

Mozilla - CA Program

Case Information

Case Number	00000110	Case Record Type	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Thailand National Root Certificate Authority (Electronic Transactions Development Agency)	Request Status	Initial Request Received

Additional Case Information

Subject	Thailand National Root Certification Authority – G1	Case Reason	New Owner/Root inclusion requested
----------------	---	--------------------	------------------------------------

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1348774
-----------------------------	---

General information about CA's associated organization

CA Email Alias 1	nrca@etda.or.th		
CA Email Alias 2			
Company Website	http://nrca.go.th	Verified?	Verified
Organizational Type	Government Agency	Verified?	Verified
Organizational Type (Others)	None	Verified?	Not Applicable
Geographic Focus	Thailand	Verified?	Verified
Primary Market / Customer Base	Customers of NRCA is Subordinate CA (Coperate CA and Government CA) and customers of our Sub CA are personal and enterprise use in Thailand	Verified?	Verified
Impact to Mozilla Users	NRCA need to have their root certificate store in trust list of mozilla for facilitate in distribution certificate to their user that use mozilla browser and for reliability. Their user that use mozilla for SSL, Secure email and Document signing.	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	1) Publicly Available CP and CPS: CP : http://www.nrca.go.th/cp/cpv3.pdf CPS : http://www.nrca.go.th/cps/cpsv3.pdf	Verified?	Need Response From CA

Recommended Practices

- 2) CA Hierarchy: [Need CA Response]
- 3) Audit Criteria:
<https://cert.webtrust.org/ViewSeal?id=2154>
<https://cert.webtrust.org/ViewSeal?id=2155>
- 4) Document Handling of IDNs in CP/CPS: [Need CA Response in which session in CP/CPS]
- 5) Revocation of Compromised Certificates: http://www.nrca.go.th/crl_cert.html
- 6) Verifying Domain Name Ownership: [Need CA Response]
- 7) Verifying Email Address Control: CA have verification procedure of e-mail address as describe in section 4.2 Certificate Application Processing on our CP/CPS
- 8) Verifying Identity of Code Signing Certificate Subscriber: [Need CA Response]
- 9) DNS names go in SAN: CA have conform with BR #9.2.1 and BR #9.2.2
- 10) Domain owned by a Natural Person: We are accept with condition about process to define Natural Person's information in certificate.
- 11) OCSP: <http://ocsp.nrca.go.th>
- 12) Network Security Controls: <http://ocsp.nrca.go.th>

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

- 1) Long-lived DV certificates: [Need CA Response]
- 2) Wildcard DV SSL certificates: in CP/CPS section 4.2.1 Performing Identification and Authentication Functions
- 3) Email Address Prefixes for DV Certs: in CP/CPS section 4.2.1 Performing Identification and Authentication Functions
- 4) Delegation of Domain / Email validation to third parties: in CP/CPS section 4.2.1
- 5) Issuing end entity certificates directly from roots: We issue subCA certificate with Offline system.
- 6) Allowing external entities to operate subordinate CAs: Our SubCA has self-operated.
- 7) Distributing generated private keys in PKCS#12 files: Please see detail in section 4.3.1 CA Actions during Certificate Issuance
- 8) Certificates referencing hostnames or private IP addresses: We do not have policy that allow private domain and private IP Address
- 9) Issuing SSL Certificates for Internal Domains: in CP/CPS section 4.2.1 Performing Identification and Authentication Functions
- 10) OCSP Responses signed by a certificate under a different root: We are updating about OCSP Responses signing process.
- 11) SHA-1 Certificates: il in section 6.1.5 Key Sizes as decript about hash algorithm SHA-256 to 512
- 12) Generic names for CAs: in CP/CPS section 3. Identification and Authentication
- 13) Lack of Communication With End Users: in CP/CPS section 1.5.2 Contact Person
- 14) Backdating the notBefore date: in section 7.1 Certificate Profile.

Verified?

Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	Thailand National Root Certification Authority - G1	Root Case No	R00000159
Request Status	Initial Request Received	Case Number	00000110

Certificate Data

Certificate Issuer Common Name
O From Issuer Field
OU From Issuer Field
Valid From
Valid To
Certificate Serial Number
Subject
Signature Hash Algorithm
Public Key Algorithm
SHA-1 Fingerprint
SHA-256 Fingerprint
Certificate Fingerprint
Certificate Version

Technical Information about Root Certificate

Certificate Summary	Verified?	Need Response From CA
Root Certificate Download URL http://www.nrca.go.th/cert/nrca/THNRCA.der	Verified?	Verified
CRL URL(s) http://www.nrca.go.th/crl/THNRCA_arfile.crl	Verified?	Verified
OCSP URL(s) http://ocsp.nrca.go.th	Verified?	Verified
Trust Bits Code; Email; Websites	Verified?	Verified
SSL Validation Type OV	Verified?	Verified
EV Policy OID(s) None	Verified?	Not Applicable
Root Stores Included In Microsoft	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. https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551	Verified?	Need Response From CA

Test Websites or Example Cert

Test Website - Valid	Verified?	Need Response From CA
Test Website - Expired		
Test Website - Revoked		
Example Cert		
Test Notes		

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

Revocation NEED: Test with http://certificate.revocationcheck.com/	Verified?	Need Response From CA
---	-----------	-----------------------

Tested	make sure there aren't any errors.		
CA/Browser Forum Lint Test	NEED: Browse to https://crt.sh/ and enter the SHA-1 Fingerprint for the root certificate. Then click on the 'Search' button. Then click on the 'Run cablint' link. All errors must be resolved/fixd.	Verified?	Need Response From CA
Test Website Lint Test	NEED: Browse to https://cert-checker.allizom.org/ and enter the test website and click on the 'Browse' button to provide the PEM file for the root certificate. Then click on 'run certlint'. All errors must be resolved/fixd.	Verified?	Need Response From CA
EV Tested	NEED: If EV treatment is being requested, then provide successful output from EV Testing as described here https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	Verified?	Need Response From CA

CA Hierarchy Information

CA Hierarchy	NEED: A description 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	CA have subCA that are operated by external third parties and they have technically constrain for subCA to comply with Section 8 to 10 in Mozilla's CA Certificate Policy and CAB Forum requirement.	Verified?	Verified
Cross Signing	CA doesn't have Cross-Signing with othor Root CA.	Verified?	Verified
Technical Constraint on 3rd party Issuer	Refer as section 8 -10 in Mozilla's CA Certificate Policy, the subordinate CA of NRCA has been certified by WebTrust (version 1.3.7) and disclosed the audit report on their web site. Including their CP,CPS and certificate publish on their web site too. CP/CPS for TDIDG3: http://www.thaidigitalid.com/download/doc/TDID%20CA%20G3%20-%20CP-CPS%201-0.pdf CP/CPS for TDIDG2: http://www.thaidigitalid.com/download/doc/TDID%20CA%20G2%20-%20CP-CPS%201-2.pdf	Verified?	Verified

Verification Policies and Practices

Policy Documentation	English CP: http://www.nrca.go.th/cp/cpv3.pdf CPS: http://www.nrca.go.th/cps/cpsv3.pdf	Verified?	Verified
CA Document Repository		Verified?	Need Response From CA
CP Doc Language	English		
CP	http://www.nrca.go.th/cp/cpv3.pdf	Verified?	Verified
CP Doc Language	English		
CPS	http://www.nrca.go.th/cps/cpsv3.pdf	Verified?	Verified
Other Relevant Documents	None	Verified?	Not Applicable

Auditor Name	BDO Malaysia	Verified?	Verified
Auditor Website	http://www.bdo.my	Verified?	Verified
Auditor Qualifications	WebTrust 2.0 : https://cert.webtrust.org/ViewSeal?id=2154 WebTrust SSL Baseline 2.0 https://cert.webtrust.org/ViewSeal?id=2155	Verified?	Verified
Standard Audit		Verified?	Need Response From CA
Standard Audit Type	WebTrust	Verified?	Need Response From CA
Standard Audit Statement Date		Verified?	Need Response From CA
BR Audit	NONE!	Verified?	Need Response From CA
BR Audit Type	WebTrust	Verified?	Need Response From CA
BR Audit Statement Date		Verified?	Need Response From CA
EV Audit	NEED only if requesting EV treatment	Verified?	Need Response From CA
EV Audit Type		Verified?	Need Response From CA
EV Audit Statement Date		Verified?	Need Response From CA
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	8.1 Compliance audit for Subordinates CA form http://www.nrca.go.th/cp/cpv3.pdf	Verified?	Verified
EV SSL Verification Procedures	No EV request	Verified?	Not Applicable
Organization Verification Procedures	Section 4.1.1 on CP/CPS (Page 22 of 73)	Verified?	Verified
Email Address Verification Procedures	See detail in section 4.2.1 Performing Identification and Authentication Functions on our CP/CPS. (Page 22 of 73) In next step CA will establish Procedure to compliance with Section 7 of the Mozilla CA Certificate Inclusion Policy	Verified?	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	Verified?	Not Applicable
Multi-Factor Authentication	As refer in section 6.7 on our CP/CPS CA have been following Network and Certificate System Security Requirements of CAB Forum.	Verified?	Verified
Network Security	As refer in section 6.7 on our CP/CPS. CA have been following Network and Certificate System Security Requirements of CAB Forum.	Verified?	Verified