



**Electronic Signatures and Infrastructures (ESI);
Data Preservation Systems Security;
Part 2: Guidelines for Assessors**

Reference

RTR/ESI-00120-2

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

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

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

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2011.
All rights reserved.

DECT™, PLUGTESTS™, UMTS™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and LTE™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	8
Foreword.....	8
Acknowledgment.....	8
Introduction	8
1 Scope	9
2 References	9
2.1 Normative references	9
2.2 Informative references.....	9
3 Definitions and abbreviations.....	10
3.1 Definitions	10
3.2 Abbreviations	10
4 Overview	10
4.1 Preservation Service types.....	11
5 Provisions based on TS 102 573	11
5.1 Compliance with the TS 101 533-1	11
5.2 DPSP Obligations specified in TS 102 573, clause 6.....	11
5.2.1 Arrangements to cover liabilities and financial stability.....	11
5.2.2 Conformance by Subcontractors.....	11
5.2.3 DPSP service provisions in abidance by the applicable legislation	12
5.2.4 Contractual aspects	12
5.2.5 Resolution of complaints and disputes.....	12
5.2.6 Organisation independence.....	13
5.2.7 DPSP Subscriber Obligations	13
5.2.8 Information for trading partners.....	13
5.2.9 Information for auditor/regulatory/tax authorities	13
6 Objectives and controls in TS 102 573, annex A.....	13
6.1 SS.1. Signature	13
6.1.1 SS.1.1. Class of Electronic Signature	13
6.1.2 SS.1.2. Certification.....	14
6.1.3 SS.1.3. Signature Creation Data	14
6.1.4 SS.1.4. Certificate Subject's Registration	14
6.1.5 SS.1.5. Certificate Revocation	14
6.2 SS.2. Maintenance of Signature over Storage Period.....	14
6.3 SS.3. Storage	15
6.3.1 SS.3.1. Authorized Access.....	15
6.3.2 SS.3.2. Authenticity and Integrity.....	15
6.3.3 SS.3.3. Data Object Readability	15
6.3.4 SS.3.4. Storage media type	16
6.3.5 SS.3.5. Data Objects Format.....	16
6.3.6 SS.3.6. Requirements on Separation and Confidentiality	16
6.4 SS.4. Reporting to and Exchanges with Authorities.....	16
6.5 SS.5. Conversion of Analog Originals to Digital Formats	16
Annex A: ISO/IEC 27001 related Long Term Preservation-specific ISMS guidelines for control assessment.....	17
A.1 Reference to ISO/IEC 27001	17
A.2 Basic ISO/IEC 27002 provision.....	17
A.3 Enhanced ISO/IEC 27002 provisions.....	17
A.4 New specific controls	17

A.5	Security Policy	17
A.5.1	Information security policy	17
A.5.1.1	Information security policy document	17
A.5.1.2	Review of the information security policy	17
A.6	Organization of information security	18
A.6.1	Internal organization.....	18
A.6.1.1	Management commitment to information security	18
A.6.1.2	Information security co-ordination	18
A.6.1.3	Allocation of information security responsibilities.....	18
A.6.1.4	Authorization process for information processing facilities	18
A.6.1.5	Confidentiality agreements	18
A.6.1.6	Contact with authorities	18
A.6.1.7	Contact with special interest groups	18
A.6.1.8	Independent review of information security	18
A.6.2	External Parties	19
A.6.2.1	Identification of risks related to external parties.....	19
A.6.2.2	Addressing security when dealing with customers	19
A.6.2.3	Addressing security in third party agreements.....	19
A.7	Asset Management	19
A.7.1	Responsibility for assets	19
A.7.1.1	Inventory of assets	19
A.7.1.2	Ownership of assets	20
A.7.1.3	Acceptable use of assets	20
A.7.2	Information classification.....	20
A.7.2.1	Classification guidelines	20
A.7.2.2	Information labelling and handling.....	20
A.8	Human resources security	20
A.8.1	Prior to Employment	20
A.8.1.1	Roles and responsibilities	20
A.8.1.2	Screening	20
A.8.1.3	Terms and conditions of employment.....	20
A.8.2	During Employment.....	21
A.8.2.1	Management responsibilities	21
A.8.2.2	Information security awareness, education, and training.....	21
A.8.2.3	Disciplinary process.....	21
A.8.3	Termination or Change of Employment.....	21
A.8.3.1	Termination responsibilities.....	21
A.8.3.2	Return of assets	21
A.8.3.3	Removal of access rights	21
A.9	Physical and environmental security	21
A.9.1	Secure Areas.....	21
A.9.1.1	Physical security perimeter	21
A.9.1.2	Physical entry controls.....	21
A.9.1.3	Securing offices, rooms, and facilities	22
A.9.1.4	Protecting against external and environmental threats.....	22
A.9.1.5	Working in secure areas.....	22
A.9.1.6	Public access, delivery, and loading areas	22
A.9.2	Equipment Security	22
A.9.2.1	Equipment siting and protection	22
A.9.2.2	Supporting utilities.....	22
A.9.2.3	Cabling security	22
A.9.2.4	Equipment maintenance.....	22
A.9.2.5	Security of equipment off-premises.....	22
A.9.2.6	Secure disposal or re-use of equipment	22
A.9.2.7	Removal of property	22
A.10	Communications and operations management.....	23
A.10.1	Operational procedures and responsibilities.....	23
A.10.1.1	Documented operating procedures	23

A.10.1.2	Change management.....	23
A.10.1.3	Segregation of duties	23
A.10.1.4	Separation of development, test, and operational facilities.....	23
A.10.2	Third party service delivery management	23
A.10.2.1	Service delivery	23
A.10.2.2	Monitoring and review of third party services.....	23
A.10.2.3	Managing changes to third party services.....	24
A.10.3	System planning and acceptance.....	24
A.10.3.1	Capacity management.....	24
A.10.3.2	System acceptance	24
A.10.4	Protection against malicious and mobile code.....	24
A.10.4.1	Controls against malicious code	24
A.10.4.2	Controls against mobile code.....	24
A.10.5	Back-up	24
A.10.5.1	Information back-up	24
A.10.6	Network security management	24
A.10.6.1	Network controls	24
A.10.6.2	Security of network services.....	25
A.10.7	Media handling.....	25
A.10.7.1	Management of removable media.....	25
A.10.7.2	Disposal of media	25
A.10.7.3	Information handling procedures	25
A.10.7.4	Security of system documentation.....	25
A.10.8	Exchange of information	25
A.10.8.1	Information exchange policies and procedures.....	25
A.10.8.2	Exchange agreements	25
A.10.8.3	Physical media in transit.....	25
A.10.8.4	Electronic messaging	26
A.10.8.5	Business information systems.....	26
A.10.9	Electronic commerce services	26
A.10.10	Monitoring.....	26
A.10.10.1	Audit logging.....	26
A.10.10.2	Monitoring system use.....	26
A.10.10.3	Protection of log information.....	26
A.10.10.4	Administrator and operator logs	26
A.10.10.5	Fault logging.....	26
A.10.10.6	Clock synchronization	26
A.11	Access control	27
A.11.1	Business requirement for access control	27
A.11.1.1	Access control policy.....	27
A.11.2	User access management.....	27
A.11.2.1	User registration.....	27
A.11.2.2	Privilege management.....	27
A.11.2.3	User password management	27
A.11.2.4	Review of user access rights	27
A.11.3	User responsibilities	28
A.11.3.1	Password use.....	28
A.11.3.2	Unattended user equipment.....	28
A.11.3.3	Clear desk and clear screen policy.....	28
A.11.4	Network access control	28
A.11.4.1	Policy on use of network services.....	28
A.11.4.2	User authentication for external connections.....	28
A.11.4.3	Equipment identification in networks	28
A.11.4.4	Remote diagnostic and configuration port protection.....	28
A.11.4.5	Segregation in networks.....	28
A.11.4.6	Network connection control.....	29
A.11.4.7	Network routing control.....	29
A.11.5	Operating system access control	29
A.11.5.1	Secure log-on procedures.....	29
A.11.5.2	User identification and authentication	29
A.11.5.3	Password management system.....	29

A.11.5.4	Use of system utilities.....	29
A.11.5.5	Session time-out.....	29
A.11.5.6	Limitation of connection time.....	29
A.11.6	Application and information access control.....	29
A.11.6.1	Information access restriction.....	29
A.11.6.2	Sensitive system isolation.....	30
A.11.7	Mobile computing and teleworking.....	30
A.11.7.1	Mobile computing and communications.....	30
A.11.7.2	Teleworking.....	30
A.12	Information systems acquisition, development and maintenance.....	30
A.12.1	Security requirements of information systems.....	30
A.12.1.1	Security requirements analysis and specification.....	30
A.12.2	Correct processing in applications.....	30
A.12.2.1	Input data validation.....	30
A.12.2.2	Control of internal processing.....	31
A.12.2.3	Message integrity.....	31
A.12.2.4	Output data validation.....	31
A.12.3	Cryptographic controls.....	31
A.12.3.1	Policy on the use of cryptographic controls.....	31
A.12.3.2	Key management.....	31
A.12.4	Security of system files.....	31
A.12.4.1	Control of operational software.....	31
A.12.4.2	Protection of system test data.....	32
A.12.4.3	Access control to program source code.....	32
A.12.5	Security in development and support processes.....	32
A.12.5.1	Change control procedures.....	32
A.12.5.2	Technical review of applications after operating system changes.....	32
A.12.5.3	Restrictions on changes to software packages.....	32
A.12.5.4	Information leakage.....	32
A.12.5.5	Outsourced software development.....	32
A.12.6	Technical Vulnerability Management.....	32
A.12.6.1	Control of technical vulnerabilities.....	32
A.13	Information security incident management.....	33
A.13.1	Reporting Information Security Events and Weaknesses.....	33
A.13.1.1	Reporting information security events.....	33
A.13.1.2	Reporting security weaknesses.....	33
A.13.2	Management of Information Security Incidents and Improvements.....	33
A.13.2.1	Responsibilities and procedures.....	33
A.13.2.2	Learning from information security incidents.....	33
A.13.2.3	Collection of evidence.....	33
A.14	Business continuity management.....	34
A.14.1	Information security aspects of business continuity management.....	34
A.14.1.1	Including information security in the business continuity management process.....	34
A.14.1.2	Business continuity and risk assessment.....	34
A.14.1.3	Developing and implementing continuity plans including information security.....	34
A.14.1.4	Business continuity planning framework.....	34
A.14.1.5	Testing, maintaining and re-assessing business continuity plans.....	34
A.15	Compliance.....	35
A.15.1	Compliance with legal requirements.....	35
A.15.1.1	Identification of applicable legislation.....	35
A.15.1.2	Intellectual property rights (IPR).....	35
A.15.1.3	Protection of organizational records.....	35
A.15.1.4	Data protection and privacy of personal information.....	35
A.15.1.5	Prevention of misuse of information processing facilities.....	35
A.15.1.6	Regulation of cryptographic controls.....	35
A.15.2	Compliance with security policies and standards and technical compliance.....	35
A.15.2.1	Compliance with security policies and standards.....	35
A.15.2.2	Technical compliance checking.....	36
A.15.3	Information System Audit Consideration.....	36

A.15.3.1	Information systems audit controls	36
A.15.3.2	Protection of information systems audit tools.....	36
Annex B:	Audit Report Framework.....	37
Annex C:	Bibliography	39
Annex D:	Change history	40
History		43

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 Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 2 of a multi-part deliverable covering provisions for secure and reliable implementation, management and assessment of long term data object preservation systems, as identified below:

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

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

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

Provisions of the present document can be used by Assessors of Data Preservation Systems aiming to verify Data Preservation Services as compliant with the TS 101 533-1 [i.4], and in abidance by the applicable legislation.

1 Scope

The present document addresses the assessment of the Information Security Management System ("ISMS") of a Data Preservation System, by specifying guidelines for Assessors when reviewing and auditing a DPS.

No provisions are stated on:

- a) Assessors' qualification for which existing documentation provides specification of an exhaustive set of provisions; for this purpose ISO/IEC 17021 [i.8] and ISO/IEC 27006 [i.5] are referred to;
- b) basic Assessors' activities, such as examining the procedures audit trail, since Assessors are assumed to be familiar with them. Additional information is specified in annex B.

The present document specifies recommendations on how to assess reliable electronic data object preservation services against the ICT security measures provided for in the sister document TS 101 533-1 [i.4].

These recommendations are based on provisions of ISO/IEC 27001 [i.1], ISO/IEC 27002 [i.2] and TS 102 573 [i.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.9], ISO 15489 [i.10], ISO 23081 [i.11] and, more in general, those dealt with by ISO/TC 46/SC11 that the reader of the present document should refer to.

NOTE: The present document and its sister document TS 101 533-1 [i.4] 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.

Not applicable.

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] ISO/IEC 27001: "Information technology -- Security techniques -- Information security management systems - Requirements".
- [i.2] ISO/IEC 27002: "Information technology -- Security techniques -- Code of practice for information security management".
- [i.3] ETSI TS 102 573: "Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data for digital accounting".

- [i.4] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".
- [i.5] ISO/IEC 27006: "Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems".
- [i.6] ISO/IEC 27007: "Information technology -- Security techniques -- Guidelines for information security management systems auditing".
- NOTE: At time of publication this international standard is in Publication stage.
- [i.7] ISO/IEC TR 27008: "Information technology - Security techniques - Guidelines for auditors on information security controls".
- [i.8] ISO/IEC 17021: "Conformity assessment -- Requirements for bodies providing audit and certification of management systems".
- [i.9] ISO 14721: "Space data and information transfer systems - Open archival information system - Reference model".
- [i.10] ISO 15489: "Information and documentation - Records management".
- [i.11] ISO 23081: "Information and documentation -- Records management processes".
- [i.12] ETSI TS 102 640: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 101 533-1 [i.4] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 101 533-1 [i.4] apply.

4 Overview

The present document is intended to be used by Assessors as a guidance to assess the compliance of a DPS with TS 101 533-1 [i.4].

Assessors should ascertain, for each of the present document clauses, that provisions in the corresponding TS 101 533-1 [i.4] clauses are complied with by the DPSP. In each of the following clauses, additional provisions may be specified that Assessors should implement.

Assessors could skip reviewing any ISO/IEC 27002 [i.2] controls if the DPSP can demonstrate that a ISO/IEC 27001 [i.1] audit has been conducted that encompasses the same DPSP SOA; the DPSP should provide the ISO/IEC 27001 [i.1] audit report and certification granted to Assessors for review in such a case.

Assessors should verify which legal system(s) the DPSP operates in and should have the necessary competence on such legal system(s) in order to be able to assess the legal compliance of providing Data Preservation Services. It is assumed that Assessors perform their review based on the same principles as assessments based on ISO/IEC 27001 [i.1].

4.1 Preservation Service types

In TS 101 533-1 [i.4] are specified:

- 1) Core Data Preservation Service each DPSP shall implement;
- 2) a number of Extended Services that a DPSP may choose to provide.

Assessors should verify compliance by the DPSP with functions specified in TS 101 533-1 [i.4] associated with Core services and with Extended services the DPSP chose to implement. Provisions for assessing Extended Services are marked with [EXT].

5 Provisions based on TS 102 573

In this clause provisions are specified for Assessors related to the requirements specified in the corresponding clause of TS 101 533-1 [i.4].

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

5.1 Compliance with the TS 101 533-1

- 1) Assessors, after having verified the SoA exhaustiveness, should assess the DPSP against all controls and procedures declared as applicable in the DPSP's SoA.
- 2) Assessors should verify the presence of a formal declaration of compliance with the controls and procedures declared as applicable in the DPSP's SoA in the DPSP's Information Security Policy Document, procedures, job descriptions, and subcontractor agreements.
- 3) Assessors should review any significant deficiencies identified or recommendations given in previous assessments, in relation to controls as per TS 101 533-1 [i.4] and ensure that the deficiencies have been corrected or properly addressed.

5.2 DPSP Obligations specified in TS 102 573, clause 6

5.2.1 Arrangements to cover liabilities and financial stability

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

- 1) Assessors should verify that the Risk Assessment process has duly taken into account the indications as in clause 5.2.1 of TS 101 533-1 [i.4], including also financial risks.

5.2.2 Conformance by Subcontractors

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

- 1) Assessors should properly identify themselves at the DPSP's and at the DPSP's external service providers' premises, upon prior DPSP notification.
- 2) Assessors should assess that agreements between the DPSP and its subcontractors are in place. These agreements should include provisions obliging DPSP subcontractors to comply with all the security measures governing the DPSP relevant to their services.
- 3) Assessors should assess that agreements between the DPSP and its subcontractors specify the right for the DPSP to perform inspections, both periodical and impromptu, on the subcontractor's premises, performed both directly by the DPSP personnel or by third parties, such as Authorities and DPSP appointed persons. Assessors should ascertain the existence of previous inspection reports.

- 4) Assessors should assess that the DPSP subcontractors comply with the dispositions specified in TS 101 533-1 [i.4].

5.2.3 DPSP service provisions in abidance by the applicable legislation

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

- 1) Assessors should verify existence of documentation suitable to demonstrate that the DPSP is a legal entity according to the applicable law.
- 2) Assessors should review the existing DPSP contractual documentation to ascertain that it specifies in readily understandable language the regulation or sets of legal requirements that are to be complied by each of the services provided.
- 3) Assessors should ascertain that the DPSP contractual documentation are written as specified in clause 5.2.3, item 5) of TS 101 533-1 [i.4].
- 4) Assessors should verify the existence of procedures addressing the issues in clause 5.2.3, item 6) of TS 101 533-1 [i.4] in order to gather evidence of the effectiveness of the controls used to identify and authenticate the legitimately entitled persons.
- 5) [EXT.1] Personal data preservation.
 - If metadata are created from personal data processing, Assessors should review the existing DPSP contractual documentation to ascertain that it contains the agreements addressing the issues in clause 5.2.3, clause 7, item b) of TS 101 533-1 [i.4]; moreover Assessors should verify that metadata are managed as private data, by the procedures addressing the issues in clause 5.2.3, item 7), letter a) of TS 101 533-1 [i.4].

5.2.4 Contractual aspects

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

- 1) Assessors should review the agreements addressing the issues and the DPSP duties towards its subscribers specified in clause 5.2.4 of TS 101 533-1 [i.4].
- 2) To assess the legal validity of the agreements between the DPSP and its subscribers, Assessors are advised to ask for legal assistance.
- 3) Assessors should verify that appropriate and effective procedures exist and that resources are allocated to meet the DPSP obligations as per clauses 5.2.4 and 5.2.1 of the TS 101 533-1 [i.4].
- 4) Assessors should verify that the DPSP is capable of correctly displaying the preserved data objects according to all its contractual agreements.

NOTE: This can be based on a sample of data objects.

5.2.5 Resolution of complaints and disputes

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

- 1) Assessors should gather evidence that the procedures related to the data objects deposit are in force and comply with the service agreement and record the information specified in items 1) and 2) of clause 5.2.5 of TS 101 533-1 [i.4].
- 2) [EXT.1] Personal Data Preservation:
 - If the DPSP provides the appropriate extended service, such as personal data preservation, Assessors should verify that procedures are in place to comply with requirements as in clause 5.2.5, item 3) of TS 101 533-1 [i.4] and check the effectiveness of these procedures.

5.2.6 Organisation independence

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

- 1) Assessors should gather evidence of the DPSP's independence from its customers or providers and that in any case its decisions regarding data objects 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 [i.3], clause 6.3)

- 1) Assessors should verify that the provisions in TS 101 533-1 [i.4], clause 5.2.7 are met; in particular that agreement(s) about the identification and authentication methods of the persons entitled to act in the name and on behalf of the subscriber are in place.
- 2) Assessors should verify that procedures are in place which ensure that subscribers provide and regularly update the information as in the clause 5.2.7, item 2) of TS 101 533-1 [i.4] to the DPSP.
- 3) Assessors should verify the existence of statements as in clause 5.2.7, item 3) of TS 101 533-1 [i.4] in the agreement with the subscriber.

5.2.8 Information for trading partners

(TS 102 573 [i.3], clause 6.4)

- 1) Assessors should verify that the terms and conditions for trading partners as indicated in TS 101 533-1 [i.4], clause 5.2.8 are implemented.
- 2) Assessors should, if applicable, ascertain the existence of evidence that subscribers are provided, directly or through pointers to other sources, with information on whether the DPSP has been granted a still in force formal recognition of its status of DPSP, or positive assessment against the present specifications, by an external body and this body's official status.

5.2.9 Information for auditor/regulatory/tax authorities

(TS 102 573 [i.3], clause 6.5)

- 1) Assessors should verify that documented procedures as specified in the clause 5.2.9 of TS 101 533-1 [i.4] are in place and implemented.

6 Objectives and controls in TS 102 573, annex A

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

6.1 SS.1. Signature

6.1.1 SS.1.1. Class of Electronic Signature

- 1) Assessors should ascertain that one of the mechanism required by TS 101 533-1 [i.4] is in place. If the adopted mechanism is based on electronic signature issued on behalf of the DPSP, the Assessor should ascertain that is at least of AdES type, in compliance with the applicable legislation.

6.1.2 SS.1.2. Certification

- 1) Assessors should assess that the DPSP complies with provisions in clause 6.1.2 of TS 101 533-1 [i.4].
- 2) If the DPSP's DS use QES, Assessors should review that, according to the applicable legislation, when the CA issued the signature qualified certificate on which the QES is based (this can be deduced from a related trusted time reference) it was recognised as a valid certification authority issuing qualified certificates by the relevant authority.
- 3) Assessors should verify that the signature certificates meet the supported signature requirements.

EXAMPLE: Any limitations of use, however specified, are to be complied with.

6.1.3 SS.1.3. Signature Creation Data

- 1) Assessors should review that, if SSCD are used, they are provided and used in compliance with the applicable CP/CPS.
- 2) Assessors should review that the DPSP activation data management procedures are consistent with what is specified by the CA.
- 3) Assessors should gather evidence that, if SSCD are not used, reliable procedures and security mechanisms are enforced ensuring the SCD confidentiality.

6.1.4 SS.1.4. Certificate Subject's Registration

- 1) Assessors should gather evidence that the DPSP DS certificates are issued upon, and consistently with, specific agreements with CAs covering provisions of TS 101 533-1 [i.4], clause 6.1.4. Assessors should gather evidence that Delegate Signers have been officially appointed by the DPSP relevant management or have been delegated by the responsible for preservation.

6.1.5 SS.1.5. Certificate Revocation

- 1) Assessors should ascertain that the certificate management agreement between the DPSP and the CA indicates who (apart from the certificate subject) is entitled to forward a request to the CA for revocation of the certificates to be used for the DPS purposes.
- 2) Assessors should ascertain the existence of an auditable and effective procedure, consistent with provision in the corresponding clause of TS 101 533-1 [i.4], for requesting revocation of the certificates used for the purpose of the DPS, by the certificate subject and by the DPSP and should verify that the procedure has been carried out consistently with the written documentation.
- 3) Assessors, if this revocation procedure has already been enacted, should verify that the audit trail makes the procedure auditable.

6.2 SS.2. Maintenance of Signature over Storage Period

- 1) Assessors should ascertain existence of, and abidance by, a procedure ensuring that the signatures the DPSP or one of its DS applies (e.g. on the Closure Evidence) are maintained as specified in clause 6.2 of TS 101 533-1 [i.4].

6.3 SS.3. Storage

6.3.1 SS.3.1. Authorized Access

See also clause 6.4.

- 1) Assessors should gather evidence as to ascertain that procedures for persons' authentication and registrations are in place. The DPSP should demonstrate compliance with such procedures.
- 2) Assessors should gather evidence as to ascertain that procedures governing the preserved data objects modification and deletion are in place. DPSP should demonstrate compliance with such procedures.
- 3) Where an end-to-end encryption for the remote access is implemented, Assessors should verify the existence of an agreement with the counterpart on the encryption system to be adopted.
- 4) Assessors should ascertain that segregation among subscribers is ensured.

6.3.2 SS.2. Authenticity and Integrity

- 1) Assessors should gather evidence as to ascertain that procedure to detect loss or surreptitious modification and/or addition of data objects as in clause 6.3.2 of TS 101 533-1 [i.4] are in place and correctly implemented.
- 2) Assessors should ascertain that provisions in clause 6.3.2 addressing the usage of Closure Evidence, including algos weakening, or of alternate mechanisms, are complied with.
- 3) Assessors should check that an exhaustive audit trail generated by the procedures as in clause 6.3.2 of TS 101 533-1 [i.4] exist.

NOTE: In order to perform the above verifications Assessors would look through the entire audit trail, spanning, e.g. from the receipt, through the Closure Evidence, up to the records of additions, modifications, deletions to the preserved data objects.

6.3.3 SS.3.3. Data Object Readability

[EXT1]

- 1) Assessors should ascertain that:
 - a) if item 1) a) of clause 6.3.3 of TS 101 533-1 [i.4] applies: all the required software, hardware and any other necessary equipment are reliably and securely kept;
 - b) if item 1) b) of clause 6.3.3 of TS 101 533-1 [i.4] applies:
 - i) formats as in such item 1) b) letter i meet the specified requirements;
 - ii) where such item 1) b) letter ii) applies, assertion by the trusted third party exists that the data objects transposed in a new format have maintained their original semantics.
- 2) Assessors should verify that the procedures as in clause 6.3.3 of TS 101 533-1 [i.4], item 2) are performed according to the required schedule.
- 3) Assessors should verify that, if degradation was identified, the DPSP properly and timely:
 - a) managed the event as a security event (see TS 101 533-1 [i.4], clause A.13);
 - b) performed the data objects recreation procedures.
- 4) Assessors should verify that the BCP encompasses also what is specified in clause 6.3.3 of TS 101 533-1 [i.4], item 1), in particular 1), a).

6.3.4 SS.3.4. Storage media type

- 1) If the DPSP has agreed with some of its subscribers upon using specific media types, Assessors should verify that these media are actually used for the data objects owned by those subscribers.
- 2) Assessors should gather evidence as to ascertain:
 - a) that the DPSP has in force procedures suitable to be timely informed when the used media types do not last for the envisaged preservation period; and
 - b) that the DPSP:
 - i) has in force procedures, if such case occurs, to timely migrate to another media type, performing data objects recreation;
 - ii) has implemented the above procedures when such an event happened.

6.3.5 SS.3.5. Data Objects Format

- 1) Assessors should ascertain that agreements between the DPSP and its service subscribers specify if the data objects submitted to the DPSP are in analog and/or in electronic formats.
- 2) Assessors should verify if the provisions in clause 6.3.5 of TS 101 533-1 [i.4] are complied with, according to the Extended Services provided.

6.3.6 SS.3.6. Requirements on Separation and Confidentiality

- 1) Assessors should verify if the provisions on Separation and Confidentiality specified in TS 102 573 [i.3], annex A SS.3.6 are complied with, through existence of auditable procedures and implementation of technical and/or organisational measures.

6.4 SS.4. Reporting to and Exchanges with Authorities

- 1) Assessors should ascertain that procedures for remote data object access, ensuring confidentiality according to the applicable law, exist, along with the rationale for their choice, and are complied with.
- 2) Assessors should ascertain compliance with TS 102 573 [i.3], annex A, SS.4.2 and clause 4.3.

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

[EXT1]

NOTE: The original title of the corresponding TS 102 573 [i.3], clause is "SS.5. Conversion of Paper Originals to Digital Formats". The following items apply not only to paper originals, but to any kind of analog data object, even audio or video ones.

- 1) Assessors should ascertain that the procedures for the conversion of analog originals to digital formats have been defined based on the outcomes of the Risk Assessment.
- 2) Assessors should verify the existence of the procedures specified in the clause 6.5, item 1) of TS 101 533-1 [i.4] and that they produce an auditable trail.
- 3) Where the clause 6.5, item 2) of TS 101 533-1 [i.4] applies Assessors should ascertain that the provisions therein specified are complied with.

Annex A: ISO/IEC 27001 related Long Term Preservation-specific ISMS guidelines for control assessment

A.1 Reference to ISO/IEC 27001

Each of the subsequent clauses, from A.5 on, addresses assessment against the corresponding TS 101 533-1 [i.4], clause in annex A, that matches the ISO/IEC 27001 [i.1] clause that is also referred to as "clause of reference".

Being provisions in such TS 101 533-1 [i.4] clauses based on ISO/IEC 27001 [i.1] and ISO/IEC 27002 [i.2], their assessment should be conducted consistently with the requirements for ISO/IEC 27001 [i.1] based auditing.

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 [i.2] clause (e.g. clause A.5.1.1 of the present document corresponds to ISO/IEC 27002 [i.2], clause 5.1.1).

A.3 Enhanced ISO/IEC 27002 provisions

Each subsequent clause, from A.5 on, matches the corresponding TS 101 533-1 [i.4], annex A clause that enhances the corresponding ISO/IEC 27002 [i.2] clause.

A.4 New specific controls

The following clauses, from A.5 on, provide indications for assessing the specific provisions specified in the corresponding clauses of TS 101 533-1 [i.4].

A.5 Security Policy

A.5.1 Information security policy

A.5.1.1 Information security policy document

- 1) Assessors should be provided with the DPSP's ISPD.
- 2) Assessors should ascertain that the ISPD addresses the preserved data objects classification levels.
- 3) Assessors should verify that audit trails provide evidence that the ISPD has been properly distributed to all interested persons.

A.5.1.2 Review of the information security policy

- 1) Assessors should verify that the ISPD is reviewed as per provisions in clause A.5.1.2 of TS 101 533-1 [i.4], item 1).
- 2) Assessors should verify the existence of records evidencing that the reviewed ISPD have been enforced consistently with the timeliness 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

- 1) Assessors should verify existence of a registration without gaps of who have been the persons Responsible for Preservation.
- 2) Assessors should verify that all depositors are made aware of the up to date DPSP organisation as per what affects them.
- 3) Assessors should verify existence of records on the education programme as provided to the DPSP persons.

A.6.1.2 Information security co-ordination

- 1) Assessors should ascertain that from the DPSP organisation chart appears that its Security is governed in a way to prevent implementation of conflicting practices in the various DPSP departments, e.g. hierarchically.

A.6.1.3 Allocation of information security responsibilities

- 1) Assessors should ascertain that the documentation specified in the clause A.6.1.3 2) of TS 101 533-1 [i.4] exists and is up to date.

A.6.1.4 Authorization process for information processing facilities

- 1) Assessors should ascertain that the DPSP has in force procedures ensuring that any new technology to be implemented is submitted to the Information Security management for approval before implementation.
- 2) Assessors should ascertain that for each of the implemented new technologies exists a specific prior consent to the implementation by the Information Security management.

A.6.1.5 Confidentiality agreements

- 1) Assessors should ascertain the existence of a DPSP procedure requiring that all formal communications to outside the DPSP are signed off by the DPSP relevant Management. Assessors may require the exhibition of some of the signed off permissions.
- 2) Assessors should ascertain the existence of procedures and regulations forbidding the DPSP employees to reveal confidential information in their contacts with outside the DPSP.

A.6.1.6 Contact with authorities

- 1) Assessors should ascertain that in the DPSP organisation chart are clearly specified the names or job titles of the officers who are entitled to speak with authorities on behalf of the DPSP.

A.6.1.7 Contact with special interest groups

- 1) Assessors should ascertain that the DPSP provides evidence of its capability to keep up to date with the information.

A.6.1.8 Independent review of information security

- 1) Assessors should ascertain that where the previous assessments have been performed by accredited auditors, the DPSP is capable to exhibit evidence that it has verified their accreditation.

A.6.2 External Parties

A.6.2.1 Identification of risks related to external parties

- 1) Assessors should ascertain that the DPSP Risk Assessment addresses also the risks related to dealing with external parties.

A.6.2.2 Addressing security when dealing with customers

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.6.2.3 Addressing security in third party agreements

- 1) Assessors should ascertain that guidelines exist, possibly supported by a check list, specifying the topics to be addressed in the agreements with third parties, consistently with the Risk Assessment.
- 2) Assessors should inspect some existing agreements to verify if they meet the guidelines as in corresponding clause A.6.2.3 of TS 101 533-1 [i.4].
- 3) Assessors should verify that for each outsourced activity the relevant management has formally accepted the specific provider's ISPD that should be positively evaluated by Assessors that have neither contractual nor company relationship with the involved provider.
- 4) Assessors should verify the agreements with external providers require service continuity by the provider suitable to meet the DPSP BCP requirements.
- 5) Assessors should verify that, for each outsourced service, the DPSP has in force a back-out plan, regularly assessed for feasibility and duly approved by the DPSP management.
- 6) Assessors should verify that the agreements with the DPSP providers explicitly provide the right for the DPSP to perform inspections at their providers as specified in corresponding clause A.6.2.3 of TS 101 533-1 [i.4].
- 7) If the DPSP operates ad hoc developed SW Assessors should verify that in an escrow facility exists the most recent version of such SW code and documentation, as in corresponding clause A.6.2.3 of TS 101 533-1 [i.4].

A.7 Asset Management

A.7.1 Responsibility for assets

A.7.1.1 Inventory of assets

- 1) Assessors should ascertain that the DPS allows at least the creation of the inventory indicated in corresponding clause A.7.1.1 of TS 101 533-1 [i.4], including the history of input, modified and deleted data objects.
- 2) Assessors should ascertain that the inventory indicated in the corresponding clause A.7.1.1 of TS 101 533-1 [i.4] complies with the applicable legislation and is auditable.
- 3) Assessors should ascertain that item 3) in the corresponding clause A.7.1.1 of TS 101 533-1 [i.4] is complied with, where applicable.
- 4) Assessors should verify that the DPSP updates its inventories with the timing as per corresponding clause A.7.1.1 of TS 101 533-1 [i.4].
- 5) Assessors should ascertain that for any data object preserved the DPSP keeps for the same time period the information specified in corresponding clause A.7.1.1 of TS 101 533-1 [i.4].

A.7.1.2 Ownership of assets

- 1) Assessors should ascertain the existence of information on appointment as per corresponding clause A.7.1.2 of TS 101 533-1 [i.4].
- 2) Assessors should verify that the "Disaster Recovery Team" authorisations are activated only upon invocation of Disaster, in real or in case of drills.

A.7.1.3 Acceptable use of assets

Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.7.2 Information classification

A.7.2.1 Classification guidelines

- 1) Assessors should ascertain that the DPSP has in force an auditable classification mechanism.
- 2) Assessors should ascertain that the classifications assigned by the data objects owners are implemented by the DPSP.
- 3) Assessors should ascertain that the contractual documentation specifies in readily understandable language the consequences of lack of indication on this data objects classification.
- 4) Assessors should ascertain that the confidentiality classification is reviewed as specified in corresponding clause A.7.2.1 of TS 101 533-1 [i.4].

A.7.2.2 Information labelling and handling

- 1) Assessors should ascertain that provisions in corresponding clause A.7.2.2 of TS 101 533-1 [i.4] are complied with.

A.8 Human resources security

- 1) Assessors should ascertain that provisions in corresponding clause A.8 of TS 101 533-1 [i.4] are complied with.

A.8.1 Prior to Employment

A.8.1.1 Roles and responsibilities

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.8.1.2 Screening

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.8.1.3 Terms and conditions of employment

- 1) Assessors should verify that each DPSP employee accepts in writing the DPSP rules, declaring also his/her awareness of the consequences for non compliance.

A.8.2 During Employment

A.8.2.1 Management responsibilities

- 1) Assessors should verify that all DPSP officers involved in the DPS operations accept in writing their job description that specifies the employee's responsibility.
- 2) Assessors should verify the existence of an employees' evaluation process to regularly assess their experience and reliability.

A.8.2.2 Information security awareness, education, and training

- 1) Assessors should ascertain that the training programs cover also information security awareness.
- 2) Assessors should verify existence of documentation evidencing that all officers operating on the DPS are formally provided in writing with information as per corresponding clause A.8.2.2 of TS 101 533-1 [i.4].

A.8.2.3 Disciplinary process

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.8.3 Termination or Change of Employment

A.8.3.1 Termination responsibilities

- 1) Assessors should ascertain that officers acting on the DPS formally accepted that the confidentiality agreement is in force even after their termination or change of employment and, where applicable, the legal consequences related to sensitive and judicial data handling.

A.8.3.2 Return of assets

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.8.3.3 Removal of access rights

- 1) Assessors should ascertain the procedures exist to timely remove the access rights of officers leaving the DPS related mansions.
- 2) Assessors should ascertain that information on officers leaving the DPS related mansions is timely communicated to all interested personnel.

A.9 Physical and environmental security

A.9.1 Secure Areas

A.9.1.1 Physical security perimeter

- 1) Assessors should ascertain that provisions in corresponding clause of TS 101 533-1 [i.4] are complied with.

A.9.1.2 Physical entry controls

- 1) Assessors should ascertain, by inspecting the records, that the procedures as in the corresponding clause A.9.1.2 of TS 101 533-1 [i.4] are complied with.

A.9.1.3 Securing offices, rooms, and facilities

- 1) Assessors should ascertain that provisions in corresponding clause of TS 101 533-1 [i.4] are complied with, with a particular attention on ISPD addressing the physical security consistently with the Risk Assessment.
- 2) Assessors should verify the existence of security measures specifically tailored for the cases of emergency.

A.9.1.4 Protecting against external and environmental threats

- 1) Assessors should ascertain that provisions in the corresponding clause A.9.1.4 of TS 101 533-1 [i.4] are met.

A.9.1.5 Working in secure areas

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.9.1.6 Public access, delivery, and loading areas

- 1) Assessors should ascertain that provisions in the corresponding clause A.9.1.6 of TS 101 533-1 [i.4] are met.

A.9.2 Equipment Security

A.9.2.1 Equipment siting and protection

- 1) Assessors should verify the existence of a study on DPS equipment siting and protection demonstrating that the issue has been dealt with.

A.9.2.2 Supporting utilities

- 1) Assessors should ascertain the existence of a suitable emergency power supply meeting the requirement as in the corresponding clause A.9.2.2 of TS 101 533-1 [i.4], and that even in case of emergency, the computer rooms environmental conditions are compatible with the human and machine activities.
- 2) Assessors may verify the above by ascertaining the existence of a study demonstrating that the issue has been dealt with.

A.9.2.3 Cabling security

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.9.2.4 Equipment maintenance

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.9.2.5 Security of equipment off-premises

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.9.2.6 Secure disposal or re-use of equipment

- 1) Assessors should ascertain the existence of records produced by the auditable procedure as in the corresponding clause A.9.2.6 of TS 101 533-1 [i.4].

A.9.2.7 Removal of property

- 1) Assessors should ascertain that the changes in the organisation as far as regards the authority to permit off-site removal of assets are timely communicated to the interested persons.

- 2) Assessors should verify that, where the ISPD requires it, the DPSP performs spot checks consistently with the clause of reference.

A.10 Communications and operations management

A.10.1 Operational procedures and responsibilities

A.10.1.1 Documented operating procedures

- 1) Assessors should ascertain the existence of the documentation, duly signed off, specified in the corresponding clause A.10.1.1 of TS 101 533-1 [i.4].
- 2) Assessors should ascertain that up to date copies of the operating procedures in force are securely kept by the relevant managers and that evidence exists that periodical inspections are performed aiming to verifying the consistency between the reference documentation and the operating procedures.

A.10.1.2 Change management

- 1) Assessors should ascertain the existence of records evidencing that the practices as in the corresponding clause A.10.1.2 of TS 101 533-1 [i.4] are complied with.

A.10.1.3 Segregation of duties

- 1) Assessors should ascertain that the segregation of duties is implemented, either by enforcing the applications or equipment features, or by organisational means.
- 2) Assessors should verify that the DPS is not operated with System Administrator's privileges.

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

- 1) Assessors should ascertain that, where sensitive data are used for testing purposes, provisions in corresponding clause A.10.1.4 of TS 101 533-1 [i.4] are complied with.
- 2) Assessors should inspect the acceptance tests traces to ascertain that personnel involved in the SW development have not directly operated on the test environment in a way to affect the test results.

A.10.2 Third party service delivery management

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.10.2.1 Service delivery

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.10.2.2 Monitoring and review of third party services

- 1) Assessors should ascertain that senior managers have been appointed by the DPSP to comply with the ISO/IEC 27002 [i.2], clause of reference, supported by either by DPSP experts or by external experts.
- 2) Assessors should ascertain the existence inside the agreements between DPSP and the external providers of provisions stating that the DPSP has the right to perform regular and extemporaneous inspections.

A.10.2.3 Managing changes to third party services

- 1) Assessors should ascertain the existence of auditable procedures, both on the DPSP and on the outsourcers, recording the change process as in corresponding clause A.10.2.3 of TS 101 533-1 [i.4].

A.10.3 System planning and acceptance

A.10.3.1 Capacity management

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.10.3.2 System acceptance

- 1) Assessors should ascertain the existence of the documentations as in the corresponding clause A.10.3.2 of TS 101 533-1 [i.4].
- 2) Assessors should ascertain the existence of securely kept documentation of each DPS related system configuration and of the periodical verifications records as in corresponding clause A.10.3.2 of TS 101 533-1 [i.4].

A.10.4 Protection against malicious and mobile code

A.10.4.1 Controls against malicious code

- 1) Assessors should ascertain the existence of the records generated by the procedures as in corresponding clause A.10.3.2 of TS 101 533-1 [i.4].
- 2) Assessors should verify that the DPSP has specified a sound rationale for its malware detection and removal applications update frequency and modality.

A.10.4.2 Controls against mobile code

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.10.5 Back-up

A.10.5.1 Information back-up

- 1) Assessors should ascertain that the back up frequency, the adopted media, the data architecture, the choice on what other assets are to be backed up are supported by technical reports consistent with the purpose of the Note in the corresponding clause A.10.5.1 of TS 101 533-1 [i.4].
- 2) Assessors should ascertain that the chosen back up copies storage locations are consistent with the BCP.
- 3) Assessors should verify the existence of records of the periodical back up copies readability checks.

A.10.6 Network security management

A.10.6.1 Network controls

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.10.6.2 Security of network services

- 1) Assessors should ascertain that the networks architecture, including Firewalls and Intrusion Detection Systems, meet the requirements in the in corresponding clause A.10.6.2 of TS 101 533-1 [i.4].
- 2) Assessors should inspect the logs taken by the Firewalls and Intrusion Detection Systems, to ascertain that the incident management procedures have been activated, where applicable.

A.10.7 Media handling

A.10.7.1 Management of removable media

- 1) Assessors should ascertain the procedures as in the corresponding clause A.10.7.1 of TS 101 533-1 [i.4] exist and have been performed.
- 2) Assessors should verify that the readability verification intervals are based on the Risk Assessment outcomes.
- 3) Assessors should verify the existence of the reports of the inspections on media readability and of executions of recovery procedures as specified in clause A.10.7.1 of TS 101 533-1 [i.4], item 6).

A.10.7.2 Disposal of media

- 1) Assessors should ascertain compliance with DPSP auditable procedures as per in corresponding clause A.10.7.2 of TS 101 533-1 [i.4].

A.10.7.3 Information handling procedures

- 1) Assessors should ascertain that the DPSP has in force procedures ensuring that no explicit reference on the data objects and on the data objects owner is present on the media labels.

A.10.7.4 Security of system documentation

- 1) Assessors should verify that the system documentation distribution procedures comply with the ISPD.
- 2) Assessors should verify the existence of report of the system documentation managing procedures as in corresponding clause A.10.7.4 of TS 101 533-1 [i.4].

A.10.8 Exchange of information

A.10.8.1 Information exchange policies and procedures

- 1) Assessors should ascertain that the adopted encryption mechanisms are either legally required or agreed upon with the recipient or depositor.

A.10.8.2 Exchange agreements

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.10.8.3 Physical media in transit

- 1) [EXT1.1] Personal Data Preservation.
- 2) Assessors should ascertain that, where personal data is in transit, the reliable transport or couriers are chosen in agreement with, or under approval by, the Controller Assessors, where confidential data and in particular personal data are in transit, should verify the existence of report evidencing that these data are encrypted.

A.10.8.4 Electronic messaging

- 1) Assessors should ascertain that, where electronic mail solutions providing evidence of shipment and delivery, such as Registered Electronic Mail [i.12] like services, are not implemented although available, the DPSP has provided a documented rationale for this choice.

A.10.8.5 Business information systems

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.10.9 Electronic commerce services

Not applicable.

A.10.10 Monitoring

A.10.10.1 Audit logging

- 1) Assessors should ascertain that for all DPS Computer systems, technical procedures ensure that logs are created that address the information specified in the clause of reference that apply to the specific system.
- 2) Assessors should ascertain that logs are available for the time specified at least on the basis of legal requirements and of the agreement with the customer.

A.10.10.2 Monitoring system use

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.10.10.3 Protection of log information

- 1) Assessors should ascertain that all logs are kept protected from loss, alteration for at least the period of time suitable to allow for exhaustive investigation when reviewing the DPSP security policy document.
- 2) Assessors should ascertain that the logs are either replicated or backed up as in corresponding clause A.10.10.3 of TS 101 533-1 [i.4].

A.10.10.4 Administrator and operator logs

- 1) Assessors should ascertain the existence of measures addressing the notification to Administrator and operator that all operations on the DPS are logged.

A.10.10.5 Fault logging

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.10.10.6 Clock synchronization

- 1) Assessors should ascertain the existence of documentation evidencing that the UTC time source is trustable.
- 2) Assessors should verify that the UTC Time is delivered unaltered to the entire DPS.
- 3) Assessors should ascertain that the all DPS component ensures that all time reference are as specified in corresponding clause A.10.10.6 of TS 101 533-1 [i.4].

A.11 Access control

A.11.1 Business requirement for access control

A.11.1.1 Access control policy

- 1) Assessors should ascertain the existence of a declaration by the Information Security Management of the Company to which the DPSP belongs, stating the compliance with the corresponding clause A.10.11.1 of TS 101 533-1 [i.4].
- 2) Assessors should ascertain that the DPSP access policies implement the provisions as the corresponding clause A.10.11.1 of TS 101 533-1 [i.4].

A.11.2 User access management

A.11.2.1 User registration

- 1) Assessors should ascertain the existence of records evidencing that provisions as in the corresponding clause A.11.2.1 of TS 101 533-1 [i.4].

A.11.2.2 Privilege management

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.11.2.3 User password management

- 1) Assessors should ascertain the compliance with provisions as in the corresponding clause A.11.2.3 of TS 101 533-1 [i.4], by:
 - a) Inspecting the project specifications.
 - b) Inspecting the applications records.
 - c) Performing operations on the interested equipment/application.
 - d) Verifying that procedures are in place to prevent any abuse of the users' PIN/password; for example no full PIN/password is to be exchanged between the user and, where existent, the contact centre.
- 2) Where sampling is necessary due to the large number of items to inspect, Assessors should adopt a meaningful sampling criterion.

A.11.2.4 Review of user access rights

- 1) Assessors should ascertain that records exists evidencing that the security incidents management has implied the user's access rights review, where applicable.
- 2) Assessors should verify that the project specifications address issues in the corresponding clause A.11.2.4 of TS 101 533-1 [i.4].

A.11.3 User responsibilities

A.11.3.1 Password use

- 1) Assessors should ascertain that users:
 - a) have been made aware of provisions in the corresponding clause A.11.3.1 of TS 101 533-1 [i.4];
 - b) have accepted in writing the rules to build, update and use of passwords
- 2) Assessors should verify the correctness of the automated password validity checks.
- 3) Assessors should verify the existence or registrations of execution of the automated password change request.

A.11.3.2 Unattended user equipment

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.11.3.3 Clear desk and clear screen policy

- 1) Assessors should ascertain the existence of documentation evidencing that all employees involved in DPSP related activities are made aware of the clear desk and clear screen policy and that they would incur in disciplinary sanctions in case of violation of these policies.
- 2) Assessors should verify the existence of records evidencing that regular and impromptu clear desk and clear screen inspections are performed by the responsible managers.

A.11.4 Network access control

A.11.4.1 Policy on use of network services

- 1) Assessors should ascertain that the DPSP has appointed a number of network officers consistent with the disaster recovery plan.
- 2) Assessors should ascertain that records and logs exist evidencing that the DPSP network can connect only with duly authorised computers and networks.
- 3) Assessors should ascertain that the DPSP network is always protected by suitable network protection systems, like firewalls, Intrusion Detection Systems, Intrusion Prevention Systems.

A.11.4.2 User authentication for external connections

- 1) Assessors should ascertain that provisions in the corresponding clause A.11.4.2 of TS 101 533-1 [i.4].

A.11.4.3 Equipment identification in networks

- 1) Assessors should ascertain that automatic DPSP equipment connection to networks should occur only upon equipment identification and that the connection channels are encrypted where applicable,

A.11.4.4 Remote diagnostic and configuration port protection

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.11.4.5 Segregation in networks

- 1) Assessors should ascertain that, where the DPS related network is not segregated, exhaustive justifications exist.

A.11.4.6 Network connection control

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.11.4.7 Network routing control

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.11.5 Operating system access control

A.11.5.1 Secure log-on procedures

- 1) Assessors should ascertain the compliance with provisions in the corresponding clause A.11.5.1 of TS 101 533-1 [i.4].

A.11.5.2 User identification and authentication

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.11.5.3 Password management system

- 1) Assessors should ascertain the compliance with provisions in the corresponding clause of TS 101 533-1 [i.4].

A.11.5.4 Use of system utilities

- 1) Assessors should ascertain that access to DPS system software utilities is proven as granted to only a limited number of users.
- 2) Assessors should ascertain the existence of system utilities execution audit trail.

A.11.5.5 Session time-out

- 1) Assessors should ascertain the existence of a formal assessment by the relevant manager stating which of the provisions in the corresponding clause A.11.5.5 of TS 101 533-1 [i.4] is best suited.

A.11.5.6 Limitation of connection time

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.11.6 Application and information access control

A.11.6.1 Information access restriction

- 1) Assessors should verify the technical documentation ensuring that:
 - a) all copies of systems logs or application audit trails are accessed only by personnel with an actual need to know;
 - b) users access only the data objects for which they have an actual need to know.
- 2) Assessors should verify that provision in the corresponding clause A.11.6.1 of TS 101 533-1 [i.4] are implemented consistently.

A.11.6.2 Sensitive system isolation

- 1) Assessors should ascertain that the DPSP implements physical, organisational and/or logical measures suitable to ensure the DPS environment isolation from other application environments.

A.11.7 Mobile computing and teleworking

A.11.7.1 Mobile computing and communications

- 1) Assessors should ascertain that the ISPD clearly specifies that if mobile devices are used in connection with DPS this is explicitly authorised in writing by a relevant manager.

A.11.7.2 Teleworking

- 1) Assessors should ascertain the compliance with provisions in the corresponding clause of TS 101 533-1 [i.4].

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

- 1) Assessors should ascertain that the specification documentation related to the DPS components, to be purchased or specifically developed by third parties, have been adequately assessed to verify that it takes in due account the security requirements identified based on the relevant Risk Analysis.
- 2) Assessors should verify the existence of independent positive evaluation or formal certification of the DPS software package or system, where applicable.
- 3) If some software package or the DPS have gone through formal acceptance test Assessors should verify the existence of test documentation asserting that the test object meets the requirements.

A.12.2 Correct processing in applications

A.12.2.1 Input data validation

- 1) Assessors should ascertain the existence of records evidencing that provisions as in the corresponding clause A.12.2.1 of TS 101 533-1 [i.4] are complied with.
- 2) Assessors should ascertain the existence of procedures ensuring the consistency between input and output data object for every acceptance phase.
- 3) Assessors should ascertain that records provide evidence that the integrity assurance mechanism agreed between DPSP and customers is regularly performed.
- 4) [EXT1] Input data object signature verification.

Assessors should verify that the agreement between DPSP and customer, as in the corresponding clause A.12.2.1 of TS 101 533-1 [i.4] are complied with, by means of the signature verification process log and of what subsequent processes step are performed.

A.12.2.2 Control of internal processing

- 1) Assessors should ascertain that for each depositor and, possibly, for each data object type, specific officers are specified as in the corresponding clause A.12.2.2 of TS 101 533-1 [i.4].
- 2) Assessors should ascertain that log records exist for procedures ensuring that no data object has been dropped or modified in each step of the entire preservation process.

A.12.2.3 Message integrity

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.12.2.4 Output data validation

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.12.3 Cryptographic controls

A.12.3.1 Policy on the use of cryptographic controls

- 1) Assessors should verify the existence of a formal DPSP documentation providing evidence that the cryptographic choices are based on by de jure or de facto technical standards, and that deviations to such policy are consistent with the exceptions mentioned in the corresponding item of TS 101 533-1 [i.4].
- 2) [EXT1] - Preserving encrypted data objects, by force of legal or service agreement.

Assessors should verify, for conditional services as in the corresponding clause A.12.3.1 of TS 101 533-1 [i.4] that:

- a) the data object, agreed or legally required, to be encrypted is not preserved in clear;
- b) dual control based procedures exist to decrypt the encrypted data object upon request by an authorised entity.

A.12.3.2 Key management

- 1) Assessors should ascertain that records exist for any key management related process.
- 2) Assessors should verify, where encryption algorithms are used, that emergency procedures exist suitable to timely deal with situations as per the corresponding clause A.12.3.2 of TS 101 533-1 [i.4]. In particular, evidence should be available that these procedures implement Dual Control. Where the DPSP has chosen not to use the Dual Control, formal documentation should exist providing the rationale for such decision.

A.12.4 Security of system files

A.12.4.1 Control of operational software

- 1) Assessors should ascertain existence of formal approval by the relevant management for every application installed in the DPS environment, possibly as a list of approved applications to be verified against the system logs.
- 2) Assessors should ascertain that no compiler or development tool is installed in the DPS production environment.
- 3) "Assessors should ascertain existence of policies requiring that before installing any application a roll back procedure is available".

A.12.4.2 Protection of system test data

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.12.4.3 Access control to program source code

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.12.5 Security in development and support processes

A.12.5.1 Change control procedures

- 1) Assessors should ascertain that where the applications are developed and tested on the same system, procedures exist to verify that the test base is reset to its original status.

A.12.5.2 Technical review of applications after operating system changes

- 1) Assessors should ascertain that:
 - a) where hardening procedures are not enforced, a formal explanation exists;
 - b) where they exist, they are performed after every change to the DPS operating systems.
- 2) Assessors should verify that, where hardening procedures are enforced, the hardening records match the DPS status.

A.12.5.3 Restrictions on changes to software packages

- 1) Assessors should ascertain that the agreements with software developers address the topic specified in the corresponding clause A.12.5.3 of TS 101 533-1 [i.4].

A.12.5.4 Information leakage

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.12.5.5 Outsourced software development

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.12.6 Technical Vulnerability Management

A.12.6.1 Control of technical vulnerabilities

- 1) Assessors should ascertain that the team, as in the corresponding clause A.12.6.1 of TS 101 533-1 [i.4], issues regular reports on the updates in security and legislation and that the ISPD have been updated accordingly.

A.13 Information security incident management

A.13.1 Reporting Information Security Events and Weaknesses

A.13.1.1 Reporting information security events

- 1) Assessors should ascertain that the security events reporting is governed by a formal procedure, applicable both to DPSP officers and subcontractors, ensuring the timely and correct reporting of such events, including assigning a correct severity level.
- 2) Assessors should verify the existence of records evidencing that all DPSP officers and subcontractors have declared in writing they have been made aware in writing of the incident reporting related procedures and of the consequences of non abidance.

A.13.1.2 Reporting security weaknesses

- 1) Assessors should ascertain that the security weaknesses reporting is governed by a formal procedure, applicable both to DPSP officers and subcontractors, ensuring the timely and correct reporting of such events, including assigning a correct severity level.
- 2) Assessors should verify the existence of records evidencing that all DPSP officers and subcontractors have declared in writing they have been made aware in writing of the weaknesses reporting related procedures and of the consequences of non abidance.

A.13.2 Management of Information Security Incidents and Improvements

A.13.2.1 Responsibilities and procedures

- 1) Assessors should ascertain the existence of the procedures mentioned in the corresponding clause A.13.2.1 of TS 101 533-1 [i.4] and of the related records.
- 2) Assessors should ascertain that the records evidence that all the required communications to the involved persons have been enacted and that the related obligations have been formally accepted.
- 3) Assessors should verify that correct and complete documentation exists of the emergency cases handling.

A.13.2.2 Learning from information security incidents

- 1) Assessors should ascertain that records of all detected security incidents and weaknesses are reliably kept up to the next Risk Assessment and Information Security Policy Document review sessions.
- 2) Assessors should verify that it is clearly indicated upon the occurrence of what minimum security event severity level the revision of the Risk Assessment and/or the ISPD is to be performed extemporaneously.

A.13.2.3 Collection of evidence

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

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

- 1) Assessors should ascertain that the DPSP BCP is designed to restart its operations within precise time periods, to be assessed against the agreements in force and the applicable legislation, and that the records of the BCP implementation procedures simulations proved to meet such limits.
- 2) Assessors should verify that tests have been made to verify that such time periods can be met or have effectively been met.

A.14.1.2 Business continuity and risk assessment

- 1) Assessors should ascertain that the DPSP BCP has been drafted giving the highest priority to the personnel safety and according to commonly accepted specifications, such as de jure or de facto standards, taking into account a Service Discontinuity Impact Analysis on the DPS components, to which a scale of criticality level has been assigned.
- 2) Assessors should verify that the DPS components have been assigned a scale of criticality level or that the DPSP has provided in the SoA an exhaustive explanation of the rationale.
- 3) Assessors should verify that the BCP specifies the maximum downtime acceptable at least for the services and processes indicated in the corresponding clause A.14.1.2 of TS 101 533-1 [i.4].

A.14.1.3 Developing and implementing continuity plans including information security

- 1) Assessors should ascertain that an assessment has been performed to identify "the acceptable loss of information and services" of the clause of reference and that the outcomes of this decision are correctly reported in the agreements with its subscribers.

A.14.1.4 Business continuity planning framework

- 1) Assessors should ascertain that the DPSP documentation clearly specifies the person, by name or role, in charge of invoking the BCP.
- 2) Assessors should verify the existence of the Disaster Recovery Team, the components of which have been formally appointed, and of the rationale for their appointment. Where these team members are not DPSP employees documentation should exist evidencing their abidance to the provisions in the corresponding clause A.14.1.4 of TS 101 533-1 [i.4].
- 3) If the disaster recovery/back up - site is under the control of a Service Provider, Assessors should verify the existence of an assessment of its reliability and of an agreement addressing the BCP requirements, including provisions also specifying adequate sanctions in case of default.

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

- 1) Assessors should ascertain that the DPSP has in place testing plans for at least the ISO/IEC 27002 [i.2] items specified in the corresponding clause A.14.1.5 of TS 101 533-1 [i.4].
- 2) Assessors should verify the existence of records evidencing that rehearsals are planned and, where applicable, have been performed according to the planned schedule, with the participation of its external services providers.

- 3) Assessors should verify that the agreements with the DPSP service providers address the obligations specified in the corresponding clause A.14.1.5 of TS 101 533-1 [i.4].
 - 4) Assessors should verify the existence of records evidencing that the DPSP has performed the inspections on its service providers as per the corresponding clause A.14.1.5 of TS 101 533-1 [i.4].
-

A.15 Compliance

A.15.1 Compliance with legal requirements

A.15.1.1 Identification of applicable legislation

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing, also in respect of ISO 15489 [i.10], part 1, chapter 5.

A.15.1.2 Intellectual property rights (IPR)

- 1) Assessors should ascertain that the DPSP policies require registering all licensed hardware and software products prior to putting them into use, except where the owner of IPR on a specific software waives its own rights, in which cases the DPSP should be able to exhibit Assessors suitable documentation.
- 2) Assessors should verify the existence of records evidencing that all licensed hardware and software products have been regularly registered with the exception in the previous item.

A.15.1.3 Protection of organizational records

- 1) Assessors should ascertain that the DPSP can exhibit documentations suitable to giving evidence that ISO 15489 [i.10], chapter 7 was taken into account when designing the DPS.

A.15.1.4 Data protection and privacy of personal information

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.15.1.5 Prevention of misuse of information processing facilities

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.15.1.6 Regulation of cryptographic controls

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

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

A.15.2.1 Compliance with security policies and standards

- 1) Assessors should ascertain the existence of reports evidencing that all managers, at any level, perform, preferably in an unscheduled way, reviews on their respective departments to ascertain compliance with the rules.
- 2) Assessors should verify the existence of records evidencing that all persons working on, and/or for, the DPS, are made aware of the consequences of non compliance.

A.15.2.2 Technical compliance checking

- 1) Assessors should ascertain that exhaustive reports of the compliance checks exist.
- 2) Where the DPSP resorts to external providers, Assessors should ascertain the existence in the agreement of the mutual obligations and responsibility as well as the scope of the testing.

A.15.3 Information System Audit Consideration

A.15.3.1 Information systems audit controls

- 1) Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing.

A.15.3.2 Protection of information systems audit tools

- 1) Assessors should ascertain the existence of procedures for installing and removal of assessing tools and that such tool are not present in the DPS.
- 2) Assessors should verify the existence of records asserting that the assessing tools removal procedures have been performed.

Annex B: Audit Report Framework

Two deliverables of the ISO/IEC 27000 family provide guidelines for auditing, respectively:

- ISO/IEC 27007 [i.6]: Guidelines for information security management systems auditing.
- ISO/IEC TR 27008 [i.7]: Guidelines for auditors on information security controls.

These ISO/IEC documents therefore cover both aspects of a DPSP ISMS: Information Security management and ISMS controls (such as in ISO/IEC 27002 [i.2]).

This annex indicates the main issues a Final Audit Report should contain. These ISO documents will be complemented with the DPSP specific requirements provided in the present document.

The structure of the Audit Report is not addressed here, as well as intermediate reports.

Assessors would clearly address in their reports at least all the topics described hereinafter, in relation to the related clauses, in order to facilitate readers in identifying common issues across different assessment reports so to perform a cross evaluation of DPSPs.

The Final Audit Report would address the following topics.

- 1) Statutory and/or customary environment of the Assessed DPSP.
- 2) List of the DPSP documentation that have been submitted to the Assessing team, prior to and during the assessment process, as well as of those that have not been submitted although required.
- 3) Statement by the Assessing team on whether the conditions to conduct an Assessment were met prior and during to the Assessment and if it was therefore deemed possible to conduct and conclude the assessment and, in case of a negative position, the reasons for this position.
- 4) If the assessment could be conducted, an overall evaluation of the DPSP: whether it was deemed as fully, partially or not compliant with the provisions of the present document.
- 5) For each clause of the present document the Assessing team would specify their evaluations as follows:
 - a) What in the present document was recommended on Assessors to verify:
 - i) was verified (this can be assumed by default);
 - ii) was not verified; in this case, the reasons for such omission will be clearly explained and if this omission was such to affect the assessment also of other items, that would be clearly indicated, or even of the ISMS overall assessment (this would be complementary to the statement as per the previous item 3).
 - b) The outcomes of the assessment:
 - iii) the DPSP has been deemed fully compliant with the requirements established in TS 101 533-1 [i.4];
 - iv) the DPSP has been deemed partially compliant or not compliant with the requirements established in TS 101 533-1 [i.4], in which case the affected requirements will be specified;
 - v) (applicable when the previous item ii) applies) shortcomings found and their severity level;

NOTE 1: The severity levels would be structured at least in three steps. An example of such severity levels definitions would be as follows:

- Severity 1: the DPSP is not compliant with the requirement at issue.
- Severity 2: the requirement at issue may not be met in some circumstances, yet workarounds for achieving the desired compliance goal exist and can be easily applied.
- Severity 3: the DPSP is substantially compliant with the requirements, although it is wished a more straightforward implementation of the DPSP requirements.

vi) (applicable when the previous item ii) applies) recommendations for the DPSP to implement in order to comply with the requirements established in TS 101 533-1 [i.4].

NOTE 2: These recommendations will be specified on a high level, since the way to implement them is to be left to the DPSP.

- 6) A possible range of dates when the DPSP the next assessment will occur.
- 7) Where audit/assessing sessions are not performed on the whole of the provisions specified in the DPSP SoA, but on a statistically meaningful sample of these provisions, it would be good practice to verify, in the subsequent assessing sessions, the provisions that have not been verified in previous sessions.

Annex C: Bibliography

- COM(2009) 324: "Commission of the European Communities Brussels, 3.7.2009 - WHITE PAPER Modernising ICT Standardisation in the EU - The Way Forward".
- 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)".
- ISO/IEC 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security".
- ISO/IEC 20000: "Information technology -- Service management".
- ITU-R Recommendation TF.460: "Standard-frequency and time-signal emissions".
- ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

Annex D: Change history

From version 1.1.1 to 1.2.1

- 1) Amended 2 errors of severity 1.
 - 1) Clause 4 - 3rd paragraph: Sentence: "Assessors could skip the review of ISO/IEC 27002 [i.2] controls - those marked with "Assessors should act consistently with requirements for ISO/IEC 27001 [i.1] based auditing" in annex A of TS 101 533-1 [i.4] ..." was flawed. It applies to any reference to ISO/IEC 27002 [i.2] provisions. Removed any limitation anywhere in annex A.
 - 2) Clause A.10.8.3: "[EXT1.1] Personal Data Preservation" moved from item 2) to item 1).
- 2) Amended 10 errors of severity S2: text subject to possible misunderstanding having possible serious consequences. Among them:
 - 1) All instances of "document" and "information" have been replaced with "data object" when preserved items were referred to.
 - 2) Clause 2.2 Entry [i.10]: removed "2001".
 - 3) Clause 2.2:
 - i) added new entry: "ETSI TS 102 640: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM)" [i.12];
 - ii) removed it from Bibliography.
 - 4) Clause 4 - 3rd paragraph: Text reworded "Assessors could skip reviewing any ISO/IEC 27002 [i.2] controls if the DPSP can demonstrate that an ISO/IEC 27001 [i.1] audit has been conducted that encompasses the same DPSP SOA; the DPSP should provide the ISO/IEC 27001 [i.1] audit report and certification granted to Assessors for review in such a case."
 - 5) New clause 4.1 added, since in the TR body there are many references to [EXT] functions:
 - 4.1 Preservation Service types
In TS 101 533-1 [i.4] are specified:
 - 1) Core Information Preservation Service each DPSP shall implement;
 - 2) a number of Extended Services that a DPSP may choose to provide.

Assessors should verify compliance by the DPSP with functions specified in TS 101 533-1 [i.4] associated with Core services and with Extended services the DPSP chose to implement. Provisions for assessing Extended Services are marked with [EXT]."
 - 6) Clause 5.1.2: This clause lacked provision for Assessors to ascertain that there is the right to inspect outsourcers. Added the following item as item 3).
 - 3) Assessors should assess that agreements between the DPSP and its subcontractors specify the right for the DPSP to perform inspections, both periodical and impromptu, on the subcontractor's premises, performed both directly by the DPSP personnel or by third parties, such as Authorities and DPSP appointed persons. Assessors should ascertain the existence of previous inspection reports.
 - 7) Clause A.9.1.3: The Assessors' items did not cover extensively all DPSP provisions, in particular item 1) "Assessors should verify that the ISPD addresses, consistently with the Risk Assessment, the physical security." Replaced item 1) with the following:
 - 1) Assessors should ascertain that provisions in corresponding clause of TS 101 533-1 [i.4] are complied with, with a particular attention on ISPD addressing the physical security consistently with the Risk Assessment."

- 8) Clause A.10.7, item 3): There was no hint to the need to verify if, had a degradation been detected, the recovery procedures have been implemented. Added to item 3):
 "and of executions of recovery procedures as specified in clause A.10.7.1 of TS 101 533-1 [i.4], item 6)".
- 9) Clause A.10.8.4: Added link to [1.12].
- 10) Clause A.11.2.3, item 1) d): Addressed just one of the possible ways to implement item 10) of the corresponding clause in TS 101-533-1 [i.4]. Modified letter d) as follows:
 "d) Verifying that procedures are in place to prevent abuse of the users' PIN/password; for example no PIN/password is to be exchanged between the user and, where existent, the contact centre."
- 11) Clause A.11.3, item 2): Item text stated: "...regular inspections clear desk and clear screen inspections are performed by the responsible managers". This did not match the TS text, where item 1) reads: "regular and impromptu inspections performed". Amended as follows:
 "regular and impromptu clear desk and clear screen inspections are performed by the responsible managers and/or by specific officers."
- 12) Clauses A.11.5.3 and A.11.7.2, item 1): It was overlooked that TS 101 533-1 [i.4] specifies provisions. Replaced text with:
 "1) Assessors should ascertain the compliance with provisions in the corresponding clause of TS 101 533 1 [i.4]."
- 13) Clause A.12.4.1 - New item added:
 "Assessors should ascertain existence of policies requiring that before installing any application a roll back procedure should be available".
- 14) Annex B - Title: No specification existed on whether this annex was "Informative" or "Normative". Specified "Informative".
- 3) Amended 11 errors of severity S3: Nice to have. Among them:
- 1) Clause 2 - Updated status of ISO/IEC 27007 [i.6] and ISO/IEC TR 27008 [i.7], Similar amendment in annex B.
 - 2) Clause 5.1 - In some subclauses the reference to the related TS 102 573 [i.3] clauses has been added.
 - 3) Clause 5.1.4 - This clause did not match section 5.1 title: "DPSP Obligations specified in TS 102 573 [i.3], clause 6" since it addressed compliance with reference document TS 101 533-1 [i.4].
 This clause level was raised to clause 5.1. Previous clause 5.1 was changed into "5.2" changing all its subclauses numbers and changing all references to previous "5.1.n" into "5.2.n".
 Additionally a more precise reference to TS 101 533-1 [i.4] was added.
 - 4) Clause 6: Text "In addition to provisions specified in TS 102 573 [i.3], annex A, the following clauses apply" was deleted as it did not fit, being in TS 102 573 [i.3] no provision on assessing DPSP.
 - 5) Clauses A.3 and A.4: the following clarifying text was added after "subsequent"/"following clause": ", from A.5 on,".
 - 6) Clause A.6.2.3, item 6): Item 6) was so generic to actually say nothing. Modified as follows:
 "6) Assessors should verify that the agreements with the DPSP providers explicitly provide the right for the DPSP to perform inspections at their providers as specified in corresponding clause A.6.2.3 of TS 101 533-1 [i.4]."
 - 7) Clause A.7.1.1, item 3): Item 3) was so generic to specify nothing. Something was forgotten. Amended as follows:
 "3) Assessors should ascertain that item 3) in the corresponding clause A.7.1.1 of TS 101 533-1 [i.4] is complied with, where applicable."

- 8) Clause A.10.8.3, item 1): Added on top "[EXT1.1] Personal Data Preservation".
 - 9) Clause A.11.2.3, item 1): Added prepositions in "ascertain the compliance with provisions as in the corresponding clause".
 - 10) Clause A.11.6.1, item 1), letter a): reworded as follows: "all copies of systems logs or application audit trails are accessed".
 - 11) Clause A.12.3.1, item 2): Added: "[EXT1] - Preserving encrypted data objects, by force of legal or service agreement."
 - 12) Annex B - 1st paragraph: ISO/IEC 27008 [i.7] has been published and ISO/IEC is likely to be published in 2012. Amended text as follows: "Two deliverables of the ISO/IEC 27000 family provide guidelines for auditing, respectively:
 - ISO/IEC 27007 [i.6]: Guidelines for information security management systems auditing.
 - ISO/IEC TR 27008 [i.7]: Guidance for auditors on ISMS controls."Subsequent text was amended consistently.
 - 13) Annex C: No specification existed on whether this annex is "Informative" or "Normative". Specified "Informative".
- 4) Amended 9 editorial errors.

History

Document history		
V1.1.1	May 2011	Publication
V1.2.1	December 2011	Publication