WP43 - Trust Services

D43.4 – Reference Implementation

Document Identification	
Date	October 31, 2014
Status	Final
Version	1.0a

Related SP/WP	SP4/WP43	**Document Reference**	D43.4
Related Deliverable(s)	D23.2, D33.3, D43.3	**Dissemination Level**	CO
Lead Participant	TUG	**Lead Author**	Christof Rath (TUG)
Contributors	Christof Rath (TUG) David Derler (TUG) Eray Özmü (USTUTT)	**Reviewers**	ULD IFAG

Abstract: This deliverable describes the reference implementation of the *FutureID* Trust Services.

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

This document describes the implementation work done in work package WP43. It covers the three parts delegated signature validation, TSL integration and trust status provisioning via DNSSEC.

Thereby, the trust status resolution is designed in a way that it can use the existing DNS infrastructure. The domain name in this case consists of the hash of a certificate and a pre-defined, meaningful base name, for example: `8b3f...2ff3.level-3.trusted.tsa.eu`. By combining multiple base domains to white- and black-lists, trust policies can be defined to act as distributed, yet user controlled, trust anchor repositories.

Some trust decisions, however, cannot be made based only on the hash of a certificate and a static base name. One example are time related decisions, like the status of a certificate at a certain point in time. Therefore, TSLs are supported along with the DNSSEC based trust status resolution. That is, the signature on the TSL itself can be verified using the trust anchors provided by the DNS approach. The TSL then provides additional input for the validation of electronic signatures.

The signature validation, in turn, is capable of verifying advanced electronic signatures (XAdES, PAdES, CAdES). It supports the validation of BES level signatures and, where the backend technology supports it, also LT and LTA level signatures. Furthermore, it is possible to extend a given signature to LT or LTA variants. The service is accessed via OASIS DSS signature validation requests.