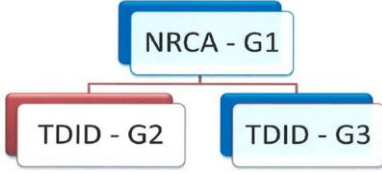


CA Hierarchy information for each root certificate

CA Hierarchy	 <pre> graph TD NRCA["NRCA - G1"] --- TDID2["TDID - G2"] NRCA --- TDID3["TDID - G3"] </pre> <p>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.</p> <p>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</p> <ul style="list-style-type: none"> • 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").
--------------	--

CA's Response to Recommended Practices

2 CA Hierarchy	
Field	Constraint
O, OU, CN	CN=Thailand National Root Certification Authority G1, OU=Thailand National Root Certification Authority, O=Electronic Transactions Development Agency (Public Organization)
Validity	minimum 8 years, maximum 30 years
Format	x.509 version 3 PKCS1
Public Key Algorithms	SHA512RSA
Message Digest Algorithms	SHA512
Certificate Policies (extension)	no limits
subjectAltName	email address
pathLenConstraint basic constraints extension	pathLenConstraint=None
4 Document Handling of IDNs in CP/CPS	We do not have policy for Document Handling of IDNs in CP/CPS We will be update in new CP/CPS by wording below <i>"For requests for internationalized domain names (IDNs) in Certificates, NRCA performs domain name owner verification to detect cases of homographic spoofing of IDNs. NRCA employs a manual process that searches various corresponding 'whois' services to find the owner of particular domain. If the search is inconclusive, the Certificate Request is rejected by the RA."</i>
6 Verifying Domain Name Ownership	Please see detail in section 3.1.6 Recognition, Authentication, and Role of Trademarks Thailand NRCA reserves no liability to any certificate applicant on the usage of Distinguished Names appearing in a certificate. The right to use the name is the responsibility of the applicant and must be in accordance to the relevant laws, regulations, legal obligations or announcements. (Pages 23/68) We will be update in new CP/CPS by wording below <i>"Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the intellectual property rights of others. NRCA, however, does not verify whether a certificate applicant has intellectual property rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. NRCA is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute."</i>
8 Verifying Identity of Code Signing Certificate Subscriber	We do not have policy for verifying Identity of Code Signing Certificate Subscriber.

Verification Policies and Practices

ITEM	Response From NRCA
CA Document Repository	2.1 Repositories Thailand NRCA posts all issued certificates in a publicly accessible website at the URL http://www.nrca.go.th . Thailand NRCA has implemented access controls to prevent unauthorized modification or deletion of information.
Standard Audit	Thailand NRCA audit following Standards (1) Webtrust Principles and Criteria for Certification Authorities Version 2.0 (2) Webtrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security - Version 2.0
Standard Audit Type	The WebTrust for Certification Authorities (http://www.webtrust.org)
Standard Audit Statement Date	1 September 2016 - 30 October 2016
BR Audit	Thailand NRCA last audit Framework by following Baseline Requirements 1.3.7
BR Audit Type	CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates (https://cabforum.org)
BR Audit Statement Date	1 September 2016 - 30 October 2016
BR Commitment to Comply	1.1 OverviewNRCA 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. (on CP/CPS Page 11 of 68)
BR Self Assessment	Done