Certification Policy of Certum's Certification Services

Version 5.2
Effective date: 1 December 2025
Status: valid

Asseco Data Systems S.A.
Jana z Kolna 11
80-864 Gdańsk, Poland

Certum
Bajeczna 13
71-838 Szczecin, Poland
https://www.certum.eu

Trademark and Copyright notice

Content

1. Introduction

Certification Policy of Certum's Certification Services describes general rules and regulations applied by Certum for public key certification process, Time-Stamping Authority (TSA) and remaining non-repudiation services. The document defines the 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 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, their 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** oraz **Certum EC-384 CA**, **Certum TLS RSA Root CA, Certum S/MIME RSA Root CA, Certum Code Signing RSA Root CA, Certum Document Signing RSA Root CA, Certum TLS ECC Root CA, Certum S/MIME ECC Root CA, Certum Code Signing ECC Root CA, Certum Document Signing ECC Root CA.**

Each of 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 TLS RSA Root CA, Certum S/MIME RSA Root CA, Certum Code Signing RSA Root CA, Certum Document Signing RSA Root CA, Certum TLS ECC Root CA, Certum S/MIME ECC Root CA, Certum Code Signing ECC Root CA, Certum Document Signing ECC Root CA** upon indirectly issuing a certificate to the subscriber confirms their identity or the credibility of other data, such as email address. Authorities also confirm that the public key possessed by such subscriber is the property of this very subscriber. Thanks to this, the relying party, upon receiving the signed message, can identify the certificate holder who made the signature and, if necessary, hold them accountable for the actions they have taken or committed to.

Certum provides services in accordance with the *WebTrust*™ (see https://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 various classes with different levels of credibility. The credibility of a certificate depends on the procedure for verifying the subscriber's identity and the effort made by Certum to check the data submitted by the subscriber in the registration application. The more information that needs to be verified, and thus the more complex the procedure, the more credible the certificate.

The Subscriber is responsible for determining which type of certificate best meets their needs. Detailed descriptions of certificate types are available on the website https://www.certum.eu. Information can also be obtained by sending an inquiry to info@certum.pl.

2.1. DV Certificates (Domain Validation)

DV certificates are issued for two separate groups: free test certificates for a shorter period of validity and standard certificate with full validity period.

DV standard certificates are issued for protecting data transmission based on SSL/TSL protocols.

DV test certificates are intended mainly for application or device test performance prior to purchasing the final certificate.

The domain verification included in the certificate is carried out in accordance with the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, available at https://www.cabforum.org/.

Detailed verification requirements are presented on the website www.certum.pl and in the Certification Practice Statement for Certum Non-Qualified Services.

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

In **DV** certificates issued to end entities, a policy identifier (OID) is included to specify the policy under which the certificate has been issued.

Certificate Name	Policy Identifier
DV SSL – Test/Commercial	2.23.140.1.2.1 1.2.616.1.113527.2.101.1

2.2. OV Certificates (Organization Validation)

OV 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 TLS Server Certificates* (https://www.cabforum.org/)

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

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

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

Certificate Name	Policy Identifier
OV SSL - Trusted	2.23.140.1.2.2 1.2.616.1.113527.2.101.2

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 https://www.certum.eu. Certificates issued within these policies have full guarantees and liabilities.

2.3. EV Certificates (Extended Validation)

EV SSL certificates provide the highest level of confidence in the subscriber's identity. The subscriber identity verification at the time of certificate issuance is performed in accordance with the current version of the *Guidelines for the Issuance and Management of Extended Validation Certificates*, available at https://www.cabforum.org/

EV SSL certificates are dedicated exclusively to legal entities and are intended for securing data transmission based on SSL and TLS protocols.

Certum verifies all data provided by the entity during the certification process. Detailed requirements regarding applicant data verification are presented on the website https://www.certum.eu and in the Certification Practice Statement for Certum's Non-Qualified Certification Services.

EV SSL certificates allow for the unambiguous confirmation of the subject's identity, the authenticity of the organization, or the trustworthiness of an external certification authority.

EV certificates issued for end entities contain the policy identifier under which the certificate is issued.

Certificate Name	Policy Identifier
EV SSL - Premium	2.23.140.1.1 1.2.616.1.113527.2.101.3

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 https://www.certum.eu. Certificates issued within this policy have full guarantees and liabilities.

2.4. Code Signing Certificates

Code Signing certificates are intended exclusively for tasks related to signing code, drivers, or applications, and the private keys of Code Signing subscribers must be protected on external devices.

Certum verifies all data provided by the entity during the certification process. Subscriber validation is carried out in accordance with the current version of the *Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates*. Detailed requirements regarding data verification are presented on the website www.certum.pl and in the **Certification Practice Statement for Certum's Non-Qualified Certification Services**.

Certificates issued under the above policies allow for the unambiguous confirmation of the subject's identity, the authenticity of the organization, or the trustworthiness of an external certification authority.

Code Signing certificates issued for end entities contain the policy identifier under which the given certificate is issued.

Certificate Name	Policy Identifier
Open Source Code Signing	2.23.140.1.4.1 1.2.616.1.113527.2.5.1.4
Standard Code Signing	2.23.140.1.4.1 1.2.616.1.113527.2.5.1.4
EV Code Signing	2.23.140.1.3 1.2.616.1.113527.2.5.1.7

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 https://www.certum.eu.

2.5. S/MIME Certificates

S/MIME certificates are issued for securing electronic mail.

Certum verifies all data provided by the entity during the certification process. Subscriber validation is carried out in accordance with the current version of the *Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates*. Detailed information regarding the verification process is described in the **Certification Practice Statement** and on the website https://www.certum.pl

S/MIME certificates issued for end entities contain the policy identifier under which the given certificate is issued.

Certificate Name	Policy Identifier
S/MIME Individual	1.2.616.1.113527.2.100.1.1 2.23.140.1.5.4.2
S/MIME Mailbox/Test	1.2.616.1.113527.2.100.2.1 2.23.140.1.5.1.2
S/MIME Organization	1.2.616.1.113527.2.100.3.1 2.23.140.1.5.2.2
S/MIME Sponsor	1.2.616.1.113527.2.100.4.1

	2.23.140.1.5.3.2

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 https://www.certum.eu.

2.6. Certificates for the National Identity Node

Certificates for the **National Identity Node** *(pl. Krajowy Węzeł Identyfikacji Elektronicznej)* are intended to ensure secure communication and authentication within the national electronic identification system.

Certum verifies all data included in the certificate application. Detailed information regarding the verification process is provided in the **Certification Practice Statement for Certum's Non-Qualified Services** and on the website https://www.certum.pl

Certificates issued for the **National Identity Node** contain the policy identifier under which the given certificate is issued:

Certificate Name	Policy Identifier
National Identity Node, request signing *(Krajowy Węzeł Tożsamości, podpisywanie żądań)*	1.2.616.1.113527.2.5.1.6.14
National Identity Node, assertion decryption (Krajowy Węzeł Tożsamości, deszyfracja asercji)	1.2.616.1.113527.2.5.1.6.14

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 https://www.certum.eu.

Certificates for the **National Identity Node** support services operated within the Polish national electronic identification system and are issued solely for entities participating in this system.

2.7. Certificates for Document Signing

Document Signing certificates are intended for the electronic signing of documents to ensure their integrity, authenticity, and non-repudiation.

Certum verifies all data included in the certificate application in accordance with the rules described in the **Certification Practice Statement for Certum's Non-Qualified Services** and with consideration of the technical and procedural requirements of the *Adobe Approved Trust List (AATL)* program.

Document Signing certificates issued for end entities contain the policy identifier under which the given certificate is issued.

Certificate Name	Policy Identifier
Document Signing	1.2.616.1.113527.2.5.1.6.11

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 https://www.certum.eu.

3. Non-repudiation services

A non-repudiation token is a string of data (a message) provided by the client to a non-repudiation authority. It contains at least a cryptographic hash, the certificate's serial number, the request number, and other relevant information, and is electronically signed by that authority.

By issuing a non-repudiation token, the non-repudiation authority confirms that a specific event has occurred in the past or at the moment of issuance. Such an event may include the submission of an electronic document, participation in an electronic data exchange process, the time of creation of an electronic signature, etc.

3.1. Time-Stamps

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 the operation of Time-Stamping Authority and additional information associated with the system are described in a separate document (see **Certum Time-Stamping Authority Policy**).

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 https://www.certum.eu**.**

3.2. OCSP confirmation response

OCSP (*Online Certificate Status Protocol*) confirmations are issued by dedicated validation authorities. Each Certum certification authority operates its own dedicated certificate status validation authority. Certificate status confirmations are issued both to individual users and commercial customers. They are primarily used in certificate validation processes. These services are publicly available and serve as an alternative to Certificate Revocation Lists (CRLs).

The operating rules of the OCSP authority, as well as additional information, are described in the Certification Practice Statement for Certum's Non-Qualified Services and on the website: https://www.certum.eu.

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 damage resulting from Certum fault or negligence. Range of the liability and liability cap depends on 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 these limitations is confirmed by the subscriber in an appropriate statement (see Certificate Acceptance). Certum guarantees uniqueness of electronic signatures of its subscriber's.

5. Certificate Acceptance

Certum liabilities and guarantees are applicable from 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 certificate may occur for various reasons (see **Certification Practice Statement**, Chapter 4.9). In particular, revocation is always required when the private key associated with the public key contained in the certificate, or the medium on which it is stored, has been compromised or there is a justified suspicion that it has been compromised.

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.

7. Relying Party

The relying party is obligated to appropriately verify every electronic signature created on the document (including the certificate), he/she/it receives. During verification process, the relying party should incorporate procedures and resources available to the 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 doubt 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 their 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 their certificate. Information about the revelation must be delivered in a manner that does not arise doubts about 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 the subscribers, and their final content will be accepted by the Director of Trust Services Division. Subscribers who don't accept implemented modifications must submit an appropriate statement to Certum and resign from services provided by Certum.

10. Fees

Certification services provided by Certum are commercial. The amount of fees depends on the level of the certificate and the type of certification service requested and is available in the price list on the website https://www.certum.eu.

Revision 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 CERTUM 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
V 4.3	24 January 2019	Update of legal base and point 2 – adaptation to current technical possibities.
V 4.4	21 February 2019	Added section 2.5 about S/MIME certificates

V 4.5	19 February 2020	Update after annual review of the document.
V 4.6	19 February 2021	Update after annual review of the document.
V 4.7	29 September 2021	Update of company address
V 4.8	28 September 2022	Update after annual review of the document.
V 4.9	09 February 2023	Added new Root CA: Certum CA, Certum Trusted Network CA, Certum Trusted Network CA 2, Certum Elliptic Curve CA, Certum Trusted Root CA oraz Certum EC-384 CA, Certum TLS RSA Root CA 2022, Certum S/MIME RSA Root CA 2022, Certum Code Signing RSA Root CA 2022, Certum Document Signing RSA Root CA 2022, Certum TLS ECC Root CA 2022, Certum S/MIME ECC Root CA 2022, Certum Code Signing ECC Root CA 2022, Certum Document Signing ECC Root CA 2022, update point 9 Certification Policy Update
V 5.0	01 September 2023	Adaptation to the provisions of Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, update of certification policies.
V 5.1	6 December 2024	Update after annual review of the document.
V 5.2	1 December 2025	Added sections 2.6 and 2.7; update of Certum Root CAs; update of policy identifiers; editorial corrections.