ETSI World Class Standards

Indo-European dialogue on
ICT standards &
Emerging Technologies

(Growth, Profitability & Nation Building)
13-14th March 2014 • New Delhi, INDIA

IN THE FRAMEWORK OF
Project
SESEI
http://eustandards.in/

SECURITY/PRIVACY AND TRUST

Presented by Riccardo Genghini (ETSI ESI and eSCG Chairman)

Digital economy: laws and standards

- The economy paradigm shift we are experiencing requires to tackle serious challenges
  - Security, Privacy and Trust are “properties” that digital services or services digitally provided must guarantee
    - Several countries (including the EU) adopted laws about electronic communications, data protection and about electronic signatures
      - E.g. the EU is going to approve a new Regulation about electronic Identification, Authentication and Signatures
    - To comply with the law requirements a huge standardization effort is ongoing worldwide
      - E.g. the EU gave mandates to the recognized European Standardisation bodies (CEN and ETSI) to support the law enforcement

Security and (electronic) documents

- eCommerce is thriving mostly without using electronic signatures, and its business models for the moment look sound.   In fact such transactions in the analogic world would be not-written (besides the issuing of a payment receipt)
- So what are the use cases for electronic signatures and electronic seals?

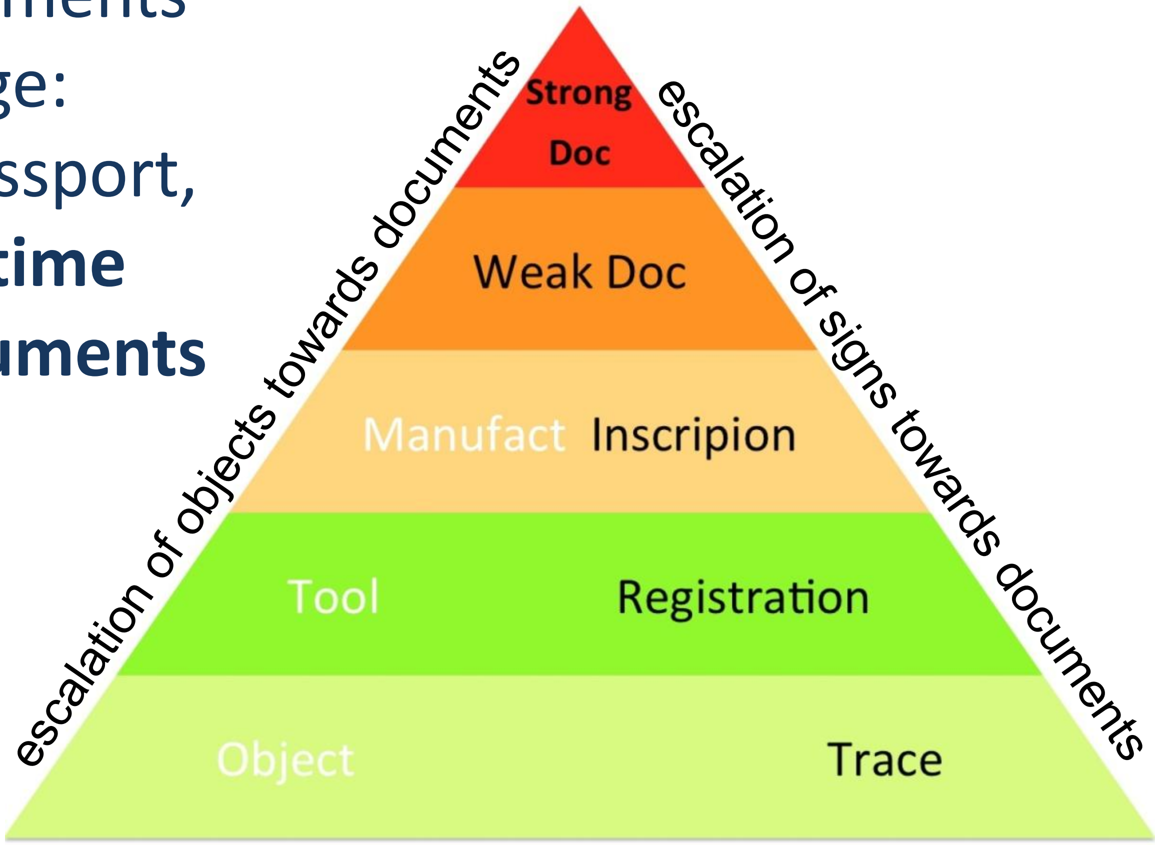
some other written digital documents needed for

DIGITAL AGREEMENT

1. What is a document?

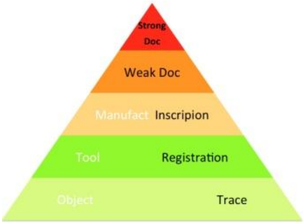
Documental pyramid

- What is a document?
- At the apex documents and objects merge:
  a banknote, a passport, are **at the same time objects and documents**


Strong Doc
escalation of objects towards documents
escalation of signs towards documents
Weak Doc
Manufact
Inscripion
Tool
Registration
Object
Trace

Copyright by Maurizio Ferraris & Riccardo Genghini 2012

Towards the document



Copyright by Maurizio Ferraris 2012

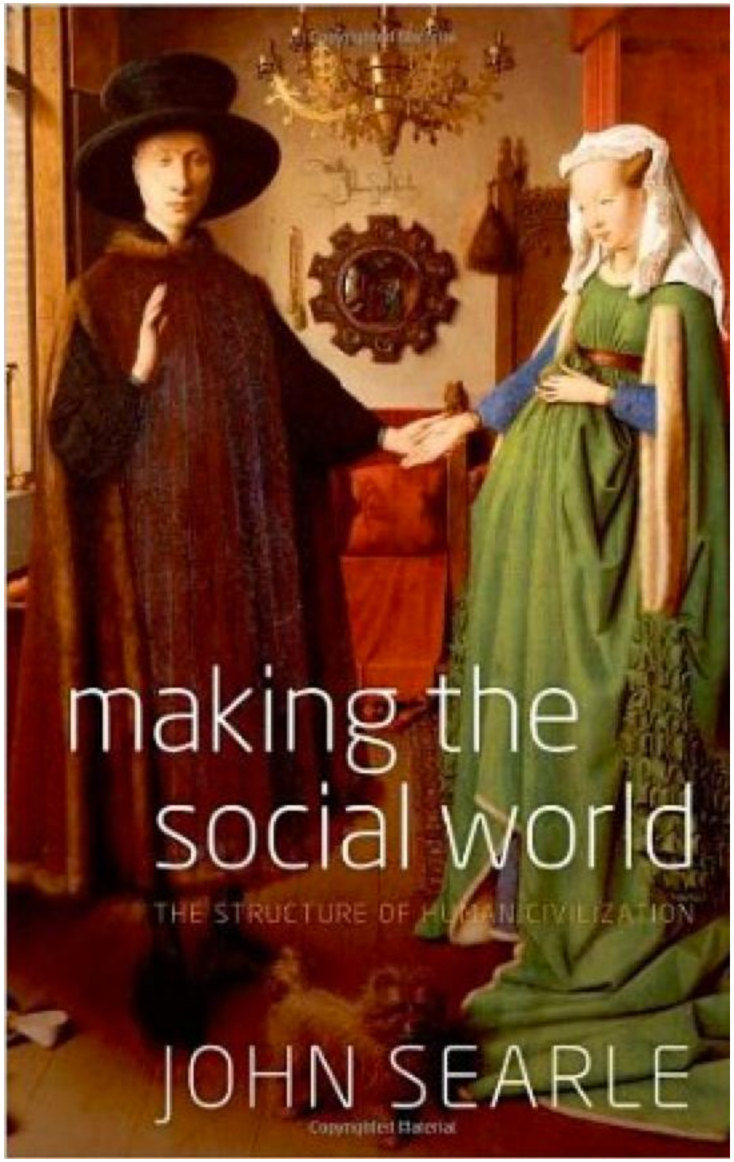
- From the bottom up
  - **Trace**: sign generated by events;
    no meaning, intention or whatsoever purpose
  - **Recording**: trace is generated on a medium (ontologically) designed for keeping the trace over time
  - **Inscriptions**: recording is (ontologically) accessible by more then one person
  - **Documents**: inscriptions generated by the author to convey a specific semantic message
    - **Documents (or weak documents)**: convey specific information to at least one additional person; no whatsoever socially accepted consequence
    - **Legal documents (or strong documents)**: socially recognized effect

Legal (strong) documents

- Legal documents may
  - have to be generated in a formal context
  - have to use a language formally accepted by the social context (in order to avoid ambiguity)
  - need to have an author that is defined or definable
  - need to have a recipient that is defined or definable
  - need to be fulfill specific formal requirements
- Legal (strong) document are
  - the Law: esp. the Codes, like the Civil or Commercial ones
  - Real Estate Registrars, Registrar of Companies, Cadastre
  - stock exchange indexes, timetables at harbors, airports, bus/train stations (ontologically dynamic in our ICT society)

Legal (strong) documents (cont'd)

- ❖ Legal (strong) document are
  - ❖ the Law: esp. the Codes, like the Civil or Commercial ones
  - ❖ Real Estate Registrars, Registrar of Companies, Cadastre
  - ❖ stock exchange indexes, timetables at harbors, airports, bus/train stations (ontologically dynamic in our ICT society)



The document is therefore a social object

2. Is a document “static”?

Strong documents are dynamic!

- Most relevant legal (strong) documents are dynamic
  - **therefore it is plainly wrong to consider trustworthy only static documents!**
  - their trustworthiness is guaranteed not only by specific rules, but also by human intervention
- “Human Interference Task Force” (1981):
  - to make information lasting for 10.000+ years, an inscription (sign on a medium) will not work because
    - sign may fade to the point of being unrecognizable
    - language will have changed so much, that nobody is able to understand it anymore (time span: 200-800 years)
    - the support of the sign may have decayed
  - only a properly designed activity ongoing for 10.000 years!

So, what about static documents??

- a static document is
  - a pragmatic, cost efficient shortcut to convey information, for short and medium term needs
  - not the best for very long term, nor the most trustworthy
    - easy forgery of paper based documents, if not physically protected (banknotes, passport)
- information mission critical or lasting an undefined timespan, requires some organization of human activity for its generation/handling/preservation
- a document not linked to a person or an organization, is somehow orphan and potentially void of a deep real meaning (also in *Phaedrus*, Plato)

Digital documents: continuity, changes

- documents’ and signatures’ function unchanged
  - if compared to their inherent nature (ontology) in the last 2000 years, even after digitalization
- **but three ontological changes**, affecting human interaction with digital data/information in spite of with analogic registrations / inscriptions / documents
  - to be perceivable/understandable, digital data require tools (displays, speakers or printers) that mediate the relation “human person - information/document”
  - creation/elaboration of data/information much more complex and sophisticated
  - LANs/Internet makes machine physical location irrelevant

Digital document: bad design

- another relevant change (?)
  - a paper document can be accessed only by those who can access the room/drawer/file, where the paper is archived
  - instead many IT systems give unrestricted access to data / information because of lack of proper design/configuration

Digital document: static, dynamic, both

- **the (overall) function of a document, does not change, because it has been produced/exchanged in digital form**
  - (some of) the properties of the document may change
  - commonplace is to state that digital documents are not inherently static, unlike paper based documents, implying that they may not be real documents
  - this hypothetical difference between analogic and digital data/information/documents (i.e. digital recordings, inscriptions and documents), in the end, comes down to how a specific digital or analogical document has been archived and preserved, and is not an ontological difference

Digital document: static, dynamic, both

- **Verba manent, scripta volant**
  - the essence of (digital) documents is their ability generate a reliable understanding of the (social/legal) reality
  - **what really matters, is not its morphology (the sign encapsulated in a document), but the long lasting trace that documents leave in our minds!**
- the ontology of a document is its social function and its **willful representation of (legal/social) reality**
- the document as such can be static, dynamic or both at the same time
  - **most relevant documents are static and dynamic at same time**

Document's ontological properties

- First: it leaves a trace in the human brain
  - If apperceived (seen, read, listened) by several humans it leaves almost identical traces in the minds of those who have apperceived it
  - Its meaning is defined by text and context
- Second: not (anymore) defined by its morphology
  - but by its (recognizable) social function
- Third: its origin must be verifiable

2. The document is non necessarily "static"

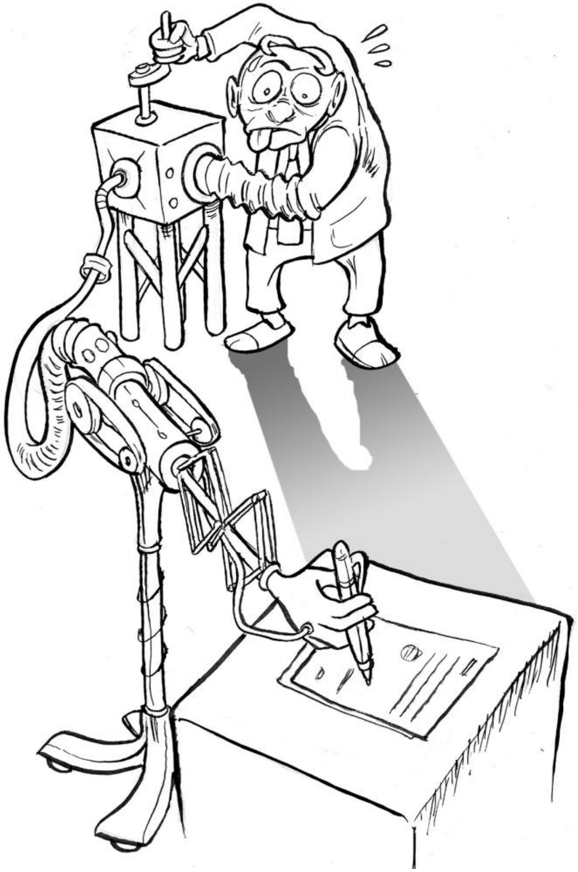
- The only "static" document of legal pre-history are the marble tables: all other documents where inherently modifiable (wax tables). No graphology!
- Documents where made "static" through seals and/or conservation
- Most relevant legal documents since the XIX Century, are at the same time static and dynamic: legal codes, cadaster, registrar of companies, real estate registrars, airport/station timetable.

3. What can electronic signature do?

- **ES**: is an evidence (no proof) that a not reliably identified signatory, has signed a digital document. Additional evidences needed. Like with fax documents, more or less. No WYSIWYS.
- **AdES**: it is a sealed document, where tampering with the content is highly unlikely but eventually possible. The quality of identification of the signatory depends very much on the process in which AdES is embedded. No WYSIWYS.
- **QES**: (quite) trustworthy identification of the signer and tamper proof document. No WYSIWYS.

4. What are electronic signatures?

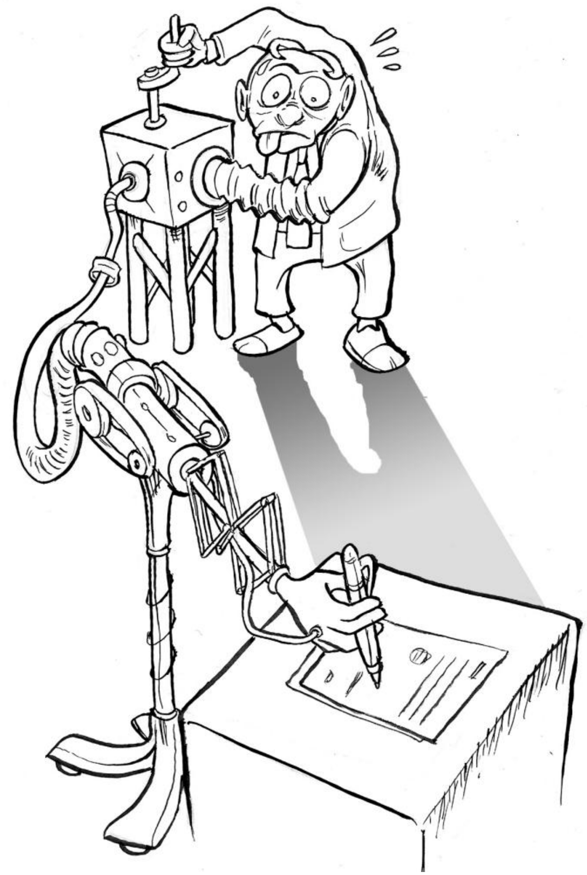
- They are substantially very different from handwritten signatures:
  - no direct perception/control of the document
  - no direct control of the signature creation process
  - need to trust in one or more TSPs
  - less secure signature creation environment
  - no WYSIWYS…



© 2002 Riccardo Genghini

5. What can we do with ES, AdES and QS?

- Electronic Signatures have the same functions of the ancient seals:
  - ❖ The signatory has to rely on some trusted third party to affix the seal,
  - ❖ has no direct control on the sealing process and on the document itself



© 2002 Riccardo Genghini

5. What can electronic signature do?

- ES: is a substitute for “fax agreements”, **not for signed letters**
- AdES: embedded in secure workflows, it is a good mean for defining the moment of “creation of a document”. Identification and authentication are managed by the ERP in which AdES are embedded. **Killer** (functional) **application** in “closed systems”. Residual security issues
- QES: the “real stuff”: but risky if the digital documents are created and signed in uncontrolled environments. Considering the equivalence to handwritten signatures, the document creation process should be managed by a trusted third party, to have an “even playing field”

6. Practical use cases: ES

- Current e-commerce and telecommunication applications

6. Practical use cases: AdES

- **Signature-Pads** Implemented by Hotels, Logistic, Postal Systems, Banks, Insurances, etc.
  - *advantage*: “business as usual” for the signer.
  - *risk*: hidden vulnerabilities, need to properly protect biometric data of the signatory. Need to encrypt biometric data with protected encryption keys. A new QTSP ?
- **Identity Management Systems** Implemented by large organisations and public administrations
  - *advantage*: identity management according to the policies specific to the organisation
  - *risk*: insufficient protection of the users

6. Practical use cases: QES QSeal

- **Transactional platforms** Implemented by Notaries, Specialized companies (Docusign, etc.):
  - combined use of Qsig, QSeals, AdES, timestamps; documents 2be signed generated in trusted environment
  - *risk/advantage (?)*: no supervision on such EU TSP, how to assess the security of the transactional platform ?
- **Long term preservation of documents** Implemented by large organisations and public administrations.
  - combined use of Qsig, QSeal, AdES, timestamps
  - *advantage*: enhanced evidential value of (unsigned) digital documents
  - *risk/advantage (?)*: no supervision … etc.

6. Practical use cases: QES QSeal

- **Trusted Wikis and Wooks** Implemented by Companies, Universities and Associations for digital learning. Qsig, Qseal, Timestamps
  - the dynamic interactive book (i.e. “iWook” a static-dynamic document), a tool for:
    - User manuals
    - School and University textbooks, publishing of scientific papers
    - Interactive learning
    - Collaborative editing
  - the so-called eBooks are just a software mimicking paper:
    - an absurdity like a moto-vehicle pulled by horses; the prehistory of digital books… just try to imagine how publishing will look like, if you put into the equation interactivity, modifiability, verifiability, etc…

Is the electronic signature enough?

- Intrinsically it is:
  - Sole control
  - SSCD
  - Collision resistant hashes
  - Trustworthy identification of the SSCD holder

BUT…

NO! 1 Long term preservation essential

- As we have seen a documents to be relevant, MUST leave a trace in our brain.
- Digital long preservation is essential for digital documents to become relevant as social objects

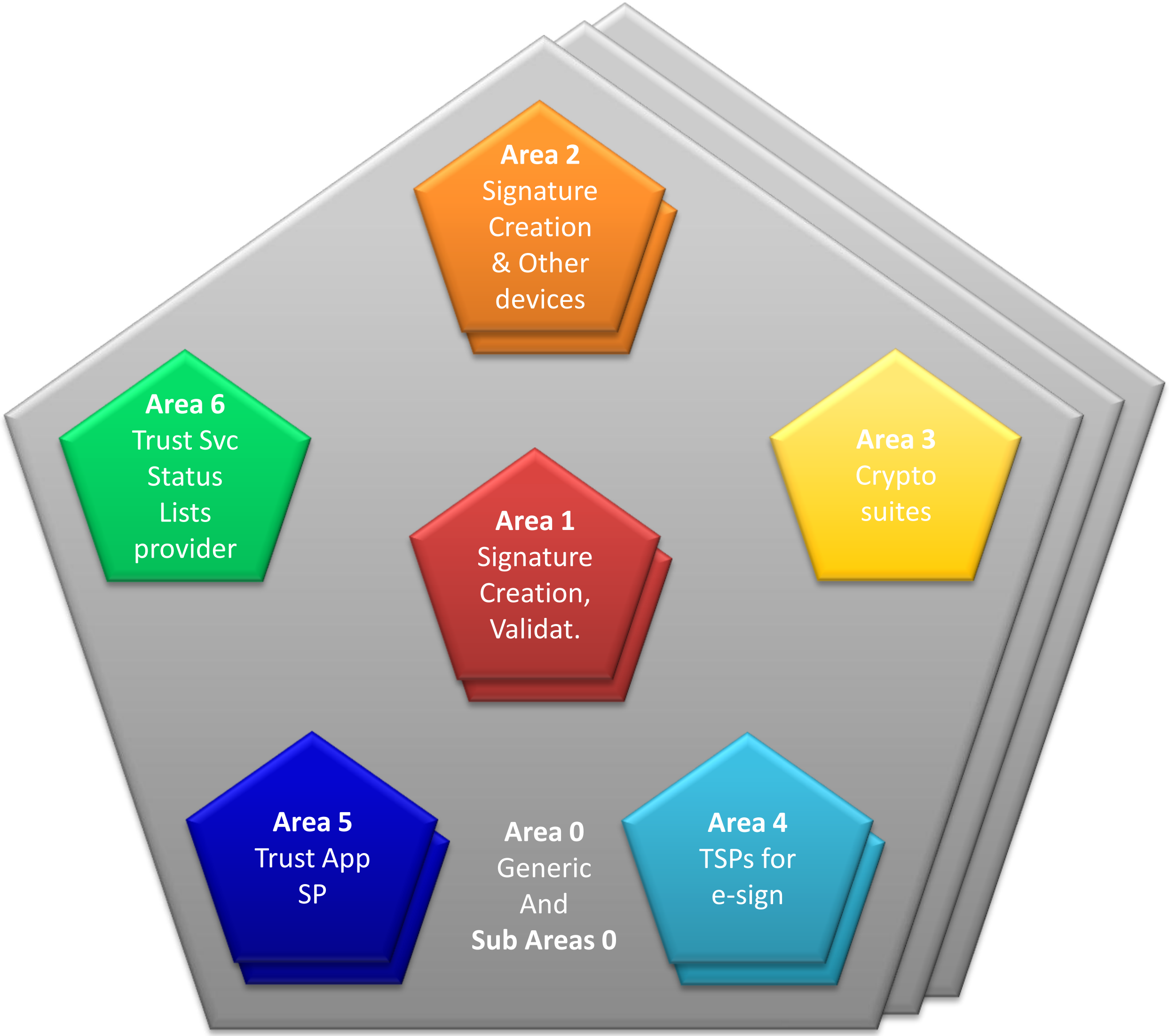
NO! 2 Trusted Third Parties needed

- If documents are prepared today in unilateral and untrustworthy ways
- In the digital era the Trusted Third Parties are still needed because
  - (ontological reason) socially (legally) and economically most important documents are **dynamic** (and not static) and precisely such documents to be handled trustworthily for all relying parties
  - (technological reason) digital documents can be **static** or **dynamic**, or **both** at the same time, depending on their technical design/implementation: in IT environment whenever such dynamic data have to be transacted, a “clearing house” “proxy” function is established

Role of CEN/ETSI: state-of-the-art

- Technical CEN/ETSI specifications on the electronic signature fulfil only one part of the function
  - verify the origin and integrity of a digital document

M/460 rationalized framework: functional areas



Area 2
Signature Creation & Other devices

Area 6
Trust Svc Status Lists provider

Area 3
Crypto suites

Area 1
Signature Creation, Validat.

Area 5
Trust App SP

Area 0
Generic And
Sub Areas 0

Area 4
TSPs for e-sign

M/460 rationalized framework

- Information about the rationalized framework and the standard being developed/updated under this umbrella can be found here:

http://www.e-signatures-standards.eu/

7. Conclusion

- **Proper understanding of the ontology of documents** is necessary to design proper document/information management systems. Working on the basis of superficial common sense, produces IT Zombie Systems
- **AdES QSig QSeal** have solved just part of the problem of signing digital documents. The other part of the problem is how to trust the content that is presented to the signatory
- **Digitally signed transactions** are substantially different from analogic documents. They are a service (not an object), they are an informative process that does not stop with the signature, they are still no social objects

Prof. Riccardo Genghini

ETSI ESI CHAIRPERSON

riccardo.genghini@ewitness.eu

www.riccardogenghini.it