NAVER BUSINESS PLATFORM Corp.
Certification Practice Statement V1.4

Contents

INTRODUCTION

1.1 Overview

This document defines the company's certification policy, operational management procedures, and other necessary instructions in servicing the Certification Authority provided by the NAVER BUSINESS PLATFORM Corp.

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.

1.2 Document Name and Identification

This document is the NAVER BUSINESS PLATFORM Corp. Certification Practice Statement. It describes the policies for the operation and management of the "NAVER Global Root Certification Authority" and "NAVER Secure Certification Authority", which are the Certification Authorities operated by the NAVER BUSINESS PLATFORM. 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.

This document covers all the certificates issued and signed by the following Certification Authority.

Subject: CN = NAVER Secure Certification Authority 1, O = NAVER BUSINESS PLATFORM Corp., C = KR

certificatePolicies.policyIdentifiers: 1.2.410.200081.2.1.1

The following revisions have been made to the original document

Date	Description	Version
28 November, 2019	Updated 5.2.2 Number of Persons Required per Task, 5.4.1 Types of Events Recorded	1.4
19 November, 2019	Yearly update	1.3
14 November, 2018	Added Appendix A: Certificate Profiles	1.2
10 September, 2018	Yearly update, including CAA record information	1.1
11 September, 2017	Initial release.	1.0

1.3 PKI Participants

The participants inside the Public Key Infrastructure (hereinafter "PKI") of the NAVER BUSINESS PLATFORM 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. The NAVER BUSINESS PLATFORM directly operates the Root Certification Authorities and Certification Authorities.

The NAVER Global Root Certification Authority is the Root Certification Authority that is self-signed and operated directly on the NAVER BUSINESS PLATFORM. This authority issues CA certificates to subordinate CAs of the NAVER BUSINESS PLATFORM.

The NAVER Secure Certification Authority issues subscriber certificates under the approval of the NAVER BUSINESS PLATFORM in accordance with this CPS. The CA can be operated with multiple CA Certificates according to the algorithms and certificate profiles specified in this document.

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 the NAVER BUSINESS PLATFORM.

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 in Korea that has issued end-user certificates from the NAVER BUSINESS PLATFORM CA. If the NAVER BUSINESS PLATFORM 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 generates and verifies a digital signature with a certificate issued by the NAVER BUSINESS PLATFORM or decrypts an encrypted document or a message.

1.3.5 Other Participants

Not applicable.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued pursuant to this 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 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 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 BUSINESS PLATFORM establishes and amends CPS.

1.5.2 Contact Person

The contact details related to the certifications of the NAVER BUSINESS PLATFORM are as follows:

- URL: https://certificate.naver.com
- E-mail: dl_rootca@navercorp.com
- Address: Alphadom tower IV, 117, Bundangnaegok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Republic of Korea

1.5.3 Person Determining CPS Suitability for the Policy

In the case that the department head of IT Security in the NAVER BUSINESS PLATFORM determines that a change to the CPS is necessary, it will be amended.

The NAVER BUSINESS PLATFORM maintains and manages amendment records of the CPS, including:

① CPS version
② Overview of applicable tasks and **its** scope
③ CPS amendment records
④ Regulation of amended CPS
   - Amendment contents
   - Reason for amendment, etc.

1.5.4 CPS Approval Procedures

The NAVER BUSINESS PLATFORM may amend this CPS. Any changes will be disclosed to the address listed in Section 1.5 of this document. The NAVER BUSINESS PLATFORM's amendments of the CPS will generally have no effect on the relying parties. However, if the NAVER BUSINESS PLATFORM will determine that changes have a significant impact on the relying parties, it may give notice to such participants in advance.

This CPS is published at https://certificate.naver.com.

The amended CPS will become effective fifteen (15) days after it has been published and be binding on all the participants in the NAVER BUSINESS PLATFORM from that point forward.

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 displays or uses NAVER BUSINESS PLATFORM certificates and distributes NAVER BUSINESS PLATFORM 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 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.

Key Pair

A Private Key and associated Public Key.

OCSP Responder

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

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.

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 BUSINESS PLATFORM 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 the AICPA/CICA WebTrust Program for Certification Authorities.

X.509

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

1.6.2 Acronyms

CA

  Certificate Authority or Certification Authority

CAB

  "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 the NAVER BUSINESS PLATFORM covers the following information:

① Certification Practice Statement(CPS)
② Most recently issued certificate revocation list(CRL)
③ Most recently issued CA certificate revocation list(ARL)
④ Root CAs and CA certificates issued by the NAVER BUSINESS PLATFORM CAs
⑤ Other documents or information deemed necessary for disclosure on the NAVER BUSINESS PLATFORM

2.2 Publication of Certification Information

The NAVER BUSINESS PLATFORM 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://certificate.naver.com

2. By email to : dl_rootca@navercorp.com

3. By mail addressed to : Alphadom tower IV, 117, Bundangnaegok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Republic of Korea

4. By telephone Tel : 1566-3880

5. By fax : (031)784-1800

2.3 Time or Frequency of Publication

The CRL is updated promptly upon the revocation of a certificate within one (1) business day following revocation. Generally, the CRL is periodically updated and reissued at least every seven (7) days, and their validity period is limited to ten (10) days.

The NAVER BUSINESS PLATFORM revises the certification policy or the CPS at least annually and updates with changes as needed to the latest version of the CA Browser Forum Baseline Requirements.

2.4 Access Controls on Repositories

The Repository is publicly available. The NAVER BUSINESS PLATFORM 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

The subscriber certificates issued by the NAVER BUSINESS PLATFORM CAs conform to X.509 standards and follow the Distinguished Name system below.

- Root CA Certificate DN
CN=NAVER Global Root Certification Authority
O=NAVER BUSINESS PLATFORM Corp.
C=KR

- CA Certificate DN
CN=NAVER Secure Certification Authority 1
O=NAVER BUSINESS PLATFORM Corp.
C=KR

- Domain Validation Subscriber Certificate DN
CN=common name

- Organization Validation Subscriber Certificate DN

CN=common name
O=organization name
OU=organizational unit
L=locality
S=state or province
C=country code

3.1.2 Need for Names to be Meaningful

The NAVER BUSINESS PLATFORM puts meaningful names in both the subjectDN and the issuerDN extensions of Certificates.

3.1.3. Anonymity or Pseudonymity of Subscribers

The NAVER BUSINESS PLATFORM does not issue anonymous or pseudonymous Certificate.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Name

No stipulation.

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 CPS, the NAVER BUSINESS PLATFORM does not verify an Applicant's right to use a trademark and does not resolve trademark disputes. The NAVER BUSINESS PLATFORM 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 must prove the ownership of his/her private key by providing a PKCS#10-formatted Certificate Signing Request, or a cryptographically equivalent proof to the NAVER BUSINESS PLATFORM.

3.2.2 Authentication of Organization Identity

The NAVER BUSINESS PLATFORM identifies and validates the applicant and all the persons, objects, devices, 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 must be performed to ensure the right to request revocation within the scope required by this CPS. It must be verified whether all the subject information that will contain the NAVER BUSINESS PLATFORM certificate applicant conforms to the requirements of this CPS and has been validated under this CPS in accordance with procedures. Such verification process is intended for:

- Identifying the applicant requesting the NAVER BUSINESS PLATFORM 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) (if applicable) of the domain name to be included in a certificate; or
- Confirming the subject ownership and control of the device's name to be included in a certificate (if applicable); or
- Confirming whether the applicant is authorized to request a certificate.

3.2.2.1 Identity

For Organization Validation Subscriber Certificate, the NAVER BUSINESS PLATFORM 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, the NAVER BUSINESS PLATFORM 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.

3.2.2.2 DBA/Tradename

If the Subject Identity Information is to include a DBA or tradename, the NAVER BUSINESS PLATFORM 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

3.2.2.4.1 Email, Fax, SMS, or Postal Mail to Domain Contact

(in accordance with section 3.2.2.4.2 of v1.4.1 of the Baseline Requirements)

Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value

The Random Value is generated by the NAVER BUSINESS PLATFORM and remains valid for use in a confirming response for no more than 30 days from its generation;

3.2.2.4.2 Constructed Email to Domain Contact

(as defined in section 3.2.2.4.4 of v1.4.1 of the Baseline Requirements)

(i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

The Random Value is generated by the NAVER BUSINESS PLATFORM and remains valid for use in a confirming response for no more than 30 days from its generation;

3.2.2.5 Authentication of an IP Address

The NAVER BUSINESS PLATFORM 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, the NAVER BUSINESS PLATFORM 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").

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.

- Legal existence and identity of Applicant - 825 days;

- Domain name - 825 days;

- Authority of Applicant - 825 days

3.2.2.8 CAA Records

See Section 4.2.4

3.2.3 Authentication of Individual Identity

The NAVER BUSINESS PLATFORM does not issue OV Certificates to natural persons.

3.2.4 Non-verified Subscriber Information

No Stipulation.

3.2.5 Validation of Authority

The CA maintains controls to provide reasonable assurance that, for authenticated certificates, Subscriber's certificate requests are accurate, authorized and complete.

If the Applicant for a Certificate containing Subject Identity Information is an organization, the CA SHALL use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.

The CA MAY use the sources listed in section 3.2.2.1 to verify the Reliable Method of Communication.

Provided that the CA uses a Reliable Method of Communication, the CA MAY establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

In addition, the CA SHALL establish a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CA SHALL NOT accept any certificate requests that are outside this specification. The CA SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.2.6 Criteria for Interoperation

Not applicable.

3.3 Identification and Authentication for Re-Key Requests

For re-key requests, The NAVER BUSINESS PLATFORM 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

3.3.2 Identification and Authentication for Re-Key After Revocation

See Section 3.2

3.4 Identification and Authentication for Revocation Request

A subscriber can directly revoke certificates, by using the subscriber's user ID and password for user identification, if they are no longer in use or if it is suspected that certificates and/or key pairs may be damaged.

The NAVER BUSINESS PLATFORM CA and RAs may revoke the related CA or subscriber certificates if the issued CA or subscriber key pair are deemed damaged or suspected of being compromised according to 4.9.1 of this CPS. Prior to certificate revocation, the NAVER BUSINESS PLATFORM CA and RAs will notify the relying parties, including the subscribers, of the certificate revocation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

• An applicant must submit an application containing a domain address, and the NAVER BUSINESS PLATFORM CA and RAs will validate the submitted application and identification documents.
• The certificate Application containing a domain name must include the domain name to be included in the certificate subject. The RAs verify if the domain name is included in WHOIS or a trusted database accepted by the NAVER BUSINESS PLATFORM.
• A revoked certificate suspected of phishing or fraud or a rejected certificate request is stored in a database operated within the NAVER BUSINESS PLATFORM. The NAVER BUSINESS PLATFORM 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 Certificate MUST be 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, the CA SHALL obtain the following documentation from the Applicant:

1. A certificate request, which may be electronic; and

2. An executed Subscriber Agreement or Terms of Use, which may be electronic.

The CA SHOULD obtain any additional documentation the CA determines necessary to meet these Requirements.

Prior to the issuance of a Certificate, the CA SHALL obtain from the Applicant a certificate request in a form prescribed by the CA and that complies with these Requirements. One certificate request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in Section 3.3.1, 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 MUST contain 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

The NAVER BUSINESS PLATFORM 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 the CAs 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.

The NAVER BUSINESS PLATFORM 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, the NAVER BUSINESS PLATFORM CAs will approve the certificate request. However, if the subscriber information is not validated or if the request does not comply with the CPS requirements, the NAVER BUSINESS PLATFORM may reject the certificate request.

4.2.3 Time to Process Certificate Applications

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

4.2.4 Certificate Authority Authorization (CAA) Records

The NAVER BUSINESS PLATFORM checks for a CAA record for each dNSName in the subjectAltName extension of the Certificate to be issued, according to the procedure in RFC 6844, following the processing instructions set down in RFC 6844 for any records found.

The following Issuer Domain Names in CAA "issue" or "issuewild" records are recognized as permitting the NAVER BUSINESS PLATFORM to issue:

- certificate.naver.com

The NAVER BUSINESS PLATFORM 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

Once these procedures have been completed, the certificate is generated and the appropriate key usage extension added.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

The NAVER BUSINESS PLATFORM will deliver certificates within a reasonable time after issuance. Generally, the NAVER BUSINESS PLATFORM delivers certificates via email to the email address designated by the Subscriber, via a programmatic method such as an API, or via download from a website.

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

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

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The Certification Authority maintains effective controls to provide reasonable assurance that the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles

4.5.2 Relying Party Public Key and Certificate Usage

No stipulation

4.6 Certificate Renewal

Certificate renewal is the process whereby a new certificate is created using an existing key pair with an updated validity period. For security reasons, the NAVER BUSINESS PLATFORM does not offer certificate renewal without changing a key pair. Before the expiration of a NAVER SSL certificate, a subscriber is required to generate a new key pair and request a new certificate in accordance with this CPS.

4.6.1 Circumstances for Certificate Renewal

A subscriber can request a renewal of a certificate from ninety (90) days before the expiration date of the issued certificate.

4.6.2 Who May Request Renewal

See Section 4.1.1

4.6.3 Processing Certificate Renewal Requests

See Section 4.2

4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

See Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

If the NAVER BUSINESS PLATFORM recognizes that the issued CA and/or subscriber certificates and the corresponding private keys are not secure, it may revoke the related certificates and private keys and reissue a certificate using a new key pair.

With the permission of the NAVER BUSINESS PLATFORM CA or RAs, a certificate can be reissued in accordance with the new certificate issuance procedure after approving the certificate reissuance requested by a subscriber.

4.7.2 Who May Request Certification of a New Public Key

See Section 4.1.1

4.7.3 Processing Certificate Re-Keying Requests

See Section 4.2

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See Section 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

See Section 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

The NAVER BUSINESS PLATFORM 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

See Section 4.1.1

4.8.3 Processing Certificate Modification Requests

See Section 4.2

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3

4.9 Certificate Revocation and Suspension

The NAVER BUSINESS PLATFORM 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

The CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;

2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;

3. The CA obtains evidence that the Subscriber'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. The CA obtains evidence that the Certificate was misused;

5. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;

6. The CA 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);

7. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;

8. The CA is made aware of a material change in the information contained in the Certificate;

9. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;

10. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;

11. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

12. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;

13. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;

14. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or

15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk

and that such Certificates should be revoked and replaced by CAs within a given period of time).

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

The Issuing CA SHALL 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 the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;

    3. The Issuing CA 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. The Issuing CA obtains evidence that the Certificate was misused;

    5. The Issuing CA 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. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;

    7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

    8. The Issuing CA's or Subordinate CA's right to issue Certificates expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;

    9. Revocation is required by the Issuing CA's Certification Practice Statement.

    10. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine Google Trust Services, Certification Practice Statement v2.2 28 that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

4.9.2 Who Can Request Revocation

The CA SHALL provide a process for Subscribers to request revocation of their own Certificates. The process MUST be described in the CA's Certificate Policy or Certification Practice Statement. The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests

and related inquiries. The NAVER BUSINESS PLATFORM may revoke a certificate without receiving a request and without reason.

Subscribers may request revocation of their own certificates by emailing dl_rootca@navercorp.com. All reports need to include sufficient detail to identify the specific certificates to be revoked.

4.9.3 Procedure for Revocation Request

The NAVER BUSINESS PLATFORM processes a revocation request as follows:

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

2. The NAVER BUSINESS PLATFORM 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, The NAVER BUSINESS PLATFORM revokes the certificate.

4. For requests from third parties, The NAVER BUSINESS PLATFORM personnel begin investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:

a. The nature of the alleged problem,

b. The number of reports received about a particular certificate or website,

c. The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and

d. Relevant legislation.

5. If the NAVER BUSINESS PLATFORM determines that revocation is appropriate; The NAVER BUSINESS PLATFORM personnel revoke the certificate and update the CRL.

The NAVER BUSINESS PLATFORM maintains a continuous 24/7 ability to internally respond to any high priority revocation requests. If appropriate, The NAVER BUSINESS PLATFORM forwards complaints to law enforcement.

4.9.4 Revocation Request Grace Period

No stipulation

4.9.5 Time Within Which CA Must Process the Revocation Request

The NAVER BUSINESS PLATFORM begins the procedure for certificate revocation within 24 hours 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 one (1) business day following the revocation.

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 the applicable CRL or OCSP responder before relying on a certificate

4.9.7 CRL Issuance Frequency

The CRL is published periodically at least every day and is valid for seven (7) days. The published CRL is posted at the following website specified in the CPS:

- ica.navercorp.com/crl

4.9.8 Maximum Latency for CRLs

The CRL is posted to the CRL repository within one (1) business day following the CRL generation.

4.9.9 On-Line Revocation/Status Checking Availability

The CAs support Online Certificate Status Protocol (OCSP) for the CA and subscriber certificates issued by the NAVER BUSINESS PLATFORM. The OCSP addresses are:

- OCSP for CA certificates: ocsp-rca.navercorp.com
- OCSP for subscriber certificates: ocsp-ica.navercorp.com

OCSP responses conform to the RFC 6960.
- The NAVER BUSINESS PLATFORM issues a separate certificate for signing an OCSP response. An OCSP signing Certificate which is signed by the CA contains an extension of the id-pkix-ocsp-nocheck type, as defined by the RFC6960.

4.9.10 On-Line Revocation Checking Requirements

OCSP response messages are updated at least every four (4) days and are valid up to ten (10) days. An OCSP responder utilizes the GET method for requesting OCSP and receiving it.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

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 the NAVER BUSINESS PLATFORM that the subscriber's certificate has been compromised.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

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

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

4.10.3 Operational 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

The NAVER BUSINESS PLATFORM does not escrow the subscribers' private keys.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

The NAVER BUSINESS PLATFORM 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

The NAVER BUSINESS PLATFORM installs and operates the CA system in a separate control zone and performs physical access control for the system.

5.1.2 Physical Access

The NAVER BUSINESS PLATFORM operates its own access control system and controls access to restricted areas by combining biometric authentication including the identification card and fingerprint recognition.

5.1.3 Power and Air Conditioning

The NAVER BUSINESS PLATFORM uses an uninterruptable power supply (UPS) to prevent serious damage from power outages.

The NAVER BUSINESS PLATFORM installs and operates an air conditioning system to maintain constant temperature and humidity.

5.1.4 Water Exposures

The NAVER BUSINESS PLATFORM installs its CA system at a distance from the floor to protect it from water exposure.

5.1.5 Fire Prevention and Protection

The NAVER BUSINESS PLATFORM 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

The NAVER BUSINESS PLATFORM controls physical access by keeping the storage and recording media used for the CA service in a fireproof safe.

5.1.7 Waste Disposal

The NAVER BUSINESS PLATFORM 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

The NAVER BUSINESS PLATFORM 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 the NAVER BUSINESS PLATFORM 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 Manager
- Certification Contact Person
- Internal Auditor
- Certification Center Operator
- Developer

5.2.2 Number of Persons Required per Task

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.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The major business contact person at the certification center operated by the NAVER BUSINESS PLATFORM 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 CPS requirements.

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

5.3.2 Background Check Procedures

The NAVER BUSINESS PLATFORM 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

The NAVER BUSINESS PLATFORM conducts the certificate management training necessary for business performance when recruiting any employees required to be educated, including the Trusted Roles.

5.3.4 Retraining Frequency and Requirements

The personnel responsible for the certification task in the NAVER BUSINESS PLATFORM 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

The NAVER BUSINESS PLATFORM 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 the NAVER BUSINESS PLATFORM certification service, the NAVER BUSINESS PLATFORM can impose the same sanctions against unauthorized actions as specified in Section 5.3.6.

5.3.8 Documentation Supplied to Personnel

The NAVER BUSINESS PLATFORM 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

The NAVER BUSINESS PLATFORM records the following events occurred in the certification system and applications and creates and records certificate management logs from the data collected in accordance with the internal audit procedures.

- Applicant and subscriber actions
  - Request to create a certificate
  - Request to revoke a certificate
- Certificate lifecycle-related events
  - Key generation
  - Damaged key notification
  - Issuance of a certificate
  - Distribution of a certificate
  - Rejection or cancellation of a certificate
  - Generation of a Certificate Revocation List(CRL)
  - Generation of an OCSP response
- Operation and management actions by personnel performing the Trusted Roles
  - Login events and use of identification and authentication mechanisms
  - Changes to the CA policy
  - Changes to the CA keys
  - Changes to the CA system configuration
- Security events
  - Successful and unsuccessful PKI system access attempts;
  - PKI and security system actions performed;
  - Security profile changes;
  - System crashes, hardware failures, and other anomalies;

- Firewall and router activities; and
- Entries to and exits from the CA facility.

5.4.2 Frequency of Processing Log

Audit logs are periodically reviewed by the NAVER BUSINESS PLATFORM on an as-needed basis.

5.4.3 Retention Period for Audit Log

The NAVER BUSINESS PLATFORM retains every audit log generated for at least seven (7) years or longer and may provide its internal or external auditors with these retained audit logs if necessary.

5.4.4 Protection of Audit Log

The audit records generated by each system are managed by the personnel designated by the NAVER BUSINESS PLATFORM, and the administrators of each system task can only view the audit records related to their tasks.

5.4.5 Audit Log Backup Procedures

The NAVER BUSINESS PLATFORM 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 Collection System (Internal vs. External)

No stipulation

5.4.7 Notification to Event-Causing Subject

No stipulation

5.4.8 Vulnerability Assessments

The NAVER BUSINESS PLATFORM periodically conducts its own scan to ensure effective security management in performing certification services.

5.5 Records Archival

5.5.1 Types of Records Archived

Records to be archived are those specified in Section 5.4.1.

5.5.2 Retention Period for Archive

The NAVER BUSINESS PLATFORM retains all the documentation relating to certificate requests and the issuance thereof, and the revocation thereof for at least seven (7) 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 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 the NAVER BUSINESS PLATFORM. 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

The procedure for providing a new CA certificate to a subject following a re-key is the same as the procedure for initially providing the CA certificate.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The CA must maintain controls to provide reasonable assurance that damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures.

The CA SHALL document 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. The CA is not required to publicly disclose its business continuity plans but SHALL make its business continuity plan and security plans available to the CA's auditors upon request. The CA SHALL annually test, review, and update these procedures.

The business continuity plan MUST 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. The CA's plan to maintain or restore the CA'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 CA'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.

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

The NAVER BUSINESS PLATFORM 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 the NAVER BUSINESS PLATFORM 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.

5.7.4 Business Continuity Capabilities After a Disaster

The NAVER BUSINESS PLATFORM 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 the NAVER BUSINESS PLATFORM discontinues operating The NAVER BUSINESS PLATFORM 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 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 the NAVER BUSINESS PLATFORM 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 the NAVER BUSINESS PLATFORM.

Subscriber Key Pairs are generated by the Subscriber.

6.1.2 Private Key Delivery to Subscriber

The NAVER BUSINESS PLATFORM 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 NAVER BUSINESS PLATFORM CA public keys are digitally signed by the Root CA operated by the NAVER BUSINESS PLATFORM. The NAVER BUSINESS PLATFORM establishes and enforces the procedures for delivering chain-certified CA certificates upon an applicant's receipt of issued certificates so that the NAVER BUSINESS PLATFORM 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)	2048

6.1.6 Public Key Parameters Generation and Quality Checking

For RSA keys, The NAVER BUSINESS PLATFORM confirms that the value of the public exponent is an odd number equal to 3 or more.

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 issued solely for the purpose of testing products with Certificates issued by a Root CA

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

The NAVER BUSINESS PLATFORM performs the generation of CA key pairs in accordance with its internal key generation procedures. At least two or more personnel participate in key pair generation.

6.2.3 Private Key Escrow

The NAVER BUSINESS PLATFORM 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 the NAVER BUSINESS PLATFORM 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

The NAVER BUSINESS PLATFORM 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 the NAVER BUSINESS PLATFORM, 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

The NAVER BUSINESS PLATFORM CA's private keys are generated and stored inside cryptographic modules which meet the requirements of 6.2.1 of this CPS.

6.2.8 Method of Activating Private Key

Under the approval of the NAVER BUSINESS PLATFORM, 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 the NAVER BUSINESS PLATFORM, 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

The NAVER BUSINESS PLATFORM may destroy CA private keys for the following reasons:

- CA certificates expired
- CA private keys damaged, leaked, or potentially compromised.

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 the NAVER BUSINESS PLATFORM 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. Test certificates are valid for thirty (30) days. Subscriber Certificate validity period can be set to (1) year or two (2) years upon subscription by a subscriber and no greater than 825 days.

6.4 Activation Data

Hardware security module(HSM) keys are stored in the corresponding modules and can only be used by the administrators authorized by the NAVER BUSINESS PLATFORM. The module activation to use a key pair in a hardware security module is performed according to the multiple control procedures implemented with a module necessary for physical access control such as smart cards.

6.4.1 Activation Data Generation and Installation

No stipulation

6.4.2 Activation Data Protection

No stipulation

6.4.3 Other Aspects of Activation Data

No stipulation

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The NAVER BUSINESS PLATFORM 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 the NAVER BUSINESS PLATFORM 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 the NAVER BUSINESS PLATFORM 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.

6.6.2 Security Management Controls

The NAVER BUSINESS PLATFORM 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

The NAVER BUSINESS PLATFORM performs network access control to the CA system server according to the network management policy. A hardware firewall device is used to control the specific ports used for issuing and validating CA and subscriber certificates.

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 the NAVER BUSINESS PLATFORM 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 the NAVER BUSINESS PLATFORM have X.509 version 3.

7.1.2 Certificate Extensions

See The NAVER BUSINESS PLATFORM Profiles APPENDIX A.

7.1.3 Algorithm Object Identifiers

See The NAVER BUSINESS PLATFORM Profiles APPENDIX A.

7.1.4 Name Forms

Each certificate includes a unique positive serial number that is never reused. Optional subfields in the subject of an SSL Certificate must either contain information verified by the NAVER BUSINESS PLATFORM or be left empty. SSL Certificates cannot contain metadata such as '.', '-' and ' ' characters or any other indication that the field is not applicable.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

The certificates issued under the NAVER BUSINESS PLATFORM use this 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 policy identifiers assigned under the CA Browser Forum are also used for Domain Validation and Organization Validation Subscriber Certificates.

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

The CRL issued by the NAVER BUSINESS PLATFORM conforms to the RFC 5280 standards.

7.2.1 Version Number(s)

The NAVER BUSINESS PLATFORM issues version 2 CRLs

7.2.2 CRL and CRL Entry Extensions

Field	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the certificate
Invalidity Date	Optional date in UTC format
Reason Code	Optional reason for revocation

7.3 OCSP Profile

The NAVER BUSINESS PLATFORM CAs support OCSP, and its responses conform to the RFC 6960 standards.

The responses to OCSP requests are provided to the Authority Information Access via an OCSP responder URL. It does not respond with a "Good" value on the certificates, which have not been issued in compliance with the CA Browser Forum's Baseline Requirements.

7.3.1 Version Number(s)

The NAVER BUSINESS PLATFORM OCSP responders conform to version 1 as defined in RFC 6960. The NAVER BUSINESS PLATFORM OCSP responders may decline to respond to messages that do not comply with RFC 5019. Specifically, The NAVER BUSINESS PLATFORM OCSP responders may not include a nonce in the reply even if a nonce is provided in the request.

7.3.2 OCSP Extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency and Circumstances of Assessment

Audits on the certification service operated and managed by the NAVER BUSINESS PLATFORM are conducted at least annually.

8.2 Identity/Qualifications of Assessor

Audits for the NAVER BUSINESS PLATFORM certification service are performed by a public accounting firm possessing the following qualifications and skills:

(1) It is independent from the NAVER BUSINESS PLATFORM;
(2) It has the ability and experience to process and conduct an audit according to the criteria specified in the WebTrust or equivalent international certification audit standards;
(3) It employs individuals who have a broad knowledge of certification services such as public key infrastructure, cryptography, etc.;
(4) It is licensed by WebTrust.org in the case of a Web Trust audit.

8.3 Assessor's Relationship to Assessed Entity

Audits for the NAVER BUSINESS PLATFORM 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 the NAVER BUSINESS PLATFORM'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

The NAVER BUSINESS PLATFORM 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 the NAVER BUSINESS PLATFORM, the related systems, policies, and procedures. The NAVER BUSINESS PLATFORM will make an audit report publicly available on its website.

8.7 Self-Audits

The NAVER BUSINESS PLAFORM 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

The NAVER BUSINESS PLATFORM may charge subscribers for the management as well as the issuance and renewal of certificates.

9.1.2 Certificate Access Fees

The NAVER BUSINESS PLATFORM may charge a reasonable fee for access to its certificate databases.

9.1.3 Revocation or Status Information Access Fees

The NAVER BUSINESS PLATFORM 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

The NAVER BUSINESS PLATFORM does not charge an additional fee for accessing or viewing this CPS.

9.1.5 Refund Policy

The NAVER BUSINESS PLATFORM establishes refund policies depending on certificate types at a general and reasonable level.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

The NAVER BUSINESS PLATFORM 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 The NAVER BUSINESS PLATFORM 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 The NAVER BUSINESS PLATFORM 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 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 CPS.

9.3.3 Responsibility to Protect Confidential Information

The NAVER BUSINESS PLATFORM, 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

The NAVER BUSINESS PLATFORM follows the privacy policy posted on its website when handling personal information.

- https://certificate.naver.com

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

The NAVER BUSINESS PLATFORM and/or its business partners own the intellectual property rights in The NAVER BUSINESS PLATFORM's services, including the certificates, trademarks used in providing the services, and this CPS.

Certificates and revocation information are the exclusive property of The NAVER BUSINESS PLATFORM.

The NAVER BUSINESS PLATFORM grants permission to reproduce and distribute certificates on a non-exclusive and royalty-free basis, provided that they are reproduced and distributed in full.

The NAVER BUSINESS PLATFORM does not allow derivative works of its Certificates or products without prior written permission.

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 CPS or in a separate agreement with a Subscriber, The NAVER BUSINESS PLATFORM does not make any representations or warranties regarding its products or services.

1. The NAVER BUSINESS PLATFORM complies, in all material aspects, with this CPS,

2. The NAVER BUSINESS PLATFORM publishes and updates CRLs and OCSP respond on a regular basis,

3. All certificates issued under this CPS will be verified in accordance with this CPS and meet the minimum requirements found herein and in the baseline requirement, and

4. The NAVER BUSINESS PLATFORM will maintain a repository of public information on its website.

9.6.2 RA Representations and Warranties

RA represents and warrants that:

1. The RA's certificate issuance and management services conform to the NAVER BUSINESS PLATFORM CP and this CPS.

2. Information provided by the RA does not contain any false or misleading information,

3. Translations performed by the RA and an accurate translation of the original information, and

4. All certificates requested by the RA meet the requirements of this CPS

9.6.3 Subscriber Representations and Warranties

The NAVER BUSINESS PLATFORM require, 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, The NAVER BUSINESS PLATFORM obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the CA, or

2. The Applicant's acknowledgement of the Terms of Use.

The NAVER BUSINESS PLATFORM implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant.

In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. The NAVER BUSINESS PLATFORM may use an electronic or "click-through" Agreement provided that the CA 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

50

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 CPS; (b) they have verified both the relevant The NAVER BUSINESS PLATFORM 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 The NAVER BUSINESS PLATFORM'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 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 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 CPS, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE."

TO THE MAXIMUM EXTENT PERMITTED BY LAW, NAVER BUSINESS PLATFORM 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 BUSINESS PLATFORM, THE CRL, AND ANY PARTICIPANT'S OR THIRD PARTY'S PARTICIPATION IN THE NAVER BUSINESS PLATFORM PKI, INCLUDING USE OF KEY PAIRS, CERTIFICATES, THE CRL OR ANY OTHER GOODS OR SERVICES PROVIDED BY NAVER BUSINESS PLATFORM TO THE PARTICIPANT.

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

The NAVER BUSINESS PLATFORM 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 The NAVER BUSINESS PLATFORM's services.

9.8 Limitations of Liability

TO THE EXTENT PERMITTED BY APPLICABLE LAW, THE NAVER BUSINESS PLATFORM 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. THE NAVER BUSINESS PLATFORM'S AGGREGATE LIABILITY UNDER THIS CPS IS LIMITED TO $500.

9.9 Indemnities

9.9.1 By Subscriber

To the extent permitted by law, each Subscriber shall indemnify The NAVER BUSINESS PLATFORM, 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 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 The NAVER BUSINESS PLATFORM, 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 The NAVER BUSINESS PLATFORM or its affiliates and used by the Relying Party, this 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 CPS becomes effective from the time set forth in this document after publication in the repository (website). Amendments to this CPS take effect after publication in the repository.

9.10.2 Termination

This 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 CPS, this 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

The NAVER BUSINESS PLATFORM may revise and change this 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. The NAVER BUSINESS PLATFORM may publish all the modified versions of the CPS on the website.

9.12.2 Notification Mechanism and Period

The NAVER BUSINESS PLATFORM may use the website or other effective methods to notify the major relying parties of changes in the CPS if necessary.

9.12.3 Circumstances Under Which OID Must be Changed

The NAVER BUSINESS PLATFORM is solely responsible for determining whether an amendment to the CPS requires an OID change.

9.13 Dispute Resolution Provisions

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

9.14 Governing Law

No stipulation

9.15 Compliance with Applicable Law

This CPS is subject to all applicable laws and regulations.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

The NAVER BUSINESS PLATFORM contractually obligates each RA to comply with this CPS and applicable industry guidelines. The NAVER BUSINESS PLATFORM also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2 Assignment

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

9.16.3 Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable. Each provision of this 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.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

The NAVER BUSINESS PLATFORM may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. The NAVER BUSINESS PLATFORM failure to enforce a provision of this CPS does not waive The NAVER BUSINESS PLATFORM right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective,

waivers must be in writing and signed by The NAVER BUSINESS PLATFORM.

9.16.5 Force Majeure

The NAVER BUSINESS PLATFORM is not liable for any delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by an occurrence beyond The NAVER BUSINESS PLATFORM reasonable control. The operation of the Internet is beyond The NAVER BUSINESS PLATFORM's reasonable control.

9.17 Other Provisions

No stipulation.

APPENDIX A : CERTIFICATE PROFILES

Root CA Certificate

Version	V3	
Serial Number	01 94 30 1e a2 0b dd f5 c5 33 2a b1 43 44 71 f8 d6 50 4d 0d	
Signature Algorithm	sha384RSA	
Issuer	CN	NAVER Global Root Certification Authority
	O	NAVER BUSINESS PLATFORM Corp.
	C	KR
Validity	20 years	
Subject	CN	NAVER Global Root Certification Authority
	O	NAVER BUSINESS PLATFORM Corp.
	C	KR
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	
Basic Constraints	Subject Type=CA Path Length Constraint=None	

CA Certificate

Version	V3	
Serial Number	06 04 62 33 a5 82 55 76 a4 82 72 69 47 18 a8 00 0f 2f 00 0d	
Signature Algorithm	sha256RSA	
Issuer	CN	NAVER Global Root Certification Authority
	O	NAVER BUSINESS PLATFORM Corp.
	C	KR
Validity	10 years	
Subject	CN	NAVER Secure Certification Authority 1
	O	NAVER BUSINESS PLATFORM Corp.
	C	KR
Authority Key Identifier	KeyID=d2 9f 88 df a1 cd 2c bd ec f5 3b 01 01 93 33 27 b2 eb 60 4b	
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	
Basic Constraints	Subject Type=CA Path Length Constraint=0	
Certificate Policy	[1]Certificate Policy: Policy Identifier=1.2.410.200081.2.1.1	

CRL Distribution Points	[1]CRL Distribution Point
	    Distribution Point Name:
	        Full Name:
	            URL=http://rca.navercorp.com/arl/Arl1Dp1.crl	

Authority Information Access	[1]Authority Info Access
	    Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
	    Alternative Name:
	        URL=http://ocsp-rca.navercorp.com/ocsp
	[2]Authority Info Access
	    Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	    Alternative Name:
	        URL=http://rca.navercorp.com/cert/naverrca1.der	

Domain Validation Subscriber Certificate

Version	V3	
Serial Number		
Signature Algorithm	sha256RSA	
Issuer	CN	NAVER Secure Certification Authority 1
	O	NAVER BUSINESS PLATFORM Corp.
	C	KR
Validity	1 year / 2 years	
Subject	CN	Common name
Authority Key Identifier	KeyID=e9 f9 eb 97 be 21 f2 54 c7 e9 26 37 02 39 ba fc b1 9b 0c e9	
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	
Key Usage	Digital Signature, Key Encipherment (a0)	
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	

Certificate Policy	[1]Certificate Policy:
	    Policy Identifier=2.23.140.1.2.1
	[2]Certificate Policy:
	    Policy Identifier=1.2.410.200081.2.2.3.1	

Subject Alternative Name	DNS Name=Domain Name 1 DNS Name=Domain Name 2 DNS Name=Domain Name 3 …	

CRL Distribution Points	[1]CRL Distribution Point
	    Distribution Point Name:
	        Full Name:
	            URL=http://ica.navercorp.com/crl/Crl1p1Dp1.crl	

Authority Information Access	[1]Authority Info Access
	    Access Method=On-line Certificate Status Protocol
	(1.3.6.1.5.5.7.48.1)
	    Alternative Name:
	        URL=http://ocsp-ica.navercorp.com/ocsp
	[2]Authority Info Access
	    Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	    Alternative Name:
	        URL=http://ica.navercorp.com/cert/naverica1.der	

Organization Validation Subscriber Certificate

Version	V3	
Serial Number		
Signature Algorithm	sha256RSA	
Issuer	CN	NAVER Secure Certification Authority 1
	O	NAVER BUSINESS PLATFORM Corp.
	C	KR
Validity	1 year / 2 years	
Subject	CN	common name
	OU	organizational unit
	O	organization name
	L	locality
	S	state or province
	C	country code
Authority Key Identifier	KeyID=e9 f9 eb 97 be 21 f2 54 c7 e9 26 37 02 39 ba fc b1 9b 0c e9	
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	
Key Usage	Digital Signature, Key Encipherment (a0)	
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	

Certificate Policy	[1]Certificate Policy:
	    Policy Identifier=2.23.140.1.2.2
	[2]Certificate Policy:
	    Policy Identifier=1.2.410.200081.2.2.3.2	

Subject Alternative Name	DNS Name=Domain Name 1 DNS Name=Domain Name 2 DNS Name=Domain Name 3 ...

CRL Distribution Points	[1]CRL Distribution Point
	    Distribution Point Name:
	        Full Name:
	            URL=http://ica.navercorp.com/crl/Crl1p1Dp1.crl

Authority Information Access	[1]Authority Info Access
	    Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
	    Alternative Name:
	        URL=http://ocsp-ica.navercorp.com/ocsp
	[2]Authority Info Access
	    Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	    Alternative Name:
	        URL=http://ica.navercorp.com/cert/naverica1.der