Terms & Conditions for Certum Qualified Trust Service - certificate issued in the signing process

Version 1.1
Effective date: July 27th 2021 r.

Asseco Data Systems S.A.
Jana z Kolna Street 11
80-864 Gdańsk, Poland
www.assecods.pl

Certum
Bajeczna Street 13
71-838 Szczecin, Poland
www.certum.pl
www.certum.eu

Table of Contents

1. Subject of regulation and scope of application of the Terms & Conditions

The purpose of this Terms & Conditions for Certum Qualified Trust Service - certificate issued in the signing process (hereinafter referred to as the **Terms & Conditions**) it to specify a detailed regulation of the legal relationship between Certum and the party that is the recipient of the service (hereinafter referred to as the **Service Recipient**). The trust service provided by Certum includes the service of issuing qualified certificates of electronic signature, including registration (application), certification and revocation.

2. Applied trust service policy

Provision of qualified trust services described in this Terms & Conditions is regulated by Certificate Policy and Certification Practice Statement of Certum Qualified Certification Service - certificate issued in the signing process (hereinafter referred to as **the CISP Policy**).

3. Certificate issuance

3.1. Certum issues a certificate based on an application (Statement), which confirms the accuracy of the data and the consent of the service recipient to assign to him/her these data in the certificate issued on the basis of this application.

3.2. Certificate is an electronic attestation, which contains the service recipient's identification data and data used to verify the authenticity of the electronic signature created with the data contained in the SimplySign component, the use of which only the service recipient has control over by having, under his/her sole control, a mobile phone for which he/she will receive a code allowing to use these data for signature.

3.3. Certificate is issued immediately from the moment of submitting a correctly completed and verified application.

3.4. The validity period of the certificate is no longer than 1 day.

4. Certificate revocation

Request for certificate revocation may be submitted by phone.

By calling the number: +48 91 4801 360, the service recipient submits an application for certificate revocation. For the application to be successfully submitted, the recipient must provide the following information:

- name and surname of the service recipient,
- telephone number of the service recipient (which he/she provided in the certificate application),
- signing code,
- certificate serial number.

The registration inspector who received the revocation application verifies the request. In case of positive verification, the certificate shall be revoked within 24 hours from the moment of accepting the application. Information about the revoked certificate is available in the OCSP service.

In case of negative verification, the certificate will not be revoked.

Revoked certificate and the private key complementary to it, stored in the hardware cryptographic module (HSM), are irreversibly removed from this carrier. The operation is performed automatically during the realization of request for certificate revocation, approved by the registration inspector.

5. Scope of the certificate usage

Certificate is used to verify (validate) electronic signature, which has a legal effect equivalent to the service recipient's own signature and as such is recognized in all European Union Member States.

6. Service recipient's obligations

6.1. By accepting the terms of provision of trust services, the service recipient agrees to join the trust service system on the terms set out in this Terms & Conditions.

6.2. Service recipient is obliged to:

- comply with the terms of provision of trust services specified in this Terms & Conditions,
- provide true and correct information,
- provide documents confirming the authenticity of the information provided,
- check the correctness of data contained in the certificate in process of certificate acceptance and in the case of not identifying any irregularities - accepting it,
- ensure sole control over the mobile phone, the number of which was provided in the application (Statement) until the signature process is completed, and not made it available to third parties,
- cease the signing process in the event of:
  - noticing errors in the data contained in the certificate,
  - loss of control (or suspected loss of control) over the mobile phone, the number of which was provided in the application (Statement),
  - receiving information about the revocation of the issued certificate,
  - receiving information about the compromise of the entity issuing certificates - Certum,
- use the signature certificate and it's corresponding data only to sign, and in accordance with the purpose and limitations declared in the certificate.

6.3. Service recipient declares that:

- he/she has read and accepted these Terms & Conditions before signing the application,
- all information provided by him/her is true,
- is liable for damages resulting from providing untrue or false data and for the consequences of incorrect use of certificates,
- he/she is aware that the certificate is, as a rule, available to the public regardless of location,
- he/she is aware that the electronic signature placed on the documents exposes the service recipient's personal data in the following scope: first name, surname and other data indicated for inclusion in the content of the certificate. Moreover, he/she

is aware that Certum has no influence on the disclosure of declarations of will on which the service recipient has placed an electronic signature;
- he/she is aware that the environment in which cryptographic operations take place with the use of data to create the electronic signature is managed by Certum.

6.4. Service recipient agrees:
- to service recipient's obligations listed in chapter 6,
- to use SimplySign component for signatures creation,
- to receive an SMS, that is needed for service completion,
- for Certum to store information related to issued certificates for the required by law period of 20 years,
- for Certum to put data used to verify the electronic signature in certificate and to use this data to verify his/hers electronic signature.

7. Restrictions in the use of the service

7.1. Service recipient does not use the service to provide content that is unlawful, offensive, false or misleading, or content containing viruses or content that may cause disruption or damage to computer systems.
7.2. Certum does not issue certificates to minors (under 18 years of age).

8. Information for relying parties

A relying party is any entity that decides to accept a signature on the basis of a qualified certificate issued by Certum in accordance with these Terms & Conditions.

Relying party is responsible for verifying the current status of the service recipient's certificate. The decision must be made by the relying party whenever he/she wants to use a certificate to verify the electronic signature, its evidential value or the evidential value of data objects. The information contained in a qualified certificate should be used by relying party to determine whether the certificate has been used according to its declared purpose.

9. Data retention period

All data on the provision of qualified trust services including all terms of provision of trust services accepted by service recipients are archived (in electronic form) and stored for a period of 20 years in accordance with the Act on Trust Services and Electronic Identification.

10. Service recipient's communication with Certum

Hotline: infolinia@certum.pl, +48 4472850[1], 801 540 340[1], +48 91 4801 340[1]
Website: www.certum.eu
Complaints: reklamacje@certum.pl, +48 91 4801 380[1]
Data Protection Officer: IOD@assecods.pl, tel. +48 42 675 63 60[1]

11. Technical requirements

The service recipient is obliged to have a mobile phone under his/her sole control.

[1] Rate per minute of connection in accordance with the operator's price list.

12. Services availability

Certum provides all qualified trust services on a continuous basis.

13. Legal basis

13.1. Legal basis for the trust services provided by Certum are following legal acts:
   a) Regulation (EU) 910/2014;
   b) Act on Trust Services and Electronic Identification;
   c) Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC;
   d) Act on the provision of electronic services.

13.2. Personal data will be processed by Asseco Data Systems S.A. solely for the purpose of issuing a qualified certificate. Recipients of the data contained in the certificate will be all entities that will have access to documents bearing an electronic signature verified with this certificate. Information on the processing of personal data, in particular on the scope of data processing, the period of their archiving and access to them, is provided at https://www.certum.eu/en/rodo/.

14. Conditions for concluding and terminating the contract

14.1. Contract for issuing a certificate is concluded at the moment of accepting the submitted application by Certum and lasts until the end of the signature creating process.

14.2. Certum reserves the right to reject applications for important reasons described in the Certification Policy.

15. Terms of disputes settlement, complaints

15.1. Subject of dispute resolution, including complaints, may only be discrepancies or conflicts between parties regarding the issue of the certificate based on the Terms & Conditions and Certification Policy regulations.

15.2. Disputes, complaints or grievances arising in relation to the use of timestamp tokens, certificates status verification tokens issued by Certum, will be settled on the basis of written information through mediation. Complaints should be submitted in writing via e-mail address: reklamacje@certum.pl or by mail on address:

Asseco Data Systems S.A.
Królowej Korony Polskiej 21, Street
70-486 Szczecin, Poland

with the note „Reklamacja".

15.3. Complaints are subjected to written examination within 21 working days of their delivery. If the dispute is not resolved within 45 working days of the conciliation proceedings, the parties have the right to take legal action. The General Court responsible for the defendant will be the competent local court to hear the case.

15.4. If other disputes arise as a consequence of the use of a Certum issued certificate or other qualified service, the subscriber shall be obliged to inform Certum in writing about the case.

16. Limitations of liability

16.1. Financial responsibility of Asseco Data Systems SA, on behalf of which Certum provides qualified services, is 250,000 EUR in relation to one event, but not more than 1,000,000 EUR for all the events (equivalent to PLN). Financial liability concerns 12-month periods in accordance with the calendar year.

16.2. Certum does not bear the financial liability defined herein in relation to other third parties who are not recipients of Certum services.

17. Compliance assessments

Qualified trust services provided by Certum are subject to audits for compliance with the requirements of applicable law.

18. Changes in the Terms & Conditions

18.1. The Terms & Conditions come into force on the day of its publication in electronic form on the website: www.certum.eu and is valid for an indefinite period of time.

18.2. Certum reserves the right to change these Terms & Conditions.

19. Glossary

Certum – organizational unit of Asseco Data Systems S.A. entered into the register of qualified trust service providers kept on behalf of the minister responsible for informatization by the National Bank of Poland. The register is published at the Internet address: www.nccert.pl.
Certificate – qualified electronic signature certificate within the meaning of the Regulation (EU) 910/2014, an electronic certificate issued by a qualified trust service provider that unambiguously assigns data for validation of an electronic signature to a natural person.
Identification data - data that uniquely identifies the service recipient, the truthfulness of which can be confirmed on the basis of the service recipient's identity document.
SimplySign component - a remotely accessible technical component, i.e. hardware cryptographic module (HSM), on which the virtual cards of the service recipients are stored, meeting the requirements of a qualified electronic signature creation device within the meaning of EU Regulation 910/2014.
Electronic Signature – qualified electronic signature within the meaning of the Regulation (EU) 910/2014.
Certificate Policy – „Certificate Policy and Certification Practice Statement of Certum Qualified Certification Service - certificate issued in the signing process" is a set of rules specifying, in particular, the rules for the provision of the trust service, the liability of the parties, available in electronic form at www.certum.eu.
eIDAS Regulation – Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Official Journal of the EU, L No 257, p. 73). The Regulation is a legal act in full force in the legal system of Poland and in all European Union countries.
Service recipient – a natural person applying for a certificate and for whom the certificate has been issued.
Act on the Provision of Electronic Services – the Act of 18 July 2002 on the provision of electronic services (Journal of Laws of 2016 item 1030 with changes).
Act on Trust Services and Electronic Identification – the Act of 5 September 2016 on trust services and electronic identification (Journal of Laws of 2019 item 162).

20. History of the document

History of document changes		
1.1	July 27th 2021	Preparation of English version of document.