FutureTrust

Experiences from the Pilots

EEMA Conference – London – June 2019
FutureTrust provides understanding in trust.

FutureTrust is paving the way to interoperability in trust.

FutureTrust acts internationally.

FutureTrust builds along European regulation (eIDAS).

FutureTrust provides understanding in trust.
Contribution of FutureTrust to eIDAS
Global Trust Service List (gTSL)

- “g” = global
- Extends the Trust Service Status List (TSL) model based on ETSI TS 199 612
- Trust Anchors and Meta Data of Identity Providers acting within the “eIDAS - Interoperability Framework”
• **Foundation** for all services in the FutureTrust architecture

• **gTSL uses different sources**
  • European List of the Lists (LoL)
  • Emerging eIDAS-nodes and other eID-Services
  • Other TSLs (e.g. Russia, South America, Asia, Africa)
  • Import of cross certificates, where no TSL is available (e.g. US)

• **Traceable Trust Assessment**
  • Distributed Ledger (e.g. OpenChain)
  • Reputation Based Web of Trust (WoT)

• **SOAP and REST interface**
  • Query according to various aspects
    e.g. Region, Service Type, Assurance Level, other policy aspect
Validation Service (ValS)

- Based on ETSI EN 319 102-1
- XML-based validation policy and returning a standardized validation report (ETSI 319 102-2)
- Open Source component
ValS components

- **Abstract Signature Core Validation**
  - allow the validation of any advanced electronic signature format (i.e. XAdES, CAdES, and PAdES, as well as the ASiC container formats) and simpler formats used within authentication tokens
- **Validation Protocols Spreader**
  - validate tokens used in more advanced protocols such as SAML 2.0 and OpenID Connect
- **Validation Policy Constraints Editor**
  - define and edit a specific validation policy to be applied during the validation process
  - also provide a mechanism to easily override an existing validation policy
- **Web-Service Validation Interface**
  - expose an interface from which users can initiate online validation requests
- **SSO-ValS Module**
  - handles the validation of authentication tokens
Signature Service (SigS)

- eID-based enrolment for qualified certificates
- Mobile creation of signatures and seals across borders
SigS

• **Remote electronic signatures**
  • outlined in recital 52 of (eIDAS: 2014/910/EU)
  • and further explained in (CEN/TS 419 241)

• The SigS will be a **software component**
  • which can be integrated in application systems
  • using appropriate service-oriented interfaces
  • and will enable the local and remote creation of electronic signatures and seals

• SigS will **itself contain**
  • an signature creation device, which hosts the private keys of the signatories,
  • or communicate with external signature creation devices (local or remote)

*Even when the keys are hosted at a central place, they must be kept under the sole control of the signatory as described in (CEN/TS 419 241)*
Preservation Service (PresS)

- Preserve the evidence of a large number of electronic signatures
- Open Source reference implementation for the ETSI-standard required for the implementation of a "Qualified preservation service for qualified electronic signatures" (Art. 34 of 2014/910/EU)
PresS support the fulfilment of the requirements of Article 34 of eIDAS

• “...a qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.”

• Technical changes can happen, which could affect the fulfillment of the requirements
  • increase of computational power
  • the improvement of existing attacks or even the discovery of completely new attacks, which may imply that the applied cryptographic algorithms become weak and do not provide sufficient protection in the long-term perspective

The purpose of the Preservation Service is to provide means for a Proof of Integrity and Proof of Existence of the provided Preservation Data Objects.
Identity Management Service (IdMS)

- Consume variety of authentication tokens
- Work with variety of mobile identification services
- Communicates with a selection of European and non-European eID services
- Transformation into standardised, interoperable and secure format (Industry Standards and eIDAS - Interoperability Architecture)
Pilots and Demonstrators

- BVA stepped out as Pilot Partner

Consortium of new partners stepped in
- DFN-CERT SERVICES GMBH (DFN-Cert)
- UNIVERSITAET LEIPZIG (Uni Leipzig)
- FACHHOCHSCHULE COBURG (HS Coburg)
The concept!
Austrian Pilot Client

• Showcase Implementation for Developers
  • [https://github.com/FutureTrustAT/ft-at-cc](https://github.com/FutureTrustAT/ft-at-cc)
  • Based on Java 8
• Signing Process is based on software keystores
  • Austrian Smartcard (Bürgerkarte) was tested successfully

The realised! „client version“
DE Pilot

Electronic Signatures

E-Mail Encryption

E-Authentication & E-Mail Encryption

Certificate Enrolment
Identity validation
1) Web application, mobile phone number
2) Redirection to IdP of the home institution
3) Identity information from IDM
4) Validation of identity information
5) Validation result to IDM

Certificate Enrollment
1) Web application
2) Redirection to IdP of the home institution
3) Identity information from IDM (including validation results)
4) Upload certificate request
5) Check identity validation, validation of certificate request
6) Issuance of certificate (X.509)
7) Notification to subscriber by the CA of issuance of certificate
A **mandate** is an **authorization** that allows the merchant bank to (repeatedly) collect money from the buyer’s bank account, as payment for a particular contract (e.g. purchase of goods & services) using the direct debit scheme.
Issuance of a mandate using a fully electronic process is an e-Mandate. The e-mandate operations (issuing, amendment and cancellation) are in real-time over the Internet and in a secured way.
e-Mandates User Experience

1. Debtor fills in web form with the required e-Mandate enrolment data...

2. ... and chooses the Bank

3. Transaction completed! Creditor receives e-Mandate signed by Debtor Bank

Debtor is redirected to homebanking, authenticates, verifies e-Mandate, chooses IBAN and authorizes
The Georgian demonstrator is presented in a separate talk.
Business aspects
• Reduced complexity
• Improved eBusiness
• An international approach

Technical aspects
• Standards for base components
• Business process automation
• Resilient and stable
• Easy to implement
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 700542