



eIDAS in the Cloud

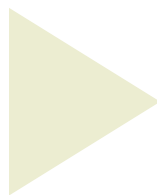


CRYPTOMATHIC
Conference - 22 November 2016

10+ Years Experience

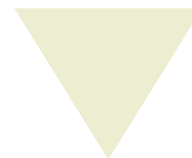
From EC Directive to eIDAS

Strong Authentication &
Electronic Signature Option
Requested by Luxembourg
Public and Banking Sector



2005 LuxTrust Founded
Trusted 3rd Party
PPP of Major LU Banks &
and Government
Cost Sharing for PKI-Based
Trust Services Provision

2009 Accredited as Trust
Services Provider in
Europe



... and beyond for
Code Signing & Website
Certificates

Monitored by Payment Sector
Supervision Body
CSSF



10+ Years Experience

Our value chain

- ▶ Strong authentication for banks and public sector in LU
- ▶ Advanced signatures & EIDs for public and private sector
- ▶ Qualified Timestamping
- ▶ Mass signature services
- ▶ Delegated RA Network → Banks & Town Halls & Board of Trade
- ▶ Real Time Enrollment & Revocation → 10-15 Minutes
- ▶ Multilingual Service Desk → 6 Languages



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

10+ Years Experience

The use cases

Access to Online Banking and Webstores

Transaction Approval & Signing

Online Tax Declaration

Secure activities in citizen one stop shop

Secure access to intranet of organizations

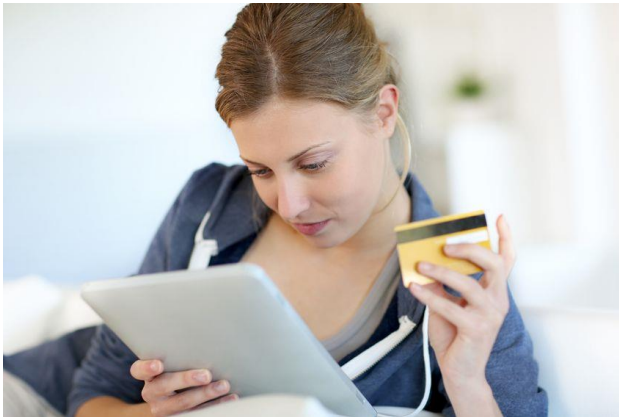
Classic PKI Cards & Roaming PKI

Any User Device → 1 Certificate for Any Service



The Challenges

Impact of mobile internet



**Handhelds replace desktops
for surfing, buying, selling, banking**

Desktops still used by professionals



**No matter which equipment is chosen
Achieve the same user experience**



The Challenges

Impact of deployed software

- ! Platform dependency creates a maintenance nightmare
- ! Customers & users handicapped by platform updates
- ! Provider has to maintain all software variants in time
- ! Life cycle management and evolutions complex for all parties

Remove client platform dependencies

Decouple service life cycle dependencies



The Challenges

Impact of chip-based devices

Smartcard access limited due to platform dependencies

Smartcard usage impeded by need for deployed software



Promote unconnected user devices

Use central authentication & signature creation



The Challenges

Impact of PSD2

Dynamic linking required for authentication data

Segregated channel required for visualizing transactions



Use devices with own channel, display and keyboard



The Vision

Trust services in the cloud



A platform-independent services portal



Easy to integrate based on adopted standards



Relieving customers of PKI complexity



Relieving customers of service evolutions



Relieving users of access constraints

The idea of ORELY was born



The Benefits

For integration

Simple integration using adopted XML-based standards



Coding examples for individual development platforms



Direct interoperability with third-party VPN products



No specific competence needed → No PKI expert needed

Offer adopted by small & medium enterprises



The Benefits

For maintenance



Customers not impacted when features are added

New features do not generally need application upgrade

Application and service life cycles decoupled

Multi-platform support without software maintenance hell

Decreasing maintenance load in favor of service evolution



Life cycle decoupling increases productivity on each side



The Benefits

For usage and compliance

Unconnected devices → Increased security & availability

Dynamic Linking → Compliance with PSD2 and stronger sole control

Seamless mobile support → Augmented user convenience

Responsive design → Same experience on any platform



Perfect life style
alignment
increases adoption



The Services

Strong authentication

- ▶ Support for various authentication mechanisms
- ▶ Enabling web applications and corporate VPN appliances
- ▶ Device selection based on desired assurance level
- ▶ Selection based on available user equipment
- ▶ Device management completely delegated to LuxTrust
- ▶ All PKI aspects completely managed by LuxTrust
- ▶ Customer needs to launch an authentication request only



The Services

Advanced electronic signatures

- ▶ Support for interoperable European signature standards
- ▶ User device selected based on desired assurance level
- ▶ Selection based on available user equipment
- ▶ Device management completely delegated to LuxTrust
- ▶ All signature & validation aspects completely managed
- ▶ Enabled by Cryptomathic Signer based on Thales HSMs
- ▶ Customer needs to launch a signature request only



THALES



CRYPTOMATHIC

The Conclusion

Facilitate eIDAS services via the cloud

- ✓ Cloud enables decoupling of concerns
- ✓ Cloud enables decoupling of service life cycles
- ✓ Cloud enables decoupling of platforms
- ✓ Cloud makes trust services simple and convenient
- ✓ Cloud can be eIDAS-compliant + mobile + qualified



500.000 USERS | VALIDATIONS IN OVER **170** COUNTRIES



Thank you!



CRYPTOMATHIC
Conference - 22 November 2016

