Certum QCA PKI Disclosure Statement

Version 1.4

Effective date: 3th of March, 2017

Status: previous

Asseco Data Systems S.A.
ul. Żwirki i Wigury 15
81-387 Gdynia
„Certum - Powszechne Centrum Certyfikacji"
ul. Bajeczna 13
71-838 Szczecin
https://certum.pl
https://certum.eu

Spis treści

1. CA contact info.

Asseco Data Systems S.A.
ul. Żwirki i Wigury 15
81-387 Gdynia

Certum - Powszechne Centrum Certyfikacji
ul. Bajeczna 13
71-838 Szczecin
strona WWW: https://certum.pl

2. Certificate type, validation procedures and usage.

Certificate type

This statement applies only to qualified certification services provided by CERTUM.

Public key qualified certificates for qualified electronic signatures and electronic seals are issued by the qualified certification authority CERTUM QCA within the CERTUM's qualified certification services.

Profile and any other limitation of certified public key certificate for qualified electronic certificates and qualified seals are issued by the CERTUM QCA is compliant with the ETSI EN 319 412.

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.
The individual requesting for the qualified certificate or a person requesting an electronic seal on behalf of the legal person must undergo a face-to-face verification procedure.

- 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.

Usage

Qualified certificates issued by **CERTUM QCA** must be used only in accordance with the Trust Services and Electronic Identification Act of 5th September 2016, (Dz. U. of 2016. Pos. 1579). 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** 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.*

3. 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 system and supervise CERTUM users and personnel efficiently, all events occurring in the system 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.

4. Obligations of subscribers.

By applying for the certificate issuance (request should consist of a hand-written signature) and entering into the Subscriber Agreement, a subscriber agrees to enter the certification system on the conditions stated in the Agreement, Certification Policy of CERTUM‘s Qualified Certification Services and Certification Practice Statement of CERTUM‘s Qualified Certification Services.

Subscriber is committed to:

- comply with the rules of the agreement made with 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 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,

- 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,

- control the access to this software, media, and devices on which the keys or passwords are stored,

- make his/her/its private keys inaccessible to other persons,

- start a procedure of revocation in the case of security violation (or security violation suspicion) of their private keys,

- 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.

5. Certificate status checking obligations of relying parties.

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

- validity of the connection between subscriber's identity and his/her/its public key (confirmed by certification authorities **CERTUM QCA**), or

- confirmation of the validity of the certificate issued by a qualified data validation authority **CERTUM QOCSP**.

A relying party is committed to:

- verify that an electronic signature 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.

6. 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.

7. Applicable agreements, Certification Practice Statement, Certification Policy.

CERTUM publishes at the repository https://www.certum.eu/ the following documents:

- Certification Policy of CERTUM’s Qualified Certification Services,

- Certification Practice Statement of CERTUM’s Qualified Certification Services.

- templates of agreements

8. 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.certum.eu/certum/cert,expertise_privacy_policy.xml.

9. Refund policy.

CERTUM makes efforts to secure the highest level of its services. If a subscriber or a relying party is not satisfied with the services, they may request certificate revocation and fee refund only if CERTUM does not fulfill its obligations and duties specified in the Subscriber Agreement and the present document.

10. Applicable law, complaints and dispute resolution.

Operating of CERTUM is based on the general rules stated in the 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.

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

Audits checking the consistency with procedural and legal regulations (particularly the consistency with Certification Practice Statement and Certification Policy) is carried out at least once a year on a basis of art.20 of eIDAS
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.

12. Identification of this document.

This document has been registered with CERTUM and has been assigned an Object Identifier (OID) of: 1.2.616.1.113527.2.4.1.0.2.1.4.

13. 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.