Terms & Conditions
for Qualified Trust Services
for agreements concluded in electronic form

Version 1.0
Date: 22.10.2018
Status: archival

1. Glossary

Certificate – qualified electronic signature certificate within the meaning of the regulation (EU) No 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;

Subscriber – a natural person applying for a certificate or for whom a certificate has been issued;

Certum – qualified trust service provider, which is the issuing of a qualified certificate for electronic signature;

Electronic Signature – qualified electronic signature within the meaning of the regulation (EU) No 910/2014;

CryptoCertum card – a technical component that meets the requirements of a qualified electronic signature creation device within the meaning of the regulation (EU) No 910/2014;

SimplySign component – a remotely available technical component that meets the requirements of a qualified electronic signature creation device within the meaning of the regulation (EU) No 910/2014;

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

SimplySign application – software on a mobile device, under the sole control of the Subscriber, enabling the use of SimplySign service;

Identification data – data uniquely identifying Subscriber, the truthfulness of which can be confirmed on the basis of the Subscriber's identity document;

Attribute – additional data contained in the certificate, whose truth is confirmed in principle by a third party;

Certificate Revocation List (CRL) – 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;

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;

Regulation (EU) No 910/2014 – 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).

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

This Terms & Conditions defines rights and obligations of the Subscriber and Certum for agreements for the provision of qualified trust services concluded in electronic form, on the terms set out in Chapter 14 of the Terms & Conditions, regarding the application and issuance of the certificate and it's management.

3. Certificate issuance

3.1. 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.

3.2. Certificate is an electronic attestation, which contains Subscriber's identification data, attributes and data used to check the authenticity of the electronic signature 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,
- SimplySign component – over which only Subscriber has sole control by possessing an unique identification 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 data located in SimplySign service.

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

3.4. Certificate contains the expiration date in accordance with the submitted application, however the validity period can't be longer than 3 years.

3.5. 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.

4. Scope of the certificate usage

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

4.2 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 Certificate revocation

5.1 Certum revokes the certificate based on:

- revocation requests submitted by the Subscriber;
- request of authorized entity whose data is contained in the certificate application;
- 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.

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

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

5.4 Once revoked certificate can't be restored.
5.5 Electronic signature created after certificate revocation has no legal effect.

6 Certificate suspension

6.1 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.
6.2 Certum publishes the status of the certificate as "suspended" on Certificate Revocation List and immediately informs the Subscriber about this fact.
6.3 Certificate suspension period can last up to 7 days.
6.4 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.
6.5 If the suspension is not canceled within 7 days from the certificate suspension date, the status of the certificate will be changed to "revoked".
6.6 If the certificate status has changed from "suspended" to "revoked", the electronic signature created during the suspension does not have legal effect.
6.7 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.

7 Subscriber's obligations

7.1 Subscriber is obliged to:
- 7.1.1 Provide true and correct information at every stage of cooperation;
- 7.1.2 Provide documents confirming the authenticity of the information provided;
- 7.1.3 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, lack of rejection results in certificate acceptance;
- 7.1.4 Ensure access protection to cryptoCertum card or SimplySign component on which the data for the electronic signature is stored, in particular by not disclosing the PIN and PUK code to unauthorized persons;
- 7.1.5 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 identification means used in the SimplySign service,
  - disclosure of PIN and PUK code (to cryptoCertum card or SimplySign service);
- 7.1.6 Immediately and permanently stop using SimplySign service or the cryptoCertum card if the certificate is revoked, suspended or expired;
- 7.1.7 Use the certificate and the corresponding data for the signature only in accordance with the purpose, objectives and limitations declared in the certificate.

7.2 Subscriber declares that:
- 7.2.1 He/she has read and accepted these Terms & Conditions before signing the application;

7.2.2 He/she has read GDPR information clause (see Chapter 13);
7.2.3 All information provided by him/her is true;
7.2.4 Is liable for damages resulting from providing untrue or false data and for the consequences of incorrect use of certificates;
7.2.5 He/she is aware that the certificate is, as a rule, available to the public;
7.2.6 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;
7.2.7 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 a qualified trust services provider, which is Asseco Data Systems S.A.

7.3 Subscriber agrees:
7.3.1 To Subscriber's obligations listed in point 7.1;
7.3.2 To use cryptoCertum card or SimplySign component for signatures creation;
7.3.3 For Certum to store information related to issued certificates for the required by law period of 20 years;
7.3.4 For Certum to create a backup copy of the data used to create an electronic signature in order to provide the minimum needed to ensure the continuity of the SimplySign service;
7.3.5 For Certum to put data used to verify the electronic signature in certificate and to use this data to verify his/hers electronic signature.

8 Restrictions in the use of the service

8.1 Subscriber is obliged to use the cryptoCertum card or the SimplySign service only in person in accordance with the purpose specified in the certificate and only during its validity period.
8.2 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.
8.3 Certum does not issue certificates to minors (under 18 years of age).

9 Information for relying parties

9.1 Certum’s relying party is any entity that decides to accept a certificate (in particular an electronic document) which may be in any way dependent on the validity of the connection between the identity of the subscriber and the data at his/hers sole disposal for electronic signature, certified by Certum.
9.2 Relying party is responsible for verifying the current status of the subscriber's certificate. The decision must be made by the relying party whenever he wants to use a certificate and tokens 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.
9.3 The relying party is obliged to accept the following conditions:
9.3.1 To verify each electronic signature placed on a document or certificate;

9.3.2 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;

9.3.3 To recognize the electronic signature to be invalid if it can't be determined whether the signature is valid or the obtained verification result is negative;

9.3.4 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;

9.3.5 To define the conditions that must be met by the certificate and the electronic signature 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.

9.4 Guarantees and liability of Certum and Subscriber are valid only for the certificate issued and accepted by Subscriber.

9.5 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 the certificates.

10 Subscriber's contact with Certum

10.1 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.

10.2 Contact information:

10.2.1 Asseco Data Systems S.A.: ul. Podolska 21, 81-321 Gdynia, Poland, www.assecods.pl, kontakt@assecods.pl

10.2.2 Certum

- Address for correspondence: ul. Bajeczna 13, 71-838 Szczecin, Poland
- Hotline: infolinia@certum.pl, +48 91 4801 340[1]
- Certificate revocation: +48 91 4801 360[1]
- Complaints: reklamacje@certum.pl, +48 91 4801 380[1] (see Chapter 15)

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

11 Technical requirements

11.1 Certum maintains a list of secure devices that includes qualified electronic signature creation devices (QSCD), such as cryptoCertum cards within the meaning of regulation (EU) No 910/2014. The list is available on Certum website www.certum.pl.

11.2 Certum has in its offer card readers for cryptoCertum cards and provides drivers necessary for their proper functioning on the website www.certum.pl.

11.3 SimplySign service is available via a devices with the Android, iOS, Windows or MAC OS operating system.

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

12 Services availability

12.1 Security Policy, implemented by Certum, takes into account the following threats, affecting the availability and continuity of the services provided:

12.1.1 Physical damage to Certum system and computer network;

12.1.2 Software failures, loss of access to data;

12.1.3 Loss of essential (from Certum's point of view) network services;

12.1.4 Failure of this portion of the Internet network through which Certum provides its services.

12.2 To prevent or limit the effects of these threats, Certum security policy covers the following issues:

12.2.1 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.).

12.2.2 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.

12.2.3 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.

12.2.4 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.

13 Legal basis

13.1 Legal basis for certificate issuance service and it's usage are following legal acts:

- Regulation (EU) 910/2014, which is a legal act that is fully applicable in the legal system of Poland and in all European Union Member States;
- Act on Trust Services and Electronic Identification of September 5, 2016 (Journal of Laws of 2019, item 162);
- Act on the provision of electronic services of 18 July 2002 (Journal of Laws of 2017, item 1219).

13.2 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:

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

13.2.2 Contact to Data Protection Officer at Asseco Data Systems S.A. has been provided in Chapter 10 Subscriber's contact with Certum.

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

13.2.4 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 and paper form) and stored for 20 years in accordance with Art. 17 sec. 2 of the Act on Trust Services and Electronic Identification.

13.2.5 Subscriber has the right to access his/hers data and the right to rectify, delete/forget, 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.

13.2.6 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.

13.2.7 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.

13.3 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.

13.4 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.

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

14 Conditions for concluding and terminating the contract

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

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

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 and revocation of the certificate based on Terms & Conditions and Certificate Policy and the Certification Practice Statement.

15.2 Disputes, complaints or grievances arising in relation to the use of certificates 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 to address: Asseco Data Systems S.A., ul. Bajeczna 13, 71-838 Szczecin, Poland, with the note "Reklamacja".

Additional contact: +48 91 4801 380[2]

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.

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

16 Limitations of liability

16.1 Financial responsibility of Asseco Data Systems S.A., 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.

16.3 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.

17 Compliance audit

17.1 Qualified trust services provided by Certum are subject to annual examination of compliance with the regulation (EU) 910/2014. The certification audit is carried out once every two years. In addition, it is recommended that at least one surveillance audit be carried out between two certification audits.

17.2 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 9001:2009 and PN ISO/IEC 27001:2007 standards, and declarations and procedures specific to Certum.

18 Changes in Terms & Conditions

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

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

18.2.1 upon publication;

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

18.3 Change in 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 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 Asseco Data Systems S.A.

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