NAVER Cloud Trust Services

Certificate Policy/Certificate Practices Statement

Version 1.0.8

27 November, 2025

Contents

1. INTRODUCTION

1.1 Overview

This Certificate Policy/Certification Practices Statement (CP/CPS) defines the company's certification policy, operational management procedures, and other necessary instructions in servicing the Certification Authority provided by NAVER Cloud Trust Services Corp. (“NAVER Cloud Trust Services”).

Between 11 September 2017 and 4 June 2023, NAVER Cloud Corp. (former NAVER BUSINESS PLATFORM) operated NAVER Global Root Certification Authority and NAVER Secure Certification Authority 1 according to NAVER Cloud Corp.'s Certification Practice Statement. As of 5 June 2023, NAVER Cloud Trust Services Corp. operates these CAs under NAVER Cloud Trust Services Corp.'s Certification Practice Statement.

This document is created in accordance with “RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, the international standard document that defines the Certificate Policy and Certification Practice Statement (CPS) framework. The company's Certificate Authority issuing the Secure Server Certificate (hereinafter “SSL”) conforms to the current version of “CA/Browser Forum (CABF) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” published by the CA/Browser Forum at http://www.cabforum.org.

In the event of any inconsistency between this CP/CPS and the Baseline Requirements, the Baseline Requirements take precedence over this document.

1.2 Document Name and Identification

This document is NAVER Cloud Trust Services Certificate Policy/Certification Practices Statement (CP/CPS). It describes the policies for the operation and management of the Certification Authorities operated by NAVER Cloud Trust Services. In particular, it specifies the legal, entrepreneurial, and technical requirements to grant, issue, renew, reissue, manage, use, and revoke certificates issued and to provide certification services to all relying parties, including subscribers.

1.2.1 Revisions

A history of changes to this document is included in APPENDIX A.

1.3 PKI Participants

The participants inside the Public Key Infrastructure (hereinafter “PKI”) of NAVER Cloud Trust Services are as follows.

① Certification Authorities

② Registration Authorities

③ Subscribers

④ Relying Parties

1.3.1 Certification Authorities

The Certification Authority (CA) is a term that refers to entities authorized to issue, renew, reissue, revoke, and manage certificates. NAVER Cloud Trust Services directly operates the Root Certification Authorities and Certification Authorities. Here is a list of Certification Authority certificates from NAVER Cloud Trust Services.

Root CAs

- NAVER Global Root Certification Authority
    - Public Key: RSA 4096
    - Serial Number: 0194301EA20BDDF5C5332AB1434471F8D6504D0D
    - Fingerprint (SHA256): 88F438DCF8FFD1FA8F429115FFE5F82AE1E06E0C70C375FAAD717B34A49E7265
    - Valid Until: 2037-08-19
- NAVER Cloud Trust Services RSA Root G1
    - Public Key: RSA 4096
    - Serial Number: 0193205EA337C2A7BB2756B16E35C27119203EF1
    - Fingerprint (SHA256): 49A2762987788D4834B32305D767760F244D507742E8C2539FD4CA3AD52C16EE
    - Valid Until: 2043-06-06
- NAVER Cloud Trust Services ECC Root G1
    - Public Key: EC secp384r1
    - Serial Number: 017F20237EE582113466C837E47815E5BE12BA15
    - Fingerprint (SHA256): A7C8681042F3675AA8505D3BA313D80F8AC3250FDF874AD29B834689C087FB11
    - Valid Until: 2043-06-06

Intermediate CAs

- NAVER Secure Certification Authority 1
    - Public Key: RSA 2048
    - Serial Number: 06046233A5825576A48272694718A8000F2F000D
    - Fingerprint (SHA256): C5EB1A7639B9D8D70B4F82ADD80794175EE4B6A3DB1861B38717C96FC1914927
    - Valid Until: 2027-08-19
- NAVER Secure Certification Authority 2
    - Public Key: RSA 4096
    - Serial Number: 149E7FC617A0789B17D776FD45C60B69754F5300
    - Fingerprint (SHA256): 571E521E5E22810D33BB1A39991143E9E64CD8DAE97D65931B194E19AEE81E86
    - Valid Until: 2035-11-19
- NAVER Cloud Trust Services G1 RSA CA1
    - Public Key: RSA 4096
    - Serial Number: 04A10F19A216DCBBF6088447D8F371ADCEE7D249
    - Fingerprint (SHA256): 17832DBB48F609B722A27507F1D327DE062D7F7B85B71325D8DD99B19FB5BAD4
    - Valid Until: 2033-06-06
- NAVER Cloud Trust Services G1 RSA CA2
    - Public Key: RSA 4096
    - Serial Number: 0931F2A391E433A99DFA9089B18EE56368893650
    - Fingerprint (SHA256): 45B3942959D74F8B546A6AB47404AFC4A583AD5FA6FFD89A827A2A78522F66FD
    - Valid Until: 2035-11-19

- NAVER Cloud Trust Services G1 RSA CA3
    - Public Key: RSA 4096
    - Serial Number: 0AE4F1A43970EF427243F96A66F9C83E8B8D6224
    - Fingerprint (SHA256): 027B4EEC38B46BFD6B5C3E028F0922D268D367698BD15E01F7BD081EC36C8369
    - Valid Until: 2028-10-19
- NAVER Cloud Trust Services G1 ECC CA1
    - Public Key: EC secp384r1
    - Serial Number: 05FAD6522186F62AE88BCB51D545F41EA4A35736
    - Fingerprint (SHA256): 882D9924FC69A00574D54C2BB4014825A1C1C71FA1D0238CAC865FE0AA4AD60B
    - Valid Until: 2033-06-06
- NAVER Cloud Trust Services G1 ECC CA2
    - Public Key: EC secp384r1
    - Serial Number: 0CD7EB1228062E6BF76156A65CE67D86CE0671ED
    - Fingerprint (SHA256): BBA98FFC6A2D5AD251B34BC6632D3DA88955CB46F4A1F4DF443980A4BF92845F
    - Valid Until: 2035-11-19
- NAVER Cloud Trust Services G1 ECC CA3
    - Public Key: EC secp384r1
    - Serial Number: 0DF5B9C54699D6873F46C53B13D980E0A7A0F466
    - Fingerprint (SHA256): 41C587A6BAC0143297D0EDC5D522B57CD8B2D1A0D4913A1B534A9F9A86668536
    - Valid Until: 2028-10-19

Between 11 September 2017 and 4 June 2023, NAVER Cloud Corp. (former NAVER BUSINESS PLATFORM) operated NAVER Global Root Certification Authority and NAVER Secure Certification Authority 1 according to NAVER Cloud Corp.'s Certification Practice Statement. As of 5 June 2023, NAVER Cloud Trust Services Corp. operates these CAs under NAVER Cloud Trust Services Corp.'s Certification Practice Statement.

1.3.2 Registration Authorities

The Registration Authorities (RA) are entities that approve and perform requests to issue, renew, reissue, and revoke subscriber certificates. The RAs identify and authenticate the individuals or entities requesting certificates and validate the submitted application information.

All the RA functions will be performed by NAVER Cloud Trust Services and none will be delegated to third parties.

1.3.3 Subscribers

A subscriber is an end user of a certificate issued by the CAs capable of using, and authorized to use, the private key that corresponds to the public key listed in a certificate.

A subscriber is an individual or entity that has end-user certificates issued by NAVER Cloud Trust Services CA. If NAVER Cloud Trust Services approves the issuance of certificates according to the procedures in Section 3.2 Initial Identity Validation of this document, individuals and entities outside of Korea may also become subscribers. To use certificates, all the subscribers are required to consent to the subscriber responsibilities and obligations specified in the "SSL Agreement" before issuing certificates.

1.3.4 Relying Parties

A relying party is any individual or entity that verifies a digital signature with a certificate issued by NAVER Cloud Trust Services or decrypts an encrypted document or a message.

1.3.5 Other Participants

No Stipulation

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued pursuant to this CP/CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the certificate.

1.4.2 Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A certificate only establishes that the information in the certificate was verified as reasonably correct when the certificate issued.

Certificates issued under this CP/CPS may not be used (i) for any application requiring fail safe performance such as (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d)weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) where prohibited by law.

Additionally, Certificates issued under this CP/CPS may not be used for “traffic management” or man-in-the middle purposes.

1.5 Policy Administration

1.5.1 Organization Administering the Document

NAVER Cloud Trust Services establishes and amends CP/CPS.

1.5.2 Contact Person

Contact details of NAVER Cloud Trust Services for cases including, but not limited to, security issues such as reporting weaknesses, requests for certification revocation related to CA services, suspected key damage, misuse and improper use of certificates are as follows:

- E-mail: dl_rootca@navercorp.com
- Address: NAVER Green Factory, 6, Buljeong-ro, Jeongja-dong, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea (13561)

1.5.3 Person Determining CPS Suitability for the Policy

In the case that the head of CA Center in NAVER Cloud Trust Services determines that a change to the CP/CPS is necessary, it will be amended.

NAVER Cloud Trust Services maintains and manages amendment records of the CP/CPS, including:

> ① CP/CPS version ② Overview of applicable tasks and its scope ③ CP/CPS revision records ④ Amended CP/CPS - Amendment contents - Reason for amendment, etc.

1.5.4 CP/CPS Approval Procedures

NAVER Cloud Trust Services may amend this CP/CPS, and any changes will be disclosed to the address listed in Section 1.5 of this document. The CP/CPS is reviewed at least annually, and updated versions are posted to the online repository at https://navercloudtrust.com/, with any updates overriding conflicting or outdated provisions in previous versions. Amendments of the

CP/CPS will generally not affect the relying parties, but if NAVER Cloud Trust Services determines that the changes have a significant impact, it may notify the affected parties in advance.

1.6 Definitions and Acronyms

1.6.1 Definitions

Affiliated Organization

An organization that has an organizational affiliation with a Subscriber and that approves or otherwise allows such affiliation to be represented in a certificate

Applicant

An entity applying for a certificate.

Application Software Vendor

A software developer whose software that displays or uses certificates and distributes root certificates.

Base Domain

A Domain Name which is formed by pruning one or more labels from the left side of a FQDN. Base Domains do not include public suffixes or any Domain Name which is created by removing one or more labels from the left side of a public suffix.

CA/Browser Forum

A group made up of Certificate Authorities and Browsers that establish and manage the requirements all public Certificate Authorities must meet.

Certificate Systems The system used by a CA or Delegated Third Party in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI-related services.

Certificate Transparency

An open framework for monitoring and auditing digital certificates. Crypto-module A hardware device such as a smartcard, token or hardware security module that generates and manages cryptographic keys securely.

Entropy

The randomness collected by a system for use in cryptography or other uses that require random data.

High Security Zone

A physical location where a CA's or Delegated Third Party's Private Key or cryptographic hardware is located.

Key Pair

A Private Key and associated Public Key.

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.

Multi-Perspective Issuance Corroboration

A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.

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.

OCSP Responder

An online software application operated under the authority of NAVER Cloud Trust Services and connected to its repository for processing certificate status requests.

P-Label

A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subseqeunt positions.

Primary Network Perspective

The Network Perspective used by the CA to make the determination of 1) the CA's authority to issue a Certificate for the requested domain(s) or IP address(es) and 2) the Applicant's authority and/or domain authorization or control of the requested domain(s) or IP address(es).

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 created with the holder corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Punycode

Punycode is a way to represent Unicode with the limited character subset of ASCII supported by the Domain Name System.

RA Practices Statement

A statement of the practices, which an RA follows.

Relying Party

An entity that relies upon either the information contained within a certificate or a time stamp token.

Secure Zone An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of Certificate Systems.

Subject

The entity named in the certificate.

Subscriber

As applicable, the entity identified as the Subject in the certificate and/or the entity that contracted with NAVER Cloud Trust Services for the certificate's issuance.

Subscriber Agreement

An agreement that governs the issuance and use of a certificate that the Applicant must read and accept before receiving a certificate.

Trusted Agent

An accountant, lawyer, notary, postal carrier or any entity certified by a State or National Government as authorized to confirm identities or other reliable third party.

WebTrust

The current version of CPA Canada's WebTrust Program for Certification Authorities.

X.509

The ITU-T standard for Certificates and their corresponding authentication framework

1.6.2 Acronyms

CA

Certification Authority

CABF

“CA/Browser” as in “CAB Forum”

CP

Certificate Policy

CPS

Certification Practice Statement

CRL

Certificate Revocation List

CSR

Certificate Signing Request

ETSI

European Telecommunications Standards Institute

FIPS

(US Government) Federal Information Processing Standard

FQDN

Fully Qualified Domain Name

FTP

File Transfer Protocol

HSM

Hardware Security Module

HTTP

Hypertext Transfer Protocol

ICANN

Internet Corporation for Assigned Names and Numbers

IETF

Internet Engineering Task Force

NIST

National Institute of Standards

OCSP

Online Certificate Status Protocol

OID

Object Identifier

PKCS

Public Key Cryptography Standard

PKI

Public Key Infrastructure

PKIX

IETF Working Group on Public Key Infrastructure

RA

Registration Authority

RFC

Request for Comments (at IETF.org)

RSP

Repository Service Provider

SHA

Secure Hashing Algorithm

SSL

Secure Sockets Layer

TLD

Top Level Domain

TLS

Transport Layer Security

TSA

Time-stamp authority

TSP

Time-stamp policy

TST

Time-stamp token

URL

Uniform Resource Locator

UTC

Coordinated Universal Time

2. PUBLICAION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The repository operated by NAVER Cloud Trust Services covers the following information:

1. Certificate Policy/Certification Practices Statement (CP/CPS)
2. Most recently issued certificate revocation list(CRL)
3. Most recently issued CA certificate revocation list(ARL)
4. Root CAs, CA Certificates, and Cross certificates issued by NAVER Cloud Trust Services
5. Other documents or information deemed necessary for disclosure on NAVER Cloud Trust Services

2.2 Publication of Certification Information

NAVER Cloud Trust Services publishes the information about the issuance and management of certificates on a website so that it will be available to any person at any time.

1. On the web: https://navercloudtrust.com/
2. By email to: dl_rootca@navercorp.com

3. By mail addressed to: NAVER Green Factory, 6, Buljeong-ro, Jeongja-dong, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea (13561)

Web pages for Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate are listed at https://navercloudtrust.com/.

2.3 Time or Frequency of Publication

The CRL is updated promptly upon the revocation of a certificate within one (1) day following revocation. Generally, the CRL is periodically updated and reissued at least every day, and their validity period is limited to seven (7) days.

NAVER Cloud Trust Services revises the CP/CPS at least annually regardless of any changes, and continues to update as needed to the latest version of the CA Browser Forum Baseline Requirements.

2.4 Access Controls on Repositories

The Repository is publicly available. NAVER Cloud Trust Services operates physical and logical security controls to protect the repository from unauthorized modification or deletion.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Type of Names

NAVER Cloud Trust Services issues Certificates with non-null subject DNs. The constituent elements of the subject DN conform to ITU X.500.

Domain Validation Subscriber Certificates contain a distinguished name in the Subject name field, and incorporate the following attributes:

- CN=common name

Organization Validation Subscriber Certificates contain a distinguished name in the Subject name field, and incorporate the following attributes:

- CN=common name

- O=organization name

- L=locality

- ST=state or province

- C=country code

NAVER Cloud Trust Services does not issue pseudonymous Certificates as Section 3.1.3 of this CP/CPS.

3.1.2 Need for Names to be Meaningful

NAVER Cloud Trust Services puts meaningful names in both the subjectDN and the issuerDN fields of Certificates.

3.1.3. Anonymity or Pseudonymity of Subscribers

NAVER Cloud Trust Services does not issue anonymous or pseudonymous Certificates.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Name

NAVER Cloud Trust Services does not, in general, enforce uniqueness of subject names. However, name uniqueness is enforced through the domain name system controlled by ICANN and that any FQDN in a Common Name must appear in a Subject Alternative Name in the certificate that has been verified in accordance with section 3.2.2.4. Also, the serial numbers assigned to certificates are unique, and generated serial numbers are not reused.

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers may not request certificates with content that infringes on the intellectual property rights of another entity. Unless otherwise specifically stated in this CP/CPS, NAVER Cloud Trust Services does not verify an Applicant's right to use a trademark and does not resolve trademark disputes. NAVER Cloud Trust Services may reject any application or require revocation of any certificate that is part of a trademark dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

A certificate applicant normally proves the ownership of his/her private key by providing a PKCS#10-formatted Certificate Signing Request, or a cryptographically equivalent proof to NAVER Cloud Trust Services.

3.2.2 Authentication of Organization and Domain Identity

NAVER Cloud Trust Services identifies and validates the applicant and all the persons, objects, and domains specified in a certificate under the following circumstances:

- During the certificate application process

- During the certificate reissuance process

The appropriate validation of an applicant's proxy is performed to ensure the right to request revocation within the scope required by this CP/CPS. All subject information to be contained in a certificate shall conform to the requirements of this CP/CPS and be validated in accordance with the procedures in this CP/CPS. Such verification process is intended for:

- Identifying the applicant requesting a certificate; or
- Confirming the existence and identity of the subject; or
- Confirming the physical location of the subject (the business presence in the physical address); or
- Confirming the ownership (or exclusive right) of the domain name to be included in a certificate; or
- Confirming whether the applicant is authorized to request a certificate.

3.2.2.1 Identity

For Organization Validation Subscriber Certificate, NAVER Cloud Trust Services verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. A Government agency in the jurisdiction of the Applicant’s legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation Letter.

Alternatively, NAVER Cloud Trust Services may verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

Generally, the certificate application is submitted online. When an applicant completes and submits an online form on the official website, NAVER Cloud Trust Services verifies:

- The identity of the organization and applicant representative; and
- The address of the organization

Identity/Address	Details
Organization Identity	1. The applicant or application representative submits information that can be proved to NAVER Cloud Trust Services (Ex: Business License, Government-issued tax document).2. Inquiry and verification of information submitted by the applicant or applicant representative in a reliable third-party database.3. Verification of organization and applicant representative identity by contacting through the information submitted by the applicant or applicant representative and contact information verified in a reliable third-party database.
Applicant Representative Identity	4. Fill out and submit the applicant representative's name, contact information, and institutional affiliation before or during the certificate application.5. While proceeding with the 3rd process of Organization Identity above, identity verification including applicant representative's employment status and representative qualification.
Organization Address	Only verified address information can be contained as geographical properties in the Subject field of the Organization Validation Subscriber Certificate. The information submitted by the applicant is compared and verified with a reliable third-party database. If there is an international standard or an official government standard for addresses, it will be followed first.**The general criteria for NAVER Cloud Trust Services to determine the address included in the certificate subject properties are as follows:• Country Name (C):** Using a two-letter country code according to ISO 3166-1 Alpha-2.• **State or Province (ST):** Using the subdivision name where the subdivision category is in State or Province according to ISO 3166-2, and not to be abbreviated.• **Locality or City (L):** The Locality field is the official English name of the city or town.

Under special circumstances, NAVER Cloud Trust Services may also verify the identity of the organization and applicant representative through a site visit and face-to-face method.

3.2.2.2 DBA/Trade name

If the Subject Identity Information is to include a DBA or tradename, NAVER Cloud Trust Services verify the Applicant's right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A Reliable Data Source;
3. Communication with a government agency responsible for the management of such DBAs or tradenames;

4. An Attestation Letter accompanied by documentary support; or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

3.2.2.3 Verification of Country

See Section 3.2.2.1

3.2.2.4 Validation of Domain Authorization or Control

Prior to issuing a Certificate, NAVER Cloud Trust Services validates that the Applicant has control over each FQDN listed in the Certificate by using at least one of the following approved methods as defined in the BR at the time of validation:

- 3.2.2.4.4 Constructed Email to Domain Contact
- 3.2.2.4.7 DNS Change
- 3.2.2.4.19 Agreed-Upon Change to Website – ACME
- 3.2.2.4.21 DNS Labeled with Account ID – ACME

NAVER Cloud Trust Services implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9 when using the 3.2.2.4.7, 3.2.2.4.19, 3.2.2.4.21. Network Perspectives observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.

3.2.2.5 Authentication of an IP Address

NAVER Cloud Trust Services does not issue a Certificate using IP Address.

3.2.2.6 Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, NAVER Cloud Trust Services shall refuse the issuance if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix” (e.g. “*.com”, “*.co.kr”). NAVER Cloud Trust Services refers to the "public suffix list" of http://publicsuffix.org/ (PSL) as the judgment criterion, and periodically checks and reflects PSL updates.

3.2.2.7 Data Source Accuracy and Validity Periods

All data sources are evaluated for reliability, accuracy, and for their protection from alteration and falsification before they are used for I&A purposes.

Data sources are revalidated in accordance with the following terms.

1. Legal existence and identity of Applicant: 397 days

2. Domain Name: 397 days

3.2.2.8 CAA Records

NAVER Cloud Trust Services's policy on checking CAA records is stated in Section 4.2.4.

3.2.2.9 Multi-perspective Issuance Corroboration

Multi-Perspective Issuance Corroboration attempts to corroborate the determinations (i.e., domain validation pass/fail, CAA permission/prohibition) made by the Primary Network Perspective from multiple remote Network Perspectives before Certificate issuance. This process can improve protection against equally-specific prefix Border Gateway Protocol (BGP) attacks or hijacks.

NAVER Cloud Trust Services MAY use either the same set, or different sets of Network Perspectives when performing Multi-Perspective Issuance Corroboration for the required

1) Domain Authorization or Control and

2) CAA Record checks.

NAVER Cloud Trust Services does not reuse or cached the information obtained from one Network Perspective when performing validation through subsequent Network Perspectives (e.g., different Network Perspectives cannot rely on a shared DNS cache to prevent an adversary with control of traffic from one Network Perspective from poisoning the DNS cache used by other Network Perspectives). All communications between a remote Network Perspective and the NAVER Cloud Trust Services take place over an authenticated and encrypted channel relying on modern protocols (e.g., over HTTPS).

A Network Perspective MAY use a recursive DNS resolver that is NOT co-located with the Network Perspective. However, the DNS resolver used by the Network Perspective MUST fall within the same Regional Internet Registry service region as the Network Perspective relying upon it. Furthermore, for any pair of DNS resolvers used on a Multi-Perspective Issuance Corroboration attempt, the straight-line distance between the two States, Provinces, or Countries the DNS resolvers reside in MUST be at least 500 km. The location of a DNS resolver is determined by the point where unencapsulated outbound DNS queries are typically first handed off to the network infrastructure providing Internet connectivity to that DNS resolver.

NAVER Cloud Trust Services does not rely on corroborations from previous attempts. There is no stipulation regarding the maximum number of validation attempts that may be performed in any period of time.

The ""Quorum Requirements"" Table describes quorum requirements related to Multi-Perspective Issuance Corroboration. If NAVER Cloud Trust Services does not rely on the same set of Network Perspectives for both Domain Authorization or Control and CAA Record checks, the quorum requirements will be met for both sets of Network Perspectives (i.e.,the Domain Authorization or Control set and the CAA record check set). Network Perspectives are

considered distinct when the straight-line distance between them is at least 500 km. Network Perspectives are considered ""remote"" when they are distinct from the Primary Network Perspective and the other Network Perspectives represented in a quorum.

The quorum requirements are as follows:

- With 2–5 remote Network Perspectives: up to 1 non-corroboration allowed
- With 6 or more remote Network Perspectives: up to 2 non-corroborations allowed

Accordingly, NAVER Cloud Trust Services must comply with the allowed number of non-corroborations based on the number of remote Network Perspectives employed during Multi-Perspective Issuance Corroboration, as well as the effective date-based requirements.

As of September 15, 2025: NAVER Cloud Trust Services MUST perform Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives, and Quorum Requirements MUST be satisfied. Certificate issuance MUST NOT proceed if the number of non-corroborations exceeds the allowed threshold.

As of March 15, 2026: NAVER Cloud Trust Services MUST perform Multi-Perspective Issuance Corroboration using at least three (3) remote Network Perspectives. In addition, at least two (2) of the Perspectives supporting the Primary MUST be distributed across distinct Regional Internet Registry (RIR) regions.

Certificate issuance must not proceed if any of these requirements are not met.

3.2.3 Authentication of Individual Identity

NAVER Cloud Trust Services does not issue individually validated Certificates to natural persons.

3.2.4 Non-verified Subscriber Information

Only verified information is contained in certificates. Optional subfields in the subject of an SSL Certificate must either contain information verified by NAVER Cloud Trust Services or be left empty.

3.2.5 Validation of Authority

If the Applicant for a Certificate containing Subject Identity Information is an organization, NAVER Cloud Trust Services uses a Reliable Method of Communication to verify the authenticity of the Applicant Representative’s certificate request. NAVER Cloud Trust Services uses the sources listed in section 3.2.2.1 to verify the Reliable Method of Communication.

The authority of Applicant Representatives to request Certificates on behalf of organizations is verified during the validation of the Applicant Representative’s identity.

NAVER Cloud Trust Services only accepts Certificate requests from individuals verified through reliable methods of communication. Among verified individuals, NAVER Cloud Trust Services

may only accept Certificate requests from individuals with written designation by the Applicant to request for Certificates. In cases that the Applicants want a list of its authorized Certificate requesters or wish to update that list, Applicants may request, which may be electronic.

3.2.6 Criteria for Interoperation

All cross-signed Subordinate CA Certificates that identify a NAVER Cloud Trust Services CA as the Subject are listed in the Repository, provided that NAVER Cloud Trust Services has arranged for or accepted the establishment of the trust relationship.

3.3 Identification and Authentication for Re-Key Requests

For re-key requests, NAVER Cloud Trust Services CA and RAs will conduct the same validation procedures as in Section 3.2 Initial Identity Validation.

3.3.1 Identification and Authentication for Routine Re-Key

See Section 3.2.2

3.3.2 Identification and Authentication for Re-Key After Revocation

See Section 3.2.2

3.4 Identification and Authentication for Revocation Request

NAVER Cloud Trust Services or the RA authenticates and identifies all certificate revocation requests made at the Subscriber's request. If identification and authentication procedures are required, NAVER Cloud Trust Services selects these procedures based on the circumstances of the request and follows a documented process.

Identification and authentication are not required in cases where the revocation request is made by NAVER Cloud Trust Services or where the request is made by reference to a revocation reason that is independent of the requester's identity.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Applicants will fulfill and submit the DV and OV Certificate application forms for NAVER Cloud Trust Services.

A revoked certificate suspected of phishing or fraud or a rejected certificate request is stored in a database operated within NAVER Cloud Trust Services. NAVER Cloud Trust Services can use such information to identify suspicious certificate requests.

In the case where the CA and the Subscriber are affiliated, Terms of Use applicable to the requested SSL/TLS Certificate is acknowledged and agreed to by an authorized applicant representative. An applicant representative is a natural person who is either the applicant, employed by the applicant, or an authorized agent who has express authority to represent the applicant, and who has authority on behalf of the applicant to acknowledge and agree to the Terms of Use.

4.1.2 Enrollment Process and Responsibilities

Prior to the issuance of a Certificate, all end entity subscribers shall submit following documentation:

1. A certificate request, which may be electronic; and
2. An agreement to Subscriber Agreement or Terms of Use, which may be electronic

NAVER Cloud Trust Services obtain any additional documentation to determine necessary to meet these requirements.

Prior to the issuance of a Certificate, NAVER Cloud Trust Services obtain from the Applicant a certificate request in a form prescribed by NAVER Cloud Trust Services and that complies with these requirements. One certificate request may suffice for multiple Certificates to be issued to the same Applicant provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request may be made, submitted and/or signed electronically.

The certificate request contains a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

4.2 Certificate Application Processing

NAVER Cloud Trust Services CA and RAs validate the accuracy of the information provided by an applicant. If an applicant directly submits a public key, the applicant can present the public key manually to NAVER Cloud Trust Services CA and RAs in the form of a PKCS#10 Certificate Signing Request (CSR).

4.2.1 Performing Identification and Authentication Functions

The RAs perform the identification and authentication of the information submitted by a subscriber as specified in Section 3.2 of this document.

NAVER Cloud Trust Services may request additional information to a subscriber in accordance with separate verification procedures for High Risk Certificate Requests.

4.2.2 Approval or Rejection of Certificate Applications

Once all the required subscriber information has been validated, NAVER Cloud Trust Services will approve the certificate request. However, if the subscriber information is not validated or if the request does not comply with the CP/CPS requirements, NAVER Cloud Trust Services may reject the certificate request.

Certificate applications that contain a new gTLD are not approved while the gTLD is still under consideration by ICANN.

NAVER Cloud Trust Services does not issue Certificates for Internal Names or Reserved IP Addresses.

4.2.3 Time to Process Certificate Applications

If the subscriber application and identification documents are processed normally, NAVER Cloud Trust Services will issue the certificate within a reasonable period of time after the certificate request.

4.2.4 Certificate Authority Authorization (CAA) Records

NAVER Cloud Trust Services checks for a CAA record for each dNSName in the subjectAltName extension of the Certificate to be issued, according to the procedure in RFC 8659, following the processing instructions set down in RFC 8659 for any records found.

The following Issuer Domain Names in CAA “issue” or “issuewild” records are recognized as permitting NAVER Cloud Trust Services to issue SSL/TLS certificate:

- navercloudtrust.com

NAVER Cloud Trust Services may decide not to check for a CAA record:

- For certificates for which a Certificate Transparency precertificate was created and logged in at least two public logs, and for which CAA was checked at time of Precertificate issuance.

- For certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Baseline Requirements section 7.1.2.3 or 7.1.2.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.

NAVER Cloud Trust Services is permitted to treat a record lookup failure as permission to issue if:

- the failure is outside the CA’s infrastructure; and

- the lookup has been retried at least once; and
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

NAVER Cloud Trust Services documents potential issuance that was prevented by a CAA record in sufficient detail to provide feedback to the CAB Forum on the circumstances.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Prior to issuing a Certificate NAVER Cloud Trust Services processes the Certificate Application and performs the required validation procedures in accordance with this CP/CPS. Once these procedures have been completed, the Certificate is generated and the appropriate key usage extension added.

Prior to signing a Certificate NAVER Cloud Trust Services performs conformance linting using appropriate tooling. If linting reports a nonconformity, a report is generated and issuance is halted.

Certificate issuance from a Root CA requires at least two authorized individuals one of whom deliberately issues a direct command in order to perform the signing operation.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

NAVER Cloud Trust Services notifies Subscriber of the issuance of a Certificate either via email.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Subscribers are solely responsible for installing the issued certificate on the subscriber's computer or hardware security module. Certificates are considered accepted on the earlier of

- The subscriber's use of the certificate,
- 30 days after the certificate's issuance.

4.4.2 Publication of the Certificate by the CA

NAVER Cloud Trust Services publishes the CA certificate in its repository and publishes end entity certificates by delivering them to the subscriber using email or an API.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

NAVER Cloud Trust Services may notify the public of the issuance of a certificate by adding it to one or more publicly accessible Certificate Transparency (CT) Logs.

RAs may receive notification of the issuance of certificates they approve.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The certificate shall be used lawfully in accordance with NAVER Cloud Trust Services's Subscriber Agreement the terms of the relevant CP/CPS. NAVER Cloud Trust Services does not manage the subscriber's private key.

See Section 9.6.3, provisions 2. and 4.

4.5.2 Relying Party Public Key and Certificate Usage

No stipulation

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

NAVER Cloud Trust Services does not offer Certificate renewal. To obtain a new certificate after a NAVER Cloud Trust Services issued Certificate has expired, the Applicant is required to generate a new Key Pair and request a new Certificate in accordance with this CP/CPS.

4.6.2 Who May Request Renewal

No stipulation

4.6.3 Processing Certificate Renewal Requests

No stipulation

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

NAVER Cloud Trust Services treats certificate re-key requests as requests for the issuance of a new Certificate.

4.7.2 Who May Request Certification of a New Public Key

No stipulation

4.7.3 Processing Certificate Re-Keying Requests

No stipulation

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

No stipulation

4.7.6 Publication of the Re-Keyed Certificate by the CA

No stipulation

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

NAVER Cloud Trust Services does not modify previously issued certificates. Any request for certificate modification will be treated as a request for the issuance of a new Certificate.

4.8.2 Who May Request Certificate Modification

No stipulation

4.8.3 Processing Certificate Modification Requests

No stipulation

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation

4.8.6 Publication of the Modified Certificate by the CA

No stipulation

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.9 Certificate Revocation and Suspension

NAVER Cloud Trust Services supports revocation of certificates, but does not allow temporary suspension or recovery of certificates.

Once a certificate has been revoked, it is marked as revoked by having its serial number added to the CRL.

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

NAVER Cloud Trust Services will revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing, without specifying a CRLReason, that NAVER Cloud Trust Services revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);

2. The Subscriber notifies NAVER Cloud Trust Services that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);

3. NAVER Cloud Trust Services obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);

4. NAVER Cloud Trust Services is made aware of a demonstrated or proven method that can easily compute the Subscriber’s Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);) (CRLReason #1, keyCompromise);

5. NAVER Cloud Trust Services obtains 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. (CRLReason #4, superseded).

NAVER Cloud Trust Services will revoke a Certificate within 5 days and use the corresponding CRLReason if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CABF Baseline Requirement (CRLReason #4, superseded);

2. NAVER Cloud Trust Services obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);

3. NAVER Cloud Trust Services is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement (CRLReason #9, privilegeWithdrawn);

4. NAVER Cloud Trust Services is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation);

5. NAVER Cloud Trust Services is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);

6. NAVER Cloud Trust Services is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);

7. NAVER Cloud Trust Services is made aware that the Certificate was not issued in accordance with the BRor thisCP/CPS (CRLReason #4, superseded);

8. NAVER Cloud Trust Services determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);

9. NAVER Cloud Trust Services's right to issue Certificates under the BR expires or is revoked or terminated, unless NAVER Cloud Trust Services has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);

10. Revocation is required by NAVER Cloud Trust Services's CP/CPS for a reason that is not otherwise required to be specified by this section 4.9.1.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL); or

11. NAVER Cloud Trust Services is made aware of a demonstrated or proven method that exposes the Subscriber’s Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise).

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

NAVER Cloud Trust Services will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies NAVER Cloud Trust Services that the original certificate request was not authorized and does not retroactively grant authorization;
3. NAVER Cloud Trust Services obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. NAVER Cloud Trust Services obtains evidence that the Certificate was misused;
5. NAVER Cloud Trust Services is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with the applicable Certification Practice Statement;
6. NAVER Cloud Trust Services determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. NAVER Cloud Trust Services or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. NAVER Cloud Trust Services's or Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless NAVER Cloud Trust Services has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by NAVER Cloud Trust Services's Certification Practice Statement; or
10. NAVER Cloud Trust Services will revoke a Cross Certificate if the cross-signed entity or Cross Certificate no longer meets the Applicable Requirements.

4.9.2 Who Can Request Revocation

The Subscriber, RA, or Issuing CA can initiate revocation.

NAVER Cloud Trust Services provides a process for Subscribers to request revocation of their own Certificates. Subscribers may request revocation of their own certificate on the following methods:

- Sending an email to dl_rootca@navercorp.com including sufficient detail to identify the specific certificates to be revoked

Additionally, Subscribers, Relying Parties, Application Software Supplier, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

4.9.3 Procedure for Revocation Request

NAVER Cloud Trust Services processes a revocation request as follows:

1. NAVER Cloud Trust Services logs the identity of entity making the request or problem report and the reason for requesting revocation. NAVER Cloud Trust Services may also include its own reasons for revocation in the log.

2. NAVER Cloud Trust Services may request confirmation of the revocation from a known administrator, where applicable, via out of band communication (e.g., telephone, fax, etc.).

3. If the request is authenticated as originating from the Subscriber, NAVER Cloud Trust Services revokes the certificate.

4. For requests from third parties, NAVER Cloud Trust Services personnel investigates the request and (if needed) revokes the applicable certificate within 24 hours after receipt.

5. If NAVER Cloud Trust Services determines that revocation is appropriate, NAVER Cloud Trust Services personnel revoke the certificate and update the CRL.

NAVER Cloud Trust Services maintains a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports. If appropriate, NAVER Cloud Trust Services forwards complaints to law enforcement.

Subscriber certificate revocation requests can be submitted to the email address disclosed in Section 1.5.2.

4.9.4 Revocation Request Grace Period

Subscribers are required to request revocation within one day after detecting the loss or compromise of the Private Key. NAVER Cloud Trust Services may grant and extend revocation grace period on a case-by-case basis.

4.9.5 Time Within Which CA Must Process the Revocation Request

NAVER Cloud Trust Services begins the procedure for certificate revocation immediately after the request has been received.

After the certificate revocation, the CAs apply the revocation to the CRL, and in no case is it later than 24 hours following the revocation.

Within 24 hours after receiving a Certificate Problem Report, NAVER Cloud Trust Services investigates the facts and circumstances related to the report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, NAVER Cloud Trust Services works with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which NAVER Cloud Trust Services will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation must not exceed the time frame set forth in Section 4.9.1.1. The date selected by NAVER Cloud Trust Services will consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that they didn’t receive the goods they ordered);and
5. Relevant legislation.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties are required to confirm the validity of each certificate in the certificate chain by checking for certificate validity, issuer to subject name chaining, policy and key use constraints and revocation status through CRL or OCSP responder before relying on a certificate.

4.9.7 CRL Issuance Frequency

NAVER Cloud Trust Services will update and reissue CRLs with a frequency greater than or equal to that required by the NAVER Cloud Trust Services CP/CPS.

CRLs are available via a publicly-accessible HTTP URL (i.e., "published").

Within twenty-four (24) hours of issuing its first Certificate, the CA will generate and publish either:

- a full and complete CRL; OR
- partitioned (i.e., "sharded") CRLs that, when aggregated, represent the equivalent of a full and complete CRL.

NAVER Cloud Trust Services issuing Subscriber Certificates:

1. will update and publish a new CRL at least every:

• seven (7) days if all Certificates include an Authority Information Access extension with an id-ad-ocsp accessMethod (“AIA OCSP pointer”); or

• four (4) days in all other cases;

2. will update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked.

NAVER Cloud Trust Services issuing CA Certificates:

1. will update and publish a new CRL at least every six (6) months;

2. will update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked.

NAVER Cloud Trust Services will continue issuing CRLs until one of the following is true:

1. all Subordinate CA Certificates containing the same Subject Public Key are expired or revoked; OR

2. the corresponding Subordinate CA Private Key is destroyed.

See Section 2.2 for CRL locations.

4.9.8 Maximum Latency for CRLs

The CRL is posted to the CRL repository within an hour following the CRL generation.

4.9.9 On-Line Revocation/Status Checking Availability

The following only applies for communicating the status of Certificates and Precertificates which include an Authority Information Access extension with an id-ad-ocsp accessMethod.

The following applies for communicating the status of all Certificates for which an OCSP responder is willing or required to respond.

OCSP responses conform to RFC 6960 and/or RFC 5019. They are either:

1. Signed by the CA that issued the Certificates whose revocation status they indicate, or

2. Signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is indicated. The OCSP Responder's signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

OCSP responders operated by NAVER Cloud Trust Services SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019. NAVER Cloud Trust Services processes the Nonce extension (1.3.6.1.5.5.7.48.1.2) in accordance with RFC 8954.

For the status of a Subscriber Certificate or its corresponding Precertificate:

- An authoritative OCSP response be available (i.e. the responder does not respond with the “unknown” status) starting no more than 15 minutes after the Certificate or Precertificate is first published or otherwise made available.
- For OCSP responses with validity intervals less than sixteen hours, NAVER Cloud Trust Services provides an updated OCSP response prior to one-half of the validity period before the nextUpdate.
- For OCSP responses with validity intervals greater than or equal to sixteen hours, NAVER Cloud Trust Services provides an updated OCSP response at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For the status of a Subordinate CA Certificate, NAVER Cloud Trust Services provides an updated OCSP response at least every twelve months, and within 24 hours after revoking the Certificate.

OCSP responses for Subscriber Certificates have a validity interval greater than or equal to eight hours and less than or equal to ten days.

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

A certificate serial is “assigned” if:

- a Certificate or Precertificate with that serial number has been issued by the Issuing CA; or
- a Precertificate with that serial number has been issued by a Precertificate Signing Certificate, as defined in Section 7.1.2.4, associated with the Issuing CA.

A certificate serial is “unassigned” if it is not “assigned”.

If the OCSP responder receives a request for the status of a certificate serial number that is “unassigned”, then the responder does not respond with a “good” status. If the OCSP responder is for a CA that is not Technically Constrained in line with Section 7.1.2.3 or Section 7.1.2.5, the responder does not respond with a “good” status for such requests.

4.9.10 On-Line Revocation Checking Requirements

No Stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No Stipulation

4.9.12 Special Requirements re Key Compromise

In the case that a private key used for a certificate electronic signature is damaged, the subscriber must immediately notify NAVER Cloud Trust Services that the subscriber's certificate has been compromised.

If subscriber's key has been compromised or subscriber suspects it has been compromised, subscriber can and should submit a key compromise report to NAVER Cloud Trust Services email address:

- dl_rootca@navercorp.com

A key compromise report must include:

1. The private key itself and (optionally) the certificate.
2. A valid email address so that subscriber can receive confirmation of the problem report and associated certificate revocations.

In accordance with CP/CPS Section 4.9.1.1, If NAVER Cloud Trust Services obtains evidence that subscriber's private key corresponding to the public key in the certificate suffered a key compromise, the certificate will be revoked in time.

4.9.13 Circumstances for Suspension

NAVER Cloud Trust Services does not suspend certificates.

4.9.14 Who Can Request Suspension

No Stipulation

4.9.15 Procedure for Suspension Request

No Stipulation

4.9.16 Limits on Suspension Period

No Stipulation

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Revocation entries on a CRL or OCSP Response MUST NOT be removed until after the Expiry Date of the revoked Certificate

4.10.2 Service Availability

NAVER Cloud Trust Services operates and maintains its CRL and OCSP capability (when applicable) with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The certificate status service is available 24x7, unless it is temporarily unavailable due to maintenance or service failure.

4.10.3 Optional Features

No stipulation

4.11 End of Subscription

A subscriber can cancel or terminate its certificate subscription through the following: - A subscriber visits the website and requests revocation to cancel the certificate service; - When a certificate expires and is not newly issued or renewed, the certificate service will be terminated.

4.12 Key Escrow and Recovery

NAVER Cloud Trust Services does not escrow the subscribers' private keys.

4.12.1 Key Escrow and Recovery Policy and Practices

No Stipulation

4.12.2 Session key encapsulation and recovery policy and practices

No Stipulation

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Security Controls

NAVER Cloud Trust Services protects the location where the CA system is installed from physical threats such as intrusion or unauthorized access by outsiders.

5.1.1 Site Location and Construction

NAVER Cloud Trust Services installs and operates the CA system in a separate control zone and performs physical access control for the system.

5.1.2 Physical Access

NAVER Cloud Trust Services operates its own access control system and controls access to restricted areas by combining biometric authentication including the identification card and fingerprint recognition.

NAVER Cloud Trust Services uses multi-factor authentication mechanisms for access control as well as additional security mechanisms designed to ensure that only authorized individuals enter the CA facilities. NAVER Cloud Trust Services enforces two-person access for all access to CA systems.

5.1.3 Power and Air Conditioning

NAVER Cloud Trust Services uses an uninterruptable power supply (UPS) to prevent serious damage from power outages.

NAVER Cloud Trust Services installs and operates an air conditioning system to maintain constant temperature and humidity.

5.1.4 Water Exposures

NAVER Cloud Trust Services installs its CA system at a distance from the floor to protect it from water exposure.

5.1.5 Fire Prevention and Protection

NAVER Cloud Trust Services uses fire detectors, portable fire extinguishers, and automatic fire extinguishing facilities in the space where the CA system is installed.

5.1.6 Media Storage

NAVER Cloud Trust Services controls physical access by keeping the storage and recording media used for the CA service in a fireproof safe.

5.1.7 Waste Disposal

NAVER Cloud Trust Services performs processing according to the internal procedures or complete destruction in disposing of any media storing keys, activation data, or sensitive files.

5.1.8 Off-Site Backup

NAVER Cloud Trust Services performs backups for the CA service. The backup location has the same level of security and control as the place where the main facility is installed.

5.2 Procedural Controls

5.2.1 Trusted Roles

All NAVER Cloud Trust Services employees who have permissions to issue and manage certificates and access and use hardware security modules are considered as major business contact persons and perform their duties as Trusted Roles. The Trusted Roles are defined as follows:

- Executive Officer
- Policy Managers
- Certificate Management Officers
- Registration Management Officers
- Validation Specialists
- Internal Auditors
- System Engineers / System Operators
- CA System Developers

5.2.2 Number of Individuals Required per Task

CA private keys can only be backed up, stored, and recovered by personnel in trusted roles using, at least, dual control in a physically secured environment. At least three people are required for CA key generation, CA private key backup, CA key recovery and CA signing key activation.

5.2.3 Identification and Authentication for Each Role

Each CA or Delegated Third Party SHALL require that each individual in a Trusted Role use a unique credential created by or assigned to that person in order to authenticate to Certificate Systems.

5.2.4 Roles Requiring Separation of Duties

Each CA or Delegated Third Party SHALL document the responsibilities and tasks assigned to Trusted Roles and implement “separation of duties” for such Trusted Roles based on the security-related concerns of the functions to be performed.

The Executive Officer, Internal Auditors, System Engineers / System Operators do not perform other trusted role tasks.

The Policy Managers and Validation Specialists do not perform certificate management or registration management tasks.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The major business contact person at the certification center operated by NAVER Cloud Trust Services establishes and performs the personnel management and management policies that can reasonably verify the competence and job aptitude of the employees in accordance with the CP/CPS requirements.

The Trusted Roles can only be performed by NAVER Cloud Trust Services employees, but some functions can be consigned to subcontracted personnel to the extent permitted by NAVER Cloud Trust Services.

5.3.2 Background Check Procedures

NAVER Cloud Trust Services validates the requirements required for employee recruitment according to the company's information security policy or human resource management policy.

5.3.3 Training Requirements and Procedures

NAVER Cloud Trust Services conducts the certificate management training necessary for business performance when recruiting any employees required to be educated, including the Trusted Roles.

The skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures, common threats to the information verification process, and CABF Baseline Requirements.

NAVER Cloud Trust Services maintains records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

NAVER Cloud Trust Services documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task. NAVER Cloud Trust Services requires all Validation Specialists to pass an examination provided by NAVER Cloud Trust Services on the information verification requirements outlined in CABF Baseline Requirements.

5.3.4 Retraining Frequency and Requirements

The personnel responsible for the certification task in NAVER Cloud Trust Services need to receive retraining necessary for performing their work annually.

5.3.5 Job Rotation Frequency and Sequence

No stipulation

5.3.6 Sanctions for Unauthorized Actions

NAVER Cloud Trust Services may impose sanctions, including suspension and termination, on personnel that performed unauthorized acts in accordance with the internal regulations.

5.3.7 Independent Contractor Requirements

In the case that an independent contractor is assigned to perform a Trusted Role of NAVER Cloud Trust Services certification service, NAVER Cloud Trust Services can impose the same sanctions against unauthorized actions as specified in Section 5.3.6.

NAVER Cloud Trust Servcies verifies that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.

5.3.8 Documentation Supplied to Personnel

NAVER Cloud Trust Services provides the internal documents and training materials on the major certification tasks for all the employees involved.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

NAVER Cloud Trust Services manages and generates essential actions and sensitive events that can be occurred in CA, RA applications and relevant systems. The log records, not only in a system but also in a manual event, are including type of event, success or failure, date and time, and user or system.

NAVER Cloud Trust Services records at least the following events:

1. CA certificate and key lifecycle events, including:
a. Key generation, backup, storage, recovery, migration, transportation, and destruction;
b. Certificate requests, renewal, and re-key requests, and revocation;
c. Approval and rejection of certificate requests;
d. Cryptographic device lifecycle management events;
e. Generation of Certificate Revocation Lists;
f. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10); and
g. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles;

2. Subscriber Certificate lifecycle management events, including:
a. Certificate requests, renewal, and re-key requests, and revocation;

b. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;

c. Approval and rejection of certificate requests;

d. Issuance of Certificates;

e. Generation of Certificate Revocation Lists; and

f. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10).

3. Security events, including:

    a. Successful and unsuccessful PKI system access attempts;

    b. PKI and security system actions performed;

    c. Security profile changes;

    d. Installation, update and removal of software on a Certificate System;

e. System crashes, hardware failures, and other anomalies;

f. Relevant router and firewall activities (as described in Section 5.4.1.1); and

g. Entries to and exits from the CA facility.

Log records include at least the following elements:

1. Date and time of record;

2. Identity of the person making the journal record (when applicable); and

3. Description of the record.

5.4.1.1 Router and firewall activities logs

Logging of router and firewall activities necessary to meet the requirements of Section 5.4.1, Subsection 3.6 MUST at a minimum include:

1. Successful and unsuccessful login attempts to routers and firewalls; and

2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and

3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and

4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

5.4.2 Frequency of Processing Log

Audit log review period cycle is determined by NAVER Cloud Trust Services depending on whether automated log monitoring and alerting is available or not. For systems capable of continuous automated log monitoring and alerting use this function to check log processing, log integrity, and automatically receive reports. At least once every month, internal auditors review the logs generated by CA systems, check the log file integrity.

For systems where continuous automated log monitoring and alerting is not possible, At least once every month, internal auditors review the logs generated by CA systems, check the log file integrity.

5.4.3 Retention Period for Audit Log

Until October 2020, retention period for the audit log were at least seven (7) years. Every audit log generated after October, 31, 2020, will be retained for at least two (2) years:

3. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1 (1)) after the later occurrence of:
a. the destruction of the CA Private Key; or
b. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1 (2)) after the revocation or expiration of the Subscriber Certificate;

3. Any security event records (as set forth in Section 5.4.1 (3)) after the event occurred.

5.4.4 Protection of Audit Log

The audit records generated by each system are managed by the personnel designated by NAVER Cloud Trust Services, and only the administrators and internal auditors can view and search the audit records generated by each system. The generated audit records are not allowed to be modified. It is designed to break the data integrity of audit records when someone attempt to modify them.

5.4.5 Audit Log Backup Procedures

NAVER Cloud Trust Services maintains formal procedures to ensure that audit logs are backed up and retained to keep them available as necessary for the CA service and as stipulated by applicable standards.

5.4.6 Audit Log Accumulation System (internal vs. external)

No stipulation

5.4.7 Notification to Event-Causing Subject

No stipulation

5.4.8 Vulnerability Assessments

NAVER Cloud Trust Services continuously monitors external and internal vulnerabilities, and evaluates risks regularly that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;

2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

After risk assessment, NAVER Cloud Trust Services establishes and implements a risk management plan.

5.5 Records Archival

5.5.1 Types of Records Archived

In addition to the logs described in Section 5.4.1, the following records are archived:

1. Documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems; and

2. Documentation related to their verification, issuance, and revocation of certificate requests and certificates.

5.5.2 Retention Period for Archive

Archived audit logs as set forth in Section 5.5.1 are retained for a period of two (2) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer.

NAVER Cloud Trust Services retains all the documentation relating to certificate requests and the issuance thereof, and the revocation thereof for at least two (2) years after the certificates become invalid or revoked.

5.5.3 Protection of Archive

The backups of information archived should be maintained and managed at a distinct and separate location with similar security and availability requirements.

5.5.4 Archive Backup Procedures

The backed-up archives can be utilized regularly in the event of the loss or destruction of the primary archives in accordance with the backup and recovery procedures.

5.5.5 Requirements for Time-Stamping of Records

All the archived records will be generated and time-stamped by utilizing the visual information used in NAVER Cloud Trust Services. Such information is not encrypted.

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

When rolling over a CA, NAVER Cloud Trust Services generates a new Key Pair and begins using the new certificate. The old CA Private Keys are still protected, and the old CA certificate is still made available to verify signatures until all of the certificates signed with the Private Key expire. Towards the end of a CA Private Key's lifetime, whether due to expiration or due to unilateral change by NAVER Cloud Trust Services, NAVER Cloud Trust Services ceases using the expiring CA Private Key to sign certificates and uses the old Private Key only to sign CRLs and OCSP responder certificates. At that time, a new CA signing Key Pair is commissioned. All subsequently issued Certificates and CRLs are signed with the new private signing key.

Both the old and new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA Certificate expiration. The new CA Public Key Certificate is provided to subscribers and relying parties through the delivery methods in Section 6.1.4.

Where a cross-signed CA performs a key rollover, NAVER Cloud Trust Services obtains a new CA Public Key (PKCS#10) or new CA Certificate from the other CA and distributes a new CA Cross Certificate as specified herein.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

5.7.1.1 Incident Response and Disaster Recovery Plans

NAVER Cloud Trust Services maintains controls to provide reasonable assurance that damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures.

NAVER Cloud Trust Services documents a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. NAVER Cloud Trust Services is not required to publicly disclose its business continuity plans but make its business continuity plan and security plans available to the NAVER Cloud Trust Services's auditors upon request. NAVER Cloud Trust Services annually tests, reviews, and updates these procedures.

The business continuity plan at least include:

1. The conditions for activating the plan,
2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective;
9. Regular testing of contingency plans.
10. NAVER Cloud Trust Services's plan to maintain or restore NAVER Cloud Trust Services's business operations in a timely manner following interruption to or failure of critical business processes
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time
13. How frequently backup copies of essential business information and software are taken;

14. The distance of recovery facilities to the NAVER Cloud Trust Services’s main site; and

15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

5.7.1.2 Mass Revocation Plans

NAVER Cloud Trust Services has a mass revocation plan, and asserts in section 5.7.1 of this CPS that it maintains a comprehensive and actionable plan for mass revocation events, that it performs annual testing of the mass revocation plan, and that it incorporates lessons learned into such plan in order to continually improve its preparedness for mass revocation events over time.

NAVER Cloud Trust Services's mass revocation plan includes clearly defined, actionable, and comprehensive procedures designed to ensure a rapid, consistent, and reliable response to large-scale certificate revocation scenarios. NAVER Cloud Trust Services is not required to publicly disclose its mass revocation plan or procedures but must make them available to its auditors upon request. NAVER Cloud Trust Services annually tests, reviews, and updates its plan and such procedures. The mass revocation plan may be integrated into NAVER Cloud Trust Services's incident response, business continuity, disaster recovery, or other similar plans or procedures, provided that provisions governing mass revocation events remain clearly identifiable and satisfy these requirements.

Mass revocation provisions include:

1. Activation criteria – specific, objective, and measurable thresholds at which the mass revocation plan is triggered based on the NAVER Cloud Trust Services's risk profile, issuance volumes, and operational capabilities;

2. Customer contact information – how subscriber and customer contact details are stored, maintained, and kept up to date;

3. Automation points – processes that are automated or could be automated, and those processes that require manual intervention;

4. Targets and timelines – for incident triage, revocation initiation, certificate replacement, and post-event review;

5. Subscriber notification methods – mechanisms for notifying impacted Subscribers;

6. Role assignments – roles and responsibilities of personnel responsible for initiating, coordinating, and executing the plan;

7. Training and education – training, awareness, and readiness activities for personnel responsible for, or supporting, the plan;

8. Plan testing – annual operational testing to assess readiness and demonstrate implementation feasibility, using one or more of tabletop exercises, simulations, parallel testing, or controlled test environments that do not involve the revocation of active Subscriber Certificates; and

9. Post-test analysis and update schedule – how lessons learned from testing or live incidents are incorporated into the plan, and how often it is reviewed and updated.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

NAVER Cloud Trust Services uses archived data for recovery when the critical data related to subscriber certificates are compromised or destroyed.

5.7.3 Entity Private Key Compromise Procedures

Once NAVER Cloud Trust Services has recognized that the private keys used in the certification service are not secure, it revokes the CA and subscriber certificates containing public keys and reissues CA and subscriber certificates by creating new key pairs. If a Root CA private key is compromised, NAVER Cloud Trust Services will inform browser vendors of the compromise and best estimate of the date of compromise.

5.7.4 Business Continuity Capabilities After a Disaster

NAVER Cloud Trust Services establishes and implements business continuity plans so as to prevent the interruption of certificate lifecycle tasks, such as certificate issuance, renewal, and revocation, and major certification services, such as the CA facility and equipment management, in the event of failure, terrorism, power outage, earthquake, fire, flood, etc.

5.8 CA or RA Termination

When NAVER Cloud Trust Services discontinues operating NAVER Cloud Trust Services CA and RAs, the impact of such action has to be minimized as much as possible in light of the prevailing circumstances. These include:

- Providing practicable and reasonable prior notice to all the subscribers;
- Assisting with the orderly transfer of service and operational records to a successor CA, if any;
- Preserving all the audit logs and retention records required by this CP/CPS for a minimum of one (1) year;
- Revoking all the certificates no later than at the time of termination.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The CA keys operated by NAVER Cloud Trust Services are generated inside a FIPS 140-2 Level 3-certified hardware security module(HSM). The generated private keys cannot be extracted outside the HSM except for the purpose of a key backup allowed by NAVER Cloud Trust Services.

Subscriber Key Pairs are generated by the Subscriber.

6.1.2 Private Key Delivery to Subscriber

NAVER Cloud Trust Services does not generate subscriber Key Pairs.

6.1.3 Public Key Delivery to Certificate Issuer

The subscribers submit a Certificate Signing Request in PKCS#10 format to the CA or RAs via a website with an SSL Certificate applied.

6.1.4 CA Public Key Delivery to Relying Parties

The CA public keys are digitally signed by the Root CA operated by NAVER Cloud Trust Services. NAVER Cloud Trust Services establishes and enforces the procedures for delivering chain-certified CA certificates upon an applicant's receipt of issued certificates so that CA certificates are delivered to the relying parties.

6.1.5 Key Sizes

Certificates MUST meet the following requirements for algorithm type and key size.

Root CA Certificates, Subordinate CA Certificates and Subscriber Certificates will follow the same requirements:

Type	Permissible Values
Digest algorithm	SHA-256, SHA-384, or SHA-512
Minimum RSA modulus size (bits)	- **Root CA:** at least RSA 4096 - **Subordinate CA:** at least RSA 2048 - **Subscriber:** at least RSA 2048
Minimum ECDSA key size (bits)	- **Root CA:** at least NIST P-384 - **Subordinate CA:** at least NIST P-256 - **Subscriber:** at least NIST P-256

6.1.6 Public Key Parameters Generation and Quality Checking

For RSA keys, NAVER Cloud Trust Services confirms that the value of the public exponent is an odd number equal to 3 or more.

For ECDSA keys, NAVER Cloud Trust Services confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Root CA Private Keys are not used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates, and OCSP Response Verification Certificates); and
4. Certificates for OCSP Response verification.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CA key pairs are archived and operated in a hardware security module with FIPS 140-2 Level 3 or higher.

6.2.2 Private Key (n out of m) Multi-Person Control

NAVER Cloud Trust Services performs the generation of CA key pairs in accordance with its internal key generation procedures. At least three personnel participate in key pair generation.

6.2.3 Private Key Escrow

NAVER Cloud Trust Services does not escrow CA key pairs to a third party.

6.2.4 Private Key Backup

The backups of CA private keys are stored in a secure location in accordance with NAVER Cloud Trust Services backup procedures. The backed-up private keys are securely stored in a fireproof safe through a hardware security module (HSM).

6.2.5 Private Key Archival

NAVER Cloud Trust Services does not archive CA private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

For CA private key backup purposes, under the approval of NAVER Cloud Trust Services, CA private keys may be extracted in accordance with the applicable instructions specified by a hardware security module manufacturer.

6.2.7 Private Key Storage on Cryptographic Module

NAVER Cloud Trust Services's private keys are generated and stored inside cryptographic modules which meet the requirements of 6.2.1 of this CP/CPS.

6.2.8 Method of Activating Private Key

Under the approval of NAVER Cloud Trust Services, the hardware security module in which CA private keys are stored may be activated in accordance with the applicable instructions specified by a hardware security module manufacturer.

6.2.9 Method of Deactivating Private Key

Under the approval of NAVER Cloud Trust Services, the hardware security module in which CA private keys are stored may be deactivated in accordance with the applicable instructions specified by a hardware security module manufacturer.

6.2.10 Method of Destroying Private Key

NAVER Cloud Trust Services may destroy CA private keys for the following reasons: • CA certificates expired • CA private keys damaged, leaked, or potentially compromised.

NAVER Cloud Trust Services may destroy a Private Key by deleting it from all known storage partitions. NAVER Cloud Trust Services also zeroizes the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with binary zeros. If the zeroization or re-initialization procedure fails, NAVER Cloud Trust Services will degaussing and/or crush, shred the device in a manner that destroys the ability to extract any Private Key.

6.2.11 Cryptographic Module Rating

Use a hardware security module that conforms to the requirements of Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

CA, RA, and subscriber certificates are archived in accordance with NAVER Cloud Trust Services backup procedures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Certificate validity expires at the time of certificate termination specified in the Certificate field. The maximum duration of an SSL/TLS end entity certificate is 398 days.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of CA activation data used to activate CA Private Keys are made during a key ceremony. Activation data is either generated automatically by the appropriate hardware security module or in such a way that meets the same needs. It is then delivered to a holder of a share of the key who is a person in a trusted role. The delivery method maintains the confidentiality and the integrity of the activation data.

6.4.2 Activation Data Protection

CA activation data is protected from disclosure through a combination of cryptographic and physical access control mechanisms.

6.4.3 Other Aspects of Activation Data

No stipulation

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

NAVER Cloud Trust Services CA system information is protected through a combination of server, OS control, physical control, and network control. The network security control is specified in Section 6.7.

Multi-Factor Authentication is implemented for all the accounts used for the lifecycle management of the certificates issued by NAVER Cloud Trust Services’s CA system.

6.5.2 Computer Security Rating

No stipulation

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The application software used in NAVER Cloud Trust Services is developed, tested, and operated in accordance with the company's system development and change policies and procedures. Hardware, including a server, is provided by a supplier selected by the company's procurement and purchasing procedures.

If NAVER Cloud Trust Services uses Linting software developed by third parties, it monitors for updated versions of that software and plan for updates no later than three (3) months from the release of the update.

6.6.2 Security Management Controls

NAVER Cloud Trust Services has established an information security organization, which implements and operates an internal control framework, and constructs and enforces technical, organizational, and procedural details.

6.6.3 Life Cycle Security Controls

No stipulation

6.7 Network Security Controls

NAVER Cloud Trust Services performs network security control to the CA Systems and supporting systems according to the network management policy:

1. Segmenting Certificate Systems into networks or zones based on their functional, logical, and physical relationship;
2. Applying equivalent security controls to all systems co-located in the same network with the Certificate Systems;
3. Maintaining Root CA Systems in a High Security Zone and in an offline state or air-gapped from all other networks;
4. Maintaining and protecting Issuing Systems, Certificate Management Systems, and Security Support Systems in at least a Secure Zone;
5. Implementing and configuring Security Support Systems that protect systems and communications between systems inside secure zones, High Security Zone and communications with non-Certificate Systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks;
6. Configuring network boundary controls (firewalls, switches, routers, and gateways) with rules that support only the services, protocols, ports, and communications that NAVER Cloud Trust Services has identified as necessary to its operations;
7. Configuring Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in NAVER Cloud Trust Services's or Delegated Third Party's operations and allowing only those that are approved by NAVER Cloud Trust Services or Delegated Third Party;

8. Ensuring that NAVER Cloud Trust Services's security policies encompass a change management process, following the principles of documentation, approval and review, and to ensure that all changes to Certificate Systems, Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems follow said change management process;

9. Granting administration access to Certificate Systems only to persons acting in Trusted Roles and require their accountability for Certificate System's security;

10. Implementing Multi-Factor Authentication to each component of the Certificate System that supports Multi-Factor Authentication;

11. Changing authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked; and

12. Applying recommended security patches to Certificate Systems within six (6) months of the security patch's availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

For NAVER Cloud Trust Services, the vulnerability response timeframe SHALL be established based on a documented risk assessment in accordance with CABF Network and Certificate System Security Requirements v2.0.5.

The assessment SHOULD take into account the CVSS score, criticality of assets, and potential impact. Identified vulnerabilities are remediated in a timely manner appropriate to their severity, with urgent cases addressed immediately. Exceptions may be documented and justified through a risk-based process.

6.8 Time-Stamping

The audit logs created by the certificates, CRL, and other certificate lifecycles contain time information. Additional Time-Stamping or encryption is not performed for such information except for the database self-encrypting.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

The certificates issued by NAVER Cloud Trust Services conform to both the RFC 5280 and the latest CA Browser Forum's Baseline Requirements.

In the cases where stipulations of the RFC 5280 and the applicable CA Browser Forum's Baseline Requirements differ, the CA Browser Forum's Baseline Requirements notion will preferentially be adhered to.

7.1.1 Version Number(s)

The subscriber certificates issued by NAVER Cloud Trust Services have X.509 version 3.

7.1.2 Certificate Extensions

If the CA asserts compliance with these Baseline Requirements, all certificates that it issues MUST comply with one of the following certificate profiles, which incorporate, and are derived from RFC 5280. Except as explicitly noted, all normative requirements imposed by RFC 5280 shall apply, in addition to the normative requirements imposed by this document. CAs SHOULD examine RFC 5280, Appendix B for further issues to be aware of.

CA Certificates - **Section 7.1.2.1** – Root CA Certificate Profile - **Subordinate CA Certificates** - **Cross Certificates** - **Section 7.1.2.2** – Cross-Certified Subordinate CA Certificate Profile - **Technically Constrained CA Certificates** - **Section 7.1.2.3** – Technically-Constrained Non-TLS Subordinate CA Certificate Profile - **Section 7.1.2.4** – Technically-Constrained Precertificate Signing CA Certificate Profile - **Section 7.1.2.5** – Technically-Constrained TLS Subordinate CA Certificate Profile - **Section 7.1.2.6** – TLS Subordinate CA Certificate Profile - **Section 7.1.2.7** – Subscriber (End-Entity) Certificate Profile - **Section 7.1.2.8** – OCSP Responder Certificate Profile - **Section 7.1.2.9** – Precertificate Profile

7.1.2.1 Root CA Certificate

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	Encoded value MUST be byte-for-byte identical to the encoded subject
validity	See Section 7.1.2.1.1
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present

Field	Description
extensions	See Section 7.1.2.1.2
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.1.1 *Root CA Validity*

Field	Minimum	Maximum
notBefore	One day prior to the time of signing	The time of signing
notAfter	2922 days (approx. 8 years)	9132 days (approx. 25 years)

Note: This restriction applies even in the event of generating a new Root CA Certificate for an existing subject and subjectPublicKeyInfo (e.g. reissuance). The new CA Certificate MUST conform to these rules.

7.1.2.1.2 *Root CA Extensions*

Extension	Presence	Critical	Description
authorityKeyIdentifier	RECOMMENDED	N	See Section 7.1.2.1.3
basicConstraints	MUST	Y	See Section 7.1.2.1.4
keyUsage	MUST	Y	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	N	See Section 7.1.2.11.4
extKeyUsage	MUST NOT	N	-
certificatePolicies	NOT RECOMMENDED	N	See Section 7.1.2.10.5
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.1.3 *Root CA Authority Key Identifier*

Field	Description
keyIdentifier	MUST be present. MUST be identical to the subjectKeyIdentifier field.
authorityCertIssuer	MUST NOT be present
authorityCertSerialNumber	MUST NOT be present

7.1.2.1.4 *Root CA Basic Constraints*

Field	Description
cA	MUST be set TRUE
pathLenConstraint	NOT RECOMMENDED

7.1.2.2 Cross-Certified Subordinate CA Certificate Profile

This Certificate Profile *MAY* be used when issuing a CA Certificate using the same Subject Name and Subject Public Key Information as one or more existing CA Certificate(s), whether a Root CA Certificate or Subordinate CA Certificate.

Before issuing a Cross-Certified Subordinate CA, the Issuing CA *MUST* confirm that the existing CA Certificate(s) are subject to these Baseline Requirements and were issued in compliance with the then-current version of the Baseline Requirements at the time of issuance.

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	See Section 7.1.2.2.1
subject	See Section 7.1.2.2.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.2.3
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.2.1 *Cross-Certified Subordinate CA Validity*

Field	Minimum	Maximum
notBefore	The earlier of one day prior to the time of signing or the earliest notBefore date of the existing CA Certificate(s)	The time of signing
notAfter	The time of signing	Unspecified

7.1.2.2.2 *Cross-Certified Subordinate CA Naming*

The subject **MUST** comply with the requirements of Section 7.1.4, or, if the existing CA Certificate was issued in compliance with the then-current version of the Baseline Requirements, the encoded subject name **MUST** be byte-for-byte identical to the encoded subject name of the existing CA Certificate.

Note: The above exception allows the CAs to issue Cross-Certified Subordinate CA Certificates, provided that the existing CA Certificate complied with the Baseline Requirements in force at the time of issuance. This allows the requirements of Section 7.1.4 to be improved over time while still permitting Cross-Certification. If the existing CA Certificate did not comply, issuing a Cross-Certificate is not permitted.

7.1.2.2.3 *Cross-Certified Subordinate CA Extensions*

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1
basicConstraints	MUST	Y	See Section 7.1.2.10.4
certificatePolicies	MUST	N	See Section 7.1.2.10.5
crlDistributionPoints	MUST	N	See Section 7.1.2.11.2
keyUsage	MUST	Y	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	N	See Section 7.1.2.11.4
authorityInformationAccess	SHOULD	N	See Section 7.1.2.10.3
nameConstraints	MAY	*[1]	See Section 7.1.2.10.8
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

In addition to the above, extKeyUsage extension requirements vary based on the relationship between the Issuer and Subject organizations represented in the Cross-Certificate.

The extKeyUsage extension **MAY** be “unrestricted” as described in the following table if:

- The organizationName represented in the Issuer and Subject names of the corresponding certificate are either:

    - The same, or
    - The organizationName represented in the Subject name is an affiliate of the organizationName represented in the Issuer name.
- The corresponding CA represented by the Subject of the Cross-Certificate is operated by the same organization as the Issuing CA or an Affiliate of the Issuing CA organization.

Table: Cross-Certified Subordinate CA with Unrestricted EKU

Extension	Presence	Critical	Description
extKeyUsage	SHOULD[2]	N	See Section 7.1.2.2.4

In all other cases, the extKeyUsage extension **MUST** be "restricted" as described in the following table:

Table: Cross-Certified Subordinate CA with Restricted EKU

Extension	Presence	Critical	Description
extKeyUsage	MUST[3]	N	See Section 7.1.2.2.5

7.1.2.2.4 Cross-Certified Subordinate CA Extended Key Usage - Unrestricted

Table: Unrestricted Extended Key Usage Purposes (Affiliated Cross-Certified CA)

Key Purpose	Description
anyExtendedKeyUsage	The special extended key usage to indicate there are no restrictions applied. If present, this MUST be the only key usage present.
Any other value	CAs MUST NOT include any other key usage with the anyExtendedKeyUsage key usage present.

Alternatively, if the Issuing CA does not use this form, then the Extended Key Usage extension, if present, MUST be encoded as specified in Section 7.1.2.2.5.

7.1.2.2.5 Cross-Certified Subordinate CA Extended Key Usage

Table: Restricted TLS Cross-Certified Subordinate CA Extended Key Usage Purposes

(i.e., for restricted Cross-Certified Subordinate CAs issuing TLS certificates directly or transitively)

Key Purpose	Description
id-kp-serverAuth	MUST be present.
id-kp-clientAuth	MAY be present.
id-kp-emailProtection	MUST NOT be present.

Key Purpose	Description
id-kp-codeSigning	MUST NOT be present.
id-kp-timeStamping	MUST NOT be present.
anyExtendedKeyUsage	MUST NOT be present.
Any other value	NOT RECOMMENDED.

Table: Restricted Non-TLS Cross-Certified Subordinate CA Extended Key Usage Purposes

(i.e., for restricted Cross-Certified Subordinate CAs not issuing TLS certificates directly or transitively)

Key Purpose	Description
id-kp-serverAuth	MUST NOT be present.
anyExtendedKeyUsage	MUST NOT be present.
Any other value	MAY be present.

Each included Extended Key Usage key usage purpose:

1. **MUST** apply in the context of the public Internet (e.g. **MUST NOT** be for a service that is only valid in a privately managed network), unless:
    a. the key usage purpose falls within an OID arc for which the Applicant demonstrates ownership; or,
    b. the Applicant can otherwise demonstrate the right to assert the key usage purpose in a public context.
2. **MUST NOT** include semantics that will mislead the Relying Party about the certificate information verified by the CA, such as including a key usage purpose asserting storage on a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance.
3. **MUST** be verified by the Issuing CA (i.e. the Issuing CA **MUST** verify the Cross-Certified Subordinate CA is authorized to assert the key usage purpose).

CAs MUST NOT include additional key usage purposes unless the CA is aware of a reason for including the key usage purpose in the Certificate.

7.1.2.3 Technically Constrained Non-TLS Subordinate CA Certificate Profile

This Certificate Profile MAY be used when issuing a CA Certificate that will be considered Technically Constrained, and which will not be used to issue TLS certificates directly or transitively.

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	See Section 7.1.2.10.1
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.3.1
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.3.2 Technically Constrained Non-TLS Subordinate CA Certificate Policies

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1
basicConstraints	MUST	Y	See Section 7.1.2.10.4
crlDistributionPoints	MUST	N	See Section 7.1.2.11.2
keyUsage	MUST	Y	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	N	See Section 7.1.2.11.4
extKeyUsage	MUST[4]	N	See Section 7.1.2.3.3
authorityInformationAccess	SHOULD	N	See Section 7.1.2.10.3
certificatePolicies	MAY	N	See Section 7.1.2.3.2
nameConstraints	MAY	*[5]	See Section 7.1.2.10.8
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

If present, the Certificate Policies extension MUST be formatted as one of the two tables below:

No Policy Restrictions (Affiliated CA)

Field	Presence	Contents
policyIdentifier	MUST	When the Issuing CA wishes to express that there are no policy restrictions, the Subordinate CA MUST be an Affiliate of the Issuing CA. The Certificate Policies extension MUST contain only a single PolicyInformation value, which MUST contain the anyPolicy Policy Identifier.
anyPolicy	MUST	
policyQualifiers	NOT RECOMMENDED	If present, MUST contain only permitted policyQualifiers from the table below.

Table: Policy Restricted

Field	Presence	Contents
policyIdentifier	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	MUST NOT	
anyPolicy	MUST NOT	The anyPolicy Policy Identifier MUST NOT be present.
Any other identifier	MAY	If present, MUST be

Field	Presence	Contents
		documented by the CA in its Certificate Policy and/or Certification Practice Statement.
policyQualifiers	NOT RECOMMENDED	If present, MUST contain only permitted policyQualifiers from the table below.

Table: Permitted policyQualifiers

Qualifier ID	Presence	Field Type	Contents
id-qt-cps (OID: 1.3.6.1.5.5.7.2.1)	MAY	IA5String	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

#7.1.2.3.3 Technically Constrained Non-TLS Subordinate CA Extended Key Usage

The Issuing CA **MUST** verify that the Subordinate CA Certificate is authorized to issue certificates for each included extended key usage purpose. Multiple, independent key purposes (e.g. id-kp-timeStamping and id-kp-codeSigning) are **NOT RECOMMENDED**.

Key Purpose	OID	Presence
id-kp-serverAuth	1.3.6.1.5.5.7.3.1	MUST NOT
id-kp-OCSPSigning	1.3.6.1.5.5.7.3.9	MUST NOT
anyExtendedKeyUsage	2.5.29.37.0	MUST NOT
Precertificate Signing Certificate	1.3.6.1.4.1.11129.2.4.4	MUST NOT
Any other value	-	MAY

7.1.2.4 Technically Constrained Precertificate Signing CA Certificate Profile

This Certificate Profile **MUST** be used when issuing a CA Certificate that will be used as a Precertificate Signing CA, as described in RFC 6962, Section 3.1. If a CA Certificate conforms to this profile, it is considered Technically Constrained.

A Precertificate Signing CA **MUST** only be used to sign Precertificates, as defined in Section 7.1.2.9. When a Precertificate Signing CA issues a Precertificate, it shall be interpreted as if the Issuing CA of the Precertificate Signing CA has issued a Certificate with a matching tbsCertificate of the Precertificate, after applying the modifications specified in RFC 6962, Section 3.2.

As noted in RFC 6962, Section 3.2, the signature field of a Precertificate is not altered as part of these modifications. As such, the Precertificate Signing CA **MUST** use the same signature algorithm as the Issuing CA when issuing Precertificates, and, correspondingly, **MUST** use a public key of the same public key algorithm as the Issuing CA, although **MAY** use a different CA Key Pair.

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	See Section 7.1.2.10.1

Field	Description
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	The algorithm identifier MUST be byte-for-byte identical to the algorithm identifier of the subjectPublicKeyInfo field of the Issuing CA. See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.4.1
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.4.2 Technically Constrained Precertificate Signing CA Extended Key Usage

Key Purpose	OID	Presence
Precertificate Signing Certificate	1.3.6.1.4.1.11129.2.4.4	MUST
Any other value	-	MUST NOT

7.1.2.5 Technically Constrained TLS Subordinate CA Certificate Profile

This Certificate Profile **MAY** be used when issuing a CA Certificate that will be considered Technically Constrained, and which will be used to issue TLS certificates directly or transitively.

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	See Section 7.1.2.10.1

Field	Description
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.5.1
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.5.1 Technically Constrained TLS Subordinate CA Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1
basicConstraints	MUST	Y	See Section 7.1.2.10.4
certificatePolicies	MUST	N	See Section 7.1.2.10.5
crlDistributionPoints	MUST	N	See Section 7.1.2.11.2
keyUsage	MUST	Y	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	N	See Section 7.1.2.11.4
extKeyUsage	MUST[8]	N	See Section 7.1.2.10.6
nameConstraints	MUST	*[9]	See Section 7.1.2.5.2
authorityInformationAccess	SHOULD	N	See Section 7.1.2.10.3
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.5.2 Technically Constrained TLS Subordinate CA Name Constraints

For a TLS Subordinate CA to be Technically Constrained, Name Constraints extension **MUST** be encoded as follows.
As an explicit exception from RFC 5280, this extension **SHOULD** be marked critical, but **MAY** be marked non-critical if compatibility with certain legacy applications that do not support Name Constraints is necessary.

Table: nameConstraints requirements

Field	Description
permittedSubtrees	The permittedSubtrees **MUST** contain at least one GeneralSubtree

Field	Description
	for both of the dNSName and iPAddress GeneralName name types, **UNLESS** the specified GeneralName name type appears within the excludedSubtrees to exclude all names of that name type. Additionally, the permittedSubtrees **MUST** contain at least one GeneralSubtree of the directoryName GeneralName name type.
GeneralSubtree	The requirements for a GeneralSubtree that appears within a permittedSubtrees.
base	See following table.
minimum	**MUST NOT** be present.
maximum	**MUST NOT** be present.
excludedSubtrees	The excludedSubtrees **MUST** contain at least one GeneralSubtree for each of the dNSName and iPAddress GeneralName name types, unless there is an instance present of that name type in the permittedSubtrees. The directoryName name type is **NOT RECOMMENDED**.
GeneralSubtree	The requirements for a GeneralSubtree that appears within a permittedSubtrees.
base	See following table.
minimum	**MUST NOT** be present.
maximum	**MUST NOT** be present.

The following table contains the requirements for the GeneralName that appears within the base of
a GeneralSubtree in either the permittedSubtrees or excludedSubtrees.

Table: GeneralName requirements for the base field

Name Type	Presence	Permitted Subtrees	Excluded Subtrees	Entire Namespace Exclusion
dNSName	MUST	The CA **MUST** confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf. See Section 3.2.2.4.	If at least one dNSName instance is present in the permittedSubtrees, the CA **MAY** indicate one or more subordinate domains to be excluded. If no dNSName instance is present in the permittedSubtrees, then the CA **MUST** include a zero-length dNSName to indicate no domain names are permitted.	
iPAddress	MUST	The CA **MUST** confirm that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf. See Section 3.2.2.5.	If at least one iPAddress instance is present in the permittedSubtrees, the CA **MAY** indicate one or more subdivisions of those ranges to be excluded. If no IPv4 iPAddress is present in the permittedSubtrees, the CA **MUST** include an iPAddress of 8 zero octets, indicating the IPv4 range of 0.0.0.0/0 being excluded. If no IPv6 iPAddress is	

Name Type	Presence	Permitted Subtrees	Excluded Subtrees	Entire Namespace Exclusion
			present in the permittedSubtrees, the CA **MUST** include an iPAddress of 32 zero octets, indicating the IPv6 range of ::0/0 being excluded.	
directoryName	MUST	The CA **MUST** confirm the Applicant's and/or Subsidiary's name attributes such that all certificates issued will comply with the relevant Certificate Profile (see Section 7.1.2), including Name Forms (See Section 7.1.4).	It is **NOT RECOMMENDED** to include values within excludedSubtrees.	The CA **MUST** include a value within permittedSubtrees, and as such, this does not apply. See the Excluded Subtrees requirements for more.
otherName	NOT RECOMMENDED	See below	See below	See below
Any other value	MUST NOT	-	-	-

Any otherName, if present:

1. **MUST** apply in the context of the public Internet, unless:
    a. The type-id falls within an OID arc for which the Applicant demonstrates ownership, or

    b. The Applicant can otherwise demonstrate the right to assert the data in a public context.

2. **MUST NOT** include semantics that will mislead the Relying Party about certificate information verified by the CA.
3. **MUST** be DER encoded according to the relevant ASN.1 module defining the otherName type-id and value.

CAs **SHALL NOT** include additional names unless the CA is aware of a reason for including the data in the Certificate.

7.1.2.6 TLS Subordinate CA Certificate Profile

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	See Section 7.1.2.10.1
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.6.1
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.6.1 TLS Subordinate CA Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1
basicConstraints	MUST	Y	See Section 7.1.2.10.4
certificatePolicies	MUST	N	See Section 7.1.2.10.5
crlDistributionPoints	MUST	N	See Section 7.1.2.11.2

Extension	Presence	Critical	Description
keyUsage	MUST	Y	See Section 7.1.2.10.7
subjectKeyIdentifier	MUST	N	See Section 7.1.2.11.4
extKeyUsage	MUST[10]	N	See Section 7.1.2.10.6
authorityInformationAccess	SHOULD	N	See Section 7.1.2.10.3
nameConstraints	MAY	*[11]	See Section 7.1.2.10.8
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.7 Subscriber (Server) Certificate Profile

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	
notBefore	A value within 48 hours of the certificate signing operation.
notAfter	See Section 6.3.2
subject	See Section 7.1.2.7.1
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.7.6
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.7.1 Subscriber Certificate Types

There are four types of Subscriber Certificates that may be issued, which vary based on the amount of Subject Information that is included. Each of these certificate types shares a common profile, with three exceptions: the subject name fields that may occur, how those fields are validated, and the contents of the certificatePolicies extension.

Type	Description
Domain Validated (DV)	See Section 7.1.2.7.2
Individual Validated (IV)	See Section 7.1.2.7.3
Organization Validated (OV)	See Section 7.1.2.7.4
Extended Validation (EV)	See Section 7.1.2.7.5

Note: Although each Subscriber Certificate type varies in Subject Information, all Certificates provide the same level of assurance of the device identity (domain name and/or IP address).

7.1.2.7.2 Domain Validated

For a Subscriber Certificate to be **Domain Validated**, it **MUST** meet the following profile:

Field	Requirements
subject	See following table.
certificatePolicies	**MUST** be present. **MUST** assert the Reserved Certificate Policy Identifier of 2.23.140.1.2.1 as a policyIdentifier. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6

All subject names **MUST** be encoded as specified in Section 7.1.4.

The following table details the acceptable AttributeTypes that may appear within the type field of an AttributeTypeAndValue, as well as the contents permitted within the value field.

Table: Domain Validated Subject Attributes

Attribute Name	Presence	Value	Verification
countryName	MAY	The two-letter ISO 3166-1 country code for the country associated	Section 3.2.2.3

Attribute Name	Presence	Value	Verification
		with the Subject.	
commonName	NOT RECOMMENDED	If present, **MUST** contain a value derived from the subjectAltName extension according to Section 7.1.4.3.	
Any other attribute	MUST NOT	-	-

7.1.2.7.3 Individual Validated (IV)

For a Subscriber Certificate to be **Individual Validated**, it **MUST** meet the following profile:

Field	Requirements
subject	See following table.
certificatePolicies	**MUST** be present. **MUST** assert the Reserved Certificate Policy Identifier of 2.23.140.1.2.3 as a policyIdentifier. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6

All subject names **MUST** be encoded as specified in Section 7.1.4.

The following table details the acceptable AttributeTypes that may appear within the type field of an AttributeTypeAndValue, as well as the contents permitted within the value field.

Table: Individual Validated Subject Attributes

Attribute Name	Presence	Value	Verification
countryName	MUST	The two-letter ISO 3166-1 country code for the country associated with the Subject. If a country is not represented by an official ISO 3166-1 country code, the CA **MUST** specify the ISO 3166-1	Section 3.2.3

Attribute Name	Presence	Value	Verification
		user-assigned code XX, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.	
stateOrProvinceName	MUST / MAY	**MUST** be present if localityName is absent, **MAY** be present otherwise. If present, **MUST** contain the Subject's state or province information.	Section 3.2.3
localityName	MUST / MAY	**MUST** be present if stateOrProvinceName is absent, **MAY** be present otherwise. If present, **MUST** contain the Subject's locality information.	Section 3.2.3
postalCode	NOT RECOMMENDED	If present, **MUST** contain the Subject's zip or postal information.	Section 3.2.3
streetAddress	NOT RECOMMENDED	If present, **MUST** contain the Subject's street address information. Multiple instances **MAY** be present.	Section 3.2.3
organizationName	NOT RECOMMENDED	If present, MUST contain the Subject's name and/or DBA/tradename. The CA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents	Section 3.2.3

Attribute Name	Presence	Value	Verification
		the difference and any abbreviations used are locally accepted abbreviations. If both are included, the DBA/tradename SHALL appear first, followed by the Subject's name in parentheses.	
surname	MUST	The Subject's surname.	Section 3.2.3
givenName	MUST	The Subject's given name.	Section 3.2.3
organizationalUnitName	MUST NOT	-	-
commonName	NOT RECOMMENDED	If present, **MUST** contain a value derived from the subjectAltName extension according to Section 7.1.4.3.	
Any other attribute	NOT RECOMMENDED	-	See Section 7.1.4.4

Additionally, subject Attributes **MUST NOT** contain only metadata such as . (dot), - (hyphen), and ' ' (space) characters, or any other indication that the value is absent, incomplete, or not applicable.

7.1.2.7.4 Organization Validated

For a Subscriber Certificate to be **Organization Validated**, it **MUST** meet the following profile:

Field	Requirements
subject	See following table.
certificatePolicies	**MUST** be present. **MUST** assert the Reserved Certificate Policy Identifier of 2.23.140.1.2.2 as a policyIdentifier. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6

All subject names **MUST** be encoded as specified in Section 7.1.4.

The following table details the acceptable AttributeTypes that may appear within the type field of an AttributeTypeAndValue, as well as the contents permitted within the value field.

Table: Organization Validated Subject Attributes

Attribute Name	Presence	Value	Verification
domainComponent	MAY	If present, this field **MUST** contain a Domain Label from a Domain Name. The domainComponent fields for the Domain Name **MUST** be in a single ordered sequence containing all Domain Labels from the Domain Name. The Domain Labels **MUST** be encoded in the reverse order to the on-wire representation of domain names in the DNS protocol, so that the Domain Label closest to the root is encoded first. Multiple instances **MAY** be present.	Section 3.2
countryName	MUST	The two-letter ISO 3166-1 country code for the country associated with the Subject. If a Country is not represented by an official ISO 3166-1 country code, the CA **MUST** specify the ISO 3166-1 user-assigned code of XX, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.	Section 3.2.2.1
stateOrProvinceName	MUST / MAY	**MUST** be present if localityName is absent, **MAY** be present	Section 3.2.2.1

Attribute Name	Presence	Value	Verification
		otherwise. If present, **MUST** contain the Subject's state or province information.	
localityName	MUST / MAY	**MUST** be present if stateOrProvinceName is absent, **MAY** be present otherwise. If present, **MUST** contain the Subject's locality information.	Section 3.2.2.1
postalCode	NOT RECOMMENDED	If present, **MUST** contain the Subject's zip or postal information.	Section 3.2.2.1
streetAddress	NOT RECOMMENDED	If present, **MUST** contain the Subject's street address information. Multiple instances **MAY** be present.	Section 3.2.2.1
organizationName	MUST	The Subject's name and/or DBA/tradename. The CA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name". If both are included, the DBA/tradename SHALL appear first, followed by	Section 3.2.2.2

Attribute Name	Presence	Value	Verification
		the Subject's name in parentheses."	
surname	MUST NOT	-	-
givenName	MUST NOT	-	-
organizationalUnitName	MUST NOT	-	-
commonName	NOT RECOMMENDED	If present, **MUST** contain a value derived from the subjectAltName extension according to Section 7.1.4.3.	
Any other attribute	NOT RECOMMENDED	-	See Section 7.1.4.4

Additionally, subject Attributes **MUST NOT** contain only metadata such as . (dot), - (hyphen), and ' ' (space) characters, or any other indication that the value is absent, incomplete, or not applicable.

7.1.2.7.5 Extended Validation

For a Subscriber Certificate to be **Extended Validation**, it **MUST** comply with the Certificate Profile specified in the then-current version of the **Guidelines for the Issuance and Management of Extended Validation Certificates**.
In addition, it **MUST** meet the following profile:

Field	Requirements
subject	See Guidelines for the Issuance and Management of Extended Validation Certificates, Section 7.1.4.2.
certificatePolicies	**MUST** be present. **MUST** assert the Reserved Certificate Policy Identifier of 2.23.140.1.1 as a policyIdentifier. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6 and the Guidelines for the Issuance and Management of Extended Validation Certificates.

Additionally, subject Attributes **MUST NOT** contain only metadata such as . (dot), - (hyphen), and ' ' (space) characters, or any other indication that the value is absent, incomplete, or not applicable.

7.1.2.7.6 Subscriber Certificate Extensions

Extension	Presence	Critical	Description
authorityInformationAccess	MUST	N	See Section 7.1.2.7.7
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1
certificatePolicies	MUST	N	See Section 7.1.2.7.9
extKeyUsage	MUST	N	See Section 7.1.2.7.10
subjectAltName	MUST	*	See Section 7.1.2.7.12
nameConstraints	MUST NOT	-	-
keyUsage	SHOULD	Y	See Section 7.1.2.7.11
basicConstraints	MAY	Y	See Section 7.1.2.7.8
crlDistributionPoints	*	N	See Section 7.1.2.11.2
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
subjectKeyIdentifier	NOT RECOMMENDED	N	See Section 7.1.2.11.4
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

Notes:

- Whether or not the subjectAltName extension should be marked **Critical** depends on the contents of the
  Certificate's subject field, as detailed in Section 7.1.2.7.12.
- Whether or not the CRL Distribution Points extension must be present depends on
  1) whether the Certificate includes an **Authority Information Access** extension with an id-ad-ocsp accessMethod, and

  2) the Certificate's validity period, as detailed in Section 7.1.2.11.2.

7.1.2.7.7 Subscriber Certificate Authority Information Access

The AuthorityInfoAccessSyntax **MUST** contain one or more AccessDescriptions. Each AccessDescription **MUST** only
contain a permitted accessMethod, as detailed below, and each accessLocation **MUST** be encoded as the specified GeneralName type.

The AuthorityInfoAccessSyntax **MAY** contain multiple AccessDescriptions with the same accessMethod, if permitted for that method.
When multiple AccessDescriptions are present with the same accessMethod, each accessLocation **MUST** be unique, and each
AccessDescription **MUST** be ordered in priority for that accessMethod, with the most-preferred accessLocation being the first entry.
No ordering requirements exist for AccessDescriptions containing different accessMethods, provided the previous requirement is satisfied.

Table: Authority Information Access

Access Method	OID	Access Location	Presence	Maximum	Description
id-ad-ocsp	1.3.6.1.5.5.7.48.1	uniformResourceIdentifier	MAY *	-	A HTTP URL of the Issuing CA's OCSP responder.
id-ad-caIssuers	1.3.6.1.5.5.7.48.2	uniformResourceIdentifier	SHOULD *	-	A HTTP URL of the Issuing CA's certificate.
Any other value	-	-	MUST NOT	-	No other accessMethods may be used.

7.1.2.7.8 Subscriber Certificate Basic Constraints

Field	Description
cA	**MUST** be FALSE
pathLenConstraint	**MUST NOT** be present

7.1.2.7.9 Subscriber Certificate Certificate Policies

If present, the Certificate Policies extension **MUST** contain at least one PolicyInformation.
Each PolicyInformation **MUST** match the following profile:

Field	Presence	Contents
policyIdentifier	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	MUST	The Reserved Certificate Policy Identifier (see Section 7.1.6.1)

Field	Presence	Contents
		associated with the given Subscriber Certificate type (see Section 7.1.2.7.1).
anyPolicy	MUST NOT	The anyPolicy Policy Identifier **MUST NOT** be present.
Any other identifier	MAY	If present, **MUST** be defined and documented in the CA's Certificate Policy and/or Certification Practice Statement.
policyQualifiers	NOT RECOMMENDED	If present, **MUST** contain only permitted policyQualifiers from the table below.

This Profile **RECOMMENDS** that the first PolicyInformation value within the Certificate Policies extension contains
the Reserved Certificate Policy Identifier (see Section 7.1.6.1).
Regardless of the order of PolicyInformation values, the Certificate Policies extension **MUST** contain exactly one Reserved Certificate Policy Identifier.

Table: Permitted policyQualifiers

Qualifier ID	Presence	Field Type	Contents
id-qt-cps (OID: 1.3.6.1.5.5.7.2.1)	MAY	IA5String	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certificatio n Practice Statement, Relying Party Agreement, or other

Qualifier ID	Presence	Field Type	Contents
			pointer to online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

7.1.2.7.10 Subscriber Certificate Extended Key Usage

Key Purpose	OID	Presence
id-kp-serverAuth	1.3.6.1.5.5.7.3.1	MUST
id-kp-clientAuth	1.3.6.1.5.5.7.3.2	MAY
id-kp-codeSigning	1.3.6.1.5.5.7.3.3	MUST NOT
id-kp-emailProtection	1.3.6.1.5.5.7.3.4	MUST NOT
id-kp-timeStamping	1.3.6.1.5.5.7.3.8	MUST NOT
id-kp-OCSPSigning	1.3.6.1.5.5.7.3.9	MUST NOT
anyExtendedKeyUsage	2.5.29.37.0	MUST NOT
Precertificate Signing Certificate	1.3.6.1.4.1.11129.2.4.4	MUST NOT
Any other value	-	NOT RECOMMENDED

7.1.2.7.11 Subscriber Certificate Key Usage

CAs **MUST** ensure the Key Usage is appropriate for the Certificate's Public Key.

Table: Key Usage for RSA Public Keys

Key Usage	Permitted	Required
digitalSignature	Y	SHOULD
nonRepudiation	N	–
keyEncipherment	Y	MAY

Key Usage	Permitted	Required
dataEncipherment	Y	NOT RECOMMENDED
keyAgreement	N	–
keyCertSign	N	–
cRLSign	N	–
encipherOnly	N	–
decipherOnly	N	–

Note: At least one Key Usage **MUST** be set for RSA Public Keys.
- The digitalSignature bit is **REQUIRED** for use with modern protocols, such as **TLS 1.3**, and secure ciphersuites.
- The keyEncipherment bit **MAY** be asserted to support older protocols, such as **TLS 1.2**, when using insecure ciphersuites.
- Subscribers **MAY** use key separation to limit risks from legacy protocols.

For most Subscribers, the digitalSignature bit is sufficient, while those using mixed secure/insecure ciphersuites
MAY assert both digitalSignature and keyEncipherment, though this is **NOT RECOMMENDED**.
The dataEncipherment bit is currently permitted but **NOT RECOMMENDED**, as it is a **Pending Prohibition (#384)**.

Table: Key Usage for ECC Public Keys

Key Usage	Permitted	Required
digitalSignature	Y	MUST
nonRepudiation	N	–
keyEncipherment	N	–
dataEncipherment	N	–
keyAgreement	Y	NOT RECOMMENDED
keyCertSign	N	–
cRLSign	N	–
encipherOnly	N	–
decipherOnly	N	–

Note: The keyAgreement bit is currently permitted, but setting it is **NOT RECOMMENDED**, as it is a **Pending Prohibition (#384)**.

7.1.2.7.12 Subscriber Certificate Subject Alternative Name

For **Subscriber Certificates**, the Subject Alternative Name **MUST** be present and **MUST** contain at least
one dNSName or iPAddress GeneralName.

- If the subject field of the certificate is an **empty SEQUENCE**, this extension **MUST** be marked **critical**, as specified in RFC 5280, Section 4.2.1.6.
- Otherwise, this extension **MUST NOT** be marked critical.

Table: GeneralName within a subjectAltName extension

Name Type	Permitted	Validation
otherName	N	-
rfc822Name	N	-
dNSName	Y	The entry **MUST** contain either a Fully-Qualified Domain Name (FQDN) or Wildcard Domain Name that the CA has validated in accordance with Section 3.2.2.4. Wildcard Domain Names **MUST** be validated for consistency with Section 3.2.2.6. The entry **MUST NOT** contain an Internal Name. The FQDN or the FQDN portion of the Wildcard Domain Name **MUST** be composed entirely of P-Labels or Non-Reserved LDH Labels joined together by a U+002E FULL STOP (".") character. The zero-length Domain Label representing the root zone **MUST NOT** be included (e.g., "example.com" **MUST** be encoded

Name Type	Permitted	Validation
		as "example.com" and **MUST NOT** be encoded as "example.com.").
x400Address	N	-
directoryName	N	-
ediPartyName	N	-
uniformResourceIdentifier	N	-
iPAddress	Y	The entry **MUST** contain the IPv4 or IPv6 address that the CA has confirmed the Applicant controls or has been granted the right to use through a method specified in Section 3.2.2.5. The entry **MUST NOT** contain a Reserved IP Address.
registeredID	N	-

7.1.2.8 OCSP Responder Certificate Profile

If the Issuing CA does not directly sign OCSP responses, it **MAY** make use of an **OCSP Authorized Responder**,
as defined by RFC 6960. The Issuing CA of the Responder **MUST** be the same as the Issuing CA for the Certificates
it provides responses for.

Field	Description
tbsCertificate	
version	MUST be v3(2)
serialNumber	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.

Field	Description
signature	See Section 7.1.3.2
issuer	MUST be byte-for-byte identical to the subject field of the Issuing CA. See Section 7.1.4.1
validity	See Section 7.1.2.8.1
subject	See Section 7.1.2.10.2
subjectPublicKeyInfo	See Section 7.1.3.1
issuerUniqueID	MUST NOT be present
subjectUniqueID	MUST NOT be present
extensions	See Section 7.1.2.8.2
signatureAlgorithm	Encoded value MUST be byte-for-byte identical to the tbsCertificate.signature.
signature	

7.1.2.8.1 OCSP Responder Validity

Field	Minimum	Maximum
notBefore	One day prior to the time of signing	The time of signing
notAfter	The time of signing	Unspecified

7.1.2.8.2 OCSP Responder Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	MUST	N	See Section 7.1.2.11.1
extKeyUsage	MUST	-	See Section 7.1.2.8.5
id-pkix-ocsp-nocheck	MUST	N	See Section 7.1.2.8.6
keyUsage	MUST	Y	See Section 7.1.2.8.7
basicConstraints	MAY	Y	See Section 7.1.2.8.4
nameConstraints	MUST NOT	-	-
subjectAltName	MUST NOT	-	-
subjectKeyIdentifier	SHOULD	N	See Section 7.1.2.11.4
authorityInformationAccess	NOT RECOMMENDED	N	See Section 7.1.2.8.3
certificatePolicies	MUST NOT	N	See Section 7.1.2.8.8
crlDistributionPoints	MUST NOT	N	See Section 7.1.2.11.2

Extension	Presence	Critical	Description
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.8.3 OCSP Responder Authority Information Access

For OCSP Responder certificates, this extension is **NOT RECOMMENDED**, as the **Relying Party** should already
possess the necessary information. To validate the given **Responder certificate**, the **Relying Party** must have
access to the Issuing CA's certificate, eliminating the need to provide id-ad-caIssuers.

Additionally, because an OCSP Responder certificate must include the id-pkix-ocsp-nocheck extension,
it is not necessary to provide id-ad-ocsp, as such responses will not be checked by **Relying Parties**.

Table: Authority Information Access for OCSP Responder

Access Method	OID	Access Location	Presence	Maximum	Description
id-ad-ocsp	1.3.6.1.5.5.7.48.1	uniformResourceIdentifier	NOT RECOMMENDED	*	A HTTP URL of the Issuing CA's OCSP responder.
Any other value	-	-	MUST NOT	-	No other accessMethods may be used.

7.1.2.8.4 OCSP Responder Basic Constraints

OCSP Responder certificates **MUST NOT** be CA certificates. The issuing CA **MAY** indicate this one of two ways: 1. By **omission** of the basicConstraints extension, or
2. By **inclusion** of a basicConstraints extension that sets the cA boolean to FALSE.

Field	Description
cA	**MUST** be FALSE
pathLenConstraint	**MUST NOT** be present

Note:
Due to **DER encoding rules**, a basicConstraints extension that sets cA boolean to FALSE **MUST** have an

extnValue OCTET STRING exactly equal to the hex-encoded bytes 3000, the encoded representation of an
empty ASN.1 **SEQUENCE** value.

7.1.2.8.5 OCSP Responder Extended Key Usage

Key Purpose	OID	Presence
id-kp-OCSPSigning	1.3.6.1.5.5.7.3.9	MUST
Any other value	-	MUST NOT

7.1.2.8.6 OCSP Responder id-pkix-ocsp-nocheck

The CA **MUST** include the id-pkix-ocsp-nocheck extension (OID: 1.3.6.1.5.5.7.48.1.5).
This extension **MUST** have an extnValue OCTET STRING that is exactly the hex-encoded bytes 0500,
the encoded representation of the ASN.1 NULL value, as specified in **RFC 6960, Section 4.2.2.2.1**.

7.1.2.8.7 OCSP Responder Key Usage

Key Usage	Permitted	Required
digitalSignature	Y	Y
nonRepudiation	N	–
keyEncipherment	N	–
dataEncipherment	N	–
keyAgreement	N	–
keyCertSign	N	–
cRLSign	N	–
encipherOnly	N	–
decipherOnly	N	–

7.1.2.8.8 OCSP Responder Certificate Policies

If present, the Certificate Policies extension **MUST** contain at least one PolicyInformation.
Each PolicyInformation **MUST** match the following profile:

Field	Presence	Contents
policyIdentifier	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	NOT RECOMMENDED	-
anyPolicy	NOT RECOMMENDED	-

Field	Presence	Contents
Any other identifier	NOT RECOMMENDED	If present, **MUST** be defined and documented in the CA's Certificate Policy and/or Certification Practice Statement.
policyQualifiers	NOT RECOMMENDED	If present, **MUST** contain only permitted policyQualifiers from the table below.

Table: Permitted policyQualifiers

Qualifier ID	Presence	Field Type	Contents
id-qt-cps (OID: 1.3.6.1.5.5.7.2.1)	MAY	IA5String	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

Notes: - See Section **7.1.2.8.2** for applicable effective dates when this extension may be included. - Because the Certificate Policies extension may be used to restrict applicable usages for a certificate,

incorrect policies may result in **OCSP Responder Certificates** that fail to validate, leading to invalid OCSP Responses.
Including the anyPolicy policy can reduce this risk but may introduce client processing complexity and interoperability issues.

7.1.2.9 Precertificate Profile

A **Precertificate** is a signed data structure that can be submitted to a Certificate Transparency log, as defined by **RFC 6962**. A Precertificate appears structurally identical to a Certificate, with the exception of a special critical poison extension in the extensions field, with the OID of 1.3.6.1.4.1.11129.2.4.3. This extension ensures that the Precertificate will not be accepted as a Certificate by clients conforming to **RFC 5280**. The existence of a signed Precertificate can be treated as evidence of a corresponding Certificate also existing, as the signature represents a binding commitment by the CA that it may issue such a Certificate.

A Precertificate is created after a CA has decided to issue a Certificate, but prior to the actual signing of the Certificate. The CA **MAY** construct and sign a Precertificate corresponding to the Certificate, for purposes of submitting to Certificate Transparency Logs. The CA **MAY** use the returned Signed Certificate Timestamps to then alter the Certificate's extensions field, adding a **Signed Certificate Timestamp List**, as defined in **Section 7.1.2.11.3** and as permitted by the relevant profile, prior to signing the Certificate.

Once a Precertificate is signed, relying parties are permitted to treat this as a binding commitment from the CA of the intent to issue a corresponding Certificate, or more commonly, that a corresponding Certificate exists. A Certificate is said to be corresponding to a Precertificate based upon the value of the **tbsCertificate** contents, as transformed by the process defined in **RFC 6962, Section 3.2**.

This profile describes the transformations that are permitted to a Certificate to construct a Precertificate. CAs **MUST NOT** issue a Precertificate unless they are willing to issue a corresponding Certificate, regardless of whether they have done so. Similarly, a CA **MUST NOT** issue a Precertificate unless the corresponding Certificate conforms to these **Baseline Requirements**, regardless of whether the CA signs the corresponding Certificate.

A Precertificate may be issued either directly by the **Issuing CA** or by a **Technically Constrained Precertificate Signing CA**, as defined in **Section 7.1.2.4**. If issued by a Precertificate Signing CA, then in addition to the **precertificate poison** and **signed certificate timestamp list** extensions, the **Precertificate issuer field** and, if present, **authorityKeyIdentifier** extension, may differ from the Certificate, as described below.

Table: When the Precertificate is issued directly by the Issuing CA

Field	Description
tbsCertificate	

Field	Description
version	Encoded value **MUST** be byte-for-byte identical to the version field of the Certificate.
serialNumber	Encoded value **MUST** be byte-for-byte identical to the serialNumber field of the Certificate.
signature	Encoded value **MUST** be byte-for-byte identical to the signature field of the Certificate.
issuer	Encoded value **MUST** be byte-for-byte identical to the issuer field of the Certificate.
validity	Encoded value **MUST** be byte-for-byte identical to the validity field of the Certificate.
subject	Encoded value **MUST** be byte-for-byte identical to the subject field of the Certificate.
subjectPublicKeyInfo	Encoded value **MUST** be byte-for-byte identical to the subjectPublicKeyInfo field of the Certificate.
issuerUniqueID	Encoded value **MUST** be byte-for-byte identical to the issuerUniqueID field of the Certificate, or omitted if absent.
subjectUniqueID	Encoded value **MUST** be byte-for-byte identical to the subjectUniqueID field of the Certificate, or omitted if absent.
extensions	See Section 7.1.2.9.1
signatureAlgorithm	Encoded value **MUST** be byte-for-byte identical to the tbsCertificate.signature.
signature	

Table: When the Precertificate is issued by a Precertificate Signing CA on behalf of an Issuing CA

Field	Description
tbsCertificate	
version	Encoded value **MUST** be byte-for-byte identical to the version field of the Certificate.
serialNumber	Encoded value **MUST** be byte-for-byte identical to the serialNumber field of the Certificate.
signature	Encoded value **MUST** be byte-for-byte identical to the signature field of the Certificate.
issuer	Encoded value **MUST** be byte-for-byte identical to the subject field of the Precertificate Signing CA Certificate.
validity	Encoded value **MUST** be byte-for-byte identical to the validity field of the Certificate.
subject	Encoded value **MUST** be byte-for-byte identical to the subject field of the Certificate.
subjectPublicKeyInfo	Encoded value **MUST** be byte-for-byte identical to the subjectPublicKeyInfo field of the Certificate.
issuerUniqueID	Encoded value **MUST** be byte-for-byte identical to the issuerUniqueID field of the Certificate, or omitted if omitted in the Certificate.
subjectUniqueID	Encoded value **MUST** be byte-for-byte identical to the subjectUniqueID field of the Certificate, or omitted if omitted in the Certificate.
extensions	See **Section 7.1.2.9.2**.

Field	Description
signatureAlgorithm	Encoded value **MUST** be byte-for-byte identical to the tbsCertificate.signature.
signature	Encoded value **MUST** be byte-for-byte identical to the signature field of the Certificate.

Note:
This profile requires that the **serialNumber** field of the Precertificate be identical to that of the corresponding Certificate.
RFC 5280, Section 4.1.2.2 requires that the **serialNumber** of certificates be unique.
For the purposes of this document, a **Precertificate shall not be considered a "certificate"** subject to that requirement,
and thus **may have the same serialNumber** as the corresponding Certificate.
However, this does not permit two **Precertificates** to share the same **serialNumber**, unless they correspond to the same Certificate,
as this would otherwise indicate there are two corresponding Certificates that share the same serialNumber.

7.1.2.9.1 Precertificate Profile Extensions - Directly Issued

These extensions apply to a **Precertificate** directly issued from a **CA**, and not from a **Precertificate Signing CA Certificate**,
as defined in **Section 7.1.2.4**.

Extension	Presence	Critical	Description
Precertificate Poison (OID: 1.3.6.1.4.1.11129.2.4.3)	MUST	Y	See Section 7.1.2.9.3
Signed Certificate Timestamp List	MUST NOT	-	-
Any other extension	*	*	The order, criticality, and encoded values of all other extensions **MUST** be byte-for-byte identical to the extensions field of the **Certificate**.

Note:
This requirement ensures that if the **Precertificate Poison** extension is removed from the **Precertificate**,

and the **Signed Certificate Timestamp List** is removed from the **Certificate**,
the contents of the extensions field **MUST** be byte-for-byte identical.

7.1.2.9.2 Precertificate Profile Extensions - Precertificate CA Issued

These extensions apply when a **Precertificate** is issued from a **Precertificate Signing CA Certificate**,
as defined in **Section 7.1.2.4**.

For such **Precertificates**, the authorityKeyIdentifier, if present in the **Certificate**, is modified in the **Precertificate**,
as described in **RFC 6962, Section 3.2**.

Extension	Presence	Critical	Description
Precertificate Poison (OID: 1.3.6.1.4.1.11129.2.4.3)	MUST	Y	See Section 7.1.2.9.3
authorityKeyIdentifier	*	*	See Section 7.1.2.9.4
Signed Certificate Timestamp List	MUST NOT	-	-
Any other extension	*	*	The order, criticality, and encoded values of all other extensions **MUST** be byte-for-byte identical to the extensions field of the **Certificate**.

7.1.2.9.3 Precertificate Poison

The **Precertificate MUST** contain the **Precertificate Poison** extension (OID: 1.3.6.1.4.1.11129.2.4.3).
This extension **MUST** have an extnValue **OCTET STRING** that is exactly the **hex-encoded bytes 0500**,
the encoded representation of the **ASN.1 NULL** value, as specified in **RFC 6962, Section 3.1**.

7.1.2.9.4 Precertificate Authority Key Identifier

For **Precertificates** issued by a **Precertificate Signing CA**, the contents of the authorityKeyIdentifier extension **MUST**
be one of the following: 1. **SHOULD** be as defined in the profile below, or; 2. **MAY** be byte-for-byte identical with the contents of the authorityKeyIdentifier extension of the corresponding **Certificate**.

Field	Description
keyIdentifier	**MUST** be present. **MUST** be identical to the subjectKeyIdentifier field of the **Precertificate Signing CA Certificate**.
authorityCertIssuer	**MUST NOT** be present.
authorityCertSerialNumber	**MUST NOT** be present.

Note:
RFC 6962 describes how the authorityKeyIdentifier present on a **Precertificate** is transformed to contain the value
of the **Precertificate Signing CA's authorityKeyIdentifier** extension (i.e., reflecting the actual issuer certificate's keyIdentifier),
thus matching the **corresponding Certificate** when verified by clients.

These **Baseline Requirements RECOMMEND** using the **Precertificate Signing CA's keyIdentifier** in **Precertificates** issued by it
to ensure consistency between the subjectKeyIdentifier and authorityKeyIdentifier of all certificates in the chain.

Although **RFC 5280** does not strictly require such consistency, some client implementations enforce it for **Certificates**,
and this helps avoid potential issues with **Certificate Transparency Logs** incorrectly implementing such checks.

7.1.2.10 Common CA Fields

This section defines fields that are common among multiple **CA Certificate** profiles.
However, these fields **may not be common** to all **CA Certificate** profiles.

Before issuing a certificate, the **CA MUST** ensure that the certificate contents, including each field,
fully comply with at least one **Certificate Profile** documented in **Section 7.1.2**.

7.1.2.10.1 CA Certificate Validity

Field	Minimum	Maximum
notBefore	One day prior to the time of signing	The time of signing
notAfter	The time of signing	Unspecified

7.1.2.10.2 CA Certificate Naming

All subject names **MUST** be encoded as specified in **Section 7.1.4**.

Table: Acceptable Subject Attributes for CA Certificates

Attribute Name	Presence	Value	Verification
countryName	MUST	The two-letter **ISO 3166-1** country code for the country in which the CA's place of business is located.	Section 3.2.2.3
stateOrProvinceName	MAY	If present, the CA's **state or province** information.	Section 3.2.2.1
localityName	MAY	If present, the CA's **locality**.	Section 3.2.2.1
postalCode	MAY	If present, the CA's **zip or postal code**.	Section 3.2.2.1
streetAddress	MAY	If present, the CA's **street address**. Multiple instances **MAY** be present.	Section 3.2.2.1
organizationName	MUST	The CA's **name or DBA**. The CA **MAY** include minor variations	Section 3.2.2.2

Attribute Name	Presence	Value	Verification
		(e.g., abbreviations), provided they are documented and commonly accepted (e.g., "Company Name Inc." instead of "Company Name Incorporated").	
organizationalUnitName	NOT RECOMMENDED	This attribute **MUST NOT** be included in **Root CA Certificates**, **TLS Subordinate CA Certificates**, or **Technically-Constrained TLS Subordinate CA Certificates**. It **SHOULD NOT** be included in other **CA Certificates**.	-

Attribute Name	Presence	Value	Verification
commonName	MUST	**SHOULD** be a unique identifier for the certificate within the issuing CA's records.	-
Any other attribute	NOT RECOMMENDED	-	See Section 7.1.4.4

7.1.2.10.3 CA Certificate Authority Information Access

If present, the AuthorityInfoAccessSyntax **MUST** contain one or more AccessDescriptions. Each AccessDescription **MUST** only contain a permitted accessMethod, as detailed below, and each accessLocation **MUST** be encoded as the specified GeneralName type.

7.1.2.10.3 CA Certificate Authority Information Access

The AuthorityInfoAccessSyntax **MAY** contain multiple AccessDescriptions with the same accessMethod,
if permitted for that accessMethod. When multiple AccessDescriptions are present with the same accessMethod:
- Each accessLocation **MUST** be unique. - Each AccessDescription **MUST** be ordered in priority for that accessMethod, with the most-preferred accessLocation being the first. - No ordering requirements are imposed for AccessDescriptions containing different accessMethods, provided the above requirements are met.

Table: Authority Information Access for CA Certificates

Access Method	OID	Access Location	Presence	Maximum	Description
id-ad-ocsp	1.3.6.1.5.5.7.48.1	uniformResourceIdentifier	MAY	*	A HTTP URL of the Issuing CA's OCSP responder.
id-ad-caIssuers	1.3.6.1.5.5.7.48.2	uniformResourceIdentifier	MAY	*	A HTTP URL of the Issuing CA's certificate.
Any other value	-	-	MUST NOT	-	No other accessMethod

Access Method	OID	Access Location	Presence	Maximum	Description
					s may be used.

7.1.2.10.4 CA Certificate Basic Constraints

Field	Description
cA	**MUST** be set to TRUE.
pathLenConstraint	**MAY** be present.

7.1.2.10.5 CA Certificate Certificate Policies

If present, the Certificate Policies extension **MUST** contain at least one PolicyInformation. Each PolicyInformation **MUST** match the following profile:

Table: No Policy Restrictions (Affiliated CA)

Field	Presence	Contents
policyIdentifier	MUST	When the Issuing CA wishes to express that there are no policy restrictions, the Subordinate CA **MUST** be an **Affiliate** of the Issuing CA. The Certificate Policies extension **MUST** contain only a **single** PolicyInformation value, which **MUST** contain the anyPolicy Policy Identifier.
anyPolicy	MUST	-
policyQualifiers	NOT RECOMMENDED	If present, **MUST** contain only permitted policyQualifiers from the table below.

Table: Policy Restricted

Field	Presence	Contents
policyIdentifier	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	MUST	The CA **MUST** include at least one **Reserved Certificate Policy Identifier** (see Section 7.1.6.1) associated with the given **Subscriber Certificate type** (see Section 7.1.2.7.1) directly or transitively issued by this Certificate.

Field	Presence	Contents
anyPolicy	MUST NOT	The anyPolicy Policy Identifier **MUST NOT** be present.
Any other identifier	MAY	If present, **MUST** be defined by the CA and documented in its **Certificate Policy and/or Certification Practice Statement**.
policyQualifiers	NOT RECOMMENDED	If present, **MUST** contain only permitted policyQualifiers from the table below.

This Profile **RECOMMENDS** that the first **PolicyInformation** value within the **Certificate Policies** extension contains the **Reserved Certificate Policy Identifier** (see **Section 7.1.6.1**).

Regardless of the order of **PolicyInformation** values, the **Certificate Policies** extension **MUST** contain exactly **one** Reserved Certificate Policy Identifier.

> **Note:**
> policyQualifiers is **NOT RECOMMENDED** to be present in any Certificate issued under this Certificate Profile
> because this information increases the size of the Certificate without providing any value to a typical **Relying Party**,
> and the information may be obtained by other means when necessary.

If the **policyQualifiers** is permitted and present within a **PolicyInformation** field, it **MUST** be formatted as follows:

Table: Permitted policyQualifiers

Qualifier ID	Presence	Field Type	Contents
id-qt-cps (OID: 1.3.6.1.5.5.7.2.1)	MAY	IA5String	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to

Qualifier ID	Presence	Field Type	Contents
			online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

7.1.2.10.6 CA Certificate Extended Key Usage

Key Purpose	OID	Presence
id-kp-serverAuth	1.3.6.1.5.5.7.3.1	MUST
id-kp-clientAuth	1.3.6.1.5.5.7.3.2	MAY
id-kp-codeSigning	1.3.6.1.5.5.7.3.3	MUST NOT
id-kp-emailProtection	1.3.6.1.5.5.7.3.4	MUST NOT
id-kp-timeStamping	1.3.6.1.5.5.7.3.8	MUST NOT
id-kp-OCSPSigning	1.3.6.1.5.5.7.3.9	MUST NOT
anyExtendedKeyUsage	2.5.29.37.0	MUST NOT
Precertificate Signing Certificate	1.3.6.1.4.1.11129.2.4.4	MUST NOT
Any other value	-	NOT RECOMMENDED

7.1.2.10.7 CA Certificate Key Usage

Key Usage	Permitted	Required
digitalSignature	Y	N
nonRepudiation	N	–
keyEncipherment	N	–
dataEncipherment	N	–
keyAgreement	N	–
keyCertSign	Y	Y
cRLSign	Y	Y

Key Usage	Permitted	Required
encipherOnly	N	–
decipherOnly	N	–

7.1.2.10.8 CA Certificate Name Constraints

If present, the **Name Constraints** extension **MUST** be encoded as follows:
- As an explicit exception from **RFC 5280**, this extension **SHOULD** be marked **critical**, but **MAY** be marked **non-critical** if compatibility with legacy applications that do not support **Name Constraints** is necessary.

Table: nameConstraints requirements

Field	Description
permittedSubtrees	The requirements for a GeneralSubtree that appears within a permittedSubtrees.
GeneralSubtree	
base	See following table.
minimum	**MUST NOT** be present.
maximum	**MUST NOT** be present.
excludedSubtrees	The requirements for a GeneralSubtree that appears within an excludedSubtrees.
GeneralSubtree	
base	See following table.
minimum	**MUST NOT** be present.
maximum	**MUST NOT** be present.

The following table contains the requirements for the GeneralName that appears within the base of a GeneralSubtree in either the permittedSubtrees or excludedSubtrees.

Table: GeneralName requirements for the base field

Name Type	Presence	Permitted Subtrees	Excluded Subtrees
dNSName	MAY	The CA **MUST** confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on their behalf. See **Section 3.2.2.4**.	If at least one dNSName instance is present in the permittedSubtrees, the CA **MAY** indicate one or more subordinate domains to be excluded.
iPAddress	MAY	The CA **MUST** confirm that the Applicant has been assigned the iPAddress range or has been authorized by	If at least one iPAddress instance is present in the permittedSubtrees, the CA **MAY** indicate one or more

Name Type	Presence	Permitted Subtrees	Excluded Subtrees
		the assigner to act on the assignee's behalf. See **Section 3.2.2.5**.	subdivisions of those ranges to be excluded.
directoryName	MAY	The CA **MUST** confirm the Applicant's and/or Subsidiary's name attributes such that all certificates issued will comply with the relevant Certificate Profile (see **Section 7.1.2**), including **Name Forms** (See **Section 7.1.4**).	It is **NOT RECOMMENDED** to include values within excludedSubtrees.
rfc822Name	NOT RECOMMENDED	The CA **MAY** constrain to a mailbox, a particular host, or any address within a domain, as specified in **RFC 5280, Section 4.2.1.10**. The CA **MUST** confirm that the Applicant has registered the domain or has been authorized by the domain registrant. See **Section 3.2.2.4**.	If at least one rfc822Name instance is present in the permittedSubtrees, the CA **MAY** indicate one or more mailboxes, hosts, or domains to be excluded.
otherName	NOT RECOMMENDED	See below	See below
Any other value	NOT RECOMMENDED	-	-

Requirements for otherName fields: 1. **MUST** apply in the context of the public Internet, unless: - The type-id falls within an **OID arc** for which the Applicant demonstrates ownership, or - The Applicant can otherwise demonstrate the right to assert the data in a public context. 2. **MUST NOT** include semantics that mislead the **Relying Party** about certificate information verified by the **CA**. 3. **MUST** be **DER encoded** according to the relevant **ASN.1 module** defining the otherName type-id and value.

CAs SHALL NOT include additional names unless there is a **specific reason** to do so.

7.1.2.11 Common Certificate Fields

This section contains fields that are **common among multiple certificate profiles**.
However, these fields **may not be common** to all certificate profiles.

Before issuing a certificate, the **CA MUST** ensure that the certificate contents, including each field,
fully comply with at least **one Certificate Profile** documented in **Section 7.1.2**.

7.1.2.11.1 Authority Key Identifier

Field	Description
keyIdentifier	**MUST** be present. **MUST** be identical to the subjectKeyIdentifier field of the **Issuing CA**.
authorityCertIssuer	**MUST NOT** be present.
authorityCertSerialNumber	**MUST NOT** be present.

7.1.2.11.2 CRL Distribution Points

The CRL Distribution Points extension **MUST** be present in: - **Subordinate CA Certificates**. - **Subscriber Certificates** that: 1. **Do not qualify as** "Short-lived Subscriber Certificates", and 2. **Do not include** an **Authority Information Access** extension with an id-ad-ocsp accessMethod.

The CRL Distribution Points extension **SHOULD NOT** be present in: - **Root CA Certificates**.

The CRL Distribution Points extension is **OPTIONAL** in: - **Short-lived Subscriber Certificates**.

The CRL Distribution Points extension **MUST NOT** be present in: - **OCSP Responder Certificates**.

Table: DistributionPoint profile

Field	Presence	Description
distributionPoint	MUST	The DistributionPointName **MUST** be a fullName formatted as described below.
reasons	MUST NOT	-
cRLIssuer	MUST NOT	-

A fullName **MUST** contain at least one GeneralName; it **MAY** contain more than one.
All GeneralNames **MUST** be of type uniformResourceIdentifier, and the **scheme MUST** be "http".
The **first GeneralName MUST** contain the **HTTP URL** of the Issuing CA's **CRL service** for this certificate.

7.1.2.11.3 Signed Certificate Timestamp List

If present, the **Signed Certificate Timestamp List** extension contents **MUST** be an **OCTET STRING**
containing the encoded **SignedCertificateTimestampList**, as specified in **RFC 6962, Section 3.3**.

Each **SignedCertificateTimestamp** included within the **SignedCertificateTimestampList MUST** be
for a **PreCert LogEntryType** that corresponds to the **current certificate**.

7.1.2.11.4 Subject Key Identifier

If present, the **subjectKeyIdentifier MUST** be set as defined in **RFC 5280, Section 4.2.1.2**.
The **CA MUST** generate a subjectKeyIdentifier that is **unique** within the scope of all **Certificates** it has issued for each unique public key.

For example, **CAs MAY**: - Generate the **subject key identifier** using an algorithm derived from the public key, or - Generate a sufficiently-large **unique number**, such as by using a **CSPRNG**.

7.1.2.11.5 Other Extensions

All extensions and extension values **not directly addressed** by the applicable certificate profile:

1. **MUST apply** in the context of the **public Internet**, unless:
    - The **extension OID** falls within an **OID arc** for which the **Applicant** demonstrates **ownership**, or
    - The **Applicant** can otherwise demonstrate the right to assert the data in a **public context**.
2. **MUST NOT** include semantics that mislead the **Relying Party** about certificate information verified by the **CA**.
3. **MUST** be **DER encoded** according to the relevant **ASN.1 module** defining the **extension** and **extension values**.

CAs SHALL NOT include additional extensions or values unless there is a **specific reason** to do so.

7.1.3 Algorithm Object Identifiers

7.1.3.1 SubjectPublicKeyInfo

The followings apply to the subjectPublicKeyInfo field within a Certificate or Precertificate. No other encodings are permitted.

7.1.3.1.1 RSA

NAVER Cloud Trust Services indicates an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters are present, and are an explicit NULL. NAVER Cloud Trust Services does not use a different algorithm to indicate an RSA key.

When encoded, the AlgorithmIdentifier for RSA keys is byte-for-byte identical with the following hex-encoded bytes: 300d06092a864886f70d0101010500

7.1.3.1.2 ECDSA

NAVER Cloud Trust Services indicates an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters use the namedCurve encoding.

- For P-256 keys, the namedCurve is secp256r1 (OID: 1.2.840.10045.3.1.7).
- For P-384 keys, the namedCurve is secp384r1 (OID: 1.3.132.0.34).

When encoded, the AlgorithmIdentifier for ECDSA keys is byte-for-byte identical

with the following hex-encoded bytes:

- For P-256 keys, 301306072a8648ce3d020106082a8648ce3d030107.
- For P-384 keys, 301006072a8648ce3d020106052b81040022.

7.1.3.2 Signature AlgorithmIdentifier

All objects signed by a NAVER Cloud Trust Services Private Key conform to these requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

In particular, it applies to all of the following objects and fields:

- The signatureAlgorithm field of a Certificate or Precertificate.
- The signature field of a TBSCertificate (for example, as used by either a Certificate or Precertificate).
- The signatureAlgorithm field of a CertificateList
- The signature field of a TBSCertList
- The signatureAlgorithm field of a BasicOCSPResponse.

No other encodings are used for these fields.

7.1.3.2.1 RSA

NAVER Cloud Trust Services uses one of the following signature algorithms and encodings. When encoded, the AlgorithmIdentifier is byte-for-byte identical with the specified hex-encoded bytes.

- RSASSA-PKCS1-v1_5 with SHA-256:

  Encoding:

  300d06092a864886f70d01010b0500

- RSASSA-PKCS1-v1_5 with SHA-384:

  Encoding:

  300d06092a864886f70d01010c0500

- RSASSA-PKCS1-v1_5 with SHA-512:

Encoding:

300d06092a864886f70d01010d0500

- RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes:

Encoding:

304106092a864886f70d01010a3034a00f300d060960864801650304020105

00a11c301a06092a864886f70d010108300d060960864801650304020105

00a203020120

- RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes:

Encoding:

304106092a864886f70d01010a3034a00f300d060960864801650304020205

00a11c301a06092a864886f70d010108300d060960864801650304020205

00a203020130

- RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes:

Encoding:

304106092a864886f70d01010a3034a00f300d060960864801650304020305

00a11c301a06092a864886f70d010108300d060960864801650304020305

00a203020140

7.1.3.2.2 ECDSA

NAVER Cloud Trust Services uses the appropriate signature algorithm and encoding based upon the signing key used.

If the signing key is P-256, the signature use ECDSA with SHA-256. When encoded, the AlgorithmIdentifier is byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040302.

If the signing key is P-384, the signature use ECDSA with SHA-384. When encoded, the AlgorithmIdentifier is byte-for-byte identical with the following hex-encoded bytes: 300a06082a8648ce3d040303.

7.1.4 Name Forms

7.1.4.1 Issuer Information

For every valid Certification Path (as defined by RFC 5280, Section 6):

• For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate is byte-for-byte identical with the encoded form of the Subject Distuished Name field of the Issuing CA Certificate.

• For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate is byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to Section 7.1 of RFC 5280. and including expired and revoked Certificates.

When encoding a Name, NAVER Cloud Trust Services ensures that:

• Each Name contains an RDNSequence.

• Each RelativeDistinguishedName contains exactly one AttributeTypeAndValue.

• Each RelativeDistinguishedName, if present, is encoded within the RDNSequence in the order that it appears in Section 7.1.4.2.

• Each Name will not contain more than one instance of a given AttributeTypeAndValue across all RelativeDistinguishedNames unless explicitly specified in this document.

7.1.4.2 Subject Information – Subscriber Certificates

NAVER Cloud Trust Services issues certificates that only include attributes in the Certificate subject field that are listed in the table below and encodes those attributes in the relative order as they appear in the table and follow the specified encoding requirements for the attribute.

NAVER Cloud Trust Services will not include these attributes unless their content has been validated as specified by, and only if permitted by, the relevant certificate profile specified within Section 7.1.2.

By issuing the Certificate, NAVER Cloud Trust Services represents that it followed the procedure set forth in its Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. NAVER Cloud Trust Services does not include a Domain Name in a Subject attribute except as specified in Section 3.2.2.4.

SSL/TLS Certificate can only contain verified information according to Section 3.2, and does not include unverified information. subject:organizationName, subject:localityName, and subject:countryName attributes must be verified in accordance with Section 3.2.2.1.

Subject attributes must not contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or No Stipulation

Wildcard FQDNs are permitted.

NAVER Cloud Trust Services does not issue certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name.

Entries in the dNSName should be in the "preferred name syntax", as specified in RFC 5280, and thus cannot contain underscore characters ('_').

7.1.4.3. Subscriber Certificate Common Name Attribute

If present, this attribute contains exactly one entry that is one of the values contained in the Certificate's subjectAltName extension. The value of the field is encoded as follows:

• If the value is a Fully-Qualified Domain Name or Wildcard Domain Name, then the value is encoded as a character-for-character copy of the dNSName entry value from the subjectAltName extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name are encoded as LDH Labels, and P-Labels are not be converted to their Unicode representation.

7.1.4.4. Other Subject Attributes

When explicitly stated as permitted by the relevant certificate profile specified within Section 7.1.2, NAVER Cloud Trust Services may include additional attributes within the AttributeTypeAndValue beyond those specified in Section 7.1.4.2.

Before including such an attribute, NAVER Cloud Trust Services:

• Documents the attributes within Section 7.1.4 of their relevant CP/CPS documents, along with the applicable validation practices.

• Ensures that the contents contain information that has been verified by NAVER Cloud Trust Services, independent of the Applicant.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers

The certificates issued under NAVER Cloud Trust Services use this CP/CPS as a certificate policy, and the related policy identifiers are specified below.

- Domain Validation Subscriber Certificate: 1.2.410.200081.2.2.3.1
- Organization Validation Subscriber Certificate: 1.2.410.200081.2.2.3.2

The following Certificate Policy identifiers are reserved for use by NAVER Cloud Trust Services as an optional means of asserting that a Certificate complies with these Requirements.

• {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)

• {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

All CRLs that NAVER Cloud Trust Services issues comply with the following CRL profile, which incorporates, and is derived from RFC 5280. Except as explicitly noted, all normative requirements imposed by RFC 5280 shall apply, in addition to the normative requirements imposed by this document. NAVER Cloud Trust Services examines RFC 5280, Appendix B for further issues to be aware of.

A full and complete CRL is a CRL whose scope includes all Certificates issued by NAVER Cloud Trust Services.

A partitioned CRL (sometimes referred to as a "sharded CRL") is a CRL with a constrained scope, such as all Certificates issued by NAVER Cloud Trust Services during a certain period of time ("temporal sharding"). Aside from the presence of the Issuing Distribution Point extension (OID 2.5.29.28) in partitioned CRLs, both CRL formats are syntactically the same from the perspective of this profile.

Minimally, NAVER Cloud Trust Services issues either a "full and complete" CRL or a set of "partitioned" CRLs which cover the complete set of Certificates issued by NAVER Cloud Trust Services. In other words, if issuing only partitioned CRLs, the combined scope of those CRLs is equivalent to that of a full and complete CRL.

7.2.1 Version Number(s)

Certificate Revocation Lists are of type X.509 v2.

7.2.2 CRL and CRL Entry Extensions

CRL Extensions

Extension	Content
authorityKeyIdentifier	Not marked critical, matches subjectKeyIdentifier of signing certificate.authorityCertIssuer and authorityCertSerialNumber not present.

Extension	Content
CRLNumber	Not marked critical, an INTEGER greater than or equal to zero (0) and less than 2^{159}, and follows a strictly increasing sequence.
IssuingDistributionPoint	For particular CRLs, marked critical, see Section 7.2.2.1 for details.

revokedCertificates Component

Component	Content
serialNumber	Byte-for-byte identical to the serialNumber contained in the revoked Certificate.
revocationDate	Date and time of revocation.
crlEntryExtensions	See the “crlEntryExtensions Component” table.

crlEntryExtensions Component

Extension	Content
reasonCode	When present (OID 2.5.29.21), not marked critical and indicates the most appropriate reason for revocation of the Certificate.Present unless the CRL entry is for a Certificate not technically capable of causing issuance and either:1) The CRL entry is for a Subscriber Certificate subject to these Requirements revoked prior to July 15, 2023, or2) The reason for revocation (i.e., reasonCode) is unspecified (0).See the “CRLReasons” table.

CRLReasons

RFC 5280 reasonCode	RFC 5280 reasonCode value	Description
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.

RFC 5280 reasonCode	RFC 5280 reasonCode value	Description
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 Baseline Requirements or the CA's CP/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.
certificateHold	6	Not included if the CRL entry is for:1) A Certificate subject to these Requirements, or2) A Certificate not subject to these Requirements and was either:A) Issued on-or-after 2020-09-30 orB) Has a notBefore on-or-after 2020-09-30.
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.

Tools that NAVER Cloud Trust Services provides to the Subscriber allow for these options to be easily specified when the Subscriber requests revocation of their Certificate, with the default value being that no revocation reason is provided (i.e. the default corresponds to the CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL).

The privilegeWithdrawn reasonCode is not available to the Subscriber as a revocation reason option, because the use of this reasonCode is determined by NAVER Cloud Trust Services and not the Subscriber.

When NAVER Cloud Trust Services obtains verifiable evidence of Key Compromise for a Certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode extension with a non-keyCompromise reason, NAVER Cloud Trust Services may update the CRL entry to enter keyCompromise as the CRLReason in the reasonCode extension. Additionally, NAVER Cloud Trust Services may update the revocation date in a CRL entry when it is

determined that the private key of the certificate was compromised prior to the revocation date that is indicated in the CRL entry for that certificate.

7.2.2.1 CRL Issuing Distribution Point

Partitioned CRLs will contain an Issuing Distribution Point extension. The distributionPoint field of the Issuing Distribution Point extension MUST be present. Additionally, the fullName field of the DistributionPointName value will be present, and its value will conform to the following requirements:

1. If a Certificate within the scope of the CRL contains a CRL Distribution Points extension, then at least one of the uniformResourceIdentifiers in the CRL Distribution Points's fullName field will be included in the fullName field of the CRL's Issuing Distribution Point extension. The encoding of the uniformResourceIdentifier value in the Issuing Distribution Point extension is byte-for-byte identical to the encoding used in the Certificate's CRL Distribution Points extension.

2. Other GeneralNames of type uniformResourceIdentifiermay be included.

3. Non-uniformResourceIdentifier GeneralName types are not included.

The indirectCRL and onlyContainsAttributeCerts fields are set to FALSE (i.e., not asserted).

NAVER Cloud Trust Services may set either of the onlyContainsUserCerts and onlyContainsCACerts fields to TRUE, depending on the scope of the CRL.

NAVER Cloud Trust Services CRLs do not assert both of the onlyContainsUserCerts and onlyContainsCACerts fields.

7.3 OCSP Profile

NAVER Cloud Trust Services provides an OCSP service for TLS certificates which conforms to the RFC 6960 standard.

If an OCSP response is for a Root CA or Subordinate CA Certificate, including cross-signed Subordinate CA Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus is present.

The CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1 Version Number(s)

No stipulation

7.3.2 OCSP Extensions

The singleExtensions of an OCSP response does not contain the reasonCode (OID 2.5.29.21) CRL entry extension..

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency and Circumstances of Assessment

Audits on the certification service operated and managed by NAVER Cloud Trust Services are conducted at least annually.

8.2 Identity/Qualifications of Assessor

A Qualified Auditor SHALL performs NAVER Cloud Trust Services's audit. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (in accordance with section 8.1 of the Baseline Requirements);
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;
5. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;
6. Bound by law, government regulation, or professional code of ethics; and
7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage

8.3 Assessor's Relationship to Assessed Entity

Audits for NAVER Cloud Trust Services certification service are performed by a public accounting firm that is independent from the subject of the audit.

8.4 Topics Covered by Assessment

Annual audits validate the proper operation of NAVER Cloud Trust Services's CA service in compliance with the WebTrust Audit Criteria and the CA Browser Forum's Baseline Requirements.

8.5 Actions Taken as a Result of Deficiency

NAVER Cloud Trust Services takes actions or supplementary measures against significant deficiencies identified during an annual audit.

8.6 Communications of Results

An audit report contains the contents of the certificates issued by NAVER Cloud Trust Services, the related systems, policies, and procedures. NAVER Cloud Trust Services will make an audit report publicly available on its website.

The audit requires that NAVER Cloud Trust Services make the Audit Report available to the public no later than 3 months after of the audit period. NAVER Cloud Trust Services is not required to make publicly available any general audit finding that does not impact the overall audit opinion.

The Audit Report contains at least the following clearly-labelled information:

1. name of the organization being audited;
2. name and address of the organization performing the audit;
3. the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certificates, that were in-scope of the audit;
4. audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);
5. a list of the CA policy documents, with version numbers, referenced during the audit;
6. whether the audit assessed a period of time or a point in time;
7. the start date and end date of the Audit Period, for those that cover a period of time;
8. the point in time date, for those that are for a point in time; and
9. the date the report was issued, which will necessarily be after the end date or point in time date

8.7 Self-Audits

NAVER Cloud Trust Services performs self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

NAVER Cloud Trust Services may charge subscribers for the management as well as the issuance and renewal of certificates.

9.1.2 Certificate Access Fees

NAVER Cloud Trust Services may charge a reasonable fee for access to its certificate databases.

9.1.3 Revocation or Status Information Access Fees

NAVER Cloud Trust Services does not charge any fees when it comes to making the CRL indicated by this document available in the repository or otherwise available to the relying parties.

9.1.4 Fees for Other Services

NAVER Cloud Trust Services does not charge an additional fee for accessing or viewing this CP/CPS.

9.1.5 Refund Policy

NAVER Cloud Trust Services establishes refund policies depending on certificate types at a general and reasonable level.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

NAVER Cloud maintains general liability insurance coverage.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following information is considered confidential information of NAVER Cloud Trust Services and is protected against disclosure using a reasonable degree of care:

1. Private Keys;
2. Activation data used to access Private Keys or to gain access to the CA system;
3. Business continuity, incident response, contingency, and disaster recovery plans;
4. Other security practices used to protect the confidentiality, integrity, or availability of information;
5. Information held by NAVER Cloud Trust Services as private information in accordance with 9.3 Confidentiality of Business Information;
6. Audit logs and archive records; and
7. Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CP/CPS).

9.3.2 Information Not Within the Scope of Confidential Information

Certificates and revocation data are not considered confidential information. Furthermore, information is not considered confidential if its disclosure is mandated pursuant to this CP/CPS.

9.3.3 Responsibility to Protect Confidential Information

NAVER Cloud Trust Services, its contractors and agents use a reasonable degree of care when processing and protecting confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

NAVER Cloud Trust Services follows the NAVER Cloud Platform Privacy Policy which is available at: https://www.ncloud.com/policy/infou/infou

9.4.2 Information Treated as Private

See Section 9.4.1

9.4.3 Information Not Deemed Private

See Section 9.4.1

9.4.4 Responsibility to Protect Private Information

See Section 9.4.1

9.4.5 Notice and Consent to Use Private Information

See Section 9.4.1

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

See Section 9.4.1

9.4.7 Other Information Disclosure Circumstances

See Section 9.4.1

9.5 Intellectual Property rights

NAVER Cloud Trust Services does not knowingly violate the intellectual property rights of third parties.

NAVER Cloud Trust Services and/or its business partners own the intellectual property rights in NAVER Cloud Trust Services's services, including the certificates, trademarks used in providing the services, and this CP/CPS.

9.5.1 Property Rights in Certificates and Revocation Information

NAVER Cloud Trust Services grants permission to reproduce and distribute certificates on a non-exclusive, royalty free basis, since certificate and revocation information produced by NAVER Cloud Trust Services's CA are statements of fact.

NAVER Cloud Trust Services reserves the right to revoke a certificate at any time and at its sole discretion, and has a liability to maintain revocation information.

9.5.2 Property Rights in the Agreement

NAVER Cloud Trust Services’s PKI service participants acknowledge that NAVER Cloud Trust Services retains all Intellectual Property Rights in and to this CP/CPS.

9.5.3 Property Rights of Names

Certificate applicants retain all rights, if they have any, in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to them. NAVER Cloud Trust Services retains all rights it has in any trademark, service mark, trade name, or other identifying trade symbols that it owns.

9.5.4 Property Rights in Key Pairs

Private Keys and Public Keys remain the property of the Subscribers who rightfully hold them.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Except as expressly stated in this CP/CPS or in a separate agreement with a Subscriber, NAVER Cloud Trust Services does not make any representations or warranties regarding its products or services.

1. NAVER Cloud Trust Services complies, in all material aspects, with this CP/CPS,
2. NAVER Cloud Trust Services publishes and updates CRLs and OCSP respond on a regular basis,
3. All certificates issued under this CP/CPS will be verified in accordance with this CP/CPS and meet the minimum requirements found herein and in the baseline requirement, and
4. NAVER Cloud Trust Services will maintain a repository of public information on its website.

9.6.2 RA Representations and Warranties

No stipulation

9.6.3 Subscriber Representations and Warranties

NAVER Cloud Trust Services requires, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, NAVER Cloud Trust Services obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

1. The Applicant’s agreement to the Subscriber Agreement with NAVER Cloud Trust Services, or
2. The Applicant’s acknowledgement of the Terms of Use.

NAVER Cloud Trust Services implements a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement apply to the Certificate to be issued pursuant to the certificate request. NAVER Cloud Trust Services may use an electronic or "click-through" Agreement provided that NAVER Cloud Trust Services has determined that such agreements are legally enforceable. A separate Agreement may be used for each certificate request, or a single Agreement may be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

The Subscriber Agreement or Terms of Use contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;

2. Protection of Private Key: An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that correspond to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);

3. Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;

4. Use of Certificate: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;

5. Reporting and Revocation: An obligation and warranty to: (a) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.

6. Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.

7. Responsiveness: An obligation to respond to the CA's instructions concerning key compromise or Certificate misuse within a specified time period.

8. Acknowledgment and Acceptance: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.6.4 Relying Party Representations and Warranties

Relying Parties represent and warrant that: (a) they have read, understand and agree to this CP/CPS; (b) they have verified both the relevant NAVER Cloud Trust Services CA's Certificate and any other certificates in the certificate chain using the relevant CRL or OCSP; (c) they will not use a Certificate if the Certificate has expired or been revoked; (d) they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate; (e) they have studied the applicable limitations on the usage of Certificates and agree to NAVER Cloud Trust Services's limitations on liability related to the use of Certificates; (f) they are solely responsible for deciding whether or not to rely on information in a Certificate; and (g) they are solely responsible for the legal and other consequences of their failure to perform the Relying Party obligations in this CP/CPS.

Relying Parties also represent and warrant that they will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a Certificate after considering:

1. Applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;
2. The intended use of the Certificate as listed in the Certificate or this CP/CPS;
3. The data listed in the Certificate;
4. The economic value of the transaction or communication;
5. The potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication;
6. The Relying Party's previous course of dealing with the Subscriber;
7. The Relying Party's understanding of trade, including experience with computer-based methods of trade; and
8. Any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

EXCEPT AS EXPRESSLY STATED IN THIS CP/CPS, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE."

TO THE MAXIMUM EXTENT PERMITTED BY LAW, NAVER CLOUD TRUST SERVICES DISCLAIMS ALL OTHER WARRANTIES, BOTH EXPRESS AND IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF ACCURACY OF INFORMATION PROVIDED WITH RESPECT TO

CERTIFICATES ISSUED BY NAVER CLOUD TRUST SERVICES, THE CRL, AND ANY PARTICIPANT'S OR THIRD PARTY'S PARTICIPATION IN NAVER CLOUD TRUST SERVICES PKI, INCLUDING USE OF KEY PAIRS, CERTIFICATES, THE CRL OR ANY OTHER GOODS OR SERVICES PROVIDED BY NAVER CLOUD TRUST SERVICES TO THE PARTICIPANT.

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1 OF THIS CP/CPS, NAVER CLOUD TRUST SERVICES DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE.

NAVER Cloud Trust Services does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time. A fiduciary duty is not created simply because an individual or entity uses NAVER Cloud Trust Services's services.

9.8 Limitations of Liability

TO THE EXTENT PERMITTED BY APPLICABLE LAW, NAVER CLOUD TRUST SERVICES SHALL NOT BE LIABLEFOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES, INCLUDING BUT NOT LIMITED TO DAMAGES FOR LOST DATA, LOST PROFITS, LOST REVENUE OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY, INCLUDING BUT NOT LIMITED TO CONTRACT OR TORT (INCLUDING PRODUCTS LIABILITY, STRICT LIABILITY AND NEGLIGENCE), AND WHETHER OR NOT IT WAS, OR SHOULD HAVE BEEN, AWARE OR ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY STATED HEREIN. NAVER CLOUD TRUST SERVICES'S AGGREGATE LIABILITY UNDER THIS CP/CPS IS LIMITED TO $500.

9.9 Indemnities

9.9.1 By Subscriber

To the extent permitted by law, each Subscriber shall indemnify NAVER Cloud Trust Services, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of its Subscriber Agreement, this CP/CPS, or applicable law; (iii) the compromise or unauthorized use of a certificate or Private Key caused by the Subscriber's negligence or intentional acts; or (iv) Subscriber's misuse of a certificate or Private Key.

9.9.2 By Relying Parties

To the extent permitted by law, each Relying Party shall indemnify NAVER Cloud Trust Services, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage,

or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of any service terms applicable to the services provided by NAVER Cloud Trust Services or its affiliates and used by the Relying Party, this CP/CPS, or applicable law; (ii) unreasonable reliance on a certificate; or (iii) failure to check the certificate's status prior to use.

9.10 Term and Termination

9.10.1 Term

The CP/CPS becomes effective from the time set forth in this document after publication in the repository (website). Amendments to this CP/CPS take effect after publication in the repository.

9.10.2 Termination

This CP/CPS and the related policy documents remain in effect until replaced by a newer version.

9.10.3 Effect of Termination and Survival

Upon termination of this CP/CPS, this CP/CPS remains in effect for all the certificates issued for the remainder of their validity period.

9.11 Individual Notices and Communications with Participants

All the participants, including the relying parties, may communicate with each other in a reasonable manner if necessary.

9.12 Amendments

9.12.1 Procedure for Amendment

NAVER Cloud Trust Services may revise and change this CP/CPS at any time at its sole discretion and without giving prior notice to its subscribers or relying parties in accordance with the procedures specified in Section 1.5.4. NAVER Cloud Trust Services may publish all the modified versions of the CP/CPS on the website.

9.12.2 Notification Mechanism and Period

NAVER Cloud Trust Services may use the website or other effective methods to notify the major relying parties of changes in the CP/CPS if necessary.

9.12.3 Circumstances Under Which OID Must be Changed

NAVER Cloud Trust Services is solely responsible for determining whether an amendment to the CP/CPS requires an OID change.

9.13 Dispute Resolution Provisions

Parties are required to notify NAVER Cloud Trust Services and attempt to resolve disputes directly with NAVER Cloud Trust Services before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14 Governing Law

This CP/CPS is governed, construed and interpreted in accordance with the laws of Republic of Korea. This choice of law is made to ensure uniform interpretation of this CP/CPS, regardless of the place of residence or place of use of NAVER Cloud Trust Services Certificates or other products and services. The law of Republic of Korea applies also to all NAVER Cloud Trust Services commercial or contractual relationships in which this CP/CPS may apply or quoted implicitly or explicitly in relation to NAVER Cloud Trust Services products and services where NAVER Cloud Trust Services acts as a provider, supplier, beneficiary receiver or otherwise.

9.15 Compliance with Applicable Law

This CP/CPS is subject to all applicable laws and regulations.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

Any entities operating under this CP/CPS may not assign their rights or obligations without the prior written consent of NAVER Cloud Trust Services. Unless specified otherwise in a contract with a party, NAVER Cloud Trust Services does not provide notice of assignment.

9.16.3 Severability

If any provision of this CP/CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CP/CPS will remain valid and enforceable. Each provision of this CP/CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

In the event of a conflict between CABF Baseline Requirements and a law, regulation or government order (hereinafter ‘Law’) of any jurisdiction in which a CA operates or issues certificates, NAVER Cloud Trust Services modifies any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law. In such event, NAVER Cloud Trust Services immediately (and prior to issuing a certificate under the modified requirement) includes in Section 9.16.3 of this CP/CPS a detailed reference to the Law requiring a

modification of these Requirements under this section, and the specific modification to these Requirements implemented by NAVER Cloud Trust Services.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

NAVER Cloud Trust Services may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. NAVER Cloud Trust Services failure to enforce a provision of this CP/CPS does not waive NAVER Cloud Trust Services right to enforce the same provision later or right to enforce any other provision of this CP/CPS. To be effective, waivers must be in writing and signed by NAVER Cloud Trust Services.

9.16.5 Force Majeure

NAVER Cloud Trust Services is not liable for any delay or failure to perform an obligation under this CP/CPS to the extent that the delay or failure is caused by natural disasters, acts of war, terrorism or any other similar cause beyond the reasonable control of NAVER Cloud Trust Services.

9.17 Other Provisions

No stipulation.

APPENDIX A: CHANGE HISTORY

The following revisions have been made to the original document.

Ver	Date	Description
1.0.0	05 June 2023	Initial publication. **Note**: This CPS was published after an update based on NAVER Cloud CPS (version 1.6.0).
1.0.1	24 August 2023	Added new root. Added the 3.2.2.4.7 DNS Change method to the section titled *3.2.2.4 Validation of Domain Authorization or Control*.
1.0.2	27 December 2023	Updated CAA record domain name in Section 4.2.4. No longer offering certificate renewals in Section 4.6 and below. Treat certificate rekey requests as requests for the issuance of a new Certificate in Section 4.7 and below. Specified revocation request grace period in Section 4.9.4. Updated online revocation and status checking availability in Section 4.9.9. Updated a method for reporting key compromise in Section 4.9.12. Updated the activation data generation and installation in Section 6.4 and below. Typo correction.
1.0.3	17 October 2024	Revised to reflect updates based on CABF BR Version 2.0.7. Change of company address. Typo correction.

Ver	Date	Description
1.0.4	26 November 2024	This document replaces the NAVER Cloud Trust Services CPS v1.0.3. Updated Section 7.1.2.
1.0.5	05 March 2025	Changed “Not Application” to “No Stipulation.” Revised Section 7.1.2 Certificate Extensions to provide a more detailed specification of RFC 5280.
1.0.6	19 June 2025	Removed the method “3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact” from section 3.2.2.4 Validation of Domain Authorization or Control.
1.0.7	1 October 2025	Domain Validation: Added ACME methods (3.2.2.4) Multi-Perspective Issuance: New MPIC requirements (3.2.2.9) Revocation/OCSP: Updated per CABF BR 2.1.0 (4.9.9) Security Controls: Updated per CABF NETSEC v2.0.5 (6.7) Subscriber/Org Naming: Clarified DBA/tradename rules per CABF BR 2.0.9 & 2.1.1 Incident Handling: Added Mass Revocation Plan (5.7.1)
1.0.8	27 November 2025	Added New Intermediate CAs (1.3.1)