WP43 – Trust Service

D43.2 - Requirements analysis

Document Identification	
Date	11.12.2013
Status	Final
Version	0.7

Related SP / WP	SP4/WP43	**Document Reference**	D43.2
Related Deliverable(s)	D21.2, D21.4, D32.1, D41.1, D43.1	**Dissemination Level**	PU
Lead Participant	SK	**Lead Author**	Tarvi Martens, Maili Keskel
Contributors	Detlef Hühnlein (ECS), Eray Özmü (USTUTT), Nuria Ituarte Aranda (Atos), Christof Rath (TUG)	**Reviewers**	Monika Drabik (CA), Detlef Houdeau (IFAG)

This document is issued within the frame and for the purpose of the FutureID project. This project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318424

Abstract

The present document provides a brief overview of relevant standards and infrastructures for trust services and specifies requirements for the Trust Service (TS) of the FutureID-infrastructure.

Document Information

History

Version	Date	Author	Changes
0.1	14.06.2013	Detlef Hühnlein	Created document structure
0.2	20.06.2013	Tarvi Martens	First draft with real content
0.3	22.10.2013	Maili Keskel	Supplemented the Table of Contents with chapter 5 and 6
0.4	05.11.2013	Nuria Ituarte Aranda	Added chapter 6
0.5	08.11.2013	Christof Rath	Added chapter 5
0.6	11.11.2013	Eray Özmü	Added chapter 4.1 which is derived from deliverable D43.1
0.65	09.12.2013	Eray Özmü	Replaced the architecture image with the new version
0.7	11.12.2013	Maili Keskel	Final version taking into consideration the reviewers comments

Table of Contents

Contents

1. Introduction

1.1 Scope

FutureID Trust Services (TS) is a framework that is capable to collect trust status information (including their digital identity and assurance level) of identity providers and to integrate that information into a common database. This database will be accessed by a validation service to validate an identity provider with respect to trustworthiness and suitability for a required assurance level.

The scope of this document is to analyze existing relevant standard and trust information sources and finally provide the requirements for the Trust Service (TS).

1.2 Outline

The present document provides in Section 2 a brief overview of existing standards and infrastructures for trust-related services and Section 3 specifies the requirements of the TS.

1.3 Terminology

1.3.1 Key Words

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].

1.3.2 Abbreviations and Notations

eID	Electronic Identity
IdP	Identity Provider
OCSP	Online Certificate Status Protocol
SP	Service Provider
TSL	Trusted-Service Status
TS	Trust Service
TSP	Trust Service Provider
TL	Trust Service Status List
VS	Validation Service
SAML	Security Assertion Markup Language
CA	Certification Authority
HTTPS	Hypertext Transfer Protocol Secure
XML	Extensible Markup Language
XKMS	XML Key Management Specification
XKISS	XML Key Information Service Specification
OASIS	Advancing Open Standards for the Information Society
CIP	The Competitiveness and Innovation framework Programme
TA	Trust Aspect
ETSI	European Telecommunications Standards Institute
QAA	Quality of Authentication Assurance

2. Standards and infrastructures for trust-related services

The most contemporary and evolving standard for distributing trust information today is ETSI standard "*Provision of harmonized Trust-service status information*" [2]. Although this standard aims to cover wide selection of trust services, the practical implementations circle around TSP providing end-user X.509 certificates.

The only practical pan-European use of Trusted Lists was triggered by the Commission Decision 2009/767/EC and amended by the Commission Decision 2010/425/EU. The result is collection of TL-s published by every Member State covering TSP-s and their services providing Qualified Certificates limited for digital signing. The "List of the Lists" miaintained by European Comission is containing pointers to individual TL-s of Member States along with necessary validation material.

It shall be noted that abovementioned TL-s are usable only in context of qualified electronic signatures and thus not covering anything else such like non-qualified certificates, certificates for authentication or HTTPS servers.

Specialized set of trust sources are Certificate Stores of browsers such as Microsoft IE, Mozilla, Apple Safari, Opera and others. Those are entriely targeted to distribute information about trusted CA-s providing certificates for HTTPS servers.

In the SAML world, trust is distributed using SAML-metadata structures as defined in [3]. These are similar to Trust Lists by containing Service Provider's information and information for validation of SAML assertions. However, SAML-metadata contains additional information about entity roles representing common combinations of SAML protocols and profiles supported by system entities.

There are several existing and widely used standards for **validation** of digitally signed content. RFC 3280 [8] Chapter 6 and RFC 4158 [9] give instructions for X.509 certificate path validation, Certificate Revocation Lists [8] and Online Certificate Status Protocol [10] are used for obtaining certificate validity information. Server-Based Certificate Validation Protocol [11] includes both certificate and path validation on the server-side. In the XML world there is standards like XML Key Management Protocol [12] suitable for registration and validiation of public keys and OASIS Digital Signature Specification [13] for signing and verifying XML documents and other data.

Another area of interest in Trust Services is **quality** of the TSP. With regard to electronic signatures in Europe, just two levels for certificates – qualified and non-qualified are defined by the Directive backed by ETSI TS 101456 [14] and ETSI TS 102042 [15]. Additionally there is dimension of SSCD (*Secure Signature Creation Device*) backed by EAL4+ [16].

There are several studies and results of EU CIP Large Scale Pilot Projects (LSP-s) proposing different methods for establishing TSP quality levels such as CROBIES study [4] aligned with PEPPOL work on the subject [5]. STORK QAA model [6] has been developed for assessing

security levels for authenticalion purposes. A newly adotped ISO standard [7] addresses entity authentication assurance like in STORK but gives more broader and international coverage.

3. The FutureID Trust Service

The following figure shows the context of the Trust Service within the FutureID Infrastructure, as explained in the FutureID Reference Architecture.

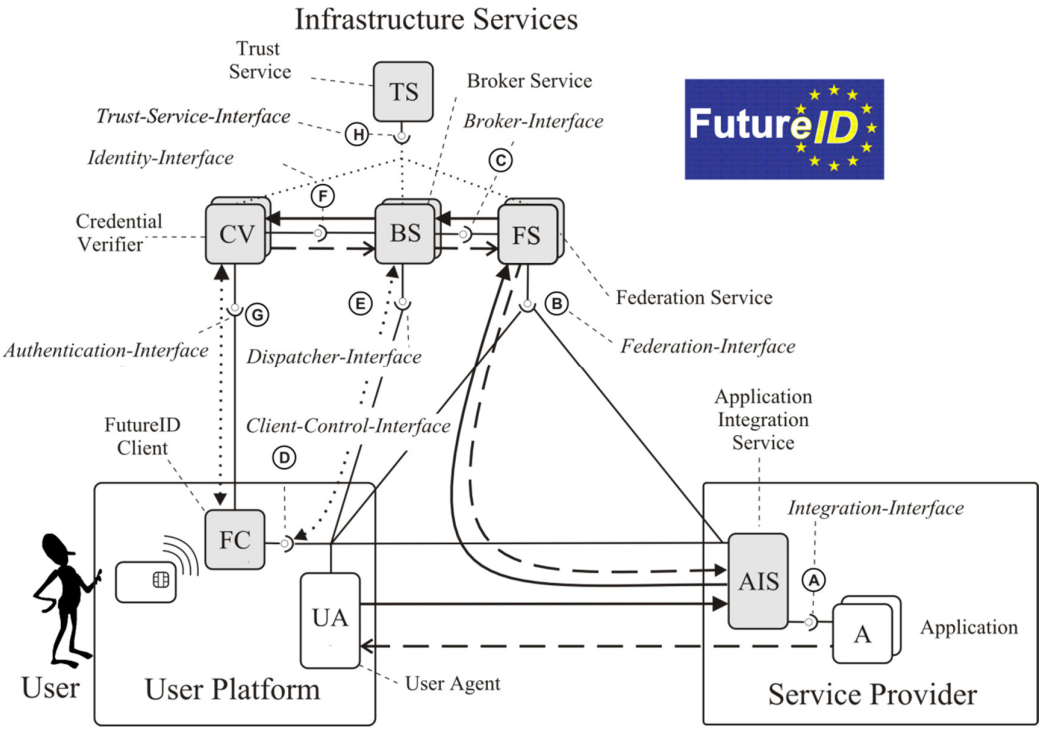

Figure 1: Trust Service within the FutureID infrastructure

FutureID Trust Service has two levels. The "upper" layer is essentially a central Trust List (FutureID-TL) in style of [2] adjusted and enhanced to accommodate the following:

- Certification Authorities issuing certificates for authentication
- Certification Authorities issuing certificates for HTTPS servers
- SAML signers – information from SAML-metadata [3] is merged into FutureID-TL

Every service in the FutureID-TL is accompanied by Quality Parameter(s). Finally, every CA service in the FutureID-TL explicitly linked with Validation Service described in the same list.

The "lower" layer is a Validation Service (FutureID-VS) which could exist in several instances and serve for implementation of local (enterprise) security policy besides performing actual validation of cryptographically signed artefacts such as

- X.509 certificates
- OCSP responses
- SAML assertions
- digital signatures
- …

The FutureID-VS makes use of FutureID-TL and applies additional security policy by:

- Filtering out individual Trust Services
- Additional (local) individual Trust Services
- Filtering out certs with weak cryptographic keys and/or algorithms
- Applying security level threshold – setting the lowest allowed value for Quality Parameter(s).

The following figure provides an outline of the FutureID Trust Service described in this chapter:

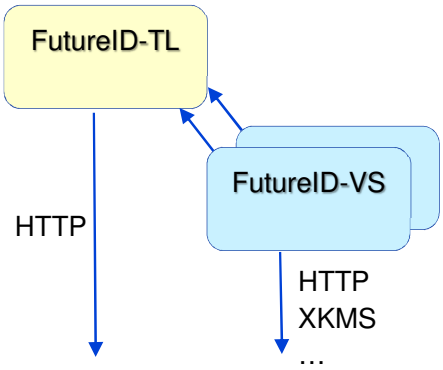

Figure 2: Trust Service

4. Requirements for Trust Service

This chapter gives an overview of the different requirements for the trust repository and the trust services. To be able to have a better understanding on how trust aspects can be met by FutureID, the deliverable D43.1 was analysed before writing the following requirements.

4.1 General Trust Aspects derived from Deliverable D43.1

Deliverable D43.1 was concerned with an in-depth analysis of different aspects of trust in context of FutureID. The outcome of this document was a list of recommendations for the FutureID project to be able to fulfill trust for the different stakeholders involved in FutureID.

The following recommendations have been made by the authors of D43.2.

No.	TA-01 – Choice of identification token
Description	Required authentication token SHOULD be considered for each transaction.

No.	TA-02 – Level of Assurance Framework
Description	FutureID SHOULD support arbitrary frameworks by providing means to map between LoA frameworks. However the use of single frameworks SHOULD be possible.

No.	TA-03 – Assurance levels
Description	The weakest link MUST define the overall assurance level. This also is applied when multiple identity tokens are merged into one.

No.	TA-04 – Federation agreement
Description	A federation agreement MUST be in place between federation partners. SP SHOULD trust the IdP regarding identity mapping, enrolment procedures and policies. User SHOULD trust the IdP to preserve the User's privacy User SHOULD trust the SP to not reveal User data unless authorized.

4.2 Trust Repository – FutureID-TL

No.	TL-01 – Standard-base
Description	The FutureID-TL MUST base on ETSI Trust List standard [2].

No.	TL-02 – SAML-Metadata-support

Description	The FutureID-TL MUST support SAML-Metadata structures as specified in [3].

No.	TL-03 – SAML-Metadata-conversion
Description	There SHALL be tools for conversion of SAML-Metadata files into FutureID-TL structure and vice versa

No.	TL-04 – Explicit-support-for-specific-CAs
Description	The FutureID-TL MUST have explicit support for root certificates and Certification Services dedicated to issuing of certificates for authentication and certificates for HTTPS.

No.	TL-05 – Quality-parameters
Description	The FutureID-TL MUST have support for indication of service quality.

No.	TL-06 – Import-from-EUTL
Description	There SHALL be tools for importing trust information from Member States national Trust Lists published according to Commission Decision 2009/767/EC and amended by the Commission Decision 2010/425/E.

No.	TL-07 – Editing-tools
Description	There SHALL be tools for editing of FutureID-TL

No.	TL-08 – OCSP-binding
Description	The FutureID-TL MUST provide means for explicitly associating a CA service to corresponding OCSP service.

4.3 Validation Service – FutureID-VS

No.	VS-01 – Trust-source
Description	The FutureID-VS MUST make use of FutureID-TS for base trust information.

No.	VS-02 – Trust-base-modification
Description	The FutureID-VS MUST support filtering out certain Trust Services or Trust Service Providers based on individual criteria. Additionally, the FutureID-VS MUST provide means for adding individual Trust Services.

No.	VS-03 – Cryptographic-strength
Description	The FutureID-VS MUST support establishment of minimum cryptographic strength in terms of algorithms and key lengths in order to filter out Trust Services falling beyond the established level.

No.	VS-04 – Quality-level
Description	The FutureID-VS MUST support establishment of minimum Quality Level in order to filter out Trust Services falling beyond the established level.

No.	VS-05 – OCSP-support
Description	The FutureID-VS MUST provide OCSP [10] service for validation of certificates from different CA-s.

No.	VS-06 – XKMS-support
Description	The FutureID-VS SHALL provide XKMS service [12] for validation of certificates (X-KISS).

No.	VS-07 – Server-based Certificate Validation Protocol (SVCP) support
Description	The FutureID-VS MAY provide SVCP [11] service for server-based validation of certificates.

No.	VS-08 – Digital Signature Service (DSS) support
Description	The FutureID-VS MAY provide DSS [13] service for validation of digital signatures.

5. Trust status information

In traditional authentication scenarios one specific type of credential is used to authenticate against a single service. In this case, the required level of trustworthiness is given implicitly by selecting the appropriate type of credential.

FutureID, as a framework that supports many types of credentials for arbitrary services, requires means to specify the quality of a credential and, hence, the quality of the resulting authentication. Thus, the service provider will, generally, not ask for a specific type of credential, but for a certain level of trustworthiness.

In the past, several frameworks evolved to classify the trustworthiness of credentials and eID tokens. Noteworthy in this context is the Quality of Authentication Assurance (QAA) framework [18] developed by STORK (see also Chapter 6). However, there are several other currently existing or evolving frameworks. *FutureID*, therefore, should be able to support multiple frameworks of trust status information.

Within *FutureID*, the Trust Services module will manage and provide this information. The trust repository will be based on ETSI Trust List [2] standard. Hence, the information about the trust status should also be stored in the TSL. The standard already defined a service level extension `additionalServiceInformation`, which can be used for that purpose. This extension requires an `URI` that identifies the additional service information and, optionally, an `InformationValue` and `OtherInformation`.

In this context the `URI` has to identify the concrete framework for trust status information and the `InformationValue` will be the numeric assurance level value, e.g. *http://www.stork.gov.eu/1.0/citizenQAALevel* and a value between 1 and 4. The `additionalServiceInformation` extension can occur multiple times for a single service, thus, it is possible to provide the trust status information for several frameworks and the service providers are free to choose any of the available frameworks.

No.	TL-09 – Non-PKI services
Description	The FutureID-TL MUST be able to handle trust and assurance information for non-PKI based services like facebook or OTP-based (One-Time Password based) authentication.

6. Assurance levels evaluation (based on STORK levels)

For the purpose of defining the authentication assurance levels in FutureID, the STORK Quality of Authentication Assurance (QAA) model has been considered (it has been considered before in [17]).

This model defines authentication assurance levels in terms of organizational and technical factors that have influence in the authentication process. Two phases set up the authentication process: registration phase and authentication phase [6].

For the registration phase, the organizational factors that should be considered are the following:

- The quality of the identification procedure
- The quality of the issue of the credential
- The quality of the entity issuing the credential

For the authentication phase (on-line electronic authentication), the technical factors that should be considered:

- The type and the robustness of a credential (e.g., an ID token)
- The security features of the authentication mechanism (that is, the quality of the mechanism) in the remote authentication

Service Providers will have to manage the associated risks such as the risk of providing a service to a wrong user.

STORK has defined 4 levels of assurance for the quality of authentication. The levels are classified according to the severity of the impact of damages that might arise from dishonest use of a person's identity. The greater the potential consequence of identity abuse the greater the confidence in the selected identity that will be needed.

STORK defines the following levels (taken from section 2.1 of [6]):

"STORK QAA level 1 is the lowest assurance level; it either assures a minimal confidence in the asserted identity or no confidence at all. Identity credentials are accepted without any form of verification. If the subscriber provides an e-mail address, the only check that is performed is the verification of the correctness of the e-mail address. This level is appropriate when negative consequences that result from an erroneous authentication have a very low or a negligible impact. This level suits recognised on-line services implementing either a minimal set of security protection mechanisms or no set at all.

STORK QAA level 2 defines the level used by those services where damage from a misappropriation of a real-world identity has a low impact. Even if the claimants are not required to appear physically during the registration, their real-world identities must be validated and a token issued by a body subjected to specific governmental agreement. Identity

tokens must be delivered with accuracy and security guarantees. Sufficiently robust authentication protocols must be used during the electronic authentication phase.

STORK QAA Level 3 defines the level used by services that may suffer substantial damages in case of an identity misuse. The registration of an identity is processed with methods that unambiguously and with a high level of certainty identify the claimant. The identity providers are supervised or accredited by the government. The credentials delivered are at least soft certificates or hard certificates. The authentication mechanisms used in the remote authentication phase are robust.

STORK QAA Level 4 is the highest assurance level and addresses those services where damage caused by an identity misuse might have a substantial impact. The registration requires at least once (i.e., the very first time of the request but not for a later renewal) either the physical presence of the claimant or a physical meeting with the claimant (e.g., a certificate is requested on-line, delivered at home, and deployed in the hands of the claimant after a physical check of his/her identity). Alternatively, in the case of on-line registration, a claimant identity is validated using trusted e-signatures. Annex II of the e-signature Directive 1999/93/EC leaves the details of identity verification to national law. Therefore, level 4 is fulfilled if the national legal requirements for issuing a qualified certificate have been met. Furthermore, the identity provider must be a qualified entity according to Annex II of the e-signature Directive. The certificates are hard certificates qualified according to Annex I of the e-signature Directive. The most robust authentication mechanisms are used during the authentication phase." [6]

The Service Provider has to analyze risks associated to provide access to certain users such as eavesdropping, replay, man-in-the-middle, not secure processes of handling out credentials, stolen passwords and so forth). These risks should be analyzed and taken into account for establishing the mapping to an authentication assurance level.

The Service Provider should also take into account that a higher level of assurance implies more security as well as the exclusion of a larger group of users who don't own credentials of that quality.

Once the levels are established for the FutureID services (taken into account the mentioned organizational and technical factors), the authentication process would be as follows: the user wishes to access a service offered by a Service Provider, first of all the user selects authentication. The Service Provider sends the request for authentication and the information of the assurance level that is required for authentication. FutureID provides a list of possible eID that can provide the user identity and satisfy the assurance level required for the Service provider. The user selects the eID, and asks for authentication to the correspondent Identity Provider.

7. Conclusion

The present document contains the specific requirements for the TS. Further requirements for the overall FutureID architecture, which in turn may induce additional requirements for the TS, can be found in the deliverables of FutureID WP 22 (i.e. D22.1-D22.7).

As the overall FutureID architecture (cf. Task 21.4) and the corresponding overall requirements (cf. Tasks 22.1-22.7) are not finalized yet, the present list of requirements may be seen as preliminary until the overall FutureID architecture and its corresponding requirements are final. Nevertheless the requirements specified in the present document already provide a fairly solid foundation for the outline and design of the TS in the following tasks of WP 43.

8. Bibliography

[1] S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, 1997.
[2] ETSI, Electronic Signatures and Infrastructures (ESI), Provision of harmonized Trust-service status information, ETSI TS 102 231 V3.1.2 , 2009.
[3] OASIS: Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, 2005.
[4] CROBIES : Study on Cross-Border Interoperability of eSignatures 2010
[5] PEPPOL Deliverable D1.3 Demonstrator and functional Specifications for Cross-Border Use of eSignatures in Public Procurement. Part 7: eID and eSignature Quality Classification
[6] STORK D2.3 - Quality authenticator scheme
[7] ISO/IEC FDIS 29115 Information technology — Security techniques — Entity authentication assurance framework
[8] RFC 3280: Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile. 2002
[9] RFC 4158: RFC Internet X.509 Public Key Infrastructure: Certification Path Building, 2005
[10] RFC 2560: X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP, 1999
[11] RFC 5055: Server-Based Certificate Validation Protocol (SCVP), 2007
[12] W3C: XML Key Management Specification (XKMS), 2001
[13] OASIS: Digital Signature Services v1.0, 2007
[14] ETSI TS 101 456: Electroninc Ssignatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, ver 1.4.3, 2007.
[15] ETSI TS 102 042: Electroninc Ssignatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, ver 2.1.1, 2009.
[16] CEN CWA 14169: Secure Signature-Creation Devices "EAL 4+", 2002.
[17] FutureID D43.1 - Analysis of Trust Aspects
[18] STORK D2.3 - Quality authenticator scheme