

GOVERNMENT NOTICE

**DEPARTMENT OF COMMUNICATIONS
(SOUTH AFRICAN ACCREDITATION AUTHORITY)**

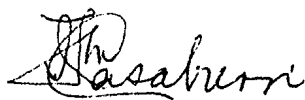
No. 504

20/06/2007

**ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT, 2002
(ACT NO. 25 OF 2002)**

ACCREDITATION REGULATIONS

The Minister of Communications has, in terms of section 41 read with section 94 of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002), made the regulations in the Schedule.



**Dr Ivy Matsepe-Casaburri
Minister of Communications**

Schedule

**REGULATIONS UNDER THE ELECTRONIC COMMUNICATIONS AND
TRANSACTIONS ACT, 2002****ACCREDITATION REGULATIONS****ARRANGEMENT OF REGULATIONS**

<i>Subject</i>	<i>Regulation No.</i>
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 requirements	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
Audits and evaluations	27
Administration and supervision	28
CHAPTER V: General	
Fees payable	29
Short title	30

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 –

"audit" means, in general, an audit by an auditor in compliance with Chapter VI of the Act and these regulations, and in the case of a certification service provider whose authentication products or services are based on Public Key Infrastructure "audit" means an audit by an auditor in compliance with Chapter VI of the Act and these regulations, including an audit in accordance with WebTrust, and "audit report" has a corresponding meaning;

"auditor" means an independent auditing firm contemplated in section 36(1)(c) of the Act that has been nominated by the South African Accreditation Authority to the Panel of Auditors specified on its website;

"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 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 or founding statement, as the case may be;
- (b) a natural person, his or her ID book or passport;
- (c) a partnership, the partnership agreement; or
- (d) a trust, the trust deed;

"evaluator" means any expert consultant engaged by the South African Accreditation Authority to monitor, inspect or evaluate an authentication service provider or its authentication products or services resulting in and used to support an electronic signature, to ensure compliance with Chapter VI of the Act and these regulations;

"SANS 21188" means SANS 21188:2006, *Public key infrastructure for financial services – Practices and policy framework*, a South African National Standard adopted by the South African Bureau of Standards on 13 October 2006;

"ITU X.509" means the International Telecommunication Union's recommendation X.509, *Information technology – Open systems interconnection – The directory: Public-key and attribute certificate frameworks*, approved in August 2005;

"PKI" means Public Key Infrastructure;

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

"revoke" means, in relation to a certificate issued by a certification service provider, to terminate the operational period of a certificate from a specific time;

"SABS/ISO 17799" means the code of practice for information security management accepted as a national standard by the South African Bureau of Standards (SABS ISO/IEC 17799) in accordance with SABS procedures on 16 February 2001;

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

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

"South African Accreditation Authority" means the Accreditation Authority established in terms of section 34 of the Act;

"suspend" means, in relation to a certificate issued by a certification service provider, 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 that comply with the criteria contemplated in section 38(3) of the Act;

"WebTrust" means the principles and criteria of the WebTrust Program for Certification Authorities developed by the American Institute of Certified Public Accountants, Inc. and the Canadian Institute of Chartered Accountants.

CHAPTER I

Administration

Administration

2. (1) These regulations must be administered by the South African Accreditation Authority.

(2) The South African Accreditation Authority must furnish the Minister with quarterly reports of its activities, including details of authentication products and services that were accredited or had their accreditation revoked or suspended and foreign authentication products and services that were recognized by the South African Accreditation Authority.

Guidelines

3. The South African Accreditation Authority may issue guidelines, directives and practice notes concerning the administration of all matters relating to accreditation in terms of the Act and these regulations.

Database

4. The database contemplated in section 36(2) of the Act must contain the following information:

(a) Particulars of each authentication service provider whose authentication products or services have been accredited, as follows:

(i) The name and, where applicable, registration details of the authentication service provider;

(ii) The names and a technical description of the accredited authentication products and services by type and class;

(iii) The business address, telephone number, website address, e-mail address and facsimile number of the authentication service provider;

(iv) The identification number and website location of the repository of the authentication service provider;

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

(c) The complaints procedures for subscribers to accredited authentication products and services;

(d) Suspended and self-terminated accreditations and recognitions; and

(e) The contact particulars of the South African Accreditation Authority.

CHAPTER II

Application for accreditation

Accreditation

5. Upon application by an authentication service provider, the South African Accreditation Authority must, if the applicant complies with the requirements of the Act and these regulations, accredit the authentication products or services resulting in and used to support an electronic signature, as an advanced electronic signature.

Manner of application for accreditation

6. (1) An application for accreditation in terms of the Act must be made to the South African Accreditation Authority by completing the application form that is available on the South African Accreditation Authority's website and must be supported by the information in regulation 7 and be accompanied by the non-refundable application fee in regulation 29(1).

(2) In order to ensure the confidentiality of applications, supporting information or any aspect of the operations of an applicant, the South African Accreditation Authority may not disclose any information marked confidential by

the applicant except for lawful purposes and must further ensure the confidentiality of the information by requesting third parties such as the evaluators to sign confidentiality agreements before accessing such confidential information.

(3) An applicant may be a single person that provides an authentication product or service or a consortium of persons that provides an authentication product or service together.

(4) If the applicant is a consortium of persons as contemplated in subregulation (3), the applicant must indicate which of the persons is the main applicant and responsible for the application for accreditation and compliance with Chapter VI of the Act and these regulations.

(5) If the applicant is a consortium of persons as contemplated in subregulation (3) and its authentication product or service is based on PKI, the certification service provider will be the main applicant and will be responsible for the application for accreditation and compliance with Chapter VI of the Act and these regulations.

Prescribed information

7. An application for accreditation must be supported by the following:

- (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 a written undertaking that it can and will comply with the requirements of its certification practice statement and certificate policy;
- (c) A declaration –
 - (i) detailing the authentication products and services resulting in and used to support an electronic signature in respect of which accreditation is sought;
 - (ii) detailing procedures in respect of the identification and authentication of subscribers to those authentication products or services, including face-to-face identification;
 - (iii) 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;
 - (iv) addressing the manner in which the applicant will comply with the requirements of the Act and these regulations;
 - (v) detailing the manner in which information about the applicant's authentication products and services as well as information pertaining to the conditions on which those products and services are offered will be made available to the general public and its subscribers;

- (vi) 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
- (vii) 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 relevant to the authentication product or service that have been outsourced;
- (e) The applicant's audited financial statements for the three years immediately preceding the application;
- (f) General technical specifications of the applicant's hardware and software systems, its information security policies, the standards it complies with, its infrastructure and the location of its facilities relevant to its authentication product or service resulting in and used to support an electronic signature;
- (g) The privacy and physical security policy that will be implemented by the applicant in its operations;
- (h) An organisational chart;
- (i) A statement dealing with the applicant's –
 - (i) human resource plan;
 - (ii) procedures for processing of authentication products and services; and
 - (iii) audits and the regularity and extent of such audits;
- (j) The full names, job description and curriculum vitae of the applicant in the case of a natural person and of the directors and management in the case of a legal person;
- (k) An audit report;
- (l) Proof of adequate insurance cover to ensure business continuity;
- (m) A disaster recovery plan.

Submission of applications

8. (1) Only hand-delivered applications will be accepted by the South African Accreditation Authority.

(2) An application that is not accompanied by the information and application fee contemplated in the Act and these regulations will not be considered.

Processing of applications

9. (1) The South African Accreditation Authority will consider an application for accreditation only after receipt of the information required in terms of regulation 7.

(2) The South African Accreditation Authority must appoint one or more evaluators to monitor, inspect or evaluate authentication service providers to ensure compliance with the Act and these regulations.

Granting of accreditation

10. (1) If the South African Accreditation Authority is satisfied that an applicant complies with the requirements of the Act and these regulations, the South African Accreditation Authority must –

- (a) communicate its decision to the applicant in writing;
- (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; and
- (d) issue a certificate of accreditation for each authentication product or service accredited, stating any conditions or restrictions subject to which it was accredited.

(2) An authentication service provider must submit an audit report upon application for accreditation and annually thereafter.

(3) An authentication service provider whose authentication products or services resulting in and used to support an electronic signature are accredited may outsource or appoint agents or contractors to carry out some or all of the operations relevant to its authentication products or services: Provided that –

- (a) it has notified the South African Accreditation Authority in writing;
- (b) the agent or contractor, as the case may be, has been audited for purposes of that specific authentication product or service, the costs of the audit to be borne in full by the authentication service provider or its agent or contractor, and an audit report has been submitted to the South African Accreditation Authority and found to be acceptable;
- (c) the South African Accreditation Authority approves the outsourcing or appointment of those agents or contractors in writing;
- (d) those agents or contractors comply with the Act and these regulations as applicable to the authentication service provider whose authentication products or services have been accredited; and

- (e) the authentication service provider is 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 South African Accreditation Authority must publish details of accredited authentication products and services resulting in and used to support an electronic signature in its publicly accessible database contemplated in regulation 4.

Refusal of application for accreditation

12. (1) The South African Accreditation Authority may refuse to accredit an authentication product or service resulting in or used to support an electronic signature, subject to subregulations (2) and (3), if –

- (a) the applicant does not provide the South African Accreditation Authority with the information contemplated in regulation 7 or the information is not complete;
- (b) the applicant does not comply with the Act or these regulations; or
- (c) an authentication service provider fails to submit an appropriate audit report as contemplated in regulation 7(k) or fails to comply with any recommendation of the South African Accreditation Authority pursuant to the audit report or an inspection or evaluation.

(2) The South African Accreditation Authority must grant an applicant the opportunity to make written representation on the reasons for refusal of accreditation.

(3) The South African Accreditation Authority must grant an applicant the opportunity to comply, within a period of 30 days, with any requirement that will render the applicant's authentication product or service accreditable.

CHAPTER III

Requirements for certification service providers

Technical requirements

13. (1) A certification service provider whose authentication products and services are based on PKI must comply with SANS 21188.

(2) All certificates issued by a certification service provider must, if accredited by the South African Accreditation Authority, conform to the ITU X.509 standard and must contain the following data, among other things:

- (a) The serial number of the certificate that distinguishes it from other certificates;
 - (b) The signature algorithm identifier that identifies the algorithm used by the certification service provider to sign the certificate;
-

- (c) The name of the certification service provider that issued the certificate;
- (d) The period of validity of the certificate;
- (e) The name of the subscriber whose public key the certificate identifies;
- (f) The public key information of the subscriber;
- (g) Confirmation that it is a certificate that has been accredited by the South African Accreditation Authority and reference to the uniform resource locator of the South African Accreditation Authority's website.

(3) Three-factor authentication or a similar acceptable level of security is required for the storage of the private key where authentication products and services are based on PKI.

Requirements for issuing certificates

14. (1) Upon receipt of an application, a certification service provider must –

- (a) establish the identity of the person or entity applying for a certificate, which must include face-to-face identification of the subscriber or authorized key holder;
- (b) establish and maintain a demonstrable and auditable process to confirm that face-to-face identification was undertaken; and
- (c) ensure that the persons performing the face-to-face identification have undergone appropriate training in comparing a subscriber with a photo in an identity document or passport and in identifying fraudulent identity documents and passports.

(2) A certification service provider may issue a certificate to any entity or person that has applied for a certificate only after the certification service provider has complied with all of the practices and procedures set forth in the certification service provider's certification practice statement and certificate policy, including procedures regarding face-to-face identification of the prospective subscriber.

(3) A certification service provider is deemed to have represented 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 the certification service provider's certification practice statement and certificate policy as incorporated by reference into the certificate.

(4) Where a certification practice statement and certificate policy have been incorporated by reference into a certificate, the following provisions are deemed to 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 and these regulations in issuing the certificate, and if the certification service provider has published the certificate or otherwise made it available to a person who relies on it the subscriber listed in the certificate has 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 states in the certificate that the accuracy of specified information has not been confirmed by the certification service provider.
- (e) The certification service provider has no knowledge of any material fact that, if included in the certificate, would adversely affect the reliability of the representations in paragraphs (a), (b), (c) and (d).

Requirements for certification practice statements

15. (1) A certification service provider whose authentication product or service has been accredited must make its certification practice statement and certificate policy for that advanced electronic signature available to the public on its website or in the manner determined by the South African Accreditation Authority.

(2) A certification service provider whose authentication products or services have been accredited must –

- (a) at least 30 days before it effects any substantive changes to its certification practice statement and certificate policy, including changes –
 - (i) in the identification process;
 - (ii) in the reliance limit of the certificates; or
 - (iii) in key generation, storage or usage;

notify the South African Accreditation Authority in writing and notify its subscribers and relying parties of the intended changes by publication on its website of its intention to effect such changes;

(b) notify the South African 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 its certification practice statement and certificate policy as it has been lodged with the South African Accreditation Authority;

(c) adhere to its certification practice statement and certificate policy when issuing a type, class or description of accredited certificates; and

(d) state clearly to subscribers and relying parties all costs and fees related to the issuing, 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 must use the following documents to identify and authenticate a subscriber or applicant for a certificate or other authentication product or service during initial registration, certificate renewal, routine rekey, rekey after revocation and when processing requests for suspension or revocation:

(a) Where the subscriber or applicant is a natural person, an original, valid –

(i) identity document;

(ii) passport; or

(iii) for certificate renewal purposes only, accredited certificate.

(b) Where the subscriber or applicant is a partnership, the constitutive documents of the partnership, if applicable, as well as the documents referred to in paragraph (a) in respect of each partner in the partnership, including the authorized key holder.

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

(i) the relevant constitutive documents;

(ii) a resolution or power of attorney of the directors authorising a specific person to apply for or otherwise deal with a specific certification service provider in relation to the issuing, renewal or replacement of certificates; and

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

(4) (a) During the identification and authentication of a subscriber or applicant as contemplated in subregulation (3), a handwritten signature must be obtained by the certification service provider from the subscriber or applicant and the certification service provider should be able to prove that the subscriber or applicant was actually present and identified and accepted the certificate.

(b) The handwritten signature referred to in paragraph (a) must be made on a subscriber agreement.

(c) A subscriber agreement must provide that the responsibility for safeguarding the private key lies with the subscriber, as does the responsibility to notify the certification service provider within 24 hours if the private key is lost or compromised.

(5) A certification service provider's certification practice statement and certificate policy must comply with the ITU X.509 standard and must contain the following:

(a) A detailed description of the identification process contemplated in regulation 14(1);

(b) Provisions governing the conduct of agents or contractors to whom operations have been outsourced as contemplated in regulation 10(3);

(c) Adequate provision for certificate renewal;

(d) Levels and reliance limits of certificates;

(e) Private key storage requirements.

Duties of subscribers

16. A certification service provider must ensure that its subscribers comply with the following duties:

(a) The subscriber whose public key is to be listed in a certificate issued by the certification service provider and accepted by the subscriber must generate the key pair using a trustworthy system as required by SANS 21188.

(b) 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, must be accurate and complete, irrespective of whether such representations are confirmed by the certification service provider.

(c) A subscriber is deemed to have accepted a certificate if he or she publishes the certificate in a repository or makes it available to a third party for use.

(d) A subscriber must guarantee 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 of which the subscriber has knowledge is true.

(e) On accepting a certificate issued by a certification service provider, the subscriber identified in the certificate must exercise all 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 authorized to create the subscriber's advanced electronic signature, and such duty continues throughout the period of validity of the certificate and during any period of suspension of the certificate.

(f) A subscriber who has accepted a certificate must, if the private key corresponding to the public key listed in the certificate has been compromised, request the issuing certification service provider to suspend or revoke the certificate within 24 hours of such loss or compromise.

Responsibilities of certification service providers

17. A certification service provider whose authentication products or services resulting in and used to support an electronic signature are accredited must –

(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 regulation 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 the reliability of a certificate issued by the certification service provider 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 issuing, 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 system as contemplated in section 38(2)(a), (b), (c) and (d) of the Act or its certification service provider certificate, use all reasonable efforts to notify any person who is or might be or will foreseeably 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 policies, procedures and practices in relation to its entire operational environment;

- (e) report to the South African Accreditation Authority any incident that may materially affect its trustworthy system in general;
- (f) ensure that all its personnel are fit and proper persons and possess the necessary knowledge, technical qualifications and expertise to carry out their duties effectively; and
- (g) comply with the Act, these regulations and any guidelines or directives issued by the South African Accreditation Authority.

Requirements prior to cessation of business

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

(2) Subject to the provisions of the relevant subscriber's agreement or the common law, a certification service provider who fails to comply with this regulation is liable for any damage or loss suffered by subscribers or relying parties as a result of such non-compliance.

Liability of certification service providers

19. Apportionment of liability must be determined in a certification service provider's certification practice statement in accordance with SANS 21188: Provided that a certification service provider cannot exclude liability resulting from its own gross negligence.

Records to be kept

20. (1) For purposes of section 38(4)(f) of the Act, the following records must be kept by a certification service provider for a period of seven years or for some other period that the South African Accreditation Authority may determine:

- (a) Applications for the issuing of certificates;
 - (b) Registration and verification documents for certificates generated;
 - (c) Certificates in a manner such that –
 - (i) no-one, with the exception of parties authorized to do so, can make changes to the certificates;
 - (ii) it is possible to verify that the information is correct; and
 - (iii) the certificate is available to the public only if this is expressly permitted by the subscriber;
 - (d) Information related to suspended certificates;
 - (e) Information related to expired and revoked certificates;
 - (f) Reliable records and logs for activities that are core to the
-

certification service provider's operations, such as certificate management, key generation and administration of its computing facilities.

(2) An accredited service provider must maintain its repository in such a manner that subscribers and relying parties can readily access records to which the authentication service provider permits access.

(3) All records must be kept in such a manner as to ensure the security, integrity and accessibility of the information and records for purposes of their retrieval and inspection by the South African Accreditation Authority.

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

(5) If a certification service provider's authentication products and services are based on PKI, key certificates must be re-signed in accordance with the key lengths specified in the certification practice statement.

Suspension and revocation of certificates

21. (1) Unless a certification service provider and a subscriber agree otherwise, the certification service provider must suspend a certificate with immediate effect upon receiving a request to do so from the subscriber listed in the certificate or a person duly authorized to act for that subscriber.

(2) The certification service provider must revoke any certificate that it issued –

(a) after receiving a request for revocation from a subscriber named in the certificate and confirming that the person requesting the revocation is the subscriber or an agent of the subscriber with authority to request the revocation;

(b) after receiving a certified copy of the subscriber's death certificate; or

(c) upon presentation of documentary proof that a subscriber that is a legal person has been wound up or deregistered or has ceased to exist.

(3) A certification service provider must revoke a certificate, regardless of whether the subscriber listed in the certificate consents, if after verification –

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

(b) a requirement for the issuing 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 a subscriber agreement with the certification service provider.

(4) Upon effecting a revocation contemplated in subregulation (3), the certification service provider must immediately notify the subscriber listed in the revoked certificate 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 as contemplated in regulation 21, the certification service provider must 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 must publish signed notices of the suspension or revocation in all such repositories.

CHAPTER IV

Suspension, revocation and termination

Suspension and revocation

23. (1) Prior to revoking the accreditation of any authentication product or service resulting in and used to support an electronic signature as contemplated in section 39 of the Act, the South African Accreditation Authority must, in addition to the requirements in section 39(2) of the Act –

(a) publish a notice in its database and in any other medium that it regards as appropriate to the effect that it is in the process of revoking the accreditation of the authentication product or service in question;

(b) appoint an accreditation officer and an evaluator to oversee the winding-up of the service provider's accredited operations;

(c) ensure that the authentication service provider communicates the revocation to subscribers and relying parties immediately;

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

(e) ensure that the accreditation officer and the evaluator each issue a report certifying compliance with the prescribed revocation process;

(f) make arrangements for the preservation of records as provided for in terms of section 38(4)(f) of the Act in accordance with the manner and period contemplated in regulation 20; and

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

(2) The South African Accreditation Authority must publish all suspensions and revocations in its publicly accessible database.

(3) If an authentication product or service is provided by a consortium of persons, the main applicant contemplated in regulation 6 must, prior to any merger, acquisition, take-over or similar business transaction that changes the composition of the consortium of persons, notify the South African Accreditation Authority of such business transaction to enable the South African Accreditation Authority to re-evaluate the authentication product or service and the accreditation.

(4) Notification under subregulation (3) above must be accompanied by –

- (a) the application fee contemplated in regulation 29(1)(a); and
- (b) relevant information that changes the original application in terms of regulation 6, subject to any other information that the South African Accreditation Authority may request.

(5) If an authentication product or service is provided by a consortium of persons and the composition of the consortium of persons changes as a result of any merger, acquisition, take-over or similar business transaction, the accreditation of the product or service is deemed suspended as contemplated in section 39 of the Act from the date of such transaction unless the South African Accreditation Authority confirms the accreditation prior to such transaction.

Procedure following suspension

24. (1) Following suspension of accreditation, the South African Accreditation Authority –

- (a) may 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;
- (b) may repeat any part of the procedure in section 39(2) of the Act;
- (c) may monitor the progress of the authentication service provider in rectifying the breach;
- (d) may consider any specific request by the relevant authentication service provider;
- (e) may 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 is remedied, the South African Accreditation Authority may lift the suspension and reinstate accreditation.

(3) The South African Accreditation Authority must, if a suspended accreditation is revoked or when suspension of accreditation is lifted, publish such information in its publicly accessible database.

Termination

25. (1) An authentication service provider whose authentication products or services resulting in and used to support an electronic signature have been accredited may terminate such accreditation at any time in terms of the Act: Provided that the authentication service provider must –

- (a) give the South African Accreditation Authority notice of its intention to cease operations 90 days before the termination of its accreditation or its ceasing to act as an authentication service provider;
- (b) before the termination of its accreditation or its ceasing to act as an authentication service provider, as the case may be, advertise its intention to terminate its accreditation in a national newspaper and in such other manner as the South African Accreditation Authority may determine;
- (c) give all its subscribers and holders of each unrevoked or unexpired certificate issued by it 60 days' notice by electronic mail and registered post of its intention to cease acting as an authentication service provider;
- (d) ensure that discontinuing its operations causes minimal disruption to its subscribers and to persons who need to verify certificates;
- (e) make arrangements for the preservation of records as contemplated in section 38(4)(f) of the Act; and
- (f) destroy all expired certificates.

(2) The South African Accreditation Authority must follow the provisions of regulation 23(1)(b), (c), (d), (e), (f), and (g) as soon as it receives a notice of termination from an authentication service provider.

Information security requirements

26. (1) Authentication and certification service providers, excluding certification service providers whose authentication products and services are based on PKI, must adhere to the information security principles of SABS/ISO 17799.

(2) A certification service provider whose authentication products and services are based on PKI must adhere to the information security principles contained in SANS 21188.

Audits and evaluations

27. (1) An applicant for accreditation must appoint and be responsible for the payment of an auditor to audit the applicant and its authentication products and services resulting in and used to support an electronic signature.

(2) The auditor must take into consideration recent audits by independent auditors provided by the authentication service provider that are relevant to the intended audit in order to reduce audit costs.

(3) The authentication service provider must submit an audit report at the time of application for accreditation.

(4) If the applicant is a consortium of persons, each person must be audited.

Administration and supervision

28. (1) Accreditation granted by the South African Accreditation Authority is subject to the condition that an authentication service provider must, on at least five days' written notice, allow the South African Accreditation Authority or an auditor appointed by the South African Accreditation Authority, as the case may be, to enter its business premises during normal business hours for purposes of audits and must upon request make available for inspection any relevant books, records, supporting documents and other documentation and must disclose all information reasonably requested by the South African Accreditation Authority or auditor and provide all support necessary to conduct the audit.

(2) To the extent that any of the information in regulations 6 and 7 submitted by an applicant changes after accreditation, the South African Accreditation Authority must be notified by the authentication service provider of such changes in writing.

CHAPTER V

General

Fees payable

29. (1) The application fee payable by authentication service providers that apply for accreditation or whose authentication products or services resulting in and used to support an electronic signature have been accredited is an amount of R20,000.00 in respect of each separate authentication product or service resulting in and used to support an electronic signature.

(2) Fees payable to the South African Accreditation Authority must be paid directly into the Department's bank account and proof of the payment submitted to the South African Accreditation Authority.

(3) All fees contemplated in subregulation (1) are non-refundable.

Short title

30. These regulations are called the Accreditation Regulations.