Certification Policy of CERTUM's Certification Services

Version 4.2

Effective date: 26 March 2018

Status: archive

Asseco Data Systems S.A.
Podolska Street 21
81-321 Gdynia, Poland
Certum - Powszechne Centrum Certyfikacji
Bajeczna Street 13
71-838 Szczecin, Poland
http://www.certum.pl

Trademark and Copyright notices

Content

1. Introduction 2
2. Certificates 2
2.1. DV Certificates (Domain Validation) 3
2.2. OV Certificates (Organization Validation) 4
2.3. EV Certificates (Extended Validation) 5
2.4. Code Signing Certificates 6
2.5. External authorities certificates 7
3. Non-repudiation services 8
3.1. Time-Stamps 8
3.2. OCSP confirmation response 9
4. CERTUM guarantees 10
5. Certificate Acceptance 10
6. Certification Services 10
7. Relying Party 11
8. Subscriber 11
9. Certification Policy Update 11
10. Fees 11
Document's history 12

1. Introduction

Certification Policy of CERTUM's Certification Services describes general rules and regulations applied by CERTUM – Powszechne Centrum Certyfikacji (further referred to as CERTUM) for public key certification process, Time-Stamping Authority (TSA) and remaining non-repudiation services. Document defines parties of this process, their responsibilities and obligations, types of certificates and applicability range. Detailed description of the above rules and the subscriber identity verification procedures is disclosed in Certification Practice Statement of CERTUM's Certification Services. The knowledge of the nature, goal and role of the Certification Policy, as well as Certification Practice Statement is particularly important from the point of view of the subscriber and relying party.

2. Certificates

Certificate is a string of data (a message), containing at least a name and an identifier of the authority issuing the certificate, subscriber's identifier, his/her/its public key, validity period and the serial number and is signed by the intermediate certification authority subordinated to one of the root certification authorities **Certum CA, Certum Trusted Network CA, Certum Trusted Network CA 2, Certum Elliptic Curve CA, Certum Trusted Root CA** and **Certum EC-384 CA**.

Certum CA, Certum Trusted Network CA, Certum Trusted Network CA 2, **Certum Elliptic Curve CA, Certum Trusted Root CA** and **Certum EC-384 CA** upon indirectly issuing a certificate to the subscriber confirm his/her/its identity or the credibility of other data, such as email address. Authorities also confirm the public key possessed by such subscriber, is the property of this very subscriber. Due to above a relying party upon reception of signed message is able to verify the owner of the certificate, which signed the message and, optionally, account him/her of the actions he/she performed or obligations he/she made.

CERTUM provides services in accordance with the *WebTrust*™ (see http://www.webtrust.org) requirements for the certification authorities. Certification authority keys are protected with the hardware security module. The authority implemented physical and procedural controls of the system. CERTUM issues certificates in a various levels of credibility. Credibility of the certificate depends of enforced subscriber's identity verification procedure and the effort used by CERTUM to verify the data submitted by the requester in his/her/its registration application. The more information should be verified, and so the procedure is more complex, the more reliable the certificate. The level of certificate may depend on the level of the security of the operating system or service server of the network hardware device subjected to the certification. CERTUM system engineers may verify the technical state and the security level of the information system prior to the issuance of the certificate of highest credibility level.

The subscriber has to state by himself/herself/itself the credibility level of the certificate most appropriate for his/her/its needs. Types of the certificates and their credibility level are described in detail in the **Certification Practice Statement of CERTUM's Certification Services**. The document is available through the web page http://www.certum.eu or via email addressed to: info@certum.pl.

2.1. DV Certificates (Domain Validation)

DV certificates are issued for two separate groups. As a free test certificates for shorter period of validity and the standard certificates with a full usage. Certificates of the first group are issued by intermediate authorities **Certum Level I CA**, **Certum Class 1 CA** and **Certum Class 1 CA SHA2**. The second group of standard certificates are issued by **Certum Level II CA** and **Certum Domain Validation CA SHA2** authorities.

Test certificates are intended mainly for the application or device test performance prior to purchasing final certificate. **DV** certificates are issued for the following types of applications: securing electronic correspondence and protecting data transmission based on SSL/TSL protocols.

CERTUM operates a procedure for verifying the identity of the subscriber that meets the *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* (http://www.cabforum.org/)

CERTUM verifies all data provided by subscriber in the certification process. The verification covers: a domain name – for SSL certificates, a common name – for S/MIME certificates, an email address and country Detailed information on identity verification requirements are described in **Certification Practice Statement of CERTUM's Certification Services** and on the website http://www.certum.eu.

It is not recommended to unambiguously verify the identity of the subject of the certificate on the basis of **DV** certificates

End-users **DV** certificates contain following policy identifiers:

Authority Name	**Policy Identifier**
Certum Level I CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-I(1)
Certum Class 1 CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5) id-ctn-certPolicy (1) id-certum-class-1(5)
Certum Class 1 CA SHA2	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5) id-ctn-certPolicy (1) id-certum-class-1(5)
Certum Level II CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-II(2)
Certum Domain Validation CA SHA2	{iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5)} id-ctn-certPolicy (1) id-certum-dv(3)

CERTUM does not bear any financial liability and no warranties apply to the test certificates (and their content) issued within above policies. However, standard certificates issued within **Certum Level II CA** and **Certum Domain Validation CA SHA2** authorities have limited guarantees and liabilities.

2.2. OV Certificates (Organization Validation)

OV certificates are issued by intermediate authorites **Certum Level III CA, Certum Level VI CA** and **Certum Organization Validation CA SHA2.**

These certificates are intended mainly for securing electronic correspondence and protecting data transmission based on SSL/TSL protocols. These certificates are intended also for the certification authorities, non-repudiation authorities and global network-based electronic transaction systems.

CERTUM operates a procedure for verifying the identity of the subscriber that meets the *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* (http://www.cabforum.org/)

CERTUM verifies all data provided by the requesters during the certification process. Detailed information on identity verification requirements are described in **Certification Practice Statement of CERTUM's Certification Services** and on the website http://www.certum.eu.

It is possible to unambiguously verify the identity of subject, the authenticity of organization or the credibility of external certification authority on the basis of **OV** certificates.

End-users **OV** certificates contain following policy identifiers:

Authority Name	Policy Identifier
Certum Level III CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-III(3)
Certum Level IV CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-IV(4)
Certum Organization Validation CA SHA2	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5) id-ctn-certPolicy (1) id-certum-ov(2)
Certum Digital Identification CA SHA2	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5)} id-ctn-certPolicy(1) id-certum-di(6) adobe(11) iso(1) member-body(2) pl(616) organization(1) idunizeto(113527) id-ccert(2) id-ctnca(5)} id-ctncertPolicy(1) id-certum-di(6) basicid(12) iso(1) member-body(2) pl(616) organization(1) idunizeto(113527) id-ccert(2) id-ctnca(5)} id-ctncertPolicy(1) id-certum-di(6) professionalid(13) iso(1) member-body(2) pl(616) organization(1) idunizeto(113527) id-ccert(2) id-ctnca(5)} id-ctncertPolicy(1) id-certum-di(6) enterpriseid(14)

Financial responsibility of CERTUM for the data in the certificates issued within above policies is presented in **Certification Practice Statement of CERTUM's Certification Services** and on the website http://www.certum.eu. Certificates issued within these policies have full guarantees and liabilities.

2.3. EV Certificates (Extended Validation)

Certificates issued by **Certum Extended Validation CA, Certum Extended Validation CA SHA2** and **Certum Extended Validation Code Signing CA SHA2** provide a highest level of confidence the identity of the subscriber. The validation process requires to follow by the current version of the *Guidelines for the issuance and Management of Extended Validation Certificates* and the *Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates* requirements available at http://www.cabforum.org/.

EV SSL certificates are issued only to legal entities and intended for protecting data transmission based on SSL/TSL protocols.

EV Code Signing certificates are issued only to legal entities and intended for protecting an application/ software code. Additionally, subscribers' private keys must be generated and protected on external devices.

CERTUM verifies all data provided by the requesters during the certification process. Detailed information on identity verification requirements are described in **Certification Practice Statement of CERTUM's Certification Services** and on the website http://www.certum.eu.

It is possible to unambiguously verify the identity of subject and the authenticity of organization on the basis of **EV** certificates.

End-users **EV** certificates contain following policy identifiers:

Authority Name	**Policy Identifier**
Certum Extended Validation CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5) id-ctn-certPolicy (1) id-certum-ev(1)
Certum Extended Validation CA SHA2	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5) id-ctn-certPolicy (1) id-certum-ev(1)
Certum Extended Validation Code Signing CA SHA2	iso(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-code-signing-requirements(3) iso(1) member-body(2) pl(616) organization(1) idunizeto(113527) id-ccert(2) id-ctnca(5) id-ctncertPolicy (1) id-certum-evcs(7)

Financial responsibility of CERTUM for the data in the certificates issued within above policies is presented in **Certification Practice Statement of CERTUM's Certification Services** and on the website http://www.certum.eu. Certificates issued within this policy have full guarantees and liabilities.

2.4. Code Signing Certificates

Code Signing Certificates are issued by **Certum Code Signing CA**.

The usage of the code signing certificates is limited to code signing only. Additionally, subscribers' private keys must be generated and protected on external devices.

CERTUM operates a procedure for verifying the identity of the subscriber that meets the *Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates* (http://www.cabforum.org/)

CERTUM verifies all data provided by the requesters during the certification process. Detailed information on identity verification requirements are described in **Certification Practice Statement of CERTUM's Certification Services** and on the website http://www.certum.eu.

It is possible to unambiguously verify the identity of subject, the authenticity of organization or the credibility of external certification authority on the basis of **OV** certificates:

End-users **Code Signing** certificates contain following policy identifiers:

Authority Name	Policy Identifier
Certum Code Signing CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5) id-ctn-certPolicy (1) id-certum-code-signing(4)
Certum Code Signing CA SHA2	iso(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) code-signing-requirements(4) code-signing(1)

Financial responsibility of CERTUM for the data in the certificates issued within above policy is presented in **Certification Practice Statement of CERTUM's Certification Services** and on the website http://www.certum.eu. Certificates issued within this policy have full guarantees and liabilities.

2.5. External authorities certificates

Certificates for external CAs are issued by intermediate certification authorities **Certum GlobalServices CA** and **Certum Global Services CA SHA2**. Entities, whom such certificates are issued to, are subjected to thorough verification, carried out by Asseco Data Systems S.A.operators. Certificates issued by **Certum Global Services CA** and **Certum Global Services CA SHA2** authorities are valid for 10 years and require hardware protection of private keys. Policy identifiers have the following form:

Authority Name	**Policy Identifier**
Certum Global Services CA	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-global-services(9)
Certum Global Services CA SHA2	{iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5)} id-ctn-certPolicy (1) id-global-services(9)

Financial responsibility of CERTUM for the data in the certificates issued within above policy is specified in dedicated **agreements.**

3. Non-repudiation services

Non-repudiation token is a string of data (message) provided by the client to one of the non-repudiation authority, containing at least the following information: cryptographic hash, serial number of certificate, number of request, etc. and is signed electronically by that authority. Non-repudiation authorities, providing services for their clients are affiliated by the **Certum CA** and **Certum Trusted Network CA**.

Non-repudiation authority, upon token issuance, confirms the occurrence of an event in the past or in that very moment. It might be submission of the electronic document, participation in data exchange, date of signature creation, etc. On the basis of received data relying party accepts the certificate and verifies the correctness of the signature relying on the credibility of **Certum CA,Certum Trusted Network CA** and **Certum Trusted Network CA 2**

3.1. Time-Stamps

Time-stamps are issued by the intermediate authority **Certum EV TSA SHA2**. Time-stamps, as the confirmation of non-repudiation, are issued to private and commercial customers. Time stamps may be incorporated in the process of electronic signature creation, acceptance of electronic transactions, archive of the data, notary of electronic documents, etc. The regulations concerning operation of Time-Stamping Authority and additional information associated with the system are described in separate document (see **Certum Time-Stamping Authority Policy**).

Time stamp token contain identifier of the policy governing the issuance of the token. This identifier has the following form:

Authority Name	Policy Identifier
Certum Time-Stamping Authority	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum-tsa(5) 1 11

Financial responsibility of CERTUM for the date, time and additional information included in the timestamps issued within above policy is presented in **Time-Stamping Authority Policy, Certification Practice Statement of CERTUM's Certification Services** and on the website http://www.certum.eu**. Certum EV TSA SHA2** gives full guarantees for issued timestamps. Information concerning fees for timestamps are presented on the website http://www.certum.eu.

3.2. OCSP confirmation response

OCSP (*Online Certificate Status Protocol*) tokens are issued by intermediate authority **Certum Validation Service**. Each CERTUM certification authority has its own dedicated certificate status validation authority. Tokens, as confirmations of certificate status, are issued to private and commercial customers. OCSP may be incorporated mainly in the process of verification of certificate status. These services are available to public and are the alternative for the Certificate Revocation List (CRL). Information on OCSP authority operation and additional information concerning provided services are presented in **Certification Practice Statement of CERTUM's Certification Services** and on the website http://www.certum.eu. **Certum Validation Service** has the following policy identifier:

Authority Name	**Policy Identifier**
Certum Validation Service	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-dvcs(6)

4. CERTUM guarantees

Depending on type of issued certificate, CERTUM guarantees, that it uses reasonable efforts to verify information included in the certificates (see Certification Practice Statement – Chapter 9.6.1). This verification is particularly important from the point of view of the relying party, who is the addressee of subscriber's messages, confirmed with the certificates issued by CERTUM. Due to above, CERTUM is financially responsible for every damages resulting from CERTUM fault or negligence. Range of the liability and liability cap depends of the level of subscriber's certificate and might include not only the subscriber but the relying party as well.

CERTUM guarantees might be limited with many restrictions. Knowledge of this limitations is confirmed by the subscriber in appropriate statement (see Certificate Acceptance). CERTUM guarantees uniqueness of electronic signatures of its subscriber's.

5. Certificate Acceptance

CERTUM liabilities and guarantees are applicable since the moment of acceptance of the issued certificate by the subscriber. General provision and method of certificate acceptance are described in Certification Practice Statement of CERTUM's Certification Services, whereas detailed – in the subscriber's statement.

6. Certification Services

CERTUM, within its infrastructure, provides four basic certification services:

- registration and issuance of a certificate,
- renewal of the certificate,
- revocation of the certificate and,
- verification of certificate status.

Remaining non-repudiation services may be provided irrespectively of CERTUM services:

- Time-Stamping Authority (TSA),
- Notary Authority (DVCS),
- Electronic Vault,
- Delivery Authority,
- Online Certificate Status Protocol (OCSP).

Registration is intended for confirming identity of a subscriber and precedes issuance of a certificate (see Certification Practice Statement, Chapter 4.1 and Chapter 4.3).

Renewal of a certificate is used when registered subscriber wishes to obtain certificate of a new public key or modify any of the data contained within the certificate, e.g. email box address (see Certification Practice Statement, Chapter 4.7 and Chapter 4.8).

Revocation of a certificates is used when a private key associated with a public key contained within the certificate or a media used for the private key storage is or is suspected to be revealed (see Certification Practice Statement, Chapter 4.9).

Verification of certificate status applies CERTUM confirmation of validity of certificate issued by CERTUM and check against placement on CRL and certificate's validity period. Verification of certificate status may be also carried out by OCSP (see Certification Practice Statement, Chapter 4.9.9)

CERTUM requires every pair of keys (private and public) to be generated by the subscriber. CERTUM may recommend devices which allow key pair generation. In particular cases CERTUM might generate unique pair of keys on its own and deliver it to the subscriber.

7. Relying Party

Relying party is obligated to appropriately verify every electronic signatures created on the document (including the certificate), he/she/it receives. During verification process, relying party should incorporate procedures and resources available to public in CERTUM. It applies, among others, to the requirement of verification of CRL published by CERTUM and verification of certification paths (see Certification Practice Statement, Chapter 9.6.4).

Every document containing deficiency in an electronic signature or resulting from this deficiency doubts should be rejected or, optionally, subjected to other means or procedures of validity verification, e.g. notary verification.

8. Subscriber

The subscriber is obligated to securely store his/her/its private key, preventing it from being revealed to any third party. In case of the private key revelation or suspicion of such revelation, the subscriber must immediately notify the authority which issued his/her/its certificate. Information about the revelation must be delivered in the manner not arising doubts to the identity of the subscriber.

9. Certification Policy Update

CERTUM Certification Policy may be subjected to periodical modifications. These modifications will be available to all of the subscribers and their final content will be accepted by PKI Services Development Team. Subscribers who don't accept implemented modifications must submit appropriate statement to CERTUM and resign from services provided by CERTUM.

10. Fees

Certification services provided by CERTUM are commercial. Height of charged fees depend on the level of issued or owned certificate and of type of requested service. Fees are presented in the pricelist, available on the website http://www.certum.eu/.

Document's history

Document modification history		
V 1.0	15th of April, 2000	Draft of the document for the discussion
V 1.27	12th of March, 2002	Entire version of the document. Document approved
V 2.0	15th of July, 2002	Detailed definition of types of certificates. Addition of non-repudiation services.
V 2.1	1st of February, 2005	Extending the policy with services provided by intermediate authority of Certum Partners.
V 2.2	9th of May, 2005	Editorial changes. Change to the company legal form and name (Unizeto Sp. z o.o. changed to Unizeto Technologies S.A,)
V 2.3	26th of October, 2005	Change of service name and logo from Unizeto CERTUM – Centrum Certyfikacji to CERTUM – Powszechne Centrum Certyfikacji.
V 2.4	19th of May, 2006	Removal of the former legal status of the company. Transfer of the details of identification documents and procedures to dedicated document.
V 2.5	12th of May, 2008	Editorial changes, adjusting document to Certificate Practice Statement
V 3.0	19th of October, 2009	Extending the policy with services provided by intermediate authority of Certum Trusted Network CA
V 3.1	12th of August 2010	Updating the information about subscriber's verification.
V 3.2	7th of October, 2011	Adding information on the new Root certificate, Code Signing CA intermediate certificate and minor changes to the verification of Level I CA certificates.
V 3.3	19th of April, 2012	CERTUM logo update
V 3.4	01 June 2015	Added the new intermediate CAs.
V 3.5	03th of November 2015	Added the new iCERTUM root certification authority Certum Trusted Network CA EC and the intermediate authorities Certum Digital Identification CA SHA2 and Certum Extended Validation Code Signing CA SHA2
V 3.6	01 April, 2016	Transfer of ownership of Unizeto Technologies S.A. Asseco Data System S.A. Adding the information on obligation to maintain certification certificate issued by Unizeto Technologies S.A. Asseco Data System S.A.
V 3.7	22 August 2016	Added information about new time-stamping authority Certum EV TSA SHA2
V 3.8	01 February 2017	Update the code signing certificates policy. Updating the information on CA/Browser Forum requirements.
V 3.9	01 August 2017	Change of Asseco Data Systems S.A. address. Added new Certification policy identifiers.
V 4.0	11 August 2017	Added new Certification policy identifiers.
V 4.1	23 March 2018	Changed root name from Certum Trusted Network CA EC to Certum Elliptic Curve CA and added new root: Certum Trusted Root CA
V 4.2	26 March 2018	Added new root: Certum EC-384 CA