



Utimaco eIDAS Update

June 2017

Thorsten Groetker
CTO

utimaco[®]

Agenda

- Recap – eIDAS, Trust Services, Standardization
- Signature Creation
- Time Stamping
- Outlook

Agenda

- **Recap – eIDAS, Trust Services, Standardization**
- Signature Creation
- Time Stamping
- Outlook

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

- Signature creation
- Seal creation
- Time stamping
- Electronic registered delivery service
- Website authentication

E
l
e
c
t
r
o
n
i
c

S
i
g
n
a
t
u
r
e



EU's trust mark for
qualified trust services

Electronic Signature vs. Electronic Seal

■ Electronic signatures

- „which is used by the signatory to sign”
- “A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.”
 - Intent / consent of the signatory
- Created by a natural person
- “Created using electronic signature creation data that the signatory can ... use under his sole control”

■ Electronic seals

- „to ensure the latter’s [data] origin and integrity”
- “Electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document’s origin and integrity.”
- Created by a legal person
 - A natural person may sign on behalf of a legal person
- “Created using electronic seal creation data that the creator of the seal can ... under its control, use for electronic seal creation”
 - Several natural persons may create seals

Standardization

- Need to translate legal requirements into technical specifications, e.g.
 - “... ensure that at least a number of advanced electronic signature formats can be technically supported ...”
 - “... providers should apply specific management and administrative security procedures and use trustworthy systems and products ...”
- Standardization mandate M/460
 - European Committee for Standardization (CEN) - Technical Committee 224 (TC 224)
 - Security Requirements, Common Criteria Protection Profiles
 - European Telecommunications Standards Institute (ETSI) – Technical Committee on Electronic Signatures and Infrastructures (TC ESI)
 - Policy Requirements, Technical Standards
 - See <https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx>

Agenda

- Recap – eIDAS, Trust Services, Standardization
- **Signature Creation**
- Time Stamping
- Outlook

QSCD – Qualified Signature Creation Devices

- Protection Profiles
 - EN 419211-x Protection profiles for secure signature creation device (SSCD)
 - Target devices: smartcards
 - EN 419221-x Protection Profiles for TSP cryptographic modules
 - Target devices: Hardware Security Modules (HSM)

- Procedure to follow: CC evaluation, then notification

- Compilation of Member States notification on SSCDs and QSCDs
 - <https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds>
 - Designated Bodies under Article 30(2) and 39(2) of Regulation 910/2014
 - Certified Qualified Signature Creation Devices under Article 31(1)-(2) and Certified Qualified Seal Creation Devices under Article 39(3) of Regulation 910/2014,
 - Secure Signature Creation Devices benefiting from the transitional measure set in article 51(1) of Regulation 910/2014

EN 419221-x Protection Profiles for TSP cryptographic modules

- EN 419221-2 Cryptographic module for CSP signing operations with backup
 - Update to former Protection Profile CWA 14167-2:2004 “CMCSOB-PP”

- EN 419221-4 Cryptographic module for CSP signing operations without backup
 - Update to former Protection Profile CWA 14167-4:2004 “CMCSO-PP”

- prEN 419221-5 Cryptographic Module for Trust Services
 - New Protection Profile
 - Version 0.15 certified
 - http://www.commoncriteriaportal.org/files/ppfiles/ANSSI-CC-PP-2016_05%20PP.pdf
 - Version 1.0
 - Integrates comments from CEN enquiry
 - Process for publication as official EN document started
 - Maintenance re-certification immediately after EN publication

prEN 419221-5 Cryptographic Module for Trust Services

- CC conformance claim
 - EAL4+
 - Augmentation results from AVA_VAN.5 Advanced methodical vulnerability analysis

- Scope
 - “... suitable for use by trust service providers supporting electronic signature and electronic sealing operations, certificate issuance and revocation, time stamp operations, and authentication services ...”

- PP Overview
 - “... generates and/or protects secret keys and other sensitive data, and allows controlled use of these data for one or more cryptographic services in support of TSP trust services ...”

prEN 419221-5 Cryptographic Module for Trust Services (cntd.)

- 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 ...”

- Usage and major security features of the TOE
 - “The threat environment the TOE is designed for is one of high threat of network compromise, and low threat of physical compromise ...”
 - ➔ Reduced requirements for side channel resistance and tamper protection

- Security Management
 - “... two separate types of keys are defined: Assigned Keys ... and general keys ...”
 - Assigned keys support sole control
 - No import, no export
 - Administrator cannot change authorization data, or set new authorization data when unblocking key

How Utimaco HSMs support prEN 419221-5

- CryptoServer Se-Series Gen2 evaluation acc. prEN 419221-5 in progress
- Target of evaluation
 - PCIe plug-in card, w/ and w/o hardware crypto accelerator
 - May be operated in CryptoServer LAN
 - All performance grades covered by certification
 - CXI interface adapted to PP requirements
 - Supports PKCS#11, JCE, etc. with limitations
- Certification expected by end of Q1 CY2018

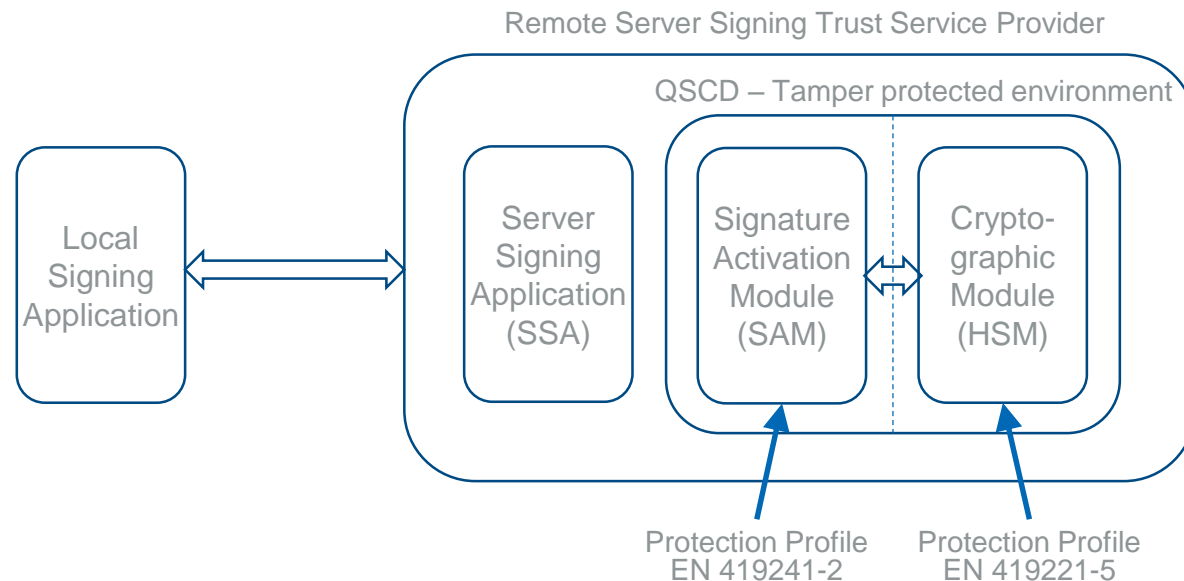
Main Features in a Nutshell

- PCIe card w/ and w/o crypto accelerator
 - 4 different performance levels
 - 16 RSA2048 sig/s .. 3200 RSA2048 bulk sig/s (via PKCS#11)
 - Preliminary benchmark results on request
 - Can be operated in CSLAN appliance
- Internal key storage
 - Extensible: per-key backup/restore supported
- General purpose host APIs (with limitations as mandated by PP)
 - CXI
 - PKCS#11
 - (JCE)
- Host APIs for assigned keys (initialization, authorization, unblocking)
 - C, Java, byte buffer
 - Initialize existing keys (imported or generated via host APIs)
 - Keys referenced via handle (based on group/name/specifier)

Disclaimer:
Features presented based on
current plans. Check final datasheet
for validated information.

Main Features in a Nutshell (cont'd)

- Full-featured Utimaco tool support
 - Administration tools: csadm, CAT
 - PKCS#11: p11tool2, P11CAT
 - General purpose command line tool (key mgmt. + cryptography): cxitool
 - HSM simulator
- Supports Remote Server Signing acc. EN 419 241



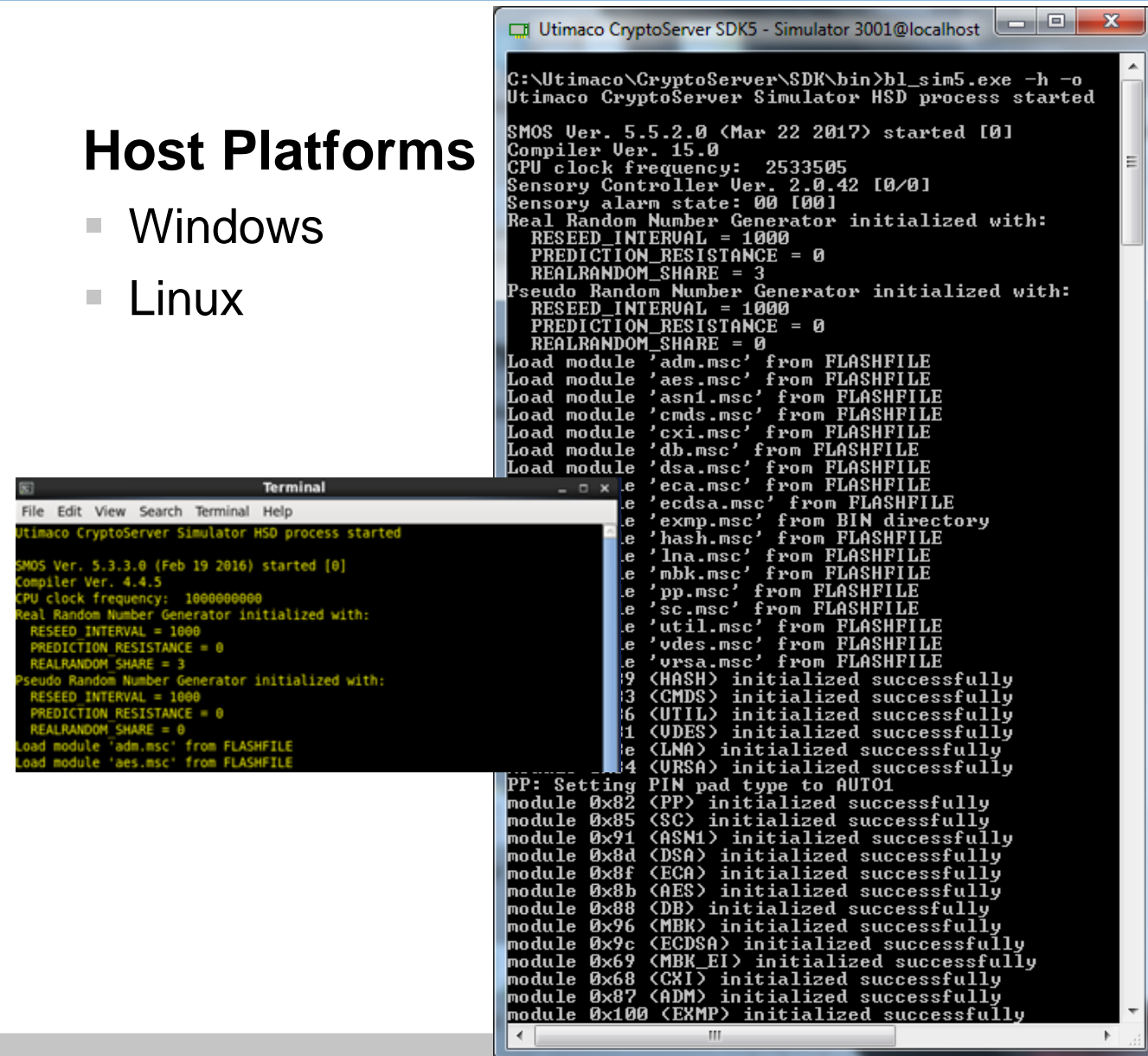
Disclaimer:
Features presented based on
current plans. Check final datasheet
for validated information.

Proven Features

- Fully-functional simulation model
 - Cryptography
 - Administration
 - Integrations
 - ... everything
- Also part of the SDK package
 - Your code running on the HSM
 - Develop, run, and debug code on the simulator

Host Platforms

- Windows
- Linux

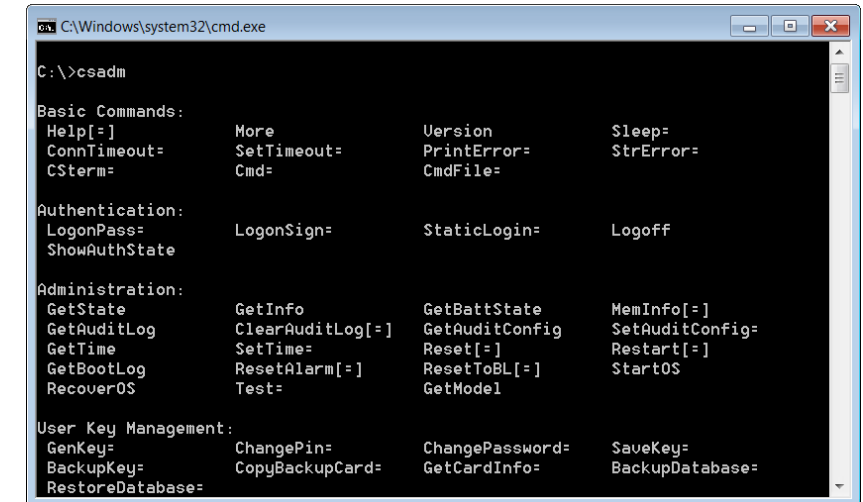
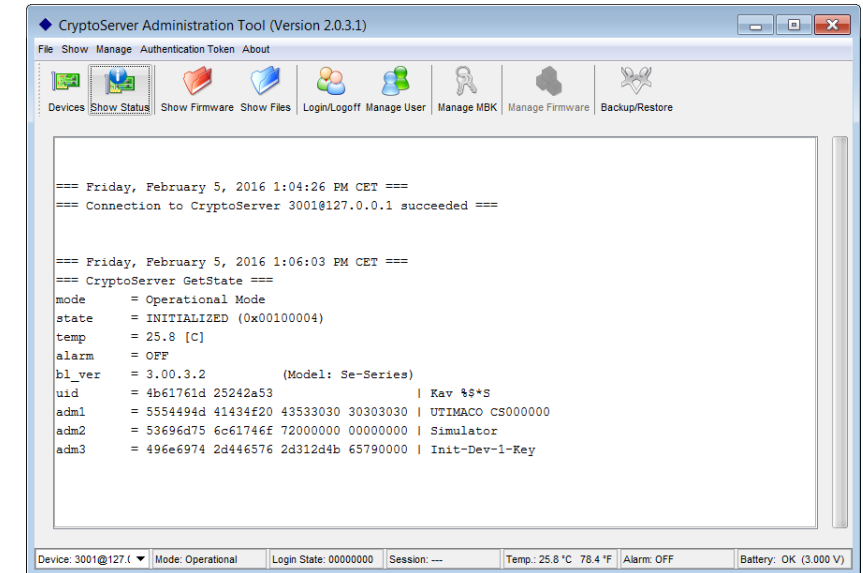
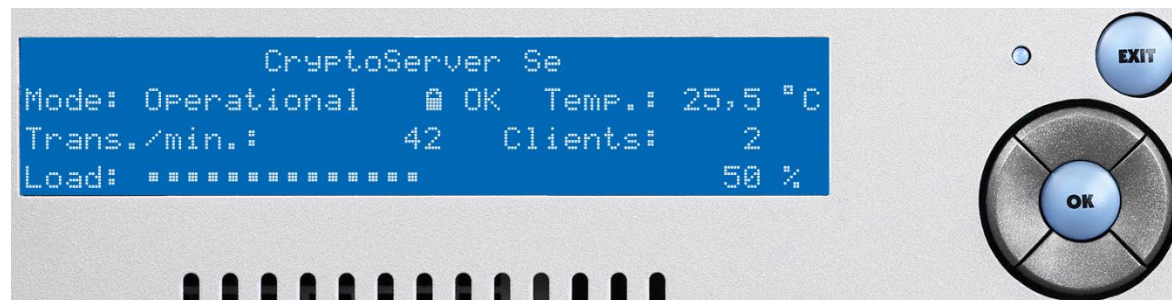


```
C:\Utimaco\CryptoServer\SDK\bin>hl_sim5.exe -h -o
Utimaco CryptoServer Simulator HSD process started

SMOS Ver. 5.5.2.0 <Mar 22 2017> started [0]
Compiler Ver. 15.0
CPU clock frequency: 2533505
Sensory Controller Ver. 2.0.42 [0/0]
Sensory alarm state: 00 [00]
Real Random Number Generator initialized with:
  RESEED_INTERVAL = 1000
  PREDICTION_RESISTANCE = 0
  REALRANDOM_SHARE = 3
Pseudo Random Number Generator initialized with:
  RESEED_INTERVAL = 1000
  PREDICTION_RESISTANCE = 0
  REALRANDOM_SHARE = 0
Load module 'adm.msc' from FLASHFILE
Load module 'aes.msc' from FLASHFILE
Load module 'asn1.msc' from FLASHFILE
Load module 'cmds.msc' from FLASHFILE
Load module 'cxi.msc' from FLASHFILE
Load module 'db.msc' from FLASHFILE
Load module 'dsa.msc' from FLASHFILE
Load module 'eca.msc' from FLASHFILE
Load module 'ecdsa.msc' from FLASHFILE
Load module 'exmp.msc' from BIN directory
Load module 'hash.msc' from FLASHFILE
Load module 'lna.msc' from FLASHFILE
Load module 'mbk.msc' from FLASHFILE
Load module 'pp.msc' from FLASHFILE
Load module 'sc.msc' from FLASHFILE
Load module 'util.msc' from FLASHFILE
Load module 'vdes.msc' from FLASHFILE
Load module 'ursa.msc' from FLASHFILE
[9] (HASH) initialized successfully
[3] (CMDS) initialized successfully
[6] (UTIL) initialized successfully
[1] (VDES) initialized successfully
[0] (LNA) initialized successfully
[4] (URSA) initialized successfully
PP: Setting PIN pad type to AUTO1
module 0x82 (PP) initialized successfully
module 0x85 (SC) initialized successfully
module 0x91 (ASN1) initialized successfully
module 0x8d (DSA) initialized successfully
module 0x8f (ECA) initialized successfully
module 0x8b (AES) initialized successfully
module 0x88 (DB) initialized successfully
module 0x96 (MBK) initialized successfully
module 0x9c (ECDSA) initialized successfully
module 0x69 (MBK_EI) initialized successfully
module 0x68 (CXI) initialized successfully
module 0x87 (ADM) initialized successfully
module 0x100 (EXMP) initialized successfully
```

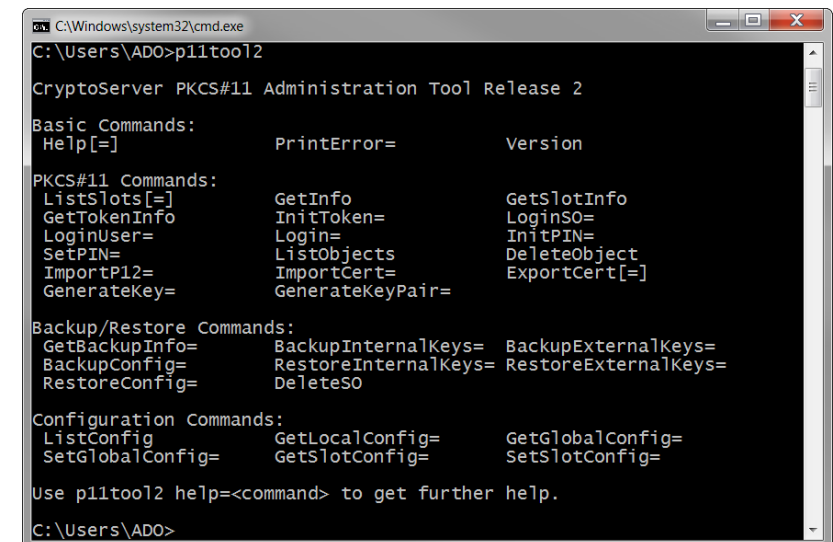
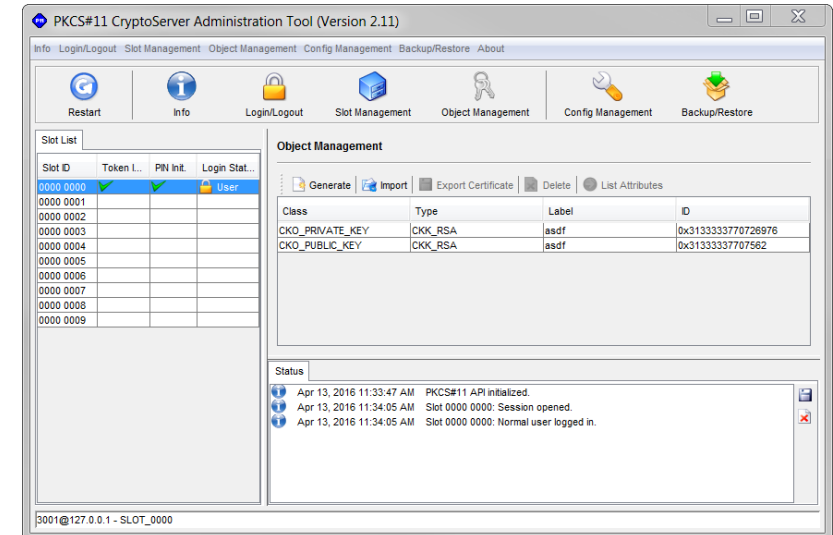

Overview

- Three administrative tools available
 - Command line tool csadm
 - GUI tool
CryptoServer Administration Tool (CAT)
 - Administration via front panel
(only for CryptoServer LAN)



Admin tools

- GUI tool (Java based):
PKCS#11 CryptoServer Administration Tool (P11CAT)
- CLI tool:
p11tool2
 - For 32-bit and 64-bit
 - For Windows and for Linux (no AIX tools)
- Note: Non-standard functionality requires usage of the general admin tools (CAT/csadm), for example
 - Unconventional user naming
 - Two-person-rule
 - Key manager role



Features

■ Functional

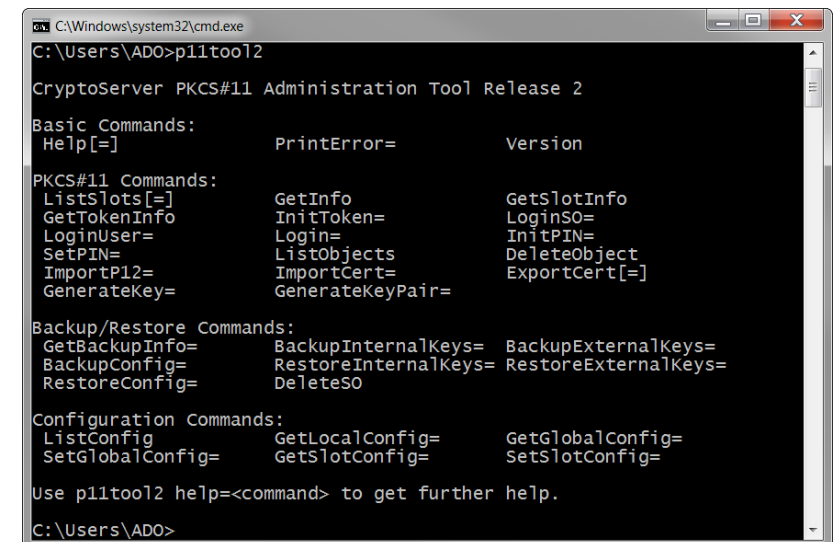
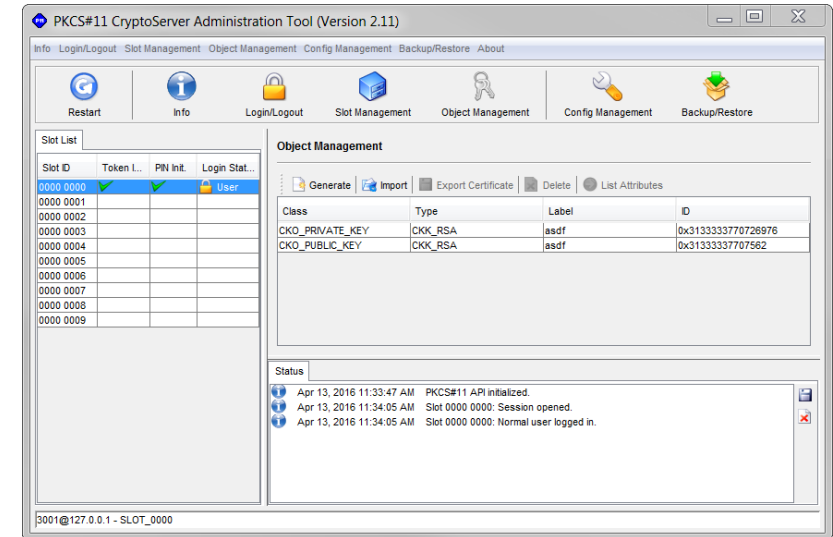
- Configurable number of PKCS#11 slots per CryptoServer
- Clustering
 - Connection-based load balancing (Least Connections)
 - Failover
- Up to 4096 parallel sessions per CryptoServer

■ Security

- Secure channel between application and CryptoServer
- Multiple authentication mechanisms supported
- Configurable m out of n authentication
- Segregation of key management and usage rights
- Interface hardening
- Failed login counter
- Thread-safe for use in multithreaded applications

Admin tools

- GUI tool (Java based):
PKCS#11 CryptoServer Administration Tool (P11CAT)
- CLI tool:
p11tool2
 - For 32-bit and 64-bit
 - For Windows and for Linux
- Note: Non-standard functionality requires usage of the general admin tools (CAT/csadm), for example
 - Unconventional user naming
 - Two-person-rule
 - Key manager role



(Remote) Server Signing

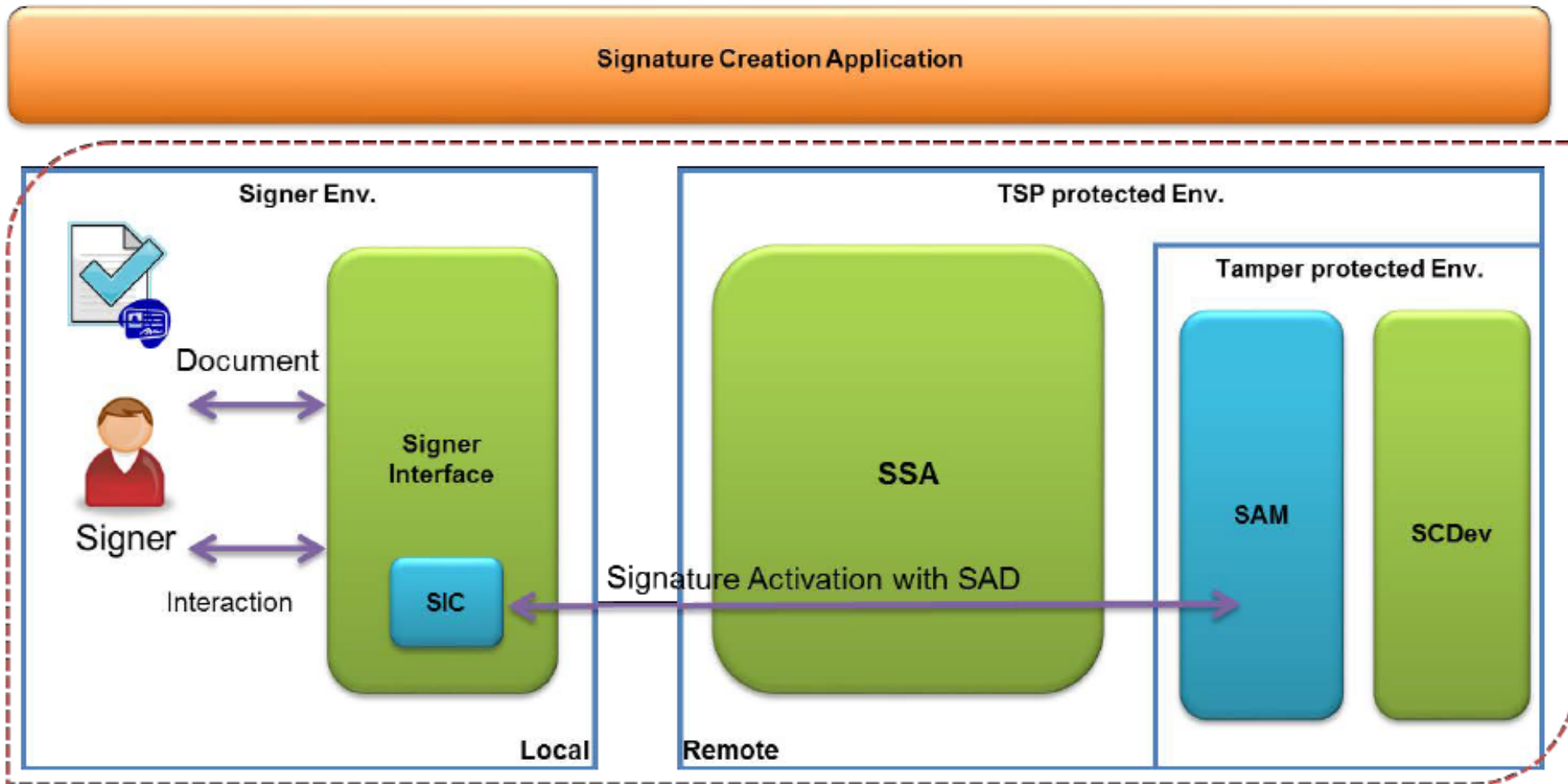
- eIDAS motivation (51):

“It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data, and the qualified electronic signature requirements are met by the use of the device.”

 - Similar handling for electronic seals

- EN 419241 Trustworthy Systems Supporting Server Signing
 - Part 1: General System Security Requirements
 - CEN enquiry in progress, results expected until June 22
 - Part 2: Protection Profile for QSCD for Server Signing
 - CEN enquiry in progress, results expected until August 3
 - Common Criteria evaluation pending, results expected until June 30

EN 419241 Trustworthy Systems Supporting Server Signing



prEN 419241-2 QSCD for Server Signing

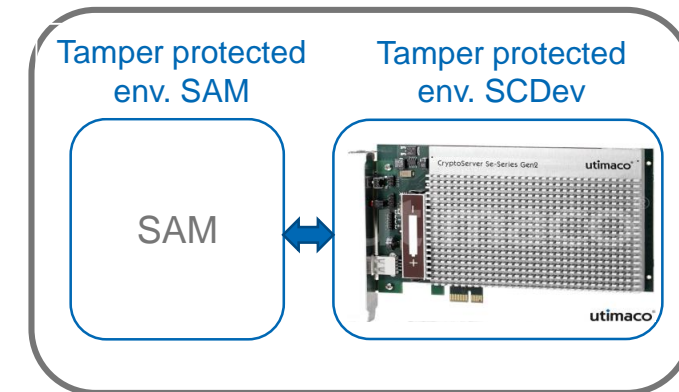
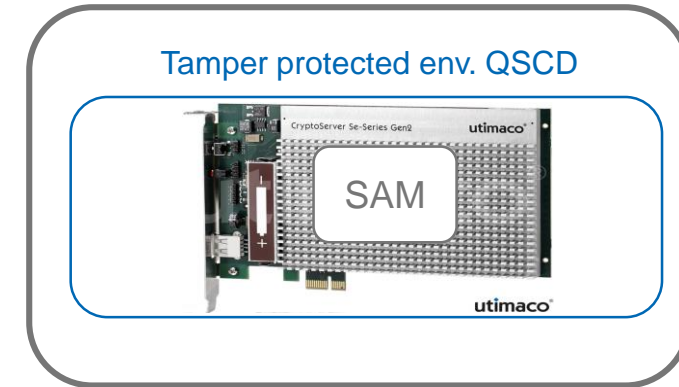
- CC conformance claim
 - EAL4+
 - Augmentation results from AVA_VAN.5 Advanced methodical vulnerability analysis

- Scope
 - "... specifies a protection profile for a Signature Activation Module (SAM), which is aimed to meet the requirements of a QSCD ..."

- TOE Overview
 - "To ensure the signer has sole control of his signing keys, the signature operation needs to be authorised. This is carried out by a Signature Activation Module (SAM), which can handle one endpoint of SAP, verify SAD and activate the signing key within a Cryptographic Module. Both the Cryptographic Module and the SAM are to be located within a tamper protected environment. "

prEN 419241-2 Tamper Protected Environment

- Common tamper protected environment
 - SAM runs within the tamper protected environment provided by the cryptographic module
 - + Use tamper protected environment of crypto module
 - - Strong dependence on crypto module implementation and certification
- Separate tamper protected environments
 - SAM runs within its own tamper protected environment
 - + Crypto module can be used as certified, also for other trust services than server signing
 - - Tamper protection must be covered during certification of SAM



How Utimaco HSMs support EN 419241

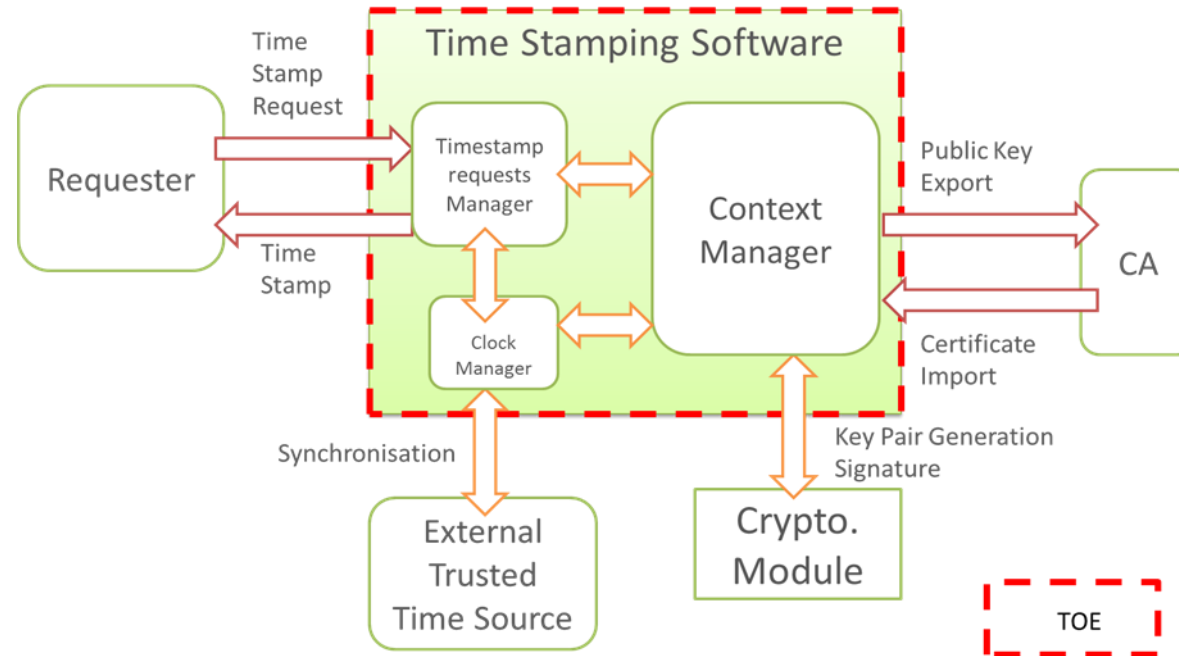
- CryptoServer Se-Series Gen2 evaluation acc. prEN 419221-5 in progress
 - Basis for server signing systems acc. EN 419241

- Utimaco supports manufacturer / integrator of server signing system
 - Common tamper protected environment
 - CryptoServer SDK for firmware development
 - Advice for certification of SAM
 - Separate tamper protected environments
 - Advice for tamper protected SAM environment
 - Integration support for CryptoServer Se-Series Gen2 and CXI interface
 - No plans to develop and certify a Utimaco server signing solution

Agenda

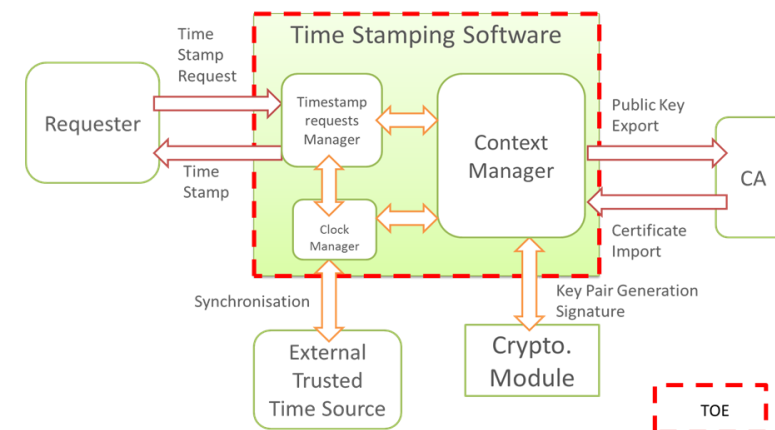
- Recap – eIDAS, Trust Services, Standardization
- Signature Creation
- **Time Stamping**
- Outlook

- prEN 419231 Protection Profile for trustworthy systems supporting time stamping

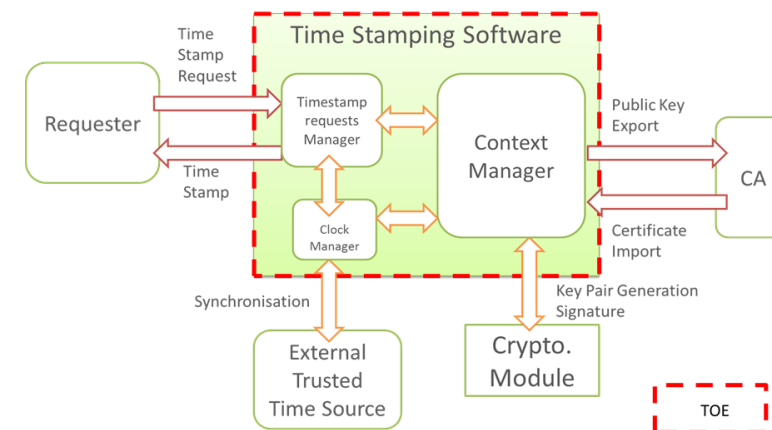


- Status
 - CC evaluation in progress, results expected until June 30
 - CEN enquiry in progress, results expected until June 22
 - Consolidation in version 1.0 for official publication

- The cryptographic module ... is a certified device that meets:
 - the requirements of [EN319421] §7.5.2 or [ETSI102023] §7.2.2 or equivalent
 - or the following:
 - meets the requirements identified in ISO/IEC 19790, level 3 or higher;
NOTE : Demonstrated conformance to FIPS PUB 140-2, level 3 is considered as fulfilment of this requirement.
 - meets the requirements identified in [CEN TS 419 221-2] or [CEN TS 419 221-4] or [CEN TS 419 221-5];
or
 - is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408, or equivalent security criteria. 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.



- The cryptographic module ... is a **certified device** that meets:
 - the requirements of [EN319421] §7.5.2 or [ETSI102023] §7.2.2 or equivalent
 - or the following:
 - meets the requirements identified in ISO/IEC 19790, level 3 or higher;
NOTE : Demonstrated conformance to **FIPS PUB 140-2, level 3** is considered as fulfilment of this requirement.
 - meets the requirements identified in [CEN TS 419 221-2] or [CEN TS 419 221-4] or [**CEN TS 419 221-5**];
or
 - is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408, or equivalent security criteria. 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.



How Utimaco HSMs support prEN 419231

- “... is a certified device that meets ...”
 - FIPS PUB 140-2, level 3
 - CryptoServer Se-Series, Se-Series Gen2 and CryptoServer CSe-Series
 - CEN TS 419 221-5
 - CryptoServer Se-Series Gen2 in progress

- CryptoServer Se-Series Gen2 advantages
 - Support for multi-tenancy and multiple keys per tenant
 - A single HSM supports multiple time stamp server
 - Same HSM can be used for time stamping, certificate services, server signing, etc.
 - Simplified system setup for TSPs providing time stamping and signature creation services
 - Broad portfolio
 - From low performance entry-level to high-performance w/ embedded crypto accelerator

- CryptoServer Se50 deployed by German qualified time stamp service provider

Agenda

- Recap – eIDAS, Trust Services, Standardization
- Signature Creation
- Time Stamping
- Outlook

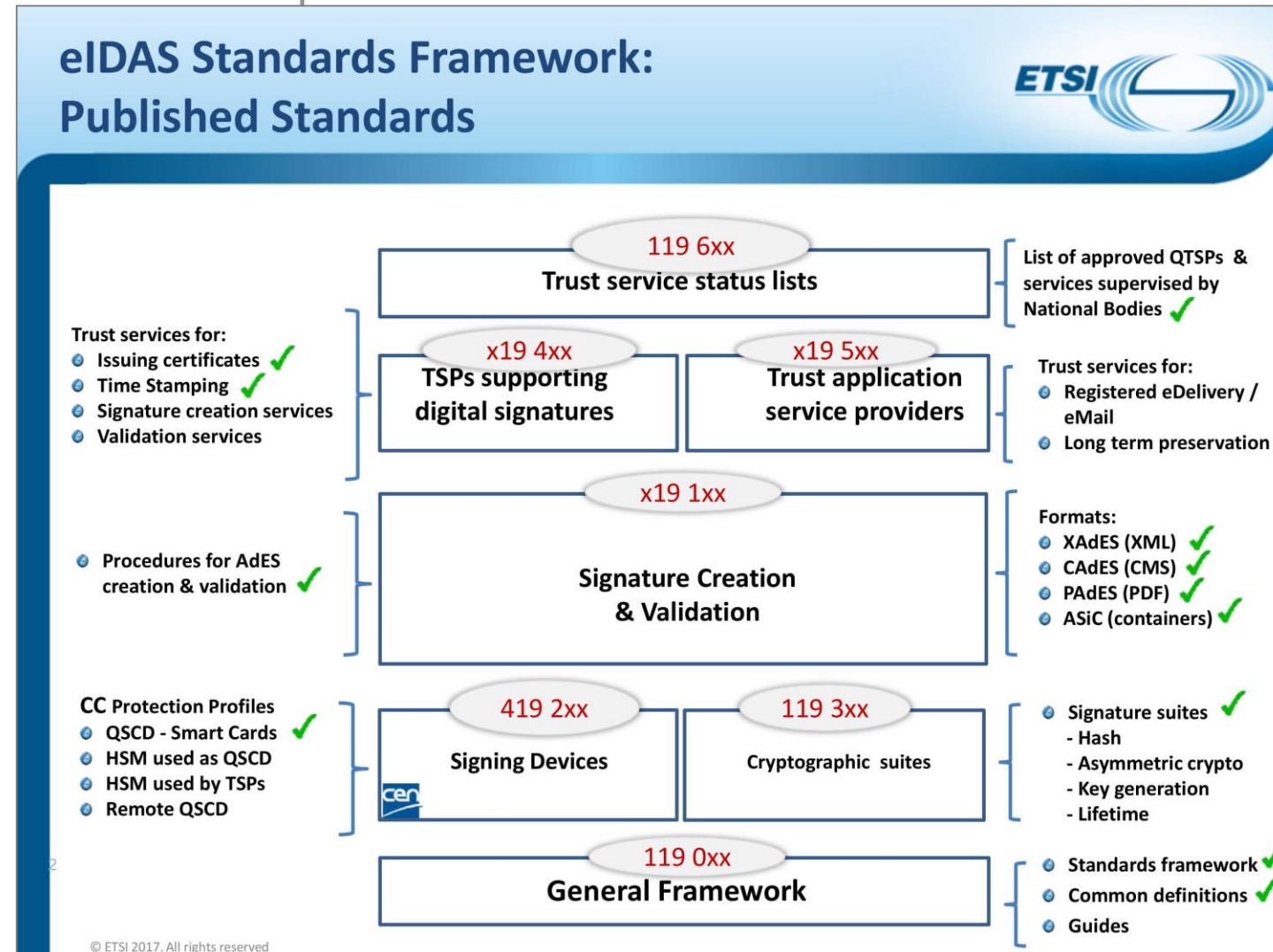
Other Trust Services

- Signature validation
 - ETSI is working on policy requirements, protocols and standards
 - Stable drafts expected in Q4 2017
 - Official publications in 2018
 - CEN will contribute security requirements and/or Protection Profiles as needed

- Electronic registered delivery / mail
 - Idem

- Long-term preservation
 - ETSI published study report SR 019500 in May
 - Next steps to be defined

Worldwide impact



Worldwide impact

Internationalisation – USA



- ETSI / US Workshop on “International Trust in digital signatures” 8 March 2017
 - Recognised equivalence between ETSI EN 319 411-1 & 2 and US Federal Bridge Policies
 - Equivalence between US Federal Bridge and EU Trust
 - Tool available to map data between different representations
 - Possible basis of cross recognition of signatures would be via trade agreement
 - Further justification needed to get buy in from US Government

Worldwide impact

Internationalisation - Japan



- ETSI / JIPDEC Workshop on “Interoperable Global Trust for Digital Signatures” to be held 4 July 2017
 - ETSI standards for trust services and signatures already widely adopted in Japan
 - Looking at adoption of Remote Signing based on EU standards

Worldwide impact



Building a standard for cloud signatures

A new industry consortium to pioneer
open digital signatures for mobile and the web

#OpenSignature



Worldwide impact



Architectures, Protocols and API Specifications for Remote Signature applications

Public pre-release version 0.1.7.9 rev. PR (2017-02)

Foreword

This document is a work by members of the Cloud Signature Consortium, a collaborative initiative among industry and academic organizations for building upon existing knowledge of solutions, architectures and protocols for Remote Electronic Signatures, also defined as Cloud-based Digital Signatures.

The Cloud Signature Consortium has developed the present specification to make these solutions interoperable and suitable for uniform adoption in the global market, in particular – but not exclusively – to meet the requirements of the European Union's Regulation 910/2014 on Electronic Identification and Trust Services (eIDAS), which formally took effect on 1 July 2016.

Quick links

[Cloud Signature Consortium](#)

[The digital signature challenge](#)

[The ecosystem that eIDAS needs](#)

[Bringing value to the industry](#)

[Contacts](#)

[Privacy policy](#)

Members

[Adobe](#)

[Asseco Data Systems](#)

[Bundesdruckerei / D-Trust](#)

[Docapost / Certinomis](#)

[Graz University of Technology](#)

[InfoCert](#)

[Intarsys Consulting](#)

[Intesi Group](#)

[Safelayer](#)

[SwissSign](#)

[Unibridge](#)

[Universign](#)

Utimaco Product Roadmap

- CryptoServer Se-Series Gen2 CC
 - Certification expected in Q1 2018

- TimestampServer 3.00
 - Major upgrade to support
 - CryptoServer running in FIPS / CC mode
 - Integrated GPS receiver, alternatively GLONASS or DCF77
 - CC certification acc. EN 419231 under investigation

Thanks for your attention

Thorsten Groetker

CTO

thorsten.groetker@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