Mozilla - CA Program

Case Information

Case Number	00000075	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Government of Kazakhstan	**Request Status**	Need Information from CA

Additional Case Information

Subject	Included Government of Kazakhstan roots	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1232689

General information about CA's associated organization

CA Email Alias 1			
CA Email Alias 2			
Company Website	http://pki.gov.kz/index.php/en	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Kazakhstan	**Verified?**	Verified
Primary Market / Customer Base	E-government, government, legal entities, individuals. All services provided free of charge for citizens of the Republic of Kazakhstan	**Verified?**	Verified
Impact to Mozilla Users	Ease of use of e-government services and interaction with executive bodies. This CA's root certificates will be encountered by individuals, legal entities, nonresidents, E-Notary and Treasury-Client information systems' users; and users of electronic government services, business systems, and email protection.	**Verified?**	Verified

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	**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	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA)	**Root Case No**	R00000104
Request Status	Need Information from CA	**Case Number**	00000075

Additional Root Case Information

Subject	Include НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA)

Technical Information about Root Certificate

O From Issuer Field	РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ»	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	Certificate is needed for creation of a common space of trust between information exchange participants in the Republic of Kazakhstan.	**Verified?**	Not Verified
Root Certificate Download URL	pki.gov.kz/cert/pki_rsa.cer	**Verified?**	Verified
Valid From	2015 Jul 27	**Verified?**	Verified
Valid To	2020 Jul 27	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	NEED: URL to a website whose SSL cert chains up to this root. Note that this can be a test site.	**Verified?**	Need Response From CA
CRL URL(s)	http://crl.pki.kz/Rsa0.crl http://crl1.pki.kz/Rsa0.crl	**Verified?**	Not Verified
OCSP URL(s)	https://ocsp.pki.kz	**Verified?**	Not Verified

Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.	**Verified?**	Need Response From CA
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	DV	**Verified?**	Verified
EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
EV Tested		**Verified?**	Not Applicable
Root Stores Included In		**Verified?**	Verified
Mozilla Applied Constraints	NEED: Please indicate the domains that the certificates in this CA hierarchy should be constrained to; e.g. to *.gov, *.mil, etc.	**Verified?**	Need Response From CA

Digital Fingerprint Information

SHA-1 Fingerprint	9F:9D:6D:43:84:5D:DC:6C:EC:6C:60:06:A6:C8:52:4B:12:3F:67:D0	**Verified?**	Verified
SHA-256 Fingerprint	AE:F2:F2:90:75:54:F1:22:92:CB:34:56:D5:11:00:62:E3:58:1D:0A:05:C0:F0:35:40:F8:70:F2:5D:5B:81:6C	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	NEED: A description (in English) of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. - List and/or describe all of the subordinate CAs that are signed by this root. - Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on. - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements.	**Verified?**	Need Response From CA
Externally Operated SubCAs	NEED: (in English) - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist, https://wiki.mozilla.org/CA:SubordinateCA_checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.	**Verified?**	Need Response From CA
Cross Signing	NEED: (in English) - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store	**Verified?**	Need Response From CA

	or not.		
Technical Constraint on 3rd party Issuer	NEED: (in English) CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of version 1.3 of the CA/Browser Forum's Baseline Requirements - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ - https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	Documentation is in Russian.	**Verified?**	Verified
CA Document Repository	www.root.gov.kz;	**Verified?**	Verified
CP Doc Language	Russian		
CP	http://root.gov.kz/cps/certificate_policy.pdf	**Verified?**	Verified
CP Doc Language	Russian		
CPS		**Verified?**	Need Response From CA
Other Relevant Documents	NEED: CP/CPS translated into English.	**Verified?**	Need Response From CA
Auditor Name		**Verified?**	Need Response From CA
Auditor Website		**Verified?**	Need Response From CA
Auditor Qualifications		**Verified?**	Need Response From CA
Standard Audit	NEED: for all root inclusion/change requests. Reference section 2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Standard Audit Type		**Verified?**	Need Response From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit		**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA

SSL Verification Procedures	NEED (CP/CPS needs to be translated into English) Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. As per section 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference section 11 of the CA/Browser Forum's Baseline Requirements (BR). BR #11.1.1 lists several ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. Simply referencing section 11 of the BRs does not specify which of those options the CA uses, and is insufficient for describing how the CA conforms to the BRs. The CA's CP/CPS must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership	**Verified?**	Need Response From CA
EV SSL Verification Procedures	Not EV	**Verified?**	Not Applicable
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert. As per section 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit, because we plan to remove the Code Signing trust bit in the next version of Mozilla's CA Certificate Policy.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED CA response (and corresponding CP/CPS sections/text) to section 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	NEED CA response (and corresponding CP/CPS sections/text) to section 7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to publicly disclosed subordinate CA certificates that chain up to certificates in Mozilla's CA program, as per Items #8, 9, and 10 of Mozilla's CA Certificate Inclusion Policy.	**Verified?**	Need Response From CA