RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

AUTOMATIZATION OF QWAC ISSUANCE

ANDREA RÖCK – ANSSI – FR

Plan

Challenges for automatization of QWACS issuance

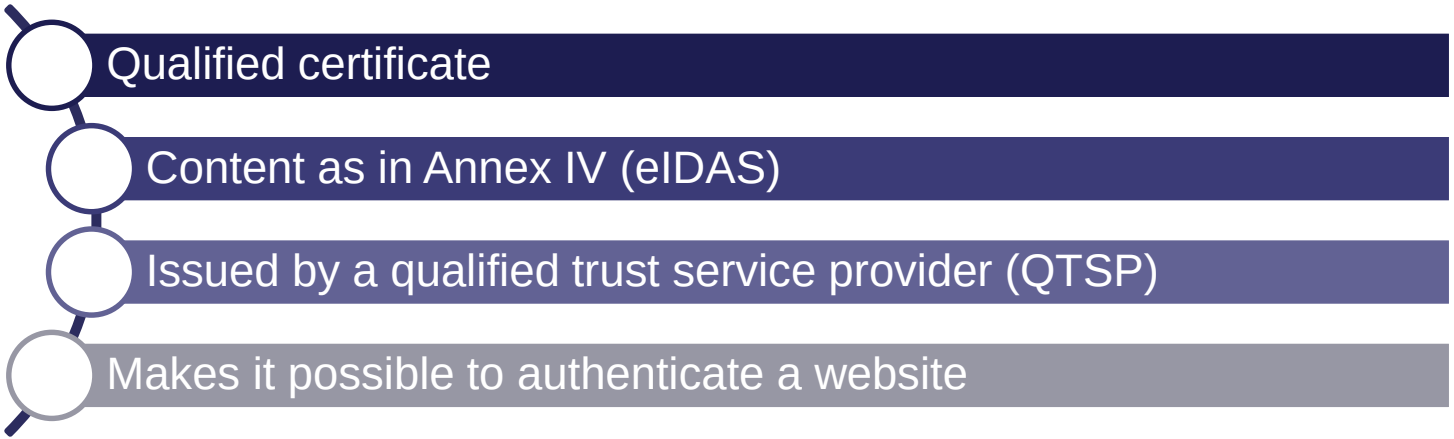
Possible approach for automatization

CHALLENGES FOR AUTOMATIZATION OF QWACS ISSUANCE

Qualified Website Authentication Certificates

As defined in Regulation (EU) No 910/2014* (eIDAS)

Goal: provide the identity of the legal / natural person behind a website



*Amended by Regulation (EU) 2024/1183 (eIDASv2) and Directive (EU) 2022/2555 (NIS2)

Qualified certificate

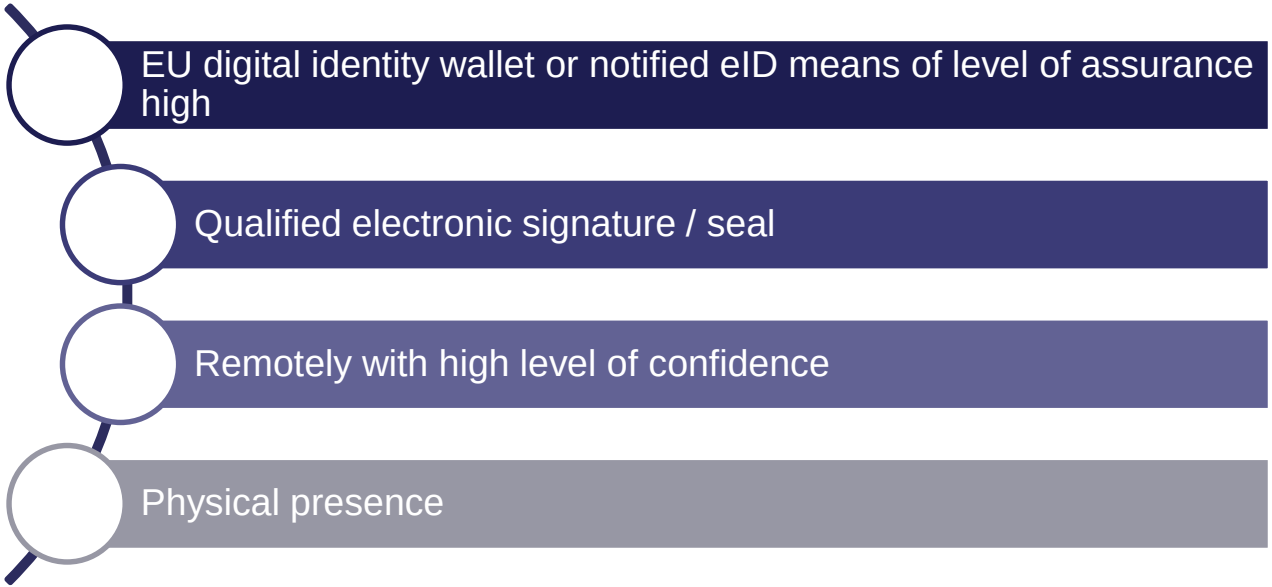
Identity verification (article 24.1a): “complete certainty” about identity for each certificate issuance

Revocation within 24h (article 24.3)

Provide revocation information (article 24.4):

- at least on a per certificate basis
- at any time and beyond the validity period of the certificate
- in an automated manner that is reliable, free of charge and efficient

Identity verification (article 24.1a)



Content as in Annex IV (eIDAS)

- Machine readable indicator of being a QWAC
- ID of QTSP (CA)
- If natural person owner: name or pseudonym
- If legal person owner: name and registration number
- Elements of the address (at least city and state)
- Domain names
- Beginning / end date
- Unique certificate identity code
- Signature of the CA
- Link to CA certificate
- Information or location certificate validity status service

Issued by qualified trust service provider (QTSP)

- Audited at least every 24 month by a conformity assessment body (ETSI EN 319 403-1)
- Qualified status delivered by **supervisory body of the member state** in which the QTSP is established
- Qualification status published in national **trusted list** and referenced by EU list of trusted lists (eIDAS Dashboard)
- Requirements for essential entities of **NIS 2** (Directive (EU) 2022/2555) and specific implementing act (CIR (EU) 2024/2690)
- Recognized within EU as begin qualified

Makes it possible to authenticate a website

Automatization

Aligned with IVC, OVC (BRG) or EVC (EVCG) requirements (1-QWAC)

Linked to a TSL certificate (2-QWAC) (ETSI TS 119 411-05)

Not needed to be recognized by browsers (QCP-w-gen in ETSI EN 319 411-2, for example for PSD2 as described in ETSI TS 119 495)

Problem

How to combine automated issuance with high confidence in the identity at each issuance of the certificate?

POSSIBLE APPROACH FOR AUTOMATIZATION

Two documents

- Automatisation de la gestion des certificats avec ACME | ANSSI (French) (2025-01-24)
  - Recommendations for the issuance of certificates with ACME
  - Reduce risks introduced by larger exposure of the CA by adding an ACME server and increasing attack vector on the user side based on adding the ACME client
  - For French public authorities, also requirements for ACME client
- FESA Position Paper on QWACs-final.pdf (2024-09-24)
  - Forum of European Supervisory Authorities for trust service providers
  - Specific to QWACs
  - Formulation more general, with ACME only as example

How to achieve high level of confidence in the identity?

- Verify the identity and put it in an external ACME account
- Cryptographic binding between the ACME client and the external account
- Fixed parameters of certificates in the external account, like list of possible domains
- Any changes or access to the external account via strong, multifactor authentication

Main steps

- Step 1 – Initial certificate application (agree to ToR, select parameters)
- Step 2 – Initial verification process (verify attributes to be put into certificate, at least identity)
- Step 3 – Creation of external account (multifactor authentication to access to the account, fix list of domain names, create binding material)
- Step 4 – Creation of ACME account and linking to external account (bound to exactly one external account)
- Step 5 – Request certificates in automated manner

Requirements on the external account

- Linked to at least one human operator
- Strong multifactor authentication for creation and any changes in the external account
- External account contains at least following parameters
  - Identity information and attributes to be put into the certificate
  - List of (sub-)domains for which certificates can be issued
  - Lifetime of eternal account
  - Associated ACME accounts
  - Binding material (KeyID and MAC key)
- Verification of identity / attributes conformant to eIDAS article 24.1a/1b
- Initial list of domain names include action of a human operator

Requirements on ACME account + binding material

ACME account

- Linked to exactly one external account
- May be possible to suspend an ACME account
- Shall allow renewal of key-pair

Binding material

- Trusted cryptographic algorithms and key generator
- Created by CA
- Protect integrity and confidentiality of the binding material

Automatization protocol

- Only accept requests for (sub-)domains that are listed in the external account
- Use multipoint validation
- Set limited number of failed domain validations
- Set limit for number of certificate requests per IP address
- Set limit for number of certificate requests per domain

Certificate authority

- Dedicated intermediate CA for automatization
- Infrastructure (ACME server, registration service, database) at least logical separated from non automated services
- Allowed domain validation challenges: HTTP-01, DNS-01 or TLS-APLN-01
- Availability of a report of the different actions linked to the external account, like number of certificates created, revoked, currently valid, list of accepted domains
- Provide possibility of testing the automated solution

What happens in case of compromise

- Compromise of external account
  - Check linked ACME account and renew them if needed
- Compromise of ACME account
  - Check generated certificates and revoke if needed
- Considers case of suspension

French proposal – ACME client requirements

- Limit privileges of ACME client
- Protection of the binding material

ANY QUESTIONS?