ETSI TS 101 533-1 V1.3.1 (2012-04)

Electronic Signatures and Infrastructures (ESI);
Data Preservation Systems Security;
Part 1: Requirements for Implementation and Management

Reference
RTS/ESI-00123-1

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

ETSI

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

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

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

Content

Intellectual Property Rights

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

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

Foreword

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

The present document is part 1 of a multi-part deliverable covering provisions for secure and reliable implementation, management and assessment of long term data preservation systems, as identified below:

TS 101 533-1: "Requirements for Implementation and Management";

TR 101 533-2: "Guidelines for Assessors".

The text taken from ISO/IEC 27002:2005: "Information technology -- Security techniques -- Code of practice for information security management" and ISO 15489-1:2001: "Information and documentation - Records management -- Part 1: General", is reproduced with the permission of the international Organization for Standardization, ISO. These can be obtained from any ISO member and from the Website of the ISO Central Secretariat at the following address: www.iso.org. Copyright remains with ISO.

Acknowledgment

The building blocks of the present document were submitted by UNINFO, the Italian standardization body for ICT, federated to UNI, Italian member body of CEN and ISO.

Introduction

In the light of EU-wide implementation of Directive 2006/123/EC [i.25], article 26, EUMS are required to "take accompanying measures to encourage providers to take action on a voluntary basis in order to ensure the quality of service provision". This will be accomplished through certification, assessment or by means of compliance with quality charters.

Among the service providers addressed by this Directive are also Data Preservation Service Providers, especially in the fiscal area, where the stored data object owner, i.e. the taxpayer, is held responsible towards the Authority for the data object exhibition even when it resorts to a service provider.

Article 17(2) of Directive 95/46/EC [i.29] states that "The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures".

In the light of the above mentioned EU Directives the purpose of the present document is to provide a common, objective and reliable basis for preservation service providers to implement, manage, and for Assessors to assess, secure Data Preservation Systems, meeting the information security related quality addressed by the above mentioned EU Directive 2006/123/EC [i.25].

Conversely, nothing is specified, neither in the present document nor in its sister TR 101 533-2 [i.24], on the auditors' qualification, as the currently existing documentation, in particular ISO/IEC 17021 [i.4], provide an official and exhaustive set of provisions.

The present document is based on TS 102 573 [3], all provisions of which apply except where otherwise specified, and provides additional security and reliability measures that, in turn, are based on the ISO/IEC 27000 [i.26] family, more in particular on ISO/IEC 27001 [1] and ISO/IEC 27002 [2].

The present document structure therefore matches that of TS 102 573 [3] and consequently, where applicable, the structure of ISO/IEC 27001 [1].

Provisions of the present document can be used by implementers and managers of Data Preservation Systems aiming to provide Data Preservation Services recognised as valid wherever the present document is endorsed, possibly by the applicable legislation.

1 Scope

The present document addresses the Information Security Management System of Data Preservation Systems, by specifying Security requirements for Data Preservation Service Providers to abide by, when implementing and managing a DPS, in order to provide Data Preservation Services that are trustable and reliable from the Information Security viewpoint.

Sister document TR 101 533-2 [i.24] provides recommendations on how to assess electronic data preservation services against the provisions specified in the present document.

These measures are based on provisions of ISO/IEC 27001 [1], ISO/IEC 27002 [2] and TS 102 573 [3], enhancing them where necessary.

The present document does not address specific document management related issues that are addressed by a number of ISO standards, such as ISO 14721 [i.5], ISO 15489 [i.17], ISO 23081 [i.27] and, more in general, those dealt with by ISO/TC 46/SC11 which the reader of the present document should refer to.

NOTE The present document and its sister document TR 101 533-2 [i.24] can be referred to by various archival management standards and standard families as a complementary and detailed set of specifications through which a reliable Information Security Management System can be implemented, managed and assessed, as regards the Data Preservation peculiarities.

2 References

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

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

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

2.1 Normative references

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

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

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

[3] ETSI TS 102 573: "Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data for digital accounting".

2.2 Informative references

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

[i.1] BS 25999-1:2006: "Business continuity management - Part 1: Code of practice".

[i.2] ISO/IEC 27005: "Information technology -- Security techniques -- Information security risk management".

[i.3] ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.4] ISO/IEC 17021: "Conformity assessment -- Requirements for bodies providing audit and certification of management systems".

[i.5] ISO 14721: "Space data and information transfer systems - Open archival information system - Reference model".

[i.6] ETSI TS 102 918: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".

[i.7] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[i.8] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

[i.9] ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".

[i.10] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[i.11] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[i.12] ETSI TS 102 778: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles".

[i.13] CWA 14170: "Security requirements for signature creation applications".

[i.14] CWA 14171: "General Guidelines for Electronic Signature Verification".

[i.15] IETF RFC 2560: "X.509 Internet Public Key Infrastructure Certificate Status Protocol - OCSP".

[i.16] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[i.17] ISO 15489: "Information and documentation - Records management".

[i.18] ISO/IEC 20000 (parts 1 to 3): "Information technology -- Service management (Part 1 "Service management system requirements", Part 2 "Part 2: Code of practice", Part 3 "Guidance on scope definition and applicability of ISO/IEC 20000-1").

[i.19] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures.

[i.20] NIST SP 800-94: "Guide to intrusion detection and Prevention Systems (IDPS)".

[i.21] FIPS 197: "Specification for Advanced Encryption Standard (AES)".

[i.22] IETF RFC 3647: "Internet X.509 Public Key Infrastructure. Certificate Policy and Certificate Practices Framework".

[i.23] ISO 9000: "Quality management systems -- Fundamentals and vocabulary".

[i.24] ETSI TR 101 533-2: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 2: Guidelines for Assessors".

[i.25] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

[i.26] ISO/IEC 27000: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

[i.27] ISO 23081 (all parts): "Information and documentation -- Records management processes -- Metadata for records".

[i.28] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[i.29] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.30] ITU-R Recommendation TF.460: "Standard-frequency and time-signal emissions".

[i.31] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax.

[i.32] ETSI TS 102 640: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM)".

[i.33] ANSI X9.17: "Financial Institution Key Management (Wholesale)".

[i.34] ETSI TS 102 176: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures".

[i.35] Commission of the European Communities COM(2009) 324: "Modernising ICT Standardisation in the EU - The Way Forward".

[i.36] NIST SP 800-90: "Recommendation for Random Number Generation Using Deterministic Random Bit Generators".

[i.37] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.38] OASIS "Open Document Format for Office Applications (OpenDocument)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 573 [3] and the following apply:

access: right, opportunity, means of finding, using, or retrieving information

NOTE: See ISO 15489 [i.17].

activation data: data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g. a PIN, a passphrase, or a manually-held key share)

NOTE: See RFC 3647 [i.22].

Advanced Electronic Signature (AdES): electronic signature which meets the following requirements:

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using means that the signatory can maintain under his sole control; and
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

NOTE: See Directive 1999/93/EC [i.19], article 2(2).

analog data object: non digital representation of acts, facts and/or data

applicability statement: See Statement of Applicability.

assessor: any physical or legal person performing an assessment on the facilities used by the DPSP to provide its Electronic Data Preservation Services, with the purpose to ascertain the DPSP compliance with the present document provisions

NOTE: Unless differently specified, association to an official auditing entity is not implied.

asset: anything that has value to the organization

NOTE: Although the data objects entrusted to the DPSP by its customers are not part of its tangible assets that are listed in the DPSP general ledger, they match this definition of "asset". In fact any damage to, or loss of, such data objects will make the DPSP liable to pay indemnities to the data objects legitimate owners. Additionally, such mishaps will tarnish the DPSP image that is mentioned in ISO/IEC 27002 [2], clause 7.1.1, letter f) among intangibles assets: "reputation and image of the organization". Therefore these data objects are to be dealt as assets.

asset owner: individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets

NOTE: The term "owner" does not mean that the person actually has any property rights to the asset (ISO/IEC 27002 [2], clause 7.1.2, footnote 2).

audit trail: set of audit records each referable to a precise point in time and containing evidence pertaining to and resulting from the execution of a process or system function

auditable: suitable to allow a smooth and exhaustive auditing process

EXAMPLE: A computing procedure should record an audit track; a procedure performed by humans should require them to record the performed steps.

certificate: See Public Key Certificate.

Certificate Policy (CP): named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

NOTE: See ISO/IEC 9594-8 [i.3].

Certification Authority (CA): authority trusted by one or more users to create and assign public-key certificates

NOTE: See ISO/IEC 9594-8 [i.3].

certification practice statement: statement of the practices that a Certification Authority employs in issuing certificates

NOTE: See ISO/IEC 9594-8 [i.3].

Certification-Service Provider (CSP): entity or legal or natural person who issues certificates or provides other services related to electronic signatures

NOTE: See Directive 1999/93/EC [i.19], article 2(11).

closure evidence: metadata suitable to provide evidence of integrity of the related set of data object the preservation of which is in force since a certain date

NOTE 1: The proof of integrity is provided by means of an auditable mechanism (e.g. QES/AdES) supported by a reliable time reference (e.g. a TST or a REM reference), or a TST supported by an audit trail suitable to identify who requested the TST itself.

NOTE 2: The closure evidence structure is not specified in the present document (examples of closure evidence can be: LTANS Evidence Record Syntax as specified in RFC 4998 [i.28]).

controller: natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (Directive 95/46/EC [i.29], article 1, letter d))

Coordinated Universal Time (UTC): time scale based on the second as defined in ITU-R Recommendation TF.460 [i.30]

customer: See subscriber.

data object owner: legal or natural person that has legitimate ownership of the deposited data object

data object depositor: any entity responsible for depositing information at an DPSP on behalf of the DPSP subscriber, upon a specific agreement with this DPSP

NOTE 1: The data object depositor may coincide with the data object owner and/or with the subscriber.

NOTE 2: There may be one or more depositors for the same DPSP subscriber, for example where the subscriber is structured in several departments, each independently depositing its own data objects.

[Electronic] Data Preservation Service: service to which data objects are entrusted in an agreed form (digital or analog) for being securely kept in digital form for a period of time specified in the applicable agreement; this service is expected to be able to exhibit all preserved data objectsat any moment during, or at the end of, the preservation period

Data Preservation Service Provider: legal or natural person that provides one or more Data Preservation Services to subscribers

Data Preservation System (DPS): set of hardware, software, policies, procedures, guidelines, practices, physical and organizational infrastructures aiming to ensure electronic data preservation for at least the period of time specified in the applicable agreements; the organizational infrastructures can be of administrative, technical, management, or legal nature

delegated signer: person who is formally delegated the responsibility to issue AdES on behalf of the DPSP

NOTE: This person can be either an DPSP employee or an external provider, where legally valid.

format conversion: process by which one or more preserved data object is transposed from one digital representation to another while maintaining its original semantics

Information Security Management System (ISMS): that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources (ISO/IEC 27001 [1]).

information security policy: document that may contain the principles and directives specific to the protection of information that is sensitive or valuable, or otherwise of importance, to the organization

NOTE: Principles contained therein will be derived from, and thus consistent with, the principles of the corporate security policy.

intrusion detection system: system that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents

NOTE: See NIST SP 800-94 [i.20].

invocation: act of declaring that an organisation's business continuity plan needs to be put into effect in order to continue delivery of key product or services

NOTE: See BS 25999-1 [i.1].

long term: period of time long enough for there to be concerned about the impacts of changing technologies, including support for new media and data formats, and of a changing user community, on the information being held in a repository

NOTE: This period extends into the indefinite future (ISO 14721 [i.5]).

metadata: data describing context, content and structure of records and their management through time, also including indexing information for retrieval

NOTE: ISO 15489 [i.17] with modification.

outsourcers: organisations providing the DPSP with services related to its DPS

owner: See Asset Owner and Data Object Owner.

personal data: any information relating to an identified or identifiable natural person ('data subject')

NOTE: An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (Directive 95/46/EC [i.29], article 2, letter a).

presentation corruption agent: any code contained in a data object, suitable to surreptitiously modify the data object presentation without changing its binary content

NOTE: Examples of Presentation Corruption Agent are: macros, hidden executable code, hidden or difficult to detect worksheet formulas, hidden byte sequences that are ignored by the originally intended presenting application but that can be recognised when the data object is processed by different applications.

preservation: act of maintaining information, in a correct and independently understandable form, possibly over the Long Term

NOTE: See ISO 14721 [i.5] with changes.

processor: natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

NOTE: See Directive 95/46/EC [i.29], article 2, letter e).

Public Key Certificate (PKC): public key of a user, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority which issued it (ISO/IEC 9594-8 [i.3])

Qualified Certificate (QC): certificate which meets the requirements laid down in annex I of the Directive 1999/93/EC [i.19] and is provided by a certification-service-provider who fulfils the requirements laid down in annex II of the same Directive 1999/93/EC [i.19]

Qualified Electronic Signature (QES): advanced electronic signature that meets the requirements as in Directive 1999/93/EC [i.19], article 5(1), i.e. is based on a qualified certificate and is created by a secure-signature-creation device

readability (data object readability): possibility for a data object to be visually read by human beings and/or to be machine processed consistently with its format

responsible [for preservation]: natural person who is in charge of the Preservation system

sensitive data: See special categories of data.

Secure Signature Creation Device (SSCD): signature-creation device which meets the requirements laid down in annex III of Directive 1999/93/EC [i.19], article 2(6)

Signature Creation Data (SCD): unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature

NOTE: See Directive 1999/93/EC [i.19], article 2(5).

Signature Creation Device: configured software or hardware used to implement the signature-creation data

NOTE: See Directive 1999/93/EC [i.19] article 2(5).

special categories of data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life

NOTE 1: See Directive 95/46/EC [i.29], article 8(1).

NOTE 2: Data that are neither sensitive nor judicial data, but whose processing may jeopardize the data subjects' fundamental rights, freedoms and dignity, are to be dealt with as "Special categories of data".

Statement of Applicability (SoA): documented statement describing the control objectives and controls that are relevant and applicable to the DPSP ISMS

NOTE: See ISO/IEC 27001 [1].

storage logical unit: storage unit that can be managed by the DPS service as self consistent

subscriber: entity that accepts an agreement on depositing data objects at the DPSP

NOTE: This entity can be a legal or natural person or a different department of the organisation the DPSP belongs to. The agreement can be endorsed either explicitly, e.g. by undersigning agreements, or implicitly, e.g. when the relationship between subscriber and DPSP are governed by common rules, such as corporate policies when they are separate departments of the same organisation.

system administrator: professional in charge of managing and servicing processing systems and/or of their components

NOTE: The scope of this definition includes other professionals that can be equated in terms of data protection risks - such as database administrators, network and security equipment administrators, and the administrators of complex software systems.

third party:

a) Any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data (Directive 95/46/EC [i.29], article 2(f)).

b) Any natural or legal person acting on behalf, and where applicable also in the name, of another natural or legal person, for example a taxable person, a customer, as in Directive 2006/112/EC [i.31].

c) Any natural or legal person who governs issuance and revocation, to one of more subjects, of qualified certificate.

time-mark: information in an audit trail from a Trusted Service Provider that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time

NOTE: See TS 101 733 [i.10].

time stamping authority: authority trusted by one or more users to provide a Time Stamping Service

NOTE: See CWA 14171 [i.14].

time stamp token: proof-of-existence for a datum at a particular point in time, in the form of a data structure signed by a Time Stamping Authority

NOTE: See CWA 14171 [i.14].

time stamping service: service that provides a trusted association between a datum and a particular point in time, in order to establish reliable evidence indicating the time at which the datum existed

NOTE: See CWA 14171 [i.14].

trading partner: natural or legal person that has trading relationships with the DPSP

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

NOTE: This term is used in preference of and with a broader application than the term Certification-Service-Provider (CSP) used in Directive 1999/93/EC [i.19] (TS 102 231 [i.9]).

unique [analog] original data object: analog data object existent in single instance, the semantics of which cannot be deduced from other data objects of any kind, the preservation of which is required by the applicable legislation or rules

3.2 Abbreviations

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

AdES	Advanced Electronic Signature
ASiC	Associated Signature Containers
BCP	Business Continuity Plan
CA	Certification Authority
CAdES	CMS Advanced Electronic Signature
COTS	Commercial Off The Shelf

CP	Certificate Policy
CRL	Certificate Revocation List
CSP	Certification-Service-Provider
DPS	[Electronic] Data Preservation System
DPSP	Data Preservation Services Provider
DS	Delegated Signer
EUMS	European Union Member State
EXT	Extended Service(s)
ICT	Information and Communications Technology
ISMS	Information Security Management System
ISPD	Information Security Policy Document
OAIS	Open Archival Information System
OCSP	Online Certificate Status Protocol

NOTE: See RFC 2560 [i.15].

PAdES	PDF Advanced Electronic Signature
PAS	Publicly Available Specification
PCA	Presentation Corruption Agent
PIN	Personal Identification Number
QC	Qualified Certificate
QES	Qualified Electronic Signature
RAID	Redundant Array of Independent Disks
REM	Registered E-Mail

NOTE: As per TS 102 640 [i.32].

SCD	Signature Creation Data
SoA	Statement of Applicability
SSCD	Secure Signature Creation Device
TLS	Transport Layer Security

NOTE: See RFC 5246 [i.37].

TSA	Time Stamping Authority
TSP	Trust Service Provider
TST	Time Stamp Token
UTC	Coordinated Universal Time
XAdES	XML Advanced Electronic Signature
XML	eXtensible Markup Language

4 Overview

The present document implies the compliance by any DPSP that implements its provisions with ISO/IEC 27001 [1], against which this DPSP is recommended to be certified. Certification against ISO 9000 [i.23] and ISO/IEC 20000 [i.18] is also recommended.

In particular DPSPs are expected to comply with the above mentioned standards, since abidance by them would, in fact, improve their capability:

1) to go out to tender for their services;

2) to provide a consistent approach by their outsourced service providers;

3) to demonstrate their ability to meet customer requirements;

4) to improve the services they provide.

The present document is based on TS 102 573 [3], in particular on policy [N+], and specifies additional security and reliability measures for the Electronic Data Preservation Service Providers (DPSP), specifically addressing the potential risks associated with data preservation, possibly in the long term. The mentioned TS 102 573 [3] is based on, and consistent with, ISO/IEC 27001 [1] and ISO/IEC 27002 [2], with which the present document is also consistent. In particular, in annex A, where necessary, are indicated additional requirements and/or the ISO/IEC 27002 [2] requirements that do not apply.

The long term preservation validity should be assured by using mechanisms suitable to achieve at least the following purposes:

a) Ensure the integrity of the whole of the preserved data objects; it should be possible at least to subsequently identify if, and which, preserved data objects have been modified, deleted or added;

NOTE 1: The whole of the data objects can be divided in smaller sets, based on different criteria: time, topics, etc.

b) Ensure the accountability of the preserved data objects integrity by creating a reliable audit trail; this is of paramount importance because by assigning the preservation responsibility to one or more specific officer adds trust to the entire preservation cycle.

NOTE 2: To achieve the above goals Advanced Electronic Signatures can be used, in any of their strains such as CAdES, XAdES, PAdES, QES, etc., as well as other suitable mechanisms, like TSTs issued by trusted TSAs and supported by a suitable audit trail.

The outcome of a Risk Assessment shall be taken into account by an DPSP when implementing the measures and controls included in the present document. The Risk Assessment outcome shall be made available also to the assessor that is expected to assess the DPSP according to TR 101 533-2 [i.24].

The Risk Assessment should be performed having as reference ISO/IEC 27005 [i.2] and shall take into account all risks associated to managing the data objects entrusted to the DPSP by its customers. Provisions on loss and damages are addressed in clause 5.2.1.

The present document may be used to implement the information security related issues within the broader scope of the Open Archival Information System (OAIS) and of Records Management, as addressed by ISO 14721 [i.5] and ISO 15489 [i.17].

Some issues of the present document can also be addressed by other publicly available specifications or standards. In this case implementers shall indicate in their Statement of Applicability (SoA) for each single item what specific provisions they do comply with (for further information on SoA, see clause 4.3).

4.1 Preservation Service types

The present document specifies:

1) the Core Data Preservation Service each DPSP shall implement;

2) a number of Extended Services that an DPSP may provide.

In the present document are indicated:

1) the functions to be implemented by an DPSP in order to provide the mandatory Core Data Preservation Service;

2) the functions to be implemented for each Data Preservation Extended Service provided by the DPSP; these Extended Services are marked [EXT].

Other services and/or functions, additional to those indicated in the present document, may be defined elsewhere (e.g. in agreements, in corporate policies, etc.), but their requirements shall not conflict with those specified in the present document.

Documents indicating the information security provisions for such additional services and/or functions should be structured like the present one.

4.2 User Community and Applicability

The present document is intended to be used by, but not exclusively, any DPSP as a guidance to implement and manage the ICT security related issues of an DPS compliant with TS 102 573 [3], ISO/IEC 27001 [1] and ISO/IEC 27002 [2], suitable to withstand assessment by independent Assessors. TR 101 533-2 [i.24] is intended to be used by such Assessors.

The DPSP is responsible for the implementation and management of the entire DPS, even when some of its functions are outsourced to external providers. Therefore provisions in the present document are expected to be complied with also if outsourced to external providers. Similarly, these outsourced services are expected to be assessed based on TR 101 533-2 [i.24]. Related provisions are specified in clause 5.2.2.

4.3 Conformance requirements

Each DPSP that wants to be recognized as compliant with the present document shall achieve, through independent assessment, formal recognition of its conformance to the requirements specified in its "Statement of Applicability", as defined in annex B for the set of functions related to the Core Data Preservation Services as well as to the Extended services and the additional provisions it provides (see clause 4.1).

The present document specifies requirements for Core Data Preservation services and requirements for Extended Data Preservation services.

An DPSP shall implement mandatory requirements for Core and Extended services unless really exceptional conditions occur. The DPSP Management can authorise deviations only after having evaluated the consequences. This decision shall be extensively justified and documented in writing.

An DPSP should implement the recommended provisions for the Core services and for the Extended services it provides. The DPSP Management can authorise deviations from these recommended provisions only after having evaluated the consequences of such deviation. This decision must be justified in writing.

An DPSP may apply optional requirements.

The "Statement of Applicability" shall take into consideration the outcomes of a Risk Assessment. The DPSP shall therein specify:

a) what control objectives and controls indicated in TS 102 573 [3], in the ISO/IEC 27002 [2] and in the present document, are selected and implemented and which ones indicated as recommended, or exceptionally as mandatory, are excluded from implementation, alongside with the rationale for their exclusion;

b) what control objectives and controls indicated in other publicly available specifications are implemented alongside with the rationale for their inclusion as specified in clauses 4 and 4.1.

5 Provisions based on TS 102 573

The provisions in TS 102 573 [3] relevant to data preservation, specified in the following clauses with the notation "(TS 102 573 [3], clause N.N, items N.N, etc.)" apply, with the addition of the provisions specified in the corresponding clauses.

NOTE: The present document uses the term "data object" in place of TS 102 573 [3] term "document", where applicable. This note may not apply to versions of TS 102 573 [3] subsequent to V1.1.1.

5.1 Compliance with the present document provisions

(TS 102 573 [3], clause 5.7)

1) The DPSP shall comply with all provisions in the present document taking into account what it specifies in its Statement of Applicability.

2) The DPSP shall transpose, as applicable, the provisions in the present document in its Information Security Policy Document, in its Operational Procedures, in the employees' job description and in all similar data objects.

3) The DPSP shall demonstrate its compliance with those provisions of present document it specifies in its Statement of Applicability to Assessors and other authorised bodies by also exhibiting prior assessment reports issued by relevant entities, where applicable.

5.2 DPSP Obligations specified in TS 102 573, clause 6

5.2.1 Arrangements to cover liabilities and financial stability

(TS 102 573 [3], clause 6.2, items 2), 3) and 5))

The DPSP shall initially perform a Risk Assessment to assess its financial stability and capability to cover liability and shall repeat it on time basis (i.e. at time intervals) and every time that substantial technical or contractual changes occur. This Risk Assessment should be financially quantitative. The DPSP shall have the financial capability and stability, by means of its own assets, an insurance policy or both, to provide the services as specified in the present document including meeting the possible indemnification.

NOTE: When addressing "indemnification", provisions in ISO/IEC 27005 [i.2] would be taken into account. In particular the DPSP is encouraged to perform the Risk Assessment cycle described below.

1) The technical risks related to each asset are evaluated and the countermeasures to be consequently enforced are chosen. The residual risks deemed as acceptable are clearly specified.

2) The above residual risks are financially evaluated quantifying for each single residual risk the financial exposure deriving for example from:

   a) the direct cost of loss (e.g. destroyed or stolen assets);

   b) the indemnification to data objects owners for damages deriving from lack of (timely) providing them with their own data objects.

3) The DPSP overall financial exposure is then evaluated taking into account:

   a) the cost of insurance policies addressing all or some of the risks identified in previous item 2);

   b) the costs of risks identified in previous item 2), possibly reduced by the insurance policies.

4) The above overall financial exposure (cost of the insurance policies plus the residual risks costs) is evaluated. If it is unacceptable for the DPSP, the Risk Assessment cycle will be repeated by the DPSP until the overall financial exposure is deemed acceptable.

5) Eventually the DPSP specifies in the SoA the final provisions to be applied as per the outcomes of the Risk Assessment.

5.2.2 Conformance by sub-contractors

(TS 102 573 [3], clause 6.2, items 6) and 7))

1) The DPSP shall bear full responsibility towards its customers for compliance with the requirements specified in the present document, with regard to the services it provides, "*even when some or all of its functionalities are undertaken by sub-contractors*" (TS 102 573 [3], clause 6.1, item 2).

2) The DPSP shall oblige, through legally valid agreement, sub-contractors to which it entrusts the provision of all or part of the services related to its DPS, to authorise access to their own premises where the DPSP related activities are fulfilled, in addition to the properly identified relevant authorities, to duly authenticated:

   a) DPSP authorised personnel;

   b) Assessors appointed by the bodies with which the DPSP has an assessment/certification agreement.

5.2.3 DPSP service provisions in abidance by the applicable legislation

(TS 102 573 [3], clause 6.2, item 1))

1) Where provisions in the present document conflict with the applicable legislation, the latter shall always prevail.

2) The DPSP shall be registered as a legal entity according to the applicable legislation and shall exhibit evidence of this to any request.

3) Abidance by the present document per se does not imply that the DPSP at issue is compliant with any legislation. The DPSP shall ensure that the services it provides are compliant with the applicable legislation.

4) The DPSP agreement documentation shall contain in readily understandable language the regulation or sets of legal requirements that are complied by each of the set of services provided.

5) Declaration in previous item 4) must be in writing using official language(s) that meet at least the following requirements:

   a) at least one of the languages shall be an EU official language;

   b) agreement by the parties on the language(s) to be used.

6) The DPSP shall have in force auditable procedures suitable to fulfil, without undue delay, requests for exhibition or delivery of the preserved data, submitted by duly authorised entities, among which the relevant authorities, and, where personal data are dealt with, the Controller.

7) [EXT.1] Personal data preservation:

   a) If the DPSP is based in one European Union Member State and preserves personal data, it shall abide by the rules of the applicable legislation regarding transfer of personal data to a third country.

   b) If the DPSP processes personal data to make up the related metadata, this shall only occur under agreement with the data objects owner/controller and these metadata shall be dealt with under the same provisions as the data objects of origin.

5.2.4 Contractual aspects

(TS 102 573 [3], clause 6.2, several items)

1) The DPSP shall implement and have in force auditable procedures ensuring that the data depositor's identity and role is duly verified when subscribing the service agreement.

2) The agreement between DPSP and data objects owners shall specify whether the DPSP has the right (or duty) to process the data in order to extract the related metadata and, where this agreement exists, the mechanism through which metadata must be derived from the data objects to be preserved.

3) The agreement between DPSP and data objects owners shall specify what roles, including e.g. Assessors and relevant authorities, are entitled to access the preserved data objects.

4) The DPSP shall implement and have in force auditable procedures, ensuring that, upon authorised request or upon closure of the preservation agreement stipulated with one or more of its customers, the DPSP shall be able to give back to their respective legal owners, in a formally agreed format, the data objects that was originally deposited within the maximum time as per subsequent item 6).

5) The format as per the previous item 4) shall be:

   a) either the data objects original format; or

   b) a format as per clause 6.3.3, item 1) b).

6) The DPSP shall agree with each subscriber consistently with what is specified in the previous item 4) the maximum time for the DPSP to:

   a) exhibit a preserved data object;

b) exhibit various sets of preserved data objects;

c) give back to the data objects owner the entire set of preserved data objects in either case: upon request or at agreement expiration.

7) The service agreement with the data objects owner shall specify whether along with the information detailed in the previous item 6), also the derived metadata are to be delivered, or not, to the data objects owner. (See also clause 5.2.3, item 6) b))

8) If the agreement with the subscriber requires that, upon occurrence of some conditions, the DPSP must automatically delete specific preserved data objects; also the related backup copies, metadata, detached electronic signatures, where applicable, and any data from which such data objects can be reconstructed or related information can be derived must be deleted by the DPSP. Closure Evidence should be structured in a way not to be affected by the above deletion or, if this is impossible, a mechanism shall be implemented providing a reference to the original Closure Evidence to maintain the trust chain.

9) The DPSP shall agree with the data objects owners the media on which the data objects are to be given back to their owners.

NOTE 1: Please refer to clause 6.3.4.

10) When giving back data objects to their respective owners, in particular upon closure of a preservation agreement, the DPSP shall provide them alongside with the electronic measures ensuring their authenticity and integrity as per the applicable legislation, for instance using electronic signatures.

11) The service agreement, unless already addressed by the applicable legislation, should specify the procedure for granting the ownership of data objects to a new data objects owner, in case the original data objects owner ceases to exist (e.g. upon death of a natural person).

12) The DPSP shall specify in its agreement with a subscriber its personnel responsible for interfacing the subscriber as regards exchanging the agreement related information, among which the data objects to be preserved. The list of these persons shall be timely kept up to date to prevent information disclosures to unauthorised persons.

NOTE 2: See clause 5.2.7, item 2) for the provisions addressing the reverse communication.

13) The DPSP shall have in force auditable procedures ensuring that the preserved data objects are delivered or exhibited to legitimately entitled persons only, including duly authorised Assessors.

14) The modalities through which the deposited data objects are made available to authorised entities shall be specified in the service agreement.

5.2.5 Resolution of complaints and disputes

(TS 102 573 [3], clause 6.2, item 5))

1) The DPSP shall have in force auditable procedures to provide subscribers for each batch of data objects deposited at the DPSP's, with one or more receipts specifying detailed information suitable to withstand as evidence of the deposit even in court, for example supported by legally valid electronic signatures. The content of this information shall be specified in the service agreement.

NOTE: See also clause A.12.2.1.

2) The DPSP shall have auditable procedures to securely and reliably record and keep:

a) Evidence of the data objects reception;

b) The instructions from the depositor on:

i) How to handle the data objects.

ii) When and how modification and deletion to the preserved data objects are to be applied.

3) [EXT1] Personal data preservation:

   a) [EXT1.1] The DPSP shall have auditable procedures to report without delay to the correct controller(s) the requests by the personal data subjects related to their preserved personal data.

   b) [EXT1.2] The DPSP shall have in force auditable procedures that, in compliance with the applicable legislation, facilitate access by the data subjects to their personal data, rendered in intelligible form, within the maximum delay provided for by such legislation.

5.2.6 Organisation independence

(TS 102 573 [3], clause 6.2, item 8))

1) In order for the DPSP structure to comply with provisions of TS 102 573 [3], clause 6.2, item 8), one of the following shall be implemented:

   a) the DPSP is a company independent from any of its customers and from any of its providers of its electronic signature certification services (Certification Authorities), of time stamping services (Time Stamping Authorities) and of time reference services (UTC time providers);

   b) if the DPSP belongs to the same organisation as one or more of its customers or of the providers mentioned in the previous item, the DPSP shall ensure that its decisions regarding data preservation and exhibition and regarding its abidance by the applicable legislation are free from undue influence.

5.2.7 DPSP Subscriber Obligations

(TS 102 573 [3], clause 6.3)

1) Provisions in TS 102 573 [3], clause 6.3, shall apply to all data objects types, with the exception of subscribers' signing keys, since the DPSP is not expected to issues electronic signatures on behalf of its subscribers; for the same reason the last paragraph does not apply either.

2) The DPSP shall oblige through agreement the subscriber to communicate to the DPSP, with the timing that shall be specified in the relevant agreement, the identity of the persons entitled to act on his behalf, their specific roles and, where applicable, the means to identify and authenticate them.

3) The DPSP shall in its agreements clearly specify that the subscriber is eventually responsible towards the authorities for the compliance with the applicable legislation of the deposited data objects content, media, formats, etc.

5.2.8 Information for trading partners

(TS 102 573 [3], clause 6.4)

1) Provisions in TS 102 573 [3], clause 6.4 shall apply, with the exception of item a) that is covered in clause A.12.2.1, item 4), whereas the term "document signed by the TSP" has the broader meaning of any data object, also related to the DPS security enforcing mechanism.

2) All subscribers shall be provided with the following information on the DPSP:

   a) Whether the DPSP performs all the preservation related functions in person or by means of external providers.

   b) Information suitable to identify the external providers that perform all or part of the preservation related functions on behalf of the DPSP.

NOTE: See also clause 6.1.2.

5.2.9 Information for auditor/regulatory/tax authorities

(TS 102 573 [3], clause 6.5)

1) The DPSP shall have in force auditable procedures that ensure that the data objects to be reviewed by and exhibited to auditors, Assessors and authorities is exhibited along with the data proving its authenticity and integrity.

2) The DPSP shall specify auditors, regulatory and tax authorities the security measures they must abide by when accessing the DPS.

6 Objectives and controls in TS 102 573, annex A

The provisions in TS 102 573 [3] relevant to data preservation specified in the following clauses apply with the addition of the provisions specified in the corresponding clauses.

NOTE: The present document uses the term "data object" in place of TS 102 573 [3] term "document", where applicable. This note may not apply to versions of TS 102 573 [3] subsequent to V1.1.1.

6.1 SS.1. Signature

1) The long term preservation validity should be assured by using Advanced Electronic Signatures, in any of their strains such as CAdES, XAdES, PAdES, QES, etc. Other appropriate mechanisms may also be used, for example based on TSTs issued by a trusted source.

NOTE: Please be aware of the different contexts for the controls and objectives for applying electronic signatures in TS 102 573 [3] and in the present document. Whilst in the context of TS 102 573 [3] electronic signatures are used by the service provider to sign data objects on behalf of a service user, in the context of the present document they are used by the service provider as a possible means to prove the integrity of a preserved set of data objects as well as, if agreed with the DPSP customer, of a single data object to be preserved on behalf of a service user (whether or not the data object to be preserved was already signed at the time of acceptance for preservation by the service provider).

6.1.1 SS.1.1. Class of Electronic Signature

1) As a derogation from the basic requirements of TS 102 573 [3] "[N+]" normalized policy requirements, the electronic signature issued on behalf of the DPSP, in particular if used on the Closure Evidence, is not required to be a QES, but shall be at least an AdES, in compliance with the applicable legislation.

NOTE: Possible AdES can be, but not exclusively, CAdES, XAdES, PAdES, ASiC as specified in TS 101 733 [i.10], TS 101 903 [i.11], TS 102 778 [i.12], TS 102 918 [i.6] respectively.

6.1.2 SS.1.2. Certification

1) Certificates issued to the DPSP DS should be based on the most recent version of ISO/IEC 9594-8 [i.3].

2) The DPSP shall inform its subscriber prior to the service subscription with:

   a) complete information on the CAs that issue signature certificates to its DS; and

   b) where the certificates used by the DPSP to support its signatures are not QCs, information on what are the Certificate Policy and the Certificate Practice Statement complied with by the issuing CA and how this CA is assessed as complying with them; and

   c) information on which are the TSAs that issue timestamps to provide the preserved data objects with trusted time references, and the respective policies.

3) If the DPSP performs bulk signatures it is recommended that the signature certificates specify limitations of use suitable to prevent misuses, such as stealthily adding bogus data objects to the signature pipeline.

EXAMPLE: Signature certificates can specify that they are to be used only to sign data objects in an DPSP context and that their signature does not imply commitment by the signer to the data object content.

6.1.3 SS.1.3. Signature Creation Data

1) Any DPSP key management activity shall be logged in an auditable way. Where SSCD are used, the DPSP shall ensure they are provided, used and activated in compliance with the applicable CP/CPS. Where SSCD are not used, the DPSP shall ensure that reliable procedures and security mechanisms are enforced ensuring the SCD confidentiality.

6.1.4 SS.1.4. Certificate subject's Registration

1) Delegate signers shall be officially appointed by the DPSP relevant management or shall be delegated by the responsible for preservation.

2) The DPSP shall require all DS certificates to be issued upon specific agreements with CAs. Such certificates should specify in the "Organization" field a reference to the DPSP.

3) Where the adopted certificates are QC, all DS shall, where legally required, have been registered by a CA operating in compliance with the Certificate Policy defined in TS 101 456 [i.7] or with a Certificate Policy recognised as suitable by the relevant Authority.

4) Where the adopted certificates are not QC, all DS should have been registered by a CA operating in compliance with the Certificate Policy defined in TS 102 042 [i.8] or with a Certificate Policy recognised as suitable by the relevant Authority, where applicable.

6.1.5 SS.1.5. Certificate Revocation

1) The DPSP shall have in force auditable procedures to effectively request for revocation of the certificates used for the purpose of the DPS. These procedures shall be consistent with the agreement with the CA, that shall specify who (apart from the certificate subject) is entitled to forward a revocation request to the CA.

2) The DPSP DS, be they employees of the DPSP or of external providers, shall request for the revocation of their certificate used in supporting AdES issued on behalf of the DPSP as soon as they become aware, or have reasonable doubts, of the compromise of the correspondent private key.

3) The DPSP shall request for revocation of one certificate that was issued upon its request:

   a) as soon as the DPSP becomes aware of, or have reasonable doubts on, the compromise of the correspondent private key, regardless of whether the certificate subject has already submitted a similar request; or

   b) upon cessation of the certificate subject from the task in relation of which the certificate was issued; in this case the revocation request shall be submitted to the CA timely enough for the revocation to come into force before the certificate subject leaves his/her office.

6.2 SS.2. Maintenance of Signature over storage period

1) The DPSP shall ensure that the signatures it issues (e.g. within the Closure Evidence) are maintained as specified in the subsequent items, so that their validity can be verified at any time during the preservation period.

2) In order to allow the reliable verification of an AdES even if its supporting certificate is revoked or expires after the signing time, a reliable time reference should always be applied to it as close as possible to the actual signing time, to provide evidence that the AdES existed before expiration or a possible certificate revocation. Possible reliable time references are:

   a) TST, the format of which should be based on RFC 3161 [i.16] and on its updates or replacements.

b) Other trusted time evidence legally valid according to the applicable legislation, i.e. assertion by a trusted entity that the signature at issue existed at a certain point in time.

c) Time-mark in an audit trail.

NOTE 1: Further information can be found in CWA 14170 [i.13].

3) The DPSP shall have in force auditable procedures for maintaining signatures that, where applicable, envisage collecting evidence supporting the validity of signatures and that should be based on existing specifications, e.g. CWA 14171 [i.14].

NOTE 2: Among the evidence types the DPSP would fetch and store, at least for as long as the related signature, can be: CRLs (when the relevant CA removes the expired certificates from the CRL) or OCSP Responses.

4) The DPSP may derogate from the available technical specifications (e.g. CWA 14171 [i.14]) if they do not meet its legal/technical needs.

NOTE 3: If the DPSP has as a reference a specification, such as CWA 14170 [i.13], that does not take into account that the CA keeps the expired certificates in the CRL, in compliance with ISO/IEC 9594-8 [i.3], the DPSP may take this fact into account in its procedures to maintain signatures.

5) If the DPSP is a legally recognised trusted entity, such as a Public Officer, previous items 1) to 4) might not apply according to applicable legislation.

6.3 SS.3. Storage

6.3.1 SS.3.1. Authorized Access

1) The DPSP shall have in place documented and auditable procedures to prevent any unauthorized access. Where applicable, the status of data objects ownership (as in the case of heirs) shall be ascertained, for example through verification at central Registries. Among authorised persons, but not exclusively, are:

a) Data objects owners, including their legal representatives that shall be named in the agreement or in subsequent papers recognised as authentic and valid.

b) Duly authorised personnel.

c) Public Authorities such as authenticated police and tax authority officers.

2) The DPSP shall modify and/or delete the preserved data objects only upon valid request by the data objects owner or in compliance of specific agreement stipulations. The DPSP shall keep an audit trail of any modification and/or deletion.

3) Where the remote access requires an end-to-end encryption to be implemented the DPSP shall agree with the counterpart what encryption system, selected among the state of art ones, best suits the specific case and shall document the reason of the choice. The previous documentation is not necessary if the encryption system is imposed by force of law or by an authority, such as national or international courts or the police forces.

4) Access authorisation to preserved data objects shall not be all encompassing, i.e. each authorised entity shall be able to access only the data objects it owns or it has specific rights for.

See also clause 6.4.

6.3.2 SS.3.2. Authenticity and Integrity

In addition to provisions in clauses 6.1 and 6.2, related respectively to the clauses SS.3.2.1 and SS.3.2.2 of TS 102 573 [3], annex A, the following provisions apply, related to TS 102 573 [3], clause SS.3.2.3:

1) In order to streamline both the preservation process and the remote exhibition of preserved data objects, the DPSP should adopt a solution based on Closure Evidence.

2) Where the Closure Evidence is used the DPSP shall document how the Closure Evidence solution is implemented, based either on a publicly available specification or on custom developed specifications.

3) Where the DPSP does not implement the Closure Evidence mechanism it shall implement documented mechanisms ensuring to achieve over time the same authenticity, integrity and accountability objectives as the signed Closure Evidence.

4) If the Closure Evidence is based on a publicly available specification, the DPSP shall document which options of such specification are implemented.

5) If the Closure Evidence is not based on public specifications, the DPSP shall draft and retain a detailed technical specification describing how the Closure Evidence is structured and maintained. It is vital that the authenticity, integrity and readability of the Closure Evidence are ensured over time.

NOTE: The Closure Evidence structure can be based as follows:

a) It contains metadata related to one specific set of preserved data objects, built up for example with the digests of at least all the data objects therein contained, including the receipt (see clause 5.2.5) related to these data objects. Thus, the Closure Evidence proves that data objects with the given digests were stored by the DPSP.

b) It is structured in a way to facilitate parsing.

c) It is updated every time a new data object, upon duly authorized request from the DPSP subscriber, is added to / deleted from the set of the preserved data objects it relates to; upon update a new Closure Evidence is created, as per the following item 7).

d) It is structured in a way to allow the traceability of data objects and the accountability of the DPSP. For every digest within the Closure Evidence, the DPSP is to be able to exhibit one of the following at any point of time:

i) the preserved data object with the corresponding digest;

ii) the documentation regarding the deletion of the data object with the corresponding digest.

e) It is verifiable even after the deletion of any data object protected by it.

6) Where the Closure Evidence is sealed with a signature, the DPSP shall state with this signature that the preservation process has been properly performed, in abidance by the present document provisions.

7) The DPSP shall have in force auditable procedures ensuring that, when the algorithms on which the Closure Evidence is based on are becoming cryptographically weak, a new Closure Evidence will be created based on state of art algorithms. This new Closure Evidence shall have a reliable link to the previous Closure Evidence to maintain the chain of trust. A similar solution shall be implemented when other mechanisms are used instead of the Closure Evidence.

6.3.3 SS.3.3. Data Object Readability

This entire clause is to be assumed to address [EXT] services aiming to ensure data objects readability.

1) To ensure data objects availability, data objects readability shall be met, either at the place of preservation or remotely, even in case of formats obsolescence. To achieve this, one of the following measures shall be implemented consistently with the applicable legislation:

a) the DPSP shall store, for all the time the data objects are kept in their original format, the software necessary to the data objects exhibition. The DPSP shall be able to make use, where necessary, also of the related hardware as well as any other necessary equipment required to perform the data objects presentation. This can be achieved either by purchasing the hardware and equipment at issue or by ensuring its use at some external service provider's.

NOTE 1: Another possible way is to store the specifications of the data objects format, and to guarantee that there will exist software applications capable of exhibiting those particular formats. This latter method can be used only if the specification of the data objects format can be obtained, e.g. in case of Open Document Format (ODF) [i.38].

b) The DPSP shall perform a format conversion as follows:

i) The DPSP shall implement it consistently with records management related ISO standards.

ii) Where the DPSP is not itself a trusted third party (e.g. a Public Officer), it shall have in force auditable procedures to require the intervention of a trusted third party attesting that the data objects transposed in a new format have maintained their original semantics.

2) The DPSP shall have in force auditable procedures to verify the actual readability of the preserved data objects at intervals, as a minimum as provided for by the applicable legislation, suitable to ensure timely detection of degradation in readability.

NOTE 2: Examples of degradation in readability are: corruption of a particular media used for storing the data object; corruption of some bits of the data object; or when all bits of a data object are available, and the DPSP can present them to authorised end users, but the DPSP cannot display the data object properly in a readable format anymore.

3) Where degradation in data object readability is detected, the DPSP shall recreate the data object at issue from its backup copies with timeliness suitable to prevent delays in the data objects exhibition upon request. This event shall be dealt with as an information security incident (see clause A.13).

4) The agreement in force between the DPSP and the data objects owners shall address what follows. If degradation in data object readability is detected and it is impossible to recreate the data object as it originally was, the DPSP shall execute an auditable procedure to formally notify the data object owners without delay.

5) The DPSP Business Continuity Management (see clause A.14) shall address also the software and hardware consistently with the previous item 1), in particular letter a).

6.3.4 SS.3.4. Storage media type

1) Where the applicable legislation does not require specific media types, and the media types are of concern to the data objects owners, the DPSP may agree on these media types with the data objects owners, provided they are chosen among the state of art ones.

NOTE: It is possible that the DPSP accepts and exhibits data objects over a network only. In this case, the data objects owner does not need to work with the media used by the DPSP.

2) In case the DPSP uses media types not suitable to last at least for the envisaged preservation period, or if the adopted media prove not to last as long as expected, the DPSP shall have written plans and auditable procedures for regularly migrating from one media type to another, performing data object recreation procedures too (see also clause A.10.7.1, items 4) and 5)).

3) If the DPSP learns that - in contrast to their specifications - the used media types do not last for the envisaged preservation period, the DPSP shall migrate to another media type in time.

6.3.5 SS.3.5. Data Objects Format

1) Agreements between the DPSP and its service subscribers shall specify explicitly if the data objects submitted to the DPSP are in analog and/or in electronic formats. See also clause 5.2.7, item 3).

2) The DPSP should submit all deposited data objects to the preservation process. Deviations may exist if EXTENDED services are provided as specified in the subsequent clauses 3 to 5, or in further EXTENDED services, and the agreement with the depositor stipulates that data objects, that the DPSP reports to the subscriber as faulty, are not to be preserved as delivered by the subscriber, as specified in the subsequent item 6).

3) [EXT1] - When the data objects submitted to the DPSP are in electronic format the DPSP shall have in force auditable procedures to verify if the received data object formats comply with the applicable legal requirements or with the formats agreed with the customer (see also clause 5.2.4, item 5).

4) [EXT2] - When the data objects submitted to the DPSP are in electronic format the DPSP shall have in force auditable procedures to verify, based on documentation issued by de jure or de facto standardisation organisations, if the received data object formats are not known as prone to hosting Presentation Corruption Agents.

NOTE: Among the "de facto" standardisation organisations are the "specialised and mostly global fora and consortia" the EU COM(2009) 324 [i.35] paper explicitly mentions and for which it suggests at section 2.5: "European policy should build on and benefit from the potential provided by fora and consortia".

5) [EXT3] - When the data objects submitted to the DPSP are in electronic format the DPSP:

   a) shall have in force auditable procedures to verify whether the received data object formats are free of Presentation Corruption Agents (see also previous item 4), and it shall notify the subscriber of any fault; and

   b) shall have available evidence of the capability of the above auditable procedures to actually verify whether the received data object formats are free of Presentation Corruption Agents. This evidence may be provided experimentally through test runs.

6) If the previous clauses from 3 to 5 apply the DPSP shall notify the subscriber of any exception and shall deal with the faulty data objects as specified in the agreement with the subscriber.

EXAMPLE: Depending on what is stated in the preservation agreement, the DPSP can submit to preservation only the compliant data objects, or else also the non compliant ones, or amend the non compliant ones and submit them to preservation once amended, etc.

7) [EXT4] - Where data objects must be preserved in XML format, all information that concurs in producing the presentation of these data objects, according to de jure or de facto standards in force that must be agreed upon with the subscriber shall also be preserved.

6.3.6 SS.3.6. Requirements on Separation and Confidentiality

1) The DPSP shall have in force auditable procedures ensuring the implementation of TS 102 573 [3], annex A, SS.3.6, in order to ensure records' confidentiality by segregating assets of different data objects owners, at least using a suitable logical access separation.

6.4 SS.4. Reporting to and Exchanges with Authorities

1) Where remote access is legally allowed or required, the DPSP shall have in force auditable procedures ensuring the implementation of TS 102 573 [3], annex A, SS.4.1, by enacting remote exhibition and submission of the preserved data objects to the requesting Authorities through secured channels, i.e. to ensure the confidentiality of:

   a) The authentication process.

   b) The transmitted data objects.

For example based on state of art TLS [i.37] protocols or on end-to-end encryption.

NOTE 1: The possibility that the said Authorities are equipped to implement on their side neither TLS channels nor end-to-end encryption is not taken into account.

NOTE 2: In this case derogation from requiring compliance with TS 102 573 [3], annex A, SS.4.2 [N+] is accepted. TS 102 573 [3] "[N]" variant of normalized policy is also acceptable.

NOTE 3: Compliance with TS 102 573 [3], annex A, SS.4.3 is ensured by compliance with clause 6.2.

6.5 SS.5. Conversion of Analog Originals to Digital Formats

Implementation of this clause provisions is to be considered an EXTENDED service.

[EXT1] The present document lays down no provision related to handling analog data objects.

1) [EXT1.1]:

   a) [EXT1.1.1] The DPSP shall have auditable procedures to convert data objects, originally in analog formats, to electronic formats, agreed upon with the data objects owner, that (see also clause 6.3.5, item 4):

      i) are formally recognised as legally valid, where applicable; or

      ii) are indicated by technical reports, issued by de jure or de fact organisations, as known, at the current state of art, as immune from PCAs.

NOTE 1: More on data object formats is at clause 6.3.3, item 1) b); more on de jure and de facto organisations is at clause 6.3.5, item 4).

   b) [EXT1.1.2] The above procedures in the previous item 1) a) shall provide for each set of analog data objects an audit trail, that should be based on de jure or de facto standard specification, specifying at least:

      i) The processing operator identifier, whose identification shall be supported by strong authentication.

      ii) An inventory of data objects making up each single batch that was input into the procedure.

      iii) The number and type of failures occurred in processing each single batch of data objects.

      iv) The number and type of manual and automated interventions performed, while converting each single batch of data objects, to remove processing problems and the data objects related to each problem; if the problem is such to require removal of data objects from the conversion process, this shall be clearly indicated, at least referring to the data objects numbering in the process.

      v) The overall number of the output data objects generated from the conversion of each single batch.

   c) [EXT1.1.3] As the last step of the conversion procedure in the previous item 1) b) the Closure Evidence should be generated.

NOTE 2: If the feature in clause 6.3.2, note, letter b) is implemented, the Closure Evidence would be generated.

2) [EXT1.2] Where one analog data object is to be digitally preserved, and it is a "unique original" an AdES should be applied on behalf of the DPSP to its electronic copy; it is recommended that the assertion provided for by TS 102 573 [3], annex A, SS.5.2, is associated to the electronic copy, even if not required by the applicable legislation.

3) [EXT1.3] The DPSP shall make available to the Assessors the outcomes of the Risk Assessment addressing the conversion from analog to digital format, specifying the rationale for the consequent operational choices.

Annex A (normative): ISO/IEC 27001 related Long Term Preservation-specific ISMS control objectives, controls and implementation guidance

A.1 Reference to ISO/IEC 27001

In each of the subsequent clauses, from A.5 on, the corresponding ISO/IEC 27001 [1] clause is specified.

A.2 Basic ISO/IEC 27002 provision

The number of each of the subsequent clauses, from A.5 on, matches the numbering of the corresponding ISO/IEC 27002 [2] clause (e.g. clause A.5.1.1 of the present document corresponds to ISO/IEC 27002 [2], clause 5.2.1).

Compliance with the controls in the ISO/IEC 27002 [2] clauses is recommended.

A.3 Enhanced ISO/IEC 27002 provisions

Each subsequent clause inherits provisions in the corresponding ISO/IEC 27002 [2] clause while specifying, where applicable, which ones do not apply, or, conversely, are deemed as mandatory, in the DPSP environment.

A.4 New specific controls

In each subsequent clause additional provisions, mandatory, recommended or optional, may be specified.

A.5 Security Policy

A.5.1 Information security policy

A.5.1.1 Information security policy document

Long Term Preservation specific controls:

a) The DPSP shall have in force Information Security Policy Document endorsed by the relevant and specifically appointed senior management, also covering the instructions from the Controller, where personal data are dealt with.

b) The ISPD shall address the data objects protection in a manner commensurate with the specific data objects sensitivity, value, and criticality (see also clause A.7.2.2) as specified in the agreements with the data objects owners.

c) The Information Security Policy Document, specifying among other things each role's duties and privileges, shall be made available, and where applicable delivered, in auditable way to all personnel involved in the DPS operations, including external providers of DPS related services. In the latter case of personnel belonging to external providers, the ISPD shall be formally delivered to the recognised representative of each external provider who shall, in turn, deliver it in an auditable way to the interested persons. See also clause A.8.1.3.

d) Where necessary for confidentiality reasons, the Information Security Policy documentation should be structured in parts to be distributed, consistently with the confidentiality level requirements, only to the persons that have the specific and actual need to know.

A.5.1.2 Review of the information security policy

Long Term Preservation specific controls:

1) The Responsible for Preservation, supported by specialised teams having as purpose to keep themselves up to date with security and legislation topics, shall ensure that the ISPD is reviewed, based on the outcomes of a previously repeated Risk Assessment:

   a) At least yearly.

   b) Upon detection of security incidents or of security weaknesses deemed at high risk by the DPSP incident management body (see also clauses A.13.2.1, item 1), and A.13.2.2, item 2).

2) The DPSP Management shall enforce the reviewed ISPD, in particular when the revision was triggered by security incidents or by identified security weaknesses, with timeliness depending on the severity of the identified risks.

3) The timeliness as in the previous item 2) shall be derived from the Risk Assessment.

A.6 Organization of information security

A.6.1 Internal organization

A.6.1.1 Management commitment to information security

Long Term Preservation specific control:

1) The DPSP shall keep exhaustive and auditable documentation, even historical, on its own organisation.

2) The DPSP should make sure that all depositors are made aware of the up to date DPSP organisation as per what affects them.

3) The DPSP should specify the data objects organisation scheme in a auditable documentation that may be made available to its subscribers since the inception of their agreement relationship.

4) The DPSP Management shall ensure that implementation of ISO/IEC 27002 [2] corresponding clause item g) ("initiate plans and programs to maintain information security awareness") includes ascertainment that the persons are timely retrained at least whenever the ISPD and/or the procedures are updated. Upon update due to security incidents a description of the occurred incident should be provided as confidential information to the persons who have the need to know.

A.6.1.2 Information security co-ordination

Long Term Preservation specific control:

1) The DPSP security shall be governed throughout the entire DPSP in a way suitable to prevent implementation of conflicting practices in the various DPSP departments (e.g. hierarchical structure).

A.6.1.3 Allocation of information security responsibilities

Long Term Preservation specific controls:

1) A suitable chain of command for the information security responsibilities shall be clearly defined, consistently with the DPSP size; the responsible persons shall be clearly identified by name and/or by role title; the identification of reference points in case of security incidents shall be continuously and unambiguously assured.

2) The documentation of clause A.6.1.1, item 1) shall indicate as a minimum who have been in the time the officers Responsible for the Preservation and for each of them in what time period.

3) Each officer, to whom information security responsibilities are allocated, shall be assigned his/her duties in writing and shall accept them in writing (see also clause A.8.2.1).

A.6.1.4 Authorization process for information processing facilities

Long Term Preservation specific control:

1) Particular care should be taken when emerging technologies are implemented, since the possible attacks on their authentication mechanisms may not be entirely known, therefore a specific sign off from the department in charge of Information Security should be obtained before implementing emerging technologies.

NOTE: With the purpose of better specifying this clause applicability, the following non exhaustive list is provided of items that fall under the term "facility".

i) buildings;

ii) building infrastructures, such as: gates, alarms, locks;

iii) Information Technology equipment, both static and portable;

iv) temporary store for media and equipment;

v) air conditioning systems, including their ducts that may convey toxic substances, virus and bacteria;

vi) regular and emergency power supplies;

vii) communication networks;

viii) personnel authenticating systems, e.g. PIN PADs, cryptographically based objects like smart cards and biometric identification systems.

A.6.1.5 Confidentiality agreements

Long Term Preservation specific controls:

1) No information on the DPSP, on its DPS related service providers, on its customers and on the preserved data objects shall be disclosed unless a derogation authorisation has been explicitly specified in writing by the data objects owner, by the DPSP management or by the DPS related service providers, respectively, depending on the information at issue, and, even in this case, it shall only be disclosed to persons with a need to know formally recognised either by the data objects owner or by the DPSP management.

2) The provision in the previous item 1) shall apply also when the DPSP advertises its own researches for personnel.

3) The confidentiality measures shall be implemented taking into account, among other things, the data objects depositor's instructions and the applicable legislation.

A.6.1.6 Contact with authorities

Long Term Preservation specific control:

1) The DPSP shall indicate by name or job title which officers are entitled to speak to authorities on behalf of the DPSP.

A.6.1.7 Contact with special interest groups

Applicable. No further control and/or implementation guidance needed.

A.6.1.8 Independent review of information security

Long Term Preservation specific control:

1) If the DPSP Management, either out of its own act of will or where so required by the applicable rules, appoints auditors to enact reviews on the DPS, these auditors shall in advance provide evidence of their compliance with the rules on auditors' conformity, such as ISO/IEC 17021 [i.4].

A.6.2 External Parties

A.6.2.1 Identification of risks related to external parties

Applicable. No further control and/or implementation guidance needed.

A.6.2.2 Addressing security when dealing with customers

Applicable. No further control and/or implementation guidance needed.

A.6.2.3 Addressing security in third party agreements

Long Term Preservation specific controls:

1) [EXT1] Data protection:

   - Outsourcing of DPS related services to organisations resident in third countries shall comply with the implementation in the applicable legislation of Directive 95/46/EC [i.29], article 25 (2).

2) The obligations specified in the agreements with third parties shall be in line with the outcomes of the Risk Assessment.

3) The inception of any DPS related outsourced activity shall be subordinated to the DPSP management's approval of the related outsourced service provider's Information Security Policy Document.

4) If the DPSP is not in possession of the skill necessary to assess the Information Security Policy Document specified in the previous item 3), it may resort to external consultants that shall have neither business nor organisational links with the service provider at issue.

5) Agreements between DPSP and its providers of DPS related services shall specify to which extent the continuity of the service providers business operations related to the DPS shall be ensured.

6) Agreements with providers of outsourced DPS related services shall ensure the existence of an effective and regularly tested back-out plan, approved by the DPSP Information Security management, which permits the DPSP to revert to internal processing and/or to move to another provider the services at issue.

NOTE 1: One example of changing service provider is the telecommunication services provision where the DPSP can have in force multiple agreements with different telcos.

7) Agreements with providers of outsourced DPS related services shall include the DPSP right to:

   a) access, through duly authorised and authenticated persons, where necessary delegated by the DPSP, the data objects preserved by the provider on behalf of the DPSP; and to

   b) perform, directly or by means of external auditors delegated by the DPSP, inspections on the providers' activities and premises, related to the DPS related services, and on the data objects they manage on behalf of the DPSP. Agreements shall specify the inspection modalities.

8) Agreements with developers of "ad hoc" software shall require them to deposit in an agreed software escrow facility the most recent version of the developed source code and the related operations documentation using agreed formats and media.

NOTE 2: The purpose of this provision is to ensure the DPSP the possibility to maintain the provided software even if the software providers go out of business.

A.7 Asset Management

A.7.1 Responsibility for assets

A.7.1.1 Inventory of assets

Long Term Preservation specific controls:

1) The DPSP shall keep, in addition to the list of kinds of asset specified in the corresponding ISO/IEC 27002 [2] clause, an auditable inventory of the data objects, where applicable subdivided by data object type, deposited by subscribers, including the history of input, modified and deleted data objects.

NOTE 1: This inventory would be dynamically derived from the DPS.

2) The asset inventory shall specify also the version of the various system components and the period where each of them was operational.

NOTE 2: The association between versions and the above operational period would be useful when performing problem determination.

3) The inventory as in the previous item 1) shall be structured at least as required by the applicable legislation, for example based on the data object owners, on their original format - analog or electronic, on their area of interest - fiscally relevant data objects, legally relevant data objects, etc.

4) If no format or structure is legally specified for the inventory indicated in the previous item 1), the DPSP may implement any structure and format that meet the above requirements.

5) The DPSP should ensure that for each storage logical unit, within the documentation indicated in clause A.6.1.1, item 1), an auditable inventory is maintained that specifies at least:

   a) the identification data of all the persons that in the time were in charge of the data preservation;

   b) the identification data of officers delegated to perform specific data preservation tasks;

   c) the location where the back-up copies are kept.

6) All inventories shall be constantly updated and their correspondence with the real assets shall be verified at least once a year.

7) For any data object, the DPSP shall keep, for the same time the data object itself is preserved and under the same measures:

   a) the documentation of all its related procedures;

   b) the related audit outcomes;

c) documentation related to incidents that have affected the preserved data objects.

A.7.1.2 Ownership of assets

Long Term Preservation specific controls:

1) The DPSP shall appoint in writing all persons acting on the DPS for the purposes of the DPSP, clearly specifying the preserved data objects and data object preserving processes each of them owns, i.e. is responsible for.

2) At least the owners of the following processes shall be specified (see also clause 6.3.5):

   a) In relation to core Processes:

      i) Secure log management process.

      ii) Incoming data objects acceptance.

      iii) Preservation core process, including Backup.

      iv) Management of the DPS related assets processing.

      v) Preserved data objects exhibition/return.

      vi) Disaster Recovery / Business Continuity Plan.

      vii) Electronic data objects deletion.

   b) In relation to EXTENDED Processes, where applicable:

      i) Analog data objects post-preservation deletion.

      ii) Incoming electronic data objects scanning with Antivirus programs.

      iii) Incoming electronic data objects format validity assessment.

   NOTE 1: Refer to clause 6.3.5, provisions related to Extended Services.

      iv) Extended data objects indexing.

      v) Signature verification.

      vi) Format conversion.

   NOTE 2: Ownership of the processes will be assigned in abidance by the job separation principle.

3) Consistently with what is specified in clause A.14.1.4, item 2), the "Disaster Recovery Team" will be entrusted with ownership of assets authority suitable to allow for resumption of operations in case Disaster is invoked, in real or in case of drills.

A.7.1.3 Acceptable use of assets

Applicable. No further control and/or implementation guidance needed.

A.7.2 Information classification

A.7.2.1 Classification guidelines

Long Term Preservation specific control:

1) Any data object shall always be assigned in an auditable way its classification level.

2) As regards the preserved data objects the DPSP shall abide by the classification requirements specified by the data objects owner.

3) The DPSP shall inform in the agreement documentation the data object owner that if no indication is provided on his data classification, the lowest applicable classification level will be enforced, providing him also with an explanation on the consequences of such classification.

NOTE: If this condition occurs in relation of personal data, the DPSP will not be held responsible for non law-abiding preservation of the data object deposited by the data object owner, unless the DPSP is also acting as the Controller.

4) The DPSP shall have an auditable procedure ensuring that the confidentiality classification of DPSP related information (procedures, policies, etc.) shall be reviewed regularly, at least once per year, to prevent obsolete classification from, on the one hand, putting at risk data objects that in the meantime have achieved a higher classification level, and, on the other hand, requiring undue effort to enforce confidentiality rules disproportionate to the current actual confidentiality level.

5) The DPSP shall oblige by agreements its subscribers to timely communicate any change in the classification level of the deposited data objects.

A.7.2.2 Information labelling and handling

Long Term Preservation specific control:

1) The DPSP shall have an auditable procedure ensuring that where different confidentiality classification levels are assigned to different data objects stored on one single media or in a storage logical unit, the overall classification level of the single unit shall be the most stringent among those of the stored data, unless the data object within is intrinsically protected consistently with their classification level.

NOTE: One example of intrinsic protection is the data object encryption.

2) The DPSP shall have an auditable procedure ensuring that each removable media (electronic, paper, etc.) shall always be labelled according to the highest classification level assigned to the data objects stored inside (see clause A.7.2.1).

3) Officers remarking that one item has no label shall report the event to the item owner and in the meantime the item shall be dealt with according to the highest classification level known for the data objects stored inside.

4) The DPSP shall have an auditable procedure ensuring that when one confidential data object is copied in various instances (on paper, electronic media, etc.) the various copies shall receive the same classification level as the original and if their classification requires protection their distribution shall be tracked.

5) Confidential data objects shall be shipped as specified in clause A.10.8.3, item 2).

A.8 Human resources security

Long Term Preservation specific controls:

1) The DPSP shall oblige through contractual agreement also its DPS related services providers to implement the provisions in this clause and in the applicable corresponding ISO/IEC 27002 [2] clauses.

2) The DPSP shall oblige by contractual agreement its outsourcing providers to allow inspections as in clauses 4.2 and A.6.2.3, item 7) b) to be performed also on the issued dealt with in these clauses and in the applicable corresponding ISO/IEC 27002 [2] clauses.

A.8.1 Prior to Employment

A.8.1.1 Roles and responsibilities

Long Term Preservation specific control:

1) At least the DPS system administrators shall be individually appointed in writing and they shall accept in writing their job.

A.8.1.2 Screening

Applicable. No further control and/or implementation guidance needed.

A.8.1.3 Terms and conditions of employment

Long Term Preservation specific control:

1) The DPSP shall oblige in writing all officers acting on the DPS to comply with the rules governing the DPS. Officers shall:

   a) declare in writing that they have been informed in writing of such rules;

   b) declare in writing that they have been informed in writing of the existence of sanctions they would incur in case of violation of the rules.

2) The procedure as in the previous item 1) should be repeated yearly. Among the therein mentioned rules is the corporate code of conduct, the Information Security Policy Document, the DPSP operating procedures, the applicable legislation in force, including the privacy related one.

See also clause A.5.1.1.

A.8.2 During Employment

A.8.2.1 Management responsibilities

Long Term Preservation specific controls:

1) The DPSP shall ensure that all DPSP officers involved in the DPS operations:

   a) have their job description formally communicated in writing; and

   b) declare in writing that they have been delivered in writing their job description.

2) Each employee's job description shall specify at least the employee's responsibilities, including those related to the information security.

3) The DPSP management shall appoint to the DPSP mansions only persons that have been evaluated as experienced and reliable.

A.8.2.2 Information security awareness, education, and training

Long Term Preservation specific controls:

1) All officers operating on the DPS shall be formally informed in writing on the security policy and procedures, including the ISPD, and shall:

   a) accept in writing the related obligations;

   b) declare in writing their awareness that they would incur in sanctions in case of violation of the security policy.

This procedure should be repeated at least every time that the security policy or the security procedures are changed.

2) The DPSP shall have in force ad hoc up to date training programs to hone the information security awareness and education of officers acting on the DPS.

NOTE 1: This training program would include also information on workplace hazards, on safeguards aiming to reducing the workers' risks, and on the proper use of these safeguards, including hazardous material handling.

NOTE 2: See also clause A.13.1.1, items 3) and 4), and clause A.13.1.2, items 3) and 4).

A.8.2.3 Disciplinary process

Applicable. No further control and/or implementation guidance needed.

A.8.3 Termination or Change of Employment

A.8.3.1 Termination responsibilities

Long Term Preservation specific controls:

1) Officers acting on the DPS shall formally be made aware that the confidentiality agreement shall be in force even after their termination or change of their employment.

2) [EXT1.1] Personal Data Preservation:

   Officers acting on DPS preserving personal data shall formally be made aware of the legal consequences of not abiding by confidentiality rules regarding sensitive and judicial personal data even after termination or change of their employment.

A.8.3.2 Return of assets

Applicable. No further control and/or implementation guidance needed.

A.8.3.3 Removal of access rights

Long Term Preservation specific controls:

1) One officer's access rights to DPSP information shall be removed when this officer leaves his assignment.

2) The DPSP organisation chart shall be timely updated to reflect one officer's termination from his/her assignment and this update shall be timely distributed to all interested officers.

A.9 Physical and environmental security

A.9.1 Secure Areas

A.9.1.1 Physical security perimeter

Long Term Preservation specific controls:

1) The DPSP Computer rooms shall be equipped with safety doors that set off an audible and visible alarm when kept open beyond a predefined period of time.

2) The DPSP shall have in force an auditable procedure to log all events that set off the alarms.

3) When there is a need to disable the alarm as in the previous items, or to lengthen the trigger interval (e.g. in case of transporting material in and out of the room), this shall be done only after specific and traceable authorisation by the person in charge of the room security.

4) All alarm setting off, the severity of which is not immediately and downgraded in an auditable way, shall be dealt with as a major security incident requiring a quick and detailed analysis.

A.9.1.2 Physical entry controls

Long Term Preservation specific controls:

1) The DPSP shall have in force auditable procedures ensuring that access to the DPSP areas where data objects are processed or stored is controlled and restricted to authorized persons only.

2) Where DPS components are located in rooms shared with other application systems, auditable procedures shall be in force ensuring that access to the DPS components is allowed only to authorised persons.

3) Visitors shall be allowed to access the DPSP areas where data objects are processed or stored only under auditable supervision by an authorised DPSP officer who shall be responsible for the visitor's acts.

4) Refer also to clause A.11 as regards physical entry authorisation.

A.9.1.3 Securing offices, rooms, and facilities

Long Term Preservation specific controls:

1) The DPSP ISPD shall have a section dedicated to a physical security plan, consistent with the outcomes of the Risk Assessment that is reviewed and updated by the senior manager in charge of the physical facilities.

2) An auditable "clean desk policy" shall be enforced requiring all DPSP officers, dealing with confidential information including all data objects to be submitted to preservation, not to leave such confidential matter in the open when they are absent.

3) The DPSP areas where its processing equipment and the preserved data objects are stored, shall be equipped with security measures that, whenever they must be evacuated in emergency, prevent unauthorised access, yet ensuring supervision by authorised persons.

4) Unattended equipment shall be placed in premises under surveillance and with physical access control implemented in order to avoid unauthorised attempts of access such equipment.

A.9.1.4 Protecting against external and environmental threats

Long Term Preservation specific control:

1) At least the entrance to the DPSP premises should be equipped with riot doors, fire doors, and other doors resistant to forcible entry. Deviations to this requirement are acceptable if the DPSP is located inside premises that per se provide such protection and if access to the DPSP from within these premises is protected by locked doors controlled either with manned reception areas or with electronic means.

A.9.1.5 Working in secure areas

Applicable. No further control and/or implementation guidance needed.

A.9.1.6 Public access, delivery, and loading areas

Long Term Preservation specific control:

1) The DPSP shall implement requirement in item b) of the corresponding ISO/IEC 27002 [2] clause with reference to the parts of the building where the preserved data objects are processed and kept.

2) When third party personnel, extraneous to the DPSP activity, is authorised to access DPSP restricted areas, they shall not have unmonitored access to DPSP computing and communications equipment.

A.9.2 Equipment Security

A.9.2.1 Equipment siting and protection

Long Term Preservation specific controls:

1) The DPSP processing equipment shall be sited in a way to prevent electromagnetic emissions, produced by this equipment, from being captured by unauthorised persons.

NOTE: This goal can be achieved not only by means of anti-Tempest attack certified technical measures, like, for example, shielded rooms or specifically designed processing systems, but also by means of organisational measures that prevent Tempest attacks from being performed undetected.

2) See also clause A.9.1.2.

A.9.2.2 Supporting utilities

Long Term Preservation specific controls:

1) In case of external power supply breakdown, an DPSP emergency power supply shall be ensured at least for the time required to perform a regular shutdown of the DPS components.

2) The DPSP shall ensure that also during the DPS components regular shutdown the computer rooms' environmental conditions are compatible with the machine and human activities.

A.9.2.3 Cabling security

Applicable. No further control and/or implementation guidance needed.

A.9.2.4 Equipment maintenance

Applicable. No further control and/or implementation guidance needed.

A.9.2.5 Security of equipment off-premises

Applicable. No further control and/or implementation guidance needed.

A.9.2.6 Secure disposal or re-use of equipment

Long Term Preservation specific control:

1) The DPSP shall have an auditable procedure ensuring that when any DPS piece of equipment is disposed of, if it is not securely destroyed, all content deemed as confidential by the DPSP, including the preserved data objects, shall be securely deleted, under the responsibility of the equipment owner, by overwriting the original data objects using techniques to make it non-retrievable. See also clause A.7.2.1.

A.9.2.7 Removal of property

Long Term Preservation specific controls:

1) The DPSP shall have in force an auditable procedure to promptly inform all interested persons of any changes in the authority in charge of permitting off-site removal of assets.

2) The DPSP should perform the spot checks mentioned in the "Other information" section of the corresponding ISO/IEC 27002 [2] clause.

A.10 Communications and operations management

A.10.1 Operational procedures and responsibilities

A.10.1.1 Documented operating procedures

Long Term Preservation specific controls:

1) The documentation as in clause A.6.1.1, item 1) shall indicate at least:

   a) The storage logical unit content structure, ensuring a logical separation at least by data objects owners and making possible a separation based on data objects and content types (e.g. based on fiscal or legal requirements, where applicable) when required by the data objects owner or legally needed.

   b) The history of the content of each storage logical unit, specifying who applied what addition, modification or deletion, when, upon whose authorisation.

   c) For each storage logical unit, information suitable to identify what back up copies exist and where they are located.

   d) What documentation specifies the indexing and searching mechanism in place for all preserved data objects.

   e) In what cases a trusted third party (e.g. a Public Officer) must be summoned and what auditable procedure must be followed.

2) If the documentation as per the previous item 1), and in particular the storage logical unit content structure as per item b), is not explicitly specified by the applicable legislation, it should be specified in the agreement between the DPSP and each data objects owner.

3) The DPSP relevant management shall formally sign off the procedures documentation before they are put into operation.

NOTE: As far as documentation related to back-up and disaster recovery/business continuity is concerned, see also clauses A.10.5 and A.14 respectively.

4) The DPSP shall securely keep up to date the documentation of the application procedures in operation, formally approved by an appointed manager, to be regularly checked against the procedures actually in operation. Any detected mismatch shall be considered, and dealt with as, a security incident.

A.10.1.2 Change management

Long Term Preservation specific controls:

1) Any change to the DPS shall be previously formally authorised by the relevant manager. Where urgent changes, due for example to malfunctions, need be applied without delay, the responsible manager shall be informed as soon as possible and shall undertake the related action that shall be documented.

2) Any change to the DPS shall be traced and auditable.

3) Regular and constant security update, e.g. of anti-malware tools, shall always be implemented as soon as they are available without requiring previous authorisation by the relevant manager. Rollback procedures shall be in force to be enacted if such updates lead to service disruption. Such cases shall promptly be reported to the relevant manager.

A.10.1.3 Segregation of duties

Long Term Preservation specific controls:

1) Segregation of duties shall be implemented in an auditable way. Organisational solutions shall be adopted to work around technical hindrances to implementing the segregation of duties.

NOTE: Segregation of duties is at least to be applied to System Administrators, System Operators, and Auditors.

2) The DPS shall not be operated with System Administrator's privileges.

A.10.1.4 Separation of development, test, and operational facilities

Long Term Preservation specific controls:

1) ISO/IEC 27002 [2], clause 10.1.4, item f) is to be interpreted with the meaning that sensitive data may be used in a tests environment only if:

   a) the information capable to identify the data subject is either removed or made anonymous; and

   b) the information context is such that the data subject identification is not possible.

2) The DPSP shall provide evidence that people who have been involved in the development of specifically developed software applications have not performed the formal acceptance test of such software in a way to affect the test results.

NOTE: Software developers can be involved in the software acceptance test, but their contribution would be such to prevent them from surreptitiously making malfunctions go unnoticed.

A.10.2 Third party service delivery management

Long Term Preservation specific controls:

NOTE: The present clause does not specify methods to manage third parties, since the DPSP will choose what better fits its size and complexity. It is however reminded that the DPSP is responsible of the preservation service in its whole, including outsourced tasks.

A.10.2.1 Service delivery

Applicable. No further control and/or implementation guidance needed.

A.10.2.2 Monitoring and review of third party services

Long Term Preservation specific controls:

1) The DPSP shall formally appoint, as responsible for the third parties services, senior managers, supported by an adequate staff, who shall comply with provisions in the ISO/IEC 27002 [2] corresponding clause.

NOTE 1: The term "adequate" refers to both the number of people and their skill.

2) Where necessary the DPSP may resort to external experts to perform the tasks in the ISO/IEC 27002 [2] corresponding clause.

NOTE 2: One example is when the DPSP lacks the necessary skill to supervise the organisation to which it outsources its services.

NOTE 3: Since the responsibility for the outsourced services remains on the DPSP, this has to verify at least if the resorted experts perform their tasks with the due accuracy.

A.10.2.3 Managing changes to third party services

Long Term Preservation specific controls:

1) The agreement between the DPSP and the providers (outsourcers) of services related to its DPS shall specify that:

   a) the outsourcers shall timely inform the DPSP, except in cases of demonstrable urgency or emergency, of their plans to modify the systems they use to provide the services at issue;

   b) where the above mentioned cases of demonstrable urgency or emergency occur, the outsourcers shall immediately inform the DPSP of the applied changes and of the reason why no previous notice had been possible;

   c) the DPSP shall timely inform its outsourcers, except in cases of demonstrable urgency or emergency, of the need to apply changes to the outsourcers' systems used to provide the services at issue;

   d) all modifications applied and the decision to apply them shall be recorded in an auditable way under the responsibility of the DPSP Manager in charge of the system being modified; modifications applied in urgency or emergency shall also be recorded in an auditable way as soon as possible.

2) The timeliness indicated in the previous item 1) letters a) and c), shall be such to allow the respective counter parties to assess the planned changes and, possibly, agree on different solutions.

A.10.3 System planning and acceptance

A.10.3.1 Capacity management

Applicable. No further control and/or implementation guidance needed.

A.10.3.2 System acceptance

Long Term Preservation specific controls:

1) Connections between two or more computer systems, even in-house, shall only be established upon authorisation by the management in charge for Information Security. See also clause A.11.4.1, item 2).

2) The DPSP management in charge for Information Security shall publish, and regularly keep up to date, security requirements related to the DPSP servers, hosts, firewalls, and other multi-user computers configuration.

3) The configuration of each DPS related system shall be approved beforehand by the management in charge for Information Security that shall securely keep the related documentation to periodically verify if these configurations have been arbitrarily changed.

4) DPSP shall have for every software or hardware used an auditable and clearly understandable documentation evidencing the approval by the manager in charge in advance of its deployment, having had the agreement by the manager in charge for the Information Security.

5) The Manager's approval of specifically developed software should be based on a traced acceptance test in an auditable way (see also clause A.10.1.4, item 3).

6) The agreement between the DPSP and each outsourcer should require the latter to have in force a formal system acceptance procedure as in ISO/IEC 27002 [2] corresponding clause and as in the previous items 1) through 4).

7) Exceptions to the provision in the previous item 6) shall be duly and justified in an auditable way by the DPSP.

A.10.4 Protection against malicious and mobile code

A.10.4.1 Controls against malicious code

Long Term Preservation specific controls:

1) Whenever an DPS related system is suspected to be infected by a computer malware it shall immediately be shut down and disconnected from all networks; the department in charge for Information Security shall be notified and it shall immediately take care of the problem. No impromptu attempt to eradicate the malware shall be performed by unauthorised personnel. This procedure shall be traced in an auditable way.

2) All encrypted externally supplied computer readable files, with the exception of those that are to be stored encrypted, shall be decrypted and undergo an approved malware checking process before further processing. This procedure shall be auditable.

3) Before any file is restored to a production computer system from backup storage media, it shall be scanned with the latest version of the adopted antimalware software.

4) Malware detection and removal applications shall implement a frequent and possibly automated self-update.

A.10.4.2 Controls against mobile code

Applicable. No further control and/or implementation guidance needed.

A.10.5 Back-up

A.10.5.1 Information back-up

Long Term Preservation specific controls:

1) The DPSP shall ensure that at least some of the backup copies it regularly creates, updates and manages, are interoperable, by implementing them:

   a) on media that meet de jure or de facto standard specifications, or are agreed upon with the subscriber;

   b) using data architectures that meet de jure or de facto standard specifications.

NOTE: The purpose of this requirement is to ensure that, where the DPSP is based on proprietary media, data architecture, formats, etc., at least some backup copy can always be restored.

2) The DPSP shall ensure that the equipment (software and, where necessary, hardware) required to restore the backed up data object is available, at least for the time the related back up copy is kept, in a version suitable to restore such data object in a readable way.

3) In addition to all preserved data objects, any other asset necessary to ensure the Business Continuity, including software applications, operations documentation, etc. shall be backed up.

4) The back up copies storage locations shall be chosen consistently with the Business Continuity Plan (see clause A.14).

5) Back up copies shall be periodically checked to ascertain their readability. The interval between two subsequent checks should be defined based on the shorter period between what is indicated by the applicable legislation and by independent technical reports (provision as per clause 6.3.4, item 3), applies where applicable).

A.10.6 Network security management

A.10.6.1 Network controls

Applicable. No further control and/or implementation guidance needed.

A.10.6.2 Security of network services

Long Term Preservation specific control:

1) The DPS networks shall be separated from the Internet and from any network by firewalls, approved by the management in charge of Information Security, that shall run on separate dedicated computers that serve no other purpose.

2) All DPSP operated networks shall be provided at least with Intrusion Detection Systems approved by the management in charge of Information Security.

3) DPSP wireless networks shall be protected through encryption and suitable Authentication and Identification mechanisms.

A.10.7 Media handling

A.10.7.1 Management of removable media

New Long Term Preservation specific controls:

1) The DPSP shall have in force auditable procedures addressing at least the following issues regarding removable media:

   a) storage of media upon their delivery by their suppliers;

   b) storage of media upon their delivery by the DPSP customers;

   c) identification and authentication of the persons / roles authorised to withdraw and deposit media from and into the various storage sites;

   d) disposal of removable media and the related authorisation;

   e) secure deletion of media content, where applicable, when no more in use for the specific purpose, including specification of the deletion mechanisms to be used.

2) The DPSP shall have in force auditable procedures to be enforced before setting into operations new or reused removable media, aiming to prevent spurious data objects and malware to be injected in the preservation process.

3) The DPSP shall have in force auditable procedures providing for regular inspections on all media in use in order to verify their technical readability (see also clauses 6.3.3 and A.10.5.1, item 5)).

4) If the media manufacturer's specification or independent technical reports indicate for the adopted media a reliable lifetime shorter than the legally required inspection interval, the Risk Assessment should take into account these reports, in addition to the applicable legislation requirements, to define the interval between inspections. The results of these Risk Assessments, including the referred to technical reports, shall be made available to the Assessors.

5) Formal minutes of the above inspections on media readability shall be kept, at least for the time the inspected media are in use, under the responsibility of an officially appointed DPSP Manager, to provide a documented history of the inspections and of their outcomes.

6) If early signs of degradation are remarked and if the used media have no self-healing capability such as, for example, in the RAID based systems, an auditable data restore procedure shall be performed from back up copies onto new media. This ensures that no reading error is propagated.

NOTE: See also clause 6.3.4, item 2).

A.10.7.2 Disposal of media

Long Term Preservation specific controls:

1) To implement ISO/IEC 27002 [2] corresponding clause, item a), the DPSP shall adopt mechanisms suitable to render unreadable the media being disposed of, among which the following ones:

   a) Securely delete the media content, where applicable (i.e. magnetic media or re-writable optical media), by repeated overwriting, on the data to be deleted, as per the applicable standards or public available specifications.

   b) Incinerate the media.

   c) Destroy the media in multiple pieces; where the media pieces can be reassembled, pieces shall be disposed of separately.

2) When disposed of, all secret, confidential, or private information in hardcopy (e.g. on paper) shall be shredded or, preferably, incinerated.

3) The media disposal shall be implemented in compliance with specific DPSP auditable procedures.

A.10.7.3 Information handling procedures

Long Term Preservation specific control:

1) When implementing the ISO/IEC 27002 [2] corresponding clause, item a) on labelling media containing confidential data, e.g. sensitive or judicial personal data, the DPSP should ensure that the labels make no explicit reference to the data themselves nor to their owners ("subjects" in case of personal data), e.g. by resorting to coding mechanisms.

NOTE: The purpose of this requirement is to prevent unauthorised persons, who happen to handle these media, from deriving information on the contained confidential data from their labels.

A.10.7.4 Security of system documentation

Long Term Preservation specific controls:

1) System documentation security shall be dealt with according to the ISPD provisions (see clause A.5.1.1).

2) The DPSP shall have in force auditable procedures to manage the system documentation security, addressing, among other things:

   a) Assigning to each system documentation component the respective classification level.

   b) Specifying for each classification level the roles authorised to access the classified information.

   c) Reporting security incidents, such as system documentation theft, loss, disclosure to non authorised persons, etc.

   d) Action to be taken in the aftermath of a reported security incident.

A.10.8 Exchange of information

A.10.8.1 Information exchange policies and procedures

Long Term Preservation specific control:

1) With reference to the ISO/IEC 27002 [2] corresponding clause, item g), the DPSP shall encrypt the exchanged information using either legally required mechanisms or mechanisms agreed upon with the recipient or subscriber. (Refer also to clause A.12.3.1.)

A.10.8.2 Exchange agreements

Long Term Preservation specific control:

1) The ISO/IEC 27002 [2] corresponding clause 10.8.2, item h) shall be interpreted, in particular the words "immediately understood" in the light of what is specified at clause A.10.7.3, item 1).

A.10.8.3 Physical media in transit

Long Term Preservation specific controls:

1) [EXT1.1] Personal data preservation:

   Where the DPSP acts as Processor on mandate by one Controller, the ISO/IEC 27002 [2] corresponding clause, item a) shall include agreement with, or approval by, the Controller, since the latter is responsible for the data handling.

2) In addition to provisions in the ISO/IEC 27002 [2] corresponding clause, the DPSP shall have in force auditable procedures ensuring that confidential data objects shall be protected from unauthorised access, e.g. by means of encryption.

A.10.8.4 Electronic messaging

Long Term Preservation specific control:

1) Where available, REM [i.32] (Registered E-Mail) like solutions should be enforced and documented, since they ensure achievement of items a), b), c), d) of the ISO/IEC 27002 [2] corresponding clause.

A.10.8.5 Business information systems

Applicable. No further control and/or implementation guidance needed.

A.10.9 Electronic commerce services

Not Applicable.

A.10.10 Monitoring

A.10.10.1 Audit logging

Long Term Preservation specific controls:

1) The DPSP shall ensure that the DPS Computer systems securely create logs, that shall include all information specified in the corresponding ISO/IEC 27002 [2] clause, primarily all significant security relevant events.

2) The length of time the audit logs are to be kept shall be defined at least on the basis of legal requirements and of the agreement with the subscriber, whichever requires a longer period.

A.10.10.2 Monitoring system use

Applicable. No further control and/or implementation guidance needed.

A.10.10.3 Protection of log information

Long Term Preservation specific controls:

1) Provisions in the ISO/IEC 27002 [2] corresponding clause shall be implemented, where applicable resorting to cryptographic solutions.

2) The whole of system logs and application logs shall be replicated or backed up at least daily, to one or more machines that are not directly accessible from the Internet.

3) The DPSP shall keep logs (at least access logs) available for a period of time suitable to allow for exhaustive investigation when reviewing the DPSP security policy documentation and in case of security incidents. This period of time should in no case be less than one year.

A.10.10.4 Administrator and operator logs

Long Term Preservation specific control:

1) All DPSP officers working on the DPS, including sub-contractors and consultants, shall be notified in writing that all operations on the DPS are logged.

A.10.10.5 Fault logging

Applicable. No further control and/or implementation guidance needed.

A.10.10.6 Clock synchronization

Long Term Preservation specific controls:

1) The DPSP shall have in force an auditable procedure, based the outcomes of the Risk Assessment, ensuring that all the applied time references, in relation to the DPS, are reliably fetched from a trusted UTC time source and maintained unaltered throughout the entire DPS.

2) All DPSP time references shall be UTC based, e.g. "UTC+1, "UTC+2", etc., to make it possible to reconcile all of them to a consistent chronology.

3) The DPSP shall ensure that all logging records express the time in a unique manner, even when the DPSP systems are located in different time zones.

NOTE: This can be achieved either by synchronising all DPS related systems on the same time zone or by explicitly stating the systems time through UTC based notation (e.g. "UTC-6").

A.11 Access control

A.11.1 Business requirement for access control

A.11.1.1 Access control policy

Long Term Preservation specific controls:

1) The DPSP Access control policy shall take into account all DPS related procedures and facilities, even those governed by other departments insisting on the DPS functions, to ensure absence of conflict on requirements on confidentiality and on segregation of roles.

2) The DPSP access policy shall differentiate the access rights of the various user types. At least the following different user access rights classes shall be defined:

   a) DPS operators;

   b) DPS system administrators;

   c) data objects owners;

   d) Auditors;

   e) Third parties, e.g. authorities.

   Namely:

   i) DPS operators shall be enabled to perform operations on the DPS and shall not be able to set or modify the configuration of the DPS systems they operate on;

   ii) DPS system administrator shall have the authority to set or modify the DPS systems configurations, but shall not have the right to act as operators on the same systems the configurations of which they set or modify;

   iii) Auditors shall have "read only" rights on the DPS;

   iv) Data objects owners should only be able to access their own data objects in "read only" mode;

NOTE 1: All requests for changes to the preserved data objects would be submitted by the data objects owners through the agreed upon procedures.

   v) Third parties shall be able to only read the information they have the authorisation to.

EXAMPLE: A customs officer would not likely have the authorisation to access health records.

3) Unattended equipments shall not be installed in premises where their surveillance is hindered, if admittance to such premises is possible to persons who are not authorized to access these equipment functions.

NOTE 2: The purpose of this requirement is to prevent unauthorised access attempts to the DPS data to be performed unnoticed.

4) Installation and use on the DPS of any code that circumvents the authorized access control mechanisms in operating systems or access control packages should be forbidden.

5) The provision in the previous item 4) may be derogated in compliance with provisions in clause A.13.2.1, item 5).

6) The DPSP shall assess and identify accesses that need to be protected against duress.

NOTE 3: A duress protection can be implemented, for example, by providing users with "duress passwords" to be employed to covertly signal that this user is being pressured to logon.

A.11.2 User access management

A.11.2.1 User registration

Long Term Preservation specific controls:

1) The DPSP shall implement provisions in item a) of the ISO/IEC 27002 [2] corresponding clause at least referred to DPS operators and DPS system administrators.

2) The DPSP shall implement provisions in items d), e), f) g) and h) of the ISO/IEC 27002 [2] corresponding clause.

A.11.2.2 Privilege management

Applicable. No further control and/or implementation guidance needed.

A.11.2.3 User password management

Long Term Preservation specific controls:

NOTE 1: A user is anyone who is lawfully entitled to access the DPSP system (e.g. employees, third parties under contractual agreements, authorities, auditors, etc.).

1) DPS user authentication shall be designed to default to denial of privileges to end users in case of access control system malfunction. Specifically appointed System Administrators shall be designated to fix the malfunctioning user authentication system.

2) After a predefined number of unsuccessful logon attempts by one user, access to the system at issue shall be locked for that user, and, where applicable, shall be unlocked only by an authorised person. All this process shall be logged in an auditable way.

NOTE 2: By "system" it is intended any information processing hardware or software equipment: computer, network, processing application, smart card, etc.

3) Under each unsuccessful access attempt no information should be fed back that can help the user identify what data was wrong.

4) The DPSP Information Security management shall have unambiguous, organized, and current records of all access privileges.

5) Vendor supplied and application default passwords shall be changed after their first use.

6) The display and, where applicable, printing of passwords shall not be in clear.

7) Each password generated by systems to be securely conveyed to an end user, shall be unique; their generation should be based on random values, complying with de jure or de facto standard specifications

NOTE 3: Some random number generators are: ANSI X9.17 [i.33], NIST SP 800-90 [i.36].

8) All computer storage media and computer memory areas used in the construction, assignment, distribution, verification or encryption of passwords or PIN, should be securely deleted, preferably using mechanism based on de jure or de fact standard specifications.

NOTE 4: Deviations to the previous provision are possible only where passwords and/or PINs are of "one time" type, or when the centrally generated password or PIN is to be changed by the user after its first usage and the involved application provides reset measures in case of undue intrusion, etc.

9) Users shall accept an obligation that they shall immediately change their passwords, whenever there is the certainty, or even a reasonable doubt, that they have been compromised, and that they shall immediately report the incident.

10) When contact centres are deployed as an emergency interface between users and applications the contact centre employee shall have not the possibility to abuse the users' password/PIN.

A.11.2.4 Review of user access rights

Long Term Preservation specific controls:

1) In addition to provisions in items a), b), c) of the ISO/IEC 27002 [2] corresponding clause, the DPSP shall review users' access rights whenever a security incident occurs that can be referred to access abuse or access control malfunction.

2) Access rights shall be revoked if not used for a predefined time period that will depend on the confidentiality of the information accessed by the users.

3) The time period addressed in item a) of the ISO/IEC 27002 [2] corresponding clause shall in no case be shorter than what is required by the applicable legislation.

A.11.3 User responsibilities

A.11.3.1 Password use

Long Term Preservation specific controls:

1) In addition to provisions in item d) of the ISO/IEC 27002 [2] corresponding clause, the DPSP should set:

   a) automated password validity checks when the users create their own passwords to verify that user built passwords are not identical or substantially similar to previous passwords used for the same application, system or network and that the user chosen passwords meet precise security requirements;

NOTE 1: Examples of these security requirements are: minimum length, used character types, character repetition, being substantially different from the previous ones, etc.

   b) automated password change request when a predefined time lapse has expired or is about to expire.

2) Where required (refer to clause A.10.1.3), the minimum password or PIN length shall be such to make it possible to divide it in two or more parts to be assigned each to a different operator suitably to prevent the reconstruction of the complete password/PIN from one single part.

3) Users shall be made aware of the rules as in the previous items of this clause.

4) Users shall accept in writing that they shall not use the same password on multiple computer systems unless authorised by the relevant manager.

NOTE 2: This provision aims to prevent that the disclosure of one user's password related to one system also affects the security of other systems.

A.11.3.2 Unattended user equipment

Applicable. No further control and/or implementation guidance needed.

A.11.3.3 Clear desk and clear screen policy

Long Term Preservation specific controls:

1) The DPSP shall enforce an auditable clear desk and clear screen policy by means of regular and impromptu inspections performed by the responsible managers and/or by specific officers. The outcome of these inspections shall be reported at least up to the Information Security managers.

2) The DPSP Employees shall be made aware that they will incur in disciplinary sanctions in case of violation of the clear desk and clear screen policy.

A.11.4 Network access control

A.11.4.1 Policy on use of network services

Long Term Preservation specific controls:

1) Within the provision b) of the ISO/IEC 27002 [2] corresponding clause the DPSP shall appoint a very small number of trustable officers, sufficient to ensure the operations continuity in case of disaster, authorised to access the DPSP network services used to create and maintain backup copies of the preserved data objects (see also clause A.14.1.4).

2) Access by any DPS computer to any network shall be explicitly approved in an auditable way by the relevant manager.

3) Connections of DPSP networks to any other computer or network shall be explicitly authorised in an auditable way by the relevant manager.

4) The DPSP networks shall always be protected by firewalls, Intrusion Detection Systems, etc., unless explicitly and authorised in an auditable way by the DPSP relevant management.

A.11.4.2 User authentication for external connections

Long Term Preservation specific controls:

1) When user authentication to networks and network connected equipment is password based, they shall abide by provisions in clause A.11.3.1.

2) User authentication to networks and network connected equipment should be implemented by means of two-factor authentication mechanisms, or similarly reliable mechanisms, at least when sensitive information are dealt with.

3) Any connection conveying authentication information shall be protected as specified in clause A.10.6.1.

A.11.4.3 Equipment identification in networks

Long Term Preservation specific control:

1) Provisions in the ISO/IEC 27002 [2] corresponding clause apply in particular to DPSP equipments that automatically connect to networks to create channels along which backup copies are transmitted to remote locations, as in the case of mirroring mechanisms. These channels shall be encrypted.

A.11.4.4 Remote diagnostic and configuration port protection

Applicable. No further control and/or implementation guidance needed.

A.11.4.5 Segregation in networks

Long Term Preservation specific control:

1) The DPSP shall evaluate if the DPS related networks are to be segregated from other networks, on the basis of the preserved data objects confidentiality level. If the DPSP decision is not to segregate, such decision shall be clearly and recorded in an auditable way.

A.11.4.6 Network connection control

Applicable. No further control and/or implementation guidance needed.

A.11.4.7 Network routing control

Applicable. No further control and/or implementation guidance needed.

A.11.5 Operating system access control

A.11.5.1 Secure log-on procedures

Long Term Preservation specific control:

1) After a predefined number of unsuccessful logon attempts by one user, the same security measures shall be implemented as in clause A.11.2.3, item 2).

A.11.5.2 User identification and authentication

Applicable. No further control and/or implementation guidance needed.

A.11.5.3 Password management system

Long Term Preservation specific control:

1) Passwords shall not be hard coded into software specifically developed or modified for the DPSP.

A.11.5.4 Use of system utilities

Long Term Preservation specific controls:

1) Access to systems software utilities shall be restricted to a small number of trusted and authorized users.

2) Systems software utilities execution shall be auditable.

A.11.5.5 Session time-out

Long Term Preservation specific control:

See also clause A.11.3.2.

1) The DPSP shall assess in what cases "clearing the screen and preventing unauthorized access" after a defined period of inactivity is deemed as not enough secure, thus requiring enforcement of the requirement "close both application and network sessions", as in the ISO/IEC 27002 [2] corresponding clause.

A.11.5.6 Limitation of connection time

Long Term Preservation specific controls.

NOTE: The provisions in the ISO/IEC 27002 [2] corresponding clause can be applicable if the DPSP customers submit the data objects to be preserved via connections on open network (i.e. the internet) triggered from their own premises over which the DPSP has no direct control, however suitable obligations on the customers can relax the related measures.

A.11.6 Application and information access control

A.11.6.1 Information access restriction

Long Term Preservation specific controls:

1) Access to systems logs or application audit trails shall be limited to the personnel with an actual need to know.

NOTE 1: It is sufficient that dedication and separation are achieved logically.

2) User privileges shall be carefully defined so that users can only gain access to preserved data objects for which they have an actual need to know.

3) Administrators of one system should not gain access to the data objects preserved in the same system. One acceptable derogation to this requirement may be a system administrator's intervention to remove malfunctions locking some preserved data objects, but in this case the system administrator's operations shall be supervised by the operator responsible for the data objects at issue, to prevent abuse on such data objects.

NOTE 2: Particular care is to be placed in assigning the rights as in item b) of the ISO/IEC 27002 [2] corresponding clause ("read, write, delete, and execute"), since the operation of deleting preserved data objects is to be performed by responsible officers.

A.11.6.2 Sensitive system isolation

Long Term Preservation specific control:

1) The DPS components should be dedicated to this application and isolated from other environments.

A.11.7 Mobile computing and teleworking

A.11.7.1 Mobile computing and communications

Long Term Preservation specific control:

1) The DPSP should not allow for mobile devices to be used in connection with its DPS.

NOTE: The DPSP activity does not usually require operations on the DPS to be performed from mobile devices.

A.11.7.2 Teleworking

Long Term Preservation specific control:

1) The DPSP should not allow for teleworking to be used on its DPS processing systems. If, for very peculiar reasons, it is implemented, the security measures specified in the ISO/IEC 27002 [2] corresponding clause shall all be enacted.

NOTE: The DPSP activity does not usually require operations on the DPS to be performed in teleworking, with the exception of security tests, like penetration tests on its networks, and the related audit activities.

A.12 Information systems acquisition, development and maintenance

A.12.1 Security requirements of information systems

A.12.1.1 Security requirements analysis and specification

Long Term Preservation specific controls:

1) When an DPSP sets in operation a Commercial Off The Shelf (COTS) or a specifically developed DPS component, the technical specifications implemented by the purchased or developed system must include requirements for security controls, specifying which controls can be performed automatically and incorporated in the information system.

2) When DPS software packages or systems are not independently evaluated or certified, they shall go through a formal acceptance test, as part of the development or acquisition processes, to grant fulfilment of the security requirements.

A.12.2 Correct processing in applications

A.12.2.1 Input data validation

Long Term Preservation specific controls:

1) The DPSP applications implementing the preservation service shall track in an auditable way all data objects submitted and shall associate each of them to a meaningful state (e.g. accepted, rejected, in process, preserved).

2) The DPSP shall implement auditable controls to prevent personnel from, unintentionally or without due authorisation, adding, modifying and deleting files or information.

3) When the data object to be preserved is electronically transmitted by the depositor to the DPSP, mechanisms shall be enforced in an auditable way to verify that the data object has been received without any alteration. These mechanisms shall be specified in the agreement with the subscriber.

NOTE: For EXTENDED controls see clause 6.3.5.

4) [EXT1] - Input data object signature verification:

   - The DPSP shall verify at the time of submission (or at any other time specified in the agreement in force), the validity of any AdES applied to the data object submitted for preservation. The agreement with the subscriber should stipulate if data objects, that the DPSP reports to the subscriber as faulty, are not to be preserved as delivered by the subscriber.

A.12.2.2 Control of internal processing

Long Term Preservation specific controls:

1) The DPSP shall identify which officers have the authorisation to add, modify, and delete data objects for each subscriber and, possibly, for each data object type.

2) The DPSP shall implement auditable procedures to verify the integrity of each processed data object throughout the entire preservation process.

NOTE: This can be achieved, for example, by comparing, at least at each key process step up to the final storage on the preservation media, the data object digest with the one computed as soon as the data object was received and by eventually implementing the Closure Evidence.

3) The DPSP shall verify and report in an auditable way, at least at each key process step, that no data object has been dropped by the process step.

A.12.2.3 Message integrity

Applicable. No further control and/or implementation guidance needed.

A.12.2.4 Output data validation

Applicable. No further control and/or implementation guidance needed.

A.12.3 Cryptographic controls

A.12.3.1 Policy on the use of cryptographic controls

Long Term Preservation specific controls:

1) The DPSP should make use of cryptographic algorithms generally recognised by de jure or de facto technical standards as suitable to withstand attacks at least for the period of time the preserved data object is required to be kept, where feasible.

NOTE 1: Some of the mentioned de jure or de facto technical standards are TS 102 176 [i.34] and FIPS 197 [i.21].

2) The DPSP should monitor cryptographic advances and, as soon as such advances provide evidence that this is necessary, update the algorithms and / or methods it makes use of.

NOTE 2: Apart from cryptographic mechanisms, other ones e.g. legal, organizational methods, can also be used for proving that a certain data object existed at a certain point of time.

3) Exceptions to the previous items may depend on:

   a) adoption of organisational measures (e.g. preservation by trusted entities like public officers) that ensure security even beyond the presumed cryptography resilience threshold;

   b) legal provisions requiring specific cryptographic solutions.

4) [EXT1] - Preserving encrypted data objects, by force of legal or service agreement.

   - When the preserved data objects are encrypted:

      a) [EXT1.1] The DPSP shall have in place suitable controls to verify that no data object related data is preserved in clear, other than the agreed metadata required, e.g. for information retrieval.

      b) [EXT1.2] The DPSP shall ensure the possibility to decrypt the encrypted data object upon request by an authorised entity, e.g. the data object owner, a Public Authority, etc. Dual control should be enforced by technical or organisational means.

      c) [EXT1.3] In case of encryption key compromise and/or unavailability refer to clause A.12.3.2, item 5).

A.12.3.2 Key management

Long Term Preservation specific controls:

1) Any DPSP key management activity shall be logged in an auditable way.

2) Where encryption algorithms are used the DPSP shall have in place auditable emergency procedures suitable to ensure the key recovery in case of loss or corruption of the key or unavailability of the personnel appointed to perform the ordinary procedures. Invocation of the emergency procedure shall be up to the relevant manager. Dual control should be enforced by technical or organisational means.

3) In case of derogation from the above provision an exhaustive description of why it was violated shall be reported to the relevant manager.

4) Where encryption algorithms are used, in case of compromise, or in case of reasonable doubt of compromise, of the decryption key, or in case the encryption algorithm is known as broken or seriously weakened, emergency and auditable procedures shall be invoked by the relevant manager to encrypt the affected data object with a different key or algorithm. Dual control should be enforced in an auditable way by technical or organisational means.

5) In case of derogation from the above provision an exhaustive description of why it was violated shall be reported to the relevant manager.

A.12.4 Security of system files

A.12.4.1 Control of operational software

Long Term Preservation specific controls:

1) The DPSP shall put in operation new and updated applications and operating system software only upon sign-off by the relevant management that formally approves the outcomes of extensive acceptance tests performed in an auditable way evidencing that the testing was successful.

2) Compilers or development tools shall not be permanently installed in the DPSP production environment, i.e. only executable code shall be permanently installed in this environment.

3) Before installing any application a roll back procedure should be available.

A.12.4.2 Protection of system test data

Long Term Preservation specific control:

1) Provisions in the ISO/IEC 27002 [2] corresponding clause, items b) and c) may be softened to allow the DPSP to keep operational information copied in the testing environment if anonymized.

A.12.4.3 Access control to program source code

Applicable. No further control and/or implementation guidance needed.

A.12.5 Security in development and support processes

A.12.5.1 Change control procedures

Long Term Preservation specific control:

1) The DPSP shall test all system changes, prior to putting them into operation, in a segregated test environment, that should not be used for development purposes. See also clause A.12.4.1, item 1). Any deviation to this segregation shall be accompanied by measures ensuring that activities performed in the development environment shall not modify the predefined test base in a permanent way.

A.12.5.2 Technical review of applications after operating system changes

Long Term Preservation specific control:

1) The DPSP should make use of operating systems that permit unwanted or unneeded functionality to be completely removed (hardening). Where applicable the "hardening" should be performed after every significant operating system update.

A.12.5.3 Restrictions on changes to software packages

Long Term Preservation specific control:

1) The DPSP shall bind by agreement every third-party supplying software packages to deliver them free of mechanisms that could be triggered by the supplier or by the software application itself without the DPSP consent.

A.12.5.4 Information leakage

Applicable. No further control and/or implementation guidance needed.

A.12.5.5 Outsourced software development

Long Term Preservation specific control:

NOTE: Provisions at clause A.12.4.1, item 1) also apply.

A.12.6 Technical Vulnerability Management

A.12.6.1 Control of technical vulnerabilities

Long Term Preservation specific control:

1) Members of the DPSP teams specified in clause A.5.1.2, item 1) shall keep them up to date with news on security, related not only to the core DPS applications, but also to the ancillary services.

A.13 Information security incident management

A.13.1 Reporting Information Security Events and Weaknesses

A.13.1.1 Reporting information security events

Long Term Preservation specific controls:

1) The DPSP shall draft and timely keep up to date clearly understandable instructions on how to report any information security related event the soonest possible upon detection. This information shall be made available to the authorised persons and may be available to them also online to make them able to access it anytime anywhere. Parts of this information that are deemed sensitive for the DPSP security shall be consistently classified and the online access to these parts shall be only allowed upon authentication.

2) The DPSP shall have an auditable procedure indicating how to classify the incidents severity.

3) All officers operating on the DPS shall be formally made aware of their responsibility, and of the existence of sanctions in case of default, to report without undue delay any information security related event, conflicting with the Security Policy in force, in compliance with the applicable instructions as in the previous items 1) and 2).

4) All officers operating on the DPS shall declare in writing that they have received the instructions as in the previous item 3). Where applicable, it shall be specified which parts of such instructions are confidential.

5) Disclosures to non authorised persons and entities on information security related events shall not be released unless upon formal authorisation by the DPSP management.

6) Where DPSP sub-contractors are involved, the instructions as in the previous item 1) shall be delivered to each sub-contractor's official representative, who in turn shall deliver them to the sub-contractor's employees who operate on the DPS related activities who shall accept them in writing.

A.13.1.2 Reporting security weaknesses

Long Term Preservation specific controls:

1) The DPSP shall draft and timely keep up to date clearly understandable instructions on how to report any security weakness the soonest possible upon detection. This information shall be made available to the authorised persons by any means (e.g. on paper, electronically, etc.). Parts of this information that are deemed sensitive for the DPSP security shall be classified consistently and access online to these parts shall be allowed upon authentication.

2) The DPSP shall specify how to classify the security weaknesses severity.

3) All officers operating on the DPS shall be formally made aware of their responsibility and of the existence of sanctions in case of default, to report without undue delay any security weakness, conflicting with the Security Policy in force, in compliance with the applicable instructions as in the previous items 1) and 2).

4) All officers operating on the DPS shall declare in writing that they have received the instructions as in the previous item 3). Where applicable, it shall be specified which parts of such instructions are confidential.

5) Disclosures to non authorised persons and entities on security weakness events shall not be released unless upon formal authorisation by the DPSP management.

6) Where DPSP sub-contractors are involved, the instructions as in the previous item 1) shall be delivered by the relevant DPSP manager to each sub-contractor's formal representative, who in turn shall deliver them to each employee, operating on the DPS related activities, who shall accept them in writing.

A.13.2 Management of Information Security Incidents and Improvements

A.13.2.1 Responsibilities and procedures

Long Term Preservation specific controls:

1) The DPSP shall have in force auditable procedures ensuring that, upon reporting on security incidents and/or security weaknesses, a response team will take over the management of the incident and/or weakness with timeliness consistent with the incident/weakness severity level (see clauses A.13.1.1, item 2) and A.13.1.2, item 2)).

2) All involved DPSP personnel and sub-contractors shall be formally made aware of the existence and purpose of the team as in the previous item 1). Where sub-contractors are involved, this information shall be formally delivered to each sub-contractor's formal representative, who in turn shall deliver it to each employee who operates on the DPS related activities who shall accept it in writing.

3) The DPSP shall appoint in writing the persons responsible to handle the reported security incidents and weaknesses. The DPSP shall provide the appointed persons with detailed instructions on how to handle the reported security incidents and weaknesses (see clauses A.13.1.1 and A.13.1.2), consistently with provisions in ISO/IEC 27002 [2] corresponding clause, and on the possible related sanctions. All involved persons, DPSP employees, sub-contractors employees and third parties, shall be made aware of who is in charge of these responsibilities. Officers and subcontractors shall exchange information on the security related events only with members of the response team, unless otherwise authorised by the relevant management.

4) DPSP employees in charge of managing reported incidents and weaknesses shall accept in writing the notification of their responsibility.

5) Actions taken in emergency cases suitable to affect the DPS security level shall be enacted under strict control of a duly authorised manager who shall be responsible for restoring the DPS to its pristine status after the emergency phase has been overcome. All phases related to the emergency shall be recorded in an auditable way, specifying also the time each single record refers to, under the responsibility of the said manager. In particular:

   a) the emergency state shall exhaustively be described;

   b) all actions performed during the entire emergency phase shall be recorded;

   c) the conditions under which the emergency was deemed as closed shall be described;

   d) the time of restoring to the DPS pristine status shall be recorded.

A.13.2.2 Learning from information security incidents

Long Term Preservation specific controls:

1) The records of all detected security incidents and weaknesses shall report information suitable to be taken in consideration in the next Risk Assessment and Information Security Policy Document review sessions, to be performed according to the planned schedule or extemporaneously depending on the events severity.

2) The DPSP shall specify upon the occurrence of what severity level of incident or security weakness a review of the Risk Assessment and/or the ISPD shall be performed extemporaneously.

A.13.2.3 Collection of evidence

Applicable. No further control and/or implementation guidance needed.

A.14 Business continuity management

A.14.1 Information security aspects of business continuity management

A.14.1.1 Including information security in the business continuity management process

Long Term Preservation specific control:

1) Depending on the DPSP services, the Business Continuity Plan shall be designed to make the DPSP capable to resume its activities without generating unacceptable delay, mainly to its trading partners and relevant Authorities, in abidance by the agreements in force and the applicable legislation requirements, yet meeting the security requirements.

NOTE 1: Refer also to clause A.7.1.1, item 5).

NOTE 2: In order to ensure timely operation resumption the BCP can deliberately not envisage resuming some lower criticality operations.

NOTE 3: A reference to drafting the BCP can be the BS 25999-1 [i.1].

A.14.1.2 Business continuity and risk assessment

Long Term Preservation specific controls:

1) Identification of and protection from risks affecting the personnel safety shall have the highest priority.

2) Each Risk Assessment Session shall include a service discontinuity Impact Analysis on the DPS components. The Business Continuity Plan shall be designed and reviewed based on the outcomes of this Impact Analysis according to commonly accepted specifications, such as de *iure* or *de facto* standards.

NOTE 1: A possible reference to drafting the BCP can be the BS 25999-1 [i.1].

3) The DPS components should be assigned a scale of criticality level.

NOTE 2: One possible scale can be the following: highly critical, critical, priority, required, deferrable.

4) The maximum down-time shall be defined for at least the key DPSP services and processes, among which:

   a) data object acquisition;

   b) data preservation process;

   c) data object exhibition.

5) The business continuity strategy shall have among its goals ensuring that the maximum down-time identified in the previous item 4) is not exceeded.

A.14.1.3 Developing and implementing continuity plans including information security

Long Term Preservation specific control:

1) The "identification of the acceptable loss of information and services" (letter b) of the ISO/IEC 27002 [2], clause of reference) shall be performed against all types of handled information, including DPSP internal documentation.

A.14.1.4 Business continuity planning framework

Long Term Preservation specific controls:

1) The DPSP BCP shall specify which officers and in which cases shall invoke the DPS related BCP, in part or in its whole.

2) The BCP shall ensure that a team of properly skilled operators ("Disaster Recovery Team") is regularly available in order to resume the operations at the disaster recovery, or back up, site with a timing that matches the timeliness identified in clause A.14.1.2, in particular at item 4).

3) When members of the Disaster Recovery Team are employees of external service providers, an arrangement with these service providers shall be in force binding them to comply with the applicable BCP provisions, including provisions in the previous item 2).

4) The disaster recovery / back up - site must be under the control:

   - [CHOICE]

     a) of the DPSP itself;

     b) of a Service Provider whose reliability is regularly either directly ascertained by the DPSP or assessed as reliable by a trusted third party.

5) The DPSP shall oblige external organisations that provide services to the DPSP BCP -through an agreement that contain also adequate sanctions- to meet the BCP requirements, including provisions in the previous items.

A.14.1.5 Testing, maintaining and re-assessing business continuity plans

Long Term Preservation specific controls:

1) The DPSP shall plan for regular test sessions at least of the following items of ISO/IEC 27002 [2], clause 14.1.5:

   "c) technical recovery testing (ensuring information systems can be restored effectively);

   d) testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site);

   e) tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment);

   f) complete rehearsals (testing that the organization, personnel, equipment, facilities, and processes can cope with interruptions)".

2) The BCP complete rehearsal (see item f) of the ISO/IEC 27002 [2], clause 14.1.5) shall be performed at least within a short time after the DPS BCP is first set up, every time it is significantly changed and when established in the Security Policy/BCP.

3) The DPSP shall oblige through agreement its Service Providers to participate to the BCP complete or partial tests and rehearsals.

4) The DPSP shall oblige through agreement its Service Providers (see also clause A.10.2.3):

   a) to timely communicate to the DPSP any significant modification to their systems involved in the BCP that might affect the recovery, and

   b) to implement such modifications only upon formal acceptance by the DPSP, with the exception of emergency cases that shall be properly documented by the Service Providers.

5) The DPSP shall perform at least yearly inspections on its service providers' locations to ascertain that their systems that provide BCP related services to the DPSP have not been changed without the DPSP being notified or that emergency modifications have a sound explanation.

A.15 Compliance

A.15.1 Compliance with legal requirements

A.15.1.1 Identification of applicable legislation

Long Term Preservation specific control:

1) The DPSP shall also satisfy provisions in ISO 15489 [i.17], part 1, chapter 5.

NOTE: It is to be remarked that items c) ("voluntary codes of best practice") and d) ("voluntary codes of conduct and ethics") of this ISO 15489 [i.17], chapter 5 perfectly match Directive 2006/123/EC [i.25], article 26 (item 1), letter b): "drawing up their own quality charter or participation in quality charters or labels drawn up by professional bodies at Community level".

A.15.1.2 Intellectual property rights (IPR)

Long Term Preservation specific controls:

1) All DPSP licensed hardware and software products in use at the DPSP's shall be registered before being activated.

2) If the owner of IPR on a specific software waivers its own rights, documentation of this waiver shall be kept along with the evidence of ownership of licenses.

A.15.1.3 Protection of organizational records

New Long Term Preservation specific control:

1) The DPSP should comply with relevant provisions set by ISO 15489 [i.17], for example in chapter 7 "Records Management Requirements".

A.15.1.4 Data protection and privacy of personal information

Applicable. No further control and/or implementation guidance needed.

A.15.1.5 Prevention of misuse of information processing facilities

Applicable. No further control and/or implementation guidance needed.

A.15.1.6 Regulation of cryptographic controls

Applicable. No further control and/or implementation guidance needed.

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

A.15.2.1 Compliance with security policies and standards

Long Term Preservation specific controls:

1) The DPSP shall have in force an auditable procedure requiring all managers, at any level, to perform, preferably in an unscheduled way, reviews on their respective departments to ascertain compliance with the rules.

2) The DPSP shall make known to all persons working on, and/or for, the DPS, the consequences of non compliance.

A.15.2.2 Technical compliance checking

Long Term Preservation specific control:

1) The DPSP shall regularly implement checks for compliance with security implementation standards as per the ISO/IEC 27002 [2] corresponding clause.

2) If the DPSP resorts to external providers it shall state in the agreement with the providers the mutual obligations and responsibility as well as the scope of the testing (e.g. penetration tests or vulnerability assessments).

3) The DPSP should adopt a methodology suitable to assure a periodical review and assessment of the operations.

A.15.3 Information System Audit Consideration

A.15.3.1 Information systems audit controls

Applicable. No further control and/or implementation guidance needed.

A.15.3.2 Protection of information systems audit tools

Long Term Preservation specific control:

1) The DPSP shall have auditable security procedures to ensure that software and hardware tools used by internal and, where applicable, external auditors are protected from unauthorised access and usage and that they are removed from the DPS when not used in assessment sessions.

Annex B (informative): Statement of Applicability Framework

An DPSP, as specified in clause 4.3 will draft a Statement of Applicability where it will specify the provisions specified in the present document that it will abide by and those that are not applicable. In this later case, the exclusion will be justified and documented in writing.

SAMPLE

Data Preservation Service Provider XXXX: Statement of Applicability Date: DD/MM/YYYY

Provisions in "ETSI TS [the present document] including annex A"

Clause #	Control (Item Number)	Type of provision (mandatory, optional, recommended)	Applicable/Not applicable	Rationale (when not applicable)

Provisions in "Other PAS"

PAS: XXX

Clause #	Control (Item Number)	Rationale for inclusion		Notes
		(LR, CO, RA (see note)	Reference	
n..n	Item x) Nth bullet			
NOTE: LR: Legal Requirement, CO: Contractual Obligation, RA: Risk Assessment outcome.				

Annex C (informative): Bibliography

- 00323/07/EN - WP 131 (Article 29): "Data Protection Working Party - Working Document on the processing of personal data relating to health in electronic health records (EHR)".
- 00323/07/EN - WP 131 (clause 8 - third item).
- ISO/IEC 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security".
- BS 25999-2:2007: "Business continuity management - Part 2: Specification".

Annex D (informative): Change history

From version 1.2.2 to 1.3.1

1) Clause 5.2.7 text "i.e. also to not fiscally relevant ones,"was removed, since the present document applies to all data object types and it is not necessary to hint to fiscal ones.

2) Clause 6.5 Note 1: removed, since the corresponding clause of TS 102 573 has been broadened to encompass all analog type data objects

3) Clause A.6.1.1 item 1): modified text as follows: "The DPSP shall keep exhaustive and auditable documentation, even historical, on its own organisation."

4) Clause A.7.2.1 Note: modified text as follows: "NOTE: If this condition occurs in relation of personal data, the DPSP will not be held responsible for non law-abiding preservation of the data object deposited by the data object owner, unless the DPSP is also acting as the Controller."

5) Clause A.10.1.1 item 1.a): modified text as follows: " …(e.g. based on fiscal or legal requirements, where applicable) …" to broaden the specification scope.

6) Clause A.10.7.3 item 1): Removed "[EXT.1] Persona Data Preservation:" since this item is generally applicable.

History

Document history		
V1.1.1	May 2011	Publication
V1.2.1	December 2011	Publication
V1.3.1	April 2012	Publication