FESA

FORUM OF EUROPEAN SUPERVISORY AUTHORITIES
FOR TRUST SERVICE PROVIDERS

Heraklion, 24 September 2024

Position Paper
On qualified website authentication certificates (QWACs)

The Forum of European Supervisory Authorities (FESA) for trust service providers is open to national bodies responsible for supervision and/or trusted lists in accordance with the eIDAS Regulation[1].

Supporting the idea of the Digital Agenda for Europe, FESA sees itself as an experienced and competent body that supports cooperation, information sharing and assistance among its members, and facilitates the exchange of views and agreement on good practices corresponding to Arts.46a(4) (a), (c) and Art.46d(1) of the eIDAS Regulation.

FESA intends to advance the harmonization of supervisory bodies' activities, to develop common points of view for dialog with political or technical institutions, in particular the European Commission and standardization institutions, and to establish a level European playing field for trust service providers in terms of supervision and enforcement.

Background and Objectives

Regulation (EU) 910/2014 (eIDAS) introduces the term ‘qualified certificate for website authentication’, informally referred to as a qualified website authentication certificate (QWAC). The goal of this type of certificate is to authenticate a website and to link the website to the natural or legal person to whom the certificate is issued. In addition, this type of certificate is a qualified certificate and as such is subject to the requirements of article 24 regarding the identity and attribute verification for qualified certificates.

Regulation (EU) 2024/1183[2] amending Regulation (EU) No 910/2014 (eIDASv2) introduces several changes that are relevant to QWACs. Specifically, web-browsers are required to recognise QWACs, and qualified trust service providers (QTSPs) have to ensure with complete certainty the identity of the natural or legal person to whom a qualified certificate is issued before the issuance of the certificate.

QWACs are usually issued by QTSPs as TLS certificates that respect both the requirements of the eIDAS Regulation and the requirements set out by the web-browsers individually, and in the CAB Forum baseline requirements. Currently, to enhance security, consideration is being given by the browsers to reduce the lifetime of TLS certificates and to use protocols like ACME[3] to automatize the issuance of TLS certificates. These considerations are thus applicable for QWACs. In addition to the reduced lifetime and automatization of the certificate issuance, other changes to aspects of certificate management provided for in the baseline requirements should be considered, such as the period during which the validation of an applicant’s control over a domain name can be re-used, and the time during which the validation of an applicant’s identity can be re-used.

[1] Regulation 910/2014/EU of the European Parliament and Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, OJ L257.

[2] 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, OJ L, 2024/1183, 30.4.2024

[3] RFC 8555: Automatic Certificate Management Environment (ACME)

The primary objective of this paper is to explore how viable solutions could be implemented that would allow for the issuance of certificates that respect the requirements of browsers on the automatization and reduced lifetimes, and which still respect the requirements for qualified certificates as laid down in the eIDAS regulation. This document does not replace the general requirements set out by CAB forum, ETSI ESI or the root stores. It adds additional requirements for linking the identity to the QWAC.

The issuance of a QWAC involves the following steps, that are undertaken for the issuance of any type of qualified certificate:

1. The subscriber signs a legal agreement with the CA and accepts the terms and conditions.
2. The subscriber applies for the issuance of the certificate.
3. The CA makes sure that it has complete certainty[4] on the identity and any attributes of the qualified certificate.
4. A key pair is created for which a certificate is requested
5. The certificate is issued with a specific lifetime (notBefore / notAfter date).

The following section describes a possible way of automatizing the issuing of a QWAC using an automated process.

NOTE: The present document describes one way of automatizing the issuance of QWACs, other alternatives might exist as well.

The usage of the ACME protocol using External Account Binding is provided as an example. Any other protocol, e.g. a CA specific one, might be used as well as long as it supports all the needed functionalities. Any descriptions specific to ACME are covered after [ACME]. In addition, the table below shows the general terms and ACME specific terms used.

General term	ACME specific term
External administration account	External account
Certificate request account	ACME account
Certificate request client	ACME client
Certificate issuing server	ACME server
Binding elements	key identifier and hash MAC

Step 1 – Initial certificate application: The subscriber subscribes to the CA and agrees to the terms and conditions. It also selects specific parameters, e.g. the domains for which certificates are requested to be issued, what type of challenges are accepted, etc.

Step 2 – Initial verification process:
The CA verifies the attributes to be put into the certificate. This covers at least the identity of the subject (legal or natural person). It can also cover checks on the ownership of the domain in addition to the verification during the challenges in step 5. See ETSI EN 319 411-2. Note, in general verifications done here are only valid for a limited amount of time.

Step 3 – Creation of external administration account:
The CA creates an external administration account for the subscriber, links this account to the subscriber and the specific parameters agreed in Step 1 and the elements verified in Step 2. The CA provides multi-factor authentication for the subscriber to connect to this account and a way to link the certificate request client to the external administration account. The subscriber designates one or more “human operator(s) of the administration account.” which are natural persons that have the right to access the administration account via the strong authentication factors.
[ACME] The CA creates an external account for the subscriber. The access to this account is protected by strong authentication means to ensure the sole control of the subscriber over external account. The CA creates a MAC key and a key identifier which is used to link an ACME client account to the external account. The external account contains the parameters, for example which certificates can be issued

[4] See Regulation (EU) 1183/2024 recital (74)

under this external account, the lifetime of the external account, etc. For more details see the section on requirements.

Step 4 – Creation of certification request account(s) and linking to external administration account:
The subscriber creates one or more certificate request account(s) and links them to the external administration account. The certificate request accounts are able to uniquely identify themselves and show that they are linked to the external administration account. The certificate request accounts contain all needed configurations to request a certificate, like the URL where to connect or the type of certificate to request. The configuration needs to be aligned with the configurations of the external administration account.
[ACME] One or more ACME accounts are created. Each of them has a public / private key pair that allows it to sign any message to the ACME server, and thus guarantee that origin of the message. The ACME accounts are linked to the external account by sending a message to the ACME server with a payload containing the key identifier that is protected by the MAC key linked to the external account, and at the same time signed by the private key of the ACME account.

Step 5 – Requesting a certificate:
The certificate request client will generate the key pair for the certificate signing request (CSR). It initiates the certificate creation process, where messages are signed by the private key of the certificate request client. The CA provides challenges for the client to prove the ownership of the domain. For example, a challenge might be based on the positioning of a specific resource on the server under the domain name or the adding of a specific TXT record in the DNS zone of the target domain.[5] Only when these challenges are replied correctly, the CSR is sent from the client to the CA. The CA verifies that the information in the certificate matches the details in the external administration account. Only if this is correct the CA issues the certificate to the client.
[ACME] The ACME client sends a request to the ACME server, responds to the challenges for all the requested domains correctly and sends the CSR. The ACME server provides the certificate.

NOTE: Complete certainty about the elements contained in the certificate is guaranteed by:

- The challenge/response regarding the control of the domain
- The cryptographic key of the certificate request client
- The link between the certificate request client and the user account
- The fixed parameters in the user account and the access to the user account via strong authentication.

It is thus important to carefully protect these elements like access to the external administration account, or any cryptographic material.

Requirements – external administration account

EAA.1: An external administration account shall be created to be used in the automated certificate issuance process.
EAA.2: The external administration account shall be linked to at least one human operator(s) of the administration account.
EAA.3: The CA shall verify the identity of the operator and that he is mandated by the subscriber to operate the administration account and that he is aware of all linked responsibilities. This verification shall be done with the same level of assurance as the verification done for EAA.6.
EAA.4: In case the certificate is issued to a natural person, the operator shall be the same natural person.
EAA.5: The access to the external administration account shall be protected by multi-factor authentication.

[5] See for example clauses 3.2.4.7, 3.2.2.4.19 and 3.2.2.4.20 of Baseline Requirements for TLS Server Certificates | CA/Browser Forum (cabforum.org)

EAA.6: The multi-factor authentication shall at least include two factors from different families of factors (what you have, what you know, what you are) achieving sufficient assurance.
EAA.7: The CA shall do a risk analysis on the multi-factor authentication to evaluate if it achieves sufficient assurance.

EXAMPLE 1: A password together with sending an OTP via SMS is not sufficient however a password together with a robust cryptographic protocol as OTP (HOTP or TOTP for example), FIDO2 or FIDO U2F, or certificate authentication (with certificate stored in smartcard) is suitable.

EXAMPLE 2: The requirements listed in Commission Implementation Regulation (EU) 2015/1502[6] for electronic identification means of level substantial or high can provide suggestions on multi-factor authentication.

EAA.8: The parameters fixed in the external administration account shall at least contain:

a) The list of domains for which certificates can be issued.
b) The lifetime of the external administration account,
c) The list of associated certificate request accounts and their status (valid, suspended, deactivated),
d) The list of binding information ([ACME] KeyID and MAC keys) sets. For each of them
    1. A human readable identifier
    2. The creation time
    3. The expiration time
    4. The revocation time, if applicable (stating when it cannot be used any more)
e) The identity information and attributes to be put into the certificates.

EAA.9: The verification of all information to be put into the certificate shall be done conformant to article 24.1a and 24.1b of eIDASv2 and the relevant CABF standard, where applicable. See ETSI EN 319 411-2 for guidance.
EAA.10: Changes of the parameters in the external administration account shall only be possible after using the multi-factor authentication or methods accepted in EAA.6.
EAA.11: Any changes of the parameters that imply changes in the content of the certificate shall be verified in the same way as was done when setting these values (see EAA.6 and EAA.9).
EAA.12: The content of the list of authorised domains shall be validated by a human operator prior to setting them in the external administration account. Automatic controls may be in place, but shall be validated in the end by an employee of the CA.
EAA.13: The verification of the information in the external administration account shall be redone at least every 398 days, in the same way as was done when setting these values (see EAA.6 and EAA.9).
EAA.14: The binding information in the external administration account shall be renewed at least after three validity cycles of the content (3x398 days) or corresponding to the state of the art recommendations of the underlying cryptographic techniques.
EAA.15: It shall be possible to renew the binding elements of the external administration account when requested by the subscriber.
EAA.16: The cryptographic secrets of the binding elements shall be used only for a single external administration account and renewed at the renewal of the external administration account.
EAA.17: In case the binding elements are compromised:

a) The external administration account shall be deactivated, which means all pending requests and new requests (e.g. changing parameters, adding new certificate request accounts) shall be stopped. Only the deactivation of associated certificate request accounts shall be possible.
b) All associated certificate request accounts shall be deactivated.
c) A new external administration account shall be created with new binding elements, based on the requirements of an initial creation.
d) For any suspect certificate request accounts (which might have been created and associated after the compromise):

[6] Implementing regulation - 2015/1502 - EN - EUR-Lex (europa.eu)

i. all issued certificates based on a request of this account shall be revoked before deactivating the account and at least 24 hours after the detection of the compromise,

ii. a new certificate request account shall be created and linked to the new external administration account.

e) Any certificate request account for which compromise is not clear shall be suspended, meaning that until the situation is analysed, no request shall be processed.

i. In case the comprise of the certificate request account was proven, this shall be handled as in the case of suspect certificate request accounts, see point d).

ii. In case it can be shown that it was not compromised, the account can be handled as a non-suspicious account, see point f).

f) For any non-suspicious certificate request account, new certificate request accounts shall be created and be linked to the new external administration account. It is not needed to revoke the issued certificates.

EAA.18: In case there is a suspicion of a compromise of the binding elements the external administration account and all associated certificate request accounts shall be suspended meaning they shall not process any requests, or deactivated. In case the compromise is confirmed, requirements

EAA.19: shall apply. In case it is confirmed that no compromise happened, the external administration account and the associated certificate request accounts shall go back to valid status.

NOTE: If the certificate request accounts were deactivated, the "going back to valid status" includes the recreation of the certificate request accounts.

EAA.20: At the end of the validity period of the external administration account, a new external administration account shall be generated using the procedures of the initial creation, with new binding material. All certificate request accounts linked to the expired external administration account shall be deactivated, and new certificate request accounts shall be linked to the new external administration account.

EAA.21: All requests linked to handling a compromise, suspicion of compromise or renewal of an external administration account shall be authenticated using strong multi-factor authentication.

Requirements – certificate request account

CRA.1: A certificate request account shall be linked to exactly one external administration account. An external administration account may be linked to different certificate request accounts.

CRA.2: It may be possible to suspend a certificate request account meaning that until the situation is analysed, no request shall be processed, for example in case of suspicion of a compromise of the private key of the certificate request account.

CRA.3: In case the private key of the certificate request account is compromise:

a) The certificate request account shall be deactivated

b) At least all certificate requested by this account, starting from the estimated date of compromise, shall be revoked.

c) A new certificate request account shall be created and linked to the external administration account.

d) If necessary, all revoked certificates shall be requested to be reissued.

CRA.4: In case there is a suspicion of a compromise of the private key of the certificate request account, the account shall the suspended, meaning that no request shall be processed, or deactivated. In case the compromise is confirmed, CRA.3 shall be applied. Otherwise, if it was shown that no compromise happened, the status of the certificate request account shall be return to valid status.

NOTE: If the certificate request accounts were deactivated, the "going back to valid status" includes the recreation of the certificate request accounts.

CRA.5: It shall be possible to renew the key-pair of the certificate request account, when requested by the subscriber through the external administration account. This can be done either by a key rollover or by deactivating the certificate request account and creating a new one.

Requirements – binding element

BE.1: The cryptographic algorithms used to create, use, transport or store the binding elements, including random number generation shall be recognized as being fit for this usage.

BE.2: The cryptographic algorithms used to create, use, transport or store the binding elements, including random number generation should correspond to SOG-IS [7]or ETSI TS 119 312[8].
BE.3: The binding elements shall be generated by the CA.
BE.4: The binding elements shall be transmitted to the subscriber in a way that provides confidentiality and integrity.
BE.5: The binding elements shall be stored by the CA in a way that provides confidentiality and integrity.

BE.6: The CA shall inform the subscriber in the terms and conditions that

a) the binding elements shall be stored in a way to provides confidentiality and integrity,
b) about the risk of compromise of the binding elements,
c) about the risk of compromise of certificate request account keys, and
d) about the risk of associating multiple certificate request accounts to a single external administration account, but also the risk of linking a single certification request account to an external administration account.

BE.7: When the binding elements are lost without a compromise, either the CA retransfers the key based on a strong authentication, or a renewal of the external administration account shall be done.

Requirements – automatization protocol

AP.1: The certificate request server shall reject all requests for creation or renewal of a certificate which does not corresponds to the parameters fixed in the external account. Specifically, no request shall be accepted where the domain is not listed in the external account.
AP.2: The certificate request server shall use multi-point validation of the domain challenges. For more details see discussion by the CABF.
AP.3: The certificate request server shall set a limit of attempts to validate the domain challenge for a specific certificate request.

EXAMPLE: Let's Encrypt impose a limit of 5 unsuccessful validations per ACME account

AP.4: The certificate request server shall set a limit on the creation of certificate request accounts per IP address.

EXAMPLE: Let's Encrypt impose a limit of 10 ACME accounts per IP address every three hours.

AP.5: The certificate request server shall set a limit of numbers of duplication for each certificate.

EXAMPLE: Let's Encrypt impose a limit of 5 certificate request per week for each domain.

AP.6: The CA shall verify CAA (Certification Authority Authorization) for the requested domain names(s) in accordance with section 3.2.2.8 of the TLS Baseline Requirements before adding the corresponding domain names in the external administration account and including them in issued certificates.
AP.7: When an exchange uses a specific standard protocol[9], then this shall be correctly implemented.

Requirements – Certificate authority

NOTE: The following requirements should counter the fact that a CA for automated certificate issuance is more exposed to the internet than a CA with no open connection.

CA.1: The automated issuance shall be done by a dedicated intermediate CA only issuing automatic certificates.
CA.2: The infrastructure components used for automated certificate issuance (registration authority, database containing the information of the external accounts, the certificate request server, the intermediate CA) shall be separated at least logically from all other infrastructures used for issuing certificates. This shall include at least:

1. the intermediate CA
2. the certificate issuing server
3. the registration service

[7] https://sogis.eu/uk/supporting_doc_en.html
[8] https://www.etsi.org/standards-search#page=1&search=119%20312
[9] e.g. RFC 8555 ACME

4. the data base

For all other components used, the QTSP shall evaluate, based on a risk analysis, if they need to be separated as well or not. This risk analysis shall take at least into account the additional risk of this service due to its exposure, as well as any risks of attacks on the automated system being exploited to attack any other service including issuance of certificates without automation.

CA.3: All exchanges between the CA, the registration authority and the certificate request server shall be protected to provide confidentiality, integrity and authenticity with state-of-the-art mechanisms.

CA.4: The lifetime of the issued certificates should not be longer than 3 months.

NOTE: Longer lifetimes introduce higher risk for the usage of compromised certificates.

CA.5: The CA shall validate the resolution of the domain challenge for each entry in the `SubjectAlternativeName` entry.

CA.6: The request for revocation of a certificate may be authenticated by the certificate request account who requested the certificate.

CA.7: [ACME] The subscriber shall be allowed to choose one of the following challenges: HTTP-01, DNS-01 or TLS-APLN-01 as profiled in section 3.2.2.4.7, 3.2.2.4.19 and 3.2.2.4.20 of the CAB/F Baseline requirements.

CA.8: The CA shall inform the subscriber of the advantages and disadvantages / risks of the different domain challenges.

EXAMPLE: HTTP challenges are easy to put in place, but the domain name verification is weaker, and an attacker able to put a file on the website might fool this challenge, TLS-APLN is easy to put in place but is not supported by all ACME clients, DNS-01 has a stronger domain name validation, but a wrong configuration might put at risk the whole DNS if the ACME client is compromised.

CA.9: A report of the different action linked to an external administration account shall be made available to the subscriber. This report shall contain at least the number of certificates created, revoked, and currently valid, as well as the current list of accepted domains.

CA.10: The subscriber shall be able to check the current status of its external administration account and the corresponding certificate request clients including current pending actions for each external and certificate request account as well as the number of certificates issued for each certificate request account.

CA.11: A testing service for the automated solution shall be provided.

CA.12: The CA shall inform the subscriber of the risks linked to using an automated service.