Print this page

Mozilla - CA Program

Case Information

Case Number	00000261	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	NAVER Business Platform, Corp. (NBP)	**Request Status**	Information Verification In Process

Additional Case Information

Subject	Include NAVER root certificate	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1404221

General information about CA's associated organization

CA Email Alias 1	dl_rootca@navercorp.com		
CA Email Alias 2			
Company Website	https://certificate.naver.com/	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	South Korea	**Verified?**	Verified
Primary Market / Customer Base	Commercial CA offering server and client authentication certs.	**Verified?**	Verified
Impact to Mozilla Users	This appears to be a new CA planning to provide TLS/SSL certs to the general public.	**Verified?**	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA/Required_or_Recommended_Practices	**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	1. Publicly Available CP and CPS: CPS section 2.2 1.1 Revision Table, updated annually: No revision table found. NEED: https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#CP.2FCPS_Revision_Table 1.2 CAA Domains listed in CP/CPS: Not found. NEED: https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#CAA_Domains_listed_in_CP.2FCPS 2. Audit Criteria: CPS section 8 3. Revocation of Compromised Certificates: CPS section 4.9.1 NEED: See section 4.9.1.1 of the BRs. 4. Verifying Domain Name Ownership: CPS sections 3.2.5.1 and 4.1.1 5. Verifying Email Address Control: N/A 6. DNS names go in SAN: Not clear NEED: CPS section 3.1.2 says: "The domain name to be included in the CN *or* SAN. 7. OCSP: CPS section 4.9.9 8. Network Security Controls: CPS section 6.7	**Verified?**	Need Response From CA

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices	**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 Practices	1. Long-lived Certificates: Not found in CPS NEED: See sections 4.2.1 and 6.3.2 of the BRs 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: No 3. Issuing End Entity Certificates Directly From Roots: CPS section 1.3.2 4. Distributing Generated Private Keys in PKCS#12 Files: NEED: CPS section 4.2 looks like NAVER may provide the key pair. 5. Certificates Referencing Local Names or Private IP Addresses: No 6. Issuing SSL Certificates for .int Domains: No 7. OCSP Responses Signed by a Certificate Under a Different Root: No 8. Issuance of SHA-1 Certificates: No 9. Delegation of Domain / Email Validation to Third Parties: No	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	NAVER Global Root Certification Authority	**Root Case No**	R00000514
Request Status	Information Verification In Process	**Case Number**	00000261

Certificate Data

Certificate Issuer Common Name	NAVER Global Root Certification Authority
O From Issuer Field	NAVER BUSINESS PLATFORM Corp.
OU From Issuer Field	
Valid From	2017 Aug 18
Valid To	2037 Aug 18
Certificate Serial Number	0194301ea20bddf5c5332ab1434471f8d6504d0d
Subject	CN=NAVER Global Root Certification Authority, OU=null, O=NAVER BUSINESS PLATFORM Corp., C=KR
Signature Hash Algorithm	sha384WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	8F:6B:F2:A9:27:4A:DA:14:A0:C4:F4:8E:61:27:F9:C0:1E:78:5D:D1
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
Certificate ID	B2:07:0F:FA:C9:FF:38:61:18:68:D4:9E:93:5F:ED:AE:E5:13:B7:96:25:68:F3:DE:01:EA:D0:5E:0A:0D:30:27
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	NEED: It appears that this root inclusion request is mostly in support of NAVER's portal; i.e. one website. So it is not clear why this root needs to be directly included, and why NAVER does not get an SSL cert chaining up to an already included CA.	**Verified?**	Need Response From CA
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8979809	**Verified?**	Verified
CRL URL(s)	http://rca.navercorp.com/arl/Arl1Dp1.crl http://ica.navercorp.com/crl/Crl1p1Dp1.crl CPS section 4.9.7: valid for 7 days	**Verified?**	Verified
OCSP URL(s)	http://ocsp-rca.navercorp.com/ocsp http://ocsp-ica.navercorp.com/ocsp CPS section 4.9.10: valid up to 10 days	**Verified?**	Verified

Mozilla Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
Mozilla EV Policy OID(s)	Not EV	**Verified?**	Verified
Root Stores Included In		**Verified?**	Verified
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs.	**Verified?**	Need Response From CA

Test Websites or Example Cert

Test Website - Valid	https://test-certificate.naver.com	**Verified?**	Need Response From CA
Test Website - Expired	https://test2-certificate.naver.com		
Test Website - Revoked	https://test1-certificate.naver.com		
Example Cert	N/A		
Test Notes	NEED: The valid test site fails. It appears that the SSL cert on the revoked test site is not revoked and in the CRL.		

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	NEED to resolve all errors: https://certificate.revocationcheck.com/test-certificate.naver.com - One or more certificate in this chain can't be trusted because of revocation or an server error. Revoked certificates can't be trusted and will cause errors like "NET::ERR_CERT_REVOKED" in browsers - Certificate status is 'Good' expecting 'Unknown' BRs section 4.9.10: "If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder SHOULD NOT respond with a "good" status. ... Effective 1 August 2013, OCSP responders for CAs which are not Technically Constrained in line with Section 7.1.5 MUST NOT respond with a "good" status for such certificates."	**Verified?**	Need Response From CA
CA/Browser Forum Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the CA/Browser Forum Baseline Requirements (BRs).	**Verified?**	Need Response From CA

	BR Lint Test: https://github.com/awslabs/certlint		
Test Website Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the X.509 rules. X.509 Lint Test: https://github.com/kroeckx/x509lint	Verified?	Need Response From CA
EV Tested	N/A	Verified?	Not Applicable

CA Hierarchy Information

CA Hierarchy	This root cert signs internally-operated intermediate certs. CPS Section 1.3.1 https://certificate.naver.com/bbs/certificateList.do	Verified?	Verified
Externally Operated SubCAs	Not allowed per CPS section 1.3.1.	Verified?	Verified
Cross Signing	Not allowed per CPS section 1.3.1.	Verified?	Verified
Technical Constraint on 3rd party Issuer	CPS section 1.3.2 says: "All the RA functions will be performed by the NAVER BUSINESS PLATFORM".	Verified?	Verified

Verification Policies and Practices

Policy Documentation	CPS is provided in Korean and English.	Verified?	Verified
CA Document Repository	https://certificate.naver.com/bbs/initCrtfcJob.do	Verified?	Verified
CP Doc Language			
CP		Verified?	Not Applicable
CP Doc Language			
CPS	https://bugzilla.mozilla.org/attachment.cgi?id=8950830	Verified?	Verified
Other Relevant Documents	Terms of Use: https://certificate.naver.com/bbs/initGuidePolicy.do	Verified?	Verified
Auditor	Deloitte	Verified?	Verified
Auditor Location	Korea	Verified?	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=2380&file=pdf	Verified?	Verified
Standard Audit Type	WebTrust	Verified?	Verified
Standard Audit Statement Date	12/27/2017	Verified?	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=2379&file=pdf	Verified?	Verified
BR Audit Type	WebTrust	Verified?	Verified

BR Audit Statement Date	12/27/2017	**Verified?**	Verified
EV SSL Audit		**Verified?**	Not Applicable
EV SSL Audit Type		**Verified?**	Not Applicable
EV SSL Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CPS section 1.1	**Verified?**	Verified
BR Self Assessment	NEED: Attach BR Self Assessment (https://wiki.mozilla.org/CA/BR_Self-Assessment) to the Bugzilla Bug.	**Verified?**	Need Response From CA
SSL Verification Procedures	CPS sections 3.2.5.1 and 4.1.1. NEED: CP/CPS must clearly specify the procedures that the CA employs. Each documented procedure should state which subsection of BR section 3.2.2.4 it is complying with. I do not believe there is enough information in the CPS to determine which of the allowed Domain Validation methods in the BRs are used. https://wiki.mozilla.org/CA/Required_or_Recommended_Practices#Verifying_Domain_Name_Ownership	**Verified?**	Need Response From CA
EV SSL Verification Procedures	N/A	**Verified?**	Not Applicable
Organization Verification Procedures	CPS sections 3.2.2, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	N/A	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	N/A	**Verified?**	Not Applicable
Multi-Factor Authentication	CPS section 6.5.	**Verified?**	Verified
Network Security	CPS section 6.7	**Verified?**	Verified