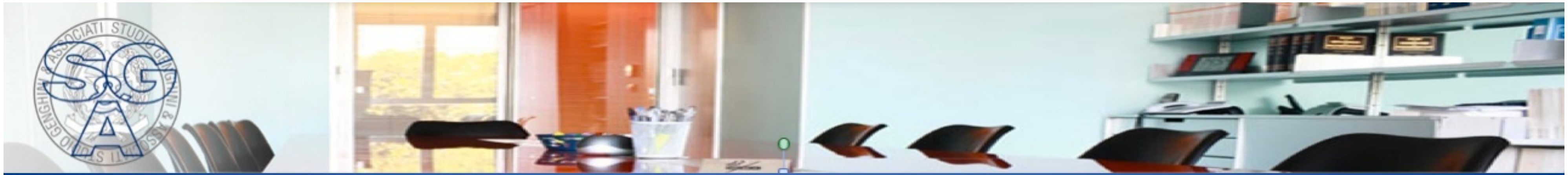


DIGITAL AGREEMENT

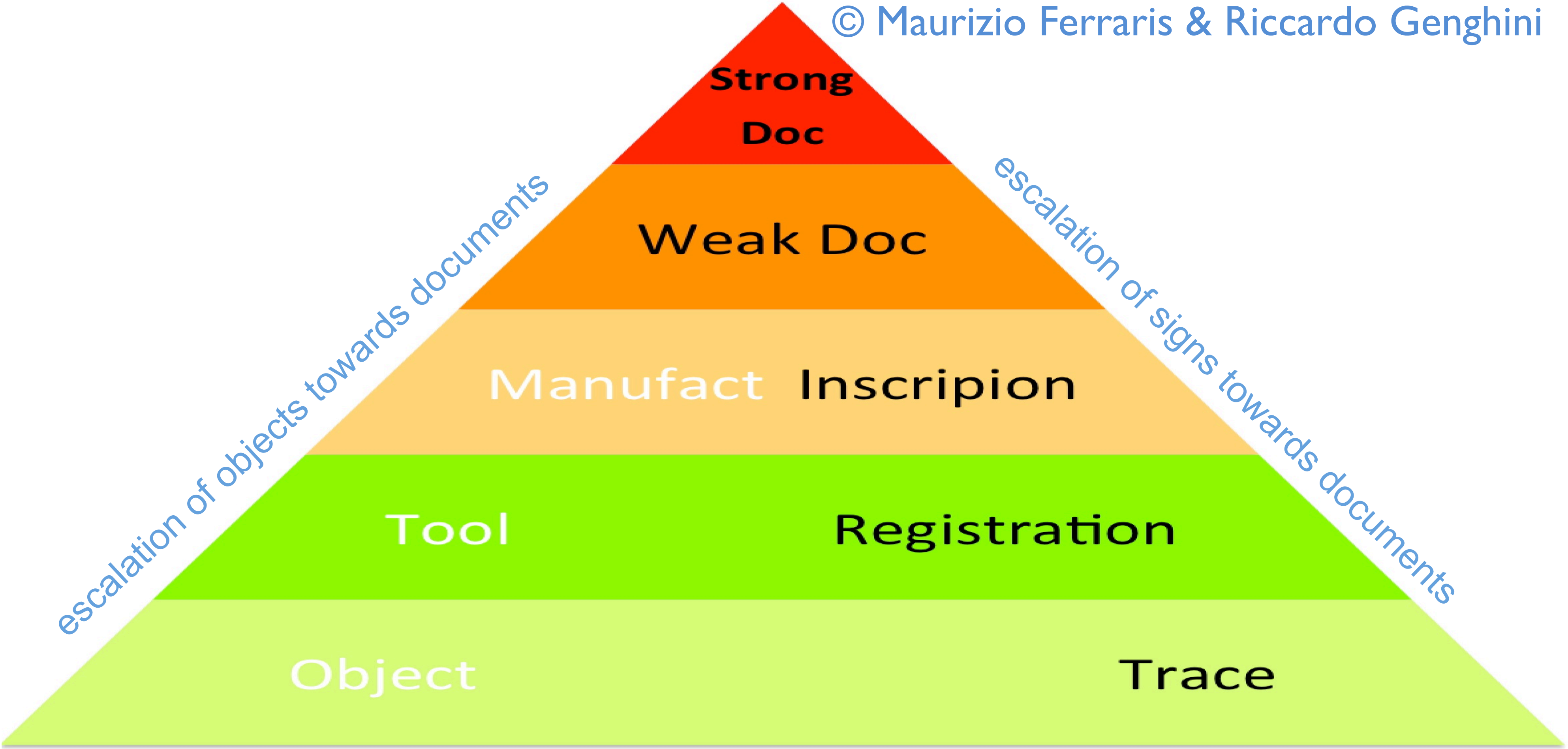
New Experiences/Recommendations with regard to the usage of eSigs/eSeals in the context of legal documents and transactions

Prof. Riccardo Genghini - Università Cattolica di Milano

EEMA Brussels 14.1.2014

© 2014 STUDIO GENGHINI & ASSOCIATI

1 WHAT IS A DOCUMENT ?



© Maurizio Ferraris & Riccardo Genghini

Strong Doc

Weak Doc

Manufact Inscripion

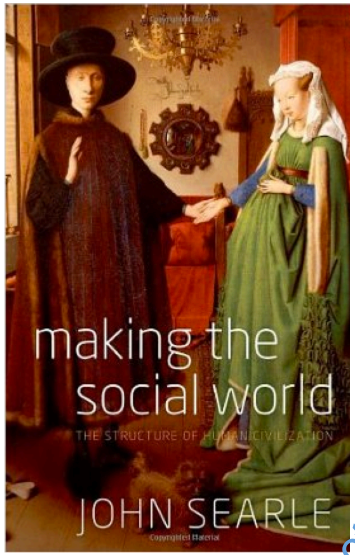
Tool Registration

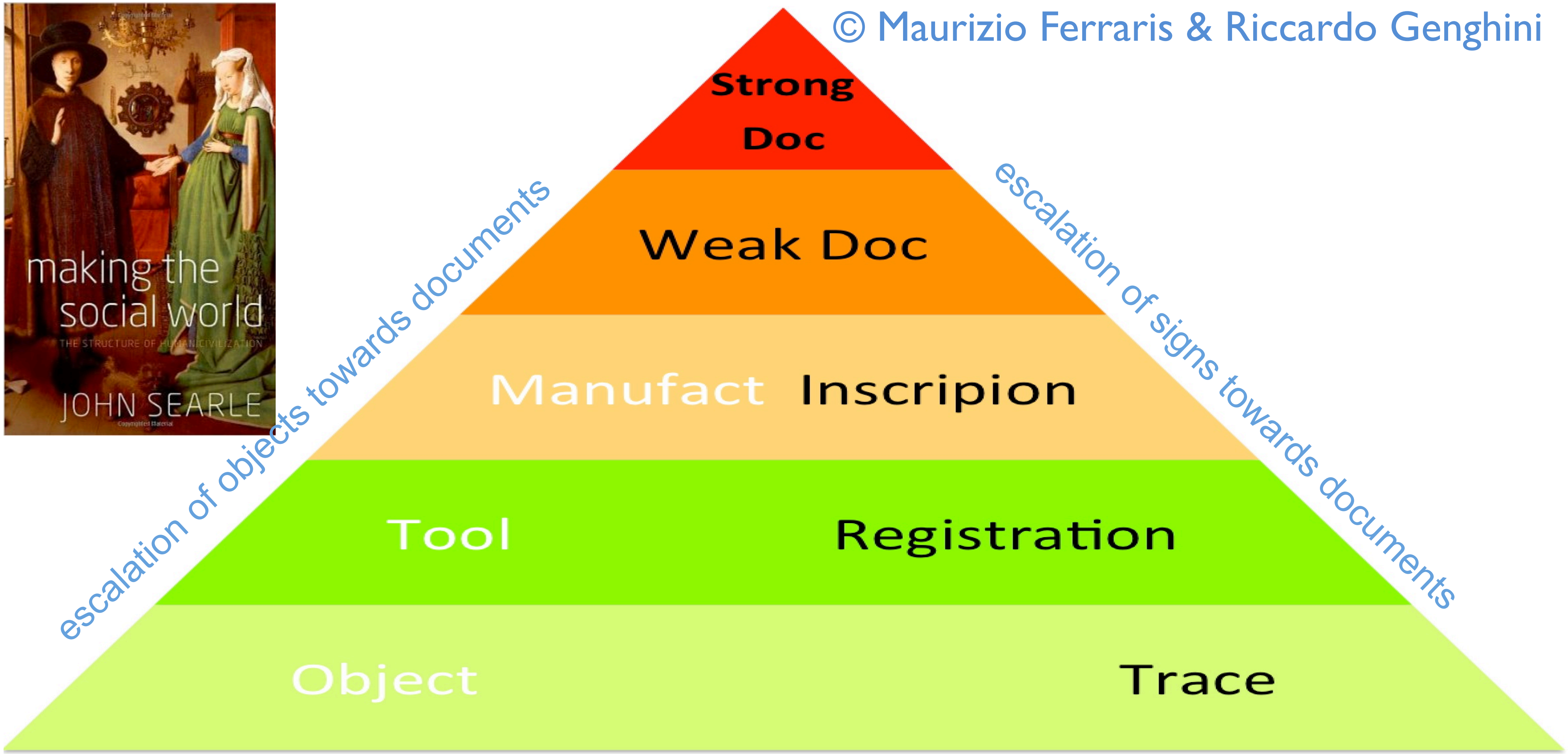
Object Trace

escalation of objects towards documents

escalation of signs towards documents

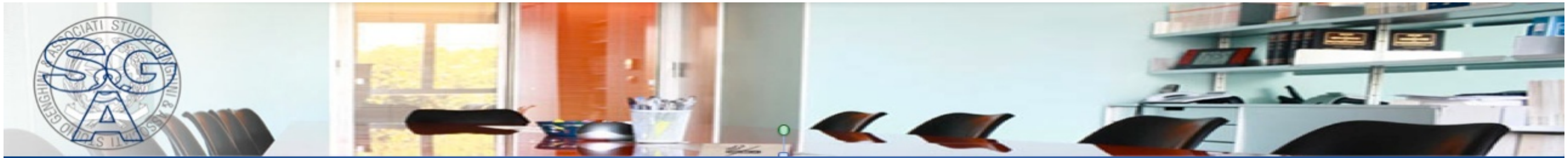
1 WHAT IS A DOCUMENT ? A SOCIAL OBJECT


making the social world
THE STRUCTURE OF HUMAN CIVILIZATION
JOHN SEARLE



© Maurizio Ferraris & Riccardo Genghini
Strong Doc
Weak Doc
Manufact
Inscripion
Tool
Registration
Object
Trace
escalation of objects towards documents
escalation of signs towards documents

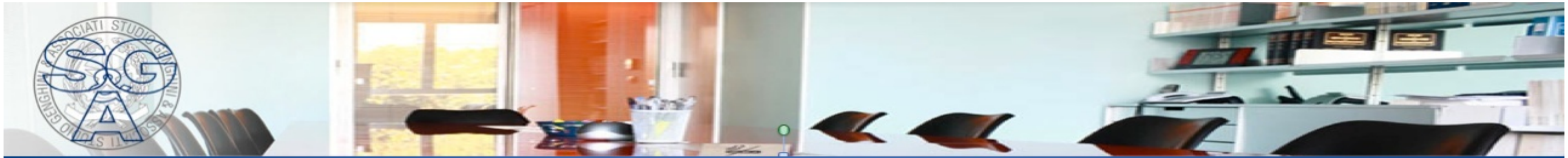
© 2014 STUDIO GENGHINI & ASSOCIATI



2 IS A DOCUMENT “STATIC” ? Not necessarily

- 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.

© 2014 STUDIO GENGHINI & ASSOCIATI



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.

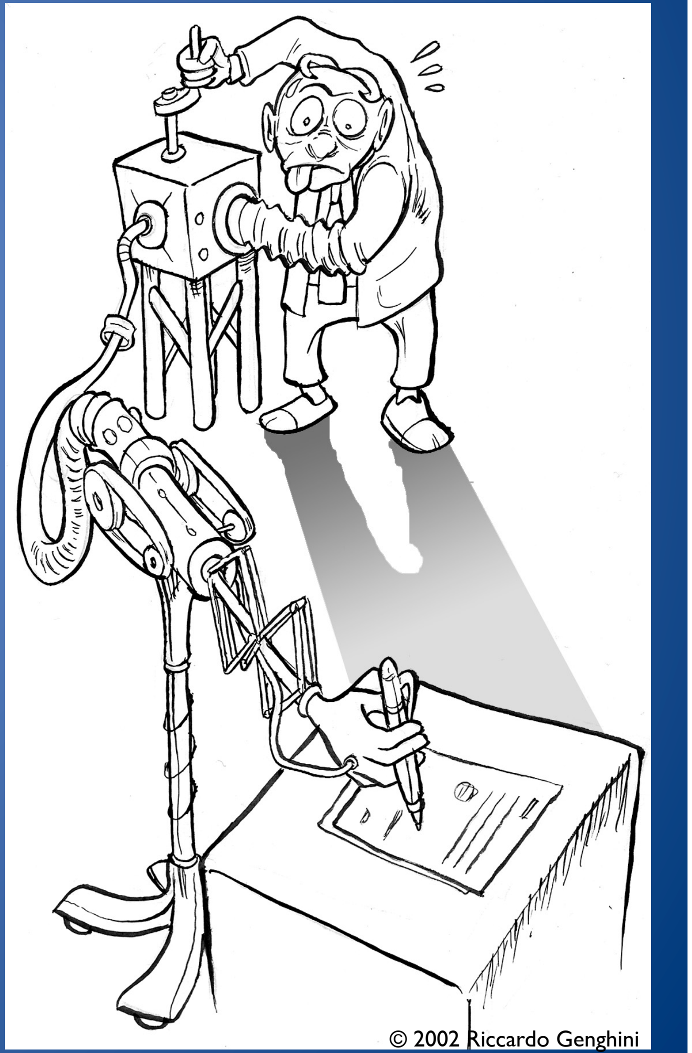
- QS: (quite) trustworthy identification of the signer and tamper proof document. No WYSIWYS.

© 2014 STUDIO GENGHINI & ASSOCIATI

4 WHAT ARE ELECTRONIC SIGNATURES?

They are substantially very different from handwritten signatures:

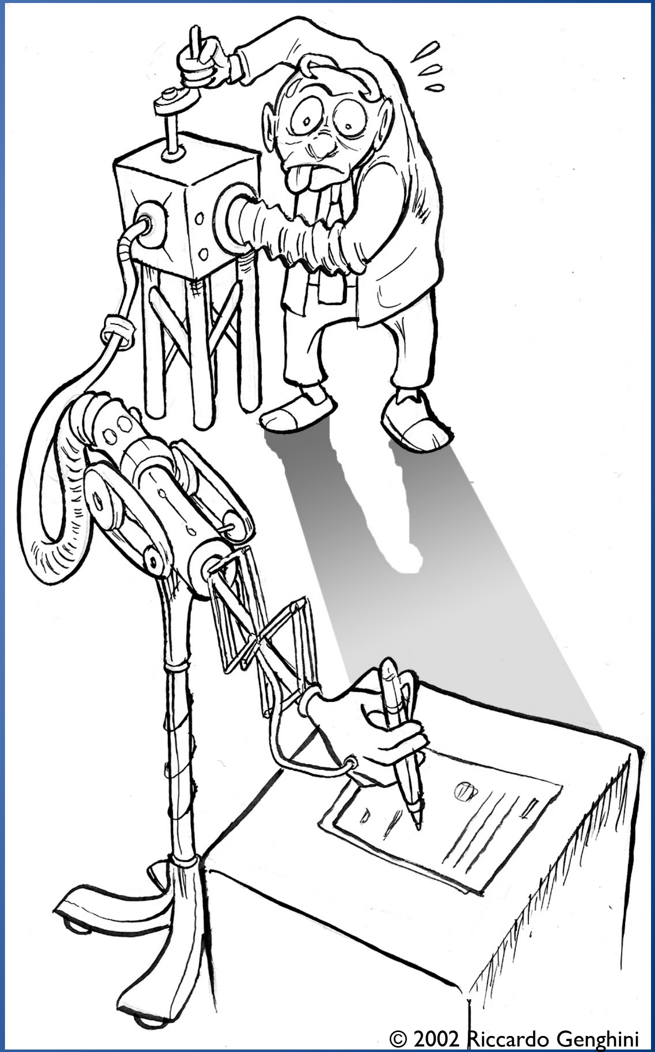
- no direct perception/control of the document
- no direct control of the signature creation process
- need to trust in one or more TSPs
- less secure signature creation environment
- no WYSIWYS...


© 2002 Riccardo Genghini

© 2014 STUDIO GENGHINI & ASSOCIATI

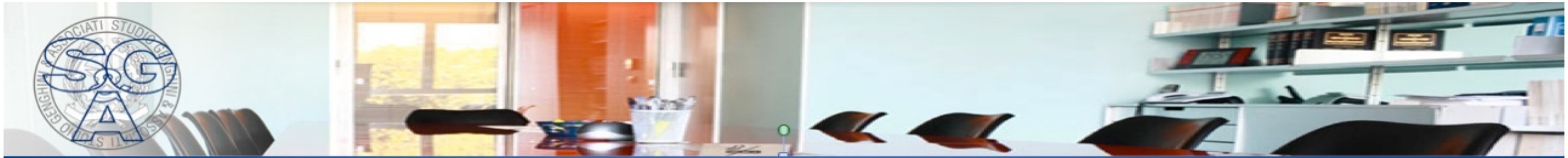
4 WHAT ARE ELECTRONIC SIGNATURES?

ELECTRONIC SIGNATURES HAVE THE SAME FUNCTION OF 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

© 2014 STUDIO GENGHINI & ASSOCIATI



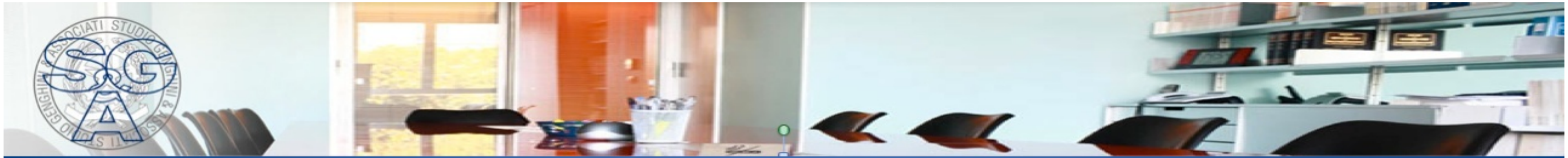
5 WHAT CAN WE DO WITH ES, AdES and QS?

- 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.

- QS: 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”.

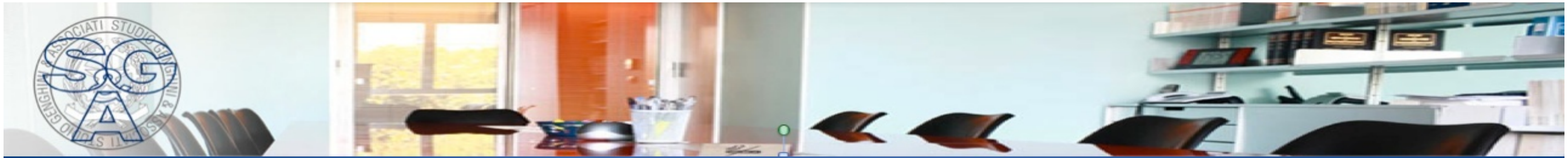
© 2014 STUDIO GENGHINI & ASSOCIATI



6 PRACTICAL USE CASES: ES

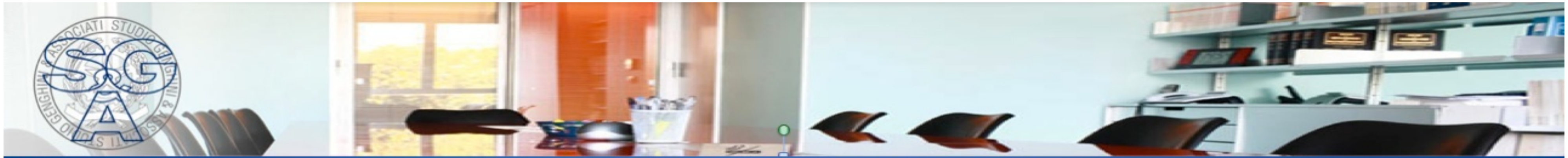
- Current e-commerce and telecommunication applications

© 2014 STUDIO GENGHINI & ASSOCIATI



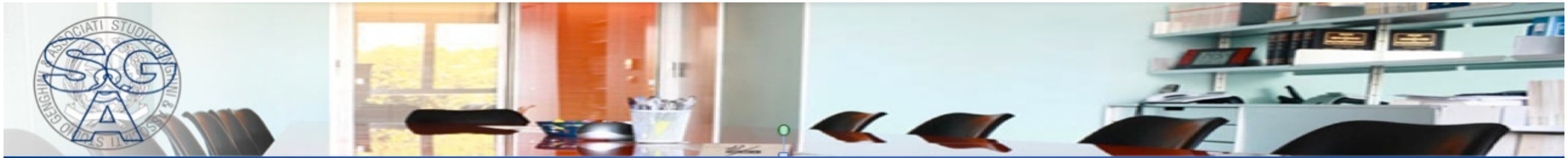
6 PRACTICAL USE CASES: AdES

- **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: QSig QSeal

- **Transactional platforms** Implemented by Notaries, Specialized companies (Docusign, etc.): combined use of Qsig, QSeals, AdES, timestamps
  Advantage: 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: QSig QSeal

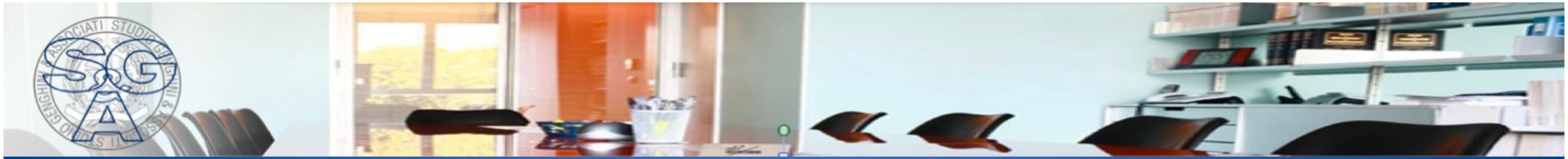
- **Trusted Wikis and Wooks** Implemented by Companies, Universities and Associations for digital learning.   Qsig, Qseal, Timestamps

  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

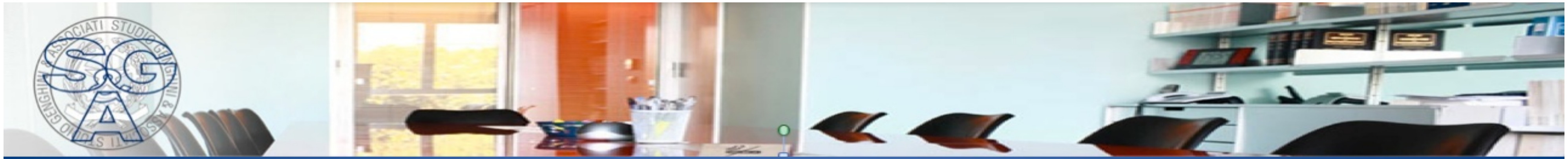
  In fact the so-called eBooks are just a software mimicking paper: an absurdity like a moto-vehicle pulled by horses. The prehistory of digital books… just try to imagine how publishing will look like, if you put into the equation interactivity, modificability, verifiability, etc…



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.

© 2014 STUDIO GENGHINI & ASSOCIATI



SG&A
Studio Genghini & Associati

Via Turati n. 29
20121   Milano   ITALIA
Tel.+39.02.637.889.900
riccardo.genghini@sng.it
www.genghinieassociati.it

© 2014 STUDIO GENGHINI & ASSOCIATI