The vision of future trends and technologies
Digital Trust

IdP

Supporting drivers

Supporting standards

Authentication Interface
Sign Transaction Interface
Sign ID Token Interface

“trust providers”

Key Vault (HSM) Component
Participant Manager Component

General Data Protection Regulation
QUALIFIZIERTER VERTRAUENS-DIENSTLEISTER (in EU)
Payment Services Directive (PSD2)
OpenID Connect

NEM ID
InfoCert
BankID

CRYPTOMATHIC
Signer and WYSIWYS in a nutshell

**Input:** Data to be signed  
**Output:** Signed data (QES level)

*In the middle:* we provide the necessary technology for the signing experience and can leverage the existing environment and procedures (KYC, IdM, DMS, Auth services etc.)

See demo [http://cryptobank.cryptomathic.com](http://cryptobank.cryptomathic.com)
Secure Audit logs: Non repudiation

- Provide an extensive audit trail where you can demonstrate that:
  - The user was authenticated with an adequate assurance level (Substantial or High))
  - The DTBS was visualised by the user before he could commit to it
  - The data to be signed is protected in integrity.
  - There is a sole control channel for carrying the DTBS to signature and for executing the signature operation.
  - The user has means to validate the operation
How to ensure a loop of trust and non repudiation

• Primary objectives
  • Ensure that the DTBS is actually protected in integrity and visualised over a trusted viewer before being effectively signed under user’s sole control with an adequate assurance level (Substantial or High)
  • Provide an extensive audit trail to ensure non repudiation of origin and emission
  • The user has means to validate the signature operation
  • The signature reaches the QES level

• Response to threats
  • Counter MITM attacks
    • Between Client and WYSIWYS server
      • SSL/TLS using White lists embedded in the client
    • Between Client and Signer
      • Session encrypted using SCK over TLS. Embeds hash into SAD
    • Man in the browser
      • Little impact since we cannot inject new documents
      • Client JS code obfuscation strengthened with SCK rolling
    • Reuse federated identity credentials
      • Use of nonce to avoid replay attacks
      • Authorisation of a signature operation is bound to document hash

Signer
  • Terminating user’s sole control in SAM
  • Managing user’s keys
  • Verifying SAD and validating IdP authenticity

WYSIWYS Server
  • Receiving doc from trusted source
  • Outputting signed doc to trusted source

Client
  • Displaying doc over trusted viewing
  • Ensuring user commitment and sole control
Turnkey solution

TSP Domain (some components can be spread on the DA side)

User Domain (w/o desktop client)

Cryptomathic WYSIWYS Client (in Browser and/or Mobile Apps)

WAF

IdP

Cryptomathic WYSIWYS Server

Cryptomathic Signer

User Management with RA Services

Signer RA

Cryptomathic Authenticator

OSCP Service

Time Stamping Service

Archival

CA
Future trends and technology

Guillaume Forget
+49 162 2946885
Guillaume.Forget@cryptomathic.com

Cryptomathic 2017 - All rights reserved