VIETNAM POST AND TELECOMMUNICATIONS GROUP

=====*=====**

PRACTICE STATEMENTS

DIGITAL SIGNATURE AND DIGITAL SIGNATURE CERTIFICATION SERVICES FOLLOW THE REMOTE DIGITAL SIGNING MODEL

(VNPT SMARTCA)

Hanoi, 2022

DIGITAL SIGNATURE AND DIGITAL SIGNATURE CERTIFICATION SERVICE UNDER REMOTE DIGITAL SIGNATURE MODEL – VNPT SMARTCA

ATTESTATION REGULATION DOCUMENTS

Effective Date:	04/08/2021
Enactment:	01
Version:	2.0

	Full Name	**Title**	**Unit**
Edit:	Nguyen Dang Huy	Patriarch	eGOV Center – VNPT-IT Company
Check:	Nguyen Thanh Phong	PDM	eGOV Center – VNPT-IT Company
Appraisal:	Nguyen Thi Thanh Chung	SPDV Management	Marketing - Sales Department – VNPT-IT Company

DOCUMENT CHANGE TRACKING TABLE

Date of revision	**What's changing**	**Effective date**	**Approve**
01/06/2021	Create new	04/08/2021	04/08/2021
08/06/2022	Update content	28/07/2022	28/07/2022

TABLE OF CONTENTS

Introduction

This document is a set of certification regulations (CPS) declaring in principle the governance policies of VNPT SmartCA in the process of providing digital signature services and certifying digital signatures under the remote digital signature model. The CPS sets out legal requirements, technical requirements, as well as business requirements for the process of approving, allocating, managing, using, revoking and reissuing digital certificates in VNPT SmartCA system. The requirements of CPS ensure the confidentiality and integrity of VNPT SmartCA service, applied to all participants in VNPT SmartCA digital signature certification service. This CPS is not a legal agreement between VNPT SmartCA and entities using digital signature services and certifying digital signatures under the remote digital signature model.

The objectives of this text are:

- VNPT SmartCA service provider operates with the regulation of digital signature certification according to the remote digital signature model and complies with the requirements in this CPS.

- Provide customers using VNPT SmartCA service about their authentication process and responsibilities.

- Provide information to trusted partners (Relying party) about the level of assurance that VNPT SmartCA certificate provides.

- This CPS complies with the laws of Vietnam as well as policies and regulations promulgated by state authorities, the Ministry of Information and other relevant authorities.

1. INTRODUCTION

1.1. Overview

VNPT SmartCA is the name of the digital signature and digital signature certification service under the remote digital signature model provided by Vietnam Post and Telecommunications Group. The regulations on digital certificate policy of VNPT SmartCA service presented in this document include: issuance of certificates, management, revocation and re-issuance of digital certificates for end-to-end subscribers, regulations on the use of digital signature services and digital signature certification under the remote digital signature model.

1.2. Name and identifying signs

This document is a set of certification regulations (CPS) declaring in principle the governance policies of VNPT SmartCA in the process of providing digital signature services and certifying digital signatures under the remote digital signature model. The CPS sets out legal requirements, technical requirements, as well as business requirements for the process of approving, allocating, managing, using, revoking and reissuing digital certificates in VNPT SmartCA system. The requirements of CPS ensure the confidentiality and integrity of VNPT SmartCA service, applied to all participants in VNPT SmartCA digital signature certification service. This CPS is not a legal agreement between VNPT SmartCA and entities using digital signature services and certifying digital signatures under the remote digital signature model.

The objectives of this text are:

- VNPT SmartCA service provider operates with digital certification regulations and complies with the requirements in this CPS.
- Provide customers using VNPT SmartCA service about their authentication process and responsibilities.
- Provide information to trusted partners (Relying party) about the level of assurance that VNPT SmartCA certificate provides.

- This CPS complies with the laws of Vietnam as well as policies and regulations promulgated by state authorities, the Ministry of Information and other relevant authorities.

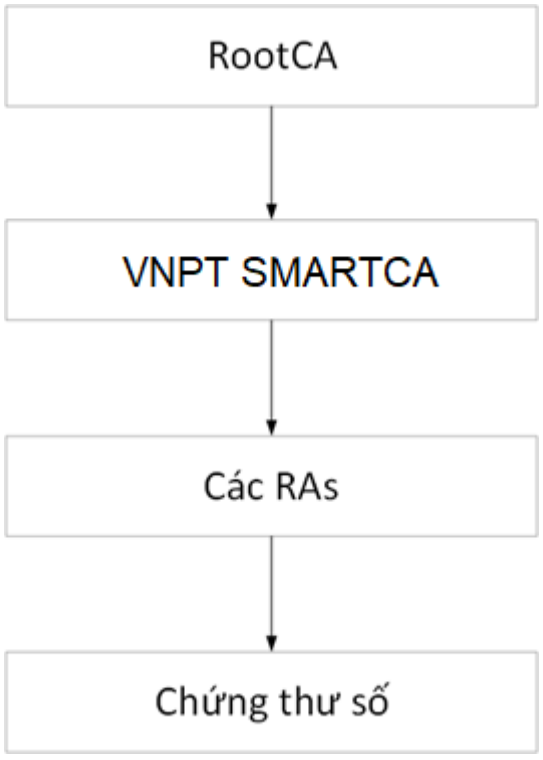
1.3. Participants of VNPT SmartCA service.

1.3.1. Certification Authorities (CA) Component

VNPT SmartCA service overview structure is presented in the diagram below. At the peak of decentralization is RootCA, the unit that licenses VNPT SmartCA to become a provider of digital signature certification services under the remote digital signature model. RootCA is also the regulator and manager of the content, policies and certification regulations of the service must follow.

VNPT SmartCA is a unit under the management of the Ministry of Information and Communications that is allowed to provide directly to end users in this trusted network.

Registration Authorities (RA) are the entities responsible for verifying information and verifying requests in VNPT SmartCA service. The RAs of VNPT SmartCA service are responsible for authenticating information about subjects who want to register to use authentication services. Subscribers' certificates can be issued from VNPT SmartCA or through RA management units.



If subscribers register to buy VNPT SmartCA service, their identity will be verified by eKYC technology on VNPT SmartCA app. After successful authentication, the subscriber

initialization will be approved by CA personnel to issue a digital certificate. To use the service, subscribers activate the key and receive the newly issued digital certificate.

The subscription period waiting for CA approval to be issued a digital certificate:

- For weekdays: up to 4 hours.
- For holidays: up to 8 hours.

Rights of VNPT SmartCA:

VNPT SmartCA is a provider of digital certificates and digital signature services and digital signature certification under the remote digital signature model. In the organizational model of VNPT SmartCA for this service, VNPT SmartCAs do not have SUB-CA to issue digital certificates but have RA units responsible for issuing certificates and digital signature services and certifying digital signatures according to the remote digital signature model for end users.

CA has the following obligations:

- Do not issue digital certificates with false information compared to reality.
- Ensure that the end-user's digital certificate meets CPS standards.
- Ensure that the place where digital certificates are stored is in accordance with the standards in the CPS, ensuring the service of revocation and use of digital certificates.

1.3.2. Registration Authorities (RA) Component

Rights of the RA:

- Receive, check, approve or reject the request to register for service and initialize VNPT SmartCA subscriber information.

Obligations of RA:

- Provide accurate information about VNPT SmartCA service to customers.
- Receive requests for digital certificates of customers according to the CPS regulations of VNPT SmartCA.
- Send requests for digital certificates and digital letters to VNPT SmartCA.
- Sign the papers and handover minutes between the two parties.
- Receive verified required information from AM to create subscriber information

1.3.3. Account Manager (AM) Components

AM's rights:

- Receive, check, approve or reject the request to register VNPT SmartCA service.

Obligations of AM:

- Receive applications for providing digital certificates and digital letters of customers in accordance with the CPS regulations of VNPT SmartCA.

- Check the information of the Contract, Appendix of the service application form and subscriber records against the original documents of the subscriber

- Sign the papers and handover minutes between the two parties.

1.3.4. Subscription

Subscriber rights:

- Digital certificates are issued in accordance with the type of digital certificate requested by the subscriber.

- The subscriber's digital certificate is accepted and operated during the validity period of the digital certificate;

- Subscribers may use digital signature services and authenticate digital signatures under the remote digital signature model according to the validity of the tariff package specified in the service provision contract.

- Subscribers have the right to request renewal and revocation of their digital certificates.

- The subscriber has the right to confirm through the registered device all actions related to his secret key.

- Subscribers have the right to extend, suspend or cancel digital signature services and digital signature certification under the remote digital signature model.

Obligations of subscribers:

- All commitments submitted by subscribers in the subscriber digital certificate application are true.

- All information provided by subscribers and contained inside digital certificates is true.

Digital certificates must be used for lawful purposes and comply with the requirements of the CPS.

- Do not forge digital certificates of VNPT.

- If there is any change in information, it must be notified to the new entry point of VNPT SmartCA service.

- Request to revoke digital certificates in case of errors that may affect all digital certificates of VNPT.

1.3.5. Recipient composition

Recipient's rights:

- The recipient is an individual or group that is trusted, checking the digital certificate of the partner according to the agreement and commitment between the two parties.

- The recipient has the right to confirm that the subscriber's information in the digital certificate is true.

- The recipient relies on the information in the digital certificate to be accurate and the information in the CPS to make a decision to implement the agreement and commitment between the two parties.

- The recipient must be the subject of the issued digital certificate or must have a legal power of attorney of the subject.

Obligations of the recipient

- Receive notices of VNPT SmartCA about cooperation conditions for 3rd parties.

- Only trust the digital certificate provided by VNPT SmartCA if it is valid and updated regularly.

- Only trust a digital certificate if it has not been revoked.

- Only trust VNPT SmartCA application on mobile devices provided by VNPT SmartCA, notified on the official website of VNPT SmartCA service

- Must immediately notify the RA if it suspects that the secret key has been disclosed, stolen or modified or destroyed;

- Must immediately notify RA if you suspect that the VNPT SmartCA application on the phone shows signs of being falsified, copied or the PIN code is exposed.

1.3.6. Other components

*) VNPT SmartCA application on mobile devices.

VNPT SmartCA application is a mobile application that helps users control all actions related to secret keys.

VNPT SmartCA application supports two mobile platforms:

- iOS, version: 10.0 and above.

- Android, version: 5.0.0 and above.

Device requirements: do not support tampered mobile devices, modified to remove the restrictions that the manufacturer has installed (these behaviors are also known as root/jaibreak).

For Android mobile devices: Google Play Protect certification is required.

*) Website VNPT SmartCA

VNPT SmartCA website is the official website of VNPT SmartCA service.

The subscriber manages the secret code to generate OTPs for the integrated gender tariff plan.

Subscribers use VNPT SmartCA application to create OTP strings for authentication during the digital signing process.

1.4. Purpose of using digital certificates

1.4.1. Legal digital certificate

All digital certificates must be used in accordance with the law and this CPS document

1.4.2. Digital certificates are not legal

Without

1.5. Management of authentication mechanism

1.5.1. Management organization

Vietnam Post and Telecommunications Group (VNPT).

VNPT Building, No. 57 Huynh Thuc Khang, Dong Da District, Hanoi, Vietnam.

1.5.2. Contact

VNPT Information Technology Company (VNPT IT).

VNPT Building, No. 57 Huynh Thuc Khang, Dong Da District, Hanoi, Vietnam.

And

Vinaphone

VNPT Building, No. 57 Huynh Thuc Khang, Dong Da District, Hanoi, Vietnam.

1.5.3. Unit that decides the legality of CPS

This CPS document is developed in accordance with the provisions of law as well as the list of mandatory standards applicable in the field of digital signatures of the Ministry of Information and Communications. VNPT SmartCA is responsible before law for the legality of this CPS document.

1.5.4. CPS approval procedure

VNPT IT is the competent unit to approve this CPS and related changes in the operation of VNPT SmartCA. Changes must be approved by Center leadership. All revised or updated versions are published at https://vnpt-ca.vn/download-page

1.6. Definitions and acronyms

Terminology	Explain
SONG	Certificate Authority – An organization providing public digital signature certification services.
CP	Certificate Policies
CPS	Certification Practice Statement
CRL	Certificate Revocation List – List of revoked digital certificates
OCSP	Online Certificate Status Protocol – is a protocol that allows checking the status of digital certificates online
Go out	Registration Authority – The organization that receives, registers and verifies information of service users.
HERMITAGE	Account Manager – Human resources act as the focal point in matters related to the contract with the subscriber.
BATTERY	The secret code is used on the mobile application to confirm all actions related to the secret key, which is set by the subscriber and known only to the subscriber.
OTP	One Time Password

2. RESPONSIBILITY FOR INFORMATION STORAGE AND DISCLOSURE

2.1. Storage

VNPT SmartCA stores subscribers' digital certificate information on Oracle, MySQL and LDAP database management systems.

The storage and updating of the list of valid and publicly expired digital certificates on the internet allows 24/7 access by VNPT SmartCA by functional servers: CRL, LDAP, OCSP. These servers are built by VNPT SmartCA located in a public network partition with broadband, located in VNPT's Data Center with stable internet connection, high speed, environmental

conditions, stable power supply and a technical team to maintain the system 24/7 to ensure the continuity of service provision and system availability.

CRL revoked digital certificate list is a list of serial numbers of revoked digital certificates published by service providers, relying parties need to check the certificates and refuse to trust these certificates. A CRL is stored in the service provider's public directory, which is created periodically over a period of time or immediately after a digital certificate is revoked or suspended. VNPT SmartCA service provider system stores and automatically updates periodically and continuously information on the list of valid and expired digital certificates. The list of CRL revocation digital certificates is placed on the CRL server to ensure 24/7 online accessibility, the access protocol to obtain the CRL can be HTTP or FTP.

Store all information related to the suspension or revocation of licenses and databases on subscriptions and digital certificates for at least 05 (five) years after the license is suspended or revoked.

2.2. Information disclosure

VNPT SmartCA system publicly announces customers' digital certificates through https://vnpt-ca.vn service website, this channel is public so that VNPT SmartCA customers can access digital certificate information and check the status of digital certificates.

For customers who self-search information through the website of the service https://vnpt-ca.vn/khach-hang/tai-lieu customers need to provide the following information to be able to perform information searches:

- Serial Number
- Full name of the subscriber (CN)
- Districts (L)
- Province/City (ST)

Customers enter this information right on the service's website.

2.3. Time and frequency of information disclosure

Regulations on authentication and digital certificates of VNPT SmartCA service providers are published and updated when there is a change at https://vnpt-ca.vn/download-page address.

The system automatically and continuously updates information about the list of valid and expired digital certificates in the database system and the directory system. At the same

time, access to determine the validity (vadility) of deeds through OCSP and CRL services is guaranteed continuously and online via the Internet 24 hours a day and 7 days a week.

2.4. Control access to information

CPS changes are made on 2 factors: (1) According to new legal documents issued by the Government, the Ministry of Information and Communications, and the National Electronic Certification Center. (2) According to the actual requirements of the process of providing services to customers but still comply with regulations of state management agencies.

CPS changes are drafted and implemented by VNPT-IT Company as follows:

- Group Report – license holder.
- Provided to VNPT – VinaPhone – the unit assigned by the Group to sign service contracts with customers.
- Make irregular reports according to Circular 17/2014/TT-BTTTT of the Ministry of Information and Communications issued on November 26, 11, 2014 stipulating the reporting regime on digital signature certification activities to the National E-Certification Center

CRL updates are performed automatically by VNPT SmartCA system.

For customers who self-search information through the website of the service https://vnpt-ca.vn/khach-hang/tai-lieu customers need to provide the following information to be able to perform information searches:

- Serial Number
- Full name of the subscriber (CN)
- Districts (L)
- Province/City (ST)

Customers enter this information right on the service's website.

3. IDENTIFICATION AND AUTHENTICATION OF REQUESTS FOR DIGITAL CERTIFICATES

3.1. Naming in digital certificates

3.1.1. Properties

VNPT SmartCA certificates comply with ITU-T X.509 standard and the provisions in RFC5280: Internet X.509 Public Key Infastructure Certificate and CRL Profile ("RFC5280").

Digital certificates that comply with the X.509 V3 standard include basic fields and required values indicating or following the constraints in the table below:

School name	**Values or constraints**
Serial Number	Unique to an Issuer
Signature Algorithm	Hash algorithm: SHA256, Signing algorithm: RSA
Issuer	Information about the issuer of the deed
Valid from	The effective time of the digital certificate. Synchronized with the Master Clock of the U.S. Naval Observatory.
Valid to	The period of expiration of the validity of the digital certificate. Synchronized with the U.S.Naval Observatory.
Subject	Information about the recipient of the digital certificate
Public Key	Encoded according to RFC5280 standard 2048-bit RSA encryption

3.1.2. Clarity and meaning of names in deeds

The domain name does not need to be meaningful or unique, but needs to correspond to the second-level domain registered with InterNIC (third-level domain registered with VNNIC).

3.1.3. Where the subscriber uses an anonymous name or pseudonym

The subscriber is not allowed to use an anonymous name or pseudonym other than his real name.

3.1.4. Rules for interpreting name patterns

There are no regulations.

3.1.5. Uniqueness of the subscriber name

The subscriber name of VNPT SmartCA service will be uniquely associated with a specified digital certificate level in the domain of VNPT SmartCA service. A subscriber can have two or more digital certificates with the same name.

3.1.6. Brand identity, authentication and role

Subjects registering digital certificates may not use names protected by intellectual property rights for other subjects in accordance with the law on intellectual property.

In case of necessity, VNPT SmartCA will request the digital certificate registrant to provide documents proving intellectual property rights to the registered name.

However, VNPT SmartCA is not responsible for any intellectual property rights disputes arising related to the use of the name of the digital certificate registrant.

In case of necessity, VNPT SmartCA reserves the right to terminate or suspend any digital certificates related to the mentioned disputes.

3.2. Verification of application for digital certificate

3.2.1. Method of proving ownership of the secret key

The person registering a digital certificate must prove that he owns the secret key corresponding to the public key recorded in the digital certificate. The method of proving ownership of the secret key will comply with PKCS#10 standard or a corresponding cryptographic method, or another method recognized by VNPT SmartCA.

3.2.2. Organization Identity Verification

Contents of verification of subscriber information as an organization include:

- Tax code
- Name of the organization.
-Address.
- Industry: business license, establishment license (original or notarized copy of digital certificate).
- Information about the user of the deed.

In the case of verifying subscriber information using electronic identity verification tools, authentication contents include:

- Verify the original identity document (CMT/CCCD/ HC), document validity period.
- Verify the certificate of business registration.
- Match the face and identity documents of the legal representative and match the information of the business registration certificate.

3.2.3. Personal Identity Verification

Contents of authenticating personal subscriber information include:

-Address.

- A valid copy of ID card or passport.

In the case of verifying subscriber information using electronic identity verification tools, authentication contents include:

- Verify original ID (CMT/CCCD/HC), document validity period

- Face matching and ID.

3.2.4. Non-verified subscriber information

There are no regulations.

3.2.5. Authentication of authority

When the name of the individual in the digital certificate is related to an organization, it is necessary to perform:

- Determine the existence of the organization through at least one third party.

- Verify the information stated in the Digital Certificate Request Form through necessary and collectable documents.

- Determine whether the identity and position of the individual in the organization correspond to the registered information or not.

3.2.6. Interoperative performance standards

There are no regulations.

3.3. Verify the key pair change offer

The subscriber who wishes to change the key pair must present a registration contract using the signed digital certificate to prove that he has the right to request it. In case of contract loss, the subscriber must provide all necessary information to match the original digital certificate registration information, including:

For organizations

- Name of the organization.

-Address.

- Industry: business license, establishment license (original or notarized copy of digital certificate).

- Information about the user of the deed.

For individuals

-Address.

- A valid copy of ID card or passport.

3.4. Verification of the request for revocation of digital letters

Only in the situations listed below, the subscriber's digital certificate will be revoked by VNPT SmartCA and published on the CRL.

A subscriber's letter digital certificate will be revoked if it falls into some of the following situations:

- VNPT SmartCA or RA, subscribers have reason to believe or suspect the compromise of the secret key of the digital certificate.

- VNPT SmartCA or RA have reason to believe that the subscriber is in breach of its obligations and responsibilities to the contract or agreements committed by the subscriber.

- VNPT SmartCA or a subscriber has reason to believe that the issued Digital Certificate is not in accordance with the provisions of the CPS. Digital certificates created for individuals are not named as in the Certificate of Use of Digital Certificates.

- The information in the Deed is incorrect.

- The continued use of this digital certificate endangers VNPT SmartCA.

When considering whether the use of digital certificates is harmful to VNPT SmartCA or not, VNPT SmartCA considers between the following factors:

- The source and name of the complaints received.

- Confirm the complainant.

- Coercion under the law.

- Respond to the registrant's harmful use.

VNPT SmartCA can revoke the administrative digital certificate if the administrator's authority ends.

The agreement between VNPT SmartCA and the subscriber requires this subscriber to promptly notify VNPT SmartCA of the risk of revealing the secret key of the subscriber's digital certificate, revealing the PIN code, revealing the secret code creating OTP, VNPT SmartCA application on the mobile device showing signs of being falsified or copied.

4. REGULATIONS ON THE MANAGEMENT OF THE LIFE CYCLE OF DIGITAL CERTIFICATES

4.1. Request for digital certificate

4.1.1. Subjects allowed to request digital certificates

Subjects allowed to request for digital certificates include:

- Any individual or organization eligible under the provisions of law and this CPS wishing to use digital certificates.

- The legal representative of the organization is eligible as prescribed by law and this CPS needs to use digital certificates.

A digital certificate is issued according to the approval of the application for a digital certificate by VNPT SmartCA or the receipt of a request from RA to issue a digital certificate. VNPT SmartCA shall issue to applicants for digital certificates one digital certificates on the basis of information on the application for digital certificates after being approved.

4.1.2. Application process for digital certificate

4.1.2.1. Traditional form

Subscribers who want to register to use digital certificates need to go to registration points including transaction points of VNPT SmartCA, or directly register transactions at VNPT's headquarters and branches.

Subscribers need to declare necessary information on the standard information declaration form of the service issued by VNPT SmartCA. Then pass it back to RA and wait for the credentials to respond.

The RAs verify the declared subscriber information and verify the subscriber information. In case the information verification is accepted or not accepted, the RAs are responsible for sending the result form notifying the information verification to the registered subscriber.

RA is responsible for making a contract for registration using digital certificates with registered subscribers in case credentials are accepted.

4.1.2.2. Application of identity verification via electronic tools

The subscriber declares the necessary information according to the form of the above service Sales apps, after making payment and signing an electronic contract, the subscriber's registration information is accepted and transferred to the identity verification step.

Verification of the identity of the subscriber is carried out automatically via electronic tools; Information to be verified is described in the section 3.2.2 and 3.2.3 This document.

4.2. Processing requests for digital certificates

4.2.1. Identity authentication

VNPT SmartCA verifies the identity of all information of the person requesting the issuance of digital certificates according to Section 3.2.

4.2.2. Accept or refuse to issue digital certificates

VNPT SmartCA only accepts requests for digital certificates if all conditions are satisfied: Successfully authenticate all information about the subjects requesting digital certificates according to section 3.2.

Subjects requesting digital certificates shall fully pay the service fee for issuance of digital certificates and digital signature services and certification of digital signatures according to the remote digital signature model to VNPT SmartCA.

VNPT SmartCA rejects a request for a digital certificate in the following cases:

- Identity verification fails at least one of the information about the person requesting a digital certificate under section 3.2.

- The person requesting the issuance of digital certificates does not provide sufficient documents as requested.

- The person requesting the digital certificate does not respond to the contact request within the specified time limit.

- Subjects requesting digital certificates have not paid the service fee for issuance of digital certificates.

- There are grounds to believe that VNPT SmartCA's issuance of digital certificates to requesters may affect the reputation and reliability of VNPT SmartCA.

4.2.3. Request processing time

VNPT SmartCA is responsible for processing requests for digital certificates within an appropriate period of time. There is no time to specify the time to complete the processing of a request for a digital certificate unless agreed in the Service Contract or CPS, however the maximum time is 3 working days. The request for digital certificate will remain valid until rejected by VNPT SmartCA.

4.3. Issuance of digital certificates

4.3.1. CA activities in issuing digital certificates

Digital certificates are created and issued based on the results of acceptance of digital certificate requests. VNPT SmartCA creates and issues digital certificates according to the information in the request for digital certificates that have been verified by identity.

4.3.2. Notification to subscribers

- VNPT SmartCA automatically notifies the Subscriber about requesting the Subscriber to activate the service via email and SMS immediately after the account is successfully initialized. The SMS receiving email and phone number are registered when the subscriber makes a request form for digital certificate.

- VNPT SmartCA automatically notifies subscribers that their digital certificate has just been issued through notification on the mobile application (VNPT SmartCA) immediately after the digital certificate is issued.

4.4. Certificate of digital certificate

4.4.1. Conditions for proving the acceptance of digital certificates

When the subscriber completes the activation of the service on the mobile application and is granted a digital certificate, the subscriber needs to sign and confirm the procedures for completing the issuance of digital certificates and initiating digital signature services and certifying digital signatures according to the remote digital signing model.

4.4.2. Announcement of digital certificates

VNPT SmartCA publicly announces the issued digital certificate on the public repository under part 2.

When the subscriber successfully activates the service on the mobile application, then the new digital certificate starts to take effect.

4.4.3. Notify other entities of the issuance of digital certificates

VNPT SmartCA will directly notify subscribers that their digital certificates have just been renewed.

4.5. Using key pairs and digital certificates

4.5.1 How to use digital certificates and subscription secret keys

The use of the secret key corresponding to the public key in the digital certificate is allowed only when the subscriber accepts the digital certificate. Digital certificates will be used legally based on the terms of the Service Contract, the terms of this CPS as well as the provisions of law. The usage of the digital certificate must correspond to the specified value of the KeyUsage field inside the digital certificate (For example, if the Digital Signature value is not in the KeyUsage field, this digital certificate cannot be used for digital signing).

The subscriber is responsible for protecting the secret key from illegal use and shall not be allowed to use the secret key when the digital certificate expires or is revoked or the digital signature service package and digital signature certification are expired according to the remote digital signature model specified in the service contract.

X.509 version 3 certificates were created in accordance with RFC5280. Key usage extensions for X.509 version 3 certificates are generally configured as setting and removing minor sections and key fields that fit into the table below. Fields that are important in extending key usage are generally set to TRUE for certificates and can be set to TRUE or FALSE for end-user registrant certificates.

	Cas	Digital certificates of individuals and	SSL digital certificate	Digital certificate Code Signning

			organizations		
Criticality		TRUE	FALSE	FALSE	FALSE
0	digitalSingnature	Clear	Set	Set	Set
1	nonRepudiation	Clear	Set	Clear	Set
2	keyEncipherment	Clear	Set	Set	Clear
3	dataEnciphermen t	Clear	Set	Clear	Set
4	keyAgreement	Clear	Clear	Clear	Clear
5	keyCertSign	Set	Clear	Clear	Clear
6	CRLSign	Set	Clear	Clear	Clear
7	encipherOnly	Clear	Clear	Clear	Set
8	decipherOnly	Clear	Clear	Clear	Set

The subscriber controls all actions related to the secret key, including: generating the secret key, generating requests for digital certificates, signing digitally.

Subscribers using VNPT SmartCA application on mobile devicesor for subscription limit packages use OTPs generated from secret codes to confirm the use of the subscriber's secret key

Subscribers sign digitally by confirming the PIN code on the registered mobile device or OTP generated from the secret code on VNPT SmartCA website.

4.5.2. How to use the recipient's digital certificate and public key

The recipient will be guaranteed by VNPT SmartCA the terms of reliability of the digital certificate. The reliability of digital certificates is determined based on each specific circumstance. If circumstances indicate that additional assurance is required, then the recipient must obtain the assurance that it should have. Before being trusted, the recipient will be independently assessed for the following factors:

- Digital certificates are used for appropriate purposes and determine that such purposes are not prohibited or limited by VNPT SmartCA, CPS or the provisions of law including the following contents:

+ Comply with the provisions of Law related to public digital signatures such as the Law on Electronic Transactions, Circular 16, Circular 22, and other documents as prescribed by Law.

+ Perform public administrative transactions: Tax, Customs, Treasury, Social Insurance, Health, Education, National Public Service Portal, and other systems as prescribed by law.

+ Performing transactions such as: Banking, securities, Insurance (life, non-life), e-contracts.

- VNPT SmartCA is responsible for guiding Subscribers to use digital certificates for the right purposes as described above and in the content of the Contract.

- VNPT SmartCA is responsible for coordinating with competent authorities to check and evaluate whether the use of digital certificates of subscribers is in accordance with the provisions of law or not in case of request of competent agencies.

- The digital certificate is used in accordance with the extension of the KeyUsage field in the digital certificate (For example, if the digital signature is not valid, the digital certificate is not trusted for the signature authenticity of the subscriber)

- Check the status of digital certificates and all CAs in the chain participating in issuing digital certificates. If any digital certificate in the chain is revoked, the recipient is responsible for reviewing the reliability of the digital signature made by the subscriber at the time before it is revoked. Any trust given may pose a risk to the recipient. When using digital certificates reasonably, recipients need to use reasonable software and hardware means to verify digital signatures or other necessary cryptographic operations. These operations include both identifying the digital certificate chain and verifying the digital signatures on all digital certificates in the chain.

4.6. Renewal of digital certificates

4.6.1. Extension conditions

- The subscriber makes a request to renew the digital certificate within 90 days before the expiry date of that certificate.

- Only subscribers with personal digital certificates or a legal representative can request renewal of digital certificates.

- Complete the cost of digital certificate renewal service.

4.6.2. Who is allowed to request an extension

Only individual subscribers or legal representatives of organizations for organizational subscribers are allowed to request renewal of digital certificates.

4.6.3. Processing requests for renewal of digital certificates

Subscribers need to carry out the procedures mentioned in section 4.1.2 and fill in the required information in the Digital Certificate Renewal Request Form according to the form issued by VNPT SmartCA. RA shall verify the subscriber's information in the Digital Certificate Renewal Request Form in accordance with section 3.2. If the information is authentic, the renewal is proceeded. If the information is false, the request is denied

4.6.4. Notify subscribers of the issuance of new digital certificates

The notification to subscribers of the issuance of new digital certificates shall comply with the provisions of section 4.2.2.

4.6.5. Terms of acceptance of renewal of digital certificates

Conditions constituting the renewal clause of the digital certificate are subject to section 4.3.1.

4.6.6. Announcement of renewed digital certificates

VNPT SmartCA is responsible for publishing digital certificates renewed on public repositories according to part 2.

4.6.7. Notify other entities of the renewal of digital certificates

VNPT SmartCA is responsible for notifying RA about the renewal of digital certificates because they verify their identity.

4.7. Change Key Pair

4.7.1. Changing conditions

Subscribers wishing to change key pairs must present a Service Contract to prove the required rights. In case of loss of contract, the subscriber must provide all necessary information in accordance with the information registered to use the original digital certificate as prescribed in section 3.2.

4.7.2. Who is allowed to request to change the key

Only individual subscribers or legal representatives of organizations for organizational subscribers are allowed to request changes to the digital certificate key.

4.7.3. Handling Key Change Requests

Subscribers need to carry out the procedures under section 4.1.2 and fill in the required information in the Key Change Request Form according to the form issued by VNPT SmartCA. VNPT SmartCA or RA shall verify the information provided by the subscriber in accordance with section 3.2. If the credentials are authentic, the key replacement is carried out. If the information is false, the request is denied.

4.7.4. Notify subscribers of the replacement of digital certificate keys

VNPT SmartCA is responsible for notifying subscribers about the renewal of digital certificates.

4.7.5. Terms of acceptance to replace digital certificate keys

Terms of acceptance of replacement of digital certificate keys according to section 4.3.1.

4.7.6. Announcement of digital certificates with replacement keys

VNPT SmartCA is responsible for publishing digital certificates that are locked on public repositories according to part 2.

4.7.7. Notify other entities about the replacement of digital certificate keys

VNPT SmartCA is responsible for notifying AM about the change of the subscriber's key because they authenticate their identity.

4.8. Cancel key pair

Cases in which the key of the subscription is canceled:

- The subscriber submits a request to cancel the lock.

- The digital certificate expires and does not apply for renewal.

- Digital certificates are revoked before expiration and not replaced with new digital certificates.

Procedure for canceling lock

VNPT SmartCA service will change the status of the subscriber on the system to the inactive state and cancel the lock and send notifications to the subscriber automatically in the following cases:

- The digital certificate expires and does not apply for renewal.

- Digital certificates are revoked before expiration and not replaced with new digital certificates.

In case the subscriber sends a request to cancel the key, VNPT SmartCA will carry out the following procedures:

Subscribers:

- Send a request for cancellation to the service provider with the signature or legal seal of the subject.

HERMITAGE:

- Verify and authenticate accurately the cancellation request information from the subject submitting the cancellation application.

- In case the information is invalid, AM automatically cancels the request and is responsible for notifying the refusal to the applicant.

- In case the information is valid, AM sends a report of credentials with a request to collect the key to RA as a basis for making the request.

Go out:

- Send the subscriber's cancellation request to VNPT SmartCA.

VNPT SmartCA:

- VNPT SmartCA authenticates RA and sent RA information, if valid, VNPT SmartCA will proceed to cancel the subscriber's key.

- VNPT SmartCA is responsible for updating information on the database of cancellation of subscribers' keys.

- VNPT SmartCA sends notifications about the cancellation of the lock directly to the subscriber or through the RA directly managed.

4.9. Change of digital certificate

4.9.1. Changing conditions

Subscribers who wish to change the digital certificate must present a Service Contract to prove the right to request. In case of loss of contract, the subscriber must provide all necessary information in accordance with the information registered to use the original digital certificate as prescribed in section 3.2.

4.9.2. Subjects allowed to request digital certificates

Only individual subscribers or legal representatives of organizations for organizational subscribers are allowed to request changes to digital certificates.

4.9.3. Handling requests to change digital certificates

AM shall validate the subscriber's information in the request to change the digital certificate in accordance with section 3.2. If the credentials are authentic, AM transfers the information to the system for RA to perform the Initiation of the request to change the digital certificate. If the information is false, the request is denied.

4.9.4. Notify the subscriber of the replacement of the digital certificate key

VNPT SmartCA is responsible for notifying AM about the change of digital certificate because they verify their identity.

4.9.5. Terms of acceptance to replace digital certificate keys

Terms of acceptance of changes to digital certificates pursuant to section 4.3.1.

4.9.6. Announcement of digital certificates has changed

VNPT SmartCA is responsible for publishing the changed digital certificate on the public repository according to part 2.

4.9.7. Notify other entities about the replacement of digital certificate keys

VNPT SmartCA is responsible for notifying AM about the change of digital certificate because they verify their identity.

4.10. Suspension and Revocation of Digital Certificates

4.10.1. Cases of revocation of digital certificates

Only in the situations listed below, the subscriber's digital certificate will be revoked by VNPT SmartCA and published on the CRL.

A subscriber's letter digital certificate will be revoked if it falls into some of the following situations:

- VNPT SmartCA or RA or AM, subscribers have reason to believe or suspect the compromise of the secret key of the digital certificate.

- VNPT SmartCA or RA or AM have reason to believe that the Subscriber is in breach of its obligations and responsibilities to the contract or agreements committed by the Subscriber.

- VNPT SmartCA or AM or a subscriber has reason to believe that the issued Digital Certificate is not in accordance with the provisions of the CPS. Digital certificates created for individuals are not named as in the Certificate of Use of Digital Certificates.

- The information in the Deed is incorrect.

- The continued use of this digital certificate endangers VNPT SmartCA.

When considering whether the use of digital certificates is harmful to VNPT SmartCA or not, VNPT SmartCA considers between the following factors:

- The source and name of the complaints received.

- Confirm the complainant.

- Coercion under the law.

- Respond to the registrant's harmful use.

VNPT SmartCA can revoke the administrative digital certificate if the administrator's authority ends.

The agreement between VNPT SmartCA and the subscriber requires this subscriber to promptly notify VNPT SmartCA of the risk of revealing the secret key of the subscriber's digital certificate.

4.10.2. Subjects of request for recall

Only individual subscribers or legal representatives of organizations for organizational subscribers are allowed to request changes to the digital certificate key.

4.10.3. Procedure for requesting revocation

Subscribers:

- Send a petition for revocation of the deed to the service provider with the signature or legal seal of the subject.

HERMITAGE:

- Verify and authenticate accurately the information requesting the revocation of the certificate from the subject submitting the revocation application.

- In case the information is not valid enough to be withdrawn, AM automatically cancels the request and is responsible for notifying the refusal to the applicant.

- Where the information is valid for revocation, AM sends a report of credentials with a request to revoke the certificate to RA as a basis for fulfilling the request.

RA:

- Send a request to stop digital certificate to VNPT SmartCA

VNPT SmartCA:

- VNPT SmartCA verifies RA and sent RA information, if valid, VNPT SmartCA will proceed to revoke the subscriber's certificate.

- VNPT SmartCA is responsible for updating information on the service's archive about revoked certificates.

- VNPT SmartCA sends notice of withdrawal directly to subscribers or through RA management directly.

4.10.4. Recall request processing time

Time for the revocation of deeds and notices should be processed as soon as possible.

4.10.5. Time for processing withdrawal requests

Time for the revocation of deeds and notices should be processed as soon as possible.

4.10.6. Request a recall check for recipients

Check the status of digital certificates at addresses: with OCSP path as http://ocsp-sha256.vnpt-ca.vn/responder and CRL as http://crl-sha256.vnpt-ca.vn/vnptca-sha256.crl.

4.10.7. Frequency of issuance of revoked digital certificates

For a CRL of 1 hour, OCSP is immediate when there is a recall request.

4.10.8. CRL's Biggest Latency Time

The biggest delay for the system to automatically update is 24 hours.

4.10.9. Support for online checking of the status of revoked digital certificates

Check the status of digital certificates at addresses: with OCSP path as http://ocsp-sha256.vnpt-ca.vn/responder and CRL as http://crl-sha256.vnpt-ca.vn/vnptca-sha256.crl.

4.10.10. Conditions for online inspection of revoked digital certificates

The recipient must check the status of the digital certificate before trusting it.

4.10.11. Other revoked digital certificate promotion forms

Without

4.10.12. Special conditions when the lock is compromised

VNPT SmartCA will use reasonable means to notify the recipient if detecting, or having reason to believe, that the secret key of one of the CAs or RAs of VNPT SmartCA has been compromised.

4.10.13. Cases of suspension

VNPT SmartCA will suspend the subscriber's digital certificate while processing the revocation of the subscriber's digital certificate.

VNPT SmartCA may directly suspend digital certificates in case it detects that the subscriber violates the terms of the service provision contract or violates the terms in accordance with current laws.

The owner of the digital certificate requests the suspension of the digital certificate.

Competent state agencies detect subscribers violating current legal provisions.

4.10.14. Who is allowed to request a suspension

Competent state authorities (such as procedural authorities, public security agencies, or ministries

Information and Communication).

VNPT SmartCA may suspend digital certificates in case real subscribers are detected currently not in accordance with the terms of the contract, violating current legal provisions.

For individual subscribers: Only the owner of the personal digital certificate has the right to request the suspension of the digital certificate.

For subscribers of organizations and enterprises: only the representative of the organization whose name has been authorized to be named on the digital certificate has the right to request the suspension of the digital certificate.

4.10.15. Procedure for requesting suspension

In case the subscription requires a pause:

Subscribers:

- Sign the application form for suspension of the deed to the service provider with the signature or legal seal of the subject.

HERMITAGE:

- Verify and authenticate accurately the information requesting suspension of the deed from the subject submitting the suspension application.

- In case invalid information is suspended, AM instructs subscribers to fill in the application form for suspension of digital certificates.

- Where the information is valid for pause, AM sends a credential report with a request to suspend the deed to RA as a basis for fulfilling the request.

RA personnel :

- Receive and create a request for a pause
- Transfer the suspension ticket to CA personnel

CA personnel:

- Check and approve the request form to suspend the subscriber's digital certificate

VNPT SmartCA:

- VNPT SmartCA authenticates the CA and CA information sent, if valid, VNPT SmartCA will proceed to suspend the subscriber's certificate.

- VNPT SmartCA is responsible for updating information on the repository of the service about the deed has been suspended.

- VNPT SmartCA sends notice of suspension directly to subscribers or through RA management directly.

In case VNPT SmartCA or competent state management agencies request to suspend:

HERMITAGE:

- Verify and authenticate accurately the information requesting suspension of the deed from the subject submitting the suspension application.

- AM sends a statement of credentials with a request to suspend the deed to the RA as a basis for fulfilling the request.

RA personnel :

- Receive and create a request for a pause
- Transfer the suspension ticket to CA personnel

CA personnel:

- Check and approve the request form to suspend the subscriber's digital certificate

VNPT SmartCA:

- VNPT SmartCA authenticates the CA and CA information sent, if valid, VNPT SmartCA will proceed to suspend the subscriber's certificate.

- VNPT SmartCA is responsible for updating information on the repository of the service about the deed has been suspended.

- VNPT SmartCA sends notice of suspension directly to subscribers or through RA management directly.

4.10.16. Suspension Time Limitations

Immediately after the end of the due diligence of the request.

4.11. Digital certificate status checking service

4.11.1. Operational characteristics

The status of digital certificates is checked through CRL, OCSP.

4.11.2. Service Availability

The digital certificate status check service is available 24/7 and without interruption.

4.11.3. Optional Features

No regulations

4.12. Termination of the Subscriber's Services

The subscriber shall terminate the use of the digital certificate in one of the following cases:

- The subscriber submits a request for termination of service.

- The digital certificate expires and does not apply for renewal.

- Digital certificates are revoked before expiration and not replaced with new digital certificates.

Service Termination Procedure

VNPT SmartCA service will change the status of the subscriber on the system to the inactive state and send notifications to the subscriber automatically in the following cases:

- The digital certificate expires and does not apply for renewal.

- Digital certificates are revoked before expiration and not replaced with new digital certificates.

In case the subscriber submits a request for service termination, VNPT SmartCA will carry out the following procedures:

Subscribers:

- Send a request for termination of service to the service provider with the signature or legal seal of the subject.

HERMITAGE:

- Verify and verify the correct information of the service termination request from the applicant.

- In case the information is invalid, AM automatically cancels the request and is responsible for notifying the refusal to the applicant.

- In case the information is valid, AM sends a report of credentials with the subscriber's request to terminate the service to RA as a basis for fulfilling the request.

Go out:

- Send a service termination request of the subscriber to VNPT SmartCA.

VNPT SmartCA:

- VNPT SmartCA authenticates RA and sent RA information, if valid, VNPT SmartCA will proceed to terminate the subscriber's service.

- VNPT SmartCA is responsible for updating information on the database of subscriber termination.

- VNPT SmartCA sends notice of service termination directly to subscribers or through direct management RA.

4.13. Storage and recovery of the Subscriber's secret key

Not provided.

5. CONTROL, MANAGEMENT AND OPERATION

5.1. Equipment, machinery, power supply, headquarters and other necessary elements

5.1.1 Construction location

The operation of VNPT SmartCA and RA is built inside a protected physical environment to prevent and detect illegal access, use or exposure of sensitive information and the system is public or concealed.

VNPT SmartCA also maintains disaster prevention measures for its CA activities. Disaster prevention measures are protected by multiple layers of physical-level security.

5.1.2. Control physical safety and security

The managing unit of digital signature and digital signature certification services under the remote digital signature model VNPT SmartCA requires all to have an employee card. In case visitors come to transaction offices, guests need to present their identity card, citizen identity card or passport. These documents will be saved at the office of the agency security guard and guests will be issued a visitor card to travel within the agency.

The right to enter and exit the place where the equipment is located for the provision of digital signature services and certification of digital signatures according to the remote digital signature model is controlled by the fingerprint checking system and security guards.

The security guard himself does not have access to the place where the device is located. This employee is responsible for preventing attempts to enter by strangers, without authority. Those who can enter the place where the device is located must be people whom the security guard knows in advance that has the authority and responsibility to enter the area, and must authenticate and authorize the fingerprint recognition system. On the other hand, where the device is located there is a continuous (24/7) monitoring camera.

System access is only given to those who are responsible for administering and monitoring the system. Therefore, incompetent people, if they can bypass the fingerprint protection and control system, are also not able to access the system.

5.1.3. Power conditions

VNPT SmartCA service delivery system is connected via UPS system, capable of providing electricity for about 30 minutes. At the same time, the building's power generation system has a generator system, which will be activated after a power outage of about 4 minutes. This ensures the power supply to the system is uninterrupted.

5.1.4. Water prevention

VNPT SmartCA needs to take precautions to minimize the problem of water entering its system.

5.1.5. Fire protection

VNPT SmartCA has a preventive plan to prevent and extinguish fire or other disasters that may cause fire or smoke. VNPT SmartCA's fire protection system needs to be designed to conform to fire protection standards.

5.1.6. Storage media

All products store information about software and data, auditing, documentation or backup information stored in VNPT SmartCA's media or storage media to ensure security with the deployment of physical means and access controls to restrict access to competent work, and protection of storage media from destruction (due to water, due to fire, due to electromagnetic fields ...).

5.1.7. Garbage disposal

Sensitive documents and resources need to be shredded before destruction. Means of collecting or transmitting sensitive information should be made inaccessible before the

disposal site. Other types of garbage are destroyed to meet VNPT's normal garbage disposal requirements.

5.1.8. Backup system

The main system of VNPT SmartCA service is located at IDC Nam Thang Long, Hanoi.

The backup system for VNPT SmartCA service is also built functionally identical to the official system and is located at IDC Tan Thuan: Lot Va.02c-03a, Street 24, Tan Thuan Export Processing Zone, Tan Thuan Dong Ward, District 7, Ho Chi Minh City.

5.2. Control process

5.2.1. Trust role

All employees must be considered before becoming trusted people working at trusted positions of VNPT SmartCA. Those selected are trusted people working in trusted positions that meet the requirements of VNPT SmartCA. Trusted persons include all employees, engineers, and consultants who access or control the authentication or encryption process that could have a significant impact on:

- The process of checking information in the digital certificate application.

- The process of providing digital signature services and certifying digital signatures according to the remote digital signing model.

- Issuing and revoking access to restricted parts of the system.

- Transfer of subscriber information or request.

- Trustees include, but are not limited to, the following components:

  - Tellers, customer service staff.
  - Employees run coding jobs.
  - Security personnel.
  - System Security Officer.
  - Design engineers.

5.2.2. Number of trusted people required for each job

VNPT SmartCA has established, maintained and has strict control procedure requirements to ensure task assignment based on ability to work and has shown that many people are trusted to perform sensitive tasks together.

5.2.3. Role identity authentication

For all those who wish to be trusted, the identity verification process is done through the human (or physical) presence of these persons prior to the implementation of security procedures and a routine vetting process (such as a passport or driver's license). The identification process will be deepened further through background checks.

VNPT SmartCA ensures that employees achieve a position of trust and that the approval department is assigned before these employees:

- Licensed access to necessary amenities.

- Be provided with electronic documents to be able to access and perform some functions on VNPT, RA or other IT systems.

5.2.4. Division of responsibilities between positions

Roles that require division of responsibilities include but are not limited to:

- Confirm the information in the application for registration of digital certificates.

- The process of accepting, refusing, or other processes of digital certificate applications, requests for revocation, renewal or registration information.

- The process of issuing and revoking digital certificates, including individuals who have access to restricted access parts of the archive.

- The process of transferring subscriber information or requests from customers.

- The process of creating, issuing or destroying a digital certificate.

5.3. Personnel control

5.3.1. Qualities, Experience and Trust Requirements

All those who want to become trusted and work at trusted positions of VNPT SmartCA system need to prove that they have appropriate resumes, good qualities and experience necessary to perform well the job requirements in the future, as well as being trusted (if any), necessary to perform digital certificate services under the management contract. The background check process is repeated at a frequency of 1 time / year with employees in trusted positions.

5.3.2. Background check procedure

Before certifying a trusted role for an employee, VNPT SmartCA performs a background check including the following elements:

- Local certificates of individuals and families.

- Confirmation of the previous working unit.

- Check and refer to colleagues.

- Confirm the highest level of training has been achieved.

- Check local and national criminal records.

- Check financial information.

- Confirmation of satisfaction of political and security conditions of political agencies and security protection of VNPT. When one of these mandatory elements cannot be achieved due to certain laws or circumstances, VNPT SmartCA will use alternative assessment techniques as permitted by law.

Factors uncovered during a background check that can be used to weed out a typical candidate are:

- The information provided by the candidate or trusted person is dishonest.

- High level of disapproval or trust of trustees.

- Criminal record.

- Inability or signs of financial non-transparency. The report includes the above information that is evaluated by the human resource management department and security personnel, thereby giving appropriate measures for each situation. These measures may include checking and removing the candidate from a trusted position or terminating the candidate's employment. The use of information collected during background checks must be consistent with state laws and policies.

5.3.3. Training Requirements

VNPT SmartCA trains employees after recruitment as well as during work to ensure employees can complete their jobs. VNPT SmartCA will keep the materials of these training sessions and regularly review and upgrade the training programs when necessary. VNPT SmartCA's training program is suitable for each individual job and usually involves:

- The basics of public key infrastructure.

- Job requirements.

- Security policies, procedures and activities of VNPT SmartCA.

- Use and operate deployed hardware and software devices.

- Reporting and transferring agreements and related issues.

- Procedures for disaster recovery and job retention. VNPT SmartCA's training program is designed to be compatible with the training program on digital signatures and digital signature certification provided by the National Electronic Certification Center (NEAC).

5.3.4. Requires regular retraining

During the working process, employees in VNPT SmartCA system will regularly be trained to improve their expertise. The training period is decided by the management unit based on the requirements so that each employee needs to maintain a level of trust and perform their jobs well.

5.3.5. Frequency of job rotation

No regulations

5.3.6. Disciplinary action for violations

Appropriate disciplinary measures are taken for illegal acts or violations of VNPT SmartCA's policies and regulations. Disciplinary action may include dismissal depending on the frequency and severity of the above-mentioned acts.

5.3.7. Independent Conclusion Requirements

In certain cases, implementation staff or independent consultants are employed in positions of trust. These employees have the same security functions and roles as VNPT SmartCA employees in their respective positions. The above subjects must be those who have completed or passed the background check procedures and are allowed to access the secured facilities of VNPT SmartCA service in their jurisdiction.

5.3.8. Provide documents to employees

VNPT SmartCA is responsible for providing employees with the necessary training programs and materials for them to complete their jobs well.

5.4. System Logging Procedures

5.4.1. VNPT SmartCA events to be logged

Verifiable events must be logged by VNPT SmartCA and RAs. Every record is electronic or manual, containing the time of the event, and the identification of the executing unit. VNPT SmartCA provides event log types in this CPS.

Types of events that can be audited include:

- Events that verify the identity of subscribers using electronic tools.

- Create CA keys.

- Toggle systems and applications on and off.

- Change CA key.

- Activation data processing for the CA's secret key.

- Physical access logs.

- Facts on the life cycle of digital certificates, including: issuance, reissuance, renewal, revocation, suspension.

- Events related to trusted persons, including: access or exit actions; create and delete passwords or change user privileges; personnel changes; - Reports on access to networks and systems that are not authorized.

- Errors in reading and writing digital certificates and archives;

- Change the policy on creating digital certificates, valid time;

- Errors arising related to digital certificates and digital signature services and digital signature certification under the remote digital signature model notified by subscribers or detected by VNPT.

5.4.2. Test log processing frequency

Audit logs are processed at least weekly for critical security and operational events. In addition, VNPT SmartCA will conduct abnormal checks based on the warnings and phenomena of the system.

5.4.3. Test Record Retention Time

Audit records must be archived in accordance with section 5.5.2.

5.4.4. Audit Log Protection

Audit logs will be protected by an electronic audit log system that includes mechanisms to protect log logs from unauthorized access, modification, deletion or interference.

5.4.5. Test log backup procedure

Every day, the audit logs will be backed up with changes and additions; and will be backed up in its entirety weekly.

5.4.6. Test system

Automated system checks are performed at the application, network and operating system levels. Specialized staff of VNPT SmartCA will perform manual inspection.

5.5. Archiving logs

5.5.1. Types of records to be kept

VNPT SmartCA will store the following information:

- The test data in section 5.4.
- Information on registration of digital certificates.
- Documents and documents enclosed with the request form for issuance of digital certificates.
- Information about the life cycle of digital certificates.
- And other information as prescribed by RootCA.

5.5.2. Retention period

The data will be kept for a period of at least 10 years from the date the digital certificate expires or is cancelled.

The data will be saved for a period of at least 10 years from the date of signing the service contract. After that time, VNPT continues to store the Subscriber's data but is not responsible for how long the storage period is committed.

In case of license suspension or revocation, store all information and databases on subscribers and digital certificates for at least 05 years from the date the license is temporarily suspended or revoked (according to Article 33, Decree 130/2018)

5.5.3. Protection of stored data

VNPT SmartCA commits that only licensed entities will be able to access and use stored data. The data storage medium is regularly maintained and managed, always ready for access.

5.5.4. The procedure for performing backups

VNPT SmartCA backup enhances the digital certificate information daily and the entire weekly backup. Copies of paper documents are stored in a secure location.

5.5.5. Time stamping requirements for records

Information records about digital certificates, CRLs, and revocation events should record the time of the event.

5.6. Change the lock

VNPT SmartCA's digital certificate can be renewed provided that the total expiry time of the key pair does not exceed the maximum expiry date prescribed by law. The new key pair of VNPT SmartCA can be generated when needed, such as replacing the old key pair that has been discontinued. Before VNPT SmartCA's digital certificate expires, VNPT SmartCA will carry out the renewal process to ensure the system operates smoothly. VNPT SmartCA will apply for renewal of digital certificates from NEAC no later than 90 days before the expiration time.

5.7. Troubleshooting, disaster and recovery

5.7.1. Procedures for handling key disclosure and incidents

Redundancy and backup should be conducted at other locations and equipment to prevent the possibility of lock disclosure and incidents. The data to be backed up includes: digital certificate registration data, inspection data, database of issued digital certificates. Backups of CA secrets are subject to section 6.2.4.

5.7.2. Computer Resources, Software and Data

When a problem occurs with computer resources, including hardware, software, data, information should be immediately sent to the specialized troubleshooting unit to carry out the planned handling process. In case of need, the disaster recovery function will be activated for use.

In case the subscriber is performing transactions, there is an incident related to equipment such as damage, fire, natural disaster, ... If the transaction cannot be executed, the transaction is called an error and the subscriber must re-execute the transaction when the system is operating normally.

In case a subscriber is performing transactions with software and data problems, the responsibility between VNPT and the Subscriber shall be enforced based on the terms specified in the contract between VNPT and the subscriber.

5.7.3. Procedures for troubleshooting secret key disclosure

When suspecting and detecting the secret key disclosure of VNPT SmartCA, the troubleshooting unit of VNPT SmartCA (Incident Response Team) will be in charge of handling with the planned procedures and procedures. Personnel of the troubleshooting unit including experts in cryptography, security, business, system operation and other functions will survey the current situation, propose solutions and implement an action plan

after being approved by the management unit of VNPT SmartCA. If VNPT SmartCA's digital certificate is revoked, the following procedures should be followed:

- The status of revocation of digital certificates of VNPT SmartCA will be published on the archive.

- All possible notification measures are used to provide information about the event of revocation of CA digital certificates to units of VNPTCA's system.

5.7.4. Ability to resume business operations after an incident

VNPT SmartCA builds a backup system at least 10 km from the official system location. VNPT SmartCA will plan, deploy and test the recovery plan after the incident to minimize the consequences caused by natural or human factors. This plan is regularly checked, reviewed and updated to suit the actual situation. When there is an incident caused by natural or human factors that causes temporary or prolonged system shutdown, the emergency response unit of VNPT SmartCA (VNPT SmartCA Emergency Response Team) is responsible for performing the recovery process after the incident. VNPT SmartCA is capable of recovering basic operations after 24 (twenty-four) hours after a failure with the following minimum:

- Issuance of digital certificates.

- Revocation of digital certificates.

- Disclosure of recall information. The database used for disaster recovery is synchronized with the operating system for the allowed period of time. Devices used for the recovery plan are protected as defined in section 5.1.1. VNPT SmartCA maintains hardware devices and backups at the disaster recovery equipment management area. The secret key of VNPT SmartCA is backed up and maintained for disaster recovery tasks as stipulated in section 6.2.4.

5.8. Decommissioning

VNPT SmartCA will notify when VNPT SmartCA or an RA terminates operations for partners and subscribers by reasonable means of communication can use. Upon termination of operation, VNPT SmartCA will carry out the termination process to minimize losses to subscribers and recipients. This procedure may include the following steps:

- Provide information about the decommissioning status of VNPT SmartCA to subscribers and recipients.

- bear the cost of these notifications.

- Carry out necessary procedures to revoke digital certificates of VNPT SmartCA.

- Continue to maintain the information storage system of VNPT SmartCA in accordance with the provisions of this CPS.

- Continue to maintain the service support system for subscribers.

- Continue to maintain the system of recall services, such as CRL, OCSP.

- Conduct the revocation of digital certificates that have not been revoked if deemed necessary.

- Refund the subscription fee if the contract has not ended.

- Destroy secret keys of VNPT SmartCA and token devices containing secret keys

- Transfer VNPT SmartCA service to another unit if any

6. ENSURING TECHNICAL SAFETY AND SECURITY

6.1. Key pair generation and distribution

6.1.1. Key pair generation

Key pair generation by a digital signature service provider and authentication of digital signatures under the remote digital signature model consists of generating the provider's own key pair (signed by the national Root CA) and generating key pairs consisting of public and secret keys for subscribers (according to clause 3, Decree 130/2018/ND-CP).

In order for the service provider system to ensure random and unique key pair generation, capable of ensuring that the secret key is not detected when there is a corresponding public key, the key generation process of VNPT SmartCA system complies with PKCS #1 version 2.1, meeting the standards in Circular No. 16/2019/TT-BTTTT issued by the Ministry of Information and Communications 05 December 2019.

The key pair generation plan of VNPT SmartCA in each case is as follows:

The subscriber's key pair will be generated by VNPT SmartCA and stored on the HSM device.

VNPT SmartCA issues digital certificates to subscribers with a minimum key length of RSA 2048 bits, so it ensures that the secret key is not detected when the corresponding public key is available.

6.1.2. Transfer of public keys to issuers

Subscribers who send public keys to VNPT SmartCA via electronic means are regulated by PKCS#10 CSR digital certificate requirements or must protect the signed data packet transmission according to SSL standards.

6.1.3. Transfer the CA's public key to the subscriber

VNPT SmartCA requires subscribers to download and install the public key of VNPT SmartCA. The public key of VNPT SmartCA is retrievable according to the clause in section 2.1.

6.1.4. Key Size

The key size needs to be long enough to ensure the safety of the secret key. The key pair length standard of VNPT SmartCA stipulates that it must be at least equivalent to the safety of RSA key pair 2048 bits for subscribers.

6.1.5. Generation of locking parameters and quality control

6.1.6. Key usage purposes (specified in X.509 v3 key usage record)

See section 7.1.2.

6.2. Control and protection of secret keys

6.2.1. Secure cryptographic device standards

VNPT SmartCA uses hardware cryptographic equipment to generate keys and store the original secret key of the CA. According to the minimum requirements, this device must meet EN 419221-5:2018 standards.

6.2.2. Multiple Secret Key Control

The secret key control mechanism of VNPT SmartCA is an international standard code-sharing mechanism, this mechanism separates the secret key activation data into different parts (n), parts held by different objects. To activate the key requires at least a larger number of 1 (m) key fragment (m =< n). At VNPT SmartCA, m >= 2 is applied.

6.2.3. Entrust the secret key

The secret key of VNPT SmartCA is not entrusted. The subscriber's secret key is entrusted under the clause of section 4.11.

6.2.4. Secret Key Backup

The secret key pair of VNPT SmartCA is backed up on a secure hardware device and placed at least 10 km away from the original storage location.

6.2.5. Secret Key Storage

When the digital certificate expires, the key pair of VNPT SmartCA will be safely stored for at least the next 5 years on hardware cryptographic equipment according to standards issued by the Ministry of Information and Communications. This key pair cannot be used for any confirmation signing activities after the expiry time, unless the digital certificate of VNPT SmartCA is renewed.

6.2.6. Transfer secret keys to/from secure cryptographic devices

The process of transferring secret keys to secure cryptographic devices is carried out according to the instructions of the equipment supplier, according to standards issued by the Ministry of Information and Communications.

6.2.7. Store secret keys on secure cryptographic devices

The process of storing secret keys to secure cryptographic devices is carried out according to the instructions of the equipment supplier, according to standards issued by the Ministry of Information and Communications.

6.2.8. Activation method using secret key

All participants of VNPT SmartCA need to protect the data used for activating the secret key from loss, theft, modification, disclosure or unauthorized use. VNPT SmartCA will agree with subscribers on the method of activating the use of secret keys for each specific type of digital certificate in the Service Contract.

6.2.9. Secret unlocking method

In case the key pair of VNPT SmartCA needs to be destroyed, VNPT SmartCA will perform the cancellation thoroughly, ensuring that the key pair after being canceled cannot be restored or used in any way. Secure cryptographic devices are physically destroyed according to the manufacturer's instructions, according to standards issued by the Ministry of Information and Communications before stopping storage.

6.2.10. Cryptographic Device Evaluation

Application of cryptographic device evaluation standards specified in Section 6.2.1.

6.3. Issues related to key pair management

6.3.1. Public Key Storage

Public keys and digital certificates are stored at VNPT SmartCA's repository, according to section 2.1.

6.3.2. Time of operation of digital certificate and key pair

The operation period of a digital certificate starts from the time of issuance stated in the attributes of the digital certificate and ends at the time of expiration mentioned in the digital certificate, except for cases where the digital certificate is revoked before the deadline. The operation time of the key pair is equal to the operation time of the corresponding digital certificate, except for cases where they are used to decrypt and check signatures. The operation time of the key pair in VNPT SmartCA digital certificate complies with the regulations of the Ministry of Information and Communications. The operation period of the key pair in the subscriber digital certificate must not exceed 5 years.

6.4. Data activation

6.4.1. Generate and deploy activation data

VNPT SmartCA chooses a password strong enough to protect the secret key. The requirement of the system login password must:

- Created by an individual.
- Have at least eight characters.
- At least one character is a letter and one character is a number.
- Have at least one lowercase character.
- Any character is not repeated 3 or more times.
- Not the same name as the operator's name.
- Do not contain part of the name in the operator's name.

6.4.2. Activation Data Protection

VNPT SmartCA recommends subscribers follow the above requirements. In addition to enhancing safety, VNPT SmartCA encourages the use of multi-authentication mechanisms (token and passphrase, biometric and token, biometric and passphrase) for the process of activating secret keys.

6.4.3. Other issues of activation data

6.4.3.1. Sending activation data

When sending secret key activation data to subscribers, VNPT SmartCA uses methods to ensure that the secret key is not lost, stolen, modified, disclosed or illegally used.

6.4.3.2. Destruction of activation data

When necessary, the secret key activation data will be destroyed by VNPT SmartCA by appropriate methods, ensuring that the data is not lost, stolen, modified, revealed or illegally used the secret key protected by such activation data.

6.5. Security control of the usage process

6.5.1. Technical requirements on computer system safety

VNPT SmartCA's network system is isolated from other systems, is offline and needs physical access to operate and use. The components of VNPT SmartCA's network system are divided by area, with devices to control, detect and prevent unauthorized access such as firewall, IDS, IPS. VNPT SmartCA requires passwords to be changed periodically and comply with password security standards, including minimum length, combination of letters, numbers and special characters. All direct physical access to VNPT SmartCA's network system is performed by trusted persons. Access operations are controlled limited to the task and function of each location.

6.5.2. Safety assessment

VNPT SmartCA complies with ISO 27001 computer system safety standards. The assessment and inspection work is conducted periodically and irregularly based on the actual situation. The system management unit is responsible for processing survey inspection reports and providing measures, plans and implementation to solve problems in the inspection reports.

VNPT SmartCA's digital signature module is certified to meet EN 419: 241-2:2019 and ISO 15408 standards.

VNPT SmartCA complies with eIDAS standards on "Standards of equipment systems for managing secret keys, digital certificates and creating digital signatures of customers" specified in the appendix "LIST OF COMPULSORY STANDARDS APPLICABLE TO DIGITAL SIGNATURES AND DIGITAL SIGNATURE CERTIFICATION SERVICES ACCORDING TO DIGITAL

SIGNATURE MODELS ON MOBILE DEVICES AND REMOTE DIGITAL SIGNATURES" in the circular 16/2019/TT-BTTTT.

6.6. Security control of the usage process

6.6.1. Control the system development process

VNPT is responsible for building and developing management software for VNPT SmartCA and RA.

VNPT SmartCA also provides both software for subscribers and recipients to perform interactive functions with VNPT SmartCA.

6.6.2. Conditions on the environment for using the service

VNPT has mechanisms and policies to control and monitor VNPT SmartCA system configuration.

With application software, VNPT SmartCA creates encryption values to ensure integrity when transferring to users.

VNPT SmartCA provides integrated APIs for 3rd party applications, regardless of application platforms.

VNPT SmartCA provides a mobile application for subscribers to control the operation of the secret key.

The subscriber's mobile device installs the VNPT SmartCA application, which will be identified by VNPT SmartCA and attached to the subscriber.

At one time, subscribers use VNPT SmartCA application on a single device.

Subscribers wishing to change devices will need to make a request to change the key pair in section 4.7.

6.6.3. User authentication authorization mechanism

The Service does not support an authentication authorization mechanism between one subscriber and another when performing transactions requiring user authentication.

6.6.4. Control the management of safety and security

VNPT SmartCA has mechanisms and policies to control and monitor VNPT SmartCA system configuration.

With application software, VNPT SmartCA creates encryption values to ensure integrity when transferring to users.

6.7. Network security monitoring

For information exchanges between VNPT SmartCA and RA conducted through the network environment, VNPT SmartCA has security measures corresponding to the standards specified in the security policy to prevent unauthorized access and other attack activities.

6.8. Time-Stamping

Not provided.

7. DIGITAL CERTIFICATE FORMAT, DIGITAL CERTIFICATE REVOCATION LIST (CRL), ONLINE DIGITAL CERTIFICATE STATUS CHECK PROTOCOL (OCSP)

7.1. Digital certificate format

The digital certificate is in X.509 format version 3 (1997) and RFC 3280 – Internet X.509 Public Key Infrastructure Certificate, according to Circular 06/2015/TT-BTTTT. At a minimum, the digital certificate component must be as follows:

VIETNAM NATIONAL ROOT CA	
Version	V3
Serial Number	009592BB8CEEAD5A24A6B8F71D7D323B5A
Signature Algorithm	SHA256withRSA
Signature Hash Algorithm	SHA256
Issuer DN	CN=Vietnam National Root CA OU=National Centre of Digital Signature Authentication O=Ministry of Information and Communications C=VN
Valid From	4/15/2014, 11:29:20 PM ICT
Valid To	4/15/2039, 11:29:20 PM ICT
Subject DN	CN=Vietnam National Root CA OU=National Centre of Digital Signature Authentication O=Ministry of Information and Communications C=VN
Public Key Size	4096 bits
Public Key Parameters	05 00
Public Key	30 82 02 0A 02 82 02 01 00 B8 AC 5A 7B 08 30 D9 70 7A 69 F5 1f E3 37

	95 4E 14 03 97 F1 BD C6 3E 7A 52 84 FE F0 A6 D6 EC 17 88 8E 45 1E BF 09 54 98 AE 7f 8f 81 D0 68 8B 83 B8 3D A2 24 1A 53 61 AD ED 63 3F 7D 34 7C A7 F3 E4 41 3e F2 CE E6 34 B8 BC D2 C5 43 B7 77 C2 F1 06 71 51 87 3F F9 56 79 3A 71 F5 9C B1 95 30 08 48 14 FC B1 EB 9D 5B 91 8C 86 2C 7D F7 5C DD 80 E0 50 99 1C 6e 79 F1 46 ae B3 4C 5f 41 1B 6C 47 dd FD C2 EB C0 B8 63 7C 84 45 A7 B9 30 2b a4 a4 d1 0b 5e 1e 86 72 d4 51 d8 59 12 84 57 88 4f 32 54 65 28 2e 08 42 49 02 3e 6a 61 6d eb 6a 42 6e 77 85 e3 14 55 60 32 79 7a fb bf 0f 63 1b e5 00 0f 28 15 0a d4 6c 0c b0 5a ae 8b ce 7e b3 72 9a 3e 39 9b 96 7c 5e cd 15 51 84 70 0b 43 b8 dd 68 ca fb 2d f8 7e bc 7f a8 22 67 8f 9d 28 8e 1d 05 ca c5 91 82 7e a6 d7 fd f3 e0 de bf f2 23 ea 89 e3 38 b8 15 80 4f fa 2f 0a 6b 0c 85 58 ed 7d 2f 76 a1 86 ec d6 e1 ea 06 9e ba 00 86 e7 f9 98 b4 85 64 1e 1c 0f 2b e2 9c 4c f1 13 61 92 43 63 14 f7 ad 42 1a 85 a6 21 d5 0a 7e 2d f1 03 5d 32 48 d9 71 8a 7b 2f 65 06 49 85 81 d1 a9 65 8e b9 a7 7c 6f ad 85 be 34 77 1c 6e d3 ec 47 eb 30 72 eb 86 45 5e d4 3f f9 dd 99 15 f4 f0 68 9a 31 37 ca ae 44 7b 57 94 6f 7d ea c3 89 0f ef 7b 37 ea da 10 cf 1e 2c c5 6a ac 6d 22 64 d4 bb cc 05 bd 71 9b a3 5d 61 b2 ba 8b 09 a2 90 c5 94 e8 a2 76 29 ec 40 95 60 50 ee 7a e2 fb 13 a5 29 e1 c5 e5 7a bd 6a 2e fa 77 c3 e4 19 55 1e 2b e7 c2 0a bf 15 6b b4 76 91 89 95 2c 6c 36 b7 df 97 40 95 68 e0 68 92 3c 41 66 78 1c e1 d5 64 b4 23 ad 7f 89 92 30 cf 25 33 07 37 1b 8c 12 41 25 ac 24 85 de b5 ea 50 a6 7f 24 cb ea 29 e6 35 ea 34 03 68 7d 02 03 01 00 01
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Subject Key Identifier	7EF087EDB1B89DFB08836FA416FDF1B8AC629B01
Basic Constraints	Subject Type=CA Path Length Constraint=None
Thumbprint	8EA95975898EFEF73B5CA92BF03F712BFBC7615F

VNPT SMARTCA RS

Version	V3
Serial Number	00FC060D806FD75F4D8BF525C77697591F
Signature Algorithm	SHA256withRSA
Signature Hash Algorithm	SHA256
Issuer DN	CN=Vietnam National Root CA OU=National Centre of Digital Signature Authentication O=Ministry of Information and Communications C=VN
Valid From	11/18/2021, 10:55:57 AM ICT
Valid To	11/18/2026, 10:55:58 AM ICT
Subject DN	CN=VNPT SmartCA RS O=VIETNAM POSTS AND TELECOMMUNICATIONS GROUP

	C=VN
Public Key Size	2048 bits
Public Key Parameters	05 00
Public Key	30 82 01 0A 02 82 01 01 00 EC 7F 4D 64 58 9E F3 17 1E D6 50 24 EB 30 09 CC 60 FE 2C D8 AF 74 8C 4A 81 50 B7 D5 3C 4F 81 55 28 C4 EE B8 94 75 B3 72 61 80 0e 62 AB F5 E7 9E 91 1E 20 DC 61 17 27 59 49 F2 96 6e 2e 42 C8 04 8C 73 2d 77 c6 0b 59 f7 78 df 85 21 13 11 01 b2 04 87 44 8c 0b 11 b2 1f 73 39 33 32 47 eb 87 58 76 75 1a f1 4d 42 a9 fe 5e ec a8 9a a6 7c 88 d7 fa f7 bd 8a 4e a3 d9 85 c9 25 ec 21 a2 2a 83 78 04 2d c1 cb 18 6a e6 bd 2e 05 4a 6e 8d 96 50 7f 51 23 76 d8 c5 a4 52 00 8b a0 0a 10 12 e9 4f d0 74 09 b4 c4 ce 57 ea 29 83 d3 95 a9 03 e1 40 8b 8f 95 96 7c 37 54 71 28 bf 3e cf 63 0f 91 6d 35 24 f1 09 8b 36 58 d2 62 60 8b 24 9c 70 b8 00 97 51 d1 b9 73 54 a8 95 b3 1f 48 41 1a df 2e 53 62 01 70 3c e5 8c 3a 76 a0 fc a3 8e 47 fd fa 80 ff 8f 0f 72 01 51 de 3f f5 tank b6 f8 5b 32 5f 98 c1 02 03 01 00 01
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Subject Key Identifier	5FEFC4EB3AF622F772D2DA193C292559BBA0FD2F
Basic Constraints	Subject Type=CA Path Length Constraint=0
Thumbprint	7ABC082FEAADD9F35A5D17FFEAFC477D909D554B

VNPT-CA SHA-256

Version	V3
Serial Number	4FEEF2A430ABB3820ADFB69198BF12D6
Signature Algorithm	SHA256withRSA
Signature Hash Algorithm	SHA256
Issuer DN	CN=Vietnam National Root CA OU=National Centre of Digital Signature Authentication O=Ministry of Information and Communications C=VN
Valid From	7/28/2020, 6:09:47 PM ICT
Valid To	7/28/2025, 6:09:47 PM ICT
Subject DN	CN=VNPT-CA SHA-256 O=VIETNAM POSTS AND TELECOMMUNICATIONS GROUP C=VN
Public Key Size	2048 bits
Public Key Parameters	05 00

Public Key	30 82 01 0a 02 82 01 01 00 c6 97 80 f9 68 c9 4a 70 13 e3 ac 5e 75 cb 10 c0 64 18 d0 ab 33 32 75 a1 e1 45 e5 a7 2d 45 10 23 5c 96 c6 f8 24 bd 6f 83 f2 9b 71 f6 b2 ae f8 41 f1 ef 19 c9 b4 2b 56 85 c3 3f 88 b3 32 0c 30 9e c3 c5 8f 38 3c 0e 55 69 74 d4 6b 0b e3 63 cb 05 35 b4 11 ea d3 7a 8c 41 82 60 bc df b5 3b d2 10 a1 9b d7 f4 15 6b b9 81 d7 21 09 e9 11 fa 6e b7 0a e3 60 15 36 09 2e 33 3b 2b b3 c1 87 5e c5 52 06 4a 17 a2 6f 60 21 1a 64 c8 tank f4 92 F8 9F B9 C8 8C B8 5F FB 9C 25 42 AC 12 06 A8 32 89 13 ED EA ED 9D CC EE 85 52 97 D5 7B 98 00 0F 78 8E 26 09 09 09 8F 9E 64 CB 11 5D 2B 33 D1 C5 02 73 69 29 37 29 31 17 CD 20 34 07 2C 1D CA 5e 14 D7 50 8D 6E 2a 97 B5 A5 63 eb 5c 91 29 34 77 5e 2a 3c 22 d8 f2 4f 53 9d ea 83 ec e1 41 37 26 66 d5 86 59 1e 5c fc 66 d4 0d ab 01 a0 c5 d3 e0 d4 23 02 03 01 00 01
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Subject Key Identifier	B64D6B6BD6A69D34ED3239EC4254ACBE3263D871
Basic Constraints	Subject Type=CA Path Length Constraint=0
Thumbprint	6E8DB7A7A020659749F0F082AF7945F600D5AD56

MIC NATIONAL ROOT CA

Version	V3
Serial Number	1BE4738A1F3EC08F479FA6CF35C59822
Signature Algorithm	SHA1withRSA
Signature Hash Algorithm	SHA1
Issuer DN	CN=MIC National Root CA OU=National CA Center O=Ministry of Information and Communications C=VN
Valid From	5/16/2008, 8:12:49 AM ICT
Valid To	5/16/2040, 8:20:32 AM ICT
Subject DN	CN=MIC National Root CA OU=National CA Center O=Ministry of Information and Communications C=VN
Public Key Size	2048 bits
Public Key Parameters	05 00
Public Key	30 82 01 0a 02 82 01 01 00 a1 3f 59 51 0e fe 30 ff 61 db 96 78 14 8b db 43 3c 36 be 61 af dc b5 3f 60 1e d3 0d 01 41 ad f8 c9 8a 42 8e c8 ed 32 86 47 c5 fe b5 f7 ea d6 44 37 10 12 c3 48 08 51 50 ba e5 57 e9 c9 8e 1c 73 09 85 33 4c e1 bb 38 ac 8e ad b7 13 04 2e 66 81 57 2d cc fb 1a fd 2e

	9c 8b fd 09 40 f0 60 17 9b 71 45 6d 7d e3 db 2a d2 bb 9a dd eb cc 5e e4 00 df d5 6c 30 85 9b bd 57 7f 2d d4 24 d3 80 fb e0 28 51 tank b0 d6 61 07 cc e5 a0 47 e7 91 6d 2f 87 58 e8 b4 ad c1 b1 46 b3 dc 5a 1d 38 09 d9 fb b5 27 98 9e 5e fc f1 f4 48 ff e8 a1 3b ff 50 33 d9 26 ab b2 99 62 9d cc 7b c8 52 4d 9e 5c 42 8b 6f 74 7e fc 94 13 de 0a d2 f0 b5 6a f8 96 4c 50 9c e6 21 8e c1 e5 97 01 4e cd 9f b0 40 19 7c 1b 59 6f 5c 38 19 9a 37 da d1 81 39 16 32 ef 81 ad b0 21 6b 11 97 c2 c1 08 bd 6f 23 5c 04 0f d3 02 03 01 00 01
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Subject Key Identifier	CD6271E461BDFE3DECB24060D38175DD3AAC6BC6
Basic Constraints	Subject Type=CA Path Length Constraint=None
CA Version	V0.0
Thumbprint	42843BC401476CDA242034B945BBF409A6BDD5C7

VNPT-CA SHA-256

Version	V3
Serial Number	71DEEFBD000000000016
Signature Algorithm	SHA1withRSA
Signature Hash Algorithm	SHA1
Issuer DN	CN=Vietnam National Root CA OU=National Centre of Digital Signature Authentication O=Ministry of Information and Communications C=VN
Valid From	6/26/2019, 2:52:00 PM ICT
Valid To	6/26/2024, 3:02:00 PM ICT
Subject DN	CN=VNPT Certification Authority OU=VNPT-CA Trust Network O=VNPT Group C=VN
Public Key Size	4096 bits
Public Key Parameters	05 00
Public Key	30 82 02 0a 02 82 02 01 00 CF 5b 28 46 68 43 c8 58 84 18 7b ff 30 2a 9e be 9c 1f 0b 7b d7 a4 03 c3 53 d3 e3 0b e8 54 b7 b1 99 4f e1 38 8c 73 39 6f 3d a1 1b cc bd 74 c1 c4 b4 cb 5a eb b6 a5 56 f9 db aa 68 9a 2c d5 56 47 47 52 57 00 A1 Multi E6 99 03 B7 F9 3D 6C 54 F1 9A B0 DD F3 6A 4E 97 8B 7E 6C 45 86 29 39 BF EE 95 94 CC DF 5A 29 F8 F0 A0 8C 89 23 6C EE B5 36 63 B3 AA F0 CE 13 E7 44 EC C5 50 C2 8C 80 B5 49 B1 04 7d 11 38 0F 5C 74 2f 72 29 84 67 fa 84 24 a4 c8 58 93 73 e7 69 35 d8 0f 0e 45 1b 0b 75 45 33 a3 8c 0c 4a f3 95 38 2c e3 77 da 8c 5e 55 c2 29 19 55 b1 01 36 e3 e4 81 1b e7 49 c8 79 0e 55 f7 00 ca 9d 1c bc b3 11

	26 6a 8b a1 a5 44 af 53 88 85 6e 78 fa 0e 00 c1 4e 4f 74 2b 3f 65 b1 12 2c 2c d9 47 0a d1 88 51 54 72 c0 0a 19 49 80 5a 1d 4a a9 7d e3 39 43 71 2d 82 e1 a6 22 66 ad dc e0 06 4e 85 00 5a f0 6d 34 0a cf e4 8d 38 a2 8d 6c 13 23 ec 19 e3 73 c1 74 7b b7 35 2a 91 ed b1 39 d6 4f ea 23 49 6b 03 c4 7a 12 9c a7 81 67 af 7b 60 4f 4c 5a e6 14 2f 95 72 05 e5 65 35 32 bf 3a d0 b3 f7 7d f6 46 29 7c 95 48 e4 d8 03 tank 0b 29 07 b3 4e c0 f5 20 d8 85 a2 a1 92 d4 7b d7 bd 02 80 d5 e4 cd a9 18 14 ec 06 9a c8 24 58 d8 ba ca 86 a7 c7 d0 f6 7d 9e e9 31 3c 1f 54 cf a0 d4 35 08 3b 9f e1 5d 2c 64 50 5d ab 9a 0e 7e 6a e8 90 14 f6 33 9d d6 f1 3d 36 53 01 tank 9b 11 86 6d ab 1b 36 d9 f4 b4 4d ed 88 63 72 80 1e 2d ce 77 91 7a de 7a f2 22 e8 5a dd b7 49 ad ef 34 86 bb da c3 c6 1f 13 ff 1c 67 75 c7 50 8e ff 64 15 51 67 8a 4f 28 c5 1b b0 0a e9 8e 1e c8 44 7b 89 d9 04 eb 1d 29 b3 f8 ae 93 b1 e0 da cd 4a 09 a6 71 ed 6f 51 26 89 ca 9e 37 bd 78 f5 c7 cc 9b fb 02 03 01 00 01
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Subject Key Identifier	0669C0D5D5028A158D467DE97CE2680A55AC6AAF
Basic Constraints	Subject Type=CA Path Length Constraint=0
Thumbprint	B1ADEC6EF075F1F98E9F51774E90B9808EDC5A60

VNPT-CA SHA-256

Version	V3
Serial Number	71DEEFBD000000000016
Signature Algorithm	SHA1withRSA
Signature Hash Algorithm	SHA1
Issuer DN	CN=Vietnam National Root CA OU=National Centre of Digital Signature Authentication O=Ministry of Information and Communications C=VN
Valid From	6/26/2019, 2:52:00 PM ICT
Valid To	6/26/2024, 3:02:00 PM ICT
Subject DN	CN=VNPT Certification Authority OU=VNPT-CA Trust Network O=VNPT Group C=VN
Public Key Size	4096 bits
Public Key Parameters	05 00
Public Key	30 82 02 0a 02 82 02 01 00 CF 5b 28 46 68 43 c8 58 84 18 7b ff 30 2a 9e be 9c 1f 0b 7b d7 a4 03 c3 53 d3 e3 0b e8 54 b7 b1 99 4f e1 38 8c

	73 39 6f 3d a1 1b cc bd 74 c1 c4 b4 cb 5a eb b6 a5 56 f9 db aa 68 9a 2c d5 56 47 47 52 57 00 A1 Multi E6 99 03 B7 F9 3D 6C 54 F1 9A B0 DD F3 6A 4E 97 8B 7E 6C 45 86 29 39 BF EE 95 94 CC DF 5A 29 F8 F0 A0 8C 89 23 6C EE B5 36 63 B3 AA F0 CE 13 E7 44 EC C5 50 C2 8C 80 B5 49 B1 04 7d 11 38 0F 5C 74 2f 72 29 84 67 fa 84 24 a4 c8 58 93 73 e7 69 35 d8 0f 0e 45 1b 0b 75 45 33 a3 8c 0c 4a f3 95 38 2c e3 77 da 8c 5e 55 c2 29 19 55 b1 01 36 e3 e4 81 1b e7 49 c8 79 0e 55 f7 00 ca 9d 1c bc b3 11 26 6a 8b a1 a5 44 af 53 88 85 6e 78 fa 0e 00 c1 4e 4f 74 2b 3f 65 b1 12 2c 2c d9 47 0a d1 88 51 54 72 c0 0a 19 49 80 5a 1d 4a a9 7d e3 39 43 71 2d 82 e1 a6 22 66 ad dc e0 06 4e 85 00 5a f0 6d 34 0a cf e4 8d 38 a2 8d 6c 13 23 ec 19 e3 73 c1 74 7b b7 35 2a 91 ed b1 39 d6 4f ea 23 49 6b 03 c4 7a 12 9c a7 81 67 af 7b 60 4f 4c 5a e6 14 2f 95 72 05 e5 65 35 32 bf 3a d0 b3 f7 7d f6 46 29 7c 95 48 e4 d8 03 tank 0b 29 07 b3 4e c0 f5 20 d8 85 a2 a1 92 d4 7b d7 bd 02 80 d5 e4 cd a9 18 14 ec 06 9a c8 24 58 d8 ba ca 86 a7 c7 d0 f6 7d 9e e9 31 3c 1f 54 cf a0 d4 35 08 3b 9f e1 5d 2c 64 50 5d ab 9a 0e 7e 6a e8 90 14 f6 33 9d d6 f1 3d 36 53 01 tank 9b 11 86 6d ab 1b 36 d9 f4 b4 4d ed 88 63 72 80 1e 2d ce 77 91 7a de 7a f2 22 e8 5a dd b7 49 ad ef 34 86 bb da c3 c6 1f 13 ff 1c 67 75 c7 50 8e ff 64 15 51 67 8a 4f 28 c5 1b b0 0a e9 8e 1e c8 44 7b 89 d9 04 eb 1d 29 b3 f8 ae 93 b1 e0 da cd 4a 09 a6 71 ed 6f 51 26 89 ca 9e 37 bd 78 f5 c7 cc 9b fb 02 03 01 00 01
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Subject Key Identifier	0669C0D5D5028A158D467DE97CE2680A55AC6AAF
Basic Constraints	Subject Type=CA Path Length Constraint=0
Thumbprint	B1ADEC6EF075F1F98E9F51774E90B9808EDC5A60

7.1.1. Version number

The digital certificate of VNPT SmartCA can be X.509 version 3.

The subscriber's digital certificate must be X.509 version 3.

7.1.2. Extension components

Key usage in X.509 version 3 digital certificate must comply with RFC 3280.

The Certificate Policies Extension cannot be used in the subscriber's digital certificate.

The Subject Alternative Names in certificate number X.509 version 3 when used are subject to the provisions of RFC 3280.

Basic Constraints: No regulations

How to use Extended Key Usage: VNPT SmartCA's digital certificate does not use this field.

For the subscriber's digital certificate, the values of this field are used as agreed upon in the Service Contract.

Point of publication of the list of revoked digital certificates: The cRLDistributionPoints field of the X.509 version 3 digital certificate contains the URL address for the user to access the CRL to check the status of the digital certificate.

7.1.3. Algorithm number

VNPT SmartCA's digital certificate uses the following algorithms:

- sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member- body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

7.1.4. Name Format

The name format of the digital certificate is as specified in section 3.1.1

7.1.5. Name constraints

There are no regulations.

7.1.6. Number of the attestation statute

The number (OID) of this CPS will be registered when VNPT SmartCA's system officially comes into operation.

7.1.7. Use of extended statute constraints

There are no regulations.

7.1.8. Syntax and regulation semantics

There are no regulations.

7.1.9. Semantic handling of expanded digital certificate regulations

There are no regulations.

7.2. Digital certificate revocation list (CRL) format

CRL needs to contain the following values

Field	*Value or requirement*
Version	See section 7.2.1
Signature Algorithm	The algorithm used to sign the list of revoked digital certificates. VNPT SmartCA uses the following algorithm according to RFC 3279 standard. Sha2WithRSAEncryption (OID: 1.2.840.113549.1.1.11)
Issuer	The executing entity signs and issues the list of revoked digital certificates.
Effective Date	The effective date of the list of revoked digital certificates. The CRL takes effect immediately upon release.
Next Update	The date of updating the next version of the list of revoked digital certificates.

Revoked Certificates	List of revoked digital certificates, including the serial number of the revoked digital certificate and the date of revocation.

7.2.1. Version number of CRL

VNPT SmartCA supports CRL format according to version 1 or version 2 of RFC 3280.

7.2.2. CRL and extensions

There are no regulations.

7.3. Online Digital Certificate Status Check (OCSP) Protocol Format

OCSP (Online Certificate Status Protocol) is a protocol that allows checking the status of digital certificates online.

7.3.1. OCSP Version Number

VNPT SmartCA supports OCSP protocol version 1 which is compliant with RFC 2560 standard.

7.3.2. OCSP Extensions

There are no regulations.

8. COMPLIANCE AND OTHER AUDITS

8.1. Frequency and technical test situations

The inspection is carried out at least annually by the inspection unit that meets the requirements of the law and the requirements of VNPT SmartCA.

8.2. Units and persons performing technical inspection

The inspection unit performing VNPT SmartCA inspection must be an independent unit with the following capabilities:

- Proficiency in public key infrastructure technology, information security tools and techniques.

- Certified by RootCA.

8.3. Contents of technical inspection

The scope of assessment includes VNPT SmartCA's operating environment, key management activities, VNPT SmartCA management and control processes, life time management of digital certificates and actual business operations.

8.4. Handling when errors are detected

Based on the results of assessment and inspection, problems and deficiencies must be pointed out and handled by the management department of VNPT SmartCA. If these issues seriously affect the safety and integrity of VNPT SmartCA, VNPT SmartCA management must develop an action plan and implement it immediately within a reasonable commercial time. For less serious incidents, VNPT SmartCA management will assess the level and determine the actions to be taken.

For serious incidents, VNPT SmartCA management department will fully report the cause, remedy and extent of impact to the National Electronic Certification Center (NEAC) within 48 hours.

8.5. Publication of technical test results

VNPT SmartCA system inspection results are published on VNPT SmartCA's website.

8.6. Frequency and cases of assessment

Audit and inspection shall be carried out at least annually or according to the certification period of system components by the inspection unit meeting the requirements prescribed by law and requirements of VNPT SmartCA.

8.7. Identity and capabilities of the unit and tester

VNPT SmartCA testing unit must be an independent unit with the following capabilities:

- Proficiency in public key infrastructure technology, information security tools and techniques.

- Certified by RootCA.

9. OTHER PROFESSIONAL AND LEGAL CONTENTS

9.1. Fees/Pricing

9.1.1. Fees for issuance or renewal of digital certificates

Subscribers using VNPT SmartCA service must pay a fee when applying for certificates, managing and creating new certificates for suppliers.

9.1.2. Fees for using digital certificates

Subscribers using VNPT SmartCA and RA services do not have to pay to create a certificate warehouse or online service to provide certificate information to trusted partners.

9.1.3. Fees for revocation or checking the status of digital certificates

According to state regulations.

9.1.4. Usage fees for other services

VNPT SmartCA does not charge this CPS access fee. The viewing of documents for purposes such as copying, reallocation will be subject to the written approval of VNPT SmartCA.

9.1.5. Regulations on fee refund

VNPT SmartCA will provide the scope for the application of the fee refund policy. This policy will be incorporated into the written agreement with the subscriber to use the service or contract.

9.2. Financial responsibility

9.2.1. Coverage

VNPT SmartCA will maintain at a significant commercial level insurance information for errors or omissions, either through fault or omission insurance programs with insurance carriers or self-undertaking. These insurance requirements do not apply to political organizations.

VNPT SmartCA conducts insurance compensation for the following cases:

- Errors caused by VNPT SmartCA , including technical errors when issuing certificates under the responsibility of CA.

- VNPT SmartCA offers insurance compensation levels and is responsible for complying with those different levels of deed insurance.

- The insurance compensation shall comply with the contract with the subscriber.

VNPT SmartCA will not be responsible in the following cases:

- Cases of using deeds not mentioned in CP, CPS

- Cases of forgery dealing with deeds.

- Use cases, improper equipment configuration, not within the responsibility of the CA used in the process of processing the certificate.

- Private key lost, destroyed by client.

- The customer loses or exposes the PIN code that protects the secret key.

- Fault of HSM equipment, when a fault occurs, the HSM equipment supplier will be responsible for compensating the customer. The compensation is made in accordance with the contract with the subscriber.

- RA errors, including authentication errors, data recognition, certificate numbers, public key values, RA not sending correct requests, etc. When this error occurs, RA will take full responsibility to the customer. The compensation is made in accordance with the contract with the subscriber.

9.2.2. Other assets

VNPT SmartCA has the financial autonomy to maintain operations and perform its tasks, and has legal liability for risks to subscribers and recipients.

9.3. Security of business information

9.3.1. Scope of information security

The following subscriber data, which will be kept confidential and private ("confidential/private information")

- VNPT SmartCA application data, approved or not approved.

Private keys are held by enterprise subscribers using a public key management system and the information needed to recover these keys.

- The conversion data (complete and audit data of the conversion process).
- Audit data created or kept by VNPT SmartCA or a subscriber.
- Audit reports generated by VNPT SmartCA or subscribers, or external auditors.
- Accidental recovery or disaster recovery projects.
- Manage the level of security in the operation of hardware, software, administrators of certificate services and of other services.

9.3.2. Information not within the scope of the confidentiality process

Digital certificates, revocation of digital certificates and information about the status of digital certificates, where VNPT SmartCA is stored and the information contained within them are not considered confidential/private information. The confidential/private information in section 9.3.1 shall not be considered private or confidential if otherwise required by law.

9.3.3. Responsibility to protect confidential information

VNPT SmartCA ensures that private information is not disclosed to 3rd parties.

9.4. Security of personal information

9.4.1. Privacy Policy

VNPT SmartCA will implement a policy to ensure its own and comply with privacy laws. VNPT SmartCA will not disclose the name or any information about the subscriber's certificate application to the outside.

9.4.2. Information considered private

All information about subscribers is not published, including issuance deeds, deed directories and online CRLs are considered private information.

9.4.3. Information that is not considered private

Under local law, all information made public in a deed is not considered private.

9.4.4. Responsibility to protect private information

Participants in VNPT SmartCA service, receiving confidential information will have to ensure that this information is not exposed to third parties and must comply with local laws in their jurisdiction.

9.4.5. Notice and Consent to Use of Private Information

In accordance with the law or as agreed between the parties, private information will not be used without the permission of the person who owns it.

9.4.6. Provision of private information as required by law or for administrative purposes

VNPT SmartCA will be allowed to disclose confidential/private information if:

- The publication process is necessary to meet the requirements of competent state agencies, the administration process or processes related to laws and management activities.

- The publication process is intended to comply with the provisions of law.

9.4.7. Other information disclosures

9.5. Intellectual Property Rights

The clear determination of intellectual property rights between participating subdomains of VNPT SmartCA, not between subscribers and partner parties, is controlled by reasonable agreements between related subdomain parties. The following sections will address intellectual property rights related to subscribers and partners.

Ownership in digital certificates and information on revocation of digital certificates

VNPT SmartCA has all intellectual property rights related to digital certificates and digital certificate revocation information issued by VNPT SmartCA.

VNPT SmartCA and subscribers allow recipients to use information on the revocation status of digital certificates to perform their functions in accordance with CRL use agreements, agreements with recipients or other appropriate agreements.

Ownership in CPS

Parties related to VNPT SmartCA services accept that VNPT SmartCA stores ownership rights corresponding to this CPS.

Name ownership

A deed user holds all trademark rights such as service name, trade in their deed application and is entitled to distinguish the name from the deed that has been issued.

Key ownership and key documents

The key pair corresponding to the digital certificate of the CA and the terminal subscriber is owned by the CA and the terminal subscriber.

9.6. Declarations and commitments

9.6.1. CA's Commitments and Guarantees

VNPT SmartCA guarantees that:

- There is no misinformation with the facts in the deed.

- VNPT's certificates meet the standards required in this CPS.

- Services of revocation and use of certificates, storage of certificates in accordance with the standards in this CPS.

- The subscription agreement may contain additional statements and commitments.

- VNPT ensures that the cryptographic devices used in the process of providing services have been certified.

9.6.2. RA Representations and Warranties

The RAs of VNPT SmartCA guarantee:

- There is no misinformation with reality in the deed.

- RA certificates meet the criteria required in this CPS.

- Service of recovery and use of deeds of storage in accordance with standards in CPS.

The subscription agreement may contain additional statements and commitments.

9.6.3. Commitment to the Subscriber's guarantee

The User Subscriber undertakes that:

- Each electronic signature using the secret key corresponding to the public key listed in the digital certificate is the electronic signature of the subscriber and the

certificate is accepted and active (when it has not expired or been revoked) during the time this e-signature is created

- Their secret private key is protected and unauthorized persons cannot access this key.

- All information provided by subscribers and contained within the deed is true

- The certificate is used for lawful purposes and complies with the requirements of the CPS.

- The subscriber is an end user and not a CA, and does not use the private key corresponding to any of the public keys listed in the certificate for digital signature purposes for any certificate (or other certified form of public key) or CRL, as a CA.

- The PIN set by the subscriber is a number with a length of 6 characters as digits. The PIN cannot be changed.

- Subscribers are responsible for protecting and not sharing PINs.

- The PIN of the subscriber cannot be changed. If in the event of a risk that someone else learns the PIN of the subscriber, the subscriber must notify the service provider requesting reactivation and create another PIN.

The subscription agreement may contain additional statements and commitments.

9.6.4. Representation of the Recipient and Guarantee Matters

The agreement with the recipient requires the recipient to have enough information to make a decision based on the information in the digital certificate. They are responsible for deciding whether or not to trust the information in the digital certificate. The recipient shall be held liable if it violates the terms of the recipient's obligations set forth in this CPS.

The agreement between VNPT SmartCA and the recipient may include additional statements and commitments.

9.6.5. Representation of other stakeholders and guarantee matters

There are no regulations.

9.7. Disclaimer

Within the limits permitted by law, the subscriber contract and the recipient may be refused guarantee by VNPT SmartCA.

9.8. Limitation of liability

Within the limits of law, subscription contracts and trust partner contracts may limit VNPT's liability capabilities. The limitation of liability includes the elimination of incidental or indirect, punitive damages.

9.9. Compensation for damages

Problems of compensation of subscribers used

When required by law, users must compensate VNPT SmartCA if it appears:

- False information or distortion of facts provided by subscribers on digital certificates
- The error of the subscriber reveals factors and factors related to the deed service, omission or falsification due to negligence or fraudulent purposes.
- The subscriber's error in securing the private key, using a trusted system, or failing to take the necessary precautions to avoid consequences.
- The subscriber's use of one name (including without limitation within a common name, domain name, email) infringes the intellectual property rights of a third party.

The contract with the corresponding subscriber may have a number of other obligations.

Compensation issues of trusted partners

When permitted by law, the trusted partner's agreement will require trusted partners to compensate VNPT SmartCA when:

- The fault of the trusted partner in performing the obligations of a counterparty.
- The trust of the trusted partner in the deed is not met in some cases.
- The trusted partner's error in checking the status of the deed to determine whether it has expired or been revoked.

The corresponding agreement of the counterparty may have some additional obligations.

9.10. Effect of the Attestation Statute

9.10.1. Term

This CPS comes into effect when VNPT SmartCA system officially comes into operation.

Additional amendments to this CPS take effect upon publication from the archive of VNPT SmartCA service.

9.10.2. Termination

This CPS, when added, will remain in effect until replaced by a new document.

9.10.3 Results of termination of validity and existences

When this CPS expires, the components of VNPT SmartCA service will not be limited by the valid terms of the issued digital certificate.

9.11. Notice to stakeholders

VNPT SmartCA will use appropriate measures to notify relevant parties about the contents of this CPS amendment and supplement.

9.12. Additions and amendments

9.12.1. Revision procedure

Modifications of this CPS will be made by VNPT SmartCA. The amendments can be in the form of a document containing all the amendments to the CPS or in an updated form. The revised or updated version is linked to the notice and update section in the repository of VNPT SmartCA service at https://www.vnpt-ca.vn/ address

9.12.2. Mechanism and notification time

Changes to the CPS are as described in section 2.4 hereof.

The latest changed CPS document will be provided by VNPT SmartCA at: http://www.vnpt-ca.vn/

In addition, if VNPT SmartCA believes that the CPS change is necessary to prevent infringement on the safety of VNPT SmartCA service, the change will immediately be implemented and take effect.

9.12.3. Altered OID cases

VNPT SmartCA does not have the authority to change OID information, the change of OID content according to the regulations and instructions of NEAC. If VNPT SmartCA deems it necessary to change the OID, VNPT SmartCA can propose to NEAC through written form.

9.13. Dispute Resolution Procedure

Disputes between VNPT, partners and subscribers

The settlement of disputes between VNPT SmartCA, the recipient and the subscriber must comply with the terms stated in the contract and on the basis of the provisions of law.

Disputes with subscribers or recipients

This case is carried out in accordance with the law.

9.14. Governing Legal System

This CPS is built in accordance with the laws of the Socialist Republic of Vietnam.

In the process of providing and using VNPT SmartCA services as well as resolving disputes arising from VNPT SmartCA service participants as well as related parties, the laws of the Socialist Republic of Vietnam will apply.

9.15. Compliance with applicable laws

CPS of VNPT SmartCA service complies with Vietnamese Regulations (Circular 16/2019/TT-BTTT, other relevant documents) and regulations in eIDAS standards.

9.16. General Terms

9.16.1. General Agreement Terms

There are no regulations.

9.16.2. Independence of Terms

In the event that an additional provision or amendment of the CPS is retained unenforceable by a trial or a competent hearing, the remainder of the CPS shall remain in effect.

9.16.3. Enforceability (power of proxy and right of disclaimer)

Any party that prevails in controversies arising out of the contract is entitled to a proxy or waiver due to a breach of one of the terms of the contract.

9.16.4. Mandatory enforcement policy

To the extent permitted by law, the subscriber's agreement and the related party agreement are required to comply with the VNPT SmartCA service protection terms.

9.17. Miscellaneous

There are no regulations.