Terms of use for non-qualified certificates

Version: 1.4

Date: 1 September 2025

Status: valid

Asseco Data Systems S.A.

Jana z Kolna Street 11

80-864 Gdańsk

Certum

Bajeczna Street 13

71-838 Szczecin

www.certum.pl

www.certum.eu

Table of Contents

§1. Definitions

1. **Applicant** – a natural person or legal entity that applies on behalf of the Subscriber for (or applies for renewal of) a certificate.
2. **Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates** – document created by the CA/Browser forum and published at http://www.cabforum.org. The document describes the minimum requirements that the Certification Authority (CA) must meet to issue publicly trusted SSL/TLS certificates.
3. **Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates** – document created by the CA/Browser forum and published at http://www.cabforum.org. The document describes requirements that the Certification Authority (CA) must meet to issue publicly trusted Code Signing Certificates.
4. **Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates** – document created by the CA/Browser Forum and published at http://www.cabforum.org. The document describes the requirements that the Certification Authority (CA) must meet to issue publicly trusted S/MIME Certificates.
5. **Certum** – Asseco Data Systems SA's (referred to as ADS) service unit providing non-qualified and qualified certification services. Qualified certification services are provided in accordance with Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579). Non-qualified certification services are provided in accordance with requirements of the AICPA/CICA WebTrust Program for Certification Authorities and Principles and Criteria for Certification Authorities - Extended Validation Audit Criteria.
6. **Certificate** – an electronic attestation signed by Certification Authority which contains at least a name or an identifier of Certification Authority, identifier of Subscriber, his/her/its public key and validity period.
7. **Certificate Request** – An electronic request for the issuance or renewal of a certificate, containing, among other things, the Subscriber's data and the data that constitutes the content of the certificate. The Certificate Request is attached to the Subscriber Agreement and contains data included in the certificate.
8. **Certification Policy** – document which specifies general rules applied by certification authority in public key certification process, defines parties, their obligations and

responsibilities, types of the certificates, identity verification procedures and area of usage. The Certification Policy is published by the Certum at http://www.certum.pl.

9. **Certification Practice Statement** – document describing in details public key certification process, its parties and defining scopes of usage of issued certificates. The Certification Practice Statement is published by the Certum at http://www.certum.pl.
10. **Code Signing Certificates** – certificates issued according to *Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates*. Code Signing Certificates are used for protection of application's code with an electronic signature and designed for developers to protect software against forgery.
11. **EV Code Signing Certificates** – certificates issued according to *Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates*. Code Signing Certificates are used for protection of application's code with an electronic signature and designed for developers to protect software against forgery.
12. **Guidelines for the issuance and management of extended validation certificates ("EV Guidelines")** – document created by the CA/Browser forum and published a http://www.cabforum.org. The EV Guidelines describe requirements that a Certificate Authorities must meet to issue EV SSL certificates.
13. **Premium EV SSL** – extended validation SSL certificate issued by Certum pursuant to the EV Guidelines that contains information specified in the EV Guidelines and that has been validated in accordance with the EV Guidelines.
14. **S/MIME Certificates** – certificates issued according to *Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates*. S/MIME certificates are designed e-mail encryption and are used for protection of electronic correspondence.
15. **SSL Certificates** – certificates issued according to *Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates*. SSL certificates are used to authenticate Subscribers (legal and natural persons, devices and websites) used by global and extranet service websites operating under the SSL/TLS/WTLS protocol.
16. **Subscriber** – an individual or an organization identified in the certificate that is the owner or has the exclusive right to use the certificate.
17. **Subscriber Representative** - a natural person to whom account on the Certum's website or account within Partner Program has been assigned and who has express authority to represent the Subscriber. Subscriber Representative is either employed by the Applicant/Subscriber or is authorized by the Applicant/Subscriber to act on their behalf.

Subscriber Representative is a person who acknowledges and agrees to these Terms of Use on behalf of the Applicant/Subscriber.

§2. Applicability

These Terms of Use apply to all Non-Qualified Certificates issued by Certum to Subscribers and to the related certification services.

§3. Restrictions on use of the service

Certum shall not issue certificates to individuals under 18 years of age.

§4. Restrictions on use of the service

4.1 Certificate Request

An Applicant or an Applicant Representative may request a Certificate from Certum by submitting an electronic application through the Customer Account on Certum's website (www.certum.pl) or through a dedicated account within the Partner Program.

A Certificate request may only concern Distinguished Names (in particular, the Common Name and Subject Alternative Name fields) that belong to the Applicant or Applicant Representative, or for which the rightful holder of the Distinguished Name has expressly authorized them to apply.

The data provided in a Certificate request shall form an integral part of these Terms of Use.

4.2 Verification

After receiving a Certificate Request, Certum reviews and verify the request in accordance with the Certification Practice Statement of Certum Non-qualified Certification Services and any applicable industry guidelines (such as the *Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Guidelines for the Issuance and Management of Extended Validation Certificates, Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates and Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates*).

4.3 Acceptance

The Applicant shall authorize the individual to whom the account on the Certum's website or the account within Partner Program has been assigned to apply for a non-qualified certificate on behalf of the Subscriber including the right to accept a certificate.

4.4 Certificate issuance

In case of successful verification of the Certificate Request, Certum will issue a certificate and immediately inform the Subscriber.

4.5 Certificate Revocation

The subscriber may revoke the certificate at any time during its validity period by using the functionality of customer account or submitting a revocation request to Certum.
Depending on the circumstances, the revocation period may be as short as 24 hours, or even less. For this reason, Certum advises against deploying publicly-trusted TLS server certificates on systems that cannot accommodate prompt revocation.

Certum must revoke subscriber's SSL or Code Signing certificate within 24 hours if any of the following circumstances occur:

- on each request of the subscriber indicated in the certificate;
- subscriber notifies Certum that the original certificate request was not authorized and does not retroactively grant authorization;
- when a private key, associated with a public key contained in the certificate or media used for storing it has been compromised, or there is a reason to strongly suspect it would be compromised[1];
- Certum obtains evidence that the validation of the request was carried out based on incorrect information;
- when the Subscriber resigns from signing the documents he was to sign using the certificate issuing service in the signing process;
- Certum is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based -on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys)

Certum should revoke a Subscriber's TLS or Code Signing certificate within 24 hours after becoming aware of circumstances requiring revocation, and in any case Certum must revoke the certificate within 5 calendar days if any of the following circumstances occur:

[1] Private key compromise means: (1) the occurrence of unauthorized access to a private key or a reason to strongly suspect this access, (2) loss of a private key or the occurrence of a reason to suspect such a loss, (3) theft of a private key or the occurrence of a reason to suspect such a theft, (4) accidental erasure of a private key.

- cryptographic standards are no longer valid, which can present risks to subscribers or Relying Parties (e.g. technical content or format of the certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties
- Certum obtains evidence that the Certificate was misused;
- when the subscriber does not comply with accepted Certification Policy or the provisions of other documents referenced in this document, which require subscriber to comply with them[2]. ,
- Certum is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the certificate is no longer legally permitted,
- Certum is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading site,
- any information within the certificate has changed,
- Certum is made aware that the certificate has not been issued in accordance with the provision of this Certification Practice Statement, Certification Policy or the provisions of other documents referenced in this document, which requires subscriber to comply with them,
- Certum determines or obtains information that any information in certificate is incorrect,
- if a certification authority terminates its services, all the certificates issued by this certification authority before expiration of declared period of service termination must be revoked, along with the certificate of the certification authority, unless Certum maintains the CRL / OCSP repository,
- when revoke is required by Certification Practice Statement or Certification Policy,
- Certum is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key or if there is clear evidence that the specific method used to generate the Private Key was flawed,
- the subscriber lingers over fees for services provided by a certification authority or other duties or obligations he/she decided to take,

[2] Primarily:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates,
- Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates,
- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates,
- Guidelines For The Issuance And Management Of Extended Validation Certificates

- the subscriber, being an employee of an organization, has not returned the electronic cryptographic card, used for storing the certificate and the corresponding private key, when terminating the contract for employment
- other circumstances, delaying or preventing the subscriber from execution of regulations of this Certification Practice Statement, emerging from disasters, computer system or network malfunction, changes in the subscriber's legal environment or official regulations of the government or its agencies.

These circumstances may also lead to the revocation of EV SSL certificates.

Certum must revoke a Subscriber's S/MIME certificate within 24 hours after becoming aware of circumstances requiring revocation, if any of the following circumstances occur:

- The Subscriber requests in writing that the CA revoke the Certificate;
- The Subscriber notifies the CA that the original Certificate Request was not authorized and does not retroactively grant authorization;
- Certum obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
- Certum is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate
- Certum obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address in the Certificate should not be relied upon.

Certum should revoke a Subscriber's S/MIME certificate within 24 hours after becoming aware of circumstances requiring revocation, and in any case Certum must revoke the certificate within 5 calendar days if any of the following circumstances occur:

- The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates
- Certum obtains evidence that the Certificate was misused;
- Certum is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
- Certum is made aware of any circumstance indicating that use of an email address or Fully - Qualified Domain Name in the Certificate is no longer legally permitted (e.g., a

court or arbitrator has revoked the right to use an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the account holder has failed to maintain the active status of the email address or Domain Name);

- Certum is made aware of a material change in the information contained in the Certificate;
- Certum is made aware that the Certificate was not issued in accordance with these Requirements or the Certum CP and/or CPS;
- Certum determines or is made aware that any of the information appearing in the Certificate is inaccurate;
- Certum's right to issue Certificates under these Requirements expires or is revoked or terminated, unless Certum has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by the Certum CP and/or CPS; or
- Certum is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed
- the subscriber lingers over fees for services provided by a certification authority or other duties or obligations he/she decided to take,
- the subscriber, being an employee of an organization, has not returned the electronic cryptographic card, used for storing the certificate and the corresponding private key, when terminating the contract for employment
- other circumstances, delaying or preventing the subscriber from execution of regulations of this Certification Practice Statement, emerging from disasters, computer system or network malfunction, changes in the subscriber's legal environment or official regulations of the government or its agencies.

In addition, Certum may revoke one or more certificates if required under applicable industry standards, including the CA/Browser Forum Baseline Requirements and the Mozilla Root Store Policy, irrespective of whether the Subscriber requests such revocation.
If certificate revocation is required, Certum will:

- provide advance notice to the affected Subscriber, and in the case of a mass revocation – to all affected Subscribers, indicating the revocation date and reason;

- enforce the revocation timelines as required under applicable industry standards, even if the Subscriber fails to take action to replace the certificate.

4.6 Certificate suspension

Certum does not support suspension.

§5. Obligations

5.1 ADS Obligations

As part of these Terms of Use, ADS undertakes to:

- issue certificates on the basis of the Certificate Request and in accordance with *the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates*, and the *Guidelines for the Issuance and Management of Extended Validation Certificates* (all documents available at http://www.cabforum.org), within 7 days of submitting the Certificate Request, but not earlier than after receipt of all necessary Subscriber documents and payment;
- verify the accuracy of all information received by Certum from the Subscriber at all times;
- provide certification services in accordance with the conditions set out in the *Certification Practice Statement, the Certification Policy*, *Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates*, *Guidelines for the Issuance and Management of Extended Validation Certificates,* this includes in particular:
  - revoking the certificate as described in the Certificate Practice Statement;
  - publishing revoked certificates on the Certificate Revocation List according to the disclosed CRL publishing periods (at least every seven days);
  - taking reasonable steps to maintain continuous 24x7 ability to revoke certificates upon the Subscriber's request;
- publish certificates in the Certum repository;
- notify subscribers (at least 7 days in advance) of the upcoming expiration of certificate validity period.

5.2 Subscriber Obligations

As part of these Terms of Use the Subscriber undertakes to:

- provide true and accurate data regarding the subject of the certificate over the certificate's validity period;
- protect the private key, control its use, and safeguard any related information corresponding to the public key contained in the certificate;
- install the certificate only on a server supporting the domain name listed in the certificate;
- use the certificate in accordance with the applicable laws of the Republic of Poland and ensure it is used only by an authorized entity,
- immediately cease using the certificate or the private key corresponding to the public key in the certificate and promptly request Certum to revoke the certificate if:
  - any of the information appearing in the certificate is untrue or inaccurate;
  - the certificate is suspected of being misused;
  - the private key has been compromised.
- immediately cease using certificate or corresponding private key upon the expiration or revocation of the certificate;
- responding to the certification authority's instructions regarding key compromise or improper use of the certificate within no more than 24 hours from the moment of receiving the notification, as well as cooperating with Certum in revocation procedures.

§6. Subscriber Statement

By submitting a Certificate Request, the Subscriber declares that:

- they have read and accepted these Terms of Use, the Certification Policy of Certum Non-Qualified Certification Services and the Certification Practice Statement of Certum Non-Qualified Certification Services;
- all information provided by the Subscriber in connection with the Certificate Request is accurate, has been voluntarily submitted, and will be administered by Asseco Data Systems S.A., headquartered in Gdańsk, ul. Jana z Kolna 11;
- they shall be liable for any damages resulting from falsification of data or improper use of the issued certificate;
- certificate may be published in the Certum repository;

- they acknowledge that one or more certificates may be revoked by Certum if required under applicable industry standards (including the CA/Browser Forum Baseline Requirements and the Mozilla Root Store Policy).

§7. ADS Guarantees

ADS guarantees that:

- its activities and services covered by these *Terms of Use* are provided with due care and in accordance with the provisions of these *Terms of Use, the Certification Practice Statement, the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, the Guidelines for the Issuance and Management of Extended Validation Certificates, the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates*, and *the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates;*
- the warranty period for certification services provided by ADS is equal to the validity period of the certificate;
- in the event of termination or cessation of certification services, Certum – in accordance with the *Certification Practice Statement* – shall refund issuance fees to the Subscriber proportionally to the remaining validity period of the certificate;
- Certum's financial warranty, in relation to the transactions covered by this guarantee, is limited to the amounts described in the Certification Practice Statement.

§8. Stipulations

ADS stipulates that:

- ADS shall not be responsible for the actions of third parties using the certificate, except for damages which are the fault of ADS,
- Certificates issued by Certum may be used only in accordance with applicable law, exclusively by an authorized entity and in compliance with these Terms of Use,
- ADS shall not be liable for the actions or omissions of the Subscriber or third parties, in particular for:
    - damages resulting from the incorrect installation or use of the certificate, or from the quality of equipment used by the Subscriber or third parties;
    - damages resulting from the improper use of issued certificates or from inadequate protection of the private key by the Subscriber or third parties.

– ADS shall not be liable for events beyond its reasonable control and occurring without its fault or negligence (force majeure).

§9. Contact information

Asseco Data Systems S.A.

Jana z Kolna Street 11

80-864 Gdańsk

Website: www.assecods.pl/en/

e-mail: kontakt@assecods.pl

Certum

Bajeczna Street 13

71-838 Szczecin

Website: www.certum.eu

e-mail: infolinia@certum.pl

Document modification history		
23.05.2018	1.0	Publishing the document in the Certum repository
29.09.2021	1.1	Change of the company's address, change of time to issue the certificate, update of the nomenclature of CA/B Forum documents
27.09.2022	1.2	Minor editorial corrections
18.12.2024	1.3	Minor editorial corrections, update of the CA/B Forum document naming, corrections after Webtrust audit notes.
01.09.2025	1.4	Addition of provisions on revocation under industry standards (CA/B Forum Baseline Requirements, Mozilla Root Store Policy) and rules for mass revocation, editorial corrections.