

(National Coat of Arms)

**KINGDOM OF CAMBODIA  
NATION RELIGION KING**

rrrpsss

**Royal Government of Cambodia**

**No.246 ANKR.BK**

**SUB-DECREE**

**ON**

**DIGITAL SIGNATURES**

rrrpsss

**ROYAL GOVERNMENT OF CAMBODIA**

- Having seen the Constitution of the Kingdom of Cambodia;
- Having seen Royal Decree No. NS/RKT/0913/903 dated 24 September 2013 on the Appointment of the Kingdom of Cambodia;
- Having seen Royal Decree No. NS/RKT/1213/1393 dated 21 December 2013 on the Adjustment of and Supplement to the Composition of the Royal Government of Cambodia;
- Having seen Royal Decree No. NS/RKT/0416/368 dated 04 April 2016 on the Adjustment of and Supplement to the Composition of the Royal Government of Cambodia;
- Having seen Royal Kram No. 02/NS/94 dated 20 July 1994 promulgated by the Law on the Organization and Functioning of the Council of Ministers;
- Having seen Royal Kram No. NS/RKM/0196/20 dated 24 January 1996 promulgated by the Law on the Establishment of the Ministry of Posts and Telecommunications;
- Having seen Sub-Decree No.39 ANKR.BK dated 28 January 2014 on the Organization and Functioning of the Ministry of Posts and Telecommunications;
- Having seen Sub-Decree No. 74 ANKR.BK dated 08 March 2015 on the Amendment of Articles 26, 27, 28 and 29 and Supplement to duplicate article 29 of Sub-Decree No. 39 ANKR.BK dated 28 January 2014 on the Organization and Functioning of the Ministry of Posts and Telecommunications;
- Pursuant to the request of the Minister of Posts and Telecommunications.

**Hereby Decide**

**Chapter**

**General Provisions**

**Article 1:**

This Sub-Decree aims to manage and promote the safe and highly effective use of digital signatures in the Kingdom of Cambodia.

**Article 2:**

The purposes of this Sub-Decree are to identify:

- The principles of digital signatures and competent authorities
- The issuance, alteration, suspension, termination and revocation of a digital signature certification license
- Certification of digital signature
- The obligations of the Certificate Authority and
- The obligations of the Owner of Digital Signature Certificate.

**Article 3:**

This Sub-Decree has its scope covering the transactions relating to digital signatures in the Kingdom of Cambodia.

**Article 4:**

The terms used in this Sub-Decree shall have the following meanings:

**Owner of Digital Signature Certificate** refers to a person who receives a Digital Signature Certificate from the Certificate Authority.

**Digital Signature Creating Key/Private Key** refers to codes in the computer system used for creating a digital signature.

**Digital Signature Verifying Key/Public Key** refers to codes in the computer system used for authenticating a digital signature.

**Data** refers to a text, image, audio, video or other marks which are created, used and saved in the computer system.

**Computer System** refers to electronic devices whether standalone or assembly of connected electronic devices or related automatic data processing devices including all types of devices which are capable to process data, including but not limited to computer, tablets and phones.

**Written Paper** refers to the letters in paper form which bear or are required to bear a signature or thumbprint, signature or thumbprint and name, signature or thumbprint and seal, name and seal, or signature or thumbprint, name and seal.

**Digital Signature Certificate** refers to the records in a computer system issued by the Certificate Authority to identify the owner of digital signature certificate who is the owner of digital signature verifying key/public key.

**Certificate Authority** refers to a legal entity which certifies a digital signature.

**Certification of Digital Signature** refers to the issuance of a digital signature certificate.

**Electronic Message** refers to the information which is created, transmitted, received or stored in electronic form in the computer system.

**Digital Signature** refers to the data attached to the electronic message to identify a digital signer and verify the original status of the electronic message signed by the digital signer.

**Public Key Infrastructure** refers to an infrastructure which is equipped with technical mechanisms and equipment, staff, policies, and procedures to safeguard the security and safety for management and utilization of a digital signature.

**License of Digital Signature Certification** refers to a license issued by the Ministry of Posts and Telecommunications to assign any legal entity as Certificate Authority.

## **Chapter 2**

### **Competent Institutions**

#### **Article 5:**

The Ministry of Posts and Telecommunications (MPTC) is an institution which is competent to manage digital signatures.

The General Department of Information and Communication Technology (GDICT) is MPTC's chief of staff for managing, issuing, inspecting and monitoring the implementation of licenses of digital signature certification according to this Sub-Decree and other related provisions.

#### **Article 6:**

MPTC shall determinate the technical standards and principles to enhance the safety and effectiveness of managing and utilizing digital signatures including:

- A- The standards and architecture of public key infrastructure
- B- The guidelines of setting up and installing public key infrastructure and utilizing digital signature.

#### **Article 7:**

GDICT shall develop and retain a list of licenses of digital signature certification by recording and verifying some information including the identity of a Certificate Authority, date of license, and technical requirements of a digital signature, authorization to do business and list of appendix.

#### **Article 8:**

GDICT shall publicly disclose the name of all Certificate Authorities in the Kingdom of Cambodia and the name of foreign Certificate Authorities accredited by the Kingdom of Cambodia.

## **Chapter 3**

### **Principle of Digital Signature**

**Article 9:**

To be regarded as a digital signature shall satisfy the following requirements:

- A- Confirm the accurate and specific identity of a digital signer.
- B- Confirm the original status of electronic message.
- C- Confirm the time and date of affixing a digital signature.
- D- Other items defined by MPTC.

**Article 10:**

Any electronic message attached with a digital signature issued by the Certificate Authority shall have the same legal effect to the written paper.

**Article 11:**

Every online financial transaction shall use a digital signature as set out in the Sub-Decree except for other related provisions jointly announced by the Ministry of Economy and Finance, the Ministry of Posts and Telecommunications and the National Bank of Cambodia.

**Article 12:**

Others' digital signature creating key shall be strictly prohibited.

Any retention or use of others' digital signature creating key shall be strictly prohibited without the written permission of the Owner of Digital Signature Certificate.

**Article 13:**

Any digital signature certificate issued by a foreign Certificate Authority shall be accredited according to the requirements of this Sub-Decree and other related provisions in the following cases:

- A- According to the approval of MPTC or
- B- According to the international accreditation agreements with the Kingdom of Cambodia.

**Chapter 4**

**License of Digital Signature Certification**

**Section 1**

**Issuance of Licenses of Digital Signature Certification**

**Article 14:**

No one may claim themselves as Certificate Authority unless they receive the license of digital signature certification from GDICT after approved by MPTC Minister as set out in this Sub-Decree and other related provisions.

**Article 15:**

Any person who intends to apply for a license of digital signature certification shall have technical skills, financial resources, ITC equipment and other qualifications and pay a deposit for guaranteeing business as defined by MPTC.

**Article 16:**

A license of digital signature certification shall be valid for 10 (ten) years as of the issuing date.

It may be renewed according to GDICT's decision after approved by MPTC Minister.

**Article 17:**

Any person who intends to apply for a license of digital signature certification shall apply to the GDICT.

The requirements and procedures of application and renewal of a license of digital signature certification shall be set out by the Prakas of MPTC.

**Section 2:**

**Contract-Based Transfer, Succession or Merger of Company and Termination of Digital Signature Certification**

**Article 18:**

The contract-based transfer, succession or merger of company or termination of digital signature certification shall be set out in the Sub-Decree and other related provisions.

**Article 19:**

In case the Certificate Authority intends to terminate the digital signature certification, the person shall:

- A- Inform the GDICT in writing at least 03 (three) months before termination by specifying the reasons for termination and being signed by the Certificate Authority.
- B- Inform the users of their services earlier at least 03 (three) months before termination.
- C- Transfer digital signature certificates and record all the digital signature certificate issued by other Certificate Authority.

The MPTC shall determine the forms and procedures of notification about the termination of digital signature certification.

**Article 20:**

The contract-based transfer, succession or merger of company or termination of digital signature certification shall be approved first by the GDICT according to MPTC's requirements.

The requirements and procedures of contract-based transfer, succession or merger of company or termination of digital signature certification shall be set out by the Prakas of MPTC.

### **Section 3:**

#### **Revocation of Digital Signature Certification License**

##### **Article 21:**

A license of digital signature certification shall be revoked in any of the following cases:

- A- The Certificate Authority is subjected to criminal punishment.
- B- The Certificate Authority is liquidated or dissolved.
- C- The Certificate Authority has forfeited a digital signature certificate.
- D- The Certificate Authority's activities post a threat to public order, security or national defense.
- E- Fake information or documents are provided by the Certificate Authority to the GDICT.
- F- The transfer of a contract, succession, merger of a company or termination of digital signature certification are conducted without following the requirements and procedures as set out in this Sub-Decree and other related provisions.
- G- Others as determined by the MPTC.

The decision on the revocation of a digital signature certification license shall be made publicly available. The procedures for the revocation of digital signature certification license shall be set out by the Prakas of the MPTC.

##### **Article 22:**

In case a license of digital signature certification is revoked, the Certificate Authority will notify the owner of digital signature certificate and transfer the digital signature certificate to other certificate authority according to the agreement or requirements as set out by the MPTC.

The MPTC shall determine the formalities and procedures of transferring a digital signature certificate in case the license of digital signature certification is revoked.

### **Section 4:**

#### **Fees of Digital Signature Certification License**

##### **Article 23:**

An applicant of digital signature certification license or Certificate Authority shall pay application fees, renewal fees, contract-based transfer fees, fees of succession or merger of a

company, fees relating to the digital signature certification license and other fees as set out by the Joint Prakas made by the MPTC and the Ministry of Economy and Finance.

## **Chapter 5**

### **Certificate of Digital Signature**

#### **Article 24:**

The Certificate Authority shall formulate the standards on the certification of digital signature in line with the provisions relating to the technical standards and principles on digital signatures as set out by the MPTC.

#### **Article 25:**

The Certificate Authority shall issue the certificate of digital signature to the applicant after meeting the requirements as defined by this Sub-Decree and other related provisions.

The Certificate Authority may suspend or terminate the use of the certificate of digital signature according to this Sub-Decree and other related provisions.

The MPTC shall determine the requirements and procedures of issuing, suspending and terminating the use of the certificate of digital signature.

#### **Article 26:**

The characteristics of the certificate of digital signature shall be defined as below:

- A- The identity of the owner of digital signature certificate
- B- The digital signature verifying key/public key of the certificate owner
- C- The description of the methods used to affix a digital signature on the certificate of digital signature.
- D- The ID number of digital signature certificate
- E- The validity period of digital signature certificate
- F- The identity of Certificate Authority
- G- The scope and purposes of using the digital signature certificate
- H- Other characteristics as set out by the MPTC.

## **Chapter 6:**

### **Obligations of Digital Signature Certificate Authority and Owners**

#### **Article 27:**

The Certificate Authority shall have the following obligations:

- A- Protect and safeguard the security and safety relating to the issuance of the certificate of digital signature and use of digital signature as set out by the MPTC and other related provisions.
- B- Don't store or own the digital signature verifying key/public key of the digital signature certificate owner except for the written agreement.

- C- Don't use or disclose the digital signature verifying key/public key of the digital signature certificate owner.
- D- Keep confidential the secret information of the digital signature certificate owner.
- E- Keep their digital signature verifying key/public key confidential and safe.
- F- Safely store and manage the records of issuing digital signature certificates within a period of ten years after the expiration of the digital signature certificate.
- G- Report immediately to the **GDICT** in case of interruption of a data processing system or tool, methods and certification system within a period of 24 (twenty-four) hours.
- H- Provide their digital signature certificate owner with the tools or means which allow a notification about the theft, loss or disclosure of digital signature creating key/private key.
- I- Provide a financial statement and non-financial information on a regular basis or upon the request of the **GDICT**.
- J- Other obligations as set out by this Sub-Decree and other related provisions.

**Article 28:**

The owner of digital signature certificate shall have the following obligations:

- A- Keep their digital signature creating key/private key confidential and safe.
- B- Notify the Certificate Authority immediately and the receiver of the data sent when the digital signature creating key/private is stolen, lost or disclosed.
- C- Other obligations as set out by this Sub-Decree and other related provisions.

**Chapter 7:**

**Settlement of Disputes**

**Article 30:**

Besides criminal offenses, all disputes arising out of the digital signature certificate, between the Certificate Authority and Certificate Authority, between the Certificate Authority and the owner shall be referred to the MPTC for resolution.

The requirements, formalities and procedures of settlement shall be set out by the MPTC. The fees for settling disputes shall be determined by the Joint Prakas of the MPTC and the Ministry of Economy and Finance.

**Chapter 8:**

**Penalties**



**Article 30:**

After issuing the license of digital signature certification, if the Certificate Authority is found violating any terms and conditions of the license or any requirements as set out by this Sub-Decree or other related provisions, the MPTC may take the following actions:

- A- Guide and instruct the Certificate Authority to meet the terms and conditions and additional requirements.
- B- Restrict the certificate of digital signature certification licenses.
- C- Suspend a license until the Certificate Authority satisfies the terms and conditions and additional requirements.

In case the Certificate Authority fails to implement the measures set out in the first paragraph above or violates the provisions of this Sub-Decree or other related provisions, the MPTC may take following actions:

- A- Suspend or terminate the work of CEO, director, management members or senior staff of the Certificate Authority.
- B- Select and empower the properly qualified staff to examine the activities of business or other related activities of the Certificate Authority. The person will report to the MPTC about the requirements as set out in the contract with the MPTC or
- C- Restrict or terminate specific or general activities of the Certificate Authority although those activities are carried out in accordance with or without confirming to the requirements of the license.

The PMTC may take the actions as provided in the first or second paragraph if a written prior notice is given to the Certificate Authority about the reasons for taking this action and an opportunity is given to the Certificate Authority to provide explanations.

**Article 31:**

The following persons shall be subject to transitional penalties applying to the transactions as stated in Article 14 of this Sub-Decree without the PMTC's license:

- Natural person: fines of 5,000,000 (five million) riel to 15,000,000 (fifteen million riel).
- Legal entity: fines of 50,000,000 (fifty million) riel to 150,000,000 (one hundred and fifty million riel).

**Article 32:**

The following persons who retain or use or others' digital signature creating key/private key without written approval of the owner of digital signature certificate shall be subject to the transitional penalties:

- Natural person: fines of 3,000,000 (three million) riel to 9,000,000 (nine million riel).

- Legal entity: fines of 25,000,000 (twenty five million) riel to 75,000,000 (seventy five million riel).

**Article 33:**

The following persons who disclose others' digital signature creating key/private key without written approval of the owner of digital signature certificate shall be subject to the transitional penalties:

- Natural person: fines of 3,000,000 (three million) riel to 9,000,000 (nine million riel).

- Legal entity: fines of 25,000,000 (twenty five million) riel to 75,000,000 (seventy five million riel).

**Article 34:**

The Certificate Authority who have carried out contract-based transfer, succession or merger of a company without the prior approval of the PMTC shall be subject to the transitional penalties of fines of 20,000,000 (twenty million) riel to 75,000,000 (seventy five million riel).

**Article 35:**

The Certificate Authority who fails to implement the obligations as stated in Article 28, Point F of this Sub-Decree shall be subject to the transitional penalties of fines of 10,000,000 (ten million) riel to 60,000,000 (sixty million riel).

**Article 36:**

The following persons who obstruct, fail to cooperate or impede the field inspection of digital signature certification licenses carried out by the official designated by the PMTC or the competent institutions shall be subject to the transitional penalties:

- Natural person: fines of 3,000,000 (three million) riel to 9,000,000 (nine million riel).

- Legal entity: fines of 10,000,000 (ten million) riel to 9,000,000 (nine million riel).

**Article 37:**

All the certificate authorities who fail to issue digital signature certificates or delay issuing digital signature certificates shall be subject to the transitional penalties of fines of 3,000,000 (three million) riel to 9,000,000 (nine million riel).

**Article 38:**

Transitional penalties shall be imposed by the PMTC.

**Article 39:**

Anyone who has violated the provisions as stipulated in Articles 31, 32, 33, 34, 35, 36, & 37 of this Sub-Decree shall be subject to the transitional fines within a period of 30 (thirty) days as of the date of receipt of the decision to impose fines.

In case any offender fails to pay the transitional fines as set out in the first paragraph above, the PMTC shall file the case to the prosecution at the Court of First Instance.

The forms of imposing fines and the management of the money from imposing fines shall be set out by the joint Prakas of the PMTC Minister and the Minister of Economy and Finance.

## **Chapter 9**

### **Final Provisions**

#### **Article 40:**

Any provisions contrary to this Sub-Decree shall be abrogated.

#### **Article 41:**

The Minister in charge of the Council of Ministers, Minister of Posts and Telecommunications, Minister of Economy and Finance, ministers of all ministries and directors of all institutions concerned shall take charge of executing this Sub-Decree according to their respective duties from the signing date onwards.

Friday 12<sup>th</sup> of 2<sup>nd</sup> Month of the Lunar Calendar, Year of the Rooster, 2561 BE

Phnom Penh, 29 December 2017

*[Signed & Sealed]*

**Prime Minister**

**Samdech Aka Moha Sena Padei Techo Hun Sen**

Has respectfully informed

Samdech Aka Moha Sena Padei Techo Hun Sen to sign

<b>Senior Minister &amp; Minister of Economy and Finance</b>  <i>[Signed]</i> <b>Aun Porn Moniroth</b>	<b>Minister of Posts and Telecommunications</b>  <i>[Signed]</i> <b>Tram Iv Tek</b>
---	--

#### **Places of Receipt:**

- Ministry of Royal Palace
- General Secretariat of Constitutional Council

- General Secretariat of Senate
- General Secretariat of National Assembly
- General Secretariat of Royal Government of Cambodia
- Prime Minister Hun Sen's Cabinet
- Samdech, H.E, Lok Chumteav, Deputy Prime Ministers' Cabinets
- As in Article 41
- Royal Gazette
- Archives- Chronicles