Lao People's Democratic Republic
Peace Independence Democracy Unity Prosperity

President of the Republic No. 025/POR

Vientiane Capital, Date: 17January 2013

DECREE OF THE PRESIDENT
OF THE LAO PEOPLE'S DEMOCRATIC REPUBLIC
ON THE PROMULGATION OF THE LAW ON ELECTRONIC TRANSACTIONS

- Pursuant to paragraph 1, Article 67, Chapter VI of the Constitution of the Lao People's Democratic Republic**;**
- Pursuant to the Resolution of the National Assembly No.032/NA, dated 7 December 2012;
- Pursuant to the Request Letter of the Standing Committee of the National Assembly No.01/SC, dated 04 January 2013.

The President of the Lao People's Democratic Republic Issues a Decree:

Article 1 **Promulgate the Law on Electronic Transactions.**

Article 2 **This Presidential Decree is effective from the date of its signing.**

President of the Lao PDR

Signed and stamped

Choummaly SAYASONE

Lao People's Democratic Republic
Peace Independence Democracy Unity Prosperity

National Assembly No. 032/NA

RESOLUTION

OF

THE NATIONAL ASSEMBLY OF LAO PEOPLE'S DEMOCRATIC REPUBLIC

ON THE APPROVAL OF THE LAW ON ELECTRONIC TRANSACTIONS OF THE LAO PEOPLE'S DEMOCRATIC REPUBLIC

ON THE PROMULGATION OF THE LAW ON ELECTRONIC TRANSACTIONS

Pursuant to paragraph 2, Article 53 of the Constitution and paragraph 1, Article 3 of the Law on National Assembly of the Lao People's Democratic Republic with respect to rights and duties of the National Assembly.

Following detailed and widespread review by the 4th Session of the 7th Legislative of the National Assembly of the contents of the Law on Electronic Transactions in the afternoon Session on the 7th December 2012.

The National Assembly Session decides:

Article 1 Approval of the Law on Electronic Transactions with unanimous votes.

Article 2 This Resolution is effective from the date of its signing.

Vientiane Capital, Date: 07 December 2012

President of the National Assembly

(Stamped and signed)

Pany YATHOTOU

Lao People's Democratic Republic

Peace Independence Democracy Unity Prosperity

National Assembly No 20/NA

Vientiane Capital, Date: 7 December 2012

LAW

ON

ELECTRONIC TRANSACTIONS

Part I
General Provisions

Article 1 – Purpose

This Law defines the principles, regulationsand measures for the formation, use, recognition, management and inspection of electronic transactions to create reliability and confidence in electronic transactions aiming atprotecting the legitimate rights and interests ofthose who are doingelectronic commerce,and ensure the use, promotion of electronic transactions, modernization, regional and international integration contributing to socio-economic development while preserving national stability, social peace, order and justice.

Article 2 – Electronic Transaction

An electronic transaction is an act of making a contract, and the provision and use of electronic government services that areconducted wholly or partly by electronic means, which includes the use of Automatic Teller Machines (ATMs), payments over the Internet, and other similar interactions.

Article 3 – Definitions

The terms used in this Law shall have the following meanings:

1. **Electronic** means electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities of technology;
2. **Digital** means the expression of any kind of information in discrete numerical form processed by computers or similar electronic devices.
3. **Electronic Communication** means any statement made, sent or received in electronic form;

4. A **Data Message** means information in the form of alphabetical letters, text, numbers, sound, codes, computer programs, software, and databases or other formats that is generated, sent, received or stored by electronic, optical, or magnetic means;
5. The **Originator** of an electronic communication is the party who generates or sends an electronic communication, or the party on whose behalf it is generated or sent, which does not include an intermediary;
6. The **Addressee** is the party that is intended to receive electronic information sent by the originator, which does not include an intermediary;
7. An **Electronic Document** means any document, record, or information that are recorded or stored on any medium by an electronic information system and that canbe read using a display, print-out and other output;
8. **Electronic Data Interchange (EDI)** means the electronic transfer from one electronic information system to another of information using an agreed technical standard to structure, use and store the information;
9. An **Electronic Record** is any document or data that is required by law or regulation to be stored when electronic storage means are used.
10. **Electronic Information System** means a system used for creating, sending, receiving, and storing data or other processing of data messages;
11. **Electronic Commerce** is the purchase, sale and other exchange of goods or services between individuals, legal entities or organizations using electronic means;
12. **Electronic Government** means electronic transactions conducted between government bodies or by government bodies with the private sector or people;
13. **Certification Service Provider** means a legal entity or organization authorized by the Science and Technology Sector to issue secure digital signature certificates and provide related services;
14. **Signature** means an electronic method used to identify a person who is the owner of the signatureand to indicate the intention of that person regarding the information contained in an electronic document;
15. **Signature Owner** means a natural person, or the authorized representative of a legal entity, who uses an electronic signature creation device in order to generate electronic signatures;
16. **Parties to Electronic Transactions**mean both suppliersand consumers of goods and services whouse electronic means for their transactions;
17. **Independence** means parties to an electronic transaction may selectany method, form and technology to carry out their electronic transaction;
18. **Have Equal Legal Status** means transactions, documents and signatures generated in electronic format and in paper format have equal validity.

Article 4 – State Policy forElectronic Transactions

The State pays attention to the importance of the use of electronic transactions by promoting and supporting[electronic] commerce [and] services, public administrationand other [electronic] transactions to develop the economy and serve the society.

The State pays attention to the development of ICT, communication and information infrastructure, and capacity buildingto ensure that electronic transactions are safe, transparent, and reliable and to protect consumers.

Article 5 – Principles of Electronic Transactions

In conducting electronic transactions the following principles shall be observed:

1. Voluntary;
2. Equality;
3. Independence;
4. Have equal legal status; and
5. Integrity for users doing transactions.

Article 6 – Scope of Application

This Law applies to individuals, legal entities,State organizations [and agencies],international organizations and civil society that use electronic transactions in Lao PDR.

This Law does not apply to:

1) The creation of a will;
2) Certificates related to births, marriage, divorce, and death;
3) Documents of title;
4) The creation, enforcement or certification of the possession of other's property or power of attorney;
5) Contracts for the sale, transfer, or other disposition of ownership or any interest in land or immovable property;
6) Petitions under the Law on Petitions;
7) Bills of exchange,bills of lading, warehouse receipts or any document that entitles the bearer or beneficiary to claim the delivery of goods,unless laws and regulationsdefine otherwise.

Article 7 – International Cooperation

The State cooperates with foreign countries and regional and international organizations on matters related to electronic transactions, by sharing of experiences, information, techniques, technology, scientific research, education, and human resource development, and complies with requirements in international agreements and treaties to which Lao PDR is a party.

Part II
Contracts, Data Messages and Electronic Documents

Chapter 1
Electronic Contracts

Article 8 – Formation of Electronic Contracts

The formation of an electronic contract using electronic means isas follows.

1. An offer and the acceptance of an offer to enter into a contract.
2. A declaration of intent or other statement by an originator or addressee of a data message or electronic document;
3. An agreement by the parties to an electronic transaction to select the technological means, electronic communications modes, and electronic signature rules.

Contracts formed electronically can be amended electronically unless the contract definesotherwise.

In addition to the above provisions, the formation of each type of an electronic contract shall be applied according to the Law on Contracts and Torts.

Article 9 – Recognition of Contracts Formed Electronically

The recognition of contracts formed electronically is as follows:

1. The parties to a contract may express their intention to enter into that transaction in the form of electronic means.
2. An electronic contract made in compliance with this Law and other relevant laws and regulations shall be legally enforceable.

Article 10 – Electronic Data Interchange

Electronic Data Interchangeand the use of electronic information systems that generate other types of automated messages are as follows:

1. An electronic contract may be formed where all the parties, or any of them, use an electronic information system that generates automated messages.
2. The parties to an electronic contract formed in this manner will be presumed to be bound thereby, whether or not they actually reviewed the terms of the agreement, provided that:
    a) The terms of the contract can be reviewed;
    b) The electronic information system used provides an opportunity to prevent or correct errors;
    c) The party using the electronic information system provides the other parties an opportunity to rescind the contract, provided that the party seeking rescission has not benefited under thatcontract.

Chapter 2
Electronic Data Messages

Article 11 – Determining the Source of and Responsibility for Electronic Data Messages (Attribution)

The determination of the source of, and responsibility for, electronic data messages are as follows:

1. Any data message sent by any electronic means shall be attributed to its originator if the data message:
    a) is actually sent by the originator, or by an agent acting on his behalf,
    b) is sent by an electronic information system that operates automatically that is established by the originator.
2. The originator of a data message named in the message is bound thereby only if the message was actually sent by the named originator or with the authority of the named originator.
3. The provisions mentioned in sections 1 and 2 of this Article will not be enforceable if within a reasonable period the addressee is notified by the originator, or by a person acting on his behalf, that due to technical errors the data message should not be attributed to the originator, and the addressee has enough time to verify this notification;
4. When a data message meets the requirements of this Article, the addressee may rely on it as an accurate expression of the intention of its originator.
5. If an addressee receives more than one identical data message from an originator, and each of the messages meets the requirements of this Article, the addressee shall rely on the first such data message sent by the originator.

In all cases, the originator and addressee may agree on the application of other regulations for determining the attribution and responsibilities for the electronic data messages [being exchanged].

Article 12 – Date,Time and Location of Sending and Receiving Electronic Data Messages

The determination of the date,time and location of sending and receiving a data message are as follows:

1. The sending date and time of electronic information are the date and time when the information is sent out from the information system under the control of the originator or any authorized individual on behalf of the originator.
2. The receiving date and time of electronic information are the date and time when the electronic information can be accessed on the electronic information system of the addressee.
3. The address of sending and receipt of electronic data messageare the location where such information is actually sent from and is actually received.

Chapter 3
Electronic Documents

Article 13 – Recognition of Electronic Documents

The recognition of electronic documents is as follows.

1. An electronic document and the information it contains shall be legally valid and enforceable according to this Law and other relevant laws and regulations;
2. Where a legal rule requires information to be in writing, or provides for certain consequences if it is not, an electronic document satisfies that legal rule if the information contained in the electronic document can be accessed for subsequent reference.

Article 14 – Using Electronic Documents as Evidence

The use of electronic documents as evidence is as follows.

1. Electronic documents may be used as evidence [in the] same [way] as other [paper] documents [that are used as] evidence, except [where] laws defined otherwise;
2. In assessing the weight to be given to a data message or electronic document, the court shall evaluate:
   (a) the data message was generated, stored or communicated;
   (b) the integrity of the information was maintained;
   (c) theoriginator, addressee, intermediary and others as necessary; and
   (d) any other relevant factors.

Article 15 – Originals

The use of electronic documents in place of an original paper document, record, or information is as follows:

1. An electronic document shall be treated as an original if the following conditions are satisfied:
   (a) there exists a reliable assurance as to the integrity of the information contained in the electronic document in its final form, whether as a document in writing or as an electronic document;
   (b) where the document, record or information is to be provided to an individual, the electronic document that is provided to the individual is capable of being displayed to that individual; and,
   (c) any additional requirements relating to the provision of an electronic document.
2. The rule in section 1 of this Article may apply to a document, record or informationin its original form or a copy;
3. The assessment of integrity shall be whether the information in the electronic document has remained complete and unaltered, apart from the introduction of any changes that arise in the normal course of communication, storage and display;

4. The assessment of reliability of information contained in the electronic document, the purpose for and all relevant circumstances in which the information was generated shall be considered.
5. An individual or legal entity may satisfy the requirement referred to in section 1 of this Article by using the services of a trusted third party, provided that the conditions set forth in section 1 of this Article are met.

A concerned Ministry may retain the requirement that a particular document, record or information be provided in original paper form.

Article 16 – Storage and Retention of Electronic Documents

Any individual, legal entity or organization may store and retain any document, record or information.Such storage and retention may be made by usinganelectronic document [format], unless the laws and regulations defined otherwise.

Article 17 – Standards for Electronic Document Storage and Retention

The standards for electronic document storage and retention are as follows.

1. The storage or retention of a document is met by using an electronic document if the following conditions are satisfied:
   (a) the information contained in the electronic document is accessible so that it can be used for subsequent reference;
   (b) the electronic document is stored or retained in the format in which it was generated, sent or received, or in a format that can be demonstrated to represent accurately the information generated, sent or received; and,
   (c) such information is stored or retained to enable the identification of the originator and addresseeof an electronic document and the date and time when it was sent or received.
2. The storage or retention of documents in accordance with section (1) of this Article does not extend to any information that is used solely to enable the message to be sent or received.
3. An individual or legal entity may satisfy the requirement referred to in section 1 of this Article by using the services of a trusted third party, provided that the conditions set forth in section 1 is this Article are met.

Article 18 – The Use of Seal

The uses of a seal on electronic documents are as follows.

1. When a law orregulation requires a legal entity or other organization to stamp a sealto a document for it to be recognized and legally valid, an Electronic Document shall have the equivalent legal value to a signed and stamped document if the Electronic Document is issued with a secure digital signature.
2. When a law orregulation requires the seal of a State Organization to be affixed to a document for it to be recognized and legally valid, an Electronic Document shall have the

equivalent legal value to a signed and sealed, or stamped, document if the electronic document is issued with a secure digital signature.

Part III
Electronic Signatures

Chapter 1
Types of Electronic Signatures

Article 19 – Types of Electronic Signature

There are three types of electronic signatures:

1. Basic electronic signature;
2. Basic digital signature; and
3. Secure digital signature.

Article 20 – Basic Electronic Signature

Basic electronic signature means data in electronic format that are in, affixed to, or technically associated with a data message, which identifies the signatory and indicates the signatory's intention in respect of the information contained in the data message.

Article 21. Basic Digital Signature

Basic digital signature means a type of electronic signature that is uniquely linked to the signatory, capable of identifying the signatory, created using means that the signatory can maintain under his sole control, andany subsequent change of the data is detectable.

Article 22. Secure Digital Signature

Secure digital signature means a type of digital signature created using technical methods that protect against the forgery of that signature by using available technology to ensure that the signature creation-data used to generate that signature can practically be used only once and can be reliably protected by the legitimate signatory against its use or discovery by others.

Chapter 2
General Requirements of Electronic Signatures

Article 23. Requirements for the Use of Electronic Signatures

General requirements for the use of electronic signatures are as follows.

1. A mutual agreement to use any type of electronic signatures shall be sufficient for the purposes of establishing an agreement between the parties;
2. The mutual agreement to use electronic signatures may contain any electronic signature rules that the parties select for the specific transaction between them, except such agreement that contradicts laws and regulations;
3. The use of secure digital signatures shall comply with regulations issued by the Ministry of Science and Technology.

The Government shall define [the type of] electronic signatures that may be used in electronic transactions where the Government is a party.

Article 24 – The Recognition of Electronic Signatures

General requirements for the recognition of electronic signatures are as follows.

1. Where a rule requires a signature, but the signature is missing from a document, an electronic signature may be applied if it:
   (a) Meets the requirementsfor electronic signature as defined in Article 25 of this Law;
   (b) Meets the specificrequirementsfor secure digital signature as defined in Article 26 of this Law;
   (c) Is proven in fact to identify the person and to indicate that person's intention in respect of the information contained in the electronic signature.
2. If an electronic signature is contested, the party that is the owner of the electronic signature must demonstrate evidence that the signature fulfills the requirements of section 1 of this Article.
3. When a secure digital signature meets the requirements of this Article, it shall be presumed to be the signature of the party unless the party contesting the validity of the secure digital signatureshalldemonstrateevidence.

Article 25 – The Validity of Electronic Signatures

General requirements for the validity of electronic signatures are as follows:

1. An electronic signature associated with a data message or electronic document is valid and may be relied upon where:
   (a) the signatory and the date and time of signature can be identified;
   (b) the electronic signature system used to generate the signature uses technical methods that can be specified and managed only by the signature's owner;
   (c) the electronic signatures created by the electronic signature system can only be stored and managed by the owner;

(d) the electronic signature system is able to access any information system that can identify whether there have been changes in the data message or electronic document.

2. Any technical method of creating an electronic signature that satisfies the requirements of section 1 of this Article shall not be denied legal effect.

Chapter 3
Specific Requirements for Secure Digital Signatures

Article 26 – Secure Digital Signature Validity

The specific requirements for the validity of secure digital signatures are as follows.

1. The technical method of creating the secure digital signature must be recognized by and comply with the regulations of the Ministry for Science and Technology.
2. A secure digital signature must be accredited by a certificate issued by a legal entity or organization authorized to provide a secure digital signature certificate or whose secure digital signature certificates are recognized by the Ministry of Science and Technology.
3. Asecure electronic signature that is genuine and reliable or a certificate issued by a registered certification services provider shall be deemed equivalent to the signature used in a traditional paper-based transactions.

Article 27 – Provision of Secure Digital Signature Certification Services

The specific requirements for the provision of digital signature certification services are as follows:

1. Secure digital signature certification services can be publicly offered by an authorized organization or legal entity, including private companies, that have met the requirements for registration and been authorized by Science and Technology Sector;
2. Certificate serviceproviders shall meet the specificrequirementsset forth in Article 26 of this Law and other relevant laws and regulations;
3. Certificate serviceproviders may develop and apply their own private accreditation practices to enhance the level of trust, security and quality in the use of secure digital signatures, provided that these private accreditation practices shall:
   (a) meet the specific requirementsas prescribed in this Law;
   (b) do not serve as a barrier to competition for certification services;
   (c) beapproved by the Ministry of Science and Technology.

Article 28 – Registration of Certificate Service Providers

The Science and Technology Sector shall be responsible for the registration of certificate service providers as follows.

1. Establish and maintain a register of certification service providers who are established in the Lao PDR where suchservice providers issue certificates to the consumers of the service.
2. Record information in a registry,including the names, addresses, and other relevant details for those certification-serviceproviders.
3. Adopt and administer the required information with the following documents:
   (a) A statement of the types of services provided;
   (b) A description of the information technology systems used;
   (c) A description of the rules, procedures, and other measures adopted by the certification services provider to protect the integrity, reliability and security of its data and the privacy and confidentiality of the personal information of its customers that it holds;
   (d) a business registration;
   (e) other information that is relevant to the administration of digital signatures in the Lao PDR.
4. Deny registration to or revoke the registration of any certification service providers whose application or whose activities do not meet the requirements of this Law and other relevant laws and regulations.

Article 29 – Recognition of Foreign Digital Signature Certificates and Signatures

The Ministry of Science and Technology will recognize foreign digital signature certificates and signatures in the following cases:

1. By examining whether the certificate offers a substantially equivalent level of genuineness and reliability as a certificate issued in Lao PDR;
2. If the certificate and signature are consistent with [recognized] international standards and any other relevant factors, except that the geographic location where the certificate is issued, [where] the electronic signature is created or used, or [where] the originator or signatory has its place of business will not be considered.

The Ministry of Science and Technology shall establish and maintain a publically-available list of the digital signature certificates issued by foreign certificate providers that are recognized under section (1) of this Article.

The recognition of a foreign secure digital signature certification that is included in a list of recognized foreign digital signature certificates shall not require an application by the foreign certificate service provider.

Article 30 – Legal Effect of Foreign Secure Digital Signature Certificates

The legal effect of foreign secure digital signature certificates and electronic signatures are as follows:

1. A secure digital signature certificate issued by a foreign certificate provider that is recognized by Article 29 of this Law shall have the same legal effect as a digital signature certificate issued in the country.
2. Any electronic signature created or used outside the country shall have the same legal effect as an electronic signature created or used within the country if it offers a substantially equivalent level of genuineness and reliability, consistent with recognized international standards and any other relevant factors.

Part IV
Electronic Transactions Used by the State Organizations

Article 31 – Forms of Electronic Transaction Used by State Organizations

Electronic transactions by state organizations are divided into three forms as follows:

1. Electronic transactions within a State organization;
2. Electronic transactions between State organizations; and
3. Electronic transactions between a State organization and individuals, legal entities, and other organizations.

The rules and standards that will apply to the use of each type of electronic transaction by State organizationsshall be stipulated inspecific regulations.

Article 32 – Acknowledgement by State Organizations of Electronic Transactions and Documents

Acknowledgement by State organizations of electronic transactions and documents is subject to the following rules.

1. State organizations may acknowledge:
   (a) Electronic documents used for the purpose of establishing information or showing that information has been stored in electronic formats;
   (b) Licenses, permits, approvals, or other information in electronic formats;
   (c) Payment of service fees using electronic means.
2. When a State organization makes a decision to select an operation method from section 1 of this Article, such organization must consider the following issues:
   (a) The means and formats for how the document or transaction is submitted, established, stored or issued.
   (b) In case electronic documents have to be provided with signatures, the formats and types of electronic signature that must be identified.

(c) The methods and formats of electronic signature that shall be attached to the electronic document or transaction.

(d) The process and operational procedures that will ensure the comprehensiveness, safety and confidentiality of electronic documents and transactions, including payments, that are sent or delivered by or stored in electronic information systems.

(e) The criteria for certifying the ownership of data messages, electronic documents and the information sent or received as part of an electronic transaction, including payments.

Part V
Intermediary

Article 33 – Intermediary

Intermediary means an individual or legal entity that provides services to others for sending, receiving or storing data messages, or hosting temporarily,providing access to a communication system and providing other services for handling data messages and electronic documents.

Article 34 – Intermediary Non-Liability

An intermediary is not liable:

1. to monitor any information contained in a data message or electronic record that it handles for a user;
2. for a data message or electronic record that it handles for a user, if an intermediary is not an originator;
3. for a data message or electronic record for which an intermediary has no actual knowledge that [the information] gives rise to liability;
4. forbackground ona data message for which an intermediary has no actual knowledge.

Article 35 – Intermediary Liability

Even if an intermediarydoes not have liability as defined in Article 34 of this Law, an intermediary still has the following liabilities:

1. Must follow regulations and procedures developed by the Ministry of Posts and Telecommunications;
2. Be subject to civil or criminal liability depending on each case if it knows the facts or circumstances where a data message would result in damage to individuals, legal entities or other organizations;
3. Must comply with any valid contractual or additional legal obligation that it may have in respect of a data message or electronic record;

   If an intermediary has actual knowledge that information in a data message or electronic record gives rise to civil or criminal liability, the intermediary shall:

   (a) Remove the data message or electronic record from any information processing system that the intermediary controls and cease to provide services in respect of that information but shall notify the originator if it is unaware[of such fact];

   (b) Notify the Post, Telecommunications, and Communications Sector or the appropriate law enforcement agency of the relevant facts and, where it is known to

the intermediary, the identity of the person for whom the intermediary was supplying services in respect of the data message or electronic record.

4. Be subject to other liabilities as defined in relevant laws and regulations.

Part VI
Prohibitions

Article 36 – Prohibitions for Secure Digital Signature Certificate Providers

Secure digital signature certificate providers are prohibited to behave as follows:

1. Provide false information in the registration application for secure digital signature certificate provider;
2. Use personal information provided by a user [for other purposes];
3. Use information concerning the user prepared by the certificate provider [for other purposes];
4. Engage in activities of an unauthorized secure digital certification service provider;
5. Create, use and publish secure digital signature certificates or electronic signatures for fraudulent or any other [unlawful] purposes that give rise to damages;
6. Misuse any [other] signature certification service for any fraudulent or other unlawful purposes;
7. Provide services with regard to data messages and electronic records that give rise to damage to national stability, security and social order;
8. Other acts that violate the laws and regulations.

Article 37 – Prohibitions for Digital Signature Certificate Users

Secure digital signature certificate service users are prohibited to have the following behaviors:

1. Provide false information in the registration application for a secure digital signature certificate;
2. Use secure digital signature certificates to defraud or for other unlawful purposes;
3. Continue the use of a false secure digital signature certificate;
4. Use data messages and electronic records that give rise to damage to national stability, security and social order;
5. Other acts that violate the Lawsand regulations.

Article 38 – Prohibitions for Intermediaries

Intermediaries are prohibited to behave as follows:

1. Provide services to facilitate the exchange of data messages and electronic transactions without authorization;
2. Engage in any prohibited act that is defined in regulations issued by the Ministry of Posts and Telecommunications;
3. Provide services with regard to data messages and electronic records that give rise to damage to national stability, security and social order;
4. Other acts that violate the lawsand regulations.

Article 39 – Prohibitions for Individuals, Legal Entities and other Organizations

Individuals, legal entities and other organizations are prohibited to behave as follows:

1. Forge electronic documents, electronic signatures or electronic certificates or use forged digital signatures;
2. Provide false information and forged electronic signatures;
3. Access, copy, restructure or take over another person's electronic signature system without [valid] authorization;
4. Use the identity of another person without authorization;
5. Claim falsely that they are representatives to claim for the suspension, cancellation or approval of digital signature;
6. Publish a forged, false, revoked or suspended digital certificate or knowingly place such certificate at the disposal of another person;
7. Provide data messages and electronic records that give rise to damage to national stability, security and social order;
8. Other acts that violate the laws and regulations.

Part VII
Resolution of Disputes

Article 40 – Forms of Dispute Resolution

Dispute resolution shall be carried out according to any of the following forms:

1. Resolution by Conciliation;
2. Administrative Dispute Resolution;
3. Resolution by Economic Dispute Resolution Authority;
4. Suing to Court;
5. International [Dispute] Settlement.

Article 41 – Resolution by Conciliation

Where a dispute involving electronic transactions occurs, the parties may resolve such dispute by discussion and compromise to secure mutual benefits.

Article 42– Administrative Dispute Resolution

An administrative dispute involving electronic transactions under the Science and Technology sector may beappealed to the Science and Technology Sector for resolution.

A person or legal entity is eligible toappeal to the Science and Technology Sector to reconsider a decision refusing to register a Secure Digital Signature Certificate Provider, or the suspension and removal of such registration. The Science and Technology Sector shall resolve the appeal within thirty working days. The absence of a response to the appeal by the deadline shall be a decision to reject the appeal.

If the appellant is not satisfied with the appeal decision, including when the appeal is rejected by a non-response, the appellant may further appeal the case to the courts for final resolution according to the laws and regulations.

Article 43– Resolution by the Economic Dispute Resolution Authority

Where an economic dispute involving electronic transactions occurs, the parties may resolve it by [using] the economic dispute resolution authority as defined in the Law on Economic Dispute Resolution upon mutual agreement.

Article 44 – Suing to Court

Whenadispute involving electronic transactions occurs, the parties may sue such dispute to the People's Court for a final decision according to the laws and regulations.

Article 45 – International Settlement

When an international dispute involving electronic transactions occurs, it shall be resolved according to the international treaties and agreements to which Lao PDR is a party.

Part VIII
Management and Inspection

Chapter 1
Management

Article 46– Management Organizations

The Government shall centrally and uniformly manage electronic transactions throughout the country by designating the Ministry of Science and Technology to be responsible for [its] management by coordinating with other relevant sectors and relevant local administrations under their jurisdictions.

The management organizations are as follows:

1. The Ministry of Science and Technology;
2. Provincial [and] Capital Departments of Science and Technology;
3. The District [and] Municipal Offices of Science and Technology;
4. Village Units of Science and Technology.

Article 47– Rights and Duties of the Ministry of Science and Technology

For the purpose of managing electronic transactions, the Ministry of Science and Technology shall have the following rights and duties:

1. to establish policies, strategic plans, programs and plans regarding the development of electronic transaction activities to propose to the government for approval;
2. to conduct research, develop and amend laws, regulations and other legislation concerning electronic transaction activities;
3. to disseminate laws and relevant legislation with regard to electronic transaction activities;

4. to issue, suspend and withdraw permits and maintain a list of digital signature certificate providers according to its responsibility;
5. to consider and resolve proposals with regard to the electronic transaction activities according to its responsibility;
6. to upgrade and improve capacity of personnel of both public and private sectors involved in electronic transactions;
7. to consider standards and methods for the protection and resolving of problems that may occur in electronic transactions according to the proposal of the Provincial [and] Capital Departments of Science and Technology;
8. to supervise [and] monitor the implementation of electronic transaction activities throughout the country;
9. to maintain confidentiality of data messages and electronic records that give rise to damage to national stability, security and social order;
10. to coordinate with other ministries or organizations and local administrations involving the implementation of electronic transaction activities;
11. to carry out international relations activities regarding electronic transaction;
12. to regularly summarize and report activities regarding electronic transaction to the Government;
13. to implement other rights and duties as defined in the laws and regulations.

Article 48– Rights and Duties of Provincial [and] Capital Departments of Science and Technology

For the purpose of managing electronic transactions, the Provincial [and] Capital Departments of Science and Technology shall have the following rights and duties:

1. to elaboratepolicies, strategic plans, programs and plans regarding the development of electronic transaction activities into their regulations, projects, programs and plans and to implement them;
2. todisseminate laws and relevant legislation with regard to electronic transaction activities;
3. to research and proposestandards and methods to prevent and resolve evolving problems that may occur in the electronic transactions to the Ministry of Science and Technology for consideration;
4. to supervise and monitor the District [and] Municipal Offices of Science and Technology to implement electronic transaction activities;
5. to collect statistics [and] information regarding electronic transactions within their jurisdictions;
6. to consider and resolveproposals with regard to electronic transactions within their jurisdictions;
7. to coordinate with other relevant sectors and parties within their jurisdictions to implement electronic transaction activities;
8. to carry out international relations and cooperation with regard to electronic transaction activities as designated by higher level;

9. to regularly summarize and report on electronic transaction activities to the Provincial [and] Capital Administrations, and the Ministry of Science and Technology;
10. to implement other rights and duties as defined in the laws and regulations.

Article 49– Rights and Duties of District and Municipal Offices of Science and Technology

For the purpose of managing electronic transactions, the District [and] Municipal Offices of Science and Technology have the following rights and duties:

1. Implement policies, strategic plans, programs and plans with regard to the development of electronic transaction activities of higher levels;
2. Disseminate laws and other legislation on electronic transactions under their jurisdictions;
3. Supervise [and] monitor the Village Units of Science and Technology on the implementation of electronic transaction activities;
4. Apply standards and methods to prevent and resolve evolvingproblems in the operation of electronic transactions;
5. Consider and resolve proposals on electronic transaction activities under their responsibilities;
6. Coordinate with relevant sectors and parties within their jurisdictions to manage electronic transaction activities;
7. Collect statistics and information on electronic transactions within their jurisdictions;
8. Regularly summarize and report electronic transaction activities to the District [and] Municipal Authorities and the Provincial [and] Capital Department of Science and Technology;
9. Implement other rights and duties as defined in the laws and regulations.

Article 50 – Rights and Duties of Village Units of Science and Technology

For the purpose of managing electronic transactions, Village Units of Science and Technology have the following rights and duties:

1. Implement projects, programs, plans and activities on the development of electronic transaction activities from higher levels;
2. disseminate laws and other legislation on electronic transactions within their villages;
3. Consider and mediateproposals on electronic transaction activities under their jurisdictions;
4. Coordinate with relevant units within their villages on the implementation of electronic transaction activities;
5. Collect statistics and information on electronic transactions within their villages;
6. Regularly summarize and report on electronic transaction activities to the Village Authorities and the District [and] Municipal Offices of Science and Technology;
7. Implement other rights and duties as defined in the laws and regulations and as designated by higher levels.

Article 51– Duties of Other Relevant Sectors

Other relevant concerned sectors, particularly the Post, Telecommunications and Communications Sector, the Industry and Commerce Sector, the Public Security Sector, the Education and Sports Sector, the Finance Sector, and the Banks shall cooperate with the Science and Technology Sector to implement and manage electronic transaction activities in accordance with their roles.

Chapter 2
Inspection

Article 52– Inspection Authorities

Inspection authorities for electronic transaction activities will include the following:

1. Internal inspection authorities that are the same authorities as for Management Authorities of electronic transactions as defined in Article 46of this Law;
2. External inspection authorities include the National Assembly, the State Audit Authority and the GovernmentInspection and Anti-Corruption Authority.

Article 53– Content for Inspection

Content for the inspection of electronic transactions include:

1. Registration and permit for the operation of secure digital signature certificate providers;
2. Secure digital signature certificate services;
3. Implementation by State organizations and other organizations of laws and relevant legislation related to electronic transactions.

Article 54– Forms of Inspection

Inspection of the content listed in Article 53of this Law shall be carried out in the following forms:

- Regular inspection;
- Inspection with prior notice;
- Sudden inspection.

Regular inspection is an inspection that is carried out in accordance with a plan and on a regular and certain period of time.

Inspection with prior notice is an inspection that is not included in the plan but is carried out by informing the audited person in advance.

Sudden inspection is an urgent inspection without informing the inspected person in advance.

An inspection of electronic transactions shall comply with laws and regulations.

Part IX
Incentives toward Outstanding Performers and Measures against Violators

Article 55– Incentives for Those with Outstanding Performances

Individuals, legal entities or organizations with outstanding performance in the implementation of this Law shall be rewarded and given other incentives according to the regulations.

Article 53 – Measures against Violators

Individuals, legal entities or organizations violating this Law shall be warned, educated, face disciplinary actions, be fined, shall pay for civil damages or face criminal actions depending on the seriousness of cases in accordance with the laws and regulations.

Part X
Final Provisions

Article 57– Implementation

The Government of Lao People's Democratic Republic shall implement this Law.

Article 58– Effectiveness

This Law is effective ninety days after the President of Lao People' Democratic Republic issues a Presidential Decree for Promulgation.

Any provision of any other law that conflicts with a provision of this Law shall be cancelled.

President of the National Assembly

Stamped and signed

Pany YATHOTOU