Interim Internal Report on Research on Protocols and Tools for Future eID Solutions

D24.3

Document Identification	
Date	July 14, 2015
Status	Final
Version	1.0

Related SP/WP	SP2/WP24	**Document Reference**	D24.3
Related Deliverable(s)	D12.3, D12.4, D22.1, D22.2, D22.3, D23.1, D24.1, D24.2, D34.1, D34.2	**Dissemination Level**	PU
Lead Participant	IBM	**Lead Author**	Jan Camenisch (IBM) Alfredo Rial (IBM)
Contributors	Jan Camenisch (IBM) Alfredo Rial (IBM) Paolo Modesti (UNEW) Daniel Slamanig (TUG) Sebastian Mödersheim (DTU) Jaap-Henk Hoepman (RU)	**Reviewers**	Lothar Fritsch (NRS) Max Tuengerthal (ECS)

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.

1 Executive Summary

The aim of the FutureID project is to build a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe. That is, the main goal of the project is to provide an architecture that allows the different eID solutions already deployed to be used in a unified and interoperable manner.

The aim of work package 24 is to address various shortcomings of existing and emerging eID solutions. In particular, we aim at extending the toolbox for the formal analysis to cope with the challenges arising in this context, such as the modelling and verification of complex, composed protocols and their privacy features. Another focus is on the development of new cryptographic mechanisms and protocols that complement privacy-enhanced credentials to match requirements that arise in large-scale environments. To this end, work package 24 conducts research on the following five tasks, and this deliverable describes the research conducted on these tasks during the second year of the FutureID project and provides a summary of the research results.

Task 24.1: Extending languages and tools for compositional reasoning. The purpose of this task is to provide languages and tools that allow the analysis of complex systems that are composed of multiple components. In the first half of year 3, we have achieved a significant step forward in the area of compositional reasoning with two kinds of *relative soundness results*. The first kind are typing results showing that any security protocol that fulfils a number of sufficient conditions has an attack if it has a well-typed attack. The second kind considers the parallel composition of protocols, showing that when running two protocols in parallel allows for an attack, then at least one of the protocols has an attack in isolation. In this deliverable, we present 1 technical report related to this task. In WP24, so far we have presented 3 publications and 1 technical report.

Task 24.2: Establishing methods and languages for privacy goals. This task aims at establishing methods and languages for the analysis of privacy goals with formal methods tools. It pursues that goal with two sub-tasks, one to establish a privacy analysis method and its formalization, and the other to establish semantics for claims languages to allow reasoning over them. For the first sub-task, we focus on applying the concept of α-β-privacy that we have developed previously to the FutureID architecture. For the second sub-task, we define and unify the concepts and features of privacy-preserving attribute-based credentials (Privacy-ABCs), provide a language framework in XML schema, and give a formal semantics to describe the effects of the transactions in a privacy-friendly authentication system using Privacy-ABCs. In this deliverable, we present 1 publication related to this task. In WP24, so far we have presented 2 publications.

Task 24.3: Privacy-friendly audit and data-handling mechanisms. Task 24.3 conducts research on data-handling mechanisms and on audits. Our research on audits can be found in previous WP24 deliverables. Data-handling mechanisms determine how user data is managed by the service provider. We focus our research on authentication methods, signatures and computations on signed data. In particular, we show how the service provider can perform computations on unencrypted signed data. We also describe a threshold password-authenticated secret sharing protocol. Additionally, we present an efficient

construction of round-optimal blind signature schemes in the standard model and we report on experiences during implementing blank digital signatures as well as optimizations that helped to improve their performance. Finally, we present design strategies for a privacy-friendly Austrian eID system in the public cloud. In this deliverable, we present 5 publications related to this task. In WP24, so far we have presented 20 publications.

Task 24.4: Development of privacy-friendly revocation mechanisms. We address the design of several privacy-friendly revocation mechanisms. First, we propose a privacy preserving revocation mechanism for privacy-enhancing attribute-based credentials that allows you to efficiently handle multiple revocation lists. Second, we study a primitive that is widely used for revocation purposes, i.e., cryptographic accumulators. Finally, we show how using epochs can help to make revocation practical while still retaining reasonable strong privacy guarantees. In this deliverable, we present 2 publications and 1 technical report related to this task. In WP24, so far we have presented 3 publications and 1 technical report.

Task 24.5: Development of methods for usable privacy. We have designed a two-factor user-authentication scheme for usable server-based eID and e-signature solutions. Current server-based eID and e-signature solutions typically rely on one-time passwords delivered to the user via short message service (SMS). This raises several issues in practice, as the use of SMS technology can be cost-effective insecure. To address these issues, we propose an alternative two-factor user-authentication scheme following a challenge-response approach. The feasibility and applicability of the proposed user-authentication scheme is evaluated by means of two concrete implementations. This way, we show that the proposed authentication scheme and its implementations improve both the cost effectiveness and the security of server-based eID and e-signature solutions. In this deliverable, we present 1 publication related to this task. In WP24, so far we have presented 5 publications and 1 poster.