S.I. 22 of 2018

ELECTRONIC TRANSACTIONS ACT

(Cap 263)

Electronic Transactions (Affixing Digital Signature) Regulations, 2018

Arrangement of Regulations

S.I. 22 of 2018

ELECTRONIC TRANSACTIONS ACT

(Cap 263)

Electronic Transactions (Affixing Digital Signature) Regulations, 2018

In exercise of the powers conferred by Section 9 of the Electronic Transactions Act, the Vice-President acting as the Minister for Information and Communications Technology hereby makes the following regulations—

Citation

1. These Regulations may be cited as the Electronic Transactions (Affixing Digital Signature) Regulations, 2018.

Interpretation

2. In these Regulations, unless the context otherwise requires —

"Act" means the Electronic Transactions Act;

"e-service" means an online version of a service publicly available on the Internet whereby all interactions are electronic in nature and a valid transaction is possible;

"printable format" means an electronic document format that can be reproduced on paper document and that is human readable;

"RFC 3161 Standards" means an Internet Engineering Task Force standards that describes the format of a request sent to a Time Stamp Authority and the response that is returned, including the establishment of several security relevant requirements for Time Stamp Authority operation, with regards to processing requests to generate responses;

"secure digital signature" means the digital signature produced and attached to the electronic document or record, which is made or certified using a digital signature certificate from a Certifying Authority which is secured and recognised by the Controller of Certifying Authority;

"Time Stamp" means the process of securely keeping track of the accurate creation and modification times of an electronic document;

"Time Stamp Protocol" means the cryptographic procedure for certifying time stamp using X.509 certificates and Public Key Infrastructure.

Electronic document

3. For the purpose of these regulations, the electronic version of a document shall be considered equivalent to the print version of the document if that document—

(a) contains the same data as the printed version; and

(b) is human readable by the following means —

(i) using a printable format which can be used to produce a printable version of the document and the printable version of the document shall allow identification and access to the corresponding or originating of the electronic version of the document by the following means —

(a) an alphanumeric reference entered into a software application or online e-service facility to access the electronic version; or

(b) a valid Uniform Resource Locator

entered in an internet browser to access the electronic version; or

(c) complementing one of the above options, provided in sub-paragraphs (i)(a) and (i)(b) with a bar-code, dot-code or Quick Response Code or other machine readable format that allows the automation of the assessing and reading of the reference to the electronic document; or

(ii) provides the person access to a software application or an online e-service facility that allows the display of the content of the electronic document and to have access to the information content of the document.

Digital signature certificate

4. A digital signature certificate shall represent unequivocally the digital identity of a natural or juridical person, and shall be considered as a recognised digital signature certificate, generating legally binding digital signature, which shall comply with the requirements provided in the Part VII of the Act and technical standards set out in Schedule 1.

Secure digital signature

5.(1) A secure digital signature shall comply with the following requirements—

(a) it is generated using a Public Key Infrastructure and the digital signature certificate, ensuring that it is—

(i) uniquely linked to the signatory;

(ii) capable of identifying the signatory;

(iii) created using means that the signatory can maintain under their sole control;

(iv) linked to the data of the electronic document or record to which it relates in such a manner that any subsequent change in the data is detectable.

(b) it is created in a manner that reasonably ensures the control and consent of the subscriber in the generation of the signature and in particular it shall be ensured that the subscriber is—

(i) aware of the contents of the electronic document being signed;

(ii) explicitly allow to use the Private Key linked to the digital certificate.

(2) A verifiable Time Stamp shall be included in the digitally signed electronic document stating the exact date and time when the digital signature is generated and the Time Stamp may be generated using—

(a) the standard protocols and formats defined in the RFC 3161 that is the Internet X.509 Public Key Infrastructure Time-Stamp Protocol and the Time Stamp Authority issuing the stamps is recognised by the Controller of Certifying Authority; or

(b) if a Time Stamp Protocol service is not available, the system time of the computer is used to generate the Time Stamp.

(3) The Controller of Certifying Authority may establish, in consultation with the Minister, administrative directive, to allow the mandatory usage of recognised Time Stamp for digital signature, using the RFC 3161 Standards.

Validation of a secure digital signature

6.(1) The validation of a Secure Digital Signature shall include the following checks—

(a) Integrity Validation, to ensure that the digital signature corresponds to the attached electronic document, has not suffered any modification since it was made;

(b) Certificate Chain Validation, to ensure that the certificate used in the generation of a signature was valid, at the time of the signature and that the time is the one represented in the Time Stamp attached to the signature, if available.

(2) The Validation Check of a signature shall provide the result in the following manner—

(a) by an invalid response indicating that either the signature format is incorrect or that the digital signature value fails the verification checks;

(b) by an incomplete validation response indicating that the format and digital signature verifications have not failed, but that there is insufficient information to determine if the electronic signature is valid;

(c) by a valid response which indicate that the signature has passed verification and it complies with the signature validation policy.

(3) The digital signature certificate used in the generation and verification of a secure digital signature shall be from a Certifying Authority recognised by the Controller of Certifying Authorities as provided in Part VII of the Act.

(4) A secure digital signature complying with the requirements specified in this document, shall be considered

legally binding and having the same validity as a manuscript signature.

Secure digitally signed document

7. For the purpose of these regulations, a secure digitally signed document is an electronic document that includes one or several digital signatures, which shall comply with the following requirements—

(a) that the electronic signature inserted in the document is a secured digital signature, as specified in regulation 5;

(b) that it extends to the properties of a digital document, as defined in these regulations, in such a way that—

(i) when the electronic document is displayed by a software application or online e-service, it provides the means to validate the signature of the document, including the verification that the certificates used for the signatures were valid at the time the signature was generated;

(ii) when the electronic document is printed, it provides means to retrieve the electronic version and verify the signatures.

(c) that a secure digitally signed document contains information required to validate the digital signature as provided in regulations 6(1) and (2).

Requirements for recognition of Certifying Authority

8.(1) The requirements for the recognition of digital certificate by the Certifying Authority shall be such as set out in Schedule 2.

(2) For the purpose of these regulations, a local or foreign Certifying Authority shall follow similar requirements provided in Schedule 2.

SCHEDULE 1

(Regulations 4)

For Digital Certificate to be recognised, the following established standards are required—

(1) that the Digital Certificate used is compliant to the International Telecommunication Union-T Standard X-509, in particular it includes a unique serial number and sufficient information to validate the certificate including the issuance of the expiry date, time and revocation checking information;

(2) that the Encryption Algorithm used is Rivest Shamir Alderman compliant, with a key length of at least 2048 bits, and not greater than the key length of the issuing Recognised Certifying Authority; and

(3) that the Hashing Algorithm is a Secure Hashing Algorithm -2 or higher or otherwise an algorithm or system expressly recognised by the Controller of Certifying Authority.

SCHEDULE 2

(Regulations 8)

Requirements for recognition of digital certificate by the Certifying Authority are as follows—

(1) that the certificate issued complies with the technical specifications provided in Schedule 1;

(2) that it is a valid Web-Trust or equivalent industry accreditation;

(3) that the Certifying Authority implements, after having a specific agreement with the Controller of Certifying Authority, a mechanism to securely export the database of issued certificate to the Controller of Certifying Authority or provide secure access to any pre-existing database as and when required;

(4) that the Electronic Transactions Act Compliance Questionnaire for Certifying Authority is completed by the subscriber and submitted to the Controller of Certifying Authority for verification; and

(5) that the Electronic Transactions Act Compliance Questionnaire is as set out below—

Government of the Republic of Seychelles

Department of Information and Communication Technology

Electronic Transactions Act Compliance Questionnaire for Certifying Authority (CA)

This assessment is based on the legal requirements applicable for a CA requesting a license to provide services related to digital certificates and electronic signatures in the Republic of Seychelles.
This questionnaire is complemented by the assessment on compliance of industry standards and best practices (e.g. WebTrust Criteria for CA), as stipulated in question number 8.

General instructions

- Please use Microsoft word or a compatible application to answer the questions, inserting your texts in the provided space below each question.

- You can complement your answers with annexes or other significant documents. It is recommended that you use Internet links to those documents, inserting the URL where appropriate. Please ensure that these links are active during the validity period of this document.

Important Notice

The information included in this questionnaire must be accurate and true. Intentional failure to this mandate is considered an offence according to applicable laws

Question 1
Art 6, 9 – If providing Software to implement Digital Signatures, describe the format used for the Digital Signatures generated. Indicate any standard used (i.e. XML-DSign, XAdES, PKCS#7, …).

Question 2
Art 11 - If providing services or solutions to implement electronic notifications based in Digital Certificates, describe who are the participating parties, the message flow and usage rules.

Question 3
Art 14 – Describe the security controls implemented to ensure that a Digital Signature fulfils the requirements of this article (i.e. Unique for the Signer, Able to Identify the Signer and Created in such a way that integrity and authenticity can be ensured). In particular, enumerate the supported encryption and hashing algorithms, and key lengths supported.

Question 4
Art 15 – Describe the controls implemented to ensure that the parties participating in digital signatures have the minimum capacitation to understand the act of an electronic transaction and digital signature. In particular describe any training or document helping the certific ate subscriber to have a basic understanding of the provided services (i.e. how to protect private keys, notify key compromises, etc.)

Question 5
Art 24 – Provide a link to a downloadable version of the Certification Practices Statement.

Question 6
Art 24 – Describe the security controls ensuring the identity of a subscriber (or authorized person) requesting a digital certificate

Question 7
Art 29-a – Describe the overall approach to Security Management, specifically it is requested to provide these documents (or links to downloadable documents): Security Policy, Privacy Policy and Disaster Recovery Plan. Please state any existing accreditation (ISO 27000, ITIL, etc).

Question 8
Art 29-b – Provide a document (or Link) with the auditor's report for the last (and valid at the moment of this application) compliance audit , understanding by "compliance" the fulfilment of WebTrust, ETSI-TS or other recognized criteria. If the CA didn't obtained a previous accreditation and requested an ad-hoc audit from the Government of Seychelles, the report of this audit should be provided.

Question 9
Art 29-c – Indicate the Standards implemented or fulfilled by the CA. In particular, estate the security standards affecting the PKI infrastructure (i.e. security level for the HSM protecting CA's private key) and end-entity protection (i.e. if providing cryptographic tokens or smart-cards to end users, estate the security standards implemented).

Question 10
Art 30 – Specify the profiles of the persons intervening in the PKI, including information on the recruiting processes that ensure the capacitation and reliance of these persons.

Question 11
Art 33-a – Describe the certificate publication services and policies (i.e. if the CA provides a public repository to publish and retrieve certificates, describe the characteristics of this repository, access rules, etc).

Question 12
Art 33-b – Indicate the CPS publication service and policies (i.e. where is the CPS available and who maintains the document)

Question 13
Art 33-c – Describe how you communicate any security threat compromising the service provided to your customers