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 31/8/2018
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 1.6.0 for last Webturst Audit scope on year 2018.
4) URL for CP : https://www.nrca.go.th/publishing-detail/cpv4th.html , URL for CPS : https://www.nrca.go.th/publishing-detail/cpsv4th.html
5) Plan to add/update in our next version of CP/CPS within August 2019, before staring Webtrust Audit on September - October 2019

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 5 of Certification Policy /Topic 1.5.5 CP Review and Update Procedures	1.5.5 CP Review and update Procedures / CAs operating under this CP shall recheck the latest of Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates from https://cabforum.org/baseline-requirements-documents or http://www.webtrust.org at least quarterly for the purpose of development, implementation, enforcement and annually update of a Certificate Policy and Certificate Practice Statement. https://cabforum.org/baseline-requirements-documents or at least quarterly for the purpose of development, implementation, enforcement and annually update of a Certificate Policy and Certificate Practice Statement.
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 5 of Certification Policy /Topic 1.5.5 CP Review and Update Procedures	1.5.5 CP Review and update Procedures / CAs operating under this CP shall recheck the latest of Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates from https://cabforum.org/baseline-requirements-documents or http://www.webtrust.org at least quarterly for the purpose of development, implementation, enforcement and annually update of a Certificate Policy and Certificate Practice Statement. https://cabforum.org/baseline-requirements-documents or at least quarterly for the purpose of development, implementation, enforcement and annually update of a Certificate Policy and Certificate Practice Statement.
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 3 of Certification Policy /Topic 1.3.2 Registration Authorities	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 8 of Certification Policy /Topic 2.1 Repositories	2.1 Repositories / All CAs that issue certificates under this policy are obligated to post all certificates issued by or to the CA and CRLs issued by the CA in a repository that is publicly accessible through all Uniform Resource Identifier (URI) references asserted in valid certificates issued by that CA. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanism to prevent unauthorized modification or deletion of information. / Thailand NRCA posts all issued certificates in a publicly accessible on the website https://www.nrca.or.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)	Page 8 of Certification Policy /Topic 2.2 Publication of Information	2.2 Publication of Information / CAs shall make information publicly available on the website (www.nrca.go.th) such as CPs, CPSs, Certificates and CRLs in repositories. For public services, they are available 24 hours per day and 7 days per week. It shall ensure that its repository or repositories are implemented through trustworthy systems.
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.	Page 8 of Certification Policy /Topic 2.2 Publication of Information	2.2 Publication of Information /CAs shall make information publicly available on the website (www.nrca.go.th) such as CPs, CPSs, Certificates and CRLs in repositories. For public services, they are available 24 hours per day and 7 days per week. It shall ensure that its repository or repositories are implemented through trustworthy systems.
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 8 of Certification Policy /Topic 2.3. Time or frequency of publication	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 8 of Certification Policy /Topic 2.4. Access controls on repositories	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.	Page 10 of Certification Policy /Topic 3.2.2.1 Identity	3.2.2.1 Identity in CP/CPS / If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. The CA SHALL verify the identity and address of the Applicant using documentation provided by, or though communication with, at least on of the following:.....
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.	Page 11 of Certification Policy /Topic 3.2.2.2 DBA/Tradename	3.2.2.2 DBA/Tradename in CP/CPS / Cas follows Sections 3.2.2.2 of CA/B Forum Baseline Requirements.
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.	Page 11 of Certification Policy /Topic3.2.2.3 Verification of Country	3.2.2.3 Verification of Country in CP/CPS / Cas follows Sections 3.2.2.3 of CA/B Forum Baseline Requirements.

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.	Page 11 of Certification Policy /Topic 3.2.2.4 Validation of Domain Authorization or Control	3.2.2.4 Validation of Domain Authorization or Control in CP/CPS / This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain. The CA SHALL confirm that prior to issuance, the CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one for the methods listed below. Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the lelevant requirement prior to Certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate. CAs SHALL maintain a record of which domain validation method, including relevant BR version number, the used to validate every domain. Note: FQDNs may be listed in Subscriber Certificates using dNSNames in the subjecAltName extention or in Subordinate CA Certificates via dNSNames in permittedSubtrees within the Name Constraints extension.
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.	Page 11 of Certification Policy /Topic 3.2.2.4 Validation of Domain Authorization or Control	3.2.2.4.1 Veridating the Applicant as a Domain Contract in CP/CPS / Cas follows Sections 3.2.2.4.1 of CA/B Forum Baseline Requirements.
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.	Page 11 of Certification Policy /Topic 3.2.2.4 Validation of Domain Authorization or Control	3.2.2.4.2 Email, Fax SMS, or Postal Mail to Domain Contact in CP/CPS / Cas follows Sections 3.2.2.4.2 of CA/B Forum Baseline Requirements.
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.	Page 11 of Certification Policy /Topic 3.2.2.4.3 Phone Contact with Domain Contac	3.2.2.4.3 Phone Contact with Domain Contact in CP/CPS / Cas follows Sections 3.2.2.4.3 of CA/B Forum Baseline Requirements.
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.	Page 11 of Certification Policy /Topic 3.2.2.4.4 Constructed Email to Domain Contact	3.2.2.4.4 Constructed Email to Domain Contact in CP/CPS / Cas follows Sections 3.2.2.4.4 of CA/B Forum Baseline Requirements.
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.	Page 11 of Certification Policy /Topic 3.2.2.4.5 Domain Authorization Document	3.2.2.4.5 Domain Authorization Document in CP/CPS / Cas follows Sections 3.2.2.4.5 of CA/B Forum Baseline Requirements.
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.	Page 11 of Certification Policy /Topic 3.2.2.4.6 Agreed Upon Change to Website -	3.2.2.4.6 Agreed Upon Change to Website in CP/CPS / Cas follows Sections 3.2.2.4.6 of CA/B Forum Baseline Requirements. -
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.	Page 12 of Certification Policy /Topic 3.2.2.4.7 DNS Change	3.2.2.4.7 DNS Change in CP/CPS / Cas follows Sections 3.2.2.4.7 of CA/B Forum Baseline Requirements.
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.	Page 12 of Certification Policy /Topic 3.2.2.4.8 IP Address	3.2.2.4.8 IP Address in CP/CPS / Cas follows Sections 3.2.2.4.8 of CA/B Forum Baseline Requirements.
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.	Page 12 of Certification Policy /Topic 3.2.2.4.9 Test Certificate	3.2.2.4.9 Test Certificate in CP/CPS / Cas follows Sections 3.2.2.4.9 of CA/B Forum Baseline Requirements.
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.	Page 12 of Certification Policy /Topic 3.2.2.4.10. TLS Using a Random Number	3.2.2.4.10 TLS Using a Random Number in CP/CPS / Cas follows Sections 3.2.2.4.10 of CA/B Forum Baseline Requirements.
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.	Page 12 of Certification Policy /Topic 3.2.2.5 Authentication for an IP Address	3.2.2.5 Authentication for an IP Address in CP/CPS / Cas follows Sections 3.2.2.5 of CA/B Forum Baseline Requirements.
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. -	Page 12 of Certification Policy /Topic 3.2.2.6 Wildcard Domain Validation	3.2.2.6 Wildcard Domain Validation in CP/CPS / Cas follows Sections 3.2.2.6 of CA/B Forum Baseline Requirements.
3.2.2.7 Data Source Accuracy Indicate how your CA meets the requirements in this section of the BRs.	Page 12 of Certification Policy /Topic 3.2.2.7 Data Source Accuracy	3.2.2.7 Data Source Accuracy / Cas follows Sections 3.2.2.7 of CA/B Forum Baseline Requirements.
3.2.3. Authentication of Individual Identity	Page 12 of Certification Policy /Topic 3.2.3. Authentication of Individual Identity	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 13 of Certification Policy /Topic 3.2.3. Authentication of Individual Identity	3.2.5 Validation of Authority in CP/CPS / Cas follows Sections 3.2.5 of CA/B Forum Baseline Requirements.
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	Page 13 of Certification Policy /Topic 3.2.3. Authentication of Individual Identity	3.2.6 Criteria for Interoperation / The 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 15 of Certification Policy /Topic 4.1.1. Who Can Submit a Certificate Application	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 15 of Certification Policy / Topic 4.1.2. Enrollment Process and Responsibilities	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 15 of Certification Policy / Topic 4.2.1. Performing Identification and Authentication Functions	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. The CA SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements. If a Delegated Third Party fulfills any of the CA's obligations under this section, the CA SHALL verify that the process used by the Delegated Third Party to identify and further verify High Risk Certificate Requests provides at least the same level of assurance as the CA's own processes.

4.2.2. Approval or Rejection of Certificate Applications	Page 16 of Certification Policy / Topic 4.2.2. Approval or Rejection of Certificate Applications	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 16 of Certification Policy / Topic 4.3.1. CA Actions during Certificate Issuance	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.	page 21 - 22 on Certificate Policy / Topic 4.9.1.1 Reasons for Revoking a Subscriber Certificate	4.9.1.1 Reasons for Revoking a Subscriber Certificate
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate	page 22 on Certificate Policy / Topic 4.9.1.2 Reasons for Revoking a Subordinate CA Certificate	4.9.1.2 Reasons for Revoking a Subordinate CA Certificate
4.9.2. Who Can Request Revocation	page 23 on Certificate Policy / Topic 4.9.2. Who Can Request Revocation	on Topic 4.9.2. Who Can Request Revocation / - The Subscriber may make a request to revoke the certificate for which the subscriber is responsible. - The CA that issues certificates under this CP may make a request to revoke its own certificate. - The 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. - The 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 23 on Certificate Policy / Topic 4.9.3. Procedure for Revocation Request	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) The CA 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) The Issuing CA or RA of the CA verifies and endorses the revocation requests and the related documents. 3) The 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) The Issuing CA with the assistance of RA will approve and process the revocation request. 5) The 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 23 on Certificate Policy / Topic 4.9.5. Time within which CA Must Process the Revocation Request	4.9.5 Time within Which CA Must Process the Revocation Request / The 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 24 on Certificate Policy / Topic 4.9.7. CRL Issuance Frequency	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 24 on Certificate Policy / Topic 4.9.9. On-line Revocation/Status Checking Availability	4.9.9. On-line Revocation/Status Checking Availability / 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 24 on Certificate Policy / Topic 4.9.10. On-line Revocation Checking Requirements	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 24 on Certificate Policy / Topic 4.9.11. Other Forms of Revocation Advertisements Available	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 25 on Certificate Policy / Topic 4.10.1. Operational Characteristics	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 25 on Certificate Policy / Topic 4.10.2. Service Availability	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		
5.2.2. Number of Individuals Required per Task	page 28 on Certificate Policy / Topic 5.2.2. Number of Individuals Required per Task	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 31 on Certificate Policy / Topic 5.2.2. 5.3.1. Qualifications, Experience, and Clearance Requirements	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 32 on Certificate Policy / Topic 5.3.3. Training Requirements	5.3.3. Training Requirements/ The 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 - Use and operation of deployed hardware and software related to CA operations - Security Risk Management - Disaster recovery and business continuity procedures
5.3.4. Retraining Frequency and Requirements	page 32 on Certificate Policy / Topic 5.3.4. Retraining Frequency and Requirements	5.3.4. Retraining Frequency and Requirements / The 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 32 on Certificate Policy / Topic 5.3.7. Independent Contractor Controls	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 33 on Certificate Policy / Topic 5.4.1. Types of Events Recorded	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 Identity of the person making the journal entry;and o Description of the entry.
5.4.3. Retention Period for Audit Logs	page 33 on Certificate Policy / Topic 5.4.3. Retention Period for Audit Logs	5.4.3. Retention Period for Audit Logs / Audit logs are retained for at least 90 days.
5.4.8. Vulnerability Assessments	page 34 on Certificate Policy / Topic 5.4.8. Vulnerability Assessments	5.4.8. Vulnerability Assessments / The CA that issues certificates under this CP must assess security vulnerability at least on a quarterly.
5.5.2. Retention Period for Archive	page 35 on Certificate Policy / Topic 5.5.2. Retention Period for Archive	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 36 on Certificate Policy / Topic 5.7.1. Incident and Compromise Handling Procedures	5.7.1. Incident and Compromise Handling Procedures / The 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 the CA system, the corresponding CA officers shall notify the 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 38 on Certificate Policy / Topic 6.1.1. Key Pair Generation	6.1.1. Key Pair Generation / The 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 38 on Certificate Policy / Topic 6.1.2. Private Key Delivery to Subscriber	6.1.2. Private Key Delivery to Subscriber / The 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 40 on Certificate Policy / Topic 6.1.5. Key Sizes	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 40 on Certificate Policy / Topic 6.1.6. Public Key Parameters Generation and Quality Checking	6.1.6. Public Key Parameters Generation and Quality Checking / Not Applicable.
6.1.7. Key Usage Purposes	page 40 on Certificate Policy / Topic 6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)	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.
6.2. Private Key Protection and Cryptographic Module Engineering Controls	page 40 on Certificate Policy / Topic 6.2. Private Key Protection and Cryptographic Module Engineering Controls	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 40 on Certificate Policy / Topic 6.2.5 Private Key Archival	6.2.5 Private Key Archival / The 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.
6.2.6. Private Key Transfer into or from a Cryptographic Module	page 40 on Certificate Policy / Topic 6.2.6. Private Key Transfer into or from a Cryptographic Module	6.2.6 Private Key Transfer into or from a Cryptographic Module / The 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 40 on Certificate Policy / Topic 6.2.7. Private Key Storage on Cryptographic Module	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 40 on Certificate Policy / Topic 6.3.2. Certificate Operational Periods and Key Pair Usage Periods	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)). Subscriber certificates issued after 1 March 2018 must have a Validity Period no greater than 825 days. Subscriber certificates issued after 1 July 2016 but prior to 1 March 2018 must have a Validity Period no greater than 39 months.
6.5.1. Specific Computer Security Technical Requirements	page 43 on Certificate Policy / Topic 6.5.1. Specific Computer Security Technical Requirements	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 45 on Certificate Policy / Topic 7.1. Certificate profile	7.1 Certificate Profice / Certificate issued by CA under this CP must comply with ITU-T Recommendation X.509 : Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks in which the certificate contains the information show in Table 3.
7.1.1. Version Number(s)	page 45 on Certificate Policy / Topic 7.1.1. Version Number	7.1.1 Version Number / Certificate issued by the CA is in accordance with X.509 version 3.
7.1.2. Certificate Content and Extensions; Application of RFC 5280	page 45 on Certificate Policy / Topic 7.1.2. Certificate Content and Extensions; Application of RFC 5280	7.1.2 Certificate Extensions ; Application of RFC 5280 / This section specifies the additional requirements for Certificate content and extensions for Certificates generated after the Effective Date.
7.1.2.1 Root CA Certificate	page 45 on Certificate Policy / Topic 7.1.2.1 Root CA Certificate	7.1.2.1 Root CA Certificate / Cas follows Section 7.1.2.1 of CA/B Forum Baseline Requirements.
7.1.2.2 Subordinate CA Certificate	page 46 on Certificate Policy / Topic 7.1.2.2 Subordinate CA Certificate	7.1.2.2 Subordinate CA Certificate / Cas follows section 7.1.2.2 of CA/B Forum Baseline Requirements. In addition, for basicConstraints, CA Field set to True and pathlen set to one.
7.1.2.3 Subscriber Certificate	page 46 on Certificate Policy / Topic 7.1.2.3 Subscriber Certificate	7.1.2.3 Subscriber Certificate / Cas follows Section 7.1.2.3 of CA/B Forum Baseline Requirements. In addition, certificatePolicies;policyQualifiers;qualifier;cPSuri must be mandatory.
7.1.2.4 All Certificates	page 46 on Certificate Policy / Topic 7.1.2.4 All Certificates	7.1.2.4 All Certificate / Cas follows Section 7.1.2.4 of CA/B Forum Baseline Requirements.
7.1.2.5 Application of RFC 5280	page 46 on Certificate Policy / Topic 7.1.2.5 Application of RFC 5280	7.1.2.5 Application of RFC 2580 / Cas follows Section 7.1.2.5 of CA/B Forum Baseline Requirements.
7.1.3. Algorithm Object Identifiers	page 46 on Certificate Policy / Topic 7.1.3. Algorithm Object Identifiers	7.1.3. Algorithm Object Identifiers / The OID of digital signature and encryption of certificate is in Table 4. Algorithm Object Identifier RSAEncryption 1.2.840.113549.1.1.1 SHA512withRSAEncryption 1.2.840.113549.1.1.13 SHA512 2.16.840.1.101.3.4.2.3 Table 4 Method of Digital Signature and Encryption with Object Identifier
7.1.4. Name Forms	page 46 on Certificate Policy / Topic 7.1.4. Name Forms	7.1.4 Name from / The name formant of Ussuer and Subject are specified in the certificate as reference to the section 3.1.1 /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	page 46 on Certificate Policy / Topic 7. Certificate, CRL and OCSP Profiles	7.1.4 Name from / The name formant of Ussuer and Subject are specified in the certificate as reference to the section 3.1.1 /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.
7.1.4.2 Subject Information	page 46 on Certificate Policy / Topic 7. Certificate, CRL and OCSP Profiles	7.1.4 Name from / The name formant of Ussuer and Subject are specified in the certificate as reference to the section 3.1.1 /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.
7.1.4.3 Subject Information - Subordinate CA Certificates	page 46 on Certificate Policy / Topic 7. Certificate, CRL and OCSP Profiles	7.1.4 Name from / The name formant of Ussuer and Subject are specified in the certificate as reference to the section 3.1.1 /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.
7.1.5. Name Constraints	page 46 on Certificate Policy / Topic 7.1.5. Name Constraints	7.1.5. Name Constraints / Cas follows Section 7.1.5 of CA/B Forum Baseline Requirements. The Thailand NRCA Root Certificate does not assert Name Constraints. It may be asserted in Thailand NRCA's Subordindate certificate if required.
7.1.6. Certificate Policy Object Identifier	page 46 on Certificate Policy / Topic 7.1.6. Certificate Policy Object Identifier	7.1.6. Certificate Policy Object Identifier / Cas follows Section 7.1.6 of CA/B Forum Baseline Requirements and the issuing Cas MUST define the Certificate Policy OID provided by Thailand NRCA's OID Structure.
7.1.6.1 Reserved Certificate Policy Identifiers	page 46 on Certificate Policy / Topic 7.1.6. Certificate Policy Object Identifier	7.1.6. Certificate Policy Object Identifier / Cas follows Section 7.1.6 of CA/B Forum Baseline Requirements and the issuing Cas MUST define the Certificate Policy OID provided by Thailand NRCA's OID Structure.
7.1.6.2 Root CA Certificates	page 46 on Certificate Policy / Topic 7.1.6. Certificate Policy Object Identifier	7.1.6. Certificate Policy Object Identifier / Cas follows Section 7.1.6 of CA/B Forum Baseline Requirements and the issuing Cas MUST define the Certificate Policy OID provided by Thailand NRCA's OID Structure.
7.1.6.3 Subordinate CA Certificates	page 46 on Certificate Policy / Topic 7.1.6. Certificate Policy Object Identifier	7.1.6. Certificate Policy Object Identifier / Cas follows Section 7.1.6 of CA/B Forum Baseline Requirements and the issuing Cas MUST define the Certificate Policy OID provided by Thailand NRCA's OID Structure.
7.1.6.4 Subscriber Certificates	page 46 on Certificate Policy / Topic 7.1.6. Certificate Policy Object Identifier	7.1.6. Certificate Policy Object Identifier / Cas follows Section 7.1.6 of CA/B Forum Baseline Requirements and the issuing Cas MUST define the Certificate Policy OID provided by Thailand NRCA's OID Structure.
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	page 49 on Certificate Policy / Topic 8. Compliance Audit and Other Assessment	8. Compliance Audit and Other Assessments / Thailand NRCA has a compliance audit mechanism in place to ensure that the requiements of its CPS are being implemented and audited for complying with the following standards:……
8.1. Frequency or circumstances of assessment	page 49 on Certificate Policy / Topic 8.1. Frequency or circumstances of assessment	8.1. Frequency or circumstances of assessment / Cas follows Section 8.1 of CA/B Forum Baseline Requirements.
8.2. Identity/qualifications of assessor	page 49 on Certificate Policy / Topic 8.2. Identity/qualifications of assessor	8.2. Identity/qualifications of assessor / WebTrust auditors must meet the requirements of Section 8.2 of Baseline Requirements.
8.4. Topics covered by assessment	page 49 on Certificate Policy / Topic 8.4. Topics covered by assessment	8.4. 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 audit meets the requirements of the audit schemes highlighted in Section 8 under which the assessment is being made. These requirements may vary as audit schemes are updated. An audit scheme is applicable to CAs in the year following the adoption of the updated scheme.
8.6. Communication of results	page 50 on Certificate Policy / Topic 8.6. Communication of results	8.6. 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 50 on Certificate Policy / Topic 8.7. Self-Audits	8.7 Self-Audits /During the period in which the CA issues Certificates, the CA SHALL monitor adherence to tis Certificate Policy, Certification Pratice Statement and these Requirements and strictly control its service quality by perfoming self audits on at least a quarterly basis againts a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

9.6.1. CA Representations and Warranties	page 54 on Certificate Policy / Topic 9.6.1. CA Representations and Warranties	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 55 on Certificate Policy / Topic 9.6.3. Subscriber Representations and Warranties	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 55 on Certificate Policy / Topic 9.8. Limitations of liability	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	page 55 on Certificate Policy / Topic 9.9 Indemnities	9.9 Indemnities / Is case of the damage occurs to the CA from the actions of subscribers or relying parties, the corresponding CA reserves the right to claim damages.
9.16.3. Severability	page 55 on Certificate Policy / Topic 9.16.3. Severability	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.