

Act 25-2002 - Electronic Communications and Transactions Act, 2002

(English text signed by the President,)
(Assented to 31 July 2002.)

ACT

To provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy for the Republic; to promote universal access to electronic communications and transactions and the use of electronic transactions by SMMEs; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-government services; and to provide for matters connected therewith.

BE IT ENACTED by the Parliament of the Republic of South Africa, as follows:—

ARRANGEMENT OF SECTIONS

Sections

CHAPTER I

INTERPRETATION, OBJECTS AND APPLICATION

- | | | |
|----|-----------------------|----|
| 1. | Definitions | |
| 2. | Objects of Act | |
| 3. | Interpretation | |
| 4. | Sphere of application | 10 |

CHAPTER II

MAXIMISING BENEFITS AND POLICY FRAMEWORK

Part 1

National e-strategy

- | | | |
|----|--|----|
| 5. | National e-strategy | 15 |
| 6. | Universal access | |
| 7. | Previously disadvantaged persons and communities | |
| 8. | Development of human resources | |
| 9. | SMMEs | |

Part 2 20

Electronic transactions policy

- | | | |
|-----|--------------------------------|--|
| 10. | Electronic transactions policy | |
|-----|--------------------------------|--|

CHAPTER III**FACILITATING ELECTRONIC TRANSACTIONS****Part 1****Legal requirements for data messages**

11.	Legal recognition of data messages	5
12.	Writing	
13.	Signature	
14.	Original	
15.	Admissibility and evidential weight of data messages	
16.	Retention	10
17.	Production of document or information	
18.	Notarisation, acknowledgement and certification	
19.	Other requirements	
20.	Automated transactions	

Part 2

15

Communication of data messages

21.	Variation by agreement between parties	
22.	Formation and validity of agreements	
23.	Time and place of communications, dispatch and receipt	
24.	Expression of intent or other statement	20
25.	Attribution of data messages to originator	
26.	Acknowledgement of receipt of data message	

CHAPTER IV**E-GOVERNMENT SERVICES**

27.	Acceptance of electronic filing and issuing of documents	25
28.	Requirements may be specified	

CHAPTER V**CRYPTOGRAPHY PROVIDERS**

29.	Register of cryptography providers	
30.	Registration with Department	30
31.	Restrictions on disclosure of information	
32.	Application of Chapter and offences	

CHAPTER VI**AUTHENTICATION SERVICE PROVIDERS****Part 1**

35

Accreditation Authority

33.	Definition	
34.	Appointment of Accreditation Authority and other officers	
35.	Accreditation to be voluntary	
36.	Powers and duties of Accreditation Authority	40

Part 2**Accreditation**

- | | | |
|-----|---|---|
| 37. | Accreditation of authentication products and services | |
| 38. | Criteria for accreditation | |
| 39. | Revocation or termination of accreditation | 5 |
| 40. | Accreditation of foreign products and services | |
| 41. | Accreditation regulations | |

CHAPTER VII**CONSUMER PROTECTION**

- | | | |
|-----|---|----|
| 42. | Scope of application | 10 |
| 43. | Information to be provided | |
| 44. | Cooling-off period | |
| 45. | Unsolicited goods, services or communications | |
| 46. | Performance | |
| 47. | Applicability of foreign law | 15 |
| 48. | Non-exclusion | |
| 49. | Complaints to Consumer Affairs Committee | |

CHAPTER VIII**PROTECTION OF PERSONAL INFORMATION**

- | | | |
|-----|---|----|
| 50. | Scope of protection of personal information | 20 |
| 51. | Principles for electronically collecting personal information | |

CHAPTER IX**PROTECTION OF CRITICAL DATABASES**

- | | | |
|-----|--|----|
| 52. | Scope of critical database protection | |
| 53. | Identification of critical data and critical databases | 25 |
| 54. | Registration of critical databases | |
| 55. | Management of critical databases | |
| 56. | Restrictions on disclosure of information | |
| 57. | Right of inspection | |
| 58. | Non-compliance with Chapter | 30 |

CHAPTER X**DOMAIN NAME AUTHORITY AND ADMINISTRATION****Part 1****Establishment and incorporation of .za domain name authority**

- | | | |
|-----|--|----|
| 59. | Establishment of Authority | 35 |
| 60. | Incorporation of Authority | |
| 61. | Authority's memorandum and articles of association | |

Part 2**Governance and staffing of Authority**

- | | | |
|-----|---------------------------------|----|
| 62. | Board of directors of Authority | 40 |
| 63. | Staff of Authority | |

Part 3**Functions of Authority**

- 64. Licensing of registrars and registries
- 65. Functions of Authority

Part 4

5

Finances and reporting

- 66. Finances of Authority
- 67. Reports

Part 5**Regulations**

10

- 68. Regulations regarding Authority

Part 6**Alternative dispute resolution**

- 69. Alternative dispute resolution

CHAPTER XI

15

LIMITATION OF LIABILITY OF SERVICE PROVIDERS

- 70. Definition
- 71. Recognition of representative body
- 72. Conditions for eligibility
- 73. Mere conduit
- 74. Caching
- 75. Hosting
- 76. Information location tools
- 77. Take-down notification
- 78. No general obligation to monitor
- 79. Savings

CHAPTER XII**CYBER INSPECTORS**

- 80. Appointment of cyber inspectors
- 81. Powers of cyber inspectors
- 82. Power to inspect, search and seize
- 83. Obtaining warrant
- 84. Preservation of confidentiality

CHAPTER XIII**CYBER CRIME**

35

- 85. Definition
- 86. **Unauthorised** access to, interception of or interference with data
- 87. Computer-related extortion, **fraud** and forgery
- 88. Attempt, and aiding and abetting
- 89. Penalties

40

CHAPTER XIV

GENERAL PROVISIONS

90.	Jurisdiction of courts	
91.	Saving of common law	
92.	Repeal of Act 57 of 1983	5
93.	Limitation of liability	
94.	Regulations	
95.	Short title and commencement	

SCHEDULE 1

SCHEDULE 2	10
------------	----

CHAPTER I

INTERPRETATION, OBJECTS AND APPLICATION

Definitions

1.	In this Act, unless the context indicates otherwise—	15
	“addressee”, in respect of a data message, means a person who is intended by the originator to receive the data message, but not a person acting as an intermediary in respect of that data message;	
	“advanced electronic signature” means an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37;	20
	“authentication products or services” means products or services designed to identify the holder of an electronic signature to other persons;	
	“authentication service provider” means a person whose authentication products or services have been accredited by the Accreditation Authority under section 37 or recognised under section 40;	25
	“Authority” means the .za Domain Name Authority;	
	“automated transaction” means an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person’s business or employment;	30
	“browser” means a computer program which allows a person to read hyperlinked data messages;	
	“cache” means high speed memory that stores data for relatively short periods of time, under computer control, in order to speed up data transmission or processing;	
	“ccTLD” means country code domain at the top level of the Internet’s domain name system assigned according to the two-letter codes in the International Standard ISO 3166-1 (Codes for Representation of Names of Countries and their Subdivision);	35
	“certification service provider” means a person providing an authentication product or service in the form of a digital certificate attached to, incorporated in or logically associated with a data message;	40
	“consumer” means any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier;	
	“Consumer Affairs Committee” means the Consumer Affairs Committee established by section 2 of the Consumer Affairs (Unfair Business Practices) Act, 1988 (Act No. 71 of 1988);	45
	“critical data” means data that is declared by the Minister in terms of section 53 to be of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens;	50
	“critical database” means a collection of critical data in electronic form from where it may be accessed, reproduced or extracted,	
	“critical database administrator” means the person responsible for the management and control of a critical database;	

Act No. 25, 2002

ELECTRONIC COMMUNICATIONS AND
TRANSACTIONS ACT, 2002

“cryptography product” means any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring-

- (a) that such data can be accessed only by relevant persons;
- (b) the authenticity of the data;
- (c) the integrity of the data; or
- (d) that the source of the data can be correctly ascertained;

“cryptography provider” means any person who provides or who proposes to provide cryptography services or products in the Republic;

“cryptography service” means any service which is provided to a sender or a recipient of a data message or to anyone storing a data message, and which is designed to facilitate the use of cryptographic techniques for the purpose of ensuring-

- (a) that such data or data message can be accessed or can be put into an intelligible form only by certain persons;
- (b) that the authenticity or integrity of such data or data message is capable of being ascertained;
- (c) the integrity of the data or data message; or
- (d) that the source of the data or data message can be correctly ascertained;

“cyber inspector” means an inspector referred to in Chapter XII;

“data” means electronic representations of information in any form;

“data controller” means any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject;

“data message” means data generated, sent, received or stored by electronic means and includes-

- (a) voice, where the voice is used in an automated transaction; and
- (b) a stored **record**;

“data subject” means any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored, after the commencement of this Act;

“Department” means the Department of Communications;

“Director-General” means the Director-General of the Department;

“domain name” means an alphanumeric designation that is registered or assigned in respect of an electronic address or other resource on the Internet;

“domain name system” means a system to translate domain names into IP addresses or other information;

“e-government services” means any public service provided by electronic means by any public body in the Republic;

“electronic agent” means a computer program or an electronic or other automated means used independently to initiate an action or respond to data messages or performances in whole or in part, in an automated transaction;

“electronic communication” means a communication by means of data messages;

“electronic signature” means data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature;

“e-mail” means electronic mail, a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication;

“home page” means the primary entry point web page of a web site;

“hyperlink” means a reference or link from some point in one data message directing a browser or other technology or functionality to another data message or point therein or to another place in the same data message;

“ICANN” means the Internet Corporation for Assigned Names and Numbers, a California non-profit public benefit corporation established in terms of the laws of the state of California in the United States of America;

“information system” means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet;

“information system services” includes the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the individual request of the recipient of the service;

“intermediary” means a person who, on behalf of another person, whether as agent or not, sends, receives or stores a particular data message or provides other services with respect to **that** data message;

“Internet” means the interconnected system of networks that connects computers around the world using the **TCP/IP** and includes future versions thereof; 5

“IP address” means the number identifying the point of connection of **a** computer or other device to the Internet;

“Minister” means the Minister of Communications;

“originator” means a person by whom, or on whose behalf, a data message purports to have been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that data message; 10

“person” includes a public body;

“personal information” means information about **an** identifiable individual, including, but not limited to-

(a) information relating to the race, gender, sex, pregnancy, marital status, 15 national, ethnic or social origin, **colour**, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;

(b) information relating to the education or the medical, criminal or employment history of the individual or **information** relating to financial transactions in 20 which the individual has been involved;

(c) any identifying number, symbol, or other particular assigned to the individual;

(d) the address, fingerprints or blood type of the individual;

(e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, **an** award or a prize to be made to another individual; 25

(f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the individual; 30

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and

(i) the name of the individual where it appears **with** other personal information 35 relating to the individual or where the disclosure of the name itself would reveal information about the individual,

but excludes information about an individual who has been dead for more than 20 years;

“prescribe” means prescribe by regulation under this Act; 40

“private body” means-

(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;

(b) a partnership which carries or has carried on any trade, business or profession; 45

OR
(c) any **former** or existing juristic person, but not a public body;

“public body” means-

(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or 50

(b) any other functionary or institution when-

(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

(ii) exercising a power or performing a function in terms of any legislation;

“registrant” means an applicant for or holder of a domain name; 55

“registrar” means an entity which is licensed by the Authority to update a repository;

Act No. 25, 2002

ELECTRONIC COMMUNICATIONS AND
TRANSACTIONS ACT, 2002

- “registry” means an entity licensed by the Authority to manage and administer a specific subdomain;
- “repository” means the primary register of the information maintained by a registry;
- “second level domain” means the subdomain immediately following the ccTLD; 5
- “SMMEs” means Small, Medium and Micro Enterprises contemplated in the Schedules to the Small Business Development Act, 1996 (Act No. 102 of 1996);
- “subdomain” means any subdivision of the .za domain name space which begins at the second level domain;
- “TCP/IP” means the Transmission Control Protocol Internet Protocol used by an information system to connect to the Internet; 10
- “TLD” means a top level domain of the domain name system;
- “third party”, in relation to a service provider, means a subscriber to the service provider’s services or any other user of the service provider’s services or a user of information systems; 15
- “transaction” means a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services;
- “universal access” means access by all citizens of the Republic to Internet connectivity and electronic transactions;
- “WAP” means Wireless Application Protocol, an open international standard developed by the Wireless Application Protocol Forum Limited, a company 20 incorporated in terms of the laws of the United Kingdom, for applications that use wireless communication and includes Internet access from a mobile phone;
- “web page” means a data message on the World Wide Web;
- “web site” means any location on the Internet containing a home page or web page; 25
- “World Wide Web” means an information browsing framework that allows a user to locate and access information stored on a remote computer and to follow references from one computer to related information on another computer; and
- “.za domain name space” means the .za ccTLD assigned to the Republic according to the two-letter codes in the International Standard ISO 3166-1. 30

Objects of Act

2. (I) The objects of this Act are to enable and facilitate electronic communications and transactions in the public interest, and for that purpose to-
- (a) recognise the importance of the information economy for the economic and social prosperity of the Republic; 35
- (b) promote universal access primarily in underserved areas;
- (c) promote the understanding and, acceptance of and growth in the number of electronic transactions in the Republic;
- (d) remove and prevent barriers to electronic communications and transactions in the Republic; 40
- (e) promote legal certainty and confidence in respect of electronic communications and transactions;
- (f) promote technology neutrality in the application of legislation to electronic communications and transactions; 45
- (g) promote e-government services and electronic communications and transactions with public and private bodies, institutions and citizens;
- (h) ensure that electronic transactions in the Republic conform to the highest international standards;
- (i) encourage investment and innovation in respect of electronic transactions in the Republic; 50
- (j) develop a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions;
- (k) promote the development of electronic transactions services which are responsive to the needs of users and consumers; 55
- (l) ensure that, in relation to the provision of electronic transactions services, the special needs of particular communities and, areas and the disabled are duly taken into account;

Act No. 25, 2002ELECTRONIC COMMUNICATIONS AND
TRANSACTIONS ACT, 2002

- (m) ensure compliance with accepted International technical **standards in the** provision and development of electronic communications **and** transactions;
- (n) promote the stability of electronic transactions in the Republic;
- (o) promote the development of human resources in the electronic transactions environment; 5
- (p) promote **SMMEs** within the electronic transactions environment;
- (q) ensure efficient use and management of the .za domain name space; and
- (r) ensure that the national interest of the Republic is not compromised through the use of electronic communications.

Interpretation

10

3. This Act must not be interpreted so as to exclude any statutory law or **the** common law from being applied to, **recognising** or accommodating electronic transactions, data messages or any other matter provided for in this Act.

Sphere of application

4. (1) Subject to any contrary provision in this section, this Act applies in respect of 15
any electronic transaction or data message.

(2) This Act must not be construed as-

- (a) requiring any person to generate, communicate, produce, process, send, receive, record, retain, store or display any information, document or signature by or in electronic form; or 20
- (b) prohibiting a person from establishing requirements in respect of the manner in which that person will accept data messages.

(3) The sections of this Act mentioned in Column B of Schedule 1 do not apply to the laws mentioned in Column A of that Schedule.

(4) This Act must not **be construed** as giving validity to any transaction mentioned in Schedule 2. 25

(5) This Act **does** not limit the operation of any law that expressly **authorises**, prohibits or regulates the use of data messages, including any requirement by or under a law for information to be posted or displayed in a specified manner, **or** for any information or document to be transmitted by a specified method. 30

CHAPTER II**MAXIMISING BENEFITS AND POLICY FRAMEWORK****Part 1****National e-strategy****National e-strategy**

35

5. (1) The Minister must, within 24 months after **the** promulgation of this Act, develop a three-year national e-strategy for **the** Republic, which must be submitted to the Cabinet for approval.

(2) The Cabinet must, on acceptance of the national e-strategy, declare the implementation of the **national e-strategy as a national** priority. 40

(3) The Minister, in developing the national e-strategy as envisaged in subsection (1)—

- (a) must determine all matters involving e-government services in consultation with the Minister for the Public Service and Administration;
- (b) must determine the roles of each person, entity or sector in the implementation of the national e-strategy; 45
- (c) must act as the responsible Minister for co-ordinating and monitoring the implementation of the national e-strategy;
- (d) may make such investigations as he or she may consider necessary;

- (e) may conduct research into and keep abreast of developments relevant to electronic communications and transactions in the Republic and internationally;
- (f) must continually survey and evaluate the extent to which the objectives of the national e-strategy have been achieved; 5
- (g) may liaise, consult and cooperate with public bodies, the private sector or any other person; and
- (h) may, in consultation with the Minister of Finance, appoint experts and other consultants on such conditions as the Minister may determine.
- (4) (a) The Minister must, in consultation with other members of the Cabinet, 10 determine the subject matters to be addressed in the national e-strategy and the principles that **must** govern the implementation thereof.
- (b) Prior to prescribing any subject **matter** and principles provided for in paragraph (a), the Minister must invite comments from all interested parties by notice in the *Gazette* and consider any comments received. 15
- (c) The national e-strategy must, amongst others, set out—
- (i) the electronic transactions **strategy** of the **Republic**, distinguishing between regional, national, continental and international strategies;
 - (ii) programmes and means to achieve universal access, human resource development and development of **SMMEs** as provided for in this Part; 20
 - (iii) **programmes** and means to promote the overall readiness of the Republic in respect of electronic transactions;
 - (iv) ways to promote the Republic as a preferred provider and **user** of electronic transactions in the international market;
 - (v) existing government initiatives directly **or** indirectly relevant to or impacting 25 on the national e-strategy and, if applicable, how such initiatives are to be **utilised** in attaining the objectives of the national e-strategy;
 - (vi) the role expected to be performed by the private sector in the implementation of the national e-strategy and how government can solicit the participation of the private sector to perform such role; 30
 - (vii) the defined objectives, including time frames within which the objectives **are** to be achieved; and
 - (viii) the **resources** required to achieve the objectives provided for in the national e-strategy.
- (5) Upon approval by the Cabinet, the Minister must publish the national e-strategy in 35 the *Gazette*.
- (6) For purposes of achieving the objectives of the national e-strategy, the Minister may, in consultation with the Minister of Finance—
- (a) procure funding from **SOURCES** other than the State;
 - (b) allocate funds for implementation of the national e-strategy to such 40 institutions and persons as **are** responsible for delivery in terms of the national e-strategy and supervise the execution of their mandate; and
 - (c) take any steps **necessary** to enable all relevant parties to carry out their respective obligations.
- (7) The Minister must annually report to the Cabinet on progress made and objectives 45 achieved or outstanding and may include any other matter the Minister deems relevant.
- (8) The Minister must annually review the national e-strategy and where necessary make amendments thereto in consultation with all relevant members of the Cabinet.
- (9) No amendment **or** adaptation of the national e-strategy is effective unless 50 approved by the Cabinet.
- (10) The Minister must publish any material revision of the national e-strategy in the *Gazette*.
- (11) The Minister must table an annual report in Parliament regarding the progress made in the implementation of the national e-strategy.

Universal access

55

6. In respect of universal access, the national e-strategy must outline strategies and programmes to—

Act No. 25, 2002**ELECTRONIC COMMUNICATIONS AND
TRANSACTIONS ACT, 2002**

- (a) provide Internet connectivity to disadvantaged communities;
- (b) encourage the private sector to initiate schemes to provide universal access;
- (c) foster the adoption and use of new technologies for attaining universal access; and
- (d) stimulate public awareness, understanding and acceptance of the benefits of Internet connectivity and electronic transacting. 5

Previously disadvantaged persons and communities

7. The Minister, in developing the national e-strategy, must provide for ways of maximising the benefits of electronic transactions to historically disadvantaged persons and communities. **including, but not limited to—** 10

- (a) making facilities and infrastructure available or accessible to such persons and communities to enable the marketing and sale of their goods or services by way of electronic transactions;
- (b) providing or securing support services for such facilities and infrastructure to assist with the efficient execution of electronic transactions; and 15
- (c) rendering assistance and advice to such persons and communities on ways to adopt and utilise electronic transactions efficiently.

Development of human resources

8. (1) The Minister, in developing the national e-strategy, must provide for ways of promoting development of human resources set out in this section within the context of the government's integrated human resource development strategies, having regard to structures and programmes that have been established under existing laws. 20

(2) The Minister must consult with the Ministers of Labour and Education on existing facilities, programmes and structures for education, training and human resource development in the information technology sector relevant to the objects of this Act. 25

(3) Subject to subsections (1) and (2), the Minister must promote skills development in the areas of-

- (a) information technology products and services in support of electronic transactions;
- (b) business strategies for SMMEs and other businesses to utilise electronic transactions; 30
- (c) sectoral, regional, national, continental and international policy formulation for electronic transactions;
- (d) project management on public and private sector implementation of electronic transactions; 35
- (e) the management of the .za domain name space;
- (f) the management of the IP address system for the African continent in consultation with other African states;
- (g) convergence between communication technologies affecting electronic transactions; 40
- (h) technology and business standards for electronic transactions;
- (i) education on the nature, scope, impact, operation, use and benefits of electronic transactions; and
- (j) any other matter relevant to electronic transactions.

SMMEs 45

9. The Minister must, in consultation with the Minister of Trade and Industry, evaluate the adequacy of any existing processes, programmes and infrastructure providing for the utilisation by SMMEs of electronic transactions and, pursuant to such evaluation, may-

- (a) establish or facilitate the establishment of electronic communication centres for SMMEs; 50

Act NO. 25, 2002**ELECTRONIC COMMUNICATIONS AND
TRANSACTIONS ACT, 2002**

- (b) facilitate the development of web sites or web site portals that will enable **SMMEs** to transact electronically and obtain information about markets, products and technical assistance; and
- (c) facilitate the provision of such professional and expert assistance and advice to **SMMEs** on ways to utilise electronic transacting efficiently for their development. 5

Part 2**Electronic transactions policy****Electronic transactions policy**

- 10. (1) The Minister must, subject to this Act, formulate electronic transactions policy. 10
- (2) In formulating the policy contemplated in subsection (1), the Minister must-
 - (a) act in consultation with members of the Cabinet directly affected by such policy **formulation** or the consequences thereof;
 - (b) have due regard to-
 - (i) the objects of this Act; 15
 - (ii) the nature, scope and impact of electronic transactions;
 - (iii) international best practice and conformity with the law and guidelines of other jurisdictions and international bodies; and
 - (iv) existing laws and their administration in the Republic.
- (3) The Minister must publish policy guidelines in the *Gazette* on issues relevant to electronic transactions in the Republic. 20
- (4) In implementing this Chapter, the Minister **must** encourage the development of innovative information systems and the growth of related industry.

CHAPTER III**FACILITATING ELECTRONIC TRANSACTIONS 25****Part 1****Legal requirements for data messages****Legal recognition of data messages**

- 11. (1) Information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message. 30
- (2) Information is not without legal force and effect merely on the grounds that it is not contained in the data message purporting to give rise to such legal force and effect, but is merely referred to in such data message.
- (3) Information incorporated into **an** agreement and that is not in the public domain is regarded as having been incorporated into a data message if such information is— 35
 - (a) referred to in a way in which a reasonable person would have noticed the reference thereto and incorporation thereof; and
 - (b) accessible in a form in which it may be read, stored and retrieved by the other party, whether electronically or as a computer printout as long as such information is reasonably capable of being reduced to electronic form by the party incorporating it. 40

Writing

- 12. A requirement in law that a document or information must be in writing is met if the document or information is-
 - (a) in the **form** of a data message; and 45
 - (b) accessible in a manner usable for subsequent reference.

Signature

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

(2) Subject to subsection (1), an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form. 5

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

(a) a method is used to identify the person and to indicate the person's approval of the information communicated: and 10

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

(4) Where an advanced electronic signature has been used, such signature is regarded as being a valid electronic signature and to have been applied properly, unless the contrary is proved. 15

(5) Where an electronic signature is not required by the **parties** to an electronic transaction, an expression of intent or other statement is not without legal force and effect merely on the grounds that— 20

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

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

Original

14. (1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if- 25

(u) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and

(b) that information is capable of being displayed or produced to the person to whom it is to be presented. 30

(2) For the purposes of subsection 1(a), the integrity must be assessed-

(u) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display; 35

(b) in the light of the purpose for which the information was generated; and

(c) having regard to all other relevant circumstances.

Admissibility and evidential weight of data messages

15. (I) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence— 40

(a) on the mere grounds that it is constituted by a data message; or

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message must be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard must be had to- 45

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the integrity of the data message was maintained;

(c) the manner in which its originator was identified; and 50

(d) any other relevant factor.

(4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract. 5

Retention

16. (1) Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if-

- (a) the information contained in the data message is accessible so as to be usable for subsequent reference; 10
- (b) the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
- (c) the origin and destination of that data message and the date and time it was sent or received can be determined. 15

(2) The obligation to retain information as contemplated in subsection (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

Production of document or information 20

17. (1) Subject to section 28, where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information, and if—

- (a) considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and 25
- (b) at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference. 30

(2) For the purposes of subsection (1), the integrity of the information contained in a document is maintained if the information has remained complete and unaltered, except for-

- (u) the addition of any endorsement; or
- (h) any immaterial change, which arises in the normal course of communication, storage or display 35

Notarisation, acknowledgement and certification

18. (1) Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met if the advanced electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or data message. 40

(2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, that requirement is met if the person provides a print-out certified to be a true reproduction of the document or information.

(3) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of an advanced electronic signature. 45

Other requirements

19. (1) A requirement in a law for multiple copies of a document to be submitted to a single addressee at the same time, is satisfied by the submission of a single data message that is capable of being reproduced by that addressee.

(2) An expression in a law, whether used as a noun or verb, including the terms “document”, “record”, “file”, “submit”, “lodge”, “deliver”, “issue”, “publish”, “write in”, “print” or words or expressions of similar effect, must be interpreted so as to include or permit such form, format or action in relation to a data message unless otherwise provided for in this Act.

(3) Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed by electronic means, that requirement is met if the document indicates that it is required to be under seal and it includes the advanced electronic signature of the person by whom it is required to be sealed.

(4) Where any law requires or permits a person to send a document or information by registered or certified post or similar service, that requirement is met if an electronic copy of the document or information is sent to the South African Post Office Limited, is registered by the said Post Office and sent by that Post Office to the electronic address provided by the sender.

Automated transactions

20. In an automated transaction-

- (u) an agreement may be formed where an electronic agent performs an action required by law for agreement formation;
- (b) an agreement may be formed where all parties to a transaction or either one of them uses an electronic agent;
- (c) a party using an electronic agent to form an agreement is, subject to paragraph (d), presumed to be bound by the terms of that agreement irrespective of whether that person reviewed the actions of the electronic agent or the terms of the agreement;
- (d) A party interacting with an electronic agent to form an agreement is not bound by the terms of the agreement unless those terms were capable of being reviewed by a natural person representing that party prior to agreement formation.
- (e) no agreement is formed where a natural person interacts directly with the electronic agent of another person and has made a material error during the creation of a data message and-
 - (i) the electronic agent did not provide that person with an opportunity to prevent or correct the error;
 - (ii) that person notifies the other person of the error as soon as practicable after that person has learned of it;
 - (iii) that person takes reasonable steps, including steps that conform to the other person’s instructions to return any performance received, or, if instructed to do so, to destroy that performance; and
 - (iv) that person has not used or received any material benefit or value from any performance received from the other person.

Part 2**Communication of data messages****Variation by agreement between parties**

21. This Part only applies if the parties involved in generating, sending, receiving, storing or otherwise processing data messages have not reached agreement on the issues provided for therein.

Formation and validity of agreements

22. (1) An agreement is not without legal force and effect merely because it was concluded partly or in whole by means of data messages.

(2) An agreement concluded between parties by means of data messages is concluded at the time when and place where the acceptance of the offer was received by the offeror. 5

Time and place of communications, dispatch and receipt

23. A data message-

- (u) used in the conclusion or performance of an agreement must be regarded as having been sent by the originator when it enters an information system outside the control of the originator or, if the originator and addressee are in the same information system, when it is capable of being retrieved by the addressee; 10
- (b) must be regarded as having been received by the addressee when the complete data message enters an information system designated or used for that purpose by the addressee and is capable of being retrieved and processed by the addressee; and 15
- (c) must be regarded as having been sent from the originator's usual place of business or residence and as having been received at the addressee's usual place of business or residence.

Expression of intent or other statement

20

24. As between the originator and the addressee of a data message an expression of intent or other statement is not without legal force and effect merely on the grounds that—

- (a) it is in the form of a data message; or
- (b) it is not evidenced by an electronic signature but by other means from which such person's intent or other statement can be inferred. 25

Attribution of data messages to originator

25. A data message is that of the originator if it was sent by-

- (a) the originator personally;
- (b) a person who had authority to act on behalf of the originator in respect of that data message; or 30
- (c) an information system programmed by or on behalf of the originator to operate automatically unless it is proved that the information system did not properly execute such programming.

Acknowledgement of receipt of data message

35

26. (1) An acknowledgement of receipt of a data message is not necessary to give legal effect to that message.

(2) An acknowledgement of receipt may be given by-

- (u) any communication by the addressee, whether automated or otherwise; or
- (b) any conduct of the addressee, sufficient to indicate to the originator that the data message has been received. 40

CHAPTER IV**E-GOVERNMENT SERVICES****Acceptance of electronic filing and issuing of documents**

27. Any public body that, pursuant to any law—

45

- (a) accepts the filing of documents, or requires that documents be created or retained;

Act No. 25, 2002

ELECTRONIC COMMUNICATIONS AND
TRANSACTIONS ACT, 2002

- (b) issues any permit, licence or approval; or
 (c) provides for a manner of payment,
 may, notwithstanding anything to the contrary in such law—
 (i) accept the filing of such documents, or the creation or retention of such documents in the form of data messages; 5
 (ii) issue such permit, licence or approval in the form of a data message; or
 (iii) make or receive payment in electronic form or by electronic means.

Requirements may be specified

28. (1) In any case where a public body performs any of the functions referred to in section 27, such body may specify by notice in the *Gazette*— 10
 (a) the manner and format in which the data messages must be filed, created, retained or issued;
 (b) in cases where the data message has to be signed, the type of electronic signature required;
 (c) the manner and format in which such electronic signature must be attached to, incorporated in or otherwise associated with the data message; 15
 (d) the identity of or criteria that must be met by any authentication service provider used by the person filing the data message or that such authentication service provider must be a preferred authentication service provider;
 (e) the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of data messages or payments; and 20
 (f) any other requirements for data messages or payments.
 (2) For the purposes of subsection (1)(d) the South African Post Office Limited is a preferred authentication service provider and the Minister may designate any other authentication service provider as a preferred authentication service provider based on such authentication service provider's obligations in respect of the provision of universal access. 25

CHAPTER V**CRYPTOGRAPHY PROVIDERS****Register of cryptography providers 30**

29. (1) The Director-General must establish and maintain a register of cryptography providers.
 (2) The Director-General must record the following particulars in respect of a cryptography provider in that register: 35
 (a) The name and address of the cryptography provider;
 (b) a description of the type of cryptography service or cryptography product being provided; and
 (c) such other particulars as may be prescribed to identify and locate the cryptography provider or its products or services adequately.
 (3) A cryptography provider is not required to disclose confidential information or trade secrets in respect of its cryptography products or services. 40

Registration with Department

30. (1) No person may provide cryptography services or cryptography products in the Republic until the particulars referred to in section 29 in respect of that person have been recorded in the register contemplated in section 29. 45
 (2) A cryptography provider must in the prescribed manner furnish the Director-General with the information required and pay the prescribed administrative fee.
 (3) A cryptography service or cryptography product is regarded as being provided in the Republic if it is provided—

- (a) from premises in the Republic;
- (b) to a person who is present in the Republic when that person makes use of the service or product; or
- (c) to a person who uses the service or product for the purposes of a business carried on in the Republic or from premises in the Republic. 5

Restrictions on disclosure of information

31. (1) Information contained in the register provided for in section 29 must not be disclosed to any person other than to employees of the Department who are responsible for the keeping of the register.
- (2) Subsection (1) does not apply in respect of information which is disclosed- 10
- (a) to a relevant authority which investigates a criminal offence or for the purposes of any criminal proceedings;
 - (b) to government agencies responsible for safety and security in the Republic, pursuant to an official request;
 - (c) to a cyber inspector; 15
 - (d) pursuant to section 11 or 30 of the Promotion of Access to Information Act, (Act No. 2 of 2000); or
 - (e) for the purposes of any civil proceedings which relate to the provision of cryptography services or cryptography products and to which a cryptography provider is a party. 20

Application of Chapter and offences

32. (1) The provisions of this Chapter do not apply to the National Intelligence Agency established in terms of section 3 of the Intelligence Services Act, 1994 (Act No. 38 of 1994).
- (2) A person who contravenes or fails to comply with a provision of this Chapter is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding two years. 25

CHAPTER VI

AUTHENTICATION SERVICE PROVIDERS

Part 1 30

Accreditation Authority

Definition

33. In this Chapter, unless the context indicates otherwise—
“accreditation” means recognition of an authentication product or service by the Accreditation Authority. 35

Appointment of Accreditation Authority and other officers

34. (1) For the purposes of this Chapter the Director-General must act as the Accreditation Authority.
- (2) The Accreditation Authority, after consultation with the Minister, may appoint employees of the Department as Deputy Accreditation Authorities and officers. 40

Accreditation to be voluntary

35. Subject to section 30, a person may, without the prior authority of any other person, sell or provide authentication products or services in the Republic.

Powers and duties of Accreditation Authority

36. (1) The Accreditation Authority may- 45

- (a) monitor the conduct, systems and operations of an authentication service provider to ensure its compliance with section 38 and the other obligations of authentication service providers in terms of this Act;
- (b) temporarily suspend or revoke the accreditation of an authentication product or service; and
- (c) appoint an independent auditing firm to conduct periodic audits of the authentication service provider to ensure its compliance with section 38 and the other obligations of authentication service providers in terms of this Act.
- (2) The Accreditation Authority must maintain a publicly accessible database in respect of—
- (a) authentication products or services accredited in terms of section 37;
- (b) authentication products and services recognised in terms of section 40;
- (c) revoked accreditations or recognitions; and
- (d) such other information as may be prescribed.

Part 2

Accreditation

Accreditation of authentication products and services

37. (1) The Accreditation Authority may accredit authentication products and services in support of advanced electronic signatures.
- (2) An application for accreditation must—
- (a) be made to the Accreditation Authority in the prescribed manner supported by the prescribed information; and
- (b) be accompanied by a non-refundable prescribed fee.
- (3) A person falsely holding out its products or services to be accredited by the Accreditation Authority is guilty of an offence.

Criteria for accreditation

38. (1) The Accreditation Authority may not accredit authentication products or services unless the Accreditation Authority is satisfied that an electronic signature to which such authentication products or services relate—
- (a) is uniquely linked to the user;
- (b) is capable of identifying that user;
- (c) is created using means that can be maintained under the sole control of that user; and
- (d) will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable;
- (e) is based on the face-to-face identification of the user.
- (2) For purposes of subsection (1), the Accreditation Authority must have regard to the following factors in respect of an authentication service provider prior to accrediting authentication products or services:
- (a) Its financial and human resources, including its assets;
- (b) the quality of its hardware and software systems;
- (c) its procedures for processing of products or services;
- (d) the availability of information to third parties relying on the authentication product or service;
- (e) the regularity and extent of audits by an independent body;
- (f) the factors referred to in subsection (4) where the products and services are rendered by a certification service provider; and
- (g) any other relevant factor which may be prescribed.
- (3) For the purposes of subsections (2)(b) and (c), the hardware and software systems and procedures must at least—
- (a) be reasonably secure from intrusion and misuse;
- (b) provide a reasonable level of availability, reliability and correct operation;

Act No. 25, 2002**ELECTRONIC COMMUNICATIONS AND
TRANSACTIONS ACT, 2002**

- (c) be reasonably suited to performing their intended functions; and
- (d) adhere to generally accepted security procedures.

(4) For the purposes of subsection (1), where the products or services are provided by a certification service provider, the Accreditation Authority may stipulate, prior to accrediting authentication products or services—

- (a) the technical and other requirements which certificates must meet;
- (b) the requirements for issuing certificates;
- (c) the requirements for certification practice statements;
- (d) the responsibilities of the certification service provider;
- (e) the liability of the certification service provider;
- (f) the records to be kept and the manner in which and length of time for which they must be kept;
- (g) requirements as to adequate certificate suspension and revocation procedures; and
- (h) requirements as to adequate notification procedures relating to certificate suspension and revocation.

(5) The Accreditation Authority may impose any conditions or restrictions necessary when accrediting an authentication product or service.

Revocation of termination of accreditation

39. (1) The Accreditation Authority may suspend or revoke an accreditation if it is satisfied that the authentication service provider has failed or ceases to meet any of the requirements, conditions or restrictions subject to which accreditation was granted under section 38 or recognition was given in terms of section 40.

(2) Subject to the provisions of subsection (3), the Accreditation Authority may not suspend or revoke the accreditation or recognition contemplated in subsection (1) unless it has—

- (a) notified the authentication service provider in writing of its intention to do so;
- (b) given a description of the alleged breach of any of the requirements, conditions or restrictions subject to which accreditation was granted under section 38 or recognition was given in terms of section 40; and
- (c) afforded the authentication service provider the opportunity to—
 - (i) respond to the allegations in writing; and
 - (ii) remedy the alleged breach within a reasonable time.

(3) The Accreditation Authority may suspend accreditation granted under section 38 or recognition given under section 40 with immediate effect for a period not exceeding 90 days, pending implementation of the procedures required by subsection (2), if the continued accreditation or recognition of the authentication service provider is reasonably likely to result in irreparable harm to consumers or any person involved in an electronic transaction in the Republic.

(4) An authentication service provider whose products or services have been accredited in terms of this Chapter may terminate such accreditation at any time, subject to such conditions as may be agreed to at the time of accreditation or thereafter.

Accreditation of foreign products and services

40. (1) The Minister may, by notice in the *Gazette* and subject to such conditions as may be determined by him or her, recognise the accreditation or similar recognition granted to any authentication service provider or its authentication products or services in any foreign jurisdiction.

(2) An authentication service provider falsely holding out its products or services to have been recognised by the Minister in terms of subsection (1), is guilty of an offence.

Accreditation regulations

41. The Minister may make regulations in respect of—

- (a) the rights and obligations of persons relating to the provision of accredited products and services;