Analysis of Trust Aspects

D43.1

Document Identification	
Date	10/12/2013
Status	Final
Version	1.1

Related SP/WP	SP4/WP43.1	**Document Reference**	D43.1
Related Deliverable(s)		**Dissemination Level**	CO
Lead Participant	KUL	**Lead Author**	Jessica Schroers (KUL)
Contributors	Jessica Schroers (KUL) Brendan Van Alsenoy (KUL) Niels Vandezande (KUL) Jos Dumortier (KUL) Harald Zwingelberg (ULD) Thomas Gross (UNEW) Christof Rath (TUG) Nuria Ituarte Aranda (ATOS Detlef Hühnlein (ECS) Tobias Wich (ECS)	**Reviewers**	Jens Kubieziel Maili Keskel

Abstract: This document gives an overview of the different notions of trust, an analysis of trust aspects in *FutureID*, and an overview of different mechanisms to enhance trust.

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

Trust is essential to the success of *FutureID*. This deliverable first examines the meaning of trust, since several different notions of trust exist. In the context of *FutureID* trust is understood in its operational sense. From this perspective, an entity can be said to trust a second entity when it makes the assumption that the second entity or system will behave exactly as it expects, or it is willing to assume the risk even though there is no certainty. Since trust stands in direct connection with expectation, this deliverable provides a high-level conceptualization of the various expectations held by the different entities that participate in *FutureID*. The remainder of this deliverable further elaborates on the following components of the *FutureID* trustframework:

(1) trust in identification, authentication and non-repudiation mechanisms;

(2) trust in the accuracy and integrity of data;

(3) trust in the reliability, availability and performance of the systems;

(4) trust in compliance with established policies.

The discussion of the first trust element starts with an overview of the main types of credentials which can be used for electronic identification, authentication and non-repudiation purposes. Afterwards two mapping frameworks, namely the STORK Quality of Authentication Assurance (QAA) model and the NIST Electronic Authentication Guideline are presented. These frameworks evaluate the identification and issuing procedures on one hand, and the remote authentication mechanisms on the other, to assess the level of assurance a certain identification token can provide.

With respect to trust in the accuracy and integrity of data, this deliverable emphasizes the importance of trust in identity attributes themselves. In order to realize this trust, the complete Identity Lifecycle along the ISO/IEC 29115 phases is considered. The Enrollment phase, Credential management phase and Entity authentication phase are analysed, so that the points where the level of trust can degrade or elevate can be identified.

For trust in reliability, availability and performance of *FutureID*, mainly two aspects are important: First the system will have to be trustworthy, and second this has to be proven to the trustor. For trust in availability and performance, the observation of system properties is important. Seeing as system engineering methods are not observable to most, service level agreements can provide guarantees. For trust in the system reliability, the use of reliable and secure components (as well as the composition of these components in a larger system) are important. There are multiple avenues for provable security and reliability guarantees in identity management systems. Security proofs can for example be given by cryptographic arguments or by the application of formal methods. Proving the usage of provable secure components to a trustor can for example be done by independent audits, or technically with trusted computing.

For trust in compliance with privacy regulations, including stated data protection and privacy policies, users generally expect compliance with the applicable legal regulations. These regulations require measures to promote transparency of processing and mechanisms to ensure consent is truly ‘informed’. In addition, data controllers must behave in accordance to their own privacy

policies. Consequently this requires that the users are able to understand the privacy policies and that relevant information is appropriately presented and not hidden within the policy. In order to improve user trust in the claims of the data controllers, privacy seals such as the European Privacy Seal (EuroPriSe) can be useful. This certification scheme not only uses the known IT-security goals (confidentiality, integrity and availability), but extends them with three privacy protection goals: unlinkability, transparency and intervenability.

An overview of the legal trust mechanisms is given by first showing the four legal risk (privacy-, authentication-, liability- and performance risk) and then giving an overview of the draft Regulation on electronic identification and trust services. Within this Regulation different trust mechanisms can be found, which can be useful for *FutureID*, in particular to respond to the legal risks and increase the trust of the parties.

Finally, by way of conclusion, an overview of the different trust aspects and mechanisms and a summary of the findings is given.