Unofficial translation

Lao People's Democratic Republic

Peace Independence Democracy Unity Prosperity

Ministry of Post and Telecommunications **No 1101/MPT**

Date: 29 May 2020

Decision
On Electronic Signatures

- Pursuant to the Law on Electronic Signatures No 59/NA, dated 12 December 2018.
- Pursuant to the organization and operation of the Ministry of Post and Telecommunications No 22/PM, dated 16 January 2017D

Minister issued the Decision as follows:

Part 1
General Provisions

Article 1 Purpose

This decision defines the principles, rules and measures for Commitment, on the management of services, the use of electronic signatures to promote the conduct of business in an orderly manner: accurate, standardized, modern and prompt, aimed at protecting the rights and interests of the state, individuals, legal entities and organizations to ensure national security, peace and social order contribute to the socio-economic development of the nation..

Article 2 Service of electronic signatures

An electronic signature is a letter, symbol, numerical symbol, sound or anything else created in electronic form to identify and verify the identity of the signatory and the accuracy of such information.

The operation of electronic signature is the management of electronic signatures, the provision of services and the use of electronic signatures of individuals, legal entities and organizations.

Article 3 Definitions

The terms used in this decision have the meaningsas following:

1. **Subscriber** means individuals, legal entities and organizations that use E-signatures services.
2. **Public key** means discloses a non-confidential security code that can be disseminated to the public and used to encrypt the information before it is transmitted through the computer system;
3. **Private key** refers to a unique security code to be used to decrypt a key pair that is a public key;
4. **Key pair** means private and public keys used in security infrastructure technology;
5. **Electronic signature certificate**means an electronic document that certifies the relationship between the user and the public key holder as an electronic document that complies with ITU-T standards;
6. **Policies of Electronic signature certificate** means documents that describe the service policies of electronic certification providers, including the application of electronic certificates by electronic certification subscribers;
7. **Registration Authority** meansthe registration authority: RA as the person who coordinates with the registration service provider when applying for the service or notifying the electronic signature through the inspection and verification of the information provided by the service subscriber;
8. **Online Public Service System** means the technical system of providing Internet services of government organizations; (as described of the Decree on Information via the Internet, No. 412, dated 10/11/2016, the provision of Internet services by government agencies refers to the provision of services by government agencies that have the authority to authorize, certify, or compile any legally valuable information within the scope of their rights and obligations to individuals, legal entities, and organizations, both domestically and internationally).

Article 4 Scope of Application

This Law applies toindividuals, legal entities or public organizationsthat provide electronic signature certification services within the Lao PDR.

Part 2
Electronic signature certification provider

Article 5 Electronic Signature Certification Provider

There are two levels of electronic signature certification providers:

1.National Root Certificate Authority

2.Sub-Certificate Authority.

Article 6 Provider of National Electronic Signature Certificate

The National Root Certificate Authority is responsible for providing electronic signature certification services to sub-electronic Certificate Authority.

The National Internet Center is responsible for issuing national electronic signature certificate authority within Lao PDR.

Article 7 Sub-Certificate Authority

Sub-Certificate Authority including:

1.Public Certificate Authority;

2.Government Certificate Authority;

3.Foreigner Public Certificate Authority;

4.Private Certificate Authority.

Article 8 Types of electronic signature certification services

The services provided for the issuance of electronic signatures are as follows:

1.Digital Certificate;

2.Secure Sockets Layer;

3.Time Stamp;

4.Other services as determined of Ministry of Post and Telecommunications.

Part 3

Issuer of a common electronic signature certificate

Article 9 Issuer of common electronic signature certificate

The issuer of a general electronic signature is a legal entity authorized by the National Root Certificate Authority to provide electronic signature certification services to individuals, legal entities or organizations, both domestic and foreign.

Article 10 Application for a license for the issuance of general electronic signature certification services

Legal entities or organizations that intend to conduct business of the certification of general electronic signatures must apply for a license from the Ministry of Post andTelecommunications, and request for an electronic signature certification from the issuer ofthe National Root Certificate Authority**.**

Applicants for a business license to provide general electronic signature certification services must submit the documents required by the Ministry of Post and Telecommunicationsset out as follows:

1. Application;
2. Executive resume;
3. Technical resume and education certificate;
4. A copy of the enterprise registration certificate or establishment certificate;
5. Certificate of Headquarters;
6. Feasibility study and technical plan;
7. Terms of service;
8. Certificate of Bank Statement from a bank in Lao PDR;
9. Other relevant documents.

Article 11 The requirements for consideration of Issuance of License for general electronic signature certification services

Applicants for a license to issue general electronic signature certification services must meet the requirements as following:

1.To submit complete documents in accordance with the requirements as specified in Article 10 of this Decision;

2.Be legal entities in accordance with the Law on Enterprises of the Lao PDR;

3.Must have a minimum registered capital of ten billion kips;

4.Not in the period of foreclosure, in the process of bankruptcy or being convicted of bankruptcy under the laws of the Lao PDR;

5.Never had my license annulled or revoked from the Ministry of Post and Telecommunications before;

6.There must be a Lao technical technician responsible for managing the electronic signature certification system and managing the database, developing the hardware and software of the electronic signature certification system;

7.Comply with other requirements set by the Ministry of Post andTelecommunications.

Article 12 Licensing Considerations

The Ministry of Posts, Telecommunications will consider issuing a license for the issuance of a general electronic signature certificate within 45 days from the date of receipt of the application with complete and accurate documentation.

In case of not considering the issuance of the license, the Ministry of Post and Telecommunications shall notify the applicant in writing within 10 working days.

Article 13 Validity of service license Issuance of general electronic signature certificate

General electronic signature certification serviceis valid for a minimum of 3 years and a maximum of 5 years and is renewable.

Article 14 Renewal of general electronic signature certification service license

Applications for renewal of business licenses for the issuance of electronic signature certificates must be submitted 90 days before the due date and must be submitted as required by the Ministry of Post and Telecommunications as follows:

1.Application;

2.A copy of the old business license;

3.Copy of enterprise registration certificate;

4.Summary of business activities in the past year

5.Last year's tax certificate;

6.Feasibility Study and technical plan (if any changed);

7.Terms of service (if changed);

8.Other relevant documents

The Ministry of Post and Telecommunications shall consider renewing the license for the issuance of a general electronic signature certificate within 15 days from the date of receipt of the application with complete and accurate documentation.

Article 15 Change, suspension or termination of services

The service needs change, additional service, suspended or dissolved deep providers of all or part must be granted the Ministry of Post and Telecommunicationsby requesting the Ministry of Post and Telecommunications with the written reasons for the change request must be submitted at least 90 days and requests for suspension or cancellation must be made at least 180 days in advance, and measures must be taken to correct, transfer or compensate its users.

Article 16 Issuance of electronic signature certification to general electronic signature certification service providers

The issuer of a national electronic signature certificate shall make a key pairing ceremony for the general electronic signature certification service provider to the witnesses and appropriate standard service providers after receiving the application from the applicant and obtaining a license to operate a general electronic signature certification service business under the Ministry of Post and Telecommunications.

Part 4
General electronic signature certification service agent

Article 17 Agents for the issuance of general electronic signature certificates

An agent for the issuance of a general electronic signature certificate is an individual or legal entities who perform a registration service, verification of the accuracy, completeness of the application and information of the applicant of the electronic signature certificate before submitting to the general electronic signature certification service, consider issuing the electronic signature certificate.

Article 18 Notification of the registration of agents for the issuance of general electronic signature certification services

The issuer of a general electronic signature must notify the issuer of the national electronic signature on his/her representative within 90 days from the date of the representative agreement by submitting the documents as following:

1.Registration notice according to the form issued by the National Electronic Signature Certificate

2.Copy of business registration certificate of the agent;

3.The contract represents an electronic signature certification service;

4.Other relevant documents

Article 19 Qualifications agents for general electronic signature services

The legal entities intending to represent the general electronic signature certification service shall have the conditionsas following:

1.Be legal entities in accordance with the Law on Enterprises of the Lao PDR;

2.Have a license to do business in information communication technology (excluding Internet coffee license);

3.Comply with other requirements as defined by the Ministry of Post and Telecommunications.

Part 5
Issuer of electronic signature certificate

Article 20 Issuer of Public Electronic Signature Certificate

Public e-signature issuer is a government entity that has registered and applied for an e-signature certification service from a national e-signature issuer to provide services to employees-civil servants and government agencies.

The National Internet Center is responsible for creating, maintaining, and developing a public electronic signature certification system.

Article 21 Use of electronic signature certificates in the public service system

The public service system of any government organization that needs to use an electronic signature certificate into the system must use an electronic signature certificatefrom a general electronic signature issuer licensed to do business by the Ministry of Post and Telecommunications and an electronic signature certificate from a national electronic signature issuer in order to people or organizations can use electronic signatures in the system.

Article 22 Use of the electronic signature certificate of the civil servants

Employees of government organizations who are required to use an electronic signature certificate in order to perform their duties within their jurisdiction must obtain an electronic signature certificate from the issuer of a public electronic signature.

In case the electronic signature certificate issued by the public electronic signature certificate is not accepted or cannot be used; the government employees may use an electronic signature certificate issued by a general electronic signature issuer or a foreign electronic signature issuer or other electronic signature issuer but must be certified by a national electronic signature certificate.

The use of an electronic signature certificate from a public electronic signature certificate holder must include the documents asfollowing:

1. Submit the application according to the form of the electronic signature of the government;
2. A copy of the certificate of appointment of the certificate holder;
3. Other documents as specified by the issuer of the government electronic signature.

Article 23 Requirements for considering the issuance of electronic signature certificates to the government employees

Requirement of issuing electronic signature certificates to employees has the conditionsas following:

1.Must complete the documents as stipulated in Article 22 of this decision;

2.To be employee with certification from his/her organization;

3.Pay fees and charges;

4.Comply with other conditions as defined by the Ministry of Post and Telecommunications.

Article 24 Electronic certificate signature for government employees

The validity of the electronic signature certificate for government employees issued by the issuer of the public electronic signature certificate is 1 to 3 years.

Article 25 Suspension or cancellation of electronic signature certificates for government employees

The issuer of a public electronic signature certificate may suspend or revoke the electronic signature certificate issued to the government employees in the cases asfollowing:

1.Relevant organizations request the suspension or cancellation;

2.The issuer of the electronic signature violates the laws, regulations or does not comply with the terms of service;

3.Do not apply for renewal;

4.Do not pay fees or service charges.

Part VI

Issuer of foreign electronic signature certificate

Article 26 Issuer of foreign electronic signature certificate

Foreign electronic signature certification issue is electronic signature issuers who have offices overseas that are certified by the National Electronic Signature Certification

Authority to provide electronic signature certification services to individuals, legal entities and organizations in Lao PDR.

Foreign electronic signature certification service agent is any legal entity in Lao PDR that is responsible for the registration, verification, and completeness of the application and the information of the applicant for the electronic signature before submitting it to the electronic signature certifier. Consider issuing the electronic signature certificate or using some of the technical systems of the foreign electronic signature issuer to issue the electronic signature to the user themselves.

Doing business as an agent for the issuance of foreign electronic signature certificates requires a business license from the Ministry of Post and Telecommunications and a certification from the issuer of a national electronic signature certificate.

Article 27 Application for a license to agent a foreign electronic signature certification service

Legal entities or organizations that intend to conduct business as the agent of foreign electronic signature certification services must apply for a business license to the Ministry of Post and Telecommunications, and request a certificate from issuer of the national electronic signature certificate.

Applicants for licenses for foreign electronic signature certification services must submit the following documents as required by the Ministry of Post and Telecommunications:

1. Application;
2. Executive resume;
3. Technical resume and education certificate;
4. Copy of business license or establishment certificate;
5. Certificate of Headquarter;
6. Feasibility study;
7. Copy of agent agreement with foreign electronic signature certificate issuer;
8. Service rules;
9. Other relevant documents.

Article 28 Requirements for consideration of issuance of license for foreign electronic signature certification service agents

Consideration of issuing a license to a foreign electronic signature certification services provider has the conditionsas following:

1.Have a representative office or service representative in Lao PDR;

2.Have a document certifying the establishment and operation of the electronic signature certification service of the country where the office is located;

3.Must meet the conditions and standards regarding the international electronic signature certification service issued by the national electronic signature certificate;

4.Comply with the requirements of the Ministry of Post and Telecommunications.

Article 29 Validity of the license of the agent for the issuance of foreign electronic signature certificate

The validity of the license of the foreign electronic signature certification agent is a maximum not more than 3 years.

Article 30 Renewal of license of foreign electronic signature certification service agent

Application for renewal of business license and certificate of foreign electronic signature certification service provider must apply at least 60 days before the expiration date and must be as required by the Ministry of Post and Telecommunications.

Article 31 Consideration of issuing the license of the agent for the issuance of foreign electronic signature certificate

The Ministry of Post and Telecommunicationswill consider issuing a license to a foreign electronic signature certification service provider within 15 working days from the date of receipt of the application, including complete and accurate documents.

In case of non-consideration, the Ministry of Post and Telecommunications will notify the applicant in writing within 10 working days.

Article 32 Consideration of issuance of certificates

The issuer of national electronic signature certificateshall consider issuing the Certificate of foreign electronic signature certification service agent to the applicant within 15 days from the date of receipt of the application and complete the documentsas following:

1. Foreign electronicsignature certification service agent application form;
2. Licensing agent for the issuance of foreign electronic signature certificates.

Article 33 Validity of the certificate

The expiration date of the foreign electronic signature certification agent's license depends on the expiration date of the foreign electronic signature certification agent license.

Article 34 Renewal, change, suspension or cancellation

Renewal of the license and certification of the agent for the issuance of foreign electronic signature certification services must be accompanied by the complete documents as specified in Article 27 of this decision and must be notified at least 30 days prior to the expiration date.

Legal entities that intend to change the content of the license, suspend or terminate the business of an agent for the issuance of foreign electronic signature services must obtain a license from the Ministry of Post and Telecommunications and submit documents to clarify the reasons.

Part 7
Issuer of a specific electronic signature certificate

Article 35 The issuer of the specific electronic signature certificate

An electronic signature certificate issuer is a legal entity or organization that registers a national electronic signature certificate to provide electronic signature certification services to employees and organizations within their organization.

In the case of using the services of a general electronic signature certification provider in Lao PDR, there is no need to register with a national electronic signature certificate issuer.

The issuer of a national electronic signature certificate will issue a specific electronic signature certificate to the applicant after registration and fulfillment of the requirements.

Article 36 Application for registration

The applications for registration of a specific electronic signature certification service are as following:

1. Registration application form;
2. Executive resume;
3. Technical resume and education certificate;
4. Copy of enterprise registration certificate and establishment certificate;
5. Feasibility study and technical plan;

6. Terms of service;
7. Other relevant documents.

Article 37 Registration requirements

Legal entities and organizations that intend to register for a specific electronic signature certification license have the conditionsas following:

1. Be legitimate legal entities in accordance with the Law on Enterprises of the Lao PDR;
2. Never had license annulled or revoked from the Ministry of Post and Telecommunications before;
3. There is a technician responsible for managing the electronic signature certification system and database management, as well as updating, developing the hardware and software of the electronic signature certification system; The technician requires a bachelor's degree or higher in Computer Security or ICT;
4. Comply with other conditions set by the National Electronic Signature Certificate.

Article 38 Consideration of issuance of certificates

The issuer of the National Electronic Signature Certificate shall consider issuing a specific electronic signature certificate to the applicant within 30 days from the date of receipt of the application and complete the documentsas following:

1. Request for Certificate Issuance of a specific electronic signature certificate holder;
2. Business license, issuance of specific electronic signature certification services;
3. Documents certifying the specific technical standards specified in the Part VIII of this Decision.

Article 39 Validation Certificate

The validity of a specific electronic signature certificate holder will be determined according to the request and requirements of the applicant but not more than 05 years.

Article 40 Renewal, change, suspension or cancellation

The provider of the specific electronic signature certificate who wants to change, add to the list, suspend, and terminate all or part of its services must notify the issuer of the foreign electronic signature for at least 30 days with a written explanation.

Part 8

Location and safety standards

Article 41 Standards for the provision of electronic signature certification services

The standard facility for providing electronic signature certification services must include the following:

1. **Location**

- The facility must have a CCTV system to monitor the recording of events at the location;
- The service provider must allocate the location and install the system properly to ensure protection from water.

2. **Access to equipment control room**

Entry-Exist to equipment control system equipped with an electronic signature certification system requires that only personnel authorized by the service provider have access to the area, which controls access by smart card access control or finger scan with password, door hold open sounder system.

3. **Electrical system and air conditioning system**

- The service provider must have a mains supply and a backup generator to prevent the operation of the system in case of a power outage.
- There is an air conditioning system to control the heat and humidity of the room by separating it from the air conditioning system in the building.

4. **Fire prevention**

The areas where the electronic signature certification system is installed must be equipped with a fire protection system with special features that do not damage electrical and electronic equipment and have been certified to ensure fire safety.

Article 42 System security standards

The security standards for the issuance of electronic signature certification services are as following:

1.Ensure the security of all information of users not to be destroyed, altered or suspended.

2.There must be a backup system to ensure normal use;

3.The security of the system must be ensured so that it is not a vulnerability that can be exploited by unscrupulous individuals to attack, damage or cause harm to others.

4.There is a system to alert and prevent attacks and unauthorized connections through the computer system.

5.Equipment used to record or store data if it is damaged or not used, it must be destroyed in an appropriate way to ensure that it is not reused or retrieved.

6.Backups of important data must be stored outside the system location to prevent loss of data in case of an emergency.

7.All technical versions used in the provision of services must be located in Lao PDR.

8.Other technical standards as defined by the Ministry of Post and Telecommunications .

Part 9

Specific standards

Article 43 Key pair generation and installation

The services provider electronic signature has to installation and key pair generation for adapting e-signature as following:

1.Key pair generation have to follow federal information processing standard (FIPS) 140-2 Level 3;

2.Private key delivery to subscriber must specify the safety procedures to transfer private key for service representative;

3.Public key delivery to certificate issuer requires the identification of public key delivery channels and identification information of the service provider;

4.The CA public key delivery to relying parties must identify the public key access channels of the relevant partners;

5.Key size must use RSA method with key pair generation length is 2.048 bit.

Article 44 Private key protection and cryptographic module engineering controls

The provider of electronic signatures, personal key protection and device management for the secret codes as following:

1.Cryptographic module standards and controls and cryptographic module rating must follow the federal standard information processing standards (FIPS) 140-2 level 3;

2.Private key multi-person control must have at least 02 personnel who can trust responsible for enter controlling;

3.Private key backup must to follow the federal standard information processing standards (FIPS) 140-2 level 3;

4.Private key archival must be stored on a secure device and for a reasonable period of time;

5.Private key transfer into or from a cryptographic module must have at least 02 personnel who can trust responsible for this key;

6.Private key storage on cryptographic module must be stored in the key management device and the private key backup in the key storage device;

7.The method of activating private key module must be operated by at least 2 designated personnel responsible for the operation and must have a valid password;

8.Method of deactivating private key must immediately log out from system after completed work;

9.The method of destroying private key must provide for the destruction of a private key when activated by an appropriate process and ensure security.

Article 45 Other aspects of key pair management

The provider of electronic signature certification must manage the key pair according to the principles as following:

1.Public key archival must be stored on a secure device and at appropriate intervals;

2.Certificate operational periods and key pair usage periods are determined by the national electronic signature issuer.

Article 46 Activation data used to install the electronic signature certificate

The provider of the electronic signature certificate must perform the following steps for the installation of the electronic signature certificate as following:

1.Activation data generation and installation must be performed during the installation of key management equipment by the person authorized to operate and must have a valid password;

2.Activation data protection activation data protection requires authentication before each private key is activated;

3.Computer security controls must have the appropriate technical requirements and details of the appropriate security technical requirements and the computer security rating must be in accordance with the standards defined by the national electronic signature certification authority.

Article 47 Life cycle technical control

The electronic signature certificate provider must manage the technical aspects of the service system by these methods as following:

1.System development controls must have a validation process before installing software used in the system;

2.Security management controls need to control the security management to access the service system and use the system appropriately and ensure security;

3.Network security controls must specify specific channels to access the network;

4. Time stamping must be installed in accordance with the standard timing device (NTP server) by the device associated with the electronic signature certification system that refers to the time from the same device.

Article 48 Defining the format of the electronic signature certificate, the revocation list and the status of the electronic signature certificate (Certificate, CRL and OCSP profiles)

The electronic signature certificate provider must specify the format of the electronic signature certificate, cancellation signature and the status of the electronic signature certificate as follows:

1.Certificate Profile must comply with ITU-T X.509 version 3 and standard of RFC 5280 Internet X.509 Public key infrastructure certificate and CRL at least.

1.1.Certificate extensions must comply with the standards of ITU-T X.509 and standards of RFC 5280 at least and consist of documents as follows:

- Key usage must be specified in the electronic signature certificate, with at least a digital signature, key Cert Sign and CRL Sign.
- CRL Distribution Points must specify which channels have access to the electronic signature cancellation list.
- Authority key identifier must specify the identification information of the issuer of the electronic signature on the electronic signature certificate.
- Subject key identifier must be specified in the electronic signature certificate.

1.2.Name Forms must specify the issuer and subject details such as country (C), Organization (O) and Common Name (CN).

2.Certification Revocation List (CRL) Profile must provide information on the list of revocation items such as Authority Key Identifier and Base CRL Number in accordance with ITU-T X.509 version 2 and standards of RFC 5280 at least.

3.Online Certificate Status Protocol (OCSP) Profile must be able to verify the status of the electronic signature certificate.

Part 10

Rights and obligations

Article 49 Rights and Obligations of Providers

Electronic signature providers have the rights and obligations as following:

1.Request to renew, change, suspend or cancel the operation of its business;

2. Suspend the provision of services to users who violate laws and regulations;

3. To cooperate with the authorities in charge of post and telecommunication staff and the relevant management -inspection organizations in managing the inspection;

4. Keep the information of service users confidential and secure, except in the case of an order from the relevant authorities;

5.Under the management and inspection of the Ministry of Post and Telecommunications;

6.Assign obligations in accordance with laws and regulations;

7.Implement other rights and obligations as stipulated in the laws and regulations.

Article 50 Rights and Obligations of Service Users

The user of the electronic signature service has the rights and obligations as following:

1.Receive quality services, convenient, prompt and safe;

2.Inquire and sue the service provider in accordance with the due process in order to be fair to the service user;

3.Pay for services in accordance with regulations;

4.Present to the organization the management and inspection of the electronic signature of the service provider;

5.Implement the rights and obligations as stipulated in the laws and regulations.

Part 11

Fees and charges

Article 51 Fees

The fee for issuing an electronic signature certificate is subject to the specific regulations promulgated from time to time.

Article 52 Service charges

The service charges for issuing an electronic signature certificate is subject to the specific regulations promulgated from time to time.

Part 12

Prohibitions

Article 53 General prohibitions

Prohibit individuals, legal entities or organizations from behaving as follows:

1. Breaking, blocking, obstructing the provision of electronic signature certification services;
2. Falsify electronic signature certificates;
3. Provide inaccurate information;
4. Pretend to be an electronic signature certification service provider;
5. Using someone else's electronic signature certificate without permission;
6. Other behavior that violates laws and regulations.

Article 54 Prohibitions for service managers

Administrative staff or government agencies responsible for the management of electronic signature certification services are prohibited from the behaviors as following:

1. Access the electronic signature certification system and disclose information about the electronic signature certification without permission;
2. Modifying, destroying or disclosing official confidential information without permission;
3. Abandonment or neglect of their responsibilities;
4. Other behavior that violates laws and regulations.

Article 55 Prohibitions for issuers of electronic signatures

The issuer of the electronic signature certificate is prohibited from engaging in the behaviors as following:

1. Provide electronic signature certification services without permission or invalidation of the license or without certification;
2. Use a license or certificate for another person to use, rent or transfer;
3. Disclose the information of the user, except for other laws or specific regulations, if otherwise specified;
4. Other behavior that violates laws and regulations.

Part 13

Management and inspection of electronic signature transactions

Article 56 Organization for management and inspection of services

The Electronic signature management and inspection agency consists of:

1. Ministry of Post and Telecommunications;
2. Department of Post and Telecommunications at the Province, Capital.

Article 57 Rights and duties of the Ministry of Post and Telecommunications

In managing the operation of the electronic signature business, the Ministry of Post and Telecommunications has the rights and duties as follows:

1. Disseminate laws and regulations related on E-signature;
2. To consider approving, renewing, altering, suspending and revoking licenses for the issuance of electronic signatures;
3. To monitor, inspect the implementation of conditions, standards, quality and regulations in accordance with this decision;
4. Warn, educate or adjust violators of other relevant laws and regulations;
5. To consider and amend the terms regarding the provision of electronic signatures, such as the quality of services and other services;
6. Collect fees and charges for the issuance of licenses, electronic signatures and other service fees in accordance with laws and regulations;
7. Perform other duties as stipulated in the laws and regulations.

Article 58 Rights and duties of the Department of Post and Telecommunication at the province and capital

In managing the operation of electronic signature operations, the Department of Post and Telecommunication at the province, capital has the rights and duties as follows:

1. Disseminate laws and regulations related on E-signature;
2. Advise on the approval, renewal, alteration, suspension and revocation of licenses for the issuance of electronic signatures;
3. Develop, maintain and upgrade personnel in the field of electronic signatures;
4. To monitor and inspect the use of electronic signatures of various organizations;
5. Receive proposals on the provision of electronic signature services, such as the quality of services and services;
6. Perform other duties as stipulated in the laws and regulations.

Part 14

Measures against violators

Article 59 Measures against violators

Individuals, legal entities or organizations that violate this decision will be educated, warned, disciplined and fined, compensated for civil damages or are subject to criminal penalties, depending on the circumstances.

Article 60 Educational Measures

Government employees or electronic signature certification providers will be trained in the cases as following:

1. Do not cooperate, suppress, delay, speak rudely or inappropriately;
2. Delaying unreasonable service or violating other prohibitions.

Article 61 Disciplinary measures

Government employees or management authorities to violate the prohibitions in this decision shall be subject to disciplinary action in accordance with applicable laws

Article 62 Fined Measures

Individuals or legal entities that violate this decision will be subject to the penalties as following:

1. Doing business issuing electronic signatures without a license will be fined 40,000,000 Kip;
2. Breaking, blocking or obstructing the operation of the electronic signature certification system, which does not cause significant damage, will be fined 5,000,000 Kip;
3. Giving a license to another person to use, rent, transfer will be fined 15,000,000 Kip;
4. Incorrect service as specified in the license will be fined 15,000,000 Kip;
5. Providing information or disseminating information on invalid electronic signatures will be fined 10,000,000 Kip;
6. Disclosure of information of service users without permission will be fined 10,000,000 Kip;
7. For service that is not in accordance with the contract or notice will be fined 15,000,000 Kip;
8. Reserving or disseminating information on electronic signature certificate late will be fined 10,000,000 Kip;

9. Do not record usage information or do not report information according to laws and regulations will be fined 10,000,000 Kip;
10. Pretending to be an electronic signature certification service provider will be fined 15,000,000 kip;
11. Using someone else's electronic signature certificate without permission will be fined 10,000,000 Kip;
12. In case of change, suspension or cancellation of the service, the late notification will be fined 10,000,000 Kip;
13. Failure to notify or late notify its agent to the issuer of the National Electronic Signature Certificate before the due date will be fined 5,000,000 Kip;
14. Renewal of business license late before the fine will be fined 5,000,000 Kip

Article 63 Measures to Suspend or Abolish

The regulatory authority will suspend or revoke the business license for providing electronic signature services as follows:

Business licenses will be suspended in the cases as following:

1. Excess services allowed in the license;
2. Falsifying, concealing or providing inaccurate information as required by the governing body;
3. Do not renew the license within 90 days after the license expires;
4. Do not operate within 12 months after receiving the license and certification;
5. Failure to pay fees and service charges to the State in accordance with laws and regulations.

Business license will be revoked in the cases as following:

1. Not amended in accordance with the conditions of the governing body or the issuer of the National Electronic Signature after being suspended;
2. Giving a license or certificate to another person to use, rent or transfer without permission;
3. Serious violations of laws and regulations.

Part 15
Final Provisions

Article 64 Implementation

The Department of Information Technology and Internet Centre shall strictly implement this decision.

Article 65 Effectiveness

This decision is effective from the date of signature and fifteen days after it is published in the Official Gazette.

Minister

Dr. Thansamay Kommasith