GOVERNMENT GAZETTE

OF THE

REPUBLIC OF NAMIBIA

N$8.00 WINDHOEK - 19 December 2025 No. 8814

CONTENTS

Page

Government Notice

MINISTRY OF INFORMATION AND COMMUNICATION TECHNOLOGY

No. 335 2025

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, after the Authority complied with 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 has completed the rule-making procedure referred to in paragraph (a),

made the regulations set out in the Schedule, which come into operation on the date of commencement of section 20 of the Act.

EMMA THEOFELUS
MINISTER OF INFORMATION AND
COMMUNICATION TECHNOLOGY

Windhoek, 27 November 2025

SCHEDULE

ARRANGEMENT OF REGULATIONS

Definitions

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

"Accreditation Regulations" means the Regulations Regarding Accreditation of Security Products and Services and Providers of Such Products and Services published under General Notice No. 953 of 17 December 2025;

"advanced electronic signature" means advanced electronic signature as defined in section 1 of the Act;

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

(a) issues the subscriber certificate necessary to give an advanced electronic signature to the subscriber;

(b) enables the verification of an advanced electronic signature created through the subscriber certificate;

(c) implements procedures for suspension and revocation of the subscriber certificate;

(d) confirms the revocation status of the subscriber certificate and advises the relying party; and

(e) issues a cross-pair certificate;

"certification service provider" means a person accredited under section 42 of the Act and regulation 6 of the Accreditation Regulations to provide certification service and to manage and issue the subscriber certificate and public key;

"international standards" includes the International Telecommunication Union - Telecommunication Standardization Sector, published in October 2019 (ITU-T X.509 (2019) and the Information Technology – Open Systems Interconnection, published in August 2020 (ISO/IEC 9594-8: 2020/Cor 2:2024);

"key pair", in an asymmetric cryptosystem, means a private key and its mathematically related public key which has a property that allows the public key to verify an electronic signature that the private key creates;

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

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

"recognised electronic signature" means an advanced electronic signature which complies with the requirements set out in section 1 of the Act and regulation 8;

"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 signer;

"signer" means a person that holds signature creation data and acts on their own behalf or on behalf of the person whom the signer 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;

"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); and

"timely revocation service" means a revocation service executed within 14 days of the date agreed upon between a subscriber and a certification service provider as contemplated in regulation 10(1)(c)(vi) and 11(1)(c)(vi).

(2) The international standards referred to in subregulation (1) are available for inspection –

(a) at the offices of the Authority, Windhoek, Freedom Plaza, Corner of Fidel Castro and Rev. Michael Scott Street, Courtside Building, 3rd and 4th floor, during office hours; and

(b) on the official website of the Authority.

Validity of electronic signature

2. (1) An electronic signature is valid if the electronic signature –

(a) is a positive act of acceptance;

(b) is visible, clear or, where applicable, audible;

(c) identifies the signer;

(d) is verifiable; and

(e) is incapable of alteration by a person other than the signer, and if altered, such alteration is detectable.

Basic electronic signature

3. (1) A basic electronic signature must meet the positive act requirements with the verifiable integrity of evidence and be supported by evidence.

(2) For purposes of subregulation (1), a basic electronic signature includes –

(a) an electronic signature made up of –

(i) a sound;

(ii) a symbol; or

(iii) a process attached to, incorporated in, or logically associated with, other data,

which is intended by the signer to serve as a signature, and includes digitised and digital signatures;

(b) a digitised signature that is a digital reproduction of a handwritten signature, such as a faxed signature, a picture of a signature or a signature capture tablet;

(c) a biometric signature that is an electronic signature made with a biometric such as body measurement, a fingerprint, retina scan, iris scan, finger vein scan, facial recognition, voice recognition, hand geometry and even earlobe geometry as an act of authentication or acceptance;

(d) a one-time password token (OTP), which 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; and

(e) any other digital signature method that may become available from time to time.

Digital electronic signature

4. (1) Digital electronic signatures must meet the positive act requirements with the verifiable integrity of evidence.

(2) For purposes of subregulation (1), a digital electronic signature includes a –

(a) windows wallet which is a mobile payment and digital wallet service that allows a user to make payments and store loyalty cards on certain devices such as mobile phones; and

(b) smart card which is a security token that has an embedded chip and 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 signature

5. (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 approval of the information communicated to such person; and

(b) having regard to all the relevant circumstances at the time the method is 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 referred to in regulation 2, that signature is treated as a valid electronic signature and to have been applied properly, unless the contrary is proved.

Identity-confirming credentials of advanced electronic signature

6. (1) When the identity of an advanced electronic signature is verified, there are generally identity-confirming credentials from three separate categories of authentication factors which are, but not limited to –

(a) knowledge factors that include things a user must know in order to log in, such as –

(i) a username;

(ii) an identity document;

(iii) a password; or

(iv) a personal identification number (PIN);

(b) possession factors that include anything a user must have in his or her possession to log in such as –

(i) a one-time password tokens (OTP tokens);

(ii) key fobs;

(iii) a smartphone with OTP apps;

(iv) employee identity documents;

(v) a SIM card; or

(vi) any other qualifying possession factor that passes international standards;

(c) inherent factors that include any biological traits the user has that are confirmed for login under the scope of biometrics such as –

(i) a retina scan;

(ii) an iris scan;

(iii) a fingerprint scan;

(iv) a finger vein scan;

(v) facial recognition;

(vi) voice recognition;

(vii) hand geometry; and

(viii) earlobe geometry.

Use and validity of advanced electronic signature

7. (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) When an advanced electronic signature referred to in subregulation (1) is used, such signature is regarded as reliable and valid in law and to have been applied properly, unless the contrary is proved.

Requirements for recognised electronic signature

8. (1) Subject to regulation 9, a recognised electronic signature is an advanced electronic signature that, apart from complying with the requirements of an advanced electronic signature under section 20(3) of the Act, is created with a subscriber certificate issued by a certification service provider after having followed an identification process and other security procedures with the signer as provided for in regulation 30 of the Accreditation Regulations.

(2) Where the law requires a recognised electronic signature of a person, that requirement is met in relation to a data message if the recognised electronic signature complies with the requirements in subregulation (4) and any relevant agreement.

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

(4) A recognised electronic signature is considered to be reliable for the purpose of satisfying the requirements referred to in section 20(3) of the Act if –

(a) the signature creation data is within the context in which it is 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 recognised electronic signature made after the time of signing, is detectable; and

(d) any alteration made to information relating to the electronic signature after the time of signing is detectable.

(5) Subregulation (4) 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 (2), the reliability of a recognised electronic signature; or

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

Equal treatment of signature technology

9. Nothing in these regulations is applied so as to exclude, restrict or deprive of legal effect of any method of creating an electronic signature that satisfies the requirements referred to in regulation 8 or otherwise meets the requirements of these regulations.

Conduct of signer

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

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

(b) without undue delay, utilise means made available by the certification service provider in accordance with regulation 11 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 has 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; or

(iv) the 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 is valid and has 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); or

(vi) whether a timely revocation service is offered;

(d) where service under paragraph (c)(v) is offered, provide a means for a signer to give notice in accordance with paragraph (b), and where a service under paragraph (c)(vi) is offered, ensure the availability of a timely revocation service; and

(e) use a trustworthy system, procedure and human resources in carrying out activities related to the use of an electronic signature to ensure the security and integrity of that signature.

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

Conduct of certification service provider

11. (1) If 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 the certification service provider in accordance with the policies and practices of such certification service provider;

(b) exercise reasonable care to ensure the accuracy and completeness of the material representations made by the certification service provider 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, 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 regulation 10(1)(b); and

(vi) whether a timely revocation service is offered;

(d) where services under paragraph (c)(v) are offered, provide a means for a signer to give notice in terms of regulation 10(1)(b), and where services under paragraph (c)(vi) are offered, ensure the availability of a timely revocation service; and

(e) utilise trustworthy systems, procedures and human resources in performing its services in accordance with regulation 13.

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

Conduct of relying party

12. A relying party must bear the 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 subscriber certificate; and

(ii) to observe any limitation applicable to the certificate.

Reliable and secure systems

13. (1) For purposes of this regulation "independent auditing body" means any registered auditing firm that is not part of the internal auditors of the certification service provider or the Authority.

(2) For the purposes of regulation 11(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, the following factors must be considered –

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

(b) quality of hardware and software systems;

(c) procedure for the application and the processing of a subscriber certificate;

(d) timelines for completion of the process referred to in paragraph (c);

(e) method of keeping records of documents or information which relate to the subscriber certificate;

(f) availability of information to a signer identified in a subscriber certificate and to a potential relying party;

(g) frequency and scope of audits conducted by an independent auditing body in respect of the systems, procedures and human resources of the certification service provider;

(h) the existence of a declaration by the Authority regarding compliance with or existence of the requirements under paragraph (a) to (g); and

(i) any other relevant factor.

Recognition of foreign digital certificate and foreign electronic signature

14. (1) In determining whether, or to what extent, a digital certificate or an electronic signature has legal effect, the following factors need not be considered –

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

(b) 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, the Authority determines that the digital certificate offers an equivalent level of reliability as a recognised electronic signature.

(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 only if it offers an equivalent level of reliability.

(4) In determining whether a digital certificate or an electronic signature offers an equivalent level of reliability for the purposes of subregulations (2) and (3), the Authority must consider international standards and 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 is not valid or effective under an applicable law.