



D42.9: Testing Report

D42.9

Document Identification	
Date	2015-10-29
Status	Final
Version	1.0

Related SP/WP	SP4/WP4.2	Document Reference	D42.9
Related Deliverable(s)	D42.1, D42.4, D42.5, D42.6, D42.7, D42.8	Dissemination Level	CO
Lead Participant	ECS	Lead Author	Max Tuengerthal (ECS)
Contributors	Max Tuengerthal (ECS) Jerzy Szczebak (CO)	Reviewers	Pedro Malaquias (KUL) Mart Toom (SK)

Abstract: In this deliverable, we provide a test report for the FutureID Universal Authentication Service (UAS).

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.

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.



1 Document Information

1.1 Contributors

Name	Affiliation
Max Tuengerthal	ECS
Jerzy Szczebak	CO

1.2 History

0.1	2015-10-16	Max Tuengerthal (ECS)	Initial version
0.2	2015-10-23	Jerzy Szczebak (CO)	Unit Test Report Basic Services
0.3	2015-10-26	Max Tuengerthal (ECS)	Introduction and Test Specifications
0.4	2015-10-26	Max Tuengerthal (ECS)	Test Results
1.0	2015-10-29	Max Tuengerthal (ECS)	Finalization after internal review

1.3 Table of Contents

1 Document Information	1
1.1 Contributors	1
1.2 History	1
1.3 Table of Contents	2
1.4 List of Figures	3
1.5 List of Tables	3
2 Introduction	4
2.1 Abbreviations and Notations	4
2.2 Terms	5
3 Test Specifications	6
3.1 Unit Tests	6
3.2 Integration Tests	6
4 Test Report	11
4.1 Unit Tests	11
4.1.1 Basic Services	11
4.1.2 Execution Environment	15
4.1.3 UAS Web Application	16
4.2 Integration Tests	16
5 Conclusion	18



1.4 List of Figures

1	Coverage report for Basic Services class BSFactoryImpl	13
2	Coverage report for Basic Services package com.comarch.security.bs	15
3	Unit test report for the Execution Environment	15
4	Coverage report for the Execution Environment	15
5	Unit test report for the UAS Web Application	16
6	Coverage report for the UAS Web Application	16

1.5 List of Tables

1	Integration test specification TEST-UAS-test-1.	7
2	Integration test specification TEST-UAS-test-2.	8
3	Integration test specification TEST-UAS-test-3.	9
4	Integration test specification TEST-UAS-eac-1.	10
5	Unit test report for the Basic Services class BSFactoryImpl.	12
6	Unit test report for the Basic Services package com.comarch.security.bs.	14
7	Integration test report.	17

SP/WP: SP4/WP4.2	Deliverable: D42.9	Page: 3 of 18	
Reference: D42.9	Dissemination: CO	Version: 1.0	Status: Final



2 Introduction

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

The FutureID Broker provides an interface for service providers to connect to the FutureID infrastructure. Therefore, service providers are able to easily integrate arbitrary eID services using various user credentials. The Broker includes the Universal Authentication Services (UAS) which in turn performs the authentication of the users.

Authentication protocols are described in the Authentication Protocol Specification (APS) language, which makes it possible to support arbitrary protocols in a very efficient manner. The APS descriptions of the authentication protocols in turn refer to appropriate Basic Services. Basic Services provide a set of common functionality like cryptographic and smart card services, which are needed by the majority of the authentication protocols. The UAS acts as a Credential Consumer (CC) and is capable of authenticating users. The UAS encompass two interfaces, the Authentication-Interface for the communication with the users (i.e., FutureID Client or Browser) and the Universal Service Interface to communicate with the Broker. The core component of the UAS is the Job Execution Environment, which runs arbitrary authentication protocols specified in the APS language.

This deliverable provides test specifications derived from the requirements on the UAS and a test report.

2.1 Abbreviations and Notations

This section itemizes the abbreviations and notations used in this document.

APDU Application Protocol Data Unit
APS Authentication Protocol Specification
ASN.1 Abstract Syntax Notation One
CA Certificate Authority
CAPS Credential-specific APS (package)
CC Credential Consumer
EAC Extended Access Control
eID Electronic Identity (Card)
JKS Java Key Store
MAC Message Authentication Code
UAS Universal Authentication Service
PAOS Reverse SOAP
SCT Simple Credential Transformer

SP/WP: SP4/WP4.2	Deliverable: D42.9	Page: 4 of 18
Reference: D42.9	Dissemination: CO	Version: 1.0
		Status: Final

SOAP originally defined as Simple Object Access Protocol
SP Service Provider

2.2 Terms

This section provides descriptions for selected terms that are used in this document. The descriptions are taken from the FutureID terminology.¹

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

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

Electronic Signature Data in electronic form which is attached to or logically associated to other electronic data and serves as a method of authentication. From a legal perspective, an electronic signature is not necessarily considered equivalent to a handwritten signature. When it meets a number of conditions, it can be put on par with a handwritten one.

Protocol A protocol may be described as a set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems (e.g. an internet protocol).

In more general terms, a protocol can be qualified a series of ordered steps involving computing and communication that are performed by two or more system entities to achieve a joint objective.

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.

Universal Authentication Service (UAS) The Universal Authentication Service (UAS) is a FutureID component that implements a simple credential transformer (SCT) that consumes user credentials. It is typically operated by a broker. It is universal in the sense that it can support multiple authentication protocols based on a declarative protocol specification. This promises to greatly facilitate multi-protocol support as compared to a collection of single-protocol SCT, each of which comes with a different installation procedure and update cycle.

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

¹FutureID, WP21 - Vision, Approach and Inventory, D21.1 - FutureID Terminology, 2013.

SP/WP: SP4/WP4.2	Deliverable: D42.9	Page: 5 of 18
Reference: D42.9	Dissemination: CO	Version: 1.0
	Status: Final	