NOTICE 1537 OF 2004
DEPARTMENT OF COMMUNICATIONS
(ACCREDITATION AUTHORITY)

NOTICE INVITING COMMENT ON PROPOSED ACCREDITATION REGULATIONS DRAFTED IN TERMS OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, 2002 (ACT NO. 25 OF 2002)

The Minister of Communications intends to make the regulations in the Schedule in terms of section 94 read with Chapter VI of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002).

Interested persons are hereby invited to furnish comments on the proposed regulations, within 30 days of the date of publication of this notice at any of the following addresses:

For attention:	Alf Wiltz The Deputy Accreditation Authority Department of Communications;
post to:	Private Bag X860 Pretoria 0001;
or deliver to:	First Floor, Block B iParioli Office Park 399 Duncan Street Hatfield;
or fax to:	(012) 4278093;
or e-mail to:	alf@doc.gov.za

Please note that comments received after the closing date may be disregarded.

Mr. Wiltz can be reached at tel. (012) 4278070/ 8217 for any enquiries.

Schedule

REGULATIONS UNDER THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT

TABLE OF CONTENTS

Subject	*Regulation No.*
ACCREDITATION REGULATIONS	
Interpretation and application	
Definitions	1
CHAPTER I: Administration	
Administration	2
Guidelines	3
Database	4
CHAPTER II: Application for accreditation	
Accreditation	5
Manner of application for accreditation	6
Prescribed information	7
Submission of applications	8
Processing of applications	9
Granting of accreditation	10
Publication of accreditation	11
Refusal of application for accreditation	12
CHAPTER III: Requirements for certification service providers	
Technical and other requirements which certificates shall meet	13
Requirements for issuing certificates	14
Requirements for certification practice statements	15
Duties of subscribers	16
Responsibilities of certification service providers	17
Requirements prior to cessation of business	18
Liability of certification service providers	19
Records to be kept	20
Suspension and revocation of certificates	21
Publication of suspension and revocation	22
CHAPTER IV: Suspension, revocation and termination	
Suspension and revocation	23
Procedure following suspension	24
Termination	25
Information security requirements	26
Evaluator	27
Administration and supervision	28
CHAPTER V: General	
Fees payable	29

Definitions

1. In these Regulations any word or expression to which a meaning has been assigned in the Act shall have the meaning so assigned and, unless the context otherwise indicates:

"accreditation agreement" means the agreement entered into between the Accreditation Authority and an authentication service provider as part of the accreditation of the authentication products or services of that service provider;

"certification practice statement" means a statement issued by a certification service provider to specify the practices that it employs in generating and issuing certificates;

"certificate policy" means a named set of rules that indicates the applicability of a certificate to a particular community or class of application or to both such community and class, as the case may be, with common security requirements;

"constitutive documents" means in the case of; (a) a legal person, certified copies of the Memorandum and Articles of Association, certificate of incorporation, founding statement, partnership agreement or trust deed, as the case may be; (b) a natural person, his or her ID book or passport;

"evaluator" means an independent auditing firm contemplated in section 36(1)(c) of the Act;

"ITU X.509" means recommendation X.509 of the International Telecommunications Union on information technology, open systems interconnection, the directory: public-key and attribute certificate frameworks;

"reliance limit" means the monetary limit specified for reliance on an advanced electronic signature;

"SABS/ ISO 17799" means a code of practice for information security management accepted as a national standard by the South African Bureau of Standards - SABS ISO/IEC 17799;

"signature creation data" means unique data, such as codes or private cryptographic keys, which are used by the signatory identified in the certificate to create an electronic signature;

"signature verification data" means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;

"suspend" means, in relation to a certificate, to suspend temporarily the operational period of a certificate from a specific time;

"the Act" means the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002);

"trustworthy system" means computer hardware, software systems and procedures which comply with the criteria determined in section 38(3) of the Act;

"revoke" means, in relation to a certificate, to terminate the operational period of a certificate from a specific time.

CHAPTER I
Administration

Administration

2 (1) These Regulations shall be administered by the Accreditation Authority.

(2) The Accreditation Authority shall furnish the Minister with quarterly reports of its activities.

Guidelines

3. The Accreditation Authority may issue guidelines, directives or practice notes relating to its administration of all matters which are required to be done in terms of the Act and these Regulations.

Database

4. The database contemplated in section 36(2) of the Act shall contain at least-

(a) the following particulars of each authentication service provider whose authentication products or services have been accredited:

(i) The name of the authentication service provider;

(ii) the names as well as the technical description of the accredited authentication products and services by type, class or other description;

(iii) the business address, telephone number, web site address, e-mail and facsimile number of the customer service department of the authentication service provider; and

(iv) the identification number and web site location of the authentication service provider's repository

(b) a description of the accreditation processes and requirements, functions and services offered by the Accreditation Authority;

(c) the complaints procedures for users of accredited authentication products and services; and

(d) the contact particulars of the Accreditation Authority.

CHAPTER II
Application for accreditation

Accreditation

5. On application by an authentication service provider, the Accreditation Authority may, after complying with the requirements of the Act and these

Regulations, accredit authentication products or services as advanced electronic signatures.

Manner of application for accreditation

6. An application for accreditation in terms of the Act shall be made to the Accreditation Authority in the form determined by the Accreditation Authority, and shall be supported by the information in regulation 7 and be accompanied by the non-refundable application fee determined in regulation 29(1).

Prescribed information

7. An application for accreditation shall be supported by-

(a) the constitutive documents of the applicant;

(b) where the applicant is a certification service provider, a copy of its Certification Practice Statement and Certificate Policy, drafted in accordance with the Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, as well as an undertaking that it can and will comply with the requirements of its Certification Practice Statement and Certificate Policy;

(c) a declaration-

(i) detailing procedures with respect to the identification and authentication of users of those authentication products or services, including face to face identification;

(ii) detailing the manner in which the applicant's authentication products or services comply with each of the provisions of section 38(1)(a), (b), (c), (d) and (e) of the Act;

(iii) addressing the manner in which the applicant will comply with requirements determined in the Act and these Regulations;

(iv) detailing the manner in which information about the applicant's authentication products and services as well as the conditions on which those products or services are offered or may be used, and how it will be made available to the general public and users of those authentication products or services;

(v) detailing the naming conventions to be used by the applicant, as well as the manner in which the applicant will deal with name ownership, name disputes, and name resolutions; and

(vi) indicating how the applicant will ensure the availability of information to third parties relying on the authentication product or service;

(d) full details of operations outsourced or to be outsourced;

(e) the applicant's audited financial statements for the three years or lessor period, when applicable, immediately preceding the application;

(f) general technical specifications of the applicant's hardware and software systems, security policies, standards it complies with and infrastructure available as well as the location of its facilities;

(g) the privacy and security policy to be followed by the applicant in its operations;

(h) an organisation chart and the details and competency of all trusted personnel of the applicant;

(i) a statement dealing with the applicant's-

(i) human resource plan;

(ii) procedures for processing of authentication products and services; and

(iii) audits, more specifically the regularity and extent of the applicant's audits;

(j) detailed profiles of directors, management and trusted personnel of the applicant;

(k) an undertaking by the applicant that it will make payment to the approved evaluator appointed by the Accreditation Authority to conduct an audit, at the reasonable fees charged by an evaluator in the circumstances;

(l) a description of any event, particularly insolvency, that could materially affect the applicant's ability to act as an authentication service provider;

(m) an undertaking by the applicant to submit a performance guarantee and to pay the annual accreditation fee prescribed in regulation 29(1)(b) within 30 days of accreditation;

(n) proof of adequate insurance cover based on reliance limits or other acceptable criteria; and

(o) a statement of the extent of accessibility of its facilities by the general public or its prospective subscribers.

Submission of applications

8. (1) Applications for accreditation shall be submitted to the Accreditation Authority by hand delivery thereof.

(2) An application which is not accompanied by all the prescribed information and fees shall not be processed.

(3) Applications shall be submitted personally to a designated official of the Accreditation Authority.

Processing of applications

9. (1) The Accreditation Authority shall process all applications for accreditation within 45 working days of the date of receipt of the last piece of information required under regulation 7, but may under circumstances beyond its control and for reasons to be recorded in writing, extend that period by not more than 45 working days.

(2) The Accreditation Authority shall cause an inspection or evaluation, as the case may be, of the applicant and its authentication products or services in terms of the Act and these Regulations.

Granting of accreditation

10. (1) If the Accreditation Authority is satisfied that the applicant has met its criteria for accreditation, the Accreditation Authority shall-

(a) communicate its decision in writing to the applicant;

(b) advise the applicant of any restrictions or conditions attached to the granting of the accreditation;

(c) advise the applicant of the effective date of the granting of the accreditation;

(d) require the applicant to pay the prescribed annual subscription fee and submit the performance guarantee within 30 days of accreditation;

(e) issue a certificate of accreditation for each authentication product or service accredited, stating any restrictions or other conditions upon which it was accredited, upon payment of all fees due; and

(f) notify the authentication service provider that accreditation is subject to the parties concluding an accreditation agreement.

(2) An authentication service provider shall be subject to periodic audits determined by the Accreditation Authority from time to time.

(3) No authentication service provider shall offer authentication products or services as accredited authentication products or services unless it has been issued with a certificate of accreditation by the Accreditation Authority in respect of each accredited authentication product or service.

(4) An authentication service provider whose authentication products or services have been accredited may outsource or appoint agents or contractors to carry out some or all of its operations, provided that-

(a) it has notified the Accreditation Authority in writing;

(b) the agent or contractor, as the case may be, has been audited by the Accreditation Authority for purposes of that specific authentication product or service, the costs of which shall be borne

in full by the authentication service provider or his or her agent or contractor;

(c) the Accreditation Authority approves the appointment of those agents or contractors in writing;

(d) those agents or contractors shall equally comply with the Act, these Regulations and the accreditation agreement applicable to the authentication service provider whose authentication products or services have been accredited; and

(e) the authentication service provider remains responsible for the activities of agents or contractors in the performance by them of the functions of the authentication service provider.

Publication of accreditation

11. The Accreditation Authority shall publish details of accredited authentication products and services in its publicly accessible database and in any other medium that it regards appropriate.

Refusal of application for accreditation

12. The Accreditation Authority may refuse to accredit an authentication product or service if-

(a) the applicant has not provided the Accreditation Authority with the information determined in regulation 7 or the information is not of a satisfactory standard or quality;

(b) the applicant is not in a position to comply with the Act or these Regulations;

(c) an applicant fails to comply with any directions or requirements of the Accreditation Authority;

(d) an authentication service provider fails to submit itself to , or act in accordance with an audit, inspection or evaluation; or

(e) any other valid reason exists for the refusal of accreditation;

Provided that the Accreditation Authority may grant an applicant the opportunity to make a written representation on the reasons for refusal of accreditation, and may grant an applicant the opportunity to comply with any requirement which will render the applicant's authentication product or service accreditable, within a period of 30 days after the Accreditation Authority has furnished the applicant with its reasons for refusal of accreditation.

CHAPTER III
Requirements for certification service providers

Technical and other requirements which certificates shall meet

13. All certificates issued by a certification service provider shall, if accredited by the Accreditation Authority, conform to the highest established international

standards, including, but not limited to ITU X.509 standard and shall, *inter alia,* contain the following data:

(a) serial number of the certificate that distinguishes it from other certificates;

(b) signature algorithm identifier that identifies the algorithm used by the certification service provider to sign the certificate;

(c) issuer name, being the name of the certification service provider that issued the certificate;

(d) the validity period of the certificate, being the beginning and end of the validity period of the certificate;

(e) name or pseudonym of the subscriber whose public key the certificate identifies;

(f) public key information of the subscriber; and

(g) confirmation that it is a certificate that has been accredited by the Accreditation Authority.

Requirements for issuing certificates

14 (1) A certification service provider shall reliably establish the identity of a person or entity applying for a certificate, which shall include face-to-face identification of the user or authorised key holder.

(2) A certification service provider may issue a certificate to a prospective subscriber only after it has-

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

(b) complied with all of the practices and procedures set forth in its Certification Practice Statement and Certificate Policy, including procedures regarding face-to-face identification of the prospective subscriber.

(3) By issuing a certificate, a certification service provider shall be deemed to represent to any person who reasonably relies on the certificate or an advanced electronic signature verifiable by the public key listed in the certificate, that the certification service provider has issued the certificate in accordance with its Certification Practice Statement and Certificate Policy incorporated by reference in the certificate.

(4) Where a Certification Practice Statement and Certificate Policy have been incorporated by reference in a certificate, the following provisions shall apply to the extent that the representations are not inconsistent with the Certification Practice Statement and Certificate Policy:

(a) The certification service provider has complied with all applicable requirements of the Act, these Regulations and the accreditation agreement in issuing the certificate, and if the

certification service provider has published the certificate or otherwise made it available to a relying person, that the subscriber listed in the certificate had accepted it;

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

(c) the subscriber's public key and private key constitute a functioning key pair;

(d) all information in the certificate is accurate, unless the certification 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

(e) the certification service provider has no knowledge of any material fact which if it had been included in the certificate would adversely affect the reliability of the representations in subparagraphs (a), (b), (c) and (d).

Requirements for certification practice statements

15. **(1)** Certification service providers whose authentication products or services have been accredited shall issue and prominently make publicly available a Certification Practice Statement and Certificate Policy for each type, class or description of accredited authentication products or services in the manner and format stipulated by the Accreditation Authority.

(2) A certification service provider whose authentication products or services have been accredited shall-

(a) lodge a certified copy of each Certification Practice Statement and Certificate Policy used for accredited authentication products or services with the Accreditation Authority;

(b) before it effects any material changes to such Certification Practice Statement and Certificate Policy, including changes-

(i) in the identification process that weaken the reliability of certificates;

(ii) in the reliance limit of the certificates; or

(iii) in key generation, storage or usage;

consult with the Accreditation Authority;

(c) notify the Accreditation Authority, its subscribers and relying parties by publication on its website of any incident that adversely or materially affects or may affect the validity of the whole or part of a Certification Practice Statement and Certificate Policy which has already been lodged with Accreditation Authority;

(d) adhere to its Certification Practice Statement and Certificate Policy when issuing a type, class or description of accredited certificates; and

(e) clearly state all costs and fees to subscribers and relying parties with respect to the issuance, revocation, suspension, retrieval or verification of the status of an accredited certificate under each type, class or description of certificates issued by it.

(3) A certification service provider shall use the following documents to identify and authenticate a subscriber or applicant for a certificate or other authentication product or service during initial registration, routine rekey, rekey after revocation and when processing requests for suspension or revocation:

(a) Where the subscriber or applicant is a natural person a combination of the originals of a-

(i) national identity document;

(ii) passport; or

(iii) current, valid accredited certificate to be used as identity for certificate renewal purposes only;

(b) where the subscriber or applicant is a partnership, the constitutive documents of the partnership as well as the documents referred to in paragraph (a) in respect of each partner of the partnership, including the authorised key holder;

(c) where the subscriber or applicant is a company, close corporation, trust or other legal entity, a combination of certified copies of-

(i) the relevant constitutive documents;

(ii) the latest audited financial statements of the applicant;

(iii) a resolution or power of attorney of the directors authorising a specific person to apply for or otherwise deal with a specific certificate service provider regarding the issue, renewal or replacement of certificates; and

(iv) the documents referred to in paragraph (a), of the directors, members or trustees of the applicant and the authorised key holder, together with a resolution appointing the representative as the authorised key holder.

Duties of subscribers

16. A certification service provider shall be responsible for ensuring that its subscribers adhere to the following:

(a) If the subscriber whose public key is to be listed in a certificate issued by the certification service provider and accepted by the subscriber,

generates the key pair, the subscriber shall generate that key using a trustworthy system;

(b) all material representations made by the subscriber to a certification service provider for purposes of obtaining a certificate, including all information known to the subscriber and represented in the certificate, shall be accurate and complete to the best of the subscriber's knowledge and belief, regardless of whether such representations are confirmed by the certification service provider;

(c) a subscriber shall be deemed to have accepted a certificate if he or she –

(i) publishes the certificate in a repository or makes it available to a third party for use; or

(ii) otherwise demonstrates approval of a certificate while knowing or having notice of its contents;

(d) by accepting a certificate issued by a certification service provider, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate that –

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

(ii) all representations made by the subscriber to the certification service provider and material to the information listed in the certificate are true; and

(iii) all information in the certificate that is within the knowledge of the subscriber is true;

(e) by accepting a certificate issued by a certification service provider, the subscriber identified in the certificate assumes a duty to exercise reasonable care to retain control of the private key corresponding to the public key listed in such certificate and prevent its disclosure to a person not authorised to create the subscriber's advanced electronic signature and such duty shall continue during the operational period of the certificate and during any period of suspension of the certificate;

(f) a subscriber who has accepted a certificate shall, if the private key corresponding to the public key listed in the certificate has been compromised, as soon as possible request the issuing certification service provider to suspend or revoke the certificate and proof of ownership of the private key.

Responsibilities of certification service providers

17. A certification service provider whose authentication products or services have been accredited shall –

(a) disclose in a publicly accessible database –

(i) its certificate that contains the public key corresponding to the private key used by that certification service provider to digitally sign another certificate (referred to in this section as a certification service provider certificate);

(ii) its Certification Practice Statement and Certificate Policy;

(iii) notice of the revocation or suspension of its certification service provider certificate;

(iv) any other fact that materially and adversely affects either the reliability of a certificate that the certification service provider has issued or the certification service provider's ability to perform its services; and

(v) all its accredited authentication products or services;

(b) use a trustworthy system to perform its services and functions, including the generation and management of its keys, the generation and management of subscribers' keys, the issuance, renewal, suspension or revocation of accredited certificates, the maintenance of its repository and the publication of accredited certificates;

(c) in the event of an occurrence that materially and adversely affects a certification service provider's trustworthy systems as contemplated in section 38(2)(a), (b), (c) and (d) of the Act or its certification service provider certificate, the certification service provider shall use reasonable efforts to notify any person who is known to be or foreseeably will be affected by that occurrence, or act in accordance with procedures governing such an occurrence specified in its Certification Practice Statement and Certificate Policy.

(d) develop, establish, maintain, and update documented and approved policies, procedures and practices over its entire operational environment;

(e) report any incident which may materially affect its trustworthy system in general to the Accreditation Authority;

(f) ensure that all its personnel are fit and proper persons, possess the necessary knowledge, technical qualifications and expertise to carry out their duties effectively; and

(g) adhere to the Act, these Regulations, the accreditation agreement applicable to it, and the guidelines or directives issued by the Accreditation Authority.

Requirements prior to cessation of business

18. (1) A certification service provider shall, prior to ceasing to act as such, comply with the requirements of the Act and these Regulations, the accreditation agreement and any guidelines or directives issued by the Accreditation Authority.

(2) A certification service provider who fails to comply with this Regulation

shall, subject to the provisions of the relevant subscriber's agreement or the common law, be liable for any damage or loss suffered by subscribers or relying parties.

Liability of certification service providers

19. A certification service provider is liable for any damages caused to any entity or legal or natural person who reasonably relies on a certificate which has been accredited by the Accreditation Authority-

(a) with regard to the accuracy at the time of issuance of all information contained in the certificate and the fact that the certificate contains all the details prescribed;

(b) for assurance that at the time of the issuance of the certificate, the signatory identified in the certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;

(c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification service provider generates them both;

(d) with regard to publication of notices of suspension or revocation in the repository specified in the certificate for publication of notice of suspension or revocation; and

(e) with regard to services it has undertaken to provide to subscribers;

unless the certification service provider proves that it has not acted negligently.

Records to be kept

20. **(1)** For the purposes of section 38(4)(f) of the Act the following records shall be kept for a period of seven years, or the period which the Accreditation Authority may determine:

(a) Applications for issue of certificates;

(b) registration and verification documents of generated certificates;

(c) certificates in a manner such that-

(i) no-one, with the exception of parties authorised to do so, can make changes to the certificates or add to them;

(ii) it is possible to verify that the information is correct; and

(iii) the certificate is available to the public only if expressly permitted by the signatory;

(d) information of suspended certificates;

(e) information of expired and revoked certificates; and

(f) reliable records and logs for activities that are core to the certification service provider's operations which activities shall include certificate management, key generation and administration of its computing facilities.

(2) An accredited authentication service provider shall maintain its repository in such a manner that it can be readily accessed by subscribers and relying parties.

(3) All records shall be kept in such a manner that ensures the security, integrity and accessibility of the information and records for the retrieval and inspection thereof.

(4) All archived records may be re-signed to protect their integrity and reliability in the event of technological advances which might impact on the reliance that can be placed on the original records.

Suspension and revocation of certificates

21. (1) Unless a certification service provider and a subscriber agree otherwise, the certification service provider shall suspend a certificate as soon as possible after receiving a request by a person whom the certification service provider reasonably believes to be-

(a) the subscriber listed in the certificate;

(b) a person duly authorised to act for that subscriber; or

(c) a person acting on behalf of that subscriber, who is unavailable.

(2) The certification service provider shall revoke a certificate that it issued-

(a) after receiving a request for revocation from the subscriber named 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) after receiving a certified copy of the subscriber's death certificate, or upon confirming by other evidence that the subscriber is deceased; or

(c) upon presentation of documents that a subscriber which is a legal person has been wound up or deregistered.

(3) A certification service provider shall revoke a certificate, regardless of whether the subscriber listed in the certificate consents, if-

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

(b) a requirement for the issuance of the certificate was not satisfied;

(c) the certification service provider's private key or trustworthy system was compromised in a manner that materially affects the reliability of the certificate; or

(d) a subscriber has breached an agreement with the certification service provider.

(4) Upon effecting a revocation contemplated in subregulation (3), the certification service provider shall immediately notify the subscriber listed in the revoked certificate, if possible, and publish the revocation in its repository.

Publication of suspension and revocation

22. Within 24 hours of suspension or revocation of a certificate by a certification service provider, the certification service provider shall publish a signed notice of the suspension or revocation in the repository specified in the certificate for publication of notice of suspension or revocation and where more than one repository is specified, the certification service provider shall publish signed notices of the suspension or revocation in all such repositories.

CHAPTER IV
Suspension, revocation and termination

Suspension and revocation

23. (1) If an authentication service provider whose authentication products or services have been accredited -

(a) fails or ceases to meet any of the requirements, conditions or restrictions subject to which accreditation was granted under section 38 of the Act, or recognition was given in terms of section 40 of the Act;

(b) has been-

(i) informed by the Accreditation Authority of its intention to suspend or revoke the authentication service provider's accreditation and given the reasons or a description of the breach;

(ii) requested by the Accreditation Authority to remedy the non-compliance or breach within a reasonable time; and

(iii) afforded the opportunity to respond to the allegations in writing within a reasonable time;

and fails to either respond in writing or remedy the breach within the time specified, the Accreditation Authority may suspend or revoke the accreditation of the authentication products or services affected by that non-compliance or breach.

(2) Prior to revoking the accreditation of any authentication products or services, the Accreditation Authority shall-

(a) notify the authentication service provider in writing of its decision as well as the reasons for the decision;

(b) publish a notice in its database to the effect that it is in the process of revoking the accreditation of the relevant authentication product or service;

(c) appoint an Accreditation Officer, and an evaluator to oversee the winding-down details of the service provider's accredited operations;

(d) ensure that the authentication service provider communicates the revocation to the subscribers and relying parties in the fastest possible medium;

(e) ensure that the service provider revokes all accredited authentication products or services issued to its users and records the manner, time and date of revocation;

(f) ensure that the Accreditation Officer and the evaluator each issues a report certifying compliance with the prescribed revocation process;

(g) make arrangements for preservation of records as provided for in terms of section 38(4)(f) of the Act in accordance with the determined manner and length of time;

(h) at its discretion or on request, assist subscribers to find an alternative supplier of authentication products or services; and

(i) ensure that the revocation is conducted with minimal disruption to subscribers and relying parties.

(3) The Accreditation Authority shall publish all suspensions and revocations in its publicly accessible database.

Procedure following suspension

24. **(1)** After the Accreditation Authority has suspended accreditation, the Accreditation Authority may -

(i) take any action necessary to confirm whether the authentication service provider still fails to meet any of the requirements, conditions or restrictions subject to which accreditation was granted or recognition given;

(ii) repeat any part of the procedure in section 39(2) of the Act;

(iii) monitor the progress of the authentication service provider in rectifying the breach;

(iv) consider any specific request by the relevant authentication service provider;

(v) re-evaluate its decision to suspend.

(2) If the breach of the requirements, conditions or restrictions subject to which accreditation was granted or recognition given continues for a period of 30 days after suspension, the relevant accreditation may be revoked.

(3) If the breach of the requirements, conditions or restrictions subject to which accreditation was granted or recognition given is remedied, the Accreditation Authority may lift the suspension and reinstate accreditation.

(4) The Accreditation Authority shall, if a suspended authentication product of service becomes a revoked authentication product of service or when suspension of an authentication product of service is lifted and the relevant accreditation reinstated, publish such information on its publicly accessible database.

Termination

25. (1) An authentication service provider whose authentication products or services have been accredited may terminate such accreditation at any time, subject to the Act, these Regulations and the accreditation agreement: Provided that the service provider shall-

(a) give notice of its intention to cease operations to the Accreditation Authority, 90 days before the termination of its accreditation or ceasing to act as an authentication service provider;

(b) advertise before the termination of its accreditation or ceasing to act as an authentication service provider as the case may be, the intention in the daily newspapers and in the manner that the Accreditation Authority may determine;

(c) give 60 days notice of its intention to cease acting as an authentication service provider to all its subscribers and holders of each un-revoked or un-expired certificate issued by it, by sending the notice by electronic mail and registered post;

(d) ensure that discontinuing its operations causes minimal disruption to its subscribers and to persons needing to verify certificates;

(e) pay reasonable restitution (not exceeding the cost involved in obtaining new certificates) to subscribers for revoking the certificates before the date of expiry;

(f) make arrangements for preservation of records as provided in section 38(4)(f) of the Act in accordance with the determined manner and length of time; and

(g) destroy all expired certificates after complying with the requirements of this regulation.

(2) The Accreditation Authority shall follow the provisions of subregulation 23(2)(c), (d), (e), (f), (g) and (h) once it receives a notice of termination from an authentication service provider.

Information security requirements

26. Accredited authentication service providers shall adhere to security policies which shall at least comply with relevant standards such as SABS/ISO 17799.

Evaluator

27. **(1)** The Accreditation Authority shall appoint one or more evaluators who shall conduct periodic audits of technical and other compliance of authentication service providers.

(2) The fees for the services of an evaluator shall be paid by the authentication service provider in respect of whom an audit was conducted.

(3) The Accreditation Authority shall ensure that an authentication service provider undertakes in writing to pay prior to the audit for services of an evaluator.

(4) The Accreditation Authority shall first approve the rate of fees charged by an evaluator, which fees shall be reasonable in the circumstances.

(5) The approved evaluator shall audit the authentication service provider or its authentication products or services in accordance with the Act, these Regulations and guidelines issued by the Accreditation Authority from time to time.

(6) An evaluator performing an audit shall submit its report to the Accreditation Authority within five working days, or as otherwise agreed, of the completion of such task.

(7) An evaluator shall further:

(a) use appropriate techniques;

(b) evaluate the reliability and quality of the systems used, the integrity, confidentiality and availability of data as well as the compliance with the specifications included in any procedure manual and the security plan approved by the Accreditation Authority which shall at least comply with relevant standards such as SABS/ISO 17799;

(c) verify that trustworthy systems contemplated in section 38 of the Act are used;

(d) issue a report with the findings, conclusions and recommendations in each case.

(8) If so instructed by the Accreditation Authority, the evaluator shall further:

(a) follow up on the audits in order to determine whether the authentication service provider has implemented the corrective actions suggested in the recommendations;

(b) issue additional reports;

(c) take part in contingency plan simulations; and

(d) furnish additional copies of all reports issued to the Accreditation Authority.

Administration and supervision

28. Accreditation granted by the Accreditation Authority, shall be subject to the condition that an authentication service provider shall allow the Accreditation Authority or an evaluator appointed by the Accreditation Authority, as the case may be, to enter its business premises during normal business hours for purposes of audits and shall upon request make available for inspection any relevant books, records, supporting documents, and other documentation and shall disclose all information reasonably requested by the Accreditation Authority or evaluator and provide all support necessary to conduct the audit.

CHAPTER V
General

Fees payable

29 (1) The fees payable by authentication service providers who apply for, or whose authentication products or services have been accredited, are as follows-

(a) Application fee: R20, 000.00;

(b) annual accreditation fee per product or service: R10, 000.00;

(c) performance guarantee per product or service: R10, 000.00.

(2) Fees payable to the Accreditation Authority shall be paid directly into the Department's bank account and proof of payment provided to the Accreditation Authority.

(3) All fees other than the performance guarantee shall be non-refundable.

(4) The Accreditation Authority may use the performance guarantee if an accredited authentication service provider fails to pay any fees due in terms of the Act or these Regulations.

(5) Save for the first annual accreditation fee which is payable upon accreditation, the annual accreditation fee shall be payable on or before 31 January of each year.

Short title

30. These regulations shall be called the Accreditation Regulations and shall come into force on a date published by the Minister by notice in the Government Gazette.

KENNISGEWING 1537 VAN 2004

DEPARTEMENT VAN KOMMUNIKASIE
(AKKREDITASIE-OWERHEID)

KENNISGEWING VAN UITNODIGING VAN KOMMENTAAR OP VOORGESTELDE AKKREDITASIEREGULASIES OPGESTEL IN TERME VAN DIE WET OP ELEKTRONIESE KOMMUNIKASIE EN TRANSAKSIES, 2002 (WET NO. 25 VAN 2002)

Die Minister van Kommunikasie beoog om die regulasies in die Skedule kragtens artikel 94 gelees met Hoofstuk VI van die Wet op Elektroniese Kommunikasie en Transaksies, 2002 (Wet No. 25 van 2002), te maak.

Belangstellende persone word hiermee uitgenooi om kommentaar te lewer op die voorgestelde regulasies binne 30 dae vanaf die datum van publikasie van hierdie kennisgewing by die volgende adres:

Vir aandag:	Alf Wiltz Adjunk Akkreditasie-owerheid Departement van Kommunikasie;
pos aan:	Privaatsak X860 Pretoria 0001;
of lewer af by:	Eerste vloer, Blok B iParioli Kantoorpark Duncanstraat 399 Hatfield;
of faks na:	(012) 4278093;
of e-pos na:	alf@doc.gov.za

Neem asseblief kennis dat kommentaar wat ontvang word na die sluitingsdatum verontagsaam mag word.

Mnr. Wiltz kan bereik word by tel. (012) 4278070/ 8217 vir enige navrae.

Bylae

REGULASIES KRAGTENS DIE WET OP ELEKTRONIESE KOMMUNIKASIE EN TRANSAKSIES

INHOUDSOPGAWE

Onderwerp	*Regulasie Nr.*
AKKREDITASIEREGULASIES	
Uitleg en toepassing	
Woordomskrywing	1
HOOFSTUK I: Administrasie	
Administrasie	2
Riglyne	3
Databasis	4
HOOFSTUK II: Aansoek om akkreditasie	
Akkreditasie	5
Wyse van aansoek om akkreditasie	6
Voorgeskrewe inligting	7
Indiening van aansoeke	8
Verwerking van aansoeke	9
Verlening van akkreditasie	10
Publikasie van akkreditasie	11
Afkeuring van aansoek om akkreditasie	12
HOOFSTUK III: Vereistes vir sertifiseringsdiensverskaffers	
Tegniese en ander vereistes waaraan sertifikate moet voldoen	13
Vereistes vir die uitreiking van sertifikate	14
Vereistes vir sertifiseringspraktykstate	15
Pligte van intekenaars	16
Verantwoordelikhede van sertifiseringsdiensverskaffers	17
Vereistes voor staking van besigheid	18
Aanspreeklikheid van sertifiseringsdiensverskaffers	19
Rekords gehou te word	20
Opskorting en intrekking van sertifikate	21
Publikasie van opskorting en intrekking van sertifikate	22
HOOFSTUK IV: Opskorting, intrekking en beëindiging	
Opskorting en intrekking	23
Prosedure na opskorting	24
Beëindiging	25
Vereistes ten opsigte van inligtingsekerheid	26
Evalueerder	27
Administrasie en kontrole	28
HOOFSTUK V: Algemeen	
Gelde betaalbaar	29

Woordomskrywing

1. In hierdie Regulasies het enige woord of uitdrukking waaraan 'n betekenis in die Wet geheg word, daardie betekenis, en tensy uit die samehang anders blyk, beteken:

"akkreditasie-ooreenkoms" die ooreenkoms aangegaan tussen die Akkreditasie-owerheid en 'n waarmerkingsdiensverskaffer as deel van die akkreditasie van die waarmerkingsprodukte of -dienste gelewer deur daardie diensverskaffer;

"sertifiseringspraktykstaat" 'n staat uitgereik deur 'n sertifiseringsdiensverskaffer om die praktyke te spesifiseer wat die verskaffer gebruik om sertifikate voort te bring en uit te reik;

"sertifikaatbeleid" 'n genoemde stel reëls wat die toepaslikheid van 'n sertifikaat op 'n sekere gemeenskap of aanwendingsklas aandui, of op beide so 'n gemeenskap en so 'n klas, na gelang van die geval, met gemeenskaplike sekerheidsvereistes;

"konstitutiewe dokumente" beteken, in die geval van (a) 'n regspersoon, gewaarmerkte afskrifte van die akte van oprigting en statute, inkorporasiesertifikaat, stigtingsverklaring, vennootskapsooreenkoms of trustakte, na gelang van die geval; (b) 'n natuurlike persoon, sy of haar ID-dokument of paspoort;

"evalueerder" 'n onafhanklike ouditeursfirma soos bedoel in artikel 36(1)(c) van die Wet;

"ITU X.509" aanbeveling X. 509 van die Internasionale Telekommunikasie-unie ten opsigte van inligtingstegnologie, verbindings tussen oop stelsels, die gids-, openbaresleutel- en attribuutsertifikaatraamwerke;

"steungrens" die monetêre grens gespesifiseer vir steun op 'n gevorderde elektroniese handtekening;

"SABS/ISO 17799" 'n gebruikskode vir Inligtingsekerheidsbestuur wat deur die Suid-Afrikaanse Buro vir Standaarde as nasionale standaard aanvaar word – SABS ISO/IEC 17799;

"handtekeningskeppingsdata" unieke data, soos kodes of private kriptografiese sleutels, wat deur die ondertekenaar in die sertifikaat gemeld gebruik word om 'n elektroniese handtekening te skep;

“handtekening bekragtigingsdata” data soos kodes of openbare kriptografiese sleutels, wat gebruik word vir doeleindes van verifiëring van elektroniese handtekening;

"opskort", met betrekking tot 'n sertifikaat, om die geldigheidstydperk van 'n sertifikaat vanaf 'n bepaalde tydstip tydelik op te skort;

"die Wet" die Wet op Elektroniese Kommunikasie en Transaksies, 2002 (Wet nr. 25 van 2002);

"betroubare stelsel" rekenaarhardeware, sagtewarestelsels en prosedures wat voldoen aan die vereistes gestel in artikel 38(3) van die Wet;

"intrek", met betrekking tot 'n sertifikaat, die beëindiging van die geldigheidstydperk van 'n sertifikaat vir 'n spesifieke tyd.

HOOFSTUK I
Administrasie

Administrasie

2 (1) Hierdie Regulasies word deur die Akkreditasie-owerheid geadministreer.

(2) Die Akkreditasie-owerheid doen kwartaalliks aan die Minister verslag van sy werksaamhede.

Riglyne

3. Die Akkreditasie-owerheid kan riglyne, aanwysings of praktyknotas uitreik rakende sy administrasie van alle aangeleenthede wat ingevolge die Wet en hierdie Regulasies gedoen moet word.

Databasis

4. Die databasis bedoel in artikel 36(2) van die Wet moet ten minste die volgende bevat:

(a) die onderstaande besonderhede van elke waarmerkingsdiensverskaffer wie se waarmerkingsprodukte of -dienste geakkrediteer is:

(i) Die naam van die waarmerkingsdiensverskaffer;

(ii) die name sowel as die tegniese beskrywing van die geakkrediteerde waarmerkingsprodukte en -dienste volgens tipe, klas of ander beskrywing;

(iii) die besigheidsadres, telefoonnommer, webwerfadres, e-posadres en faksimileenommer van die waarmerkingsdiensverskaffer se kliëntediensdepartement; en

(iv) die identifikasienommer en webwerfruimte van die waarmerkingsdiensverskaffer se bewaarplek;

(b) 'n beskrywing van die akkreditasieproses en -vereistes, die funksies en dienste deur die Akkreditasie-owerheid aangebied;

(c) die klagteprosedures vir gebruikers van geakkrediteerde waarmerkingsprodukte en -dienste; en

(d) die kontakbesonderhede van die Akkreditasie-owerheid.

HOOFSTUK II
Aansoek om akkreditasie

Akkreditasie

5. Op aanvraag van 'n waarmerkingsdiensverskaffer kan die Akkreditasie-owerheid na voldoening aan die vereistes van die Wet en hierdie Regulasies, waarmerkingsprodukte of -dienste as gevorderde elektroniese handtekeninge akkrediteer.

Wyse van aansoek om akkreditasie

6. 'n Aansoek om akkreditasie ingevolge die Wet moet by die Akkreditasie-owerheid ingedien word op die wyse voorgeskryf deur die Akkreditasie-owerheid, en moet gestaaf word deur die inligting in Regulasie 7 en vergesel gaan van die nie-terugbetaalbare geld bepaal in Regulasie 29(1).

Voorgeskrewe inligting

7. 'n Aansoek om akkreditasie moet gestaaf word deur –

(a) die konstitutiewe dokumente van die aansoeker;

(b) indien die aansoeker 'n sertifiseringsdiensverskaffer is, 'n afskrif van sy sertifiseringspraktykstaat en sertifiseringsbeleid, opgestel ooreenkomstig 'Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework', asook 'n onderneming dat hy aan die vereistes van sy sertifiseringspraktykstaat en sertifiseringsbeleid kan en sal voldoen;

(c) 'n verklaring –

(i) met besonderhede van prosedures rakende die identifikasie en waarmerking van gebruikers van daardie waarmerkingsprodukte of -dienste, insluitend identifikasie van aangesig tot aangesig;

(ii) met besonderhede van die wyse waarop die aansoeker se waarmerkingsprodukte of -dienste voldoen aan elke bepaling van artikel 38(a), (b), (c), (d), en (e) van die Wet;

(iii) waarin die wyse aangespreek word waarop die aansoeker aan die vereistes neergelê in die Wet en in hierdie Regulasies sal voldoen;

(iv) met besonderhede van die wyse waarop inligting aangaande die aansoeker se waarmerkingsprodukte of -dienste asook die voorwaardes waarop daardie produkte of dienste aangebied of gebruik kan word, en hoe dit aan die algemene publiek en aan gebruikers van daardie waarmerkingsprodukte of –dienste beskikbaar gestel sal word;

(v) met besonderhede van die naamgewingskonvensies wat die aansoeker gaan gebruik, asook die wyse waarop die aansoeker naameienaarskap, naamgeskille en naambesluite sal hanteer; en

(vi) wat aandui hoe die aansoeker die beskikbaarheid van inligting aan derde partye wat op die waarmerkingsproduk of -diens staatmaak, sal verseker;

(d) volle besonderhede van aktiwiteite wat uitbestee is of sal word;

(e) die aansoeker se geouditeerde finansiële state vir die tydperk van drie jaar of minder, indien van toepassing, wat die aansoek onmiddellik voorafgaan;

(f) algemene tegniese spesifikasies van die aansoeker se harde- en sagtewarestelsels, sekerheidsbeleid, standaarde waaraan dit voldoen en beskikbare infrastruktuur asook die ligging van sy fasiliteite;

(g) die privaatheids- en sekerheidsbeleid wat die aansoeker in sy aktiwiteite sal volg;

(h) 'n organisasiekaart en die besonderhede en bevoegdhede van al die aansoeker se vertroude personeel;

(i) 'n staat van die aansoeker se –

(i) menslikehulpbronplan;

(ii) prosedures vir die verwerking van waarmerkingsprodukte en -dienste; en

(iii) oudits, meer spesifiek die gereeldheid en omvang van die aansoeker se oudits;

(j) gedetailleerde profiele van die aansoeker se direkteure, bestuur en vertroude personeel;

(k) 'n onderneming van die aansoeker dat hy die goedgekeurde evalueerder wat deur die Akkreditasie-owerheid aangestel is om 'n oudit uit te voer, teen die redelike tarief sal betaal wat deur 'n evalueerder in die omstandighede gehef word;

(l) 'n beskrywing van enige gebeurtenis, veral bankrotskap, wat die aansoeker se vermoë om as 'n waarmerkingsdiensverskaffer te funksioneer, wesenlik sou kan raak;

(m) 'n onderneming van die aansoeker om 'n prestasiewaarborg te gee en die jaarlikse akkreditasiegeld voorgeskryf in regulasie 29(1)(b) binne 30 dae na akkreditasie te betaal;

(n) bewys van voldoende versekeringsdekking gegrond op steungrense of ander aanvaarbare kriteria; en

(o) 'n staat van die mate van toeganklikheid van die aansoeker se fasiliteite vir die algemene publiek of die aansoeker se voornemende intekenaars.

Indiening van aansoeke

8 **(1)** Aansoeke om akkreditering moet per hand by die Akkreditasie-owerheid ingedien word.

(2) 'n Aansoek wat nie van al die voorgeskrewe inligting en gelde vergesel word nie, sal nie verwerk word nie.

(3) Aansoeke moet persoonlik by 'n aangewese beampte van die Akkreditasie-owerheid ingedien word.

Verwerking van aansoeke

9 **(1)** Die Akkreditasie-owerheid moet alle aansoeke om akkreditasie verwerk binne 45 dae na ontvangs van die laaste inligting wat ingevolge Regulasie 7 vereis word, maar kan hierdie tydperk in omstandighede buite sy beheer en om redes wat op skrif gestel moet word met hoogstens 45 werksdae verleng.

(2) Die Akkreditasie-owerheid moet 'n inspeksie of evaluering, na gelang van die geval, van die aansoeker en sy waarmerkingsprodukte of -dienste laat uitvoer kragtens die Wet en hierdie Regulasies.

Verlening van akkreditasie

10 **(1)** Indien die Akkreditasie-owerheid oortuig is dat die aansoeker aan sy akkreditasiekriteria voldoen het, moet die Akkreditasie-owerheid –

(a) sy besluit skriftelik aan die aansoeker meedeel;

(b) die aansoeker in kennis stel van enige beperking of voorwaarde verbonde aan die verlening van akkreditasie;

(c) die aansoeker in kennis stel van die datum waarop die akkreditasie van krag word;

(d) die aansoeker versoek om die voorgeskrewe jaarlikse intekengeld te betaal en die prestasiewaarborg binne 30 dae na akkreditasie in te dien;

(e) by betaling van alle verskuldigde gelde, 'n akkreditasiesertifikaat uitreik vir elke waarmerkingsproduk of -diens wat geakkrediteer is, met vermelding van enige beperking op of ander voorwaarde van akkreditasie; en

(f) die waarmerkingsdiensverskaffer in kennis stel dat akkreditasie onderhewig is aan die sluiting van 'n akkreditasie-ooreenkoms deur alle partye.

(2) 'n Waarmerkingsdiensverskaffer sal onderhewig wees aan periodieke oudits soos van tyd tot tyd deur die Akkreditasie-owerheid bepaal word.

(3) Geen waarmerkingsdiensverskaffer mag waarmerkingsprodukte of -dienste as waarmerkingsprodukte of -dienste verskaf nie tensy 'n akkreditasiesertifikaat deur die Akkreditasie-owerheid vir elke waarmerkingsproduk of -diens aan hom uitgereik is nie.

(4) 'n Waarmerkingsdiensverskaffer wie se waarmerkingsprodukte of -dienste geakkrediteer is, kan sommige of al sy werksaamhede uitbestee of agente of kontrakteurs daarvoor aanstel, met dien verstande dat –

(a) die Akkreditasie-owerheid skriftelik daarvan verwittig is;

(b) die agent of kontrakteur, na gelang van die geval, deur die Akkreditasie-owerheid vir die doeleindes van die spesifieke waarmerkingsproduk of -diens geouditeer is, waarvan die koste ten volle deur die waarmerkingsdiensverskaffer of deur sy of haar agent of kontrakteur gedra moet word;

(c) die Akkreditasie-owerheid die aanstelling van hierdie agente of kontrakteurs skriftelik moet goedkeur;

(d) hierdie agente of kontrakteurs eweneens aan die Wet, hierdie Regulasies en die akkreditasie-ooreenkoms wat geld vir die verskaffer van die waarmerkingsproduk of -dienste wat geakkrediteer is, moet voldoen; en

(e) die waarmerkingsdiensverskaffer verantwoordelik bly vir die werksaamhede van agente of kontrakteurs in hul uitvoering van die waarmerkingsdiensverskaffer se funksies.

Publikasie van akkreditasie

11. Die Akkreditasie-owerheid moet besonderhede van geakkrediteerde verskaffers van waarmerkingsprodukte en -dienste in 'n databasis wat toeganklik is vir die publiek en in enige ander medium wat hy as geskik beskou, publiseer.

Afkeuring van aansoek om akkreditasie

12. Die Akkreditasie-owerheid kan weier om 'n waarmerkingsproduk of -diens te akkrediteer indien –

(a) die aansoeker die Akkreditasie-owerheid nie van die inligting wat in Regulasie 7 bepaal word, voorsien het nie of indien die inligting nie van 'n bevredigende standaard of gehalte is nie;

(b) die aansoeker nie in die posisie is om aan die Wet of hierdie Regulasies te voldoen nie;

(c) 'n aansoeker versuim om aan enige aanwysing of vereiste van die Akkreditasie-owerheid te voldoen;

(d) 'n waarmerkingsdiensverskaffer versuim om 'n oudit te ondergaan of om in ooreenstemming met 'n oudit, inspeksie of evaluering op te tree; of

(e) daar enige ander geldige rede bestaan om akkreditering te weier;

met dien verstande dat die Akkreditasie-owerheid 'n aansoeker die geleentheid kan gee om 'n skriftelike voorlegging te doen met betrekking tot die redes waarom akkreditasie geweier is, en 'n aansoeker die geleentheid kan gee om te voldoen aan enige vereiste wat die aansoeker se waarmerkingsproduk of -diens akkrediteerbaar sal maak binne 'n tydperk van 30 dae nadat die Akkreditasie-owerheid sy redes vir die weiering van akkreditasie aan die aansoeker voorsien het.

HOOFSTUK III
Vereistes vir sertifiseringsdiensverskaffers

Tegniese en ander vereistes waaraan sertifikate moet voldoen

13. Alle sertifikate wat deur 'n akkreditasiediensverskaffer uitgereik word moet, indien dit deur die Akkreditasie-owerheid geakkrediteer is, aan die hoogste

gevestigde internasionale standaarde voldoen, insluitend maar nie beperk nie tot die ITU X.509-standaard, en moet onder andere die volgende data bevat:

(a) die reeksnommer van die sertifikaat wat dit van ander sertifikate onderskei;

(b) die handtekeningsalgoritme-identifiseerder wat die algoritme identifiseer wat die sertifiseringsdiensverskaffer gebruik om die sertifikaat te teken;

(c) die uitreiker se naam, synde die naam van die sertifiseringsdiensverskaffer wat die sertifikaat uitgereik het;

(d) die geldigheidstydperk van die sertifikaat, synde die begin en die einde van die geldigheidstydperk van die sertifikaat;

(e) die naam of skuilnaam van die intekenaar wie se openbare sleutel deur die sertifikaat geïdentifiseer word;

(f) inligting oor die intekenaar se openbare sleutel; en

(g) bevestiging dat dit 'n sertifikaat is wat deur die Akkreditasie-owerheid geakkrediteer is.

Vereistes vir die uitreiking van sertifikate

14 **(1)** 'n Sertifiseringsdiensverskaffer moet die identiteit van 'n persoon of persone wat aansoek om 'n sertifikaat doen, op betroubare wyse bepaal, wat identifikasie van die gebruiker of gemagtigde sleutelhouer van aangesig tot aangesig moet insluit.

(2) 'n Sertifiseringsdiensverskaffer mag 'n sertifikaat slegs aan 'n voornemende intekenaar uitreik nadat eersgenoemde –

(a) 'n versoek om uitreiking van die voornemende intekenaar ontvang het; en

(b) al die praktyke en prosedures nagekom het wat in sy sertifiseringspraktykstaat en sertifikaatbeleid uiteengesit is, insluitend prosedures vir die identifikasie van die voornemende intekenaar van aangesig tot aangesig.

(3) Deur 'n sertifikaat uit te reik word die sertifiseringsdiensverskaffer geag om aan enige persoon wat redelikerwys staatmaak op die sertifikaat of op 'n gevorderde elektroniese handtekening wat geverifieer kan word deur middel van die openbare sleutel wat op die sertifikaat aangetoon word, voor te hou dat die sertifiseringsdiensverskaffer die sertifikaat uitgereik het in ooreenstemming met sy sertifiseringspraktykstaat en sertifikaatbeleid wat deur verwysing by die sertifikaat ingelyf is.

(4) Waar 'n sertifiseringspraktykstaat en sertifikaatbeleid deur verwysing by 'n sertifikaat ingelyf is, is die volgende bepalings van toepassing in so verre die voorstellings nie onbestaanbaar met die sertifiseringspraktykstaat en sertifikaatbeleid is nie:

(a) Die sertifiseringsdiensverskaffer het by die uitreiking van die sertifikaat aan al die toepaslike vereistes van die Wet, hierdie Regulasies en die akkreditasie-ooreenkoms voldoen, en indien die sertifiseringsdiensverskaffer die sertifikaat gepubliseer of op 'n ander wyse die sertifikaat aan 'n persoon beskikbaar gestel het wat daarop staatmaak, dat die intekenaar wat in die sertifikaat genoem word, dit aanvaar het;

(b) die intekenaar wat in die sertifikaat geïdentifiseer is, hou die private sleutel wat ooreenstem met die openbare sleutel wat in die sertifikaat genoem word;

(c) die intekenaar se openbare sleutel en private sleutel vorm 'n werkende sleutelpaar;

(d) alle inligting in die sertifikaat is akkuraat, tensy die sertifiseringsdiensverskaffer in die sertifikaat gemeld of deur verwysing 'n verklaring in die sertifikaat ingelyf het dat die akkuraatheid van die gespesifiseerde inligting nie bevestig word nie; en

(e) die sertifiseringsdiensverskaffer dra geen kennis van enige wesenlike feit wat, as dit in die sertifikaat ingesluit sou wees, die betroubaarheid van die voorstellings in subparagrawe (a), (b), (c) en (d) sou aantas nie.

Vereistes vir sertifiseringspraktykstate

15 (1) Sertifiseringsdiensverskaffers wie se waarmerkingsprodukte of -dienste geakkrediteer is, moet 'n sertifiseringspraktykstaat en sertifikaatbeleid vir geakkrediteerde waarmerkingsproduk of -diens van elke tipe, klas of beskrywing uitreik en opvallend openbaar beskikbaar stel op die wyse en in die formaat wat deur die Akkreditasie-owerheid bepaal word.

(2) 'n Sertifiseringsdiensverskaffer wie se waarmerkingsprodukte of -dienste geakkrediteer is, moet –

(a) 'n gewaarmerkte afskrif van elke sertifiseringspraktykstaat en sertifikaatbeleid wat vir geakkrediteerde waarmerkingsprodukte en -dienste gebruik word, by die Akkreditasie-owerheid indien;

(b) voordat hy enige wesenlike verandering aan sodanige sertifiseringspraktykstaat en sertifikaatbeleid aanbring, insluitend veranderings –

(i) in die identifikasieproses wat die betroubaarheid van sertifikate verminder;

(ii) aan die steungrens van die sertifikate; of

(iii) in die voortbring, berging of gebruik van sleutels;

met die Akkreditasie-owerheid oorleg pleeg;

(c) die Akkreditasie-owerheid, sy intekenaars en staatmakende partye deur publikasie op sy webwerf verwittig van enige voorval wat die geldigheid van 'n sertifiseringspraktykstaat en sertifikaatbeleid wat reeds by die Akkreditasie-owerheid ingedien is, in sy geheel of gedeeltelik nadelig of wesenlik raak of kan raak;

(d) sy sertifiseringspraktykstaat en sertifikaatbeleid nakom wanneer hy geakkrediteerde sertifikate van 'n tipe, klas of beskrywing uitreik;

(e) alle koste en gelde deur intekenaars en staatmakende partye betaalbaar ten opsigte van die uitreiking, intrekking, opskorting, herwinning of verifiëring van die status van 'n geakkrediteerde sertifikaat van elke tipe, klas of beskrywing deur hom uitgereik, duidelik aantoon.

(3) 'n Sertifiseringsdiensverskaffer moet die volgende dokumente gebruik om 'n intekenaar of aansoeker om 'n sertifikaat of 'n ander waarmerkingsertifikaat of -diens te identifiseer en te waarmerk tydens aanvanklike registrasie, roetine hersleuteling, hersleuteling na intrekking en wanneer opskortings- of intrekkingsversoeke verwerk word:

(a) Waar die intekenaar of aansoeker 'n natuurlike persoon is, 'n kombinasie van die oorspronklike eksemplare van 'n –

(i) nasionale identiteitsdokument;

(ii) paspoort; of

(iii) lopende, geldig geakkrediteerde sertifikaat slegs vir gebruik as identiteit vir die hernuwing van 'n sertifikaat;

(b) waar die intekenaar of aansoeker 'n vennootskap is, die konstitutiewe dokumente van die vennootskap asook die dokumente waarna in paragraaf (a) verwys word ten opsigte van elke vennoot van die vennootskap, insluitend die gemagtigde sleutelhouer;

(c) waar die intekenaar of aansoeker 'n maatskappy, beslote korporasie, trust of ander regsliggaam is, 'n kombinasie van gewaarmerkte afskrifte van –

(i) die betrokke konstitutiewe dokumente;

(ii) die aansoeker se jongste geouditeerde finansiële state;

(iii) 'n besluit of volmag van die direkteure wat 'n spesifieke persoon magtig om aansoek te doen om of om andersins te handel met 'n spesifieke sertifiseringsdiensverskaffer met betrekking tot die uitreiking, hernuwing of vervanging van sertifikate;

(iv) die dokumente waarna in paragraaf (a) verwys word van die direkteure, lede of trustees van die aansoeker en die gemagtigde sleutelhouer, tesame met 'n besluit wat die verteenwoordiger as die gemagtigde sleutelhouer aanstel.

Pligte van intekenaars

16. 'n Sertifiseringsdiensverskaffer is verantwoordelik om toe te sien dat sy intekenaars aan die volgende voldoen:

(a) As die intekenaar wie se openbare sleutel in 'n sertifikaat gemeld staan te word wat deur die sertifiseringsdiensverskaffer uitgereik en deur die aansoeker aanvaar staan te word die sleutelpaar voortbring, moet die intekenaar hierdie sleutel met behulp van 'n betroubare stelsel voortbring;

(b) alle wesenlike voorstellings wat die intekenaar op 'n sertifiseringsdiens maak om 'n sertifikaat te bekom, insluitend alle inligting wat aan die intekenaar bekend is en in die sertifikaat weergegee word, moet na die beste van sy wete en oortuiging akkuraat en volledig wees, ongeag of sulke voorstellings deur die sertifiseringsdiensverskaffer bevestig word;

(c) 'n sertifikaat word geag deur die te intekenaar aanvaar te wees as hy of sy –

(i) die sertifikaat in 'n bewaarplek publiseer of dit vir gebruik aan 'n derde party beskikbaar maak;

(ii) op 'n ander wyse goedkeuring van 'n sertifikaat toon terwyl hy of sy die inhoud ken of daarvan bewus is;

(d) deur 'n sertifikaat wat deur 'n sertifiseringsdiensverskaffer uitgereik is, te aanvaar, sertifiseer die intekenaar wat in die sertifikaat genoem word teenoor almal wat redelikerwys op die inligting in die sertifikaat vervat staatmaak dat –

(i) die intekenaar regmatig die private sleutel hou wat ooreenstem met die openbare sleutel wat in die sertifikaat gemeld word;

(ii) alle voorstellings wat deur die intekenaar aan die verskaffer van die sertifiseringsdiens gemaak is en wesenlik is met betrekking tot die inligting wat in die sertifikaat verstrek word, waar is; en

(iii) alle inligting waarvan die intekenaar kennis dra, waar is;

(e) deur 'n sertifikaat wat deur 'n sertifiseringsdiensverskaffer uitgereik is te aanvaar, aanvaar die intekenaar wat in die sertifikaat geïdentifiseer is 'n plig om redelike sorg te dra om beheer te behou oor die private sleutel wat ooreenstem met die openbare sleutel wat in die sertifikaat gemeld word en om die bekendmaking daarvan aan 'n persoon wat nie gemagtig is om die intekenaar se gevorderde elektroniese handtekening te skep nie, te voorkom,

en hierdie plig sal voortduur solank die sertifikaat geldig is en tydens enige tydperk van opskorting van die sertifikaat;

(f) 'n intekenaar wat 'n sertifikaat aanvaar het moet, indien die private sleutel wat ooreenstem met die openbare sleutel wat in die sertifikaat vermeld is, gekompromitteer is, so gou moontlik die uitreikende sertifiseringsdiensverskaffer versoek om die sertifikaat en die bewys van eienaarskap in te trek of op te skort.

Verantwoordelikhede van sertifiseringsdiensverskaffers

17. 'n Sertifiseringsdiensverskaffer wie se waarmerkingsprodukte of dienste geakkrediteer is, moet –

(a) in 'n databasis met openbare toegang die volgende bekend maak:

(i) sy sertifikaat wat die openbare sleutel bevat wat ooreenstem met die private sleutel wat deur daardie sertifiseringsdiensverskaffer gebruik word om 'n ander sertifikaat digitaal te onderteken (waarna in hierdie artikel as die sertifiseringsdiensverskaffersertifikaat verwys word);

(ii) sy sertifikasiepraktykstaat en sertifikaatbeleid;

(iii) kennisgewing van die intrekking of opskorting van sy sertifiseringsdiensverskaffersertifikaat;

(iv) enige ander feit wat óf die betroubaarheid van 'n sertifikaat wat deur die sertifiseringsdiensverskaffer uitgereik is, óf die sertifiseringsdiensverskaffer se vermoë om sy dienste te lewer, wesenlik en nadelig raak; en

(v) al sy geakkrediteerde waarmerkingsprodukte en -dienste;

(b) 'n betroubare stelsel gebruik om sy dienste en funksies te verrig, insluitend die voortbring en bestuur van sy sleutels, die voortbring en bestuur van intekenaars se sleutels, die uitreiking, hernuwing, opskorting of intrekking van geakkrediteerde sertifikate, die instandhouding van sy bewaarplek en die publikasie van geakkrediteerde sertifikate;

(c) in geval van 'n voorval wat 'n sertifiseringsdiensverskaffer se betroubare stelsels soos bedoel in artikels 38(2)(a),(b), (c) en (d) van die Wet of sy sertifiseringsdiensverskaffersertifikaat wesenlik en nadelig raak, moet die sertifiseringsdiensverskaffer redelike pogings aanwend om enige persoon van wie dit bekend is of voorsien kan word dat hy of sy deur daardie voorval geraak sal word in kennis te stel, of optree in ooreenstemming met prosedures wat sodanige voorval reël en gespesifiseer word in sy sertifikasiepraktykstaat en sertifikaatbeleid;

(d) gedokumenteerde beleide, prosedures en praktyke ten opsigte van sy totale bedryfsomgewing ontwikkel, vestig, handhaaf en byhou;

(e) enige voorval wat sy betroubare stelsel in die algemeen wesenlik kan raak, aan die Akkreditasie-owerheid rapporteer;

(f) toesien dat al sy personeellede bekwame en geskikte mense is en die nodige kennis, tegniese kwalifikasies en vakkundigheid besit om hul pligte effektief uit te voer; en

(g) voldoen aan die Wet, hierdie Regulasies, die akkreditasie-ooreenkoms wat op hom van toepassing is en aan die riglyne of aanwysings uitgereik deur die Akkreditasie-owerheid.

Vereistes voor staking van besigheid

18 (1) 'n Sertifiseringsdiensverskaffer moet, voordat hy ophou om as sulks op te tree, aan die vereistes van die Wet en hierdie Regulasies, die akkreditasie-ooreenkoms en alle riglyne of aanwysings wat die Akkreditasie-owerheid mag uitreik, voldoen.

(2) 'n Sertifiseringsdiensverskaffer wat versuim om aan hierdie Regulasie te voldoen is, onderworpe aan die bepalings van die betrokke intekenaar se ooreenkoms of die gemenereg, aanspreeklik vir enige verlies of skade gely deur intekenaars of staatmakende partye.

Aanspreeklikheid van sertifiseringsdiensverskaffers

19. 'n Sertifiseringsdiensverskaffer is aanspreeklik vir enige skade gedoen aan enige entiteit of natuurlike persoon wat redelikerwys staatmaak op 'n sertifikaat wat deur die Akkreditasie-owerheid geakkrediteer is –

(a) ten opsigte van die akkuraatheid ten tye van die uitreiking van alle inligting in die sertifikaat vervat en die feit dat die sertifikaat al die voorgeskrewe besonderhede bevat;

(b) vir versekering dat die ondertekenaar wat in die sertifikaat geïdentifiseer is ten tye van die uitreiking van die sertifikaat die handtekeningskeppende data gehou het wat ooreenstem met die handtekeningverifiërende data wat in die sertifikaat verstrek of geïdentifiseer word;

(c) vir versekering dat die handtekeningskeppende data gehou en die handtekeningverifiërende data op komplementêre wyse gebruik kan word in gevalle waar die sertifiseringsdiensverskaffer beide voortbring;

(d) met betrekking tot die publikasie van kennisgewings van opskorting of intrekking in die bewaarplek wat in die sertifikaat vir die publikasie van opskortings- of intrekkingskennisgewings gespesifiseer word; en

(e) met betrekking tot dienste wat hy onderneem het om aan intekenaars te lewer,

tensy die sertifiseringsdiensverskaffer bewys dat hy nie nalatig opgetree het nie.

Rekords gehou te word

20 (1) Vir die doeleindes van artikel 38(4)(f) van die Wet moet die volgende rekords vir 'n tydperk van 7 jaar of vir die tydperk wat die Akkreditasie-owerheid mag bepaal, gehou word:

(a) Aansoeke om uitreiking van sertifikate;

(b) registrasie en verifiëringsdokumente van sertifikate wat voortgebring is;

(c) sertifikate op so 'n wyse dat –

(i) niemand behalwe partye daartoe gemagtig veranderings daaraan of toevoeging daartoe kan maak nie;

(ii) dit moontlik is om te verifieer dat die inligting korrek is;

(iii) die sertifikaat slegs vir die publiek beskikbaar is indien die ondertekenaar uitdruklik daartoe instem;

(d) inligting oor opgeskorte sertifikate;

(e) inligting oor verstreke en ingetrekte sertifikate;

(f) betroubare rekords en logboeke vir kernwerksaamhede van die sertifiseringsdiensverskaffer, welke werksaamhede sertifikaatbestuur, sleutelvoortbringing en administrasie van sy rekenaarfasiliteite insluit.

(2) 'n Geakkrediteerde waarmerkingsdiensverskaffer moet sy bewaarplek op so 'n wyse in stand hou dat intekenaars en staatmakende partye geredelik toegang daartoe het.

(3) Alle rekords moet op so 'n wyse bewaar word dat die sekerheid, integriteit en toeganklikheid van die inligting en rekords vir die herwinning en inspeksie daarvan verseker is.

(4) Alle geargiveerde rekords mag herteken word om hul integriteit en betroubaarheid te beskerm in die geval van tegnologiese vooruitgang wat die mate waarin daar op die oorspronklike rekords gesteun kan word, kan affekteer.

Opskorting en intrekking van sertifikate

21 (1) Tensy 'n sertifiseringsdiensverskaffer en 'n intekenaar anders ooreenkom, moet die sertifiseringsdiensverskaffer 'n sertifikaat so gou moontlik opskort nadat 'n versoek ontvang is van 'n persoon van wie die sertifiseringsdiensverskaffer redelikerwys meen dat hy of sy –

(a) die intekenaar is wat in die sertifikaat gemeld word;

(b) 'n persoon is wat behoorlik gemagtig is om vir daardie intekenaar op te tree;

(c) 'n persoon is wat namens daardie intekenaar optree wat nie beskikbaar is nie.

(2) Die sertifiseringsdiensverskaffer moet 'n sertifikaat intrek wat hy uitgereik het –

(a) na ontvangs van 'n intrekkingsversoek van die intekenaar in die sertifikaat gemeld en wat bevestig dat die persoon wat die intrekking versoek, die intekenaar is of 'n agent van die intekenaar met magtiging om die intrekking aan te vra;

(b) na ontvangs van 'n gewaarmerkte afskrif van die intekenaar se doodsertifikaat, of na bevestiging deur middel van ander bewysmateriaal dat die intekenaar oorlede is; of

(c) by aanbieding van dokumente dat 'n intekenaar wat 'n regspersoon is, gelikwideer of gederegistreer is.

(3) 'n Sertifiseringsdiensverskaffer moet 'n sertifikaat intrek, met of sonder toestemming van die intekenaar in die sertifikaat gemeld, indien –

(a) 'n wesenlike feit in die sertifikaat weergegee vals is;

(b) 'n vereiste vir die uitreiking van die sertifikaat nie nagekom is nie;

(c) die sertifiseringsdiensverskaffer se private sleutel of betroubare stelsel op 'n wyse gekompromitteer is wat die betroubaarheid van die sertifikaat wesenlik raak; of

(d) 'n intekenaar 'n ooreenkoms met die sertifiseringsdiensverskaffer verbreek het.

(4) Wanneer 'n intrekking soos bedoel in subregulasie (3) gedoen word, moet die sertifiseringsdiensverskaffer die intekenaar in die ingetrekte sertifikaat

gemeld onmiddellik in kennis stel, indien moontlik en die intrekking in sy bewaarplek publiseer.

Publikasie van opskorting en intrekking van sertifikate

22. Binne 24 uur na opskorting of intrekking van 'n sertifikaat deur 'n sertifiseringsdiensverskaffer moet die sertifiseringsdiensverskaffer 'n getekende kennisgewing van die opskorting of intrekking in die bewaarplek wat in die sertifikaat vir die publikasie van kennisgewing van opskorting of intrekking gespesifiseer is, publiseer, en waar meer as een bewaarplek gespesifiseer is, moet die sertifiseringsdiensverskaffer getekende kennisgewings van die opskorting of intrekking in al daardie bewaarplekke publiseer.

HOOFSTUK IV
Opskorting, intrekking en beëindiging

Opskorting en intrekking

23 (1) Indien 'n waarmerkingsdiensverskaffer wie se waarmerkingsprodukte of -dienste geakkrediteer is –

(a) versuim of ophou om aan enigeen van die vereistes, voorwaardes of beperkings te voldoen onderworpe waaraan akkreditering kragtens artikel 38 van die Wet verleen of erkenning ingevolge artikel 40 van die Wet gegee is;

(b) **(i)** deur die Akkreditasie-owerheid ingelig is dat laasgenoemde van voorneme is om die waarmerkingsdiensverskaffer se akkreditasie op te skort of in te trek en redes of 'n beskrywing van die skending verstrek is;

(ii) deur die Akkreditasie-owerheid versoek is om die nie-voldoening of skending binne 'n redelike tyd reg te stel;

(iii) die geleentheid gegee is om binne 'n redelike tyd op die bewerings te reageer;

en versuim om óf skriftelik te reageer óf die skending binne die gespesifiseerde tyd reg te stel, kan die Akkreditasie-owerheid die akkreditasie van waarmerkingsprodukte of -dienste wat deur daardie nie-voldoening geaffekteer word, opskort of intrek.

(2) Voordat die akkreditasie van waarmerkingsprodukte of -dienste opgeskort of ingetrek word, moet die Akkreditasie-owerheid –

(a) die waarmerkingsdiensverskaffer skriftelik van sy besluit asook van die redes vir die besluit in kennis stel;

(b) 'n kennisgewing in sy databasis publiseer dat hy besig is om die akkreditasie van die betrokke waarmerkingsproduk of -diens in te trek;

(c) 'n Akkreditasiebeampte en 'n evalueerder aanstel om toesig te hou oor die detail van die afwikkeling van die diensverskaffer se geakkrediteerde werksaamhede;

(d) verseker dat die waarmerkingsdiensverskaffer die intrekking deur middel van die vinnigste moontlike medium aan die intekenaars en staatmakende partye meedeel;

(e) verseker dat die diensverskaffer alle geakkrediteerde waarmerkingsprodukte of –dienste wat aan sy gebruikers uitgereik is intrek en die wyse, tyd en datum van intrekking aanteken;

(f) verseker dat die Akkreditasiebeampte en die evalueerder elkeen 'n verslag uitreik ter sertifisering van nakoming van die voorgeskrewe intrekkingsproses;

(g) reëlings tref vir die behoud van rekords soos voorsien kragtens artikel 38(4)(f) van die Wet ooreenkomstig die bepaalde wyse en tydperk;

(h) in sy diskresie of op versoek intekenaars help om 'n alternatiewe verskaffer van waarmerkingsprodukte of -dienste te vind;

(i) verseker dat die intrekking met die minste ontwrigting vir intekenaars en ondersteunende partye uitgevoer word.

(3) Die Akkreditasie-owerheid moet alle opskortings en intrekkings in sy vir die publiek toeganklike databasis publiseer.

Prosedure na opskorting

24 (1) Nadat die Akkreditasie-owerheid akkreditasie opgeskort het, kan die Akkreditasie-owerheid –

(i) enige stappe doen wat nodig is om te bevestig of die waarmerkingsdiensverskaffer steeds in gebreke bly om aan enigeen van die vereistes, voorwaardes of beperkings onderworpe waaraan akkreditasie verleen of erkenning gegee is, te voldoen;

(ii) enige deel van die prosedure in artikel 39(2) van die Wet herhaal;

(iii) die waarmerkingsdiensverskaffer se vordering met die regstelling van die skending moniteer;

(iv) enige spesifieke versoek van die betrokke waarmerkingsdiensverskaffer oorweeg;

(v) sy opskortingsbesluit in heroorweging neem.

(2) Indien die skending van die vereistes, voorwaardes of beperkings onderworpe waaraan akkreditering verleen of erkenning gegee is langer as 'n tydperk van 30 dae na opskorting voortduur, kan die betrokke akkreditasie ingetrek word.

(3) Indien die skending van die vereistes, voorwaardes of beperkings onderworpe waaraan akkreditering verleen of erkenning gegee is, reggestel word, kan die Akkreditasie-owerheid die opskorting ophef en akkreditasie herstel.

(4) Die Akkreditasie-owerheid moet, wanneer 'n opgeskorte waarmerkingsproduk of –diens 'n ingetrekte waarmerkingsproduk of -diens word, of wanneer die opskorting van 'n waarmerkingsproduk of -diens opgehef word en die betrokke akkreditasie herstel word, sodanige inligting in sy vir die publiek toeganklike databasis publiseer.

Beëindiging

25 (1) 'n Waarmerkingsdiensverskaffer wie se waarmerkingsprodukte of -dienste geakkrediteer is, kan sodanige akkreditering te eniger tyd beëindig, onderworpe aan die Wet, hierdie Regulasies en die akkreditasie-ooreenkoms, met dien verstande dat die diensverskaffer –

(a) kennis van sy voorneme om sy werksaamhede te staak 90 dae voor die beëindiging van sy akkreditasie moet gee, of voordat hy ophou om as waarmerkingsdiensverskaffer op te tree;

(b) voor die beëindiging van sy akkreditasie, of voordat hy ophou om as waarmerkingsdiensverskaffer op te tree, na gelang van die geval, die voorneme in die dagpers en op die wyse wat die Akkreditasie-owerheid mag bepaal, moet adverteer;

(c) 60 dae kennis van sy voorneme om op te hou om as waarmerkingsdiensverskaffer op te tree aan sy intekenaars en aan houers van elke oningetrekte of onverstreke sertifikaat wat hy uitgereik het, moet gee, deur die kennisgewing per elektroniese en per geregistreerde pos te stuur;

(d) moet toesien dat die staking van sy aktiwitieite die minste moontlike ontwrigting vir sy intekenaars en vir persone wat sertifikate moet verifieer, veroorsaak;

(e) redelike vergoeding (nie meer as die koste om nuwe sertifikate te verkry nie) aan intekenaars moet betaal vir die intrekking van sertifikate voor die verstrykingsdatum;

(f) reëlings moet tref vir die behoud van rekords soos voorsien kragtens artikel 38(4)(f) van die Wet ooreenkomstig die bepaalde wyse en tydperk; en

(g) alle verstreke sertifikate vernietig na voldoening aan die vereistes van hierdie regulasie.

(2) Die Akkreditasie-owerheid moet die bepalings van subregulasies 23(2)(c), (d), (e), (f), (g) en (h) nakom wanneer hy kennis van beëindiging van 'n waarmerkingsdiensverskaffer ontvang.

Vereistes ten opsigte van inligtingsekerheid

26. Geakkrediteerde waarmerkingsdiensverskaffers moet 'n sekerheidsbeleid, wat ten minste moet voldoen aan relevante standaarde soos SABS/ISO 17799, nakom.

Evalueerder

27 (1) Die Akkreditasie-owerheid moet een of meer evalueerders aanstel wat periodieke oudits moet uitvoer van tegniese en ander voldoening deur waarmerkingsdiensverskaffers.

(2) Die gelde vir die dienste van 'n evalueerder word betaal deur die waarmerkingsdiensverskaffer ten opsigte van wie 'n oudit gedoen is.

(3) Die Akkreditasie-owerheid moet toesien dat 'n waarmerkingsdiensverskaffer voor die oudit skriftelik onderneem om vir die evalueerder se dienste te betaal.

(4) Die Akkreditasie-owerheid moet eers die tarief wat deur 'n evalueerder gevra word, goedkeur, welke tarief in die omstandighede redelik moet wees.

(5) Die goedgekeurde evalueerder moet die waarmerkingsdiensverskaffer of sy waarmerkingsprodukte of -dienste ouditeer in ooreenstemming met die Wet, hierdie Regulasies en die riglyne wat van tyd tot tyd deur die Akkreditasie-owerheid neergelê word.

(6) 'n Evalueerder wat 'n oudit uitvoer moet sy verslag binne vyf dae na voltooiing van die opdrag, of soos andersins ooreengekom, aan die Akkreditasie-owerheid voorlê.

(7) Voorts moet 'n evalueerder:

(a) toepaslike tegnieke aanwend;

(b) die betroubaarheid en kwaliteit evalueer van die gebruikte stelsels, die integriteit, vertroulikheid en beskikbaarheid van data asook die

voldoening aan die spesifikasies ingesluit in enige prosedurehandleiding en die sekerheidsplan goedgekeur deur die Akkreditasie-owerheid, wat ten minste moet voldoen aan relevante standaarde soos SABS/ISO 17799;

(c) vasstel of betroubare stelsels soos bedoel in artikel 38 gebruik word;

(d) in elke geval 'n verslag met bevindings, gevolgtrekkings en aanbevelings uitreik.

(8) Indien die Akkreditasie-owerheid dit verlang, moet die evalueerder voorts:

(a) die oudits opvolg om te bepaal of die waarmerkingsdiensverskaffer die regstellende stappe wat in die aanbevelings voorgestel is, gedoen het;

(b) bykomende verslae uitreik;

(c) deelneem aan gebeurlikheidsimulasies;

(d) bykomende afskrifte voorsien van alle verslae wat aan die Akkreditasie-owerheid uitgereik is.

Administrasie en kontrole

28. Akkreditasie verleen deur die Akkreditasie-owerheid is onderworpe aan die voorwaarde dat 'n waarmerkingsdiensverskaffer die Akkreditasie-owerheid of 'n evalueerder aangestel deur die Akkreditasie-owerheid, na gelang van die geval, tydens normale kantoorure vir ouditdoeleindes op sy perseel moet toelaat en op versoek enige relevante boek, rekord, stawende of ander dokument ter insae beskikbaar moet stel, alle inligting wat redelikerwys deur die Akkreditasie-owerheid of evalueerder aangevra word moet verstrek en al die bystand moet gee wat vir die oudit nodig is.

HOOFSTUK V
Algemeen

Gelde betaalbaar

29 (1) Die gelde wat betaal moet word deur waarmerkingsdiensverskaffers wat aansoek doen om akkreditasie of wie se waarmerkingsprodukte of -dienste geakkrediteer is, is soos volg:

(a) Aansoekgeld: R20, 000.00

(b) Jaarlikse akkreditasiegeld per produk of diens: R10, 000.00

(c) Prestasiewaarborg per produk of diens: R10, 000.00

(2) Gelde betaalbaar aan die Akkreditasie-owerheid moet direk in die Departement se bankrekening inbetaal word, en bewys van betaling moet aan die Akkreditasie-owerheid voorsien word.

(3) Geen gelde is terugbetaalbaar nie, behalwe die prestasiewaarborg.

(4) Die Akkreditasie-owerheid kan die prestasiewaarborg gebruik indien die geakkrediteerde waarmerkingsdiensverskaffer in gebreke bly om enige gelde wat ingevolge die Wet of hierdie Regulasies verskuldig is, te betaal.

(5) Behoudens die eerste jaarlikse akkreditasiegeld, wat by akkreditasie betaalbaar is, is die jaarlikse akkreditasiegeld voor of op 31 Januarie van elke jaar betaalbaar.

Kort titel

30. Hierdie regulasies sal bekendstaan as die Akkreditasieregulasies en kom in werking op 'n datum deur die Minister gepubliseer deur kennisgewing in die Staatskoerant.