D13.1.3 Internal Bulletin #3 August 2013

Document Identification	
Date	12/09/2013
Status	Published internally
Version	101

Related SP / WP	SP13	**Document Reference**	D13.1.3
Related Deliverable(s)	13.1.3	**Dissemination Level**	PU/CO
Lead Participant	EEMA	**Lead Author**	Jon Shamah
Contributors	All	**Reviewers**	RD, HR

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

1. Executive Summary

This is the third quarterly internal newsletter with the aim to enable a consortium wide coordination and agreements on dissemination, reporting on the dissemination activities, key goals and identified potentials, as well as a review of project outcomes to date.

2. Document Information

1.1 Contributors

Name	Partner
Jon Shamah	EEMA
Fiona Hawkins	EEMA
*	All other Partners

1.2 History

Version	Date	Author	Changes
100	04/09/2013	JS / EEMA	Initial
101	12/09/2013	JS / EEMA	Minor changes

1.3 Table of Figures

N/A

1.4 Table of Tables

N/A

1.5 Table of Acronyms

N/A

1.6 Referenced Documents

N/A

3. Table of Contents

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

5. Internal Newsletter #3 - August 2013

Internal
Newsletter 3
Sept 2013

FutureID Shaping the Future of Electronic Identity

LATEST NEWS

July/August vacations have meant that many tasks and work packages have continued to progress but have not had notable changes in status.

CHANGE OF CONSORTIUM:

GTO has terminated participation in FutureID. New Partner: Radbound University. Request for Amendment has been made. We wait for approval by EC.

CHANGE OF PERSONNEL:

- Jan Zibuschka (FHG) -> changed jobs, is now at BOSCH Research
- Pouyan Sepehrdad (TUD) has left the project

DISSEMINATION:

There is a new WIKI page for reporting dissemination centrally. It can be found at: https://publicwiki-01.fraunhofer.de/Future_ID/index.php/WP13:_Dissemination_Reporting

Christian Hanser, Daniel Slamanig - "Warrant-Hiding Delegation-by-Certificate Proxy Signature Schemes" - 14th International Conference on Cryptology in India (INDOCRYPT 2013)

Christian Hanser, Daniel Slamanig - "Blank Digital Signatures" - 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2013)

Bernd Zwattendorfer, Daniel Slamanig - "On Privacy-Preserving Ways to Porting the Austrian eID System to the Public Cloud" - 28th IFIP TC-11 International Information Security and Privacy Conference (SEC 2013)

Bernd Zwattendorfer, Daniel Slamanig - "Privacy-Preserving Realization of the STORK Framework in the Public Cloud" - 10th International Conference on Security and Cryptography (SECRYPT 2013)

FUTUREID TEAMS UP WITH LEADING EUROPEAN INSTITUTIONS, ASSOCIATIONS, ENTERPRISES AND PROJECTS TO LAUNCH THE NON-PROFIT OPEN SIGNATURE INITIATIVE

This initiative (http://opensignature.org) aims at improving transparency and interoperability with respect to electronic signature technology and related trust services. The Open Signature Initiative is open for all stakeholders with respect to electronic signatures in Europa and is initially supported by the European Network and Information Security Agency (ENISA), the European Association for eIdentity and Security (EEMA), the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), the German IT Security Association (TeleTrusT), the Estonian Certification Center (AS Sertifitseerimiskeskus, SK), the Open eCard Project, the STORK 2.0 Project, AuthentiDate International AG, the Competence Center for Electronic Signatures in Health Care (CCESigG), ecsec GmbH, GAD eG, Giesecke & Devrient GmbH, intarsys consulting GmbH, OpenLimit SignCubes AG, Procilon Group, Thames Stanley GmbH, Trustable Ltd and of course the FutureID Project.

EXTERNAL NEWS

LSP & SUSTAINABILITY

- Final report on long term sustainability of the EU Large Scale Pilots is published by Deloitte

EU REGULATION ON EIDAS

- Public hearing of ITRE is scheduled on 18th of Sep; final agenda is not published yet.
- Trilog (Parliament, Council, Commission) would be expected in Oct./Nov. 1st reading along Parliament is expected on 10th of Dec.

WP, DELIVERABLES AND TASK NEWS

WP01

As project month is approaching, the preparations for the review, the annual project management report, and the financial report are running. The report will be due 4 weeks after the end of M12.

WP2.1 VISION, APPROACH AND INVENTORY

"Work package 21 is currently working on the FutureID reference architecture (D21.4), which will be released by project month 12. The Business and Use Case analysis (D21.5) is currently analysing the top 5 use cases which emerged from the PESTLE analysis.

D21.4: REFERENCE ARCHITECTURE

Last activities in scope of this task focused on investigating of different architecture configurations that may use not all infrastructure components. Results of this analysis have been presented in form of self-describing pictures.

Current work goes into details with description of objectives and approach to particular backend components.

The newest version of the 21.4 deliverable is accessible on the wiki.

WP2.2 REQUIREMENTS ANALYSIS

TASK 22.2:

The deliverable addresses the security requirements for the client and the backend components. Requirements were defined by developing the security problem definition and deriving security objectives from it. The deliverable is almost complete and first reviewer comments have been integrated. A submission close to the deadline is expected.

TASK 22.5: SOCIO ECONOMIC REQUIREMENTS

Deliverable D22.5 is currently being finalized and will be delivered on time. It builds upon B2B- and B2C-scenarios, and conducted a stakeholder analysis. The deliverable provides general socio economic requirements and specific requirements for B2B- and B2C- scenarios. Thus, it enables a complete view on the FutureID infrastructure from the end-user and from the business perspective.

TASK 22.6: LEGAL REQUIREMENTS

The objective of this task is to provide an overview on the different legal requirements for FutureID, which are for example regulated by the Data protection - , e-Commerce - and e-Signature Directive. Currently the draft is in review. It should be finished at the beginning of September.

TASK 22.7:

Work on deliverable D22.7 is proceeding according to schedule and should be finished by the end of August. The work was bolstered by the WP 22 synchronization meeting held in Kiel in the middle of July. D22.7 details the accessibility and inclusion requirements that should ensure that the FutureID client is usable by the most people possible regardless of disability. The deliverable also includes legal requirements for handling personal user data that is related to accessibility and inclusion functionality.

D22.7: ACCESSIBILITY AND INCLUSION REQUIREMENTS

This is now ready for submission and available on LiveLink

WP2.3 DESIGN GUIDELINES

Work Package 23 has been completed. All deliverables have been submitted.

WP3.2: EID SERVICES

D32.3: INTERFACE AND MODULE SPECIFICATION

The deliverable provides a specification of the interfaces and modules of eID Services provided by the FutureID client. It specifies the architecture, the interfaces, and the extension mechanisms to support arbitrary authentication protocols, credentials and plug-ins. It also states the credentials management, the identity and attribute selection as well as the negotiation of Levels of Assurance.

The deliverable is currently under review and will be finished within the next weeks.

D32.4: IMPLEMENTATION OF BASIC AND GENERIC MODULES

The basic and generic modules for the FutureID client comprise an Event Manager, the Dispatcher integration, the Service Access Layer (SAL), the Add-on Framework, Application Protocol Data Units (APDU), an Error Management, and an Internationalization support.

The modules are assigned to the partners and will be implemented until November.

TASK 32.8 LEGAL ANALYSIS OF EID CLIENT SERVICES

The objective of this task is to produce a comprehensive analysis of the legal framework surrounding the provisioning of FutureID client services. Particular attention will be given to issues of data protection and national restrictions on the use of eID credentials in cases where this is necessary. At the moment preparative work is done in expectation of the final version of 22.6 and the finalization of administrative processes of the RU.

WP3.3: ESIGNATURE SERVICES

TASK 33.6 LEGAL ANALYSIS OF ESIGNATURE SERVICES

The objective of this task is to produce a comprehensive analysis of the legal framework surrounding the provisioning of FutureID eSignature Services. Particular attention will be given to the legal framework set forth by Directive 1999/93/EC and the ongoing developments with regard to the draft eIDAS Regulation. At the

moment preparative work is done in expectation of the final version of 22.6 and the finalization of administrative processes of the RU.

WP3.4: USER INTERFACE

TASK 34.2

During Task 34.2, Design Mock-ups were created for the FutureID client. Three different Mockups show the possible layout and usage of the provided functions for the FutureID client, as a desktop, mobile and desktop application. As the authors encourage feedback and opinions on the mockups, they have been uploaded to the FutureID Wiki, on the Task 34.2 page.

D34: IMPLEMENTATION OF BASIC AND GENERIC MODULES

The basic and generic modules for the FutureID client comprise an Event Manager, the Dispatcher integration, the Service Access Layer (SAL), the Add-on Framework, Application Protocol Data Units (APDU), an Error Management, and an Internationalization support.

The modules are assigned to the partners and will be implemented until November.

WP3.6: BROWSER INTEGRATION

D 36.X

The first deliverable D36.1 is currently in progress and is planned to be ready for review in mid of October. This means we are on track with the new DoW timeline. The second one D36.2 will be started September.

WP4.1: IDENTITY BROKER

D41.1: IDENTITY BROKER REQUIREMENTS

Finalised and fixes first cornerstones with respect to the central FutureID infrastructure.

TASK 41.6 LEGAL ANALYSIS OF THE IDENTITY BROKER

The objective of this task is to produce a comprehensive analysis of the legal framework surrounding the provisioning of the Identity Broker services. Particular attention will be given to issues of data protection and intermediary liability. At the moment preparative work is done in expectation of the final version of 22.6 and the finalization of administrative processes of the RU.

WP4.2: UNIVERSAL AUTHENTICATION SERVICE

D42.2: INTERFACE AND MODULE SPECIFICATION AND DOCUMENTATION

The deliverable describes the design and the architecture of the Universal Authentication Service. It comprises the specification of the interfaces which provides the communication to the Identity Broker and the FutureID client, respectively. Furthermore, this document provides a brief overview of the Basic Services and the Job Execution Environment of the Universal Authentication Service.

The deliverable is nearly finished and will be reviewed soon.

D42.3: AUTHENTICATION PROTOCOL SPECIFICATION LANGUAGE

DTU is driving the design of the Authentication Protocol Specification)APS) language (D42.3, to be submitted). This deliverable D42.3 is a result of discussions with our task partners via several telephone conferences. In

this deliverable, we introduced Future AnB, the projected APS language for the FutureID project. We presented its syntax and defined its formal semantics by translation to (an extended version of) strands to easily connect to the input languages of various tools like AVISPA and ProVerif. We also show how to translate protocol specifications in Future AnB into Java programs.

WP4.3: TRUST SERVICES

TASK 43.1 ANALYSIS OF TRUST ASPECTS

The objective of this task was to analyze the main aspects of trust within FutureID. The task has been finished.

WP44 APPLICATION INTEGRATION SERVICES

D 44.1 DESCRIPTION OF ENTERPRISE ARCHITECTURE

This has been submitted.

D 44.2 APPLICATION INTEGRATION REQUIREMENTS

This has just entered internal review and is planned to be submitted by early September

WP4.5 SERVER TESTBED

D45.1 REQUIREMENTS REPORT

Task 45.1, which provides a set of requirements to the server testbed has been submitted. Also the work on D45.2 has started, in order to provide a reference implementation environment for the server testbed, using a composition of toolsets, such as tools used for GUI testing, test (documentation) automation, and web service testing. By composing these toolsets, the server testbed will be able to deal with the various potential use cases of the FutureID infrastructure.

UPCOMING INDUSTRY EVENTS

MOBILITY IN A GLOBALIZED WORLD

Date: **16/09/2013,** Stuttgart, Germany Information

ENISA-WS ALONG EIDAS

Date: **24 /09/2013**, Brussels, Belgium Information

WS OF AN EU FUNDING PROJECT ALONG eIDAS

Date: **25/09/2013**, Brussels, Belgium Information

NFC WORLD CONGRESS

Date: **25/09/2013** Nice, France. Information

WORLD EID CONGRESS

Date: **25/09/2013**, Nice, France Information

INTERNATIONAL SECURITY SOLUTIONS EUROPE (ISSE)

Date: **22/10/2013**, Brussels, Belgium Information

RSA

Date: **29/10/2013**, Amsterdam, Netherlands. Information

CCS 2013 (ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY)

Date: **04/11/2013**, Berlin, Germany. Information

ICT 2013

Date: **6/11/2013,** Vilnius, Lithuania. Information

IDENTITYNEXT

Date: **19/11/2013**, Den Haag, Netherlands. Information

CARTES

Date: **19/11/2013**, Paris, France. Information

INTERNET IDENTITY WORKSHOP 16

Date: **22/11/2013**, Mountain View, USA. Information

FUTURE OF IDENTITY WORKSHOP OF ENISA AND G&D;

Date: **28/11/2013**, Brussels, Belgium Information