Terms & Conditions for CERTUM PCC Qualified Trust Services

Version 1.1

Date: 1 of August 2017

Status: archival

Asseco Data Systems S.A.
Podolska Street 21
81-321 Gdynia
CERTUM – General Certification Center
Bajeczna Street 13
71-838 Szczecin
https://certum.pl
http://certum.eu

Table of Contents

§1. Subject of regulation

1. This document, hereinafter referred to as "the Regulations", governs the basic rights and obligations of parties to the contract for the provision of qualified trust services, provided electronically within the meaning of the *Act on the provision of electronic services*, which consists of the following services:
    1) issuing qualified electronic signature certificates and electronic seal, including:
        a. registration and certification,
        b. rekeying (key update),
        c. certificate data modification,
        d. certificate revoking or suspending,
    2) electronic time stamp service,
    3) certificate status verification service,
    4) qualified electronic signature and qualified electronic seal validation service.
2. CERTUM reserves the right to change the Regulations. All changes to the Regulations come into force within 7 days from the date of their publication on website http://www.certum.pl. Subscribers will be informed about any changes in the Regulations via mailing system, no later than 7 days before the changes to the Regulations.
3. Each time after the changes have been made to the Regulations a new, currently valid version is published on the website of the certification authority at the address http://www.certum.eu, with the designation of next version.
4. CERTUM website is designed for visually impaired people, who would like to apply for a qualified electronic signature. The contrast ratio between text and background can be adjusted and text resized, which does not affect the functionality and readability of the website.
5. The provisions of the Regulations concern the provision of trust services within the meaning of *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 electronic identification and trust services in relation to electronic transactions in the internal market and repealing Directive 1999/93/EC and the Trust and Electronic Identity Services Act of 5 September 2016 (Journal of Laws of 2016, item 1579).*

§2. Regulatory Entity

1. Qualified trust services are provided by Asseco Data Systems S.A with the seat in Gdynia at Podolska Street 21, entered into the National Court Register maintained by the District Court for Gdańsk-Północ, VIII Economic Division of the National Court Register, under the number KRS 0000421310, share capital 120 002 940,00 PLN (paid in full), by the organically separated Certum – Powszechne Centrum Certyfikacji (hereinafter referred to as CERTUM).

2. By decision of the Minister of Development No. 1/47610-16/16 dated April 1, 2016, Asseco Data Systems S.A. with the seat in Gdynia, was entered under number 14 in the register of qualified trustees connected with the electronic signature.
3. These Terms and Conditions, Certificate Policy and Certification Practice Statement, and price lists are available to the trustees, on the CERTUM website and at the CERTUM Registration System sites.
4. CERTUM has a termination plan developed in accordance with the requirements of *Regulation (EU) No 910/2014 of the European Parliament and of the Council* and the *Act on Trust Services and Electronic Identification,* which is mandatory for trust service providers. Description of proceedings in case of activity termination is included in Certificate Policy and Certification Practice Statement of CERTUM's Qualified Certification Services, while more detailed way of action is described in CERTUM termination plan, which is the internal CERTUM procedure.

§3. Trust services policy

1. Provision of qualified services is governed by the Certificate Policy and Certification Practice Statement, which is available on the CERTUM Certification Authority's web site at:

   https://certum.pl

   This document has been assigned an Object Identifier:

   OID: 1.2.616.1.113527.2.4.1.0.1.5.1
2. The structure and substantive content of the Certificate Policy and Certification Practice Statement comply with the RFC 3647. It also complies with the requirements of Chapters 5 and 6 of the ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI) standard; Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

§4. Restrictions on use of the service

1. Subscribers are required to use CERTUM services
   1) in accordance with their use as defined in the Certificate Policy and Certification Practice Statement and in accordance with the content of the certificate,
   2) in accordance with the agreement between the Subscriber and Asseco Data Systems S.A.,
   3) only during their validity period,
   4) only until the certificate is revoked; during the suspension of the certificate, the subscriber may not use the private key.
2. Limitations on the use of trust services
   1) does not store a cryptographic card containing a private key with a personal identification number (PIN),

2) does not share or transfer its private keys and the passwords it uses to the third parties.

It is forbidden to use of CERTUM certificates in contrary to the purpose of the type of certificate specified in the Certificate Policy and Certification Practice Statement.

§5. Obligations of subscriber

1. By entering into a trust service contract, the subscriber agrees to join the trust services system under the terms of the Agreement, Certificate Policy and Certification Practice Statement.
2. The subscriber is obliged to:
   1) comply with the terms of the agreement signed with Asseco Data Systems S.A.,
   2) provide a valid and reliable and correct information to the Registration Point at every level of cooperation,
   3) provide documents confirming the validity of the data contained in the application in order to fulfill the requirements of the registration process, the declaration of invalidity specified in the Certificate Policy and Certification Practice Statement, revocation and renewing the certificate,
   4) promptly notify CERTUM of any errors or defects in its certificate or changes in its contents,
   5) use her or his key pair and public key of other trustees only in a manner compliant with Certificate Policy and Certification Practice Statement, and to ensure the security and integrity of hers or his private keys, including:
      a. control and secure access to devices containing its private keys,
      b. to immediately inform the Main Registration Point of any circumstances whereby his or her private key has been disclosed to the third party or as a result of which the subscriber may suspect that the private key may be disclosed to third parties,
      c. to immediately inform the certification authority about the loss of a certificate card or loss of a PIN number,
   6) protect the secure access to media on which passwords and keys are stored,
   7) treatment of loss or disclosure (transfer of another unauthorized person) password on parity with the loss or disclosure of a private key,
   8) in the event of a breach of protection (or a suspected breach of protection) of the private key, immediately proceed to the certificate revocation procedure,
   9) discontinue use of the invalidated, suspended or invalid certificate,
   10) use a qualified public key certificate and the corresponding private key only in accordance with the declared purpose, objectives, and restrictions stated in the certificate.
3. Subscriber who downloads the timestamp token should verify the digital signature of the office and check the CRL.

CERTUM provides real-time certificate status verification service. The service also allows you to obtain information about the certificate revocation beyond its validity period. Using OCSP, it is possible to acquire more frequent and up-to-date information (in comparison to sole CRL usage) about a certificate status

4. Subscriber using a qualified trust service agrees to refrain from using the services to provide a content that is unlawful, offensive, untrue or potentially misleading, content containing viruses or content that may cause interference or damage to computer systems.
5. On receiving a certificate, a subscriber is committed to check its contents, particularly the correctness of the data and complementariness of a public key with the private key he/she/it possesses. If the subscriber fails to find any faults in the certificate, he or she can accept the certificate (no refusal results acceptance of the certificate).

   If the issued certificate has any faults, the subscriber should immediately request the revocation of the certificate.

   An application for certificate revocation can be submitted to Primary Registration Authority only by authorized persons personally, by phone, by fax or by mail.

§6. Technical requirements.

1. In order to use qualified trust services, the Subscriber must have an end device that allows him/her to use the Internet and have software that allows him/her to use the services that meet the minimum technical requirements:
   1) operating system Microsoft Windows, Mac OS, Android, iOS (CERTUM guarantees the correct operation of services for these versions of operating systems, which are currently supported by manufacturers or distributors),
   2) web browsers: Mozilla Firefox, Internet Explorer, Google Chrom, Safari (especially with Java script support),
   3) processor: Pentium 800 MHz,
   4) operational memory: 256 MB RAM,
   5) appropriate applications to use the Services,
   6) software provided to user by CERTUM at the service launch stage.

§7. Terms of conclusion and termination of the agreement

1. Terms of concluding agreements for the provision of qualified trust services are specified in the Certificate Policy and the Certification Practice Statement.
2. Termination of the agreement for the provision of qualified trust services is possible only in the case of revocation of a qualified electronic signature or electronic seal, made under conditions specified in the Certificate Policy and the Certification Practice Statement.

§8. Informations for relying parties

1. CERTUM relying party is any entity that decides to accept a qualified electronic signature or seal or other authenticated electronic credential, time stamp service or validation service for qualified signatures and electronic stamps. (In particular an electronic document) that may be in any way contingent on:

   1) the validity or relevance of the link between the identity of the subscriber and the public key belonging to it, certified by a qualified certification authority, or

   2) the binding of the electronic signature or stamp to the electronic token, issued by a qualified electronic time stamp authority, or

   3) confirmation of the current status of a certificate issued by a qualified certification authority, or

   4) a validation token issued by a qualified service.

2. The relying party is responsible for verifying the current status of the subscriber's certificate and other tokens and credentials received from it. The decision of such a relying party must always be taken when it wishes to use a certificate, tokens and credentials to verify the electronic signature, its evidential value or the evidential value of the data objects. The information contained in a qualified certificate relying party should be used to determine whether the certificate has been used according to its declared purpose.

3. No matter what type of CERTUM service is provided, the relying party is obliged to accept the terms and conditions set out in this document this means:

   1) to accept the conditions set out in the Certificate Policy and Certification Practice Statement, Validation Policy for Qualified CERTUM Certum QESValidationq, etc. The relying party accepts the above mentioned certification. Conditions at the time of the first referral to any service provided by CERTUM or the first acceptance of the subscriber's signature. Warranty and liability of CERTUM or subscriber are valid from the time the subscriber has accepted the certificate issued,

   2) to verify each signature or electronic credential placed on the document or certificate, timestamp validation, certificate status validation, validation and validation of the cryptographic operation,

   3) to use software and hardware whose security level is in accordance with the level of vulnerability and the level of credibility of the certificates used,

   4) to consider the digital signature as invalid if using your software and hardware cannot determine whether the digital signature is valid or the result of the verification is negative,

   5) trust only those public key certificates:

      a) which are used according to the declared purpose and are suitable for use in areas that have previously defined by relying party. For example, in the form of a signature policy,

b) whose status has been verified based on the current list of revocable certificates, or using the OCSP service provided by CERTUM,

6) to determine the conditions to be met by a public key certificate and digital signature to be recognized by This page is important; These conditions can be formulated, for example, by the appropriate signature policy and published.

4. If a document or electronic signature is time-stamped or otherwise associated with other tokens, the credentials issued by CERTUM are for rational trust building to a verified token or credential, the relying party should additionally:

   1) verify whether the token, the credential was properly duly certified electronically, and whether the private key used by the qualified electronic time stamp office was not disclosed until the token verification credentials were validated; (Unless the time used meets certain date requirements) The status of the private key can be verified on the base on the verification of the public key complementary to it,

   2) check restrictions on the use of electronic signature and electronic stamp certificates, electronic time stamp tokens, on-line status verification tokens, data validation tokens as defined in Certificate Policy and Certification Practice Statement and in agreement concluded with CERTUM.

§9. Data retention period

All data on the provision of qualified trust services including all subscriber contracts are archived (in electronic and paper form) and stored for a period of 20 years in accordance with the Trust and Electronic Identification Services Act of 5 September 2016.

§10. Limitation of Liability

1. Financial responsibility of Asseco Data Systems SA, on behalf of which CERTUM provides qualified services, is equivalent to PLN 250,000 in relation to one event, but not more than 1,000,000 Euro for all the events. Financial liability concerns 12-month periods in accordance with the calendar year.
2. CERTUM does not bear the financial liability defined herein in relation to other third parties who are not recipients of CERTUM services.
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.

§11. The legal system used

1. The services are provided in accordance with *EU Regulation 910/2014 of 23rd July 2014 on electronic identification and trust services for electronic transactions in the internal market and*

repealing Directive 1999/93/EC and *the Law of 5th July 2014 September 2016 on trust and electronic identification (Dz. U. of 2016 pos. 1579).*

2. Subscribers data is processed by Asseco Data Systems S.A., in accordance with the *Personal Data Protection Act of 29th August 1997 (t.j. Dz.U. z 2016 r. poz. 922)*. Subscribers have the right to view and correct the transferred personal data. The Privacy Policy is available at:

   http://www.certum.pl/certum/cert,onas_informacje_prawne.xml

3. All court disputes will be resolved by the General Court competent for the defendant's local registered office.

§12. Dispute Resolution Conditions

1. Depending on the subject for disputes, including complaints, can be only discrepancies, or conflicts between the parties regarding issuance and revocation of the certificate based on the provisions of the Certificate Policy and Certification Practice Statement, and the agreements concluded.

2. Any disputes or complaints arising out of the use of certificates, certification certificates, time stamp tokens, certificate status tokens issued by CERTUM shall be settled on the basis of written information by mediation. Complaints should be addressed in writing to:

   Asseco Data Systems S.A.

   Bajeczna Street 13

   71-838 Szczecin

3. Complaints are subjected to written examination within 21 days of their service to the address indicated in sec. 2 of this paragraph. If the dispute is not resolved within 45 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.

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.

§13. Compliance audits

1. Qualified trust services provided by CERTUM are subject of the annual eIDAS compliance review pursuant to Art. 20 points 1 and 17.4. *European Parliament and Council Regulation (EC) No 910/2014* on electronic identification and trust services for electronic transactions in the internal market of 23 June 2014 replacing Directive 1999/93/EC. According to the provisions of chapter 7 of ETSI EN 319 403 "Compliance of the trust service providers" –which regulates the operation of entities confirming compliance of trust service providers - certification audit is performed every two years. In addition, it is recommended that at least one maintenance audit will be conducted between two certification audits.

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.

§14. Contact informations

Asseco Data Systems S.A.

Podolska Street 21

81-321 Gdynia

Website: https://www.assecods.pl

e-mail: kontakt@assecods.pl

CERTUM – Powszechne Centrum Certyfikacji

Bajeczna Street 13

71-838 Szczecin

Website: http://certum.eu

e-mail: infolinia@certum.pl

§15. Availability of services

1. Security Policy, implemented by CERTUM, takes into account the following threats, affecting the availability and continuity of the services provided:
   1) physical damage to the CERTUM system and computer network,
   2) software failures, loss of access to data,
   3) loss of CERTUM services critical to the Viewpoint of the network services,
   4) failure of this portion of the Internet through which CERTUM makes available its services.
2. To prevent or limit the effects of these threats, CERTUM security policy covers the following issues:
   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.).

2) Controlling changes. On the target system, upgraded versions of the software are only possible after performing a rigorous testing on the model system, following strict procedures.

3) Backup system. In the event of a failure to operate 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 CERTUM is started. Backup system. CERTUM uses backup software with data that can be restored and serviced at any time.

4) Backup system. CERTUM uses software that makes backups of data that can be restored and *serviced at any time.*

§16. Glossary

Terms used in this Terms and Conditions are:

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 – General Certification Center (pl. CERTUM – Powszechne Centrum Certyfikacji, abbreviated as CERTUM or CERTUM PCC) – service unit of Asseco Data Systems SA, providing non-qualified and qualified trust services. Qualified trust services provide for the issuance of qualified public key certificates for electronic signatures and seals, time stamps, online status verification, data validation and receipt and submission, in particular pursuant to the Act of 5 September 2016 trust services and electronic identification (OJ 2016. pos. 1579).

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 http://www.certum.eu.

Certificate (public key certificate, PKC) – an electronic certificate by which the data used to verify the electronic signature are assigned to the person submitting an electronic signature and which permit the identification of the osoby.

EIDAS Regulation – European Parliament and Council Regulation (EU) No 910/2014 on electronic identification and trust services in relation to electronic transactions in the internal market and repealing Directive 1999/93/EC.

Electronic Seal – electronic data which is added to or electronically linked to other data in electronic form to ensure the authenticity of origin and integrity of related data.

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.

Primary Registration Authority (PRA) – registration authority whose additional duty is to approve the rest of the RA's and is allowed to generate – on behalf of a certification authority – key pairs, successively subjected to certification process.

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.

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 entity.

Qualified Trust Services – Trusted Services Provided by a qualified trust service provider.

Subscriber – natural person or in the case of electronic stamp a legal person or organizational unit without legal personality which is the subject has a private key that corresponds to the public key contained in the certificate and does not itself issue certificates to other parties. A subscriber may be the same as an entity, or represent another subscriber. (Note: ETSI EN 319 411-1 5.4.2).

Subscriber agreement – this agreement is entered into between Asseco Data Systems S.A. And a subscriber ordering a personal qualified certificate to act on its own behalf or a qualified professional certificate to perform tasks on behalf of the entity represented by the subscriber.

Trusted Services and Electronic Identity – the Act of 5 September 2016 on trust and electronic identification.

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.

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.