

ETSI Specifications for Information Preservation

STF-401 - Information Communication
Technology Security in
Information Preservation

Franco Ruggieri

What we'll talk about

- Needs for specifications in Information Preservation
- Legal background
- ETSI role
- ETSI specifications
- ETSI specifications Samples
- Current e-signature related projects
- ETSI specifications outlook in Europe
- Information Preservation in Italy.

Why specifications on ICT Security in Information Preservation?

- ❑ Information Long Term preservation has two facets:
 1. Any information must be reliably available
 2. It must be possible to retrieve any information
- ❑ A number of ISO standards address issues related to item 2, namely: “Records Management Systems – RMS”, among which:
 - Already available
 - ISO 14721 (Open Archival Information System – OAIS)
 - ISO 15489 family (Records Management)
 - ISO 23081 family (Metadata for records)
 - Under development:
 - ISO 14641 family (Document management)
 - ISO 30300 family (Management system for records).

... but no existing standard / spec. addressed Item 1:

“Any information must be **reliably** available”

- ❑ Consequences if this gap had not been addressed:
 - Information could be tampered with (Added, Changed, Deleted)
 - Information could “decay” → records, formats and media can become unreadable
 - Information could be destroyed by accident
 - Etc.: you name them
- ❑ In this situation of lack of provisions, users with the need to resort to some Information Preservation Service Provider would have no independent providers’ assessment and they could therefore find themselves in the realm of “**Asymmetric Information**”.

Asymmetric Information: this is the point

- ❑ In 2001 George Akerlof, Michael Spence, and Joseph E. Stiglitz were awarded the Nobel Prize for Economy “**for their analyses of markets with asymmetric information.**”
- ❑ As back as in 1970 George Akerlof had already explained¹ how Asymmetric Information finishes up in excluding from the market best products / services to the benefit of the less good ones.

¹ “The Market for Lemons: Quality Uncertainty and the Market Mechanism”



Legal background

Just some hint ...

Directive 95/46/EEC (Personal Data Protection)

□ Article 17 – Security of processing

...

2. The Member States shall provide that **the controller must**, where processing is carried out on his behalf, **choose a processor providing sufficient guarantees** in respect of the **technical security measures** and **organizational measures** governing the processing to be carried out, and **must ensure compliance** with those measures.

Yes, but HOW
can the Controller
ascertain this on an even basis?

Services Directive (2006/123/EC)

Art. 26:

Any kind of
service

- 1) Member States shall, in cooperation with the Commission, take accompanying measures to **encourage** providers to take action **on a voluntary basis** in order to **ensure the quality of service** provision, in particular through use of one of the following methods:
 - (a) **certification or assessment** of their activities by independent or accredited bodies;
 - (b) drawing up their own **quality charter** or participation in quality charters or labels drawn up by professional bodies at Community level.

Certification/Assessment/Quality Charter
based on what?

Then in ETSI

- ❑ This need was perceived as well as the related risks and to this purpose a Technical Proposal to develop specifications aiming to fill in this gaping hole was submitted to the EU Commission
- ❑ The EU Commission funded this project and STF 401, a Task Force to develop guidance for **Information Preservation Service Providers**, was set up and began working on 15/3/2010.

ETSI

1. ETSI is one of the three European Standardisation Organisations officially recognised by the European Union (effective since Directive 83/189/EEC), enabling valuable access to European markets, that produces globally applicable standards for Information & Communications Technologies including fixed, mobile, radio, broadcast, internet, aeronautical and other areas.
2. ETSI is structured in Technical Committees that work through Specialist Task Forces – STF – that develop Technical Specifications (Normative), Technical Reports (Recommendations), etc.
2. Specialist Task Force – STFs are teams of highly-skilled experts working together over a pre-defined period to draft an ETSI standard under the technical guidance of the Technical Committee of reference and with the support of the ETSI Secretariat. The task of the STFs is to accelerate the standardization process in areas of strategic importance and in response to urgent market needs.

For more information, please visit:

<http://portal.etsi.org/stfs/process/home.asp>

István Zsolt Berta



Dino Esposito



Franco Ruggieri
Task Leader



a.k.a.

"The magnificent seven"



Íñigo Barreira



Paloma Llaneza Gonzales



The
STF 401
team

Gregor Karlinger



Sandro Fontana



Task Editor

The
STF 401
team



STF 401 Members Skills

ID	Name	Company	Qualification
FR	Ruggieri, Franco	FIR DIG Consultants, support Uninfo	Expert in ICT Security and in ETSI Standard writing, Coordinator of the UNINFO WG (SCD) on the same subject
IB	Barreira, Iñigo	Izenpe S.A.	Responsible for Basque Government Long Term preservation service. Expert in ICT Security.
IZB	Berta, Istvan Zsolt	Microsec Ltd	Responsible for Hungarian Long Term preservation service provider. Expert in ICT Security.
DE	Esposito, Alfredo	InfoCert s.p.a.	Internal Auditor of Infocert, one of the major Italian Qualified Certification Authority and long term preservation service provider
SF	Fontana, Sandro	GT50 srl., support Uninfo	ISO/IEC 27001 Lead Auditor. Responsible for the auditing related items in the UNINFO WG delivering analogue specifications
GK	Karlinger, Gregor	XiTrust Secure Technologies, support TELECOM. RESEARCH CENTER (FTW)	Long time experience with secure document storage based on electronic signatures (ETSI STF 155, 178– CAdES, XAdES). Architect and project manager in several projects for long term storage of electronic documents in Austria.
PLL	Llaneza Gonzales, Paloma	Llaneza A+A CB, support AENOR	Expert in ICT Security. Editor of ISO/IEC 27004. Member of a large number of ISO/IEC standardisation teams, in particular in the 27000 family

STF 401 Purpose

To publish a multi part deliverable:

ETSI TS 101 533-1: Technical Specification – Information
Preservation Systems Security

Part 1: Requirements for Implementing and Managing

ETSI TR 101 533-2: Technical Report – Information Preservation
Systems Security

Part 2: Guidelines for Assessor

This multi part deliverable is based on and extends:

ISO/IEC 27001 and ISO/IEC 27002

ETSI TS 102 573

Provisions of these documents are applicable, except where openly
said otherwise.

STF 401 Purpose - More in depth

“Technical, structural, organisational, management, etc. aspects
 and provisions of these ICT services are covered”

Information
 Preservation
 Service Provider

Not
 addressed

Issues related to:

1. Authentication and Integrity of the single document/information out of the IPSP environment if stripped off the IPSP security measures
2. Archival (i.e. non ICT security) related matters, e.g.:
 1. “virtual folder”
 2. “metadata” (including their format, content, etc.)
 3. etc.
3. Specific legal compliance requirements: TS and TR have not as a goal to meet the legal requirements of any specific EUMS.

Where we are

- ❑ Deliverables were published on 18/5/2011 (proud to say: 24 days ahead of schedule!)

Freely available from URL: <http://pda.etsi.org/pda/queryform.asp>

Just type in “101 533”

Individually downloadable publications, free-of-charge

Search for	<input type="text" value="101 533"/>	<input checked="" type="radio"/> exact expression
		<input type="radio"/> any words
		<input type="radio"/> all words
Search in <small>(default is all)</small>	<input type="checkbox"/> Title	<input type="checkbox"/> Technical Body Name
	<input type="checkbox"/> Standard Type and Doc N°	
Versioning	<input type="checkbox"/> All versions	
<input type="button" value="Search"/> <input type="button" value="Reset"/>		
<input checked="" type="radio"/> 10 items/page <input type="radio"/> 50 items/page <input type="radio"/> All on 1 page		

- ❑ STF 401 has finished its life cycle, planned on 11/6/2011
- ❑ Future steps: no one yet. Should any improvement be recognised as necessary ETSI will likely start a new STF
- ❑ No progression to EN is currently envisaged.

Some detail

- ❑ Two service classes:
 - Base service – mandatory → **A.k.a.: “Garbage In Garbage Out”**
 - Extended services – optional → e.g. verifying deposited information format suitability not to host malware, verifying e-signatures validity, etc.
- ❑ For each service class, TS provisions to implement/manage it can be:
 - Mandatory
 - Recommended (can be ignored only if the related consequences have been analysed in depth and accepted, documenting the decision)
 - Optional
- ❑ All TR provisions for Assessing an IPSP are “recommended”.

Some TS (implementing and managing) Samples – 1

❑ 5.1.1. Arrangements to cover liabilities and financial stability

The IPSP shall initially perform a Risk Assessment to assess its financial stability and capability to cover liability and shall repeat it on time basis ... and every time that technical or contractual substantial changes occur. ... The IPSP shall have the financial capability and stability, through its own assets, an insurance policy or both, to provide the services as specified in the present document including meeting the possible indemnification

❑ 6.3.2 . Authenticity and Integrity

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

❑ Closure Evidence

➤ “Metadata suitable to provide evidence of integrity of the related set of information preserved in a certain time period.”

- NOTE 1: The proof of integrity is provided by means of an auditable mechanism (e.g. QES/AdES) supported by a reliable time reference (e.g. a TST or a REM reference), or a TST supported by an audit trail suitable to identify who requested the TST itself
- NOTE 2: ... (examples of closure evidence can be: LTANS Evidence Record Syntax as specified in RFC 4998).”

Some TS (implementing and managing) Samples – 2

❑ 6.3.3. Document Readability

1. ... documents readability shall be met, ... , even in case of formats obsolescence. To achieve this the IPSP:
 - a. depending on the applicable legislation, **shall** store, ... , the **SW** necessary to the documents exhibition. Where necessary also the related **HW** shall be kept as well as **any other necessary equipment** ...;
 - b. Where the applicable legislation requires or allows **format conversion**:
 - i. The IPSP shall implement it **consistently with records management related ISO standards**
 - ii. Where the IPSP is not itself a trusted third party (e.g. a Public Officer), it shall have in force **auditable procedures to require the intervention of a trusted third party** attesting that the documents transposed in a new format have maintained their original semantics.
- ...
- 3) Where a degradation in information readability is detected, the IPSP shall **recreate** the information at issue **from its backup copies** with a timeliness suitable to prevent delays in the documents exhibition upon request. This event shall be dealt with as an **Information Security incident**

Some TS (implementing and managing) Samples – 3

❑ 6.3.5 Documents Format

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

❑ A.7.1.2 Ownership of assets

1. The IPSP shall appoint in writing all persons acting on the IPS for the purposes of the IPSP, clearly specifying the preserved information and information preserving processes each of them owns, i.e. is responsible for

❑ A.7.2.1 Classification guidelines. ← “confidentiality” addressed here

1. Any information shall always be assigned its classification level.

Some TR (assessing) Samples

Statement of
Applicability

❑ 5.1.4. Compliance with the TS

1. Assessors, after having verified the SoA exhaustiveness, should assess the IPSP against all controls and procedures declared as applicable in the IPSP's SoA.

❑ 6.3.2. Authenticity and Integrity

- 1) Assessors should gather evidence as to ascertain that procedures to detect loss or surreptitious modification and/or addition of documents ... are in place and correctly implemented

❑ 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 ...ETSI TS 101 533-01 are complied with. ← **i.e. anonymized**

**Parsing the STF 401 deliverables is over
It was about time!!!**



Some ancillary information

Some Current E-Signature Related European Projects ETSI

- Under EU Mandate M 460, ETSI is revising, since February 2011 up to May 2012, most of the reports and specifications developed from 2001 on, to the purpose of updating and simplifying them, among which:
 - Signature formats and profiles
 - Signature Creation and Verification Applications (SCA/SVA)
 - Certificate profiles
 - Etc.

Some Current E-Signature Related European Projects Comité Européen de Normalisation – CEN (another ESO)

- 1. Under EU M 460 CEN is reviewing, up to May 2012, signature creation devices certification criteria and Service Providers' Trustworthy Systems Security Requirements
CWA → EN**
- 2. Under EU funding CEN is conducting since early 2010 up to early 2012 the 3° phase of a Workshop on E-invoicing (that began in 2005) with the purpose of releasing CEN Workshop Agreements (CWA). These CWAs are expected to facilitate implementing VAT Directive 2010/45/EU to be transposed into the EUMS legislation by 31/12/2012.**

TS/TR 101 533 Implementation at EU level

- ❑ Having these deliverables been developed upon EU appointment, we expect EUMS to benefit by adopting them. This will allow:
 - End Users to make a learned choice (in the light of Directive 2006/123/EC) on reliable IPSPs all over Europe
 - IPSPs to broaden their market to the entire Europe;
- ❑ Certification based on these deliverables depends on the specific country: 2006/123/EC recommends “certification or assessment”.

Information Preservation in Italy

- ❑ Since 1999 in Italy it is legally possible to digitally preserve all kinds of documents, also analog ones (paper, “chemical” movies, etc.); regarding fiscally relevant ones, specific legal instruments were issued as back as in 2004
- ❑ UNI, the Italian standardisation organisation, issued in 2010 a standard for the “closure evidence”, based on a XML structured set of documents digest and metadata
- ❑ In December 2010 a new legislative instrument (“Code for Digital Administration”) was issued; new legally binding Technical Rules will be drafted (in several “layers”) that will eventually be based on TS 101 533-01 and TR 101 533-02 as regards ICT security. To be finalised in early 2012
- ❑ *More about Italy. All this activity on ICT security in information preservation began on 12/6/2009 when UNINFO (the ICT branch of UNI) launched a project to this purpose. When STF 401 started we decided to build on what UNINFO had done that far. Since then, both UNINFO and STF 401 deliverables have been kept aligned. Final approval was awarded for both of them on the last week of February 2011.*



Main ETSI Activities

portal.etsi.org/portal/server.pt/community/home/312



30 Jul 2011 - 19:38:44 (GMT +2)
Sophia Antipolis - France

Username

Password

Remember me

Login

[Sign Up](#)
[Forgot your password ?](#)

- Home
- People
- Manage
- Events
- Approve
- Guide
- Help
- Search

IPR	WEBstore		FC	IPR	OCG	NUG	3GPP	AERO	ATTM
	BRAN	BROADCAST	CLOUD	DECT	EE	eHEALTH	EMTEL	ERM	ESI
?	HF	INT	ITS	LI	M2M	MCD	MSG	MTS	PLI
	RRS	RT	SAFETY	SAGE	SCP	SES	STQ	TETRA	TISPAN
	USER	ISG	NSO	STF	WORKSHOP	Closed			

- Meeting Calendar
- DARE

Events: workshops, PLUGTEST®, conferences

<http://www.etsi.org/WebSite/NewsandEvents/events.aspx>

**Thank you
for your attention**

Questions?

franco.ruggieri@fastwebnet.it