eIDAS compliant Trust Services with Utimaco HSMs

March 15, 2018

Dieter Bong
Product Manager

utimaco®

eIDAS compliant Trust Services with Utimaco HSMs

Agenda

- eIDAS and Trust Services
- Policy and Security Requirements for Trust Service Providers
- Trust Services with Utimaco HSMs

What is eIDAS?

- Regulation No 910/2014 of the European Parliament and of the Council on “electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC”

- Published July 23rd 2014
  - Adoption of implementing acts and delegated acts by July 1st 2016
  - Replaces national signature laws on July 1st 2016

- eIDAS aims at
  - Increasing the use of electronic IDs and electronic signatures
  - Fostering cross-border electronic transactions
  - Strengthening the European market

Trust Services

Trust Services Use Cases

- [Qualified] Electronic Signature
  - Signing a contract, an official document (e.g. land record), a commercial proposal, etc.
- [Qualified] Electronic Seal
  - Sealing official documents (e.g. tax bill, electronic drivers license, University diploma)
- [Qualified] Time Stamp
  - Establishing the time of contract signing, attestation issuance, etc.
  - Long-term validity and preservation of electronic records
- Some use cases have legal background, more will follow
  - Even w/o specific regulation, the legal assumption of authenticity and integrity of a document / transaction with a qualified signature / qualified seal may foster adoption

Policy and Security Requirements

Policy and Security Requirements Overview

Standards	Title
ETSI EN 319 401	General Policy Requirements for Trust Service Providers
ETSI EN 319 411	Policy and security requirements for Trust Service Providers issuing certificates Part 1 – General requirements Part 2 – Requirements for Trust Service Providers issuing EU qualified certificates
ETSI EN 319 421	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

Drafts	Title
ETSI TS 119 441	Policy requirements for TSP providing signature validation services
ETSI TS 119 495	Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive 2015/2366/EU

- See https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

Trust Services Use Cases – PSD2

- Draft ETSI TS 119 495 ”Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive 2015/2366/EU”
  - Introduction
    - *The RTS [Regulatory Technical Specification] defines requirements on the use of qualified certificates (as defined in eIDAS) for website authentication and qualified certificates for electronic seal for communication among payment and bank account information institutions.*
  - Scope
    - *Certificates for electronic seals can be used for providing evidence with legal assumption of authenticity (including identification and authentication of the source) and integrity of a transaction.*
    - *Certificates for website authentication can be used for identification and authentication of the communicating parties and securing communications.*
  - 4.1 Use of Qualified Certificates
    - *The electronic seal provides strong evidence, capable of having legal effect, that given data is originated by the legal entity identified in the certificate.*

- ETSI workshop „eIDAS meets PSD2”
  - http://www.etsi.org/news-events/events/1266-eidasmeetspsd2

Policy and Security Requirements

Selected Requirements – Segregation of Duties & Access Control

- EN 319 401 General Policy Requirements for TSPs
  - 7.1.2 Segregation of duties
    - *Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the TSP assets.*
  - 7.4 Access control
    - *b) The TSP shall administer user access of operators, administrators and system auditors. The administration shall include user account management and timely modification or removal of access.*
    - *c) … separation of security administration and operation functions.*

- ➔ Utimaco HSMs support distinct roles for security administration, i.e. HSM administration, user account management, key management and key usage/operation functions

Policy and Security Requirements

Selected Requirements – Dual Control

- EN 319 411 Policy and security Requirements for TSPs issuing certificates
  - 6.5.1 Key pair generation and installation
    - *a) CA key pair generation … shall be undertaken … under, at least, dual control.*
  - 6.5.4 Activation data
    - *a) The installation and recovery of the CA's key pairs in a secure cryptographic device shall require simultaneous control of at least two trusted employees.*
- EN 319 421 Policy and security Requirements for TSPs issuing Time-Stamps
  - 7.6.2 TSU key generation
    - *a) The generation of the TSU's signing key(s) shall be undertaken … under, at least, dual control.*
  - 7.6.3 TSU private key protection
    - *b) If TSU private keys are backed up, they shall be copied, stored and recovered only by personnel in trusted roles using, at least, dual control …*

- ➔ Utimaco HSMs support at least dual control for security critical operations
  - 4-eyes-principle
  - m-of-n quorum with m greater or equal 2

Policy and Security Requirements

Selected Requirements – Certification

- EN 319 411-1 Policy and security requirements for TSPs issuing certificates
  - 6.3.5 Key pair and certificate usage
- EN 319 421 Policy and security Requirements for TSPs issuing Time-Stamps
  - 7.6.2 TSU key generation

  - *CA key pair generation / The generation of the TSU's signing key(s) shall be carried out within a secure cryptographic device which:*
    - *i) is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [1], or equivalent national or internationally recognized evaluation criteria for IT security. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures; or*
    - *NOTE 1: Standards specifying common criteria protection profiles for TSP cryptographic modules, in accordance with ISO/IEC 15408 [1], are currently under development within CEN as CEN TS 419 221-2 [i.16], CEN TS 419 221-3 [i.17], CEN TS 419 221-4 [i.18], or CEN EN 419 221-5 [i.19].*
    - *ii) meets the requirements identified in ISO/IEC 19790 [2] or FIPS PUB 140-2 [6], level 3.*
    - *The secure cryptographic device should be as per i).*
  - *The CA / TSU private signing key shall be held and used within a secure cryptographic device as indicated … above.*

Policy and Security Requirements

Selected Requirements – Certification

- *ii) … meets the requirements identified in ISO/IEC 19790 [2] or FIPS PUB 140-2 [6], level 3*
  - ➔ CryptoServer Se-Series Gen2
  - ➔ CryptoServer CSe-Series
  - Each w/ FIPS-validated firmware package

- *The secure cryptographic device should be as per i)*
  - CC EAL4 (or higher) certification
  - ➔ CryptoServer CP5

CryptoServer CP5

Target of Evaluation – Hardware

- CryptoServer Se-Series Gen2
  - Cryptographic boundary = „Everything underneath the heat sink“
- Delivered as
  - Standalone PCIe card
  - Integrated into CryptoServer LAN
- All performance grades
  - Models Se12, Se52, Se500 and Se1500

Target of Evaluation – Administration

- Administration functions
  - User account management
  - Audit log
  - Firmware update
  - Remote management

- Access control mechanisms
  - Username – password
  - Keyfile
  - Smartcard
  - 4-eyes principle
  - M-of-n quorum

- Attention: Some functions require dual control
  - E.g. firmware update

Target of Evaluation – Cryptographic Algorithm Requirements

- EN 319 411-1 Policy and security requirements for TSPs issuing certificates
  - 6.3.5 Key pair and certificate usage
    - *i. subject keys should be generated using an algorithm as specified in ETSI TS 119 312*
    - *ii. a key length and algorithm should be as specified in ETSI TS 119 312 [i.10] for the uses of the certified key …*
  - 6.5.1 Key pair generation and installation
    - *b) CA key pair generation should be performed using an algorithm as specified in ETSI TS 119 312 [i.10] for the CA's signing purposes.*
    - *c) The selected key length and algorithm for CA signing key should be one which is specified in ETSI TS 119 312 [i.10] for the CA's signing purposes.*
- EN 319 421 Policy and security Requirements for TSPs issuing Time-Stamps
  - 7.6.2 TSU key generation
    - *c) The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time-stamps key should be as specified in ETSI TS 119 312 [i.7].*

Target of Evaluation – Cryptographic Algorithm Requirements

- ETSI TS 119 312 Cryptographic Suites
  - Based on the agreed cryptographic mechanisms of the SOG-IS Crypto Evaluation Scheme

- Hash functions
  - SHA2: SHA-224, SHA-256, SHA-384, SHA-512, SHA512/256
  - SHA3: SHA3-256, SHA3-384, SHA3-512

- Signature schemes
  - RSA-PKCS#1v1_5, RSA-PSS
    - Recommended key size: >= 1900 bit
  - DSA (FF-DLOG DSA)
  - EC-DSA (EC-DLOG EC-DSA)
    - NIST P-256, P-384, P-521
    - Brainpool P256r1, P384r1, P512r1
    - FRP256v1
  - EC-SDSA-opt (EC-DLOG EC-Schnorr)

Target of Evaluation – Cryptographic Algorithm Support

- ETSI TS 119 312 Cryptographic Suites
  - Based on the agreed cryptographic mechanisms of the SOG-IS Crypto Evaluation Scheme

- Hash functions
  - SHA2: SHA-224, SHA-256, SHA-384, SHA-512, SHA512/256
  - SHA3: SHA3-256, SHA3-384, SHA3-512 + SHA3-224

- Signature schemes
  - RSA-PKCS#1v1_5, RSA-PSS
    - Recommended key size: >= 1900 bit
  - DSA (FF-DLOG DSA)
  - EC-DSA (EC-DLOG EC-DSA)
    - NIST P-256, P-384, P-521
    - Brainpool P256r1, P384r1, P512r1
    - FRP256v1
  - EC-SDSA-opt (EC-DLOG EC-Schnorr)

Target of Evaluation – Cryptographic Algorithm Support

- ETSI TS 119 312 Cryptographic Suites
  - Based on the agreed cryptographic mechanisms of the SOG-IS Crypto Evaluation Scheme

- Hash functions
  - SHA2: SHA-224, SHA-256, SHA-384, SHA-512, SHA512/256
  - SHA3: SHA3-256, SHA3-384, SHA3-512 + SHA3-224

- Signature schemes
  - RSA-PKCS#1v1_5, RSA-PSS
    - Recommended key size: >= 1900 bit key sizes >= 2048 bit
  - DSA (FF-DLOG DSA)
  - EC-DSA (EC-DLOG EC-DSA)
    - NIST P-256, P-384, P-521 + P-224
    - Brainpool P256r1, P384r1, P512r1 + P224r1, P320r1, P224t1, P256t1, P320t1, P384t1, P512t1
    - FRP256v1
  - EC-SDSA-opt (EC-DLOG EC-Schnorr)

Target of Evaluation – Cryptographic Algorithm Support in addition to ETSI TS 119 312

- Data encryption & decryption
  - AES CBC / OFB / CTR
  - AES GCM / CCM
  - RSAES-OAEP / RSAES-PKCS1-v1_5
- Message Authentication Code
  - AES CMAC / GMAC
  - HMAC
- ECDH Key Derivation
- Random number generation
  - Class DRG.4 per [AIS 20/31], seeded by PTRNG of class PTG.2

Target of Evaluation – Firmware and Software

- Firmware
  - Bootloader and firmware running inside the cryptographic boundary
    - SMOS, ADM, CXI, VRSA, AES, …
  - w/ limitations as mandated by CC and EN419221-5

- Software
  - Supporting software running outside the cryptographic boundary
  - Administration tool „csadm“
  - Cryptographic API „CXI API C/C++“
    - w/ PKCS#11 Provider etc. on top
  - Key management tool „cxitool“

Target of Evaluation – Key Authorization

- EN 419221-5 Cryptographic Module for Trust Services, TOE Overview
  - "Authorisation as a user of a secret key is always separately required before a key can be used in a cryptographic function …"
  - "Re-authorisation conditions such as determining a time period or number of uses of a key …"

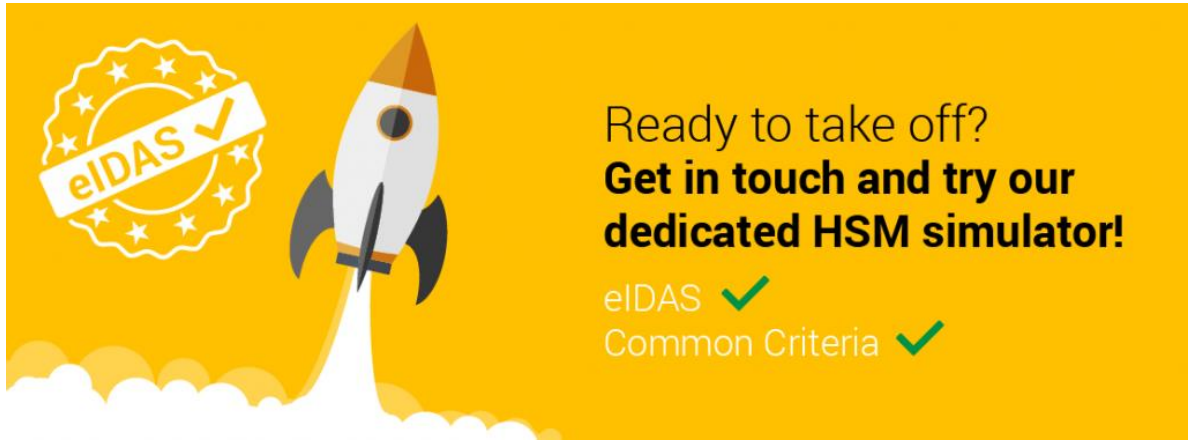
- Key authorization support
  - „kaapi" as extension to CXI API
  - Key authorization commands in cxitool

CryptoServer CP5

Status and Next Steps

- CC evaluation in progress
  - Certification expected around end Q2 / early Q3

- CryptoServer CP5 simulator available



- Integration Guides w/ leading PKI applications
  - Microsoft ADCS, PrimeKey EJBCA, Nexus Certificate Manager, etc.

eIDAS compliant Trust Services with Utimaco HSMs

Summary

- Utimaco HSMs …
  - Support policy and security requirements that Trust Service Provider must implement
  - Fulfil certification requirements
    - Today: SecurityServer package ➔ FIPS 140-2 Level 3 validated
    - Soon: CryptoServer CP5 package ➔ Common Criteria EAL4+ certified acc. EN 419221-5
  - Can be tested and evaluated using our free simulators

Thanks for your attention

Dieter Bong

Product Manager

dieter.bong@utimaco.com

Utimaco IS GmbH

Germanusstraße 4
52080 Aachen
Germany
Tel +49 241 1696 200
Fax +49 241 1696 199
Email hsm@utimaco.com

Utimaco Inc.

Suite 150
910 E Hamilton Ave
Campbell, CA 95008
United States of America
Tel +1 844 884 6226
Email hsm@utimaco.com