World Bank and MENA Countries visit to FEDICT

eID tools: trust, efficiency and online security

Sylvie Lacroix
Managing Partner
eIDs and in particular eID cards can reveal to be tremendous opportunities to secure and further boost the electronic society and supported business

- Legal framework is in place
  - E.g. Regulation EU 910/2014 on eID and trust services

- Technical framework is mature; technologies fully embedded in off-the-shelf applications.
  E.g.:
How eID makes such opportunities possible?

Physical Identification

Data capture

Authentication

Signature

Citizen XYZ
BirthDate dd/mm/yyyy
City ABC
Guarantor

Validation services

Signature

Physical identification

Authentication

Data capture

How eID makes such opportunities possible?
Technical background: cryptography and digital signatures

Card holds 2 (auth. / signature) citizen’s cryptographic key pairs

Private key: secret code used by a mathematical function to render a data unintelligible (i.e. encrypt data). 1100101

Public key: public code used by the reverse mathematical function to retrieve the initial data from the encrypted data. 0100001

The tricks:
- easy to create the pair, quasi impossible to find the secret from the public
- a different unique key pair for each citizen

If yes, was created by the person that holds the secret 1100101 matched with 0100001

Principle underlying:
- authentication
- signature (non-repudiation)
Trust in signatures relies in the guarantee that a PK \texttt{0100001} belongs to a particular citizen.

\(\Rightarrow\) an entity, trusted by the community (e.g. hired by government), called Certification Authority, certifies the link \{public key – citizen\} in a PK Certificate.

- The certificate is a signed statement by the CA
- The CA’s signature is trusted because the CA’s key is published in official journal, e.g.
- The CA is empowered to check citizens’ info (e.g. Nat. Reg. DBs)

Trust in cert. relies in the quality of the CA & certification services:

- \textbf{CA policies}: good cryptography, CA devices, user device (to protect the private key), trusted personnel, possibility to revoke and publish revocation status to verifying parties (i.e. validation services), insurances, ...

Trust in CA policies relies in the level of assurance on the CA (\textit{audit} – legal framework)
EU Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market, a new legislative framework for eID, e-signatures and other trust services.
Electronic signature: data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

**Advanced electronic signature:**
(a) is uniquely linked to the signatory (PK pair unique)
(b) is capable of identifying the signatory (PK certificate);
(c) is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control (PK protected in a secure device); and
(d) is linked to the data signed therewith in such a way that any subsequent change in the data is detectable (PK intrinsic: signature is not verified if data is changed).

**Qualified electronic signature:** is an AdES with a qualified certificate and a qualified signature creation device (e.g. a smart-card that is certified against certain protection profiles).
Where legal and technical meets (2/2)

Digital signature: suitable technology for electronic signatures equivalent to handwritten, web authentication and seals for legal persons, \textit{provided}:
- CA, issued certificates and signing devices are \textit{qualified}

To validate and trust the qualification in a machine processable way through:
- EU Trusted Lists of supervised CAs, established by Member States
- & List of the Lists as EU Central point of access.
Sweet dream or reality?

Very big stakeholders « talk » PKI, eIDs and smart-cards since many years (MS, Apple, Adobe, ...)

Very big stakeholders develop the integration with EU Trusted Lists and endorse EU Standards for CA Audit

*Trusted lists and trust stores are similar concepts that can be used in parallel. E.g.:

- need to check that an AdES is qualified ➔ tec.: is the certificate qualified?
  ➔ your apps check TL
- need to have secure surf ➔ tec.: is the certificate « EV »? ➔ « green bar » in browser (the CA is recognised by the browser; present in trust store)

... browsers's trust store criteria can be Q_CA_audit (ETSI 101 456 – 102 042 and up-dates accepted)

A lot of open sources tools are available (e.g. from EC) for SMEs to integrate eSignature and Authentication in a fully trusted and legal way.

... definitely a reality – no excuse for not using these tools
Questions ? - Contact information

Olivier DELOS (CISSP, CISA)
Mobile: +32 477 78 79 74
Email: olivier.delos@sealed.be
Web: www.sealed.be

Sylvie LACROIX (CISA)
Mobile: +32 477 78 79 75
Email: sylvie.lacroix@sealed.be
Web: www.sealed.be