THALES

www.thales-esecurity.com

Thales e-Security

Quick Start Guide on Standards for eIDAS Trust Service Providers Issuing Certificates and Supporting Remote Signing

Release: 1.2
Date: 7 November 2016
Author: Nick Pope

1. Introduction

This quick start guide for Trust Service Providers identifies the standards and other sources of information sources of mandated / recommended for TSPs issuing certificates and providing remote signing services.

This is not aimed at providing a precise definition of how to meet compliance requirements but provides guidance on available sources of information which may be towards achieving compliance. No liabilities are undertaken regarding the advice given in the document.

SHALL is used to indicate standards / sources mandated directly or by indirect assumptions implied through the regulation.

SHOULD is used to indicate standards / sources which are identified as current best practice for meeting eIDAS as they were developed specifically to support eIDAS.

2. Auditor Accreditation

A TSP is required to produce an audit report to demonstrate that it meets the requirements of the eIDAS regulation. The auditor SHALL be accredited as the appropriate competence under Regulation (EC) No 765/2008. This in practice means that the auditor is accredited as a "conformity assessment body" by one of the national accreditation bodies who are a member of the European Forum for Accreditation (see http://www.european-accreditation.org/ea-members). Most of the accreditation bodies list "conformity assessment bodies" which they have accredited and for what purposes.

The eIDAS accreditation SHOULD meet the requirements of ISO 17065[1] as specified in ETSI EN 319 403[2].

A group of accredited conformity assessment bodies for eIDAS have been established called the ACAB Council (see: http://www.acab-c.com/accredited-bodies/). However, this list is by no means complete (currently only lists LSTI and TuvIT) and a number of other audit bodies are known to be offering eIDAS audits across Europe although their accreditation status is unknown (this includes PWC in Belgium, KPMG in the Netherlands).

Note: Accreditation under Webtrust does not meet the eIDAS requirements. However, the international scheme for PKI services established under the CA Browser forum (see: https://cabforum.org/) recognised by Microsoft, Google and other major web application providers accepts audits made under the above EU scheme as an alternative to Webtrust.

3. TSP Requirements

The regulation does not identify any specific standards which may be used to demonstrate conformance to the regulation. However, it is considered that conformance to recognised best practice standards SHOULD be used to demonstrate conformance.

Trust service providers issuing certificates or providing time-stamping services SHOULD conform to the standards identified at: https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx. It is recommended that the HSMs employed are recognised as QSCD under the regulation or conform to CEN EN 419 221-5.

[1] ISO and CEN standards can be obtained through your national standards body

[2] ETSI standards are available for free download at: http://www.etsi.org/standards-search

Note: the recommended general standard for TSPs issuing certificates ETSI EN 319 411-1 builds on the requirements of the CA Browser Forum and it is recognised as a means of demonstrating compliance the CAB Forum Baseline and EV requirements.

Currently, generally accepted standards for remote signing are still under development and not expected to be supported by products for more than a year. However, general security requirements for remote signing are specified in CEN TS 419 241 and products based on this standard SHOULD be adopted by TSPs for remote signing. In addition, the general standard for TSP operations (ETSI EN 319 401) SHOULD also be applied to the remote signing elements of the TSP.

4. Further Information

Further information on eIDAS is provided in the Thales white paper: "The impact of the European eIDAS Regulation, understanding the new requirements and the need for hardware security modules".

Nick Pope, Principal Consultant, Thales, nick.pope@thales-esecurity.com

Nick has been involved with standards relating to Regulations and Directives since 1999. He is vice-chairman of ETSI ESI, a group concerned with eIDAS standards for electronic signature and trust infrastructures. He has edited a number of ETSI specifications on signature formats and trust service policies. Within CEN TC 224 WG17, he is the ETSI liaison representative and UK principle expert, as well as attending on behalf of Thales.

THALES

www.thales-esecurity.com

About Thales e-Security

Thales e-Security is a leading global provider of data encryption and cyber security solutions to the financial services, high technology manufacturing, government and technology sectors. With a 40-year track record of protecting corporate and government information, Thales solutions are used by four of the five largest energy and aerospace companies, 22 NATO countries, and they secure more than 80 percent of worldwide payment transactions. Thales e-Security has offices in Australia, France, Hong Kong, Norway, United Kingdom and United States. For more information, visit www.thales-esecurity.com

Follow us on:

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Unit 4101 41/F 248, Queen's Road East, Wanchai, Hong Kong, PRC • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com