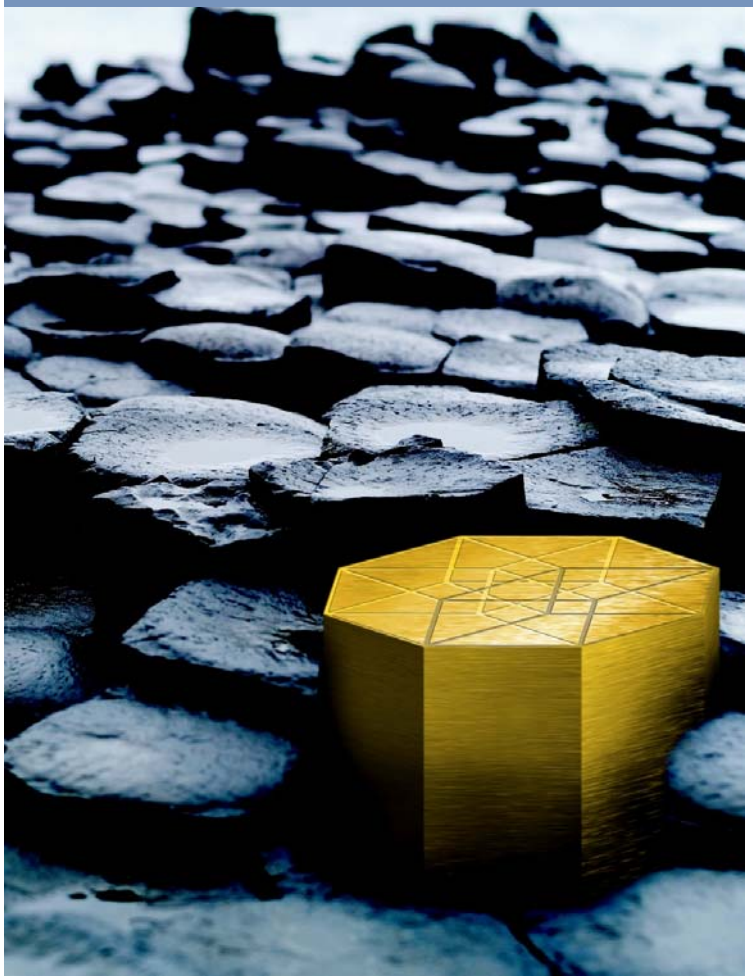
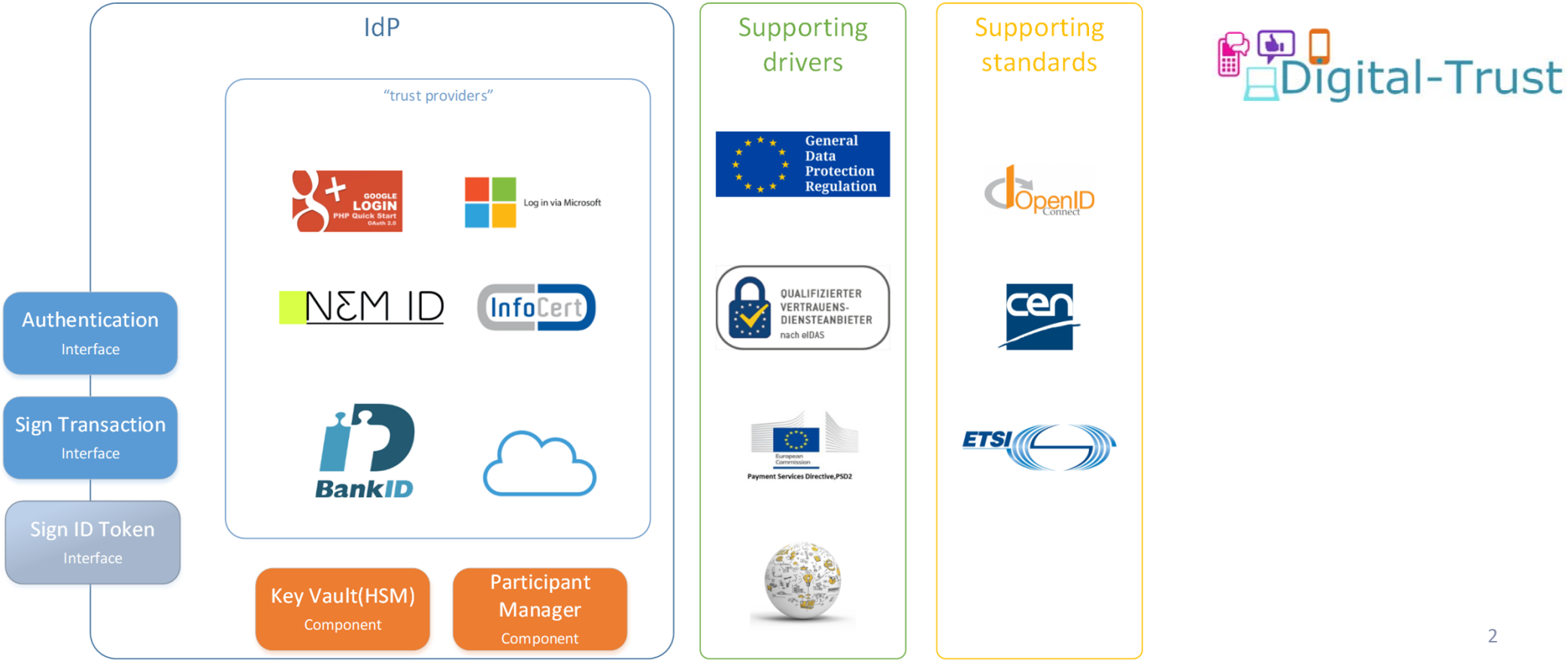
CRYPTOMATHIC



The vision of future trends and technologies

CRYPTOMATHIC

Digital Trust



Digital-Trust

CRYPTOMATHIC

Signer and WYSIWYS in a nutshell

Input: *Data to be signed*

Output: *Signed data (QES level)*

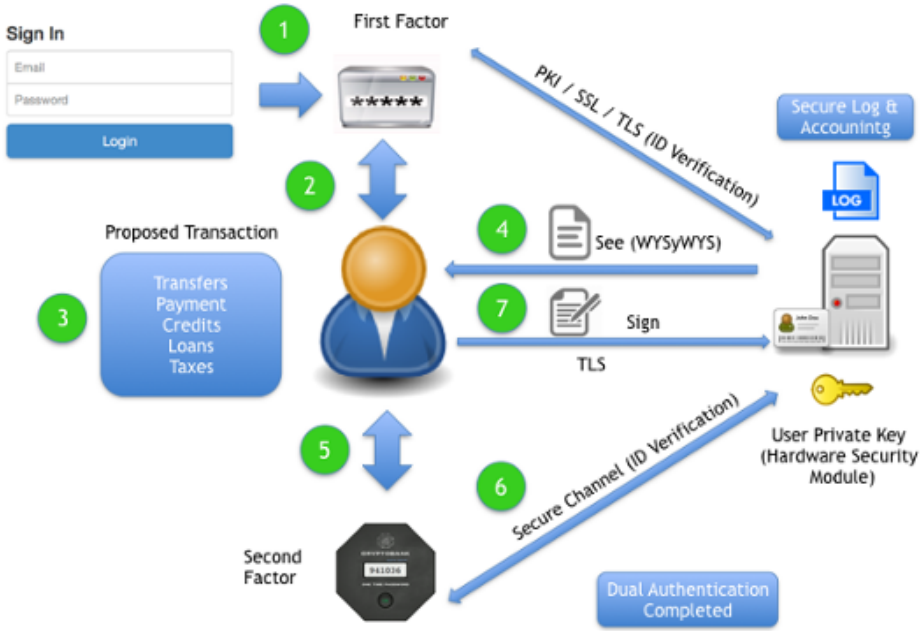
In the middle: *we provide the necessary technology for the signing experience and can leverage the existing environment and procedures (KYC, IdM, DMS, Auth services etc.)*

See demo http://cryptobank.cryptomathic.com

CRYPTOMATHIC

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

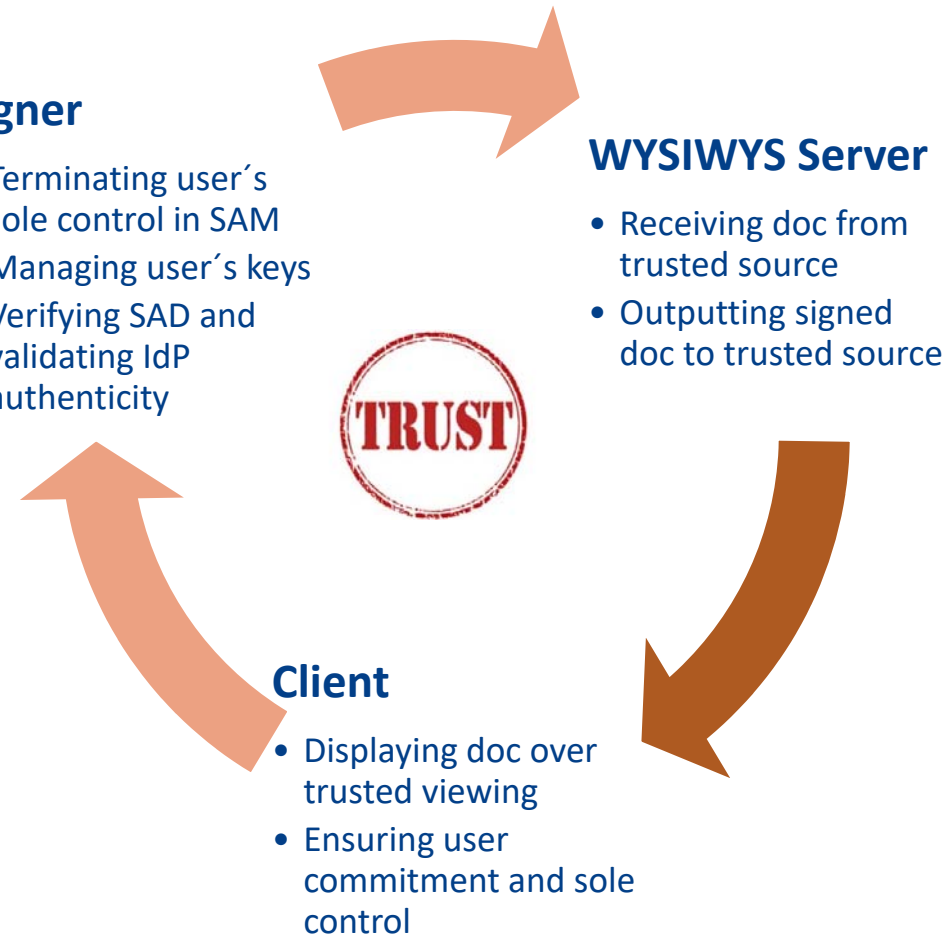


CRYPTOMATHIC

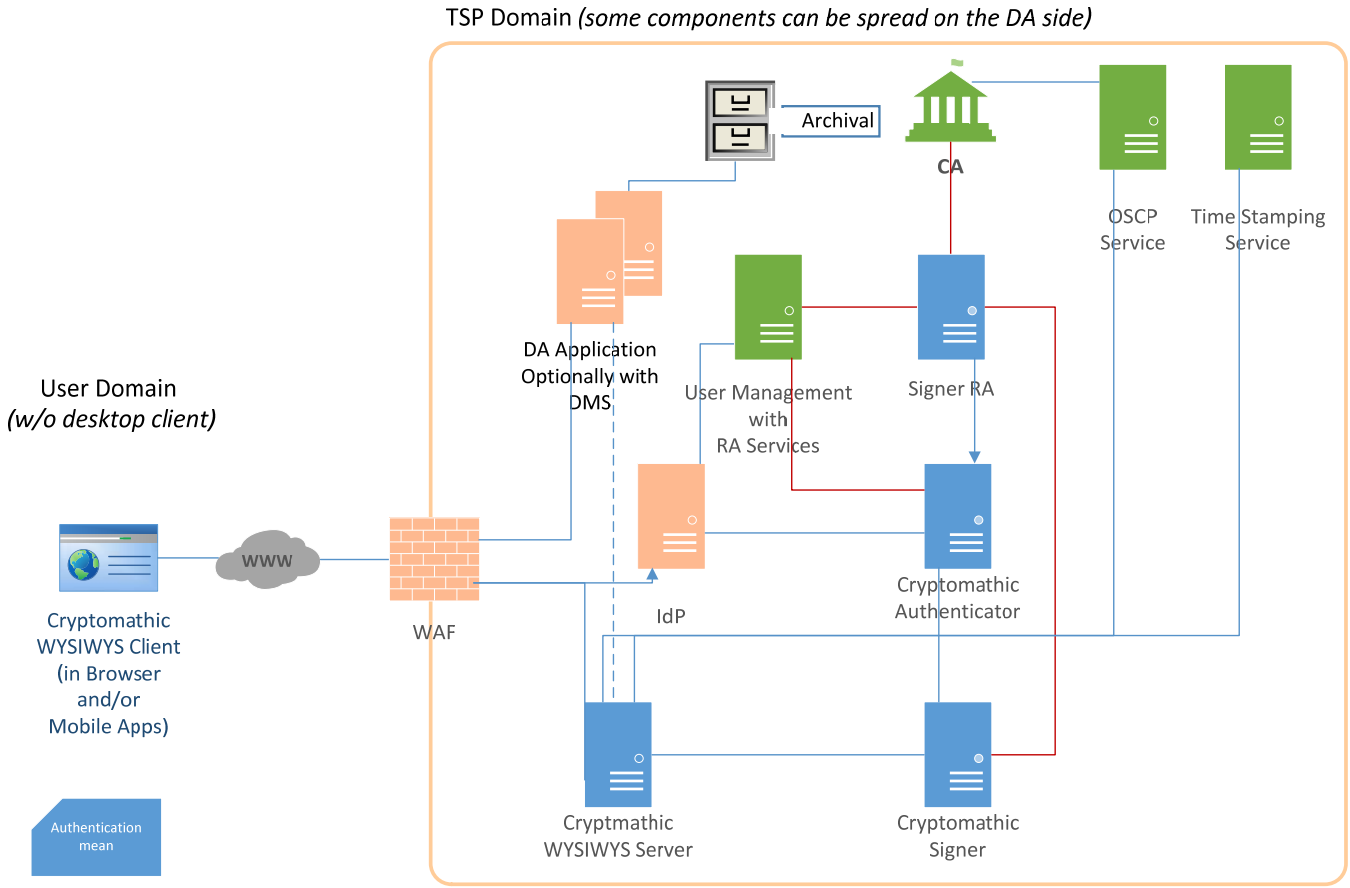
How to ensure a loop of trust and non repudiation

- 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

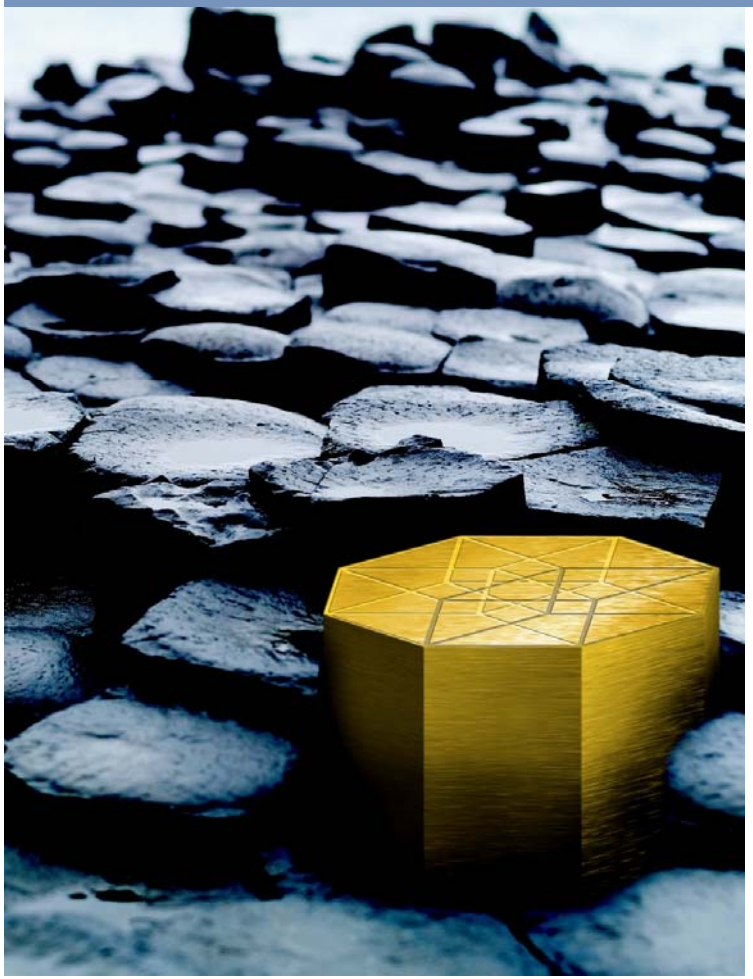
- Response to threats
  - Counter MITM attacks
    - Between Client and WYSIWYS server
      - SSL/TLS using White lists embedded in the client
    - Between Client and Signer
      - Session encrypted using SCK over TLS. Embeds hash into SAD
    - Man in the browser
      - Little impact since we cannot 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



Turnkey solution



CRYPTOMATHIC



Future trends and technology

Guillaume Forget

+49 162 2946885

Guillaume.Forget@cryptomathic.com