CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)

Introduction must include:
1) CA's Legal Name
2) Clear indication (subject and SHA1 or SHA256 fingerprints) about which root certificates are being evaluated, and their full CA hierarchy. In considering a root certificate for inclusion in NSS, Mozilla must also evaluate the current subordinate CAs and the selection/approval criteria for future subordinate CAs. Mozilla's CA Certificate Policy requires full disclosure of non-technically-constrained intermediate certificates chaining up to root certificates in NSS.
3) List the specific version(s) of the BRs that you used. For example: BR version 1.4.2, with the exception of the Domain Validation section 3.2.2.4 for which we used BR version 1.4.1.
4) List the specific versions of the CA's documents that were evaluated, and provide direct URLs to those documents. All provided CA documents must be public-facing, available on the CA's website, and translated into English.
5) If you intend to submit your self-assessment with statements such as "will add/update in our next version of CP/CPS", indicate when you plan to provide the updated documents.
Note: When you are doing your BR Self Assessment, if you find that the required information is not currently in your CP/CPS documents, then you may indicate what your CA currently does, how it is currently documented, that the next version of your CP/CPS will contain this information, and when the next version of your CP/CPS will be available.

Document Update on 17/5/2017

1) CA's Legal Name : Thailand NRCA (National Root Certificate Authority)
2) Root Certificate using Algorithm SHA-512 refer on CPS Topic 7.1.2.9 Subject Key Identifier
3) NRCA used BR Version 1.3.8 for last Webturst Audit scope on year 2016.
4) URL for CP : http://www.nrca.go.th/cp/cpv3.pdf , URL for CPS : http://www.nrca.go.th/cp/cpsv3.pdf
5) Plan to add/update in our next version of CP/CPS within July 2017, before staring Webtrust Audit on August - September 2017

BR Section Number	List the specific documents and section numbers of those documents which meet the requirements of each BR section	Explain how the CA's listed documents meet the requirements of each BR section.
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	Page 14 Certification Policy	on Topic 1.5.5 CP Review and update Procedures / CAs operating under this CP shall recheck lastest of Baseline Requirements for the Issuance and Mangement of Publicy-Trusted Certificates from https://cabforum.org/baseline-requirements-documents/ or http://www.webtrust.org at least quarterly for the propose of develop, implements, enforce and annually update a Certificiate Policy and Certificate Practice Statenment. , that confirm our CA is fully compliant with all items when Audit assessment currently just in times and our CA improve compliance when CABForum revisions new versions .
1.2.2. Relevant Dates Note the Compliance date for eachitem in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	Page 14 Certification Policy	on Topic 1.5.5 CP Review and update Procedures / CAs operating under this CP shall recheck lastest of Baseline Requirements for the Issuance and Mangement of Publicy-Trusted Certificates from https://cabforum.org/baseline-requirements-documents/ or http://www.webtrust.org at least quarterly for the propose of develop, implements, enforce and annually update a Certificiate Policy and Certificate Practice Statenment. , that confirm our CA is fully compliant with all items when Audit assessment currently just in times and our CA improve compliance when CABForum Relevant Date by new versions .

1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.	Page 11 Certification Policy	on Topic 1.3.2 Registration Authorities / A Registration Authority (RA) is a person or legal entity that collects and verifies each subscriber's identity and information that is to be entered into the subscriber's public key certificate. RA performs its function in accordance with the CPS of the CA and is responsible for: - The registration process - The identification and authentication process.	
2.1. Repositories Provide the direct URLs to the CA's repositories	Page 10 Certification Prictice Statement	on Topic 2.1 Repositories / Thailand NRCA posts all issued certificates in a publicly accessible website at the URL **"http://www.nrca.go.th. "**	
2.2. Publication of information "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." --> Copy the specific text that is used into the explanation in this row. (in English)		will add/update in our next version of CP/CPS	
2.2. Publication of information "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." --> List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.		will add/update in our next version of CP/CPS	
2.3. Time or frequency of publication Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.	Page 18 on Certification Policy	on Topic 2.3 Time or Frequency of piblication / The CA that issues certificates under this CP shall publish its certificates and CRLs as soon as possible after issuance, An updated version of this CP will be made publicly available within one working day of the approval of changes. CA that issues certificates under this CP shall update and publish its CPS accordingly within thirty days after update.	
2.4. Access controls on repositories Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.	Page 18 on Certification Policy	on Topic 2.4 Access control on repositories / CA that issues certificates under this CP shall protect information not intended for public dissemination or modification. Certificates and CRLs in the repository shall be publicly available through the Internet. CA shall detail what information in the repository shall be exempt from automatic availability and to whom, and under which conditions the restricted information may be made available. CA shall maintain effective procedures and controls over the management of its repositories.	

3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, indicate how your CP/CPS meets the requirements in this section of the BRs.		will add/update in our next version of CP/CPS by / 3.2.2.1 CABF Verification Requirements for Organization Applicants / EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the STN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively.	
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, indicate how your CP/CPS meets the requirements in this section of the BRs.		will add/update in our next version of CP/CPS by /3.2.2.2 Mozilla Verification Requirements for Organization Applicants / For requests for internationalized domain names (IDNs) in Certificates, Symantec performs domain name owner verification to detect cases of homographic spoofing of IDNs. Symantec employs an automated process that searches various ‘whois’ services to find the owner of a particular domain. A search failure result is flagged for manual review and the RA may manually reject the Certificate Request. Additionally, the RA rejects any domain name that visually appears to be made up of multiple scripts within one hostname label. Symantec actively participates in the CA/Browser Forum providing input to the standards for IDN Certificates and conforms to standards ratified by that body.	
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, indicate how your CP/CPS meets the requirements in this section of the BRs.		will add/update in our next version of CP/CPS by / 3.2.2.3 Verification of Country / If the subject:contryName field is present, the Thailand NRCA verifies the country associated with the Subject using a method identified in Section 3.2.2.1	
3.2.2.4 Validation of Domain Authorization or Control Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS. The CA's CP/CPS must clearly describe the acceptable methods of domain validation. It is *not* sufficient for the CP/CPS to merely reference the BRs. Enough information must be directly provided in the CP/CPS for the reader to be able to understand how the CA performs domain validation.		will add/update in our next version of CP/CPS by / 3.2.2.4 Authorization by Domain Name Registrant / For each Fully-Qualified Domain Name listed in a Certificate , Thailand NRCA confirms that, as of the date the Certificate was issued, the Applicant (or the Applicant's Parent Company, Subsidiary Company or Affiliate, collectively referred to as "Applicant" for the purpose of this Section) either is the Domain Name Registrant or has control over the FQDN by: - communicating directly wit hthe Domain Name Registrant using the contact information listed in the WHOIS records "registrant","technical" or "administrative" field. - Relying upon a Domain Authorization Document approved by the Domain Name Registrant. The document MUST be dated on or after the certificate request date or used by Thailand NRCA to verify a previously issued certificate and that the Domain Name's WHOIS record has not been modified since the previous certificate issuance.	
3.2.2.4.1 Validating the Applicant as a Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.		will add/update in our next version of CP/CPS on 3.2.2.4	

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.		will add/update in our next version of CP/CPS on 3.2.2.4	
3.2.2.4.3 Phone Contact with Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.		will add/update in our next version of CP/CPS on 3.2.2.4	
3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.		will add/update in our next version of CP/CPS on 3.2.2.4	
3.2.2.4.5 Domain Authorization Document If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.		will add/update in our next version of CP/CPS on 3.2.2.4	
3.2.2.4.6 Agreed-Upon Change to Website If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.		will add/update in our next version of CP/CPS on 3.2.2.4	
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.		will add/update in our next version of CP/CPS on 3.2.2.4	
3.2.2.4.8 IP Address If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.		will add/update in our next version of CP/CPS on 3.2.2.4	
3.2.2.4.9 Test Certificate If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.		will add/update in our next version of CP/CPS on 3.2.2.4	
3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.		will add/update in our next version of CP/CPS on 3.2.2.4	

3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, indicate how your CA meets the requirements in this section of the BRs.		will add/update in our next version of CP/CPS by / 3.2.2.5 Authentication for an IP Address / Thailand NRCA do not issue certificates for IP Address	
3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then indicate how your CA meets the requirements in this seciton of the BRs.		will add/update in our next version of CP/CPS by / 3.2.2.6 Wildcard Domain Validation /Thailand NRCA do not issue Wildcard Domain Validation Certificates.	
3.2.2.7 Data Source Accuracy Indicate how your CA meets the requirements in this section of the BRs.		will add/update in our next version of CP/CPS by / 3.2.2.7 Data Source Accuracy / Prior to use any data source as a reliable data source, Thailand NRCA evaluates the source ofr its reliability, accuracy and resistance to alteration of falsification.	
3.2.3. Authentication of Individual Identity	page 20 on Certificate Policy	on Topic 3.2.3 Authentication of Individual Identity / Public key certificates bind public keys to identities. However, the entity to be identified depends on the application for which the public keys are used. Identifying different types of entity requires different evidence and procedures. CA that issues certificates under this CP shall state in its CPS the types of entity that the CA will support and details the required evidence and procedures.	
3.2.5. Validation of Authority	page 20 on Certificate Policy	on Topic 3.2.5 Validation of Authority / Registration Authority is responsible for verifying and authenticating an authorized representative of a juristic person by checking the following documents - Authorized Representative Appointment Letter from the relevant juristic person or other document of the same kind, corporate sealed and signed by the authorized director of the juristic person, as specified under the Certificate of Corporate Registration issued by the Department of Business Development, Ministry of Commerce, with a certified true copy of identification card or passport of the authorized director of such juristic person. - A certified true copy of identification card or passport of the authorized representative of the juristic person. RA verifies and endorses the integrity of documents.	
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	page 20 on Certificate Policy	on Topic 3.2.6 Criteria for Interoperation / PA promotes interoperation between CAs issuing certificates under this CP and other CAs which may or may not issue certificates under this CP (for example, overseas CA(s)). Thailand NRCA will interoperate with other Certification Authorities after signing the agreement or Memorandum of Understanding (MOU) on behalf of all CAs under Thailand NRCA trust model	
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	page 22 on Certificate Policy	on Topic 4.1.1 Who Can Submit a Certificate / Organization who wishes to operate a CA in Thailand may complete and submit an application for certificates to Thailand NRCA. Other certificate applications may be submitted to the CA that issues certificates under this CP by the Subscribers listed in Section 1.3.3, or an RA on behalf of the Subscriber.	

4.1.2. Enrollment Process and Responsibilities	page 22 on Certificate Policy	on Topic 4.1.2 Enrollment Process and Resposibilities / All communications among CA and RA supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets and personally identifiable information shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data. **Subscribers are responsible for providing accurate information on their certificate applications.**	
4.2. Certificate application processing			
4.2.1. Performing Identification and Authentication Functions Indicate how your CA identifies high risk certificate requests.	page 22 on Certificate Policy	on Topic 4.2.1 Performing Identification and Authentication Functions / Information in certificate applications must be verified as accurate before certificates are issued. Procedures to verify information in certificate applications shall be specified in the CPS. The identification and authentication of the subscriber must meet the requirements specified for subscriber authentication as specified in Sections 3.2 and 3.3. The components of the PKI (e.g., CA or RA) that are responsible for authenticating the subscriber’s identity in each case must be identified in the CPS.	
4.2.2. Approval or Rejection of Certificate Applications	page 23 on Certificate Policy	on Topic 4.2.2. Approval or Rejection of Certificate Applications / Any certificate application that is received by a CA that issues certificates under this CP, for which the identity and authorization of the applicant has been validated, will be duly processed. However, the CA must reject any application for which such validation cannot be completed. RA will coordinate with the CA to approve or reject certificate applications and notifies the results to subscribers.	
4.3.1. CA Actions during Certificate Issuance	page 23 - 24 on Certificate Policy	on Topic 4.3.1. CA Actions during Certificate Issuance / Upon receiving the request, CA that issues certificate under this CP and its RA will: - Verify the identity of the requester as specified in Section 3.2; - Verify the authority of the requester and the integrity of the information in the certificate request as specified in Section 4.1; - CAO must ensure the accuracy information in a CSR that conform with Section 6. If not conform in Section 6 CAO must be reject that Sub CA CSR. - Generate and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate); and - Make the certificate available to the subscriber after confirming that the subscriber has formally acknowledged their obligations as described in Section 9.6.3. All authorization and other attribute information received from a prospective subscriber shall be verified before inclusion in a certificate. The responsibility for verifying prospective subscriber data shall be described in a CA’s CPS.	
4.9.1.1 Reasons for Revoking a Subscriber Certificate Reasons for revoking certificates must be listed in the CA's CP/CPS.		will add/update in our next version of CP/CPS	

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate		will add/update in our next version of CP/CPS	
4.9.2. Who Can Request Revocation	page 30 on Certificate Policy	on Topic 4.9.2. Who Can Request Revocation / - Subscriber may make a request to revoke the certificate for which the subscriber is responsible. - CA that issues certificates under this CP may make a request to revoke its own certificate. - CA that issues certificates under this CP may also revoke any issued certificate whenever it knows or reasonably suspects that the circumstances as specified in section 4.9.1 occurred. - Registration Authority (RA) may also make a request to revoke a certificate for which a subscriber is responsible whenever it knows or reasonably suspects that the circumstances as specified in section 4.9.1 occurred. - Court order	
4.9.3. Procedure for Revocation Request	page 30 on Certificate Policy	on Topic 4.9.3. Procedure for Revocation Request / CA that issues certificates under this CP shall provide the procedure that requester can request for revocation 24x7. Subscriber requesting revocation is required to follow the procedures such as: 1) Subscriber submits the revocation request and related documents to the certificate issuing CA, or an RA of the CA, providing that the information is genuine, correct and complete. 2) Issuing CA or RA of the CA verifies and endorses the revocation requests and the related documents. 3) RA is responsible for verifying and authenticating an authorized representative of a juristic person by following the procedures as specified in Section 3.2. 4) Issuing CA with the assistance of RA will approve and process the revocation request. 5) Issuing CA, or via a RA of the CA, informs the revocation result to the subscriber. For revocation of certificate, PA must be informed	
4.9.5. Time within which CA Must Process the Revocation Request	page 31 on Certificate Policy	on Topic 4.9.7. CRL Issuance Frequency / CA that issues certificates under this CP must revoke certificates as quickly as practical upon endorsement of revocation request. Revocation requests should be processed within one business day or, whenever possible, before the next CRL is published.	
4.9.7. CRL Issuance Frequency	page 31 on Certificate Policy	**on Topic 4.9.7. CRL Issuance Frequency / CA that issues certificates under this CP will issue a CRL in the following circumstances:** **-** Issue a CRL whenever a certificate or a subscriber certificate is revoked. - Issue a CRL for certificates every six months whether or not the CRL has any changes. - Issuing CA must issue a CRL for subscriber certificates at least once a day whether or not the CRL has any changes	
4.9.9. On-line Revocation/Status Checking Availability	page 31 on Certificate Policy	on-line status checking is optional for Thailand NRCA and CAs operating under this CP. Where on-line status checking is supported, status information shall be regularly updated and available to relying parties.	

4.9.10. On-line Revocation Checking Requirements Indicate how your CA meets all of the requirements listed in this section, including support of GET, update frequency, preventing errounious return of "good" status.	page 31 on Certificate Policy	on Topic 4.9.10 On-line Revocation Checking Requirements / Relying Parties may optionally check the status of certificates through the Thailand NRCA's Online Certificate Status Protocol (OCSP) service, if provided by Thailand NRCA, and/or check the status of subscriber certificates through the issuing CA's OCSP service, if provided by the issuing CA. Client software using on-line status checking need not obtain or process CRLs.	
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	page 32 on Certificate Policy	on Topic 4.9.11 Other Forms of Revocation Advertisements Available / Other forms of Revocation Advertisements can be provided in accordance with Trust Service Principles and Criteria for Certification Authorities Version 2.0	
4.10.1. Operational Characteristics	page 32 on Certificate Policy	on Topic 4.10.1. Operational Characteristics / The status of certificates is available through the Thailand NRCA's website and LDAP using the appropriate software. The status of subscriber certificates can be checked through the issuing CA's website and LDAP using the appropriate software.	
4.10.2. Service Availability	page 33 on Certificate Policy	on Topic 4.10.2. Service Availability / CA that issues certificates under this CP shall implement backup systems for providing certificate status services and put the best efforts to make such services available 24x7	
5. MANAGEMENT, OPERATIONAL, and Physical CONTROLS		will add/update in our next version of CP/CPS	
5.2.2. Number of Individuals Required per Task	page 37 on Certificate Policy	On Topic 5.2.2. Number of Individuals Required per Task / Where multi-party control is required, all participants shall hold a trusted role. Multi-party control shall not be achieved using personnel that serve in a Security Auditor role with the exception of audit functions. The following tasks shall require two or more persons: - Generation, activation, and backup of CA keys - Performance of CA administration or maintenance tasks - Archiving or deleting CA audit logs. At least one of the participants shall serve in a Security Auditor role - Physical access to CA equipment - Access to any copy of the CA cryptographic module - Processing of third party key recovery requests	
5.3.1. Qualifications, Experience, and Clearance Requirements	page 39 on Certificate Policy	On Topic 5.3.1. Qualifications, Experience, and Clearance Requirements / All personnel of CA that issues certificates under this CP must be examined with their qualifications in terms of the requisite background, experience in order to ensure their prospective job responsibilities, competency and satisfaction	

5.3.3. Training Requirements and Procedures	page 39 - 40 on Certificate Policy	On Topic 5.3.3. Training Requirements and Procedures / CA that issues certificates under this CP must provide its officers with appropriate training as well as the requisite on-the-job training needed to perform their job responsibilities related to CA operations with competency and satisfaction. The training programs include the following as relevant: - Basic cryptography and Public Key Infrastructure (PKI) concepts - Information Security Awareness Thailand National Root Certification Authority: Thailand NRCA Electronic Transactions Development Agency (Public Organization) Certificate Policy - 40 - - Use and operation of deployed hard ware and software related to CA operations - Security Risk Management - Disaster recovery and business continuity procedures	
5.3.4. Retraining Frequency and Requirements	page 40 on Certificate Policy	on Topic 5.3.4. Retraining Frequency and Requirements / CA that issues certificates under this CP must provide its officers with appropriate training at least once a year on the topics related to Information Security Awareness. Additional training may be considered if there is a change in hardware and software related to CA operations	
5.3.7. Independent Contractor Controls	page 40 on Certificate Policy	on Topic 5.3.7. Independent Contractor Controls / In case that independent contractors or consultants is employed and is obliged to pass the background check procedures specified in Section 5.3.2. Any such contractor or consultant are only permitted to access to CA's secure facilities if they are escorted and directly supervised by trusted officers at all times. For system maintenance purposes, operating staffs must present their employee identification card to Trusted Persons for verification and record. They must be also escorted and directly supervised by trusted officers at all times.	

5.4.1. Types of Events Recorded	page 41 on Certificate Policy	on Topic 5.4.1. Types of Events Recorded / CA that issues certificates under this CP must log the following significant events: o CA Key Life Cycle Management, including: o Key generation, backup, storage, recovery, archival, and destruction o Cryptographic Module life cycle management events o CA and Subscriber certificate life cycle management events, including: o Certificate Applications, rekey, and revocation o Approval or rejection of requests o Generation and issuance of certificates and CRL o Security-related events including: o Successful and unsuccessful access attempts to CA systems o Security system actions performed by CA officers o Security profile changes o System crashes, hardware failures and other anomalies o Firewall and router activity o CA facility visitor entry/exit - Log entries include the following elements: o Date and time of the entry o Automatic journal entries o Identity of the entity making the journal entry o Type of entry	
5.4.3. Retention Period for Audit Logs	page 42 on Certificate Policy	On Topic 5.4.3. Retention Period for Audit Logs / Audit logs are retained for at least 90 days.	
5.4.8. Vulnerability Assessments	page 42 on Certificate Policy	On Topic 5.4.8. Vulnerability Assessments / CA that issues certificates under this CP must assess security vulnerability at least on a quarterly.	
5.5.2. Retention Period for Archive	page 43 on Certificate Policy	On Topic 5.5.2. Retention Period for Archive / Records shall be retained for at least 10 years, unless there are specific requirements (according to the Accounting Act B.E. 2543)	

5.7.1. Incident and Compromise Handling Procedures	page 45 on Certificate Policy	on Topic 5.7.1. Incident and Compromise Handling Procedures / CA that issues certificates under this CP shall have an incident response plan and a disaster recovery plan. If compromise of a CA is suspected, an independent third-party investigation shall be performed in order to determine the nature and the degree of damage. Issuance of certificates from that CA shall be stopped immediately upon detection of a compromise. If a CA private signing key is suspected of compromise, the procedure outlined in section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA private key needs to be declared compromised. In case that there an event affects to security of CA system, the corresponding CA officers shall notify PA and Thailand NRCA if any of the following occur: - Suspected or detected compromise of any CA system or subsystem - Physical or electronic penetration of any CA system or subsystem - Successful denial of service attacks on any CA system or subsystem - Any incident preventing a CA from issuing and publishing a CRL or on-line status checking prior to the time indicated in the next Update field in the currently published CRL, or the certificate for on-line status checking suspected or detected compromise.	
6.1.1. Key Pair Generation	page 48 on Certificate Policy	On Topic 6.1.1. Key Pair Generation / CA that issues certificates under this CP generates a key pair and store the private key in a cryptographic key management device that meets Federal Information Processing Standard (FIPS) 140-2 Level 3 under multi-person control. Cryptographic keying material used by CAs to sign certificates, CRLs or status information are required to be generated in FIPS 140-2 Level 3 or equivalent standard validated cryptographic modules. Multi-party control is required for CA key pair generation, as specified in section 6.2.2. CA key pair generation must create a verifiable audit trail demonstrating that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation. Subscriber key pair generation shall be performed by the subscriber. If the CA that issues certificates under this CP generates key pairs for subscriber, the CA shall generate key within a secure FIPS 140 validated cryptographic hardware.	

6.1.2. Private Key Delivery to Subscriber	page 48 on Certificate Policy	On Topic 6.1.2. Private Key Delivery to Subscriber / CA that issues certificates under this CP must generate the key pair by themselves. If the CA that issues certificates under this CP generates key pairs for subscriber, the CA shall develop a procedure to securely distribute private key to subscriber.	
6.1.5. Key Sizes	page 49 on Certificate Policy	on Topic 6.1.5 Key Sizes / This CP requires use of RSA signature algorithm and additional restriction on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA public keys with the minimum key size of 4,096 bits Thailand NRCA root certificate and CAs that issues certificates and CRLs under this CP should use the SHA-256, or SHA-384, or SHA-512 hash algorithm when generating digital signatures. CAs that issue certificates signed with SHA-256, or SHA-384, or SHA-512 must not issue certificates signed with SHA-1.	
6.1.6. Public Key Parameters Generation and Quality Checking	page 49 on Certificate Policy	on Topic 6.1.6. Public Key Parameters Generation and Quality Checking / Not Applicable.	
6.1.7. Key Usage Purposes	page 49 on Certificate Policy	on Topic 6.1.7. Key Usage Purposes / The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension. Public keys that are bound into subscriber certificates shall be used only for signing or encrypting. Public key that are bound into certificates shall be used only for signing certificates and status information such as CRLs. Only Thailand NRCA shall issue certificates to CAs located in Thailand./ Update CP/CPS by include these content in 6.1.7 / Thailand NRCA allows using its key pair for digital signature verification, Self-signed Certificate and signing certificate to other certification providers (Certificate Signing) certificate revocation (CRL Signing) and OCSP Response Verification Certificate (OCSP Signing).	
6.2. Private Key Protection and Cryptographic Module Engineering Controls	page 50-51 on Certificate Policy	6.2. Private Key Protection and Cryptographic Module Engineering Controls/... 6.2.1 to 6.2.11 Update CP/CPS by add these content In Section 6.2. Private Key Protection and Cryptographic Module Engineering Controls 6.2.1 Cryptographic Module Standards and Controls Thailand NRCA uses a FIPS 140-2 Level 3 validated hardware cryptographic module for signing operations. 6.2.2 Private Key (n out of m) Multi-person Control Accessing private key of Thailand NRCA must be performed by at least two persons with Trusted Role. 6.2.7 Private Key Storage on Cryptographic Module Thailand NRCA private key stored in a Cryptographic Module and back up the private key in another Cryptographic Module.	

6.2.5. Private Key Archival	page 51 on Certificate Policy	on Topic 6.2.5 Private Key Archival / CA private key beyond the validity period will be kept at least 10 years and stored in Cryptographic Module with FIPS 140-2 Level 3 standards. Update CP/CPS by include thiese content in 6.2.6. /For Subordinate CA, Private Keys must be archival by Subordinate CA or authorization by the Subordinate CA.	
6.2.6. Private Key Transfer into or from a Cryptographic Module	page 51 on Certificate Policy	on Topic 6.2.6 Private Key Transfer into or from a Cryptographic Module / CA private keys may be exported from the cryptographic module only to perform CA key backup procedure. At no time shall the CA private key exist in plaintext outside the cryptographic module.	
6.2.7. Private Key Storage on Cryptographic Module	page 51 on Certificate Policy	on Topic 6.2.7 Private Key Storage on Cryptographic Module / Thailand NRCA and CA operating under this CP shall store its Private Keys on a cryptographic module which complies with FIPS 140-2 Level 3 or above standard.	
6.3.2. Certificate Operational Periods and Key Pair Usage Periods	page 52 on Certificate Policy	on Topic 6.3.2. Certificate Operational Periods and Key Pair Usage Periods / The certificate validity period and key pair associated with the certificate can be used up to the expiry date specified in the certificate. Public key can be used to verify the digital signature even if the certificate is expired but the digital signature to be verified must be created before expiry date of the certificate. For the private key, it can be used to decrypt even if certificate is expired. The validity period of Thailand NRCA root certificate is 23 years and validity period of certificates is not more than 20 years. Certificate operational periods and key pair usage periods shall be assessed by PA at least once a year or as necessary especially in an incident that is believed to significantly impact trustworthiness of the CA. (With technical limitations on UTC Time, the certificate issued by Thailand NRCA and its subordinate CA shall not have expiry date exceeding year 2580 (AD 2037)).	
6.5.1. Specific Computer Security Technical Requirements	page 53 on Certificate Policy	on Topic 6.5.1. Specific Computer Security Technical Requirements / CA operated under this CP shall limit the number of application installed on each computer to minimize security risks. Those applications are hardened based on the instructions provided by software manufacturer. In addition, installed applications shall be regularly reviewed for security updates to ensure that no vulnerability is exposed.	
7.1. Certificate profile	page 55 on Certificate Policy	on Topic 7.1 Certificate Profice / Certificate issued by CA under this CP must comply with ITU-T Recommendation X.509 (11/08): Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks and ISO / IEC 9594-8:2008 Information technology standard. - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks in which the certificate contains the information shown in Table 3.	
7.1.1. Version Number(s)	page 55 on Certificate Policy	on Topic 7.1.1 Version Number / Certificate issued by CA is in accordance with ITU-T Recommendation X.509 standard ISO / IEC 9594- 8:2008 and designated to be version 3.	

7.1.2. Certificate Content and Extensions; Application of RFC 5280	page 55 on Certificate Policy	on Topic 7.1.2 Certificate Extensions / Additional information on the certificate issued by CA is complied with ISO / IEC 9594-8:2008 standard, which contains at least the following:	
7.1.2.1 Root CA Certificate	NRCA-Certificate Policy Section 7.1.2.1 Root CA Certificate	will add/update in our next version of CP/CPS by / "on Topic 7.1.2.1 Root CA Certificate This extension shall be marked as critical. Certificates shall assert the minimum required for functionality. Signature certificates shall assert Digital Signature and Non-Repudiation. Encryption certificates shall assert either keyencipherment or keyagreement. Certificates shall assert digital signature, Non-Repudiation, keyCertSign and CRLSign. Update CP/CPS by Include these content in / 7.1.2.1 Root Certificate a. basicConstraints The pathLenConstraint field SHOULD NOT be present b. keyUsage keyUsage If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set. (By CBA)"	
7.1.2.2 Subordinate CA Certificate	Section 7.1.2.2 Subordinate CA Certificate	will add/update in our next version of CP/CPS	
7.1.2.3 Subscriber Certificate	Subordinate's Certificate Policy http://www.thaidigitalid.com/wp-content/uploads/2016/12/TDID-CA-CP-CPS-2-1.pdf Section 7	will add/update in our next version of CP/CPS	
7.1.2.4 All Certificates	NRCA-Certificate Policy Section 7. Certificate, CRL and OCSP Profiles Subordinate's Certificate Policy section 7. Certificate, CRL and OCSP Profiles	will add/update in our next version of CP/CPS	
7.1.2.5 Application of RFC 5280	NRCA-Certificate Policy Section 7. Certificate, CRL and OCSP Profiles Subordinate's Certificate Policy section 7. Certificate, CRL and OCSP Profiles	will add/update in our next version of CP/CPS	
7.1.3. Algorithm Object Identifiers	page 49 on Certificate Policy Section 6.1.5 Key Size	on Topic 6.1.5 Key Size / Thailand NRCA root certificate and CAs that issues certificates and CRLs under this CP should use the SHA-256, or SHA-384, or SHA-512 hash algorithm when generating digital signatures. CAs that issue certificates signed with SHA-256, or SHA-384, or SHA-512 must not issue certificates signed with SHA-1.	
7.1.4. Name Forms	page 18 on Certificate Policy Section 7.1.4. Name Forms Section 3.1.1 Types of Names	on Topic 3.1.1 Types of Names CA that issues certificates under this CP shall specify the naming convention that it has adopted, such as X.501 Distinguished Names (DN) or other forms of names such as web site certificates. Alternative name forms including for example an electronic mail address or a personal identification number may be included to ensure that the certificate of a person can be unambiguously identified.	
7.1.4.1 Issuer Information	NRCA-Certificate Policy Section 7. Certificate, CRL and OCSP Profiles	In section 7. Certificate, CRL and OCSP Profiles	

7.1.4.2 Subject Information	NRCA-Certificate Policy Section 7. Certificate, CRL and OCSP Profiles	In section 7. Certificate, CRL and OCSP Profiles	
7.1.4.3 Subject Information - Subordinate CA Certificates	NRCA-Certificate Policy Section 7. Certificate, CRL and OCSP Profiles	In section 7. Certificate, CRL and OCSP Profiles	
7.1.5. Name Constraints	NRCA-Certificate Policy Section 7. Certificate, CRL and OCSP Profiles	In section 7. Certificate, CRL and OCSP Profiles	
7.1.6. Certificate Policy Object Identifier	NRCA-Certificate Policy Section 7. Certificate, CRL and OCSP Profiles	In section 7. Certificate, CRL and OCSP Profiles	
7.1.6.1 Reserved Certificate Policy Identifiers	NRCA-Certificate Policy Section 7. Certificate, CRL and OCSP Profiles	In section 7. Certificate, CRL and OCSP Profiles	
7.1.6.2 Root CA Certificates	NRCA-Certificate Policy Section 7. Certificate, CRL and OCSP Profiles	In section 7. Certificate, CRL and OCSP Profiles	
7.1.6.3 Subordinate CA Certificates	NRCA-Certificate Policy Section 7. Certificate, CRL and OCSP Profiles	In section 7. Certificate, CRL and OCSP Profiles	
7.1.6.4 Subscriber Certificates	Subordinate's Certificate Policy http://www.thaidigitalid.com/wp-content/uploads/2016/12/TDID-CA-CP-CPS-2-1.pdf Section 7	In section 7. Certificate, CRL and OCSP Profiles	
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	page 60 on Certificate Policy	on Topic 8. Compliance Audit and Other Assessments / CAs operated under this CP has compliance audit mechanism in place to ensure that the requirements of their CPS are being implemented and enforced.	
8.1. Frequency or circumstances of assessment	page 60 on Certificate Policy	on Topic 8.2 Frequency or Circumstances of Assessment / CAs and RAs shall be subject to a periodic compliance audit in respect of Trust Service Principles and Criteria for Certification Authorities Version 2.0 and CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates – Version 1.1.6 Network and Certificate Systems Security Requirements – Version 1.0 at least once a year	
8.2. Identity/qualifications of assessor	page 60 on Certificate Policy	on Topic 8.3 Identity/Qualifiations of Assesor / The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA's CPS and this CP. Assessment must be done by an ISO / IEC 27001:2005 and / or the Trust Service Principles and Criteria for Certification Authorities Version 2.0 and CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates – Version 1.1.6 Network and Certificate Systems Security Requirements – Version 1.0 certified auditors with the understanding of the certification service business.	

8.4. Topics covered by assessment	page 60 to 61 on Certificate Policy	on Topic 8.5 Topics covered by assessment / The purpose of compliance audit is to verify that a CA and its RAs comply with all the requirements of the current version of this CP and the CA's CPS. The scope of assessment shall follow that in the list below. - Trust Service Principles and Criteria for Certification Authorities Version 2 http://www.webtrust.org/homepage-documents/item54279.pdf - WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0 http://www.webtrust.org/homepage-documents/item79806.pdf - WebTrust Principles and Criteria - SSL Baseline with Network Security 2.0 https://cabforum.org/baseline-requirements-documents/	
8.6. Communication of results	page 61 on Certificate Policy	on Topic 8.7. Communication of results / After the assessment is completed, the audit compliance report and identification of corrective measures will be sent to PA within 30 days of completion	
8.7. Self-Audits	page 60 on Certificate Policy	on Topic 8.1 Compliance audit for Subordinate CA /For the Subordinate CA that is technically constrained in accordance with SSL baseline Requirements Section 9.7. CA monitors the Subordinate CA's adherence to the CA's Certificate Policy and the Subordinate CA's Certification Practices Statement and performs quarterly assessments against a randomly selected sample of at least three percent (3%) of the Certificates issued by the subordinate CA in the period beginning immediately after the last samples was taken.	
9.6.1. CA Representations and Warranties	page 65 on Certificate Policy	on Topic 9.6.1. CA Representations and Warranties / CA assures that - Procedures are implemented in accordance with this CP. - Any certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this CP. - Certification Practice Statement (CPS) will be provided, as well as any subsequent changes, for conformance assessment. - The CA operation is maintained in conformance to the stipulations of the CPS. - The registration information is accepted only from approved RAs operating under an approved CPS. - All information contained in the certificate issued by the CA is valid and appropriate. Evidence that due diligence was exercised in validating the information contained in the certificates is maintained. - Certificates of subscribers found to have acted in a manner counter to their obligations in accordance with section 9.6.3 will be revoked. - All information regarding certificate issuance and certificate revocation are processed through the procedure specified in the CPS of the corresponding CA.	

9.6.3. Subscriber Representations and Warranties	page 66 on Certificate Policy	on Topic 9.6.3. Subscriber Representations and Warranties / By using the subscriber certificate, the subscriber assures that - He/She accurately represents itself in all communications with the CA. - The private key is properly protected at all times and inaccessible without authorization. - The CA is promptly notified when the private key is suspected loss or compromise. - All information displays in the certificate is complete and accurate. - The certificate will be used legitimately under laws, related regulations, terms, conditions and other related service announcements of the CA by authorized persons.	
9.8. Limitations of liability	page 67 on Certificate Policy	on Topic 9.8. Limitations of liability / CA is responsible for any damage incurred in the event of damage caused by the use of the service systems from the willful act or gross negligence of the corresponding CA. The response to the damage is under determination of CA.	
9.9.1. Indemnification by CAs		no Topic Indemnification by CAs / will add in our version of CP/CPS will add/update in our next version of CP/CPS	
9.16.3. Severability	page 69 on Certificate Policy	on Topic 9.16.3 Severability Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated.	