Supporting the practical implementation of the eIDAS regulations in Europe and beyond

An eIDAS Mobile Signature Platform

www.futuretrust.eu

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 700542
Against the background of the regulation 2014/910/EU on electronic identification (eID) and trusted services for electronic transactions in the internal market (eIDAS), the FutureTrust project aims at supporting the practical implementation of the regulation in Europe and beyond. For this purpose, the FutureTrust project will address the need for globally interoperable solutions through basic research with respect to the foundations of trust and trustworthiness, actively support the standardisation process in relevant areas, and provide Open Source software components and trustworthy services which will ease the use of eID and electronic signature technology in real world applications.

On 1 July 2016 the signature-related part of the eIDAS-Regulation (2014/910/EU) has become fully applicable across Europe and the Signature Directive (1999/93/EC) has been repealed at the same time. Among the major advancements related to this move is the introduction of electronic seals according to Article 3 (25) and (26) and remote electronic signatures as outlined in recital 52 of (2014/910/EU) and further explained in (CEN/TS 419 241).

While the introduction of remote electronic signatures and seals, for which the private key is hosted in a secure server component, is expected to minimize the number of smart card based Qualified Signature Creation Devices (QSCD), there are still many signature cards out there, which should be usable in a web-based environment using the “ChipGateway Protocol” (ChipGateway), which is to be standardised within the OASIS DSS-X TC.

The purpose of the FutureTrust Signature Generation and Sealing Service (SigS) is to support the creation of electronic signatures and
seals using local and remote signature creation devices.

The FutureTrust 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. For this purpose, the FutureTrust SigS will either itself contain an appropriate signature creation device, which hosts the private keys of the signatories, or communicate with external signature creation devices, which may be local (with respect to the user) or remote (e.g. at a trust service provider). 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).

One may distinguish the Enrolment phase and the Usage phase. During enrolment, the later Signatory uses his eID and the eID-Service to perform an eID-based identification and registration at the FutureTrust SigS.

The FutureTrust SigS will create a key pair for the Signatory and requests a certificate at a Certification Authority (CA), which will be operated by a Trust Service Provider according to (2014/910/EU).

Within the Enrolment step, the FutureTrust SigS will also provide appropriate credentials to the Signatory and its mobile device, which can later on be used to authenticate at the FutureTrust SigS in order to trigger the signature creation within some application specific context.
Participants

Federal Office of Administration Germany

EEMA (Belgium)

Arhs Spikeseed (Luxembourg)

Federal Computing Centre of Austria

ecsec GmbH (Germany)

Giesecke & Devrient GmbH (Germany)

LAW trusted Third Party Services (Pty) Ltd (S Africa)

Ministry of Interior Republic of Serbia

Multicert (Portugal)

Public Service Development Agency (Georgia)

PwC (Belgium)

Ruhr-Universität Bochum (Germany)

Secure Information Technology Center Austria

Southampton University (UK)

Trustable Ltd (UK)

Türkiye Bilimsel veTeknolojik Arastrum Kurumu TÜBİTAK (Turkey)

Program Information
Project No: 700542
Start: June 2016
Duration: 3 years
Email: info@futuretrust.eu
Web: www.futuretrust.eu

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 700542

February 2018