Terms & Conditions for Certum Qualified Trust Services

Version 2.8
Effective date: November 18th, 2026

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

Elektronicznie podpisany
przez
Asseco Data Systems S.A.
2026.11.10 07:56:31 +00:00

Certum
ul. Bajeczna 13
71-838 Szczecin
www.certum.pl
www.certum.eu

Table of Contents

1. Subject of regulation and scope of application of the Terms & Conditions 3
2. Applied trust services policies 3
3. Provided services 3
   3.1. Certificate issuance 3
   3.2. Certificate revocation 4
   3.3. Certificate suspension 4
4. Scope of the certificate usage 5
5. Subscriber's obligations 5
6. Restrictions in the use of the service 7
7. Information for relying parties 7
8. Data retention period 9
9. Subscriber's communication with Certum 9
11. Services availability 10
12. Legal basis 10
13. Conditions for concluding and terminating the contract 11
14. Terms of disputes settlement, complaints 12
15. Limitations of liability 13
16. Compliance assessments 13
17. Changes in the Terms & Conditions 13
18. Glossary 14

History of the document 16

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

The purpose of this document (hereinafter referred to as **the Terms & Conditions**) is to specify a detailed regulation of the legal relationship between the provider of qualified trust services – **Certum** and the party that subscribes to the service (hereinafter referred to as **the subscriber**). Trust services provided by Certum include:

a) the service of issuing qualified certificates of electronic signature and electronic seal, including: registration and certification, rekeying (key update), certificate data modification, revocation or suspension of the certificate,
b) electronic time stamp service,
c) electronic certificate status service,
d) qualified electronic signature and qualified electronic seal validation and preservation service,
e) qualified electronic registered delivery service
f) management of remote electronic signature/seal creation devices service.

2. Applied trust services policies

Provision of qualified trust services is governed by the "Certificate Policy and Certification Practice Statement of Certum's Qualified Certification Services".

Regarding to qualified electronic signature and qualified electronic seal validation and preservation service supported service policies and preservation profiles are described in "Policy of qualified validation service and qualified preservation service for qualified electronic signatures and electronic seals (Certum QESValidationQ)".

Both documents are available on the Certum website at: www.certum.eu.

3. Provided services

3.1. Certificate issuance

a) Certum issues certificates based on the application, which confirms the accuracy of the provided data and subscriber's consent to assign to him/her these data in the certificate issued on the basis of this application.
b) Subscriber may apply for a new certificate on his/her own through an individual account on the panel.certum.pl website.

   Note: It is not possible to change the name of the account, i.e. the e-mail address for which the account in panel.certum.pl was established. The only exception is to create a new account in the process of certificate rekeying.
c) Certificate is an electronic attestation, which contains subscriber's identification data, attributes and data used to check the authenticity of the electronic signature (seal) created by means of the data contained in:
   - cryptoCertum card – to which the subscriber is the only user and only he/she knows the PIN and PUK code, enabling its use in order to place an electronic signature (seal),

- SimplySign component – over which only subscriber has sole control by possessing an unique authentication means, with the help of which the subscriber will be identified and logged in the SimplySign service, and the PIN/PUK code which only he/she knows enables him/her to directly use the signature (seal) data located in SimplySign service.

d) SimplySign service subscribers have access to their certificates through an individual account at panel.certum.pl.

   Note: It is not possible to change the name of the account, i.e. the e-mail address for which the account in panel.certum.pl was created.

e) Certificate is issued within 7 business days from the date of submitting the correctly filled and verified application.

f) Certificate contains the expiration date in accordance with the submitted application, however the validity period can't be longer than 3 years and 65 days.

g) Certum sends subscriber information about the upcoming end date of the certificate's validity. The message is delivered to the e-mail address specified in the registration process 60, 30, 14 and 7 days before the end of the certificate's validity.

3.2. Certificate revocation

a) Certum revokes the certificate based on:
   - revocation requests submitted by the subscriber,
   - request of authorized entity whose data is contained in the certificate application,
   - request of an authorized entity on the basis of a previously concluded agreement, which allows such a possibility,
   - information on the threat of the legal or actual interest of the subscriber or third parties resulting from the use of the certificate, about which subscriber shall be immediately notified.

b) The entity confirming the attribute is obliged to submit certificate revocation request in case of discrepancy of the attribute with the actual state.

c) Certum revokes certificate and publishes its status as "revoked" within a period not longer than 24 hours from the effective receipt of revocation request.

d) Once revoked certificate can't be restored.

e) Certificate revocation is equivalent to loss of certificate validity and results in termination of the contract.

f) Contract termination due to certificate revocation does not result in reimbursement of costs incurred by the subscriber that arise from the subject of the contract.

g) Electronic signature created after certificate revocation has no legal effect.

h) Revocation request can be submitted via panel.certum.pl and revoke.certum.eu portals.

3.3. Certificate suspension

a) Certum suspends the validity of the certificate in case of obtaining plausible information, however, it requires an additional check on the risk of the legal or actual interest of Subscriber or third parties resulting from the use of the certificate.

b) Certum publishes the status of the certificate as “suspended” on Certificate Revocation List and immediately informs the subscriber about this fact.
c) Certificate suspension can be canceled, restoring its validity if the conditions determining the suspension have proved to be false, in particular after subscriber confirms this fact.
d) If the suspension is not canceled within 7 days from the certificate suspension date, the status of the certificate remains “suspended”.
e) If the certificate status has changed from “suspended” to “revoked”, the electronic signature created during the suspension does not have legal effect.
f) After cancelation of certificate suspension, the legal effect of the electronic signature verified with this certificate, created during the suspension, takes place at the moment of cancelation of this suspension.

4. Scope of the certificate usage

Certificate is used to verify (validate) electronic signature or electronic seal.

Qualified electronic signature has a legal effect equivalent to the subscriber’s own signature. A qualified electronic seal has a legal effect equivalent to its physical counterpart.

Certificate, in relation to attribute placed in it, does not give subscriber any special roles, rights or authorizations other than those arising exclusively from the content of this attribute.

5. Subscriber’s obligations

By accepting the terms of provision of trust services, the subscriber agrees to join the trust service system on the terms set out in the Terms & Conditions and the Certificate Policy and Certification Practice Statement.

5.1. Subscriber is obliged to:

a) comply with the terms of provision of trust services specified in the Terms & Conditions and the Certificate Policy and Certification Practice Statement,
b) provide true and correct information at every stage of cooperation,
c) provide documents confirming the authenticity of the information provided,
d) 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,
e) ensure sole control and not to disclose his/hers cryptoCertum card or the SimplySign component, on which the data for the electronic signature is stored to third parties and not disclose the PIN and PUK code,
f) start certificate revocation procedure in case of:
   - noticing errors in the data contained in the certificate,
   - noticing certificate defects,
   - changes to the data contained in the certificate,
   - loss of control (or suspected loss of control) over the data used to create electronic signature,

- loss of the cryptoCertum card or authentication means used in the SimplySign service,
- disclosure of PIN and PUK code (to cryptoCertum card or SimplySign service)

g) immediately and permanently stop using SimplySign service or the cryptoCertum card if the certificate is revoked, suspended or expired,

h) use the signature and seal certificate and their corresponding data only to sign or seal and in accordance with the purpose and limitations declared in the certificate,

i) if subscriber is a natural person – is obliged to exercise sole control and not to disclose to third parties his cryptoCertum card or SimplySign component on which the data for electronic signature is stored and not to disclose the PIN and PUK code – applies to qualified electronic signature certificates,

j) if subscriber is a legal person (also applies to unincorporated organizations) – is obliged to exercise control and not disclose to third parties his cryptoCertum card or SimplySign component on which the data for electronic seal is stored and not to disclose the PIN and PUK code – applies to qualified electronic seal certificates.

5.2. Subscriber declares that:

a) he/she has read and accepted these Terms & Conditions before signing the application,

b) he/she has read GDPR information clause (see Chapter 12),

c) all information provided by him/her is true,

d) is liable for damages resulting from providing untrue or false data, for the consequences of incorrect use of certificates or data for creating signature or seal,

e) he/she is aware that the certificate is, as a rule, available to the public,

f) he/she is aware that the electronic signature placed on the documents exposes the Subscriber's personal data in the following scope: first name, surname and other data indicated for inclusion in the content of the certificate. In addition, he/she confirms that the declarations of will on which the subscriber has created electronic signature may be, according to the decision of the subscriber, available without restriction regardless of the location. Asseco Data Systems S.A., a qualified trust service provider – has no influence on the circulation of such signed documents;

g) he/she is aware that the environment in which cryptographic operations take place with the use of data to create the electronic signature (seal) is managed by a qualified trust services provider, which is Asseco Data Systems S.A - applies to SimplySign service subscribers.

5.3. Subscriber agrees:

a) to subscriber's obligations listed in Chapter 5,

b) to use cryptoCertum card or SimplySign component for signatures or seals creation,

c) for Certum to store information related to issued certificates for the required by law period of 20 years,

d) for Certum to create a backup copy of the data used to create an electronic signature (electronic seal) in order to provide the minimum needed to ensure the continuity of the SimplySign service,

e) for Certum to put data used to verify the electronic signature (seal) in certificate and to use this data to verify his/hers electronic signature (seal).

5.4. Subscriber who downloads timestamp token should verify the electronic seal of the authority and check the Certificate Revocation List for revocation of the authority's certificate.

5.5. Certum provides OCSP service for verification of qualified certificates on-line. This service allows obtaining information about certificate revocation also outside its validity period.

5.6. The Customer of qualified electronic registered delivery is obliged to:

- comply with the terms of the qualified electronic registered service provided by Asseco Data Systems S.A.,
- provide the serving point of the Registration System network with true and correct information at each stage of cooperation,
- provide documents verifying the accuracy of the data contained in the application in order to fulfill the requirements of the registration process as set forth in the "Certificate Policy and Certification Practice Statement of Certum's Qualified Certification Services" and the "Policy and Practice Statement of Certum eDelivery Qualified Service – electronic registered delivery",
- inform Certum immediately of any errors or changes in data,
- use the qualified electronic registered service only for lawful purposes.

6. Restrictions in the use of the service

6.1. Subscriber 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.

6.2. SimplySign service is not aimed at M2M (machine-to-machine) applications and mass signing or sealing of electronic documents. As part of this service, subscriber has the number of signatures or seals at the level of 5000 within a month. Above this value, the service provider has the right to limit the service performance, e.g. up to 100 signatures and seals per day.

6.3. Certum does not issue certificates to minors (under 18 years of age).

7. Information for relying parties

7.1. Certum's relying party is any entity that decides to accept a qualified electronic signature (seal), timestamp service, validation and preservation service for qualified signatures and electronic seals (in particular in conjunction with the document) or eDelivery service that may be in any way dependent on:

a) validity of the link between the identity of the subscriber and the public key belonging to him/her, certified by a qualified certification authority, or

b) binding of electronic signature or seal with electronic timestamp token, issued by a qualified electronic timestamp authority, or

c) confirmation of current status of a certificate issued by a qualified certification status verification authority, or

d) validation report issued by a qualified service,
e) eDelivery service evidence.

7.2. Relying party is responsible for verifying the current status of the subscriber's certificate or any other tokens received from it. The decision must be made by the relying party whenever he wants to use a certificate and tokens to verify the electronic signature (seal), 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.

7.3. Regardless of the type of services rendered by Certum, the relying party is obliged to accept the following conditions:
a) to accept the conditions set out in the Terms & Conditions, Certificate Policy and Certification Practice Statement, Validation and Preservation Policy for Qualified Certum QESValidationQ,
b) to verify each electronic signature (seal) placed on a document or certificate, timestamp token, certificate status token, validation report, eDelivery service evidence,
c) to correctly and properly perform cryptographic operations using software and hardware, whose level of security is consistent with level of sensitivity of processed information and level of reliability of certificates used,
d) to recognize the electronic signature (seal) to be invalid if it can't be determined whether the signature (seal) is valid or the obtained verification result is negative,
e) to trust only those certificates:
   – which are used according to the declared purpose and are suitable for use in areas that have previously defined by relying party, i.e. in the form of a signature policy,
   – whose status has been verified, i.e. based on the Certificate Revocation List, or using the OCSP service provided by Certum,
f) to define the conditions that must be met by the certificate and the electronic signature (seal) so that it is considered valid by that party. These conditions can be formulated, for example, in the form of an appropriate signature policy and published.

7.4. If a document or electronic signature is time-stamped or otherwise associated with other tokens, in order to rationally build trust in the verified token, the relying party should additionally:
a) verify whether the token was properly certified electronically, and whether the private key used by the qualified electronic time stamp authority was not disclosed until the token verification credentials were validated (unless the time used meets certain date requirements); status of the private key can be verified on the base on the verification of the complementary public key,
b) check restrictions in the use of electronic signature and electronic seal certificates, electronic timestamp tokens, on-line status verification tokens, data validation reports defined in Certificate Policy and Certification Practice Statement, Terms & Conditions and Validation and Preservation Policy for Qualified Certum QESValidationQ.

7.5. Guarantees and liability of Certum are valid only for the certificate issued and accepted by subscriber.

7.6. Certificate Revocation Lists are issued at specified intervals or each time after suspension or revocation of one of the issued certificates. They contain:
- name of the certification authority that issued them,
- date of current and next publication,
- serial numbers, dates and reasons for revocation (or suspension) of certificates.

7.7. In case of electronic signature formats or electronic seal formats that are not supported by qualified validation and preservation service, a message will be provided that the request cannot be processed.

7.8. In case qualified validation and preservation service is unable to collect and verify all the validation data, a message will be provided that the request cannot be processed.

7.9. In case of qualified electronic registered delivery service the relying party is obliged to thoroughly verify each confirmation received by it. For that purpose, the relying party shall:

a) verify that all certificates of trust service providers included in the certification path belong to certification authorities and that they have been granted the right to certify electronic registered deliveries,

b) specify the date and time of confirmation. This is done with a qualified electronic time stamp embedded in the confirmation.

8. Data retention period

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

Records of video calls obtained in the process of remote identity verification are stored up to 14 days, after this time the records are destroyed.

9. Subscriber's communication with Certum

In case of revocation, suspension or cancellation of suspension of the certificate, subscriber will receive information on his/hers e-mail address or telephone (SMS message) depending on which contact subscriber indicated while requesting a certificate or agreed otherwise with Certum.

Contact information:

Name:	Certum
Address for correspondence:	Bajeczna St. 13, 71-838 Szczecin, Poland
Hotline:	infolinia@certum.pl, +48 91 4801 340[1]
Certificate revocation:	revoke.certum.eu
Website:	www.certum.eu
Complaints:	reklamacje@certum.pl, +48 91 4801 380[1]

[1] Rate per minute of connection according to the operator's price list

Data Protection Officer: IOD@assecods.pl, tel. +48 42 675 63 60[1]

10. Technical requirements

a) Certum maintains a list of secure devices that include qualified electronic signature creation devices (QSCD), such as cryptoCertum cards and hardware security module (HSM), which stores SimplySign virtual subscriber cards within the meaning of eIDAS Regulation. The list is available on Certum website: www.certum.pl.
b) Certum has in its offer card readers for cryptoCertum cards and provides drivers necessary for their proper functioning on the website www.certum.pl.
c) SimplySign service is available via a device with the Android, iOS, Windows or MAC OS operating system.

11. Services availability

11.1. Security Policy, implemented by Certum, takes into account the following threats, affecting the availability and continuity of the services provided:
   a) physical damage to Certum system and computer network,
   b) software failures, loss of access to data,
   c) loss of essential (from Certum's point of view) network services,
   d) failure of this portion of the Internet network through which Certum provides its services.

11.2. To prevent or limit the effects of these threats, Certum security policy covers the following issues:
   a) Disaster recovery plan – all subscribers and relying parties are promptly and appropriately informed of any major failure or disaster related to any component of the computer system and network as appropriate. The system recovery plan includes a series of procedures that are performed when any part of the system is compromised (damaged, disclosed, etc.).
   b) Controlling changes – upgraded versions of the software in the target system are only possible after performing a rigorous testing on the model system, following strict procedures.
   c) Backup system – in the event of a failure preventing the operation of Certum within a maximum of 24 hours, a backup center will be started, which will take over the basic functions of the certification authority until the main center in Certum is started.
   d) Backup system – Certum's system uses software that makes backup copies of data that allows them to be restored and audit serviced at any time.

12. Legal basis

12.1. Legal basis for the trust services provided by Certum are following legal acts:
   a) eIDAS Regulation, which is a legal act that is fully applicable in the legal system of Poland and in all European Union countries;
   b) Act on Trust Services and Electronic Identification of September 5, 2016 (Journal of Laws of 2021 r. item 1797);

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 of 18 July 2002 (Journal of Laws of 2017, item 1219)

12.2. According to art. 13 para. 1 and 2 of the General Data Protection Regulation of 27 April 2016, hereinafter referred to as "the GDPR" , we would like to inform you that:

a) Asseco Data Systems S.A. is the administrator of personal data

b) Contact to Data Protection Officer at Asseco Data Systems S.A. has been provided in Chapter 9.

c) Personal data will be processed for the purposes necessary to provide the service, pursuant to art. 6 par. 1 lit. b of the GDPR.

d) All data regarding the provision of qualified trust services, including personal data and all terms for the provision of trust services accepted by the Subscriber, are archived (in electronic or paper form) and stored for 20 years in accordance with Art. 17 sec. 2 of the Act on Trust Services and Electronic Identification.

e) Subscriber has the right to access his/hers data and the right to rectify, delete/forget (after the expiration of the obligation under Art. 17 sec. 2 of the Act on Trust Services and Electronic Identification), limit processing, right of data transfer, right to object, the right to withdraw consent at any time without affecting the legality of processing, which was made on the basis of consent before its withdrawal. All the rights mentioned above can be implemented by submitting an application at www.daneosobowe.assecods.pl.

f) The subscriber has the right to lodge a complaint to the Regulatory Body if he/she considers that processing of his personal data violates provisions of the GDPR.

g) Providing personal data is a condition for the provision of services. Subscriber is obliged to provide it, and the consequence of not providing personal data will be the inability to carry out the process of issuing the certificate.

12.3. Certum is an organizational unit of Asseco Data Systems S.A. entered into the register of qualified trust service providers maintained on behalf of the minister of digitalization by the National Bank of Poland. This register is published at the website: www.nccert.pl.

12.4. The implementation of qualified trust services by Certum is defined in detail in "Certificate Policy and Certification Practice Statement of Certum's Qualified Certification Services" available at website: www.certum.pl.

12.5. In matters not regulated, the provisions of the generally applicable law are in effect.

13. Conditions for concluding and terminating the contract

13.1. Contract for the provision of qualified trust services is concluded after submission of certificate application by subscriber, acceptance by him/her the Terms & Conditions and the Certification Policy and the Certification Practice Statement and confirmation of his/hers identity.

13.2. Each subsequent certificate application requires re-validation of subscribers identity.

13.3. Resignation from trust services is possible only in case of revocation of a qualified electronic signature certificate (seal), according to terms specified in the Certificate Policy and the Certification Practice Statement.

13.4. Certum reserves the right to refuse certification applications in the following cases:

- when the subscriber cannot prove his/her rights to proposed DN,
- validity date of the applicant's identity document, whose data (number and series number) included in the certificate is shorter than the certificate's validity date,
- if there is suspicion or certainty that the subscriber falsified the data or stated false data,
- if the applicant fails to deliver the required set of formal documents, constituting as an attachment to the application,
- in case of detection of corrections or modifications in submitted formal documents,
- if the validity date of submitted documents is exceeded – the documents whose date of creation exceeds 3 months,
- if the validity date of certificate application is exceeded – the applications whose filling date exceeds 3 months,
- from other reasons not specified above, upon prior notice of **security inspector**.

If the required set of formal documents is not provided, the required set of documents of the entity (in case of certificates with the entity's data) Certum reserves the right to destroy them within 3 months from the date of receipt.

14. Terms of disputes settlement, complaints

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

14.2. Disputes, complaints or grievances arising in relation to the use of timestamp tokens, issued by Certum certificates status verification tokens, validation and preservation service, eDelivery service 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 to address:	Asseco Data Systems S.A., Królowej Korony Polskiej St. 21 70-486 Szczecin, Poland with the note "Reklamacja"

14.3. Complaints are subjected to written examination within 14 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.

14.4. 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.

15. Limitations of liability

15.1. 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.

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

15.3. To supervise the efficient operation of Certum, all these events occurring in the system, which have a significant impact on the operational safety of Certum, are recorded. Registered events include, but are not limited to: registration, certification, update, revocation and suspension of certificates, timestamp, data validation, certificate status verification, and generation of keys for Certum, and any events occurring in the system that have a significant impact for the safety operation of Certum.

16. Compliance assessments

16.1. Qualified trust services provided by Certum are subject to annual examination of compliance with eIDAS Regulation. The certification audit is carried out once every two years. Additional surveillance audit is carried out between two certification audits.

16.2. In addition, Certum is also auditing the compliance of the Integrated Management System – Information Security Management System and Quality Management System. The purpose of this audit is to determine the degree of compliance of the Certum service unit or its components with that implemented by Asseco Data Systems S.A. Integrated Management System, which covers the requirements of PN-EN ISO 9001:2015 and PN ISO/IEC 27001:2017 standards, and declarations and procedures specific to Certum.

17. Changes in the Terms & Conditions

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.

17.1. Certum reserves the right to change these Terms & Conditions. Any changes to the Terms & Conditions will be communicated clearly on the website specified in Chapter 17 and enter into force:

- upon publication,
- in relation to subscribers who hold valid certificates – with the lapse of at least 7 days from the date of publication of changes to the Terms & Conditions, subject to paragraph 3 below.

17.2. Change in the Terms & Conditions resulting in a reduction or limitation of rights acquired by subscriber, authorizes the Subscriber to submit a resignation from the services provided

within 7 days from the date of receiving information about the entry into force of changes to the Terms & Conditions. In the situation described in the preceding sentence, subscriber is obliged to submit a statement made in writing and sent to the address of Certum.

17.3. Mentioned above changes to the Terms & Conditions will also be communicated to Subscribers via e-mail.

18. Glossary

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 2021, item 1797 with changes).

Audit – make an independent review and evaluation of system performance to test the adequacy of the system oversight measures; Whether the system operates in accordance with the established Certificate Policy and Certification Practice Statement and the resulting operating procedures and to detect security breaches and recommendations for identified changes in monitoring measures, certification policies and procedures.

Certum – qualified trust services provider for the issuance of qualified certificates for electronic signatures and seals, time stamps, online status verification and data validation.

Certificate Policy and Certification Practice Statement – document describing in detail the process of the public key certification, the participants of the process, their responsibilities, types of certificates, identity verification procedures used for their issuance, and the areas of application of obtained certificates, published on the website available at address www.certum.eu.

Certificate – qualified electronic signature or seal certificate within the meaning of the eIDAS Regulation.

Certificate data modification - creation of a new certificate on the basis of the certificate that is currently owned by the subscriber. A new certificate has a different public key, a new serial number, and it differs in at least one field (its contents or appearance) from the certificate on the basis of which it is being issued.

Certificate Revocation List – list containing serial numbers, dates and reasons for certificate revocation (or suspension). It also contains the name of the certification authority that issued it and the date of the current and next publication. The list is issued at specified intervals or after each suspension or annulment of one of the issued certificates.

CryptoCertum card – a technical component that meets the requirements of a qualified electronic signature creation device within the meaning of eIDAS Regulation ;

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 with Regulation

(EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation as regards establishing the European Digital Identity Framework.

Electronic Signature (Seal) – qualified electronic signature (electronic seal) within the meaning of the eIDAS Regulation.

Identification data – data uniquely identifying subscriber, the truthfulness of which can be confirmed on the basis of the subscriber's identity document, if the subscriber is a legal entity (also applies to organizations without legal personality) its data are verified on the basis of registration documents;

Personal Identification Number (PIN) – code securing cryptographic card against unauthorized usage.

Personal Unlocking Key (PUK) – code used for cryptographic card unlocking and changing of the PIN.

Private key – a key pair of asymmetric keys of the entity, which is only used by the entity. In the case of the system of asymmetric private key defines a signature. The asymmetric encryption system crash is a private key that defines a decryption transformation.

Public key – a key from an asymmetric key pair of an entity that can be made public. For an asymmetric signature system, the public key specifies a verification transformation. In the case of an asymmetric encryption system, the public key specifies the cryptographic transformation.

SimplySign component – a remotely available technical component that meets the requirements of a qualified electronic signature creation device within the meaning of the eIDAS Regulation.

SimplySign Service – a service consisting in managing the infrastructure in which SimplySign is located, a component under the control of the Subscriber.

Qualified electronic time stamp – a service consisting of attaching to electronic data logically associated with the signed or electronic credentials, the time stamp at the time of execution of the service, and the electronic credential of the data generated by the TSP.

Subscriber – a natural person in case of an electronic signature or a legal entity in case of an electronic seal requesting a certificate or for which a certificate has been issued. Subscriber is also a natural person or a legal entity or an unincorporated entity that uses the service of qualified time stamping, signature/seal validation and signature/seal preservation and registered electronic delivery eDelivery.

Trust Service Provider (TSP) – means any natural or legal person who provides at least one service of confidence as qualified or unqualified trust service provider.

Working day – day from Monday to Friday excluding Saturdays, Sundays and public holidays specified in the Act of 18 January 1951. On days off from work (uniform text Journal of Laws of 2015 item 90).

History of the document

History of document changes		
1.0	26th July 2017	Document preparation.
1.1	1 August 2017	Change to the address of Asseco Data Systems S.A.
1.2	29 June 2018	"Signed agreement" was changed to "acceptance of terms of provision".
1.3	1 September 2018	Update of the OID number assigned to the Certification Policy and the Certification Practice Statement
2.0	27 June 2019	Document preparation – combining of "Terms & Conditions for Certum Qualified Trust Services" and "Terms & Conditions for Certum Qualified Trust Services for contracts concluded in electronic form" into one document.
2.1	9 September 2020	Introducing editorial corrections
2.2	December 30th, 2020	Introducing editorial corrections
2.3	July 27th 2021	Change to certificate revocation request path, change to the address of Asseco Data Systems S.A. and other editorial corrections.
2.4	June 1st 2022	Added new qualified eDelivery service *(Qualified electronic registered delivery service is currently being audited in compliance with the eIDAS Regulation and will be made available to subscribers upon receiving of all relevant certificates)*
2.5	February 26th , 2024	Added information about the inability to change the name of the account in panel.certum.pl.
2.6	July 8th, 2024	Corrections in connection with the amendment of the eIDAS Regulation.
2.7	October 16th, 2026	Implementation of editorial changes – periodic review.
2.8	November 18th, 2026	Editorial changes have been made, updated procedures for handling paper documentation.