M. Talamo, H. Roßnagel, D. Hühnlein, C. Schunck (Ed.): Open Identity Summit 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 – 27

FutureTrust – Future Trust Services for Trustworthy Global Transactions

Detlef Hühnlein[1], Tilman Frosch[2], Jörg Schwenk[2], Carl-Markus Piswanger[3], Marc Sel[4], Tina Hühnlein[1], Tobias Wich[1], Daniel Nemmert[1], René Lottes[1], Stefan Baszanowski[1], Volker Zeuner[1], Michael Rauh[1], Juraj Somorovsky[2], Vladislav Mladenov[2], Cristina Condovici[2], Herbert Leitold[5], Sophie Stalla-Bourdillon[6], Niko Tsakalakis[6], Jan Eichholz[7], Frank-Michael Kamm[7], Jens Urmann[7], Andreas Kühne[8], Damian Wabisch[8], Roger Dean[9], Jon Shamah[9], Mikheil Kapanadze[10], Nuno Ponte[11], Jose Martins[11], Renato Portela[11], Çağatay Karabat[12], Snežana Stojičić[13], Slobodan Nedeljkovic[13], Vincent Bouckaert[14], Alexandre Defays[14], Bruce Anderson[15], Michael Jonas[16], Christina Hermanns[16], Thomas Schubert[16], Dirk Wegener[17], and Alexander Sazonov[18]

[1] ecsec GmbH, Sudetenstraße 16, 96247 Michelau, Germany, {firstname.name}@ecsec.de
[2] Ruhr Universität Bochum, Universitätsstraße 150, 44801 Bochum, Germany, {firstname.name}@rub.de
[3] Bundesrechenzentrum GmbH, Hintere Zollamtsstraße 4, A-1030 Vienna, {firstname.name}@brz.gv.at
[4] PwC Enterprise Advisory, Woluwedal 18, Sint Stevens Woluwe 1932, Belgium, {firstname.name}@be.pwc.com
[5] A-SIT, Seidlgasse 22/9, A-1030 Vienna, Austria, {firstname.name}@a-sit.at
[6] University of Southampton, Highfield, Southampton S017 1BJ, United Kingdom, {S.Stalla-Bourdillon, N.Tsakalakis}@soton.ac.uk
[7] Giesecke & Devrient GmbH, Prinzregentestraße 159, 81677 Munich, Germany, {firstname.name}@gi-de.com
[8] Trustable Limited, Great Hampton Street 69, Birmingham B18 6E, United Kingdom, {kuehne,damian}@trustable.de
[9] European Electronic Messaging Association AISBL, Rue Washington 40, Bruxelles 1050, Belgium, {r.dean, jon.shamah}@eema.org
[10] Public Service Development Agency, Tsereteli Avenue 67A, Tbilisi 0154, Georgia, mkapanadze@sda.gov.ge
[11] Multicert – Servicos de Certificacao Electronica SA, Lagoas Parque Edificio 3 Piso 3, Porto Salvo 2740 266, Portugal, {firstname.name}multicert.com
[12] Turkiye Bilimsel Ve Tknolojik Arastirma Kurumu, Ataturk Bulvari 221, Ankara 06100, Turkey, cagatay.karabat@tubitak.gov.tr
[13] Ministarstvo unutrašnjih poslova Republike Srbije, Kneza Miloša 103, Belgrade 11000, Serbia, {firstname.name}@mup.gov.rs
[14] Arηs Spikeseed, Rue Nicolas Bové 2B, 1253 Luxembourg, Luxembourg, {firstname.name}@arhs-developments.com
[15] Law Trusted Third Party Service (Pty) Ltd. (LAWTrust), 5 Bauhinia Street, Building C, Cambridge Office Park Veld Techno Park, Centurion 0157, South Africa, bruce@LAWTrust.co.za
[16] Federal Office of Administration (Bundesverwaltungsamt), Barbarastr. 1, 50735 Cologne, Germany, {firstname.name}@bva.bund.de
[17] German Federal Information Technology Centre (Informationstechnikzentrum Bund, ITZBund), Waterloostr. 4, 30169 Hannover, Germany, {firstname.name}@itzbund.de
[18] National certification authority Rus CJSC (NCA Rus), 8A building 5, Aviamotornaya st., Moscow 111024, Russia, sazonov@nucrf.ru

Abstract: Against the background of the regulation 2014/910/EU [EU1] on electronic identification (eID) and trusted services for electronic transactions in the internal market (eIDAS), the FutureTrust project, which is funded within the EU Framework Programme 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 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. The FutureTrust project will extend the existing European Trust Service Status List (TSL) infrastructure towards a "Global Trust List", develop a comprehensive Open Source Validation Service as well as a scalable Preservation Service for electronic signatures and seals. Furthermore it will provide components for the eID-based application for qualified certificates across borders, and for the trustworthy creation of remote signatures and seals in a mobile environment. The present contribution provides an overview of the FutureTrust project and invites further stakeholders to actively participate as associated partners and contribute to the development of future trust services for trustworthy global transactions.

Keywords: Trust, eID, Trust Services, Global Trust List, electronic Signatures and Seals, Validation, Preservation, eID-based enrolment of Qualified Certificates, remote and mobile Signing and Open Source.

1 Background and Motivation

There are currently around 150 trust service providers across Europe[19], which issue qualified certificates and/or qualified time stamps. Hence, the "eIDAS ecosystem" with respect to these basic services is fairly well developed. On the other hand, the provision of qualified trust services for the validation and preservation of electronic signatures and seals as well as for registered delivery and the cross-border recognition of electronic identification schemes have been recently introduced with the eIDAS regulation [EU1]. However, these services are not yet available in a mature, standardised, and interoperable manner within Europe.

In a similar manner, the practical adoption and especially the cross-border use of eID cards, which have been rolled out across Europe, is – despite previous and ongoing research and development efforts in pertinent projects, such as STORK, STORK 2.0, FutureID, e-SENS, SD-DSS, Open eCard, OpenPEPPOL and SkIDentity – still in its infancy. In general there is no opportunity to use national eID means in foreign environment. In particular, it is often not yet possible in practice to use an eID card from one EU Member State to enrol for a qualified certificate and secure signature creation device (SSCD) in another Member State.[20]

[19] See [EUTL], [DIR] and [3xA16] for example.

[20] Note, that such a cross-border enrolment for qualified certificates may become especially interesting in combination with remote and mobile signing services, in which no physical SSCD needs to be shipped to the user, because the SSCD is realized as central Hardware Security Module (HSM) hosted by a trusted service

In particular the following problems seem to be not yet sufficiently solved and hence will be addressed in the FutureTrust project:

P1. No comprehensive Open Source Validation Service

Multiple validation services are available today. They range from offering revocation information to full validation against a formal validation policy. These services are operated by public and private sector actors, and allow relying parties the validation of signed or sealed artefacts. However, there is currently no freely available, standard conforming and comprehensive Validation Service, which would be able to verify arbitrary advanced electronic signatures in a trustworthy manner. To solve this problem the FutureTrust project will contribute to the development of the missing standards and the development of such a comprehensive Validation Service.

P2. No scalable Open Source Preservation Service

The fact that signed objects lose their conclusiveness if cryptographic algorithms become weak induces severe challenges for applications, which require maintaining the integrity and authenticity of signed data for long periods of time. Research related to the strength of cryptographic algorithms is addressed in many places, including ECRYPT-NET[21], and does not fall within the scope of FutureTrust. Rather, the FutureTrust project will aim at solving this problem by contributing to the development of the missing standards and the implementation of a scalable Open Source Preservation Service that makes use of processes and workflow to ensure preservation techniques embed the appropriate cryptographic solutions.

P3. Qualified electronic signatures are difficult to use in mobile environments

Today, applying for a qualified certificate involves various paper-based steps. Furthermore, to generate a qualified signature, typically a smart card based signature creation device has to be used, which is complicated in mobile environments due to the need for middleware and drivers that are often not supported on the mobile device. The FutureTrust project will aim at changing this by creating a mobile Signature Service, which supports eID-based enrolment for qualified certificates and the remote creation of qualified electronic signatures initiated by using mobile devices.

P4. Legal requirements of a pan-European eID metasystem

The first part of the eIDAS-regulation that deals with eIDM systems aims to create a standardized interoperability framework but does not intend to harmonize the respective national eIDM systems. Instead it employs a set of broad requirements, part of which is the mandatory compliance of all systems to the Data Protection Directive [EC2]. The

provider, which fulfils the requirements of [CEN1], and against the background of the eIDAS-regulation (see e.g. Recital 51 of [EU1]) one may expect that such a scenario may soon become applicable across Europe and beyond.

[21] https://www.cosic.esat.kuleuven.be/ecrypt/net/

Directive will soon be replaced by the General Data Protection Regulation (GDPR) [EU3], which introduces new concepts and safeguards for data protection. To facilitate compliance with the GDPR, the FutureTrust project will conduct desk research to analyse how the newly emerged privacy and data protection legislation impacts on existing laws and derive a list of necessary characteristics that an EU eID and eSignatures metasystem should incorporate to ensure compliance.

P5. Legally binding electronic transactions with non-European partners are hard to achieve

While the electronic signature directive [EC1] and the eIDAS-regulation [EU1] define the legal effect of qualified electronic signatures, there is no comparable global legislation and hence electronic transactions with business partners outside the European Union are challenging with respect to legal significance and interoperability. To work on a viable solution for this problem the FutureTrust project will conduct basic research with respect to international legislation, contribute to the harmonization of the relevant policy documents and standards and build a "Global Trust List", which may form the basis for legally significant electronic transactions around the globe.

P6. Scope of eIDAS interoperability framework is limited to EU

In a similar manner, the scope of the interoperability framework for electronic identification according to Article 12 of [EU1] is limited to the EU. There are many aspects of an international interoperability framework that need to be assessed, especially in regard of to the changes in privacy and data protection highlighted above.[22] Against this background, the FutureTrust project will extend the work from pertinent research and large-scale pilot projects to integrate non-European eID-solutions in a seamless and trustworthy manner, after defining the requirements and assessing the impact of data transfers beyond the European Union.

P7. No formal foundation of trust and trustworthiness

To be able to compare eID solutions on an international scale, there is no international legislation which would allow to "define" trustworthiness. Instead, scientifically sound formal models must be developed which describe international trust models, and especially model to compare the trustworthiness of different eID services.

To demonstrate the viability and trustworthiness of these formal models, and show that the developed components can be used in productive environments, the FutureTrust project will implement real world pilot applications in the area of public administration, eCommerce, eBusiness and eBanking.

[22] For example, data transfers to the US are currently not clearly regulated after the invalidation of the 'Safe Harbor' agreement by the EUCJ (C-362/14). The EU officials are currently in negotiations on a new arrangement, named 'EU-US Privacy Shield' which was halted after a contradictory opinion from the WP29 (WP238).

2 The FutureTrust Project

In order to solve the problems mentioned above, the FutureTrust partners (see Section 2.1) have sketched the FutureTrust System Architecture (see Section 2.2), which includes several innovative services, which are planned to be used in a variety of pilot projects (see Section 2.8).

This will in particular include the design and development of a Global Trust List (gTSL) (see Section 2.3), a Comprehensive Validation Service (ValS) (see Section 2.4), a scalable Preservation Service (PresS) (see Section 2.5), an Identity Management Service (IdMS) (see Section 2.6) and last but not least a mobile Signature Service (mSignS) (see Section 2.7).

2.1 FutureTrust Partners

The FutureTrust project is carried out by a number of core partners as depicted in Figure 1, which includes Ruhr-Universität Bochum (Germany), ecsec GmbH (Germany), Arhs Spikeseed (Luxembourg), EEMA (Belgium), Federal Computing Centre of Austria (Austria), Federal Office of Administration Germany (Germany), Price Waterhouse Coopers (PWC) (Belgium), University of Southampton (United Kingdom), multicert (Portugal), Giesecke & Devrient GmbH (Germany), Trustable Ltd. (United Kingdom), Secure Information Technology Center – Austria (Austria), Public Service Development Agency (Georgia), Türkiye Bilimsel veTeknolojik Araştırma Kurumu (Turkey), LAW Trusted Third Party Services (Pty) Ltd. (South Africa), Ministry of Interior Republic of Serbia (Serbia).

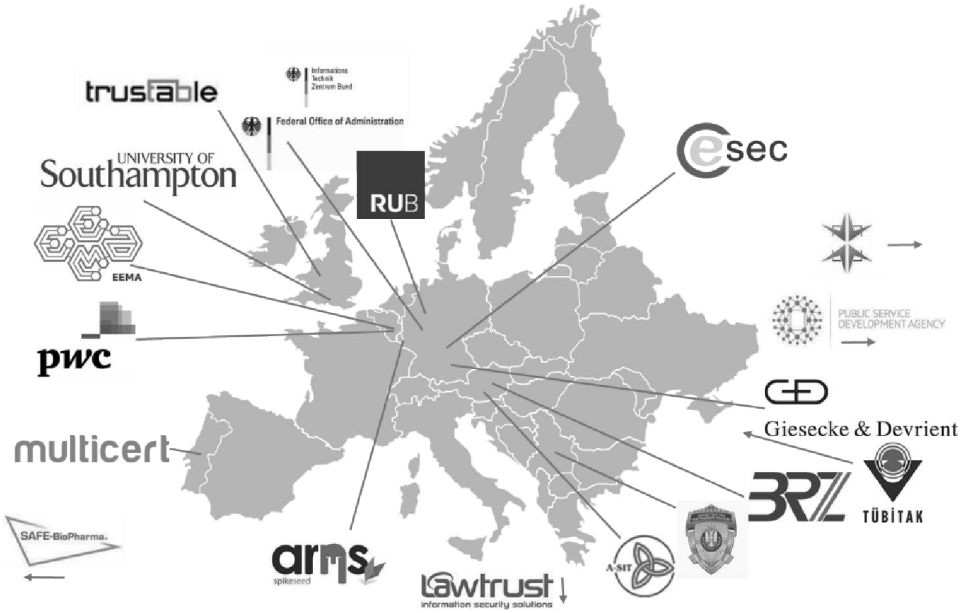

Figure 1: FutureTrust Partners

Furthermore the FutureTrust project is supported by selected subcontractors and an unlimited number of associated partners, which currently includes the German Federal Information Technology Centre (Informationstechnikzentrum Bund (ITZBund)), A-SIT Plus GmbH (Austria), the SAFE Biopharma Association (USA) and the National Certification Authority Rus (NCA Rus) (Russia).

Note that the FutureTrust project is open for collaboration with additional associated partners and especially invites **Trust Service Providers** according to [EU1] or similar policy frameworks to participate in the FutureTrust project and benefit from the envisioned research and development.

2.2 FutureTrust System Architecture

As shown in Figure 2, the FutureTrust system integrates existing and emerging eIDAS Trust Services, eIDAS Identity Services and similar Third Country Trust & Identity Services and provides a number of FutureTrust specific services, which aim at facilitating the use of eID and electronic signature technology in different application scenarios.

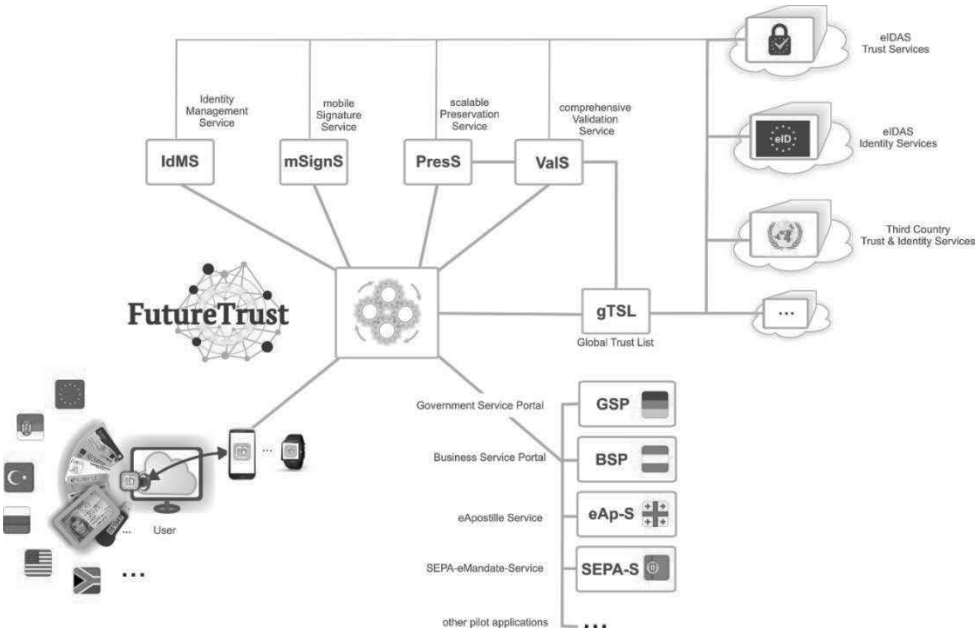

Figure 2: FutureTrust System Architecture

2.3 Global Trust List (gTSL)

The gTSL is envisioned to become an Open Source component, which can be deployed with the other FutureTrust services or as standalone service and which allows to manage Trust Service Status Lists for Trust Services and Identity Providers. The gTSL will allow to import the European "List of the Lists" (LOTL), which is a signed XML document according to [ETSI7] and all national Trust Service Status Lists (TSLs) referenced therein. This LOTL is currently published by the European Commission. This import includes a secure verification of the digital signatures involved. The gTSL will also allow to import Trusted Lists from other geographic regions, such as the Trust List of the Russian Federation[23] for example, and it is envisioned that the gTSL will generate a "virtual US-American Trust List" from the current set of available cross-certificates. gTSL will provide support for the traceable assessment of trust related aspects for potential trust anchors both with and without known trustworthiness and assurance levels[24] by providing claims or proofs of relevant information with respect to the trustworthiness of a trust service. This may give rise for a reputation based "web of trust" for trust services. It is expected that the corroboration of information from

[23] See http://e-trust.gosuslugi.ru/CA/DownloadTSL?schemaVersion=0.

[24] [EU1] implicitly defines the levels "qualified" and "non-qualified" for trust service providers and explicitly introduces in Article 8 the assurance levels "low", "significant" and "high" for electronic identification schemes.

relatively independent sources[25] will help to establish trustworthiness. Furthermore the gTSL is planned to provide a web interface as well as a SOAP or REST interface allowing for a small set of predefined queries, to allow the other FutureTrust services or other gTSL deployments to access the validated data. For implementation of the underlying gTSL model various options have already been identified. These include traditional models such as a Trusted Third Party model and a Trust List, as well as innovative models such as a semantic web ontology and a blockchain ledger.

2.4 Comprehensive Validation Service (ValS)

The major use case of ValS is the validation of Advanced Electronic Signatures (AdES) in standardized formats, such as CAdES, XAdES and PAdES for example. In order to support the various small legal and regulatory differences with respect to electronic signatures coming from different EU Member States or other global regions, the ValS will support practice oriented XML-based validation policies for electronic signatures, which consider previous work in this area, such as [ETSI4] and [ETSI6] and current standards, such as [ETSI1] and [ETSI8] for example. The ValS is envisioned to issue a verification report to the requestor of the service, which may be based on a revision of the OASIS DSS Signature Verification report [OAS4], which in particular considers the procedures defined in [ETSI1] and the XML-based validation policies mentioned above. This revised verification report may be brought back to standardization as a contribution to EN 319 102-2, which is planned[26] to be developed, but for which the standardization work has not yet started. Finally, it seems worth to be mentioned that the ValS is planned to be designed in an extensible manner, such that modules for other not (yet) standardized signatures or validation policies can be plugged into the ValS in a well-defined manner.

2.5 Scalable Preservation Service (PresS)

The PresS is used to preserve the integrity and conclusiveness of a signed document over its whole lifetime. For this purpose, the FutureTrust Preservation Service as outlined in Figure 3 will use the ValS and existing external time stamping services in order to produce Evidence Records according to [RFC1] and possibly [RFC2]. As depicted in Figure 3 the Preservation Service may support different input interfaces based on [OAS1] and [BSI1] for example and integrate various types of storage systems.

Unlike in [BSI2] the FutureTrust Preservation Service may however not use a rather inefficient XML-based Archive Information Package (AIP) structure, but possibly a zip-based container along the lines of the Associated Signature Container (ASiC) specification according to [ETSI2] as this would provide an easy to use and space efficient container format. An important goal of the envisioned Preservation Service is

[25] See [Sel16].
[26] See [ETSI5].

scalability, which may be realized by using efficient data structures, such as Merkle hash trees as standardized in [RFC1] for example. Using hash tree based signatures[27] may also provide additional security in the case that quantum computers have been built, because any digital signature that is in use today (based on the RSA assumption or on the discrete log assumption) can be forged in this case. However, message authentication codes (MACs), block-chain constructions and signature algorithms based on hash-trees seem to remain secure. Thus it is an interesting research question, whether fully operational and sufficiently performant preservation services can be built on MACs, block-chains or hash-trees alone.

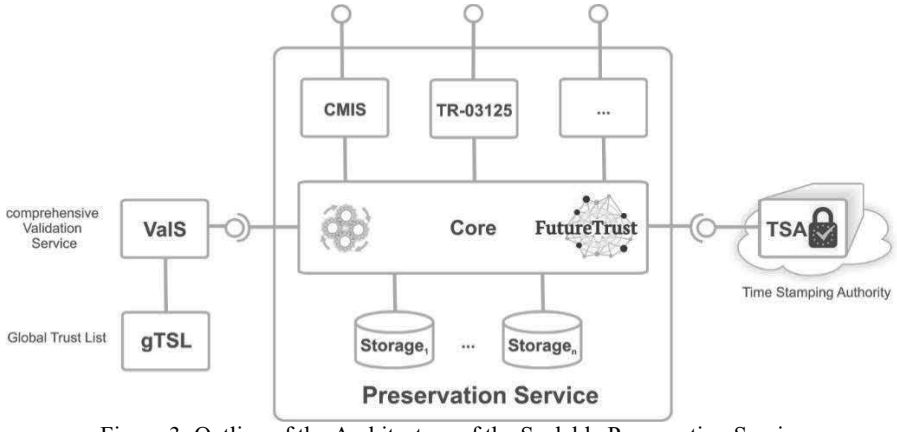

Figure 3: Outline of the Architecture of the Scalable Preservation Service

2.6 Identity Management Service (IdMS)

Many EU Member States and some non-European countries have established eID services, which produce slightly different authentication tokens. Within the EU, most[28] of these services produce SAML tokens (see [Zwa12]) and the eIDAS interoperability framework [eIDAS] is also based on [SAML]. In addition, industrial standardization activities have produced specifications like FIDO[29] or GSMA's MobileConnect[30] which have gained a broad customer base. The IdMS will be able to consume a broad variety of such authentication tokens (SAML, OpenID Connect, OAuth), work with a broad variety of mobile identification services (FIDO, GSMA MobileConnect, European Citizen cards) and transform them into a standardized, interoperable[31] and secure[32] format. The

[27] See [Buc09].
[28] The [Fra16] system seems to be an exception to this rule, as it produces and accepts identity tokens according to the [Ope15] specification.
[29] See [FID15].
[30] See [MOB] and [GSM15].
[31] Due to the fact that SAML is a very complex and highly extensible standard, the integration of different eID services considering all extensions points is a rather challenging task. In order to enable the communication between all eID services, their interoperability has to be thoroughly analysed.

choice of this standardized format will be based on industry best practices, and on the eIDAS interoperability framework [eIDAS]. Moreover, the IdMS is envisioned to be able to directly communicate with a selection of European and non-European eID services.

2.7 Mobile Signature Service (mSignS)

The mSignS will enable the remote creation of qualified electronic signatures and seals in a mobile environment[33]. For this purpose the mSignS will be operated in a secure environment and may contain an appropriate Hardware Security Module (HSM) which hosts the private keys of the signatories. While these keys are hosted at a central place, they are kept under the sole control of the Signatory as described in [CEN1]. In order to reach this seemingly contradictory requirement the FutureTrust project will in particular research means for securely sharing the private signing key between the mobile device of the Signatory and the HSM located at the mSignS or the along the lines of [Kut13].

---

[32] Based on [eIDAS] it is clear that SAML 2.0 will form the basis for eIDAS Interoperability Framework according to Article 12 of [EU1] and [EU2], but it is currently likely that the Assertions will be simple "Bearer Tokens", which is not optimal from a security point of view. Furthermore, the different authentication flows and optional message encryptions result in complex standard and thus expose conforming implementations to new attacks. In the last years, several papers (see e.g. [Som12]) showed how to login as an arbitrary use in SAML Single Sign-On scenarios or decrypt confidential SAML messages (see e.g. [Jag11]). Thus, existing eID services can be evaluated against known attacks and existing risks can be discovered. As a result, a metric to measure the security of eID services will be elaborated.

[33] See [Kub15] and [ETSI3] for more information on mobile signatures.

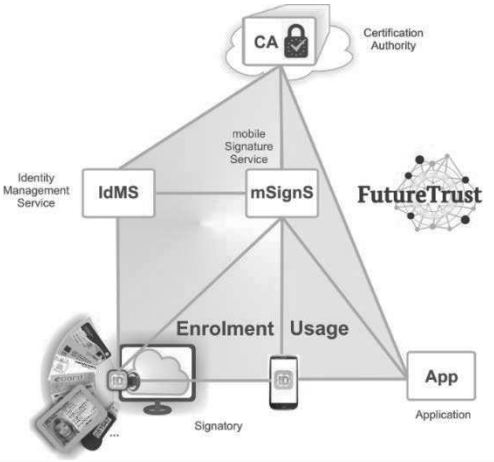

Figure 4: Enrolment and Usage Phase for Mobile Signing

As outlined in Figure 4, one may distinguish the enrolment phase and the usage phase. During enrolment, the Signatory uses his eID and the IdMS to perform an eID-based identification and registration at the mSignS or the Certification Authority (CA). The mSignS or the CA will create a key pair for the Signatory and requests or create a certificate. Within the enrolment phase, the mSignS or the CA will also provide appropriate credentials to the Signatory and her mobile device, which can later on be used to authenticate at the mSignS in order to trigger the signature creation within some application specific context. The OASIS DSS Extension for Local Signature Computation [OAS2] may be used as a protocol to expose the signing functionality of a local key under Signatory's sole control.

2.8 FutureTrust Pilot Applications

The FutureTrust consortium aims to demonstrate the project's contributions in a variety of demonstrators and pilot applications, which are planned to include a Governmental Service Portal, a Business Service Portal, an e-Apostille Validation System and a SEPA e-Mandate Service according to [EPC] for example. Furthermore the FutureTrust project is open for supporting further pilot applications related to innovative use cases for eID and electronic signature technology.

3 Summary and Invitation for Collaboration

The present paper provides an overview of the FutureTrust project, which will start on June 1st 2016 and which will be funded by the European Commission within the EU Framework Programme for Research and Innovation (Horizon 2020) under the Grant

Agreement No. 700542 with up to 6,3 Mio. .

As explained throughout the paper, the FutureTrust project will conduct basic research with respect to the foundations of trust and trustworthiness, actively support the standardisation process in relevant areas, and plans to provide innovative Open Source software components and trustworthy services which will enable ease the use of eID and electronic signature technology in real world applications by addressing the problems P1 to P7 introduced in Section 1.

Against this background the FutureTrust consortium invites interested parties, such as Trust Service Providers, vendors of eID and electronic signature technology, application providers and other research projects to benefit from this development and join the FutureTrust team as associated partner.

References

[EC1] 1999/93/EC. (1999). Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093.

[EU1] 2014/910/EU. (2014). Regulation (EU) No 910/2014 of the European Parliament and of the council 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/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

[EU2] 2015/1501/EU. (2015). Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014. *of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance)* . http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0001.

[EU3] 2016/679/EU. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, . *and repealing Directive 95/46/EC and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)* . http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

[3xA16] 3xA Security AB . (2016). EU Trust Service status List (TSL) Analysis Tool. http://tlbrowser.tsl.website/tools/.

[EC2] 95/64/EC. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.

[BSI1] BSI TR-03125-E. (2015, January 31). Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI). *Preservation of Evidence of Cryptographically Signed Document - Annex E: Concretisation of the Interfaces on the Basis of the eCard-API-Framework* . https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/

TG03125/BSI_TR_03125_TR-ESOR-E_V1_2_EN.pdf?__blob=publicationFile&v=4: Technical Guideline 03125, Annex E, Version 1.2.

[BSI2] BSI TR-03125-F. (2015, January 31). Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI). *Preservation of Evidence of Cryptographically Signed Documents - Annex F: Formats* . https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/BSI_TR_03125_TR-ESOR-F_V1_2_EN.pdf?__blob=publicationFile&v=2: Technical Guideline 03125, Annex F, Version 1.2.

[Buc09] Buchmann, J., Dahmen, E., & Szydlo, M. (2009). Hash-based digital signature schemes. In *Post-Quantum Cryptography* (pp. 35-93). Springer.

[CEN1] CEN/TS 419 241. (2014). Security Requirements for Trustworthy Systems supporting Server Signing.

[DIR] Directory of Signature Creation Devices. (2016). *Open Signature Initiative*. Retrieved from http://opensignature.org/devices/

[eIDAS] eIDAS Spec. (2015, November 26). eIDAS Technical Subgroup. *eIDAS Technical Specifications v1.0* . https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v10.

[EPC] EPC 208-08. (2013, April 9). European Payments Council. *EPC e-Mandates e-Operating Model - Detailed Specification* . Version 1.2: http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/epc-e-mandates-e-operating-model-detailed-specification/epc208-08-e-operating-model-detailed-specification-v12-approvedpdf/.

[ETSI1] ETSI EN 319 102-1. (2016, May). Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, Version 1.1.1. http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf.

[ETSI2] ETSI EN 319 162-1. (2015, August). Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers. http://www.etsi.org/deliver/etsi_en/319100_319199/31916201/01.00.00_20/en_31916201v010000a.pdf.

[ETSI3] ETSI SR 019 020. (2016, February). The framework for standardisation of signatures: Standards for AdES digital signatures in mobile and distributed environments. *V1.1.1* . http://www.etsi.org/deliver/etsi_sr/019000_019099/019020/01.01.01_60/sr_019020v010101p.pdf.

[ETSI4] ETSI TR 102 038. (2002, April). TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies.

[ETSI5] ETSI TR 119 000. (2016, April). Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview. Version 1.2.1: http://www.etsi.org/deliver/etsi_tr/119000_119099/119000/01.02.01_60/tr_119000v010201p.pdf.

[ETSI6] ETSI TS 102 853. (2012, July). Electronic Signatures and Infrastructures (ESI); Signaturue verification procedures and policies. *V1.1.1* . http://www.etsi.org/deliver/etsi_ts/102800_102899/102853/01.01.01_60/ts_102853v010101p.pdf.

[ETSI7] ETSI TS 119 612. (2016, April). Electronic Signatures and Infrastructures (ESI); Trusted Lists. *Version 2.2.1* . http://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.02.01_60/ts_119612v020

201p.pdf.
[ETSI8] ETSI TS 199 172-1. (2015, July). Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents. http://www.etsi.org/deliver/etsi_ts/119100_119199/11917201/01.01.01_60/ts_11917201v010101p.pdf.
[EUTL] EU Trusted Lists of Certification Service Providers. (2016). *European Commision*. Retrieved from https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers
[FID15] FIDO. (2015). *FIDO Alliance*. Retrieved from https://fidoalliance.org/
[Fra16] FranceConnect. (2016). https://doc.integ01.dev-franceconnect.fr/.
[MOB] GSMA. (2015). *Introducing Mobile Connect – the new standard in digital authentication*. Retrieved from http://www.gsma.com/personaldata/mobile-connect
[GSM15] GSMA-CPAS5. (2015). CPAS 5 OpenID Connect - Mobile Connect Profile - Version 1.1. https://github.com/GSMA-OneAPI/Mobile-Connect/tree/master/specifications.
[Jag11] Jager, T., & Somorovsky, J. (2011). How to break xml encryption. *Proceedings of the 18th ACM conference on Computer and communications security* .
[Kub15] Kubach, M., Leitold, H., Roßnagel, H., Schunck, C. H., & Talamo, M. (2015). SSEDIC.2020 on Mobile eID. *to appear in proceedings of Open Identity Summit 2015.*
[Kut13] Kutylowski, M., & Kubiak, P. (2013, May 06). Mediated RSA cryptography specification for additive private key splitting (mRSAA). *IETF Internet Draft, draft-kutylowski-mrsa-algorithm-03* . http://tools.ietf.org/html/draft-kutylowski-mrsa-algorithm-03.
[OAS1] OASIS CMIS v1.1. (2013, May 23). Content Management Interoperability Services (CMIS). http://docs.oasis-open.org/cmis/CMIS/v1.1/CMIS-v1.1.html.
[OAS2] OASIS DSS LocSig. (2015, July 27). *DSS Extension for Local Signature Computation Version 1.0.* Retrieved from Committee Specification: http://docs.oasis-open.org/dss-x/localsig/v1.0/cs01/localsig-v1.0-cs01.pdf
[OAS3] OASIS DSS v1.0. (2010, November 12). *Profile for Comprehensive Multi-Signature Verification Reports Version 1.0.* Retrieved from http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-vr-cs01.pdf
[OAS4] OASIS-DSS. (2007, April 11). *Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0.* Retrieved from OASIS Standard: http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html
[Ope15] OpenID Connect. (2015). OpenID Foundation. *Welcome to OpenID Connect* . http://openid.net/connect/.
[RFC1] RFC 4998. (2007, August). Gondrom, T.; Brandner, R.; Pordesch, U. *Evidence Record Syntax (ERS)* . https://tools.ietf.org/html/rfc4998.
[RFC2] RFC 6238. (2011, July). Jerman Blazic, A.; Saljic, A.; Gondrom, T. *Extensible Markup Language Evidence Record Syntax (XMLERS)* . https://tools.ietf.org/html/rfc6283.
[SAML] SAML 2.0. (2005, March 15). *OASIS Standard.* Retrieved from Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf
[SDDSS] SD-DSS. (2011, August 09). *Digital Signature Service | Joinup*. Retrieved from https://joinup.ec.europa.eu/asset/sd-dss/description
[Sel16] Sel, M. (2016). Improving interpretations of trust claims, published in the proceedings of the. *Trust Management X: 10th IFIP WG 11.11 International Conference, IFIPTM 2016* (pp. 164-173). Darmstadt, Germany: Springer.
[SkID] SkIDentity. (2016). Retrieved from https://www.skidentity.com/

[Som12] Somorovsky, J., Mayer, A., Schwenk, J., Kampmann, M., & Jensen, M. (2012). On breaking saml: Be whoever you want to be. *Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)* .

[STO2] STORK 2.0. (2014). Retrieved from https://www.eid-stork2.eu/

[STO] STORK. (2012). Retrieved from https://www.eid-stork.eu/

[Zwa12] Zwattendorfer, B., & Zefferer, T. T. (2012). The Prevalence of SAML within the European Union. *8th International Conference on Web Information Systems and Technologies (WEBIST)*, (pp. 571-576). http://www.webist.org/?y=2012.