# Digital signature : regional opportunity to ease trade exchange within MENA

Exploratory seminar on e-signatures for e-business transactions in MENA, AMMAN, November 11th 2013

Thibault de Valroger

OPENTRUST

# Digital Signature market dynamics

- High growth trend at worldwide level
  - +48% yearly growth estimated by Gartner in 2012

- 3 approaches commonly observed :
  - High-end smart card based solutions : depends on massive equipment => initial investment
  - Intermediate server based + authentication solutions :
    - Easy to deploy for Service providers and operated by certified Trust Service Providers
    - Real success in BtoC (France, Italy,  Austria, Nordics)
    - Compliant with EU advanced signature
  - Low-end solutions for low-risk BtoB documents (for instance signing an NDA) ; no clear liability

# EU 1999/93 Directive (1/2)

- Establishes digital signature *admissibility as evidence in legal proceedings within the EU*
- Distinguishes 3 levels
  - Advanced Signature
  - Advanced Signature based on Qualified Certificate : same as Avanced signature but with strenghened level of security
  - Qualified Signature (meaning same requirements than above + smart card, generically called « SSCD ») : grants presumable reliability
- Requires mutual recognition of qualified signature for CSP having proved compliance on a *voluntary accreditation* basis (i.e. certification)

# EU 1999/93 Directive (2/2)

- International cooperation is covered :
  - Qualified certificate may be issued outide EU and are then recoginzed under the same conditions
  - Countries outside EU may use qualified certificates issued by a CSP based in EU
  - Certificates issued outside EU under different conditions may also be recognized but according to bilateral agreement

- The eIDAS regulation project should renew those principals, with coverage by an agreement between the country and the UE under article 218 of TFEU

# Digital Signature regulatory dynamics

- European eIDAS regulation project (2014-2015)
  - Regulation (rather than Directive) = good for interoperability, good for liability
  - Evolution of technologies taken into account
    - Server based e-signature
    - Update of requirements in security and cryprography
  - New services should be covered by the regulation
    - Electronic seals
    - E-Delivery services (certified / registered e-mail)
    - Timestamping
  - More maturity in concepts and models
    - Separation between digital identification and digital signature
    - Multi-acceptance models
    - Possibility of cross recognition of lower levels than qualified signature

# Some examples in MENA
# 2 levels accreditation scheme

## Morocco

National eSignature law : YES
Accreditation authority : ANRT
CSP : Only one (Barid eSign)
National citizen eID : No
Recognition of foreign CSP : YES under bilateral or multilateral agreement

Class 3 very close to qualified signature and grants presumable liability.
Class 2 equivalent to advanced signature.

## Algeria

National eSignature law : YES
Accreditation authority : ARPT
CSP : Not yet
National citizen eID : No
Recognition of foreign CSP : YES under bilateral agreement

# Some examples in MENA : National CSP scheme

## Tunisia

National eSignature law : YES

National CSP : ANCE (can certify other CA)

National citizen eID : No

Recognition of foreign CSP : YES under bilateral agreement (through ANCE)

## Oman

National eSignature law : YES

National CSP : ITA (can certify other CA)

National citizen eID : YES

Recognition of foreign CSP : YES under ministerial decision





OPENTRUST

# Open questions and challenges

- How to ease mutual recognition of Digital signature within EU / MENA ?
  - Need is mainly on BtoB (less for citizens) => multilateral agreement on CSP cross recognition ?

- How to harmonize evolution of regulations ?
  - Needed to adapt to technology evolution as well as business needs


# Thanks for your attention.

**11-13 rue René Jacques - 92131 Issy-les-Moulineaux Cedex - France**

**+33 (0)1 55 64 22 00 - www.opentrust.com**