Can PKI be made simple enough to be used by non-experts?

Signature formats and context

Antonio Lioy

(lioy @ polito.it)

Politecnico di Torino

Dip. Automatica e Informatica

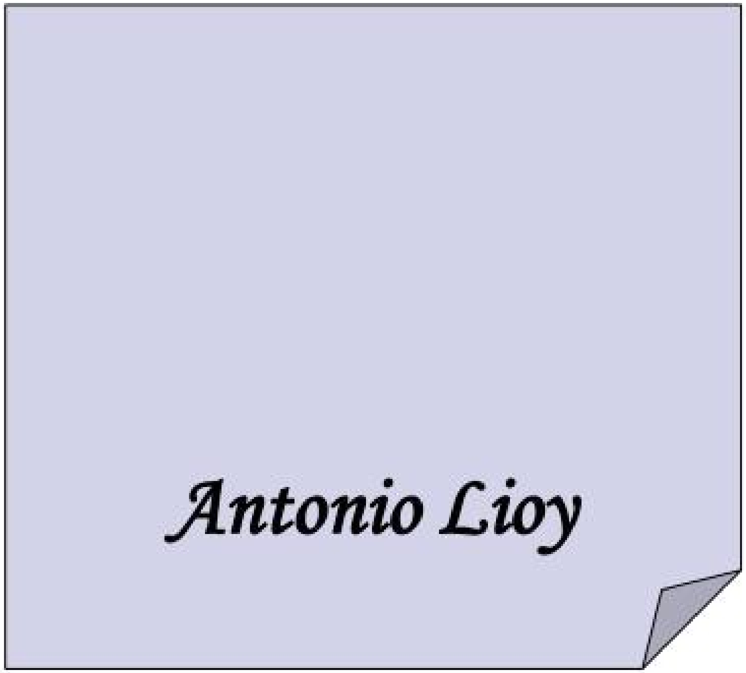
User expectation

Is it possible
to create an
interoperable signed
e-document?

Yes, if you use card X
with reader Y
via application W
… and you own a QC
from provider Z!

User perception

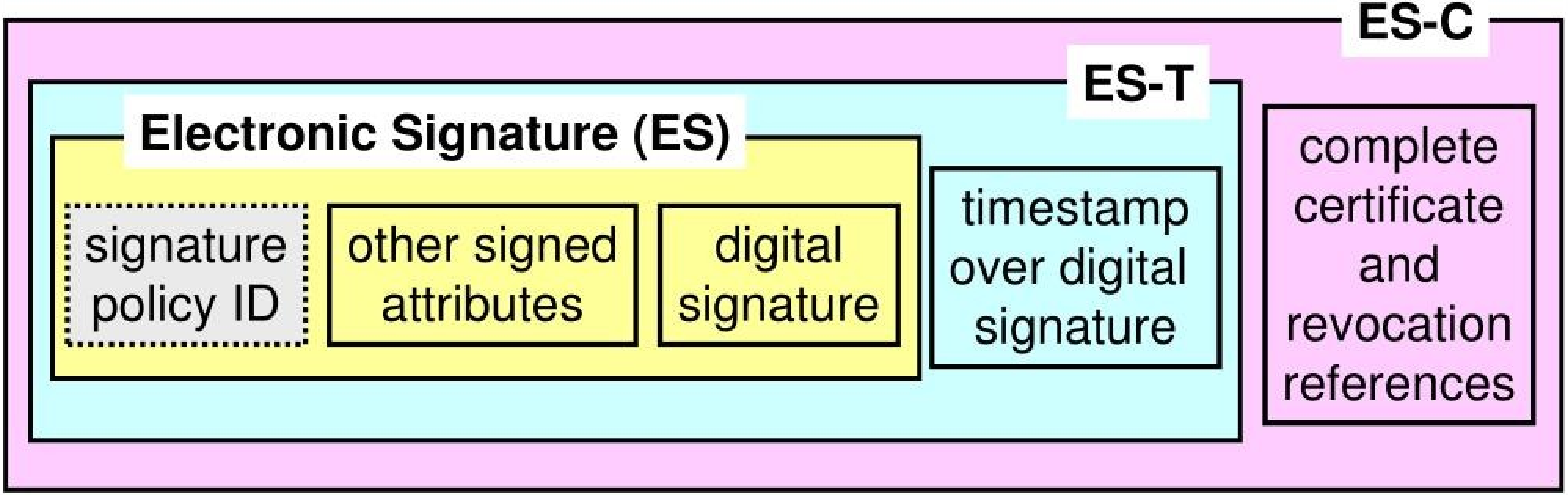
- perceived difference between signature and document
- “electronic signature? wonderful, so I can e-sign a blank e-document …”



ETSI work

- **ETSI TS 101 733 (version 1.4.0)**
- **builds on other standards:**
  - RFC-2630 [CMS] Cryptographic Message Syntax
  - RFC-2634 [ESS] Enhanced Security Services
- **great richness of options**
- **current work towards a simplification …**
- **… while retaining richness of expressivity**

ETSI ES formats


ES-C
ES-T
Electronic Signature (ES)
signature policy ID
other signed attributes
digital signature
timestamp over digital signature
complete certificate and revocation references

plus the ES-X formats …

Timestamping

- **attestation of signature time is important**
  - e.g. to check that certificate is not revoked
- **attestation can be:**
  - contained inside the document itself (e.g. TST)
  - provided externally (e.g. by the receiving system)

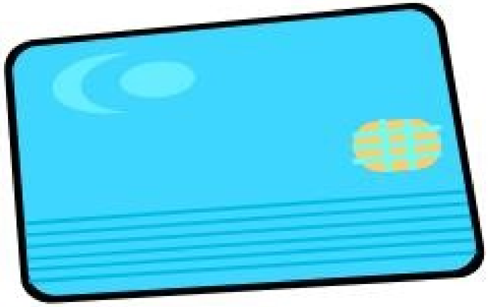
WYSIWYS

- What You See Is What You Sign
- highly desirable
- it’s a matter of the application developers
- do we really need it? let’s compare it to fine prints in paper documents …

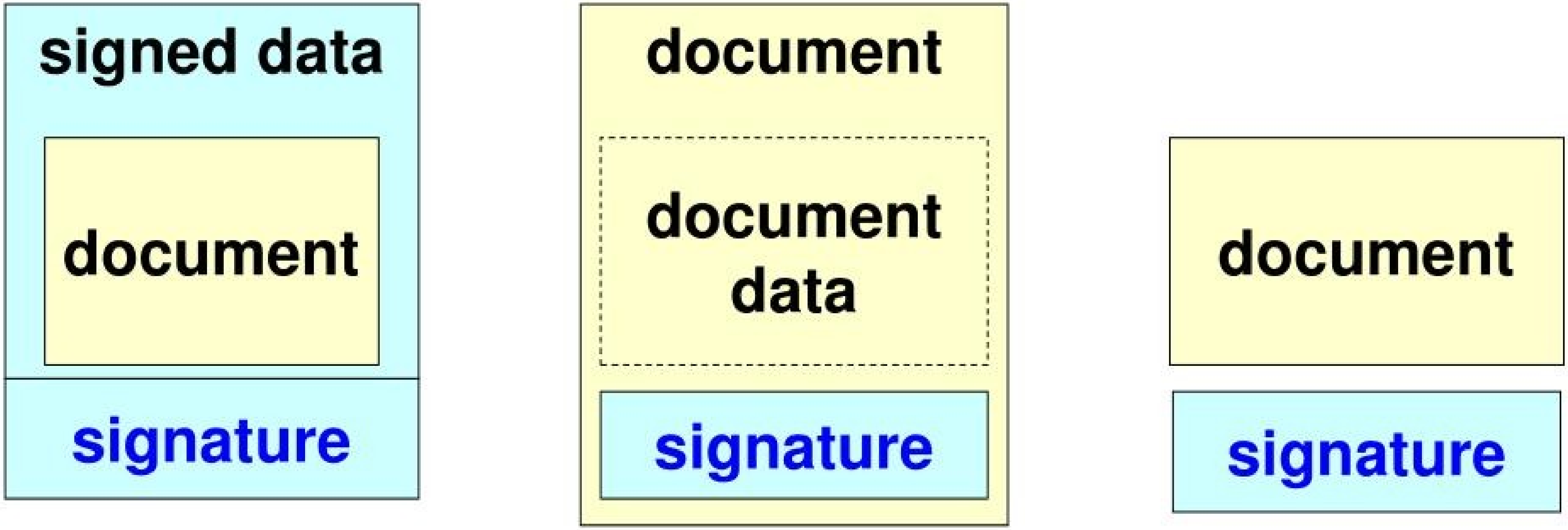
SSCD

- Secure Signature Creation Device
- better known as “smart-card”
- should be a solution to the problems of secure key storage and signature creation …
- … but too often it is THE PROBLEM for the user

- it’s a complex problem (card, reader, API, application) … but we managed it in GSM!



Signed document formats



signed data

document

signature

enveloping signature

document

document data

signature

enveloped signature

document

signature

detached signature

Conclusion

Have e-documents to be more secure than paper documents?

We run the risk to kill the idea
while looking for the perfect solution.