Certificate Policy and Certification Practice Statement for TLS Certificates

Certum

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

Version 1.0.0

Date of publication 2026-04-29

Table of contents

1. INTRODUCTION

Asseco Data Systems S.A. operating as Certum, the legal successor to Unizeto Technologies S.A., is the Certification Authority (CA) providing services for all core Public Key Infrastructure (PKI) operations, including receiving certification requests, issuing certificates, revoking certificates, publishing Certificate Revocation Lists (CRLs), and providing real-time status verification through OCSP services.

1.1 Overview

This combined Certificate Policy (CP) and Certification Practice Statement (CPS) document (CP/CPS) defines the policies, principles, and practices related to Certum's publicly trusted TLS certification services.

The Certum Public Key Infrastructure (Certum PKI) issues publicly trusted TLS certificates at the following levels of assurance: Domain Validated (DV), Organization Validated (OV), and Extended Validation (EV), as defined in the applicable CA/B Forum requirements.

Certum conforms to the latest published version of CA/B Forum Baseline Requirements:

- The CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates (TLS BR) - https://cabforum.org/working-groups/server/baseline-requirements/documents/
- The CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates (EV Guidelines) - https://cabforum.org/extended-validation
- The CA/B Forum Network and Certificate System Security Requirements - https://cabforum.org/network-security-requirements

Certum conforms to the latest published version of root store policies of major application software suppliers, including:

- Apple Root Store Program - https://www.apple.com/certificateauthority/ca_program.html
- CCADB Policy - https://www.ccadb.org/policy
- Chrome Root Program Policy - https://googlechrome.github.io/chromerootprogram/
- Microsoft Root Program Requirements - https://github.com/TrustedRootProgram/Program-Requirements/blob/main/Requirements.md
- Mozilla Root Store Policy - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

If any inconsistency exists between this document and the normative provisions of an applicable industry guideline or standard (applicable requirements), then the applicable requirements take precedence over this CP/CPS.

If any inconsistency exists between this document (applicable to TLS certificates) and the *Certification Practice Statement of Certum's Certification Services* or *Certification Policy of Certum's Certification Services*, both governing all certificates issued by Certum (being documents progressively superseded by dedicated, single-purpose CP/CPS documents) this document shall take precedence.

1.2 Document name and identification

This document is titled *Certificate Policy and Certification Practice Statement for TLS Certificates* (referred to as the CP/CPS). It is a public document that describes the practices and policies of Certum for its publicly trusted TLS certification services.

This document is structured in accordance with the Internet Engineering Task Force (IETF) standard RFC 3647.

The OID arc for Certum is 1.2.616.1.113527.2.

```
{iso(1) member-body(2) pl(616) organization(1) unizeto(113527) 2(2)}
```

See Section 7.1 for a Certificate Policy object identifiers.

See Appendix A for a list of revisions to this document.

1.3 PKI participants

1.3.1 Certification authorities

Certum is the sole operator of all Root Certification Authorities (Root CAs) and Subordinate Certification Authorities (Subordinate CAs) dedicated to Certum's publicly trusted TLS certification services.

- Root CAs are used to issue Subordinate CAs
- Subordinate CAs are used to issue end-entity certificates

All certification authorities operate within its PKI, including certificate issuance, revocation, and maintenance of CRLs and OCSP services.

1.3.1.1 Certum Root CA

Certum Trusted Network CA (G1)

- Key: RSA 2048
- Serial Number: 279744 (0x444c0)
- SHA-256 Fingerprint: 5C:58:46:8D:55:F5:8E:49:7E:74:39:82:D2:B5:00:10:B6:D1:65:37:4A:CF:83:A7:D4:A3:2D:B7:68:C4:40:8E
- Valid until: 2029-12-31

Certum Trusted Network CA 2 (G1)

- Key: RSA 4096
- Serial Number: 21:d6:d0:4a:4f:25:0f:c9:32:37:fc:aa:5e:12:8d:e9
- SHA-256 Fingerprint: B6:76:F2:ED:DA:E8:77:5C:D3:6C:B0:F6:3C:D1:D4:60:39:61:F4:9E:62:65:BA:01:3A:2F:03:07:B6:D0:B8:04
- Valid until: 2046-10-06

Certum Trusted Root CA (G2)

- Key: RSA 4096
- Serial Number: 1e:bf:59:50:b8:c9:80:37:4c:06:f7:eb:55:4f:b5:ed
- SHA-256 Fingerprint: FE:76:96:57:38:55:77:3E:37:A9:5E:7A:D4:D9:CC:96:C3:01:57:C1:5D:31:76:5B:A9:B1:57:04:E1:AE:78:FD
- Valid until: 2043-03-16

Certum EC-384 CA (G2)

- Key: ECC 384
- Serial Number: 78:8f:27:5c:81:12:52:20:a5:04:d0:2d:dd:ba:73:f4
- SHA-256 Fingerprint: 6B:32:80:85:62:53:18:AA:50:D1:73:C9:8D:8B:DA:09:D5:7E:27:41:3D:11:4C:F7:87:A0:F5:D0:6C:03:0C:F6
- Valid until: 2043-03-26

Certum TLS RSA Root CA (G3)

- Key: RSA 4096
- Serial Number: e7:dd:21:38:a2:c9:41:46:ff:5f:12:17:89:95:05:53
- SHA-256 Fingerprint: ED:12:A6:E9:28:92:39:D6:6C:A1:D2:44:CE:90:C6:23:AC:30:5A:D0:56:02:DA:35:2B:CF:C5:FE:F2:C4:45:8D
- Valid until: 2048-01-26

Certum TLS ECC Root CA (G3)

- Key: ECC 384
- Serial Number: b0:7e:c0:cb:2e:05:e6:3c:71:da:0d:7f:99:79:71:f3
- SHA-256 Fingerprint: 63:0C:CB:83:B0:18:0A:99:24:95:E0:39:D2:61:3C:32:87:A8:10:2F:8A:8D:70:3D:B1:33:0A:3E:86:D4:E6:53
- Valid until: 2048-01-26

1.3.1.2 Certum cross-signed CA

For the purpose of backward compatibility with older versions of major application software suppliers' root stores, Certum has issued cross-certificates between its own Root CAs:

G1 → G1

Certum Trusted Network CA (G1) → Certum Trusted Network CA 2 (G1)

- Key: RSA 4096
- Serial Number: 1b:b5:8f:25:2a:df:23:00:49:28:c9:ae:3d:7e:ed:27
- SHA-256 Fingerprint: 08:E7:EA:C9:98:A6:2C:41:55:CC:4C:BC:5E:DA:32:F5:B4:1A:12:C0:12:F2:9A:B3:43:3B:D3:66:34:81:49:F0
- Valid until: 2029-09-17

G1 → G2

Certum Trusted Network CA (G1) → Certum Trusted Root CA (G2)

- Key: RSA 4096
- Serial Number: d8:e0:74:4b:58:24:91:9f:bd:08:84:7d:f7:20:20:fa
- SHA-256 Fingerprint: FB:13:89:0C:7A:B1:4F:F7:B9:4B:27:14:50:3E:31:12:3B:FD:D3:40:FC:4D:97:97:43:16:6E:04:69:B4:7A:88
- Valid until: 2028-09-19

Certum Trusted Network CA (G1) → Certum EC-384 CA (G2)

- Key: ECC 384
- Serial Number: da:fd:4b:f5:41:21:e0:27:d6:86:96:22:5f:1f:ce:e8
- SHA-256 Fingerprint: B7:24:50:AB:F5:04:7A:8A:F6:3E:C9:D8:7E:33:14:84:85:0B:18:49:A2:55:0A:82:A8:6D:B6:B4:1E:D3:87:60
- Valid until: 2028-09-19

G1 → G3

Certum Trusted Network CA (G1) → Certum TLS RSA Root CA (G3)

- Key: RSA 4096
- Serial Number: cd:26:56:ac:6b:5b:52:19:3a:d2:3a:f6:6d:52:0a:a3
- SHA-256 Fingerprint: EB:0C:60:FD:1B:A9:55:59:18:40:FB:7B:56:3A:DB:46:50:1B:E8:E7:59:29:64:D8:FF:79:D4:79:D3:62:1D:10

- Valid until: 2029-12-30

Certum Trusted Network CA (G1) → Certum TLS ECC Root CA (G3)

- Key: ECC 384
- Serial Number: a3:b6:74:50:69:73:1e:98:7a:04:71:18:b5:83:06:cd
- SHA-256 Fingerprint:
  E4:EF:90:ED:90:3D:C9:87:6B:0A:0B:C9:A8:DE:21:D9:FD:04:1E:31:1A:16:0D:C7:F2:
  DB:C7:AB:98:7D:CA:14
- Valid until: 2029-12-30

G2 → G3

Certum Trusted Root CA (G2) → Certum TLS RSA Root CA (G3)

- Key: RSA 4096
- Serial Number: 34:8f:d5:3b:17:f7:f4:76:8a:95:35:0c:16:b4:2d
- SHA-256 Fingerprint:
  23:3B:E8:34:67:8F:98:81:2F:50:3E:94:D9:B5:21:AE:AC:33:AA:9B:EE:1B:8B:A2:0C:D
  5:B2:D9:8F:33:98:A8
- Valid until: 2036-04-15

Certum EC-384 CA (G2) → Certum TLS ECC Root CA (G3)

- Key: ECC 384
- Serial Number: 0e:1c:85:7b:dc:cf:72:be:af:2b:cf:64:8f:85:71:85
- SHA-256 Fingerprint:
  1E:78:33:B1:74:7E:F5:BE:C0:6F:C2:23:7D:B8:1E:91:F2:3D:E8:16:1D:37:59:F9:A9:49
  :33:4F:92:8D:59:70
- Valid until: 2036-04-15

1.3.1.3 Certum Subordinate CA

Certum Subordinate CAs under G2 and G3 hierarchies are issued in a following structure, to separate the different levels of assurance for TLS certificates:

- Subordinate CA for DV TLS
- Subordinate CA for OV TLS
- Subordinate CA for EV TLS

1.3.2 Registration authorities

Registration Authorities (RAs) are entities that perform identification and authentication of certificate Applicants, verify their authorization to request certificates, and support the approval of certificate issuance and revocation requests.

Certum acts as the sole Registration Authority (RA) and performs all identification and authentication activities directly, including domain name and IP address validation. Certum does not delegate these validation functions to third parties.

Certum may utilize trusted third-party verification processes to support the validation of Applicant identity where required. Such processes do not constitute separate RAs. Certum reviews all collected information and makes the final decision regarding validation and certificate issuance.

1.3.3 Subscribers

A Subscriber is a natural person or legal entity that has been issued a certificate and holds or controls the private key.

Subscribers are required to act in accordance with Subscriber Agreement or Terms of Use, including:

- Provide accurate and truthful information
- Promptly notify Certum of any change in the information included in the certificate
- Ensure protection of the private key
- Use the certificate in accordance with this CP/CPS
- Promptly notify Certum of any suspected key compromise
- Immediately cease use of the certificate upon expiration or revocation

1.3.4 Relying parties

A relying party is any natural person or legal entity that relies on a TLS certificate issued by Certum to verify a server's identity or establish a secure, encrypted communication channel.

Prior to relying on any certificate, a relying party should:

- Verify the status of the certificate and all certificates in its chain using the applicable CRL or OCSP services provided by Certum
- Read and understand the terms of this CP/CPS

1.3.5 Other participants

Other participants are entities that provide services in support of Certum's PKI but do not act as Certification Authorities, Registration Authorities, Subscribers, or relying parties.

Such participants MAY include, but are not limited to:

- Providers of certificate status services (e.g., OCSP responders and CRL distribution services)
- Providers of repositories and publication services
- Infrastructure and service providers supporting PKI operations
- Business partners, including authorized resellers

All other participants are required to act in accordance with applicable agreements and this CP/CPS.

1.4 Certificate usage

1.4.1. Appropriate certificate uses

TLS certificates issued under this CP/CPS shall be used for the purposes of:

- Server authentication - establishing a secure TLS channel between a Subscriber's server and relying parties
- Client authentication - verifying the identity of individuals, organizations, or devices in mutual TLS (mTLS) scenarios, where permitted by the applicable certificate profile

Permitted usage MUST align with the Key Usage (KU) and Extended Key Usage (EKU) extensions defined in the certificate profile, as well as applicable laws and Subscriber Agreement or Terms of Use.

The level of assurance depend on the validation type:

- Domain Validation (DV) TLS certificates are suitable for low-risk environments, due to the identity of the Subscriber not being verified beyond their control of the domain
- Organization Validation (OV) TLS certificates are suitable for medium-risk environments where assurance of both domain control and the legal existence of the organization is required
- Extended Validation (EV) TLS certificates are suitable for high-risk environments and provide the highest level of assurance, following The EV Guidelines to verify the legal, physical, and operational existence of the entity

1.4.2 Prohibited certificate uses

Certificates issued under this CP/CPS shall not be used for any of the following purposes:

- High-risk infrastructure (Fail-safe) - any application requiring fail-safe performance where certificate failure could lead to death, personal injury, or catastrophic environmental damage
- Unauthorized interception - Man-in-the-Middle (MITM) purposes or surreptitious traffic interception without the explicit permission of the domain registrant
- Improper identity assurance - utilizing Domain Validated (DV) TLS certificates as proof of the legal existence or organizational identity of the Subscriber
- PKI Infrastructure roles - acting as a Certification Authority (CA) or using end-entity certificates to sign or issue other certificates or CRLs
- Technically unintended use - any application outside the scope defined by the Key Usage (KU) and Extended Key Usage (EKU) extensions in the certificate profile
- Illegal activities - any purpose that is inconsistent with applicable laws, regulations, or export/import restrictions

Disclaimer: By issuing a certificate, Certum confirms only that the information was verified at the time of issuance and does not provide a guarantee of the Subscriber's ongoing honesty, reliability, or trustworthiness.

1.5 Policy administration

1.5.1 Organization administering the document

This CP/CPS is administered by Certum Policy Authority.

The official address of the organization is:

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

1.5.2 Contact person

Questions, comments, or requests regarding this CP/CPS shall be directed to Certum using the following contact details:

Certum Certification Authority
Certum Policy Authority
ul. Bajeczna 13
71-838 Szczecin
Poland

Email: policy.pki@certum.pl

To report certificate-related issues, including revocation requests or concerns regarding this CP/CPS, Certum provides a Certificate Problem Report available at:

https://problemreport.certum.pl

This channel should be used for submitting Certificate Problem Reports, including suspected certificate misuse, compromise, or non-compliance.

1.5.3 Person determining CPS suitability for the policy

The Certum Policy Authority determines the suitability and applicability of this CP/CPS.

1.5.4 CPS approval procedures

This CP/CPS is approved and amended by the Certum Policy Authority.

This CP/CPS becomes effective upon its publication in the official Certum repositories.

All modifications, including editorial updates and changes required by regulatory or industry standards, are recorded in the revision history of this document.

1.6 Definitions and acronyms

See Appendix B for a list of definitions and acronyms.

1.6.1 Definitions per RFC 2119

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this CP/CPS shall be interpreted in accordance with RFC 2119.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Certum operates and maintains a publicly accessible Repository accessed at:

https://www.certum.eu/en/repository/ and https://repository.certum.pl/

Audit Attestation Letters are published at:

https://support.certum.eu/en/cert-about-us-about-webtrust/

2.2 Publication of certification information

Certum publishes a comprehensive set of documentation which includes but is not limited to:

- This combined CP/CPS and CP and CPS documents for other services
- Publicly trusted Root CA certificates, cross-signed CA certificates and Subordinate CA certificates
- Terms of Use
- Privacy Policy
- Reliable Data Sources
- Templates and sample documents

Certificate Revocation Lists (CRLs) available at distribution points specified in each certificate, all are available at:

https://crl.certum.pl

Online Certificate Status Protocol (OCSP) checking is available at:

https://ocsp.certum.pl

2.3 Time or frequency of publication

CP/CPS is reviewed at least once every 365 days or whenever changes in industry standards (such as CA/B Forum requirements) necessitate an update and is published after approval, typically within 7 days of approval.

The publicly trusted Root CA certificates, cross-signed CA certificates and Subordinate CA certificates are published as soon as possible after issuance.

Audit Attestation Letters are published according to Section 8.6.

CRLs are published according to Section 4.9.7.

Other updates are published as soon as possible after creation or update, typically within 7 days of approval.

2.4 Access controls on repositories

The information published in the Certum Repository is publicly available, unrestricted and continuously accessible.

Certum applies both logical and physical security controls to prevent unauthorized modification, deletion, or tampering with Repository contents.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

For Domain Validation (DV) TLS certificates, the Distinguished Name (DN) information MUST be limited to domain-related identifiers and MUST NOT include organization identity information.

For Organization Validation (OV) TLS and Extended Validation (EV) TLS certificates, the Distinguished Name (DN) MUST include verified organization identity information in accordance with the applicable certificate profile described in Section 7.1.

Subject Alternative Names (SAN) extension MUST include a Fully-Qualified Domain Name (FQDN) and/or an IP address.

3.1.2 Need for names to be meaningful

Certum requires that names contained in certificates be meaningful and permit the identification of the subject.

Certificate requests containing names that are misleading, ambiguous, exceed the scope of the performed validation, or cannot be validated will be rejected.

3.1.3 Anonymity or pseudonymity of Subscribers

Certum does not issue certificates containing anonymous or pseudonymous subject information.

3.1.4 Rules for interpreting various name forms

Distinguished Names in certificates are interpreted using X.500 standards and ASN.1 syntax.

Domain names are interpreted in accordance with applicable DNS standards.

Organization identity information containing non-ASCII characters MAY be normalized or transliterated into ASCII equivalents (e.g., replacing characters such as “ę” with “e” or “ö” with “oe”).

Commonly recognized language variants or translations of geographic names MAY be accepted (e.g., “Warsaw” instead of “Warszawa”).

3.1.5 Uniqueness of names

Unique subject names are not enforced.

3.1.6 Recognition, authentication, and role of trademarks

Certum does not issue certificates containing names, trademarks, or other identifiers that the Applicant is not entitled to use.

Disputes concerning trademarks or naming rights are not adjudicated. In cases of conflict or uncertainty, certificate requests MAY be rejected or issued certificates MAY be revoked.

3.2 Initial identity validation

Certum MAY request documentation from the Applicant to support the validation of a certificate request in accordance with the requirements applicable to the requested certificate type.

Any indication of document alteration, falsification, or misrepresentation of identity or status constitutes grounds for rejection of the certificate request and MAY result in revocation of any certificates issued based on such information.

3.2.1 Method to prove possession of private key

The Applicant proves possession of the private key corresponding to the public key included in the certificate request through the submission of a Certificate Signing Request (CSR) in PKCS#10 format.

3.2.2 Authentication of organization identity

3.2.2.1 Identity

Certum verifies the legal identity of organizations for all OV and EV TLS certificates using reliable and independent sources, such as government registries or qualified business databases.

A list of approved sources is maintained at:

https://www.certum.eu/en/organization-validation-sources

Verification confirms:

- The legal existence of the organization
- The full legal name as recorded in official registries
- The registered address or address of existence/operation

For EV TLS certificates, enhanced verification procedures are applied. These procedures include additional verification of:

- The legal existence of the organization within its jurisdiction
- The organization’s operational existence
- The organization’s physical address

All verification actions and evidence are recorded and retained for audit purposes. Information used for organization validation remains valid for a maximum period according to Section 4.2.1.

Certum MAY request or accept additional official documentation not explicitly listed above, where necessary to ensure reliable and accurate verification of the information provided in the certificate application.

3.2.2.2 DBA/Trade Name

An Applicant MAY request inclusion of a trade name (also referred to as a "Doing Business As" or DBA name) in a certificate.

Certum verifies the Applicant's right to use the requested trade name using methods described in Section 3.2.2.1 or

- An attestation letter accompanied by documentary support; or form of identification that the Certum determines to be reliable
- A utility bill, bank statement, credit card statement, government issued tax document, or other form of reliable identification

Such verification confirms that the trade name is registered, legally recognized, or otherwise associated with the Applicant.

3.2.2.3 Verification of Country

Certum verifies the country by verifying the address using the methods described in Section 3.2.2.1.

3.2.2.4 Validation of Domain Authorization or Control

Certum verifies the Applicant's control over each domain name included in the certificate request. This verification is performed prior to certificate issuance and is conducted exclusively within Certum Systems and it is not delegated to third parties.

Certum supports following methods defined in the TLS BR:

- 3.2.2.4.4 Email to a Constructed Address
- 3.2.2.4.7 DNS Change
- 3.2.2.4.18 Agreed-Upon Change to Website v2
- 3.2.2.4.19 Agreed-Upon Change to Website - ACME

Additionally Certum MAY perform validation procedure with checks against additional data sources and blacklists.

3.2.2.5 Authentication for an IP Address

Certum verifies the Applicant's control over each IP address included in the certificate request. This verification is performed prior to certificate issuance and is conducted exclusively within Certum Systems and it is not delegated to third parties.

Certum supports following methods defined in the TLS BR:

- 3.2.2.5.1 Agreed-Upon Change to Website
- 3.2.2.5.6 ACME "http-01" method for IP Addresses

Additionally Certum MAY perform validation procedure with checks against additional data sources and blacklists.

3.2.2.6 Wildcard Domain Validation

A wildcard domain name is defined as a string starting with an asterisk and a full stop (*.) followed by a Fully-Qualified Domain Name (FQDN).

If the FQDN portion of any wildcard domain name is "registry-controlled" label or a "public suffix", such as *.com or *.pl, Certum MUST reject the certificate request unless the Applicant proves its rightful control of the entire Domain Namespace.

Wildcard domain names are strictly prohibited for EV TLS certificates.

3.2.2.7 Data Source Accuracy

Before any data source is used as a Reliable Data Source, Certum evaluates the source for reliability, accuracy, and resistance to alteration or falsification.

The list of approved data sources is reviewed at least annually. Following each review, an updated version of the list is published on Certum's website.

3.2.2.8 CAA Records

Certum MUST retrieve and process CAA records in accordance with RFC 8659 for each dNSName in the subjectAltName extension that does not contain an onion domain name.

CAA record checking is performed in conjunction with the domain control validation process and MUST be successfully completed before any certificate issuance.

3.2.2.9. Multi-Perspective Issuance Corroboration

Certum implements Multi-Perspective Issuance Corroboration (MPIC) to corroborate the determinations made during domain validation (Section 3.2.2.4) and CAA checking (Section 3.2.2.8) from multiple remote network perspectives before certificate issuance.

Network perspectives are selected to ensure geographic diversity, with a minimum straight-line distance of at least 500 km between them.

3.2.3 Authentication of individual identity

Certum does not issue TLS certificates to natural persons.

3.2.4 Non-verified Subscriber information

Certum does not include unverified information in TLS certificates.

3.2.5 Validation of authority

For certificate requests that include an organization name, Certum verifies that the Applicant is authorized to act on behalf of the named legal entity at the time of issuance and possesses the right to represent the entity.

Verification of the individual's identity and authority is performed using Reliable Data Sources, official documentation (such as authorizations, powers of attorney, or employment certificates), or through a reliable method of communication (such as telephone or email) with an authoritative source within the organization.

3.2.6 Criteria for interoperation

Certum MAY provide interoperation services to certify external Certification Authorities (CAs). Such interoperation MAY include cross-certification or other forms of trust establishment.

Interoperation is permitted only if the following criteria are met:

- The external CA operates under a Certificate Policy (CP) and Certification Practice Statement (CPS) that is compatible with or at least as strict as this CP/CPS
- Certum performs a due diligence assessment of the external CA to ensure it meets Certum's security and operational requirements
- A formal agreement is in place between Certum and the external CA, defining the mutual rights and obligations of the parties

All cross-certificates issued by Certum are disclosed in the Certum Repository and to the Common CA Database (CCADB).

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Subscribers MAY request a re-key of certificate. Authorization for re-key MAY be established through submission of a certificate request using a Certum System.

For re-key requests, Certum MAY perform revalidation of the Applicant but MAY also rely on information obtained during the previous identification process.

3.3.2 Identification and authentication for re-key after revocation

If a certificate is revoked and revocations is unrelated to security incidents, Subscribers MAY submit a new re-key request. This request is treated as routine re-key and is subject to the same identification and authentication requirements as described in Section 3.3.1.

3.4 Identification and authentication for revocation request

The party that manages the Certum System account to which certificate is issued MAY request revocation by authenticating to a Certum System and requesting revocation via that system.

Anyone may request revocation by Certificate Problem Report web form. This requires passing additional verification steps conducted by Certum using methods described in Section 3.2.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

A certificate application may be submitted by the Applicant or by a person authorized to act on behalf of the Applicant. The Applicant is responsible for the accuracy of all information provided.

Certum does not issue certificates to Applicants located in jurisdictions where issuance would violate the laws of the Republic of Poland or applicable international sanctions.

4.1.2 Enrollment process and responsibilities

The enrollment process MAY include:

- Submission of a certificate Application
- Generation of a key pair
- Submission of a public key
- Acceptance of the applicable Terms of Use or Subscriber Agreement
- Provision of supporting documentation, as required
- Payment of applicable fees

The Applicant is responsible for providing accurate and complete information in the certificate Application and for fulfilling all requirements of the enrollment process.

Failure to provide accurate information or to comply with these requirements MAY result in rejection of the certificate Application.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Certum performs identification and authentication procedures during the processing of each certificate application to verify the identity and authority of the Applicant in accordance with the methods described in Section 3.2.

All identification and authentication procedures MUST be successfully completed prior to the issuance of a certificate.

If the necessary data is not available from trusted internal sources, Certum obtains it directly from the Applicant or from Reliable Data Sources.

Certum MAY reuse validation data and documentation obtained during previous identification processes, provided that such information remains accurate and was obtained no more than 398 days prior to the issuance date.

Certum maintains documented procedures to identify high-risk certificate requests that require additional verification activity prior to approval. These procedures include maintaining an internal database of previously revoked certificates and rejected applications associated with suspected phishing, fraud, or other malicious concerns. Certum MAY reject certificate applications based on this data.

4.2.2 Approval or rejection of certificate applications

Certum MAY approve certificate applications only when all provided information is successfully validated.

Certum MUST NOT issue a certificate including internal names or IP addresses marked as reserved by IANA.

Certum MAY reject a certificate application for any reason, including but not limited to:

- Certificate application containing a new gTLD that is still under consideration by ICANN
- The Applicant provides false or misleading information, or submits altered or falsified documentation
- Certificate application is identified as high-risk or potentially fraudulent
- Issuance of the certificate would pose legal, regulatory, security, or reputational risk to the CA or to the trust ecosystem
- The Applicant failing to complete Identification and Authentication procedures within 30 days of submission of the certificate application

Applicants whose applications have been rejected may subsequently reapply.

The Applicant SHALL not be entitled to any refund or compensation where false or misleading information has been provided or falsified documentation has been submitted.

4.2.3 Time to process certificate applications

Certum makes reasonable efforts to process certificate applications and issue certificates within 7 business days from the receipt of a complete application, provided that the issuance time for a given type of certificate is specified on Certum's website.

The actual processing time is primarily dependent on:

- The Applicant's responsiveness in providing necessary details and explanations
- The completeness and accuracy of the submitted application
- The availability of information from Reliable Data Sources

Certum MAY extend the processing time or reject an application if the Applicant fails to provide the required documentation within a reasonable timeframe or if complications arise during the verification process.

Certum SHALL NOT be held responsible for delays resulting from events outside of its reasonable control.

4.2.4 Certificate Authority Authorization (CAA)

As part of the TLS certificate issuance process, Certum validates Certification Authority Authorization (CAA) DNS records for each `dNSName` included in the `subjectAltName` extension of the certificate to be issued.

CAA records are validated in accordance with: - RFC 8659 and TLS BR Section 3.2.2.8

Certum recognizes the following issuer domain names in CAA “issue” or “issuewild” property tags as granting authorization for issuance by Certum:

- certum.pl
- certum.eu

Certum recognizes `accounturi` and `validationmethods` parameters, in accordance with RFC 8657.

Parameter `accounturi` must have format of URL: - For certificate requests issued by ACME: - `https://acme.certum.pl/account/{account identifier}` - For certificate requests not issued by ACME: - `https://certmanager.certum.pl/account/{account identifier}`

Parameter `validationmethods` must have value of:

- For certificate requests issued by ACME:

Domain Name Validation Methods	Supported values
Agreed-Upon Change to Website - ACME	http-01ca-tbr-19
DNS Change	dns-01ca-tbr-7

- For certificate requests not issued by ACME:

Domain Name Validation Methods	Supported values
Agreed-Upon Change to Website v2	ca-tbr-18
DNS Change	ca-tbr-7
Constructed Email to Domain Contact	ca-tbr-4

A Certificate shall not be issued if any of the following conditions is met: - CAA record does not authorize Certum - CAA record contains an unrecognized property with the critical flag set - CAA record does not authorize requesting account - CAA record does not authorize chosen domain name verification method - CAA record contains parameter `accounturi` and/or `validationmethods` in a format that does not comply with RFC 8657

Failures in CAA record lookup or validation do not constitute authorization to issue a Certificate.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Certum SHALL perform certificate issuance only after successful completion of the validation procedures applicable to the certificate type, as specified in Section 3 and Section 4.2.

Precertificates are subject to pre-issuance linting to verify technical conformity. The pre-issuance linting uses industry-recognized tools, including ZLint and pkilint. If a non-conformity is detected, issuance is halted.

Linting process may be used to verify technical conformity of final certificates.

Precertificates are submitted to Certificate Transparency logs in accordance with applicable requirements.

Certificate issuance by a Root CA requires deliberate action by authorized personnel in Trusted Roles to perform certificate signing operation.

4.3.2 Notification to Subscriber by the CA of issuance of certificate

Certum may notify the Applicant of the issuance of the certificate by email or alternative means how to obtain the certificate. This notification does not include the certificate itself.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The Subscriber is responsible for reviewing the contents of the issued certificate, including verification of the accuracy of the information contained therein and the correspondence of the public key with the associated private key.

A certificate is deemed accepted when the Subscriber:

- Downloads and installs on server or uses the certificate in any cryptographic operation, or
- 7 days from the date the certificate is made available

Acceptance of the certificate constitutes the Subscriber's declaration that, prior to using the certificate, the Subscriber has reviewed this CP/CPS and agrees to comply with it and with the applicable Terms of Use or Subscriber Agreement.

4.4.2 Publication of the certificate by the CA

All Publicly trusted Root CA certificates, cross-signed CA certificates and Subordinate CA certificates are published in the Certum Repository described in Section 2.1.

Certum makes end-entity certificates available to Subscribers via the Certum Systems.

4.4.3 Notification of certificate issuance by the CA to other entities

Information about certificates intended for use is made available to the public via the publication of pre-certificates to Certificate Transparency logs. Certum does not guarantee issuance of a final certificate for every precertificate.

Certum may notify other entities involved in the enrollment process of certificate issuance.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers SHALL:

- Use certificate solely for their intended purpose and in accordance with applicable laws, this CP/CPS, and the applicable Terms of Use or Subscriber Agreement
- Protect their private keys against unauthorized access, disclosure, or use
- Cease using a private key and the associated certificate immediately upon revocation or expiration of the certificate

Certificates SHALL be used only within their validity period and in accordance with the Key Usage (KU) and Extended Key Usage (EKU) extensions specified in the certificate.

4.5.2 Relying party public key and certificate usage

Relying parties SHALL:

- Verify the status of a certificate prior to reliance, including checking revocation information
- Ensure that the certificate is used only for its intended purpose and within its validity period
- Rely on a certificate only to the extent permitted by this CP/CPS and applicable agreements

The decision to rely on a certificate SHALL remain the sole responsibility of the relying party.

4.6 Certificate renewal

Certificate renewal results in the issuance of a new certificate to the Subscriber without changing the Subscriber or other participant's public key or any other information in the certificate.

4.6.1 Circumstance for certificate renewal

Certum does not support certificate renewal with key reuse.

The term "renewal" in Certum offer and Certum Systems is a commercial designation and does not reflect the formal renewal process as defined in this CP/CPS. Each such

“renewal” request SHALL require the generation of a new key pair and the submission of a corresponding public key.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to Subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

Re-keying results in the issuance of a new certificate to the Subscriber with a newly generated public key and a new serial number.

4.7.1 Circumstance for certificate re-key

Subscribers may request a re-key for any reason.

Subscriber MAY add a domain name or IP address to the SAN of the new certificate, but other information in the subject MUST remain unchanged. New domain names or IP addresses MUST be validated in accordance with the applicable procedures described in Section 3.2.

4.7.2 Who may request certification of a new public key

Multiple certificates MAY be issued for the same Subscriber under a single subscription period.

See Section 4.1.1.

4.7.3 Processing certificate re-keying requests

Certum MAY rely on previously validated information if it remains valid. Otherwise, Certum SHALL perform validation in accordance with Section 4.1 and Section 4.2.

4.7.4 Notification of new certificate issuance to Subscriber

See Section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See Section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

See Section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

See Section 4.4.3.

4.8 Certificate modification

Certificate modification results in the issuance of a new certificate to the Subscriber due to changes in the information in the certificate other than the Subscriber public key.

4.8.1 Circumstance for certificate modification

Certum does not support certificate modification. Each certificate request SHALL require the generation of a new key pair and the submission of a corresponding public key.

4.8.2 Who may request certificate modification

Not applicable.

4.8.3 Processing certificate modification requests

Not applicable.

4.8.4 Notification of new certificate issuance to Subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

4.8.6 Publication of the modified certificate by the CA

Not applicable.

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.9 Certificate revocation and suspension

Certificate revocation permanently ends the operational period of a certificate before its original expiry date. Certificates that have expired cannot be revoked. Certum does not support certificate suspension.

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for revoking a Subscriber certificate

The Subscriber may request revocation of their certificate at any time. When requesting a revocation, the Subscriber should select the revocation reason that best matches their circumstances:

- Key compromise: the Subscriber has reason to believe that their private key has been compromised (CRLReason #1, keyCompromise)
- Cessation of operation: the Subscriber no longer controls the domain name(s) listed in the certificate or no longer uses the certificate due to discontinuation of the associated domain or service (CRLReason #2, cessationOfOperation)
- Affiliation changed: the Organization name or other subject identity information included in the certificate has changed (CRLReason #3, affiliationChanged)
- Superseded: the certificate has been replaced with a new certificate (CRLReason #4, superseded)

When none of the listed reasons apply to the revocation request, the Subscriber should not provide a reason other than “unspecified”. Without specifying a CRLreason, Certum may revoke the certificate (CRLReason “unspecified (0)” which results in no reasonCode extension being provided in the CRL);

The reasons listed above represent the revocation reasons available to the Subscriber when submitting a revocation request. The full list of revocation reasons applied by Certum is specified in Section 7.2.2.

Certum SHALL revoke a Subscriber certificate within 24 hours or 5 days, as applicable, for all reasons specified in the TLS BR Section 4.9.1.1.

4.9.1.2 Reasons for revoking a Subordinate CA Certificate

Certum SHALL revoke a Subordinate CA certificate within 7 days, for all reasons specified in the TLS BR Section 4.9.1.2.

4.9.2 Who can request revocation

Certificate revocation can be requested by:

- The Subscriber or its authorized representative
- The party that manages the Certum System account to which certificate is issued

- Other third parties for problems related to compromise, fraud, misuse any other matter related to certificate
- Certum may revoke a certificate without receiving a request and without reason

4.9.3 Procedure for revocation request

Certum SHALL maintain a continuous 24/7 ability to accept and respond to revocation requests and Certificate Problem Reports.

Revocation request may be initiated by Certum System account to which certificate is issued. This method is intended solely for certificates managed within that account.

- Required information includes the certificate identifier and the reason for revocation
- The certificate revocation request is processed immediately
- The Subscriber is informed of the revocation by email or other appropriate means

Revocation request MAY also be submitted through a Certificate Problem Report, as described in Section 1.5.2. This method MAY be used to request revocation of any certificate issued by the CA.

- Required information includes but is not limited to the certificate identifier, the reason for revocation, and sufficient contact information to enable the CA to authenticate the requester and obtain additional information if necessary
- Certum processes the revocation request and MAY perform verification procedures in accordance with Section 3.2
- Certum MAY contact the Subscriber or other relevant parties to verify the request and obtain any additional information necessary to process the request
- Upon successful verification, the CA revokes the certificate and notifies the Subscriber of the revocation by email or other appropriate means

4.9.4 Revocation request grace period

Subscribers SHALL report any circumstances that constitute grounds for certificate revocation without undue delay, but no later than 24 hours after detecting the incident. This obligation applies particularly in the event of suspected or confirmed private key compromise.

4.9.5 Time within which CA must process the revocation request

Certum SHALL process revocation request within 24 hours after receiving a Certificate Problem Report in accordance with TLS BR Section 4.9.5.

After investigation and confirmation, Certum SHALL revoke the certificates within 24 hours or 5 days, as applicable to not exceed the time frame set forth in Section 4.9.1.1.

Status of the revoked certificate will be reflected in the OCSP responses within 1 hour, and in the CRLs within 24 hours.

4.9.6 Revocation checking requirement for relying parties

Relying Parties should check validity of each certificate in the certificate chain prior to relying on the certificate, including checking revocation information using applicable OCSP or CRL.

4.9.7 CRL issuance frequency

For CAs issuing Subscriber certificates, Certum SHALL:

- Update and publish a new CRL at least every 7 days
- Update and publish a new CRL within 24 hours after recording a certificate as revoked

For CAs issuing CA certificates, Certum SHALL:

- Update and publish a new CRL at least every 12 months
- Update and publish a new CRL within 24 hours after recording a certificate as revoked

4.9.8 Maximum latency for CRLs

CRLs are published to the CRL repository automatically usually within 10 minutes of generation and no later than 24 hours.

4.9.9 On-line revocation/status checking availability

OCSP responder locations (URLs) SHALL be included in the Authority Information Access (AIA) extension of the respective certificates.

OCSP responses SHALL conform to RFC 6960 and/or RFC 5019.

OCSP responses SHALL be digitally signed by OCSP responder whose certificate is signed by the issuing CA.

The responder's signing certificate SHALL contain an extension of type `id-pkix-ocsp-nocheck`, as defined in RFC 6960.

4.9.10 On-line revocation checking requirements

The Certum OCSP responder SHALL:

- Support the HTTP GET method for receiving status requests
- Not respond with a "good" status for a certificate serial number that is "unused" or "unassigned"

For the status of Subscriber certificates, Certum SHALL:

- Ensure that OCSP responses have a validity interval of at least 8 hours but no more than 10 days

- Make an authoritative OCSP response available starting no more than 15 minutes after a certificate or precertificate is first published or otherwise made available

For the status of Subordinate CA certificates, Certum SHALL:

- Update OCSP information at least every 12 months
- Update OCSP information within 24 hours after revoking a Subordinate CA certificate

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements re key compromise

Key compromise can be demonstrated in one of the following ways:

- Submission of a CSR with Common Name containing text “This key is compromised” or similar, signed with a compromised key, or
- Submission of the private key itself

4.9.13 Circumstances for suspension

Certum does not support certificate suspension.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

Certificate status information is available via CRL and an OCSP responder.

Revocation entry on a CRL or OCSP response MUST NOT be removed until after the expiry date of the revoked certificate.

4.10.2 Service availability

Certum operates CRL and OCSP capability with resources sufficient to provide a response time of 10 seconds or less under normal operating conditions.

Certificate status services are available 24x7, unless temporarily unavailable due to maintenance or service failure.

4.10.3 Optional features

Not applicable.

4.11 End of subscription

A Subscriber's subscription to certificate services ends when:

- certificate expires and is not replaced
- certificate is revoked and not replaced
- Certum ceases to provide certificate services

4.12 Key escrow and recovery

Certum does not support key escrow.

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

Certum implements physical and environmental security controls as part of its overall security program, in order to protect certificate data and certificate management processes against unauthorized access, damage, and disruption. These controls are implemented in a manner commensurate with the sensitivity of the systems and data being protected.

5.1.1 Site location and construction

Certum operates within facilities of Asseco Data Systems S.A. selected and maintained based on security, operational, and risk considerations. All facilities are solidly constructed to prevent unauthorized entry and are located within a selected set of locations evaluated for their physical security.

Critical PKI systems, including Certification Authority systems and cryptographic modules, are located in dedicated, physically protected high-security zones separated from general office environments. These areas are designed and maintained to prevent unauthorized access, damage, and interference, and to ensure appropriate protection of certificate data and certificate management processes.

5.1.2 Physical access

Physical access to Certum facilities is restricted to authorized personnel and controlled through access control systems. All of entrances and exits are secured or monitored by guards or monitoring/control systems.

Access rights are assigned based on roles and responsibilities and are subject to authentication mechanisms and monitoring. Entry to protected areas is controlled using access control systems, including microchip cards or equivalent mechanisms.

Access to high-security zones hosting critical PKI systems is limited to specifically authorized personnel performing Trusted Roles. Additional restrictions may apply to sensitive operations, including multi-person control where required.

All access to protected areas is monitored, and entry and exit events are recorded. Visitors, auditors, and service personnel may access protected areas only when authorized and, where required, under the supervision or escort of authorized Certum personnel.

5.1.3 Power and air conditioning

Certum facilities are equipped with power supply systems designed to ensure continuous operation of critical systems. These include uninterruptible power supply (UPS) systems and backup power generators.

Environmental controls, including air conditioning and temperature monitoring, are implemented to provide reliable operations 24/7.

5.1.4 Water exposures

Certum facilities are protected against water-related risks through the use of humidity and water detection sensors installed in high-security zones.

These sensors are integrated with the building security system. In the event of detection, appropriate personnel are notified and response procedures are initiated, including escalation to facility management, safety personnel, and system administrators, as appropriate.

5.1.5 Fire prevention and protection

Certum facilities are equipped with fire detection and fire suppression systems compliant with local standards and regulations for fire safety.

Server rooms and areas hosting critical systems are protected by automatic fire detection systems and gas-based fire suppression systems designed to minimize damage to equipment and ensure continuity of operations.

5.1.6 Media storage

Media containing sensitive information, including backup media and system data, are stored in secure locations with access restricted to authorized personnel.

Storage locations are protected against unauthorized access, environmental threats, and damage.

5.1.7 Waste disposal

Media and materials containing sensitive information are disposed of in a secure manner to prevent unauthorized access to data:

- Paper documents containing sensitive information are destroyed on-site by shredding
- Storage devices are physically destroyed or securely erased using approved utilities to prevent data recovery, in accordance with NIST SP 800-88 or equivalent standards
- Private keys stored on HSMs are erased (zeroized) upon device retirement in a way that makes recovery impossible

5.1.8 Off-site backup

Certum maintains backup copies of critical data and system configurations. Backup media are stored in secure off-site facilities that are geographically diverse from the primary site to ensure availability in the event of a regional disaster.

Access to backup media is restricted to authorized personnel. Backup processes are designed to ensure the integrity and availability of stored data.

Backups are periodically tested through restoration to verify if they are reliable.

5.2 Procedural controls

Certum implements procedural controls to ensure that critical Certification Authority operations are performed securely, in accordance with defined roles, responsibilities, and separation of duties principles.

5.2.1 Trusted Roles

Roles at Certum that involve access to or control over Certificate Data, cryptographic operations, or Certificate Management Processes are designated as Trusted Roles. These roles are established to share responsibility, limit individual action, and ensure that no single person can circumvent security measures.

Trusted Roles include, but are not limited to:

- Management personnel - responsible for certification services
- System Administrators and System Operators - responsible for installing, configuring, and maintaining PKI systems
- Security Officers - responsible for administering and implementing security practices
- Audit Officers - responsible for reviewing and archiving audit logs and overseeing compliance
- Validation Officers - responsible for identity vetting and approving certificate issuance or revocation

Trusted Roles are assigned based on the principle of least privilege and require appropriate authorization prior to being granted access to systems or facilities.

5.2.2 Number of persons required per task

Sensitive PKI operations are performed under multi-person control (dual control) to ensure that no single individual can circumvent security measures.

Such operations require the participation of at least two authorized individuals performing designated Trusted Roles, including:

- Security Officer (or equivalent control role)
- Hardware Security Module (HSM) Operator
- Shared Secret Holders, where applicable

Observers, such as auditors, may be present during such operations.

5.2.3 Identification and authentication for each role

All personnel acting in Trusted Roles are subject to identification and authentication procedures prior to being granted access to systems or facilities.

Access to Certum Systems is restricted to authorized personnel and controlled through authentication mechanisms.

User accounts are uniquely assigned to individuals, linked to specific roles, and restricted according to the functions required for those roles.

5.2.4 Roles requiring separation of duties

Certum enforces separation of duties to reduce the risk of unauthorized or improper actions.

Access rights are granted strictly in accordance with assigned roles.

The following role combinations are prohibited:

- Role of Security Officer MUST NOT be combined with the role of System Administrator
- Personnel responsible for audit or control functions MUST NOT perform operational roles related to certificate issuance, system administration, or security management

Inactivity time-outs and account lockout policies are enforced to prevent unauthorized access. Certum performs regular reviews of all system accounts and ensures that access rights are revoked within 24 hours of an individual's termination or change in job responsibilities.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Personnel performing Trusted Roles or other functions related to certification services are required to possess appropriate qualifications, experience, and competencies relevant to their responsibilities.

Certum requires that such personnel meet the following requirements:

- Personnel possess at least secondary education and the knowledge, experience, and competencies necessary for their specific job functions
- Personnel are engaged through employment contracts or other civil-law agreements that define their assigned roles, rights, and obligations
- Personnel complete mandatory training relevant to their responsibilities prior to commencing their duties, including training on security, personal data protection, and privacy policies

- Personnel are free from conflicts of interest that could affect the impartiality of certification services
- Personnel act in accordance with Certum policies implementing the CA/Browser Forum Baseline Requirements and other applicable industry standards

Access to systems and facilities is granted only after appropriate authorization and assignment of responsibilities

5.3.2 Background check procedures

Prior to being granted access to systems or facilities associated with certification services, personnel are subject to background verification procedures, where permitted by applicable law.

The scope and extent of such verification are commensurate with the sensitivity of the role.

Preparation and background checks for Trusted Roles include:

- Confirmation of the individual's identity
- Criminal record check
- Confirmation of previous employment
- Verification of references and professional licenses
- Verification of the highest education degree relevant to the role
- Where permitted law prevents the access to certain information, Certum is authorized to use substitute investigative techniques that provide substantially similar information

Certum is entitled to reject a candidate or take disciplinary action against an employee in a Trusted Role if it is determined that the individual:

- Provided misleading or false information during the vetting process
- Has highly unfavorable or untrustworthy professional references

In such events, further actions are conducted in accordance with the internal security procedures of Asseco Data Systems S.A. and applicable laws.

5.3.3 Training requirements

Personnel performing duties as part of Certum certification services or identity verification processes are required to complete training appropriate to their roles.

Training includes:

- All relevant CP, CPS and CP/CPS
- Role-specific procedures and documentation
- Security mechanisms and procedures
- Systems and software used in certification processes

- Incident and disaster response procedures
- Common threats to the information verification process, including phishing and social engineering tactics
- Applicable industry standards, such as CA/Browser Forum Baseline Requirements
- Personnel involved in identity verification processes receive additional training specific to identity validation requirements.

5.3.4 Retraining frequency and requirements

Personnel receive periodic retraining to maintain and update their knowledge and skills.

Retraining programs are designed to reflect and address any relevant changes to Certum PKI operations. Personnel are also made aware of new developments in the PKI industry, including security-related incidents at other Trust Service Providers and best practices identified by standards organizations.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Certum enforces disciplinary measures for unauthorized actions or violations of applicable policies and procedures.

Such measures are applied in accordance with internal personnel policies and applicable laws and include, but are not limited to, the restriction or revocation of access rights, suspension, and termination of employment.

5.3.7 Independent contractor requirements

If independent contractors are engaged in activities related to certification services, they are required to comply with applicable training, security, and procedural requirements appropriate to the roles they perform.

Independent contractors are not authorized to perform critical certification operations unless explicitly approved and subject to the same controls as Certum personnel performing comparable functions.

External personnel who have not completed applicable verification procedures may access Certum facilities only under the supervision or escort of authorized Certum personnel.

5.3.8 Documentation supplied to personnel

Personnel are provided with documentation necessary to perform their duties securely and effectively.

This includes policies, procedures, role-specific instructions, and other relevant documentation related to certification services.

5.4 Audit logging procedures

Certum implements audit logging procedures to record, monitor, and analyze events relevant to the security of certificate data and certificate management processes.

Audit logs are used to support the detection of unauthorized activities, operational issues, and security incidents.

5.4.1 Types of events recorded

Certum records events related to the operation and security of certification services, including but not limited to:

- Access to systems supporting certification operations
- System and security events
- Administrative actions performed by authorized personnel
- Certificate lifecycle operations (including issuance and revocation)
- Changes to system configuration where relevant to certification services

5.4.2 Frequency of processing log

Audit logs are reviewed on a regular basis and in response to detected anomalies, incidents, or operational needs.

5.4.3 Retention period for audit log

Certum retains log records according to the following schedule:

- CA key and certificate lifecycle events - for at least 2 years following the destruction of the CA private key or the revocation or expiration of the final CA certificate associated with that key
- Subscriber certificate lifecycle management events - for at least 2 years after the revocation or expiration of the Subscriber certificate
- Security event records - for at least 2 years after the event occurred

5.4.4 Protection of audit log

Audit logs are protected against unauthorized access, modification, and deletion.

Access to audit logs is restricted to authorized personnel.

5.4.5 Audit log backup procedures

Audit logs are included in backup processes to ensure their availability in case of system failure or data loss.

5.4.6 Audit collection system (internal vs. external)

Audit logs are collected and maintained using systems operated by Certum.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

Certum implements a vulnerability management process to identify, assess, and remediate security vulnerabilities affecting systems supporting certification services.

Vulnerability assessments are performed on a annual basis and in response to significant changes to systems or infrastructure.

These assessments include vulnerability scanning, configuration reviews, and other security evaluation activities appropriate to the systems involved.

Identified vulnerabilities are assessed and addressed in accordance with their assessed risk and applicable procedures.

5.5 Records archival

Certum maintains records related to certification services in order to support operational, security, audit, and legal requirements.

Archived records are retained, protected, and made available in accordance with applicable policies and regulatory requirements.

5.5.1 Types of records archived

Certum archives records relevant to certification services, including but not limited to:

- Certificate application and registration data
- Identity verification information
- Certificate lifecycle events (including issuance and revocation)
- Audit logs
- System and security records relevant to certification operations
- Agreements and documentation related to certification services

5.5.2 Retention period for archive

All records described in Section 5.5.1 are retained for at least 2 years.

5.5.3 Protection of archive

Archived records are protected against unauthorized access, modification, and destruction.

Access to archived records is restricted to authorized personnel.

5.5.4 Archive backup procedures

Archived records are subject to backup procedures to ensure their availability and integrity in case of data loss or system failure.

5.5.5 Requirements for time-stamping of records

Where applicable, records are associated with date and time information to support their integrity and traceability.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

Certum uses newly generated key pairs for newly issued CA and Subscriber certificates.

5.7 Compromise and disaster recovery

Certum maintains internal procedures that include a Business Continuity Plan (BCP)/Disaster Recovery Plan to ensure the restoration of guaranteed service levels in the event of exceptional circumstances, such as natural disasters or catastrophic events.

5.7.1 Incident and compromise handling procedures

Certum maintains procedures for incident handling and response to security threats as part of its Business Continuity Plan (BCP).

The BCP defines the conditions for activation, emergency response procedures, contingency procedures, and procedures for restoring certification services. It also includes requirements for personnel awareness, roles and responsibilities, and regular review and maintenance of the plan.

Certum tests the effectiveness of the BCP at least annually and whenever significant changes are introduced.

Certum maintains a Mass Revocation Plan, which defines the actions to be taken in the event that a rapid, coordinated, and secure revocation of a significant number of certificates is required.

The Mass Revocation Plan includes:

- Criteria for triggering the plan
- Roles and responsibilities of personnel
- Training requirements

- Procedures for notifying Subscribers and relying parties
- Target timeframes for initiating and completing revocation activities

The effectiveness of the Mass Revocation Plan is tested as part of BCP testing and after significant process changes.

The BCP also addresses:

- Recovery objectives for critical certification processes
- Backup and restoration of critical systems and data
- Requirements for secure storage of cryptographic materials at backup locations
- Geographical separation of primary and backup facilities
- Procedures for safeguarding assets during disruptions
- Acceptable system outage and recovery conditions

5.7.2 Computing resources, software, and/or data are corrupted

In the event of corruption of computing resources, software, or data, Certum implements procedures to identify and assess the extent of the incident and its impact on certification services.

Appropriate actions are taken to contain the issue and restore affected systems and data from trusted sources, including backups and redundant or alternate systems.

Restored systems and data are verified prior to resuming normal operations.

Where the corruption affects certification processes or issued certificates, Certum may take appropriate actions, including revocation of affected certificates and issuance of replacement certificates.

Where necessary, procedures defined in the Business Continuity Plan and Disaster Recovery Plan are invoked.

5.7.3 Entity private key compromise procedures

Certum maintains procedures to respond to the compromise or suspected compromise of private keys associated with certification services.

In the event of such compromise, Certum implements actions appropriate to the nature and scope of the incident, which may include:

- Immediate cessation of use of the compromised private key
- Revocation of certificates associated with the compromised key
- Notification of affected parties, including Subscribers and relying parties, as required
- Generation and deployment of replacement key pairs and certificates
- Implementation of additional measures to mitigate the impact of the compromise

Where applicable, Certum also takes steps to restore the secure operation of certification services and re-establish trust in issued certificates.

5.7.4 Business continuity capabilities after a disaster

Certum maintains business continuity and disaster recovery capabilities to ensure the availability and continuity of certification services following a disaster or major disruption.

These capabilities include the use of backup systems, redundant or alternate processing facilities, and procedures for restoring critical systems and data.

Certum implements measures to protect certification systems and sensitive materials against loss, unauthorized access, or further damage during and after a disruptive event.

Recovery procedures are designed to restore certification services in a controlled and secure manner, including the restoration of systems, data, and cryptographic materials.

Certum performs periodic testing and review of its business continuity and disaster recovery arrangements to ensure their effectiveness.

5.8 CA or RA termination

When it is necessary to terminate the operation of a Certum CA, Certum is committed to minimizing the impact of such termination on Subscribers and relying parties.

Before terminating its certification services:

- Certum notifies all Subscribers with active certificates at least 90 days before the scheduled termination date via email and through its official website to allow them to transition to another Trust Service Provider
- Certum uses reasonable commercial efforts to minimize disruptions and provides compensation for certificate fees proportional to the unused validity period, in accordance with applicable service agreements and internal policies
- Upon the final termination date, Certum revokes all certificates that remain valid and unexpired, issues a final CRL with a nextUpdate field indicating the end of operations, and revokes its own CA certificates
- Certum destroys all private keys

To maintain business continuity, Certum is authorized to transfer its responsibilities to a successor entity.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pairs for Certum CAs are generated in a secure environment using Hardware Security Modules (HSMs), as specified in Section 6.2.1.

The generation process is conducted by personnel in Trusted Roles during a formal key generation ceremony in accordance with a documented script.

Particularly when generating a CA key pair intended for a Root CA certificate, the procedure is observed by an independent external auditor. Certum maintains auditable evidence that the ceremony followed this CP/CPS and ensured the integrity and confidentiality of the key pairs.

Subscriber key pairs are generated by the Subscriber.

6.1.2 Private key delivery to Subscriber

Certum does not generate Subscriber private keys.

6.1.3 Public key delivery to certificate issuer

Subscribers may provide their public key to Certum in the form of Certificate Signing Request (CSR) in PKCS#10 format. Submission is made electronically via the Certum Systems.

6.1.4 CA public key delivery to relying parties

Certum CAs public keys are made available from the Certum Repository (see Section 2.1).

Certum CAs public keys are also provided as trust anchors in browser, operating system, or other software trusted root stores.

6.1.5 Key sizes

The following algorithms and key lengths are permissible for Certum Root CAs, Subordinate CAs and Subscriber certificates:

Certum Root CA

- RSA: 2048b, 3072b, 4096b
- ECDSA: NIST P-256, P-384

Certum Subordinate CA

- RSA: 2048b, 3072b, 4096b
- ECDSA: NIST P-256, P-384

Certum Subscriber certificates

- RSA: 2048b, 3072b, 4096b
- ECDSA: NIST P-256, P-384

6.1.6 Public key parameters generation and quality checking

The following additional criteria are required for RSA keys (based on Sections 5.3.3, NIST SP 800-89):

- Public exponent MUST be an odd number equal to 3 or more
- Public exponent is in the range between 2^16 + 1 and 2^256 - 1
- Modulus is an odd number
- Modulus is not the power of a prime, and
- Modulus has no factors smaller than 752

The following additional criteria apply to ECDSA keys (based on Sections 5.6.2.3.2 and 5.6.2.3.3 of NIST SP 800-56A, Revision 2). The validity of all ECDSA keys is confirmed using one of the following methods: - ECC Full Public Key Validation Routine, or - ECC Partial Public Key Validation Routine

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Certum assigns certificate key usages according to their intended purpose through the X.509 v3 Key Usage field.

Private keys corresponding to Certum Root CA certificates MUST NOT be used to sign certificates except in the following cases:

- Self-signed certificates to represent the Root CA itself
- Certificates for Subordinate CAs and cross certificates
- Certificates for infrastructure purposes (internal CA operational device certificates)
- Certificates for OCSP response verification

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Certum implements physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA private key outside the validated system or device specified in Section 6.2.7 consists of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the private key.

Certum encrypts its private key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic module standards and controls

All Certum Systems signing certificates, CRLs or generating OCSP responses use FIPS 140-2 Level 3 or higher or Common Criteria EAL4+ security specifications.

Certum CA private keys are maintained in physically secure environments and are never stored in unencrypted form outside HSMs.

6.2.2 Private key (n out of m) multi-person control

All access to Certum CAs private keys, whether physical or logical, requires the participation of multiple individuals serving in Trusted Roles. This applies to all instances of the private keys, including production and backup copies, both on-site and off-site.

6.2.3 Private key escrow

Certum CAs private keys are not escrowed.

6.2.4 Private key backup

Backups of Certum CAs private keys are stored in a secure manner in accordance with applicable Certum backup policy.

Certum CAs private keys are backed up, stored, and recovered only by personnel in Trusted Roles using, at least, dual control in a physically secured environment.

6.2.5 Private key archival

Private keys belonging to Certum are not archived by parties other than Certum.

6.2.6 Private key transfer into or from a cryptographic module

Certum CAs private keys are generated within HSMs and are exported only for redundancy or backup purposes. When exported, keys are encrypted before leaving the HSM and are decrypted only within the destination HSM, using a process that always requires multi-person control.

All transfers of Certum CAs private keys into or out of a cryptographic module are carried out in accordance with the procedures defined by the vendor of the respective module.

6.2.7 Private key storage on cryptographic module

Certum stores CA private keys on a hardware cryptographic module as specified in Section 6.2.1.

6.2.8 Method of activating private key

Certum activates CA private keys in accordance with the instructions and documentation provided by the manufacturer of the hardware security module.

6.2.9 Method of deactivating private key

Certum deactivates CA private keys in accordance with the instructions and documentation provided by the manufacturer of the hardware security module.

6.2.10 Method of destroying private key

Certum destroys CA private keys in accordance with the instructions and documentation provided by the manufacturer of the hardware security module.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

See Section 5.5.

6.3.2 certificate operational periods and key pair usage periods

Certum Root CA and Subordinate CA key pairs have lifetimes corresponding to their certificates:

- Maximum validity period of Root CA is 25 years
- Maximum validity period of Subordinate CA is 15 years

Type	Maximum key usage period	Maximum certificate validity period
Certum Root CA	25 years	25 years
Certum Subordinate CA	15 years	15 years

The maximum validity period of Subscriber TLS certificates depends on their issuance date:

- Maximum validity period of Subscriber certificates issued before 15 March 2026 is 398 days;
- Maximum validity period of Subscriber certificates issued on or after 15 March 2026 and before 15 March 2027 is 200 days;
- Maximum validity period of Subscriber certificates issued on or after 15 March 2027 and before 15 March 2029 is 100 days;
- Maximum validity period of Subscriber certificates issued on or after 15 March 2029 is 47 days.

Subscriber certificate issued on or after	Certificate issued before	Maximum validity period
N/A	2026-03-15	398 days
2026-03-15	2027-03-15	200 days

Subscriber certificate issued on or after	Certificate issued before	Maximum validity period
2027-03-15	2029-03-15	100 days
2029-03-15	N/A	47 days

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data used to activate Certum CAs private keys is generated during a key ceremony as described in Section 6.1.1. The activation data is transferred to personnel performing in a Trusted Role to use it or store it.

6.4.2 Activation data protection

Activation data is protected from unauthorized disclosure via both physical and logical means.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Certum Systems are protected to prevent unauthorized access or alteration of CA software and data. Multifactor authentication is employed for system access. Security patches are applied in a timely manner, and vulnerability scans are performed on a regular basis.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

Certum maintains documented procedures governing the acquisition and development of its CA systems, ensuring that all components meet security, performance, and reliability requirements. Dedicated hardware and software are maintained solely for the operation of CA functions.

Certum utilizes software that has undergone formal testing to ensure its suitability and fitness for purpose. Hardware is acquired through a controlled procurement process that leverages reputable, industry-standard vendors. All shipments of hardware are received by person in Trusted Roles and inspected for signs of tampering. Hardware Security Modules (HSMs) are delivered in tamper-evident packaging, and tamper-bag serial numbers are verified with the vendor upon receipt. Each HSM is tested in accordance with established procedures prior to being placed into production use.

Certum maintains a dedicated CA testing environment that is logically and physically separated from the production environment. The testing platform is designed to replicate the production environment as closely as possible, without access to the CA private keys used for trusted certificates. This environment supports comprehensive testing of software and systems before deployment to production, ensuring security and stability.

Certum has established and enforces formal change control policies and procedures to be followed whenever CA systems are modified. All proposed changes MUST be reviewed and approved by person in Trusted Roles who are independent of the individual requesting the change. Each change request, along with its associated reviews and approvals, is fully documented.

When Certum develops software for use in CA operations, development follows defined policies and methodologies that promote software quality, security, and integrity. These practices include peer reviews, structured testing, and documentation of all code modifications.

For linting software developed by third parties, Certum monitors for updated versions of such software and plan for implementation of updates within three months of their public release. Certum may perform linting on the corpus of its unexpired and unrevoked Subscriber certificates each time the linting software is updated, in order to verify continued compliance with applicable certificate profiles and issuance policies.

6.6.2 Security management controls

The current configuration of the Certum System, as well as all modifications and updates, is recorded and subject to formal change control procedures. Configuration management controls implemented within the Certum System ensure continuous verification of application integrity and version.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

Certum adheres to the CA/Browser Forum's Network and Certificate System Security Requirements.

Certum implements appropriate network security controls and safeguards designed to prevent unauthorized access to its CA systems.

Certum's network architecture follows a multi-tiered and segmented. Firewalls are configured according to a least-privilege, allowlist-based policy, permitting only necessary network traffic whenever feasible.

Certum Root CA private keys are maintained offline in a secure and controlled environment.

Certum adopts the following timeframes for addressing vulnerabilities:

- High-priority within 96 hours
- Medium-priority within 7 days
- Low-priority within 30 days

6.8 Time-stamping

Certum ensures that the time sources used in all time-stamping operations remain accurate, reliable, and verifiable through NTP (Network Time Protocol).

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Certum certificates are issued in conformance with RFC 5280. Certificate extensions, their criticality settings, and cryptographic algorithm object identifiers are implemented in accordance with the specifications defined in RFC 5280. Certum complies with the technical requirements outlined in Section 6.1.5 and Section 6.1.6 of this document.

In the event of a conflict between the provisions of RFC 5280 and the applicable CA/Browser Forum requirements, Certum adheres to the requirements of the CA/Browser Forum.

Root CA certificate profile

Field or extension	Value
`version`	See Section 7.1.1
`serialNumber`	A non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG
`issuer`	Contains `countryName`, `organizationName` and `commonName`
`validity`	See Section 6.3.2
`subject`	Same as Issuer DN
`subjectPublicKeyInfo`	See Section 6.1.5, Section 6.1.6, and Section 7.1.3
`signatureAlgorithm`	See Section 6.1.5, Section 6.1.6, and Section 7.1.3
`basicConstraints` (critical)	`cA=True`
`keyUsage` (critical)	`keyCertSign`, `cRLSign`
`subjectKeyIdentifier`	SHA-1 hash of `subjectPublicKeyInfo`

Note: The old Certum Root CA certificates does not follow the current Root CA certificate profile as it predates today's standards.

Subordinate CA certificate profile

Field or extension	Value
`version`	See Section 7.1.1
`serialNumber`	A non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG
`issuer`	Contains `countryName`, `organizationName` and `commonName`
`validity`	See Section 6.3.2
`subject`	Same as Issuer DN
`subjectPublicKeyInfo`	See Section 6.1.5, Section 6.1.6, and Section 7.1.3
`signatureAlgorithm`	See Section 6.1.5, Section 6.1.6, and Section 7.1.3

Field or extension	Value
authorityKeyIdentifier	Identical to the subjectKeyIdentifier field of the Issuing CA
basicConstraints (critical)	cA=True, pathLenConstraint (optional)
certificatePolicies	anyPolicy
crlDistributionPoints	HTTP URL of the Issuing CA's CRL service for this certificate
keyUsage (critical)	keyCertSign, cRLSign
subjectKeyIdentifier	SHA-1 hash of subjectPublicKeyInfo
extKeyUsage	id-kp-serverAuth, id-kp-clientAuth (optional)
authorityInformationAccess	A HTTP URL of the Issuing CA's OCSP responder and a HTTP URL of the Issuing CA's certificate

Note 1: The old Certum Subordinate CA certificates does not follow the current Root CA certificate profile as it predates today's standards.

Note 2: The certificate profile of cross-certified Subordinate CA, which is a special type of the Subordinate CA certificate, is issued in accordance with TLS BR Section 7.1.2.2.

TLS Server End Entity certificate (DV)

Field or extension	Value
version	See Section 7.1.1
serialNumber	A non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG
issuer	Derived from Issuing CA
validity	See Section 6.3.2
subject	Contains commonName
subjectPublicKeyInfo	See Section 6.1.5, Section 6.1.6, and Section 7.1.3
signatureAlgorithm	See Section 6.1.5, Section 6.1.6, and Section 7.1.3
authorityInformationAccess	A HTTP URL of the Issuing CA's OCSP responder and a HTTP URL of the Issuing CA's certificate
authorityKeyIdentifier	Identical to the subjectKeyIdentifier field of the Issuing CA
certificatePolicies	2.23.140.1.2.1, 1.2.616.1.113527.2.101.1 (optional)
extKeyUsage	id-kp-serverAuth, id-kp-clientAuth (optional)
subjectAltName	A sequence of one or more dNSNames or ipAddresses.
keyUsage (critical)	digitalSignature, keyEncipherment (optional)
basicConstraints (critical)	cA=False
crlDistributionPoints	HTTP URL of the Issuing CA's CRL service for this

Field or extension	Value
	certificate
Signed Certificate Timestamp List	In accordance with RFC 6962.
`subjectKeyIdentifier`	SHA-1 hash of `subjectPublicKeyInfo` (optional)
Precertificate poison	In accordance with RFC 6962 (in Precertificates only)

TLS Server End Entity certificate (OV)

Field or extension	Value
`version`	See Section 7.1.1
`serialNumber`	A non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
`issuer`	Derived from Issuing CA
`validity`	See Section 6.3.2
`subject`	Contains `countryName`, `stateOrProvinceName` (optional), `localityName` (optional), `organizationName`, `commonName`
`subjectPublicKeyInfo`	See Section 6.1.5, Section 6.1.6, and Section 7.1.3
`signatureAlgorithm`	See Section 6.1.5, Section 6.1.6, and Section 7.1.3
`authorityInformationAccess`	A HTTP URL of the Issuing CA's OCSP responder and a HTTP URL of the Issuing CA's certificate
`authorityKeyIdentifier`	Identical to the `subjectKeyIdentifier` field of the Issuing CA
`certificatePolicies`	2.23.140.1.2.2, 1.2.616.1.113527.2.101.2 (optional)
`extKeyUsage`	`id-kp-serverAuth`, `id-kp-clientAuth` (optional)
`subjectAltName`	A sequence of one or more `dNSNames` or `ipAddresses`
`keyUsage` (critical)	`digitalSignature`, `keyEncipherment` (optional)
`basicConstraints` (critical)	`cA=False`
`crlDistributionPoints`	HTTP URL of the Issuing CA's CRL service for this certificate
Signed Certificate Timestamp List	In accordance with RFC 6962.
`subjectKeyIdentifier`	SHA-1 hash of `subjectPublicKeyInfo` (optional)
Precertificate poison	In accordance with RFC 6962 (in Precertificates only)

TLS Server End Entity certificate (EV)

Field or extension	Value

Field or extension	Value
version	See Section 7.1.1
serialNumber	A non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG
issuer	Derived from Issuing CA
validity	See Section 6.3.2
subject	Contains businessCategory, jurisdictionCountryName, jurisdictionStateOrProvinceName(optional), jurisdictionLocalityName(optional), serialNumber, countryName, stateOrProvinceName (optional), localityName (optional), postalCode (optional), streetAddress (optional), organizationName, commonName
subjectPublicKeyInfo	See Section 6.1.5, Section 6.1.6, and Section 7.1.3
signatureAlgorithm	See Section 6.1.5, Section 6.1.6, and Section 7.1.3
authorityInformationAccess	A HTTP URL of the Issuing CA's OCSP responder and a HTTP URL of the Issuing CA's certificate.
authorityKeyIdentifier	Identical to the subjectKeyIdentifier field of the Issuing CA
certificatePolicies	2.23.140.1.1, 1.2.616.1.113527.2.101.3 (optional)
extKeyUsage	id-kp-serverAuth, id-kp-clientAuth (optional)
subjectAltName	A sequence of one or more dNSNames or ipAddresses
keyUsage (critical)	digitalSignature, keyEncipherment (optional)
basicConstraints (critical)	cA=False
crlDistributionPoints	HTTP URL of the Issuing CA's CRL service for this certificate.
Signed Certificate Timestamp List	In accordance with RFC 6962.
subjectKeyIdentifier	SHA-1 hash of subjectPublicKeyInfo (optional)
Precertificate poison	In accordance with RFC 6962 (in Precertificates only)

7.1.1 Version number(s)

All certificates use X.509 version 3.

7.1.2. Certificate extensions

The certificate extensions comply with RFC 5280 and the TLS BR.

This Section specifies the additional requirements for certificate content and extensions for certificates.

7.1.3 Algorithm object identifiers

Certum issues certificates using the algorithms identified by the following OIDs:

Algorithm Name	OID
`sha256WithRSAEncryption`	1.2.840.113549.1.1.11
`sha384WithRSAEncryption`	1.2.840.113549.1.1.12
`sha512WithRSAEncryption`	1.2.840.113549.1.1.13
`ecdsa-with-SHA256`	1.2.840.10045.4.3.2
`ecdsa-with-SHA384`	1.2.840.10045.4.3.3
`ecdsa-with-SHA512`	1.2.840.10045.4.3.4

7.1.4 Name forms

Certum issues certificates whose naming conventions follow RFC 5280 and the guidelines specified in Section 7.1.4 of the TLS BR.

7.1.5 Name constraints

Certum does not create Subordinate CAs that include name constraints.

7.1.6 Certificate policy object identifier

See Section 7.1.

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

See Section 7.1.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

CRL profile

Field or extension	Value
`version`	v2
`signature`	See Section 7.1.3.
`issuer`	Byte-for-byte identical to the `subject` field of the Issuing CA

Field or extension	Value
thisUpdate	The date and time the CRL was issued
nextUpdate	See Section 4.9.7
revokedCertificates	Certificates that have been revoked
authorityKeyIdentifier	Identical to the subjectKeyIdentifier field of the Issuing CA
CRLNumber	The serial number of this CRL in an incrementally increasing sequence of CRLs

7.2.1 Version number(s)

CRL use X.509 version 2.

7.2.2 CRL and CRL entry extensions

For CRL extensions see Section 7.2.

CRL entry extensions (revokedCertificates components)

Component	Value
serialNumber	serialNumber contained in the revoked certificate.
revocationDate	The date and time revocation occurred. The revocation date may be backdated if the reasonCode is keyCompromise.
crlEntryExtensions	Contains reasonCode.

CRL reasonCode extension for end-entity certificates (RFC 5280 reasonCode value in brackets):

- unspecified (0) - Represented by the omission of a reasonCode. MUST be omitted if the CRL entry is for a certificate not technically capable of causing issuance unless the CRL entry is for a Subscriber certificate subject to these Requirements revoked prior to July 15, 2023.
- keyCompromise (1) - Indicates that it is known or suspected that the Subscriber's private key has been compromised.
- affiliationChanged (3) - Indicates that the Subject's name or other Subject Identity Information in the certificate has changed, but there is no cause to suspect that the certificate's private key has been compromised.
- superseded (4) - Indicates that the certificate is being replaced because: the Subscriber has requested a new certificate, the CA has reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the certificate should not be relied upon, or the CA has revoked the certificate for compliance reasons such as the certificate does not comply with these CA/Browser Forum Baseline Requirements or the CA's CP or CPS.

- `cessationOfOperation` (5) - Indicates that the website with the certificate is shut down prior to the expiration of the certificate, or if the Subscriber no longer owns or controls the domain name in the certificate prior to the expiration of the certificate.
- `privilegeWithdrawn` (9) - Indicates that there has been a Subscriber-side infraction that has not resulted in keyCompromise, such as the certificate Subscriber provided misleading information in their certificate Request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use. This reason code is not made available for selection by Subscribers and is applied solely by Certum where appropriate.

7.3 OCSP profile

Certum provides an OCSP service that complies with the RFC 6960 standard.

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

The `singleExtensions` of an OCSP response does not contain the `reasonCode` CRL entry extension.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

Compliance audits are conducted at least annually. The period during which Certum issues publicly trusted certificates is divided into an unbroken sequence of consecutive audit periods. No audit period exceeds 1 year in duration.

8.2 Identity/qualifications of assessor

External audits are performed by an independent entity authorized to conduct WebTrust audits.

Such entity:

- Is independent from Certum and free from conflicts of interest
- Is authorized to perform WebTrust audits applicable to Certum's publicly trusted services
- Employs personnel with demonstrated expertise in Public Key Infrastructure (PKI) technology, information security controls, and IT auditing
- Is bound by applicable law, regulation, or a professional code of ethics
- Maintains appropriate professional liability insurance coverage

8.3 Assessor's relationship to assessed entity

The external auditor is independent from Certum and does not have any financial interest, business relationship, or other arrangement that could create a conflict of interest or bias.

8.4 Topics covered by assessment

The annual external audit is conducted in accordance with the current versions of the applicable WebTrust Principles and Criteria, as published by CPA Canada and available at:

https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

The audit covers the WebTrust programs applicable to Certum's publicly trusted TLS services, including, as relevant:

- WebTrust for Certification Authorities
- WebTrust for Certification Authorities – TLS Baseline Requirements
- WebTrust for Certification Authorities – Extended Validation (TLS)
- WebTrust for Certification Authorities – Network Security

The audit evaluates whether Certum maintains effective controls to provide reasonable assurance that its practices are properly disclosed and that its TLS certification services operate in accordance with this CP/CPS and applicable requirements.

8.5 Actions taken as a result of deficiency

If a deficiency is identified during an audit, the auditor documents the finding and notifies Certum.

Depending on the nature and severity of the deficiency, Certum will:

- Develop and document a remediation plan
- Implement corrective actions within a commercially reasonable timeframe
- Update its policies, procedures, or technical controls where necessary

Where applicable, the auditor may verify that the identified deficiency has been adequately resolved.

Certum evaluates whether any corrective action is required with respect to previously issued certificates and takes appropriate measures in accordance with applicable requirements.

8.6 Communication of results

Certum makes its annual Audit Report publicly available no later than 3 months after the end of the audit period.

Audit Reports are published in PDF format in the public repository and are text-searchable (See Section 2.1).

Certum is not required to make publicly available any audit findings that do not affect the overall audit opinion

8.7 Self-audits

Certum performs internal self-audits at least quarterly in accordance with the applicable CA/Browser Forum requirements. These audits are conducted against a randomly selected sample of the greater of 1 certificate or at least 3% of the certificates issued during the audited period.

Self-audits assess whether certificate issuance and lifecycle management activities are performed in compliance with this CP/CPS and applicable requirements.

The results of self-audits are documented and reviewed by authorized personnel. Identified deficiencies are addressed in accordance with Section 8.5.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Certum is entitled to charge Subscribers fees for the verification and issuance of certificates. All applicable fees are made clear to Applicants during the application process.

Certum does not charge fees for certificate revocation.

9.1.2 Certificate access fees

Certum does not charge fees for access to certificates or trust service provider certificates.

9.1.3 Revocation or status information access fees

Certum does not charge a fee for the revocation of certificates.

Certum does not charge a fee for access to standard certificate status information via CRL or OCSP.

Certum may charge for providing customized revocation information or other value-added status services.

9.1.4 Fees for other services

Certum may charge fees for services outside the standard issuance process.

9.1.5 Refund policy

Subscriber has the right to request a refund of the paid fee within 14 days of certificate issuance if the service is performed in a manner inconsistent with this CP/CPS or the applicable Subscriber Agreement or Terms of Use. Certum is authorized to revoke the certificate upon granting a refund.

Termination of the contract resulting from a necessary revocation due to Subscriber's breach does not entitle the Subscriber to any refund.

9.2 Financial responsibility

9.2.1 Insurance coverage

Certum maintains Professional Indemnity (Errors and Omissions) insurance coverage and Commercial General Liability insurance coverage.

The Professional Indemnity insurance provides coverage with a policy limit of USD 10,000,000 per claim and in the aggregate during the insurance period.

The maintained insurance coverage meets or exceeds the requirements set forth in the current EV Guidelines.

The financial warranty of Asseco Data Systems S.A. concerning the issuance of EV certificates is subject to the liability limitations set forth in this CP/CPS and applicable agreements.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No additional stipulations. Liability and warranty provisions are set forth in this CP/CPS and in the applicable agreements.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Certum treats as confidential all non-public information obtained in the course of providing certification services and protects such information in accordance with applicable law and internal security policies.

Confidential information includes, but is not limited to:

- private keys
- Certificate application records and supporting documentation
- Subscriber and Relying Party agreements
- Transaction and audit logs
- Internal audit reports and security assessments
- Business continuity and disaster recovery plans
- Internal operational documentation related to CA and RA systems
- Any other non-public information obtained in connection with the provision of certification services

Certum does not collect, store, or escrow Subscribers' private keys.

9.3.2 Information not within the scope of confidential information

The following information is not considered confidential:

- Information included in issued certificates
- Certificate status and revocation information (CRLs, OCSP responses)
- This CP/CPS and other publicly available policy documents
- Information required to be disclosed pursuant to applicable law or a binding court or governmental order

9.3.3 Responsibility to protect confidential information

Certum implements appropriate technical and organizational measures to protect confidential information against unauthorized access, disclosure, alteration, or destruction.

Personnel in Trusted Roles are bound by confidentiality obligations.

9.4 Privacy of personal information

9.4.1 Privacy plan

Personal data provided to Certum by Subscribers are processed in accordance with:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR); and
- The applicable Polish Act on Personal Data Protection

The scope of personal data collected and processed by Certum is limited to the purposes for which such data are required.

Personal data are processed for the following purposes:

- Conclusion and performance of an agreement for the issuance of a non-qualified certificate, pursuant to Article 6(1)(b) GDPR
- Compliance with legal obligations imposed on the data controller, pursuant to Article 6(1)(c) GDPR, including obligations arising from applicable trust services and electronic identification legislation
- Ensuring compliance with applicable industry standards, based on the legitimate interest of the controller in maintaining a high level of service quality, pursuant to Article 6(1)(f) GDPR
- Remote identity verification, based on separately expressed consent, pursuant to Article 6(1)(a) and, where applicable, Article 9(2)(a) GDPR

Detailed information regarding consent, where required, is provided at the time such consent is obtained.

Personal data are used exclusively in connection with the provision of certification services.

Personal data are protected in accordance with the privacy and security policies of Asseco Data Systems S.A.

9.4.2 Information treated as private

Private information includes personal data relating to a Applicant that is collected during the application or verification process and is not included in issued certificates, or certificate revocation information (CRLs or OCSP responses).

9.4.3 Information not deemed private

Information available in certificates, CRLs, or OCSP is not considered private.

Any document published in the Certum Repository (Section 2.1) is not considered private.

9.4.4 Responsibility to protect private information

Any Certum employee or authorized person who has access to personal data collected in connection with certificate issuance is bound by confidentiality obligations.

Certum implements appropriate technical and organizational measures to protect personal data against unauthorized access, disclosure, alteration, or destruction.

9.4.5 Notice and consent to use private information

Unless otherwise provided in this CP/CPS or in an applicable agreement, personal data SHALL NOT be processed beyond the purposes described herein without a valid legal basis under applicable law, including, where required, the consent of the data subject.

Additional information regarding the processing of personal data is available in the Asseco Data Systems S.A. Privacy Policy published at:

https://www.assecods.pl/en/privacy-policy

9.4.6 Disclosure pursuant to judicial or administrative process

Confidential information or personal data may be disclosed to courts, law enforcement authorities, or administrative bodies only where required by applicable law and upon fulfillment of all legal requirements binding in the Republic of Poland.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

Asseco Data Systems S.A. operating as Certum retain all intellectual property rights in and to:

- This CP/CPS and related policy documents
- Certificates and revocation information issued by Certum
- Certum trademarks, service marks, logos, and other branding elements
- Certum Systems, software, documentation, and related materials

Certificates and revocation information remain the exclusive property of Certum. Certum grants permission to reproduce and distribute certificates in their entirety, provided that they are not modified or used in a misleading manner.

Private and public keys associated with a certificate remain the property of the Subscriber identified in the certificate.

All other intellectual property rights remain with their respective owners.

9.6 Representations and warranties

Certum makes to all Subscribers and relying parties certain representations regarding its public certification services, as described below.

Certum reserves its right to modify such representations as it sees fit or as required by law.

Except as expressly stated in this document or in a separate agreement with the Subscriber, to the extent specified in the relevant sections of this document, Certum represents, in all material aspects, to:

- Comply with this document and its internal or published policies and procedures, specifically this CP/CPS
- Make available a copy of this document and applicable policies to requesting parties via the Certum Repository
- Comply with applicable laws and regulations, including personal data protection laws such as GDPR
- Provide infrastructure and certification services, including but not limited to the establishment and operation of the Certum Repository for the management of PKI services
- Provide prompt notice in case of the compromise of its own private keys to all affected Subscribers
- Provide and validate application procedures for the various types of certificates it makes available, verifying the Subscriber's identity and their right to use or control the domain names or IP addresses
- For Extended Validation (EV) certificates, verify and confirm the legal existence and identity of the organization in accordance with the EV Guidelines
- Issue digital certificates in accordance with this document and fulfill its obligations presented herein
- Revoke certificates for any of the specific reasons and within the timeframes (24 hours or 5 days) defined in this document and TLS BR
- Publish accepted certificates and Certificate Revocation Lists (CRLs).
- Provide support to Subscribers and relying parties as described in this document, including the provision of online status verification services via OCSP

The Subscriber also acknowledges that Certum has no further obligations beyond those expressly stated in this document.

9.6.1 CA representations and warranties

Not applicable.

9.6.2 RA representations and warranties

Not applicable.

9.6.3 Subscriber representations and warranties

Certum requires each Applicant to acknowledge and accept a Subscriber Agreement or Terms of Use that is legally enforceable against the Subscriber. By accepting a certificate, the Subscriber represents and warrants to Certum and to any relying parties that:

- All information provided to Certum during the application, enrollment, and throughout the certificate lifecycle is accurate, complete, and true
- Subscriber maintains sole control, keeps confidential, and takes all reasonable measures to protect the private key
- Subscriber will review and verify the accuracy of the information contained in the certificate prior to its installation and use
- Certificate is used exclusively for authorized and legal purposes, consistent with the intended use defined in this CP/CPS and the applicable Subscriber Agreement or Terms of Use
- Subscriber will promptly notify Certum and request revocation if any information in the certificate becomes inaccurate or if there is any actual or suspected compromise of the private key
- Subscriber will immediately cease all use of the certificate and its associated private key upon expiration or revocation
- Subscriber will not use the private key to sign any other certificate or CRL as a Certification Authority
- The use of information provided by the Subscriber (e.g., domain names, organization names) does not infringe upon the intellectual property or proprietary rights of any third party
- The Subscriber will respond to Certum's instructions regarding certificate misuse or key compromise within the timeframe specified by the CA
- The certificate will not be used in high-risk systems or applications requiring fail-safe performance, where failure of the certificate could result in death, personal injury, or severe environmental damage

9.6.4 Relying party representations and warranties

Relying parties represent and warrant that, prior to relying on a certificate issued by Certum, they have read, understand, and agree to this CP/CPS and the applicable relying party agreement.

To exercise reasonable reliance, a relying party is responsible for:

- Obtaining sufficient knowledge on the use of digital certificates and PKI to make an informed decision regarding the degree of reliance
- Confirming the validity of each certificate in the certification path (up to the Root CA) by checking current revocation status via CRL or OCSP prior to any act of reliance
- Ensuring the certificate has not expired and is not revoked at the time of reliance
- Verifying that the certificate is used exclusively for its intended purpose and within the limitations defined by the Key Usage (KU) and Extended Key Usage (EKU) extensions
- Taking all reasonable steps to minimize risk by considering the economic value of the transaction, the potential loss or damage from erroneous identification, and any other indicia of reliability pertaining to the Subscriber
- Acknowledging that the final decision to rely on a certificate rests solely with the relying party, who bears all consequences, including legal liability, for any failure to observe these obligations

Any reliance on a certificate in a manner inconsistent with these requirements is at the Relying Party's own risk.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

Warranties of Certum are based on the general rules stated in the present CP/CPS and it is in accordance with the superior legal acts in force in the Republic of Poland. Disclaimer of warranties should be specified in an agreements with Subscribers and Certum.

9.8 Limitations of liability

If damages are the fault of Certum or of the parties that Asseco Data Systems S.A. made agreement with in such a way that the fault is transferred to Certum, the collective financial warranties (total liability for damages) of Certum in relation to all parties (including relying parties) cannot exceed (in a single case) the total amount of sums for credibility level:

DV TLS certificates

- Collective Certum's liability limit 200 000 EUR
- Certum's liability limit per covered damage 600 EUR

OV TLS certificates

- Collective Certum's liability limit 400 000 EUR
- Certum's liability limit per covered damage 15 000 EUR

EV TLS certificates

- Collective Certum's liability limit 1 000 000 EUR
- Certum's liability limit per covered damage 15 000 EUR

9.9 Indemnities

9.9.1 Subscriber liability

Subscriber liability results from the obligations and warranties stated in Section 9.6.3. The liability conditions are governed by an agreement with Asseco Data Systems S.A.

9.9.2 Relying party liability

Relying party liability results from the obligations and warranties stated in Section 9.6.4. The liability conditions may be governed by an agreement with Certum and a Subscriber.

Agreements with Subscribers and Certum require that relying parties have a sufficient amount of information to make a decision about the approval or rejection of an electronic signature while verifying it.

The parties should state the financial value of transaction that will be approved by them solely on the basis of the information set in a certificate and familiarize with information specified in Section 9.6.4.

9.10 Term and termination

9.10.1 Term

This CP/CPS becomes effective from the moment of marked with the status valid and publication in the Certum Repository.

Appendices to this CP/CPS become effective upon publication in the Certum Repository.

9.10.2 Termination

This CP/CPS is in force (has a current status) up to the moment of marked with the status valid and publication and approval of its new version.

9.10.3 Effect of termination and survival

Upon termination of this CP/CPS, Subscribers and relying parties are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual notices and communications with participants

Unless otherwise specified by agreement between the parties, participants will use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

These methods include, but are not limited to:

- Notices sent to the email addresses provided by the participant
- Communication utilizing contact information collected and validated during the application and identity verification process

General announcements intended for all participants, such as the publication of CRLs or changes to this CP/CPS, are handled through the Certum Repository rather than through individual notices.

9.12 Amendments

9.12.1 Procedure for amendment

Certum reviews this CP/CPS at least annually and is authorized to make changes as deemed necessary. Amendments are approved by the Certum Policy Authority and are evidenced by a new version number and an updated publication date in the document history.

9.12.2 Notification mechanism and period

Certum publishes all updated versions of this CP/CPS in its public Certum Repository (See Section 2.1).:

- Significant changes that have a material impact on participants are subject to a notification
- Editorial changes, such as corrections of spelling, grammar, or internal references, may be made without notice

9.12.3 Circumstances under which OID must be changed

The Certum Policy Authority retains sole discretion to determine whether an amendment to this CP/CPS requires a change to the Object Identifier (OID) of the policy.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

This CP/CPS and any related agreements SHALL be governed by and construed in accordance with the laws in force in the Republic of Poland.

9.15 Compliance with applicable law

Certum operates and provides its services in full compliance with all applicable national, local, and foreign laws, rules, regulations, ordinances, decrees, and orders.

To ensure legal integrity across all jurisdictions:

- Certum and all Participants comply with all applicable restrictions on the export or import of software, hardware, or technical information, particularly those relating to cryptographic products
- Certum meets the requirements of applicable data protection legislation, including the European General Data Protection Regulation (GDPR) and the Polish Personal Data Protection Law, implementing appropriate technical and organizational measures to protect personal data
- Certum maintains all necessary licenses and authorizations required by the laws of the jurisdictions in which it operates for the issuance and management of certificates.
- In delivering its PKI services, Certum complies in all material respects with high-level international standards and relevant laws governing TLS certificates

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CP/CPS and the documents incorporated herein by reference constitute the entire agreement between the parties, superseding all prior understandings or representations regarding this subject matter. In the event of any conflict between the provisions of this CP/CPS and a specific agreement with a participant, the terms of that specific agreement shall prevail with respect to the relevant party.

9.16.2 Assignment

Participants may not assign their rights or obligations under this CP/CPS without the prior written consent of Certum. Any attempted assignment without such consent is void. This document is binding upon and inures to the benefit of the parties and their respective successors and permitted assigns.

9.16.3 Severability

If particular parts of the present document or the agreements made on the grounds of it are regarded as violating the law in force or against the law, a competent court can order to respect the remaining (i.e. in accordance with the law) part of CPS or agreements already made, unless questioned parts are not significant from the point of view of exchange (e.g. commercial transaction) that the parties agreed on.

Resolution severability is particularly crucial in the agreements mentioned in chapter 9.6. If a severability clause is not included in an agreement, the whole agreement can be against the law even if this is not the parties intention.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Certum may seek indemnification and claim reasonable attorneys' fees, costs, and expenses from any Participant for damages and losses related to that Participant's conduct or breach of this CP/CPS.

This document SHALL be enforced as a whole, whilst failure by any person to enforce any provision of this document SHALL not be deemed a waiver of future enforcement of that or any other provision. No breach of any provision of this CP/CPS will be deemed waived unless the waiver is provided in writing and signed by an authorized representative of Certum

9.16.5 Force Majeure

Certum SHALL not be liable for failure or delay in the performance of its obligations where such failure or delay results from events beyond its reasonable control and without its fault or negligence.

9.17 Other provisions

No stipulation

APPENDIX A - Revisions

Version	Change Description	Date
1.0.0	Initial version	2026-04-29

APPENDIX B - Definitions, acronyms and references

Definitions

Applicant - The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Attestation Letter - A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Period - In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement.

Audit Report - A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

CAA - From RFC8659: "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue."

Certificate - An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Data - Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Policy - A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report - Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Profile - A set of documents or files that defines Certificate content and Certificate extensions, e.g. a Section in a CA's CPS or a certificate template file used by CA software.

Certificate Revocation List - A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority - An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs.

Certification Practice Statement - One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Certum Systems - The systems and technical interfaces operated by Certum for the provision of certification services, including certificate application, issuance, management, and revocation, such as CertManager, API, and ACME.

Control - "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country - Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

CSPRNG - A random number generator intended for use in a cryptographic system.

Domain Contact - The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Label - From RFC8499: "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names."

Domain Name - An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.

Expiry Date - The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Internal Name - A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top-Level Domain registered in IANA's Root Zone Database.

IP Address - A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.

Issuing CA - In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Key Compromise - A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.

Key Pair - The Private Key and its associated Public Key.

Legal Entity - An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Linting - A process in which the content of digitally signed data such as a Precertificate (RFC 6962), Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a tbsCertificate (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in these Requirements.

Network Perspective - Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is typically first handed off to the network infrastructure providing Internet connectivity to that perspective.

Object Identifier - A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder - An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Onion Domain Name - A Fully Qualified Domain Name ending with the RFC7686 ".onion" Special-Use Domain Name.

Online Certificate Status Protocol - An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Precertificate - A signed data structure that can be submitted to a Certificate Transparency log, as defined by RFC 6962 and containing the critical poison extension (OID: 1.3.6.1.4.1.11129.2.4.3).

Private Key - The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key - The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures or encrypt messages.

Public Key Infrastructure - A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates.

Random Value - A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

Registration Authority (RA) - Any Legal Entity that is responsible for identification and authentication of subjects of Certificates but does not issue Certificates.

Reliable Data Source - An identification document or source of data used to verify Subject Identity Information that is generally recognized as reliable.

Reliable Method of Communication - A method of communication verified using a source other than the Applicant Representative.

Relying Party - Any natural person or Legal Entity that relies on a Valid Certificate.

Repository - An online database containing publicly disclosed PKI documents and certificate status information.

Requirements - The Baseline Requirements found in this document.

Reserved IP Address - An IPv4 or IPv6 address contained in IANA special registries.

Root CA - The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers.

Subject - The entity identified in a Certificate.

Subject Identity Information - Information that identifies the Certificate Subject.

Subordinate CA - A Certification Authority whose Certificate is signed by a Root CA or another Subordinate CA.

Subscriber - A natural person or Legal Entity to whom a Certificate is issued.

Subscriber Agreement - An agreement between the CA and the Applicant/Subscriber specifying rights and responsibilities.

Terms of Use - Provisions regarding acceptable uses of a Certificate.

Trusted Root Store - A collection of trusted root Certification Authority certificates (Root CA Certificates) maintained and distributed by a software vendor, operating system, web browser, or other platform, which is used by applications to establish trust in certificate chains. A Certification Authority certificate included in a Trusted Root Store is treated as a trust anchor for the purpose of validating TLS certificates and other X.509 certificates.

Validity Period - From RFC 5280: “The period of time from notBefore through notAfter, inclusive.”

WHOIS - Information retrieved from the Domain Name Registrar or registry via WHOIS or RDAP.

Acronyms

CA - Certification Authority

CAA - Certification Authority Authorization

CP - Certificate Policy

CPS - Certification Practice Statement

CRL - Certificate Revocation List

DBA - Doing Business As

DNS - Domain Name System

FIPS - Federal Information Processing Standards

FQDN - Fully Qualified Domain Name

HSM - Hardware Security Module

IANA - Internet Assigned Numbers Authority

ICANN - Internet Corporation for Assigned Names and Numbers

ISO - International Organization for Standardization

OCSP - Online Certificate Status Protocol

PKI - Public Key Infrastructure

RA - Registration Authority

SSL - Secure Sockets Layer

TLS - Transport Layer Security

References

RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*. S. Bradner, March 1997.

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. D. Cooper et al., May 2008.

RFC 6962, *Certificate Transparency*. B. Laurie et al., June 2013.

RFC 7686, *The ".onion" Special-Use Domain Name*. J. Appelbaum et al., October 2015.

RFC 8499, *DNS Terminology*. P. Hoffman et al., January 2019.

RFC 8659, *DNS Certification Authority Authorization (CAA) Resource Record*. P. Hallam-Baker et al., November 2019.

ITU-T X.509, International Telecommunication Union, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

ISO/IEC 9594-8, International Organization for Standardization, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

CA/Browser Forum Baseline Requirements, Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, https://cabforum.org/working-groups/server/baseline-requirements/documents/

CA/Browser Forum Extended Validation Guidelines, Guidelines for the Issuance and Management of Extended Validation Certificates, https://cabforum.org/working-groups/server/extended-validation/documents/

CA/Browser Forum Network and Certificate System Security Requirements, Network and Certificate System Security Requirements, https://cabforum.org/working-groups/netsec/documents/

WebTrust for Certification Authorities, WebTrust audit program for Certification Authorities. https://www.cpacanada.ca/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

WebTrust for Certification Authorities – TLS Baseline Requirements, WebTrust program covering TLS Baseline Requirements. https://www.cpacanada.ca/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

WebTrust for Certification Authorities – Extended Validation, WebTrust program covering Extended Validation Certificates. https://www.cpacanada.ca/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

WebTrust for Certification Authorities – Network Security, WebTrust program for Network Security. https://www.cpacanada.ca/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria