Terms of use for non-qualified certificates

Version: 1.2

Date: 27 September 2022

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 Certificates** – document created by the CA/Browser forum and published at http://www.cabforum.org. The Guidelines describe certain of the minimum requirements that Certification Authority (CA) must meet in order to issue publicy trusted SSL/TLS certificates.
3. **Certum** – Asseco Data Systems SA's (reffered 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.
4. **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.
5. **Certificate Request** – An electronic request from a Subscriber to the Certum requesting that the Certum issue an EV SSL certificate to the Subscriber. The Certificate Request is attached to the Subscriber Agreement and contains data included in the certificate.
6. **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. Certification Policy is published by the Certum at http://www.certum.pl.
7. **Certification Practice Statement** – document describing in details public key certification process, its parties and defining scopes of usage of issued certificates. Certification Practice Statement is published by the Certum at http://www.certum.pl.
8. **Code Signing Certificates** – certificates used for protection of application's code with an electronic signature. Designed for developers to protect software against forgery.
9. **EV Code Signing Certificates** - certificates issues by Certum pursuant to the *Guidelines for the issuance and management of Extended Validation Code Signing Certificates*, used for protection of application's code with an electronic signature. Designed for developers to protect software against forgery.
10. **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 certain of the minimum requirements that a Certificate Authorities must meet in order to issue EV SSL certificates.
11. **Guidelines for the issuance and Management of Extended Validation Code Signing Certificates ("EV Code Signing Guidelines")** - document created by the CA/Browser

forum and published at http://www.cabforum.org. The EV Code Signing Guidelines describe certain of the minimum requirements that a Certificate Authorities must meet in order to issue EV Code Signing certificates.

12. **ID Certificates** – certificates designed for electronic signing and encrypting e-mails and used in the protection of electronic documents.
13. **Premium EV SSL** – extended validation SSL certificate issues 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. **Subscriber** – an individual or an organization identified in the certificate that is the owner or has the exclusive right to use the certificate.
15. **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 Useon behalf of the Applicant/Subscriber.

§2. Applicability

These Terms of Use covers all non-qualified certificates issued by Certum to Subscribers and certification services related to these certificates.

§3. Restrictions on use of the service

Certum does not issue certificates to persons under 18 years of age.

§4. Restrictions on use of the service

4. 1 Certificate Request

Applicant or Subscriber Representative may request certificates from Certum by submitting the request electronically through applicant's account on the Certum's website at www.certum.pl and through dedicated account within Partner Program. Applicant or Subscriber Representative may request certificates only for Distunguishes Name (especially CommonName and AlternativeSubjectName extensions) registered to Subscriber or, if the Subscriber expressly authorizes Applicant/Subscriber Representative to manage Distinguishes Name included in the certificate. All certificate request data is incorporated into this document as 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's Non-qualified Certification Services and any applicable industry guidelines (such as the *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Guidelines for the Issuance and Management of Extended Validation Certificates* oraz *Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing 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 and Suspension

Subscribers can revoke the certificate on their own at any time during the certificate validity period using the functionality of online accounts or requesting to Certum.

Certum revokes subscriber's SSL or Code Signing certificate within 24 hours if the following situation occurs:

- 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 on the basis of 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 revokes subscriber's SSL or CodeSigning certificate within 5 days if the following situation occurs:

[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 requires 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 have to 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,
- 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.

[2] Primarily:

- Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates,
- Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates,
- Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates oraz Guidelines For The Issuance And Management Of Extended Validation Certificates

Certum revokes subscriber's S/MIME certificate as soon as possible if the following situation occurs:

- the subscriber indicates that the original certificate request was not authorized and does not retroactively grant authorization;
- the Certum obtains reasonable evidence that the subscriber's private key (corresponding to the public key in the certificate) has been compromised or is suspected of compromise;
- the Certum obtains reasonable evidence that the certificate has been used for a purpose outside of that indicated in the certificate or in the Certum's terms of use;
- the Certum receives notice or otherwise becomes aware that a subscriber has violated one or more of its material obligations under the certificates terms of use;
- the Certum receives notice or otherwise becomes aware of any circumstance indicating that use of the email address in the certificate is no longer legally permitted;
- the Certum receives notice or otherwise becomes aware of a material change in the information contained in the certificate;
- the Certum determines that certificate was not issued in accordance with the Certum's Certificate Policy or Certification Practice Statement;
- the Certum determines that any of the information appearing in the certificate is not accurate;
- the Certum ceases operations for any reason and has not arranged for another CA to provide revocation support for the certificate;
- the Certum private key used in issuing the certificate is suspected to have been compromised;
- the Certum determines that the certificate was issued in violation of the applicable requirements.
- 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.

4.6 Suspension of the certificate

Certum does not support suspension.

§5. Obligations

5.1 ADS Obligations

As part of the 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 Certificates, Guidelines for the Issuance and Management of Extended Validation Certificates* oraz *Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates* requirements available at http://www.cabforum.org within 7 days of submitting the Certificate Request but not earlier than after receipt of all necessary Subscriber's documents and payment,
- verify that all of information received by Certum from the Subscriber is accurate at all times,
- provide certification services in accordance with the conditions set out in the Certification Practice Statement, the Certification Policy, the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates the EV Guidelines and the EV Code Signing Guidelines, this concerns in particular:
- revoking the certificate as described in the Certificate Practice Statement;
- publishing revoked certificate on the Certificate Revocation List according to disclosed CRL publishing periods (at least every seven days);
- providing reasonable steps to maintain a continuous 24x7 ability to revoke certificates upon subscriber's request.
- publish certificates in the Certum repository,
- notify subscribers (at least 14 days in advance) about forthcoming certificate validity period expiration.

5.2 Subscriber Obligations

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

- provide true and correct data regarding the subject of the certificate over the certificate validity period
- protect private key - controlling the use of private key corresponding to the public key placed in the certificate and to protect any information related thereto,
- install certificate only on the server supporting a domain name listed in the certificate,
- use the certificate in accordance with the law in force in the Republic of Poland and use certificate only by an authorized entity,
- immediately stop using the certificate or the private key corresponding to the public key placed in the certificate and to promptly request Certum to revoke the certificate in the event that:
    - any of the information appearing in the certificate is not true or not accurate;
    - the certificate is suspected to has been misused;
    - the private key has been compromised.
- immediately stop using certificate or private key corresponding to the public key placed in the certificate at the expiration or revocation time of the certificate.

§6. Subscriber Statement

The Subscriber declares that:

- he/she thoroughly familiarized with and accepted these Terms of Use, the Certification Policy of Certum's Non-Qualified Certification Services and the Practice Statement of Certum's Non-Qualified Certification Services,
- any information provided by the Subscriber regarding the Certificate Request is correct and true and has been given voluntarily and Asseco Data Systems S.A. established in Gdańsk, Jana z Kolna 11 will be the administrator of this data,
- bears liability for the damages that are a consequence of falsifying of data and inappropriate usage of the issued certificate,
- certificate might be published in the Certum repository.

§7. ADS Guarantees

ADS guarantees, that:

- its activity and services covered by these Terms of Use are provided with adequate care and in accordance with provisions of these Terms of Use, the *Certification Practice Statement*, the *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Guidelines for the Issuance and Management of Extended Validation Certificates* oraz *Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.*
- the warranty period for certification services rendered by ADS is equal to the validity period of the certificate.
- in the case of termination or cessation of certification services, Certum– in accordance with the *Certification Practice Statement* – pays compensations of issuance fees to the subscriber proportionally to remaining validity period of the certificate.
- Certum financial warranty, in relation to the transactions covered by the guarantee, is limited to amounts described in the *Certification Practice Statement*.

§8. Stipulations

ADS reserves that:

- does not take any responsibility for the actions of other 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 the principles of the law, only by an authorized entity and in accordance with these Terms of Use,
- does not bear responsibility for the consequences of the actions of Subscriber and third parties, particularly for:
- damages arising from the incorrect installation and usage of the certificate and damages due to the quality of equipment used by the Subscriber and third parties;
- the damages arising from inappropriate usage of issued certificates or inappropriate security of the private key by the Subscriber and third parties.
- does not bear responsibility for unforeseen events beyond its reasonable control and occurring without its fault or negligence (force majeure).

§9. Contact informations

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