Certum PKI Disclosure Statement

Version 1.11

Effective date: July 27th 2021

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

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

Table of Contents

Contact info

Asseco Data Systems S.A.
ul. Jana z Kolna Street 11,
80-864 Gdańsk, Poland
Website: www.assecods.pl/en
e-mail: kontakt@assecods.pl

Certum
Bajeczna Street 13
71-838 Szczecin, Poland
Website: www.certum.eu
e-mail: kontakt@assecods.pl

1. Certificate type, verification procedures and usage

1.1. Certificate type

This statement applies only to qualified trust and electronic timestamp services provided by Certum.

Qualified services operate under a qualified certification authority Certum QCA 2017, which issues public key qualified certificates for qualified electronic signatures and electronic seals, qualified electronic timestamp authority Certum QTST 2017, which issues electronic timestamp tokens, qualified authority CERTUM QDVCS and Certum QESValidationQ, which provides service of validationof qualified electronic signatures and qualified electronic seals.

Profile and any other limitation of qualified public key certificate for qualified electronic certificates and qualified seals are issued by the Certum QCA 2017 is compliant with the ETSI EN 319 412.
Profile and any other limitation of electronic timestamp issued by the Certum QTST 2017 is compliant with the ETSI EN 319 422.

CERTUM QDVCS and Certum QESValidationQ services issue validation token, which has a structure consistent with RFC 3029 (chapter 9).

1.2. Identity validation procedures

Qualified certificate is issued to an individual based on the verification of their identity. Verification of the individual may be carried out in a registration authority, by notary or other person who is authorized to confirm identity of the certificate holder.

Confirmation of the identity of the owner of the certificate and the person applying for an electronic seal on behalf of the entity is based on valid documents:

- ID card or
- passport,

and additionally, in the case of individuals acting for the organization or a person requesting an electronic seal on behalf of the legal person:

- the authorization of the subscriber to act and to use the certificate or electronic seal on behalf of the institution or legal entity.
- the official government record of the registration.

Verification of the recipients of services provided by the electronic timestamp authority and the validation authority is based on an electronic signature, optionally it can be carried out by a person who verifies the identity, in accordance with the rules for verification of applicants for a qualified certificate.

1.2.1. Identity verification by an authorized representative of Certum

Confirmation of the subscriber's identity is based on a valid identity card or passport via the Registration Point or Identity Confirmation Point. Confirmation of the subscriber's identity can be done in three ways:

- through personal appearance at a Registration Point or Identity Confirmation Point,
- by a visit of an authorized Certum representative to the location where the subscriber is currently staying,
- remotely, through secure electronic communication means, ensuring constant voice and visual contact of the person confirming identity with the subscriber.

In the case of a remote verification process, the subscriber's identity is confirmed by two additional independent methods implemented during the ongoing process:

- authentication of the applicant in an external reliable electronic identification system using electronic identification means issued in that system, i.e. by making a bank verification transfer via the Blue Media service,

independent video verification path provided by the AriadNEXT service, which additionally serves to check the originality of the presented identity document and to compare the image of a person with a photo that is contained the presented document.

1.2.2. Identity verification using a video-identification system

Identity verification is performed by an external service provider using video means to confirm the identity of the person applying for the certificate in a way that ensures credibility equivalent to physical presence[1].

1.2.3. Identity verification by a notary public

Certum accepts certificate applications signed by the subscriber in the presence of a notary public who confirms this fact.

[1] Video-identification service that Certum use is provided by IDnow GmbH

1.2.4. Identity verification based on a qualified electronic signature

In a special cases, when a person applying for a qualified certificate has a valid qualified certificate, their identity can be confirmed on the basis of a certification application bearing the qualified signature of that person.

1.2.5. Identity verification using an electronic identification means

Identity verification may be performed remotely, using an electronic identification means for which the physical presence of the person applying for the certificate was ensured prior to the issuance of the qualified certificate, and the identification means meets the requirements of a medium or high level of security within the meaning of the eIDAS regulation. In particular, these may be electronic identification means issued by banks. The level of security is always confirmed by an auditor examining the compliance of Certum's operations with eIDAS regulations, based on a direct audit or on the basis of documents from an audit performed by another authorized entity. The indication of accepted means of electronic identification and the description of their use in the process of issuing the certificate is included in the appropriate procedure subject to assessment by an auditor.

Usage

Qualified certificates issued by Certum QCA 2017 must be used only in accordance with the Trust Services and Electronic Identification Act of 5th September 2016, (Dz. U. of 2019. Pos. 162). This means that certificates may be used to verify secure electronic signatures which are proofs of act of will and proof of connection with the data of various trust levels to which it has been attached.

Qualified certificates issued by Certum QCA 2017 are issued in compliance with *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,* hereinafter referred to as eIDAS Regulation.

Qualified electronic timestamp authority Certum QTST 2017 issue electronic timestamp tokens, which, in terms of the Civil Code (art. 81§2 pkt.3), produce legal consequences of a certified date. The primary use of electronic timestamps is to mark long-term electronic qualified signatures with reliable time. Electronic timestamp issued by the Certum QTST 2017 may also be used in any other cases that require a comparable electronic timestamp service.

Qualified electronic timestamp authority service is provided in accordance with the eIDAS Regulation.

The certification policy identifier (OID) placed by Certum QTST 2017 in electronic time stamp tokens is as follows: 1.2.616.1.113527.2.4.1.14.

Qualified electronic signatures and timestamp validation service CERTUM QDVCS and Certum QESValidationQ 2017 issues electronic confirmation of validity of a qualified public key certificate, qualified electronic signature, qualified electronic seal.

Qualified electronic signatures and seals validation service is provided in accordance with the eIDAS Regulation.

Time stamping services and validation services for qualified electronic signatures and qualified electronic seals are available 24/7 (without any planned outages).

2. Reliance limits

The financial warranty of Asseco Data Systems S.A. in relation to individual event amounts equivalent of an 250.000 € but total financial warranties of Asseco Data Systems S.A. in relation to all such events cannot exceed the amount of 1.000.000 €. Financial liability applies to 12-month periods what is equivalent to the calendar year.

In order to manage operation of Certum systems and supervise Certum users and personnel efficiently, all events occurring in the systems and having essential impact on Certum security are recorded.

Certum event logs include in particular: operations associated with registration, certification, revocation and suspension of certificates, rekey and renewal procedures, issuance of timestamp issuance, data validation, validation of a certificate's status, key generation for a certification authority and every event having significant importance on security and normal activity of Certum.

3. Subscribers obligations

By applying for the certificate issuance and accepting the terms of provision of trust services, a subscriber agrees to enter the certification system on the conditions stated in the terms of provision of trust services, Certification Policy and Certification Practice Statement of Certum‘s Qualified Certification Services and Terms &Conditions for Certum Qualified Trust Services.

Subscriber is committed to:

- comply with the terms of provision of trust services by Asseco Data Systems S.A.,
- state true data in applications submitted to the certification authority,
- submit or present of required documents confirming the information included in a certification request,
- immediately inform Certum about any errors, defects or changes in the certificate,
- apply his/her/its own key pair and the public keys of other certification services users only for the purposes stated in the Certificate Policy and Certification Practice Statement

and to take all reasonable measures to keep confidential, and properly protect at all times the private key, including:
  - control of the access to devices containing his/her/its private key,
  - immediately inform Primary Registration Authority when a private key, has been, or there is a reason to strongly suspect it would be compromised,
  - immediately inform Primary Registration Authority about the loss of a certificate card or loss of a PIN number,
- control the access to this software, media, and devices on which the keys or passwords are stored,
- treating a loss or disclosure (transfer to another unauthorized person) of password equally to loss or disclosure (transfer to another unauthorized person) of private key,
- in case of security violation (or security violation suspicion) of private keys immediately start a procedure of certificate revocation
- stop using revoked, suspended or unvalid certificate,
- apply qualified certificate and the corresponding private keys only for the purpose stated in the certificate and in accordance with the aims and restrictions stated in this document.

Electronic signature usage constraints

- to create no any electronic signature or electronic seal with its private key if the validity period of certificate has expired and certificate has been revoked or suspended,
- not to store the cryptographic card containing the private key together with a personal identification number (PIN),
- not to share and communicate her/his private keys and passwords to third parties.

The subscriber who receives the timestamp token should verify the digital signature of the authority and check the CRL for revocation of the authority certificate.

4. Certificate status checking obligations of relying parties

A relying party, using Certum services, can be any entity who accept the qualified electronic signature and electronic seal relying on:

- validity of the connection between subscriber's identity and his/her/its public key (confirmed by certification authorities Certum QCA 2017), or
- association of a signature or electronic seal with an electronic timestamp token issued by a qualified electronic timestamp authority Certum QTST 2017, or
- confirmation of the validity of the certificate issued by a qualified data validation authority CERTUM QOCSP
- validation token issued by qualified service CERTUM QDVCS and Certum QESValidationQ 2017.

A relying party is committed to:

- verify that an electronic signature or electronic seal has been created by means of a private key corresponding to a public key set in the subscriber's certificate issued by Certum, and
- verify that a signed message (document) or a certificate have not been modified after signing it,
- carry out cryptographic operations accurately and correctly, using the software and devices whose security level complies with the sensitivity level of the certificate being processed and the trust level of applied certificates,
- consider the electronic signature or the certificate to be invalid if by means of applied software and devices it is not possible to state if the electronic signature or the certificate are valid or if the verification result is negative,
- trust only these qualified certificates that are used in accordance with the declared purpose and are appropriate for applicability ranges that were specified by the relying party, and the status was verified on the basis of the valid Certificate Revocation Lists or OCSP service available at Certum,
- verify if the token or the confirmation were correctly certified electronically, and whether the private key used by the qualified electronic timestamp authority Certum QTST 2017, the qualified CERTUM QDVCS and QSValidationQ 2017 validation service was not disclosed until the token verification, confirmation (unless the time in them meets the requirements of a certain date); status of a private key can be verified based on the verification of a complementary public key,
- that the time contained in them meets the requirements of a certain date. The status of a private key can be verified based on the verification of a complementary public key.

5. Limited warranty and disclaimer/Limitation of liability

Certum does not take any responsibility for the actions of third parties, subscribers and other parties not associated with Certum. In particular, Certum does not bear responsibility for:

- damages arising from forces of nature: fire, flood, gale, other situations such as war, terrorist attack, epidemic, and other natural disasters or disasters caused by people,
- damages arising from the installation and usage of applications and devices used for generating and managing cryptographic keys, encryption, creating of an electronic signature that are included in the unauthorized applications list (applicable to relying parties) or are not included in the authorized applications list (applicable to subscribers),
- damages arising from inappropriate usage of issued certificates (term inappropriate understood as the use of a revoked, invalidated or suspended certificate)
- storage of false data in Certum database and their publication in a public certificate key issued to the subscriber in the case of subscriber's stating such false data.

6. Applicable agreements, Certification Policy and Certification Practice Statement, Terms & Conditions

Certum publishes at the repository www.certum.eu the following documents:

- Certificate Policy and Certification Practice Statement of Certum‘s Qualified Certification Services,
- Validation Policy of CERTUM’s QESValidationQ Qualified Validation Service for qualified electronic signatures and qualified electronic sealsTerms & Conditions for Certum Qualified Trust Services.
- Document templates.

7. Privacy policy

Subscriber data is processed by Asseco Data Systems SA, in accordance with the Act of 29 August 1997 On The Protection of Personal Data (OJ 2016 item. 922, the new consolidated text of the Act). Privacy Policy is available at:

https://www.assecods.pl/o-firmie/regulaminy/

8. Refund policy

Certum makes efforts to secure the highest level of its services. Subscriber may request certificate revocation and fee refund only if Certum does not fulfill its obligations and duties specified in the terms of provision of trust services, Certificate Policy and Certification Practice Statement and the present document.

9. Applicable law, complaints and dispute resolution

Operating of Certum is based on the general rules stated in the Certificate Policy and Certification Practice Statement and it is in accordance with the superior legal acts in force in the Republic of Poland.

Disputes related to Certum’s qualified services will be first settled through conciliation.

If the complaint is not settled within 45 days of the commencement of conciliatory process, the parties can hand over the dispute to appropriate court. The court, appropriate for case handling, will be the Public Court of the defendant.

In the instance of the occurrence of arguments or complaints following the usage of an issued certificate or services delivered by Certum, subscribers commit themselves to notify Certum of the reason for the argument or complain.

10. CA and repository licenses, trust marks, and audit

Audits checking the compliance with procedural and legal regulations (particularly the consistency with Certificate Policy and Certification Practice Statement) is carried out at least once a year on a basis of art.20 of the eIDAS Regulation. Audited qualified services provided by Certum are on a trusted list - TSL list (A list of qualified service providers, along with information about the provision of trust services, in accordance with eIDAS Regulation).

Certum's services are subject to annual audit of the Integrated Management System which includes the requirements of the standards: PN-EN ISO-9001:2009 and PN ISO/IEC 27001:2014.

11. Identification of this document

This document has been registered with Certum and has been assigned an Object Identifier:

OID: 1.2.616.1.113527.2.4.1.0.2.1.11

12. Registration points, points of the identity confirmation

Registration points and points of the identity confirmation register subscribers and verify their identity. List of registration points and points of the identity verification you can find on:

https://sklep.certum.pl/partnersmap.

Document History

Historia zmian dokumentu		
1.0	25.02 2015.	Based on ETSI EN 319 411-2 model disclosure statement
1.1	01.04 2016	Transfer of ownership of Unizeto Technologies S.A. Asseco Data System S.A.
1.2	17.10.2016	Update on legislation.
1.3	23.12.2016	Update on legislation.
1.4	08.03.2017	Update on eseal product information, deletion on WebTrust conformity.
1.5	26.04.2017	Update on electronic timestamp and validation.
1.6	01.08.2017	Change to the address of Asseco Data Systems S.A.
1.7	29.06.2018	"Signed agreement" was changed to "acceptance of terms of provision".
1.8	27.06.2019	Added a special case of issuing a certificate on the basis of an application with a qualified signature of the applicant
1.9	09.09.2020	Added added remote identity verification path for subscribers, added editorial corrections
1.10	December 30th, 2020	Added alternative identity verification paths, removal of authorities that are no longer valid.
1.11	July 27th 2021	Corrections after eIDAS compliance auditor notes, change to the address of Asseco Data Systems S.A. and other editorial corrections.