GOVERNMENT GAZETTE

OF THE

REPUBLIC OF NAMIBIA

N$27.20 WINDHOEK - 17 December 2025 No. 8808

CONTENTS

Page

General Notice

COMMUNICATIONS REGULATORY AUTHORITY OF NAMIBIA

No. 953 2025

REGULATIONS REGARDING ACCREDITATION OF SECURITY PRODUCTS AND SERVICES AND PROVIDERS OF SUCH PRODUCTS AND SERVICES: ELECTRONIC TRANSACTIONS ACT, 2019

The Communications Regulatory Authority of Namibia under sections 47 read with sections 41 to 46 of the Electronic Transactions Act, 2019 (Act No. 4 of 2019) and after having followed the rule-making procedure in terms of 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, has –

(a) made the regulations set out in the Schedule; and

(b) determined that the regulations come into operation on a date determined by the Chairperson by notice in the *Gazette.*

T. MUFETI
CHAIRPERSON
COMMUNICATIONS REGULATORY AUTHORITY OF NAMIBIA

SCHEDULE

ARRANGEMENT OF REGULATIONS

PART 1
INTRODUCTORY PROVISIONS

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 –

"certificate of accreditation" means a certificate issued to a certification service provider under regulation 6;

"certification practice statement" means a statement issued by a certification service provider specifying the practices that the service provider employs in issuing a subscriber certificate;

"certificate of recognition" means a certificate issued to a foreign person recognised as certification service provider under regulation 23;

"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 given on the basis of subscriber certificates;

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

(d) checking the revocation status of the subscriber certificate and advising the relying party; and

(e) issuing cross-pair certificates;

"certification service provider" means a person accredited under regulation 5 to provide certification service and manage and issue subscriber certificates and public keys;

"Communications Act" means the Communications Act, 2009 (Act No. 8 of 2009);

"cross pair certificate" means a digital certificate that establishes a trust relationship between two certification service providers or entities holding certificates issued by different certification service providers;

"international standards" means 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 having a property that allows the public key to verify an electronic signature that the private key creates;

"key personnel" means employees who have direct responsibility for the day to day operations, security and performance of a certification service provider, or whose duties directly involve the issuance, renewal, suspension, revocation of certificates, the process of identification of any person requesting a certificate, the creation of private keys or the administration of the certification service providers computing facilities;

"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;

"public entity" means –

(a) an "office", "ministry" or "agency" of government as defined in section 1 of the Public Service Act, 1995 (Act No. 13 of 1995);

(b) a body established by or under the Namibian Constitution or an Act of Parliament; or

(c) a private entity that –

(i) is totally or partially owned by the State, or financed, directly or indirectly, by the State; or

(ii) carries out statutory functions or services or public functions or services;

"standard subscriber agreement" means an agreement between the certification service provider and its subscriber for the provision of recognised electronic signatures.

"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;

"subscriber certificate revocation list" means a list of subscriber certificates that have been revoked under regulation 9; and

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

PART 2
ACCREDITATION OF SECURITY PRODUCTS AND
CERTIFICATION SERVICE PROVIDERS

Types of products and services that may not be provided without being accredited

2. A person may not –

(a) supply digital or electronic product or provide certification service;

(b) carry on or operate, or hold himself or herself out as carrying on or operating or providing certification service,

unless such –

(i) product or service has been accredited; or

(ii) person has been accredited and issued with a certificate of accreditation as a service provider,

by the Authority in terms of section 42 of the Act and in accordance with regulation 5.

Classification of security products, security services and providers of such products and services

3. Every digital or electronic product, every digital or electronic service, or every provider of such product or service that has as its purpose referred to in section 41(1) of the Act is classified as security product, security service, or provider of security products or security services, respectively, and are treated as such in terms of the Act and these regulations.

Accreditation of security products and services

4. (1) A person who wishes to apply for accreditation of a security product or as a supplier or provider of a security product must apply to the Authority in a manner determined by the Authority.

(2) A person who wishes to operate as a certification service provider must -

(a) in addition to requirements provided in sections 41 and 42 the Act; or

(b) with the approval of the Minister in case of an applicant who is a public entity,

apply to the Authority for accreditation as a certification service provider in terms of regulation 5.

Application for accreditation as certification service providers

5. (1) The application for accreditation to operate as certification service provider is made on Form 1 set out in Annexure 1, and is accompanied by –

(a) proof of payment of a non-refundable application fee as set out in Annexure 3;

(b) a certification practice statement referred to in regulation 15;

(c) an undertaking signed by the applicant to –

(i) undergo and pass an initial audit; and

(ii) fulfil other requirements relating to qualification, expertise, manpower, financial resources and infrastructure facilities necessary as determined by the Authority from time to time for the granting of accreditation; and

(d) proof of the approval of the Minister in case of a public entity.

(2) The Authority must within 90 days of receipt of an application for accreditation grant or refuse the application but if on good reason a decision cannot be made within this period, the Authority may extend with any period not exceeding 60 days.

(3) The Authority, in considering an application for accreditation, must have regard to –

(a) the financial and technical capability of the applicant;

(b) the ability of an advanced electronic signature to –

(i) uniquely be linked to the subscriber;

(ii) identify the subscriber;

(iii) be maintained under the sole control of the subscriber;

(iv) be linked to the data or data message to which it relates in a manner that any subsequent change of the data or data message is detectable; and

(v) enable face to face identification of the subscriber;

(c) the quality of the hardware and software systems;

(d) the procedures for the processing of products or services;

(e) the availability of information to third parties relying on the certification service;

(f) the regularity and extent of audits by an independent body;

(g) the ability of the applicant to comply with the applicable certification service standards;

(h) whether applicant has, within a period of 10 years immediately preceding the date of his, her or its accreditation been convicted, whether in Namibia or elsewhere, of an offence involving fraud or dishonesty or has been convicted of an offence under the Act or these regulations;

(i) any other relevant factor the Authority may determine.

(4) Where applicable, this regulation applies to a public entity, with –

(a) the necessary modifications required in the context; and

(b) such other modifications as the Authority may determine in the public interest.

(5) Where the Authority refuses an application for accreditation, it must inform the applicant, in writing, giving reasons for its refusal.

(6) The Authority may request for further particulars in respect of an application for accreditation, and where the Authority requests for such particulars the period referred to in subregulation (2) stops running for that period and resumes upon receipt of the requested particulars.

Issuance of certificate of accreditation

6. (1) Where an application for accreditation made under regulation 5 meets all the requirements and conditions, the Authority must –

(a) grant the application; and

(b) issue the applicant with a certificate of accreditation in Form 2 set out in Annexure 1.

(2) A certificate of accreditation issued in terms of this regulation is valid for a period of four years.

(3) A certification service provider must at all times display its certificate of accreditation in a conspicuous manner in its place of business.

(4) The Authority, as soon as practical after the issuance, renewal, suspension or revocation of a certificate of accreditation, must announce the issuance, renewal, suspension or revocation of the certificate by notice –

(a) on its website; and

(b) in any other media of its choice circulating widely.

(5) A holder of a certificate of accreditation must pay to the Authority the annual fee set out in Annexure 3 before the anniversary date of the certificate.

(6) A holder of a certificate of accreditation who fails to pay the annual fee on the applicable due date, the holder must pay an additional prescribed fee for every day the amount due is not paid.

(7) Where the annual fee for a certificate of accreditation remains unpaid for a period of 90 days as from the date the fee is due, the Authority, after giving the holder of a certificate an opportunity to be heard, may revoke the certificate.

(8) A certification service provider who fails to comply with the condition under subregulation (4) or (5) is liable to a penalty contemplated in section 115(4) of the Communications Act, 2009 and is guilty of an offence and on conviction liable to a fine not exceeding N$500 000 or to imprisonment for a period not exceeding two years.

Amendment of accreditation

7. (1) A certification service provider may, at any time during the validity of its certificate of accreditation, apply to the Authority for amendment of the terms or conditions of accreditation or any matter relating to the accreditation.

(2) An application for amendment of accreditation is accompanied by the application fee set out in Annexure 3.

(3) The Authority must upon receipt consider the application for amendment of accreditation and may grant or refuse the application.

(4) Where the application for amendment of accreditation is granted, the Authority –

(a) must make the relevant amendments to the certificate, terms or conditions of accreditation, upon payment of the fee set out in Annexure 3;

(b) must, allow the certificate to continue to have effect as varied until its expiry;

(c) may not refund any fees paid with respect to the accreditation.

(5) The Authority, on its own motion, may vary the terms or conditions of accreditation where the amendment is necessary –

(a) in the public interest; or

(b) to address the concerns of the members of the public or subscribers.

(6) The Authority, before making any amendment of the terms or conditions of accreditation issued under subregulation (5), must notify the certification service provider concerned of its intention to amend the accreditation –

(a) in the manner specified in the notice; and

(b) specifying the period, not being less than 30 days from the date of receipt of the notice, within which the service provider may make a written representation to the Authority in respect of the proposed amendment.

Renewal of accreditation

8. (1) A certification service provider who wishes to renew its accreditation must apply to the Authority for the renewal of accreditation at least 90 days before the date of expiry of its certificate of accreditation.

(2) An application for renewal of accreditation is made in Form 1 set out in Annexure 1 and is accompanied by –

(a) an application for renewal of accreditation fee set out in Annexure 3;

(b) the latest version of the certification precise statement;

(c) a copy of the latest version of the standard subscriber agreement;

(d) the audited financial statements of the two preceding years, where applicable;

(e) a latest audited report; and

(f) any other necessary information as the Authority may request.

(3) An application for renewal of certificate of accreditation is considered by the Authority within 60 days from the date of receipt of the application but if on good reason a decision cannot be made within this period, the Authority may extend with any time not exceeding 60 days.

(4) The Authority must grant a renewal of certificate of accreditation where it is satisfied that the applicant –

(a) meets the requirements of the Act and these regulations; and

(b) has complied with the terms and conditions imposed on its accreditation.

Refusal to grant and renew accreditation

9. (1) The Authority may refuse to grant or renew accreditation where –

(a) the applicant –

(i) fails to comply with any provision of the Act or these regulations or the certification service standards;

(ii) fails to provide the Authority with further information it requested regarding the processing of the application concerned;

(iii) is wound up or liquidated;

(iv) has, within a period of 10 years immediately preceding the date of his, her or its accreditation or renewal, been convicted, whether in Namibia or elsewhere, of any offence involving fraud or dishonesty or has been convicted of any offence under the Act or these regulations; or

(v) or any of its owners or key personnel is found guilty of misconduct involving fraud or dishonest;

(b) it is not satisfied with –

(i) the qualifications or experience of the key personnel of the applicant;

(ii) the financial standing of the applicant or its significant owners; or

(iii) the record of past performance or expertise of the applicant or of its personnel;

(c) it has reason to believe that the applicant may not be able to act in the best interest of its subscribers or customers having regard to the reputation, character, financial integrity and reliability of the applicant or any of its significant owners or key personnel; or

(d) it is of the opinion that it is in the interest of the public to do so.

(2) The Authority must inform the applicant of the reasons for refusal to grant or renew accreditation.

Suspension, revocation and lapsing of certificate of accreditation

10. (1) The Authority may suspend or revoke the certificate of accreditation of a certification service provider if –

(a) the Authority is of the view that the information provided in the application for accreditation is false, misleading or inaccurate;

(b) the certification service provider –

(i) fails to undergo an audit required under regulation 18;

(ii) is likely to be wound up;

(iii) fails to carry on the business for which it was accredited; or

(iv) contravenes or fails to comply with any term or condition in respect of its accreditation;

(c) the Authority finds that the certification service provider or any of its key personnel has not performed their duties efficiently, honestly or fairly; or

(d) the Authority is satisfied with the grounds for suspension or revocation after having received a written request by the certification service provider to suspend or revoke the accreditation.

(2) Where the Authority is satisfied that a certification service provider is not complying with or has not complied with a term or condition of accreditation, the Authority may suspend or revoke the certificate of accreditation.

(3) The Authority must notify the certification service provider in writing of any intended suspension or revocation of certificate of accreditation including –

(a) the reasons for suspension or revocation;

(a) the timelines for rectification of non-compliance; and

(b) the action that it intends to take in the event of non-compliance with the notice within the period specified in the notice.

(4) The Authority may not suspend or revoke a certificate of accreditation without first giving the certification service provider an opportunity to be heard and to comply with the directives of the Authority, if any, within a reasonable specified period.

(5) The Authority, in determining whether it is necessary to suspend or revoke a certificate of accreditation, must consider the extent of loss or damages to persons likely to be affected by the suspension or revocation.

(6) A certificate of accreditation which remains unutilized for six months from the date of issue lapses automatically at the expiry of six months.

Surrender of certificate of accreditation

11. (1) Where a certification service provider decides not to continue providing the certification service, the service provider must –

(a) notify the Authority in writing of the surrender of the certificate of accreditation; and

(b) agree with the Authority on the terms and conditions of the surrender of the certificate of accreditation with particular reference to anything done or any benefit obtained under the certificate.

(2) Where a certificate of accreditation is surrendered, its validity ends and the certification service provider –

(a) ceases all entitlements to any benefits arising from the certificate; and

(b) is not entitled to a refund of any fees paid with respect to the certificate.

Cede, pledge, encumber and dispose of certificate of accreditation

12. A certification service provider may not cede, pledge, encumber or otherwise dispose of its certificate of accreditation except under regulation 13.

Transfer and assignment of certificate of accreditation

13. (1) A certification service provider may transfer or assign its certificate of accreditation to any person with the prior approval of the Authority.

(2) An application for approval to transfer or assign a certificate of accreditation is made to the Authority in a manner and form determined by the Authority, and the Authority may, within 60 days of receipt of the application -

(a) grant the application on the terms and conditions that it may determine, and issue a transfer of certificate of accreditation upon payment of transfer fee set out in Annexure 3; or

(b) refuse the application and give reasons for the refusal.

Audit report

14. (1) A certification service provider must provide an information audit report compiled by an auditor appointed by the Authority.

(2) All fees relating to the audit report is borne by the certification service provider.

(3) The audit report must confirm in respect of –

(a) an advanced electronic signature that it –

(i) conforms with the requirements of section 41 of the Act and is capable of identifying the signer;

(ii) is created by qualifying signature creation and signature verification devices;

(iii) is based on a qualifying certificate; and

(iv) complies with the international standards with which the certification service provider claims in its application for accreditation; and

(b) a certification service provider that it –

(i) satisfies the requirements and conditions set out in Annexure 2;

(ii) has systems in place to ensure compliance with the Act and these regulations;

(iii) has sufficient financial resources to provide for professional indemnity or insurance cover as determined by the Authority; and

(iv) has personnel who satisfy the requirements and conditions set out in Annexure 2.

Certification practice statement

15. (1) A certification service provider must –

(a) prepare a certification practice statement in accordance with the certification service standards, these regulations and guidelines issued by the Authority from time to time; and

(b) submit the certification practice statement to the Authority for approval before accreditation is granted, renewed or any operation commenced.

(2) A certification service provider, in its certification practice statement, must specify –

(a) any limitation of its liabilities and, particularly, the implication of reliance limitations specified; and

(b) the subscriber identity verification method for the issuance, suspension, revocation and renewal of subscriber certificate.

(3) When the Authority approves a certification practice statement, the certification service provider may not change the statement without a prior written approval of the Authority.

(4) A certification service provider must –

(a) file with the Authority a copy of its certification practice statement and specify its effective date; and

(b) publish it on its website which is accessible to members of the public.

(5) A certification service provider must record all changes made to its certification practice statement together with the effective date of each change.

(6) A certification service provider must keep in a secure manner a copy of each version of its certification practice statement and record the date it came into effect and the date it ceased to have effect.

Database of accredited security products and certification service providers, suspended and revoked accreditations

16. (1) The Authority must keep and maintain a database of all security products and certification service providers accredited by the Authority and suspended and revoked accreditations.

(2) The register must contain –

(a) the name and address of the certification service provider; and

(b) a description of the certification service provider.

(3) The Authority must publish the register on its website and by any other means it thinks fit for access to the public.

Change in ownership, management and operation of certification service provider

17. (1) A certification service provider that wishes to change its ownership, management or operations may make an application to the Authority for approval.

(2) Upon receipt of an application for change of ownership, management or operations the Authority may –

(a) request the applicant to submit an audit report; or

(b) suspend or revoke the accreditation of the service provider.

(3) Where an audit report is requested, all expenses is borne by the certification service provider.

(4) Where the Authority has authorised a change in the ownership or management of a certification service provider, it must publish a copy of the latest certification practice statement of the certification service provider on its website and by any other means it thinks fit for access to the public.

Review and audits

18. (1) The Authority must monitor the conduct, systems and operations of every certification service provider to ensure that it complies with the Act, these regulations and certification service standards and, where necessary –

(a) require a service provider to undergo an audit if it is of the opinion that –

(i) a significant change in the ownership or operations of the certification service provider has occurred, or

(ii) such audit is reasonably required or is otherwise necessary;

(b) issue such direction to the certification service provider concerned for compliance as it thinks necessary; or

(c) suspend or revoke the accreditation after having given the certification service provider an opportunity to be heard.

(2) Where an audit is required in terms of subregulation (1)(a), a certification service provider must at its own cost commission an audit report to be compiled by an auditor appointed by the Authority which must be completed within such period as the Authority may specify.

(3) A certification service provider who refuses or fails to comply with the remedial directive issued under subregulation (1)(b) commits an offence and the Authority may deal with the matter as contemplated by Chapter X of the Communications Act.

Inquiry into allegation of misconduct

19. (1) The Authority may inquire into any allegations that –

(a) a significant change in the ownership, management or operations of a certification service provider has occurred, the approval of which has not been granted in terms of regulation 17;

(b) a member of the key-personnel of the certification service provider has committed an act which may render him or her guilty of misconduct and unfit to continue with certification service;

(c) a certification service provider has contravened a provision of the Act, these regulations or certification standards; or

(d) a certification service provider is in breach of its certification practice statement or the terms of its standard subscriber agreement.

(2) If, after inquiring into an allegation made under subregulation (1) and having given the certification service provider an opportunity to be heard and the Authority is of the opinion that the allegation is proven, it must take any appropriate action under regulation 17.

(3) If the Authority is of the opinion that the allegation under subregulation (1) is made in bad faith, it may require the person who made the allegation to be liable for the costs related to the inquiry including costs of an audit that may be required.

Appeal to High Court

20. Subject to regulation 50, a certification service provider aggrieved by a decision of the Authority may within 30 days of receipt of the decision appeal to the High Court.

PART 3
FOREIGN CERTIFICATION SERVICE PROVIDERS

Recognition as foreign certification service providers

21. The Authority may recognise a foreign certification service provider as a certification service provider for the purposes of these regulations, where the service provider –

(a) is duly licensed or certified or authorised to issue certification services in the country in which it operates;

(b) complies with the requirements of the Act and these regulations, especially regulation 5, and international standards; and

(c) has established a suitable and qualified local agent to provide certification service in Namibia.

Application for recognition

22. (1) An application for recognition as a foreign certification service provider for the purposes of these regulations is made to the Authority in a manner determined by the Authority.

(2) An application for recognition as certification service provider is accompanied by –

(a) proof that the requirements under regulation 21 have been satisfied, including a report from a qualified auditor certifying that the certification standards and technical requirements have been satisfied;

(b) the prescribed fee; and

(c) such other information or documents as the Authority may require.

Granting of recognition

23. (1) On receipt of an application for recognition made under regulation 22, the Authority must consider the application within 60 days of receipt.

(2) Upon consideration of the application after having had regard to all the requirements, conditions and suitability of the applicant, the Authority may grant the application with or without conditions or refuse the application.

(3) Where the Authority grants the application, the Authority must issue the applicant with a certificate of recognition as certification service provider and register its name on the database list referred to in regulation 16.

(4) Regulations 6, 8, 9, 10, 14, 15, 18 and 19 and all the terms and conditions regarding a certificate of accreditation apply with the necessary changes to a certificate of recognition.

(5) A holder of a certificate of recognition must pay to the Authority the annual fee set out in Annexure 3 before the anniversary date of the certificate.

(6) Where a holder of a certificate of recognition fails to pay the annual fee on the applicable due date, the holder must pay an additional prescribed fee for every day the amount due is not paid.

(7) Where the annual fee for a certificate of recognition remains unpaid for a period of 90 days as from the date the fee is due, the Authority, after giving the holder of the certificate an opportunity to be heard, may revoke the certificate.

(8) Where the Authority refuses an application for recognition, the Authority must immediately notify the applicant in writing of its refusal and the reasons for its refusal.

(9) Where a holder of a certificate of recognition issued under subregulation (3) issues a subscriber certificate to a subscriber, such certificate is valid for the purposes of the Act and these regulations.

Suspension, revocation and lapsing, ceding, pledging, encumber, disposing, transfer, assignment and surrender of certificate of recognition

24. (1) The provisions applicable to accreditation of certification service providers relating to suspension, revocation, lapsing, ceding, pledging, encumber, disposing, transfer, assignment and surrender of certificates of accreditation apply with the necessary changes to the suspension, revocation, lapsing, ceding, pledging, encumbering, disposal, transfer, surrender and assignment, of certificates of recognition.

(2) The Authority, by notice in the *Gazette*, may revoke the certificate of recognition granted under regulation 23 –

(a) if the Authority finds that the recognised foreign certification service provider no longer satisfies the requirements contemplated under regulation 21; or

(b) if the recognised foreign certification service provider applies for a revocation of the recognition.

(3) A revocation under subregulation (2)(b) is without prejudice to a fresh application for recognition being made by the foreign certification service provider.

(4) Where the Authority is satisfied that a recognised foreign certification service provider has contravened or not complied with any of the requirements, conditions and suitability of recognition under regulation 23(2), it may revoke the recognition.

Register of recognised foreign certification service providers

25. (1) The Authority must –

(a) publish a list of recognised foreign certification service providers in such form and manner as it may determine; and

(b) keep and maintain a Register of recognised foreign certification service providers in such form as it may consider fit.

PART 4
ADVANCED ELECTRONIC SIGNATURE SCHEME, KEY MANAGEMENT AND ISSUANCE OF SUBSCRIBER CERTIFICATES

Approval of advanced electronic signatures

26. (1) An advanced electronic signature scheme must be approved for the purposes of the Act and these regulations if –

(a) the advanced electronic signature scheme uses a secure public-key algorithm for the generation of the key pair and a secure public-key algorithm and hash function for the creation of the electronic signature;

(b) the advanced electronic signature scheme satisfies the technical component requirements; and

(c) the electronic signature created is not capable of being modified to contain a subliminal channel.

(2) A key pair used to create and verify an electronic signature may not be used to encrypt and decrypt any messages.

Storage and control of private keys

27. (1) The data storage medium for the private key may be hardware- based or software-based.

(2) If the data storage medium of the private key –

(a) is hardware-based, the subscriber holding the private key must ensure that the token, smart card or other external devices in which the private key is stored is kept in a secure place and in a secure manner; or

(b) is software-based, the subscriber holding the private key must ensure that the computer system in which the private key is stored is reasonably secure.

(3) A subscriber holding the private key must –

(a) keep secret the personal identification numbers or other data used for the identification of the rightful holder of the private key in conjunction with the data storage medium for the private key;

(b) exercise reasonable care in retaining control of the private key corresponding to the public key listed in its certificate;

(c) prevent the disclosure of the private key to a person not authorised to create electronic signature concerned; and

(d) continue to take control of the private key during the operational period of its certificate and during any period of suspension of its certificate.

Disposal of key pairs

28. (1) If a key pair is no longer in use or to be used, or if the private key of the key pair is compromised, the holder of the key pair must dispose of it in a suitable manner, including by destroying it.

(2) A holder of the key pair to be disposed of must use secure means and method to destroy the keys.

(3) Despite subregulation (1), if the holder desires to retain a key pair that is no longer in use or to be used, or that has been compromised, the holder must ensure that the key pair is stored by a reasonably secure method.

Issuance of subscriber certificates

29. (1) A certification service provider, on receipt of an application from a prospective subscriber, may grant the application, if –

(a) the prospective subscriber is the person to be listed in the certificate to be issued;

(b) in the case of a prospective subscriber acting through an agent, the certification service provider has verified that the subscriber has authorised the agent to have custody of the private key of the subscriber and to request issuance of a certificate listing the corresponding public key;

(c) the information in the certificate to be issued is accurate;

(d) the subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(e) the private key is capable of creating an electronic signature;

(f) the public key to be listed in the certificate can be used to verify an electronic signature affixed by the private key held by that subscriber;

(g) information regarding the conditions of usage of the certificate and limits on the value of transactions, where applicable, is available; and

(h) sufficient information that can be used to locate or identify one or more repositories in which notification of the revocation or suspension of the certificate would be listed if the certificate is suspended or revoked.

(2) A certification service provider must –

(a) determine, based on official documents, the identity of the person to whom the certificate is issued; and

(b) specify, in the certification practice statement, the subscriber identity verification method applied in the issuance of certificates.

(3) A certification service provider must –

(a) give a subscriber an opportunity to verify the contents of the certificate before the subscriber accepts it;

(b) inform a subscriber, in writing, of the legal effect of an advanced electronic signature, the limitations on the use of certificates and the dispute resolution procedures applicable; and

(c) warn subscribers, in writing, not to allow third parties to use signature creation data associated with signature verification data in the certificate.

(4) Where the subscriber –

(a) accepts the issued certificate, the certification service provider must publish a signed copy of the certificate in a repository;

(b) does not accept the certificate, the certification service provider may not publish the certificate.

(5) Once a certification service provider has issued a subscriber certificate and the subscriber has accepted the certificate, but a fact that may significantly affect the validity or reliability of the certificate subsequently becomes known to the service provider, the service provider must notify the subscriber without undue delay.

(6) A certification service provider must log and keep in a secure manner the date and time of all transactions relating to the issuance of a subscriber certificate.

(7) Where a certification service provider issues an additional certificate to a person based on a valid certificate held by the same person and subsequently the original certificate is suspended or revoked, the service provider must investigate and determine whether the new certificate should also be suspended or revoked.

Particulars of subscriber certificates

30. A subscriber certificate must set out –

(a) the number of the certificate;

(b) the name of the subscriber;

(c) the personal identification code or registry code of the subscriber;

(d) the public key of the subscriber;

(e) the period of validity of the certificate;

(f) the issuer and registry code of the issuer; and

(g) a description of the limitations on the scope of use of the certificate.

Obtaining subscriber certificate

31. A subscriber must ensure that –

(a) all material representation to a certification service provider for purposes of obtaining a subscriber certificate; and

(b) all information known to the subscriber and represented in the certificate,

are accurate and complete to the best of his or her knowledge and belief, regardless of whether such representations are confirmed by the certification service provider.

Acceptance of subscriber certificate

32. (1) A subscriber is deemed to have accepted a subscriber certificate, if the subscriber –

(a) publishes or authorises the publication of the certificate –

(i) to one or more persons; or

(ii) in a repository; or

(b) otherwise demonstrates approval of the certificate while knowing or having notice of its contents.

(2) A subscriber who accepts a certificate issued by a certification service provider, must certify that –

(a) the subscriber rightfully holds the private key corresponding to the public key listed in the certificate;

(b) a representation made by the subscriber to the certification service provider to the information listed in the certificate is true; and

(c) information in the certificate that is within the knowledge of the subscriber is true.

Disclosure and compliance with certification practice statement

33. (1) A certification service provider must disclose –

(a) its certificate that contains the public key corresponding to the private key used by that certification service provider to digitally sign another certificate;

(b) a certification practice statement referred to in regulation 15;

(c) a notice of the revocation or suspension of certificate; and

(d) any other fact that materially and adversely affects either the reliability of a certificate that the service provider has issued or the ability of the service provider to carry out its obligations.

(2) In the event of an occurrence that materially and adversely affects the trustworthy system of a certification service provider or a certificate issued by it, the service provider must –

(a) use reasonable efforts within 24 hours to notify any person who is known or likely to be affected by that occurrence; and

(b) act in accordance with procedures governing such an occurrence as specified in its certification practice statement.

Prohibition of publication of subscriber certificate

34. A person may not publish a subscriber certificate or otherwise make it available to another person if –

(a) that person is not the certification service provider;

(b) the subscriber listed in that certificate has not accepted it; or

(c) the certificate has been suspended or revoked, unless that publication is for the purpose of verifying an electronic signature created prior to that suspension or revocation.

Representation on issuance of subscriber certificate

35. A certification service provider by issuing a subscriber certificate, represents to any person who reasonably relies on the certificate, that –

(a) the service provider has issued the certificate in accordance with the applicable certification practice statement incorporated by reference in the certificate, or of which the relying party has notice;

(b) the service provider has complied with requirements under these regulations for issuing of certificate, and that the subscriber listed in the certificate has accepted it;

(c) the subscriber identified in the certificate holds the private key corresponding to the public key listed in the certificate;

(d) the public key and private key of the subscriber constitute a functioning key pair;

(e) information in the certificate is accurate, unless the service provider has stated in the certificate or incorporated by reference in the certificate a statement that the accuracy of specified information is not confirmed; and

(f) the service provider has no knowledge of any material fact which if included in the certificate would adversely affect the reliability of the representations in paragraphs (a) to (e).

Recommended reliance limits

36. A certification service provider –

(a) must, in issuing a certificate to a subscriber, specify a recommended reliance limit in the certificate; and

(b) may specify different reliance limits in different certificates as it considers fit.

Limitation of liability for certification service provider

37. Subject to an agreement between a certification service provider and a subscriber, a certification service provider is not liable –

(a) for any loss caused by reliance on a false or forged electronic signature of a subscriber, if, with respect to the false or forged electronic signature, the certification service provider complied with the requirements of this Act; or

(b) in excess of the amount specified in the certificate as its recommended reliance limit for either –

(i) a loss caused by reliance on a misrepresentation in the certificate of any fact that the certification service provider is required to confirm; or

(ii) failure to comply with requirements for issuance of the certificate and representations on issuance of the certificate.

Suspension of subscriber certificate

38. (1) A certification service provider may suspend a subscriber certificate –

(a) on request by the subscriber listed in the certificate or a person duly authorised by that subscriber;

(b) by court order;

(c) if there are reasonable grounds to believe that –

(i) incorrect data has been entered in the certificate; or

(ii) it is possible to use the private key corresponding to the public key contained in the certificate without the consent of the subscriber; or

(d) on the ground of misrepresentation by the subscriber or a person acting on behalf of the prescriber.

(2) Where the private key corresponding to the public key listed in the subscriber certificate has been compromised, the subscriber must as soon as possible request the issuing certification service provider to suspend or revoke the certificate.

Notice of suspension

39. A certification service provider must, after the suspension of a certificate under regulation 38, publish a signed notice of the suspension in the repository.

Revocation of subscriber certificate

40. A certification service provider must revoke a subscriber certificate –

(a) on receiving a request for revocation by the subscriber listed in the 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;

(b) on receiving a certified copy of the death certificate of the subscriber, or on confirming by other evidence that the subscriber is dead; or

(c) on presentation of documents effecting a dissolution of the subscriber, or on confirming by other evidence that the subscriber has been dissolved or ceases to exist.

Revocation without consent of subscriber

41. (1) A death certificate must revoke a subscriber certificate, regardless of whether the subscriber listed in the certificate consents, where the certification service provider confirms that –

(a) a material fact represented in the certificate is false;

(b) the private key or trustworthy system of the certification service provider was compromised in a manner materially affecting the reliability of the certificate;

(c) an individual subscriber is dead; or

(d) a subscriber has been dissolved, wound up or otherwise ceases to exist.

(2) The certification service provider must, where it revokes the subscriber certificate under subregulation (1), immediately notify the subscriber listed in the certificate.

Notice of revocation of subscriber certificates

42. (1) A certification service provider must, publish a signed notice of the revocation under regulation 40 or 41 in a repository specified in the subscriber certificate.

(2) The certification service provider must, where one or more repositories are specified, publish a signed notice of the revocation in all those repositories.

Publication of revocation list of subscriber certificates

43. (1) A certification service provider must maintain a revocation list of subscriber certificates.

(2) A certification service provider that contravenes subregulation (1) commits an offence and is liable, on conviction, to a fine not exceeding N$50 000.

Management of records

44. (1) A certification service provider must keep securely all records relating to –

(a) issuance, renewal, suspension and revocation of subscriber certificates, including the identity of any person requesting a subscriber certificate;

(b) the process of generating key pairs by the subscribers and by itself;

(c) the administration of its computing facilities; and
(d) such other information as may be determined by the Authority.

(2) A certification service provider may keep its records in paper- based form, electronic form or any other form and avail the records to the Authority in a manner the Authority requires.

(3) A certification service provider must index, store, and preserve the records kept under subregulation (2) in a form that the records may be reproduced in an accurate, complete, legible manner and a manner accessible to the Authority or to any authorised person.

(4) A certification service provider must retain –

(a) a record of all the subscriber certificates it has issued and preserve them so that they are accessible;

(b) all records required to be kept under subregulation (1); and

(c) all the logs of the creation of the archive of certificates,

for a period of not less than seven years.

Obligations of subscribers for generating keypairs

45. (1) Where a subscriber wishes to generate a keypair whose public key is to be listed in a certificate and accepted by the subscriber, the subscriber must generate that key pair using a trustworthy system.

(2) This regulation does not apply to a subscriber who generates the key pair using a system approved by a certification service provider.

Information system audit

46. (1) A certification service provider must conduct an information system audit annually and submit the audit report to the Authority.

(2) Despite subsection (1), the Authority may require a certification service provider to conduct an information system audit as and when the Authority considers it necessary at the cost of the certification service provider.

Security guidelines

47. (1) Every certification service provider has the sole responsibility concerning the integrity, confidentiality and protection of information employed in its operation, including the classification, declassification, labelling, storage, access and destruction of information according to their value, sensitivity and importance in the operations of the certification service provider.

(2) The Authority must, from time to time, issue in the form of directives or guidelines –

(a) Information Technology Security Guidelines; and

(b) Security Guidelines for Certification Service Providers,

which are aimed at protecting the integrity, confidentiality and availability of service of certification service providers.

(3) Every certification service provider must formulate its Information Technology and Security Policy for its operations in compliance with the guidelines referred to in subregulation (2) and must submit it to the Authority for approval before the commencement of its operation.

(4) A certification service provider must submit any change made by it to its Information Technology and Security Policy to the Authority within 14 days of effecting the change and the Authority must notify the certification authority whether the change is approved.

Incident handling

48. (1) A certification service provider must develop and implement an incident management plan which cover, inter alia, the following incidents –

(a) compromise of key;

(b) unauthorised or unlawful penetration of the system and network of the certification service provider;

(c) unavailability of its infrastructure; and

(d) registration, generation, use, suspension or revocation of certificates which is fraudulent.

(2) Where an incident referred to in subregulation (1) occurs, the certification service provider must report the incident to the Authority within 24 hours.

Data collection and protection

49. (1) A certification service provider may only collect personal data directly from the subscriber and in so far as it is necessary for the purposes of the Act and these regulations.

(2) A certification service provider may only collect data from a third party, if the subscriber gives his or her written consent.

(3) Any data collected under the Act and these regulations is only used for the purposes of the Act and these regulations unless –

(a) the Act or any other law permits otherwise; or

(b) the subscriber has given his or her written consent for the data to be used for other purposes.

Appeals against decisions of certification service providers

50. A person aggrieved with the decision of a certification service provider may appeal to the Authority within 14 days of receipt of the decision or notice of suspension or revocation.

Reconsideration by Authority

51. The Authority may, on application or on its own motion, review, rescind or vary a decision made by it within 90 days of the decision in compliance with section 31 of the Communications Act and section 43(1) of the Act.

ANNEXURE 1

Form 1

COMMUNICATIONS AUTHORITY OF NAMIBIA (CRAN)

Electronic Transactions Act, 2019 (Act No. 4 of 2019)

Regulations Regarding Accreditation of Security Products
and Certification Service Providers, 2025

Application for Accreditation/Renewal

The application form is for Certification Service Providers who desire to be accredited, recognised or renew their accreditation, under the Regulations Regarding Accreditation of Security Products and Services and Providers of such Products and Services ("Regulations") made under the Electronic Transactions Act. The applicants are required to comply with the Certification Service Standards (CSS) issued by the Communications Regulatory Authority of Namibia (CRAN)

As Certification Service Provider
(Section 42/Regulation 5)

SECTION 1: PARTICULARS OF THE APPLICANT

1.1 Applicants Details

Company/ Public entity Name:	
Physical Address:	
Postal address:	
Telephone:	
Facsimile:	
Mobile:	
Email:	

Form 1 (Continue)

1.2 Contact Person Details (Official Communication)

Name:	
Designation:	
Physical **Address:**	
Postal Address:	
National I.D / Passport No.	
Telephone: (Work)(Res)	
Email Address	
Facsimile:	
Mobile:	
Email:	

1.3 □ Public Entity or □ Private Entity

1.4 Company Registration: …….. State whether company is:

Public Limited/ Private Limited Owned by State/ Others (please specify): …….....
…….....

Main business activity	
Company website (URL)	

The following information should be attached:

(a) Company registration certificate, where the applicant company is a subsidiary of another company, information about the parent and ultimate holding companies (the entire group structure) must be provided; and

(b) A certified true copy of the applicant company's resolution(s):

(i) to apply for accredited or recognition as Certification Service Provider, or (in the case of an accredited secure digital signature provider applying for renewal of its accreditation) for renewal of its accreditation; and

(ii) to authorise, for the purpose of making this application on the applicant company's behalf, the person(s) making the application.

Form 1 (Continue)

1.3 Ownership:

Provide names, addresses and contact details of Directors/ Board Members:

Name of Company/ Individual	
Country of Incorporation/ Nationality	
National I.D/Passport No. Company Registration Number	
Physical Address	
Postal Address	
Share %	

Name of Company/Individual	
Country of Incorporation/Nationality	
National I.D/Passport No. Company Registration Number	
Physical Address	
Postal Address	
Share %	

Please attach Shareholder Certificates

Form 1 (Continue)

1.4 Management Structure

Provide the details of the key executive management

Name:	Name:
Designation:	Designation:
Physical Address:	Physical Address:
Postal Address:	Postal Address:
National I.D/Passport No.	National I.D/Passport No.
Telephone: (Work) (Res)	Telephone: (Work) (Res)
Facsimile:	Facsimile:
Mobile:	Mobile:
Email:	Email:

Provide the curriculum vitae for the key personnel. The applicant is required to provide contact details of the key personnel as per the Certification Service Standards. (applicable to private entities only)

Nome:	Name:
Designation:	Designation:
Physical Address:	Physical Address:
Postal Address:	Postal Address:
National I.D/Passport No:	National I.D/Passport No:
Telephone: (Work) (Res)	Telephone: (Work) (Res)
Facsimile:	Facsimile:
Mobile:	Mobile:
Email:	Email:

SECTION 2: LEGAL PROCEEDINGS INFORMATION

1.1 Has the applicant ever been involved in any legal proceeding or dispute settlement in Namibia or elsewhere in its capacity as a Certification Service Provider?

Yes No

If the answer to the above question is "yes", please furnish complete details (please attach a separate sheet if the space provided is inadequate).

.....
.....
.....
.....
.....
……...
...……
……...
.....

Form 1 (Continue)

1.2 Has the applicant company or its substantial shareholder or any of their respective directors and key executives, or any of the trusted persons, ever been convicted of an offence for which the conviction involved a finding that it/he/she acted fraudulently or dishonestly?

Yes No

If the answer to the above question is "yes", please furnish complete details (please attach a separate sheet if the space provided is inadequate).

SECTION 3: ACCOMPANYING DOCUMENTS

The Applicant should attach the following documents:

(a) Full technical description of the advanced electronic signature system;

(b) Certification Practice Statement of the applicant;

(c) Standard subscriber agreement;

(d) Audited report in accordance with Certification Service Standards Compliance Checklist issued by the Authority;

(e) Privacy/security policy;

(f) Detail Business Plan covering the following:

(i) Profit and loss accounts, balance sheets and cash flow statements, target market, business strategy. All assumptions used e.g. asset depreciation policies, subscriber projections, budget and annual increase/decrease in operating expenditure should be clearly explained;

(ii) Financial ratios including return on assets, return on equity, operating profit margin, net profit margin, current ratio, quick ratio and debt-equity ratio;

(iii) All capital expenditure and working capital requirements for the preceding five years of operations;

(iv) Source of Funding;

(v) Proposed fee structure for the advanced electronic signature;

(vi) Human Resource plan including the organisational chart, curriculum vitae of the key personnel;

(g) Incident Management plans and Disaster Recovery Plan; and

(h) Audited Financial Report for the previous two (2) years.

SECTION 4*:* DECLARATION

1. In applying to CRAN to operate as an accredited Certification Service Provider under the Electronic Transactions Act, 2019 and the Regulations, I declare that all the above information provided by the company is true and complete.

2. In the event that any of the information provided by the company is found to be false or misleading, the Authority reserves the right to take appropriate enforcement action against the company under the Act and the Regulations (including, without limitation, suspending and revocation of the accreditation of the company).

Applicant Name: …….....

Name of Representative: …….....

Signature: .....….....

Designation.....

Date: .....

Company Stamp: .....

Form 2

COMMUNICATIONS AUTHORITY OF NAMIBIA (CRAN)

Electronic Transactions Act, 2019 (Act No. 4 of 2019)

Regulations Regarding Accreditation of Security Products and Services and Providers of Such Products and Services, 2025

Certificate of Accreditation as Certification Service Provider

(Regulation 6)

Communications Regulatory Authority (CRAN), in the exercise of powers conferred upon it under section 42 of the Electronic Transactions Act, 2019 (No. 4 of 2019), hereby issues a

CERTIFICATE OF ACCREDITATION AS CERTIFICATION SERVICE PROVIDER

to……

Having its registered office at ……to offer certification service and manage and issue subscriber certificates and public keys to the potential subscribers for a period of five (5) years, subject to the provisions of the Electronic Transactions Act, 2019 (No. 4 of 2019) and the conditions in Annexure 1 attached hereto and such regulations and conditions as have been or may be imposed from time to time.

The Service Provider must at all times display the Certificate in a conspicuous place at the registered offices of the Service Provider.

Given under my Hand and Seal at .....this .....day of ..... 20.....

(Accreditation Mark)

…….. (Signature)

Chief Executive Officer

ANNEXURE 2
COMMUNICATIONS AUTHORITY OF NAMIBIA (CRAN)

Electronic Transactions Act, 2019 (Act No. 4 of 2019)

Regulations Regarding Accreditation of Security Products
and Services and Providers of Such Products and Services, 2025

Requirements and Conditions for Electronic Signature Creation and Verification Devices, Qualifying Certificates, Service Providers and Key Personnel

(Regulation 13)

A. **Requirements for Qualifying Signature Creation Devices**

1. A qualifying signature creation device must, by appropriate technical and procedural means, ensure as a minimum that –

   (a) the signature creation data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;

   (b) the signature creation data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology; and

   (c) the signature creation data used for signature generation can be reliably protected by the legitimate signatory' against use by others.

2. A qualifying signature creation device should not alter the date to be signed or prevent such data from being presented to the signer prior to the signature process.

B. **Requirements for Qualifying Signature-Verification Devices**

1. During the signature-verification process it must be ensured with reasonable certainty that –

   (a) the date used for verifying the signature corresponds to the data displayed to the verifier;

   (b) the signature is reliably verified, and the result of that verification is correctly displayed;

   (c) the verifier can, as necessary, reliably establish the contents of the signed data;

   (d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;

   (e) the result of verification and the identity of the signatory are correctly displayed;

   (f) the use of a pseudonym is clearly indicated; and

   (g) any security-relevant changes can be detected.

C. **Requirements for Qualifying Certificates**

1. A qualifying certificate must contain –

   (a) an indication that the certificate is issued as a qualifying certificate;

(b) the identification of the certification service provider and the jurisdiction in which it is established;

(c) the name of the signatory or pseudonym, which must be identified as such;

(d) provision for a specific attribute of the subscriber, if relevant, depending on the purpose for which the certificate is intended;

(e) signature verification data which corresponds to signature creation data under the control of the signer;

(f) an indication of the beginning and end of the period of validity of the certificate;

(g) the identity code of the certificate;

(h) the advanced electronic signature of the certification service provider issuing it;

(i) limitations on the scope of use of the certificate, if applicable; and

(j) limits on the value of transaction for which the certificate can be used, if applicable.

D. **Requirements for Qualifying Certification Service Providers**

1. A certification service provider must –

(a) be a fit and proper person to the satisfaction of the Communications Regulatory Authority;

(b) demonstrate the reliability and expertise necessary for providing certification services;

(c) demonstrate adherence or the ability to adhere to these Regulations;

(d) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;

(e) ensure that the date and time when a certificate is issued or revoked can be determined precisely;

(f) verify, by appropriate means, the identity and, if applicable, any specific attributes of the person to whom a certificate is issued;

(g) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

(h) take measures against forgery of certificates, and in cases where the certification service provider generates signature creation data, guarantee confidentiality during the process of generating such data;

(i) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Act, and these Regulations, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

(j) not store or copy signature creation data of the person to whom the certification service provider provided key management services;

(k) before entering into a contractual relationship with a person seeking a certificate to support his or her electronic signature, inform that person by means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing. Relevant parts of this information must also be made available on request to third parties relying on the certificate; and

(m) use trustworthy systems to store certificates in a verifiable form so that –

(i) only authorised persons can make entries and changes;

(ii) information can be checked for authenticity;

(iii) certificates are publicly available for retrieval in only those cases for which the consent the consent of the certificate holder has been obtained; and

(iv) any technical changes compromising these security requirements are apparent to the operator.

E. **Requirements for Key Personnel of Qualifying Certification Service Providers**

1. A certification-service-provider must ensure that its key personnel –

(a) are fit and proper persons to carry out the duties assigned to them; and

(b) have not within a period of ten (10) years preceding their employment been convicted, whether in Namibia or elsewhere, of –

(i) an offence involving fraud or dishonesty; or

(ii) an offence under the Act or these Regulations.

2. Key personnel must possess the relevant expert knowledge, experience, and qualifications necessary for the services provided, expertise in electronics signature technology and familiarity with prior security procedures, they must also apply administration and management procedures which are adequate and correspond to recognised certification service standards and must possess knowledge of the Act and these Regulations.

Signed at……. on this..……..day of……..…….20…….....

…….. (Signature)
Chief Executive Officer

ANNEXURE 3

COMMUNICATIONS AUTHORITY OF NAMIBIA (CRAN)
Electronic Transactions Act, 2019 (Act No. 4 of 2019)

Regulations Regarding Accreditation of Security Products
and Services and Providers of Such Products and Services, 2025

Fees Payable under the Regulations

(Regulations 5, 6, 7, 8, 9, 13, 22 and 23)

Item	Description of Item	Fees in NAD (N$)
1	Application for Accreditation	20 000
2	Certificate of Accreditation	30 000
3	Annual Fee Certificate of Accreditation	30 000
4	Additional Fee for Unpaid Annual Fee Certificate of Accreditation per Day	2 000
5	Application for Renewal of Certificate of Accreditation	20 000
6	Renewal of Certificate of Accreditation	30 000
7	Application for Amendment of Accreditation (Certificate, Terms or Conditions)	20 000
8	Amendment of Accreditation (Certificate, Terms or Conditions)	30 000
9	Application for Transfer of Certificate of Accreditation	20 000
10	Transfer of Certificate of Accreditation	30 000
11	Application for Recognition	30 000
12	Certificate of Recognition	40 000
13	Annual Fee Certificate of Recognition	40 000
14	Additional Fee for Unpaid Annual Fee Certificate of Recognition per Day	3 000
17	Application for Renewal of Certificate of Recognition	30 000
18	Renewal of Certificate of Recognition	40 000