BMSP

Certification Authority : Certificate Practice Statement

Ver 1.8

Document Revision History

Date Version Description

Certificate practice Statement

JUL 2024

1.8

Date	Version	Description
12/9/2022	1.0	Initial Released
05/06/2024	1.0.5	Major change Management Reviews and fixed
24/06/2024	1.5	Revised items to comply with Thailand NRCA recommendation.
15/07/2024	1.6	Change the company name to BMSP CA on behalf of BMSP
18/07/2024	1.7	Revised items to comply with Thailand NRCA recommendation.
22/07/2024	1.8	Revised items to comply with Thailand NRCA recommendation.

Table of Contents

List of Tables

1. Introduction

1.1 Overview

BMSP Company Limited (NCL) has been changing the game since its inception in 1991. With a strong focus on innovation and reliability, NCL has become a trusted name in the IT industry. Over the years, they have made strategic investments and founded multiple companies in IT and non-IT-related industries, cementing their position as pioneers.

NCL's IT sector is nothing short of impressive. Bangkok Systems & Software Company Limited offers software development and cybersecurity distribution. At the same time, Bangkok MSP Company Limited provides managed IT services, including IT Operation as a Service, IT Management as a Service, SOC Operation as a Service, and Data Protection as a Service. Their vision is to make top-tier cybersecurity accessible to small and medium-sized businesses without requiring a significant personnel investment.

In addition to their in-house offerings, NCL has a joint venture with Capricorn Identity Services Pvt. Ltd., India's 4th largest local certificate provider. This partnership allows NCL to provide HSM as a Service, reducing ownership costs of PKI-Based digital signing and becoming a Certificate Authority Provider under NRCA in Thailand.

NCL's commitment to Thailand's digital community is unwavering. They founded Bangkok Systems Business Solution to support digital legal compliance with platforms like eTax, eSign, eStamp, eConsent, and more. They aim to create trust in digital identification, documents, contracts, and transactions, providing more flexible methods like integration & API to solve digital challenges for enterprises.

At NCL, they believe in the power of innovation and the importance of building trust in the digital age. With their expertise and dedication, they are leading the charge towards a more secure and reliable digital future.

This document is BMSP CA Certification Practice Statement (CPS). It states the practices that BMSP employs in providing certification services, including without limitation, issuing, managing, revoking, and renewing certificates in accordance with the specific requirements of the BMSP Certificate Policy (CP).

The purpose of this document is to identify a baseline set of security controls and practices to support the secure issuance of certificates. This baseline set of controls has been written in the form of a Certificate Policy (CP). As defined by ITU Recommendation X.509, a Certificate Policy is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements." That is, a Certificate Policy defines the expectations and requirements of the relying party community that will trust the certificates issued by its CAs. The governance structure that represents the relying party is known as Policy Authority (PA). As such, PA is responsible for identifying the appropriate set of requirements for a given community, and oversees the CAs that issue certificates for that community. CAs which operated under Thailand NRCA Trust Model must be conformance to this Certificate Policy.

This CPS also sets out the certification service scope and procedures of BMSP, as well as to specify duties, functions, legal obligations and potential liabilities of participants in the systems used by BMSP. The document structure and topics conform to the Internet Engineering Task Force (IETF) RFC 3647 for Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

1.2 Document Name and Identification

This Certificate Practice Statement is published by BMSP Company Limited (NCL) and specifies the baseline set of security controls and practices that CAs located in Thailand employ in issuing, revoking, or suspending and publishing certificates. And clarify the statements in the certificate policy

Internet Assigned Numbers Authority (IANA) has assigned the country OID 2.16.764 to Thailand. For identification purposes, this Certificate Policy bears an Object Identifier (OID) "2.16.764.1.1.X.X".

Type of policy	Policy OID
Common BMSP OID	2.16.764.1.1.XX
Certificate Policy	2.16.764.1.1.XX
Certificate Practice Statement	2.16.764.1.1.XX

Table 1 Type of Policy

1.3 PKI Participants

1.3.1 Certification Authority

Thailand NRCA is the highest-level Certification Authority, trust anchor, of the PKI domain in Thailand. Thailand NRCA is responsible for managing Subordinate CAs.

1.3.2 Subordinate Certification Authority (Subordinate CA)

The BMSP CA is establish and operate on the infrastructure by Bangkok MSP Co,Ltd . The BMSP Certification Authority responsible issuance of a digital certificate to a person or legal entity by using a collection of hardware, software, personnel, and operating procedures that create, sign, and issue certication of public key for Subscribers and for publication of Certificate Revocation List, also known as CRL in accordance with CP/CPS regulations.

A Subordinate Certification Authority (Subordinate CA) responsible for issuance and management of Subscriber certificates including:

1) Approving the issuance of certificates
2) Publication of certificates
3) Revocation of certificates
4) Publication of certificate status information through Certificate Revocation Lists (CRLs) and/or Online Certificate Status Protocol (OCSP) responders
5) Subordinate CA key and certificate life cycle management
6) Establishment and maintenance of its Certificate Policy (CP) and Certification Practice Statement (CPS)
7) Ensuring that all aspects of the CA services, operations, and infrastructures are performed in accordance with this Certificate Policy.

1.3.3 Registration Authority

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.

1.3.4 Subscribers

The term "Subscriber" as used in this CPS refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information. CAs who want to subscribe a certificate from BMSP for signing and issuing certificates or certificate status information, and so become a subscribers CA of BMSP and will be qualified as Subscribers.

Certificate Entity	Subscriber
Person	Individual
Enterprise	Trustee of Authorized Organisation
Legal Entity	

Table 2 Certificate Entity

1.3.5 Relying Parties

A Relying Party is a person or entity that acts in reliance on the validity of the binding of the Subscriber's name to a public key. The Relying Party uses a Subscriber's certificate to verify a digital signature that is generated using the private key corresponding to the public key listed in a certificate. A Relying Party may or may not be a Subscriber of the BMSP.

1.3.6 Other Participants

1.3.6.1. Policy Authority

Policy Authority (PA) decides that a set of requirements for certificate issuance and use are sufficient for a given application. PA has roles and responsibilities as follows:

1. Establish certificate policy and certification practice statement of BMSP and other certification authorities under the Thailand NRCA trust model.
2. Arrange for a review of certificate policy and certification practice statement of BMSP and other certification authorities under the Thailand NRCA trust model on a regular basis.

1.3.6.2. Third Party

The BMSP CA selects other authorities, which provide related trust services, such as time stamp authority (TSA), Trust Management Module and Data Centre Co-host as the collaborative partners, the related information shall be disclosed on the website and the collaboration mechanism and mutual rights and obligations shall be describe in the CPS.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The usage of a certificate issued under Trust model of BMSP is limited to support the following core security needs. The appropriate certificate uses are follows:

1) Natural Person Certificates are issued to individuals or generic civilians for security of electronic transactions. Valid for 1 or 2 years.
2) Juristic Person Certificates are issued to legal persons including governmental or private organizations or companies for security of electronic transactions. Valid for 1 or 2 years.
3) Enterprise User Certificates are issued to officials of an organization including governmental or private organizations or companies for security of electronic transactions. Valid for 1 or 2 years.
4) TLS/SSL Certificate are used for Web Server Authentication. Valid for 1 year.
5) S/MIME Certificate are used for Secure e-mail Valid for 1 year.

Applicable Type of Certificate	Appropriate Use
Natural Person Certificate Juristic Person Certificate Enterprise User Certificate	Used in the process of digitally signing a document, this ensures that the portion of the document signed by the signer remains unmodified.

TLS/SSL Certificate	Use to secure web server communication. TLS/SSL Certificate provide encryption and authentication for data transmitted between a web server and a web browser.
S/MIME Certificate	Use to secure electronic-mail communication. S/MIME Certificate provide encryption and authentication for data transmitted between a Mail server and application or e-mail client.

Table 3 Applicable Type of Certificate

1.4.2 Prohibited Certificate Uses

A certificate issued in accordance with this CPS shall be used only for the purpose as specified in Section 1.4, and in particular shall be used only to the extent the use is consistent with applicable laws.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Policy Creation Authority of the Certificate Authority

1.5.2 Contact Person

If you have any questions regarding this CPS or a subscriber wishes to report a missing key, you may directly contact the BMSP CA.

The Director of BangkokMSP
Bangkok MSP Company Limited
555/2, Floor B, SSP Tower, Soi Sukhumvit 63 (Ekamai),Kwang Klongton Nua, Khet Wattana, Bangkok 10110 THAILANDTel: (+662) 0927464
Email: NCLCA@bmsp.tech
Website: Https://bmsp.tech

1.5.3 Person Determining CPS Suitability for the Policy

The BMSP CA shall first check whether the CPS conforms to relevant CP regulations and then submit the CPS to the Policy Authority for review and approval. After approval, BMSP CA shall officially use the CP/CPS.
In accordance with the regulations defined in the Electronic Transactions Act, the CPS established by the CA must be approved by the competent authority, before it is provided externally for certificate issuance service.

1.5.4 CPS Approval Procedures

BMSP proposes any changes of CPS must be approved by the PA of the Certificate Authority before the change is effective.

After the change approved by the PA and the CPS revisions take effect, the revised CPS content shall take precedence in the event of a discrepancy between the revised and original content. If the revisions are made by attached document, the attached documents shall take precedence in the event of discrepancy between the attached documents and the original CPS. the Version of the CP/CPS shall be revised in the Change Log section before it is published CPS to the channel as listed in Section 2.2.

1.5.5 Review and Update Procedures

BMSP SHALL review the latest SSL/TLS and S/MIME Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates, and the Network and Certificate System Security Requirements from https://cabforum.org/ at least quarterly for the purpose of developing, implementing, and enforcing, and update the Certificate Policy and Certification Practice Statement annually.

1.6 Definitions and Acronyms

1.6.1 Definitions

See Table 4 for a list of definitions.

Term	Definition
Certificate	A form of electronic documents used for verifying the relationship between entities and public key. A certificate is issued in compliance with ITU-T Recommendation X.509 RFC 5280, Baseline Requirements of CA/Browser Forum and NRCA Recommendation.Information technology - Open systemsinterconnection - The Directory: Public-key and attribute certificate

	frameworks and ISO/IEC 9594-8:2008 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks.
Certificate Policy (CP)	The document, which is entitled “BMSP Certificate Policy”, describes the principal statement and applications of certificates.
Certificate Repository	Source for storage and publication of certificates and certificate revocation lists.
Certificate Revocation	A certificate may be revoked prior to its expiration date. Once revoked, it can no longer be used.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew certificates.
Certification Practice Statement (CPS)	The document, which is entitled “Thailand National Root Certification Authority Certification Practice Statement”, describes the procedures and scope of the certification authority, duties and obligations of the parties that acts in reliance of a certificate.
Cryptographic Module	Specialized equipment used to maintain, manage and operate the key pair.
Digital Signature	A Digital Signature is a mathematical scheme for demonstrating the authenticity and integrity of a digital message or document.
Directory Service	A storage for publication of certificates and certificate revocation lists following the X.500 Standard or LDAP.
Entity	Individual, Server, Operating Unit / Site, or any Device that is under the control of the individual.
Key Pair	A Key Pair refers to two separate keys of the asymmetric cryptographic system, one of which is secret (Private Key) and another is public (Public Key). The two parts of the key pair are mathematically linked in the ways that one key locks or encrypts the plaintext, and the other unlocks or decrypts the cipher text. Neither key can perform both functions by itself.

	The Key Pair can be used to authenticate the digital signature as well as maintain confidentiality of information.
OCSP (Online Certificate Status Protocol)	A protocol used for verifying status of a certificate.
Private Key	The key used to create a digital signature and can be used to decrypt the message that is encrypted with its pair of public key, to obtain the original message
Public Key	The key used to verify a digital signature to ensure the integrity of electronic message and also to encrypt message to maintain its confidentiality.

Table 4 Terms and Definitions

1.6.2 Acronyms

See Table 5 for a list of acronyms.

Acronym	Term
CA	Certification Authority
CAA	Certification Authority Authorization
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DNS	DNS Domain Name System
ETDA	Electronic Transactions Development Agency
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name.
DN	Distinguished Name
NRCA	National Root Certification Authority
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
SSL	Secure Sockets Layer

TLS	Transport Layer Security

Table 5 A list of Acronyms

2. Publication and Repository Responsibilities

2.1 Repositories

Issuer CAs that issue certificates under this CPS 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 (URLI) references asserted in valid certificates issued by that CA. Issuer CAs shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information and promote consistent access to certificates and CRLs.

2.2 Publication of Certification Information

Issuer CAs shall makes information publicly aviailable on the web such as CPs, CPSs, Certificates and CRLs and related information in repositories.. It shall ensure that its repository or repositories are implemented through trustworthy systems.

2.3 Time or Frequency of Publication

The Certificate will be published on the X.500 Directory immediately on issuance within seven calendar days after accepting issuance by an upper level CA (NRCA Thailand).
The Certificate Authority will keep the Certificate Policy/Certificate Practice Statement up to date and published on their website (https://www.bmspca.tech) as reference for all Subscribers and general public within a working day of the approval of changes.
The latest versions of CRLs are published within 24 Hours after updating and of their approval (See section4.9.7 and 4.9.9. for additional details.)

2.4 Access Controls on Repositories

The BMSP CA has implemented logical and physical access control as well as network security measures to authenticate and restrict modification or deletion to the repository. The adding, deleting, or modifying repository entries can be performed only by authorized personnel of BMSP. And the BMSP website is used as repositories for Subscribers and Relying Parties to access the publication documents.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

BMSP Certificates contain a Distinguished Name (DN) in the Issuer and Subject fields, following the X.501 Information technology – Open Systems Interconnection – The Directory: Models. The Distinguished Names consist of the components specified in Table 4 below.

Attribute Name	Value
Country (C) =	TH
Organization (O) =	BMSP(Public Organization) or <organization name>
Common Name (CN) =	Thailand National Root Certification Authority - G1 or <certification authority name>

Table 6 Type of Name

3.1.2 Need for Names to be Meaningful

The names contained in a certificate must be in English with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the certificate, for example, through the verification of Jurisdiction of Incorporation and/or Certificate of Registration issued by the Department of Business Development, Ministry of Commerce.

3.1.3 Anonymity or Pseudonymity of Subscribers

BMSP does not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in X.501 standard. Rules for interpreting e-mail addresses are specified in RFC 2822.

3.1.5 Uniqueness of Names

The distinguished names of CA subscriber must be unique within the domain of BMSP CA. Depending on the type of certificate (SSL, SMIME) different elements/attributes of the certificate ensure uniqueness.

3.1.6 Recognition, Authentication, and Role of Trademarks

BMSP CA reserves no liability to any certificate applicant on the usage of Distinguished Names appearing in a certificate. The right to use the name is the responsibility of the applicant and must be in accordance to the relevant laws, regulations, legal obligations or announcements.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The Subscriber self generates the key pairs and creates the PKCS#10 Certificate Signing Request and signs it with the private key. When applying for a certification, the Certificate Signing Request is submitted to the RA. The RA shall use the Subscriber's public key to verify the signature on the Certificate Signing Request to prove that the Subscriber is in possession of the corresponding private key.

3.2.2 Authentication of Organization Identity

CA Subscribers will submit their applications for certificates with the its name, business address in Thailand, and the Certificate of Corporate Registration of the CA issued by the Department of Business Development, Ministry of Commerce. BMSP verifies the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA.

3.2.2.1 Identity

CA Subscribers will submit their applications 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 and verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1). A government agency or Incorporating Agency or Registration Agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;

2). A third party database that is periodically updated and considered a Reliable Data Source;

3). A site visit by the BMSP CA or a third party who is acting as an agent for the BMSP CA; or

4). An Attestation Letter.

The BMSP CA may use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.

Alternatively, BMSP CA may verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government- issued tax document, or other form of identification that BMSP CA determines to be reliable.

The certification documents shall be affixed with the seal of the organization and responsible person The RAO shall check the authenticity of the application information submitted by the organization and representative identity and verify that the representative has the right to apply for the certificate in the organization's name, the organization must submit the correct certification documents which have been approved by the competent authority or a legally authorized body (such as a court) to the RAO.

Suppose the organization has completed the registration procedure with the competent authority or completed the counter or online process identification and authentication procedure by the CA, RA or CA-trusted authority or individual of the CA or RA in compliance with the above counter or online process identification and authentication procedure or complete Thailand e-KYC (Electronic Know Your Customer) regulation for identification and authorization mechanism and left behind registration or supporting information for identification and authentication before certificate application. In that case, the CA or RA may allow the submission of supporting information during certificate application in place of the above identification and authentication methods.

3.2.2.2 DBA/Tradename

BMSP CA verifies DBA/tradename when the Subject Identity Information included. Verification the Applicant's right to use the DBA/tradename using at least one of the following:

1). Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;

2). A Reliable Data Source

3). Communication with a government agency responsible for the management of such DBAs or tradenames;

4). An Attestation Letter accompanied by documentary support; or

5). A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

3.2.2.3 Verification of Country

Issuer CAs SHALL verify the information for Subordinate CAs using the following sources:

1) Commercial entities: The Department of Business Development (DBD)
2) Noncommercial Thai entities: Authorized Thai government organization/agencies
3) Foreign entities: The authorized national government/agencies of that country.

3.2.2.4 Validation of Domain Authorization or Control

BMSP CA employs the approved methods to confirm that the Subscriber requesting a certificate possesses the proper authority or control over the domain.

The Subscriber is required to demonstrate control over the domain (DNS-Based Validation) by either creating a DNS record with a unique value provided by BMSP CA, which can be validated by querying the DNS record from the Internet, or by following the instructions in a message sent to the email address of the domain’s Subscriber, technical, or administrative contact as listed in the domain’s WHOIS record.

A message is sent to the email address of the domain's Subscriber, technical, or administrative contact as listed in the domain's WHOIS record. This email contains important instructions and verification steps for the domain validation process.

In compliance with the CA / Browser Forum *Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates* for each Fully-Qualified Domain Name listed in a Certificate, BMSP CA confirms that, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by using one or more of the following methods:

3.2.2.4.1 Validating the Applicant as a Domain Contact

This method of domain validation is not used.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Communicating a Random Value via email, fax, SMS, or postal mail to a Domain Contact and receiving a confirming response utilizing the Random Value to the request for approval.

3.2.2.4.3 Phone Contact with Domain Contact

This method of domain validation is not used.

3.2.2.4.4 Constructed Email to Domain Contact

Communicating with the Domain's administrator by (1)Using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@") and an Authorization Domain Name. (2) Include a random value in the email. (3) Receiving a confirming response utilizing the Random Value.

3.2.2.4.5 Domain Authorization Document

This method of domain validation is not used.

3.2.2.4.6 Agreed-Upon Change to Website

This method of domain validation is not used.

3.2.2.4.7 DNS Change

Confirm the Applicant's control over the FQDN by confirming the presence of a Random Value in a DNS CNAME, TXT or CAA record for an ADN or an ADN that is prefixed with a label that begins with an underscore character.

If a Random Value is used, the CA or RA shall provide a Random Value unique to the Certificate request and shall not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for the reuse of validated information relevant to the Certificate.

3.2.2.4.8 IP Address

No IP address certificates are issued under this CPS.

3.2.2.4.9 Test Certificate

This method of domain validation is not used.

3.2.2.4.10 TLS Using a Random Number

This method of domain validation is not used.

3.2.2.4.11 Any Other Method

This method of domain validation is not used.

3.2.2.4.12 Validating Applicant as a Domain Contact

Confirming the Applicant is the Domain Name Contact directly with the Domain Name Registrar by determining that the Domain was registered using the same account as the certificate.

3.2.2.4.13 Email to DNS CAA Contact

Confirm the Applicant's control over the FQDN by emailing a Random Value and then receiving a confirming response utilizing the Random Value. The Random Value will be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set will be found using the search algorithm defined in RFC 8659 Section 3.

Each email may confirm control of multiple FQDNs, provided each email address is a DNS CAA Email Contact for each ADN Name being validated. The same email may sent to numerous recipients as long as all recipients are the DNS CAA Email Contacts for each ADN being validated.

The Random Value shall be unique in each email. The email may be re-sent, including reusing the Random Value, provided its contents and recipient(s) remain unchanged. The Random Value shall remain valid for a confirming response for 30 days from its creation.

3.2.2.4.14 Email to DNS TXT Contact

This method of domain validation is not used.

3.2.2.4.15 Phone Contact with Domain Contact

Confirm the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the ADN. Each phone call may confirm control of multiple ADNs provided the same Domain Contact phone number is listed for each ADN being verified, and they offer a confirming response for each ADN.

If someone other than a Domain Contact is reached, the CA may request to be transferred to the Domain Contact.

If the CA reaches voicemail, it may leave the Random Value and the ADN(s) being validated. The Random Value must be returned to the CA to approve the request.

The Random Value shall remain valid for a confirming response for 30 days from its creation.Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

This method of domain validation is not used.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

This method of domain validation is not use.

3.2.2.4.18 Agreed‑Upon Change to Website v2

v

(i) The entire Request Token or Random Value must not appear in the request used to retrieve the file, and

(ii) the CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Number:

(iii) Must be located on the Authorization Domain Name and

(iv) Must be located under the "/.well-known/PKI-validation" directory and

(v) Must be retrieved via either the "http" or "https" scheme, and

(vi) Must be accessed over an Authorized Port.

The CA follows redirects, and the following apply:

(vii) Redirects must be initiated at the HTTP protocol layer.

a. For validations performed on or after July 1, 2021, redirects will only be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects must be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.

b. For validations performed before July 1, 2021, redirects will only result from an HTTP status code result within the 3xx Redirection class of status codes, as defined in RFC 7231, Section 6.4.

(viii) Redirects must be to resource URLs either via the "http" or "https" scheme.

(ix) Redirects must be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

(x) The CA must provide a Random Value unique to the certificate request.

(xi) The Random Value must remain valid in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA must follow its CPS.

Note: Once the FQDN has been validated using this method, the CA also does NOT issue certificates for other FQDNs that end with all the labels of the validated FQDN. This method is NOT suitable for validating Wildcard Domain Names. Thailand NRCA does not issue Subscriber Certificates.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

This method of domain validation is not used.

3.2.2.4.20 TLS Using ALPN

This method of domain validation is not used

3.2.2.5 Authentication for an IP Address

No IP address certificates are issued under this CPS

No IP address certificates are issued under this CP.

3.2.2.5.1 Agreed-Upon Change to Website

This method of IP Address validation is not used.

3.2.2.5.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

This method of IP Address validation is not used.

3.2.2.5.3 Reverse Address Lookup

This method of IP Address validation is not used.

3.2.2.5.4 Any Other Method

This method of IP Address validation is not used.

3.2.2.5.5 Phone Contact with IP Address Contact

This method of IP Address validation is not used.

3.2.2.5.6 ACME “http-01” method for IP Addresses

This method of IP Address validation is not used.

3.2.2.5.7 ACME “tls-alpn-01” method for IP Addresses

This method of IP Address validation is not used.

3.2.2.6 Wildcard Domain Validation

BMSP CA employs the approved methods to confirm that the Subscriber requesting a certificate possesses the proper authority or control over the wildcard domains.

"The Subscriber is required to demonstrate authority or operational control over the entire domain, encompassing all subdomains covered by the wildcard certificate. This verification can be accomplished through the same methods outlined in standard domain validation (section 3.2.2.4). However, additional validation checks are necessary to ensure control over the wildcard domain. These additional validation methods include but are not limited to: Performing DNS-based validation not only for the primary domain but also for a representative sample of subdomains, thereby confirming control across the entire wildcard scope. Obtaining explicit documented approval from individuals or groups responsible for the domain's administration, especially when different subdomains have distinct administrative contacts. These measures are essential to ensure comprehensive control over the wildcard domain.

3.2.2.7 Data Source Accuracy

Before using any data source as a Reliable Data Source, BMSP CA shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification.

Criteria for this evaluation shall include:

- The age of the information provided
- The frequency of updates to the information source
- The data provider and purpose of the data collection
- The public accessibility of the data availability, and
- The relative difficulty in falsifying or altering the data.

For S/MIME Certificates, Enterprise RA records are a Reliable Data Source for Individual Subject attributes included in Sponsor-validated Certificates issued to the Enterprise RA's Organization.

Prior to using any data source as a QIIS, BMSP CA SHALL:

1. Ensure that:
    1. Industries other than the certificate industry rely on the database for accurate location, contact, or other information; and
    2. The database provider updates its data on at least an annual basis.
2. Check the accuracy of the database and ensure its data is acceptable, including reviewing the database provider's terms of use. In particular, BMSP SHALL NOT use any data in a QIIS that BMSP CA knows is
    1. self-reported and
    2. not verified by the QIIS as accurate.BMSP CA does not issue Subscriber Certificates.

3.2.2.8 CAA Records

The Certificate Authority provides certificate authority authorization service from the Subscriber’s CAA record, provided the CAA record is set to “BMSP.tech”.

The authorization process consists of confirmation whether the SSL Certificate uses BMSP.tech as the CAA record. If not, the RA will not issue an SSL certificate. The CAA record can be accessed via https://dnschecker.org/#CAA/google.com.

The Subscriber must be set DNS Values follow the table.

SSL Brand	Record Type	Flags	Tag	Value/Answer/Destination
BMSP	CAA	0	issue	BMSP.tech

Table 7 CAA Record

3.2.2.9 Validation of Mailbox Authorization or Control

This section defines the permitted processes and procedures for confirming the Applicant's control of Mailbox Addresses to be included in issued Certificates.

BMSP CA SHALL verify that Applicant controls the email accounts associated with all Mailbox Fields referenced in the Certificate or has been authorized by the email account holder to act on the

BMSP CA SHALL NOT delegate the verification of mailbox authorization or control.

Completed validations of the Applicant authority **may** be valid for issuing multiple Certificates over time. In all cases, Validation must have been initiated within the period specified in the relevant requirement (Section 4.2.1) before Certificate issuance.

3.2.2.9.1 Validating authority over mailbox via domain

BMSP CA MAY confirm the Applicant, such as an Enterprise RA, has been authorized by the email account holder to act on the account holder's behalf by verifying the entity's control over the domain portion of the Mailbox Address to be used in the Certificate.

An Applicant that confirms control of the domain part of an email address is authorized for any local part followed by the at-sign ("@"), followed by the Authorization Domain Name or by any other Domain Name that ends with all the Domain Labels of the validated Authorization Domain Name.

BMSP CA SHALL use only the approved methods described in Section 3.2.2.4 to perform this verification. The Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate for domain validation.

3.2.2.9.2 Validating control over mailbox via email

BMSP CA MAY confirm the Applicant's control over each Mailbox Field to be included in a Certificate by sending a Random Value via email and then receiving a confirming response utilizing the Random Value.

Control over each mailbox address shall be confirmed using a unique Random Value. The random value shall be sent only to the email address being validated and shall not be shared in any other way.

The Random Value SHALL be unique in each email and remain valid in a confirming response for no more than 24 hours from its creation.

The Random Value SHALL be reset upon each instance of the email sent by BMSP CA to a Mailbox Address. However, all relevant Random Values sent to that Mailbox Address MAY remain valid for use in a confirming response within the validity period described in this Section.

In addition, the Random Value SHALL be reset upon the user's first use if it is intended for additional use as an authentication factor following the Mailbox Address verification.

3.2.2.9.3 Validating applicant as operator of associated mail server(s)

BMSP CA MAY confirm the Applicant's control over each Mailbox Field to be included in the Certificate by confirming control of the SMTP FQDN to which a message delivered to the Mailbox Address should be directed. The SMTP FQDN SHALL be identified using the address resolution algorithm defined in RFC 5321 Section 5.1, which determines which SMTP FQDNs are authoritative for a given Mailbox Address. If more than one SMTP FQDN has been discovered, BMSP CA SHALL verify control of an SMTP FQDN following the selection process at RFC 5321 Section 5.1. Aliases in MX record RDATA SHALL NOT be used for this validation method. To confirm the Applicant's control of the SMTP FQDN, BMSP CA SHALL use only the currently approved methods described in Section 3.2.2.4.

3.2.3 Authentication of Individual Identity

There are regulations regarding identification documents, checking procedure as shown in sub sections.

3.2.3.1 In-person Verification

The applicant must verify his / her identity in person at the BMSP CA. The RA must check written documentation: The applicant shall provide information which includes name, ID number and at least present at least one original approved photo ID (such as national ID card) during certificate application to the RAO to authenticate the applicant’s identity.

If an applicant (such as minor under 18 years old) is unable to submit the above photo ID, government issued written documentation (such as household registration) sufficient to prove the identity of the applicant and one adult with legal capacity to guarantee the applicant's identity in writing may be used in its place. The identity of the adult providing the written guarantee must pass through the above authentication.

3.2.3.2 e-KYC Verification

The applicant shall provide at least following information:

1). Government Issue Photo ID

2). Government Issue Verification Challenge

3). Mobile Number

BMSP CA shall verify validity and ownership of specify mobile number. The likeness of the individual is compared to the Photo ID. The information of Photo ID is inspected with issued government sector using verification challenge. This method requires that the applicant has access to an internet-enabled device, a working webcam or other video equipment.

Entities that can perform this verification:

1). Certificate Authority (CA)

2). Registration Authority (RA)

The system will verify user information with the Authoritative Source (AS) from government sector to ensure the correctness of user profile, and the operator of the system will verify the correctness of the uploaded information and images.

Alternatively, BMSP CA may verify the Applicant entity through the Government Sector, Trust Enterprise, third-party KYC, BMSP KYC, or email verification methods.

3.2.4 Non-verified Subscriber Information

Information that is not verified shall not be included in certificates.

3.2.5 Validation of Authority

When there is a connection between a certain individual and the certificate subject name when performing a certificate lifecycle activity such as a certificate application or revocation request, the BMSP CA or the RA shall perform a validation of authority to verify that the individual can represent the certificate subject such as:

1). Authorized Representative Appointment Letter from the relevant juristic person or other document of the same kind, corporate sealed and signed by the authorized representative 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.

2. A certified true copy of identification card or passport of the authorized representative of the juristicperson. The RA verifies and endorses the integrity of documents.

For certificates issued by the BMSP CA to organizations and individuals, if the e-mail address is recorded in the certificate subject name field for secure e-mail use, the RA shall use the following method to verify the certificate applicant is able to control the e-mail account recorded on the certificate: Use the RA system to send e-mails requesting the subscriber to click on reply or input a certification code during certificate application to verify that the e-mail address is owned by that person.

3.2.6 Criteria for Interoperation

Not Applicable.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Identification and authentication requirements are specified in Section 3.2

3.3.2 Identification and Authentication for Re-key after Revocation

Identification and authentication requirements are specified in Section 3.2.

3.4 Identification and Authentication for Revocation Request

Identification and authentication requirements are specified in Section 3.2.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Applicants may be individuals applying for Individual Certificates or individuals authorized to apply for Enterprise Certificates on behalf of their company to maintain the security of their electronic transactions. They may apply for Certificates listed in section 1.3.

4.1.2 Enrollment Process and Responsibilities

The BMSP CA and the RA, ensuring that the procedure complies with the CP and CPS provisions, rely on the certificate applicant to provide accurate and sufficient information. This includes details such as the organization's legal name or code, the certificate applicant's name or website fully qualified domain name, all based on the specific certificate type. By doing so, the certificate applicant plays a crucial role in the issuance process, making them an integral part of the system.

1) The subscriber shall follow the relevant application regulations, as outlined in the Certificate Practice Statement (CPS), and verify the accuracy of the information submitted for the application.

2) After the BMSP CA approves the certificate application and issues the certificate, the subscriber shall accept it in accordance with the regulations in section 4.4 of the CPS, which detail the acceptance process.

3) After receiving the certificate issued by the BMSP CA, the subscriber must diligently verify the accuracy of the information on the certificate and adhere to the regulations in section 1.4.1 of the CPS for its usage. These regulations specify the acceptable uses and restrictions of the certificate. In the event of any discrepancy in the certificate information, the subscriber must promptly notify the RA and refrain from using the certificate until the issue is resolved.

4) The subscriber's responsibility extends to the safeguarding and responsible use of their private key. This key is not just a component of the certificate's security, but a crucial one. Any negligence in its handling can lead to serious consequences. By emphasizing this, we aim to underline the importance of the subscriber's role in maintaining the security of the system.

5) If a subscriber certificate must be suspended, restored, revoked, or reissued, the subscriber shall follow the regulations in Chapter 4. If a certificate needs to be revoked due to the leakage or loss of private key information, the subscriber shall promptly notify the RA, but the subscriber shall still bear the legal responsibility for using that certificate before the change.

6) The subscriber shall carefully select computer environments and trustworthy application systems. If the rights of relying parties infring upon due to factors such as the computer environment or application system, the subscriber shall bear sole responsibility.

7) If the BMSP CA is unable to operate normally for some reason, the subscriber shall speedily seek other ways for completion of legal acts and may not be used as a defense to others.

8) For the TLS/SSL Certificate Application, the applicant must update the CAA Record on the domain host's DNS server to Https://www.bmspca.tech

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The BMSP CA and the RA shall ensure that the system and procedure are sufficient to verify that the subscriber identity complies with CP and CPS regulations. The initial registration procedure implement to comply by the rules in section 3.2 of the CPS. The certificate applicant shall submit correct and complete factual information. The information required for the certificate application shall contain required and optional information.
Only the information listed on the certificate profile presented on the certificate. The information submitted by the certificate applicant and contact records kept by the CA and RA during the application process shall be properly maintained in a secure, auditable manner by CP and CPS regulations.

4.2.2 Approval or Rejection of Certificate Applications

The BMSP CA should review the registration from the electronic certificate application and supporting evidence for completeness and authenticity before issuing the certificate. In cases where some part or entirety of the electronic certificate application is either incorrect or incomplete, In case of

1) Submitted by document the RA will return the document to the Subscriber with an explanation.

2) Submitted by e-document via the RA portal the RA will maintained properly and notify to the Subscriber with an explanation.

4.2.3 Time to Process Certificate Applications

After receiving the application, the Registration Authority will verify the supporting evidence. The electronic certificate will be issued within the next operating day if the supporting evidence is complete.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

1) The Certificate Authority will verify the supporting evidence and CSR file (if any) from the Subscriber for congruence and notify the Subscriber if any discrepancies are found.
2) Once verified, the Registration Authority will record the registrar will record the information from the electronic certificate application and issue the certificate.
3) The registrar will verify the issued certificate and information on the issued certificate.
4) The registrar delivers the electronic certificate to the Subscriber by appropriate means.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

BMSP CA may deliver Certificates securely within a reasonable time after issuance. Generally, BMSP CA delivers Certificates via email to the email address designated by the Subscriber during the application process.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The Certificate Authority will only recognize the Subscriber's Certificate Acceptance when the Subscriber has completed the following steps:

1. The Subscriber uses the notify email to activate the certificate through the website.
2. The Subscriber signs and sends the certificate acceptance form to the CA.

The CA will only activate the certificate if the Subscriber has used email to activate the certificate and the Subscriber has sent the signed certificate acceptance form back to the CA.

4.4.2 Publication of the Certificate by the CA

All certificates shall be published in repositories. Publication arrangements of subscriber certificate are specified in the CPS of the issuing CA.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

CAs operation under this CP will notify the subscriber via email.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers refer to entities that request and obtain certificates approved by the BMSP CA. Their relationship with the certificate subject is shown in section 1.3.3. The use of certificates is stipulated in section 1.4.1. Subscriber key pair generation shall comply with the regulations in section 6.1.1. Subscribers must independently possess and control the right and capability to the private key corresponding to the certificate. Subscribers themselves do not issue certificates to others. Subscribers shall protect the private key from unauthorized use or disclosure. The Subscriber shall only use the Private keys for correct keyUsages (key usages listed in the keyUsages extension of the certificate) such as digitalSignature or keyEncipherment. Subscribers must correctly use certificates according to the certificatePolicies extension listed on the certificates.

4.5.2 Relying on Party Public Key and Certificate Usage

The parties responsible for using the public key or certificate shall follow the regulations and conditions for each certificate category issued by the CA. Relying parties must refer to and verify the certificate status described in the Certificate Policy/Certification Practice Statement.

4.6 Certificate Renewal

Certificate renewal means the issuance of a new Certificate without changing the Public Key or any other information in the Certificate. Certificate renewal is not allowed by The CP and CPS.

4.6.1 Circumstance for Certificate Renewal

Not Applicable.

4.6.2 Who May Request Renewal

Not Applicable.

4.6.3 Processing Certificate Renewal Requests

Not Applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not Applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not Applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not Applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not Applicable.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

The certificate subscriber's private key shall be routinely re-keyed by the regulations in section 6.3.2 governing the certificate subscriber's private key usage period.

The subscribers who hold certificates, if the certificate has not been revoked, the BMSP CA or the RA may start to process the re-key and new certificate application one month before the Subscriber's private key usage period expires. The regulations in sections 4.1 and 4.2 implement the new certificate application procedures. After the subscriber certificate is revoked, its private key is suspended. After the key pair is re-keyed, a new certificate may be applied for with the CA or RA in accordance with the regulations in section 4.2.

4.7.2 Who May Request Certification of a New Public Key

A subscriber or legally authorized third party (representative authorized by the organization) may submit a subscriber certificate application with the BMSP CA.

4.7.3 Processing Certificate Re-keying Requests

A new certificate application is submitted to the BMSP CA. The procedures of certificate re-keying requests as specified in Section 3.1, 3.2, 3.3, 4.1 and 4.2 of the CPS.

4.7.4 Notification of New Certificate Issuance to Subscriber

The Notification to subscriber certificates re-key shall notify the result of new certificate issuance to the Subscriber according to the procedures specified in Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

The section 4.7.5 in the Thailand NRCA CPS for circumstances constituting the BMSP CA's acceptance of the CA certificate re-key. The Subscriber's re-key procedure is specified in sections 4.1, 4.3 and 4.4.

4.7.6 Publication of the Re-keyed Certificate by the CA

The BMSP CA that issues certificates under this CP shall publish the re-keyed according to the procedure in Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The BMSP CA that issues certificates under this CP shall notify the result of certificate issuance to other entities according to the procedure in Section 4.4.3.

4.8 Certificate Modification

For the BMSP CA CP/CPS, “certificate modification” means issuing a new certificate with non-essential information changed without changing the Key Pair related to the original certificate.

4.8.1 Circumstance for Certificate Modification

Modifying a Certificate means creating a new Certificate for the same subject with authenticated information that differs slightly from the old Certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with this CPS. The new certificate may have the same or a different subject, such as a public key.

Any re-issuance of a certificate in which information other than the Key Pair changes, shall be considered certificate modification. The original Certificate may be revoked after modification is complete, but the original Certificate shall not be further renewed, re-keyed or modified.

4.8.2 Who May Request Certificate Modification

Not Applicable.

4.8.3 Processing Certificate Modification Requests

Not Applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not Applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not Applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not Applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not Applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

The BMSP CA SHALL revoke a Subscriber Certificate within seven (7) days if one or more of the following occurs:

1) Private key lost, stolen, modified, disclosed without authorization or has been subject to other damage or misuse
2) The information listed on the certificate is sufficient to have a significant effect on subscriber trust.
3) Certificate is no longer needed for use.
4) The Subscriber does not authorize the original certificate request, and the Subscriber is unwilling to grant authorization retroactively.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

BMSP CA will revoke a Subordinate CA Certificate within seven (7) days after receiving and confirming one or more of the following occurred:

1) The Subordinate CA requests revocation in writing;
2) The Subordinate CA notifies BMSP CA that the original Certificate request was not authorized and does not retroactively grant authorization;
3) BMSP CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a key compromise or no longer complies with the requirements of sections 6.1.5 and 6.1.6 of the applicable Baseline Requirements or any section of the Mozilla Root Store policy;
4) BMSP CA obtains evidence that the CA Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement;
5) BMSP CA confirms that the CA Certificate was not issued by or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6) BMSP CA determines that any of the information appearing in the CA Certificate is inaccurate or misleading;
7) BMSP CA or the Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CA Certificate;

8) BMSP CA or the Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated unless DigiCert has made arrangements to continue maintaining the CRL/OCSP Repository;
9) Revocation is required by BMSP CA Certificate Policy and/or Certification Practice Statement or
10) The technical content or format of the CA Certificate presents an unacceptable risk to application software suppliers or Relying Parties.

4.9.2 Who Can Request Revocation

1) The Subscriber may make a request to revoke the certificate for which the subscriber is responsible.
2) The BMSP CA may make a request to revoke its own certificate.
3) The BMSP CA may also revoke any issued certificate whenever it knows or reasonably suspects that the circumstances as specified in section 4.9.1 occurred.
4) 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.
5) Court order
6) Relying Parties, Application Software Suppliers, and other non-subscribers may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates and request certificate revocation as described in Section 4.9.3.

4.9.3 Procedure for Revocation Request

CA that issues certificates under this CP SHALL provide the procedure that a requester can request for revocation 24x7 via online protal and Certificate Problem Reports. A Subscriber requesting revocation is required to follow the procedures such as:

1) The certificate revocation applicant shall submit the request per the RA's guidelines. After the RA receives the request, the relevant review procedures are implemented, and records of all certificate revocation requests are kept, including the applicant's name, contact information, reason for revocation, and time and date of revocation, to serve as a basis for subsequent accountability.
2) After the RA completes the review, the certificate revocation application information is sent to the BMSP CA.

3) When the BMSP CA receives the certificate revocation application information sent by the RA, the BMSP CA first checks the relevant RA's authorization status to verify its authorized assurance level and scope. Afterwards, the certificate is revoked based on the request sent by the RA.
4) f the application does not pass the above checking, the BMSP CA shall send the related erroneous message to the RA and refuse to handle subsequent related work. If the RA has any questions, the RA may directly contact the BMSP CA to understand the source of the problem.
5) To ensure the security, integrity, and non-reputability of the information transmitted by the BMSP CA and RA, the certificate application information is affixed with a digital signature, encrypted, and transmitted through the network using transport layer security (TLS) protocols.
6) The BMSP CA uses the same BMSP CA private key to issue the certificate to publish the serial number of the revoked certificate and the reason for revocation to the CRL by digital signature.
7) Provide a timelier OCSP inquiry service (e.g. the status of being revoked, the status of being applied, or the status is valid).
8) The BMSP CA receives certificate problem reports and provides the certificate problem response mechanism 24x7, as specified in section 4.9.3.1.

Relying Parties, Application Software Suppliers, and other non-subscribers may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates and request certificate revocation as described in Section 4.9.3.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this CPS.

4.9.5 Time within Which CA Must Process the Revocation Request

The Subscriber submits a certificate revocation application, the RA shall promptly complete the review procedure within one working day. If the revocation application information is error-free and passes the review, the BMSP CA shall complete the certificate revocation work within one working day.

The BMSP CA shall investigate and confirm if the following principles accept the request for certificate revocation within 24 hours of receiving the certificate problem reports. If the request for certificate revocation is accepted after the confirmation, the operation of certificate revocation will proceed according to the regulations of Section 4.9.3.

1) The claimed problematic content.
2) The quantity of the certificate problem reports of the certificate or the Subscriber.

3) The entity submits the certificate problem report.

4) The related laws and regulations.

Relying Parties, Application Software Suppliers, and other non-subscribers may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates and request certificate revocation as described in Section 4.9.3.

4.9.6 Revocation Checking Requirement for Relying Parties

Checking procedure: Before using certificates issued by the BMSP CA, the relying parties shall check the CRL or OCSP responses published by the BMSP CA to verify the validity of the certificates. The relying parties shall also confirm the revoking time of certificates, the validity of signatures of the CRL or OCSP responses, and the validity of certificate chains.

The BMSP CA publishes suspended and revoked certification information on the repository for checking purposes. There are no restrictions for the checking of CRL by relying parties. The website is as follows: https://www.bmspca.tech/

4.9.7 CRL Issuance Frequency

The CRL issuance frequency of the BMSP CA is at least once per day. Issued CRLs are valid for no more than 24 hours, allowing the system to continue operating for 12 hours when the latest CRL fails to be downloaded. Before the CRL expires, the BMSP CA may issue a new CRL. The new CRL validity period may overlap the validity period of the old CRL. Even though the old CRL has not yet expired, relying parties may still obtain the new CRL from the BMSP CA repository to receive the updated certificate revocation information.

4.9.8 Maximum Latency for CRLs

The BMSP CA shall publish the CRL at the latest before the nextUpdate listed on the CRL within one hour after generation.

4.9.9 On-line Revocation/Status Checking Availability

Relying parties can access the OCSP on the following URL:

https://www.bmspca.tech/

4.9.10 On-line Revocation Checking Requirements

Relying Parties may optionally check the status of certificates through the BMSP CA Online Certificate Status Protocol (OCSP) service. Reference in section 4.9.9.

4.9.11 Other Forms of Revocation Advertisements Available

Not Applicable.

4.9.12 Special Requirements Regarding Key Compromise

The Certificate Authority has policies for handling acute data leakage and continuity of service. Any data leakage regarding the Subscriber's private key will be communicated to the Subscriber, and the affected certificate will be revoked.

4.9.13 Circumstances for Suspension

Certificate Suspension refers to a temporary suspension that makes the certificate temporarily unusable. The Certificate Authority or Subscriber may suspend a certificate in the following circumstances:

1.) The private key is suspected to be known, accessed, or used by a third party.

2.) The password is suspected to be used to access the private key, which becomes known by a third party.

3.) The Subscriber does not comply with the CA's terms and conditions for certificate use, certificate policy/certificate practice statement, or service agreement.

4.) Following a court order or prosecution.

4.9.14 Who Can Request Suspension

1.) Certificate Authority

2.) Registration Authority

3.) Certificate Owner

4.9.15 Procedure for Suspension Request

There are list methods for suspension requests:

1.) The owner makes an acknowledge to the registration authority officer requesting suspension. The officer will then verify the Subscriber's authority and immediately suspend the certificate.
2.) If the owner submits an electronic certificate suspension request to the registration authority officer, the officer will suspend the certificate within one operating day after verifying the Subscriber's authority.

4.9.16 Limits on Suspension Period

BMSP CA sets the maximum period a certificate may be suspended to 30 days. If the Certificate remains suspended throughout the period, the requestor has until the 30th day to confirm its unsuspension, or it will be revoked. BMSP CA will maintain an internal policy and procedure to manually or programmatically review the certificate suspensions in this period to ensure the certificates do not pass the stated timeframe.

The Certificate will be revoked for “Key Compromise” if the subscriber does not remove it from hold (suspension) within that period.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The BMSP CA provides CRLs and OCSP inquiry services. The URLs of these services are recorded on the subscriber certificate's CRLDistributionPoints and authorityInfoAccess extensions.The revocation record of a certificate in CRL or OCSP response will only be removed once that revoked certificate expires.

4.10.2 Service Availability

The BMSP CA has implemented backup systems for providing certificate status services and put the best efforts to make such services available 24x7.

4.10.3 Optional Features

Not Applicable.

4.11 End of Subscription

A Subscriber’s subscription service ends if its Certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12 Key Escrow and Recovery

The BMSP CA does not provide escrow service for personal keys. Subscribers are responsible for the secure retention of personal keys. Personal keys issued to the Subscribers must only be appropriately used according to the category.

4.12.1 Key Escrow and Recovery Policy and Practices

Reference in the section 4.12.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Reference in the section 4.12.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The IDC systems providing BMSP CA services are located at two secure facilities, i.e. the main site in Bangkok and the disaster recovery site in a geographic location reasonably apart from the main site. That is compliant with ISO27001 (Information Security Management System: ISMS). Both secure facilities are equipped with physical access controls as follows:

1) Four layers of physical access controls
2) Two-factor authentication for accessing the server rooms
3) CCTVs (Closed Circuit Televisions) record the activity in the server room at all times
4) Smoke detector and fire extinguisher (using electronic equipment safe agent) systems

The server rooms are accessible by the BMSP officers only. If a non-BMSP officer requires access to the room, authorization from BMSP MUST be provided in order to allow that person to enter the server room. At all times, such a person MUST be accompanied by the BMSP officer.

Certificate issuing servers and Cryptographic Module are stored in a separate rack where physically accessing to such systems requires a user to perform a two-factor authentication.

5.1.2 Physical Access

The BMSP CA has established suitable measures to control connections to BMSP CA service hardware, software and hardware security module.

Access to the certificate issuance systems, a critical component of BMSP CA, is strictly limited to the responsible officers of the corresponding CA. Any other individual requiring access to the CA systems' service area must obtain proper authorization in advance. This stringent policy ensures that only authorized personnel are granted access, and all visits are meticulously recorded in the access log. Furthermore, all visitors are required to be accompanied by the responsible officer throughout their visit. The certificate-issue servers and Cryptographic Modules are stored in a secure area where physical access necessitates dual-control and two-factor authentication, further enhancing the security of these systems.

5.1.3 Power and Air Conditioning

The IDC systems providing BMSP CA have backup power capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. Both secure facilities are equipped with power generators and Uninterrupted Power Supplies (UPS) and The air-conditioning systems for both secure facilities maintain the temperature and the humidity of the server rooms to the appropriate level.

The repositories (containing certificates and CRLs) shall be provided with Uninterrupted Power Supplies (UPS) sufficient for a minimum of 6-hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 Water Exposures

The IDC systems providing secure facilities for BMSP CA will be constructed and equipped, and procedures will be implemented to prevent floods or other damaging exposure to water, e.g., on a raised floor fitted with a water sensor.

5.1.5 Fire Prevention and Protection

The IDC systems providing secure facilities for BMSP CAs will be constructed and equipped, and procedures shall be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures shall meet all local applicable safety regulations and a fire extinguishing system that operates quickly and effectively without causing damage to electrical equipment.

5.1.6 Media Storage

The BMSP CA protects all media holding back up critical system data or any other sensitive information in the secure environment defined in section 5.11.

5.1.7 Waste Disposal

All waste and unused equipment must be disposed of according to a controlled procedure. The disposal of unused data or any information complies with ISO 27001 standard requirements.

5.1.8 Off-site Backup

The off-site backup location is the disaster recovery site that automatically syncs with the main facility. The backup content shall include information and system programs.

5.2 Procedural Controls

5.2.1 Trusted Roles

To ensure that assignments of critical functions of the BMSP CA are properly distinguished to prevent undetected malicious use of the system, the trusted role authorized to perform each system access task is clearly defined. A combination of access control and key management, BMSP CA does not allow individuals to access the entire system. The roles in operation are divided for security and must at least consist but are not limited to :

Trusted role operations include:

Trusted Roles for Certification Authority

Consist of:

1.) CA Operation Manager, responsible for
   - Management of the Subscribers' Private Keys
   - Making and supervising the security policies regarding certificating service system
   - Reviewing the operation of System Support and System Administrator officers

2.) System Support Officers responsible for
   - Defining important parameters for systems relating to the certificating services system
   - Operation and management of computer network devices relating to the certificating service system
   - Defining important parameters for computer network devices relating to the certificating service system

3.) System Administrator Officers responsible for

- Performance tuning and security hardening for the computers
- Management of Subscribers' private keys
- Making and supervising the security policies regarding certificating service system
- Reviewing the operation of System Support officers and CA operators

4.) CA Operators responsible for

- Operation and management of computers for the certificating service system
- Maintenance of the computer operating system
- Operation and management of data storage for the certificating service system

5.) RA Operators, responsible for

- Reception of electronic certificate applications
- Identification and verification of Subscribers
- Issuance of certificates
- Reception of certificate revocation requests
- Revocation of certificates as requested by the Subscribers
- Publishing certificate revocation lists

6.) RA Auditors responsible for

- Auditing RA Operator

7) Executives who manage CA infrastructural trustworthiness

- Management of the CA Infrastructure

5.2.2 Number of Persons Required per Task

As described above, operational tasks allow a balanced, secure, and accountable operation. The fundamental principles for task sharing are:

1.) The CA Operator must be separated from the System Administrator to ensure separation from the audit log.

2.) Any task involving CA system or database access must require at least two operators. One will be the operator, and the other will be the inspector.

5.2.3 Identification and Authentication for Each Role

The standard process must officially select personnel assigned for the operation to ensure "trustworthiness".

5.2.4 Roles Requiring Separation of Duties

The duties of CA and RA officers are separated.

1) CA Officers' main tasks are operating and managing certificate service systems, related software (Database, firewall, and LDAP), and system backup.
2) RA Officers' main tasks are reviewing electronic certificate applications, verifying supporting evidence, and issuing, suspending and revocating certificates.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

The BMSP CA will select trustworthy officers based on the knowledge and skills required in operation. The selection process will include a criminal background check. The criminal background check will be reconducted every five years.

The candidate must have a bachelor's degree in computer science, Information Technology, Computer Engineering, or a related field, and the qualifications certificate standard must be related to the role.

All personnel of BMSP CA must be examined with their qualifications in terms of the requisite background, experience in order to ensure their prospective job responsibilities, competency and satisfaction.

5.3.2 Background Check Procedures

Prior to commencement of employment, the Human Resource Department, BMSP CA conducts the following background checks:

1) Identification card
2) House registration
3) Certificate of the highest education
4) Criminal records
5) Professional certificate (if any)
6) Confirmation letter of previous employment
7) Background Check (Recheck at least every five years)

BMSP CA may also use other measurements for background checks. If the provided information is found to be false, if the education/professional background is found to be unmatched, or if the person has certain criminal convictions, that person shall not be considered to work with the BMSP CA.

5.3.3 Training Requirements and Procedures

BMSP CA provides its officers with appropriate training and the requisite on-the-job training to perform their job responsibilities related to CA operations with competency and satisfaction. The training programs include the following as relevant:

1) Basic cryptography and Public Key Infrastructure (PKI) concepts
2) Information Security Awareness
3) Use and operation of deployed hardware and software related to CA operations
4) Security Risk Management
5) Disaster recovery and business continuity procedures

5.3.4 Retraining Frequency and Requirements

The BMSP CA shall be aware of any changes and related work procedures, laws and regulations. BMSP CA provides its officers with appropriate training at least once a year on topics related to Information Security Awareness. Additional training may be considered if there is a change in hardware and software associated with CA operations, and the training status shall be recorded to ensure that work procedures and regulatory changes are understood.

5.3.5 Job Rotation Frequency and Sequence

The BMSP officers' performance will be assessed every two years, where job rotation and promotion will also be considered.

5.3.6 Sanction for Unauthorized Actions

BMSP CA-related personnel shall be subject to appropriate administrative and disciplinary action for violations of the CP, CPS, or other procedures announced by BMSP CA. Proper legal action shall be taken in severe cases that result in damages.

5.3.7 Independent Contractor Requirements

BMSP CA shall follow section 5.3 5.3.3 5.3.2 5.3.8 for the security requirements of personnel employed.

5.3.8 Documentation Supplied to Personnel

The BMSP CA shall make available to related personnel relevant documentation regarding the CP, CPS,BMSP CA system operation manuals, the Electronic Transactions Act, and its enforcement rules.

5.4 Audit Logging Procedures

The BMSP CA shall keep security audit logs for all CA-related events. Security audit logs shall be collected by automatic system generation, logbook or paper. BMSP CA shall retain all security audit logs and make them available during compliance audits. The archive retention keeps auditable security audit logs regulations in section 5.5.2.

5.4.1 Types of Events Recorded

The following events will be logged on the system:

CA Events Recorded

1) CA key life cycle management events
2) Key Generation, Backup, Storage,
3) CA and Subscriber certificate life cycle management
4) Certificate application, Renewal, Revocation
5) Successful or unsuccessful processing of the request

RA Events Record

1) RA Operation log
2) Method used to validate identification document

Environment Events Record

1.) Security-related events including

2.) Security profile changes

3.) System crashes, hardware failures

4.) Firewall and router activity

5.) Facility visitor entry and exit

5.4.2 Frequency of Processing Log

The BMSP CA shall review audit logs and explain the significant events. The weekly review includes examining all log entries and assessing any warnings or anomalies. Audit checking results shall be documented at least quarterly.

5.4.3 Retention Period for Audit Log

Audit logs on the archival repository shall be retained on-site for three months and ten years. The log retention management system shall be operated according to the regulations in sections 5.4.4, 5.4.5, and 5.4.6. When the retention period for audit information ends, audit personnel are responsible for removing the information.

5.4.4 Protection of Audit Log

Audit logs shall be kept securely with a digital signature to ensure the integrity of the log file and only viewed by authorized personnel.

5.4.5 Audit Log Backup Procedure

The audit log will be automatically backed up to the Log Server every day.

5.4.6 Audit Log Accumulation System (Internal vs. External)

Audit logs shall be kept on all BMSP CA security-related events. Security audit logs shall be collected by automatic system generation, logbook, or paper. The service provider keeps the OS, application, and firewall log on the local machine and keeps the backup at the DR site. All security audit logs shall be retained and made available during compliance audits.

5.4.7 Notification to Event-Causing Subject

Not Applicable.

5.4.8 Vulnerability Assessments

BMSP CA assesses security vulnerability at least on a quarterly basis.

5.4.9 Penetration Test Assessments

BMSP CA assesses security penetration test at least on a yearly basis.

5.5 Records Archival

5.5.1 Types of Records Archived

The following events will be recorded:

CA Events Recorded

1.) CA key life cycle management events

2.) Key Generation, Backup, Storage.

3.) CA and Subscriber certificate life cycle management

4.) Certificate application, Renewal, Revocation

5.) Successful or unsuccessful processing of the request

RA Events Record

1.) RA Operation log

2.) Method used to validate identification document

Environment Events Record

1.) Security-related events including

2.) Security profile changes

3.) System crashes, hardware failures

4.) Firewall and router activity

5.) Facility visitor entry/exit

5.5.2 Retention Period for Archive

Records shall be retained for at least ten years unless there are specific requirements (according to the Accounting Act B.E. 2543) for the Retention Period for Archives.

The retention period for BMSP CA file information is ten years, and the application programs used to process file data are also kept for 10 years.

5.5.3 Protection of Archive

Records archival are stored in secure facilities and can be accessed only by authorized persons.

5.5.4 Archive Backup Procedure

Records archival are backed up and saved in secure storage media following the BMSP Back up procedures:

5.5.5 Requirements for Time Stamping of Records

BMSP CA computer systems regularly calibrated to ensure the accuracy and trustworthiness of electronic records' date and time information. For archived electronic documents (such as certificates, CRLs and audit logs), the timestamping information on each record shall include the date and time information, and accurate times following system calibration shall be used. These records shall have appropriate digital signature protection and be able to check the date and time information on the records for alteration.

5.5.6 Archive Collection System (Internal or External)

The information referenced in section 5.5.1 will be kept using the proper procedure at the Data Centre and Data Recovery sites.

5.5.7 Procedures to Obtain and Verify Archive Information

Archive information may be obtained by relevant personnel after formal authorization is received. The audit person shall follow verification procedures when verifying archive information. The authenticity of signatures and dates on written documents must also be verified.

5.6 Key Changeover

The regulations in section 6.3.2 shall regularly renew the BMSP CA private keys. After the key pair is renewed, an application for a new certificate shall submitted to the BMSP CA. The new certificate shall be published in the repository for subscriber downloading.

Certificate subscriber private keys shall regularly renewed by the certificate subscriber private key usage period regulations in section 6.3.2.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

BMSP CA shall have an incident response and disaster recovery plan. If compromise of a BMSP CA is suspected, an independent third-party investigation shall be performed to determine the nature and the degree of damage. Issuance of certificates from that BMSP CA shall be stopped immediately upon detection of a compromise. If a BMSP 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 BMSP CA needs to be rebuilt if only some certificates need to be revoked, and if the BMSP CA private key needs to be declared compromised.

In case that there an event affects to security of BMSP CA system, the corresponding BMSP CA officers shall notify PA and Thailand NRCA if any of the following occur:

1) Suspected or detected compromise of any BMSP CA system or subsystem.
2) Physical intrusion or electronic penetration of any BMSP CA system or subsystem.
3) Successful denial of service attacks or disruption on any BMSP CA system or subsystem.
4) Any incident preventing BMSP CA from issuing and publishing a CRL or online status checking prior to the time indicated in the *nextUpdate* field in the currently published CRL, or the certificate for online status checking suspected or detected compromise.

Changes that are motivated by a security concern such as certificate misissuance or a root or intermediate certificate compromise can be reported via CA Incident Response system.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

The BMSP CA establishes recovery procedures for computing resource, software and data corruption and conducts annual drills.

Suppose the BMSP CA's computer equipment is damaged or unable to operate, but the CA signature key has yet to be destroyed. In that case, the priority shall be restoring the operation of the BMSP CA repository and re-establishing certificate issuance and management capabilities.

5.7.3 Recovery Procedures after Key Compromise

The CA provides procedures for continuity and management in cases of compromises of the CA signature key information. If the private key of the CA or Subscriber is compromised, NRCA and all related Subscribers will be notified. All affected private keys and certificates will be revoked immediately once the compromise is confirmed.

5.7.4 Business Continuity Capabilities after a Disaster

BMSP CA shall prepare a disaster recovery plan which have been tested,verified and continually updated. A full restoration of services will be done within 24 hours in case of disaster.

5.8 CA or RA Termination

During service termination, the BMSP CA shall follow CA service termination procedures by related regulations in the Electronic Signatures Act. The BMSP CA shall follow the item below to ensure the rights
of subscribers and relying parties:

1.) The BMSP CA shall notify the competent authority and subscribers of the service termination 30 days in advance.

2.) The BMSP CA shall take the following measures when terminating their service:

2.1.) For certificates valid at termination, arrangements shall be made for another CA to take over the service. Matters regarding service termination and service acceptance by other CAs shall published in the repository, and subscribers with valid certificates shall notified, but they shall not apply if notification cannot be made.

2.2.) All records and files during the operation period shall be handed over to the other CA taking over this service.

2.3.) If no CA is willing to take over the BMSP CA service, a report shall be submitted to the competent authority to arrange for another CA to take over this service.

2.4.) If the competent authority arranges for another CA to take over the service but no other CA takes over the service, the BMSP CA shall revoke the valid certificates, publish the revoked certificates in the repository and notify all certificate-related persons 30 days before service termination. The BMSP CA shall refund the certificate issuance and renewal fees based on the certificate's validity.

2.5.) The competent authorities, if necessary, may publish the certificates still valid at the time of revocation.

6. Technical Security Controls

BMSP CA shall implement and maintain appropriate technical security controls to govern all operations of the BMSP CA PKI.

6.1 Key Pair Generation and Installation

BMSP CA shall generate and install all CA Key Pairs in a physically secure environment on secure cryptographic equipment by personnel in trusted roles and using the methodology detailed in Section 6.1.1.
Access to physical modules shall be controlled as detailed in Section 6.2.

6.1.1 Key Pair Generation

Cryptographic keying material Thailand NRCA uses to sign certificates, CRLs or status information are generated in FIPS 140-2 Level 3 or equivalent standard validated cryptographic modules. Multi-party control is required for Thailand NRCA key pair generation, as specified in Section 6.2.2. Thailand's NRCA key pair generation has established a transparent audit trail, proving that the security procedures were meticulously followed. The documentation of the procedure has shown that appropriate role separation was used. An independent third party has validated the execution of the key generation procedures by witnessing the key generation and examining the signed and documented record of the key generation. The Subordinate CA shall perform subordinate CA key pair generation. The Subordinate CA is required to generate
the signature key pairs for digital signature by FIPS 140 FIPS 140-2 Level 3 validated hardware cryptographic modules to support source authentication. The subordinate CA shall not generate keys for SSL certificates.
1. The generated key pair shall be explicitly used as a Subordinate CA key pair under the
hierarchy of the "Thailand NRCA".
2. The private key shall be used exclusively for CA signing operations, including issuing end-entity certificates and CRL generation.
3. The public key shall be included in the Subordinate CA's Certificate signed by the "Thailand NRCA".

6.1.1.1 CA Key Pair Generation

For CA key pairs used as a CA key pair for a root certificate, the CA is required to:

1) Prepare and follow a key generation script.

2) Have a qualified auditor witness the CA key pair generation process or record a video of the entire CA key pair generation process.

3) Have a qualified auditor issue a report indicating that the CA followed its key ceremony during its key and certificate generation process and that the controls were used to ensure the integrity and confidentiality of the key pair.

For other CA key pairs that are for the operator of the Root CA or an affiliate of the Root CA, the CA should:

1) Prepare and follow a key generation script.

2) Have a qualified auditor witness the CA key pair generation process or record a video of the entire CA key pair generation process.

In all cases, the CA must:

1) Generate the CA key pair in a physically secured environment as described in this CP/CPS.

2) Generate the CA key pair using personnel in trusted roles under the principles of multiple-person control and split knowledge.

3) Generate the CA key pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in this CP/CPS.

4) Log its CA key pair generation activities.

5) Maintain adequate controls to provide reasonable assurance that the private key was generated and protected in conformance with the procedures described in its CP/CPS and, if applicable, its key generation script.

6.1.1.2 RA Key Pair Generation

No stipulations

6.1.1.3 Subscriber Key Pair Generation

Please ensure to reject a certificate request if any of the following conditions are met:

1) The Key Pair does not meet the requirements outlined in Section 6.1.5 and Section 6.1.6.

2) There is clear evidence that the specific method used to generate the Private Key was flawed.

3) The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise.

4) The CA has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1.

5) The CA is aware of a demonstrated or proven method to compute the Applicant's Private Key quickly based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

Additionally, if the Subscriber Certificate contains an extKeyUsage extension containing the values id-kpserverAuth [RFC 5280] or anyExtendedKeyUsage [RFC 5280], the Subordinate CA should not generate a Key Pair on behalf of a Subscriber or accept a certificate request using a Key Pair previously generated by the CA.

6.1.2 Private Key Delivery to Subscriber

If BMSP or an RA generates a key for a Subscriber, it must securely deliver the Private Key to the Subscriber. Keys may be delivered electronically (such as through secure email or stored in a cloud-based system) or on a hardware cryptographic module.

6.1.3 Public Key Delivery to Certificate Issuer

After the Subscriber generates the key pair, the Subscriber shall deliver the public key in PKCS# 10 certificate application file format to the RA. The RA shall deliver the public key to the CA via secure channels after it is verified by the regulations in section 3.2.1 that the Subscriber has the corresponding private key.

Secure channels referred in this section means the use of transport layer security (TLS) or other equivalent ormore secure data encryption transmission protocols.

6.1.4 CA Public Key Delivery to Relying Parties

The CA’s public key will be delivered to the relying parties by attaching it to the Subscriber’s Certificate or downloading it from the CA’s website.

6.1.5 Key Sizes

The BMSP CA uses 4096-bit RSA keys and a SHA-512 hash function algorithm to issue certificates and CRLs. Subscribers must use at least 2048-bit Public Keys for RSA or 224 bits for elliptic curve algorithms or other key types of equivalent security strength.

6.1.6 Public Key Parameters Generation and Quality Checking

Cryptographic keying material used by BMSP CA to sign certificates, CRLs, or status information is generated in FIPS 140-2 Level 3 or equivalent standard-validated cryptographic modules. Multi-party control is required for BMSP CA key pair generation, as specified in Section 6.2.2.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The BMSP CA's signature private key issues certificates and CRLs. The NRCA issues theBMSP CA's public key certificate. The key usage bits used for the keyUsage extension setting are key CertSign and CRLSign.
When the Subscriber's token is a software token, the keyUsage extension may contain key Encryption and digital Signature simultaneously.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

All CA private keys must be stored in a secure Hardware Security Module to facilitate key signing operations. BMSP CA must safeguard its CA private keys in a system or device that has been validated to meet at least FIPS 140-2 level 3, FIPS 140-3 level 3, or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher). These requirements include protecting the private key and other assets against known threats.

6.2.2 Private Key (n out of m) Multi-person Control

The BMSP CA key splitting multi-person control uses n-out-of-m. It is a perfect secret-sharing method for private key splitting and recovery. Besides, n and m must be values greater than or equal to 2, and n must be less than or equal to m. This method can provide the highest security level for the BMSP CA private key multi-person control. Therefore, it can be used as the activation method for private keys (see section 6.2.8). There are no further regulations for multi-person control of subscriber private keys.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

BMSP CA private key backups follow the key-splitting multi-person control methods in section 6.2.2. The medium verified with FIPS 140-2 Level 3 or above standards may serve as the private key-splitting storage media.

The BMSP CA's signature private key backup is under the same multiparty control as the original signature key. More than one copy of the signature private key is stored off-site. All copies of the BMSP CA's signature private key are accounted for and protected like the original.

The BMSP CA backups are the signature private keys in the FIPS 140-2 Level 3 validated hardware cryptographic module.

6.2.5 Private Key Archival

The CA private key beyond the validity period will kept for at least ten years and stored in a Cryptographic Module with FIPS 140-2 Level 3 standards. The BMSP CA's signature private key of the user is not archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The BMSP CA transfers the private key into the cryptographic modules with FIPS 140-2 Level 3 standards under the following events:

1.) Key generation or cryptographic module replacement.
2.) Regarding key splitting, the BMSP CA private key recovery process applies a secret sharing method (n-out-of-m control). This method allows the private key recover by combining multiple shares of the key. Once the private key secret sharing media recovers, the complete private key is stored securely in the hardware cryptographic module.
3.) Encryption safeguards the private key importation method during the cryptographic module replacement. This ensures that the secret key code remains confidential and is not exposed outside the cryptographic module during the importation process. Additionally, the related confidential parameters generated during the importation process must be destroyed once the private key importation is completed.

6.2.7 Private Key Storage on Cryptographic Module

BMSP CA shall store and back up the Private Keys on a cryptographic module which complies with FIPS 140-2 Level 3 or above standard.

6.2.8 Method of Activating Private Key

The private keys of the BMSP CA and Subscribers will be activated by an authorization process through hardware with the same level of security and only with a valid password.

6.2.9 Method of Deactivating Private Key

The multi-person control methods in section 6.2.2 control the deactivation of BMSP CA private keys. The BMSP CA deactivated a subscriber's private key upon a revocation request from the Subscriber.

6.2.10 Method of Destroying Private Key

BMSP CA will delete the private keys from Cryptographic Module and its backup by overwriting the private key or initialize the module with a zeroization function of Cryptographic Module. The event of destroying BMSP CA must be recorded into evidence under section 5.4.

6.2.11 Cryptographic Module Capabilities

The BMSP CA Cryptographic Module complies with FIPS 140-2 Level 3 standard.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

BMSP CA securely controls the certificate archival procedure by section 5.5.

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 specified in table below . 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 CAshall not have expiry date exceeding year 2580 (AD 2037)).

The validity period of certificates issued under this CPS SHALL NOT exceed the maximum validity periods listed in the table below.

Type	Maximum Validity Periods
Thailand NRCA Certificate G1	23 years.
Thailand NRCA Certificate G2/G3	20 years.
Subordinate CA Certificate under G1	20 years.
Subordinate CA Certificate under G2/G3	17 years.
Personal Certificate	2 years
Organization or Legal entity Certificate	2 years
AATL End Entity Certificates	2 years
SSL/TLS Certificates	398 days (Certificates issued on or after 1 September 2020)
S/MIME Certificates: Strict/Multipurpose	825 days
S/MIME Certificates: Legacy	1185 days

Table 8 Maximum Certificate Validity Periods

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The BMSP CA activation data, such as the Personal Identification Number (PIN) and passwords for accessing the CA systems, are user-selected and protected under multi-person control by each person holding that activation data.

6.4.2 Activation Data Protection

Data used to unlock private keys is protected from disclosure by being stored in a safe and accessible only to authorized persons.

6.4.3 Other Aspects of Activation Data

Not Applicable.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The BMSP CA has arranged a system security plan that incorporates the computer security technical requirements for certificating according to the ISO 27001 (Information Security Management System: ISMS) and WebTrust for CA (Trust Service Principles and Criteria for Certification Authorities) Standards.

6.5.2 Computer Security Rating

The BMSP CA has arranged a system security plan incorporating computer security rating for certificating according to the ISO 27001 (Information Security Management System: ISMS) and WebTrust for CA (Trust Service Principles and Criteria for Certification Authorities) Standards.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

BMSP CA has mechanisms in place to control and monitor the acquisition and development of its CA systems. Change requests require the approval of at least one administrator, which is different from the person submitting the request. BMSP CA only installs software on CA systems if the software is part of the CA's operation. CA hardware and software are dedicated to performing CA operations.

Vendors are selected based on their reputation in the market, ability to deliver quality products, and likelihood of remaining viable in the future. Management is involved in the vendor selection and purchase decision process. Non-PKI hardware and software are purchased without identifying the purpose for which the component will be used. All hardware and software are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without the opportunity for tampering.

Some PKI software components used by BMSP CA are developed in-house or by consultants using standard software development methodologies. All such software is designed and developed in a controlled environment and subjected to quality assurance review. Other software is purchased commercially off-the-shelf (COTS). Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors, as discussed above.

Equipment and software updates are purchased or developed like the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to BMSP CA operations is scanned for malicious code on first use and periodically afterwards.

6.6.2 Security Management Controls

The security management controls are controlled and managed under the ISO 27001 (Information Security Management System: ISMS) WebTrust for CA (Trust Service Principles and Criteria for Certification Authorities) systems with the details regarding the tools, procedures, and trusted personnel described under item 5.2.1: Trusted Roles.

6.6.3 Life Cycle Security Controls

The BMSP CA has conducted the risk assessment that identifies and mitigates the life-cycle security risks are rated as 'high risk' and 'very high risk' in the certificate system regulartly.

6.7 Network Security Controls

The network control for certificating system has been designed to only use related computers and devices. BMSP CA system is connected to secure internal network and protected by firewalls.
The hardware and software firewalls (only configurable by IT Security Manager) are utilized to prevent intrusion from external source. The system also includes Intrusion Protection System (IPS) and Anti-Virus. The certificate public services (i.e CRLs, OCSP) are allowed to access through public internet.

6.8 Time-stamping

The system clock will be set in the time setting device (NTP Server) which shall be accurate to within three minutes. Any recording time in the system will refer to the same time setting device.

7. Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

Certificates issued by the BMSP CA under this CPS comply with RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. ETDA Recommendation on ICT Standard forElectronic Transactions (15-2560: Certificate and Certificate Revocation List (CRL) Profile) is an extension for CAs to use as guidance for issuing certificates in Thailand other than those specified by the Thailand NRCA.

The Directory: Public-key and attribute certificate frameworks in which the certificate contains the information shown in Table 9.

Field	Value or Value Constraint
version	Version of certificate, the details are described in section 7.1.1
Serial Number	Reference number of Certificate Issue
signature	The method of digitally sign consists of Asymmetric cryptographic algorithms (Public Key Algorithm) and data digestion (Hash Function) which Certificate Authority is used to sign the certificate in form of Object Identifier (OID).
issuer	The name of the Certificate Authority in the certificate must be in the format of Distinguished Name (DN) in accordance with ISO / IEC 9594-2.
validity	Period of certificate usage is specified by the begin date (notBefore) and expiration date (notAfter)
subject	Specify the entity name of Certificate Authority as the owner of public key in the certificate
Subject Public Key Info	Specify the type of public key and subject value of public key

Table 9 Fields in The Certificate

7.1.1 Version Number

The certificate issued by BMSP CA is in accordance with ITU-T Recommendation X.509 standard ISO / IEC 9594-8:2008 and designated as version 3.

7.1.2 Certificate Content and Extensions; Application of RFC 5280

Additional information on the certificate issued by BMSP CA is complied with ISO / IEC 9594-8:2008, RFC 5280 including the latest version of CA/B Forum TLS Baseline Requirements Section 7.1.2 and ETDA Recommendation on ICT Standard for Electronic Transactions (15-: Subscriber Certificate Profile) standard, which contains at least the following:

1.) Authority Key Identifier: Public key of the CA
2.) Key Usage: Intended usage for the key
3.) Extended Key Usage: Extended usage for the key
4.) CRL Distribution Points: Location of the CRL for status check
5.) Basic Constraints: Categories of the certificate, whether it belongs to the CA or Subscribers and the maximum number of certificate chains.
6.) Certificate Policies: Reference to the Certificate Policy in the form of Object Identifier (OID)

7.1.2.1. CA Certificate Profile

Issure CA follows Section 7.1.2.1 of CA/B Forum TLS Baseline Requirements.

7.1.2.2. Cross-Certified Subordinate CA Certificate Profile

CAs under this CP dose not issue cross-certificates.

7.1.2.3. Technically Constrained Non-TLS Subordinate CA Certificate Profile

Not applicable.

7.1.2.4. Technically Constrained Precertificate Signing CA Certificate Profile

Not applicable.

7.1.2.5. Technically Constrained TLS Subordinate CA Certificate Profile

Not applicable.

7.1.2.6. Subordinate CA Certificate Profile

Issure CA follows Section 7.1.2.6 of CA/B Forum TLS Baseline Requirements.

7.1.2.7. Subscriber Certificate Profile

Issure CA follows Section 7.1.2.7 of CA/B Forum TLS Baseline Requirements.

7.1.2.8. OCSP Responder Certificate Profile

Specify the related information with public key of Certificate Authority into certificate of subscribers by hashing the public key of Certificate Authority with Hash Algorithm SHA-256, or SHA-384 or SHA-512. Issure CA follows Section 7.1.2.8 of CA/B Forum TLS Baseline Requirements.

7.1.2.9. Precertificate Profile

Issure CA follows Section 7.1.2.9 of CA/B Forum TLS Baseline Requirements.

7.1.2.10. Common CA Fields

Issure CA follows Section 7.1.2.10 of CA/B Forum TLS Baseline Requirements.

7.1.2.11. Common Certificate Fields

Issure CA follows Section 7.1.2.11 of CA/B Forum TLS Baseline Requirements.

7.1.3 Algorithm object identifiers

The OID of digital signature and encryption of certificate is in Section 1.2.

Algorithm	Object Identifier
SHA256withRSAEncryption	1.2.840.113549.1.1.11
SHA384 with RSA Encryption	1.2.840.113549.1.1.12
SHA512withRSAEncryption	1.2.840.113549.1.1.13
ECDSAWithSHA256	1.2.840.10045.4.3.2
ECDSAWithSHA384	1.2.840.10045.4.3.3
ECDSAWithSHA512	1.2.840.10045.4.3.4

Table 10 Method of digital signature and encryption with Object Identifier

7.1.4 Name Forms

Each Certificate includes a unique serial number. Optional subfields in the subject of any public certificate must either contain information verified by BMSP CA or be left empty. SSL/TLS and S/MIME Certificates cannot contain metadata such as '.', '-' and "characters or and/or any other indication that the value/field is absent, incomplete, or not applicable.

For CAB Forum requirements as listed in section 1.1 BMSP CA has a process that limits information in OU fields from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless BMSP CA has verified this information by section 3.2 and the Certificate also contains subject:organizationName, subject:givenName,

subject: surname, subject:localityName, and subject:countryName attributes, also verified by section 3.2.
BMSP CA doesn't issue public SSL/TLS or S/MIME Certificates with an OU attribute.

The names in the Certificate Issuer and Certificate Subject fields of the certificate are distinguished names according to the X.500 standard.

The Distinguished Name (DN) of BMSP CA will use the following information:

C = TH
S = <State>
L = <Locality>
O = <Customer Corporate name in English>
organizationIdentifier = <Customer Corporate tax ID>
OU = <Department Name in English >
Title = <Position in organization>
Serial Number = <identification ID>
Givenname = <Customer First Name in Thai>
SN = <Customer Last Name in Thai>
CN = <Customer Name in English>
E = <Email>

The information that appears as the DN also depends on the Certificate Policy, viewable on the BMSP CA Website (https://www.bmspca.tech).

7.1.5 Name Constraints

Name constraints not Applicable.

7.1.6 Certificate Policy Object Identifier

BMSP CA follows section 7.1.6 of CA/B Forum Baseline Requirement and also define the Certificate Polic OID provided by Thailand NRCA’s OID Structure.

7.1.7 Usage of Policy Constraints Extension

Not Applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

The CA has described its policy qualifiers, syntax, and semantics under the Certificate Policy on the BMSP CA Website (URL: https://www.bmspca.tech).

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not Applicable.

7.2 CRL Profile

The BMSP CA's certificate revocation list complies with ITU-T X.509 v2 and has the following details as in Table 9. In addition, the CRL Profile shall be by ETDA Recommendation on ICT Standard for Electronic Transactions (ขมธอ. 15-2560: CERTIFICATE AND CERTIFICATE REVOCATION LIST (CRL) PROFILE has following details as in Table 11.

Field	Value or Value Constraint
version	Version of the certificate revocation list will be version number 2 as provided in section 7.2.1.
signature	The method of digitally sign consists of Asymmetric cryptographic algorithms (Public Key Algorithm) and data digestion (Hash Function) which Certificate Authority is used to sign the certificate in form of Object Identifier (OID).
issuer	The name of the Certificate Authority in the certificate must be in the format of Distinguished Name (DN) in accordance with ISO / IEC 9594-2.

thisUpdate	The date and time of the revocation list.
nextUpdate	Specified date and time to the next update of certificate revocation list. If necessary BMSP CA will issue the certificate revocation list before schedule.
revokedCertificates	A list of the serialNumber of the certificate has been revoked with specific the date and time of revocation.

Table 11 Item list in Certificate Revocation

7.2.1 Version Number(s)

CRLs issued by the BMSP CA shall be by RFC 5280 and designated version 2 standard.

7.2.2 CRL and CRL Entry Extensions

The information on certificate revocation lists issued by Certification Authority is complied with ISO / IEC 9594-8:2012 standard and contains at least the following:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Subject Key Identifier of the CRL issuer certificate
Invalidity Date	Optional date in UTC format
Reason Code	Specify reason for revocation if included.
Issuing Distribution Point	Configured per RFC 5280 requirements, if included.

Table 12 CRL and CRL Entry Extensions

7.2.2.1. AuthorityKeyIdentifier

This attribute indicates information associated with the certificate's public key, which subscribers digitally sign. The signing uses the SHA-256, SHA-384, or SHA-512 hashing algorithm of the Certificate Authority's public key.

7.2.2.2. BaseCRLNumber

This attribute indicates the sequence number that the Certificate Authority assigns to each revoked certificate to order the certificate revocation list.

7.2.2.3. reasonCode

This attribute indicates the Reason Code (0-9) of revoked certificate.

7.2.2.4. invalidityDate

This attribution indicates the start time when using the pair of private keys and the revoked certificate is insecure. It is defined in Greenwich Mean Time (GMT) format.

7.2.2.5. issuingDistributionPoint

This attribution is used to locate the certificate revocation list (Distribution Point), indicates that it is for a Certification Authority or subscribers, and includes the reasons for revocation (Reason Code).

7.3 OCSP Profile

The BMSP CA provides OCSP inquiry services that comply with IETF PKIX Working Group RFC 6960 and RFC 5019 standards. The BMSP CA OCSP service website is contained in the authorityInfoAccess extension.

7.3.1 Version Number(s)

The BMSP CA's OCSP uses X.509 OCSP Version 1 standard according to the RFC 2560 standard (https://www.ietf.org/rfc/rfc2560.txt).

7.3.2 OCSP Extensions

Not Applicable.

8. Compliance Audit and Other Assessments

The BMSP CA adheres to the ISO 27001 (Information Security Management System: ISMS) standard for policies regarding risk assessment and security and has arranged for internal and external audits with the latest WebTrust for CA (Trust Service Principles and Criteria for Certification Authorities) and WebTrust for CA - SSL Baseline (WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security) standards published on http://www.cabforum.org for its certificating and management for trustworthiness.

BMSP CA has a compliance audit mechanism in place to ensure that its CP/CPS requirements are being implemented and audited for complying with the following standards:

1.) Adobe Approved Trust List – Technical Requirements (if applicable).

2.) Electronic Transactions Act, B.E. 2544 (2001) and related versions.

3.) The NRCA CP.

8.1 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 at least once a year.

8.2 Identity/Qualifications of Assessor

The BMSP CA will retain a qualified auditor to perform the BMSP CA compliance audit work. The auditor will be familiar with BMSP CA operations and authorized by the CPA as a licensed WebTrust practitioner to perform WebTrust Principles and Criteria for Certification Authorities to provide fair and impartial audit services.

Audit personnel shall be a qualified and authorized Certified Information Systems Auditor (CISA) or have equivalent qualifications and shall at least possess the experience of conducting a WebTrust for CA signature audit twice at four man-days or the experience of conducting a CA information security management audit twice at eight man-days. The BMSP CA shall conduct identity identification of audit personnel during audits.

8.3 Assessor's Relationship to Assessed Entity

Auditors must be independent of the BMSP CA and RAs being audited, or they must be sufficiently organizationally separated from those entities and shall provide an unbiased, independent evaluation. To ensure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining its CA facility or certification practice statement. The CAM shall determine whether a compliance auditor meets this requirement. There must not be a conflict of interest with the CA.

8.4 Topics Covered by Assessment

A compliance audit verifies 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 applies to CAs in the year following the adoption of the revised scheme.

8.5 Actions Taken As a Result of Deficiency

CA’s officers must plan to improve deficiencies (Non-conformity) based on the assessment results with explicit operating time. The **improvement** plan will be submitted to auditors and Thailand NRCA **(The BMSP CA is a Subordinate CA)** to ensure that sufficient security of the system is still in place.

8.6 Communication of Results

After the assessment is completed, the audit compliance report and identification of corrective measures (if any) must be sent to the PA within 30 days of completion. However, the audit compliance report must be sent to the PA and made publicly available within three months after the end of the audit period. In the case of delay, the CA shall provide an official letter signed by the qualified auditor.

8.7 Self-Audits

The Certificate Authority (CA) must strictly adhere to its Certificate Policy, Certification Practice Statement, and these Requirements during the period it issues certificates. To maintain service quality, the CA must conduct quarterly self-audits against a randomly selected sample of either one certificate or at least three per cent of the certificates issued by the CA since the previous self-audit.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The certificate issuance and renewal fees will be agreed upon between the BMSP CA and subscribers in the related business contract terms and conditions.

9.1.2 Certificate Access Fees

The BMSP CA does not charge for the Subscriber's access to the certificate issued by the BMSP CA.

9.1.3 Revocation or Status Information Access Fees

The BMSP CA does not charge for Subscribers' access to the CRL published on its website.

9.1.4 Fees for Other Services

The BMSP CA does not charge subscribers any fee for downloading CP or CPS.

9.1.5 Refund Policy

Suppose a subscriber cannot use a certificate because of an error from BMSP CA. In that case, an investigation will conducted, and BMSP CA will issue a new certificate. If the Subscriber does not accept the newly issued certificate, Subscribers must request refunds in writing within 30 days of issuing a Certificate. After receiving the refund request, BMSP CA may revoke the Certificate and refund the amount paid by the Applicant minus any applicable application processing fees.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

The BMSP CA is responsible for damage only if caused by intentional acts or gross negligence.

Entities acting as relying parties shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

9.2.2 Other Assets

The CA is a legal entity registered by Thai law with asset Information is available in the financial statement on the Department of Business Development's (Ministry of Commerce) website.

9.2.3 Insurance or Warranty Coverage for End-entities

The CA guarantees the accuracy of the information on the certificate. In case of any mistake associated with the RA or CA, the Subscriber must notify the CA within 15 days after issuance. The CA will then issue a new certificate free of charge.

9.3 Confidentiality of Business Information

Electronic certification service providers have defined the scope of confidentiality for business information as limited to submitted documents and information obtained from third parties in pursuit of service agreements, contracts, or other service documents.

9.3.1 Scope of Confidential Information

The BMSP CA or RAs' generation, receipt, and safekeeping of information shall be deemed to be confidential.

1.) Private keys and passphrases used for operations.
2.) Key splitting safekeeping information.
3.) Subscriber application information.
4.) Audit and tracking logs generated and kept by the BMSP CA.
5.) Audit logs and reports made by audit personnel during the audit process.
6.) Operation-related documents are listed as confidential-level operations.

Current and departed BMSP CA, RA personnel, and various audit personnel shall keep confidential information.

9.3.2 Information Not within the Scope of Confidential Information

Following information is not within the scope of confidential information:

1.) Certificate Practice Policy of certification authority

2.) Certificate uses policy

3.) Information inside certificate

4.) Certificate revocation

5.) Information without impact on security and reliable of CA’s system such as articles and news

9.3.3 Responsibility to Protect Confidential Information

The BMSP CA have security measures in place to protect confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The BMSP CA has posted its personal information protection statement and privacy declaration on its website.The BMSP CA conducts privacy impact analysis and personal information risk assessments and has established a privacy protection plan.

9.4.2 Information Treated As Private

Any personal information listed on any certificate application is considered private and may only be disclosed with the Subscriber's consent or by related laws and regulations. Information that cannot be obtained through the certificate and CRL or subscriber information obtained through certificate catalogue service and personally identifiable information to maintain the operation of CA trusted roles

such as names together with biometric data, personal information on confidentiality agreements or contracts are deemed private information which requires protection. The BMSP CA and RAs implement security control measures to prevent personally identifiable information from unauthorized disclosure and leakage.

9.4.3 Information Not Deemed Private

Identification information or information listed on certificates is not deemed to be confidential and private unless stipulated otherwise. Issued certificates, revoked certificates, suspension information, and CRLs published in the repository are deemed confidential and private.

9.4.4 Responsibility to Protect Private Information

The personal information required for the operation of the BMSP CA, in either paper or digital form, must be security stored and protected by the personal information protection and privacy rights declaration posted on the website and comply with WebTrust Principles and Criteria for Certification Authorities Audit Criteria, CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security. The BMSP CA shall negotiate the protection of private information with RAs.

9.4.5 Notice and Consent to Use Private Information

Personal information shall not be used for other purposes without the consent of the Subscriber or unless stipulated otherwise in the Personal Information Protection and Privacy Rights Declaration and CPS. The Subscriber may check the Subscriber's application information specified in section 9.3.1 paragraph (3). However, the BMSP CA reserves the right to collect reasonable fees from subscribers applying for access to this information.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

In the event of court order or administrative order, BMSP CA needs to disclose personal information with required by law or officers under the law.

9.4.7 Other Information Disclosure Circumstances

None

9.5 Intellectual Property Rights

BMSP CA is the sole owner of the intellectual property rights associated with the certificate, certificate revocation information, and this certificate practice statement. The CAs must not violate the intellectual property rights of third parties, including copyrights, patents, trademarks, or trade secrets. Additionally, due to legal restrictions, CAs must use all materials and software products related to intellectual property.

The company agrees that the CP may be freely downloaded from the CA repository. Copying and relevant copyright regulations may be distributed, but it must be copied in full, and the copyright must be noted as being owned by the issuing CA.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

CA assures that

1) Procedures are implemented in accordance with the CP of BMSP.
2) Any certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this CP.
3) Certification Practice Statement (CPS) will be provided, as well as any subsequent changes, for conformance assessment.
4) The CA operation is maintained in conformance to the stipulations of the CPS.
5) The registration information is accepted only from approved RAs operating under an approved CPS.
6) 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.
7) Certificates of subscribers found to have acted in a manner counter to their obligations in accordance with section 9.6.3 will be revoked.
8) All information regarding certificate issuance and certificate revocation are processed through the procedure specified in the CPS of the corresponding CA.

9.6.2 RA Representations and Warranties

An RA shall assure that

1) Its RA registration operation is performed in conformance to the stipulations of the approved CPS of the corresponding CA and related regulations.
2) 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.
3) The obligations are imposed on subscribers in accordance with section 9.6.3, and subscribers are informed of the consequences of not complying with those obligations.

9.6.3 Subscriber Representations and Warranties

By using the subscriber certificate, the subscriber assures that

1) He/She accurately represents itself in all communications with the CA.
2) The private key is properly protected at all times and inaccessible without authorization.

3) The CA is promptly notified when the private key is suspected loss or compromise.

4) All information displays in the certificate is complete and accurate.

5) The certificate will be used legitimately under laws, related regulations, terms, conditions and other related service announcements of the CA by authorized persons.

9.6.4 Relying Party Representations and Warranties

In case of relying party representations use the certificate, the relying party shall properly verify information inside the certificate before use and accepts the fault of single side verification.

9.6.5 Representations and Warranties of Other Participants

Not Applicable.

9.7 Disclaimers of Warranties

The Certificate Authority (CA) does not provide any express or implied warranties except those stated in this Certificate Policy and Certification Practice Statement. It also does not guarantee commercial performance or any specific purpose.

9.8 Limitations of Liability

The disclaimers and limitations on liabilities in this CPS are fundamental to using BMSP CA Certificates and services.

All liability is limited to actual and legally provable damages. BMSP CA is not liable for:

1. Any indirect, consequential, special, or punitive damages or any loss of profit, revenue, data, or opportunity, even if BMSP CA is aware of the possibility of such damages;

2. Liability related to fraud or willful misconduct of the Applicant;

3. Liability related to the use of a Certificate that exceeds the limitations on use, value, or transactions as stated either in the Certificate or this CPS

4. Liability related to the security, usability, or integrity of products not supplied by BMSP CA, including the Subscriber’s and Relying Party’s hardware or

5. Liability related to the compromise of a Subscriber’s Private Key.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, (iv) whether DigiCert failed to follow any provision of this CPS, or (v) whether any provision of this CPS was proven ineffective.

To the extent BMSP CA has issued and managed the Certificate(s) at issue in compliance with this CPS and its CPS, DigiCert shall have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s). To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall limit DigiCert's and the applicable Affiliates' liability outside the context of any extended warranty protection program. Limitations of liability shall include excluding indirect, special, incidental, and consequential damages.

9.9 Indemnities

Indemnity claims shall be agreed between the CA and Subscribers. However, in cases where relying parties use the certificate without checking the CRL, the CA reserves its right to deny any indemnity claims for any damage to arise. If damage occurs to the CA from the actions of the CA reserves the right to claim damages to subscribers, subscribers or relying parties.

9.10 Term and Termination

9.10.1 Term

The CPS and any attachments take effect when published on the BMSP CA website and repository and remain in effect until replaced with a newer version.

9.10.2 Termination

This CPS takes effect until it is terminated.

9.10.3 Effect of Termination and Survival

The terms and impact of the CPS termination will communicated through the BMSP CA website and repository. This communication will highlight the provisions that remain in effect after CPS termination. At the very least, the responsibilities related to protecting confidential information will continue after CPS termination.

9.11 Individual Notices and Communications with Participants

The CA provides means of communication for Subscribers, including telephone and email, as shown on the CA's website. BMSP CA will communicate to those participants using a reliable channel as soon as possible of the importance of information.

9.12 Amendments

The CA reserves the right to modify, add, cancel, or change any terms of service within this document.

9.12.1 Procedure for Amendment

The CPS undergoes a regular annual assessment to determine if any amendments are needed to maintain its assurance level. Amendments can be made by attaching documents or directly revising the CPS content. If the CP or the OID is amended, the CPS shall be amended accordingly. The notice may be a letter, email, or announcement on the CA website: https://

9.12.2 Notification Mechanism and Period

If the CA or its Subscriber believes that modifying, adding, cancelling, or changing the terms will reduce their legitimate rights, the RA or Subscriber can request to terminate the service as outlined in this document. They must notify the CA at least 30 days before the effective date of termination unless the law requires the modification, addition, cancellation, or change of terms.

9.12.3 Circumstances under Which OID Must Be Changed

If changes to the CP do not impact the certificate's usage and assurance level as specified in the CP, then the CP OID does not need to be modified. Any adjustments made to the CP OID should reflected in the corresponding changes to the CPS.

9.13 Dispute Resolution Provisions

9.13.1 Disputes between Issuer and subscriber

The decisions made by BMSP CA regarding matters within the scope of this CPS are final. Any claims should submitted to BMSP CA at the following address:

The Director of BangkokMSP
Bangkok MSP Company Limited
555/2 Floor B SSP Tower, Soi Sukhumvit 63 (Ekamai),Kwang Klongton Nua, Khet Wattana, Bangkok 10110 THAILANDTel: (+662) 0927464
Email: NCLCA@bmsp.tech
Website: Https://bmsp.tech
In the event of uncertainty, the Policy Authority has jurisdiction over the dispute.

9.13.2 Disputes between Issuer and Relying Parties

The procedure is the same as stated in Section 9.13.1. In undefined situations, the PA has jurisdiction over the dispute.

9.14 Governing Law

The laws of the Kingdom of Thailand will govern the CPS.

9.15 Compliance with Applicable Law

The BMSP CA complies with the laws of the Kingdom of Thailand regarding electronic certificate issuance.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This document, the certificate application, and the terms of certificate use are essential information the CA provides to the Subscribers regarding the terms for managing the certificate. It is equivalent to an agreement between the CA and Subscribers to process and comply with such a document.

9.16.2 Assignment.

The CA agrees not to transfer the rights or duties described in this document, whether partially or in its entirety, to a third party unless prior written consent is obtained from the Subscriber.

Such consent, under paragraph one, does not relieve the CA of the liabilities accrued as a result of this agreement; thus, the CA shall share the liabilities for damages caused by the recipient, whether willfully or by negligence.

9.16.3 Severability

In circumstances where any part of this document becomes void, incomplete, or unenforceable by law, the affected clause or clauses shall not affect the applicability of other complete and enforceable clauses within this agreement.

Regarding the issuance of SSL certificates, the CPS complies with the requirements in the official version of the Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates issued by CA/Browser Forum (http://www.cabforum.org); however, if the related requirements of the Baseline Requirements conflict with the related domestic laws and regulations complied by the CPS; the CPS may adjust to satisfy the requirements and regulations and notify the CA/Browser Forum about the changed contents of the CPS. Suppose the domestic laws and regulations are not applicable anymore, or the Baseline Requirements are revised their contents to be compatible with the domestic laws and regulations. In that case, the CPS will delete and amend the adjusted contents. The actions mentioned above shall completed in 90 calendar days.

9.16.4 Enforcement

The party that violates the agreement will be responsible for all incurred costs, including attorney fees resulting from non-compliance with this document and related documents. Any waiver or extension granted by any party under this document will considered specific to that instance only and does not imply a waiver of rights under this document.

9.16.5 Force Majeure

In this case, each party shall not be held liable for the damages resulting from the inability or delay to act according to this document due to force majeure.

In circumstances where one party cannot act according to this document due to force majeure, the affected party must immediately notify the other party in writing, describing the nature of the force majeure, action taken to mitigate or negate the impact of such force majeure, and estimation of possibility of the force majeure to subside.

Force majeure may refer to events beyond the control of each party that result in the inability or impossibility to perform their duties described in this document. Force majeure may include natural disasters, earthquakes, fires, explosions, strikes, labour disputes, protests, accidents, epidemics, storms, floods, wars, revolutions, civil unrest, and shortages of resources such as water, electricity, fuel, or labour.

If force majeure persists for longer than 30 days, both parties may agree to terminate the service or certificate issuance according to this contract.

9.17 Other Provisions

Not Applicable.