World Class Standards

STF-401

ICT Security in Information Preservation

Franco Ruggieri

ETSI 6th Security Workshop

Sophia Antipolis 20/01/2011

World Class Standards

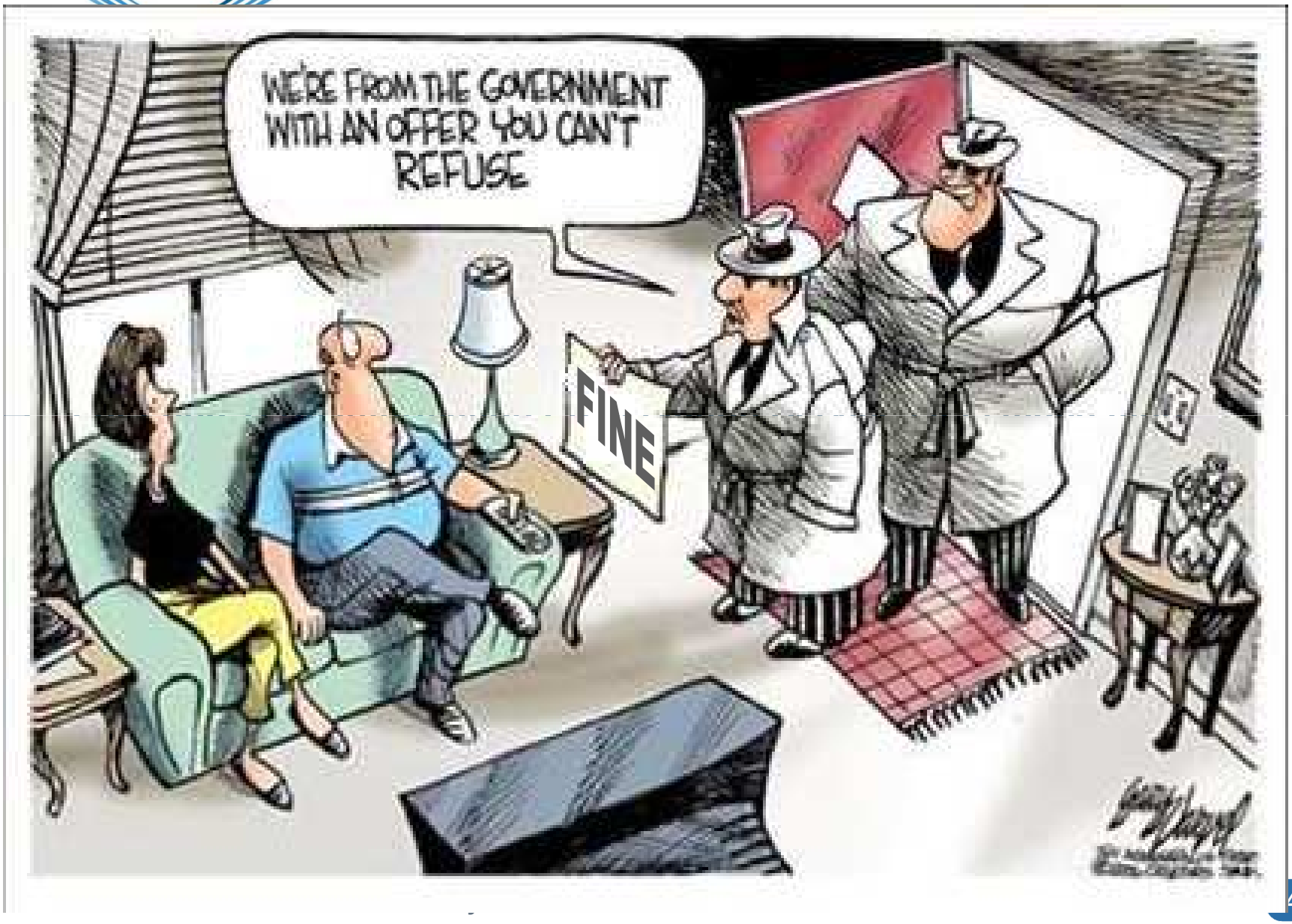
Why specifications on ICT Security in Information Preservation?

- 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":
  - 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 addresses Item 1:

"Any information must be ***reliably*** available"

- Consequences if this gap is not addressed:
  - Information can be tampered with (Added, Changed, Deleted)
  - Information can "decay" ➔ record, format and media can become unreadable
  - Information can be destroyed by accident
  - Etc.: you name them
- In this situation of lack of provisions, users resorting to an Information Preservation Service Provider find themselves in the realm of "***Asymmetric Information***".


WE'RE FROM THE GOVERNMENT WITH AN OFFER YOU CAN'T REFUSE
FINE

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:

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, "*We, the people of …*" ETSI[1]

- … perceived this need and the related risks and submitted the EU Commission a Technical Proposal to develop specifications aiming to fill in this gaping hole
- The EU Commission funded this project and STF[2] 401 was born

1. ETSI is recognised as an official European Standards Organisation 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. 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 an ETSI Technical Body 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

World Class Standards

STF 401 Terms of Reference

- **STF Title: "Best Practices for secure long term document storage"**
- **Scope:**

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 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.

ToR - More in depth

"Te ctural, organisational, management, etc. aspects ons of these ICT services are being covered"

Information Preservation Service Provider

Not addressed

Issues ted to:

1. Authe and Integrity of the ***single*** document/information ***out of the IPSP environment***
2. Archival (i.e. non ICT security) related matters, e.g.:
   1. "virtual folder"
   2. "metadata" (including their format, content, etc.),
   3. specific legal compliance requirements: the TS and TR do not have as purpose to meet the legal requirements of any specific EUMS.

Where we are

- **TS 101 533-01: provisions to implement and manage an IPSP**
  - Submitted to a first round of the ETSI TC comments in 10/2010
  - Undergoing a 2°round between 12/2010 and 1/2011
- **TR 101 533-02: provisions to assess an IPSP**
  - Undergoing an ETSI TC commenting phase between 12/2010 and 1/2011
- **Goal: to achieve ETSI TC's OK for publishing in time to meet contractual obligations with the EU:**

  Deliverables to be published by ***11/6/2011***

  They will be available for free from URL:

  http://pda.etsi.org/pda/queryform.asp.

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 type provisions to implement / manage them can be:
  - Mandatory
  - Recommended (can be ignored only if the related consequences have been analysed in depth and accepted)
  - Optional
- All provisions for Assessing an IPSP are "recommended".

Content samples

- Arrangements to cover liabilities
- Conformance by sub-contractors
- Organisation independence
- IPSP Subscriber Obligations
- Class of Electronic Signature
- Authorized Access
- Authenticity and Integrity
- Document Readability
- Information security policy
- Management commitment to inf. security
- Asset Management
- Physical and environmental security
- Communications and operations MGMT
- Information security incident MGMT
- Business continuity and risk assessment
- …

Addressed both in the TS and in the TR

Based on ETSI TS 102 573

Based on ISO/IEC 27002

Some TS Samples – 1 (provisional)

- **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, through ***its own assets, by means of 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*** related to one specific ***preservation set*** built up with ***the digests of at least all the documents therein contained***, preferably structured in a way to ***facilitate parsing***, that provides ***proof of integrity*** 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."

Some TS Samples – 2 (provisional)

6.3.3. Document Readability

1. **To ensure documents readability, … , even in case of formats obsolescence, the IPSP:**

   [CHOICE]

   a. **… 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. **… shall:**

      i. Transpose documents from one format about to become obsolete into a new format…. chosen, …, among those that:

      1) Are officially recognised as legally valid, where applicable, or
      2) Are indicated by independent technical reports as been known, at the current state of art, as immune from Presentation Corruption Agents.

   …

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 Samples – 3 (provisional)

- **A.6.1.5. Confidentiality agreements**
  1. No information on the IPSP, on its IPS related service providers, on its customers and on the preserved information ***shall be disclosed unless a derogation authorisation*** …, and, even in this case, it shall only be disclosed to ***persons with a need to know formally recognised*** either by the information owner or by the IPSP management.
- **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.**
  1. Any information shall always be assigned its classification level.

Statement of Applicability

Some TR Samples (provisional)

- **5.1.4. Compliance with the TS**
  1. Assessors should review the IPSP risk analysis and the 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*** as in clause 6.3.2. of TS 101 533 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 corresponding clause A.10.1.4 of ETSI TS 101 533 are complied with. ← i.e. anonymized


István!
Dino!
Franco!
a.k.a.
"The magnificent seven"
Iñigo!
Paloma!
Gregor!
Sandro!

World Class Standards

Questions?

franco.ruggieri@fastwebnet.it