DHBW Stuttgart

eIDAS2, NIS2
Signatures, Seals and EUDI-Wallets

Cyber Security | 06.10.2025

Gerald Dißauer | Lecturer
A-SIT Secure Information Technology Center Austria

Agenda

Introduction

eIDAS & eIDAS2 – General Overview

Remote Signature/Seal Solutions and EUDI-Wallets

Practical Every-day Experiences from eIDAS Certifications

Summary

DEMONSTRATION
OPERATIONAL SYSTEM FROM AUSTRIA

ID Austria – the Austrian eID-System

Key Figures[1]

- **More than 4M**[2] active users - mainly between Mo-Fr and ca. **07:00 – 20:00**
- Between **100.000 to 250.000 signature creations per 24h** on average
- Between **4.5mio to 6.5mio signature creations per month** on average
- Between **150.000 to 200.000** logins on digital services per day on average

Selected Use Cases – via App „Digitales Amt“

- Access e-Government applications *(e.g., finanzonline.gv.at/, gesundheitskasse.at/, digital drivers licence, digital proof of age, digital car registration, digital proof of identity)*
- Electronically sign PDF documents legally valid

AUSTRIAN EID OVERVIEW
FACTS AND HISTORY

Introduced in 2005 on a voluntary basis

- Defines functions and enables various technology
- Sector-specific persistent identifiers
- Qualified electronic signature
- Representation on behalf and mandates

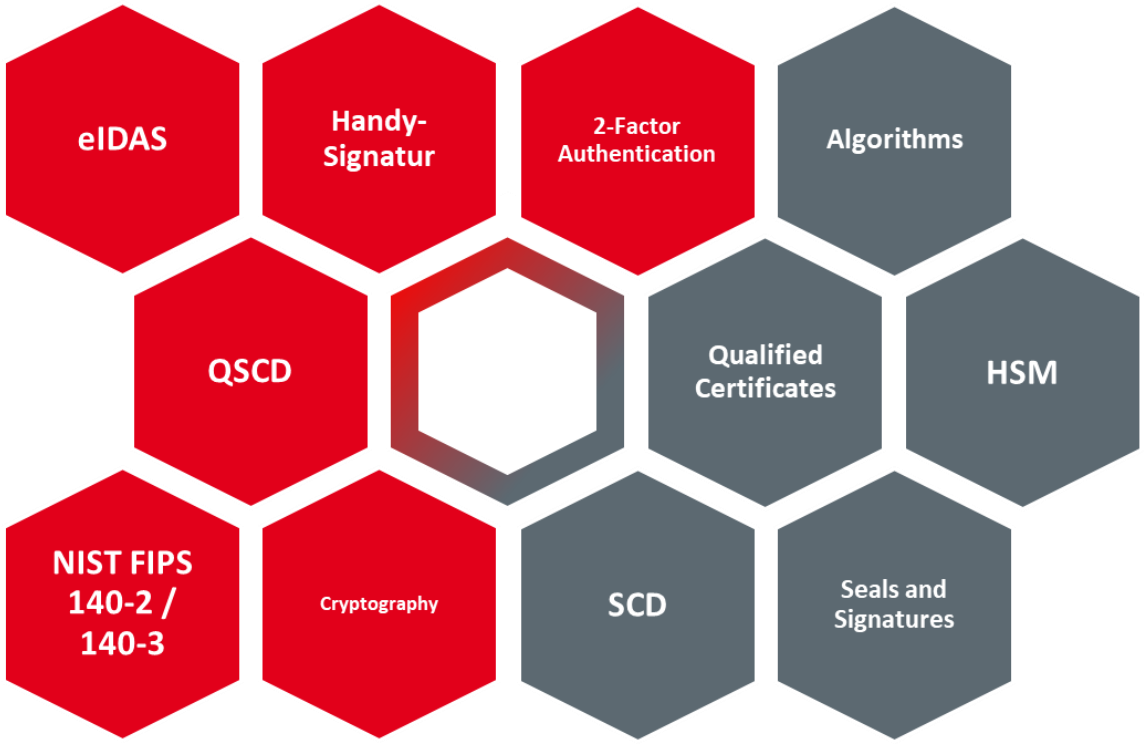
Technology neutral

- Smartcards *(e.g., former eCard)*
- Smartphones *(OS e.g., Android, iOS)*

Redesign is in operation – but transition to AT-EUDIW ongoing

Focus on mobile devices using the new *„ID Austria“*

KEYWORDS


eIDAS
Handy-Signatur
2-Factor Authentication
Algorithms
QSCD
Qualified Certificates
HSM
NIST FIPS 140-2 / 140-3
Cryptography
SCD
Seals and Signatures

OVERVIEW OF FIGURES
AUSTRIAN STATISTICS | A GREAT SUCCESS STORY

(1) Austrian active e-Cards and Mobile E-ID
(2) Monthly use of Austrian Mobile E-ID
(3) SMS-OTP vs. AppQR/Biometrics

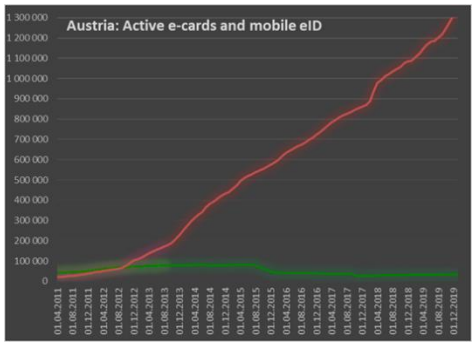


Image Source: H. Leitold (A-SIT)

1

Image Source: H. Leitold (A-SIT)

2

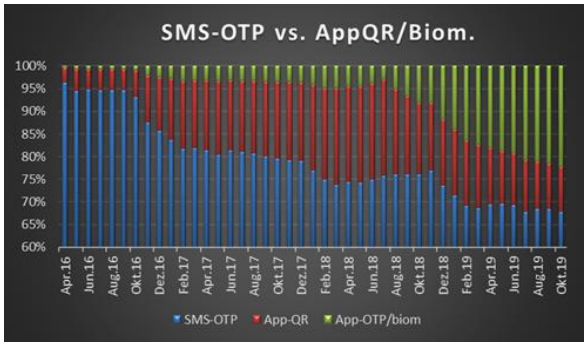


Image Source: H. Leitold (A-SIT)

3

SOME OBSERVATIONS
DIGITAL SIGNATURE SOLUTIONS AND CERTIFICATION

Distinction between two kinds of certifications[1]

(1) IT security **certification based** on **international standards** *(e.g., ISO 15408)* Obtained a lot of experiences in the last decades *(e.g., Smartcards)*

(2) **Certification** using **alternative processes** *(international standards are not available e.g., for innovative technologies such as mobile signing solutions, cloud signing)* Upcoming innovative solutions where standards are very limited

Smartphone Product Cycle

Smartcard Product Cycle

Certification Requirements Must Not Restrict Required Technology

[1] cf. recital (55), REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Agenda

Introduction

eIDAS & eIDAS2 – General Overview

Remote Signature/Seal Solutions and EUDI-Wallets

Practical Every-day Experiences from eIDAS Certifications

Summary

RELEVANT LEGISLATION FOR SIGNATURE SOLUTIONS
OVERVIEW | EU AND AUSTRIA | 5 SELECTED LEGAL BASES

EU Level

- REGULATION (EU) No 910/2014 *(eIDAS)*[1]
- COMMISSION IMPLEMENTING DECISION[2] (EU) 2016/650
- **REGULATION (EU) 2024/1183 *(eIDAS2)*[3] 20.5.2024 entered into force**

Austrian Legislation

- Signatur- und Vertrauensdienstegesetz – SVG[4] *(if applicable)*
- Signatur- und Vertrauensdiensteverordnung – SVV[5] *(if applicable)*

[1] cf. REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[2] cf. COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

[3] cf. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

[4] cf. Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG, BGBl. I Nr. 50/2016 vom 08.Juli 2016)

[5] cf. Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung – SVV, BGBl. II Nr. 208/2016

RELEVANT LEGISLATION FOR SIGNATURE SOLUTIONS
OVERVIEW | EU AND AUSTRIA | 5 SELECTED LEGAL BASES

EU Level

- REGULATION (EU) No 910/2014 *(eIDAS)*[1]
- COMMISSION IMPLEMENTING DECISION[2] (EU) 2016/650
- **REGULATION (EU) 2024/1183 *(eIDAS2)*[3] 20.5.2024 entered into force**

Austrian Legislation

- Signatur- und Vertrauensdienstegesetz – SVG[4] *(if applicable)*
- Signatur- und Vertrauensdiensteverordnung – SVV[5] *(if applicable)*

eIDAS2 also denoted as „eIDAS-Amendment“

WHAT IS THE MAIN PURPOSE?
DIGITAL SIGNATURES, SEALS, IDENTITIES and TIMESTAMPS

EUDI[1] Wallet is new

- issued for both legal and natural persons until end of 2026 by Member States *(can be delegated)*
- Shall be certified by conformity assessment bodies
- cross-border reliance of EUDI Wallets issued by MS

Changes for Qualified Trust Service Providers

- Cyber Security risk-management measures from Art. 21 NIS2 (2022/2555)
- No „new“ remote identification pursuant to Art. 24(1)d eIDAS

Most relevant changes in Certifications of Signature and Seal Creation Devices

- Validity up to at most 5 years, every 2 years vulnerability assessment as an obligation

[1] EUDI – European Digital Identity

3 TYPES OF ELECTRONIC SIGNATURES
ELECTRONIC SIGNATURE, ADVANCED, AND QUALIFIED

*‘**electronic signature**’ means 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;*[1]

*‘**advanced electronic signature**’ means an electronic signature which meets the requirements set out in Article 26;*[1]

*‘**qualified electronic signature**’ means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;*[1]

[1] cf. L 257/84, REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

QUALIFIED SIGNATURE CREATION DEVICE (QSCD) OPERATED BY TSPS UNDER THE EIDAS REGULATION

'qualified certificate for electronic signature' *means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;*[1]

'qualified electronic signature creation device' *means an electronic signature creation device that meets the requirements laid down in Annex II;*[2]

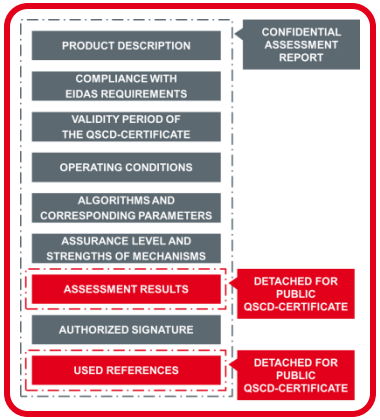
[1] cf. L 257/84, REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

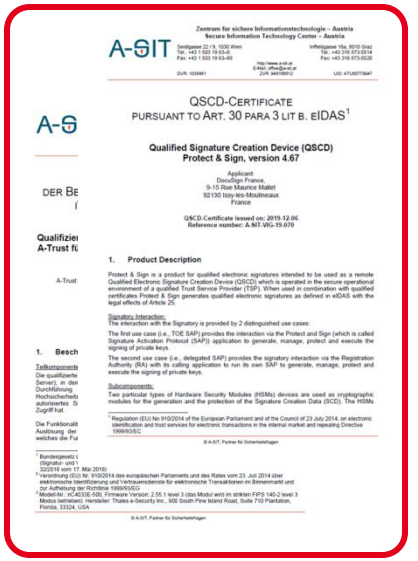
[2] cf. L 257/85, REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

QSCD CERTIFICATE
PURSUANT TO ART. 30 PARA 3 LIT B. EIDAS

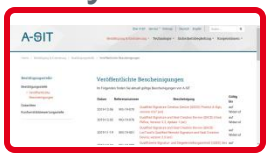
Certification of qualified electronic signature creation devices

- Conducted by confirmation bodies such as A-SIT *(or others)*
- A-SIT publishes issued QSCD certificates on its website[1]
- Basic Structure of a QSCD Certificate and Report





- Similar structure
- Report has one more headline
- QSCD certificate publicly[1] available *(if requested)*



[1] Annotation: Published QSCD certificates (see examples above) retrievable: https://www.a-sit.at/bestaetigung-evaluierung/bestaetigungsstelle/downloads/ [Accessed: 2020-02-09]

NIS2 REQUIREMENTS FOR QTSPS

Newly introduced under eIDAS2 (Art. 20) of eIDAS-amendment

Emphasis on **Article 21 NIS2 Directive** ***(„Cybersecurity risk-management measures“)***

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

HOW TO DEAL WITH THIS AS A QTSP?

First and foremost – most of the requirements are covered by ISO 27001:2022 certification of an ISMS

Why?

For reference:
ENISA Implementing Guidance (Oct. 2024)
A mapping of the security requirements between ISO 27001:2022 and QTSP relevant ETSI EN 319 401 is included therein

eIDAS2 CERTIFICATION PROCESS
AN OVERVIEW

Electronic Identification, Authentication and Trust Services (eIDAS) regulation 910/2014 amended by Regulation 2024/1183 (eIDAS2 / „eIDAS amendment“)

- Framework to establish common standards for electronic identification and trust services
- Examples: Electronic signatures, seals, time stamps, and certificates or EUDI Wallets, Website Authentication
- Defines standards and requirements for trust services
- Roles and responsibilities of the stakeholders defined for certification
- 2 basic kinds: (1) Conformity Assessment and (2) Certifications

EIDAS2-REQUIREMENTS FOR QSCDS

REQUIREMENTS FOR QSCDS UNDER THE EIDAS2 LAYED DOWN IN THE ANNEX II

4 *(1)* Requirements that include a series of other requirements

1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:

(a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;

(b) the electronic signature creation data used for electronic signature creation can practically occur only once;

(c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;

(d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.

REQUIREMENTS FOR QSCDS UNDER THE EIDAS2 | cont'd
LAYED DOWN IN THE ANNEX II

4 *(2-4)* Requirements that include a series of other requirements

2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.

3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.

4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:

(a) the security of the duplicated datasets must be at the same level as for the original datasets;

(b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

Agenda

Introduction

eIDAS & eIDAS2 – General Overview

Remote Signature/Seal Solutions and EUDI-Wallets

Practical Every-day Experiences from eIDAS Certifications

Summary

TECHNICAL ARCHITECTURE OF QSCDS

REMOTE SIGNATURE SOLUTIONS | BASIC ARCHITECTURE
QUALIFIED SIGNATURE CREATION DEVICES (QSCDs)

- TW4S – **T**rustworthy **S**ystem **S**upporting **S**erver **S**igning
- CA – Certification Authority
- DTBS/R – Data to be signed *(representation)*
- HSM – Hardware Security Module
  SAD – Signature Activation Data
- SAM – Signature Activation Module
- SCA – Signature Creation Application
- SIC – Signature Interaction Component
- SSA – Server Signing Application
- TOE – Target of Evaluation
- TSP – Trust Service Provider

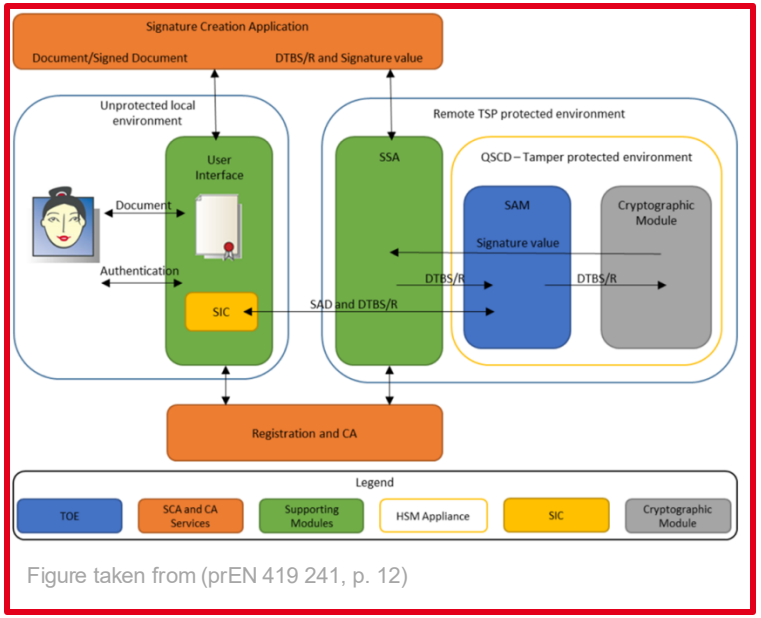


Figure taken from (prEN 419 241, p. 12)

TECHNICAL ARCHITECTURE OF QSCDS[1]
CRYPTOGRAPHIC PRODUCTS | EXAMPLES

Selected Subcomponents for QSCDs *(the TOE)*

- Hardware Appliance *(e.g., with a dedicated function that includes cryptographic modules)*
- **Cryptographic modules** *(e.g., **HSMs** which perform cryptographic operations)*
- SAP *(e.g., Software)*
- Operational in protected environments *(e.g., certified data centers, TSPs)*
- Interaction components *(e.g., software)* to interact with remote environments *(e.g., CA, calling application, time stamping authority)*

Signature Creation Data and Signature Validation Data

- SCD/SVD keypairs *(i.e., asymmetric; private/public)*
  e.g., created and destroyed for one signature creation process
- Certified security functions of **HSMs** to perform cryptographic operations

[1] Important Annotation: Only publicly available data are taken into account and the practical implementation may differ

THE BASIC COMPONENTS OF A QSCD
HSM AND SAM

Qualified Signatures / Seals require Qualified Signature/Seal Creation Device

Two main components form a QSCD

- **Hardware Security Module:** The QSCD is used to protect (and erase) the cryptographic key material used for the generation of signatures and seals. The HSM can be certified against e.g., Protection Profile EN 419 221-5 *„Cryptographic Module for Trust Services“*
- **Signature Activation Module:** A QTSP uses a SAM to activate the signing key and binding its use to a given signing request of a signatory/seal creator. The SAM is integrated into the tamper protected TSP environment and it interacts with the HSM. The whole solution can be certified against e.g., PP EN 419 241-2 *“QSCD for Server Signing“*

THE BASIC COMPONENTS OF A QSCD | cont´d
HSM AND SAM

Protection Profiles EN 419 221-5 (HSM) and
Protection Profile EN 419 241-5 (SAM)

are exemplary PPs that designated bodies can accept in the decision to qualify a solution as a QSCD under eIDAS2

WHY DO WE NEED A QSCD?
QUALIFIED TRUST SERVICS UNDER eIDAS2 RELY ON A QSCD

What is a Trust Service and what is a TSP?

- **Trust Service:** A Trust Service is an electronic service that is responsible for creating, verifying and validating electronic signatures, seals, timestamps, delivery services, certificates, website authentication

- **Trust Service Provider:** A TSP is defined as a natural or legal person who provides one or more trust services either as a qualified (QTSP) or „unqualified“ trust service provider (TSP). A QTSP has „qualified status“ which is determined from the supervisory body hence QTSPs undergo at least every 24 months a so called conformity assessment pursuant to Art. 20 eIDAS2 considering all provided qualified trust services.

CERTIFICATION PROCESS FOR A QSCD UNDER eIDAS2

A QSCD is a technical conjunction of (1) HSM and (2) SAM (cf., slides before)

Prerequisites

- The HSM can be either certified against e.g., Common Criteria (e.g., EAL4 or higher) or alternatively against e.g., NIST FIPS 140-2 (or -3) level 3
- The SAM and the HSM form the QSCD
- The SAM can also be integrated into the Firmware of the tamper-proof HSM
- The SAM and the HSM can function as a remote QSCD operated by a Qualified Trust Serviced Provider if certain requirements pursuant to Art. 30 eIDAS are met.
- Operation of the QSCD under the operating conditions in the QSCD Certificate

WHAT IS INCLUDED IN THE CERTIFICATION PROCESS?
QUICK OVERVIEW

- Evidence checking and validation
- Technical Testing of the QSCD solution
- Verifying that the evidence matches the technical solution

The certification process covers e.g.,

- Secure cryptographic key handling (e.g., generation, usage, zeroization)
- Protection against tampering (mainly from the HSM)
- Secure audit logging
- End-to-end security
- Secure operation of the QSCD
- QSCD lifecycle, key lifecycle, lifecycle of related roles

HSMS FOR QSCDS
SELECTED EXAMPLES | DIGITAL SIGNATURE SYSTEMS

- SafeNet PCIe Hardware Security Module and SafeNet PCIe Hardware Security Module for SafeNet Network HSM

  Firmware Versions: 6.10.7, 6.10.9, and 6.11.2;
  Hardware Versions: VBD-05-0100, VBD-05-0101, VBD-05-0103;

  #2489

  Firmware Versions: 6.24.6 [1] and 6.24.7 [2];
  Hardware Versions: VBD-05-0100 [1, 2], VBD-05-0101 [1, 2], VBD-05-0102 [1, 2] and VBD-05-0103 [1, 2];

  #3268

- nShield F3 10+ [1], nShield F3 500+ [2], nShield F3 6000+ [3], nShield F3 500+ for nShield Connect+ [4], nShield F3 1500+ for nShield Connect+ [5] and nShield F3 6000+ for nShield Connect+ [6]

  Firmware Versions: 2.51.10-2, 2.55.1-2, and 2.55.2-2
  Hardware Versions: nC4033E-010 [1], nC4433E-500 [2], nC4433E-6K0 [3], nC4433E-500N [4], nC4433E-1K5N [5] and nC4433E-6K0N [6], Build Standard N

  #2149

HSM AND SAM AS TOE FOR QSCDs
SELECTED EXAMPLES

- Utimaco CryptoServer CP5
- ProtectServer Internal Express 2
- nCipher nShield Solo XC
- SafeNet Luna PCI-E (K6), K7, K7+
- DocuSign HSM Appliance
- Thales nShield Solo/Solo+
- nShield Connect/connect+/Connect XC
- …

HSMs are mostly certified against CC, NIST 140-2 (transition to 140-3), ANSSI and other comparable standards

EUDI-WALLET | cont´d
2 MAIN SCENARIOS

EUDI Wallets can be implemented in two main categories

1) Wallet-centric Architecture
2) QTSP-centric Architecture

Three main roles

1) Wallet
2) Qualified Trust Service Provider
3) Relying Party

EUDI-WALLET | cont´d
2 MAIN SCENARIOS

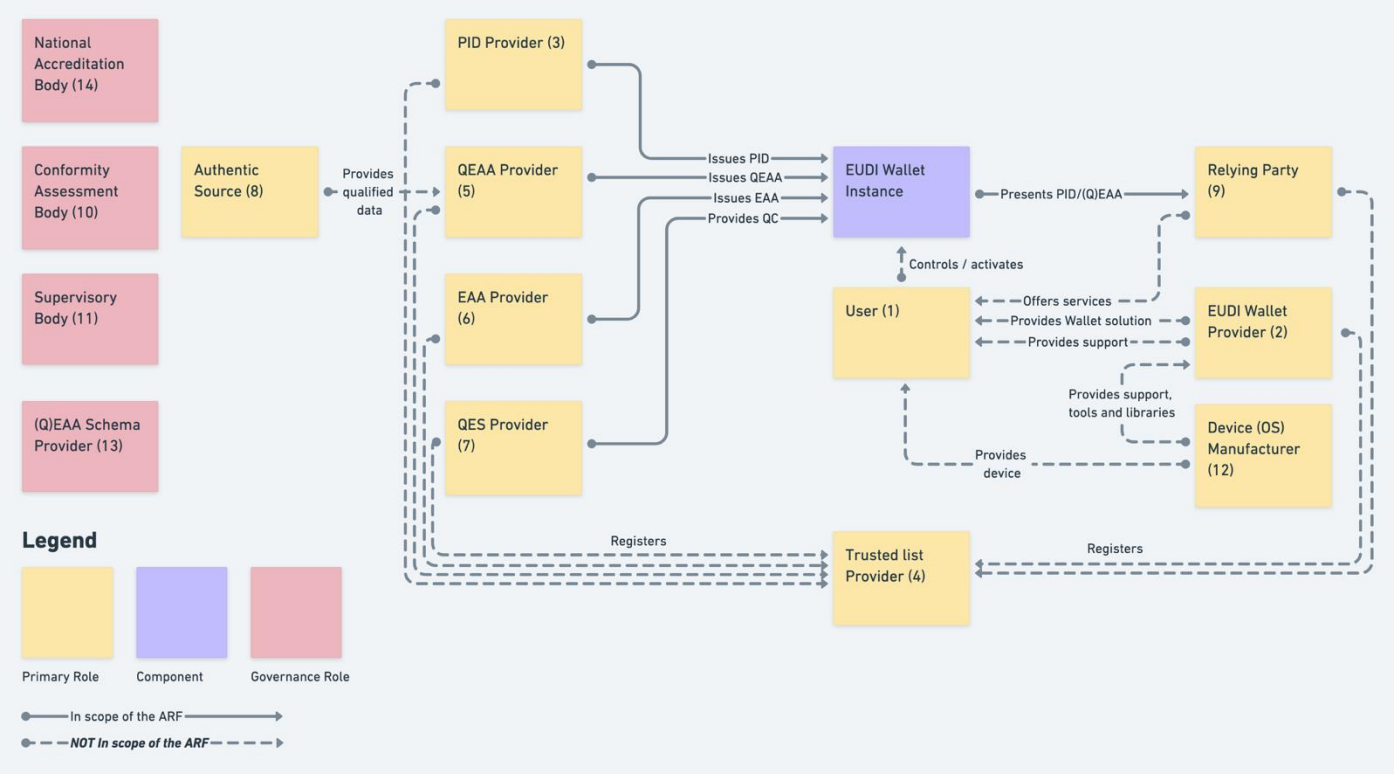
Wallet-centric model

- The wallet acts as a means for the user to initiate, control and approve transactions
- The SIC/SCA is integrated into the wallet
- The QTSP can be selected by the user via the wallet
- Interfaces: Relying Party to Wallet and Wallet to QTSP

QTSP-centric model

- The wallet acts as a means to authenticate and authorize signatures
- The SIC/SCA is integrated into the Relying Party or QTSP
- The Relying Party selects the QTSP
- Interfaces: Relying Party to QTSP and Wallet to QTSP

ROLES IN THE EUDIW-ECOSYSTEM

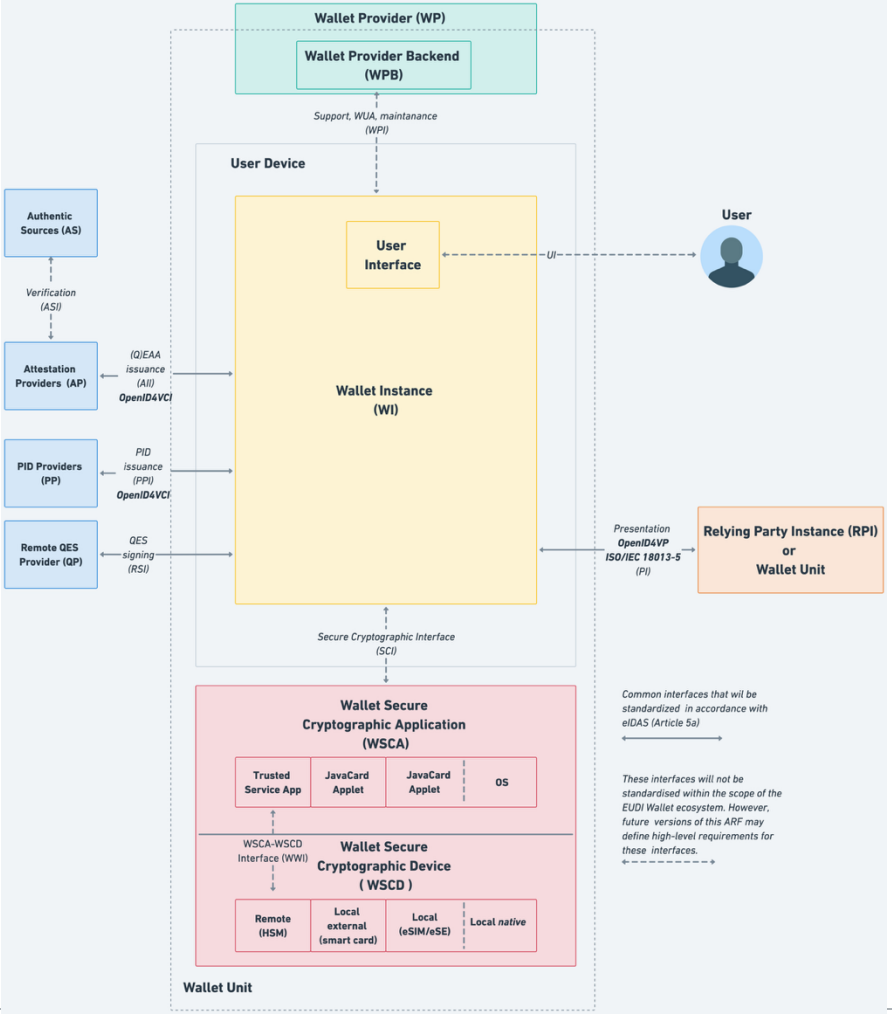


ROLES IN THE EUDIW-ECOSYSTEM | cont´d
TAKEN FROM ARF

Roles from the figure
1.End Users of EUDI Wallets
2.EUDI Wallet Providers
3.Person Identification Data Providers
4.Trusted Lists providers
5.Qualified Electronic Attestation of Attributes (QEAA) Providers
6.Non-qualified Electronic Attestation of Attributes (EAA) Providers
7.Qualified and non-qualified certificate for electronic signature/seal Providers
8.Authentic Sources
9.Relying Parties
10.Conformity Assessment Bodies (CAB)
11.Supervisory bodies
12.Device manufacturers and related subsystems providers
13.(Q)EAA Schema Providers
14.National Accreditation Bodies

Source: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.1.0/arf/

Source: ARF


Wallet Provider (WP)
Wallet Provider Backend (WPB)
Support, WUA, maintanance (WPI)
User Device
Authentic Sources (AS)
Verification (ASI)
Attestation Providers (AP)
(Q)EAA issuance (AII)
OpenID4VCI
PID Providers (PP)
PID issuance (PPI)
OpenID4VCI
Remote QES Provider (QP)
QES signing (RSI)
User Interface
UI
User
Wallet Instance (WI)
Presentation OpenID4VP ISO/IEC 18013-5 (PI)
Relying Party Instance (RPI) or Wallet Unit
Secure Cryptographic Interface (SCI)
Wallet Secure Cryptographic Application (WSCA)
Trusted Service App
JavaCard Applet
JavaCard Applet
OS
WSCA-WSCD Interface (WWI)
Wallet Secure Cryptographic Device (WSCD)
Remote (HSM)
Local external (smart card)
Local (eSIM/eSE)
Local native
Wallet Unit
Common interfaces that wil be standardized in accordance with eIDAS (Article 5a)
These interfaces will not be standardised within the scope of the EUDI Wallet ecosystem. However, future versions of this ARF may define high-level requirements for these interfaces.

WHAT FOR AN EUDIW?
6 MAJOR USE-CASES

1) **eGov Services.** *A secure digital ID that will allow citizens to quickly and securely prove their identity as part of their online citizenship procedures.*

2) **Bank Account Opening.** *A secure digital ID that can be used to open current and savings bank accounts everywhere in Europe, including across borders.*

3) **SIM Card Registration.** *A secure digital ID suitable for activating pre-paid & post-paid mobile telephone contracts online, including cross-border subscriptions.*

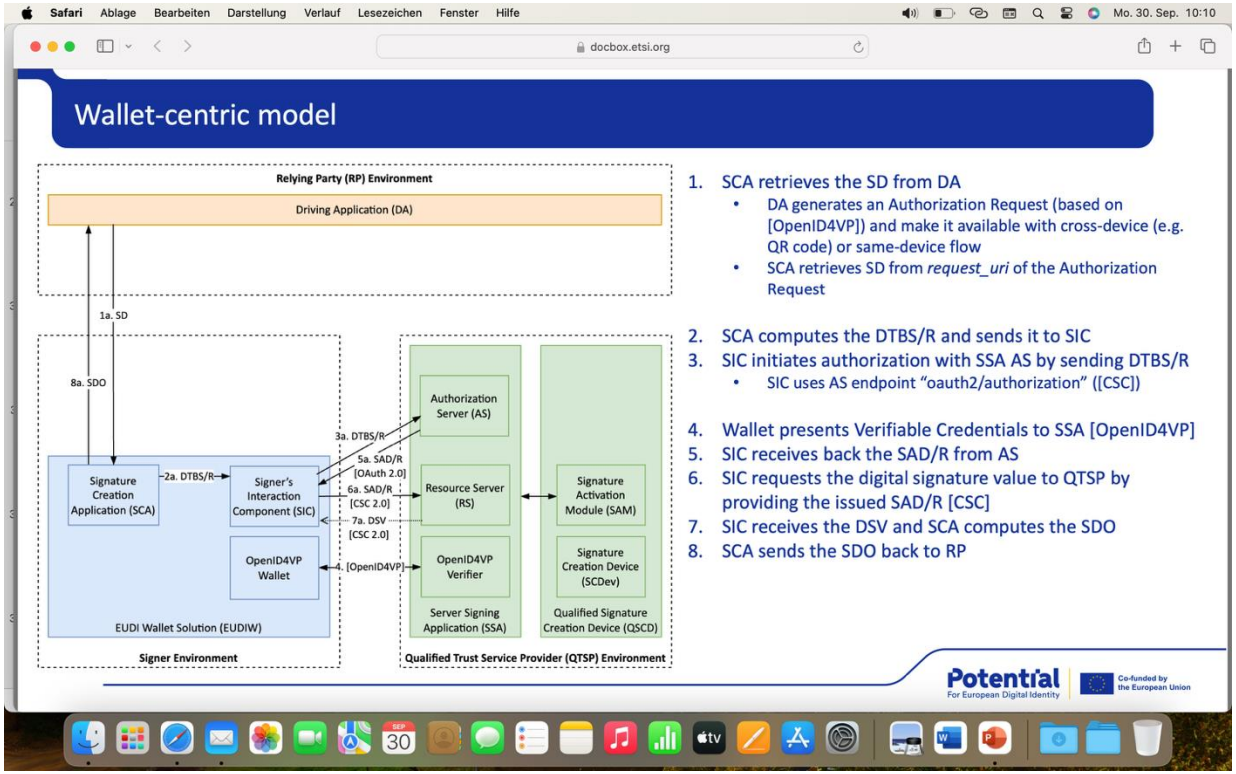
4) **Mobile Driving Licence.** *A secure digital driving licence that will be accepted by car rental agents and police officers everywhere in Europe.*

5) **Qualified eSignature.** *A secure qualified digital signature that will enable all citizens across Europe to sign documents and declarations remotely.*

6) **ePrescription.** *A secure digital way to fill or refill prescriptions anywhere in Europe.*

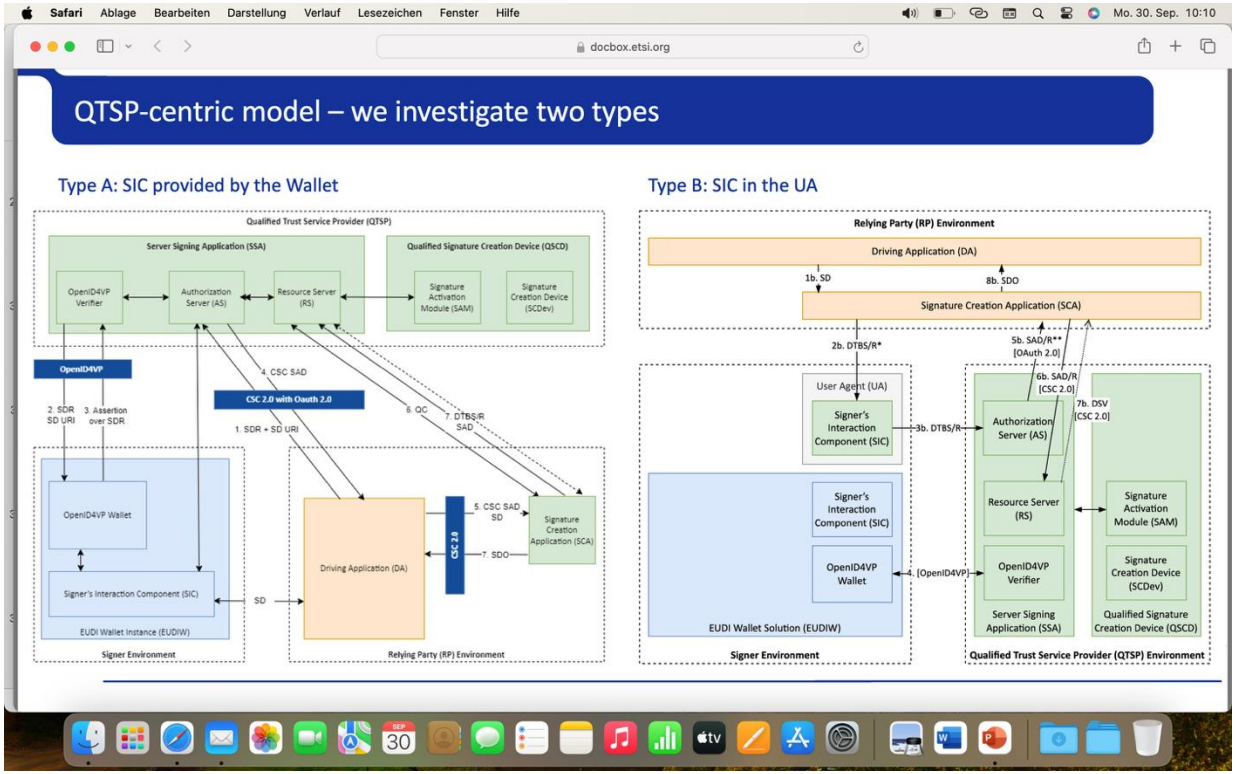
Source: https://www.digital-identity-wallet.eu/6-use-cases/ [Accessed: 6.10.2025]

WALLET-CENTRIC MODEL
TAKEN FROM ETSI WORKSHOP ONLINE[1] 11/09/2024



[1] https://docbox.etsi.org/esi/Open/workshops/202409_CEN_ETSI_Workshop/DAY2-6%20Signing%20%26%20the%20Wallet/DAY2-6-66%202024-09-11%20ETSI%20LSP%20QES%20v2%20Herbert%20Leitold.pdf [Accessed: 29.9.2024]

QTSP-CENTRIC WALLET MODEL
TAKEN FROM ETSI WORKSHOP ONLINE[1] 11/09/2024



[1] https://docbox.etsi.org/esi/Open/workshops/202409_CEN_ETSI_Workshop/DAY2-6%20Signing%20%26%20the%20Wallet/DAY2-6-66%202024-09-11%20ETSI%20LSP%20QES%20v2%20Herbert%20Leitold.pdf [Accessed: 29.9.2024]

ASSURANCE OF HSM-SECURITY FUNCTIONS

ASSURANCE LEVEL AND STRENGTHS OF MECHANISMS
NIST FIPS 140-2 VALIDATION CERTIFICATE (NIST and CSEC)

Consolidated Validation Certificate


FIPS 140-2 Consolidated Validation Certificate

August 2018

Image Source: NIST[1]

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
[…]	[…]	[…]	[…]	[…]
3268	08/24/2018	SafeNet PCIe Hardware Security Module and SafeNet PCIe Hardware Security Module for SafeNet Network HSM	Gemalto	Hardware Version: VBD-05-01 00 [1, 2], VBD-05-0 101 [1, 2], VBD-05-0102 [1, 2) and VBD-05-0103 [1,2]; Firmware Version: 6.24.6 [1] and 6.24.7 [2]

NIST FIPS 140-3 (i.e., the Successor of NIST FIPS 140-2) was Published 03-2019 | 104-3 Effective since 09-2019 | 140-3 Testing begins in 09-2020

ASSURANCE LEVEL AND STRENGTHS OF MECHANISMS
COMMON CRITERIA EAL4+ | SELECTED EXAMPLE

Common Criteria Certificate


Certificato n. 1/16
Prodotto: nShield HSM Family v11.72.02
Sviluppato da: Thales e-Security Ltd.
EAL4+
(AVA_VAN.5)

Image Source: OCSI

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
[…]	[…]	[…]	[…]	[…]
1/16	03/10/2016	nShield HSM Family v11.72.02	Thales e-Security Ltd.	firmware version 2.55.1

Extending a Standard EAL Package with e.g., AVA_VAN.5 is denoted by EAL4+ | '+'

7 ASSURANCE LEVELS ASSIGNED TO GRADE TESTING
EAL4+ WITH ADDED ASSURANCE REQUIREMENTS

Assurance Level	TOE Assurance | Explanation
EAL 1	Functionally Tested
EAL 2	Structurally Tested
EAL 3	Methodically Tested and Checked
EAL 4	Methodically Designed, Tested and Reviewed
EAL 5	Semi-Formally Designed and Tested
EAL 6	Semi-Formally Verified Design and Tested
EAL 7	Formally Verified Design and Tested

Degree of Assurance: - +

EAL 2 / EAL 4 often used for products

EAL 5 – EAL 7 require formal methods

A Higher EAL Does Not Necessarily Imply More Security

CRYPTOGRAPHIC TECHNIQUES AND PARAMETERS

NIST FIPS 140-2 | CRYPTOGRAPHIC TECHNIQUES
SUPPORTED CRYPTOGRAPHY BY CERTIFIED HSMS

- Symmetric key algorithms *(AES, EES)*
- Asymmetric key algorithms *(DSA, ECDSA, RSA)*
- Message authentication methods *(CBC-MAC, CCMP, GMAC, HMAC)*
- Hash functions *(SHA-224, SHA-256, SHA-384, SHA-512)*
- Random number generators *(RNG for DSA/ECDSA/RSA)*
- Deterministic random bit generators *(DRBG w.r.t. NIST SP 800-90A Revision 1)*
- Key management *(KAS ECC w.r.t. NIST SP 800-56A Revision 3)*

Why Might One Choose ECDSA Over RSA in Practical Applications?

CRYPTOGRAPHIC ALGORITHMS AND PARAMETERS
SELECTED EXAMPLES OF DIGITAL SIGNATURE SYSTEMS

Asymmetric Cryptography

- RSASSA-PKCS1-v1_5 or RSASSA-PSS[1] and modulus lengths 4096 bits
- RSASSA-PSS *(FIPS PUB 186-4 and RFC 8017)* key lengths 3072 and 4096 Bit
- ECDSA pursuant to FIPS PUB 186-4 with curve P-256 and length of parameters p, q of 256-Bit
- ECDSA with curves *(NIST FIPS PUB 186-4)* P-256, P-384, P-521, K-283, B-283, K-409, B-409, K-571, B-571
- ECDSA with SHA-256, SHA-384 or SHA-512 *(FIPS PUB 186-4)* key length 256, 384 and 512 Bit

Hash Value Computation

- SHA-256 *(e.g., pursuant to ISO/IEC 10118-3)*
- SHA-256, SHA-384 and SHA-512 *(FIPS 180-4)*

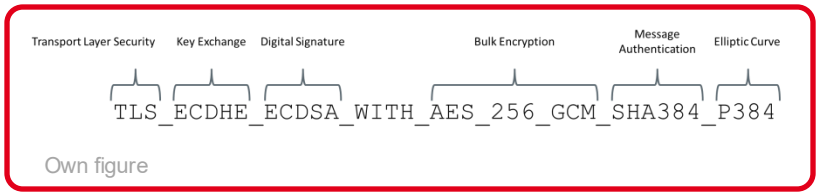
Validate applied techniques and corresponding parameters accordingly (e.g., ECCG ACM or BSI TR-02102-1)

[1] Newer, improved scheme than old scheme to dealing with digital signatures.

TRANSPORT LAYER SECURITY
TLS CIPHER SUITES | EXTRACTED EXAMPLES

Examples for applied TLS 1.2 Cipher Suites – but legacy with ECCG ACM[1]

```
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
```



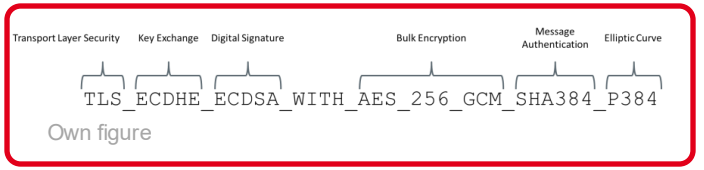
Own figure

Legacy → 31.12.2025
As well legacy → **RSA with 2k keys** → 31.12.2025 (ECCG ACM confirmed SOG-IS)
Legacy → 31.12.2031 (currently, this can change)

[1] ECCG ACM retrievable via: https://certification.enisa.europa.eu/document/download/a845662b-aee0-484e-9191-890c4cfa7aaa_en?filename=ECCG%20Agreed%20Cryptographic%20Mechanisms%20version%202.pdf [Accessed: 6.10.2025]

5 TLS 1.3[1] AEAD CIPHER SUITES
PARTICULAR EXAMPLES | recap

- TLS_AES[1]_256_GCM[2]_SHA384
- TLS_CHACHA20[3]_POLY1305[5]_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256



Own figure

TLS 1.3 (i.e., the TLS 1.2 Successor) was Published as RFC 8446[6] in 08-2018

[1] AES – Advanced Encryption Standard
[2] GCM – Galois Counter Mode
[3] CHACHA20 – A 256 bit 20 round Stream cipher and a variant of Salsa20 where ChaCha is the family of stream ciphers
[4] BEAST – Browser Exploit Against SSL/TLS
[5] CRIME – Compression Ratio Info-leak Made Easy
[1] cf. IETF, RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3, August 2018

Hence a Transition to TLSv1.3 is not a bad idea

OPERATING CONDITIONS FOR QSCDS

OPERATING CONDITIONS FOR QSCDS
SELECTED EXAMPLES | DEFINED VENDOR-SPECIFICALLY

- The **QSCD** must be **operated** by a **qualified trust service provider under** the **eIDAS** regulation
- The qualified trust service provider must **operate** the **QSCD** in a **protected environment**
- **Restrict** the **physical access to** the **QSCD**
- **Protection against** the possibility of **attacks** based on compromising electromagnetic radiation
- **Equivalent** high level of **protection** for **all sub-components** *(including components used for security purposes)*
- **Employees** holding trusted roles shall meet the personnel **requirements** defined in **ETSI EN 319 401**
- **Physical** and **IT security** used to host and operate the QSCD components shall be compliant with **ETSI EN 319 401**
- **HSMs** must be **initialised** and **operated** according to their **FIPS 140-2 level 3** or **Common Criteria EAL4+ certification**
- […]

The Validity Until Further Notice of an Issued QSCD Certificate is Bound to the Operating Conditions and Other Limitations

Agenda

Introduction

eIDAS & eIDAS2 – General Overview

Remote Signature/Seal Solutions and EUDI-Wallets

Practical Every-day Experiences from eIDAS Certifications

Summary

EXPERIENCES FROM EUDIW DEVELOPMENTS
CONSOLIDATED OBSERVATIONS FROM PRACTICE

- **Increasingly used** remote signature solutions in the market *(eIDAS/eIDAS2)*
- **Observed higher dynamics** in the **technology environment** for remote-QSCDs than for Smartcards
- **Pushback** effect **of** both **SMS-OTP** and **AppQR**[2] triggered by increasing Biometric Authentication via App *(i.e., AppBiometric)*
- Remote QSCDs operated by QTSPs, or organizations that fulfill the requirements of a QTSP are a main pillar for EUDIW

[1] SMS-OTP – Short Message Service One-Time-Password
[2] AppQR – Application Quick Response *(Code)*

EXPERIENCES FROM EUDIW DEVELOPMENTS | cont'd
CONSOLIDATED OBSERVATIONS FROM PRACTICE

- **Similar principle** for certified QSCD-solutions
  (e.g., certified HSMs apply cryptographic operations to perform critical signature creation)
- **Differences in the environments** *(e.g., HSM-environment)* for certified remote-QSCDs and QTSP environments
- **SCD[1]** are **protected** by **hardware elements** in **practice**
- **Sole control** for the signatory via **multi-factor authentication** *(e.g., biometric, knowledge, possession)* **Examples:** FaceID/TouchID, Passphrase, Device-Possession
- Selected **corporations[2]** obtained **certifications** for **remote-QSCDs**
  A-Trust *(AT)*, DocuSign *(FR)*, Entrust *(CA/ES - Safelayer)*, Intesi *(IT)*, LuxTrust *(LU)*, Monet+ *(CZ)*, PrimeSign *(AT)*, Swisscom *(CH),* Ubiqu *(NL)*, Ivnosys *(ES),* Thales *(US/CA)* and others

[1] SCD – Signature Creation Data
[2] Retrievable: https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds [Accessed: 2024-09-29]

Agenda

Introduction

Fundamental Principles of Remote Signature Solutions

Requirements and Technical Architecture to Operate QSCDs

Practical Every-day Experiences from eIDAS Certifications

Summary

SUMMARY
COVERED TOPICS

- **Clarified** basic **terminology** and **requirements** under the **eIDAS2** regulation
- **Clarified** requirements derived from **NIS2 Directive**
- **Explored security requirements** under the applicable law
- **Presented** the basic **technical architecture** of **EUDIW**
- **Presented** the basic **technical architecture** of remote **QSCDs**
- **Identified Cryptographic algorithms**, corresponding **parameters** and **strengths of mechanisms** that are applied for **EUDIW operations**
- **Extracted** concrete **examples** of **hardware modules** that **perform cryptographic operations** in **tamper-resistant environments**
- **Derived** vendor-specific **operating conditions** for trust service providers
- **Discussed experiences** from conducted projects