**LESOTHO DIGITAL SIGNATURE REULATIONS**

(*Note form Consultants: these provisions were extracted as is from the IT Bill 2005. These provisions are not all suitable to be included in Regulations but all provisions were retained from the IT Bill to reflect work done in 2005. The provisions only address the administration of digital signatures using PKI technology. Consultants are of the opinion that the Kingdom of Lesotho should keep in mind the infrastructure and associated costs in promulgating regulations for secure electronic signatures and the need to enact technologically neutral provisions.)*

## *Interpretation*

**1**. In these Regulations, unless the context otherwise requires:-

 “asymmetric cryptosystem” means a system capable of generating a secure key pair, consisting of a private key for creating a digital signature, and a public key to verify the digital signature;

“certification authority” means a person who or an organization that issues digital certificates *[and may provide other services related to electronic signatures]*;

“certification practice statement” means a statement issued by a certification authority to specify the practices that the certification authority employs in issuing digital certificates;

“Controller” means the Controller of Certification Authorities appointed under section 47 (1) and includes a Deputy or an Assistant Controller of Certification Authorities appointed under section 47 (2);

“correspond”, in relation to a private key or public key, means to belong to the same key pair;

“digital certificate” means a record issued for the purpose of supporting digital signatures which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair;

"digital signature" means an electronic signature consisting of a transformation of a electronic communication using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic communication and the signer’s public key can accurately determine -

1. whether the transformation was created using the private key that corresponds to the signer’s public key; and
2. whether the initial electronic communication has been altered since the transformation was made;

“hash function" means an algorithm mapping or translating one sequence of bits into another, generally smaller, set (the hash result) such that -

1. a electronic communicationyields the same hash result every time the algorithm is executed using the same record as input;
2. it is computationally infeasible that a record can be derived or reconstituted from the hash result produced by the algorithm; and
3. it is computationally infeasible that 2 electronic communications can be found that produce the same hash result using the algorithm;

“key pair”, in an asymmetric cryptosystem, means a private key and its mathematically related public key, having the property that the public key can verify a digital signature that the private key creates;

“licensed certification authority” means a certification authority licensed by the Controller pursuant to these Regulations;

"operational period of a digital certificate" begins on the date and time the digital certificate is issued by a certification authority (or on a later date and time if stated in the digital certificate), and ends on the date and time it expires as stated in the digital certificate or is earlier revoked or suspended;

"private key" means the key of a key pair used to create a digital signature;

public key" means the key of a key pair used to verify a digital signature;

public key" means the key of a key pair used to verify a digital signature;

“repository” means a system for storing and retrieving digital certificates or other information relevant to digital certificates;

“revoke a digital certificate” means to permanently end the operational period of a digital certificate from a specified time;

“subscriber” means a person who is the subject named or identified in a digital certificate issued to him and who holds a private key that corresponds to a public key listed in that digital certificate;

“suspend a digital certificate” means to temporarily suspend the operational period of a digital certificate from a specified time;

“trustworthy system” means computer hardware, software and procedures that -

1. are reasonably secure from intrusion and misuse;
2. provide a reasonable level of availability, reliability and correct operation;
3. are reasonably suited to performing their intended functions; and
4. adhere to generally accepted security procedures;

“valid digital certificate” means a digital certificate that a certification authority has issued and which the subscriber listed in it has accepted; and

"verify a digital signature" , in relation to a given digital signature, record and public key, means to determine accurately that -

1. the digital signature was created using the private key corresponding to the public key listed in the digital certificate; and
2. the electronic communication has not been altered since its digital signature was created.

## *Secure digital signature*

**2**. When any portion of an data message is signed with a digital signature, the digital signature shall be treated as a secure electronic signature with respect to such portion of the record, if -

1. the digital signature was created during the operational period of a valid digital certificate and is verified by reference to the public key listed in such digital certificate; and
2. the digital certificate is considered trustworthy, in that it is an accurate binding of a public key to a person’s identity because -

(i) the digital certificate was issued by a licensed certification authority operating in compliance with the regulations made under section 48 ;

(ii) the digital certificate was issued by a certification authority outside Kingdom of Lesotho recognised for this purpose by the Controller pursuant to regulations made under section 49;

(iii) the digital certificate was issued by a public body approved by the Minister to act as a certification authority on such conditions as he may by regulations impose or specify; or

(iv) the parties have expressly agreed between themselves (sender and recipient) to use digital signatures as a security procedure, and the digital signature was properly verified by reference to the sender’s public key.

## *Presumptions regarding digital certificates*

**3**. It shall be presumed, unless evidence to the contrary is adduced, that the information (except for information identified as subscriber information which has not been verified) listed in a digital certificate issued by a licensed certification authority is correct if the digital certificate was accepted by the subscriber.

## *Unreliable digital signatures*

**4**. Unless otherwise provided by law or contract, a person relying on a digitally signed data message assumes the risk that the digital signature is invalid as a signature or authentication of the signed data message, if reliance on the digital signature is not reasonable under the circumstances having regard to the following factors-

1. facts which the person relying on the digitally signed data message knows or has notice of, including all facts listed in the digital certificate or incorporated in it by reference;
2. the value or importance of the digitally signed data message, if known;
3. the course of dealing between the person relying on the digitally signed data message and the subscriber and any available indicia of reliability or unreliability apart from the digital signature; and
4. any usage of trade, particularly trade conducted by trustworthy systems or other electronic means.

# Duties of licensed certification authorities and subscribers

# General Duties Relating to Digital Signatures

## *Reliance on digital certificates foreseeable*

**5**. It is foreseeable that persons relying on a digital signature will also rely on a valid digital certificate containing the public key by which the digital signature can be verified.

## *Prerequisites to publication of digital certificate*

**6**. No person may publish a digital certificate or otherwise make it available to a person known by that person to be in a position to rely on the digital certificate or on a digital signature that is verifiable with reference to a public key listed in the digital certificate, if that person knows that -

1. the certification authority listed in the digital certificate has not issued it;
2. the subscriber listed in the digital certificate has not accepted it; or
3. the digital certificate has been suspended or revoked, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

# Duties of Certification Authorities

## *Trustworthy system*

**7**. A certification authority must utilise trustworthy systems in performing its services.

## *Disclosure*

**8**. (1) A certification authority shall disclose -

1. its digital certificate that contains the public key corresponding to the private key used by that certification authority to digitally sign another digital certificate (referred to in this section as a certification authority digital certificate);
2. any relevant certification practice statement;
3. notice of the revocation or suspension of its certification authority digital certificate; and
4. any other fact that materially and adversely affects either the reliability of a digital certificate that the authority has issued or the authority’s ability to perform its services.

(2) In the event of an occurrence that materially and adversely affects a certification authority’s trustworthy system or its certification authority digital certificate, the certification authority shall —

1. use reasonable efforts to notify any person who is known to be or foreseeably will be affected by that occurrence; or
2. act in accordance with procedures governing such an occurrence specified in its certification practice statement.

## *Issue of digital certificate*

**9**. (1) A certification authority may issue a digital certificate to a prospective subscriber only after the certification authority -

(a) has received a request for issuance from the prospective subscriber; and

(b) has —

(i) if it has a certification practice statement, complied with all of the practices and procedures set forth in such certification practice statement including procedures regarding identification of the prospective subscriber; or

(ii) in the absence of a certification practice statement, complied with the conditions in subsection (2).

(2) In the absence of a certification practice statement, the certification authority shall confirm by itself or through an authorised agent that -

1. the prospective subscriber is the person to be listed in the digital certificate to be issued;
2. if the prospective subscriber is acting through one or more agents, the subscriber authorised the agent to have custody of the subscriber’s private key and to request issuance of a digital certificate listing the corresponding public key;
3. the information in the digital certificate to be issued is accurate;
4. the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the digital certificate;
5. the prospective subscriber holds a private key capable of creating a digital signature; and
6. the public key to be listed in the digital certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber.

(3) The requirements of subsection (2) shall not be waived or disclaimed by the certification authority, the subscriber, or both.

## *Representations upon issuance of digital certificate*

**10**. (1) By issuing a digital digital certificate, a certification authority represents to any person who reasonably relies on the digital certificate or a digital signature verifiable by the public key listed in the digital certificate that the certification authority has issued the digital certificate in accordance with any applicable certification practice statement incorporated by reference in the digital certificate, or of which the relying person has notice.

(2) In the absence of such certification practice statement, the certification authority represents that it has confirmed that -

1. the certification authority has complied with all applicable requirements of this Act in issuing the digital certificate, and if the certification authority has published the digital certificate or otherwise made it available to such relying person, that the subscriber listed in the digital certificate has accepted it;
2. the subscriber identified in the digital certificate holds the private key corresponding to the public key listed in the digital certificate;
3. the subscriber’s public key and private key constitute a functioning key pair;
4. all information in the digital certificate is accurate, unless the certification authority has stated in the digital certificate or incorporated by reference in the digital certificate a statement that the accuracy of specified information is not confirmed; and
5. the certification authority has no knowledge of any material fact which if it had been included in the digital certificate would adversely affect the reliability of the representations in paragraphs (a) to (d).

(3) Where there is an applicable certification practice statement which has been incorporated by reference in the digital certificate, or of which the relying person has notice, subsection (2) shall apply to the extent that the representations are not inconsistent with the certification practice statement.

## *Suspension of digital certificate*

**11**. Unless the certification authority and the subscriber agree otherwise, the certification authority that issued a digital certificate shall suspend the digital certificate as soon as possible after receiving a request by a person whom the certification authority reasonably believes to be -

1. the subscriber listed in the digital certificate;
2. a person duly authorised to act for that subscriber; or
3. a person acting on behalf of that subscriber, who is unavailable.

## *Revocation of digital certificate*

**12**. A certification authority shall revoke a digital certificate that it issued -

1. after receiving a request for revocation by the subscriber named in the digital certificate; and confirming that the person requesting the revocation is the subscriber, or is an agent of the subscriber with authority to request the revocation;
2. after receiving a certified copy of the subscriber’s death certificate, or upon confirming by other evidence that the subscriber is dead; or
3. upon presentation of documents effecting a dissolution of the subscriber, or upon confirming by other evidence that the subscriber has been dissolved or has ceased to exist.

## *Revocation without subscriber’s consent*

**13**. (1) A certification authority shall revoke a digital certificate, regardless of whether the subscriber listed in the digital certificate consents, if the certification authority confirms that -

1. a material fact represented in the digital certificate is false;
2. a requirement for issuance of the digital certificate was not satisfied;
3. the certification authority’s private key or trustworthy system was compromised in a manner materially affecting the digital certificate’s reliability;
4. an individual subscriber is dead; or
5. a subscriber has been dissolved, wound-up or otherwise ceased to exist.

(2) Upon effecting such a revocation, other than under subsection (1) (d) or (e), the certification authority shall immediately notify the subscriber listed in the revoked digital certificate.

## *Notice of suspension*

**14**. (1) Immediately upon suspension of a digital certificate by a certification authority, the certification authority shall publish a signed notice of the suspension in the repository specified in the digital certificate for publication of notice of suspension.

(2) Where one or more repositories are specified, the certification authority shall publish signed notices of the suspension in all such repositories.

## *Notice of revocation*

**15**. (1) Immediately upon revocation of a digital certificate by a certification authority, the certification authority shall publish a signed notice of the revocation in the repository specified in the digital certificate for publication of notice of revocation.

(2) Where one or more repositories are specified, the certification authority shall publish signed notices of the revocation in all such repositories.

# Duties of Subscribers

## *Generating key pair*

**16**. (1) If the subscriber generates the key pair whose public key is to be listed in a digital certificate issued by a certification authority and accepted by the subscriber, the subscriber shall generate that key pair using a trustworthy system.

(2) This section shall not apply to a subscriber who generates the key pair using a system approved by the certification authority.

## *Obtaining digital certificate*

**17**. All material representations made by the subscriber to a certification authority for purposes of obtaining a digital certificate, including all information known to the subscriber and represented in the digital certificate, shall be accurate and complete to the best of the subscriber’s knowledge and belief, regardless of whether such representations are confirmed by the certification authority.

## *Acceptance of digital certificate*

**18.** (1) A subscriber shall be deemed to have accepted a digital certificate if he or she -

1. publishes or authorises the publication of a digital certificate -

(i) to one or more persons; or

(ii) in a repository; or

1. otherwise demonstrates approval of a digital certificate while knowing or having notice of its contents.

(2) By accepting a digital certificate issued by himself or a certification authority, the subscriber listed in the digital certificate certifies to all who reasonably rely on the information contained in the digital certificate that -

1. the subscriber rightfully holds the private key corresponding to the public key listed in the digital certificate;
2. all representations made by the subscriber to the certification authority and material to the information listed in the digital certificate are true; and
3. all information in the digital certificate that is within the knowledge of the subscriber is true.

## *Control of private key*

**19**. (1) By accepting a digital certificate issued by a certification authority, the subscriber identified in the digital certificate assumes a duty to exercise reasonable care to retain control of the private key corresponding to the public key listed in such digital certificate and prevent its disclosure to a person not authorised to create the subscriber’s digital signature.

(2) Such duty shall continue during the operational period of the digital certificate and during any period of suspension of the digital certificate.

## *Initiating suspension or revocation of digital certificate*

**20**. A subscriber who has accepted a digital certificate shall as soon as possible request the issuing certification authority to suspend or revoke the digital certificate if the private key corresponding to the public key listed in the digital certificate has been compromised.

# Offences

## *Publication for fraudulent or unlawful purpose*

**21**. Any person who knowingly creates, publishes or otherwise makes available a digital certificate for any fraudulent or unlawful purpose shall be guilty of an offence and shall be liable on conviction to a fine not exceeding [*to be specified*] or to imprisonment for a term not exceeding [*to be specified*] years or to both.

## *False or unauthorised request*

**22**. Any person who knowingly misrepresents to a certification authority his identity or authorisation for the purpose of requesting for a digital certificate or for suspension or revocation of a digital certificate shall be guilty of an offence and shall be liable on conviction to a fine not exceeding [*to be specified*] or to imprisonment for a term not exceeding [*to be specified*] or to both.

## *Appointment of Controller and other officers*

**23**. (1) The Minister shall appoint a Controller of Certification Authorities for the purposes of this Act and, in particular, for the purposes of licensing, certifying, monitoring and overseeing the activities of certification authorities.

(2) The Controller may, after consultation with the Minister, appoint such number of Deputy and Assistant Controllers of Certification Authorities and officers as the Controller considers necessary to exercise and perform all or any of the powers and duties of the Controller under this Act or any regulations made thereunder.

(3) The Controller, the Deputy and Assistant Controllers and officers appointed by the Controller under subsection (2) shall exercise, discharge and perform the powers, duties and functions conferred on the Controller under this Act or any regulations made thereunder subject to such directions as may be issued by the Minister.

(4) The Controller shall maintain a publicly accessible database containing a certification authority disclosure record for each licensed certification authority which shall contain all the particulars required under the regulations made under this Act.

(5) In the application of the provisions of this Act to digital certificates issued by the Controller and digital signatures verified by reference to those digital certificates, the Controller shall be deemed to be a licensed certification authority.

(6) The Controller has the power to administer and enforce Parts V and VI of this Act and for this purpose the Controller has powers set out in Part XIV of this Act. For the purpose of Part XIV-

1. the Controller is a “relevant authority” in relation to certification authorities; and
2. certification authorities are the “relevant subjects” in relation to the Controller; and
3. Parts V and VI are the relevant parts of this Act in relation to the Controller’s authority under this Act.