CA Owner Name: NAVER BUSINESS PLATFORM Corp.

**-- General information about CA's associated organization --**

|  |  |
| --- | --- |
| CA Email Alias 1 | *hanyong.park@navercorp.com* |
| CA Email Alias 2 | *dl\_rootca@navercorp.com* |
| Company Website | <https://certificate.naver.com> |
| Organizational Type | Private Corporation |
| Geographic Focus | The Republic of Korea (South Korea) |
| Primary Market / Customer Base | NAVER BUSINESS PLATFORM is a commercial CA that will provide certificates to customers who are users of the web portal and other services provided by NAVER Corporation over the World. We will offer both server authentication and client authentication.  |
| Impact to Mozilla Users:  | The portal and other services we provided should be equally adjusted at any mainstream browsers especially Firefox. |

**-- Required and Recommended Practices --**

Recommended Practices: https://wiki.mozilla.org/CA/Required\_or\_Recommended\_Practices

|  |  |
| --- | --- |
| Do You, as an official representative of this CA agree to the following Recommended Practices Statement? | I have reviewed Mozilla's lists of Required and Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below. |

CA's Response to Recommended Practices:

*CAs response to each of the items listed in https://wiki.mozilla.org/CA/Required\_or\_Recommended\_Practices*

|  |  |
| --- | --- |
| Publicly Available CP and CPS | Yes. We published our CPS and its English version on the official website.CPS (Korean): https://certificate.naver.com/bbs/initCrtfcJob.doCPS (English): https://certificate.naver.com/bbs/initCrtfcJob.do |
| Audit Criteria | WebTrustRefer to CPS section 8.1, 8.2, 8.3 and 8.4. |
| Revocation of Compromised Certificates | Yes. Our CA system can revoke compromised and/or suspicious certificates. Refer to CPS section 3.4 and 4.9.1. |
| Verifying Domain Name Ownership | Yes. We verify a user email is one of email addresses listed in the "registrant", "technical", or "administrative" WHOIS records and a selected whitelist of local addresses, which are limited to local-parts of "admin", "administrator", "webmaster", "hostmaster", and "postmaster". We will verify the email address by sending an email including a random value which is complied with CA/BF BRs.Refer to CPS section 3.2.5.1 and 4.1.1.  |
| Verifying Email Address Control | Yes. We verify user emails via challenge-response.Refer to CPS section 4.4. |
| DNS names go in SAN | Required. |
| OCSP | Yes. We provide http OCSP responders.Refer to CPS section 4.9.9.  |
| Network Security Controls | Yes. We have completed the WebTrust for SSL audit.Refer to CPS section 6.7 |

**-- Forbidden and Potentially Problematic Practices --**

Potentially Problematic Practices: https://wiki.mozilla.org/CA/Forbidden\_or\_Problematic\_Practices

|  |  |
| --- | --- |
| Do You, as an official representative of this CA agree to the following Problematic Practices Statement? | I have reviewed Mozilla's lists of Forbidden and Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below. |

CA's Response to Problematic Practice:

*CA's response to each of the items listed in https://wiki.mozilla.org/CA/Forbidden\_or\_Problematic\_Practices*

|  |  |
| --- | --- |
| Long-lived Certificates | Our certificates maximum lifetime is 24 months. |
| Non-Standard Email Address Prefixes for Domain Ownership Validation | Only email addresses listed in the "registrant", "technical", or "administrative" WHOIS records and a selected whitelist of local addresses, which are limited to local-parts of "admin", "administrator", "webmaster", "hostmaster", and "postmaster" are verified and approved.  |
| Issuing End Entity Certificates Directly From Roots | Our Root CA doesn’t issue any certificates to End Entities.  |
| Distributing Generated Private Keys in PKCS#12 Files | We provide PEM files.  |
| Certificates Referencing Local Names or Private IP Addresses | We don’t issue any certificates including Local Names or Private IP Addresses.  |
| Issuing SSL Certificates for .int Domains | We don’t issue any certificates for .int domains.  |
| OCSP Responses Signed by a Certificate Under a Different Root | Our OCSP certificates are under the same Root.  |
| Issuance of SHA-1 Certificates | We don’t issue SHA-1 certificates.  |
| Delegation of Domain / Email Validation to Third Parties | We don’t allow third party for delegation of domain / email validation.  |
| Allowing External Entities to Operate Subordinate CAs | We don’t have external entities to operate subordinate CAs.  |
| Generic Names for CAs | Our CA names are sufficiently unique to allow relatively straightforward identification of the CA. |

**- Policies and Practices -**

|  |  |
| --- | --- |
| Policy Documentation | Korean |
| CA Document Repository | List of Root and Sub-CA certificate: <https://certificate.naver.com/bbs/certificateList.do>CPS: <https://certificate.naver.com/bbs/initCrtfcJob.do>Terms of Use:<https://certificate.naver.com/bbs/initGuidePolicy.do> |
|  |  |
| CP | N/A. We don’t have a CP. |
| CPS: | Korean and English CPS documents:<https://certificate.naver.com/bbs/initCrtfcJob.do> |
| Other Relevant Documents | Service Terms of Use (Korean): <https://certificate.naver.com/bbs/initGuidePolicy.do> |
| Auditor Name | Deloitte Korea |
| Auditor Website | <https://www2.deloitte.com/kr/en.html> |
| Auditor Qualifications | <http://www.webtrust.org/licensed-webtrust-practitioners-international/item64419.aspx> |
| Standard Audit URL | <https://cert.webtrust.org/ViewSeal?id=2380> |
| Standard Audit Type | WebTrust - Trust Services Principles and Criteria for Certification Authorities v 2.0 |
| Standard Audit Statement Date | 26 December, 2017 |
| BR Audit URL | <https://cert.webtrust.org/ViewSeal?id=2379> |
| BR Audit Type | WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2 |
| BR Audit Statement Date | 26 December, 2017 |
| EV SSL Audit URL | N/A |
| EV SSL Audit Type | N/A |
| EV SSL Audit Statement Date | N/A  |
| BR Commitment to Comply | Refer to CPS section 2.3 and 7.1. |
| BR Self Assessment | The BR Self-Assessment document will be attached to the Bugzilla Bug.  |
| SSL Verification Procedures | NAVER BUSINESS PLATFORM CA verifies domain authorization or control using either (1) Confirming g the Applicant's control over the FQDN by sending a Random Value via email. The Random Value MUST be sent to an email address identified as a Domain Contact that means The Domain Name Registrant, technical contact, or administrative contract as listed in the WHOIS record of the Base Domain Name. The Random Value SHALL be unique in each email. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. Or (2) Confirm the Applicant's control over the FQDN by (i) sending an email to one or more addresses created byusing 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the atsign("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii)receiving a confirming response utilizing the Random Value.Refer to CPS section 3.2.5.1 and 4.3.2. |
| EV SSL Verification Procedures | N/A |
| Organization Verification Procedures | Refer to CPS section 3.2.2, 3.2.2.1 and 3.2.5.  |
| Email Address Verification Procedures | N/A |
| Multi-Factor Authentication | 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.Refer to CPS section 6.5. |
| Network Security | Refer to CPS section 6.7. |

**-- Technical Information about each Root Certificate --**

***Provide the following information for each root cert for which you are requesting inclusion or change.***

**-- Root Certificate #1  --**

|  |  |
| --- | --- |
| Root Certificate Name | NAVER Global Root Certification Authority |

**- Certificate Data -**

|  |  |
| --- | --- |
| Root Certificate Download URL:  | <https://certificate.naver.com/cmmn/fileDown.do?atch_file_path=CERTILIST&atch_file_nm=1c3763b33dbf457d8672371567fd1a12.crt&atch_real_file_nm=naverrca1.crt> |
| Certificate Issuer Common Name | NAVER Global Root Certification Authority |
| O From Issuer Field | NAVER BUSINESS PLATFORM Corp. |
| OU From Issuer Field | N/A |
| SHA-256 Fingerprint | 88:F4:38:DC:F8:FF:D1:FA:8F:42:91:15:FF:E5:F8:2A:E1:E0:6E:0C:70:C3:75:FA:AD:71:7B:34:A4:9E:72:65 |
| CRL URL(s) | Sub-CA CRL: <http://rca.navercorp.com/arl/Arl1Dp1.crl>Subscriber certs CRL:<http://ica.navercorp.com/crl/Crl1p1Dp1.crl>Refer to CPS section 2.3, 4.9, 4.9.5, 4.9.6, 4.9.7 and 4.9.8. |
| OCSP URL(s) | Sub-CA AIA:<http://ocsp-rca.navercorp.com/ocsp>Subscriber certs AIA:<http://ocsp-ica.navercorp.com/ocsp>Refer to CPS section 4.9.9 and 4.9.10.  |
| Mozilla Trust Bits | Websites    |
| SSL Validation Type | DV; OV |
| Mozilla EV Policy OID(s) | Not requesting EV for this Root |
| Root Stores Included In | Microsoft (ongoing) |
| Mozilla Applied Constraints | This Root doesn’t have any name constraints.  |

**- Test Websites or Example Cert -**

|  |  |
| --- | --- |
| Test Website - Valid | <https://test-certificate.naver.com/> |
| Test Website - Expired | <https://test2-certificate.naver.com> |
| Test Website - Revoked | <https://test1-certificate.naver.com> |
| Example Cert:    | N/A |

**- CA Hierarchy Information –**

|  |  |
| --- | --- |
| CA Hierarchy: | NAVER Global Root Certification Authority currently has the following internally-operated intermediate CA. - NAVER Secure Certification Authority 1 |
| Externally Operated SubCAs: | There are currently no externally operated subCAs issued from this Root. |
| Cross Signing: | This Root has not been cross-signed by any other CAs. |
| Technical Constraint on 3rd party Issuer: | This Root doesn’t have technical constraints on 3rd party issuer.  |

**-- End Root Certificate #1 --**