Intro to central signing and Cryptomathic Signer

A new signing experience

What do these 2 things have in common?

Signature

The traditional function of a signature is to give evidence of the provenance of a document **(identity)** and the intention **(will or intent)** of an individual with regard to that document.

We primarily sign for the benefit of a **relying party.**

Protection and security are only valuable if they do not cramp life excessively.

[Carl Jung, Psychiatrist]

What is the key to success for digital signature

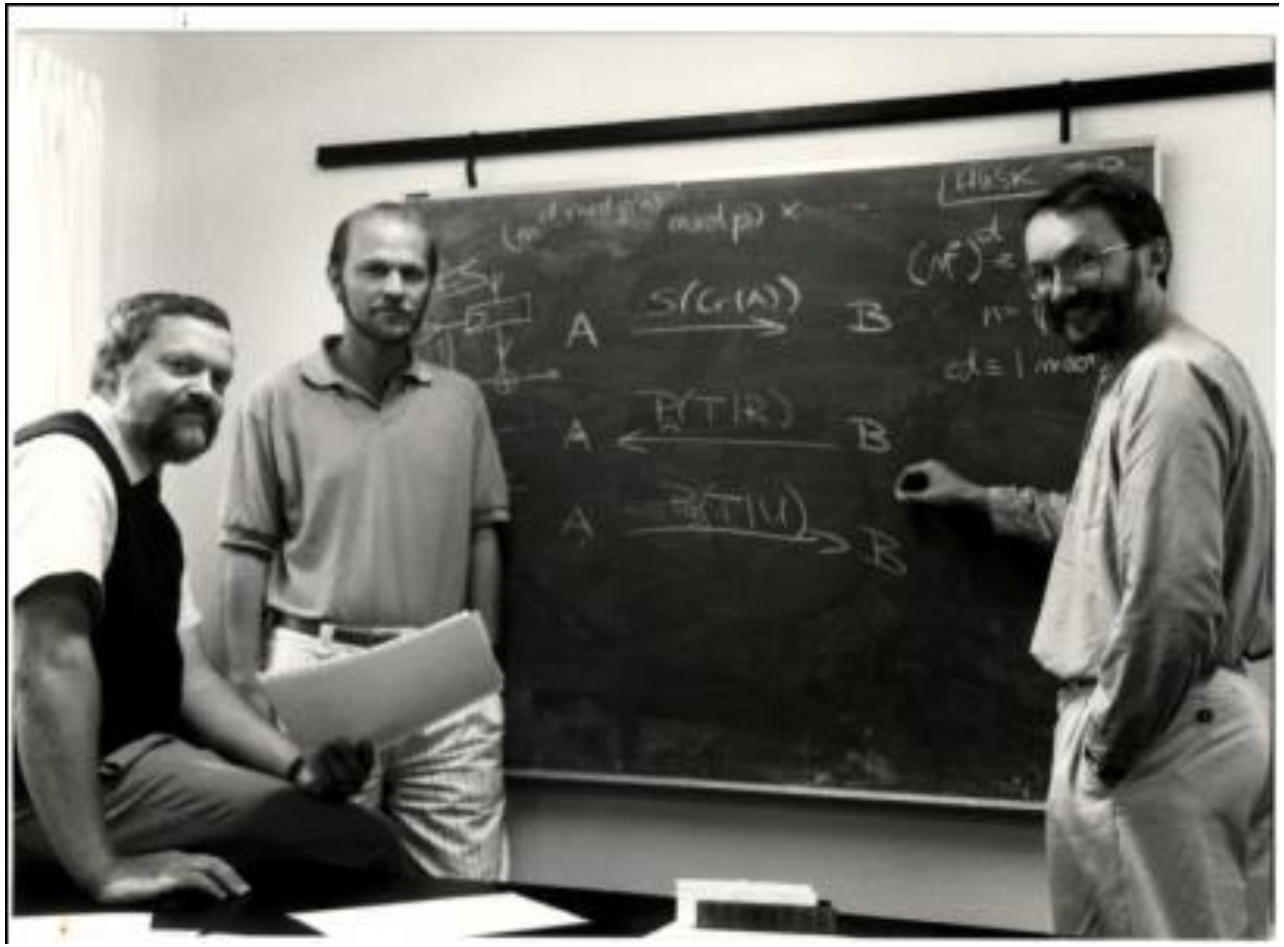
- Quoting one of our key clients going through digital transformation

> *In the space of 12 months, we changed the way people have been signing for centuries, so you can expect some friction. This requires equivalence with the legacy world to allow for the most trustworthy step to be digitalised.*

- Indeed, digitalisation induces a new trust paradigm
  - where the will or intent applies to a digital document
  - where the identity is also digitalised. (signing is brought to the cloud)
  - where the boundaries of the trust ecosystem become very loose.

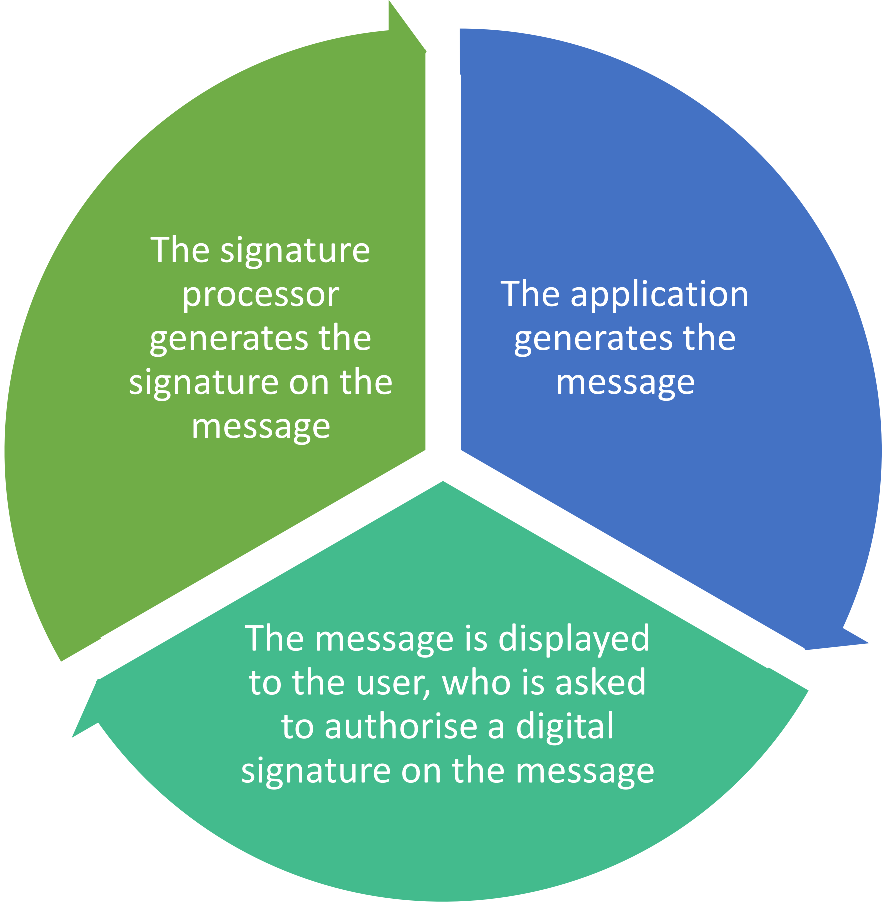
Back to the late 80´s and 90´s

- Aarhus University:
  - Peter Landrock Prof (Department of Mathematics)
  - Jørgen Brandt Associate Prof (Departments of Computer Science and Mathematics)
  - Ivan Damgaard Prof (Department of Computer Science)



Pioneering WYSIWYS

When generating a signed message the three components will come into play as follows

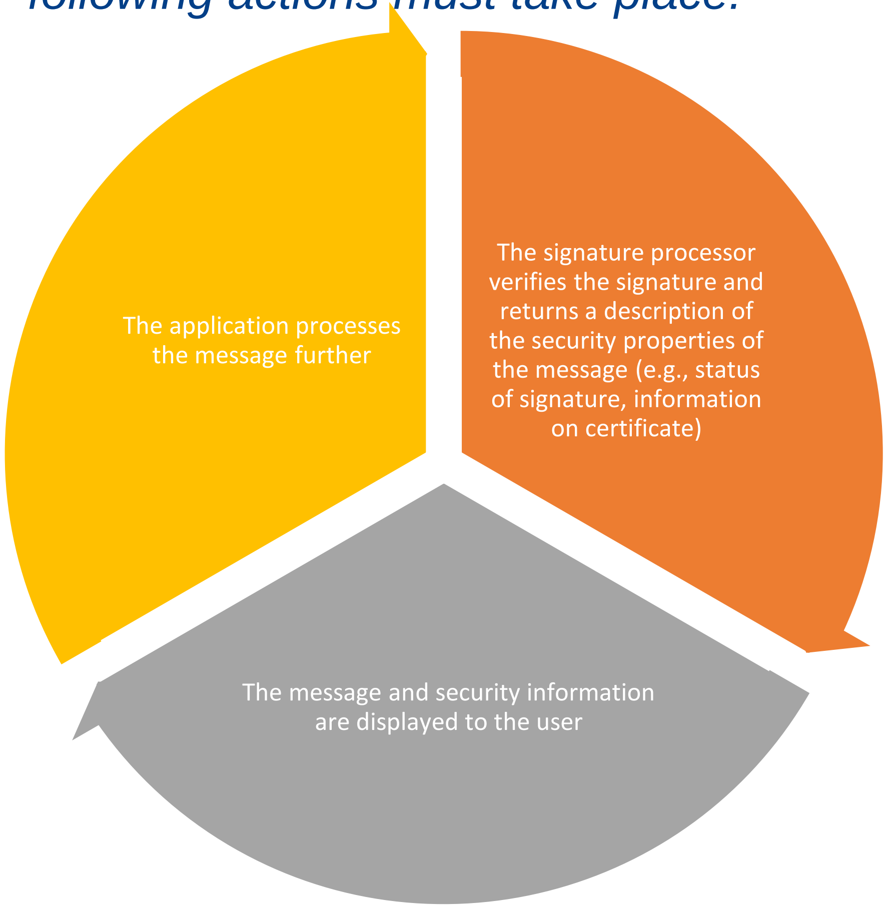


The application generates the message

The message is displayed to the user, who is asked to authorise a digital signature on the message

The signature processor generates the signature on the message

When receiving a signed message the following actions must take place:



The signature processor verifies the signature and returns a description of the security properties of the message (e.g., status of signature, information on certificate)

The message and security information are displayed to the user

The application processes the message further

WYSIWYS in a nutshell

The UI constitutes a channel between the user and the other two components. In order to ensure WYSIWYS, it is essential that the channel between the user and signature processor is secure. (authenticity of message and sender):

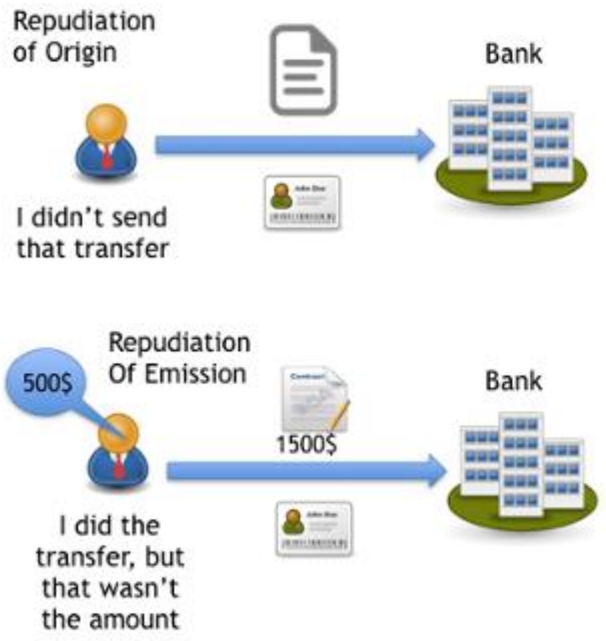
- when a request for authorisation is shown to the user, the user must be certain that the request comes from the right application and has not been changed.
- when the signature processor receives a document to be signed it must be ensured that this is the right document and that the signature has been authorised by the right person.
- When the result of a verification of a signed document is shown to the user, the user must be assured that the information is correct (right document, correct verification of security information).

CRYPTOMATHIC

The need to provide non-repudiation

Non repudiation is a *security service that provides protection against false denial of involvement in a communication.* In banking, the ECB differentiates:

- **Non-Repudiation of Origin (NRO)** makes a link between the message and the sender of the message. It can provide legal evidence that a person in fact sent the message
- **Non-Repudiation of Emission (NRE)** makes a link between the sender of the message and the content of the message. It can provide legal evidence that a person sent that specific message


Repudiation of Origin
Bank
I didn't send that transfer
500$
Repudiation Of Emission
1500$
Bank
I did the transfer, but that wasn't the amount

CRYPTOMATHIC

Conceptualising Signer - back in 2001

- Cryptomathic engineered the first *EasySign* solution with central key escrow
- And sold it to SDC

Before deciding on EasySign SDC in Denmark (the co-developer and first customer) had KPMG evaluate the applicability of EasySign in a solution that requires non-repudiation. The report was positive.

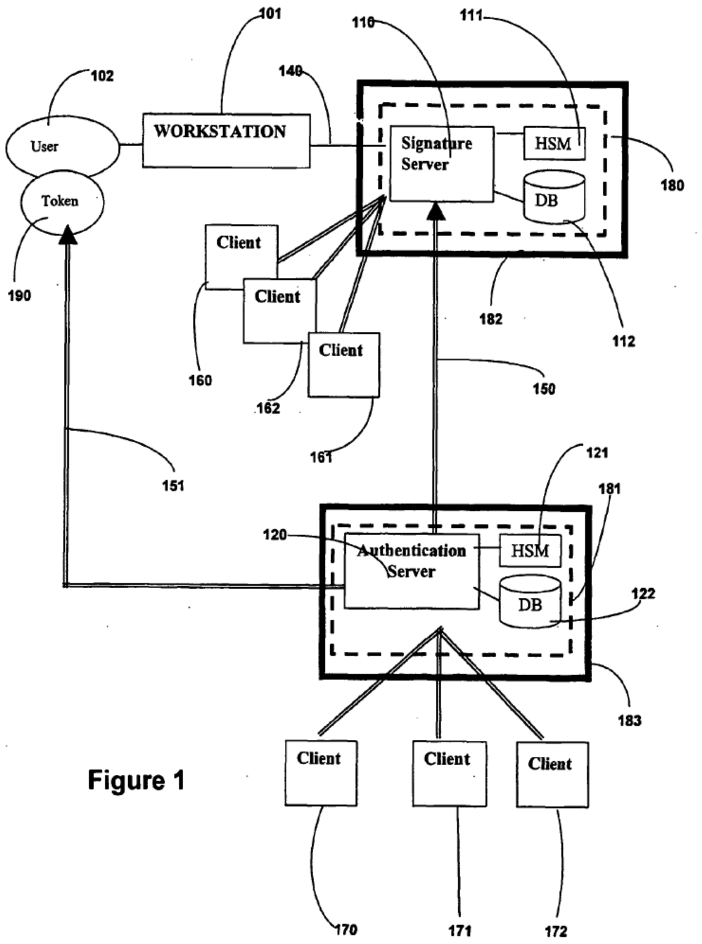
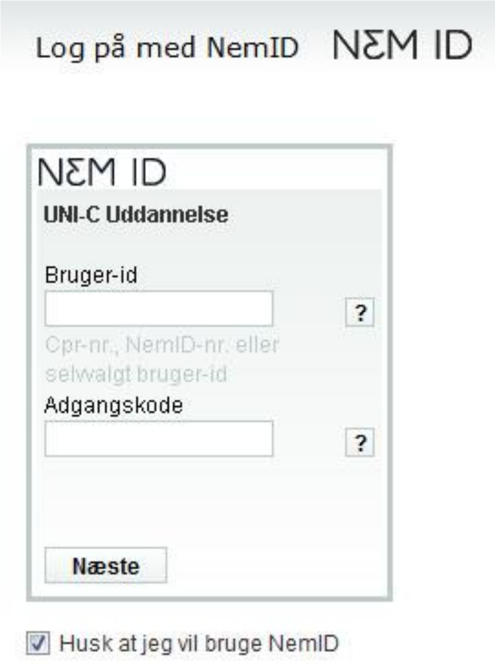


Figure 1

NemID – probably the most popular deployment



Log på med NemID NEM ID

NEM ID

UNI-C Uddannelse

Bruger-id

□ ?

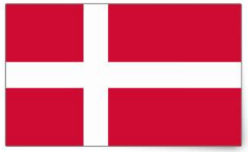
Cpr-nr., NemID-nr. eller selvalgt bruger-id

Adgangskode

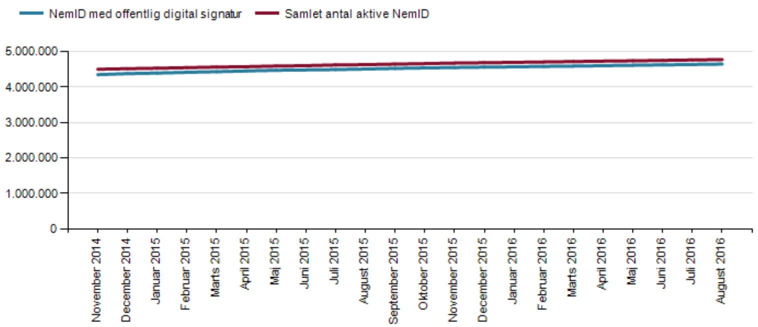
□ ?

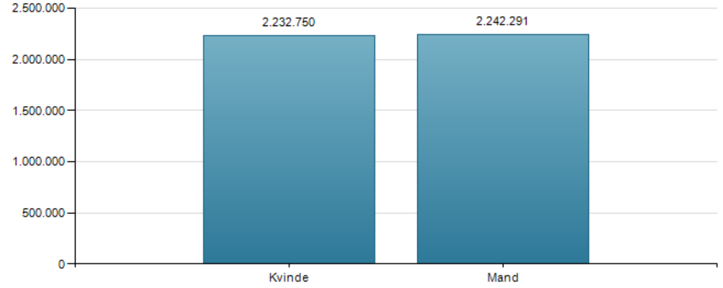
Næste

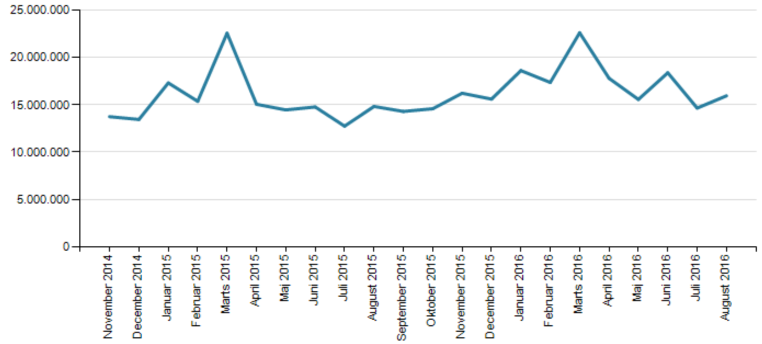
☑ Husk at jeg vil bruge NemID



NEM ID

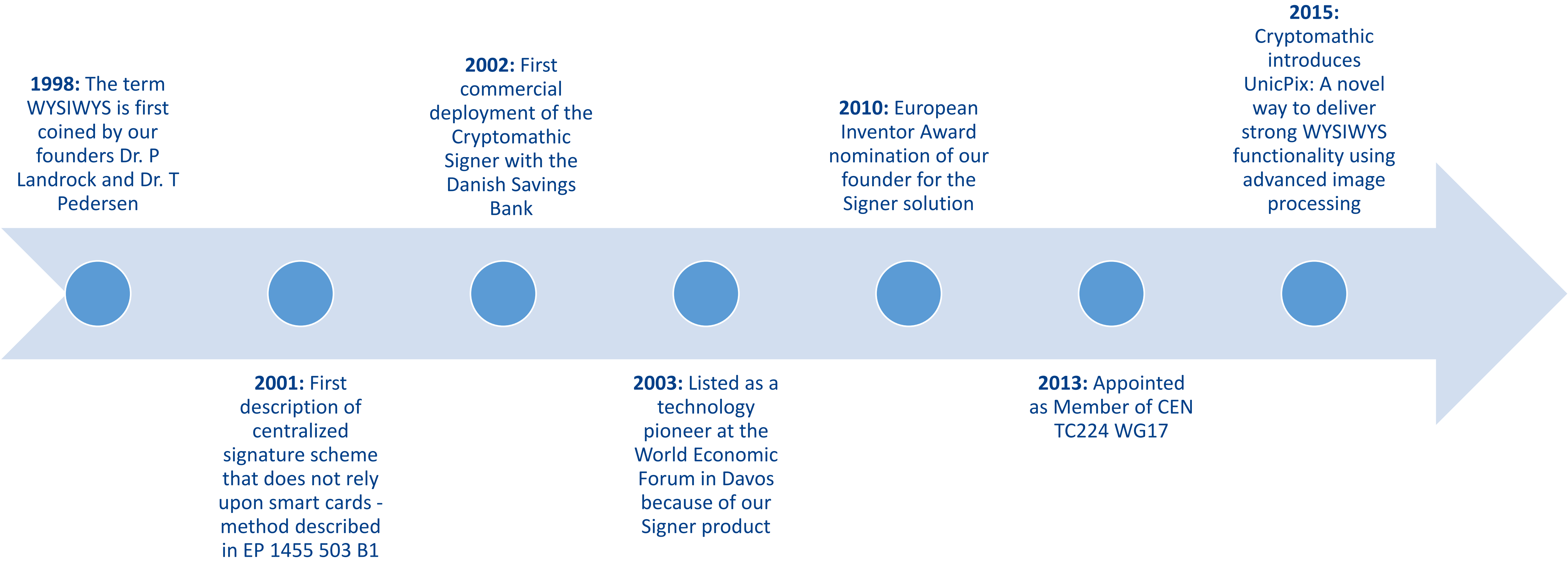






CRYPTOMATHIC

Cryptomathic and central signing



1998: The term WYSIWYS is first coined by our founders Dr. P Landrock and Dr. T Pedersen

2001: First description of centralized signature scheme that does not rely upon smart cards - method described in EP 1455 503 B1

2002: First commercial deployment of the Cryptomathic Signer with the Danish Savings Bank

2003: Listed as a technology pioneer at the World Economic Forum in Davos because of our Signer product

2010: European Inventor Award nomination of our founder for the Signer solution

2013: Appointed as Member of CEN TC224 WG17

2015: Cryptomathic introduces UnicPix: A novel way to deliver strong WYSIWYS functionality using advanced image processing

Current trends/threats call out for signing

Goal: address augmented threats, adapted service models and new compliance reqs

Nonrepudiation of engagement: Use transaction signing to follow best ECB practice

- Use of XAdES manifest signatures applied to order transfers
- Demonstrate user sole control and intent with WYSIWYS

Paperless: Save time, money & sign remotely

- Benefit from legal force of the 910/2014 EU Regulation (eIDAS)
- Provide an end-to-end digital journey
- Provide mobility and outstanding UX

Security : Industrialised and more sophisticated attacks

- Strong authentication does not defeat Man in the browser and man in the middle attacks
- The classic PKI card turns out to be a weak device
- A strong audit trail is necessary (mandated for IRS or MAS)

technology & change management

Rapid technology switch: Provide versatile and flexible trust services

- SAML v2 authentication
- Signature service integrating with various applications
- Flexible and mobile friendly user interface (zero footprint javascript based client interface based on responsive design)

CRYPTOMATHIC

The main drivers of the end-to-end digital journey

Business Drivers

Digitalisation – bring online what was previously offline.

Savings in cost and time

Streamlined UX to enable business and increase confidence

Compliance & Legal

eIDAS defines a clear legal framework for trust services.

QES offers equivalence to hand-written signatures

Non repudiation demonstration

IT Drivers

Security to tackle the 2FA shortcomings and offer signing anywhere anytime on any device

Leverage existing technology (CA, auth services, etc.)

CRYPTOMATHIC

Cryptomathic digital signature offering

Delivering a new signing experience

The rationale: deliver a new signing experience

The signing service is an ENABLER for your digitalisation strategy.

Add digital signatures to secure transactions and documents – this is when strong user consent is required !

Signer delivers a great UX (users show their consent)

- Great usability (i.e. all devices, all scenarios)
- Visual experience (WYSIWYS and Folklore)
- Make PKI details transparent to the user

Legally binding

- Reach the level of hand written signatures i.e. QES
- Ensure non repudiation
- Strong security design and sole control

Signer and WYSIWYS in a nutshell

Input: Data to be signed

Output: Signed data (QES level)

In the middle: leverage existing driving application, user identity management system, CA, authentication means…

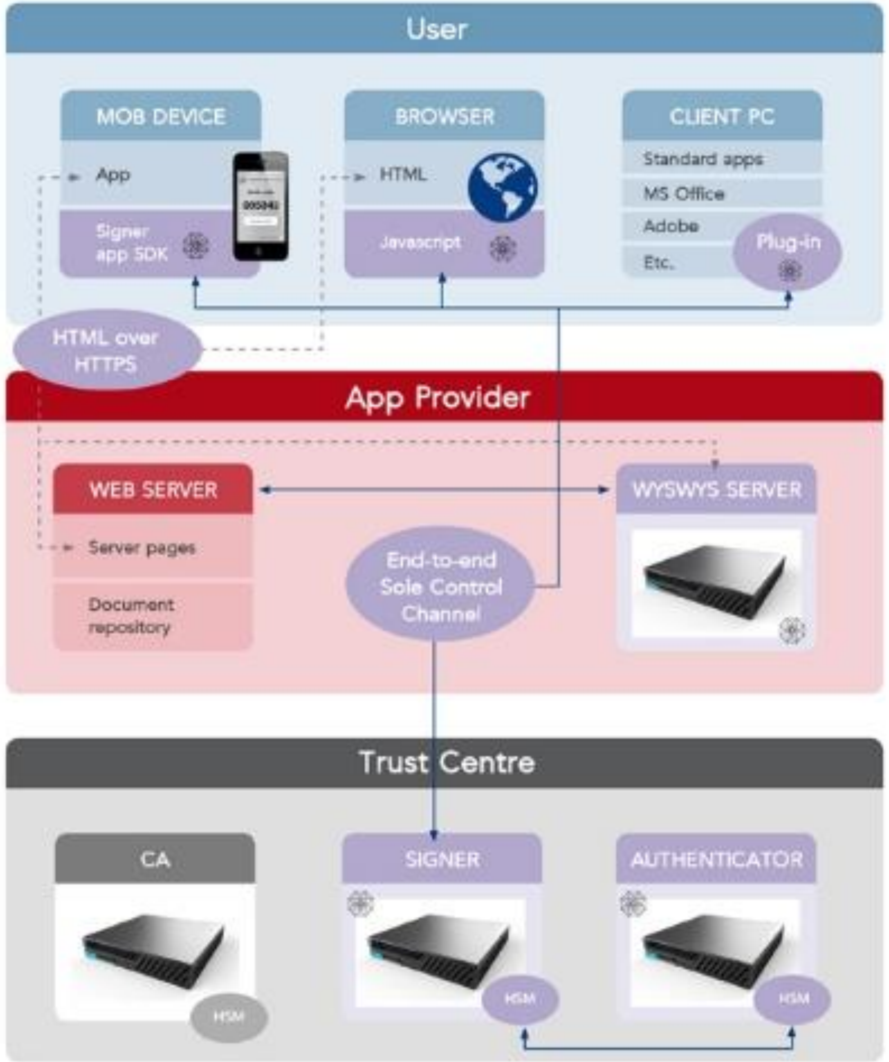
Cryptomathic Signer, a new signing experience

PKI in the background:

Safe deposit your key in a tamper evident environment (HSM)!

Offer remote digital signature services in a IaaS oriented architecture

Centralised (policy based) PKI management for TSP



Signer makes PKI transparent to the end-user

- Signer abstracts the complexity of PKI to deliver a smooth UX:
  - Signer manages the key(s) (generation and usage inside the HSM)
  - The Certificate Authority manages the certificates (as in legacy PKI deployments – using cert requests)
- Central signing renders operations easier
  - Key generation and cert management workflow can be automated
  - Revocation can suspend key usage – CRL/OCSP is no longer a headache
  - Different policies and assurance levels can be supported seamlessly.

Signer leverages 2 Factor Authentication

- Either using OAuth Open ID standard
  - Used widely by the industry (e.g. Facebook, google or the likes)
  - Cryptomathic Authenticator
    - Versatile authentication server supporting almost all crypto based authentication techniques (OATH, SMS based, etc.)
    - Signing protocol is readily supported
    - User provides a static and dynamic password verified by Signer/Authenticator
- Or using SAML from an IdP
  - SAML v2.0 assertions are used to retain sole control
  - Signing protocol is based on session keys derived from the signing request
  - User leverages legacy authentication techniques

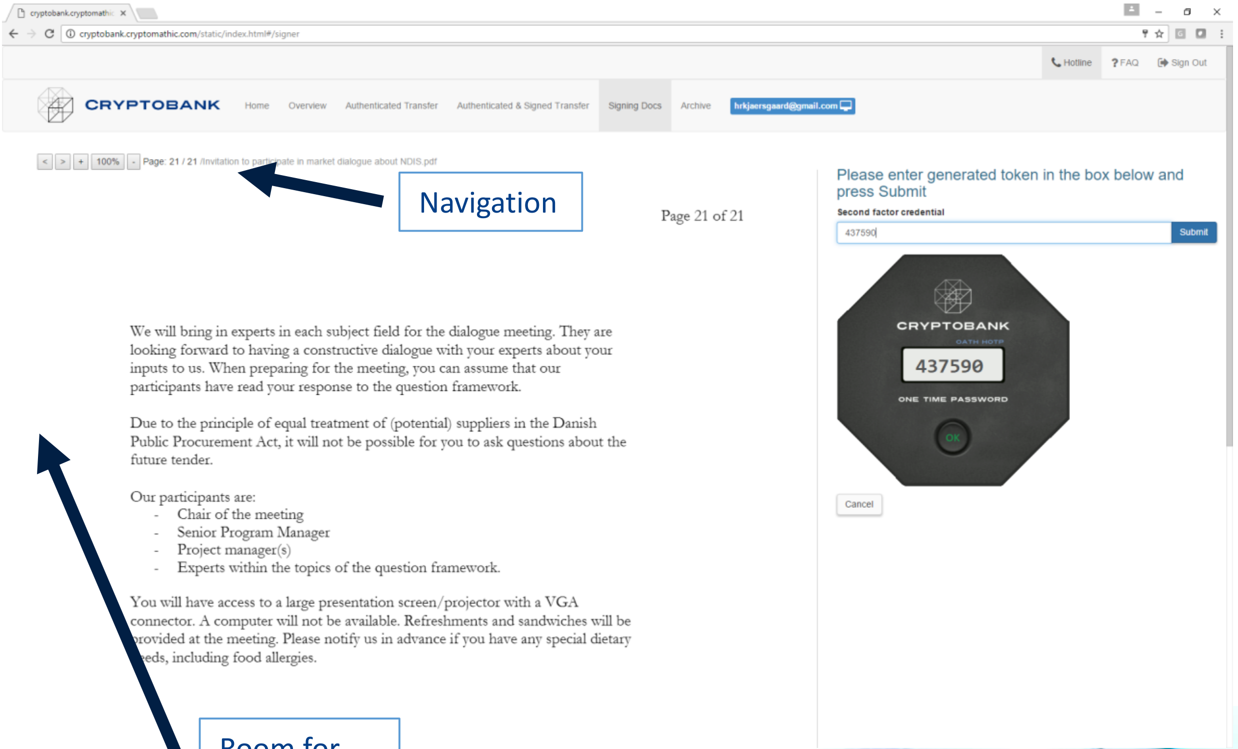
Something you know.

Something you have.

CRYPTOMAThIC

WYSIWYS Signing Experience

- **Provide comparable experience on multiple devices**
- **Establishes trust and confidence**
    - The signatory is able to visually identify what is being signed
    - The signatory can inspect the result (the signed document)
    - The signed document will be recognizable to the signatory afterwards



Page: 21 / 21 /Invitation to participate in market dialogue about NDIS.pdf

Navigation

Page 21 of 21

We will bring in experts in each subject field for the dialogue meeting. They are looking forward to having a constructive dialogue with your experts about your inputs to us. When preparing for the meeting, you can assume that our participants have read your response to the question framework.

Due to the principle of equal treatment of (potential) suppliers in the Danish Public Procurement Act, it will not be possible for you to ask questions about the future tender.

Our participants are:

- Chair of the meeting
- Senior Program Manager
- Project manager(s)
- Experts within the topics of the question framework.

You will have access to a large presentation screen/projector with a VGA connector. A computer will not be available. Refreshments and sandwiches will be provided at the meeting. Please notify us in advance if you have any special dietary needs, including food allergies.

Please enter generated token in the box below and press Submit

Second factor credential

437590

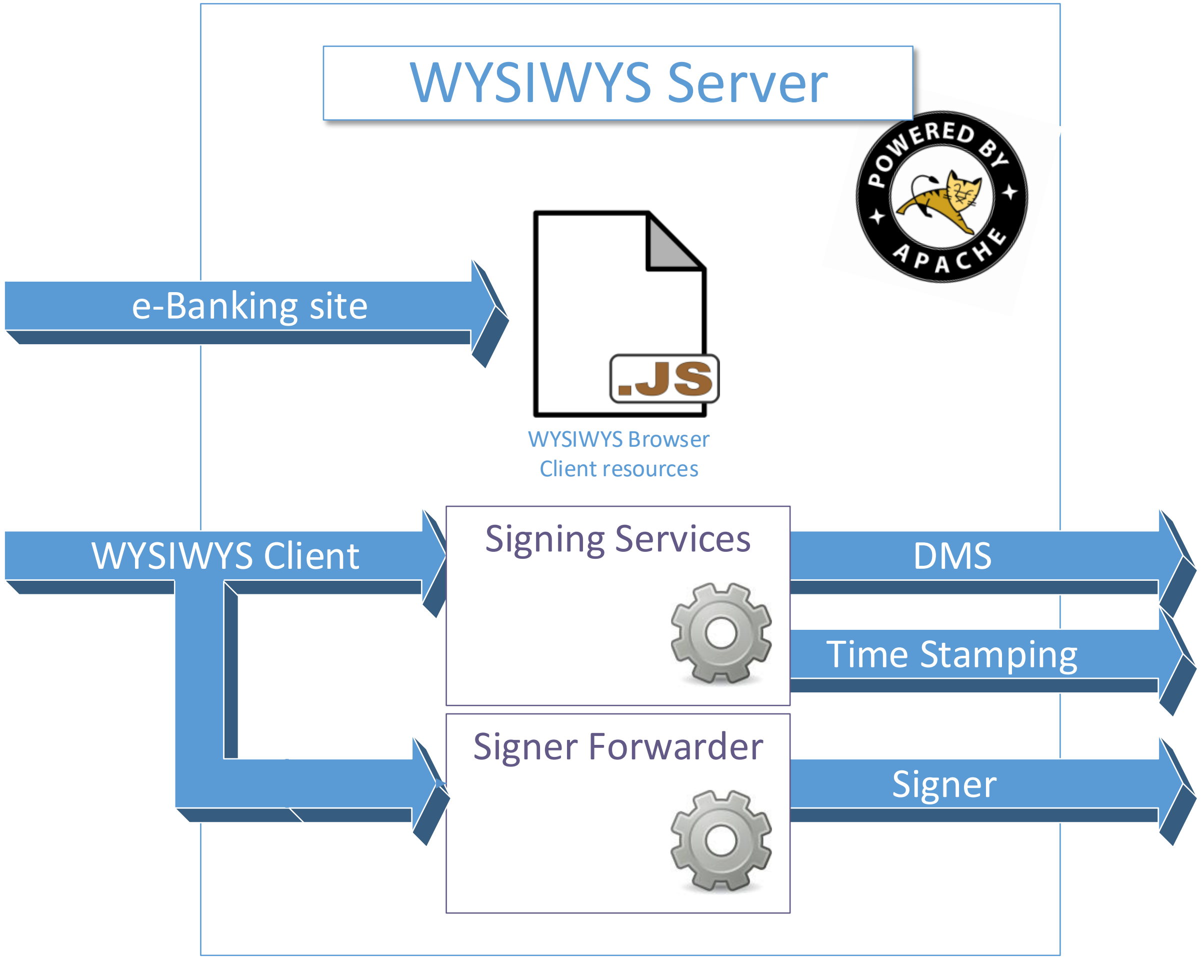
Room for thumbnails

CRYPTOMAThIC

WYSIWYS Signing Experience (option)

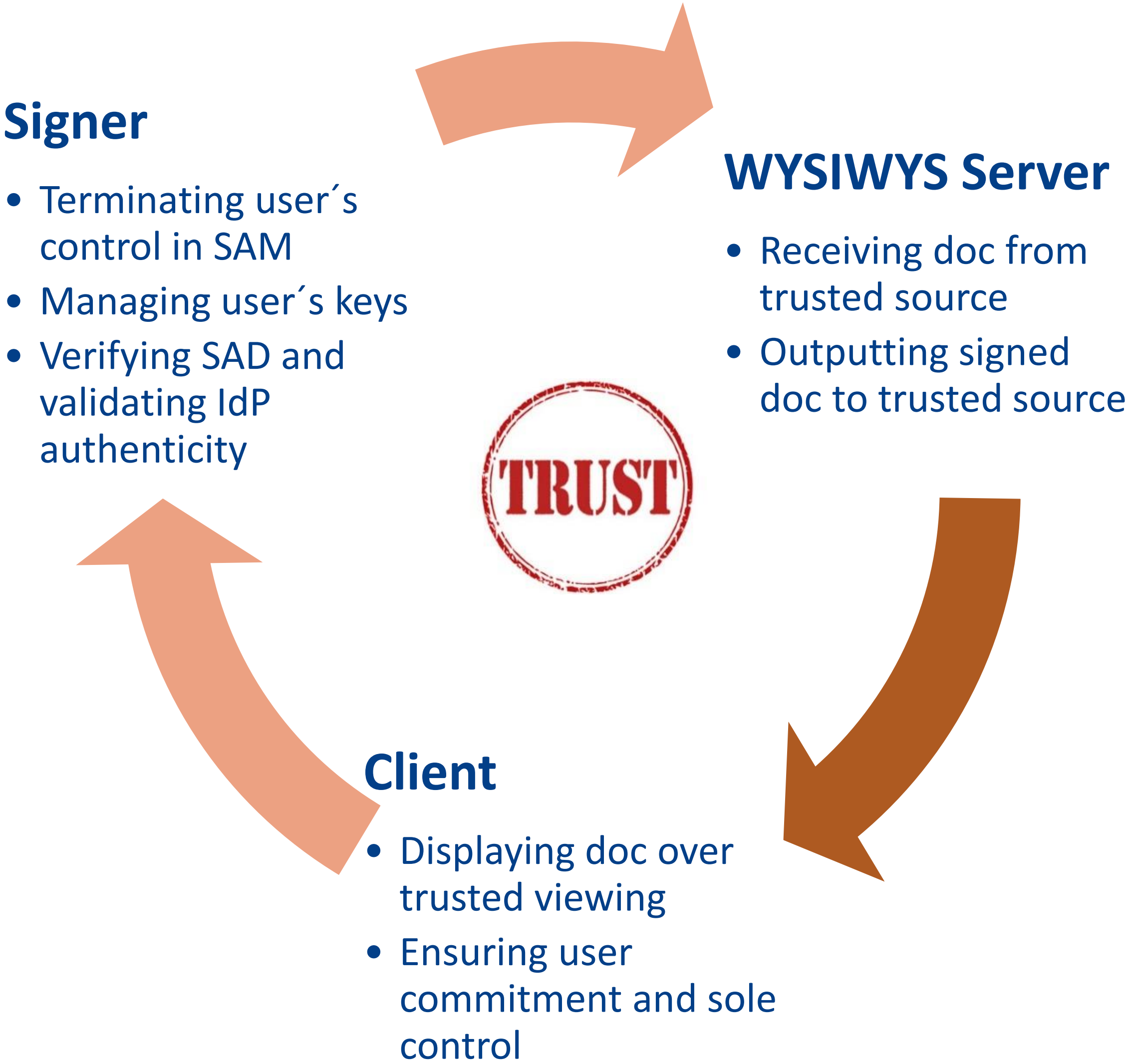
- **JavaScript WYSIWYS client running in browser or embeded in mobile app**
- **Easy to deploy servlets for hosting WYSIWYS browser client resources* and running signing services**
- **Brokering services for**
  - Document retrieval and storage
  - PDF document rendering
  - Electronic signatures through Cryptomathic Signer
- **Providing PDF signature functionality**

*** iPad WYSIWYS Client is self-contained**



Designed to ensure a loop of trust

- Primary objectives
  - Ensure that the DTBS is actually visualised over a trusted viewer before being effectively signed under user´s sole control.
  - Provide an extensive audit trail to ensure non repudiation of origin and emission
- 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 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

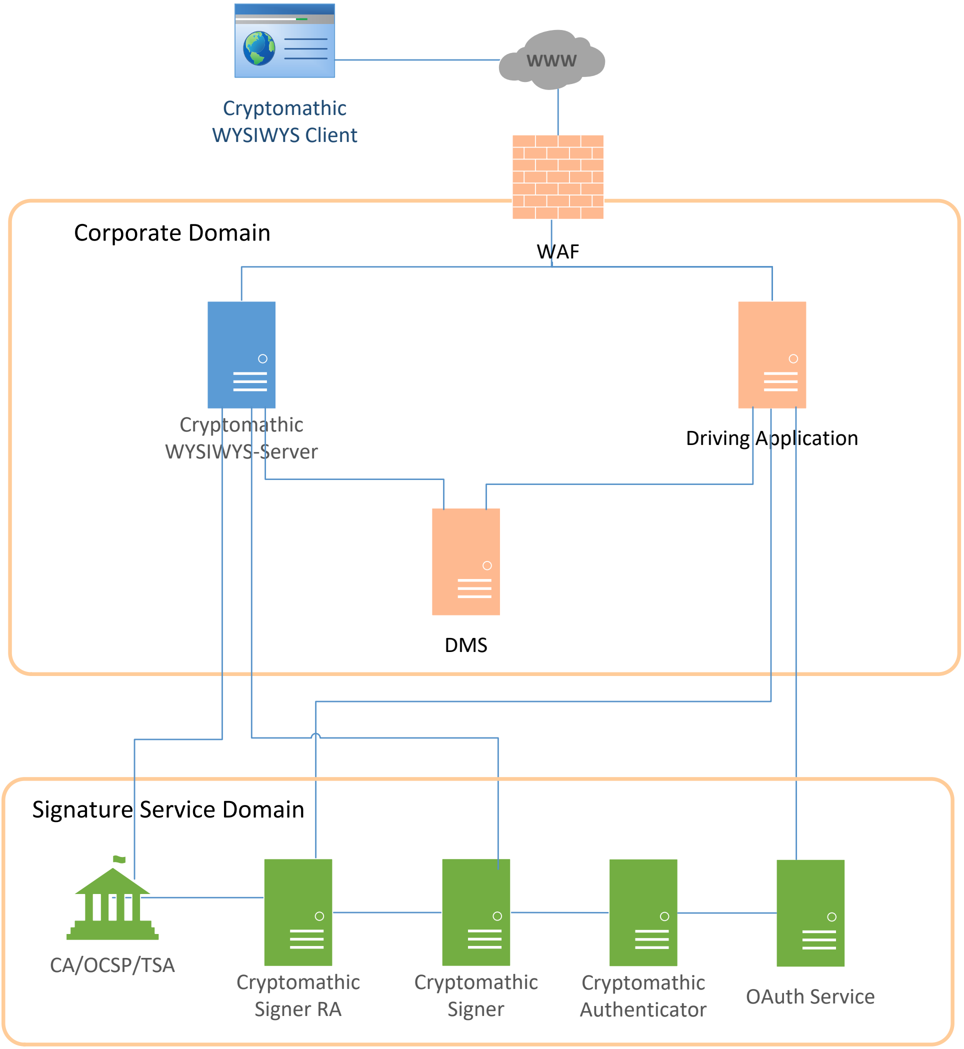
Client

- Displaying doc over trusted viewing
- Ensuring user commitment and sole control

Turnkey solution

External integration points:

- **Interface with User Management**
  - Signer RA exposes a RESTFul API to Establish certificate
  - Functionality to integrate with internal or external CA is already built in
- **Front End- API for WYSIWYS and Signing**
  - Javascript API abstracting the complexity of the signature worksflow
  - Offer a customisable trusted viewer
- **DMS API to WYSIWYS Server**
  - Java/ Rest API to get DTBS and upload signed data
- **Authentication IdP**
  - Javascript based leverages SAMLv2 or OAuth
  - Designed for 2-step authentication (login and authorise signature operation)



Thank you !

guillaume.forget@cryptomathic.com

Digitally signed by:
Guillaume Forget
Signature powered by CRYPTOMATHIC Signer