security in development and support processes

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

MaxIP Applications should be developed, tested and put in operation according to clearly defined security procedures.

ISO/IEC 17799 [3] controls in clause 12.5 should be implemented.

MinIP No special provisions.

CAP-TSP Applications should be developed, tested and put in operation according to clearly defined quality assurance procedures.

ISO/IEC 17799 [3] controls in clause 12.5 should be implemented

5.2.9.6 Technical vulnerability management

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

MaxIP The organization should have in place a regular process to monitor published security vulnerabilities and to consequent timely upgrade the security measures.

ISO/IEC 17799 [3] control in clause 12.6 should be implemented.

MinIP No special provisions.

CAP-TSP A regular process of monitoring published security vulnerabilities should be in place along with a consistent timely upgrade of the security measures.

ISO/IEC 17799 [3] control in clause 12.6 should be implemented.

5.2.10 Information security incident management

5.2.10.1 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.

MaxIP Even where the applicable legislation or regulation does not requires any specific measure to handle security incidents, given the high fiscal relevance of this kind of implementations, it is highly recommended to set in place suitable incident reporting and management procedures and policies involving internal and external officers and users.

ISO/IEC 17799 [3] controls in clause 13.1 should be implemented.

MinIP No special provisions.

CAP-TSP The TSP should have in place suitable incident reporting and management procedures and policies involving internal and external officers and users.

ISO/IEC 17799 [3] controls in clause 13.1 should be implemented.

5.2.10.2 Management of information security incidents and improvements

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

MaxIP For the same reason indicated in clause 5.10.1, managing security incidents and improving the information security management system is highly recommended.

ISO/IEC 17799 [3] controls in clause 13.2 should be implemented.

MinIP No special provisions.

CAP-TSP The TSP should have in place suitable incident management procedures and policies.

ISO/IEC 17799 [3] controls in clause 13.1 should be implemented.

5.2.11 Business continuity management

5.2.11.1 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.

MaxIP The same rationale as in clause 5.2.7.3 MaxIP applies. In fact, there is a need to timely meet the deadlines set by the fiscal regulation and to exhibit the fiscal documents whenever necessary, thus a suitable Business Continuity Plan should be carefully evaluated, taking also into account its benefits, cost of system implementation, legal penalty, insurance policies price, loss of image and of customer base.

ISO/IEC 17799 [3] controls in clause 14.1 should be implemented.

MinIP No special provisions.

CAP-TSP To timely meet the deadlines set by the fiscal regulation also to exhibit the fiscal documents whenever necessary, a suitable Business Continuity Plan should be carefully evaluated. This should be addressed by a Service Level Agreement.

ISO/IEC 17799 [3] controls in clause 14.1 should be implemented.

5.2.12 Compliance

5.2.12.1 Compliance with legal requirements

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

MaxIP Obviously, compliance with the law is required. Where cross border document validity is sought for, it may be necessary to abide by all involved countries legislation/regulations.

MinIP The minimum goal to achieve is to abide by the organization country of residence's legislation/regulation.

CAP-TSP Obviously, compliance with the law is required. Where cross border document validity is sought for, it may be necessary to abide by all involved countries legislation/regulations.

5.2.12.2 Compliance with security policies and standards and technical compliance

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

MaxIP Security Policy compliance should be met.

ISO/IEC 17799 [3] controls in clause 15.2 should be implemented to achieve Security Policy compliance. Where legislations/regulations are applicable, they prevail, but the ISO/IEC 27001 [4] annex A provisions, implemented by adopting the practices indicated in ISO/IEC 17799 [3], should be also used to fill in the possible gaps.

MinIP No special provisions.

CAP-TSP Security Policy compliance should be met.

ISO/IEC 17799 [3] controls in clause 15.2 should be implemented to achieve Security Policy compliance. Where legislations/regulations are applicable, they prevail, but the ISO/IEC 27001 [4] annex A provisions, implemented by adopting the practices indicated in ISO/IEC 17799 [3], should be also used to fill in the possible gaps.

5.2.12.3 Information systems audit considerations

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

MaxIP Auditing according to generally recognized methods is indispensable to ensure continuous trustworthiness to the fiscal documents issuing and storing organizations, even where no specific legal requirement exists in this regard.

ISO/IEC 17799 [3] controls in clauses 15.3.1 to 15.3.2 should be implemented.

MinIP No special provision is specified in addition to what can be required by the relative country legislation.

However it is wished that any organization implementing an ISMS develops and maintains it based on the ISO/IEC 17799 [3], the ISO/IEC 2700x series or a nationally developed guidance.

CAP-TSP Even where no specific legal requirement exists in this regard, an appropriate auditing process should be in place.

ISO/IEC 17799 [3] controls in clauses 15.3.1 to 15.3.2 should be implemented.

Annex A: Country details

A.1 Signature and storage requirements

NOTE: MaxIP, MinIP and CAP-TSP to be removed before passing to ESI.

A.1.1 Signature

A.1.1.1 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 documents.

Country	Details
DE	**Electronic invoices:** Only for electronic transmission of VAT invoices it is required to have an Advanced Electronic Signature with a qualified certificate.
FR	Concerning electronic invoices, an Advanced Electronic Signature is required. But, it is not mandatory to have a qualified certificate.
IT	Where fiscally relevant document are signed, a Qualified Electronic Signature is required, with the exception of customs declarations, where, for historical reasons, a digital signature is still required that can be dubbed a "Directive 1999/93/EC [5] Article 5(2) signature".
SP	BPR, owner of the service Servicio de Certificación de los Registradores, SCR, has defined different certification policies depending on the type of certificate, personal, professional, certificates for persons that are civil servants, certificates for person that represents an entity, or certificates for persons that are registrars. So far BPR system manages PKCS#7 based on qualified certificates, but provisions are made for evolving to XAdES signatures. IGAE's system for public expenses dossiers, on its turn, requires XAdES-BES signature based on qualified certificates. As for e-invoices, Spanish legislation requires Advanced Electronic Signatures with qualified certificates.
UK	There is no legal or statutory requirement for advanced electronic signatures in the UK.

A.1.1.2 Certification

Objective: To obtain certificate from authority who can reliably certify public key and maintain revocation status information.

Country **Details**

DE

All fiscally relevant data:

The non mandatory accreditation includes a thorough analysis by independent third parties on technical, organizational and procedural security implemented.

All CAs in Germany have the accreditation, although not all legal requirements demand it. In legislation you find the whole range of security implemented, from simple electronic signatures to advanced electronic signatures or qualified electronic signatures or qualified electronic signatures with certificates from accredited certificate service providers.

There are no requirements in the general accounting principles. The rules refer only vaguely to "adequate" security measures.

Electronic invoices:

Only for electronic transmission of VAT invoices it is required to have an Advanced Electronic Signatures with a qualified certificate.

FR

Electronic signature of electronic invoices: certificates, not necessarily qualified certificates.

And certificates not necessarily tied to a natural person, but also company certificate accepted.

Value Added Tax e-declaration: certificates issued by a "reference Certificate Authority", i.e. recognized by the MINEFI (Ministry of Economy and Finance).

IT

CAs qualified as per Directive 1999/93/EC [5] article 3(3) are necessary, since Qualified Electronic Signatures are required. There is no need for adopting CAs accredited as per Directive 1999/93/EC [5] article 3(2), but in practice all qualified CAs are also accredited by the relevant Governmental body (CNIPA).

SP

The Business and Property Registry (BPR henceforth), owner of the service Servicio de Certificación de los Registradores, (SCR henceforth), has defined different certification policies depending on the type of certificate, personal, professional, certificates for persons that are civil servants, certificates for persons that represent an entity, or certificates for persons that are registrars.

The so-called "Intervención General de la Administración del Estado" (IGAE henceforth), an internal control entity belonging to the Spanish Finance Ministry and responsible for inspecting the expenses dossiers from the public agencies also for carrying out public audits on the expenses according to the so-called yearly plan for auditing, has put in place a system for managing the submission and approval of expenses dossiers within the Spanish public administration. This system works with qualified certificates aligned with TS 101 862 [16].

For e-invoicing, the AEAT (Spanish Tax Agency) recognizes only certain certificate types issued by a number of CAs.

UK

In UK tScheme is the recognized scheme for 2trustworthy2 CAs, although any assurance scheme (e.g. Webtrust) would be acceptable.

A.1.1.3 Signature creation data

Objective: To ensure that the private signing key is kept secure.

Country	Details
DE	**Electronic invoices:** This is a mandatory requirement as far as qualified electronic signatures with secure signature creation devices need to be used. Generally, no HSM however is accepted, only smartcards or tokens; HSM may only be accepted if evaluated as SSCD against the legal requirements of Signature Legislation. NOTE: It is important to discuss how the bulk signing is done! This also applies to other fiscally relevant data.
FR	For Electronic invoices, there is not an obligation to have private signing key in a HSM. But, the private key is to be kept under exclusive control of the signatory. Where qualified electronic signatures are used, the private key is to be in an SSCD. Software protection is possible concerning other document types.
IT	When creating fiscally relevant documents, qualified electronic signatures are to be used, so a CC EAL4 or ITSEC E3 certified SSCD/HSM is to be used, with the exception of when unsigned e-invoices are sent via EDI (although it is not crystal clear under which security measures).
SP	As per BPR's system, users may go to the corresponding Register office and there they personally generate the key pair using the office's facilities, or they may download key pair generation code for running it on their own machines. In any case, it is necessary that they go to the Register office to obtain the corresponding password-protected cryptographic card. As per the IGAE system, there are plans for generalizing the usage of cryptographic cards for the first term of 2007. As per e-invoice, the "REAL DECRETO 1496/2003, de 28 de noviembre, publicado el 29 de noviembre del 2003" [RD 1496/2003] requires the usage of a secure signature creation device ("dispositivo seguro de creación de firmas") according to article 2, points 6 and 10, of Directive 1999/93/EC [5].
UK	No special requirements.

A.1.1.4 Certificate subject's registration

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

Country Details

DE **Electronic invoices:**

This is a mandatory requirement as far as qualified electronic signatures are used, i.e. in case of electronic invoices (VAT).

In that case the usage of a certificate from a certification service provider is needed. CA's in Germany are following clear guidelines and requirements mentioned in the Electronic Signature legislation.

Registration of the certificate holder: only natural person, is to be identified properly by RA or CA.

The same principles apply for other fiscally relevant data.

FR All MINEFI recognized certification authorities are to respect obligations of document "PC-Type" that is a Certification Policy template. The registration procedures are described, that can be considered consistent with TS 101 456 [17].

IT Requirements on identity and attributes verification at registration are very detailed, and the accreditation process also evaluates the Registration procedures, so, since a Qualified Electronic Signature is mandatory for electronically signed documents, both these aspects are met.

SP In BPR's system the common requirement to all certificate types is to present identity card or similar document. Other "trusted" documents strongly depend on the certificate type (i.e. subject's roles and values) are also required.

Qualified certificates required for using IGAE's system require presentation of identity card or similar document. Registering in the IGAE's service may be done electronically using this certificate.

UK No special requirements.

A.1.1.5 Certificate revocation

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

Country **Details**

DE **Electronic invoices:**

This is a mandatory requirement as far as qualified electronic signatures are used, i.e. in case of electronic invoices (VAT).

In that case the usage of a certificate from a certification service provider is needed. CA's in Germany are following clear guidelines and requirements mentioned in the Electronic Signature legislation.

Revocations: all CA's need to update a revocation list with all revoked certificates; this list or repository can be checked online or at certain time intervals free of charge.

The same principles apply for other fiscally relevant data.

FR All MINEFI recognized certification authorities are to respect obligations of document "PC-Type" that is a Certification Policy template.

Apart that certificates cannot be suspended, the rest is even more rigid than TS 101 456 [17]. For example, in this document it is also specified who can submit a revocation request.

IT Requirements on revocation requesters authentication and authorization are very detailed, and the accreditation process also evaluates revocation, so, since using a Qualified Electronic Signature is mandatory for el-signed fiscally relevant documents, both these aspects are met.

SP BPR's certification policies define the consequences of the certificate revocation and the revocation procedures, addressing also who can request the certificate revocation. The general rule is that the revocation is to be requested in the offices that the Business Registry has designated for these purposes. On special circumstances of high urgency, revocation may also be electronically requested. BPR makes its CRLs publicly available through Web and LDAP. Every time a certificate is revoked, the CRLs are re-published.

IGAE will follow the policy that the so called "Consejo Superior de Administración Electrónica" (Council for Electronic Administration) will define for the Spanish Public Administration (Administración General del Estado).

UK No special requirements.

A.1.2 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.

Country	**Details**
DE	Electronic invoices and general fiscally relevant data: This is explicitly stated for electronic invoices and it follows as a general requirement out of the storage guidelines requiring that the authenticity and the integrity of all electronically stored information need to be verified. However it is not required that the certificates which have been used fro the creation of electronic invoices are still valid when the tax inspection happens.
FR	The law concerning electronic signature of e-invoices says: the recipient of the invoice is to verify the validity of the certificate when he receives the invoice and during the storage period. So, the invoice, the invoice signature and the certificate is to be stored in **the original version.** But, this law says nothing concerning requirements for the verification of the signature of the certificate over the storage period.
IT	All fiscally relevant electronic documents are to be stored electronically. Every 15 days for e-invoices and yearly for other document types a file is created with the digests of each of all stored documents and this file is signed. The signature is to be a Qualified Electronic Signature and is to be also time stamped. Digests file, Qualified Electronic Signature and TST are entrusted to the Tax Authority. No other measure to ensure long life of the signature is required, since the Tax Authority acts as the safe place vouching for the signature and TST validity in the years. NOTE: Due to a current lack of regulation on how to forward this time stamped signature to the Tax Authority, the implementation of the above provision is suspended. Furthermore, Time Stamping Authorities, including accredited QCA that is to also provide such service, will keep all issued TSTs on non modifiable media (be they physically or logically WORM) for at least 5 years. Special agreements can be arranged with customers to lengthen this period. These TSTs have legal value.
SP	Corporate accounts have to be stored for 5 years. When these documents are delivered to BPR electronically signed, the system verifies the signature and signs and time-stamps an electronic notification that will prove in the future that the sender's certificate is valid at that time. As for public administration expenses dossiers within IGAE's system, this has still to be regulated through a future law dealing with e-Government. As for e-invoices, the "REAL DECRETO 1496/2003, de 28 de noviembre, publicado el 29 de noviembre del 2003" [RD 1496/2003] mandates that the storage is made in such a way that ensures readability in their original format, as well as availability of electronic signature associated data and mechanisms.
UK	No special requirements.

A.1.3 Storage

A.1.3.1 Authorized access

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

Country **Details**

DE **Electronic invoices and general fiscally relevant data:**

The accounts need to be made available to the tax inspectors and law enforcement officers on request (direct online access not required). Very often the rule says "remote-access", which is access to accounting data on media like CD, DVD, WORMs etc. but not into the live system.

Storage is to support the requirements of the data protection directive.

There is only a general requirement: that data need to be accessed without any limitation for filtering, calculations etc. This principle is ruling the computerized tax auditing.

The storage procedures or applications need to be properly documented in order to guarantee that the stored data can be accessed again without difficulties.

There are specific rules on the storage of computerized accounting systems. These principles are:

remote access is not online access;

access can be immediate access, mediated access to the database or the data management system or handover of stored data on storage media.

FR Concerning electronic invoices and their signature, an obligation exists to make the documents available to the French government:

At administration's request, data is to be returned in clear language by the company in charge of assuring that an invoice has been issued, even if it is not the same person/company issuing the invoice; Clear language means "to provide information in a format commonly admitted in the commercial domain". The information can be required from the sender and the recipient; the information is to be returned on screen, on an electronic media or on paper, if the tax administration asks for it.

There is no technical aspect in order to respect this obligation.

IT Tax Authority inspectors have the right to access any fiscally relevant document, that, when electronically stored, is to be accessible, along with the related certificates, also by telematic means, as well as transferable to electronic or paper media. This data is to also be accessible via indexed searches.

SP BPR's system performs Access Control. Book accounts are accessible to the owners and the Spanish Tax Agency inspectors.
Annual account books only accessible to persons that have already been registered in the service and after having paid the corresponding fee for every access.
A recent Spanish law make this information accessible to any public servant and notary . Use of electronic signature is required in these cases.

Access to public expenses dossiers within IGAE's databases is made through an intranet using dedicated lines and secure authentication only by IGAE's auditors. The security policy defines who and how this access is to be made.

UK The accounts need to be available to the tax inspectors and law enforcement officers on request (direct online access not required).

Storage needs to support the requirements of the data protection directive.

A.1.3.2 Authenticity and integrity

Objective: To maintain the authenticity of origin and integrity of a set of fiscally relevant data, also detecting loss or unauthorized addition of documents, held in storage for the legally required period.

Country **Details**

DE **Electronic invoices:**

Documents as well as data describing or testimonials of authenticity and integrity of the data (e.g. qualified electronic signatures) are stored.

General fiscally relevant documents:

No specific requirement regarding the need of electronic signatures.
This general principle would imply that the documentation of the procedures and the log files of the transmission etc. is to be stored, to guarantee that no change has taken place during the transmission. This implies that e.g. the original messages have to be stored and should be linked to any other document (e.g. contracts, etc.).

FR Concerning electronic invoices **,an advanced electronic signature is used.** E-invoices integrity is ensured by the signatures applied to them. All data (invoices, signature, certificate) is to be stored in original format. The legislation also allow other mechanisms like EDI which ensures integrity of invoices.

IT Fiscally relevant documents integrity is ensured by using Qualified Electronic Signature and by the measures in clause A.1.2 "Maintenance of Signature over storage period" that ensure that no fiscally relevant document is changed or deleted, either intentionally or by accident.

NOTE: Changes due to malicious code are not addressed here nor in clause A.1.2. They are addressed in clause A.1.3.5.

SP The integrity of the documents delivered to BPR is ensured by their being signed. Once the documents have been signed, they are electronically submitted to the BPR using a SSL secure channel.

The integrity of documents delivered to IGAE is ensured by their signatures and the access control imposed in its intranet.

E-invoices integrity is ensured by the signatures applied to them. The legislation also allow other mechanisms like EDI when mechanisms are in place for ensuring integrity.

UK VAT Invoices may be protected by any mechanism that "imposes a satisfactory level of control over the authenticity and integrity of your invoice data".

The supporting invoice data is to be "accurate and complete". Similar requirements exist for the processing of accounts. This includes requirements that loss or addition of documents is detected.

The invoices need to be held as sent/received (i.e. in their original format) and have to be accessible and readable throughout the storage period.

Allow other mechanisms than "Advanced Electronic Signatures" for integrity of VAT invoices.

Generally, no specific requirement for other types of fiscally relevant document.

A.1.3.3 Readability

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

Country **Details**

DE

Data is not be corrupted and made unreadable, e.g. because of occurred changes or damages. From that point of view "readability" means that data should not be damaged.

They should also not be encrypted or if encrypted, there should be a decryption tool available.

Data may be machine readable or human readable. No specific requirement for PDF or any other format, which allow humans to read and understand. It needs to be noted that if the data are stored only in a format like PDF or TIFF etc. these formats are not allowed for archiving purposes. PDF or similar can only be in addition to the original electronic data.

Machine-readability is to also be guaranteed, i.e. all relevant data without limitation as regards filtering, controlling, cross checking, etc.

Electronic invoices:

The invoices have to be readable during the complete storage period. No changes whatsoever are allowed. Invoices have to be accessible and readable throughout the storage period. Any transformation or conversion of data needs to be documented.

General fiscally relevant data:

General fiscally relevant documents need to be "auditable" by tax authorities without any limitation; any change of format, any conversion has to be noted down.
In case of using electronic signatures or cryptographic processes the keys have to be stored.

FR

As regards electronic invoices, an electronic invoice is defined as a structured message with the possibility to be read by a computer and to be automatically processed with one-to-one means. All electronic invoices have to be stored in their original format.

If requested by the French tax administration the document has to be transposed into a paper format.

IT

Readability of all documents stored as per the rules in force is to be ensured: documents have to be in an "un-modifiable" format, i.e. without any macro or hidden code, since they can change the documents presentation, as specified in clause A.1.3.5.

Where documents are becoming unreadable for whatever reason, documents have to be converted to another format, provided that a trusted person attests the correspondence of the content.

SP

Readability of both annual accounts and book accounts has to be preserved. Document's formats (TIFF or text) are specified by BOE (Boletin Oficial del Estado) the official bulletin publishing Spanish legislation.

BPR system includes mechanisms able to detect malicious code and macros within incoming electronic documents.
As said before, e-invoices "readability" have to be preserved in their original format.

UK

Invoices have to be accessible and readable throughout the storage period.

A.1.3.4 Storage media type

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

Country **Details**

DE

Storage media can be optical media or any other electronic storage media (e.g. disks, CD-Rom, DVDs, etc. It can also be disks, as long as their file systems are FAT or MS-DOS). There is no specific technology mentioned.

The storage is to be on a medium which does not allow any changes. In case of temporary storage on changeable media the IT system has to be able to guarantee the integrity.

FR

All messages are to be kept/stored in their original format:

-on a numeric support during at least six years;

-on a support chosen by a company during the following three years.

If a hardware and/or software environment had been modified, the company has to do the conversion and keep the compatibility of files with the original format.

IT

The only requirements clearly mandated is:

1) The stored document has to be legible in any moment at the storing organization's, etc.

2) The stored document can be also exhibited with telematic means.

Apart from this, the person in charge of the storage is to periodically verify (at most every five years) that stored documents are still actually readable. In order to prevent one media to become unreadable, because of technical obsolescence or physical degradation, its content is to be timely copied onto another suitable media.

SP

Storage media used by BPR system is to be such that satisfy the requirement of readability of both annual accounts and book accounts by those entities and persons identified in a previous clause.

UK

Invoices have to be accessible and readable throughout the storage period.

A.1.3.5 Documents format

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

Country	Details
DE	As regards the format of electronic documents in general, no specific format is required by law. As regards fiscally relevant documents in electronic format, they have to be protected against loss of integrity by technical or organizational measures. As regards readability by tax inspections machine-readable type of data are preferred, as they can be checked by digital tax inspection methods.
FR	According to the law, an electronic invoice is a structured message with the possibility to be read by a computer and to be automatically processed with one-to-one mean. For example, XML and PDF formats can be used for electronic invoices, but this is not the case for Word, Excel formats.
IT	Electronically signed documents are to have neither macros nor any hidden code whatsoever. This is more rigid than the general electronic signature requirements that demands hidden code not to change the document presentation.
SP	Annual and book accounts formats for being submitted to BPR, are specified in BOE the official daily bulletin for publishing Spanish legislation. So far TIFF and text formats have been defined. Work on XBRL is now starting. Electronic documents' format exchanged with IGAE are also specified in BOE.
UK	XML is generally the preferred format for Tax related reports. No restrictions on VAT invoices.

A.1.3.6 Separation and confidentiality of stored data

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

Country	Details
DE	The storage is to be clearly separated between the different companies; it can be the same company storing the data, but the storage or the archives is to be clearly separated, e.g. different storage media.
FR	The same company can store information of several companies using separate means; a common storage for invoices of several companies does not conform to the law.
IT	No specification related to service providers providing storage services for multiple taxable persons. The relevant Decree by the Ministry of Economy and Finance 23/1/2004 states (Article 3(1) letter d): "*Fiscally relevant electronic documents …. are stored … provided that their chronological order is assured and there is no solution of continuity for each tax period; furthermore, search and extraction functions must be provided for the information from the electronic archives based on surname, name, denomination, fiscal code, VAT registration number, date or logical association of them.*"
SP	Both BPR and IGAE systems satisfy the requirement of keeping the documents coming from each entity separated from the documents coming from the rest of entities.
UK	No special provisions. Information generally treated as company confidential.

A.1.4 Reporting to and exchanging data with authorities

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

Country **Details**

DE **Electronic invoices and general fiscally relevant data:**

Access is generally granted only to tax authorities, the access modes are defined as remote. The data is to be stored on an unchangeable medium.

FR Companies have to declare their Value Added Tax by electronic means. This declaration is to be digitally signed if the declaration is made via the WEB. The connexion is along a secure channel (HTTPS) and client authentication (by certificate) is used.

IT Companies have to deposit their accounting reports yearly at the relative Chamber of Commerce solely in electronic format, signed with a Qualified Electronic Signature.

Other fiscally relevant electronic documents will be entrusted to the relevant authority as soon as the specific provision is issued, as specified in clause A.1.2. Every 15 days for e-invoices and yearly for other document types a file is created with the digests of the stored documents. It is signed with a Qualified Electronic Signature and time stamped. Digests file, Qualified Electronic Signature and TST are entrusted to the Tax Authority.

Customs related declarations are to be signed with a Directive 1999/93/EC [5] article 5(2) signature.

SP Companies can electronically and securely submit their book accounts and annual accounts (balance sheets) to the Business Registry. They have to perform this submission yearly. The exchange takes place using a secure channel (SSL). The electronic documents are signed by the sender in order to protect their integrity and to identify the sender, using the certificate issued by the SCR service.

Public agencies securely submit their signed expenses dossiers and receive signed reports authorizing such an expense or identifying potential problems in the submitted dossiers.

Access to e-invoices is to be granted to the Spanish Tax Agency.

UK Submission of accounting reports is generally protected using SSL with clients authenticated by password or authentication certificate.

A.1.5 Conversion of paper originals to digital formats

Objective: To ensure that, when fiscally relevant documents originally in paper, or other non-digitally encoded formats (e.g. audio, microfiche) are converted into digital format, their content is preserved without any change.

Country **Details**

DE **Electronic invoices and general fiscally relevant data:**

If originally paper documents have been scanned in, it has to be secured that the paper and the electronic data are matching.

FR The law about image of original document requires that the copy is to be an exact and durable reproduction of original document. This verification is to be made when the copy is created. This copy can be given as proof if the original does not exist any more.

There is an important exception as regards electronic invoices: When a paper invoice has already been issued, the scanned paper invoice cannot be considered as the original even if the scanned version has an electronic signature.

IT Documents that are originally analogical (e.g. on paper) can be transformed in electronic format, e.g. by scanning them, or, for those being produced, by keeping their print images/converting them into a suitable readable and unchangeable format. The correspondence between electronic and analogic format is ensured via a Qualified Electronic Signature:

1) issued by the person in charge of storage if these documents are not in unique copy, i.e. if their content can be rebuilt from other documents that have to be kept, even by other subjects;

2) issued by a notary or other public officer if they are in unique copy.

SP No regulation generally applicable to any scanned paper document exists so far in Spain; only for specific types of documents, none of which affects any document exchanged within IGAE's system.

Scanned documents are allowed by BPR if they are electronically signed. An exception is external audit reports on corporates. Even if they are scanned and electronically submitted, the original documents are required.

As per invoices, it is foreseen to give legal support to their digitalization.

UK No special provisions.

A.2 Information security management

A.2.1 Security policy

A.2.1.1 Information security policy

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

Country **Details**

DE No mandatory provisions. But it would be recommendable that the guidelines from industry organizations are taken into account.

In some areas like electronic invoicing for VAT purposes it is required that the IT procedures of electronic invoicing are documented.

In addition, the "IT Grundschutz Manual" of the German "Bundesamt für Sicherheit in der Informationstechnik" (BSI) is to be mentioned as a guidance to implementing a suitable ISMS.

FR No general requirement exists for security policy. Concerning Data storage, many companies follow the standard AFNOR (NF Z42-013 and NF Z 43-400). But, it is not an obligation.

IT No general requirement exists in Italy for security policy in the fiscally relevant digital documents field.

Regarding electronic fiscal documents storage, the relevant Decree by the Minister of Economy and Finance (DMEF 23/1/2004) mandates abidance by CNIPA Deliberation 11/2004 addressing what is called "Conservazione sostitutiva" (Substitutive [*document*] conservation). This Deliberation requires that implementing organizations specify the adopted security measures, but no indication even on how this documentation is to be structured is given.

Something similar to a Security Policy document is instead required for organizations providing complementary services to the organizations at issue such as QCAs and REM (Registered E-Mail) providers.

NOTE: Being a QCA requires to abide by specific rules, some requirements, like storing revocation information, lie upon them instead of on the organizations under discussion, thus relieving the latter ones of this accomplishment. Similar remarks apply to REM providers, that are required to authenticate senders and to keep track of what is sent and delivered.

SP BPR has defined a security information policy that accomplishes with the "LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal", on protection of personal data and put restrictions on access to the information. Intentions are to progress towards alignment with ISO/IEC 17799 [3].

As for IGAE, its system follows the requirements established by the security policy defined by the so-called "Comité de coordinación de la seguridad informática" (security coordination committee, horizontal within the Finance Ministry), that deals with this kind of issues. It is the intention of this committee to align this policy with ISO/IEC 17799 [3].

UK No special provisions.

ISO/IEC 17799 [3] controls in clauses 5.1.1 to 5.1.2 appropriate to both signatures and storage.

A.2.2 Organizing information security

A.2.2.1 Internal organization

Objective: To manage information security within the organization.

Country	Details
DE	No mandatory provisions. But it is recommended that the guidelines from industry organizations and from auditors are taken into account. In some areas like electronic invoicing for VAT purposes it is required that the IT procedures of electronic invoicing are documented. See also the IT Grundschutz Manual.
FR	No specific requirement.
IT	No specific requirement. Something similar to a Security Policy document is required for QCAs and REM providers, that also addresses the need for Security policy management and for appointment of specific security officials.
SP	BPR has an offices in each capital of province in Spain and in other cities. Each office deals with the documents that are submitted to it and is responsible for them. Situations are strongly dependant on the size of the city, the resources of the specific register and the volume of managed documentation but electronic access is provided by a centralized system that performs access control. The information security organization within IGAE follows the dictates of the security policy defined by the security coordination committee. There exists the role of the Security Corporative Manager.
UK	No special provisions. ISO/IEC 17799 [3] controls in clauses 6.1.1 to 6.1.8 appropriate to both signatures and storage.

A.2.2.2 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.

Country **Details**

DE No mandatory provisions.

But it would be recommendable that the guidelines from industry organizations and from auditors are taken into account. In some areas like electronic invoicing for VAT purposes it is required that the IT procedures of electronic invoicing are documented. In case of external service providers there need to be clear contracts in place separating the tasks and clearly describing the authorizations.

See also the IT Grundschutz Manual.

FR No specific requirement concerning signature asset.

Many companies respect the standard AFNOR Z42-013. In this document, there are recommendations when an external party is present in the storage process:

A contract is to be signed between the company and the external party.

The company has to verify if the external party complies with the standard AFNOR Z42-013.

External party has to give attestation to prove the capacity to do the work.

IT No detailed requirements on outsourcers are specified in the applicable regulation, however, the organizations outsourcing the substitutive conservation are always and in any case responsible for the conservation, even when implemented by external organizations, therefore which measures they impose on outsourcers is a private matter between these parties and is irrelevant to the legislation.

The same responsibility principle applies to QCAs and REM providers.

SP No special provisions as BPR's internal information is not accessed, processed, communicated or managed by external parties.

UK No special provisions.

ISO/IEC 17799 [3] controls in clauses 6.2.1 to 6.2.3 appropriate to both signatures and storage.

A.2.3 Asset management

A.2.3.1 Responsibility for assets

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

Country **Details**

DE No general provisions.

In case of accredited certificate service provider there is a range of additional security measures to be looked at.

See also the IT Grundschutz Manual.

FR Concerning electronic invoices, the only requirement concerning signature is that "*certificate signing key pair must be activated under exclusive control of the signatory*".

Concerning activating DATA for private key of CA recognized by French government (PRIS V1):

"The control of the CA private key is to be made with authentication of n among m person."

PRIS V2 :

This data is to be protected with integrity and with confidentiality. A trusted person must be assigned the responsibilityof this data . In the higher level, there has to be at least two people.

Only these people can access this data

Concerning personal data, there is a law "2004-801" which gives a lot of requirements.

If you have personal data in our system (disk etc.), we have to make a statement to the French entity CNIL (La Commission Nationale de l'Informatique et des Libertés). This data is to be protected with integrity and with confidentiality.

IT The only requirement as per legal rules, is that that each signing device is to be under the sole control of the signer and that, when the signing key pair is generated by the signer, it is to be generated inside the SSCD. No other asset related responsibility is addressed.

SP BPR establishes that the signing devices are to be under the control of the signer. Users may go to the corresponding register office and personally generate the key pair using the office's facilities, or they may download key pair generation code for running it on their own machines. In any case, they are to go to the register office to obtain the corresponding cryptographic card, for which they are responsible.

UK No special provisions.

ISO/IEC 17799 [3] controls in clauses 7.1.1 to 7.1.3 appropriate to both signatures and storage.

A.2.3.2 Information classification

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

Country	Details
DE	No general provisions. In case of accredited certificate service provider there is a range of additional security measures to be looked at. See also the IT Grundschutz Manual.
FR	No such requirement is specified in the French legislation. There exist in France three level in norm PRIS V2 (template of certification policies for signature, authentication and encryption services, template of timestamp policy) about the information : level one : information that has medium sensitivity and criticality; level two : information that has high sensitivity and criticality; level three : information that has very high sensitivity and criticality. NOTE: The provision in level three is more strict than in level one. In these three levels the private key and its activation data is to be kept by the certificate owner. We can note that reference certificate authorities are to follow the level one.
IT	No such requirement is specified, apart from the signing private key, its activation data, and the secret code assigned to a certificate owner to request for his certificate revocation in emergency, that are to be kept confidential. In addition, personal sensitive data are to be handled as per the persona data protection laws (namely Dlgs 196/2003).
SP	Annual accounts are publicly accessible once the corresponding fee has been paid. Book accounts are not publicly accessible (only registers, tax inspectors, public servants and notaries may access them). BPR also manage property information, which is not accessible on line. There are a number of different types of property information managed by BPR, classified by degree of criticality. Public administrations expenses dossiers within IGAE's data base are accessed in a controlled way. The operations that may be performed by each person depends on its specific position within IGAE.
UK	No special provisions. Accounting information may be handled under a single classification unless required otherwise for business reasons. Private signing keys will require special handling procedures.

A.2.4 Human resources security

A.2.4.1 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.

Country	Details
DE	No general provisions. In case of accredited certificate service provider there is a range of additional security measures to be looked at. Selection of staff and surveillance of staff depending on the sensitivity of workplaces. See also the IT Grundschutz Manual.
FR	No such requirement is specified in the French legislation. Norm PRIS V2 recommends: *All employees working for the CA service are to sign a confidentiality clause on their job.* *Companies are to be sure that their employees are competent in their jobs.*
IT	No requirement: privacy rules impose strong limitations to this kind of screening.
SP	No requirements are specified in Spanish legislation, nevertheless, BPR assesses technical qualification before contracting people who will work in its CA service. Being a public agency IGAE has to follow the regulated public competition system for that part of the staff who are civil servants.
UK	No special provisions. ISO/IEC 17799 [3] controls in clauses 8.1.1 to 8.1.3 appropriate to both signatures and storage.

A.2.4.2 During employment

Objective: To 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.

Country	**Details**
DE	No general provisions. In case of accredited certificate service provider there is a range of additional security measures to be looked at. Selection of staff and surveillance of staff depending on the sensitivity of workplaces. See also the IT Grundschutz Manual.
FR	No requirement for this objective.
IT	Privacy and Trade Union rules prevent from an arbitrary direct monitoring that may imply a remote control on personnel's operations. On the other hand the rules in force, be they provided by the Civil and/or Criminal Code or by the labour collective contract, allow for disciplinary actions, or worse, to be undertaken should personnel's misbehaviour be ascertained. QCAs and REM providers are explicitly required to have in place a training programme to ensure that all involved personnel is suitably and timely educated on their duties, on the involved SOFTWARE and HARDWARE products and on the procedures to enforce.
SP	No specific requirements on Spanish legislation, nevertheless BPR organizes a formative course once per year. IGAE also supports formative courses for its selected staff (like those for getting the ISACA certificate on security auditing).
UK	No special provisions. ISO/IEC 17799 [3] controls in clauses 8.2.1 to 8.2.3 appropriate to both signatures and storage.

A.2.4.3 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.

Country **Details**

DE No general provisions.

In case of accredited certificate service provider there is a range of additional security measures to be looked at. Selection of staff and surveillance of staff depending on the sensitivity of workplaces.

See also the IT Grundschutz Manual.

FR No requirement for this objective.

IT No such requirement exists in the regulations, since it is the employer's responsibility to meet the necessary security needs.

SP Within the team responsible of PKI in BPR, when an employee leaves it, he has to give back his cryptographic token for accessing the system to his superior.

The "Resolución de 24 de mayo de 2005 de la IGAE, publicada en el BOE de 17 de junio de 2005." [R 144/2005] establishes that when a member of IGAE staff leaves IGAE, his role as user of IGAE's system is to automatically finish, and that his immediate superior within IGAE's hierarchy is responsible for ensuring the enforcement of this rule.

UK No special provisions.

ISO/IEC 17799 [3] controls in clauses 8.3.1 to 8.3.3 appropriate to both signatures and storage.

A.2.5 Physical and environmental security

A.2.5.1 Secure areas

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

Country **Details**

DE No special provisions.

In case of accredited certificate service provider there is a range of additional security measures to be looked at. Selection of staff and surveillance of staff depending on the sensitivity of workplaces. Needs to be described in the security policy.

See also the IT Grundschutz Manual.

FR There is no requirement concerning signature asset.

However, for Storage, some companies follow the standard AFNOR Z 42-013. In this standard, some recommendations are given for secure areas :

There must be several secure areas in order to split stored data.;

Every area must be physically protected.

IT No specific requirement exists on the fiscally relevant documents issuing organizations. Instead Qualified Certification Authorities and REM providers are to ensure that systems are located in secured areas and that access to their systems and applications, as well as to the related premises, is allowed only to authorized personnel and logged.

CNIPA Deliberation 11/2004 (by which also conservation of fiscally relevant electronic documents is to abide) requires that the person in charge of substitutive (documents) conservation implements suitable measures (this person is to choose) to ensure physical and logical security of the storing system and of the involved media.

SP Access to the Data Processing Centre of the BPR's CA requires cards and biometric devices. As for the register offices spread all around the country, the situation is very different, depending on the size of the city and the volume of managed data.

IGAE's database is also physically protected by a number of security measures established in the security policy defined by the security coordination committee.

UK No special provisions.

ISO/IEC 17799 [3] controls in clauses 9.1.1 to 9.1.6 appropriate to both signatures and storage.

A.2.5.2 Equipment

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

Country **Details**

DE No general provisions.

In case of accredited certificate service provider there is a range of additional security measures to be looked at. Selection of staff and surveillance of staff depending on the sensitivity of workplaces. Needs to be described in the security policy.

See also the IT Grundschutz Manual.

FR No specific requirement for this objective.

IT No specific requirement exist. QCA related duties, apart from those related to the certificate issuing system, are to be derived from a suitable risk assessment they are supposed to perform and the result of which is to be included in their Security Plan.

However, CNIPA Deliberation 11/2004 (see bibliography) requires that the person, in charge of substitutive conservation, implements suitable measures to ensure media physical and logical security.

SP No specific provisions in BPR. Very different situations depending on the city. Higher degree of protection put in place in the equipment within the CA's CPD.

The "Resolución de 24 de mayo de 2005 de la IGAE, publicada en el BOE de 17 de junio de 2005." [R 144/2005] establishes that all the work stations within networks pertaining to IGAE is to be set-up according to a well established technical procedure for computing systems integration.

UK No special provisions.

A.2.6 Communications and operations management

A.2.6.1 Operational procedures and responsibilities

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

Country	Details
DE	No general provisions. Segregation of duties is of particular importance in accounting arena, also with regards key management. See also the IT Grundschutz Manual.
FR	There is no requirement concerning signature asset. However, for storage, some companies follow the standard AFNOR Z 42-013. In this standard, some recommendations are given for operational procedures : *"Operational procedure must exist and must be written with some information concerning methods and organizations to manage stored data (creation, destruction, reading, printing stored data)"*.
IT	Information processing management and operation requirement, such as segregation of duties, is requested for Qualified Certification Authorities only and just at high level.
SP	Segregation of duties is performed within the BPR's CA team. IGAE also performs segregation of duties: management is segregated from auditing. As per information security, development and maintenance duties are segregated from production and exploitation. Roles and responsibilities are clearly specified in the "Resolución de 24 de mayo de 2005 de la IGAE, publicada en el BOE de 17 de junio de 2005". [R 144/2005] regulating access control to data bases of IGAE.
UK	Segregation of duties (ISO/IEC 17799 [3] clause 10.1.3) is of particular importance in the accounting arena, also with regards to key management. ISO/IEC 17799 [3] controls appropriate to both signatures and storage

A.2.6.2 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.

Country	Details
DE	No general provisions. Clear contracts need to in place in case of outsourcing. See also the IT Grundschutz Manual.
FR	No specific requirement for this objective.
IT	No requirement is specified, since this obligation is implied by the principal organization being responsible for anything regarding the service, including incidents. To QCAs provisions of Article 6 of Directive 1999/93/EC [5] apply: "*A certification service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:…unless the certification-service-provider proves that he has not acted negligently*". REM providers are to ensure that, apart from disasters, their service up time is 99,8 % on each quarter, with a maximum system down time per single incident of 50 % of the above service level. This applies also when services are outsourced.
SP	BPR's PKI services are offered 24 hours per day. Delivery of publicly available information electronically requested is to occur within the following 48 hours, otherwise, this information is to be given for free. BPR has defined a number of quality of service parameters.
UK	No special provisions. ISO/IEC 17799 [3] controls appropriate to both signatures and storage

A.2.6.3 System planning and acceptance

Objective: To minimize the risk of systems failures.

Country	Details
DE	No general provisions. See also the IT Grundschutz Manual.
FR	No specific requirement for this objective.
IT	No special provisions for fiscal documents issuers. REMs are implicitly obliged to plan in advance their system requirements so to abide by the legally required service level.
SP	BPR conducts statistics of its SCR system. It has concluded that April and July are the busiest months in terms of book and annual accounts submission. It then, increases its staff and the contracted bandwidth during the last weeks of these months.
UK	No special provisions. ISO/IEC 17799 [3] controls appropriate to both signatures and storage

A.2.6.4 Protection against malicious and mobile code

Objective: To protect the integrity of software and information.

Country	Details
DE	No general provisions. See also the IT Grundschutz Manual.
FR	No specific requirement for this objective.
IT	Very high level, but rigid, requirements on protection against malicious code can be found in the personal data protection and in the QCA related legislation. Fiscally relevant electronic document are required not to have any macro or hidden code inside.
SP	BPR's and IGAE's system include mechanisms for early detection of malicious code within the incoming documents. In addition, BPR system is audited by an external auditor once per year.
UK	No special provisions. ISO/IEC 17799 [3] controls appropriate to both signatures and storage

A.2.6.5 Back-up

Objective: To maintain the integrity and availability of information and information processing facilities.

Country	Details
DE	No general provisions. See also the IT Grundschutz Manual.
FR	No specific requirement for this objective concerning signature asset. Concerning storage, in Standards AFNOR , there are following obligations : backup of documents, indexes are to be made; security copy is to be made. But, concerning restoration of backup, there exists no requirement. In norm PRIS V2, certification authority has to have a commitment concerning the restoration of CA service after a destruction for example. This commitment gives the time of the restoration. The higher the level, the shorter the time.
IT	Only for QCAs back up sites are explicitly required, but the following requirement of CNIPA Deliberation 11/2004 on substitutive conservation: "*The stored document must be exhibited as legible in any moment* …" implies the need for backup copies and for disaster recovery sites, including backup storage sites.
SP	BPR's CA has defined a backup policy. IGAE also has a back up policy for expenses dossiers and reports.
UK	No special provisions. ISO/IEC 17799 [3] controls most appropriate to storage.

A.2.6.6 Network security management

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

Country **Details**

DE No general provision.

See also the IT Grundschutz Manual.

FR No specific requirement.

IT Requirements regarding the network protection are specified only for REM providers.

SP Both BPR's SCR and IGAE have defined their own policies for securely managing their networks.

UK ISO/IEC 17799 [3] controls particularly applicable to reporting and remote access to the data.

A.2.6.7 Media handling

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

Country **Details**

DE No general provisions.

In case of electronic invoices these general storage rules are effective also for documents as well as testimonials of authenticity and integrity of the data (e.g. qualified electronic signatures), even if following other rules the validity of these testimonials is already passed.

The invoices are to be readable during the complete storage period. No changes whatsoever are allowed.

See also the IT Grundschutz Manual.

FR No specific requirement for signature.

Concerning storage. In the standard AFNOR Z 42-013, there is an obligation to have formal attestation of:

Authorization to store documents.

Record of documents.

Destruction of information.

Concerning the last proof. This attestation is to be made before the real destruction.

These attestations are kept on paper support or WORM like optical support. If possible these attestations are to be issued by the storage organization and will only be verified by the operator. In order to ensure them a reliable security these media are to be stored in a protected and specific area, separated from desktop areas.

No requirement for the access. Just a requirement for three level of user access (see clause A.2.7.2).

IT No requirement.

SP BPR has defined a policy of protection of media for its services. Magnetic tapes are kept in secure environments.

UK No special provisions.

ISO/IEC 17799 [3] controls in clause 10.7 are most appropriate to storage and management of keys.

A.2.6.8 Exchange of information

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

Country	Details
DE	No general provisions. In case of transmitting electronic invoices measures to guarantee authenticity and integrity need to implemented. See also the IT Grundschutz Manual.
FR	No specific requirement.
IT	No legal requirement.
SP	Annual and book accounts electronically submitted to the BPR are kept confidential in their transit on the Internet by using SSL.
UK	No special provisions. ISO/IEC 17799 [3] controls most appropriate to storage.

A.2.6.9 Electronic commerce services

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

Country	Details
DE	No general provisions.
FR	No specific requirement.
IT	No security rules exist on how electronic commerce services are to be secured. Only measures regarding how personal and sensitive data are to be protected are specified, for example by means of authentication, managed privileges, encryption, etc. Where these data types are sent by electronic means, suitable measures may need to be agreed with the telecommunication companies if you do not make use of VPN or similar mechanisms or do not encrypt the data. Sensitive data can only be processed upon notification to and, where necessary, authorization by the Authority for the Data Privacy.
SP	BPR puts in place measures for keeping confidential information secure. As per the provision of services, it also puts in place security measures for on-line transactions ending in fee payment (provision on annual accounts and information on properties).
UK	No special provisions. ISO/IEC 17799 [3] controls in clauses 10.9.1 to 10.9.2 most appropriate to reporting.

A.2.6.10 Monitoring

Objective: To detect unauthorized information processing activities.

Country	Details
DE	No general provision.
	See also the IT Grundschutz Manual.
FR	Concerning electronic invoices, French administration can control the respect of technical norms for the signature and can control the system of the creation of electronic invoices.
	Concerning storage, in the standard AFNOR Z42-013, there is an obligation to have at least an audit per year. This audit can be an internal and/or external audit.
IT	Regulation on QCAs and REM providers indicate that a person responsible for audit is to be assigned, but no indication exists on how to perform audit inspections, and on logging requirements specifically related to fiscally relevant document issuance and storage, etc.
SP	BPR's system performs monitorization of unauthorized information processing activities.
	IGAE also performs monitorization of all the critic systems, especially accesses. The information on authorization and denegation of users access to the database is to be kept at least two years.
UK	No special provisions.
	ISO/IEC 17799 [3] controls in clauses 10.10.1 to 10.10.6 are appropriate to signing and storage.
	In addition audit information is required for signing functions.

A.2.7 Access control

A.2.7.1 Business requirement for access control

Objective: To control access to information.

Country	Details
DE	No special provisions.
	See also the IT Grundschutz Manual.
FR	No specific requirement.
	However, all standard (AFNOR Z42 013, PRIS V2) have as recommendation to have logical and physical access.
	It is a logical recommendation.
IT	Only QCAs, REM Providers and Privacy related rules require access control policies to be in place.
SP	As said before, BPR system allows annual accounts be accessed by any registered entity after fee payment. On the other side, only the corporate itself, Spanish Tax Agency inspectors and civil servants may gain access to the corporate book accounts.
	The "Resolución de 24 de mayo de 2005 de la IGAE, publicada en el BOE de 17 de junio de 2005" [R 144/2005] specifies requirements for access control to IGAE databases.
UK	No special provisions.
	ISO/IEC 17799 [3] controls in clause 11.1.1 are appropriate to signing and storage.

A.2.7.2 User access management

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

Country **Details**

DE No special provisions.

See also the IT Grundschutz Manual.

FR No specific requirement concerning signature.

But, concerning storage, in the norm ANFOR Z42-013, we find three level of user access:

system level;

operator level; and

consultation level.

All companies following this standard are to implement these levels.

IT No special provisions.

SP BPR's PKI usage requires control access.

Each member of IGAE staff is assigned an access profile specifying the set of applications and databases that is granted to access. IGAE system only allows its own inspectors to access public expenses dossiers database. Critical systems or those containing personal data, are to use profiles for granting or denying access.

UK No special provisions.

For internal access ISO/IEC 17799 [3] controls in clauses 11.2.1 to 11.2.4 are appropriate to storage.

A.2.7.3 User responsibilities

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

Country	Details
DE	No general Provision. See also the IT Grundschutz Manual.
FR	No specific requirement concerning signature. But, concerning storage, in the norm ANFOR Z 42-013, we have a recommendation concerning passwords: Passwords are to have at least 5 characters and are also to be changed often. A period of three months in order to change passwords is good.
IT	No requirement. Internal users can be made aware of their responsibilities in this field, and, where the service/application sensitivity requires it, also in writing. Misbehaviour may be sanctioned based on the legislation in force and the working contract.
SP	No special provisions within BPR. The "Resolución de 24 de mayo de 2005 de la IGAE, publicada en el BOE de 17 de junio de 2005" [R 144/2005] establishes that it is the responsibility of each member of IGAE's staff to know the aforementioned resolution and apply whatever rules are given there. Each member commits himself to use the database information exclusively for the purposes he is entitled to.
UK	No special provisions. ISO/IEC 17799 [3] Controls in clauses 11.3.1 to 11.3.3 are appropriate to signing and storage, with additional controls on responsibilities for keeping smart cards secure.

A.2.7.4 Network access control

Objective: To prevent unauthorized access to networked services.

Country	Details
DE	No general Provision. See also the IT Grundschutz Manual.
FR	No specific requirement.
IT	No specific requirement.
SP	BPR controls network resources access through active directory. The "Resolución de 24 de mayo de 2005 de la IGAE, publicada en el BOE de 17 de junio de 2005" [R 144/2005] establishes general rules on network access control.e.g. who will authorize the subscription of a certain person as user of the network before the system manager, who will process such authorization, etc.
UK	No special provisions. ISO/IEC 17799 [3] controls in clauses 11.4.1 to 11.4.2, particularly relevant to use of storage. Segregation of networks particularly applicable to TTP services. Other controls generally applicable.

A.2.7.5 Operating system access control

Objective: To prevent unauthorized access to operating systems.

Country	**Details**
DE	No general Provision.
	See also the IT Grundschutz Manual.
FR	No specific requirement concerning signature.
	But, concerning storage, in the norm AFNOR Z 42-013, we find three level of user access:
	system level;
	operator level; and
	consultation level.
	All companies following this standard are to implement these levels.
IT	QCAs are required to make use of Operating Systems certified per ITSEC F-C2/E2 or equivalent.
SP	No special provisions.
UK	No special provisions.
	ISO/IEC 17799 [3] Controls in clauses 11.5.1 to 11.5.6 are most appropriate to storage.

A.2.7.6 Application and information access control

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

Country	**Details**
DE	No general Provision.
	See also the IT Grundschutz Manual.
FR	No specific requirement concerning signature.
	But, concerning storage, in the norm ANFOR Z 42-013, we find three level of user access:
	system level;
	operator level; and
	consultation level.
	All companies following this standard are to implement these levels.
IT	Such requirements exist only for QCAs and REM providers.
	Privacy rules address these issues regardless of the provided service, as they are focused on personal and sensitive data management.
SP	BPR performs access control to information based on the certificate profile.
	IGAE performs access control to expenses dossiers database based on a profile depending on the inspector's adscription centre.
UK	No special provisions.
	ISO/IEC 17799 [3] controls in clause 11.6.1 is most appropriate to storage. Clause 11.6.2 is most applicable to signing keys.

A.2.7.7 Mobile computing and teleworking

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

Country	Details
DE	No general Provision. See also the IT Grundschutz Manual.
FR	No specific requirement.
IT	No specific provision.
SP	BPR system allows teleworking through VPNs in certain cases. IGAE's inspectors frequently perform remote access IGAE's database through VPN according to rules dictated by the security policy.
UK	No special provisions.

A.2.8 Information systems acquisition, development and maintenance

A.2.8.1 Security requirements of information systems

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

Country	Details
DE	No general Provision. See also the IT Grundschutz Manual.
FR	No specific requirement.
IT	No stipulations.
SP	No special provisions.
UK	No special provisions. ISO/IEC 17799 [3] controls in clause 12.1 are appropriate to storage and signing.

A.2.8.2 Correct processing in applications

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

Country	Details
DE	No general Provision. See also the IT Grundschutz Manual.
FR	No specific requirement.
IT	No stipulations, except for signature creation applications and devices, that are to "ensure the integrity of the electronic documents the signature refers to. Electronic documents are to be presented to the signer before the signature, clearly and without any ambiguity, and the will to sign has to be requested…". The latter requirement does not apply to signatures issued by means of automated procedures, like the e-invoicing issuing procedures. These procedures are to be clearly activated by the signer, whose will to issue this signature is to be clearly specified in the automatically signed documents.
SP	BPR system does not put special provisions. IGAE's system includes controls in its applications checking information coherence within the documents submitted by public agencies.
UK	No special provisions. ISO/IEC 17799 [3] controls in clause 12.2.1 may be appropriate to input of data into storage. Other controls are best targeted at objectives described in clause 5.

A.2.8.3 Cryptographic controls

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

Country	Details
DE	No general Provision. See also the IT Grundschutz Manual.
FR	No specific requirement.
IT	Key management is addressed by the legal requirements that regard keys used in electronic signatures and to ensure the personal sensitive data privacy. Where protection of sensitive data (e.g. related to a person's health, religion, sexual habits, etc.) is concerned, encryption is specifically required by the related law, that also implies cryptographic key management.
SP	Annual and book accounts are encrypted by SSL while circulating through Internet. Once they are in the BPR system, they are deciphered.
UK	No specific requirements. General use of commercial SSL accepted.

A.2.8.4 Security of system files

Objective: To ensure the security of system files.

Country	Details
DE	No general Provision.
	See also the IT Grundschutz Manual.
FR	No specific requirement.
IT	Requirements on system files access are laid down to some detail only for QCAs and for REM providers. Sensitive data privacy protection rules indicate this type of protection at high level.
SP	Files containing personal data have to respect what is established by Personal Data Protection Law.
UK	No special provisions.
	ISO/IEC 17799 [3] controls in clauses 12.4.1 to 12.4.3 are appropriate to storage and signing.

A.2.8.5 Security in development and support processes

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

Country	Details
DE	No general Provision.
	See also the IT Grundschutz Manual.
FR	No specific requirement.
IT	No such requirement is specified.
SP	Any change in the applications has to ensure the alignment with Personal Data Protection Law.
	In addition to that, IGAE never performs tests with actual data.
UK	No special provisions.
	ISO/IEC 17799 [3] controls in clauses 12.5.1 to 12.5.3, 12.5.5 are appropriate to storage and signing. Covert signalling issues (clause 12.5.4) are not necessary since those with access to data are assumed to be trusted with the proper use of that data.

A.2.8.6 Technical vulnerability management

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

Country	Details
DE	No general Provision. See also the IT Grundschutz Manual.
FR	No specific requirement.
IT	The personal data protection law requires the implementation of mechanisms and systems suitable to prevent exploitation of processing systems vulnerabilities. Since fiscally relevant documents may encompass also data pertaining to legal persons, such requirements are to be taken into account. CAs and REM providers are required to regularly perform and maintain a Risk Assessment procedure.
SP	A yearly external audit is performed on the BPR system which assess and make recommendations. IGAE is conducting risk analysis and producing contingency plans.
UK	No special provisions. ISO/IEC 17799 [3] control in clause 12.6.1 is appropriate to storage and signing.

A.2.9 Information security incident management

A.2.9.1 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.

Country	Details
DE	No general Provision. See also the IT Grundschutz Manual.
FR	No specific requirement.
IT	No legal stipulation addresses the security incident management.
SP	BPR maintains a data base on system incidents. IGAE notifies incidents through a corporative system. Incidents are recorded.
UK	No special provisions. ISO/IEC 17799 [3] controls in clauses 13.1.1 to 13.1.2 are appropriate to storage and signing.

A.2.9.2 Management of information security incidents and improvements

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

Country	**Details**
DE	No general Provision. See also the IT Grundschutz Manual.
FR	No specific requirement.
IT	No legal requirement.
SP	BPR has defined processes for managing security incidents. The Corporate Security Manager coordinates incidents management. He generates the email notifying them and after its closure will also generate the corresponding notification email.
UK	No special provisions. ISO/IEC 17799 [3] controls in clauses 13.2.1 to 13.2.2 are appropriate to storage and signing.

A.2.10 Business continuity management

A.2.10.1 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.

Country	**Details**
DE	No general Provision. See also the IT Grundschutz Manual.
FR	No specific requirement.
IT	Service level requirements are specified only for the REM. The QCA related rules just require a disaster recovery plan is in force. No impact analysis is required. However, personal data privacy law, that forbids any loss of data, applies. Electronic substitutive documents conservation requires in any case that "the conserved document must be made readable in any moment documents…. also by telematic means". This implies a business continuity plan to be enacted not to become liable for default.
SP	BPR has elaborated a continuity plan for dealing with service discontinuation.
UK	No special provisions. This is a general business issue.

A.2.11 Compliance

A.2.11.1 Compliance with legal requirements

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

Country	Details
DE	No general Provision. See also the IT Grundschutz Manual.
FR	No specific requirement. Companies are to respect French laws.
IT	Obviously compliance with the law is required by the law.
SP	Obviously all the systems claim compliance with what is required by the law. Specifically, IGAE is to accomplish, among others, what is stated in the "Resolución de 24 de mayo de 2005 de la IGAE, publicada en el BOE de 17 de junio de 2005" [R 144/2005].
UK	Legislation relating to the VAT Directive is most relevant.

A.2.11.2 Compliance with security policies and standards and technical compliance

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

Country **Details**

DE No general Provision.

See also the IT Grundschutz Manual.

The IT-Grundschutz Certificate or a self-declaration offers companies and agencies the possibility of making transparent their efforts regarding IT security. This can serve as a quality feature providing competitive advance with both customers and business partners and thus can bring competitive advantage. After consulting with registered IT-Grundschutz users and IT security experts, the BSI has defined three variants of the IT-Grundschutz qualification: the IT-Grundschutz Certificate and the self-declarations "IT-Grundschutz entry level" and "IT-Grundschutz higher level".

Issue of the IT-Grundschutz Certificate is based on an audit carried out by an external auditor licensed with the BSI. The outcome of the audit is an audit report which is submitted to the certification authority that decides on the issue of IT-Grundschutz Certificates. The baseline set of criteria on which the procedure is based is the latest version of the BSI's IT-Grundschutz Manual. The "Audit Scheme for Auditors" describes the audit procedure followed, the audit report, the decision and issue of the IT-Grundschutz Certificate.

FR Concerning electronic invoices, French administration can control the respect of technical norms for the signature.

Concerning storage, in the standard AFNOR Z 42-013 there is an obligation to have at least an audit per year. This audit can be internal and/or external audit.

IT Where security policies are required by the law, they are to be met.

Something close to security policies is required for CAs and for REM, although they do not perfectly match ISO/IEC 17799 [3] structure. However they are to be met as expected. In fact the presence of an internal Auditor Manager is specifically required by both regulations on Qualified Electronic Signature and on REM.

SP BPR system is audited once yearly.

IGAE system will be audited once every two years in terms of Personal Data Protection Law conformance.

UK No special provisions.

ISO/IEC 17799 [3] controls in clauses 15.2.1 to 15.2.2 are appropriate to storage and signing.

A.2.11.3 Information systems audit considerations

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

Country **Details**

DE No general Provision.

See also the IT Grundschutz Manual.

IT security audit required by audit companies following their own audit procedures.

Certification by BSI possible and recommended.

The IT-Grundschutz Certificate or a self-declaration offers companies and agencies the possibility of making transparent their efforts regarding IT security. This can serve as a quality feature providing competitive advance with both customers and business partners and thus can bring competitive advantage. After consulting with registered IT-Grundschutz users and IT security experts, the BSI has defined three variants of the IT-Grundschutz qualification: the IT-Grundschutz Certificate and the self-declarations "IT-Grundschutz entry level" and "IT-Grundschutz higher level".

Issue of the IT-Grundschutz Certificate is based on an audit carried out by an external auditor licensed with the BSI. The outcome of the audit is an audit report which is submitted to the certification authority that decides on the issue of IT-Grundschutz Certificates. The baseline set of criteria on which the procedure is based is the latest version of the BSI's IT-Grundschutz Manual. The "Audit Scheme for Auditors" describes the audit procedure followed, the audit report, the decision and issue of the IT-Grundschutz Certificate.

FR No specific requirement.

IT No audit tool is required by the applicable regulations, although CAs and REM rules require that an Audit Manager is in place.

SP No special provisions.

UK No special provisions.

ISO/IEC 17799 [3] controls in clauses 15.3.1 to 15.3.2 are appropriate to storage and signing.

History

Document history		
V1.1.1	July 2007	Publication