salesforce.com.

Case: 00000072

Case Information

Case Number	00000072	**Case Owner**	Kathleen Wilson
CA Owner/Certificate Name	Government of Korea, Ministry of the Interior	**Case Record Type**	CA Owner/Root Inclusion Request
All Fields Verified?	No	**Request Status**	Initial Request Received

Additional Case Information

Subject	Include Korea Government Root Cert	**Date/Time Opened**	12/15/2015 3:09 PM
Case Reason	New Owner/Root inclusion requested	**Date/Time Closed**	
Case Origin		**Type**	
Status	Open	**Priority**	Medium

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1226100

General information about CA's associated organization

CA Email Alias 1			
CA Email Alias 2			
Company Website	https://www.gpki.go.kr/	**Company Website (Verified?)**	Not verified
Organizational Type	Government Agency	**Organizational Type (Verified?)**	Verified
Organizational Type (Others)		**Organizational Type Others (Verified?)**	Not Applicable
Geographic Focus	Korea	**Geographic Focus (Verified?)**	Verified
Primary Market / Customer Base	Digital certificates are issued to administration institutions and public offices of the Government of Korea	**Primary Mkt / Customer Base (Verified?)**	Verified
Impact to Mozilla Users	NEED: Why does the CA need to have their root certificate directly included in Mozilla's products, rather than being signed by another CA's root certificate that is already included in NSS? Mozilla CA certificate policy: We require that all CAs whose certificates are distributed with our software product ... provide some service relevant to typical users of our software products	**Impact to Mozilla Users (Verified?)**	Need Response From CA

Existing CA Contact Information

Contact Name		**Contact Type**	
Contact Phone		**Contact Department**	
Contact Email		**Contact Title**	

New CA Contact Information

New Contact Name	KIM, IN SOO	**New Contact Type**	Primary POC
New Contact Phone	+82-2-2031-9831	**New Contact Department**	

| **New Contact Email** | kis@klid.or.kr | **New Contact Title** | |

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of 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	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices 1) Publicly Available CP and CPS: 2) CA Hierarchy: 3) Audit Criteria: 4) Document Handling of IDNs in CP/CPS: 5) Revocation of Compromised Certificates: 6) Verifying Domain Name Ownership: 7) Verifying Email Address Control: 8) Verifying Identity of Code Signing Certificate Subscriber: Not applicable. Mozilla is no longer enabling the Code Signing trust bit for root certificates. 9) DNS names go in SAN: 10) Domain owned by a Natural Person: 11) OCSP: 12) Network Security Controls:	**CA's Reponse to Recom Prac (Verified?)**	Need Response From CA

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of 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	NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices 1) Long-lived DV certificates: 2) Wildcard DV SSL certificates: 3) Email Address Prefixes for DV Certs: 4) Delegation of Domain / Email validation to third parties: 5) Issuing end entity certificates directly from roots: 6) Allowing external entities to operate subordinate CAs: 7) Distributing generated private keys in PKCS#12 files: 8) Certificates referencing hostnames or private IP addresses: 9) Issuing SSL Certificates for Internal Domains: 10) OCSP Responses signed by a certificate under a different root: 11) SHA-1 Certificates: 12) Generic names for CAs: 13) Lack of Communication With End Users: 14) Backdating the notBefore date:	**CA's Response to Prob Prac (Verified?)**	Need Response From CA

Description Information

| **Description** | |

Internal Comments

**Comments by
Mozilla on Case**

Public Comments

Comments   Korea Local Information Research & Development Institute (KLID) provides CA services on behalf of the
                  Management of the Interior (MOI) of the Korean Government.

System Information

Created By   Kathleen Wilson, 12/15/2015 3:09 PM   Last Sync Date/Time

Last Modified By   Francis Lee, 9/7/2016 8:07 PM

Root Cases
R00000112

Root Certificate Name	**GPKIRootCA1**
Request Status	**Initial Request Received**
O From Issuer Field	**Government of Korea**
Certificate Summary	**The main purpose of the Government of Korea, Root Certificate Authority is to issue the Subordinate Certification Authorities of the GPKI**
Valid From	**8/3/2011**
Valid To	**8/3/2031**

Case History
12/15/2015 3:09 PM

User	**Kathleen Wilson**
Action	**Created.**