



Social Economic Evaluation of FutureID

D12.6

Document Identification	
Date	23.10.2015
Status	Final
Version	1.01

Related SP / WP	SP1 / WP12	Document Reference	D12.6
Related Deliverable(s)	D12.1, D22.1, D21.2, D21.4	Dissemination Level	PU
Lead Participant	FHG	Lead Author	Heiko Roßnagel (FHG)
Contributors	Heiko Roßnagel (FHG), Rachele Sellung (FHG), Michael Kubach (USTUTT)	Reviewers	DTU, G&D

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

This document and its content are the property of the FutureID Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the FutureID Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the FutureID Partners.

Each FutureID Partner may use this document in conformity with the FutureID Consortium Grant Agreement provisions

Not to be distributed outside the FutureID Consortium

Document name:	SP1 /WP12			Page:	1 of 52		
Reference:	D12.6	Dissemination:	PU	Version:	1.01	Status:	Final

1. Abstract

In deliverable 12.6, we summarize the social-economic evaluation of the FutureID project. We evaluate each of the requirements that were established in WP22 on three tiers of artifacts: Reference Architecture, Implementation, and Pilots. We elaborate on how each requirement was applied in the evaluation and what the results are. The results of this evaluation are very promising regarding all tiers of artifacts.

Document name:	SP1 /WP12	Page:	2 of 52				
Reference:	D12.6	Dissemination:	PU	Version:	1.01	Status:	Final

2. Document Information

2.1 Contributors

Name	Partner
Rachelle Sellung	FHG
Heiko Roßnagel	FHG
Michael Kubach	USTUTT

2.2 History

Version	Date	Author	Changes
0.1	05.08.2015	Rachelle Sellung	First outline and draft of content
0.4	17.08.2015	Rachelle Sellung	Additional Content added from the Wiki to the document regarding Reference Architecture
0.5	21.08.2015	Michael Kubach	Additional Content added to the tables in the Implementation
0.6	02.09.2015	Heiko Roßnagel	Critiqued and Suggested changes to document
0.7	07.09.2015	Rachelle Sellung	Made Minor and Technical Changes
0.8	24.09.2015	Heiko Roßnagel	Added Pilot Evaluation of SER and further minor changes
0.9	08.10.2015	Michael Kubach	Suggested Minor Changes to Document
1.0	22.10.2015	Rachelle Sellung	Final changes to Document
1.01	30.10.2015	Rachelle Sellung, Michael Kubach	Minor changes due to reviewers' feedback

Document name:	SP1 /WP12	Page:	3 of 52
Reference:	D12.6	Dissemination:	PU
Version:	1.01	Status:	Final

3. Table of Contents

1. Abstract	2
2. Document Information	3
2.1 Contributors	3
2.2 History	3
3. Table of Contents	4
4. Table of Figures	5
5. Glossary of Terms	6
6. Acronyms	11
7. Project Description	12
8. Overall Evaluation Approach	13
9. Evaluation	14
9.1 Reference Architecture	15
9.2 Implementation	29
9.3 Pilot(s)	43
10. Conclusion	58

Document name:	SP1 /WP12	Page:	4 of 52				
Reference:	D12.6	Dissemination:	PU	Version:	1.01	Status:	Final

4. Table of Figures

Figure 1 Distribution and Classification of Socio-Economic Requirements	14
Figure 2 Reference Architecture Evaluation Results	29
Figure 3 Implementation Evaluation Results	43
Figure 4 Pilots Evaluation Results	57

Document name:	SP1 /WP12				Page:	5 of 52	
Reference:	D12.6	Dissemination:	PU	Version:	1.01	Status:	Final

5. Glossary of Terms

Based on FutureID Terminology wiki of Wed Nov 12 15:19:32 2014.

address

An address is the identifier for a specific termination point and is used for routing to this termination point.

application (A)

An application is a software component run by a service provider that implements an actual service offering. Applications are typically accessible via HTTP through a web server. A service provider can run one to several applications; they typically run in some application server, container, or framework, as for examples servlets in a J2EE servlet container.

application integration service (AIS)

The Application Integration Service (AIS) is the interface of the service provider to connect to the FutureID infrastructure. It provides authentication to the application and can interface to existing authorization components. A legacy AIS is an off-the-shelf relying party implementation of a given federation dialect (SAML, WS-*, OAuth, OpenID). The FutureID AIS is a custom implementation that provides more functionality and better privacy. An AIS consists of one access filter (AF) and one to several simple credential transformers (SCTs).

attribute

An attribute is a physical or abstract named property belonging to an entity. An attribute has a key and a value.

authentication

Authentication is the process of corroborating a claimed set of attributes or facts with a specified, or understood, level of confidence.

availability

Availability can be described as the property of being accessible and useable upon demand by an authorized entity.

In the context of service level agreements, availability generally refers to the degree to which a system may suffer degradation or interruption in its service to the customer as a consequence of failures of one or more of its parts.

broker

A broker is an organization that acts as intermediate in the authentication process and typically runs multiple FutureID software components, most prominently a broker service. In some

Document name:	SP1 /WP12	Page:	6 of 52				
Reference:	D12.6	Dissemination:	PU	Version:	1.01	Status:	Final

contexts, it can also refer to the set of components operated by the organization. The overall infrastructure typically incorporates a large number of brokers and both, users and service providers, have at least a broker with whom they have a trust and possibly commercial relationship. Service providers can also act as brokers, running broker components themselves; in the most privacy-friendly setting, also users run broker components on their platform.

claim

A statement made by one entity about itself or another entity that a relying party considers to be in doubt until it passes Claims Approval.

consent

The general permission granted by an individual to a requesting entity to use the individual's personal information in some agreed manner. Consent can be expressed, implied, or provided through an authorized representative.

credential

A credential is a verifiable set of attributes that describe an entity. The major properties of a credential are issuer and format (such as X.509 token or SAML bearer assertion). User credentials are credentials that are typically long-lived and controlled by the user; Session credentials are typically short-lived and are created and consumed as part of the overall authentication process.

electronic identity

An electronic identity is a collection of identity attributes in an electronic form (eq. digital identity)

federated identity

A federated identity is a partial identity which is the result of federation, and which usually implies that the entity to which this identity corresponds is recognized by several service providers or applications that are part of the federation.

See also federation. federation; circle of trust.

federation service (FS)

Federation Services (FS) interface the FutureID infrastructure to legacy service provider that operate only existing relying party implementations for a given federation dialect (e.g., SAML, OpenID, WS-Trust, OAuth). It receives a legacy authentication request and issues a FutureID authentication request. A FutureID broker typically runs several Federation Services in order to cater to different types of Service Providers. Technically, an FS receives an authentication request from the Application Integration Service. I.e., for authentication requests, the FS behaves like an Identity Provider towards the SP.

FutureID client (FC)

Document name:	SP1 /WP12	Page:	7 of 52				
Reference:	D12.6	Dissemination:	PU	Version:	1.01	Status:	Final

The FutureID Client (FC) is a software component installed on the user platform that is a rich client supporting user-centric authentication. While users without FC can participate in the FutureID infrastructure, only the use of a FC achieves full functionality and privacy. The FC can take full control of the authentication flow, provides the user interface for user decisions on disclosure, trust and policy, supports digital signature, and interfaces to various tokens (such as smart cards).

hardware token

A hardware token is a physical token that contains credentials, i.e. information attesting to the integrity of identity attributes. Proving physical possession of the token may involve one of several techniques, including the supply of a PIN or biometric.

identification

- i. Identification in terms of registration: identification as the process of using claimed, observed or assigned attributes of an entity to establish a partial identity of that entity.
- ii. Identification as entity authentication: identification as the verification of the link between an entity and the asserted (partial) identity.
- iii. Identification in terms of identifiability: identification as the process of "individualizing" a particular entity within a set of subjects.

identity

The identity of an entity is the dynamic collection of all of the entity's attributes.

An entity has only one identity. As such, the identity of an entity this is more a fluid and evolving ("philosophical") concept, rather than a practical one.

An entity has only one identity, but it is neither possible nor desirable for an information system to gather all the attributes of a specific entity. Information systems focus on a specific subset of relevant attributes, commonly referred to as 'partial identities'.

identity management (IdM)

The definition, designation and administration of identity attributes and the management of access to and the usage of applications, services and resources.

identity provider (IdP)

An identity provider is a service provider that creates, maintains, and manages identity information for principals and who may provide entity authentication services to other service providers within an identity management architecture (e.g. within a federation).

interoperability

Document name:	SP1 /WP12	Page:	8 of 52				
Reference:	D12.6	Dissemination:	PU	Version:	1.01	Status:	Final

The ability of independent systems to exchange meaningful information and initiate actions from each other, in order to operate together to mutual benefit. In particular, it envisages the ability for loosely-coupled independent systems to be able to collaborate and communicate; the possibility of use in services outside the direct control of the issuing assigner.

name

A name is the identifier of an entity (e.g., subscriber, network element) that may be resolved/translated into an address.

permission

A permission describes a set of defined actions, which correspond to a subset or the entirety of all possible uses of the controlled or protected resources, which an entity is entitled to perform (typically 'read', 'modify', 'create' and/or 'delete' resources).

personal data

Any information relating to an identified or identifiable natural person (the data subject).

resource

The term resource is a generic term which is generally used to refer to entities with some value, systems and services.

Computing systems and services are for example disk space on a file server, electronic mailboxes, the system software, applications, services, data repositories, data objects,

Non-computing systems and services may be anything from natural persons (e.g., employees) to physical assets (e.g., desk, telephone, mobile phone, laptop).

security policy

A security policy is a set of rules and practices that specify (or determine) how a system or organization should protect (or protects) data exchange, data storage, sensitive and/or critical system resources, and the use and provision of security services and facilities.

service

A digital entity comprising software, hardware and / or communications channels that interacts with subjects.

service provider (SP)

Entity that provides services to other entities.

token

Document name:	SP1 /WP12	Page:	9 of 52				
Reference:	D12.6	Dissemination:	PU	Version:	1.01	Status:	Final

A token is any hardware or software component that contains credentials related to attributes. They may take any form, ranging from a digital data set to smart cards or mobile phones. They can be used for both data/entity authentication and authorization purposes.

transparency

The data protection goal Transparency ensures that all privacy-relevant data processing including the legal, technical and organizational setting can be understood by all involved parties including the Users.

trust

A measure of reliance on the character, ability, strength, or truth of someone or something.

trust infrastructure

The technical infrastructure used by system entities in order to trust each other. Trust infrastructures may be built on Public Key Infrastructure, Kerberos, etc.

trust service (TS)

A FutureID Trust Service manages trust related knowledge in the FutureID infrastructure. In particular, it manages which issuers of user credentials (e.g. X.509 certificates) and session credentials (e.g. SAML Assertions, or WS-* claims) are trusted and at which trust level.

trusted third party (TTP)

A trusted third party is a third party trusted by other entities to perform one or more specific actions within a specific context or sector.

verification

The process or an instance of establishing the truth or validity of something.

Document name:	SP1 /WP12	Page:	10 of 52				
Reference:	D12.6	Dissemination:	PU	Version:	1.01	Status:	Final

6. Acronyms

A

application

TTP

trusted third party

FC

FutureID client

SP

service provider

TS

trust service

IdP

identity provider

IdM

identity management

AIS

application integration service

FS

federation service

Document name:	SP1 /WP12	Page:	11 of 52				
Reference:	D12.6	Dissemination:	PU	Version:	1.01	Status:	Final

7. Project Description

The FutureID project builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe, which integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims.

The FutureID infrastructure will provide great benefits to all stakeholders involved in the eID value chain. Users will benefit from the availability of a ubiquitously usable open source eID client that is capable of running on arbitrary desktop PCs, tablets and modern smart phones. FutureID will allow application and service providers to easily integrate their existing services with the FutureID infrastructure, providing them with the benefits from the strong security offered by eIDs without requiring them to make substantial investments.

This will enable service providers to offer this technology to users as an alternative to username/password based systems, providing them with a choice for a more trustworthy, usable and innovative technology. For existing and emerging trust service providers and card issuers FutureID will provide an integrative framework, which eases using their authentication and signature related products across Europe and beyond.

To demonstrate the applicability of the developed technologies and the feasibility of the overall approach FutureID will develop two pilot applications and is open for additional application services who want to use the innovative FutureID technology

Future ID is a three-year duration project funded by the European Commission Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318424

Document name:	SP1 /WP12	Page:	12 of 52				
Reference:	D12.6	Dissemination:	PU	Version:	1.01	Status:	Final

8. Overall Evaluation Approach

The FutureID Evaluation approach uses a *Design Science Methodology framework* to organize and harmonize the multi-disciplinary evaluation approaches for all three artifacts; Reference Architecture, Implementation, and Pilots.

To provide a closer look, FutureID has simplified its evaluation process into three easy steps. First, we **identify** each of the Artifacts, which in their case are two pilots, a reference architecture, and implementation. Second, we **clarify** how each interdisciplinary team define expectations for each of the artifacts and they develop requirements regarding their disciplines need. FutureID has interdisciplinary teams that cover a wide spectrum of important perspectives regarding; technical merit, security, privacy, usability, socio-economic, and legal. This step is ranked regarding importance and is utilized by using the Evaluation Wiki Tool, which is explained below. Lastly, we **re-evaluate**, which is when each requirement identified will be reevaluated on whether they should be really implemented or initiated in each artifact. Of course, with the complexity of some of the artifacts a conclusive evaluation could not be sufficiently executed with just this process, therefore, FutureID has used extra evaluation steps to properly consider specific needs of some of the artifacts. For example, there are test-beds used to better grasp the outlook of the pilots.

The Evaluation Wiki tool is a quality control mechanism that has been used for the core evaluation of FutureIDs results. The Evaluation Wiki tool has a variety of different beneficial functions that lead to a practical and more optimal evaluation method. On the practical side, it presents an easy to read, adjust and comprehensive solution for documentation of the evaluation requirements needed for each artifact. Each artifact can be sub categorized into viewing each of the importance levels of requirements (must, should, may, all) on the main page of the Evaluation Wiki tool. The Evaluation Wiki tool classifies each requirement, from which interdisciplinary team it's from, comment section, and its rank of importance.

While collaborating with multiple disciplines, harmonizing and consolidating a wide spectrum of requirements proved to have some difficulties and major conflicts. In order to resolve this problem, FutureID included another addition to the Evaluation Wiki tool and to the Evaluation work package. The addition was an added deliverable that clarifies similarities, relations, and conflicts among requirements. This is a necessary task that all large scale interdisciplinary projects should have in harmonizing requirements in evaluations. This task helped provide an insight on how all of the requirements can cooperate and be applied all together.

In addition to these processes, the testbed has proven to be a great technical method in testing the implementation and pilot applications. It is built of three different levels of testing; unit testing, integration testing, and system testing. The implementation artifact is tested using the unit, integration, and system testing. While the pilots are tested on only the system level testing, the form of evaluation methods between different artifacts obviously varies. However, the Design Science Evaluation methods are broad enough to cover a wide range of techniques.

Document name:	SP1 /WP12	Page:	13 of 52				
Reference:	D12.6	Dissemination:	PU	Version:	1.01	Status:	Final

9. Evaluation

The following tables include a comprehensive list of results regarding all of the Socio-Economic requirements for each Artifact. Further, the methodology explained above was applied and utilized in the process of evaluating all of the Socio-Economic Requirements for each of the three artifacts: Reference Architecture, Implementation, and the Pilots. In application to each artifact, each requirement was asked to state the classification of importance, how it was tested, and the final result. The classification of importance has four different options; Must, May, Should, and Not Applicable. Further, each requirement was tested either automatically or manually. Furthermore, after testing the applicable requirements for each artifact, each requirement was given a Passed, Neutral, or Not Passed status for the individual evaluation. In Figure 1 below, it depicts a diagram on the distribution and classification of the Socio-Economic Requirements for each of the artifacts. The original levels depict the requirements in a general state prior to being applied to each individual artifact.

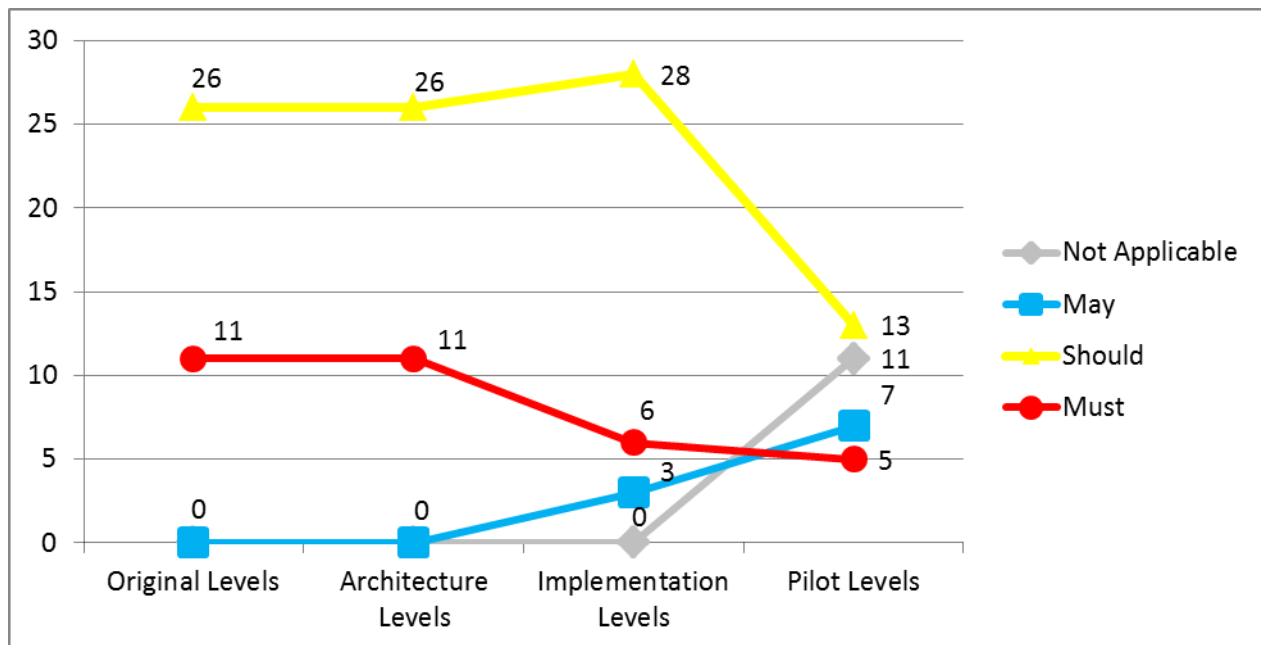


Figure 1 Distribution and Classification of Socio-Economic Requirements

Document name:	SP1 /WP12			Page:	14 of 52
Reference:	D12.6	Dissemination:	PU	Version:	1.01
Status:	Final				

9.1 Reference Architecture

SER-01.1	Support of different business cases
Description	Different stakeholders and different scenarios require different business cases. There is no existing business case that fits all use cases. Therefore FutureID MUST support different use and business cases (Applies to: Broker, AIS, GI).
Classification on Architecture	must
How has it been tested?	Manually
Result	Passed

SER-01.10	Support of anonymous authentication
Description	In some use cases (B2B as well as B2C), users have an interest in protecting their privacy and service providers don't need personal information about the users. Therefore, FutureID MUST support anonymous authentication (Applies to: FC, IdB, US, FS, AIS).
Classification on Architecture	must
How has it been tested?	Manually
Result	Passed

SER-01.11	Support of non-anonymous authentication
Description	In some use cases (B2B as well as B2C), users and service providers have an interest in certifying personal information about the user. Therefore, FutureID MUST support non-anonymous authentication allowing the Service Providers to obtain the personal data necessary for their use case (Applies to: FC, IdB, US, FS, AIS).

Document name:	SP1 /WP12	Page:	15 of 52
Reference:	D12.6	Dissemination:	PU
Version:	1.01	Status:	Final

Classification on Architecture	must
How has it been tested?	Manually.
Result	Passed

SER-01.12	Global applicability
Description	Service providers in the B2B scenario as well as companies in the B2C scenario operate on a global market. As a result of this, they prefer solutions that are deployable on a global scale. Therefore, FutureID infrastructure SHOULD provide global applicability.
Classification on Architecture	should
How has it been tested?	Manually.
Result	Passed

SER-01.2	Provide added value for all stakeholders involved
Description	Stakeholders are relatively satisfied with the solutions they currently use for authentication. This implies that, to implement FutureID, all relevant stakeholders MUST be provided with some added value, e.g. additional revenue; cost savings, usability, privacy or security benefits.
Classification on Architecture	must
How has it been tested?	Manually.
Result	Passed

Document name:	SP1 /WP12	Page:	16 of 52
Reference:	D12.6	Dissemination:	PU
Version:	1.01	Status:	Final

SER-01.3	Support of different deployment models
Description	Different stakeholders and different scenarios require different models of deployment. There is no deployment mode that fits all use cases. Therefore FutureID MUST support different deployment models (Applies to: IdB, GI).
Classification on Architecture	must
How has it been tested?	Manually.
Result	Passed

SER-01.4	Support of price differentiation
Description	Different users have a varying willingness to pay. To build up a sustainable business case, these users and service providers must get addressed differently to charge them according to their willingness to pay. Therefore Future ID MUST support price differentiation of the users and service providers according to their willingness to pay.
Classification on Architecture	must
How has it been tested?	Manually.
Result	Passed

SER-01.5.1	Support of different forms of revenue generation
Description	The FutureID solution and its elements consume financial resources to operate. Therefore, there SHOULD be a sustainable stream of revenue high enough to cover these financial resources. However, not all users or stakeholders can be charged. [Therefore FutureID MUST support different forms of revenue generation (Applies to: IdB, AIS, GI).]

Document name:	SP1 /WP12	Page:	17 of 52
Reference:	D12.6	Dissemination:	PU
Version:	1.01	Status:	Final

Classification on Architecture	should
How has it been tested?	Manually.
Result	Passed

SER-01.5.2	Support of different forms of revenue generation
Description	[The FutureID solution and its elements consume financial resources to operate. Therefore, there SHOULD be a sustainable stream of revenue high enough to cover these financial resources. However, not all users or stakeholders can be charged.] Therefore FutureID MUST support different forms of revenue generation (Applies to: IdB, AIS, GI).
Classification on Architecture	must
How has it been tested?	Manually.
Result	Passed

SER-01.6	Support of different forms of revenue distribution
Description	The FutureID solution and its elements consume financial resources to operate. Therefore, there needs to be a sustainable stream of revenue high enough to cover these financial resources required by all actors involved. However, not all users or stakeholders can be charged, according to this, not all organizations that run one of the components of FutureID can directly generate revenue. Therefore FutureID MUST support different forms of revenue distribution between the organizations that run components of FutureID (Applies to: IdB, GI).
Classification on Architecture	must
How has it been tested?	Manually.
Result	Passed

SER-01.7	Interoperability
Description	Different scenarios, uses cases and business cases are characterized by different services and authentication methods. Therefore, a great variety of services and authentication methods MUST be supported (Applies to: FC, IdB, US, FS, and AIS).
Classification on Architecture	must
How has it been tested?	Manually.
Result	Passed

SER-01.8	Mobile support
Description	The use of mobile devices is increasing in importance for both, consumer as well as professional services. However, authentication for access through mobile devices remains a challenge in many use cases. Therefore, FutureID SHOULD support authentication through mobile devices (Applies to: FC).
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-01.9	Platform independence
Description	In consumer as well as in business environments a huge variety of platforms is used. To maximize the potential user base, which is in the interest of IdBs and Service Providers, FutureID SHOULD be designed so that it can be used without regard to the platform that the end-user is running. (Applies to: FC).
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-02.1	Support existing company tokens
Description	A huge variety of tokens is currently in used in companies. The roll-out of a new special token is expensive. The solution therefore SHOULD support already rolled out company tokens. (Applies to: FC, IdB, US).
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-02.10	Anonymous credentials
Description	Companies sometimes want to disguise the detailed identity of a particular employee to a partner company in a project. However, it must be assured that the respective employee is authorized for access. Therefore FutureID SHOULD support anonymous credentials to anonymously verify attributes not directly linked to an identity such as “works on project X” (Applies to: IdB).
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-02.2	Easy implementation of new company tokens
Description	New partners (customers, suppliers) or changes in the security policies may require new tokens. The solution SHOULD therefore support the easy implementation of new tokens (Applies to: FC, IdB, US).
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-02.3	Support of a client-less mode
Description	The client MUST provide the functionality to perform authentication to the FutureID backend, to a service provider, to a hardware token and to an external identity provider.
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-02.4	Fully organization-internal deployment
Description	Due to security policies or for other reasons, companies may require running the FutureID solution completely inside one organization or company. Large companies might not be willing to trust other organizations in critical areas such as the protection of intellectual capital. Moreover, they can afford (market power, financial resources, and expertise) not to do so. Therefore the solution SHOULD support fully organization-internal deployment without the need to integrate other organizations to run parts of the solution (Applies to: IdB).
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-02.5	The organization must be able to keep direct control over the permissions
Description	The assignment of permissions, e.g. for accessing documents that contain important intellectual capital, is a very sensitive issue. Companies are not willing to give up control over this issue. Therefore, assignment of permissions SHOULD remain inside the respective organization.
Classification on Architecture	should

How has it been tested?	Manually.
Result	passed

SER-02.6	Provision by a trusted third party
Description	Precompetitive cooperation, supported by trusted third parties that perform various functions that require high trust, such as network provision, is an important element in industries with high market pressure and high pressure to cooperate at the same time. To enable this, FutureID SHOULD enable that trust-critical elements, such as the IdB, are operated by trusted third parties (Applies to: IdB).
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-02.7.1	Transparency for error diagnostics
Description	Down times are extremely expensive and have to be avoided. In the unfortunate event of a downtime, the service MUST be transparent enough to identify the reason for the downtime as quickly as possible. [Therefore, the responsibility for the functioning of each element MUST be transparent. This is of particular importance when different organizations provide different parts of the solution.]
Classification on Architecture	must
How has it been tested?	Manually.
Result	passed

SER-02.7.2	Transparency for error diagnostics
Description	[Down times are extremely expensive and have to be avoided. In the unfortunate event of a downtime, the service MUST be transparent enough to identify the reason for the downtime as quickly as possible.] Therefore, the responsibility for the functioning of each element MUST be transparent. This is of particular importance when different organizations provide different parts of the solution.
Classification on Architecture	must
How has it been tested?	Manually.
Result	passed

SER-02.8	Competition between different IdBs
Description	Competition between providers that run the IdBs may stimulate service quality and security as well as lower costs. Therefore it SHOULD be made possible, that there can be several competing organizations at the same time that operate IdBs (Applies to: IdB, FS).
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-02.9	Cost savings
Description	The companies are quite satisfied with the security and usability of their current solutions. Cost savings are the main drivers they mention that could bring them to implement the FutureID solution. Therefore FutureID SHOULD provide cost savings for the companies.

Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-03.1	Easy and cheap implementation for service providers
Description	Service providers are often very small firms with no specialized IT-knowledge and limited financial resources. This means to optimize the usability and implementation costs for the service providers it SHOULD be provided at an economical cost.
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-03.10	One Client for all credentials
Description	Given that End-Users may process numerous credentials it SHOULD be possible to provide a single client to organize all credentials. This will allow to utilize a higher amount of interactions among each of the contributors in the infrastructure. Applies to: (FC).
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-03.11	High Usability
Description	The usability and understanding of the services and applications SHOULD be a main benefit to the End-Users. Given that End-Users may have a wide range of competence with this technology it is important to make it as simple and usable as possible. Applies to: (FC)
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-03.12	Support of a Variety of Credentials
Description	Given that there are a wide range of different eID credentials provided to End-Users that have various attributes included. The support of credentials SHOULD contain a wide range with various attributes included. Applies to: (FC, US, IdB). If necessary “unknown” attributes MAY be possible to be processed as attribute-value-pair.
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-03.13	Classification of Security Levels for Credentials
Description	It's known that there are a wide range of credentials that have different standards and criteria for security. A system SHOULD be created that establishes criteria for different levels of security for various types of credentials. Applies to: (FC, IdB, TS)
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-03.2	Little to no costs for End-Users
Description	According to empirical research[71], results showed that there is a very low or non-existent willingness of end-users to pay for federated identity management systems. Therefore, having a little to no cost could create an advantage for the End-Users. Thus, there SHOULD be little to no costs for End-Users.
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-03.3	The solution should support anonymous authentication
Description	Use cases found in various industries, need only certain credible information such as age verification. Acceptance of the technology could be raised, if the users could select to authenticate anonymously. Thus, anonymous authentication SHOULD be supported.
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-03.4	The solution should support the certification of various credentials
Description	For some use cases (e.g. shipping), the certification user addresses is seen as beneficial by the stakeholders. Therefore, the FutureID solution SHOULD offer a service or support to be able to certify attributes based on different credentials of a User.
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-03.5	Support of authentication with username and password
Description	The majority of service providers are satisfied with the traditional method of authentication with username and password. In this perspective, the FutureID solution SHOULD support this form of authentication, in addition to more secure methods of authentication.
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-03.6	Use of existing validated credentials
Description	Having End-Users who have numerous validated credentials it is important to make the most use of existing credentials. FutureID SHOULD support the use of existing credentials. In turn, this will aid the adaptation process of End-Users. Applies to: (FC, US, IdB)
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-03.7	Options and Assistance to Users with Disabilities
Description	While End-Users come with a wide range of abilities the FutureID solution SHOULD provide options and opportunities to users who are faced with disabilities. Applies to: (FC)
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-03.8	Supports multiple accounts of users
Description	Given that most users possess more than one account, FutureID SHOULD support numerous accounts of users to be able to provide convenience and usability to the user. Applies to: (FC, IdB)
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

SER-03.9	Personalization should be possible
Description	As an advantage and benefit to the End-User it SHOULD be possible to give the End-Users the control to decide which credentials to use for which services and applications. Applies to: (FC, IdB)
Classification on Architecture	should
How has it been tested?	Manually.
Result	passed

In Figure 2, it shows very positive results regarding the Reference Architecture evaluation results, where all requirements that were applicable for this artifact were passed in all importance levels.

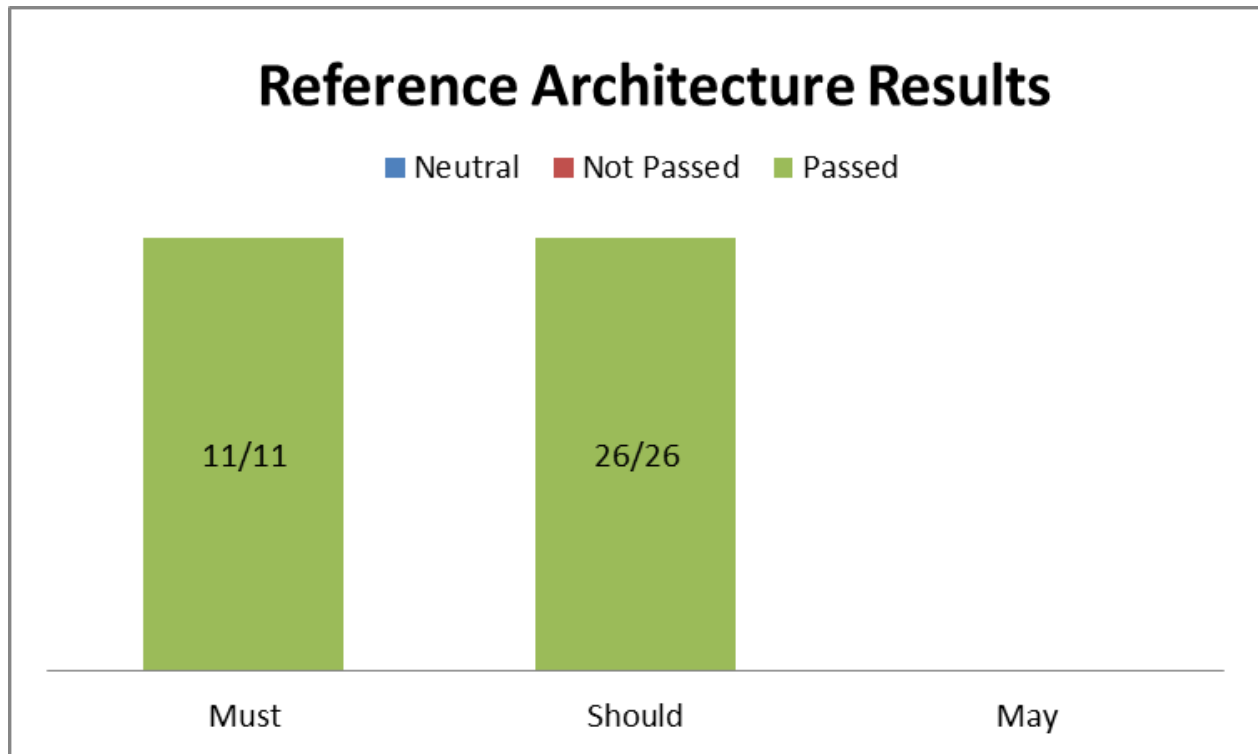


Figure 2 Reference Architecture Evaluation Results

9.2 Implementation

Note: Requirements on Implementation and Pilot level are evaluated as “Neutral” if in principle the implementation is possible, but in the concrete roll-out is dependent on the specific configuration.

SER-01.1	Support of different business cases
Description	Different stakeholders and different scenarios require different business cases. There is no existing business case that fits all use cases. Therefore FutureID MUST support different use and business cases (Applies to: Broker, AIS, GI).
Classification on Implementation	should
How has it been tested?	Manually
Result	Passed

Document name:	SP1 /WP12	Page:	29 of 52
Reference:	D12.6	Dissemination:	PU
Version:	1.01	Status:	Final

SER-01.10	Support of anonymous authentication
Description	In some use cases (B2B as well as B2C), users have an interest in protecting their privacy and service providers don't need personal information about the users. Therefore, FutureID MUST support anonymous authentication (Applies to: FC, IdB, US, FS, AIS).
Classification on Implementation	should
How has it been tested?	Manually
Result	Passed

SER-01.11	Support of non-anonymous authentication
Description	In some use cases (B2B as well as B2C), users and service providers have an interest in certifying personal information about the user. Therefore, FutureID MUST support non-anonymous authentication allowing the Service Providers to obtain the personal data necessary for their use case (Applies to: FC, IdB, US, FS, AIS).
Classification on Implementation	should
How has it been tested?	Manually
Result	Passed

SER-01.12	Global applicability
Description	Service providers in the B2B scenario as well as companies in the B2C scenario operate on a global market. As a result of this, they prefer solutions that are deployable on a global scale. Therefore, FutureID infrastructure SHOULD provide global applicability.
Classification on Implementation	should

Document name:	SP1 /WP12	Page:	30 of 52
Reference:	D12.6	Dissemination:	PU
Version:	1.01	Status:	Final

How has it been tested?	Manually.
Result	Passed

SER-01.2	Provide added value for all stakeholders involved
Description	Stakeholders are relatively satisfied with the solutions they currently use for authentication. This implies that, to implement FutureID, all relevant stakeholders MUST be provided with some added value, e.g. additional revenue; cost savings, usability, privacy or security benefits.
Classification on Implementation	should
How has it been tested?	Manually
Result	Passed

SER-01.3	Support of different deployment models
Description	Different stakeholders and different scenarios require different models of deployment. There is no deployment mode that fits all use cases. Therefore FutureID MUST support different deployment models (Applies to: IdB, GI).
Classification on Implementation	should
How has it been tested?	Manually
Result	Passed

SER-01.4	Support of price differentiation
Description	Different users have a varying willingness to pay. To build up a sustainable business case, these users and service providers must get addressed differently to charge them according to their willingness to pay. Therefore Future ID MUST support price differentiation of the users and service providers according to their willingness to pay.
Classification on Implementation	must
How has it been tested?	Manually.
Result	Passed

SER-01.5.1	Support of different forms of revenue generation
Description	The FutureID solution and its elements consume financial resources to operate. Therefore, there SHOULD be a sustainable stream of revenue high enough to cover these financial resources. However, not all users or stakeholders can be charged. [Therefore FutureID MUST support different forms of revenue generation (Applies to: IdB, AIS, GI).]
Classification on Implementation	should
How has it been tested?	Manually.
Result	Passed

SER-01.5.2	Support of different forms of revenue generation
Description	[The FutureID solution and its elements consume financial resources to operate. Therefore, there SHOULD be a sustainable stream of revenue high enough to cover these financial resources. However, not all users or stakeholders can be charged.] Therefore FutureID MUST support different forms of revenue generation (Applies to: IdB, AIS, GI).
Classification on Implementation	must
How has it been tested?	Manually.
Result	Passed

Document name:	SP1 /WP12	Page:	32 of 52
Reference:	D12.6	Dissemination:	PU
Version:	1.01	Status:	Final

SER-01.6	Support of different forms of revenue distribution
Description	The FutureID solution and its elements consume financial resources to operate. Therefore, there needs to be a sustainable stream of revenue high enough to cover these financial resources required by all actors involved. However, not all users or stakeholders can be charged, according to this, not all organizations that run one of the components of FutureID can directly generate revenue. Therefore FutureID MUST support different forms of revenue distribution between the organizations that run components of FutureID (Applies to: IdB, GI).
Classification on Implementation	must
How has it been tested?	Manually.
Result	Passed

SER-01.7	Interoperability
Description	Different scenarios, uses cases and business cases are characterized by different services and authentication methods. Therefore, a great variety of services and authentication methods MUST be supported (Applies to: FC, IdB, US, FS, and AIS).
Classification on Implementation	must
How has it been tested?	Manually.
Result	Passed

SER-01.8	Mobile support
Description	The use of mobile devices is increasing in importance for both, consumer as well as professional services. However, authentication for access through mobile devices remains a challenge in many use cases. Therefore, FutureID SHOULD support authentication through mobile devices (Applies to: FC).
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-01.9	Platform independence
Description	In consumer as well as in business environments a huge variety of platforms is used. To maximize the potential user base, which is in the interest of IdBs and Service Providers, FutureID SHOULD be designed so that it can be used without regard to the platform that the end-user is running. (Applies to: FC).
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-02.1	Support existing company tokens
Description	A huge variety of tokens is currently in used in companies. The roll-out of a new special token is expensive. The solution therefore SHOULD support already rolled out company tokens. (Applies to: FC, IdB, US).
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-02.10	Anonymous credentials
Description	Companies sometimes want to disguise the detailed identity of a particular employee to a partner company in a project. However, it must be assured that the respective employee is authorized for access. Therefore FutureID SHOULD support anonymous credentials to anonymously verify attributes not directly linked to an identity such as “works on project X” (Applies to: IdB).
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-02.2	Easy implementation of new company tokens
Description	New partners (customers, suppliers) or changes in the security policies may require new tokens. The solution SHOULD therefore support the easy implementation of new tokens (Applies to: FC, IdB, US).
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-02.3	Support of a client-less mode
Description	The client MUST provide the functionality to perform authentication to the FutureID backend, to a service provider, to a hardware token and to an external identity provider.
Classification on Implementation	may
How has it been tested?	Manually.
Result	passed

SER-02.4	Fully organization-internal deployment
Description	Due to security policies or for other reasons, companies may require running the FutureID solution completely inside one organization or company. Large companies might not be willing to trust other organizations in critical areas such as the protection of intellectual capital. Moreover, they can afford (market power, financial resources, and expertise) not to do so. Therefore the solution SHOULD support fully organization-internal deployment without the need to integrate other organizations to run parts of the solution (Applies to: IdB).
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

Document name:	SP1 /WP12	Page:	35 of 52
Reference:	D12.6	Dissemination:	PU
Version:	1.01	Status:	Final

SER-02.5	The organization must be able to keep direct control over the permissions
Description	The assignment of permissions, e.g. for accessing documents that contain important intellectual capital, is a very sensitive issue. Companies are not willing to give up control over this issue. Therefore, assignment of permissions SHOULD remain inside the respective organization.
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-02.6	Provision by a trusted third party
Description	Precompetitive cooperation, supported by trusted third parties that perform various functions that require high trust, such as network provision, is an important element in industries with high market pressure and high pressure to cooperate at the same time. To enable this, FutureID SHOULD enable that trust-critical elements, such as the IdB, are operated by trusted third parties (Applies to: IdB).
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-02.7.1	Transparency for error diagnostics
Description	Down times are extremely expensive and have to be avoided. In the unfortunate event of a downtime, the service MUST be transparent enough to identify the reason for the downtime as quickly as possible. [Therefore, the responsibility for the functioning of each element MUST be transparent. This is of particular importance when different organizations provide different parts of the solution.]
Classification on Implementation	must

Document name:	SP1 /WP12	Page:	36 of 52
Reference:	D12.6	Dissemination:	PU
Version:	1.01	Status:	Final

How has it been tested?	Manually.
Result	passed

SER-02.7.2	Transparency for error diagnostics
Description	[Down times are extremely expensive and have to be avoided. In the unfortunate event of a downtime, the service MUST be transparent enough to identify the reason for the downtime as quickly as possible.] Therefore, the responsibility for the functioning of each element MUST be transparent. This is of particular importance when different organizations provide different parts of the solution.
Classification on Implementation	must
How has it been tested?	Manually.
Result	passed

SER-02.8	Competition between different IdBs
Description	Competition between providers that run the IdBs may stimulate service quality and security as well as lower costs. Therefore it SHOULD be made possible, that there can be several competing organizations at the same time that operate IdBs (Applies to: IdB, FS).
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-02.9	Cost savings
Description	The companies are quite satisfied with the security and usability of their current solutions. Cost savings are the main drivers they mention that could bring them to implement the FutureID solution. Therefore FutureID SHOULD provide cost savings for the companies.
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-03.1	Easy and cheap implementation for service providers
Description	Service providers are often very small firms with no specialized IT-knowledge and limited financial resources. This means to optimize the usability and implementation costs for the service providers it SHOULD be provided at an economical cost.
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-03.10	One Client for all credentials
Description	Given that End-Users may process numerous credentials it SHOULD be possible to provide a single client to organize all credentials. This will allow to utilize a higher amount of interactions among each of the contributors in the infrastructure. Applies to: (FC).
Classification on Implementation	should

How has it been tested?	Manually.
Result	passed

SER-03.11	High Usability
Description	The usability and understanding of the services and applications SHOULD be a main benefit to the End-Users. Given that End-Users may have a wide range of competence with this technology it is important to make it as simple and usable as possible. Applies to: (FC)
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-03.12	Support of a Variety of Credentials
Description	Given that there are a wide range of different eID credentials provided to End-Users that have various attributes included. The support of credentials SHOULD contain a wide range with various attributes included. Applies to: (FC, US, IdB). If necessary “unknown” attributes MAY be possible to be processed as attribute-value-pair.
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-03.13	Classification of Security Levels for Credentials
Description	It's known that there are a wide range of credentials that have different standards and criteria for security. A system SHOULD be created that establishes criteria for different levels of security for various types of credentials. Applies to: (FC, IdB, TS)
Classification on Implementation	should

How has it been tested?	Manually.
Result	passed

SER-03.2	Little to no costs for End-Users
Description	According to empirical research[71], results showed that there is a very low or non-existent willingness of end-users to pay for federated identity management systems. Therefore, having a little to no cost could create an advantage for the End-Users. Thus, there SHOULD be little to no costs for End-Users.
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-03.3	The solution should support anonymous authentication
Description	Use cases found in various industries, need only certain credible information such as age verification. Acceptance of the technology could be raised, if the users could select to authenticate anonymously. Thus, anonymous authentication SHOULD be supported.
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-03.4	The solution should support the certification of various credentials
Description	For some use cases (e.g. shipping), the certification user addresses is seen as beneficial by the stakeholders. Therefore, the FutureID solution SHOULD offer a service or support to be able to certify attributes based on different credentials of a User.
Classification on Implementation	should

How has it been tested?	Manually.
Result	passed

SER-03.5	Support of authentication with username and password
Description	The majority of service providers are satisfied with the traditional method of authentication with username and password. In this perspective, the FutureID solution SHOULD support this form of authentication, in addition to more secure methods of authentication.
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-03.6	Use of existing validated credentials
Description	Having End-Users who have numerous validated credentials it is important to make the most use of existing credentials. FutureID SHOULD support the use of existing credentials. In turn, this will aid the adaptation process of End-Users. Applies to: (FC, US, IdB)
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-03.7	Options and Assistance to Users with Disabilities
Description	While End-Users come with a wide range of abilities the FutureID solution SHOULD provide options and opportunities to users who are faced with disabilities. Applies to: (FC)
Classification on Implementation	should

How has it been tested?	Automated
Result	Passed

SER-03.8	Supports multiple accounts of users
Description	Given that most users possess more than one account, FutureID SHOULD support numerous accounts of users to be able to provide convenience and usability to the user. Applies to: (FC, IdB)
Classification on Implementation	Not applicable
How has it been tested?	
Result	

SER-03.9	Personalization should be possible
Description	As an advantage and benefit to the End-User it SHOULD be possible to give the End-Users the control to decide which credentials to use for which services and applications. Applies to: (FC, IdB)
Classification on Implementation	may
How has it been tested?	Manually.
Result	Neutral

In Figure 3, the applicable requirements evaluated depict a positive outlook. All requirements were either decided Passed or Neutral for the Implementation artifact.

Document name:	SP1 /WP12	Page:	42 of 52
Reference:	D12.6	Dissemination:	PU
Version:	1.01	Status:	Final

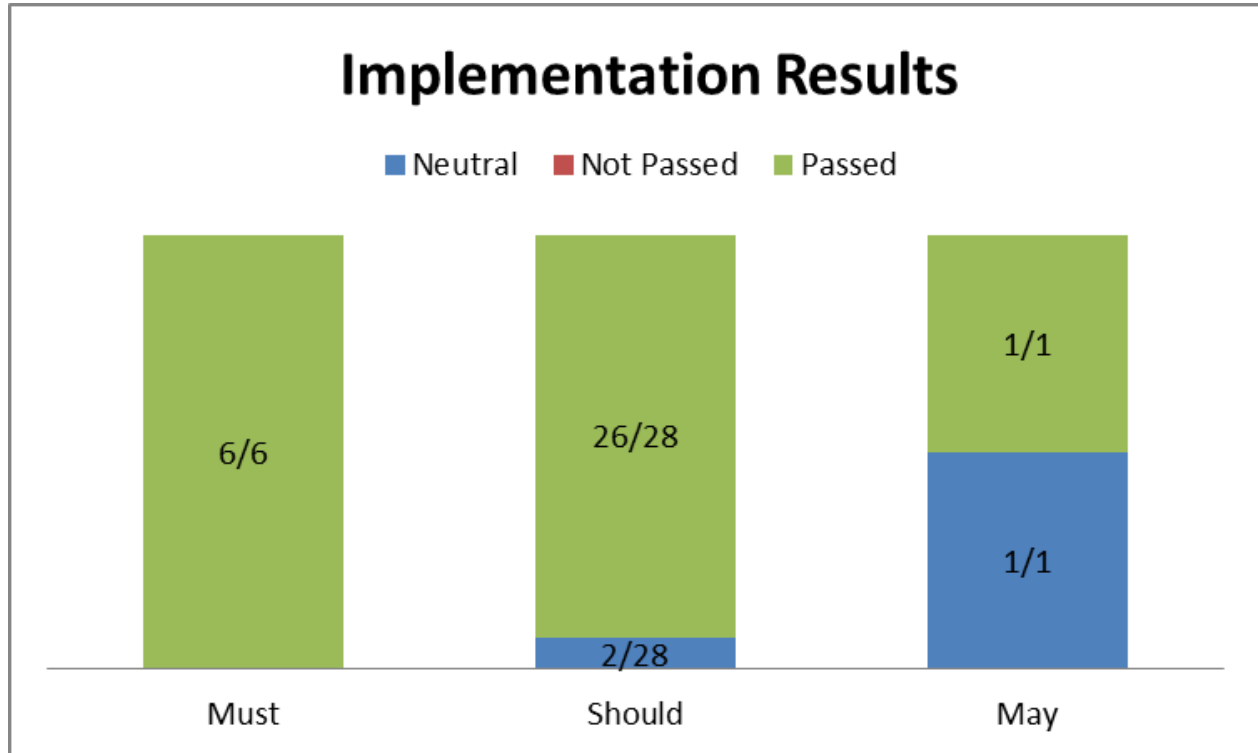


Figure 3 Implementation Evaluation Results

9.3 Pilot(s)

This section provides the results regarding the Socio-Economic Evaluation for the Pilots. The results section should be assumed to reflect the results for both pilots; citizen services and e-learning services for enterprises. If there is a difference within the results, it will be specified.

SER-01.1	Support of different business cases
Description	Different stakeholders and different scenarios require different business cases. There is no existing business case that fits all use cases. Therefore FutureID MUST support different use and business cases (Applies to: Broker, AIS, GI).
Classification on Implementation	not applicable
How has it been tested?	
Result	

SER-01.10	Support of anonymous authentication
Description	In some use cases (B2B as well as B2C), users have an interest in protecting their privacy and service providers don't need personal information about the users. Therefore, FutureID MUST support anonymous authentication (Applies to: FC, IdB, US, FS, AIS).
Classification on Implementation	not applicable
How has it been tested?	
Result	

SER-01.11	Support of non-anonymous authentication
Description	In some use cases (B2B as well as B2C), users and service providers have an interest in certifying personal information about the user. Therefore, FutureID MUST support non-anonymous authentication allowing the Service Providers to obtain the personal data necessary for their use case (Applies to: FC, IdB, US, FS, AIS).
Classification on Implementation	should
How has it been tested?	Manuel
Result	Passed

SER-01.12	Global applicability
Description	Service providers in the B2B scenario as well as companies in the B2C scenario operate on a global market. As a result of this, they prefer solutions that are deployable on a global scale. Therefore, FutureID infrastructure SHOULD provide global applicability.
Classification on Implementation	should

Document name:	SP1 /WP12	Page:	44 of 52
Reference:	D12.6	Dissemination:	PU
Version:	1.01	Status:	Final

How has it been tested?	Manually.
Result	Passed

SER-01.2	Provide added value for all stakeholders involved
Description	Stakeholders are relatively satisfied with the solutions they currently use for authentication. This implies that, to implement FutureID, all relevant stakeholders MUST be provided with some added value, e.g. additional revenue; cost savings, usability, privacy or security benefits.
Classification on Implementation	may
How has it been tested?	Manually.
Result	Passed

SER-01.3	Support of different deployment models
Description	Different stakeholders and different scenarios require different models of deployment. There is no deployment mode that fits all use cases. Therefore FutureID MUST support different deployment models (Applies to: IdB, GI).
Classification on Implementation	not applicable
How has it been tested?	
Result	

SER-01.4	Support of price differentiation
Description	Different users have a varying willingness to pay. To build up a sustainable business case, these users and service providers must get addressed differently to charge them according to their willingness to pay. Therefore Future ID MUST support price differentiation of the users and service providers according to their willingness to pay.
Classification on Implementation	must
How has it been tested?	Manually.
Result	Passed

SER-01.5.1	Support of different forms of revenue generation
Description	The FutureID solution and its elements consume financial resources to operate. Therefore, there SHOULD be a sustainable stream of revenue high enough to cover these financial resources. However, not all users or stakeholders can be charged. [Therefore FutureID MUST support different forms of revenue generation (Applies to: IdB, AIS, GI).]
Classification on Implementation	should
How has it been tested?	Manually.
Result	Passed

SER-01.5.2	Support of different forms of revenue generation
Description	[The FutureID solution and its elements consume financial resources to operate. Therefore, there SHOULD be a sustainable stream of revenue high enough to cover these financial resources. However, not all users or stakeholders can be charged.] Therefore FutureID MUST support different forms of revenue generation (Applies to: IdB, AIS, GI).
Classification on Implementation	must
How has it been tested?	Manually.
Result	Passed

Document name:	SP1 /WP12	Page:	46 of 52
Reference:	D12.6	Dissemination:	PU
Version:	1.01	Status:	Final

SER-01.6	Support of different forms of revenue distribution
Description	The FutureID solution and its elements consume financial resources to operate. Therefore, there needs to be a sustainable stream of revenue high enough to cover these financial resources required by all actors involved. However, not all users or stakeholders can be charged, according to this, not all organizations that run one of the components of FutureID can directly generate revenue. Therefore FutureID MUST support different forms of revenue distribution between the organizations that run components of FutureID (Applies to: IdB, GI).
Classification on Implementation	must
How has it been tested?	Manually.
Result	Passed

SER-01.7	Interoperability
Description	Different scenarios, uses cases and business cases are characterized by different services and authentication methods. Therefore, a great variety of services and authentication methods MUST be supported (Applies to: FC, IdB, US, FS, and AIS).
Classification on Implementation	Should
How has it been tested?	Manually.
Result	Passed

SER-01.8	Mobile support
Description	The use of mobile devices is increasing in importance for both, consumer as well as professional services. However, authentication for access through mobile devices remains a challenge in many use cases. Therefore, FutureID SHOULD support authentication through mobile devices (Applies to: FC).
Classification on Implementation	not applicable
How has it been tested?	
Result	

SER-01.9	Platform independence
Description	In consumer as well as in business environments a huge variety of platforms is used. To maximize the potential user base, which is in the interest of IdBs and Service Providers, FutureID SHOULD be designed so that it can be used without regard to the platform that the end-user is running. (Applies to: FC).
Classification on Implementation	may
How has it been tested?	Manually.
Result	passed

SER-02.1	Support existing company tokens
Description	A huge variety of tokens is currently in used in companies. The roll-out of a new special token is expensive. The solution therefore SHOULD support already rolled out company tokens. (Applies to: FC, IdB, US).
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-02.10	Anonymous credentials
Description	Companies sometimes want to disguise the detailed identity of a particular employee to a partner company in a project. However, it must be assured that the respective employee is authorized for access. Therefore FutureID SHOULD support anonymous credentials to anonymously verify attributes not directly linked to an identity such as “works on project X” (Applies to: IdB).
Classification on Implementation	not applicable
How has it been tested?	
Result	

SER-02.2	Easy implementation of new company tokens
Description	New partners (customers, suppliers) or changes in the security policies may require new tokens. The solution SHOULD therefore support the easy implementation of new tokens (Applies to: FC, IdB, US).
Classification on Implementation	should
How has it been tested?	Manually.
Result	Neutral

SER-02.3	Support of a client-less mode
Description	The client MUST provide the functionality to perform authentication to the FutureID backend, to a service provider, to a hardware token and to an external identity provider.
Classification on Implementation	not applicable
How has it been tested?	
Result	

SER-02.4	Fully organization-internal deployment
Description	Due to security policies or for other reasons, companies may require running the FutureID solution completely inside one organization or company. Large companies might not be willing to trust other organizations in critical areas such as the protection of intellectual capital. Moreover, they can afford (market power, financial resources, and expertise) not to do so. Therefore the solution SHOULD support fully organization-internal deployment without the need to integrate other organizations to run parts of the solution (Applies to: IdB).
Classification on Implementation	not applicable
How has it been tested?	
Result	

SER-02.5	The organization must be able to keep direct control over the permissions
Description	The assignment of permissions, e.g. for accessing documents that contain important intellectual capital, is a very sensitive issue. Companies are not willing to give up control over this issue. Therefore, assignment of permissions SHOULD remain inside the respective organization.
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-02.6	Provision by a trusted third party
Description	Precompetitive cooperation, supported by trusted third parties that perform various functions that require high trust, such as network provision, is an important element in industries with high market pressure and high pressure to cooperate at the same time. To enable this, FutureID SHOULD enable that trust-critical elements, such as the IdB, are operated by trusted third parties (Applies to: IdB).
Classification on Implementation	not applicable
How has it been tested?	
Result	

SER-02.7.1	Transparency for error diagnostics
Description	Down times are extremely expensive and have to be avoided. In the unfortunate event of a downtime, the service MUST be transparent enough to identify the reason for the downtime as quickly as possible. [Therefore, the responsibility for the functioning of each element MUST be transparent. This is of particular importance when different organizations provide different parts of the solution.]
Classification on Implementation	must

How has it been tested?	Manually.
Result	passed

SER-02.7.2	Transparency for error diagnostics
Description	[Down times are extremely expensive and have to be avoided. In the unfortunate event of a downtime, the service MUST be transparent enough to identify the reason for the downtime as quickly as possible.] Therefore, the responsibility for the functioning of each element MUST be transparent. This is of particular importance when different organizations provide different parts of the solution.
Classification on Implementation	must
How has it been tested?	Manually.
Result	passed

SER-02.8	Competition between different IdBs
Description	Competition between providers that run the IdBs may stimulate service quality and security as well as lower costs. Therefore it SHOULD be made possible, that there can be several competing organizations at the same time that operate IdBs (Applies to: IdB, FS).
Classification on Implementation	not applicable
How has it been tested?	
Result	

SER-02.9	Cost savings
Description	The companies are quite satisfied with the security and usability of their current solutions. Cost savings are the main drivers they mention that could bring them to implement the FutureID solution. Therefore FutureID SHOULD provide cost savings for the companies.
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-03.1	Easy and cheap implementation for service providers
Description	Service providers are often very small firms with no specialized IT-knowledge and limited financial resources. This means to optimize the usability and implementation costs for the service providers it SHOULD be provided at an economical cost.
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-03.10	One Client for all credentials
Description	Given that End-Users may process numerous credentials it SHOULD be possible to provide a single client to organize all credentials. This will allow to utilize a higher amount of interactions among each of the contributors in the infrastructure. Applies to: (FC).
Classification on Implementation	should

How has it been tested?	Manually.
Result	passed

SER-03.11	High Usability
Description	The usability and understanding of the services and applications SHOULD be a main benefit to the End-Users. Given that End-Users may have a wide range of competence with this technology it is important to make it as simple and usable as possible. Applies to: (FC)
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-03.12	Support of a Variety of Credentials
Description	Given that there are a wide range of different eID credentials provided to End-Users that have various attributes included. The support of credentials SHOULD contain a wide range with various attributes included. Applies to: (FC, US, IdB). If necessary “unknown” attributes MAY be possible to be processed as attribute-value-pair.
Classification on Implementation	should
How has it been tested?	Automated.
Result	passed

SER-03.13	Classification of Security Levels for Credentials
Description	It's known that there are a wide range of credentials that have different standards and criteria for security. A system SHOULD be created that establishes criteria for different levels of security for various types of credentials. Applies to: (FC, IdB, TS)
Classification on Implementation	not applicable

How has it been tested?	
Result	

SER-03.2	Little to no costs for End-Users
Description	According to empirical research[71], results showed that there is a very low or non-existent willingness of end-users to pay for federated identity management systems. Therefore, having a little to no cost could create an advantage for the End-Users. Thus, there SHOULD be little to no costs for End-Users.
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-03.3	The solution should support anonymous authentication
Description	Use cases found in various industries, need only certain credible information such as age verification. Acceptance of the technology could be raised, if the users could select to authenticate anonymously. Thus, anonymous authentication SHOULD be supported.
Classification on Implementation	not applicable
How has it been tested?	
Result	

SER-03.4	The solution should support the certification of various credentials
Description	For some use cases (e.g. shipping), the certification user addresses is seen as beneficial by the stakeholders. Therefore, the FutureID solution SHOULD offer a service or support to be able to certify attributes based on different credentials of a User.
Classification on Implementation	not applicable

How has it been tested?	
Result	

SER-03.5	Support of authentication with username and password
Description	The majority of service providers are satisfied with the traditional method of authentication with username and password. In this perspective, the FutureID solution SHOULD support this form of authentication, in addition to more secure methods of authentication.
Classification on Implementation	May
How has it been tested?	Manually.
Result	neutral

SER-03.6	Use of existing validated credentials
Description	Having End-Users who have numerous validated credentials it is important to make the most use of existing credentials. FutureID SHOULD support the use of existing credentials. In turn, this will aid the adaptation process of End-Users. Applies to: (FC, US, IdB)
Classification on Implementation	should
How has it been tested?	Manually.
Result	passed

SER-03.7	Options and Assistance to Users with Disabilities
Description	While End-Users come with a wide range of abilities the FutureID solution SHOULD provide options and opportunities to users who are faced with disabilities. Applies to: (FC)
Classification on Implementation	May
How has it been tested?	Manually.
Result	passed.

SER-03.8	Supports multiple accounts of users
Description	Given that most users possess more than one account, FutureID SHOULD support numerous accounts of users to be able to provide convenience and usability to the user. Applies to: (FC, IdB)
Classification on Implementation	not applicable
How has it been tested?	
Result	

SER-03.9	Personalization should be possible
Description	As an advantage and benefit to the End-User it SHOULD be possible to give the End-Users the control to decide which credentials to use for which services and applications. Applies to: (FC, IdB)
Classification on Implementation	not applicable
How has it been tested?	
Result	

Below in Figure 4, the applicable requirements for the Pilots were evaluated and depict further promising results. The results show that all applicable requirements were rated either Passed or Neutral.

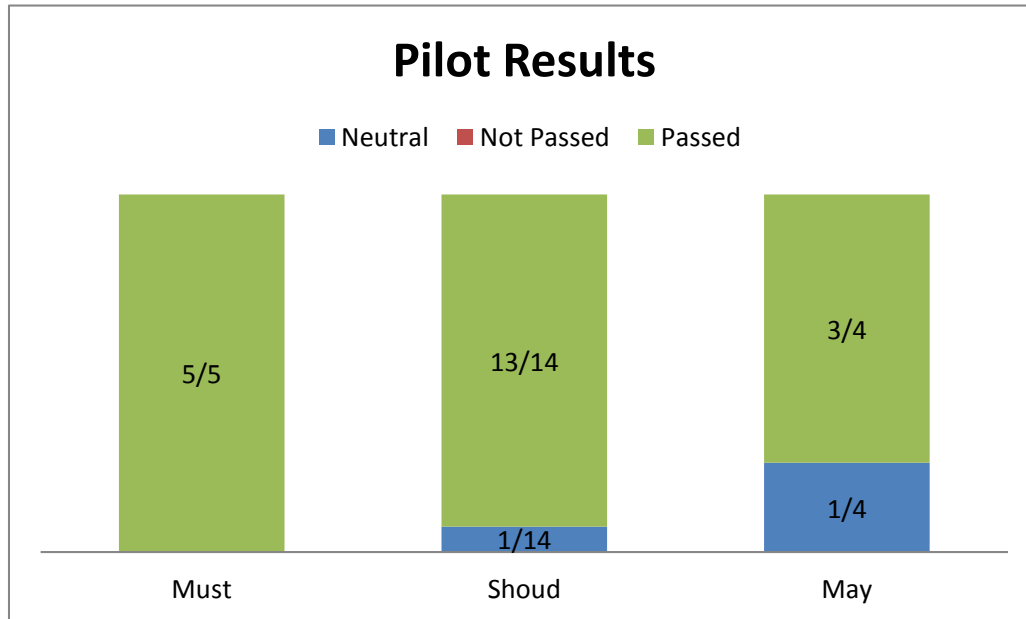


Figure 4 Pilots Evaluation Results

Document name:	SP1 /WP12	Page:	57 of 52
Reference:	D12.6	Dissemination:	PU
Version:	1.01	Status:	Final

10. Conclusion

Overall, the Socio-Economic Requirements evaluation of all three artifacts has led to promising results. For instance, all requirements regarding all artifacts have resulted in either a passed or a neutral status. There were only 4 requirements that received a neutral status; 2 were on a pilot level with the importance of should and may. Further, there were 2 requirements that received a neutral status on the implementation level as well. Regarding application, every requirement was applied to the Reference Architecture artifact. There was one requirement that was not applicable regarding the Implementation artifact and 14 requirements that were not applicable for the Pilots.

Concluding, it can be seen that FutureID's artifacts have shown exceptional results regarding the evaluation of the Socio-Economic requirements that were established and depicted above. This can be interpreted as showing promise in being flexible and attractive for market adaption. While FutureID has made progress in eID technology being tuned to fit some major Socio-Economic requirements, there is still room to improve and to expand on these requirements and expectations.

Document name:	SP1 /WP12				Page:	58 of 52	
Reference:	D12.6	Dissemination:	PU	Version:	1.01	Status:	Final