Revocations

Guide for Certum's Partners

www.certum.eu

asseco DATA SYSTEMS

Table of Scope

1. What does a Certification Authority do?

The CA (Certification Authority) is an independent entity that issues digital certificates, thus binding a public key to data included in the certificate. Such an association is preceded by proper verification that the applicant has a private key that is compatible with the public key as well as of the correctness of the data that will be included in the certificate. Key compatibility verification is based on cryptography principles. Verification of data is based on clearly established rules, that are considered secure, written down in the Certification Practice Statement [1] of each Certification Authority.

Certum has been a Certification Authority since 1998 and from the very beginning our mission is to ensure that our customers feel secure in the digital world. We have been a member of CA/Browser Forum [2] for years, participating in the development of today's standards for SSL, Code Signing or S/MIME certificates. Annual WebTrust audits [3] confirm that we meet all security requirements, procedures, processes and operations. We are constantly developing and following increasingly stringent security standards regarding both infrastructure and cryptography as well as procedures and verification of data in certificates.

2. Why do SSL certificates work?

One of the most popular certificates issued by Certification Authorities are SSL certificates [4], which form the basis for the security of online communication by ensuring the privacy of data transmitted between servers and web browsers.

Due to the constantly growing number of domains in the world, it is not possible for browsers to know all existing SSL certificates. Instead, the existence of a Trusted Third Party is used, whose functions are performed by Certification Authorities. By adopting such a scheme, the browser only checks whether the SSL certificate was issued by the trusted Certification Authority. The process of gaining browser's trust requires the Certification Authority to meet high security standards and demonstrate compliance with the latest good practices, which is confirmed by a positive result of WebTrust or ETSI audit. Only when the Certification Authority proves that it is trustworthy, certificates it issues become by default trusted by web browsers, and neither the domain owner nor the customer need to configure anything extra for a website using such an SSL certificate to be recognized as secure by Chrome, Edge, Firefox, Opera, Safari and other browsers.

3. How do OV and EV certificates differ from DV?

All SSL certificates ensure the security of data transmission, but SSL certificates also have another task: they are used to verify the identity of domain owner. Each user of the domain can download the certificate and verify the data included in the certificate. The guarantee of the correctness of this data is verification, which is carried out by the Certification Authority before the certificate is issued. The list of permitted methods of verification recognized as secure is defined, in the case of SSL certificates, by records elaborated by CA/Browser Forum, which are adopted to browser policies.

SSL certificates are divided into three categories depending on the complexity of the verification process:

- ✓ Domain-Validated (DV) are certificates that do not provide any information about the entity that owns the domain, because the verification is only about confirming the control over the domain. Such certificates are suitable for private parties, but should not be used by organizations.
- ✓ Organization-Validated (OV) are certificates that provide basic information about the organization that owns the domain.
- ✓ Extended Validation (EV) are certificates that provide extended information to uniquely identify the organization that owns the domain and confirm its credibility.

Thanks to the data in OV and EV certificates, the user can identify the entity that owns the domain and treat this data as reliable information, because it has been meticulously verified by a Trusted Third Party.

4. What if there is an error in the certificate?

Despite the constant efforts to reduce the risk of making mistakes, it may happen that the Certification Authority issues an incorrect certificate. Proper response to such an error is thus essential.

No error in a certificate issued by a Trusted Third Party can be considered insignificant. A typo in the organization's name or an incorrect address can make it impossible to identify the organization unambiguously and reduce customer trust or mislead the customer. In the era of phishing based on small “errors” in data, the care of correct domain and organization identification data is a key element in ensuring customer security.

For this reason, the security standards clearly indicate that in case of any error in the certificate it must be revoked. It is in the interest of both the certificate owner and the Certification Authority to take appropriate steps to revoke the erroneous certificate and replace it with a new one in the shortest time possible.

5. What does the revocation of such a certificate look like?

The Certification Authority, which detects an incorrect issue, or which receives a notification of an incorrect issue, shall immediately inform the owner of the certificate about the situation. The standards for SSL certificates require the certificate to be revoked within 24 hours of notification to the Certification Authority. In particular cases this period may be extended to a maximum of 5 days. The time to revoke an erroneous certificate depends on the scale of the threat, for instance:

- ✓ in case of compromising the private key of a certificate or incorrectly performed domain verification it will be maximum of 24 hours;
- ✓ in case of an incorrect field value in the subject of the certificate, it will be maximum of 5 days.

For a complete list of reasons for revocation with the specified revocation time, please refer to the Certification Practice Statement (item 4.9.1). Exceeding the revocation deadline is unacceptable and may even result in a loss of trust for the Certification Authority.

Revoking a certificate means placing its serial number in the Certificate Revocation List (CRL) and marking it as "revoked" in the OCSP (Online Certificate Status Protocol) database, as a result of which browsers will not recognize it as a trusted one.

For the sake of continuity of security, before revoking the certificate it is recommended to replace it with a new, correct one.

6. How does a new certificate issuance look like?

As soon as Certum receives and confirms the notification of an incorrectly issued certificate, Certum contacts the customer to inform him of this fact. This makes it possible to quickly replace the certificate before it is revoked. In order to ensure the continuity of certificates, it is recommended to prepare a customer service process in case an

incorrect issue is detected. This process should include informing the customer immediately about the situation and quickly enabling him to replace the erroneous certificate with a new, correct one.

Certum allows issuing a new certificate with corrected data in one of two manner, depending on the reason for the revocation:

1. Reissue operation:

- ✓ in case the key is compromised or the certificate structure is incorrect it is possible to use **reissue** operation — the advantage of this method is the lack of additional verifications and automatic issuance of the certificate; the reissue method does not allow changing data

2. Submit new request:

- ✓ in case the key is compromised or the certificate structure is incorrect, it is also possible to **submit new request** — for this method, it is required to repeat the process of domain and data verification for the certificate
- ✓ in case of incorrect data, it is necessary to **submit the new request** with correct data — for this method, it is necessary to repeat the domain and data verification process for the certificate

[1] https://www.certum.eu/en/cert_expertise_practice_statement/

[2] https://cabforum.org/

[3] https://www.support.certum.eu/en/cert-about-us-about-webtrust/

[4] https://www.certum.eu/en/ssl-certificates/

Certification Authority Certum

Asseco Data Systems S.A.

ul. Królowej Korony Polskiej 21
70-486 Szczecin

www.certum.eu