

An auditor's view of...



eIDAS and their certification

INTRODUCTION

- e-WALLET
- Qualified Trust Services revised / new
- eIDAS 2 and audit
- eIDAS 2 and standards
- eIDAS 2 and where with him...

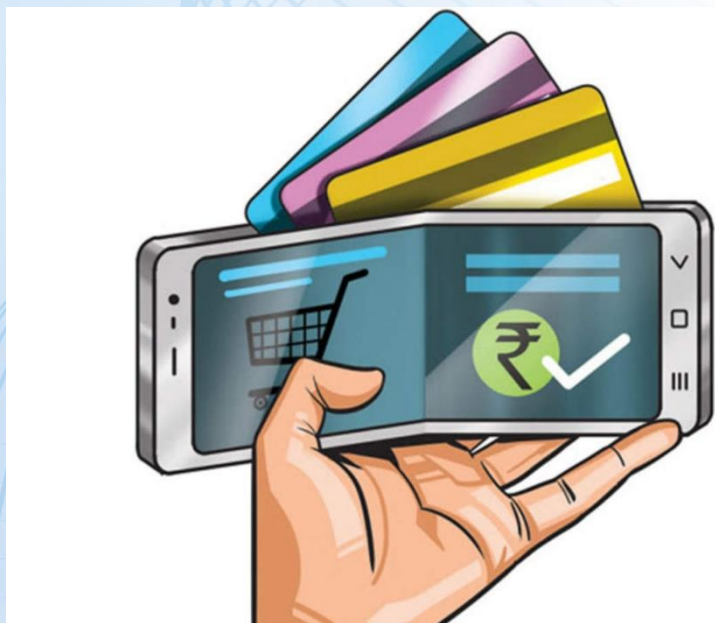


EUDIW (eWallet)



- A means of electronic identification.
- Possibility of use also during attendance control.
- The user decides which data to provide about himself.
- State obligation to ensure the issuance of at least one EUDIW.
- Users may/may not use a wallet.
- Use for public / private sector.
- Harmonized approach.

NEED to KNOW for e-WALLET



NEW SERVICE

- ATTRIBUTES - claims based on personal identification data and confirmation of required attributes.
 - Generation of pseudonyms.
 - "Peer to peer" communication between two wallets of different users.
 - User access to data on completed transactions via the dashboard in the wallet.
 - The user should be able to ask the relying party to delete personal data according to the GDPR.
 - The user should be able to report the relying party to the Office for Personal Data Protection if they receive an allegedly illegal or suspicious request for data.
-
- Assumption of issuance of implementing acts by the end of 2024
 - The obligation to have the service in place by the end of 2026

Qualified Trust Services



- The existing types of trust services have been retained.
- New types defined:
 - issuing electronic confirmations of attributes,
 - management of means for creating remote, electronic signatures or means for creating remote electronic seals,
 - electronic archiving service,
 - electronic record book ("electronic ledger").
- Obligation for internet browser providers to recognize "QWACs" (Qualified Website Authentication Certificates) in order to display the identity of the website owner in a user-friendly manner.

Scope of Trust Services

What will be changed

- Information security – EU directive NIS2
- Improving QTS interoperability through the adoption of Implementing Acts (IA).
- Limitation of the validity of the QSCD certification of means for 5 years with regular vulnerability assessment.



Existing types of trust services



- Issuing certificates for electronic signatures, certificates for electronic seals, certificates for authenticating websites or certificates for the provision of other trust services
- Verifying the validity of certificates for electronic signatures and seals
- Issuing electronic time stamps
- Long term preservation service
- Trust delivery service (e-mail, files)
- Remote sign and seal (not qualified service)

What is new for Qualified electronic signature

- Creating a qualified electronic signature for natural persons free of charge.
- Member States can take appropriate measures so that free qualified electronic signatures for natural persons were used for non-professional purposes.



NEW set of Qualified Trust Services



- Issuing electronic confirmations of attributes
- Verifying the validity of the electronic confirmation of attributes
- Electronic archiving of electronic data and electronic documents
- Recording electronic data in an electronic record book

Revised Article 15

*Accessibility for people with disabilities
and special needs*



New obligation to comply with the United Nations Convention on the Rights of Persons with Disabilities and with the accessibility requirements contained in Directive (EU) 2019/882

Article 20 - NEW rules

Oversight of qualified trust service providers



Paragraph 1

- Qualified trust-building service providers shall be audited by a conformity assessment body at their own expense at least once every 24 months. The audit shall confirm that qualified trust-building service providers and the qualified trust-building services provided by them meet the requirements set out in this Regulation and Article 21 of Directive (EU) 2022/2555 (NIS 2 - Measures to manage cyber security risks).
- Qualified trust-building service providers shall submit the final compliance assessment report to the supervisory authority within three working days of its receipt.

Article 20 - NEW rules

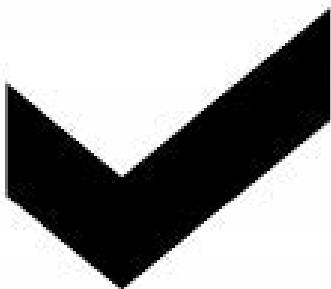
Oversight of qualified trust service providers



Paragraph 1a

Qualified trust service providers **shall inform the supervisory authority** of planned audits **at least one month** in advance and, upon request, shall allow the supervisory authority to participate as an observer.

Milestones for auditing



- 24 months from the date of entry into force of this amended Regulation, the Commission shall assess whether it is necessary to adopt implementing acts establishing a list of reference standards and, where appropriate, establishing specifications and procedures for guaranteed trust services
- 12 months after the date of entry into force of this amending Regulation, the Commission shall establish, by means of implementing acts, a list of reference standards and, where necessary, specifications and procedures for qualified trust services

Sign and Seal

What is still valid

eIDAS Art. 25 paragraph 2

A qualified electronic signature has the same legal effect as a handwritten signature.

Annex I

j) Qualified certificates for electronic signatures shall contain an appropriate note (at least in a form suitable for automatic processing) if data for creating electronic signatures associated with data for verifying the validity of electronic signatures are contained in a qualified means for creating electronic signatures (QSCD).

A handwritten signature in black ink on a white background. The signature is cursive and appears to read "P. Smith". It features a large, looped initial "P" and a long, sweeping underline.

Standards for creation Sign and Seal remotely



SAM modul Protection Profile

- CEN EN 419 241: Trustworthy Systems Supporting Server Signing
 - Signature activation system with SCAL1
 - Signature activation system with SCAL2

Trust service

- ETSI TS 119 431-1 - TSP service components operating a remote QSCD / SCDev
- ETSI TS 119 431-2 - TSP service components supporting AdES digital signature creation
- ETSI TS 119 432 - Protocols for remote digital signature creation
- Cloud Signature Consortium (CSC) specification

Remote Sign and Remote Seal

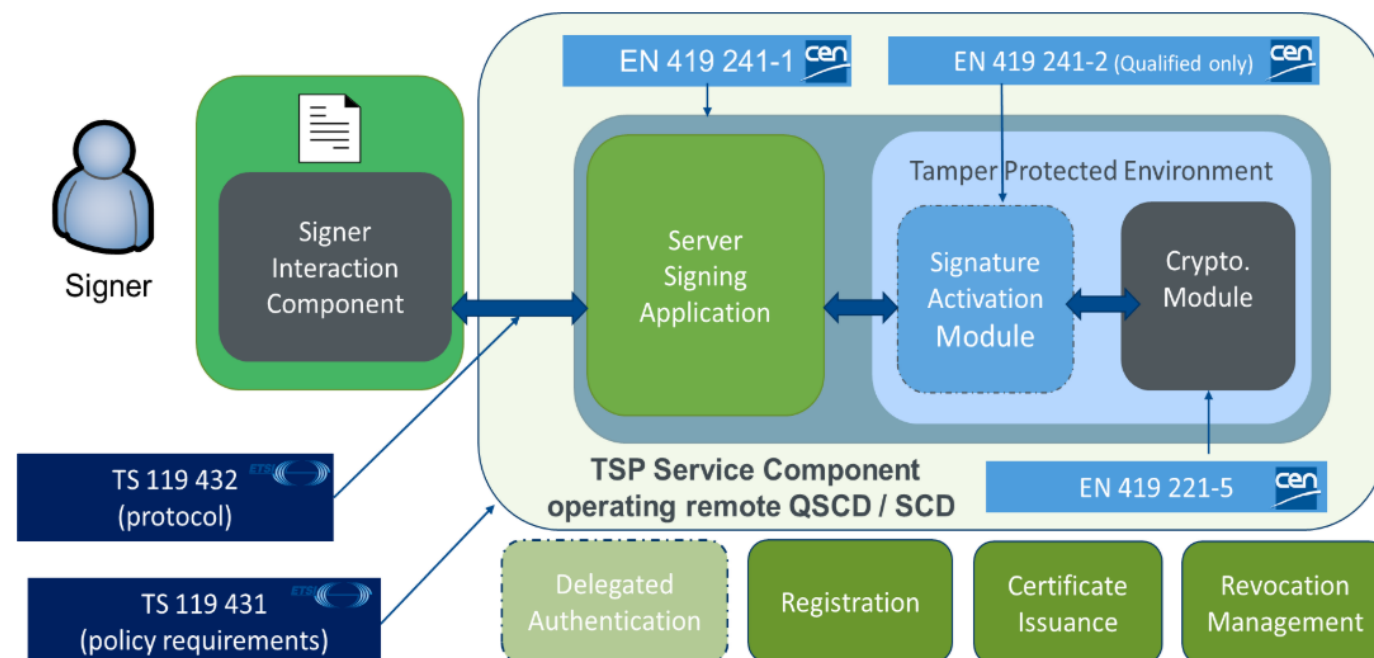
management of means for creating electronic signatures or seals remotely

3 SSASC Policies:

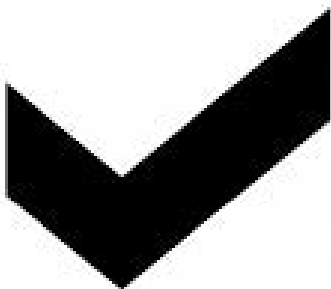
LSCP: Lightweight SSASC Policy (less demanding than NSCP, linked to SCAL1)

NSCP: Normalized SSASC Policy (general recognized best practice, linked to SCAL2)

EUSCP: EU SSASC Policy (linked to eIDAS regulation with specific requirements to QSCD management)



Links / Sources



- European Commission website on EUDIW:
<https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home>
- Github for the EUDIW prototype:
<https://github.com/eu-digital-identity-wallet>
- European Digital Identity – Questions and Answers:
https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_2664
- Council press release on the adoption of eIDAS2 at the Council meeting on 26 March 2024:
<https://www.consilium.europa.eu/en/press/press-releases/2024/03/26/european-digital-identity-eid-council-adopts-legal-framework-on-a-secure-and-trustworthy-digital-wallet-for-all-europeans/>
- Text approved by the Council:
<https://data.consilium.europa.eu/doc/document/PE-68-2023-REV-1/cs/pdf>

Thank you for your attention



Ing. Ivan Seyček
Ivan.Seycek@relsie.cz

Ing. Martin Dudek
Martin.Dudek@relsie.cz