# NAVER BUSINESS PLATFORM Corp. Certification Practice Statement

v1.0

# 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.

## 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

### 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

The NAVER BUSINESS PLATFORM CA can issue the following certificates:

- Security Server Certificate: Server Authentication and Client Authentication

① A server certificate is a certificate that can be issued to subscribers by the NAVER BUSINESS PLATFORM CAs to validate the service domain names (Domain Validation) operated, provided, or possessed by the subscribers.

② A client certificate is a certificate that can be issued to a natural person or an organization operating a server by the NAVER BUSINESS PLATFORM CAs to verify whether it possesses a private key. In order to verify whether the private key owner is the individual or organization specified in the Subject field of an actual certificate, the NAVER BUSINESS PLATFORM CAs validate the organization information (Organization Validation).

### 1.4.2 Prohibited Certificate Uses

Not applicable.

## 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: NAVER Green Factory, 6 Buljeong-ro, Bundang-gu, Seongnam-si, Gyeonggi-do

#### 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

Not applicable.

## 2. PUBLICAION AND REPOSITORY RESPONSIBILITIES

The NAVER BUSINESS PLATFORM CAs are operated by the IT Security Team of the NAVER BUSINESS PLATFORM. Please feel free to contact dl_rootca@navercorp.com with any questions.

### 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.

- https://certificate.naver.com

## 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 pursuant to the CA Browser Forum's requirements.

## 2.4 Access Controls on Repositories

Any information related to CPS, certificate issuance, and management is publicly available on the website.

# 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.

- Country (C)
- Organization (O)
- Organizational Unit (OU)
- State or Province (S)
- Locality (L)
- Common Name (CN)
- E-mail Address

### 3.1.2 Need for Names to be Meaningful

The domain name included in the Common Name(CN) or Subject Alternative Name(SAN) attribute must identify one or more specific domains.

The NAVER BUSINESS PLATFORM may issue wildcard certificates containing an asterisk (*) for the Common Name.

### 3.1.3. Anonymity or Pseudonymity of Subscribers

The NAVER BUSINESS PLATFORM CAs do not issue certificates including anonymity.

### 3.1.4 Rules for Interpreting Various Name Forms

Not applicable.

### 3.1.5 Uniqueness of Name

Not applicable.

### 3.1.6 Recognition, Authentication, and Role of Trademarks

A certificate applicant is prohibited from infringing the intellectual property and trademark rights of others. The related intellectual property and trademark rights are validated by separate procedures held by the NAVER BUSINESS PLATFORM until a Certificate Signing Request is approved.

## 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 through a PKCS#10-formatted Certificate Signing Request or a cryptographically equivalent proof provided the applicant or applicant's proxy. However, subscriber key pairs can be generated from the NAVER BUSINESS PLATFORM CAs on behalf of an applicant.

### 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 Data Accuracy and Validity Period

The NAVER BUSINESS PLATFORM validates applicant information via a third-party agency providing reliable data. The maximum validity period of validated data is as follows.

- Legal documents: Up to 39 months
- Domain names: Up to 39 months
- Identification documents of an applicant: Up to 39 months

#### 3.2.2.2 Wildcard Domain Validation

In the case of issuing a certificate with a domain name containing a wildcard character(*), the CAs or RAs will determine if the wildcard character is in the leftmost and if the country and organization can be identified at least by its domain.

### 3.2.3 Authentication of Individual Identity

Not applicable.

### 3.2.4 Non-verified Subscriber Information

In the case that a certificate DN value includes an organizational unit(OU) value, the CAs or RAs

may use the information specified in the application or the proof submitted by an applicant.

#### 3.2.5 Validation of Authority

If a certificate contains a personal or an organization name, the CAs or RAs will conduct the following identity verification:

- In the case of an individual, a copy of personal identification card, passport, or driver's license
- In the case of an organization, a business registration certificate or a value that can be verified in a DB operated by the country being deemed reliable by the CAs
- In the case of an organization representative, use a business registration certificate, employment certificate, or a value that the RAs can confirm the identity of an applicant using the phone and/or postal information of an organization

#### 3.2.5.1 Validation of Domain Name

The NAVER BUSINESS PLATFORM must validate all the domain names to be included in a certificate in accordance with the following procedures.

- Whether or not it is issued by the RAs approved by Internet Assigned Numbers and Numbers(ICANN) or Internet Assigned Numbers Authority(IANA);
- Whether or not the domain registration information is disclosed in WHOIS and the organization name, address and name, and contact information to be included in the certificate subject information are specified;
- Whether or not it adheres to other additional validation procedures deemed necessary for the NAVER BUSINESS PLATFORM.

#### 3.2.6 Criteria for Interoperation

Not applicable.

### 3.3 Identification and Authentication for Re-Key Requests

For re-key requests, the CAs 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

Not applicable.

#### 3.3.2 Identification and Authentication for Re-Key After Revocation

Not applicable.

### 3.4 Identification and Authentication for Revocation Request

A subscriber can directly revoke certificates if they are no longer in use or if it is suspected that certificates and/or key pairs may be damaged.

The CAs 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. Prior to certificate revocation, the CAs or RAs will notify the relying parties, including the subscribers, of the certificate revocation.

## 4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

### 4.1 Certificate Application

The NAVER BUSINESS PLATFORM CAs publish the information about the issuance and management of certificates on the website so that it will be available to any person at any time.

- The NAVER SSL Certificate is a certificate containing its domain name in the subject DN value of a subscriber certificate.

#### 4.1.1 Who Can Submit a Certificate Application

- An applicant must submit an application containing a domain address, and the CAs or RAs will validate the submitted application and identification documents.
- The NAVER SSL 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 CAs can use such information to identify suspicious certificate requests.

#### 4.1.2 Enrollment Process and Responsibilities

An applicant for a NAVER SSL Certificate must provide the CAs or RAs with the following at a minimum:

- The identification documents of a subscriber or organization that has requested a certificate subject;

• The public key to be included in a certificate if a subscriber has generated its own key pair;
• The information required to prove the ownership and control of the domain name included in a certificate;
• Any other information that the NAVER BUSINESS PLATFORM CAs or RAs determine to be necessary.

## 4.2 Certificate Application Processing

The CAs or RAs validate the accuracy of the information provided by an applicant through the following:

• 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).
• If the NAVER BUSINESS PLATFORM has provided the issuance of a key pair, the CAs can generate an asymmetric key pair on behalf of an applicant.

### 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 does not check the Certificate Authority Authorization(CCA) DNS resource records for certificate application processing.

## 4.3 Certificate Issuance

### 4.3.1 CA Actions During Certificate Issuance

Prior to issuing a new certificate, the CAs verify the information of a new certificate application as follows:

- Confirming the uniqueness of the public key information submitted by the certificate applicant;
- Confirming the DN value and key extension submitted by the certificate applicant;
- Confirming the identification document according to the validation procedures of the certificate product requested by the certificate applicant.

### 4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

The CAs will send an e-mail notifying the issuance of a certificate to the e-mail address submitted by a subscriber upon request.

## 4.4 Certificate Acceptance

The subscribers can download certificates from the NAVER BUSINESS PLATFORM website via the website link contained in the e-mail specified in Section 4.3.2.

The subscribers who download certificates must fulfill the responsibilities and obligations imposed by the CPS and the NAVER SSL Service Agreement.

### 4.4.1 Conduct Constituting Certificate Acceptance

The subscribers can access the NAVER BUSINESS PLATFORM website and download certificates via the site link included in their e-mail.

### 4.4.2 Publication of the Certificate by the CA

Not applicable.

### 4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

### 4.5 Key Pair and Certificate Usage

The subscribers can only use certificates and private keys for applications that conform to the extended key usage purposes specified in the certificates. The subscribers must discontinue using

the certificates or private keys after revocation or expiration of the certificates.

#### 4.5.1 Subscriber Private Key and Certificate Usage

Not applicable.

#### 4.5.2 Relying Party Public Key and Certificate Usage

Not applicable.

### 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

Certificate renewal requests follow the same procedures used when issuing a new certificate.

#### 4.6.3 Processing Certificate Renewal Requests

Certificate renewal requests follow the same procedures used when issuing a new certificate.

#### 4.6.4 Notification of New Certificate Issuance to Subscriber

Certificate renewal requests follow the same procedures used when issuing a new certificate.

#### 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Certificate renewal requests follow the same procedures used when issuing a new certificate.

#### 4.6.6 Publication of the Renewal Certificate by the CA

Certificate renewal requests follow the same procedures used when issuing a new certificate.

#### 4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Certificate renewal requests follow the same procedures used when issuing a new certificate.

### 4.7 Certificate Re-Key

Certificate reissuance is the process whereby a new certificate is created without updating a validity period by changing a key pair.

#### 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 CAs 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

Certificate reissuance can be conducted by the CAs or requested by a subscriber.

#### 4.7.3 Processing Certificate Re-Keying Requests

Certificate reissuance follows the same procedures used when issuing a new certificate.

#### 4.7.4 Notification of New Certificate Issuance to Subscriber

Certificate reissuance follows the same procedures used when issuing a new certificate.

#### 4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Certificate reissuance follows the same procedures used when issuing a new certificate.

#### 4.7.6 Publication of the Re-Keyed Certificate by the CA

Certificate reissuance follows the same procedures used when issuing a new certificate.

#### 4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Certificate reissuance follows the same procedures used when issuing a new certificate.

### 4.8 Certificate Modification

The NAVER BUSINESS PLATFORM does not modify previously issued certificates. It will be separated and treated as a new certificate issuance or certificate reissuance request according to the information requested by a subscriber.

#### 4.8.1 Circumstances for Certificate Modification

Not applicable.

#### 4.8.2 Who May Request Certificate Modification

Not applicable.

#### 4.8.3 Processing Certificate Modification Requests

Not applicable.

#### 4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

#### 4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

#### 4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

#### 4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

## 4.9 Certificate Revocation and Suspension

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

The NAVER BUSINESS PLATFORM will revoke a subscriber certificate if any of the following occurs:

- The NAVER BUSINESS PLATFORM stops operating;
- A NAVER BUSINESS PLATFORM CA Certificate is revoked;
- The private key of the NAVER BUSINESS PLATFORM CA is stolen, disclosed in a fraudulent manner, or compromised;
- The private key associated with the public key contained in a subscriber certificate or the medium keeping a private key is stolen, leaked, or suspected of such.

#### 4.9.2 Who Can Request Revocation

The subscribers can make requests for the revocation of their certificates.

- A subscriber or its representative who performs a certificate issuance request;
- Anyone in possession of, or with access to, the private key corresponding to the public key indicated in a certificate;
- Anyone who provides the proof of the ownership or control of a certificate;
- Anyone who has been authorized to revoke certificates by the NAVER BUSINESS PLATFORM.

#### 4.9.3 Procedure for Revocation Request

The NAVER BUSINESS PLATFORM performs the revocation of all certificates. To revoke one directly, a subscriber will request via the website. If a request is related to damage of a subscriber's private key, the requestor should contact dl_rootca@navercorp.com. All the certificate revocation requests must include a specific reason (such as suspicion of private key hacking).

### 4.9.4 Revocation Request Grace Period

Not applicable.

### 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.
- When a subscriber certificate expires, the certificate is terminated.

### 4.9.6 Revocation Checking Requirements for Relying Parties

The relying parties are required to verify the validity of an applicable certificate through the CRL before using the 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 2560 and/or RFC 5019.
- The NAVER BUSINESS PLATFORM issues a separate certificate for being signed by an OCSP

response. A certificate signed by an OCSP responder contains an extension of the id-pkix-ocsp-nocheck type, as defined by the RFC2560.

#### 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

The NAVER BUSINESS PLATFORM maintains and manages the CRL repository used for verifying

certificate revocation validity.

#### 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

Not applicable.

### 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.

## 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

The minimum number of people to perform the Trusted Roles is as follows:

- At least two people accompany each other and perform the operation and management of the CA system server.
- The CA key pair generation task must be performed by the personnel required by the internal key generation procedures, and at least two people should conduct the hardware security module activation.

### 5.2.3 Identification and Authentication for Each Role

The NAVER BUSINESS PLATFORM documents and manages that certain tasks of the Trusted Roles cannot be performed by the same person.

### 5.2.4 Roles Requiring Separation of Duties

The NAVER BUSINESS PLATFORM separates the Trusted Roles to ensure the stability and reliability of certification tasks.

## 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

Not applicable.

### 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

### 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

Not applicable.

### 5.4.6 Audit Collection System (Internal vs. External)

Not applicable.

### 5.4.7 Notification to Event-Causing Subject

Not applicable.

### 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)

Not applicable.

#### 5.5.7 Procedures to Obtain and Verify Archive Information

Not applicable.

### 5.6 Key Changeover

The same procedures as issuing an initial CA certificate are applied in the case that a new CA certificate is provided due to CA key pair reissuance.

### 5.7 Compromise and Disaster Recovery

#### 5.7.1 Incident and Compromise Handling Procedures

The NAVER BUSINESS PLATFORM uses the dual-installed system resources and software to recover upon system resource and/or software failures.

#### 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 CAs 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.

The subscribers may submit a public key and a certificate request signed by a private key to the NAVER BUSINESS PLATFORM after the subscribers generate the public key and private key in a manner authorized by the NAVER BUSINESS PLATFORM. Also, the subscribers can obtain a public key, a private key, and a certificate request signed by the private key, which is generated through the website provided by the NAVER BUSINESS PLATFORM.

### 6.1.2 Private Key Delivery to Subscriber

If applicable, the NAVER BUSINESS PLATFORM delivers it to a subscriber in a secure manner in accordance with the related procedures for transferring confidential information.

### 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

The key length of the Root CA operated by the NAVER BUSINESS PLATFORM is RSA 4096 bits. The subscriber certificate key length is 2048 bits.

#### 6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable.

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

Subscriber certificates should be used in accordance with the key usage purposes. The purposes of the key usage are specified in the Subscriber Certificate Extension Key Usage field.

### 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 securely archives CA private keys at a location distinct from the main system operation site. Subscriber private keys are not archived.

### 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

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

### 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. NAVER SSL Certificate validity period can be set to (1) year or two (2) years upon subscription by a subscriber.

## 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

Not applicable.

#### 6.4.2 Activation Data Protection

Not applicable.

#### 6.4.3 Other Aspects of Activation Data

Not applicable.

## 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

Not applicable.

## 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

Not applicable.

## 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-Stamping 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

#### 7.1.2.1 Root CA Certificate

The NAVER BUSINESS PLATFORM issues Root CA certificates as follows:

- CN = NAVER Global Root Certification Authority, O = NAVER BUSINESS PLATFORM Corp., C = KR

#### 7.1.2.2 CA Certificate

The NAVER BUSINESS PLATFORM issues subordinate CA certificates as follows:

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

#### 7.1.2.3 CA Browser Forum's Requirements for Certificate Extension Field

The subscriber certificate extension fields issued by the NAVER BUSINESS PLATFORM comply

with the CA Browser Forum's Baseline Requirements. Subscriber certificates as follows are issued.

- Domain Validation: NAVER Secure SSL Certificate
- Organization Validation: NAVER Secure Pro, NAVER Secure Multi, NAVER Secure Wildcard SSL Certificate

#### 7.1.2.4 Other Certificates

The NAVER BUSINESS PLATFORM may issue the following certificates to use the CA system. These certificates are not issued to subscribers and are issued only to the personnel approved by the NAVER BUSINESS PLATFORM through the internal issuance process.

- CA Administrator Certificates
- RA Administrator Certificates
- OCSP Signature Certificates
- Internal Auditor Certificates

### 7.1.3 Algorithm Object Identifiers

The NAVER BUSINESS PLATFORM does not issue any CA or subscriber certificates using the SHA-1 hash algorithm.

### 7.1.4 Name Forms

#### 7.1.4.1 Issuer Information

The contents of the Certificate Issuer field are consistent with a CA certificate DN as specified in Section 7.1.2.2 of this document in accordance with the RFC 5280 standards.

#### 7.1.4.2 Subject Information

The Subject field value of the subscriber certificates issued by the NAVER BUSINESS PLATFORM has the following Distinguished Name system.

- Common Name (CN): Name of the domain for which a subscriber requested
- Organization (O): Name of the organization to which a subscriber belongs
- Organization Unit (OU): Organization details (eg_ministry names)
- State or Province (S): Address of the organization to which a subscriber belongs (eg_Seoul)
- Location (L): Address of the organization to which a subscriber belongs (eg_Gangnam-gu)

#### 7.1.5 Name Constraints

Not applicable.

#### 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 in Section 1.2.

- certificatePolicies.policyIdentifiers: 1.2.410.200081.2.1.1

The policy identifiers assigned under the CA Browser Forum are also used for Domain Validation and Organization Validation SSL Certificates.

#### 7.1.7 Usage of Policy Constraints Extension

The Policy Constraint Extension field shall be empty.

#### 7.1.8 Policy Qualifiers Syntax and Semantics

Not applicable.

#### 7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

### 7.2 CRL Profile

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

#### 7.2.1 Version Number(s)

Not applicable.

#### 7.2.2 CRL and CRL Entry Extensions

Not applicable.

### 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)

Not applicable.

#### 7.3.2 OCSP Extensions

Not applicable.

# 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.

# 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

Not applicable.

#### 9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

### 9.3 Confidentiality of Business Information

Not applicable.

#### 9.3.1 Scope of Confidential Information

Not applicable.

#### 9.3.2 Information Not Within the Scope of Confidential Information

Not applicable.

#### 9.3.3 Responsibility to Protect Confidential Information

Not applicable.

## 9.4 Privacy of Personal Information

The NAVER BUSINESS PLATFORM publishes its Privacy Statement on its website, which is at:

- https://certificate.naver.com/

### 9.4.1 Privacy Plan

Not applicable.

### 9.4.2 Information Treated as Private

Not applicable.

### 9.4.3 Information Not Deemed Private

Not applicable.

### 9.4.4 Responsibility to Protect Private Information

Not applicable.

### 9.4.5 Notice and Consent to Use Private Information

Not applicable.

### 9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Not applicable.

### 9.4.7 Other Information Disclosure Circumstances

Not applicable.

### 9.5 Intellectual Property rights

Not applicable.

## 9.6 Representations and Warranties

### 9.6.1 CA Representations and Warranties

#### 9.6.1.1 Limited Warranty

Not applicable.

#### 9.6.1.2 CABF Warranties and Obligations

Not applicable.

### 9.6.2 RA Representations and Warranties

Not applicable.

### 9.6.3 Subscriber Representations and Warranties

Not applicable.

### 9.6.4 Relying Party Representations and Warranties

Not applicable.

### 9.6.5 Representations and Warranties of Other Participants

Not applicable.

## 9.7 Disclaimers of Warranties

Not applicable.

## 9.8 Limitations of Liability

Not applicable.

## 9.9 Indemnities

### 9.9.1 By Subscriber

Not applicable.

### 9.9.2 By Relying Parties

Not applicable.

## 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

Not applicable.

### 9.13 Dispute Resolution Provisions

Not applicable.

### 9.14 Governing Law

Not applicable.

### 9.15 Compliance with Applicable Law

Not applicable.

### 9.16 Miscellaneous Provisions

Not applicable.

#### 9.16.1 Entire Agreement

Not applicable.

#### 9.16.2 Assignment

Not applicable.

#### 9.16.3 Severability

Not applicable.

### 9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

Not applicable.

### 9.16.5 Force Majeure

Not applicable.

## 9.17 Other Provisions

Not applicable.