EU PROJECT «FUTURETRUST»: APPLICATIONS, PILOT, AND DEMONSTRATORS

Carl-Markus Piswanger / Detlef Hühnlein / Nuno Ponte / Christoph Zehetner / Christina Hermanns / Mikheil Kapanadze / Snezana Stojicic / Roger Dean

eGovernment Architect, Federal Computing Centre of Austria
Hintere Zollamtsstraße 4, 1030 Vienna, AT
carlmarkus.piswanger@brz.gv.at

CEO, ECSEC
Sudetenstraße 16, 96247 Michelau, DE
detlef.huehnlein@ecsec.de

Head of Advanced Solutions, Multicert
Lagoas Park, 2470-266 Porto Salvo-Oeiras, PT
nuno.ponte@multicert.com

Trust Centre Architect, Federal Computing Centre of Austria
Hintere Zollamtsstraße 4, 1030 Vienna, AT
christoph.zehetner@brz.gv.at

Acting Director of IT Development Department / Deputy Chairperson, Public Service Development Agency of the Ministry of Justice
Akaki Tsereteli Avenue 67a, 0154 Tbilisi, GE
mkapanadze@sda.gov.ge

eService Analyst, Ministarstvo unutrašnjih poslova
Kneza Miloša 103, 11000 Belgrade, RS
snezana.stojicic@mup.gov.rs

Director Special Projects, EEMA
Rue Washington 40, 1050 Brussels, BE
r.dean@eema.org

Keywords: ***eIDAS, Trust Services, EU Project***

Abstract: *EIDAS regulation represents a major topic for Europe's eGovernments and the requirements to fulfil the obligations of the regulation are not to be underestimated. The regulation aims at «trust services» in Europe (and beyond), and these are ICT applications. FutureTrust project will provide such applications: for Mobile Signing, Identity Management, a Validation and Preservation Service and the Global Trust Service List. Furthermore, FutureTrust will provide one pilot and several demonstrators to show the capability of the developed applications in the real world. Austria, Georgia, Germany, Portugal and possibly Serbia will provide practical implementations within different domains (private and public sector).*

1. Introduction

The European Regulation (EU) No 910/2014 on electronic identification (eID) and trusted services for electronic transactions in the internal market (eIDAS)[1] formulates standards and processes about how electronic trust services have to be set up and operated in Europe to reach high acceptance and traceability regarding proper service delivery. The FutureTrust project (www.futuretrust.eu), funded by the EU Framework Pro-

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN).

gramme for Research and Innovation (Horizon 2020) under Grant Agreement No. 700542, aims at supporting the practical implementation of the regulation in Europe and beyond. For this purpose, the FutureTrust project addresses the definition, development and test of applications for the support of globally interoperable ICT solutions. Basic research fosters the attempt with respect to the foundations of trust (and trustworthiness) as well as an active support of the European standardisation process in the relevant areas. The FutureTrust project will provide Open Source software components and trust services, which will ease the use of eID and electronic signature technology in real world applications. Furthermore, the project will extend the existing

European Trust Service Status List (TSL) infrastructure towards a «Global Trust List», will develop comprehensive trust services, such as a Validation Service (ValS) and a Preservation Service (PresS) for electronic signatures and seals and will provide components for the eID-based application – the Identity Management Service (IdMS) – for qualified certificates across borders, and a Mobile Signature Service (mSignS) for the trustworthy creation of remote signatures and seals in a mobile environment.

2. Overview of FutureTrust Services

FutureTrust develops an array of fundamental Services for trust in electronic business (and government), which are considered as building blocks. They should play a major role in increasing cross-border trust at a global scale. Nowadays the problems of the establishment of trust are not sufficiently solved, both in the field of technology and the necessary processes. The European eIDAS regulation provides a model of a trust organization and FutureTrust project extends it with a global perspective. The FutureTrust services are designed as part of a process chain, not detached. That enhances the future-proof ability of the services and opens ground to several exploitation models, which hopefully accelerates acceptance and widespread.

2.1. FutureTrust Architecture

The architecture of FutureTrust projects respects the given organisation of trust services, both from the legal perspective and the existing trust architecture in Europe. The FutureTrust services will be implemented following European standards within a distributed system to fulfil the needs of the European Member States. The use of Open Source for the main services ValS, PresS and gTSL will ease the applicability among the pilots and after the project in Europe and beyond.

2.2. Identity Management (IDM)

Most European member states have already introduced national eID cards, which can be used for online identification and strong authentication in eGovernment and eBusiness. Nonetheless, the number of issued eIDs still has a large potential for an advance in growth. Among the challenges to reach that goal are coping with the high diversity of the eID solutions, the uncertainty with respect to security and trust issues and, as well, the lack of usability in mobile environments.

Recent initiatives have appeared to support strong authentication in the internet and especially for mobile technologies, such as the FIDO Alliance[2], supported by major enterprises from the IT industry, and the Mobile Connect initiative GSMA[3] driven by the GSM Association. While these initiatives currently feature strong authentication, they do not yet provide a solution for trustworthy identities as provided by eID cards or electronic passports, for example.

Against this background the FutureTrust project bases its work on the results of pertinent research projects, such as FutureID[4] and SkIDentity[5], in order to build a comprehensive, flexible, privacy-aware and ubiqui-

2 https://fidoalliance.org/ (all websites last accessed on 2 January 2018).

3 http://www.gsma.com/.

4 ETSI EN 319 102-1 (Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures).

5 https://www.skidentity.de/.

tously usable Global Identity Management Infrastructure, which in particular integrates the SAML (2.0) based eIDAS-interoperability framework (eIDAS – Interoperability Architecture, 2015)[6], the «OpenID Connect»[7] based Mobile Connect infrastructure, non-European eID cards and other authentication tokens using ISO/IEC 24727[8] and, last but not least, ePassports according to ICAO 9303[9].

2.3. Mobile Signature Service (mSig)

Several EU member states show positive experiences with respect to remote signing in mobile environments.

The general approach to host the private signing key of a signatory in a central Hardware Security Module (HSM) and let it only authenticate with appropriate means to the central system in order to trigger the creation of a qualified electronic signature seems to be a promising approach for the creation of qualified electronic signatures in mobile environments. While the current processes to apply for a centrally hosted qualified certificate in Austria and Italy are currently based on traditional paper based processes, in the future one may envision using existing national and emerging pan-European eID techniques for this application and enrolment process. Thus, the FutureTrust project analyses the legal and regulatory details with respect to eID-based application and enrolment for qualified certificates in the EU Member States, design a serviceoriented reference architecture with appropriate components and interfaces based on international standards, such as OASIS DSS[10] and SAML (for example) and provide a corresponding reference implementation, which supports the eID-based enrolment for qualified certificates and the mobile creation of eSignatures and eSeals cross-borders.

2.4. Validation Service (ValS)

To cope with the challenge to extend the validation capabilities of electronic signatures on a global scale, resulting from a potentially vast number of signatures in circulation, the implementation of a standardised validation service is required. This service must be flexible enough to adapt to the peculiarities not only of European legislation, but also of the member countries and the rest of the world. The Comprehensive Validation Service should be far more open and flexible compared to a conventional case in a closed, internal environment. Indeed, each country currently has its own specifications with respect to electronic signatures.

Another challenge that must be addressed by the validation service relates to the confusion and discrepancy prevailing in the validation standards – or outright their absence. The forthcoming standard ETSI EN 319 102-1[11] specifies how an advanced electronic signature is to be verified and relies implicitly, as well as explicitly, on signature creation policies, signature augmentation policies and signature validation policies.

However, these various policies are yet to be formally defined and hence far from being standardised.

2.5. Preservation Service (PresS)

Another important challenge introduced with the eIDAS regulation (see Article 34 «Qualified preservation service for qualified electronic signatures») is related to the preservation of the conclusiveness of electronic signatures and related signed objects (certificates, revocation information, time stamps, etc.) over a long period of time. It is well known that the conclusiveness of cryptographically signed data is itself a function of time, as cryptographic algorithms may become weak. Therefore, it is necessary to provide suitable measures to preserve the evidence of signed data (e.g. in the area of electronic registers for birth or land registers). As matter of fact, there are the first approaches towards the implementation of preservation services and various

6 https://joinup.ec.europa.eu/sites/default/files/eIDAS_interoperability_architecture_v1.00.pdf.
7 https://openid.net/connect/.
8 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=61066.
9 http://www.icao.int/publications/pages/publication.aspx?docnum=9303.
10 https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss.
11 http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.00.00_20/en_31910201v010000a.pdf.

related standards produced by ETSI TS 101 533-1[12], ISO (ISO 14641 and ISO 14721)[13] and IETF (RFC 4998 and RFC 6238)[14]. However, there is no commonly agreed reference architecture and comprehensive standard yet, which should define the requirements for a qualified preservation service according to Article 34 of the eIDAS regulation. Fortunately, this standardisation work is just about to be started within ETSI.

2.6. Global Trust Service List

The current «trusted lists» and «list of trusted lists» focusses on electronic signatures. The expansion of the trusted lists according to ETSI TS 199 612[15] towards eSeals and other trust services introduced with the eIDAS-regulation is bringing a significant improvement. The FutureTrust project goes one step further and extends this concept in two dimensions in order to create a «Global Trust List». This list on the one hand side includes the necessary trust anchors and metadata necessary for the envisioned «Global Identity Management Infrastructure» (see above), and on the other hand covers other regions beyond Europe and supports the assessment of assurance levels and features the distributed management.

For this purpose, the FutureTrust project will extend the Trusted Lists standard in order to cover metadata and trust anchors for SAML (2.0) and Identity Provider, FIDO-related trust information and integrate the ICAO Public Key Directory[16]. Furthermore, the FutureTrust project provides user friendly means for the assessment of the trustworthiness of trust services and identity providers, and for the distributed management of the «Global Trust List».

3. Overview on the FutureTrust Pilot and Demonstrator

The FutureTrust project represents an Innovation Action (IA), which means a direct link to applicability.

Thus, beside the design and the development it is important to demonstrate the capabilities of the services in a wide range. The project adopted a high grade of practical use, bringing three demonstrators and one pilot in the field, envisaging Technical Readiness Level up to «7» (TRL7). The demonstrators/pilot will be established three times in the governmental field (maybe four times) and one demonstrator in the private sector.

The existing setup of the demonstrators/pilots is therefore particularly advantageous due to the balanced mix.

The following sub chapters provide overviews on the demonstrators and the pilot.

3.1. The Austrian Pilot: eInvoice

The Austrian pilot will be implemented in the field of eInvoicing. The FutureTrust pilot partner BRZ (Austrian Federal Computing Centre) develops and operates the Austrian shared application «eInvoice submission to the Austrian Public Sector»[17] by order of the Austrian Federal Ministry of Finance. The service was chosen because of the international approach of the application. Although eSignatures are not mandatory for the submission of eInvoices, the use of eSignatures is not forbidden either. The pilot will use the application to show the use case of eSignature validation, to send a vivid signal for FutureTrust's service use to the Austrian government and economic players. The eInvoice System is integrated in the Austrian governmental business portal «USP»[18], which provides user identification, authentication and access control of users, when using integrated eServices.

---

12 Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management (http://www.etsi.org/deliver/etsi_ts/101500_101599/10153301/01.02.01_60/ts_10153301v010201p.pdf).

13 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=54911 and http://www.iso.org/iso/catalogue_detail.htm?csnumber=57284.

14 https://tools.ietf.org/pdf/rfc4998.pdf and https://tools.ietf.org/pdf/rfc6238.pdf.

15 ETSI EN ETSI TS 199 612 (Electronic Signatures and Infrastructures (ESI); Trusted Lists).

16 http://www.icao.int/Security/FAL/PKD/Pages/default.aspx.

17 https://www.erechnung.gv.at/erb?p=info_erb&locale=en_GB.

18 https://www.usp.gv.at.

User authentication is also mandatory when using web service communication from integrated eServices, particularly also in focus of the pilot. USP offers a specific authentication service to prove applying organisations (companies, associations, other entities), and the respective agent's authority, within a process with human interaction and approval.

After the initial login at USP the authorised agent could open assigned eServices, one of them is the eInvoice System, which offers several channels to transfer eInvoices to the Austrian government. One of the channels represents the web service interface. Therefore, the upload of a certificate to the IDM of USP is needed. The validation of the certificate could be done with FutureTrust's Validation Service ValS. After the successful fulfilment of this process step, the user can use the eInvoice System with web service communication. The authentication certificate will be proved with ValS within each request, to proof the authenticity and validity. If the document is additionally digital signed, the eInvoice System will use ValS again, to prove the eSignature, using gTSL as well.

3.2. The Georgian Demonstrator: e-Apostille

The Georgian web-based e-Apostille Validation System will run a registry of Apostille issuers to hold metadata about Apostilles issued by them. It will allow specific rules of Apostille processing (including parsing of documents to query specific information like Apostille Number, Verification Code etc.), which may vary from country to country. The information will be collected during an initial (and continuous) «Metadata Provisioning» process.

Once a document, which is electronically signed by a competent body, is uploaded into the system, signature validity verification will take place, using the FutureTrust Validation Service (ValS). If this step is successful the authorisation of the party and the status of the e-Apostille will be verified, if this is supported by the issuing body. In this case, the status of e-Apostille will be queried from the database of the respective issuer. For this purpose a connector interface, which may be realised as a web service over a TLS-connection, will be specified. In order to maintain the conclusiveness of the issued e-Apostilles the User may store the document in the FutureTrust Preservation Service.

3.3. The German Demonstrator: FT Box

The Federal Office of Administration in Germany (BVA) develops and operates several applications by order of the German Federal Ministry of Interior, and will support FutureTrust project with a demonstrator. The demonstrator website will be called https://www.app.bva.bund.de. The link-part «app» stands for application and can be any kind of application or register as for example www.bafoegonline.bva.bund.de or www.azr.bva.bund.de. Even if this «app»-website is not yet in place, the plan is for all applications with a higher requested level of security than just password and username access to build a so called «FutureTrust Box». It offers an authentication process for the notified eIDs in combination with an eID-Service within web application. It allows access via the German electronic identity «Elektronischer Personalausweis – nPA» or electronic residence permit, European IDs or any international ID, which is notified by the European Commission. The box encapsulates the authentication process to ease the implementation in web applications.

The website https://e-id.bva.bund.de[19] already provides integrated user identification/authentication and access control of users for some applications, when using integrated eServices. The idea for the BVA demonstrator is to extend the identification/authentication service based on the eIDAS regulation towards a gTSL «Global Trust Service List» and become international, not just European.

[19] https://e-id.bva.bund.de/pa-authsservice/app/flow/anmeldenFlow?execution=e3s1.

3.4. The Portuguese Demonstrator: SEPA eMandate

The main objective of the SEPA eMandate Service is to replace the paper copy in the mandate flow for Direct Debit by an electronic mandate. This enables Debtors to issue, amend or cancel Direct Debits in a secure electronic way.

This eService allows Debtors and Creditors to exchange and process mandates for Direct Debits fully electronically, which offers advantages for all the entities involved in this process (Debtors, Creditors, Debtor Banks and Creditor Banks). There are two entities, which have a key role in the SEPA eMandate Service, (1) Routing Service: the entity operating in agreement with Creditor Banks to provide access to validation services offered by Debtor Banks; and (2) Validation Service: the entity operating in agreement with and on behalf of Debtor Banks for signing of e-Mandate proposals initiated by Debtors through the electronic channels of Creditors and the routing services offered by Creditor Banks.[20]

To allow an easy integration in the Debtor Bank platform, a validation service plug-in will be developed providing an extensive set of features like access control, data validation and preparation, and HSM communication management. The validation service plug-in is an independent system that communicates with the existing Debtor Bank platform, offering all the core functionalities out-of-the-box and with well-known integration points which allow for a smooth integration. In addition to these services, the demonstrator will include a functional mock-up of a Debtor Bank, integrating advanced authentication and signature with an eID. Extending the authentication process with an eID introduces a second authentication factor (knowledge and ownership). Signature with the eID also extends the currently approved specification for SEPA eMandate services by introducing a countersignature (or similar proof of authentication) by the Debtor over the already required signature from the Debtor Bank.[21] This enhances the legal binding of the authorisation process and complies with the requirements of the European Banking Authority: «Guidelines on the security of internet payments»[22], which requires strong customer authentication based on two factor authentication of which at least one is dynamic, for the authorisation of payment transactions.

3.5. The Serbian Demonstrator

Furthermore one involved partner from a Non-EU country is interest to enlarge their perspective in the project and step in as a piloting partner as well. The Republic of Serbia is willing to participate in the project as a demonstrating partner. They have proposed two different demonstrator setups:

- Renewal or issuing electronic certificate on citizen Identity Card
- Digital signature available for citizens with chip-less version of ID cards

In the following proceedings we will provide deeper information on that demonstrator.

4. Status and Next Steps

FutureTrust project reached its first year and the stage of first review. The deliverables on the «design» of the applications and the pilot/demonstrators have been accepted. The next step in the project is the implementation the applications, including the test procedures. The pilot and demonstrators will be implemented throughout 2018 and the pilots and demonstrators should last for one year.

---

[20] European Payments Council. EPC e-Mandates eOperating Model – Detailed Specification. Version 1.2 (EPC 208-08., 2013): http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epcdocuments/epc-e-mandates-eoperating-model-detailed-specification/epc208-08-eoperating-model-detailed-specification-v12-approvedpdf/.

[21] European Payments Council (footnote 20).

[22] https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+(Guidelines+on+the+security+of+internet+payments)_Rev1.