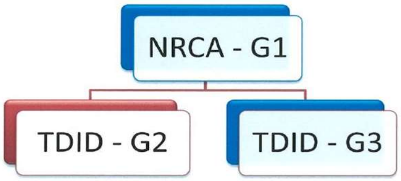
General information about the CA's associated organization

CA Company Name	Thailand National Root CA - G1 ("Thailand NRCA")
website URL	http://nrca.go.th
Organizational Type	Gorvernment
	Electronic Transactions Development Agency ("ETDA") is established on 25 November, 2010 under the Ministry of Information and Communication Technology (MICT) and according to the proposal of the Office of the Public Sector Development Commission (OPDC) to function as the main agency responsible for developing, promoting and supporting electronic transactions in order to create trust, opportunity and equity for all. ETDA's main mission is to conduct studies and research while providing support for the Electronic Transactions Commission and related agencies. ETDA has implemented Thailand National Root CA (Certificate Authority) Project ("Thailand NRCA") on fiscal year 2014. The Thailand NRCA allows interoperability of authenticating digital certificates issued by different service providers and serves as a central trust mechanism connecting digital signature systems used domestically and internationally. Thus it is an important infrastructure that reinforces secure and safe electronic transactions. With the effort of a group of PKI technology service providers or operators, the Thailand PKI Association was established in 2009 with an aim to increase Thai society's knowledge and understanding of PKI technology and to strengthen technical assistance among members. Past activities of the Association included a campaign for a higher level of PKI technology application; the action taken to have technical trials on issuance of digital certificates to domestic service; and implementation of system trials on interoperability with foreign CAs (CA-CA Interoperability).
Primark Maket /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
Impact to Mozilla Users	NRCA need to have our root certificate store in trust list of mozilla for facilitate in distribution our certificate to our user that use mozilla browser and for reliability. Our user that use mozilla for SSL, Secure email and Document signing.
Include in other major browsers	Microsoft
CA Primary Point of Contact (POC)	Mr.Thitikorn Trakoonsirisak (Email : nrca@etda.or.th)

Technical information about each root certificate

Certificate Name	Thailand National Root Certification Authority - G1
Certificate Issuer Field	Thailand National Root Certification Authority - G1
Certificate Summary	2
Monzilla Applied Constraints	We have procedure about Domain Name verification and identification that comply with CAB forum, Baseline Requirement and mozilla's CPS. About Type of our SSL certificate that we need to issue only SSL certificate not EV SSL at this time.
Root Cert URL	http://www.nrca.go.th/cert/nrca/THNRCA.der
SHA1 Fingerprint	66 f2 dc fb 3f 81 4d de e9 b3 20 6f 11 de fe 1b fb df e1 32
Valid From	2013-03-27
Valid To	2036-03-27
Certificate Version	V3
Certificate Signature Algorithm	SHA512
Signing key parameters	RSA module length 4096 Bits
Test Website URL (SSL) Example Certificate (non-SSL)	 http://www.nrca.go.th/cert/nrca/THNRCA.der
CRL URL	http://www.nrca.go.th/crl/THNRCA_arlfile.crl
OCSP URL (Requird now for end-entity certs)	http://ocsp.nrca.go.th
Request Trust Bits	serverAuth,clientAuth,codeSigning,emailProtection,timeStamping,Document Signing and OCSPSigning
SSL Validation Type	OV
EV Policy ODI(s)	-
Non-sequential serial numbers and entropy in cert	We used SHA-256 for signature algorithm, RSA 2048 bits, and 32 bits randomly generated serial number for our subscriber certificate.
Response to Recent CA Communication(s)	We have already responded to CA communication.

CA Hierachy information for each root certificate

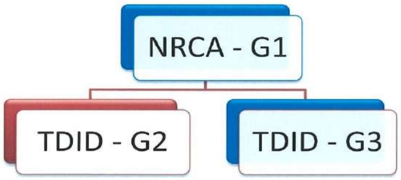
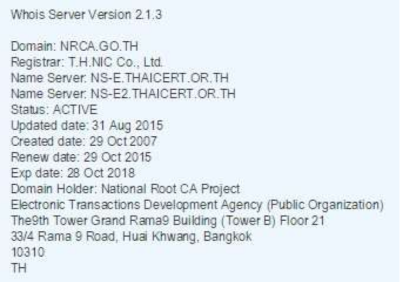
CA Hierachy	 ETDA's key functions is to develop, promote and support Thailand's digital signature environment. To that end, ETDA has adopted the Root CA trust model to address issues arising from incompatibility of proprietary data or incompatibility of software originating from different CAs. The Root CA trust model is administered by Thailand's National Root CA ("NRCA") which recognizes certificates issued by each of Thailand's CAs and allows for interoperability of cross-verification. ETDA is seeking a WebTrust accredited third party assurance provider to assess the adequacy and effectiveness of controls employed for certification authority operations. BDO would be assessing the conformity of • Root CA : the Thailand National Root Certificate Authority - G1 ("NRCA") • Subordinate CA : Thai Digital ID Company Limited – G2 ("TDID – G2") ,Thai Digital ID Company Limited – G3 ("TDID – G3").

Externally Operated SubCAs	We have subCA that are operated by external third parties and we have technically constrain for subCA to comply with Section 8 to 10 in Mozilla's CA Certificate Policy and CAB Forum requirement.
Cross-Signing	We don’t have Cross-Signing with othor Root CA.
Technical Constraints on Third-party Issuers	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 https://cert.webtrust.org/ViewSeal?id=1947 https://cert.webtrust.org/ViewSeal?id=1948

Verification Policies and Practices

Policy Documentation	Language(s) that the documents are in: English CP : http://www.nrca.go.th/cp/cpv3.pdf CPS : http://www.nrca.go.th/cps/cpsv3.pdf
Audits	BDO Malaysia
Baseline Requirements (SSL)	http://www.nrca.go.th/cp/cpv3.pdf 1.1 Overview (Page 12 of 73) NRCA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.
SSL Verification Prodecures	If you are requesting to enable the Websites (SSL/TLS) trust bit. 8.1 Compliance audit for Subordinates CA form http://www.nrca.go.th/cp/cpv3.pdf
Organization Verification Procedures	Please see details in section 4.1.1 on CP/CPS (Page 22 of 73)
Email Address Verification Procedures	Please see detail in section 4.2.1 Performing Identification and Authentication Functions on our CP/CPS. (Page 22 of 73) In next step we will establish Procedure to complince with Section 7 of the Mozilla CA Certificate Inclusion Policy
Code Signing Subscriber Verification Procedures	
Multi-factor Authentication	We have been following Network and Certificate System Security Requirements of CAB Forumn. As refer in section 6.7 on our CP/CPS
Network Security	We have been following Network and Certificate System Security Requirements of CAB Forumn. As refer in section 6.7 on our CP/CPS

Respone to Mozilla's CA Recommended Practies (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Avaiable CP and CPS	CP : http://www.nrca.go.th/cp/cpv3.pdf
	CPS : http://www.nrca.go.th/cps/cpsv3.pdf
CA Hierachly	
Audit Criteria	https://cert.webtrust.org/ViewSeal?id=2154
	https://cert.webtrust.org/ViewSeal?id=2155
Document Handing of IDNs in CP/CPS	http://www.nrca.go.th/cp/cpv3.pdf
	http://www.nrca.go.th/cps/cpsv3.pdf
Revocation of Compromised Certificates	http://www.nrca.go.th/crl_cert.html
Verfying Domain Name Ownership	 Whois Server Version 2.1.3 Domain: NRCA.GO.TH Registrar: T.H.NIC Co., Ltd. Name Server: NS-E.THAICERT.OR.TH Name Server: NS-E2.THAICERT.OR.TH Status: ACTIVE Updated date: 31 Aug 2015 Created date: 29 Oct 2007 Renew date: 29 Oct 2015 Exp date: 28 Oct 2018 Domain Holder: National Root CA Project Electronic Transactions Development Agency (Public Organization) The9th Tower Grand Rama9 Building (Tower B) Floor 21 33/4 Rama 9 Road, Huai Khwang, Bangkok 10310 TH
Verifying Email Address Control	We have verification procedure of e-mail address as decribe in section 4.2 Certificate Application Processing on our CP/CPS
Verifying Identity of Code Signing Certificate Subscriber	-
DNS name on in SAN	We have conform with BR #9.2.1 and BR #9.2.2
Domain owned by a Natural Person	We are accept with condition about process to define Natural Person's information in certificate.
OCSP	http://ocsp.nrca.go.th

Response to Mozilla's list of Potentially Problematic Practices

(https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	In the future for review CP/CPS we will have this section to compliance Mozilla policy.
Wildcard DV SSL certificates	Please see detail in section 4.2.1 Performing Identification and Authentication Functions on our CP/CPS. In the future for review CP/CPS we will have this section to compliance Mozilla policy.

Email Address Prefixes for DV Certs	Please see detail in section 4.2.1 Performing Identification and Authentication Functions on our CP/CPS. In the future for review CP/CPS we will have this section to compliance Mozilla policy.
Delegation of Domain /Email validation to third parties	Please see detail in section 4.2.1 Performing Identification and Authentication Functions on our CP/CPS. In the future for review CP/CPS we will have this section to compliance Mozilla policy.
Issuing end entity certificates directly from roots	We issue subCA certificate with Offline system.
Allowing external entities to operate subordinate Cas	Our SubCA has self-operated.
Distributing generated private keys in PKCS#12 files	Please see detail in section 4.3.1 CA Actions during Certificate Issuance
Certificates referencing hostnames or private IP Address	We do not have ploicy that allow private domain and private IP Address.
Issuing SSL Certificate for Internal Domains	Please see detail in section 4.2.1 Performing Identification and Authentication Functions on our CP/CPS.
OCPS Responses signed by a certificate under a different root	We are updating about OCSP Responses siging process.
SHA-1 Certificates	Please see detail in section 6.1.5 Key Sizes as decript about hash algorithm SHA-256 to 512
Generic names for Cas	Please see detail in section 3. Identification and Authentication on our CP/CPS.
Lack of Communication With End Users	Please see detail in section 1.5.2 Contact Person on our CP/CPS.
Backdating the notBefore date	Please see detail in section 7.1 Certificate Profile.