GOVERNMENT GAZETTE

OF THE

REPUBLIC OF NAMIBIA

N$8.00 WINDHOEK - 20 December 2024 No. 8541

CONTENTS

Page

General Notice

COMMUNICATIONS REGULATORY AUTHORITY OF NAMIBIA

No. 837 2024

NOTICE OF INTENTION TO MAKE ELECTRONIC SIGNATURE REGULATIONS: ELECTRONIC TRANSACTIONS ACT, 2019

The Communications Regulatory Authority of Namibia, as instructed by the Minister of Information and Communication Technologies under section 58(3) of the Electronic Transactions Act, 2019 (Act No. 4 of 2019) to conduct a rule-making procedure in terms of the Communications Act, 2009 (Act No. 8 of 2009) read with the Regulations regarding Rule-Making Procedures published under General Notice No. 334 of 17 December 2010 −

(a) publishes this Notice of Intention by the Minister to make Electronic Signature Regulations as set out in Schedule 2; and

(b) provides the concise statement of the reasons and purpose for the proposed regulations set out in Schedule 1.

The Authority invites the providers of services and the public to submit comments in writing to the Authority on or before 30 January 2025, and a written comment must −

(a) contain the name and contact details of the person making the written submissions and the name and contact details of the person or entity on whose behalf the written submissions are made, if different;

(b) be clear and concise; and

(c) be sent or delivered −

(i) by hand to the head office of CRAN, Communications House, 56 Robert Mugabe Avenue, Windhoek;

(ii) by post to CRAN, Private Bag 13309, Windhoek, Namibia; or

(iii) by electronic mail to CRAN email address: legal@cran.na.

In terms of regulation 7 of the Regulations regarding Rule-Making Procedures the Authority herewith gives notice that it will hold a hearing regarding the proposed regulations as follow:

DATE: 31 January 2024
TIME: 08h00 to 13h00
VENUE: Droombos Country lodge

The public is invited to make comments or oral submissions at the hearing. Notice of oral submissions to be made during the hearing must be submitted to the Authority not later than 10 days before the date of the hearing. Such written notice must be accompanied by a concise statement setting out the basis and rationale for the oral submissions.

Oral submissions made at the aforesaid public hearing must −

(a) contain the name and contact details of the person making the written submissions and the name and contact details of the person or entity on whose behalf the written submissions are made, if different;

(b) be clear and concise.

The aforesaid notice of oral submissions must be sent or submitted to the Authority in the manner provided above.

T. MUFETI
CHAIRPERSON
COMMUNICATIONS REGULATORY AUTHORITY OF NAMIBIA

SCHEDULE 1

CONCISE STATEMENT OF PURPOSE

The purpose of the rule-making procedure is for the Authority to comply with the instruction of the Minister made under section 58(3) of the Electronic Transactions Act, 2019 to conduct the rule-making procedure in terms of the Communications Act –

(a) to introduce to the public the proposed regulations that will introduce an advanced electronic signature and govern and protect the process for the use of electronic signatures as provided for in section 20 of the Electronic Transactions Act, 2019; and

(b) ensure that the proposed regulations are in line with the enabling legislation, the Electronic Transactions Act, 2019 and that it covers all other necessary concerns for the services providers and the public.

SCHEDULE 2

GOVERNEMENT NOTICE

MINISTRY OF INFORMATION AND COMMUNICATION TECHNOLOGY

No. 2024

ELECTRONIC SIGNATURE REGULATIONS:
ELECTRONIC TRANSACTIONS ACT, 2019

Under section 20 of the Electronic Transactions Act, 2019 (Act No. 4 of 2019) read with section 58 of that Act I have –

(a) after having instructed the Communications Regulatory Authority of Namibia under subsection (3) of that section 58 to conduct a rule-making procedure in terms of the Communications Act, 2009 (Act No. 8 of 2009) and the Regulations Regarding Rule-Making Procedures published under General Notice No. 334 of 17 December 2010 as amended by General Notice No. 554 of 14 October 2021; and

(b) after the Authority having completed the rule-making procedure referred to in paragraph (a),

made the regulations set out in the Schedule.

E. THEOFELUS
MINISTER OF INFORMATION AND
COMMUNICATION TECHNOLOGIES

SCHEDULE

ARRANGEMENT OF REGULATIONS

Definitions

1. In these regulations a word or phrase to which a meaning has been assigned in the Act has that meaning, and unless the context otherwise indicates –

"certification service" means a security service referred to in section 41 of the Act, and includes the service of −

(a) issuing subscriber certificates necessary for giving advanced electronic signatures to subscribers;

(b) enabling the verification of advanced electronic signatures created on the basis of subscriber certificates;

(c) implementing procedures for suspension and revocation of subscriber certificates;

(d) checking the revocation status of the subscriber certificates and advising the relying parties; and

(e) issuing cross-pair certificates;

"certification service provider" means a person accredited under regulation 4 of the Regulations Regarding Accreditation of Security Products and Certification Service Providers published under General Notice No…to provide certification service and manage and issue subscriber certificates and public keys;

"recognised electronic signature" means an advanced electronic signature complying with the requirements set out in regulation 7;

"relying party" means a person that may act on the basis of a digital certificate or an electronic signature;

"signature creation data", in the context of electronic signatures which are not digital signatures, means data intended to designate those secret keys, codes or other elements which, in the process of creating an electronic signature, are used to provide a secure link between the resulting electronic signature and the person of the signer;

"signer" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;

"subscriber" means a person who is the subject named or identified in a subscriber certificate issued to that person and who holds a private key that corresponds to a public key listed in that certificate, and a signer has a corresponding meaning;

"subscriber certificate" means a digital record issued to a subscriber by a certification service provider for the purpose of supporting electronic signatures which purports to confirm the identity or other significant characteristics of the person who holds a particular keypair;

"the Act" means the Electronic Transactions Act, 2019 (Act No. 4 of 2019).

Electronic signatures

2. (1) In terms of section 20 of the Act a reference in any law, contract or any other legal instrument to a signature or the signing of a document is construed to include a reference to a recognised electronic signature, unless -

(a) a contrary intention appears from the law or document concerned;

(b) the law in question provides for a process that is incompatible with the use of an electronic signature;

(c) the law in question is not construed in such a manner that a reference to the writing in question is construed to include a data message as contemplated in section 19 of the Act.

(2) Subsection (2) of section 20 of the Act provides that nothing in that section is construed as limiting the use of an electronic signature that is not a recognised electronic signature if parties agree to such use or if a law provides for such use.

(3) A legally valid electronic signature must –

(a) be a positive act of acceptance, visible and clear;

(b) identify the signer; and

(c) be verifiable.

(4) The basic electronic signatures that need positive act requirements and supporting evidence are such as:

(a) *Electronic signatures:* Data attached to, incorporated in, or logically associated with other data, which is intended by the signer to serve as a signature, and include digitised and digital signatures;

(b) *Digitised signature:* Digital reproduction of a handwritten signature, e.g. faxed signature, a picture of a signature or a signature capture tablet;

(c) *Biometric signature:* General description of an electronic signature made with a biometric (body measurement such as a fingerprint, retina scans, iris scans, finger vein scans, facial recognition, voice recognition, hand geometry and even earlobe geometry) as an act of authentication or acceptance.

(d) *One Time:* A one-time password token (OTP token) is a security device or software program that produces new single-use passwords or passcodes at preset time intervals, and in both software and hardware versions, password tokens are programmed for a time interval upon which the old password expires and a new one is created.

(5) The basic electronic signatures mentioned in subregulation (4) do not use a public or private key encryption process to ensure integrity.

(6) Digital signatures and advanced electronic signatures are server based and use a public or private key encryption process to ensure integrity.

(7) Digital signatures that need positive act requirements with the verifiable integrity of evidence are, but not limited to −

(a) *Windows wallet:* A window wallet is a mobile payment and digital wallet service that lets users make payments and store loyalty cards on certain devices such as mobile phones; and

(b) *Smartcard:* A smart card is a security token that has an embedded chip, so a smart card connects to a reader either by direct physical contact (chip and dip) or through a short-range wireless connectivity standard such as Near Field Communication (NFC).

Use of electronic signatures

3. (1) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if –

(a) a method is used to identify the person and to indicate his or her approval of the information communicated; and

(b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.

(2) Where an electronic signature is not required by the parties to an electronic transaction, an expression of intent or other statement is not invalid merely on the grounds that −

(a) it is in the form of a data message; or

(b) it is not evidenced by an electronic signature but is evidenced by other means from which the intent or other statement of such person can be inferred.

(3) Where an electronic signature is used as a valid signature, that signature is treated as a valid electronic signature and to have been applied properly, unless the contrary is proved.

Advanced electronic signatures

4. (1) An advanced electronic signature is in terms of section 1 of the Act an electronic signature which is designed so that together with a security procedure it is possible to verify that the signature −

(a) is unique to the signer for the purpose for which it is used;

(b) can be used to identify objectively the signer of the data message;

(c) was created and affixed to the data message by the signer or using a means under the sole control of the signer; or

(d) was created and is linked to the data message to which it relates in a manner such that any changes in the data message can be detected.

(2) For an electronic signature to be classified as an advanced electronic signature, it must be a positive act with verifiable integrity and face-to-face (F2F) certification by the certification service provider.

(3) There are identity-confirming credentials from three separate categories of authentication factors that classically falling into three categories, but not limited to −

(a) knowledge factors that include things a user must know in order to log in: Usernames, IDs, passwords and personal identification numbers (PINs) all fall into this category;

(b) possession factors that include anything a user must have in his or her possession to log in, and this category includes one-time password tokens (OTP tokens), key fobs, smartphones with OTP apps, employee ID cards, SIM cards and any other qualifying possession factor that passes accepted international technical standards; and

(c) inherence factors that include any biological traits the user has that are confirmed for login, this category includes the scope of biometrics such as retina scans, iris scans, fingerprint scans, finger vein scans, facial recognition, voice recognition, hand geometry and even earlobe geometry.

(4) An advanced electronic signature is an electronic signature created with a subscriber certificate issued by a certification service provider after following a face-to-face identification process with the signer.

(5) An electronic signature must −

(a) identify the signer;

(a) be identified as an advanced electronic signature;

(c) detect any subsequent alteration or corruption of the signed data message or document legal framework for electronic signatures; and

(d) use a three-factor contemplated in subregulation (3) or equivalent signing mechanism so as to ensure the highest reliability of the signature.

Use of advanced electronic signatures

5. (1) Where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met if an advanced electronic signature is used.

(2) Subject to subregulation (1), an advanced electronic signature is not without legal force and effect merely on the grounds that it is in electronic form.

(3) Where an advanced electronic signature has been used, such signature is regarded as reliable and valid in law and to have been applied properly, unless the contrary is proved.

Equal treatment of signature technologies

6. Nothing in these regulations is applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in regulation 7, or otherwise meets the requirements of these regulations.

Requirements for recognised electronic signature

7. (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Subregulation (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in subregulation (1) if −

(a) the signature creation data is within the context in which it used, linked to the signer and to no other person;

(b) at the time of signing, the signature creation data was under the control of the signer and of no other person;

(c) any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(4) Subregulation (3) does not limit the ability of a person −

(a) to establish in any other way, for the purpose of satisfying the requirement referred to in subregulation (1), the reliability of an electronic signature; or

(b) to adduce evidence of the non-reliability of an electronic signature.

Satisfaction of electronic signature requirements

8. (1) The Authority must determine which electronic signatures satisfy the requirements of regulation 7.

(2) Where a recognised electronic signature is or has been used, such signature is regarded as a valid electronic signature and to have been applied properly, unless the contrary is proved.

(3) Any determination made under subregulation (1) must be consistent with recognized international standards.

Conduct of signer

9. (1) Where signature creation data is used to create a signature that has legal effect, each signer must −

(a) exercise reasonable care to avoid unauthorised access and use of its signature creation data;

(b) without undue delay, utilise means made available by the certification service provider pursuant to regulation 10, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signer to rely on or to provide services in support of the electronic signature if −

(i) the signer knows that the signature creation data have been compromised;

(ii) circumstances exist which are known to the signer to give rise to a substantial risk that the signature creation data may have been compromised;

(iii) the signer that is identified in the subscriber certificate had control of the signature creation data at the time when the certificate was issued;

(iv) that signature creation data was valid at or before the time when the subscriber certificate was issued;

(c) provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise −

(i) the method used to identify the signer;

(ii) any limitation on the purpose or value for which the signature creation data or the certificate may be used;

(iii) that the signature creation data are valid and have not been compromised;

(iv) any limitation on the scope or extent of liability stipulated by the certification service provider;

(v) whether means exist for the signer to give notice pursuant to paragraph (b);

(vi) whether a timely revocation service is offered;

(e) where services under paragraph (d)(v) are offered, provide a means for a signer to give notice pursuant to paragraph (b), and, where services under paragraph (d)(vi) are offered, ensure the availability of a timely revocation service;

(f) utilize trustworthy systems, procedures and human resources in performing its services.

(2) A signer bears the legal consequences of its failure to satisfy the requirements of subregulation (1).

Conduct of certification service providers

10. (1) Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, such certification service provider must −

(a) act in accordance with representations made by it with respect to its policies and practices;

(a) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the subscriber certificate throughout its life cycle or that are included in the certificate;

(c) provide reasonably accessible means that enable a relying party to ascertain from the subscriber certificate −

(i) the identity of the certification service provider;

(ii) that the signer that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;

(iii) that signature creation data were valid at or before the time when the certificate was issued;

(d) provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise −

(i) the method used to identify the signer;

(ii) any limitation on the purpose or value for which the signature creation data or the certificate may be used;

(iii) that the signature creation data are valid and have not been compromised;

(iv) any limitation on the scope or extent of liability stipulated by the certification service provider;

(v) whether means exist for the signer to give notice pursuant to paragraph (b);

(vi) whether a timely revocation service is offered;

(e) where services under paragraph (d)(v) are offered, provide a means for a signer to give notice pursuant to paragraph (b), and, where services under paragraph (d)(vi) are offered, ensure the availability of a timely revocation service; and

(f) utilise trustworthy systems, procedures and human resources in performing its services.

(2) A certification service provider bears the legal consequences of its failure to satisfy the requirements of subregulation (1).

Reliable and secure systems

11. For the purposes of regulation 10(1)(f) in determining whether, or to what extent, any systems, procedures and human resources utilised by a certification service provider are reliable and secure, regard may be had to the following factors −

(a) financial and human resources, including existence of assets;

(b) quality of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records and timelines;

(d) availability of information to signers identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the State or an accreditation authority regarding compliance with or existence of the foregoing; or

(g) any other relevant factor.

Conduct of relying party

12. A relying party must bear the legal consequences of its failure −

(a) to take reasonable steps to verify the reliability of an electronic signature; or

(b) where an electronic signature is supported by a subscriber certificate, to take reasonable steps −

(i) to verify the validity, suspension or revocation of the certificate; and

(ii) to observe any limitation with respect to the certificate.

Recognition of foreign certificates and electronic signatures

13. (1) In determining whether, or to what extent, a digital certificate or an electronic signature is legally effective, no regard may be had −

(a) to the geographic location where the certificate is issued or the electronic signature created or used; or

(b) to the geographic location of the place of business of the issuer or signer.

(2) A digital certificate issued outside Namibia has the same legal effect in Namibia as a digital certificate issued in Namibia if it offers a substantially equivalent level of reliability.

(3) An electronic signature created or used outside Namibia has the same legal effect in Namibia as an electronic signature created or used in Namibia if it offers a substantially equivalent level of reliability.

(4) In determining whether a digital certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of subregulation (2) or (3), regard must be had to recognised international standards and to any other relevant factors.

(5) Despite subregulations (2), (3) and (4), where parties agree, as between themselves, to the use of certain types of electronic signatures or digital certificates that agreement is recognised as sufficient for the purposes of cross-border recognition unless that agreement would not be valid or effective under applicable law.

———————