eIDAS - electronic Identification and Trust Services for Electronic Transactions

September 2016

Dieter Bong
Product Manager

utimaco®

Agenda

- eIDAS – An Overview
- Electronic Identification
- Electronic Trust Services
- Standardization
- How Utimaco addresses eIDAS Requirements

eIDAS – An Overview

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 – An Overview

Why eIDAS?

- Directive 1999/93/EC “Community framework for electronic signatures”
  - Gives direction for implementing electronic signatures in national signature Laws

- What did actually happen?
  - Differing “interpretations” in national signature laws
  - Security requirements varied considerably between countries
  - Incompatible technical solutions
  - No cross-boarder usage, low public acceptance

- EU Parliament and Council therefore issued
  - Regulation 910/2014
    - Binding for all EU countries
  - Standardization mandate M/460 to CEN, CENELEC and ETSI
    - Standards, security requirements, policy requirements, Common Criteria Protection Profiles, etc.

eIDAS – An Overview

Applicability

- eIDAS is applicable to
  - Public eIDs
    - eID card, passport
    - Smartcard, USB token, …
  - Public Trust Services
    - Certificate Provider, …
- eIDAS is not (per se) applicable to
  - Private eIDs
    - Company IDs, payment cards, …
  - Closed user groups
    - eID card used for access to company PC/network, …
- eIDAS does not
  - Mandate introduction of online services using eIDs
  - Forbid online services that don‘t use an eID
    - e.g. German 2-step online tax declaration may remain in place: upload electronic tax declaration + handwritten signature on print-out

Electronic Identification

eID Regulations in eIDAS

- Member states may notify national electronic identification schemes to EU Commission
  - No obligation to notify a national eID
    - No obligation to introduce a national eID

- Member States must recognize notified electronic identification schemes of other Member States for online services
  - No obligation to recognize non-notified eIDs for online services
    - No obligation to recognize only notified eIDs for presence-services

➔ Mutual recognition of eIDs

- Electronic IDs may be issued to natural and legal persons
  - We‘ll come back to that later

Electronic Trust Services

Trust Services

- Signing
- Sealing
- Timestamping
- Electronic registered delivery service
- Website authentication

Electronic Signature

EU's trust mark for qualified trust services

Electronic Signatures

- Electronic signature
  - “Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign”
    - E.g. scan of a handwritten signature

- Advanced electronic signature
  - Electronic signature that is
    - uniquely linked to the signatory
    - capable of identifying the signatory
    - created using electronic signature creation data that the signatory can … use under his sole control
    - linked to the data signed therewith in such a way that any subsequent change in the data is detectable

- Qualified electronic signature
  - “Advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures”

Electronic Seals

- Electronic seal
  - “Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity”
- Advanced electronic seal
  - Electronic seal that is
    - uniquely linked to the creator of the seal
    - capable of identifying the creator of the seal
    - created using electronic seal creation data that the creator of the seal can … under its control, use for electronic seal creation
    - linked to the data signed therewith in such a way that any subsequent change in the data is detectable
- Qualified electronic seal
  - Advanced electronic seal that is created by a qualified electronic seal creation device, and which is based on a qualified certificate for electronic seal

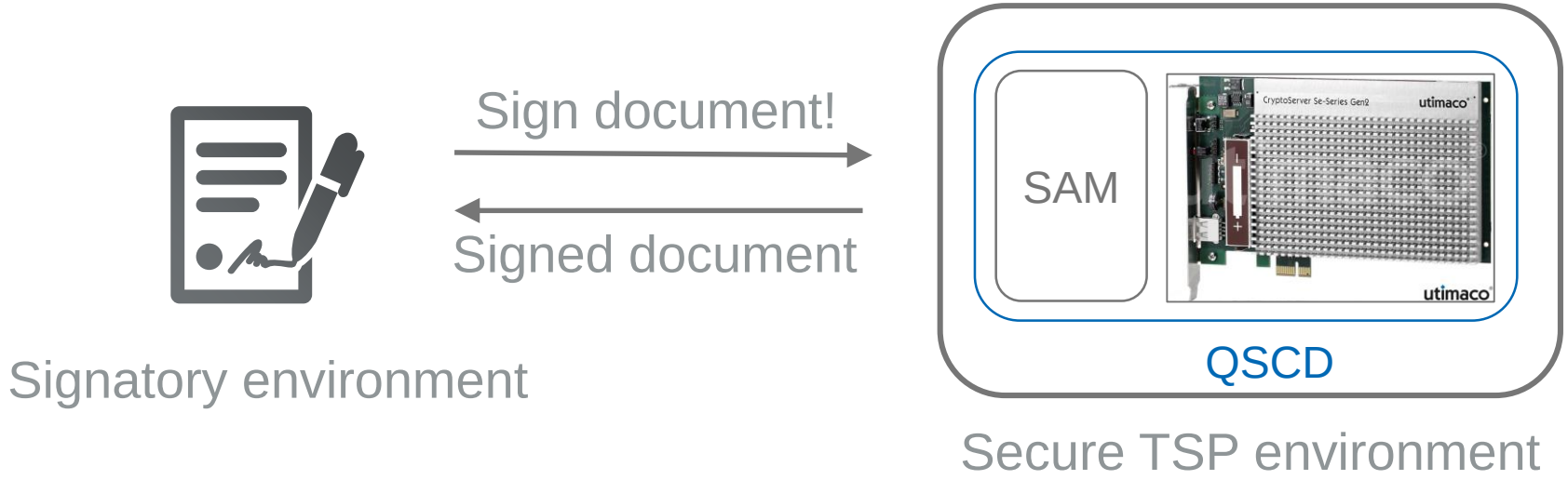
Electronic Trust Services

Electronic Signatures vs. Electronic Seals

- 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

Remote Electronic Signatures

- Aka. Remote Server Signing
- “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.”
- Similarly: electronic seals



Standardization

CEN - ETSI

- 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
    - Very recent publication on https://portal.etsi.org//TBSiteMap/ESI/ESIActivities.aspx

Standardization

CEN TC224 Work Groups

- WG15: European Citizen Card
- WG16: Application Interface for smart cards used as Secure Signature Creation Devices
- WG17: Protection Profiles in the context of SSCD

Standardization

CEN TC224 WG17

- EN 419221 Protection Profiles for TSP Cryptographic modules
  - Part 1: Overview
  - Part 2: Cryptographic module for CSP signing operations with backup
  - Part 3: Cryptographic module for CSP key generation services
  - Part 4: Cryptographic module for CSP signing operations without backup
  - Part 5: Cryptographic Module for Trust Services

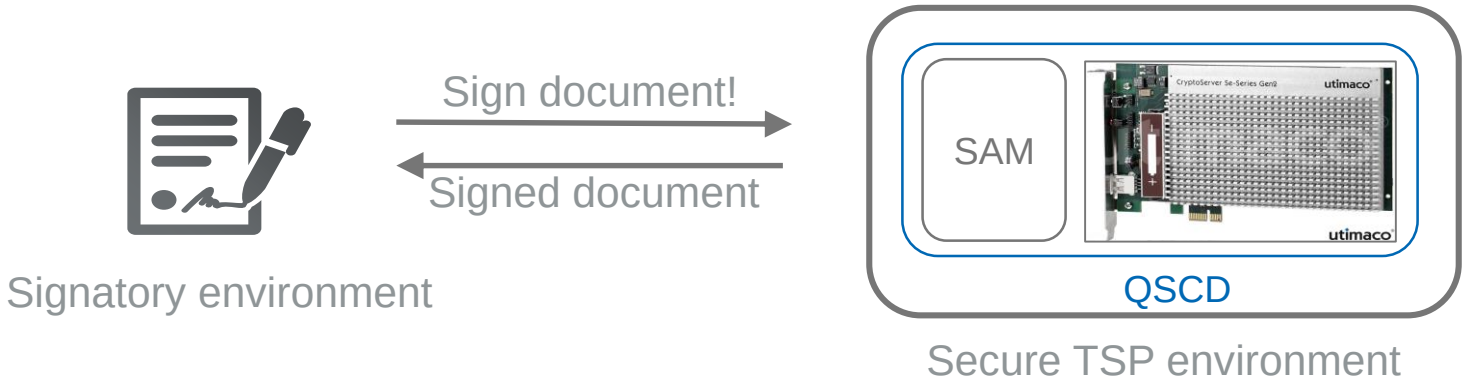
  - Parts 1 to 4 have recently been published CEN Technical Standard
  - Part 5 has been submitted for evaluation

- EN 419231 Protection Profile for trustworthy systems supporting time stamping
  - Submitted for evaluation
  - Timestamping system must use a cryptographic module that meets the requirements identified in CEN TS 419221-2/-4/-5 or ISO/IEC 19790 level 3 (FIPS Level 3) or EN 319421 §7.5.2 or ETSI 102023 §7.2.2

Standardization

CEN TC224 WG17

- EN 419241 Trustworthy Systems Supporting Server Signing
  - Part 1: General System Security Requirements
    - Security requirements for server-side system, signature application protocol, signature activation module (SAM), signer authentication, …



  - Part 2: Protection Profile for QSCD for Server Signing
    - Cryptographic module shall be certified against EN 419221-5

  - Both parts in work

How Utimaco addresses eIDAS Requirements

- FIPS Level 3 validated Hardware Security Modules
  - CryptoServer Se-Series
  - CryptoServer Se-Series Gen2 (review pending)
- Common Criteria certification
  - CryptoServer Se-Series Gen2 evaluation against EN 419221-5 in progress
- Technical consulting
- Integration support
  - Training
  - Setup and installation

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