eIDAS – Server Signing with Utimaco HSMs

June 14, 2018

Dieter Bong
Product Manager

utimaco®

Agenda

- eIDAS and Trust Services
- Server Signing Requirements
- Server Signing with Utimaco HSMs

eIDAS – Recap

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

eIDAS – Recap

Trust Services

eIDAS – Server Signing

Motivation

- eIDAS paragraph (52)
  - “The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits.”
  - “... remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products … in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory.”

eIDAS – Server Signing

Terminology: Remote Signature Creation - Server Signing - Local Signing

- “Remote Signature Creation” = “Server Signing”
  - eIDAS paragraph (52) uses the term Remote Signature Creation
  - EN 419241 uses the term Server Signing

- “Server Signing” = signature/seal creation by trust service provider on behalf of signatory
  - Customer signs a loan agreement using a smartphone app
    - Bank handles customer key, customer authorizes key usage on his smartphone
  - Trust Service Provider seals electronic invoices in the name of enterprises

- “Local Signing” = signature/seal creation by signatory
  - Signing a document at my PC, using a signature smartcard or USB token
  - Sealing electronic invoices using an HSM operated in the company data center
  - Timestamping documents/data as eIDAS Trust Service using a TSP signing key

eIDAS – Server Signing

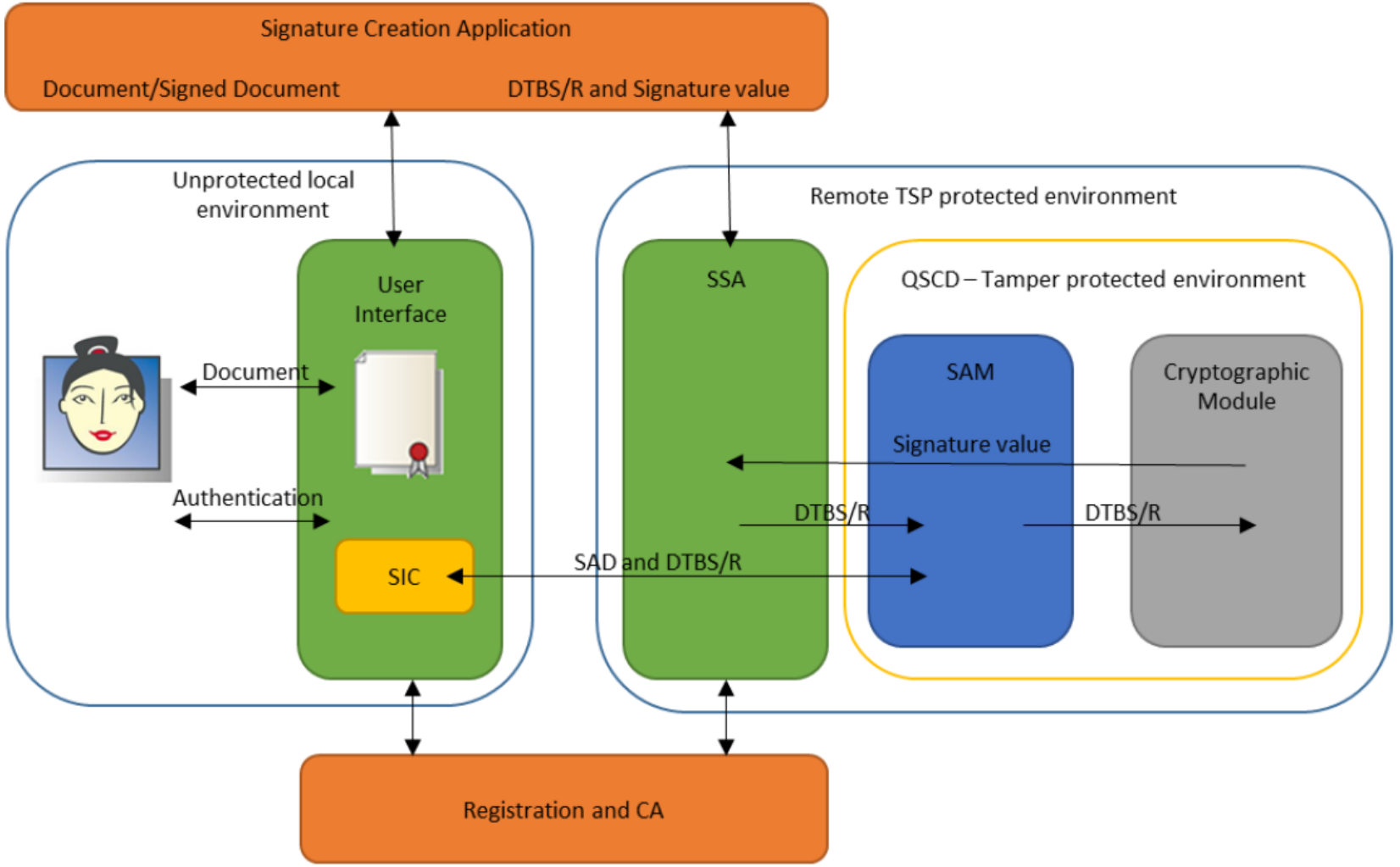
Requirements

- EN 419241 Trustworthy Systems Supporting Server Signing
  - Part 1: General System Security Requirements
  - Part 2: Protection Profile for QSCD for Server Signing

- Status
  - EN 419241-1 passed formal vote, awaiting publication
  - EN 419241-2
    - Passed CEN enquiry
    - Passed CC evaluation w/ a few minor comments, updated version submitted, certification pending

eIDAS – Server Signing

EN 419241 Trustworthy Systems Supporting Server Signing



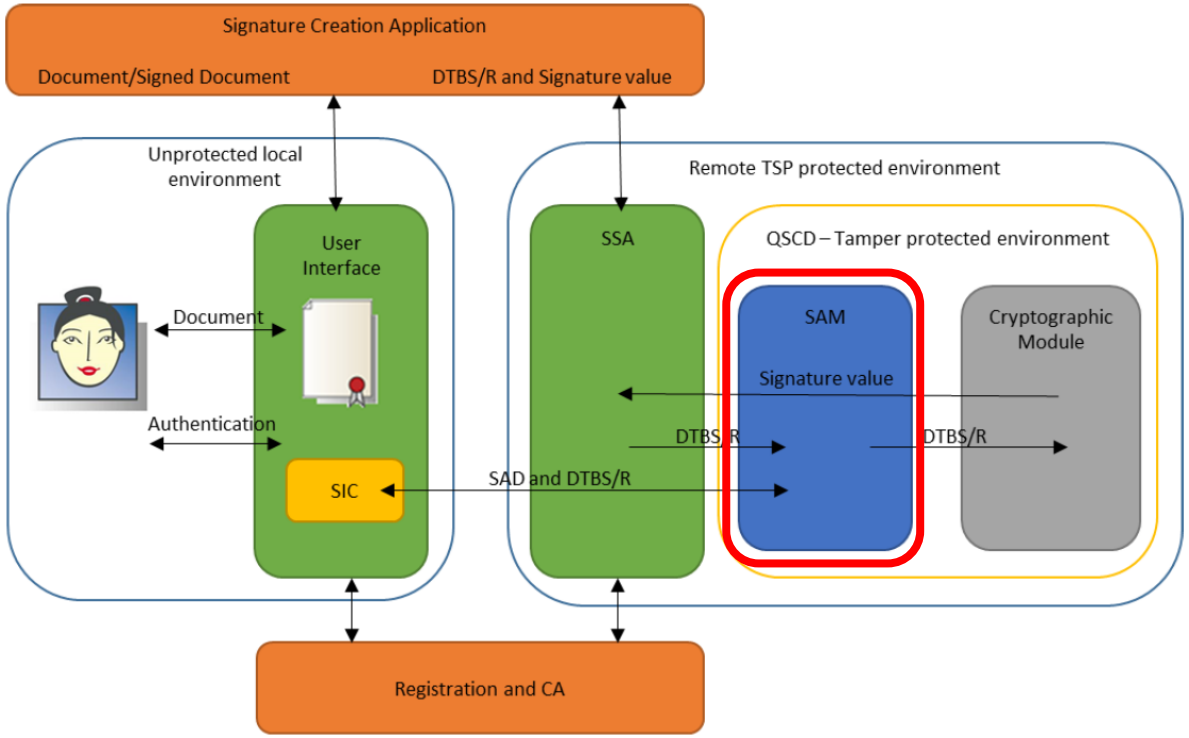
SIC = Signer Interaction Component
SSA = Server Signing Application
SAM = Signature Activation Module
SAD = Signature Activation Data
DTBS/R = Data To Be Signed
SAM = Signature Activation Module
QSCD = Qualified Signature Creation Device

eIDAS – Server Signing

EN 419241-2 Protection Profile ”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 …”



eIDAS – Server Signing

EN 419241-2 Protection Profile ”QSCD for Server Signing”

- TOE Overview
  - “A trustworthy system supporting server signing (TW4S) is a system that offers remote digital signatures as a service. It ensures that signer’s signing key or keys are only used under the sole control of the signer for the intended purpose.“
  - “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. ”
  - “The SAM module is the TOE of this PP. The TOE and Cryptographic Module certified against [EN 419 221-5] is required to obtain a QSCD.”

eIDAS – Server Signing

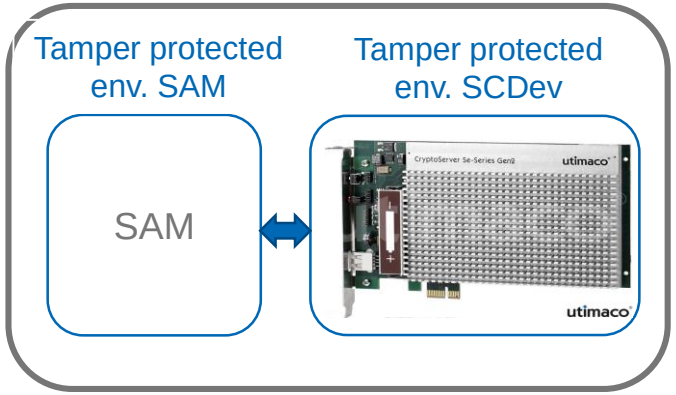
CryptoServer CP5

- 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
- Evaluation acc. EN 419221-5 is in final stage

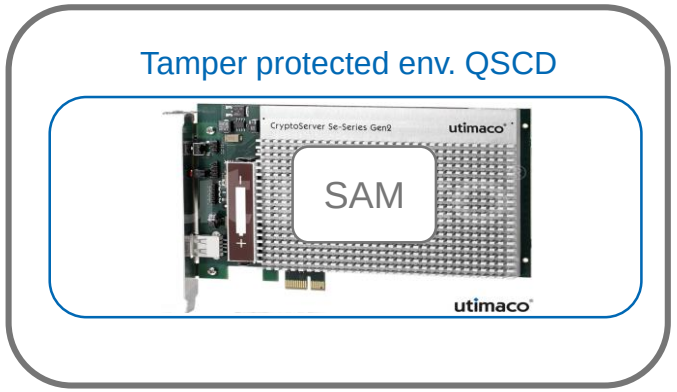
eIDAS – Server Signing

EN 419241-2 Tamper Protected Environment

- Separate tamper protected environments
  - SAM runs within its own tamper protected environment
  - “External SAM”



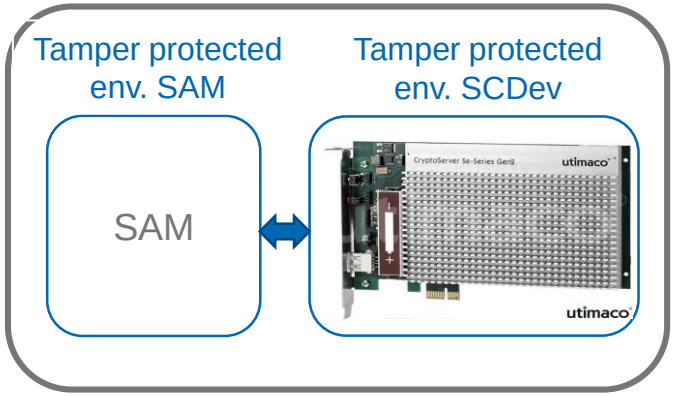
- Common tamper protected environment
  - SAM runs within the tamper protected environment provided by the cryptographic module
  - “Internal SAM”



eIDAS – Server Signing with Utimaco HSMs

External SAM

- SAM runs within its own tamper protected environment
  - E.g. FIPS compliant network appliance
- Why?
  - Existing solution for server signing is updated to integrate an HSM certified acc. EN 419221-5
- How?
  - CryptoServer CP5 integration via “external” interfaces
    - CXI API, Utimaco’s proprietary cryptographic API
    - PKCS#11 w/ proprietary extensions for key authorization
- Certification covers SAM
  - CryptoServer CP5 is used as certified



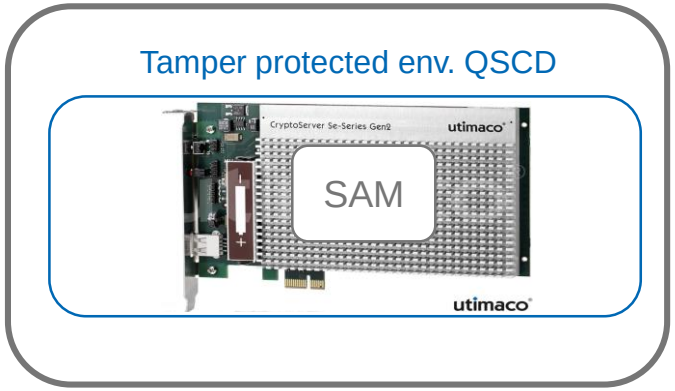
eIDAS – Server Signing with Utimaco HSMs

Internal SAM

- SAM runs within the tamper protected environment provided by CryptoServer CP5

- Why?
  - Solution vendor / customer already uses CryptoServer w/ custom firmware and extends this for Server Signing

- How?
  - CryptoServer CP5 SDK for development of SAM firmware, using “internal” firmware interfaces



- Certification covers SAM but may require CryptoServer CP5 re-certification
  - CryptoServer CP5 internal interfaces have partly been evaluated
  - If SAM firmware uses additional internal interfaces => re-certification required to include these interfaces in certification report

eIDAS – Server Signing with Utimaco HSMs

Utimaco SAM ?

- Utimaco has no plans to develop and certify our own SAM and server signing solution
  - Client components and solution development are not our business
  - We are not competing with our partners

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