



Integration of selected applications

Deliverable D44.6

Document Identification	
Date	25/10/2015
Status	Final
Version	1.01

Related SP / WP	WP44.6	Document Reference	D44.6
Related Deliverable(s)	D44.4	Dissemination Level	PU
Lead Participant	EEMA	Lead Author	Jon Shamah
Contributors	Jon Shamah (EEMA); ECS; GD	Reviewers	FHG, USTUTT

This document is issued within the frame and for the purpose of the *FutureID* project. This project has received funding from the 7

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.

Document name:	Integration of Applications				Page:	0 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final



1. Executive Summary

With the increasing use of online services and the mobile internet, banks and international e-commerce owners are more and more pursuing a multi-channel strategy to reach their customers. Beyond the classical bricks and mortar approaches, the online channel has been gaining more attraction in recent years. The use of mobile devices is speeding up this trend even further and reaches from classical online-banking to other bank-related or bank-operated services as well as consumer retail high-street stores.

This deliverable analyses what constitutes an application that would most benefit integration with FutureID and then chooses a small number of real external applications to determine the gaps between FutureID research and real deployments.

The two applications that were chosen and subsequently integrated with FutureID were:

- ECIM Cloud Marketplace for Intelligent Mobility: (<http://www.ecim-cities.eu>)
- Fraunhofer Group Wiki: Wikimedia collaboration environment for entire Fraunhofer Research Group. (<http://www.fraunhofer.de>).

Additionally a laboratory demo of ABC4Trust (<http://abc4trust.eu>) transforming FutureID credentials into ABCs was carried out.

Document name:	WP44.6				Page:	1 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

2. Document Information

2.1 Contributors

Name	Partner
Jon Shamah (JS)	EEMA
Frank-Michael Kamm (FMK)	GD
Max Tuengerthal (MT)	ECSEC

2.2 History

Version	Date	Author	Changes
0.001	25/04/14	JS	Initial
0.002	29/05/14	JS	Criteria Introductions
0.003	06/10/14	JS	Criteria Introductions
0.004	07/10/14	JS	Candidate descriptions
0.005	09/10/14	JS/FMK	Candidate descriptions
0.006	20/05/15	JS	Substantial update
0.007	01/10/15	JS	Reflecting actual integrations
1.00	29/10/15	JS	For review
1.01	29/10/15	JS	Release

Document name:	WP44.6				Page:	2 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

2.3 Table of Tables

Table 1:	Exemplar Attributes	9
Table 2:	Selection Criteria Priorities sorted by Domain	10
Table 3:	Selection Criteria sorted by Priority	11
Table 4:	List of candidates	13
Table 5:	Accepted and rejected candidates	19
Table 6:	Timetable	21

Document name:	WP44.6				Page:	3 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

3. Table of Contents

1.	Executive Summary	1
2.	Document Information	2
2.1	Contributors	2
2.2	History	2
2.3	Table of Tables	3
3.	Table of Contents	4
4.	Project Description	6
5.	Introduction	7
6.	Methodology	8
6.1	Step 1: Collection of Criteria	8
6.2	Step 2: Prioritization of Criteria (by type)	10
6.3	Collection of Submissions	12
7.	Exemplar Selection Results	13
7.1	Candidates Submitted	13
7.2	Descriptions of Candidates	13
7.3	Analysis of Candidate Submissions	18
8.	Exemplar Integration Planning	20
9.	Collection of Socio-Economic Information	22
9.1	ECIM	22
9.2	Fraunhofer Wiki	23
9.3	ABC4Trust	24
10.	The Integration Experience	25
10.1	ECIM	25
10.2	Fraunhofer Wiki	25
10.3	ABC4Trust	26
11.	Sustainability	27
11.1	Sustainability of the FutureID architecture	27
12.	Conclusions	28
13.	Appendix 1 Service Provider Prioritisation Tool	29
14.	Appendix 2: Introductory Letter to Exemplars	30

Document name:	WP44.6				Page:	4 of 34
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status: Final

15.	Appendix 3: Socio-Economic Questionnaire	33
15.1	General background questions	33
15.2	Identity Management	33
15.3	Integration and Added Value of FutureID	33
15.4	Additional questions.....	34

Document name:	WP44.6				Page:	5 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

4. 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:	WP44.6				Page:	6 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

5. Introduction

This task will integrate exemplary applications into the FutureID Infrastructure using the Application Integration Service implemented in task 44.3. Selected applications will be integrated in close cooperation with associated partners of the consortium.

The purpose is to extend the demonstration of FutureID from the originally project pilots to real commercial and active services and thus form a sustainable project.

This deliverable consists of five steps:

1. Collection of criteria
2. Prioritization of criteria
3. Searching for candidate exemplar services based on compliance against those criteria
4. Gaining approval from at least two of those candidates to integrate FutureID into their services
5. Actual integration of FutureID into those services
6. Possible monitoring of the use of FutureID in those services by other programs within Horizon2020¹ or CEF².

This deliverable will link into deliverable **D13.8 “Exploitation Planning and Reporting”** and **WP12 Consolidation and Evaluation**.

¹ Horizon2020: <http://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020>

² Connecting Europe Facility: <http://ec.europa.eu/digital-agenda/en/connecting-europe-facility>

Document name:	WP44.6				Page:	7 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

6. Methodology

The selection criteria for the best exemplar applications determine which Application Service Providers will be asked to integrate FutureID.

These criteria are chosen through gathering opinions and views from across all the FutureID partners. They are then introduced into a scoring algorithm, and weighted by importance.

The scoring algorithm takes the form:

SCORE
 = [(criteria #1 weight) x (candidate strength in criteria #1)]
 + [(criteria #2 weight) x (candidate strength in criteria #2)]
 + [(criteria #3 weight) x (candidate strength in criteria #3)]
 + [...etc.....]

This methodology ensures an impartial and object ranking of most suitable applications for allocation of effort, and should improve the chances of a successful and useful exemplar.

6.1 Step 1: Collection of Criteria

Each FutureID Partner was asked to list their top 10 attributes that they considered 'important' for a successful FutureID-enabled application service.

The attributes collected are listed in Table 1:

Partner	Description
G-D	Very high security in authentication: two-factor authentication, use of hardware tokens, secure system architecture, high trust in federation result. -> high-value application, high-trust application
G-D	Very high trust in identity: use of official eID tokens, verified attributes -> high-value applications, legally binding applications (e-government or private sector)
G-D	Cross-border interoperability: use of eID tokens in other countries -> cross-border/international applications
G-D	Privacy: no user tracking due to broker, selective disclosure of credentials/attributes -> privacy-sensitive applications
G-D	Cost competition: cheaper to use FutureID than to set up own infrastructure -> cross-border, high-value, high trust applications
G-D	Flexibility/future proof: new ID tokens and protocols can be added without modifications on the service side -> applications with dynamic change of user group (and thus used tokens)

Document name:	WP44.6	Page:	8 of 34
Reference:	D44.6	Dissemination:	PU
Version:	1.01	Status:	Final

G-D	Some top candidates: pan-European student enrolment, voter registration for local government elections (where all EU citizens can vote), web-shop for high-value customized goods.
FHG	Large user base
FHG	Using software that is common (i.e WordPress, Typo3, JBOSS, Apache, Wikimedia, OwnCloud, etc.)
FHG	An AIS implementation exists for this platform (there will be a Java an C++ implementation)
FHG	Strong interest by Service Provider to use stronger authentication than username and password
FHG	Interest to support different tokens
ULD	The application should offer different ways of authentication; among these there should be at least one privacy-preserving authentication solution (e.g. attribute-based credentials).
ULD	The application should support the use case of disclosing a proof over one or more attributes of an eID instead of disclosing the eID attribute as such (e.g. being of age instead of disclosing the exact birthdate).
ULD	The application should provide sufficient transparency on all data processing for all parties involved. Only this will enable meaningful decisions.
ULD	The application should provide ways for all parties involved to intervene if necessary in an easy and convenient manner, e.g. for notifying errors, correcting errors, dealing with requests from users such as exercising their data subject rights etc.
ULD	The application should take into account all legal requirements.
ULD	There must not be obvious infringements to legal requirements in the use cases to demonstrate the FutureID functionalities.
ECS	<i>Make a big impact in the market</i>

Table 1: Exemplar Attributes

Document name:	WP44.6				Page:	9 of 34
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status: Final

6.2 Step 2: Prioritization of Criteria (by type)

Table 2: Selection Criteria Priorities sorted by Domain

Document name:	WP44.6				Page:	10 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final



Domain	Criteria	Priority (High to Low)
Authentication	Secure	9.09
Privacy	No user tracking in broker	9
Domain	Criteria	Priority 1=Low, 10=High
Application Type	Trustworthy	8.5
Application Type	Valuable	6.36
Identity	Trusted	8.72
Identity	Trustworthy	8.90
European Dimension	Impact	8.63
European Dimension	Legal binding transactions	7.09
European Dimension	Interoperability	8.63
European Dimension	FutureID is cheaper than multilateral	6.27
Privacy	Selective disclosure of attributes	6.81
Users	Large User Base	8.36
Authentication	Using different Tokens	7.81
Privacy	Expanding User Base	6.27
Privacy	Appropriate Transparency	8.36
European Dimension	Varied	6.81
European Dimension	Cross-Border	8
Authentication	Churn	3.45
Authentication	Interest to improve strength of authentication	7.9
European Dimension	Impact	8.63
Authentication	Optional privacy preserving login	7.9
Privacy	Cross-Border	8.00
Privacy	Privacy Sensitive	7.9
Privacy	Interoperability	8.63
Authentication	Multi-Factor	7.81
Authentication	Multi-Factor	7.81
Privacy	Optional privacy preserving login	7.36
Application Type	Secure	9.09
Application Type	Legal binding transactions	7.90
Application Type	Interest to improve strength of authentication	9.09
Users	Using different Tokens	8.36
Users	Optional privacy preserving login	7.90
Identity	Trusted	8.72
Identity	Uses Notifiable eIDs	6.81
Users	Trusted Federation Capable	6.27
Users	Large User Base	6.72
Other	Uses Notifiable eIDs	6.81
Other	User-Friendly	6.63
Privacy	Selective disclosure of attributes	8.54
Application Type	Valuable	6.36
Application Type	Privacy Sensitive	7.90
Other	Accessible	6.36
Other	Optional privacy preserving login	7.36
Application Type	FutureID is cheaper than multilateral	6.27
Application Type	No user tracking in broker	9.09
Users	Expanding User Base	8.36
Users	Appropriate Transparency	6.27
Identity	Aggregation of attribute values / proofs on attributes	5.18
Identity	Trusted Federation Capable	6.27
Technology	Existing EIS	5.36
Technology	Existing EIS	6.63
Technology	Varied Protocols	3.54
Technology	Transaction Rollback or error correcting	5.45
Technology	Existing EIS	5.63
Technology	Transaction Rollback or error correcting	5.45
Technology	Varied Protocols	5.54
Technology	Java	5.36
Privacy	Transaction Rollback or error correcting	5.45
Privacy	Aggregation of attribute values / proofs on attributes	5.18
Technology	Technology.PHP	4.81
Other	Green – as in eco-friendly	4.9
Technology	Technology.Ruby	4.63
Other	Technology.PHP	4.81
Other	Technology.DotNet	4.36
Other	Technology.Ruby	6.36
Other	Accessible	6.63
Other	User-Friendly	6.63
Other	Technology.DotNet	4.36
Technology	Eco-Friendly	4.90
Technology	C#	3.54
Users	Churn	3.45

Table 3: Selection Criteria sorted by Priority

Document name:	WP44.6	Page:	11 of 34
Reference:	D44.6	Dissemination:	PU
Version:	1.01	Status:	Final

6.3 Collection of Submissions

After consolidation of the criteria considered as important, FutureID partners were then asked to consider the relative importance of each criterion. This was within a scale of 1 to 10, with a score of 1 denoting “little importance” and a score of 10 denoting “highly important”. The consolidated list with the average score per criteria are shown in Table 2 and Table 3. This algorithm was then distributed to FutureID partners in the form of an automated spreadsheet (See Appendix 1)

Scoring can be up to a maximum of approx **2250**, that being a perfectly suited exemplar application for FutureID.

The period for submission of applications was from M18–M24.

Document name:	WP44.6				Page:	12 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

7. Exemplar Selection Results

7.1 Candidates Submitted

Partner	Candidate Name	Candidate Description	FutureID Score
EEMA	ECIM	EU SmartCity project	2097
IBM	ABC4Trust as a Service	Issuance of ABC in response to a FutureID request using an eID	1896
EEMA	EEMA Website Portal	The member access portal for EEMA resources. For use by members only	1781
EEMA	ISSE Registration	Registration Portal for international events operated by Revolution-events	1766
SK	Digidoc	Estonian Document Portal	1722
FHG	Fraunhofer WikiMedia	The internal WikiMedia service for employees	1706
GD	ELSTER	German Federal Tax Portal. Useable by any EU citizen	1405
GD	Deutschebank Portal	Login portal for online banking. Multi-national banks typically have a separate login for each country, mainly username/password.	1267

Table 4: List of candidates

7.2 Descriptions of Candidates

7.2.1 ECIM

(<http://www.ecim-cities.eu>)

The European Cloud Marketplace for Intelligent Mobility (ECIM) platform concentrates on achieving three goals:

- Allow cities and businesses to easily migrate services to the cloud
- Open cloud-based services to innovators for use as the basis for new services
- Facilitate easy access and cross-border adoption of cloud-based services across Europe

Document name:	WP44.6				Page:	13 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

To achieve these targets, ECIM will upgrade the existing and successful EPIC Project (<http://www.epic-cities.eu>) cloud platform configuration and services to create an open innovation environment, allowing the public sector, SMEs and citizens to collaborate, develop innovative new services that are more user-centric, and easily market them across Europe through a growing network of 'Smart Cities'.

As mobility consistently constitutes a high priority for Cities, Service providers and Citizens, and can easily find practical cross-border applications, the ECIM platform uses mobility and parking as a validation scenario in each pilot site.

Each pilot city (Barcelona, Brussels and Issy-les-Moulineaux) tests the same existing services and a final proof of concept will be tested in wider Birmingham.

ECIM pilots will migrate a range of services to the cloud, using an XML web service exposed through a Restful API.

Private Sector Services:

- BePark Off-Street Parking Services
- Mobile-For On-Street Parking
- PaybyPhone
- CenGROUP (a network of 25 local buses)

Public Sector Services:

- ePayment, to be implemented in Brussels, Issy and Barcelona
- On-Street Parking Locator, to be implemented in Brussels
- STORK-eID, to be implemented in Brussels

Pilot cities will make use of the Living Lab Methodology to efficiently engage Citizens and SMEs in developing new innovative applications.

In parallel, the pilot sites will work together to create new cloud-based mobile parking services and solutions:

- eID Parking Permit (parking permits issued based on national ID cards)
- MyNeighbourhood Community Parking (sharing parking spaces with neighbours)
- Park-With-Us (P2P parking space rental)
- Intelligent Parking Locator (guiding drivers to the closest available free parking spot)

Pilot sites will test a range of scenarios, combining multiple services with local datasets to deliver enhanced functionality.

In order to validate the re-use of ECIM services across local and national borders and test their interoperability, ECIM will leverage the transport network of partner CenGROUP to run a Proof of Concept (PoC) in wider Birmingham. Additionally, it is planned that eIDs from a number of Member States, including STORK, will be utilized for login of super-users in differing countries.

Document name:	WP44.6				Page:	14 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

These super-users will have the ability to add and delete code, alter application parameters, including payment gateways and bank accounts, and access log files.

The project is due to end in Q3 2016.

7.2.2 ABC4Trust as a Service

The goal of ABC4Trust is to address the federation and interchangeability of technologies that support trustworthy yet privacy-preserving Attribute-based Credentials (ABC). So far, credentials such as digitally signed pieces of personal information or other information used to authenticate or identify a user were not designed to respect the user's privacy. They inevitably reveal the identity of the holder even though the application at hand often needs much less information, for instance only the confirmation that the holder is a teenager or is eligible for social benefits. In contrast to that, Attribute-based Credentials allow a holder to reveal just the minimal information required by the application, without giving away full identity information. These credentials thus facilitate the implementation of a trustworthy and at the same time privacy-protecting digital society.

ABC4Trust credentials will be issued as a result of a request from a FutureID user. The ABC4Trust integration would be at demonstrator / lab level only.

7.2.3 EEMA Website Portal

EEMA is an independent association of IT professionals, businesses and governments, providing business and technical networking opportunities at both local and regional levels in the broad areas associated with digital identity and its applications, including security.

For 25 years, EEMA has been Europe's leading independent, non-profit e-Identity & Security association, working with its European members, governmental bodies, standards organisations and interoperability initiatives throughout Europe to further e-Business and legislation.

EEMA's remit is to educate and inform around 160 Member organisations (and over 1,500 Member contacts) on the latest developments and technologies, at the same time enabling Members of the association to compare views and ideas

The EEMA website is a highly visible international website for use by infosecurity and identity experts across Europe. As a statement of support of DG-Connect's objectives, the FutureID integration would provide added value to EEMA's standing in that directorate.

7.2.4 ISSE Registration

ISSE is an international security conference held by EEMA. The system is operated by Cirdata Ltd. Cirdata is a technology-driven organisation providing fully integrated audience management and development solutions for publishers, event organisers and data owners.

Document name:	WP44.6				Page:	15 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

Online registration and data capture is the first stage of almost any event, and the key to its success. Cirodata creates advanced customer journeys using flexible, dynamic, intelligent web and mobile forms together with apps that simplify and improve the customer experience, whilst capturing and reporting core data. Cirodata's Fusion platform provides event organisers with 24/7 access to real-time data through easy-to-read dashboards and reporting.

All major payment providers are integrated into the registration process allowing the direct collection of revenue by the organiser. Delegate payments and fees can be handled in multiple currencies and localised VAT schemes. Full e-commerce functionality is available through Cirodata's dedicated and flexible shopping cart.

The use of eIDs will speed up delegate registration and encourage uptake.

7.2.5 Digidoc

DigiDoc is a system that is widely-used in Estonia for storing, sharing and digitally signing documents. Digidoc has received almost 100 million signatures by 2012 and has a growth rate of over 100% each year.

Because digital signatures carry the same legal weight as paper signatures in Estonia, a secure, easy-to-use platform is needed to give government institutions, businesses and private persons a way to transmit files and add digital certifications.

After logging into the DigiDoc system with an ID card or Mobile ID, a user can upload any document, digitally sign it, and forward it to other parties for their signatures. Any type of file can be entered for signature – a word processing document, a photo or even an instant messaging chat. Voice recordings can be uploaded by phone.

The documents are stored in a unique folder for each user. Every time users log on, they see their own uploaded files and as well as any they have signed. DigiDoc utilizes the public key encryption of the Estonian ID card and Mobile ID, meeting the EU's strictest standards for security.

The system is extensively used in Estonia's public sector, handling everything from court documents to municipal contracts. It's also commonly used in the banking industry, though its popularity in all areas of business is growing rapidly.

7.2.6 Fraunhofer WikiMedia Access

Fraunhofer is Europe's largest application-oriented research organization. Its research efforts are geared entirely to people's needs: health, security, communication, energy and the environment. As a result, the work undertaken by its researchers and developers has a significant impact on people's lives. Fraunhofer shapes technology and designs products. It strives to improve methods and techniques.

Within the group of 23,000 staff are qualified scientists and engineers. It has a €2 billion annual research budget totalling. Of this sum, €1.7 billion is generated through contract research. More

Document name:	WP44.6				Page:	16 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

than 70 percent of the Fraunhofer-Gesellschaft's contract research revenue is derived from contracts with industry and from publicly financed research projects. Almost 30 percent is contributed by the German federal and Länder governments in the form of base funding.

Affiliated international research centres and representative offices provide contact with the regions of greatest importance to present and future scientific progress and economic development.

As a result, its Wikimedia resource is required to be highly secure but currently relies username/passwords for access despite each Fraunhofer employee holding a PKI-based smartcard. The integration of FutureID would significantly improve the security of the WIKI and expand opportunities for safe collaboration.

7.2.7 ELSTER

The ELSTER online portal provides the following services to all tax citizens in Germany:

- Information about electronic tax card (only possible for a registration with identification number)
- Request for activation for tax account query (with signature card)
- Tax account query (with signature card)
- Personal Mailbox
- Issuing a certificate / registration with signature card
- Personal Mailbox
- Request for activation of electronic transmission of messages about actually exempt investment income of summary reports, notifications according to the EU -Zinsrichtlinie from church control data and requests for refunds of VAT (sending mass data on the ELMA5 interface of the Federal Central Tax Office)
- Request for activation of electronic transmission of documents in the process application for VAT refund domestic entrepreneurs abroad (UStVEU)
- Request for allocation of an EMAK -number
- Application for admission to church tax deduction method under § 51a paragraph 2c Income Tax Act (ITA), modification and deletion of data
- Registration display for attending the taxation schemes of a one-stop shop

The ELSTER online portal manages credentials as follows:

- Creating profiles: In order to expedite the completion of forms, profiles can be created. They contain data that remains on the registration periods of time equal to such. Example, name, tax identification number, telephone number, etc. When filling out a form, a corresponding profile can be selected and the associated profile data is then automatically filled in the form.
- User Settings: The user can set the e-mail notification of incoming information in a personal mailbox individually.
- Display the permissions of my user account.
- Security Settings: The PIN of the Software or security -Zertifikats sticks can be changed here.

Document name:	WP44.6	Page:	17 of 34				
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

- Delete account (also in the public domain): The user account can be deleted anytime, and it will destroy all data. The user account cannot be reactivated.
- Exchange of safety Sticks: Users of the ELSTER, ELSTER special with stick or G & D Starsign USB token can change to a G & D Starsign Crypto USB token, without having to re-register
- Change the type of login: Users of ELSTER-Plus can upgrade to ELSTER, ELSTER special or base, without having to re-register.
- Internet-export declarations-Plus (IAA -Plus): With an electronic ELSTER certificate the user can login via the customs portal online and complete / submit a IAA-Plus declaration when the export consignment is declared to a German customs office of export.

7.2.8 Deutschebank Online Portal

Since the number of multi-million user credential leaks increased dramatically over the last year and as a consequence the European Central Bank published “recommendations” to migrate to two-factor authentication, the European banks see an increasing pressure to improve authentication security. At the same time, they would like to maintain the highest possible convenience for their customers and offer services like Single-Sign-On for all bank-operated services. Many larger banks operate in several European countries and therefore need multi-national solutions in contrast to today’s nation-specific approaches.

At this point, FutureID could provide significant benefits in terms of security, user convenience and cost optimisation for banks and customers. With the ability to address multi-national eID credentials it could in particular provide a benefit for banks with international footprint since it allows to maintain one single authentication solution for all European countries, using all relevant European eIDs. From the user perspective, an easy-to-use two-factor authentication solution is provided with a strong identity proof. It can therefore simplify processes like the online identification for opening a new bank account.

Banks could provide further user convenience while maintaining high security when they allow to derive credentials from an official eID card for later use on mobile devices. With these mobile IDs the user could authenticate in a simple, yet secure way (e.g. when storing the derived ID on a Secure Element) after an initial enrolment with their official eID card. The use of FutureID would dramatically reduce the effort on the bank side for supporting all the different types of eIDs in Europe.

Deutsche Bank has a large number of international clients for eBank Account Management (eBAM) where a federated use of eIDs would be of significant advantage and where existing efforts have proven too costly.

7.3 Analysis of Candidate Submissions

The number of submissions for exemplar applications were in part a result of two linked questions:

- Doubts over the sustainability of the FutureID architecture

Document name:	WP44.6				Page:	18 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

- Amortization of effort by the service providers.

The long term availability and maintenance of FutureID components was a concern for those applications that were already in production and for this reason any integration was likely to be conducted within a test environment only.

It should be remembered that even if the integration effort and code is provided without charge, the cost of testing (and possibly certifying) the integration for a real system may be considerable. Unless there is an actual immediate business need, resources may not be available and the benefits not immediately realisable.

As a result of the above and other planning issues unconnected to FutureID, these candidates were further reduced in number as follows:

Partner	Candidate Name	Accepted	Status	Explanation
EEMA	ECIM	✓	Proceed using Apache AIS	Continuing requirement for high assurance admin login
FHG	Fraunhofer WikiMedia	✓	Proceed using Jbos AIS	Requirement for secure card-less authentication for multiple stakeholders
IBM	ABC4Trust as a Service	✓	Proposal as lab demo only	Limited resources within project timeline for full demo.

GD	ELSTER	✗	Proposal terminated	Politically too complex to integrate within timeline of FutureID
SK	Digidoc	✗	Proposal terminated	Limited resources at SK
GD	Deutschebank Portal	✗	Proposal terminated	Limited resources at Deutschebank to integrate into testbed
EEMA	ISSE Registration	✗	Proceed	Limited window for integration
EEMA	EEMA Website Portal	✗	Proposal terminated	Website under redevelopment

Table 5: Accepted and rejected candidates

Document name:	WP44.6				Page:	19 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

8. Exemplar Integration Planning

The integration of FutureID components into applications followed a standard format of engagement with the Exemplars (excluding ABC4Trust demo).

		Dates Completed	
Action.1	Confirmation and agreement for participation	ECIM	Fraunhofer
	Each candidate Exemplar receives the introductory letter (Appendix 2) which includes basic terms and conditions of use, including liability waiver. This ensures that the Exemplar has confidence in the ongoing support and availability of FutureID as well as clear visibility of limits regarding to SLAs and liabilities	07/05/2014	07/05/2015
Action. 2	Face-to-face or webex meetings covering business and semi-technical topics	ECIM	Fraunhofer
	The purpose of these meetings is to discuss practicalities and timescales of the integration exercise and to ensure that no gaps remain between parties.	15/04/2015	13/05/2015
Action. 3	Provision of technical specification of the AIS to the Exemplar Technical lead	ECIM	Fraunhofer
	This can be found in full as FutureID deliverable: D44.03 Technical Specification for AIS.	16/05/2015	16/05/2015
Action. 4	Confirmation of systems compatibility	ECIM	Fraunhofer
	This is a due diligence milestone for the Exemplar.	25/06/2015	10/06/2015
Action. 5	Collection of socio-economic information	ECIM	Fraunhofer
	A questionnaire was compiled to record the socio-economic criteria that influenced the decision of Exemplars to be included in FutureID trials. This is detailed in document: "WP12 FutureID Interview Guideline Value Proposition". The detailed questions are shown in Appendix 3, and the responses are recorded in WP12.	06/10/2015	02/07/2015
Action. 6	Integration workshop between ECSEC and Exemplar technical team and workshare allocations	ECIM	Fraunhofer
	This is the main workshop at technical level, confirming the details of the integration.	23/09/2015	16/09/2015
Action. 7	Integration	ECIM	Fraunhofer
	The actual integration between the AIS and the Exemplar application	19/09/2015	16/10/2015

Document name:	WP44.6				Page:	20 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

Action. 8	Testing and Sign off	ECIM	Fraunhofer
	Completion of technical assistance from FutureID project	30/10/2015	
Action. 9	Production and long-term relationship with a participating FutureID partner)	ECIM	Fraunhofer
	Sustainability action	After end of project	

Table 6: Timetable

The ABC4Trust integration consisted of an ad hoc technical demonstration in the laboratory.

Document name:	WP44.6	Page:	21 of 34				
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

9. Collection of Socio-Economic Information

This chapter presents the results of a qualitative interviews that were performed by the FutureID project with users of the Fraunhofer wiki pilot, and the ongoing value discussions and interview with the technical coordinators of the ECIM project. In the case of the Fraunhofer wiki pilot, the interview was conducted in collaboration with the SkIDentity Project (<http://SkIDentity.de>).

As “users” we understand all parties using FutureID: end users, service providers as well as identity providers. The goal of the interviews was to assess the value proposition of the FutureID technology for its prospective users. Thereby, the future market development of the outcomes of FutureID, particularly after the project’s end, can be prepared.

9.1 ECIM

(<http://www.ecim-cities.eu>)

The telephone interview took place on 13th of October 2015 with Hugo Kerschot, the project manager for ECIM. He has the final decision on selection.

ECIM is an CIP Innovation project consortium looking for sustainability/business opportunities. The business will be offering a platform/market place for intelligent mobility solutions. As it is still an ongoing project and not a company, the customer-base is so not yet 100% defined but will address: end consumers of smart mobility services; mobility service providers looking for opening their market; and cities, companies, organisations looking for integrated mobility solutions.

The market place concept will provide the consumer with better mobility services, which are: faster, cleaner, and cheaper. It will bring different mobility players together and offer them added value (single sign-on, single payment solution, broader market access...).

The ECIM project has a specific requirement for EU-wide strong authentication to secure the administrative and super-user access to the ECIM platform for developers and administrators of dozens of different services on the platform. A low assurance authentication, using username and password was also chosen so that application users would have frictionless access, via a mobile phone to ECIMs services, primarily built upon mobility and public transport.

FutureID will provide the trust and security needed when new mobility service providers and developers want to log onto the ECIM marketplace and do business with ECIM.

It is expected that the cost should be zero for the trial, but with low-level fees acceptable in the production version. What is essential are well documented specifications and manuals. At present there is little information regarding SLAs and longer term pricing.

Document name:	WP44.6				Page:	22 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

The FutureID implementation will be deemed a success with a good technical solution, a good SLA and low maintenance.

As a background, from the conception of the project, it was understood that the issuance of a single authentication token would inhibit the take up the ECIM marketplace development. ECIM was always intended to be accessed by a geographically and organisationally diverse set of developers building new and regional services. The potential cost of issuance and lifecycle management of ECIM specific credentials would also be restricting.

FutureID was decided upon by ECIM management at an early stage as being potentially capable to federate its super-users via the STORK2.0 initiative by the EU and directly via specific member state eIDs and corporate identities.

Several technical and planning meeting were held regarding the strong authentication requirement and Single-Sign-On during the course of 2015 with the resultant decision to integrate.

9.2 Fraunhofer Wiki

(<https://futureid-test.izs.fraunhofer.de/mw/>)

The interview took place on 2nd of July 2015 with representatives of the Fraunhofer Headquarters.

- The following persons were present:
- Andreas Abele (FhG Headquarters)
- Björn Vollmer (FhG Headquarters)
- Detlef Hühnlein (ECSEC GmbH)
- Heiko Roßnagel (FhG IAO)
- Karin Haenelt (FhG Headquarters)
- Max Tüngerthal (ECSEC GmbH)
- Michael Kubach (FhG IAO)
- Oliver Schumacher (FhG Headquarters)

In the beginning of the interview the currently used authentication methods were presented. Internal employees are using their smartcard or a username/password combination for authentication whereas external employees are mostly limited to the username/password method. This method is known to be very easy to implement in web applications but from the information security point of view completely out of date. Numerous cyber-attacks can be applied to bypass this mechanism by stealing the username and password combination. Since most projects include numerous partners with access to sensitive data, the possibility of an unauthorized access of a third party is fairly high. This leads to the fact that the future demand for secure, so called “strong” authentication and authorization methods is estimated to be high. The use of more secure authentication mechanisms allows the secure handling of sensitive data

Document name:	WP44.6				Page:	23 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

and thereby meets the requirements of future projects and business partners that handle highly confidential data.

In the following part of the interview the added value of the FutureID technology is discussed. The interview partners assume a reduction of administration costs and an increase in the user acceptance. The handling of multiple systems even within a single project is very time consuming when username/password combinations are used. Every participating partner requires the creation of a user account and the associated credential management. The use of a federated identity management system like FutureID gives the administrators of the wiki the possibility to bypass this effort and dedicate more resources on user role management. Furthermore, potential problems considering privacy issues and an unclear methodology to delete user accounts were identified. As a result, the importance of a reliable user role management to address these problems was pointed out.

9.3 ABC4Trust

(<http://www.abc4trust.eu>)

As this was a technical demonstration only, there was no socio-economic analysis.

Document name:	WP44.6				Page:	24 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

10. The Integration Experience

10.1 ECIM

There exists a SAML plugin for Liferay that could have been used for the integration of ECIM. However, this plugin is only available for Liferay Pro and ECIM uses only the community edition of Liferay. Therefore, we had to develop our own Liferay plugin that connects Liferay with the AIS. This plugin was developed by ECSEC. The main difficulty was to become acquainted with Liferay plugin development. It turned out that Liferay is highly extensible and it was therefore no problem to make the connection between Liferay's authentication mechanisms and the AIS / FutureID. However, this high extensibility comes with high complexity and it therefore took 10 person-days to develop the plugin.

The application can be found here: <http://platform.ecim-cities.eu/> .

The enrolment in ECIM is self-registration:

1. The user authenticates with FutureID. The SAML assertion contains the firstName and the lastName and optionally the email of the user.
2. Liferay then shows a registration form where available attributes are pre-filled and readonly. The user has to provide missing attributes:
 - email (required) (if not provided by FutureID)
 - gender (optional)
 - dateOfBirth (optional)
3. The user can complete registration by pressing "Save".

The following credentials will be accepted by ECIM:

- STORK
- German eID
- Estonian eID
- Portuguese eID
- Austrian eHealth Card
- Facebook
- LinkedIn
- Software Certificates (for testing)

10.2 Fraunhofer Wiki

For the Fraunhofer Wiki integration ECSEC developed a Media Wiki extension that connects to the AIS. Conceptually the main challenge was to find a good solution for user provisioning. In contrast to the other applications (ECIM and ABC4Trust), the Fraunhofer Wiki does not allow users to self-register. Instead an administrator of the wiki creates accounts. These accounts then have to be connected to FutureID pseudonyms that are derived from the user's credential (e.g.,

Document name:	WP44.6				Page:	25 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

an eID card). This task was solved by a flexible Identity Management component that connects FutureID pseudonyms with user accounts based on email confirmation.

Fraunhofer provided ECSEC access to a demo Media Wiki instance that is identical to productively used wikis. Therefore, it was very easy for ECSEC to test the extension under realistic conditions. Such a playground simplifies and therefore speeds up development. Also, results, open issues, and possible solutions can be discussed easier by experimenting and looking at such a demo. Integrators should therefore insist on getting access to such a playground.

The demo can be found here: <https://futureid-test.izs.fraunhofer.de/mw/>

The next step is to integrate the FutureID Wiki ([https://publicwiki-01.fraunhofer.de/Future ID](https://publicwiki-01.fraunhofer.de/Future_ID)) this is expected to be integrated by end of November.

The final step then is to make the extension available to all public wikis of Fraunhofer. There is no timeline for this step yet.

10.3 ABC4Trust

The ABC4Trust integration was constructed in the IBM Research Laboratory and as such was a technical only exercise to show that FutureID credentials could successfully be transformed into ABC4Trust credentials. A plug-in was easily modified to provide the correct interface. The demo can be found at: <https://futureid-abc4trust-issuer.mybluemix.net> .

Document name:	WP44.6				Page:	26 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

11. Sustainability

11.1 Sustainability of the FutureID architecture

FutureID is an FP7 project and as such has a life of three years. Without a sustainability plan in place the ability to convince application owners to invest in integrating FutureID for a short period only is challenging.

There are two potential options for sustainability of the exemplars after the end of the FutureID project.

11.1.1 Long Term Sustainability

As part of task T13.5, “Exploitation Planning & Reporting”, and its associated deliverables D13.5.1, D13.5.2 and D13.5.3, sustainability and exploitation of FutureID will be managed through the FutureID Foundation. This foundation will support the present and expected FutureID implementations as well as managing IPR, development and ongoing research. It is expected that the FutureID Foundation will offer technical support as part of its business value and the exemplar solutions could be maintained through this organisation. It is expected to take a number of months before the FutureID Foundation will be functional, and an interim support mechanism is required. The exact scope and membership has also yet to be determined.

11.1.2 Interim Sustainability

To ensure sustainability in the interim, ECSEC has undertaken, if needed, to incorporate FutureID into the SkiDentity project (<http://SkiDentity.de>) for which it is a service provider. The goal of SkiDentity is to build a solid bridge between electronic identity cards (eID) and the existing and emerging cloud computing infrastructures. For this purpose, the existing components, services and trust infrastructures are integrated into a comprehensive, legally valid and economically viable identity infrastructure for the cloud. Special attention is given to the demands of small and medium enterprises and authorities.

Document name:	WP44.6				Page:	27 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

12. Conclusions

FutureID clearly has value.

Even at its basic configuration, without the use of multiple broker services, the simplicity of integration, the broad base of credentials available to utilise – including many eIDs - and the capability to add new credentials easily has a strong appeal to organisations that span multiple domains and user sectors, whether they are geographically separated or separated by sector.

The perception of expense and effort in establishing a suitable federated identity system from scratch will lead to an increase in smaller and cheaper applications starting to be utilised, and will be fuelled by the ever increasing ‘App’ market. Simple low cost and low effort integration is therefore essential and FutureID provides that.

As the market matures and expands and applications evolve their existing requirements, the need for the advanced, but as yet not production ready features of FutureID, especially digital signing and multiple broker services will become apparent.

Document name:	WP44.6				Page:	28 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

13. Appendix 1 Service Provider Prioritisation Tool



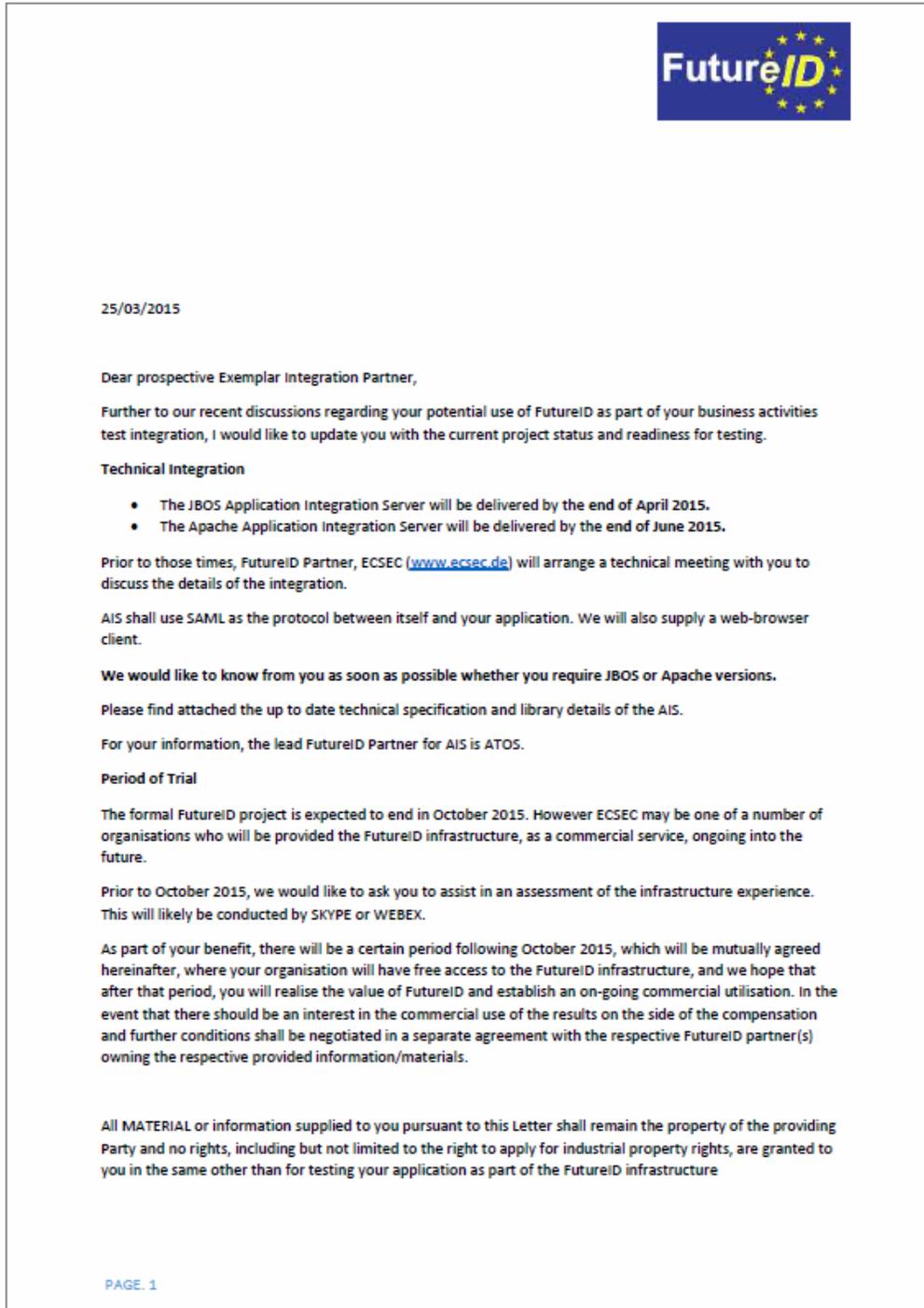
D44.6: Prospective FutureID Exemplar Service ScoreChart

Partner Shortcode		Description	
Date			
Partner contact			
Partner mobile			
Service Name			
Operator			
URL			
TOTAL SCORE	0.00		

Score 1=low match to criteria, 10=high match to criteria (if unsure score as 5 and highlight yellow)

Detail	SubGroup	Score /10	Comment
Application Type	Visible	0	
	Trustworthy	0	
	Legal binding transactions	0	
	FutureID is cheaper than multilateral	0	
Users	Long term use	0	
	Large User Base	0	
	Expanding User Base	0	
	Different types of users and credentials	0	
European Dimension	Turnover of users	0	
	Impact	0	
	Cross-Border	0	
Authentication	Interoperability	0	
	Multi-Factor	0	
	Secure	0	
	Interest to improve strength of authentication	0	
Identity	Interest in using different Tokens	0	
	Optional privacy preserving login	0	
	Trusted	0	
Privacy	Trusted Federation Capable	0	
	Uses National eIDS	0	
	Selective disclosure of attributes	0	
	Privacy Sensitive	0	
	Optional privacy preserving login	0	
Technology	No user tracking in broker	0	
	Appropriate Transparency	0	
	Java	0	
	C++	0	
	Existing EIS	0	
	Varied Protocols	0	
	Transaction Rollback or error correcting	0	
Technology PHP	0		
Technology Ruby	0		
Technology DotNet	0		
Other	Accessible	0	
Other	User-friendly	0	
Other	Green-as in eco-friendly	0	
Other	Privacy: Aggregation of attribute values / proofs on attributes	0	

Please return to jshamk@ejconsultants.co.uk (D44.6 Lead)



14. Appendix 2: Introductory Letter to Exemplars

Document name:	WP44.6				Page:	30 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

Document name:	WP44.6				Page:	31 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

Therefore, it is understood that you will not be permitted to distribute to others the accessible information and/or MATERIAL without the providing Party's written consent.

If you agree to test your application as part of the FutureID infrastructure you agree to use the MATERIAL and information in compliance with all applicable statutes and regulations.

To the extent that the MATERIAL has not been destroyed or used during such evaluation or testing and unless there is no other agreement between the Parties or any other obligation to keep MATERIAL, any MATERIAL shall be returned to the providing Party at the request of the providing Party

Liability

Please note that this is a non-commercial period. For that reason we suggest that FutureID is not integrated into your production application but rather into a test environment. After this trial period, we hope that you will incorporate it into your production business on a commercial basis with ECSEC or others. Any material, in particular software components, hardware or information delivered to you pursuant to our discussions and this letter, is understood to be experimental in nature and may have hazardous properties. You confirm by signing this letter that the providing Party MAKES NO REPRESENTATIONS AND EXTENDS NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED. THERE ARE NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE USE OF THE MATERIAL OR INFORMATION WILL NOT INFRINGE ANY PATENT, COPYRIGHT, TRADEMARK, OR OTHER PROPRIETARY RIGHTS. Unless prohibited by law, you assume all liability for claims for damage against it by third parties which may arise from the use, storage or disposal of the delivered issues or accessible property or information except that, to the extent permitted by law, the providing Party shall be liable to you when the damage is caused by the gross negligence or willful misconduct of the providing Party.

FutureID Logo

Please also find attached a copy of the FutureID Associate logo, which recognises your assistance and when placed on your communications will demonstrate your contribution to this important European project.

We look forward to working with you on this exciting project.

Sincerely

Jon Shamah

FutureID

PAGE. 2

Document name:	WP44.6	Page:	32 of 34				
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

15. Appendix 3: Socio-Economic Questionnaire

15.1 General background questions

- Please explain to us, what your company/organization is doing. What product is it selling, what kind of service does it offer?
- Who are your (main) customers/users?
- What is the end-benefit for the customer/user?
- What makes your offering unique and different, how are you trying to differentiate from your competitors?
- What is your personal position in your company/organization?

15.2 Identity Management

- What role does authentication play for your product/service?
- How is the authentication performed at the moment (Smartcards, Mobile Phones, Username/Password...)?
- What are the challenges concerning authentication?
- With what partner could you federate with (e.g. clients, supply-chain partners, stakeholders, external staff)?

15.3 Integration and Added Value of FutureID

- Which value could FutureID deliver to you as user of the technology?
- Which value could FutureID deliver to your users/customers?

Examples how Value could be created are through:

- Newness of the value (e.g. entirely new technology)
- Performance (e.g. more power, faster, bigger)
- Customization (tailoring the product to the specific needs of an individual customer/customer segment)
- “Getting the job done” (customers/users can just focus on their core competencies)
- Design (immaterial value)
- Brand/status (immaterial value)
- Price (e.g. similar value at a lower price)
- Cost reduction (helping customers to reduce costs)
- Risk reduction (helping customers to reduce risks)
- Accessibility (making services accessible to customer that earlier were not able to use them)
- Convenience/usability

Document name:	WP44.6				Page:	33 of 34	
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final

- Which one of your users'/customers' problems with authentication are we trying to solve?
 - How could FutureID help in solving these problems?
- Which of your needs as a user/customer of FutureID' are we satisfying?
 - Which of the needs of your users/customers are we satisfying?
- What bundles of products and services can be offered by using FutureID to each of your user/customer segment?
- How can the costs for the federation get paid? (transactional, flat-rate... - what is the business model)

15.4 Additional questions

- What are the existing technologies in use?
- What costs do you expect for the change (related to value)?
- What technical information is needed to implement FutureID?
- Are there internal resources available or is are they outsourced?
- What business information is needed (and in what format) to assist in the business decision processes?
- Who are the final decision makers (levels and role): Technical owner, business owner, procurement owner?
- What are the amortisation and ROI parameters?
- What are the criteria for a 'successful' implementation?

Document name:	WP44.6	Page:	34 of 34				
Reference:	D44.6	Dissemination:	PU	Version:	1.01	Status:	Final