A GREEN PAPER ON ELECTRONIC COMMERCE FOR SOUTH AFRICA

Co-ordinated and compiled by the
Department of Communications
Republic of South Africa

November 2000

INVITATION TO COMMENT

The public is invited to respond to the national Green Paper on Electronic Commerce. Written responses should reach the Department of Communications at the address below not later than 31 February 2001.

Written comments on the Green Paper should be sent to:

By Post / By Hand
Attention: Dillo Lehlokoe or Francis Malema
Department of Communications

Private Bag X860
Pretoria
0001

Department of Communications
Iparioli Office Park
Room 231 Nkululeko House
399 Duncan Street
Hatfield
Pretoria

By E-mail:
E-mail: dillo@doc.pwv.gov.za or francis@doc.pwv.gov.za

By Fax:
(012) 427-8085

For further enquiries please phone:
Ms D Lehlokoe at (012) 427-8037or Mr F Malema at (012)427-8194

FOREWORD

Dear Colleagues

I am very happy to introduce this Green paper on electronic commerce and communications to you.

We embark on an extraordinary and challenging period in the history of our world. In just a few decades, we have been rocketed into a new Information Society. Changes that have occurred in the past decade supersede what has transpired in the past fifty years. A society driven by a technology that is taking us, daily, into new ways of being; new ways of understanding, interpreting and living in our world, revolutionising society, culture, politics, the economy and technological innovations.

It offers us new potential for development and progress. In the process, it has thrown up new and demanding challenges; exciting challenges. Sometimes alarming challenges. Challenges that demand that we seriously re-think the economic paradigm shift to post industrialism and how we view our place in it.

An Electronic commerce has, in many ways, created a marketplace without conventional rules; a marketplace, indeed, that challenges many of our preconceived notions and practices. It is also a marketplace that may seem to defy regulation yet at the same time requiring regulation as an enabling tool. It requires that we think carefully about its implications, both positive and negative, for our society, our country and our continent.

The Green Paper raises some of the questions and issues embedded in e-commerce. There may be many more. This is why we have opened this discussion to as wide an audience as possible. It is, in particular, crucially important that we include the previously marginalised majority of our people in our discussions and thinking, for this is a debate that affects all South Africans.

We hope and expect that all those who will be affected by the e-commerce will play a role in helping us move forward on some of the crucial issues this document raises and others that you may feel to be important. Together we can begin to contextualise the kind of challenges confronting us and the opportunities that may accrue.

Allow me to take this opportunity to thank those of you who tirelessly contributed to the process of developing a policy framework for electronic commerce. My sincere gratitude goes to the members of the working groups for their inputs and to the members of the technical task team for drafting the Green paper. Your continued contribution and extended participation is extremely critical for the path that lies ahead.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Electronic commerce (hereinafter referred to as e-commerce) touches all major aspects of economic life and presents a series of complex issues. It involves the integration of many elements of technology, infrastructure, business operation and public policy. All these elements need to operate together as smoothly as possible to yield the maximum benefits to public. Most importantly, e-commerce requires new skills and forms of industrial organisation, it therefore also needs to be looked at from social and political angles.

As a starting point, a discussion paper on e-commerce was prepared and it is available at the following website: http://www,ecomm-debate.co.za. Issues and questions raised in the e-commerce Green paper are targeted at two distinct audiences; people who are knowledgeable in the subject, such as experts and professionals; and individuals and enterprises who use e-commerce as a medium to communicate, produce, sell and deliver. The issues are contentious and are being debated at the national and international level.

The Green Paper is divided into four categories listed below. Each category contains key issues or areas of concern that need serious consideration in e-commerce policy formulation:

- the need for confidence in the security and privacy of transactions performed electronically;
- the need to enhance the information infrastructure for electronic commerce;
- the need to establish rules that will govern electronic commerce;
- the need to bring the opportunities of e-commerce to the entire population.

Each chapter gives a general background to a specific issue, discusses challenges and problems, paints the international as well as national scenario and pose policy questions relating to the issue. The document seeks answers and proposals relating to some of the challenges and pressing questions regarding the development and implementation of e-commerce.

Chapter 1 introduces the subject of e-commerce in the context of globalisation and the information society. It highlights the importance of e-commerce and hence the need for faster adoption of e-commerce by individuals, enterprises and governments. This chapter further introduces the rationale behind government involvement in developing policy framework for e-commerce.

Chapter 2 begins to layout a legal foundation for e-commerce. Questions and uncertainties concerning the validity, legal effect and enforceability of transactions conducted through electronic means are raised. Other areas involving legal issues relevant to e-commerce include taxation, customs duties, intellectual property rights, data protection, consumer protection, authentication, and jurisdiction and liability issues.

Chapter 3 discusses issues fundamental to establishing the validity, recognition and enforcement of electronic cotracts and communications. The chapter is based on the United Nations Commission for International Trade Law (UNCITRAL) Model Law document on electronic commerce. Some of these issues ensure the legal recognition for data communications; evidence; formation and validity of contracts and the recognition of electronic documents by parties; time and place of dispatch of electronic messages; signature.

Chapter 4 explores issues around e-commerce and taxation, including classification of income, source based Vs residence based taxation, administration and compliance issues. New technologies such as the Internet have effectively eliminated national borders on the information highway and these poses inherent problems of jurisdiction and enforcement. This chapter will attempt to explore the implications of not taxing Internet sales and whether new taxes should be introduced.

Chapter 5 concentrates on discussions of e-commerce within the World Trade Organisation. This chapter emphasises the importance of determining how the WTO provisions apply to the various forms of electronic transactions. In embarking on a national policy development initiative on e-commerce, it is imperative that South Africa, as member, takes cognisance of its WTO commitments. Firstly, to ensure that such as policy is compatible with the relevant WTO rules and regulations, and secondly, to determine the impact of e-commerce on these commitments, thirdly, to influence the WTO processes and programmes in the development of e-commerce rules.

Chapter 6 deals with some of the intellectual property protection issues raised by electronic commerce. It has become relatively easier to infringe intellectual property rights through the use of electronic technology. This chapter shows that the implementation of copyright, trademark and patent protection in an electronic environment constitutes a serious challenge to the development of e-commerce. These new technologies pose challenges to the existing legislation and enforcement mechanisms. The chapter further reviews recent international developments in the areas of intellectual property protection and electronic commerce.

Chapter 7 addresses concerns over lack of privacy on the Internet and security fears. These two concerns deter an adoption and use of e-commerce by individuals, organisations, enterprises and governments. If electronic commerce is to expand, trust needs to be established between parties. This chapter explores ways of establishing the integrity, authenticity, confidentiality and non-repudiation of information and transactions. Legal, procedural and technical means to ensure security and protect privacy are discussed. The discussions cover ways of providing a balance between the ability to combat on-line criminal activities while providing opportunities for users to use the new technologies.

In Chapter 8, consumers must be assured of confidence when conducting on-line transactions brochured. This chapter investigates and identifies the possible mechanisms of protecting consumers against dangers resulting from the easy and convenience of buying on-line. Ways to resolve dispute between buyers and merchants, redress and enforcement mechanisms are required to gain consumer confidence in the electronic environment.

Chapter 9 deals with the information communication infrastructural requirements for e-commerce. The chapter highlights the major challenges and barriers presented by the infrastructure requirements of a digital economy. Access and affordability are discussed as one of the major pre-conditions to be satisfied if individuals and enterprises are to participate in e-commerce. The growth of e-commerce depends on broad and affordable access to infrastructure, enabled by convergence of technologies, forward looking telecommunications policy, robust network infrastructure, sufficient bandwidth and support for targeted applications.

Chapter 10 discusses aspects of Internet governance and in particular the assigning and management of domain names within the South Africa country-level domain. This will be increasingly important as e-commerce expands and domestic companies establish Internet-based marketing and services that will be associated in the public mind with their brand name and hence their on-line domain. Issues around dispute resolution (i.e. trade marks Vs domain names) and security concerns are addressed. Organisational framework and possible structures are dealt with.

Chapter 11 discusses the infrastructure for electronic payments. Instruments such as credit and debit cards and smart cards are discussed in this chapter. Questions surrounding the security of these forms of payment are among the key concerns. The Reserve Bank's position Paper on electronic payment systems serves as a key reference to this chapter.

Chapter 12 highlights the benefits that can be gained from e-commerce especially with the implementation of successful strategies and the contribution that e-commerce can make to sustainable socio-economic growth. Strategies of promoting new business opportunities, market development, education and training, awareness and enablement, skills and jobs are identified.

Chapter 13 concentrates on how can the South African government become a model user of e-commerce. The chapter emphasises the importance of delivering government services on-line and using e-commerce applications in procurement and service delivery. It further investigates what actions need to be taken in becoming an electronic government. The challenges are vast and need the development of a comprehensive e-government strategy.

1. INTRODUCTION

1.1. GLOBALISATION AND THE INFORMATION SOCIETY

The transition of the global economy from an industrial focus to one based on knowledge and information presents numerous opportunities and challenges to countries, especially those in the developing world. This new paradigm has a significant impact on the way people lead their lives. It is enabled by the use of Information and Communications Technologies (ICTs) which have led to the compression of time and space. However, lack of infrastructure, prohibitive costs of access to infrastructure where it is available, poor quality of infrastructure, shortage of relevant skills, low levels of literacy and inadequate investment in technological development are hindering progress toward exploiting the new generation of ICTs in developing countries

Underpinning the importance of ICTs is digitisation. This has enabled the convergence of telecommunications, broadcasting, information technology and publishing. The increasing pace of technological innovations, such as the rapid integration of the Internet and other telecommunications based activities into nearly every sphere of business has given rise to new ways of communicating, learning and conducting business. The Internet has facilitated the establishment of a “borderless” environment for communications and the electronic delivery of certain services. Enter electronic commerce also known as e-commerce

Convergence of technologies is the major driving factor that contributes to the exponential growth of electronic commerce. Convergence goes beyond the use of technology to develop new products and services and is seen as a vehicle to improve the quality of life of society in South Africa and other developing countries. Convergence will open new opportunities for all as everyone gains equal access to information and the global markets. Small business will be able to compete on an equal footing with big business.

What is needed is an environment that is conducive to conducting business and sharing information with confidence. Government will provide support by setting policy and regulatory frameworks that are appropriate to the information communications technology sector while taking cognisance of the pervasive nature of e-commerce and the challenges pertaining to legal and security matters.

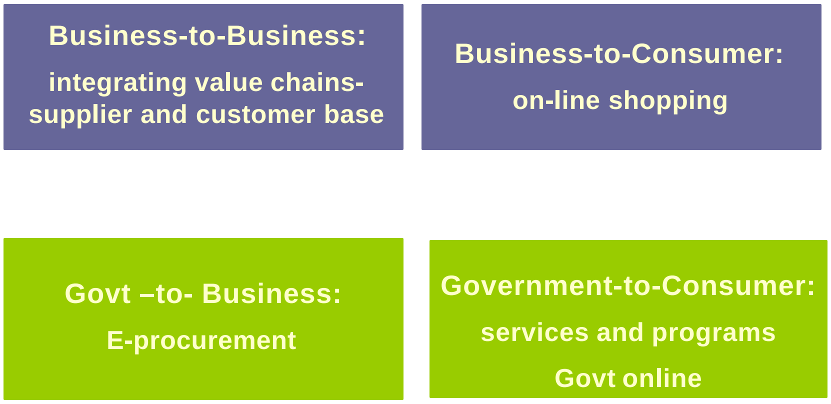
What is e-commerce?

Electronic commerce can be defined broadly as :

“The use of electronic networks to exchange information, products, services and payments for commercial and communication purposes between individuals (consumers) and businesses, between businesses themselves, between individuals themselves, within government or between the public and government and, last, between business and government ”

This definition encompasses the many kinds of business activities that are being conducted electronically, and conveys the notion that electronic commerce is much more comprehensive than simply the purchasing goods and services electronically.

Different Types of E-commerce:



Business-to-Business:
integrating value chains- supplier and customer base

Business-to-Consumer:
on-line shopping

Govt –to- Business:
E-procurement

Government-to-Consumer:
services and programs
Govt online

What are the benefits of e-commerce?

E-commerce is transforming the global marketplace and its impact is being felt across the full range of business and government. E-commerce requires an open, predictable and transparent trading environment, which operates across territorial borders and jurisdictions. To foster such an environment and to realise its full economic potential necessitates international co-operation, which will be instrumental in developing the enabling conditions for its growth.

Countries have to work together to remove barriers or impediments to the free flow of electronic products and services across jurisdictions and by resolving problems that may arise due to its borderless character. Government is shown to be the appropriate vehicle to ensure that this is possible.

The main benefits of e-commerce are demonstrable by the following achievements:

- **Improved response time**. Quick and cost efficient way through which to communicate and update information.
- **Improved competitive positioning.** Electronic commerce has a potential to level the playing field for small and large entities throughout the world. Small and Medium Enterprises and public sector customers reap the benefits of e-commerce.
- **Ease of concluding deals and financial transactions.** Click-and-pay technology is gaining popularity as a means through which to transact. Published information, communicating, buying, selling, paying and checking orders occurs 24 hours a day, 365 days a year.
- **Extended market reach and thus increased revenue potential.** Geographic barriers or boundaries are removed. There is an increased number of Internet users to market products and services at lower cost and much faster.
- **Increased consumer convenience and choice.** Consumers can easily locate hard to find goods and services, and also have a wide choice from which to make a purchase anytime, anywhere.
- **Reduced prices.** Increased competition forces organisations to produce better quality products at reduced cost.
- **Improved customer service.** Information is shared more quickly through the use of an electronic medium.

1.2 UNDERLYING PRINCIPLES FOR THE DEVELOPMENT OF E-COMMERCE POLICY

The development of the Green Paper and, subsequently, e-commerce policy in South Africa is based upon the following set of underlying principles:

1. Quality of life: to improve the quality of life of people through the optimal use and the exploitation of electronic commerce, thus ensuring socio-economic development and facilitating equitable development. This is consistent with the constitutional requirements and obligations.
2. International Benchmarking: to ensure international consistency, alignment and harmonisation. South Africa needs to be in line with international treaties and develop an e-commerce policy that is based on international trends and benchmarks while taking cognisance of South Africa's special requirements.
3. Consultative process: to be consultative, transparent and to balance the interests of the broader spectrum of stakeholder through the solicitation of the public to participate in the deliberations. This is an

ongoing process and has been taking place via electronic and written submissions by individuals and interest groups.

4. Flexibility: to be flexible in establishing rules and regulations for governance. The introduction of new measures and elements into law will take place within the relevant branches of law.
5. Technology neutrality: to cause the proposed legal framework be technology neutral
6. Supporting private-sector-led and technology-based solutions and initiatives wherever possible
7. Public-Private partnership: to establish public/private partnerships that will promote and encourage the development and use of electronic commerce. The private sector will remain a critical driving force in the effort to optimise the potential of e-commerce.
8. Supporting small, medium and micro enterprises (SMMEs) and informal sector: to facilitate the promotion and development of SMMEs and the informal sector, and contribute to their speedy adaptation of e-commerce.

1.3 WHY THE GREEN PAPER ON ELECTRONIC COMMERCE?

The Green Paper is intended to provide a platform from which to translate topical issues around e-commerce into government policy. The Green paper itself is not a policy document nor an academic paper, but is essentially a consultative document designed to raise questions on issues that need to be addressed by the Government policy formulation process.

Several policy issues arise as a result of the proliferation of e-commerce. These include development and access to the ICTs; taxation; security and privacy; protection of intellectual property; content development and regulation; electronic payment systems; standards and interoperability.

Transacting over the Internet can mean, for example, that a purchaser and vendor are located at different sides of the world; a scenario, which has prompted concerns for consumer protection and the right to redress. One of the main concerns generated by e-commerce is the priority that must be accorded to issues such as privacy of personal information to safeguard public interest. Any regulatory regime that South Africa adopts must be consistent and compatible with international frameworks.

1.4 THE PROCESS

The policy formulation process entails the creating of the following documents:

- Discussion Paper (July 1999),
- Green Paper (October 2000), (current phase)
- White Paper (2nd quarter 2001) and
- Specific legislation (3rd or 4th Quarter 2001.

The Green Paper will be used to:

- Build onto the Discussion Paper on Electronic Commerce.
- Consult stakeholders and solicit comments with a view to defining policy around e-commerce issues and laying a legal foundation appropriate for e-commerce in SA.
- Identify possible implications for broader economic and social policies
- Pose questions for policy consideration; in responding to the questions raised one should also make reference to the discussion paper and other relevant documents. See the e-commerce debate website: www.ecomm-debate.co.za
- Identify immediate actions for implementation by government and private sector in parallel with the process

Responses or submissions to the Green Paper are not limited to questions raised in the Green Paper; inputs on related activities and how they affect or contribute to the development of e-commerce are also welcome.

The process is expected to be complete in the third or fourth quarter of 2001 with the enactment of the necessary legislation and establishment of the necessary organisational framework or structures.

1.5 WHAT IS THE ROLE OF GOVERNMENT?

Government's role will be instrumental in developing the enabling conditions for growth of e-commerce by preventing and removing barriers. To foster a stable environment and to realise the full economic potential of e-commerce requires government participation. Challenges for government specifically revolve around:

p The need for adequate protection.

p Promoting easy and affordable access to information and communications infrastructure, technologies services

p Expanding policy issues associated with greater and faster broadband deployment and forward looking telecommunications market
p Ensuring rapid adoption of e-commerce by SMMEs
p Promoting and reinforcing education, skills development and awareness
p Positioning government as a model user of e-commerce in procurement and service delivery processes
p Adjusting the existing domestic and international regimes to this new reality
p Facilitating the development of the coherent SADC e-commerce framework

As with many other countries the challenge is for South Africa to develop a policy framework and strategy that will optimise and exploit the benefits of e-commerce. South Africa has to move quickly to strategically position itself and develop competitive edge within this new economy, based on its own particular political, social, cultural, economic and technological conditions. Government is committed to providing a supportive and responsive domestic environment for e-commerce.

In the light of the above, the resulting e-commerce policy framework should:
p Promote business growth and development through innovation and competition;
p Enable new job creation;
p Expand international trade and new markets;
p Attract foreign and local investment; and
p Improve the quality of life of all South Africans

1.6 BRIEF INTERNATIONAL PERSPECTIVE

E-commerce is being debated in various forums such as the OECD, APEC and WTO, WIPO, ITU, UNCTAD, World Bank, UNCITRAL. National governments are also moving to explore implications of e-commerce. The work of these organisations in the area of e-commerce is summarised as follows:

Organisation for Economic Co-operation and Development (OECD)
Representing the largest volume and amounts of transaction (about 90%) the OECD has been by far the leader in the development of an e-commerce framework.

International Telecommunication Union (ITU)
Currently busy with the development of practical handbooks for telecommunications policy makers and regulators covering issues related to e-commerce in conjunction with the World Bank. The ITU will also seek to raise

awareness of the role of telecommunications reform in the development of e-commerce with special emphasis on developing countries in terms of infrastructural development, market liberalisation and the proliferation of electronic services.

United Nations Commission of International Trade Law (UNCITRAL)
Has developed and adopted model law on e-commerce in 1996, which offers national legislators a set of internationally acceptable rules as to how a number of legal obstacles to the communications of legally significant information in the form of electronic communications can be dealt with. Most member countries, irrespective of their sovereign privacy laws have largely ratified the UNCITRAL model law.

United Nations Conference of Trade And Development (UNCTAD)
Has published a set of documents, prevalent being electronic commerce: legal considerations." The document proposes joint collaborative efforts with UNCITRAL. UNCTAD proposes to further work jointly with the World Intellectual Property Organisation (WIPO), and the International Chamber of Commerce.

World Intellectual Property Organisation (WIPO)
The WIPO arbitration and mediation centre has established an internet based, online dispute resolution system that can provide a neutral, speedy and inexpensive means of resolving disputes without the physical movement of persons and things. WIPO further provides a legal framework to deal with issues of Intellectual Property and e-commerce.

World Bank
Provides financial and other resource assistance in the development of e-commerce policies and applications. The World Bank further provides advocacy in building proper tax legislation including issues of taxation related to e-commerce.

World Trade Organisation (WTO)
The GATS provides a legal framework for all trade in electronic goods and services. TRIPS provides a framework for trade related aspects of Intellectual property rights and e-commerce.

International Labour Organisation (ILO)
Ongoing monitoring of the impact of digitisation on the protection of the rights performances works and remuneration of performers, journalists and the labour force in the electronic communications arena.

What is important to notice is that there is a great drive towards coherency and condensation of selective developments in international forums. Specific views and activities by each organisation on various areas of e-commerce will be dealt with throughout the paper.

1.6.1 AFRICAN PERSPECTIVE

The report prepared by UNCTAD *"Building Confidence: Electronic Commerce and Development"* has analysed the current status of Africa's readiness for e-commerce and identified possible strategies for improvement. According to the report there are over 550,000 dial-up Internet accounts for the over 750 million people in Africa. The Internet has numerous obstacles affecting its diffusion in Africa, namely, a shortage of telephone lines, lack of power supply, lack of access to computers, prices charged for access, slow speed and quality of service, content and language, etc.

Although so far participation by African nations in many of global forums and treaty organisations (as listed above) has been limited, some African countries and regional formations are already showing interest in the adoption of e-commerce and have initiated e-commerce-related activities. Africa's infrastructure initiatives/ strategies for e-commerce include:

- National Information Communication Infrastructure plan (NICI),
- African Connection – aimed at supporting the development of the underlying infrastructure required, the target is to lay 50 million lines in Africa over the next 5 years
- SADC (the Southern African Development Community) has begun to lay some of the groundwork for an e-commerce policy in its "Theme Document – SADC in the Next Millennium – The Opportunities and Challenges of Information Technology
- WTC (World Trade Centers Association) Trade Centres in Africa – aimed at promoting trade.
- Telkom SAFE (South Africa-Far East) cable, in collaboration with Malaysia Telecom, which will lay fibre between South Africa and Malaysia
- SAT-3/WASC (South Atlantic Telephony/West African Submarine Cable)- has been combined with SAFE
- Africa-One – aims to put an optical fibre necklace around the entire continent.
- RASCOM – to launch its own satellite
- Other related initiatives/plans include COMESA (Common Market for Eastern and Southern African), ECOWAS (Economic Community of West African States), EAC (East African Co-operation).

The African continent, SADC region in particular, will have to work on a coherent e-commerce strategy that would help the region to leapfrog not only the infrastructure, but also the implementation of e-commerce.

2. LEGAL FRAMEWORK

2.1 BACKGROUND

The current legal framework is tailored for paper-based commercial transactions. Therefore a need exists to formulate a new legal framework that also includes those transactions that are concluded electronically. From a policy perspective such a legal framework would have to address all the different factors and challenges that are associated with using an information and communication technology platform for a transaction to be legally valid.

Legal challenges around policy formulation in e-commerce basically revolve around the following issues to mention but a few.

- the application to electronic communications of statutory provisions which mandate paper or paper-based concepts such as original, writing and signature;
- Electronic formation of contracts
- Admissibility of electronic evidence;
- Authenticity and integrity of electronic communications;
- Information of material significance to confirm or enforce certain obligations to both dispatcher and recipient of goods or services, such as the time and place of dispatch and receipt of electronic information.
- Verification of dispatch
- Acknowledgement of receipt
- Management and retention of records
- Protection of the consumer
- New laws applicable and the relevance of the older ones
- Legal implications of e-commerce

To provide a certain and stable environment for conducting business, consumer protection becomes critical. The reason is that while the new environment provides new opportunities for business, it also brings new types of threats in the form of electronic fraud, cybercrime and new forms of cyber terrorism. The main areas that are cause for concern include privacy, fair trade, copyright protection, access by law enforcement agencies to information, increasing cross border business in consumer trade, computer crime, hacking and other aspects of the current legal framework designed to protect the rights of citizens. Because of the ease of operating across borders in the electronic environment, many of these issues have an international dimension that will be subject to negotiation of agreements, and potentially, to treaties in international forums.

The Internet on which e-commerce is strongly based makes it easy to operate across conventional country borders and poses new challenges for the laws of the country. This suggests that new laws will have an international perspective that includes negotiating new rules and common standards of practice that are relevant in the global environment. For example some countries have a legal framework that is heavily influenced by its international obligations, either through enacting such obligations in domestic legislation or through the Courts interpreting domestic statute or common law in -terms of such obligations.

It is acknowledged that e-commerce is not taking place within a legal vacuum for which a totally new legal framework needs to be created. There is a need to adapt existing laws and regulations to accommodate e-commerce. In this regard the Department of Communications has commissioned Edward Nathan & Friedland to carry out an audit of South African law, by reviewing the law, identifying areas that could constitute barriers to the development of e-commerce, and suggest options to eliminate such barriers.

Principles that underpin the formation of the e-commerce legal framework

Principles that underpin the work of government and stakeholders in shaping the legal framework for e-commerce basically revolve around the following principles:

1. The need for legislation to support the national implementation of electronic commerce transactions within a framework of international standards
2. The need to ensure that commercial transactions can be effected either through paper or electronic means without presenting uncertainty about the latter.
3. The desire to recommend legislation and limit it to areas where it is likely to increase the overall efficiency of South African commercial transactions. Any proposed legislation should not be cumbersome, but should minimise the regulatory burden on business and government, and keep litigation and costs to a minimum.
4. To ensure that any laws that are enacted to adapt to the law of contract are expressed in a technologically neutral manner; so that changes in the law are not restricted to existing technology but can also apply equally to new and future technology.
5. Any proposed legislation must be uniform and conform to existing international standards and rules. The United Nations Commission on International Trade Law (UNCITRAL), through its the Model Law on electronic commerce has also contributed significantly in this regard.

Issues to be considered within the legal framework include the following:

- Types of electronic transactions to be covered by the proposed legislation
- Uniform Commercial code for e-commerce
- Intellectual property rights
- Privacy and security
- Contracting and trade laws
- Place of jurisdiction in cross border e-commerce transactions
- E-commerce and multilateral trading system
- Electronic payment systems
- Governance in domain naming
- Taxation in the e-commerce environment
- Consumer protection issues
- Protection of personal data
- Institutional and organisational framework
-

The relevant sections throughout the document further elaborate and expand on the legal implications of the above issues.

QUESTIONS FOR POLICYCONSIDERATION

1. *South Africa must become a key player in influencing the global legal framework of the e-commerce environment. Can we single out areas where we could lead and influence?*
2. *Should the South African legal framework be guided by the model set by UNCITRAL?*
3. *There are other legal frameworks that are currently being formulated that are country specific. Which countries come close to representing a legal framework that will be significantly useful in South Africa's legal framework?*
4. *What laws need to be addressed in South Africa that are extremely critical to shape the South African e-commerce legal framework?*
5. *Does the South African legal system have a rule of law about infringements outside the country's border and other jurisdiction matters; if so how is judgement enforced?*
6. *Taking cognisance of the changing nature of technology, how flexible should the laws be that are being proposed to accommodate future changes?*

   What other issues are to be considered in the formulation of a legal framework that are not covered in this chapter.

3. CONTRACTING AND TRADE LAWS

3.1 INTRODUCTION

This section deals with matters directly affecting the legality and enforceability of commercial transactions.

Every country in the world has a legal framework in which its citizens are ensured of the validity and certainty of its traditional paper based commercial transactions. South Africa has to determine which of its long established legal foundations of contract law are challenged by electronic commerce and to what extent. South Africa also has to determine whether new issues, if any, introduced to contract law by the emergence of electronic commerce, require legislative intervention.

Issues fundamental to establishing the validity, recognition and enforcement of electronic commerce in contracting are identified in the United Nations Commission for International Trade Law Model Law document on electronic commerce as follows:

* Ensuring the legal recognition for a data message
* Admissibility and evidential weight of electronic messages
* Formation and validity of contracts and the recognition of electronic documents by parties
* Attribution of electronic documents
* Time and place of dispatch of electronic communications
* Signature

Currently South African law recognizes verbal agreements as legally binding, and that writing is not essential for the contract to b e deemed valid. However if each of the involved parties, or if a statute requires writing with or without signature, the contract will be deemed valid if there is compliance with such requirements. For example, the Credit Agreements Act No. 75 0f 1980. Therefore it is important to reach equality between electronic and traditional commerce.

Principles. The following principles were followed with regard to evaluating the need for electronic commerce legislation:

* **Not to re-invent the wheel.** Build on the extensive work that has already been done by international organisations and other jurisdictions.
* **Conform with international standards.** South Africa could introduce the "best" e-commerce laws in the world, based on international best practice.

However in so doing South Africa should strive to retain legal independence.

* **Enabling and not regulatory legislative intervention.** Introduce legislation that seeks to give equal status and recognition to both electronic and traditional (non-electronic) commerce.

* **Allow for contractual freedom and self-regulation.** Introduce legislation that allows contractual freedom or flexibility in shaping the commercial relationship

3.2 ENSURING THE LEGAL RECOGNITION OF ELECTRONIC COMMUNICATIONS

As a general rule, commercial transactions need not be concluded in writing to become valid and enforceable in South Africa. As in most countries, contracting and trade laws in South Africa were developed in a paper-based environment, and as a result, these laws contain provisions and terms ordinarily associated with paper-based documents and actions. These laws include words such as “document”, “writing”, “signature”, “original”, “copy”, “stamp”, “seal”, “register”, “file”, “deliver”, etc. In terms of the ordinary rules of construction, the definitions of these terms may be confined to a paper-based environment. Some of the terms are irrelevant or not applicable in e-commerce based transactions. Since some laws locally and internationally require compliance with terms such as “original”, “duplicate”, “copy”, “registration”, “filing”, “certification”, “seal”, “stamps”, “authentication” etc either to establish or enforce an agreement. Non-compliance with these requirements may directly or indirectly affect the validity or enforceability of a transaction

Legislation governing contracting and trade that is technology neutral is required. The use of an electronic medium should not affect the laws that would ordinarily govern the transaction. In particular, the intended legislation should provide clarity on how electronic communications will satisfy requirements by law to the extent that:

- an electronic communication constitutes a document;
- certain information be “in writing”;
- certain information be presented or retained in its “original” form;
- certain documents, records or information be retained;
- a document (electronic communication) be authenticated.

QUESTIONS FOR POLICY CONSIDERATION

1. *To what extent should Government introduce legislation on the legal recognition of electronic documents and communications? What considerations should be taken into account?*

2. *Should legislation prescribe standards to which electronic documents must conform before qualifying as "writing" or "original"?*
3. *What exceptions, if any, should be provided for (e.g. wills and sale of land agreements)?*
4. *To what extent should SA have regard to international guidelines and national legislative initiatives?*

3.3 ADMISSIBILITY AND EVIDENTIAL WEIGHT OF ELECTRONIC COMMUNICATIONS

Evidence, whether contained in documents or led through oral evidence, must be *admissible* before a court would have regard thereto. Certain admissible evidence carries more *evidential weight* or *value* than others. In terms of the rules of evidence, the admissibility or evidential weight of evidence would depend on whether the "*best evidence*" thereof had been presented to the court.

With regard to paper-based documentation, the "best evidence" rule provides that an original of a document must be presented to the court. If the original has been lost, destroyed or is unduly burdensome to obtain, a party may lead secondary evidence to prove that a copy thereof (e.g. a photocopy) is a true copy of the original. However, the evidential weight of such secondary evidence may be less.

In the electronic environment, the distinction between original and copy becomes blurred. Documents created electronically (e.g. by word processor) have different attributes than a paper-based documents. Even though admissible, the evidential weight of electronic documents may be adversely affected by their ease of alteration without leaving any trace. Can or should a printout be said to be a "copy" (secondary evidence) of the "original" electronically stored version? It should be kept in mind that paper documents have generally carried substantial evidential weight because of the inherent inalterability thereof.

Discrepancies arising from the inaccuracy of computer evidence led to the enactment of the Computer Evidence Act 57 of 1983. However, problems experienced regarding its implementation led to an investigation by the South African Law Commission. The Commission found the Computer Evidence Act inadequate, even though the Act was expressly meant to address the admissibility of "computer evidence" in civil proceedings. According to the Commission, the reason for the inadequacy is the stringent requirement about authentication of computer printouts prior to their admission as evidence. It would seem that the Computer Evidence Act applies only to computer printouts where the data contained therein were created by some human agency or intervention. Accordingly, computer evidence created automatically without human intervention would not be governed by the Act. Thus courts would consider evidence with a view to how it was generated.

Therefore, law that provides clear guidelines on the admissibility and evidential weight of electronic records is required. Such law should possibly draw a distinction between computer evidence created with and without human intervention.

QUESTIONS FOR POLICY CONSIDERATION

1. *To what extent should Government introduce legislation on the admissibility and evidential weight of electronic communications and what considerations should be taken into account?*
2. *Is the current Law Commission initiative sufficient to address the problem? If not, what should the Commission take into account?*
3. *How should the law treat computer evidence generated with and without human intervention?*

3.4 FORMATION AND VALIDITY OF CONTRACTS AND THE RECOGNITION BY PARTIES OF ELECTRONIC DOCUMENTS

An agreement is concluded between two parties upon the acceptance by one party of the valid offer of another. In the absence of specific legislation requiring formalities, an offer and the acceptance of an offer can be expressed orally, in writing or by the conduct of the parties.

Although South African law is likely to give legal effect to an offer and acceptance in electronic format directly generated between two parties, some uncertainty may exist with regard to the absence of immediate human intervention in the generation by computers of electronic messages expressing offer and acceptance. An example of the latter is electronic data interchange (EDI), "click-wrap and shrink-wrap". To date the legality of the latter mode of contracting has not been tested.

Apart from electronic communications geared for the conclusion of a contract, certainty should also be provided regarding the use by parties of electronic messages geared for the performance of contractual obligations. Specific examples are notice of defective goods, an offer to pay, notice of places where a contract will be performed and recognition of debt.

3.4.1 Recommendations

The drawing up of legislation that recognises the validity and enforceability of a contract formed by transmitting an electronic communication. Furthermore, between the originator and the addressee of an electronic message, a declaration of will or other statement should also not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of an electronic communication

QUESTIONS FOR POLICY CONSIDERATION

1. *To what extent should Government introduce legislation on the formation and validity of contracts and on the recognition by parties of electronic documents, and what considerations should be taken into account*
2. *Should the law prescribe specific procedures for offers and acceptance thereof in electronic form?*
3. *How should the law treat offers and acceptance of offers or other messages expressed as electronic communications generated automatically by computers without human intervention?*

3.5 ATTRIBUTION OF ELECTRONIC DOCUMENTS

Certain "default" rules or presumptions have been developed by the law over many years in terms of how the court, in certain circumstances, will deem a purported state of affairs to be a fact or the truth unless proven otherwise. In the absence of these presumptions, a party trying to prove a contract or a certain state of affairs may find it unduly burdensome or even impossible to prove or defend a claim.

There may be a question as to whether an electronic communication was in fact sent by the person who is indicated as being the originator. In the case of a paper-based communication, the question would arise as the result of an alleged forged signature of the purported originator. In an electronic environment, an unauthorised person may have sent the message but the authentication by code, encryption or the like, might be accurate. Due to the impersonal (not face-to-face) and instantaneous nature of e-commerce transactions, commercial practice may require the law to provide some measure of certainty in this regard.

The law may have to deal with the issue of attributing an electronic communication to its purported originator by establishing a legal presumption that in certain circumstances a communication would be considered as a message sent or authorised by the originator. Such a presumption must be qualified where the addressee knew or ought to have known that the electronic communication was not that of the originator. In traditional transactions, no express presumption of attribution exists. However, in terms of the doctrine of "estoppel" in South African law, a purported originator who never sent nor authorised a communication to be sent, may nevertheless be held bound in law if his negligent conduct, whether by action or omission, induced a reasonable belief of authenticity in the mind of the addressee, which caused the latter to act thereon to his/her peril.

Due regard should be taken that legal presumptions, if any, would apply only in the absence of contractual arrangements governing attribution, for example, the use of certification authorities.

QUESTIONS FOR POLICY CONSIDERATION

1. *To what extent should Government introduce legislation on attribution of electronic documents and what considerations should be taken into account?*
2. *Should e-commerce be perceived as introducing higher risk, if so, would this perceived risk factor justify specific legislative intervention concerning the attribution and reliance of electronic communication?*
3. *What exceptions to legislative intervention, if any, should apply?*
4. *Should presumptions be applied with regard to the attribution of electronic messages, and would these cause any imbalance in legal treatment of traditional and electronic transactions.*

3.6 TIME AND PLACE OF DISPATCH AND RECEIPT OF ELECTRONIC COMMUNICATION

To test and enforce compliance with the existing rules of law, it is important to ascertain the time and place of receipt of information.

The use of electronic communication techniques makes it difficult to ascertain the time and place of contracting. It is not uncommon for users of electronic commerce to communicate from one country to another without knowing the location of any information systems through which the communication is effected. Furthermore, the location of certain communication systems may change without either of the parties being aware of the change. The question is whether the law should take into account the location of information systems and their components; or whether there are more objective criteria, such as the place of business of the parties, that should be considered.

In terms of South African law, two general methods are applied by courts to establish the time and place of contracting. The distinguishing factor in each is the mode of delivery or communication used. The ***expedition theory*** generally applies to postal contracts and provides that a contract concluded via the post comes into existence at the place where and time. When a letter of acceptance is posted or the telegram of acceptance is handled in a post office. The ***information theory*** generally applied to modes of direct, interactive communication (e.g. the telephone) and provides that a contract is concluded at the place where and time when the acceptance is brought to the mind of the offeror. The question arises whether these theories provide adequate solutions or guidance where parties contract by electronic means (e.g. by exchange of email).

The time when and place where an e-commerce contract is concluded are fundamental to determining whether South African courts have jurisdiction to adjudicate a dispute involving both local and foreign nationals and, if so, which country's laws our courts would apply. The capacity of one of the parties to contract (e.g. matrimonial property issues in different countries) may also be affected by the place where a contract is deemed to have been concluded.

QUESTIONS FOR POLICY CONSIDERATION

1. *To what extent should Government introduce legislation that provides clarity on the time and place of dispatch and receipt of electronic communications for the application of both the expedition and information theories to hold, and what considerations should be taken into account? In particular:*
2. *How should the law deal with issues relating to jurisdiction, choice of law and capacity to contract in an electronic commerce environment?*

3.7 SIGNATURE

As a general rule, written agreements need not be signed to become binding. However, when legislation or the parties require signatures, this requirement must be complied with for the agreement to be valid or enforceable. Signatures, in whatever form, serve primarily to (a) confirm or endorse the intent; (b) identify the signatory and (c) authenticate and confirm the integrity of the document signed.

In the faceless, impersonal environment of the Internet, these objectives will play a vital role in creating confidence in e-commerce transacting. In this regard, technology has been developed (generally referred to either as *electronic* or *digital* signature that serves to accomplish these objectives. The following distinction between *electronic* and *digital* signatures will be noted.

Electronic signature is a generic, technology neutral term that refers to the universality of all the various methods by which one can "sign" an *electronic* record. Electronic signatures can take many forms and can be created by many different technologies. Examples include a name typed at the end of an e-mail message by the sender; a digitised image of a hand-written signature that is attached to an electronic document; a secret code or PIN; a code that the sender of a message uses to identify herself; a biometrics-based identifier e.g. a fingerprint; and a digital signature created through the use of public key cryptography.

Digital signature is simply a term for one technology-specific type of electronic signature. It involves the use of public key cryptography to "sign" a message. For our purposes, we will use the same distinction between *digital* and *electronic* signatures hereinafter.

It is unclear whether the South African law would afford all forms of electronic signatures the same legal recognition and evidential weight as hand-written signatures. In the absence of specific requirements prescribed by legislation, the law generally appears to be flexible enough to regard any *mark or symbol* applied by a contract party signifying her or his intent to be contractually binding and therefore constituting a *signature*. However, in the absence of clear court rulings, parties will continue to use electronic signatures with some degree of legal risk. Moreover, some legislation may be drafted such that it confines signature requirements to a hand-written ink-on-paper format to accommodate electronic signatures.

The question arises then whether electronic signatures should be regulated to ensure the adherence to certain standards. In the absence of electronic signature standards, whether legislated or not, the general rule is that the party relying on an electronic signature would have to prove to a court that the underlying technology achieves the objectives.

In general, governments may elect to follow one of the following options with regard to digital or *electronic* signatures:
(a) no regulation or standards;
(b) private sector regulation;
(c) compulsory adherence to legislated standards; or
(d) voluntary registration in terms of legislated standards.

QUESTIONS FOR POLICY CONSIDERATION

1. *To what extent should Government introduce legislation on the recognition of electronic signature as equivalent to traditional signature and what considerations should be taken into account? In particular, which of the following options should Government follow and to what extent:*
2. *(a) no regulation or standards;*
3. *(b) private sector regulation;*
4. *(c) compulsory adherence to legislated standards; or*
5. *(d) voluntary registration in terms of legislated standards?*

4. ELECTRONIC COMMERCE AND SOUTH AFRICAN TAXATION

4.1 INTRODUCTION

As e-commerce changes the traditional ways of doing business, new electronic products and delivery systems result. Certain products may be delivered electronically rather than in physical form: examples include computer software, music, video clips, photographs and a whole range of written text. Where such products are sold, the important issue is whether payments are royalties, or for the provision of goods or services not involving the use of copyright. E-commerce gives rise to an issue concerning the characterisation of income under double taxation agreements. Taxation rules distinguish between the sale of goods, the provision of services and the use of intangibles. Where double taxation agreements are followed, the question of how taxing rights are allocated will have to be resolved. For example, many double taxation agreements allow the source country to tax royalty payments, payments for the lease of property and, in some cases, payments for certain types of services.

There is a legitimate concern by certain governments that the development of the Internet may have the effect of shrinking the tax base and hence reducing fiscal revenue. The reasons behind these concerns are on the one hand the difficulties inherent in defining jurisdiction in cyberworld; and on the other hand the problem of administration and enforcement. In addressing these problems and in developing a taxation framework, it is important to ensure that the taxation systems are fair, predictable and do not distort the conduct of business. The challenge therefore for South Africa is to develop a taxation policy that is not isolated from its e-commerce partners.

4.2 INTERNATIONAL PERSPECTIVE ON TAXATION

International organisations and governments have highlighted principles that should guide the work of governments in the field of taxation of electronic commerce. These include the Organisation for Economic Co-operation and Development (OECD), the U.S. government and the World Trade Organisation (WTO).

4.2.1 OECD Perspective

The principles-based approach adopted by the OECD culminated with an agreement that the following widely accepted general tax principles should apply to the taxation of e-commerce:

- **Neutrality.** Taxation should seek to be neutral and equitable between forms of e-commerce and between conventional and electronic forms of commerce. Business decisions should be motivated by economic rather than tax considerations. Taxpayers in similar situations carrying out similar transactions should be subject to similar levels of taxation. In other words there is no need for a special new tax such as a "flat rate" or a "bit" tax.
- **Efficiency.** Compliance costs for taxpayers and administrative costs for the tax authorities should be minimised as far as possible.
- **Certainty and Simplicity:** The tax rules should be clear and simple to understand so that taxpayers can anticipate the tax consequences in advance of a transaction, including knowing when, where and how the tax is to be accounted.
- **Effectiveness and Fairness:** Taxation should produce the right amount of tax at the right time. The potential for evasion and avoidance should be minimised and counter-acting measures should be proportionate to the risks involved; and
- **Flexibility:** The systems for taxation should be flexible and dynamic to ensure that they keep pace with the technological and commercial developments.

The above framework is not at odds with the views held by SARS. Nevertheless, care should be taken to ensure that the existing South African tax-base is not eroded by international decisions favouring nations with sophisticated and developed economies.

4.2.2 The US Treasury Department

The document "*Selected Tax Policy Implications of Global Electronic Commerce*" dated November 1996, identifies the following points:

- New technologies, such as the Internet, have effectively eliminated national borders on the information highway. As a result, cross-border transactions may run the risk that countries will claim inconsistent taxing jurisdictions, and that taxpayers will be subject to quixotic taxation.
- In order to ensure that these new technologies are not impeded, the development of substantive tax policy and administration in this area should be guided by the principle of neutrality.
- Transactions in cyberspace will likely accelerate the current trend to de-emphasize traditional concepts of source-based taxation, increasing the importance of residence-based taxation.

- Another major category of issues involves the classification of income arising from transactions in digitized information.
- The major compliance issue posed by e-commerce is the extent to which electronic money is analogous to cash and thus creates the potential for anonymous and untraceable transactions.

On 21 October 1998, the Internet Tax Freedom Act was signed as public law 105-277 in the USA. This Act places a moratorium on any new taxes on Internet access and created a commission to study and make recommendations about domestic and foreign policies toward the taxation of e-commerce. This commission completed its work on 3 April 2000 with a number of proposals, including an extension of the moratorium on new taxes on Internet access and support for the extension of the WTO moratorium on tariffs and duties on electronic transmissions. It should be stressed that the Internet Tax Freedom Act is in respect of new taxes and has no bearing on existing tax legislation, for example, the taxing of Internet sales for income tax or sales tax purposes.

QUESTIONS FOR POLICY CONSIDERATION

1. *To what extent should South Africa adopt the OECD and the U.S principles as stated above?*
2. *What would be the implications of not adopting and/or adapting these principles?*
3. *To what extent would the current moratorium on custom duties affect the South African fiscal revenue?*

4.3 E-COMMERCE AND TAXATION CHALLENGES

4.3.1 Characterization of income

Residence versus Source. The tension between residence-based and source-based taxation lies at the heart of the e-commerce debate. Most first-world countries follow the principle of taxing worldwide income of residents of the country and income sourced in that country belonging to non-residents. Where a double tax agreement (DTA) exists, income sourced in that country is only taxed in the case of non-residents where certain types of income are involved or a Permanent Establishment as defined by the DTA is present. Double taxation is avoided through DTAs, which make the residence country responsible for giving credit relief or exemption for foreign income taxed at source.

The basis of the South African income tax system is to change from one of source to one of residence with effect from 1 January 2001. This represents a major tax policy change in South Africa and in many respects pre-empts any such policy recommendation that might have arisen from the "E-commerce Debate". It should be borne in mind that this switch is much broader than catering for e-commerce alone. As such, much of the rest of this "residence versus source" debate relates to the position up until 31 December 2000.

It should, however, be noted that source will remain an issue for non-residents whose income is derived from a South African source after 1 January 2001. As a general rule, income earned from a South African source is taxable in South Africa. The provisions of section 9 of the Income Tax Act, 58 of 1962 as amended, extend the circumstances under which amounts are deemed to have accrued from sources within the Republic. These are referred to as the 'deeming provisions'

The deeming provisions give rise to two important tests. The first is in respect of natural persons and involves residence, and relates to the question as to whether the person concerned is 'ordinarily resident' in the Republic of South Africa? The second is in respect of legal persons and relates to whether such an entity is 'managed and controlled ' in South Africa. In the context of e-commerce, there should be no problems regarding natural persons. The second is cause for concern and thus is addressed further in the following sub-sections:

Residence of Companies. Section 1, of the Income Tax Act, 58 of 1962, as amended, defines a 'domestic company' as *'a South African company or a company, which is managed and controlled in the Republic'.* In the world of e-commerce, a company may for all practical purposes only exist in cyberspace. Business can be conducted electronically with directors meeting by way of video-conferencing. SARS may now find it challenging to establish whether a company is in fact 'managed and controlled' in the Republic. The Katz Commission's main criticism of the definition of a domestic company is that it has proven subject to relatively simple, formalistic manipulation. This concept is also out of line with the commonly used, and much more substantial, tax treaty expression of 'effective management'. The Commission further recommends that the concept of effective management as referred to in Article 4(3) of the OECD Model Tax Convention be used consistently to designate the tax residence of persons other than natural persons. This recommendation has been taken up in the proposed change to the residence basis of taxation, as a company's residence will be determined by its place of incorporation or effective management. Even with the suggested change, determining whether an 'e-company' is effectively managed in the Republic could prove problematic. This is an international problem and is the subject of efforts by a working group of the OECD.

Residence of a Trust. In Section 1 of the Act a 'person' is defined as including an insolvent estate, the estate of a deceased person and any trust. A trust is considered to be a person for tax purposes. Where reference is made to the ordinary residence of a ‘person’ (other than a company), for example in Section 9(1) of the Act,it also includes a trust. It is submitted further that if the executors, administrators or trustees are resident in the Republic and if the estate or trust fund is administered from the Republic, the estate or trust is resident in the Republic. Each instance must be decided on its own merits, but the place where the assets of the estate or trust are managed or controlled may well be crucial. Sections 9C and D of the Act create no new difficulties as to the residence of a trust. Residence is established in Section 9C(1) where ‘resident’ is defined as meaning any natural person who is ordinarily resident in the Republic and any person other than a natural person which has its place of effective management in the Republic. Hence, the residence of a trust, being a person other than a natural person, would be the same as that of a company. The proposed change to the residence basis of taxation builds on this formulation, as the residence of a trust will be determined by its place of formation or effective management.

***Residence of a Partnership*.** A partnership in South Africa is not a separate legal *persona* distinct from the persons who constitute the partnership, nor is it recognised by the Income Tax Act as a distinct taxable entity.

Transfer Pricing. If it is determined that an enterprise does have a Permanent Establishment in another country, another important issue then arises of how to attribute profits to the Permanent Establishment. The Committee on Fiscal Affairs is currently considering this question as part of the wider issue of the application of the OECD transfer pricing guidelines to e-commerce.

4.3.2 Indirect (Consumption) Taxes

Even more urgent tax issues arise in relation to the application of indirect taxes to e-commerce.

Place of Consumption. Indirect taxes should apply where consumption takes place, and an international consensus should be sought on the identification of the place of consumption. Consensus is essential to avoid double taxation or unintentional non-taxation, particularly as double taxation treaties do not apply to indirect taxes. The main difficulties that arise here are that the supplier may not be able to determine the location of the customer and may also be outside the fiscal jurisdiction of the authorities in the country where the consumption takes place.

Electronic Products. The supply of electronic products should not be treated as a supply of goods. Many Revenue authorities have already reached this conclusion, which means that, under most VAT systems, the supply of electronic products would be treated as a supply of services. This treatment would prevent the problems that could otherwise arise in relation to taxes on importation and the application of place-of-supply rules.

"Reverse Charge" Mechanism. The use of the "reverse charge" mechanism or similar mechanisms should be considered for the taxation of businesses that acquire services and intangible property from suppliers outside the country. In relation to VAT systems, the "reverse charge" mechanism requires the customer to account for output VAT on imported services, but it also gives a right to an input tax deduction.

Private Consumers. The collection of indirect taxes from private consumers represents the major area of concern in relation to the application of indirect taxes to e-commerce. Three main options have been considered:

- The supplier is required to account for taxation in the country of consumption.
- The customer is required to account for the tax. This is the position in South Africa where goods are not required to be entered through Customs and Excise or a service is rendered.
- The payment intermediary (such as the bank or credit card company dealing with the payment) is required to account for the tax.

Each of these three alternatives is potentially unsatisfactory and it has been suggested that the best approach may be to require the supplier to account for the tax but to simplify greatly the existing registration procedures.

OECD and EC Treatment. How Vat should be treated online has not been fully resolved. The European Commission and the OECD have a position, which appears not to adequately address the issue. The blanket characterisation of all on-line deliveries as supplies of services, even where a similar product can be delivered physically at a zero or reduced rate, does not appear to be fair. Unless rates and other differences in treatment are equalised, this will result in the heavier consumption taxation of many electronic commerce transactions.

Fortunately these problems are less likely to occur with the South African VAT system as a result of the limited number of zero ratings and the uniformity of the system.

4.3.3 Customs and Excise

When establishing the treatment of imported supplies for customs duty purposes, a distinction should be drawn between goods ordered electronically but delivered by traditional means and direct on-line delivery of electronic products. With the increased use of electronic media as a method of ordering goods, there is likely to be a parallel increase in the number of small packages arriving in South Africa. As e-commerce becomes more popular and a greater number of small packages enter SA, so too will the workload of the customs component increase. SARS has already increased its presence at the three places of postal entry into the country. Noteworthy is that in South Africa even if an imported good is exempted from Customs Duty in terms of a *de minimus* rule, VAT is still payable.

4.3.4 Gaming and Betting

E-commerce has the potential to facilitate the growth of internet-based gaming and betting. “Virtual Casinos” established outside of South Africa will escape the need to be licensed as well as the duties payable unless this issue is urgently addressed. The e-commerce forum of the Department of Communications would be the ideal facilitator in resolving this issue.

4.3.5 Stamp Duty

An issue requiring consideration in respect of stamp duty is where a transaction might be carried out without the need for a hardcopy legal document. In the United Kingdom in 1986, a Stamp Duty Reserve Tax (SDRT) was introduced as a backup for stamp duty where a transaction was carried out without the execution of a legal document. At that time, SDRT did no more than fill a few gaps. The two taxes do not apply simultaneously.

QUESTIONS FOR POLICY CONSIDERATION

1. *What further challenges can be identified that e-commerce poses to taxation?*
2. *What further measures and mechanisms should be put in place to address the challenges as stated in section 4.3 above?*
3. *What implications does Internet gambling have on fiscal revenue and foreign exchange control policy?*
4. *How should indirect taxes on electronic products be collected form private consumers?*

4.4 THE THREAT OF CYBER CASH

Payment systems fall into two basic categories: “accounted” and “unaccounted” systems. Accounted systems require payment to be effected through a third party, independent of the payer and the recipient. Examples are cheques and credit card transactions. The key feature is that accounted systems generate a record, linked to a person, which can be produced if necessary for tax or for other audit purposes.

Unaccounted systems allow value to be transferred without the involvement of an independent third party. The obvious example is cash. Here the key features are that there is no independent record and no need to identify the parties to the transaction.

Electronic payment systems can be categorised as either credit card systems, stored value cards (SVCs) or network money. SVCs or "smart cards" are like debit cards where the store of value is on the card and not in a linked bank account. The card user prepays the issuer, the value of which the issuer inscribes on the SVC. The card keeps track of the progressive decline in the inscribed value as the card is used to make purchases. In South Africa, a number of banks are at fairly advanced stages of SVC introduction.

Network money also represents stored value, which has been pre-purchased, but with the difference that the value is stored on the Internet or on devices attached to the Internet such as computers instead of a plastic card. Network money is therefore, transferable over the Internet. Electronic money can in principle be sent overseas with as little formal difficulty as attaching an enclosure to e-mail and sending it to a supplier. It is secure, not in principle limited to any maximum value, and delivery costs are low. From an audit trail perspective, payments such as these are very unlikely to be monitored.

A factor that may to some extent retard the popularity of electronic money, currently at any rate, is culture. People need to trust the system and the system needs to be useable and secure. Network money still requires substantial development to rid itself of the shackles of cultural conservatism. However, it is not believed that this will take v ery long, if the Internet is used as the yardstick in technological advancement.

The Australian Tax Office (ATO) notes that the widespread use of such unaccounted electronic payment systems would be a matter of extreme concern to most revenue authorities, allowing the enduringly problematic domestic physical cash economy to migrate to an international electronic cash economy. Revenue authority concerns regarding unaccounted electronic payment systems would be greatly alleviated by the inclusion of an appropriate minimum level of accountability in such systems. The ATO sees electronic money, and particularly unaccounted electronic money with its capability of effecting payment at a distance, likely to significantly and adversely impact upon the enforcement of tax law. The evasion potential of conventional cash is limited by its "hand-to-hand" nature. Payments of electronic money can be made across the globe in seconds.

The ATO make the following two recommendations:

- A regulatory distinction should be drawn between accounted and unaccounted payment systems; and
- Principles governing access to the records of electronic money issuers need to be developed internationally.

QUESTIONS FOR POLICY CONSIDERATION

1. What implications does cyber cash electronic money have for foreign exchange control policy?

2. What principles should be developed to give access to the records of electronic money issuers and users?

4.5 TAX ADMINISTRATION AND COMPLIANCE ISSUES

Identification. The accurate identification of the party responsible for paying a particular tax is a fundamental requirement of any taxation system. Tracing the physical owner of a website inadequately identified, can be a time-consuming process often with reliance having to be placed upon a third party. Conventional businesses are easier to keep track of as they operate from a physical and geographical location that can be visited. In addition, all conventional correspondence of Companies, Close Corporations and Trusts in South Africa require the relevant registration number to be displayed. As there is to some extent a blurring of the mere advertising and the actual trading capabilities of an enterprise's website, some attention ought to be given to drafting a minimum standard in respect of identification requirements.

It is considered advisable from both the SARS perspective and, as noted in Chapter 8, the consumer's perspective that a minimum standard of on-line contact information be required of enterprises using a website. The following information should be furnished on any commercial website owned by a South African resident, company, close corporation or trust: trading name of the business; the physical as well as the postal address of the business; an e-mail address; telephone or other contact information and statutory registration number in respect of companies; close corporations and trusts.

Many tax administrations consider information such as the above as the only means of identifying businesses engaged in e-commerce.

Information. The ability to access reliable and verifiable taxpayer information is essential for any tax administration to be able to do its job properly. Electronic accounting records have been used for years. In many instances SARS has been able to place reliance on secondary sources within the country in order to verify the reliability of the digital records. Where electronic data systems are sophisticated the businesses concerned are generally large, independently audited, with adequate segregation of duties, ownership and management. There would thus be some confidence that the electronic records are complete and accurate. Development in the nature of e-commerce potentially alter this.

A further problem that may to some extent complicate matters is that the storage of information overseas is becoming easier and cheaper as a result of reduced storage and transmission costs. It is also highly likely that many encryption keys will be stored overseas – particularly in respect of multinational enterprises.

Evidence. In South Africa, tax laws as described above have developed to provide a framework for the collection and retention of commercial documents by taxpayers. To date the law has been based on physical businesses conducting business using traditional methods to record their transactions. This legal framework is also dependent on established rules of evidence which apply in court to test the probity of facts and documents. A foundation has been laid by the SA Law Commission to ensure the admissibility and probative value of computer evidence in litigation.

The ATO considers that where the integrity of electronic records can be verified and ensured, the records should have the same standing as traditional paper documents.

Collection. Some of the most efficient collection mechanisms are those which make use of a leverage point. A common example is PAYE where a limited number of employers collect the taxes on behalf of SARS from a significant number of taxpayers. Collection activities are concentrated, in other words. As e-commerce tends to eliminate the “middleman”, so too could tax collection efficiency be reduced.

All collection proposals, in essence, require a greater degree of international co-operation in revenue collection than currently exists. To this end the OECD is considering developing an article for inclusion in its Model Tax Convention to allow for assistance by one State in the collection of tax for another State. Efficient tax collection mechanisms are fundamental to an effective tax administration and as the risks are essentially common to all administrations. The UK Inland Revenue, in its report of November 1999, concludes that many of these risks can best be tackled in co-operation with other countries.

QUESTIONS FOR POLICY CONSIDERATIONS

1. *SARS has already indicated some of the perspectives in the tax administration of electronic transactions. What other views and proposals should be taken into consideration?*

4.6 AREAS OF CONCERN FOR POLICY CONSIDERATION

Areas of immediate concern to SARS, which could seriously impact upon the effectiveness of ensuring tax compliance in respect of e-commerce within South Africa, are reflected below. Accordingly, it is suggested that policy recommendations be formulated and the necessary action taken to ensure that the e-commerce environment in South Africa is fair and equitable for all stakeholders:

- **Residence Basis of Taxation.** A policy decision in this regard has already been made as announced by the Minister of Finance in the Budget Speech of 23 February 2000. With effect from tax years ending on or after 1 January 2001, South African residents will be taxed on “worldwide” income, irrespective of where in the world that income was earned.
- **Electronic Money.** Principles governing access to the records of electronic money issuers need to be developed.
- **Identification of website owners.** Principles governing the information to be furnished on any commercial website owned by a South African resident, company, close corporation or trust need to be developed.

Many commentators are of the opinion that there is no need, at this stage, for the implementation of any new taxes relating specifically to e-commerce and that with modifications, where necessary, existing legislation is capable of coping with the risks concerning e-commerce transactions. Most of the developments taking place internationally are going to require consensus from all stakeholders in order to ensure that e-commerce is harnessed and not effectively stifled.

QUESTIONS FOR POLICY CONSIDERATION

1. *In your opinion, is there any need to introduce new taxes on electronic commerce transmissions? If yes, how should they be administered?*

5. THE MULTILATERAL TRADING SYSTEM AND E-COMMERCE

5.1 INTRODUCTION

The Multilateral Trading System (MTS) is currently embodied in the WTO, and the term “multilateral” is used because not all countries are members of the WTO. The predecessor of the WTO was the General Agreement on Tariffs and Trade (GATT), the rules of which governed international trade from the time of its establishment in 1948 until the birth of the WTO in 1995. The WTO was legally established on 1 January 1995 and currently consists of 136 members. It is the only international body dealing with the rules of trade between nations. The WTO Agreements negotiated and signed by most of the world’s trading nations, provide the legal ground-rules for international commerce in order to promote a stable, predictable and transparent multi Internet trading system. In effect, these agreements are contracts, binding governments to keep their trade policies within agreed limits.

In essence, the establishment of the WTO has considerably circumscribed the freedom of sovereign governments to develop macroeconomic policy. All such policies must be WTO-consistent, and if not found to be so by a dispute settlement panel, may result in retaliatory measures by the aggrieved country or countries. The legal enforceability of the WTO and its Agreements stem from the fact that they are permanent, unlike the GATT, which was ad hoc. As an international organisation the WTO has a sound legal basis because members have ratified the WTO Agreements and incorporated them into national legislation. Further, the Agreements themselves describe how the WTO is to function. It is therefore clear that all WTO member countries have to take cognisance of their WTO commitments when formulating macroeconomic policy since these commitments are contractual obligations which governments have agreed to undertake.

Although e-commerce is currently being debated in various multilateral forums such as the OECD, WIPO and WTO, sufficient consensus in other areas around e-commerce has not been reached. To facilitate the growth of e-commerce it is essential that trade agreements and the domestic laws implementing them are, and should be technologically neutral, applying the same rules to an economic transaction, irrespective of the technology used to produce or deliver the product.

There is an agreement among Governments that the international and domestic regulation of commerce has been and will continue to be dealt with in various international forums, but principally within the framework of rules and procedures set out in the WTO Agreement.

As a founding Member of GATT and the WTO, South Africa is committed to the development of a stable, predictable and transparent Multilateral Trading System. In embarking on a national policy development initiative on e-commerce it is imperative that SA take cognisance of its WTO commitments, firstly, to ensure that such policy is compatible with the relevant WTO rules and regulations, and secondly, to determine the impact of e-commerce on these commitments. The e-commerce Work Programme currently underway in the WTO should inform the first step in this analytical process currently underway in the WTO.

CHALLENGES REGARDING THE USE OF THE INTERNET FOR E-COMMERCE TRANSACTIONS

In dealing with the issues around e-commerce MTS, the following concerns should be addressed:

- Market access for products conducive to e-commerce
- Issues linked to customs valuation; import licensing; rules of origin; technical barriers to trade and tariff concessions

Classification issues such as e-commerce transactions, for example, trade in goods, services.

5.2 STRUCTURE OF THE WTO

The WTO's top level decision-making body is the Ministerial Conference, which meets at least once every two years. Below this is the General Council (normally ambassadors and heads of delegations in Geneva, but sometimes officials sent from members' capitals) which meets several times a year in the Geneva headquarters. The General Council also meets as the Trade Policy Review Body and the Dispute Settlement Body. At the next level, the Goods Council, Services Council and Intellectual Property (TRIPS) Council report to the General Council. Numerous specialised committees, working groups and working parties deal with the individual agreements and other areas such as the environment, development, membership applications and regional trade agreements.

5.2.1 Fundamental principles underpinning the WTO agreements

Although some exceptions are allowed, two fundamental principles underpin all the WTO Agreements:

* **Most favoured nation principle** (MFN): a concession granted by one country to another must be extended to all other Member countries; and
* **National treatment**: countries should treat foreign nationals, products, services and intellectual property no different from their own, once they have entered their domestic markets.

5.2.2 E-commerce, regulatory issues and the WTO

At the second WTO Ministerial Conference in Geneva in 1998 Ministers adopted a Declaration on e-commerce which was twofold:

* that the General Council would establish a comprehensive work programme to examine all trade-related issues relating to global electronic commerce, taking into account the economic, financial and development needs of developing countries, and to report on the progress of the work programme, with any recommendations for action, to the Third Session; and
* that member countries would continue to refrain fom imposing customs duties on all electronic transmissions (commonly referred to as the "moratorium").

In September 1998 the General Council established a Work Programme on electronic commerce for the relevant WTO bodies, namely the Council for Trade in Services, the Council for Trade in Goods, the Council for TRIPS and the Committee for Trade and Development. An interim review of progress in the implementation of the Work Programme was conducted by the General Council in March 1999. The final Reports, including recommendations, of these four bodies were submitted to the General Council on 31 July 1999. Based on these Reports the General Council was supposed to have submitted recommendations for decision by Ministers at the Seattle Ministerial Conference which took place in December 1999. The two key aspects of such a decision would have been whether to abolish or extend the current moratorium on the levying of customs duties on electronic transmissions; and whether to extend the current Work Programme on e-commerce. In the Seattle Ministerial Conference, South Africa, together with the Southern African Development Community (SADC), supported the extension of the moratorium until the next Ministerial Conference when it would be reviewed.

However, the failure of the WTO Seattle Ministerial Conference to reach consensus on the launching of a new round of trade negotiations has resulted in a lapse on the way forward for the multilateral trading system. This has resulted in confusion and ambiguity as to the current status of the moratorium on the levying of customs duties on electronic transmissions. Member country proposals on the moratorium, in the run-up to Seattle, ranged from the US calling for a permanent ban on such duties, to some developing countries refusing to extend it altogether. In general, most countries seemed agreeable to a limited extension of the moratorium until the next Ministerial Conference when it will be reviewed.

The Reports on the e-commerce work programme submitted by the TRIPS Goods, and Services Councils to the General Council in July 1999 were inconclusive, and the general consensus was that the "educative process" should continue.

5.3 THE GOODS COUNCIL

The Goods Council is faced with the challenge of determining whether e-commerce means dealing with goods and services, or something altogether different. Agreement on such classification is important since it impacts on whether such trade is governed by the rules of GATT, General Agreement on Trade in Services (GATS) or a combination of the two. The classification issue is dependent on defining the products of e-commerce. Neither the term "*goods*", nor the term "*service"* is strictly defined in multilateral commercial agreements. Until the advent of the "digital world" the distinction between goods and services was fairly evident. However, innovations in communications and information technologies together with the birth of the Internet have seen this distinction becoming increasingly blurred in regard to certain products of electronic commerce. From a legal perspective, the application of the rules of GATT or GATS depends upon the definition of the products of e-commerce.

Where goods are ordered and paid for over the Internet, but physically delivered to the buyer, it is clear that the rules of GATT would apply. Merchandise and services can be bought, paid for and delivered via the digital medium. The most common examples are books, CDs, videos, software, financial services and distance education learning. When such transactions occur no physical or tangible goods are crossing borders, and this raises the question of whether the levying of customs duties are applicable in these circumstances.

5.4 THE SERVICES COUNCIL

Thus far there is general agreement on the following issues:

- That the electronic delivery of all services falls within the scope of GATS;
- Electronic delivery of services can take place under all 4 modes of supply. To explain, the GATS classify services according to the mode of delivery. There are four modes: cross-border supply (mode 1), consumption abroad (mode 2), commercial presence (mode 3), and the movement of natural persons (mode 4).
- that GATS is technologically neutral in that it draws no distinction between the different technological means through which a service may be delivered (e.g., in person, by mail, courier, or Internet);

- while recognising Members' rights to regulate domestically, governments should strive to ensure that such regulations do not become trading barriers themselves.

It should be not ed that GATS Article XIV provides for General Exceptions in which issues such as protection of privacy, public morals, and prevention of fraud could be accommodated. There is, however, a process mandated under Article VI.4 of GATS to develop disciplines for domestic regulation.

A contentious point that has emerged is the lack of clarity as to the distinction between services provided under Mode 1 and that of Mode 2. Assuming that electronic trade is subjected to the GATS discipline, it is certain that member countries will have great difficulty in differentiating between modes 1 and 2. There are no clear-cut objective criteria that can be brought to bear on this classification. Therefore, it is likely to be negotiated as part of the next round of negotiations. The choice of classification has two principal implications.

Firstly, the classification will determine the liberalising impact of the commitments made in the UR and post-UR GATS negotiations on services. During these negotiations countries made commitments based on the modes of supply of services. Consequently, the impact of these commitments will, to a large degree, depend on whether electronic trade is classified as being supply by mode 1 or mode 2. For example, if a country gave full market access under mode 2 for a particular financial service that is traded electronically, the commitment would have no liberalising impact if e commerce is classified as supply under mode 1 rather than2. It is therefore obvious that the liberalising impact of previous commitments will depend on the mode of supply under which e-commerce is classified.

From the schedules of commitments it would seem that countries undertook more obligations for liberalisation under mode 2 than under mode 1. Accordingly, the liberalising impact of the commitments will be greater if e-commerce is classified under mode 2. It would appear that developed countries would be the greatest beneficiaries since they are net exporters of electronic services, and would enjoy increased market access if these services are classified under mode 2.

Secondly, the classification will determine jurisdictional issues for purposes of regulation and dispute settlement. In terms of current international law, for supply under mode 1, the transaction is considered to have occurred in the country where the buyer resides. The regulatory regime of the importing country is then applicable to the transaction. Conversely, under mode 2, the law of the country of residence of the supplier is applicable. Countries are therefore likely to opt for mode 1 if they are of the view that they need to protect their buyers' interests. It seems evident that some tension will be inherent in the choice of classification depending on the objective. The market accesses objective favours mode 2 whereas the consumer protection objective tends towards mode1. In making their liberalisation commitments in the UR and post-UR negotiations countries, in general, considered electronic transactions between suppliers and recipients in different countries as cross-border transactions. It would therefore seem prudent to treat them as such since an alternative interpretation may yield unintended liberalisation effects.

There is a further complicating factor regarding the classification of e commerce under GATS. Although there appears to be an emerging consensus in the WTO that all e-commerce transactions are covered by the provisions of GATS, irrespective of the medium of delivery, there still remains some important issues that are yet unresolved. Currently, most products that are delivered electronically, like telecommunications and financial services, are covered in the services classification lists. However, will this cover all existing services and all digital transactions? There is as yet no compulsory or universally agreed classification system for existing services. Generally, the coding system used is that based on the provisional Central Products Classification (CPC) of the United Nations, although it is not fully comprehensive since it is not used in a number of sectors, including financial services, telecommunications, air transport and maritime transport. Further, the CPC was last issued in 1989 which makes it highly likely that current technological developments and delivery options could not have been foreseen. The concept of "technological neutrality" could also prove problematic since even in cases of CPC the description may not be technologically neutral in that it may describe means of delivery without accounting for electronic means. Since this classification does not apply across the board (especially to new services that have emerged or may emerge) it is common practice to adopt the category of "other services". Such classification is both arbitrary and questionable.

For discussion of intellectual property matters, refer to the section on **Intellectual Property**

5.5 DECLARATION ON TRADE IN INFORMATION TECHNOLOGY

At the Singapore Ministerial Declaration on Trade in Information Technology Products (ITA) was concluded at the Singapore Ministerial Conference in December 1996. At that time 29 Member countries signed the Agreement. Since then many other countries have joined the ITA. The ITA requires all participating countries to reduce tariffs to zero on a range of IT products, which are stipulated in the Declaration, by 1 January 2000. Some of the products covered are semi-conductors, telecommunication products, scientific instruments, computer software and semi-conductor manufacturing equipment.

It is evident that most of the hardware and software necessary for the conduct of e-commerce is covered by the ITA, although talks have begun in the WTO to expand its product coverage even further. South Africa is not a signatory to the ITA, but perhaps an analysis should be done as to whether it is in our interests to remain outside of it. This should not in any way be interpreted as advocating that SA should join, but should rather be seen as an observation that the technological and economic milieu of the global economy has changed markedly since the ITA was completed in 1996, and that in the light of this, alternative strategies should possibly be explored.

5.6 Trade and Development Committee

This Committee has been primarily concerned with the potential of e commerce to promote economic growth and development in developing countries; in other words, the development dimension of e-commerce. There has been a general acknowledgement that the development perspective should serve as a point of departure for a multilateral debate on e-commerce. Although not a solution to all the trade problems facing developing countries, e-commerce could enhance growth and development by increasing the efficiency of economic activities and promoting a balanced development of the global economy. However, such benefits would remain beyond the reach of developing countries if they do not possess the necessary infrastructure, which makes e-commerce possible.

Developing countries can play a vital role in promoting the growth of e-commerce within and among themselves by instituting appropriate educational, industrial, technological and economic policies. Nevertheless, developed countries and multilateral organisations such as the WTO, ITU, UNCTAD, World Bank and WIPO should ensure that they provide sufficient technical assistance and human resource development programmes to enable developing countries to make the transition from “traditional” to “information” societies. This is essential if the benefits of e-commerce are to be universal. Anything less will result in continuing growth of the gap between rich and poor countries and the continuing deprivation of billions of people of the so-called technological wonders of the twenty first century.

Electronic commerce should not be viewed as a sector of economic activity, but rather be seen as an instrument that can aid developing countries in the fight against economic marginalisation. SA has stated its commitment to poverty alleviation worldwide, especially within Africa. As the most needy continent, the challenge of development in Africa is the most daunting. As a member of SADC, SA is committed to promoting economic growth and development in the region, since SADC constitutes an important market for SA goods and services. Promoting the development of telecommunications infrastructure and ICT networks in SADC and throughout Africa is therefore considered a priority. Such development, however, will require substantial levels of direct foreign investment which will only translate into development if it includes the necessary transfer of technical and managerial skills, as well as the development of local industrial and commercial enterprises. A key challenge facing SA, and developing countries in general, is the development of programmes to leverage such foreign investment into the telecommunications sector.

QUESTIONS FOR POLICY CONSIDERATION

1. *What is the current impact of the moratorium* on the levying of customs duties on electronic transmissions *on the South African customs revenue, and on SACU customs revenue?*
2. *What approach should SA adopt in positioning the country and other developing countries in the debate within the WTO, and how should the views of business, labour, NGOs and civil society be articulated in such a discussion?*
3. *Should SA consider joining the ITA and what would be the consequences of such a move, and how would this compare with the status quo?*
4. *Is there a need of domestic regulation of e-commerce?*
5. *The fact that many services can now be delivered electronically has implications for most countries' services commitments since many of these commitments were made without consideration of electronic delivery of such services. What is the potential impact of this on SA's commitments?*
6. *What are the potential consequences of SA's services commitments if e-commerce is classified as either* ***mode 1*** *(cross border supply) or* ***mode 2*** *(consumption abroad)?*
7. *In view of the fact that there are increasing calls that Internet Service Providers (ISPs) be scheduled as separate service providers in GATS commitments, what should SA's approach be, considering Telkom's current monopoly?*
8. *How can SA further strengthen the development dimension in the deliberations of the Committee on Trade and Development?*
9. *How can SA, as Chair of the NAM and as a member of other multilateral and regional organisations such as G77 & China, the OAU and SADC use its influence to advance the technological development of the South?*
10. *As the technological powerhouse of Africa, what role can SA play in promoting the growth of e-commerce in SADC and the rest of Africa?*

6. INTELLECTUAL PROPERTY RIGHTS AND E-COMMERCE

6.1 INTRODUCTION

Intellectual property rights are legal means to protect and balance the interests of an individual against those of the public. This is done in terms of disclosure, dissemination, alteration, use and abuse of ideas, with an exclusive right to control and profit from invention and/or authorship of such intangible goods, services and ideas. The World Intellectual Property Organisation (WIPO) classifies intellectual property into two categories, namely, industrial property, such as inventions, trademarks, industrial designs and appellations of origin and copyright literature that refers to items such as musical, artistic, photographic and audio-visual works.

It has become relatively easier to infringe intellectual property through the use of electronic technologies. Therefore there is an urgent need to formulate a system of laws that define and protect intellectual property as a response to technological change, particularly emerging circumvention technologies that are constantly defying copyrights on electronic systems. In this context, it becomes increasingly challenging to ensure intellectual property rights and related neighbouring rights are applied to the electronic environment in a manner that is promoting e-commerce.

6.2 CHALLENGES AROUND THE PROTECTION OF INTELLECTUAL PROPERTY RIGHTS

Some of the problems around the adaptation, protection and enforcement of intellectual property rights in e-commerce are:

- There could be excessive regulations limiting or discouraging the generation, use and sharing of ideas
- Difficulty in distinguishing between the original owner of intellectual property and the host or custodian of such property in an electronic environment
- The availability of free, unsolicited, and cheap electronic goods and services online
- Availability of inexpensive (sometimes free), sophisticated and innovative methods for reproduction and distribution often referred to as circumventing technologies including duplicating devices of intellectual property.
- Absence of adequate legislation relating to the protection of indigenous South African intellectual property.
- Limited presence in South Africa of adequate capacity, instruments and mechanisms to monitor and protect intellectual property rights
- The ever changing technological innovations relating to the use of Internet for commercial transactions

- The dominance of developed countries in the creation of Intellectual Property
- The global nature of e-commerce, the Internet transcending boarders, juxtaposed to traditionally local or territorial nature of intellectual property laws
- Inadequate legal framework to regulate rights and responsibilities for and on behalf of Internet Service Providers in terms of liability.

6.3 LOCAL CONTEXT

South African intellectual property law is not fully equipped to deal with the implications of the internet, convergence, multimedia, digital technology and hence ecommerce. The advent of the Internet has changed the underlying assumptions of the original copyright laws entailed in the Copyrights Act 98 of 1978. The Trade Marks Act no. 194 of 1993 provides for instances under which trademarks cannot be infringed, yet domain naming has created a loop-hole in the Act, i.e. Trademarks Vs domain names (discussed in detail later).

For South African laws to comply with the Agreement on Trade-Related Aspects of Intellectual Property (TRIPs), which forms part of the package of agreements and instruments establishing the World Trade Organisation (WTO), intellectual property statutes were amended by the Intellectual Property Laws Amendment Act (Act 38 of 1997).

Although it is believed that the amendments adequately provide for and accommodate e-commerce, certain changes are envisaged in the near future to ensure full compliance and to meet new demands and realities of e-commerce. The changes largely revolve around terminology and scope of definition of some words and clauses of the act. Most words do not accommodate electronic versions of goods and services.

The application of traditional copyright law to open, public, global networks such as the Internet is hindered by the fact, that traditional protection of intellectual property rights has always specifically referred to the protection of information contained in tangible media such as books. Therefore convergence of traditional forms of communication into a single electronic environment presents challenges in the attempt to amend the Act and accommodate this new environment.

Thus it is crucial for South African intellectual property law to keep abreast of technological development and for the South African Parliament to enact legislation that conforms with innovation.

6.4 INTERNATIONAL CONTEXT

Debates relating to intellectual property rights are ongoing in international forums such as the World Intellectual Property Organisation, the World Trade Organisation, the European Union and the Organisation for Economic Co-operation and Development and the Internet Corporation for Assigned Names and Numbers, with the purpose of finding a suitable framework for intellectual property rights.

There is currently no sufficient international agreement on various issues fundamental to the protection of intellectual property rights in the electronic environment. To date multilateral and bilateral treaties prove to be the most feasible way to deal with trans-boarder intellectual property related issues. Traditionally, intellectual property rights are limited by territorial boundaries. The scope of the rights established in each country is determined by that country and the effect of those rights, as well as their protection, are, in principle, confined to the territory of the country. The trend is that the copyright law of the country, in which an act of infringement takes place, presides over the matter. However, the transnational nature of e-commerce suggests that several national laws could apply to a single act of transgression. This can create legal uncertainty that may unduly hamper the progress and the growth of e-commerce and the general flow of information, at the same time also facilitating resolutions of issues.

The TRIPS Agreement (The Agreement on Trade-Related Aspects of Intellectual Property) was adopted in 1994 to provide rules concerning trade-related intellectual property rights, basic principles of previous intellectual property conventions, standards regarding availability, scope, and use of intellectual property rights. Appropriate enforcement, multilateral dispute settlement procedures and transitional arrangements for countries are also included in the agreement. Administered by the WTO, the TRIPS Agreement is enforced through WTO consultative panels and dispute resolution mechanisms.

TRIPS basically covers copyrights and related rights such as the “rights of broadcasters, performers, producers, of sound recording and broadcasting organisations; industrial designs and patents including the protection of layout and design of integrated designs; undisclosed information including trade secrets and test data; trademarks and service marks. It also outlines the main elements and standards of protection to be provided by each member, the nature of the subject matter to be protected, the rights to be conferred and permissible exceptions those rights, as well as the duration of protection. It further outlines enforcement mechanisms on behalf of the standards and their protection. These include provision of civil and administrative procedures, criminal procedures, remedies, the procedures, remedies for such an environment and other dispute resolution mechanisms. Further, TRIPS also allows developing member countries with a grace period and autonomy to implement compliant necessary changes as recommended in the agreement.

The contribution of the Internet in the creation, production, and use of literary and artistic works, performances and phonograms, including its potential to undermine the basic tenets of copyright and related rights, has compelled the WIPO to lead the adoption of two treaties in December 1996, namely, the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT). These treaties are commonly referred to as the "Internet treaties". These treaties address issues of the definition and scope of rights in the electronic environment, and some of the challenges of online enforcement and licensing. Although South Africa has signed the WCT, it has not yet implemented this treaty.

The mandate of WIPO regarding intellectual property protection. To give impetus to the efforts to reach global consensus on the protection of intellectual property, WIPO has developed a "digital agenda" to pursue over the next two years, namely:

- Broaden the participation of developing countries through the use of WIPONET and other means for access to intellectual property information, participation in global policy formulation and opportunities to use their intellectual property assets in e-commerce.
- Bring into effect the WCT and the WPPT treaties before December 2001.
- Promote adjustment of the international legislative framework to facilitate e-commerce through the extension of the principles of the WPPT to audiovisual performances, the adaptation of broadcasters' rights to the digital era and progress toward a possible international instrument on the protection of databases.
- Implement the recommendations of the Report of the WIPO Domain Name Process and pursue the achievement of compatibility between identifiers in the real and virtual worlds through the establishment of rules for mutual respect and the elimination of contradictions between the domain name system and intellectual property rights.
- Develop appropriate principles with the aim of establishing, at the appropriate time at the international level, rules for determining the circumstances of intellectual property liability of Online Service Providers (OSPs) which are compatible and workable within a framework of general liability rules for OSPs.
- Promote adjustment of the institutional framework for facilitating the exploitation of intellectual property in the public interest in a global economy.

- Introduce and develop online procedures for the filing and administration of international applications for the PCT, the Madrid System and the Hague Agreement at the earliest possible date.
- Study and, where appropriate, respond in a timely and effective manner to the need for practical measures designed to improve the management of cultural and other digital assets at international level.
- Study any other emerging intellectual property issues related to electronic commerce and, where appropriate, develop norms in relation to such issues.
- Co-ordinate with other international organisations in the formulation of appropriate international positions on horizontal issues affecting Intellectual Protection, in particular the validity of electronic contracts and jurisdiction.
- On December 1999, the Department of Trade and Industry (DTI) consulted stakeholders with a view to accede to these Treaties. The majority of stakeholders cautioned that before acceding to them, South Africa should analyse the benefits which accrue to small and medium enterprises.

6.5 COPYRIGHT

Copyrights are referred to as the rights to ensure protection of information from duplication and distribution. Computers are changing the way that copyrighted goods can be illegally copied and distributed.

Violation of copyrights is difficult to monitor in the electronic environment, since content exists not physically but in electronic form and can be instantaneously distributed without even being copied. All of this occurs cheaply and easily. This creates new challenges for copyright owners and law enforcement agencies in that the distinction originally drawn between copying and distribution is blurred. The Intellectual Property Laws Amendment Act, 1997 introduced a number of amendments into the Copyrights Act in order to provide for digitised formats of copyrighted goods. A number of legal issues still need to be addressed. To highlight but a few: -

- The reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted thereunder, fully apply in the digital environment, in particular to the use of works in digital form. It is understood that the storage of a protected work in digital form in an electronic medium constitutes a reproduction within the meaning of Article 9 of the Berne Convention. At issue then is whether electronic reproduction is "reproduction" in terms of the South African copyright law, whether temporary storage is "reproduction", whether the copyrights owner can and should prohibit/authorise the digitisation of his/her copyright work, whether technology devices/measures to reproduce and or prevent unauthorised reproduction should be protected.

The WIPO Copyright Treaty responds to this fundamental change by requiring each country to specify that creators have the basic property right to control distribution of copies of their creations. The Treaty also requires each country to provide in its laws for a copyright owners exclusive right of making available its works to the public for on demand access. This makes it clear that the traditional property rights of copyright owners apply in cyberspace.

The Department of Trade and Industry proposed amendments to clarify issues of “fair deal” in the Copyright Act, 1993. The proposals will be tabled in Parliament soon.

The Copyright Act No.98 of 1978, recognises the notion of "fair use", which provides that copyright shall not be infringed by any fair dealing with certain works, such as copying for purposes of research or private study or personal or private use, etc. The Berne Convention noted that the "fair use" provisions in the context of digitised use should be approached just as they are in "traditional" environments. Commercial use, which harms actual or potential markets, will, therefore, probably constitute infringement, whereas non-profit educational transformative use will most probably often be deemed fair. Between these extremes the courts (or parliament) will have to determine what constitutes fair use?

QUESTIONS FOR POLICY CONSIDERATION

The following questions arise: -

1. *How should liability be determined in copyright infringements given intangibility and documents in transit?*
2. *What is the potential liability of end-users "reproducing" infringing copies (transient copies) of copyrighted works by the mere act of viewing them on their PC's, etc?*
3. *How do we strike a balance of enforcing and monitoring intellectual property rights with the need to promote use of ecommerce and cyberspace publishing?*
4. *Is framing (the incorporation of a website within a website) and hyperlinking (the creation of digital paths linking two or more websites) an infringement of copyright?*
5. *How are the expenses, efforts, duration and technical evidence demands for enforcing copyright protection in court going to be implemented?*
6. *What constitutes fair use of copyright material in an electronic environment?*

6.6 PATENTS

The process of patenting entails the registration and protection by law of new and innovative ideas that have industrial or commercial value. An invention can be defined to be a novel idea, which permitsin practice the solution of a specific problem in the field of technology. More formally WIPO defines a patent to be a document, issued by a government office, which describes the invention and creates a legal situation in which the patented invention can only be exploited (altered, used or sold) by, or with the authorisation of the patentee.

Lack of material objects is not the only problem for intellectual property rights owners, posed by the digitalisation of information. Information in digital form is much more easily manipulated and adapted than traditional forms of information and the changes are much harder to detect. Again historically patents are technical and territorial in nature. There is an increasing need to protect software, business practices, formulas, recipes etc. The scope of definition and the criterion in rendering a patent therefore have to be widened with emphasis on protection, monitoring and enforcement measures. This should apply on a local and a legally compatible and interoperable global basis. There is a need to implement a global integrated mechanism for the administration and issuing of patents to synchronise the growth, globally, of the knowledge based society.

Under the PCT system, the PCT-EASY software has been introduced, and the establishment of further legal and technical standards for electronic filing and processing of PCT applications is underway.

The Patent Law Treaty (PLT) which is designed to streamline and harmonize formal requirements set by national and regional patent offices for filing and processing of national and regional patent applications, the maintenance of patents and certain additional requirements related to patents and patents applications, including electronic filling (signatures and forms) of patents applications, has also been adopted by WIPO.

6.7 Trademarks

A trademark is a sign, or a combination of signs, capable of distinguishing goods and services of one undertaking to those of other undertakings. The sign may consist of one or more distinctive words, letters, numbers, drawings, pictures, emblems, colours or combination of colours. The emergence of a truly global electronic market place has created an increase in demand for brand-named consumer goods and, unfortunately a concomitant rise in illegal copying and reproduction of these goods.

Trademarks Act are an old practice of protecting the public from fraud and brand confusion; promoting the goodwill of business and facilitating product distinction and integrity in society.

The Trademarks Act no. 194 of 1993 sec. 34 and 35 presently provides for instances where trademark rights will be infringed, which generally revolves around the prevention of registration of already registered trademarks. The framework regarding the unauthorised use of trademarks in relation to goods and services in the traditional environment should hold for the virtual environment as well. Therefore the definition of a Mark as per Act should be amended to accommodate digitised marks. The scope of the Act should be enhanced to accommodate the digital, virtual and electronic environment

Trademarks are territorial in nature i.e. their registration applies to a particular country or jurisdiction. There is a general discrepancy between the national scope of trademark laws and the international nature of electronic commerce, particularly since e-commerce is borderless and instantaneous in nature. For example, different parties can register a trademark in different jurisdictions at almost the same time.

Provision has been made by article 6b of the Paris Convention for the protection of Industrial Property attempts to provide for the protection of "well known marks". This article provides for the prohibition and/or cancellation of use of a trademark, which institutes a reproduction, imitation, and translation or is likely to create confusion of a mark. However the shortcoming here is that the definition of "a well known mark" is relative and only goods are mentioned and not services and digitised products.

Another issue is of trademarks or "well-known marks" as domain names? Domain names are to be understood to be essentially addresses allocated to websites through which traders, vendors and virtual locations can be identified and located on the Internet. Currently there are no definite linkages between trademarks and domain names. This means that one can register a trademark as a domain name irrespective of whether the trademark belongs to one or not. Naturally this does not appeal to the original owner of the trademark, and unfortunately the Act does not provide any guidelines. However this still constitutes an infringement in that the uniqueness of the mark will no longer hold. This is called "Cybersquatting" as perpetrators do not register trademarks as domain names with the purpose of trading but rather with a purpose of selling the domain name to the original owner of the trademark. This issue definitely calls for immediate global and national attention. The issue of cybersquatting is even aggravated in instances where the trademark is not registered at the domicile or jurisdiction of the domain name.

It was very difficult to resolve these issues before WIPO Dispute Resolution were adopted by ICANN. Further, South Africa may encourage the litigants jointly or unilaterally, to submit a dispute to WIPO Dispute Resolution Panel.

It is uncertain to what extent the Trademarks Act No. 194 of 1993 would or should apply to domain names. Section 34(1)(a) of the Act protects the proprietor of a registered trade mark from the unauthorised use, in the course of trade, in relation to goods or services for which the mark is registered, of an identical mark or a mark so nearly resembling it as to be likely to deceive or cause confusion. Section 34(1)(b) provides a similar protection with relation to a mark used on or in relation to similar goods or services. Section 34(1)(c), that deals with "dilution" of a trade mark, provides that unauthorised use of a registered mark which is identical or similar to a mark which is also well-known in South Africa would amount to infringement, if such use is likely to take unfair advantage of, or be unfairly prejudicial to its distinctive character or repute (it is not necessary to prove deception or confusion). The same principle applies to the dilution of well-known "foreign marks", even if the foreign mark is not registered in South Africa (Section 35).

Under the Business Names Act No. 27 of 1960, sections 4 and 5 of the Act, the Registrar of Companies has the power to prohibit the use of certain forms of domain names to the extent that no person may carry on any business under any name, title or description which includes the words "government" or any other words, or any *abbreviation* (e.g. gov). In terms of the Act, the Registrar of Companies, it is submitted, may have concurrent jurisdiction with any body or organisation administering domain names to the extent that the Registrar may order the removal of such names or description used as domain names.

QUESTIONS FOR POLICY CONSIDERATION

1. *Who should hold the rights of a trademark registered in different jurisdictions by different parties almost at the same time? What is the basis of determining this?*
2. *Does there appear to be shortcomings in terms of the Trade Marks Act of 1993 in terms of addressing the digital or electronic environment? If yes what are those shortcomings and what are the kind of amendments that need to be implemented?*
3. *Should there be a linkage of administration between trademark registry and the domain name registry to prevent cybersquatting?*
4. *How can SA utilise digital technology to promote protection of local indigenous knowledge?*
5. *What are the implications of these treaties for SA in terms of its capacity for monitoring and enforcing violations of the intellectual property rights protected by these treaties?*

6. *What proposals can SA make in the upcoming TRIPS review to ensure that the development dimension is entrenched in the TRIPS Agreement?*
7. *Does South Africa's intellectual property law address the challenges posed by e-commerce?*

7. BUILDING TRUST IN THE ELECTRONIC ECONOMY

7.1 INTRODUCTION

The growth and development of electronic commerce relies primarily on building the confidence of the consumer, business and government in the e-commerce environment. Transmission of information over the Internet for the purpose of trading and communication presents new and sophisticated forms of threat for both the sender and the recipient of information.

One of the main differences between e-commerce and traditional commerce is that electronic transactions are largely impersonal, anonymous. Business and consumers require assurance that transactions that occur in an online environment are secure and private.

Security measures used in conventional commerce may not be adequate to provide trust in the electronic economy. For example, in a non-electronic or traditional environment, information is held in files securely locked in cupboards, or even in wall safes, depending on the sensitivity of information. The electronic world provides for the same information to be widely accessible via various media. Therefore it is crucial to ensure that information to those for whom it is intended, access information, and instruments that will ensure verification of parties to a transaction are available

To ensure transaction security, the following elements are necessary:

Authentication: securing the identities of the parties to a transaction
Confidentiality - ensuring that the information is kept private
Integrity – ensuring that that information or process has not been modified or corrupted without detection
Non-repudiation: ensuring neither party can refute that the transaction occurred, i.e. ensures that the transaction is binding.

Legal, procedural and technical means to ensure the security of data is important to allow ecommerce to reach its full potential. For instance, admissibility of electronic signatures in a court of law could further enhance the confidence in e-commerce transaction.

The role of government should be to legislate or regulate if necessary and issue licenses where appropriate to encourage user trust; that of the private sector would be to introduce voluntary codes and develop technological solutions. This requires active partnership between government and the private sector.

This chapter will therefore focus on security and related issues, which include public key infrastructure, public key cryptography, digital certificates, electronic signatures, privacy and lawful access to encrypted data.

7.2 PUBLIC KEY INFRASTRUCTURE

What is a Public Key Infrastructure?

A public key infrastructure (PKI) makes it possible for you to identify and trust another Internet user, which can be another person, a computer or other hand-held devices and/or some other electronic entity. In a PKI, digital identification, called digital certificate is used to prove the identity of Internet users. This certificate can also be used to verify a digital signature, which can be attached to e-mail. The signature itself is created using public key cryptography.

PKI provides confidentiality; integrity; authentication and non-repudiation. The goal of a PKI is to establish and maintain a trustworthy networking environment by providing keys and certificate management services that enable encryption and electronic signature capabilities across applications.

7.2.1 What is Public Key Cryptography?

Public Key Cryptography is essentially a method of keeping data secure and protected by applying a mathematical formula to obscure the information being transmitted. In cryptography, this mathematical formula or a value is used to transform information into a form that is unreadable (i.e. encrypted). The information can only be transformed back into a readable form (i.e. decrypted) using a complementary algorithm and a second related value. These values are called public keys. One key is made publicly available (public key) while another is kept secret (private key). Public keys are usually embedded in digital certificates. By embedding the public key value in a digital certificate, the identity of the person, computer or entity identified in the digital certificate can be strongly associated with the public key value.

Digital signatures are one of the primary ways public key cryptography can be used to make Internet communication safer. To create a digital signature for e-mail, for example, a copy of the communication is encrypted using a private key. This encrypted information is called digital signature – digitally signed message. The digitally signed message is sent along with sender's digital certificate to another person. The digitally signed message (or digital signature) can only be decrypted and verified using public key embedded in the sender's digital certificate. A digital signature can therefore be used to identify a person or a computer or a hand-held device. It can also be used to ensure that a message or file has not been tampered with.

While cryptography has many benefits, these same technologies can be used to hide trans-border criminal activities and threaten national security. Therefore rules are required to govern the use and sale of cryptographic materials.

General guiding principles on the use of cryptographic methods

OECD recommends a less restrictive approach in the development and use of cryptography, as recommended in the summary of its guidelines:

* Users should have a right to choose any cryptographic method, subject to applicable law
* Cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments
* Technical standards, criteria and protocols should be developed and promulgated at the national and international level
* The fundamental rights of individuals to privacy, including secrecy of communication and protection of personal data, should be respected in national cryptography policies and in the implementation of cryptographic methods
* National cryptography policies should allow lawful access to plain text, or cryptographic keys of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible
* Whether established by contract or legislation, the liability of individuals or entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated
* Governments should co-operate to co-ordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade

The adoption of the above principles does not imply a complete denial of the need of government involvement, through regulation or otherwise. For instance, although technical standards are currently being developed by international standards setting bodies, the Government should foster compliance with such international standards. Accepting local or proprietary standards may well lead to South Africa being cut off from the global e-commerce market.

QUESTIONS FOR POLICY CONSIDERATION

South Africa has to consider its stance with regard to promoting the benefits of increased data security and to ensuring that law enforcement agencies will be able to investigate criminal and other illicit transmissions. These deliberations must take into account the various policies of other countries and the role that South Africa wishes to play in promoting uniform standards internationally. Key questions relating to the above are as follows:

1. *To what extent do existing laws impact on the development, use and sale of cryptographic materials?*
2. *Should South Africa adopt specific policies and legislation now to encourage and/or restrict the use of encryption in commercial data transmissions or should South Africa wait and take cue from what is being formulated by other countries?*
3. *To encourage greater public confidence in ecommerce, should the South African government officially endorse certain cryptographic methods, or TTP/CA institutions?*
4. *What restrictions, if any, should be placed on the use and sophistication of cryptography in domestic businesses' electronic transactions?*
5. *Should government law enforcement agencies have access to public keys to private cryptographic technology? What rules should apply and which institutions should be involved?*
6. *How should South Africa participate in international deliberations and agreements toward common standards for cross-border data security and access, or should South Africa have its own local/proprietary standards?*
7. *To what extent should the state be involved in the control and interoperability of encrypted material?*
8. *Should there be control of the production sale (both export and import) and use of encrypted material?*
9. *Should South Africa adopt the above-mentioned OECD guideline as an international benchmark?*
10. *Are there unique South African circumstances that will need special mention or a different set of guidelines from those of the OECD?*

7.3 WHAT IS A CERTIFICATION AUTHORITY?

A Certification Authority (CA) is a trusted third party that is responsible for creating, distributing, and revoking digital certificates. A CA issues digital certificates to link digital signatures to particular individuals or business functions. A process of binding a public key value to a person, computer, or entity is called certification. CA also responds to queries about the validity of certificates that they have issued. CAs revoke certificates when information in the certificate becomes unexpectedly invalid. CAs can be either commercial and/or governmental.

One of the main policy debate surrounding private sector CAs is whether they should require formal licensing by government or whether self regulation without official endorsement should be allowed. In view of the potential importance of CA activities and the potential liability questions that could arise, public licensing may be necessary. A licensing regime would obviously offer strong re-assurance to the public that licensed CA is reliable and responsible. The opposing view contends that the hierarchy of licensing government certification and industry CAs could stifle e-commerce development.

QUESTIONS FOR POLICY CONSIDERATION

It is recommended that a voluntary but statutory framework for the licensing scheme be introduced. This would build consumer confidence in that their interests are well looked after. The benefit of a voluntary scheme is that the decision on whether or not to rely on a statutory scheme is left to the end user. For example, where trust already exists between the parties to a transaction, there may be less need for 'trust' in the service provider. Users of approved service providers would also benefit from the assurance that their electronic signatures would likely be given legal effect throughout the country.

1. Is the above recommendation viable?
2. If South Africa intends establishing certification and public key infrastructure policies, there are several options and questions that will need to be addressed, among them:
3. *Where CAs are to be licensed, will it be necessary to define general policies or guidelines applicable to CAs and to appoint an official agency to issue licenses and monitor compliance with the policy standards?*
4. *What should be the general policies or guidelines governing CAs?*
5. *What architecture should a South African PKI/CA have? The following are the options for consideration: establishment of a Root (level 0) Government Certification Authority, which would certify the public keys of level 1 CAs in individual government departments. The Root Government CA might cross-certify root CAs in private industry sectors. Establish public/private forum type CA with a joint board.*
6. *Should legislation be passed to require mandatory, or at least voluntary, licensing of industry CAs and what structure should the licensing regime take?*
7. *Which agencies should be responsible for establishing policy (the role of the policy approval authority) and for managing and implementing the licensing (the role of the policy management authority)?*

8. *What should be the obligations and responsibilities, and the potential liability, of publicly licensed CAs with regard to electronic transactions, electronic signatures, and cryptography?*
9. *Should the UN and EU standards apply to the makeup and operations of licensed CAs?*
10. *What organisations can be licensed to be CAs? Will unlicensed CAs be allowed to offer services?*
11. *What distinctions need to be made between certification authorities and other forms of trusted third parties?*
12. *To what extent should South African policy draw on and be reconciled with emerging international standards for certification and the potential for multiple competing certification authorities and certification procedures, applying to transactions across international boundaries?*

7.4 LEGAL ISSUES PERTAINING TO PRIVACY OF COMMUNICATIONS

Public safety, crime control, national intelligence agencies and regulatory requirements all require effective and timely gathering of accurate information and evidence about activities of criminal elements. The effectiveness of these agencies in monitoring criminal activities, investigating and prosecuting offenders often depend on their ability to conduct electronic surveillance of communications and to search or inspect places including computers for relevant information. There is also a concern that key recovery or weak encryption gives government too much power and technical capacity to engage in mass surveillance.

Therefore, while there are legitimate reasons of providing lawful state access to encrypted information, implementation of such a practice raises human rights concerns mainly with respect to privacy and freedom of expression. Cryptography policy must be assessed against costs and benefits in terms of basic human rights, commercial interest, public security and crime prevention. As in many democratic countries, the rights of privacy and freedom of expression of all South Africans are constitutionally protected through the Bill of Rights.

Privacy rights seek to prohibit the state from decrypting data without some compelling justification, on the other hand, the right to freedom of expression extends to both the production of cryptographic product and their use to protect the messages that are being expressed or data being stored. These guarantees are important but not absolute in that privacy invasion, seizure of data, or interception of communication must be justified and authorized by a judge.

7.4.1 CURRENT SITUATION IN SOUTH AFRICA

In South African law the individual's right to privacy and information is enshrined in the constitution. Section 14 (d) of the constitution provides for the protection of the privacy of the individual with regard to communication. However, Section 36 limits certain privacy rights where 'reasonable and justifiable'

Section 32 of the constitution provides for the individuals right to 'access to information' The Promotion of Access to Information Act of 2000 has enacted to give effect to the right stipulated by section 32.

QUESTIONS FOR POLICY CONSIDERATION

1. *Is the current privacy regime adequate to address privacy challenges imposed by the electronic environment?*
2. *To what extent does the Interception and Monitoring Prohibition Act (N0 127 of 1992) address issues of privacy in the electronic environment?*
3. *What technical standards, criteria, and protocols should be developed and promulgated at national and international level to deal with issues of privacy?*

7.5 CYBER CRIME AND LAWFUL STATE ACCESS TO ENCRYPTED DATA.

While the internet age has brought with it opportunities and challenges for both business and consumers, it has also generated new forms of criminal activities, improved methods of committing crimes, and new ways to conceal evidence.

"Cybercrimes" are illegal acts, the commission of which involves the use of an electronic system, networks, technologies and devices such as the telephone, microwave and satellite.

Where a computer is involved, it could be the object of a crime, an instrument used to commit a crime or a repository of evidence related to a crime**.** The first example is when a hacker tries to steal information from or damage, a computer or computer network. The second, is when the computer replaces the telephone as a tool in an illegal telemarketing operation or simply to transmit child pornography. Last, is when the computer is used to store records of illegal schemes such as money laundering schemes or drug trafficking transactions?

Therefore restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against such criminal attacks. It would not however totally prevent criminals from using these technologies. Most countries in the world have no restrictions on the use of cryptography, which maybe freely used, manufactured, and sold without restriction. This is the international trend on cryptography, which puts emphasis on the liberalisation of controls on cryptography, and the development of market based, user driven cryptography products and services.

However this poses a problem for law enforcement agencies in their quest to monitor electronic crimes. In South Africa, the Working Group on Security and Privacy has therefore recommended that:

- Legislation, if necessary, be passed to compel any party holding the keys to such communications or data to provide, under a suitable judicial warrant, those communications or data in a format intelligible to the investigator. Failure to do so should then be made a criminal offence. Interception may only be authorized where this is judged necessary in the interests of national security and /or for the detecting serious crime
- No legislation be adopted that incorporates compulsory key escrow or key recovery, on the grounds of increased costs, increased vulnerability of security, and inability to enforce the applicable law.

It is possible that local law enforcement agencies already have the rights envisaged under the above recommendation, provided that the existing laws on search and seizure are suitably widely interpreted, to allow for the "intangible" nature of electronic communications and data.

In South Africa, a working committee for the South African Law Commission after reviewing the Interception and Monitoring Prohibition Act (No. 127 of 1992) and comparing it with the legal position of EU, Canada, Hong Kong and the United States; have recommended that the Act be amended to protect the consumer and the State from criminal activities through proper definition of words and clauses that may have ambiguity. The UK has adopted a similar position according to its Draft Regulatory Impact Assessment of the Draft Electronic Communications Bill (DTI, July 1999).

- Legitimate users of cryptography will, recognising the need to protect their data, and hence to protect their keys against accidental loss, make use of trusted Cryptographic Service Providers to archive keys. For that matter, even criminals making use of encryption will probably see a necessity for keeping back-up copies of their cryptographic keys. It is therefore also recommended that the government investigate whether there is a need to create a criminal offence of *"Unlawful use of encryption to obstruct justice", as was done in a U.S. Senate Bill of 1996.*

QUESTIONS FOR POLICY CONSIDERATION

1. *Should the use of cryptography be regulated?*

   The following are ***possible options*** *aimed at addressing the use of cryptography:*

   * ***Weak cryptography****: Under this scenario users with some exception would only be allowed to use cryptographic systems that can be broken by law enforcement agency in actual time*
   * ***Key escrow****: In this case government agencies hold the users decryption keys. Under the court order the trustees holding the keys would be required to relinquish the keys. Key escrow raise a number of practical and complex questions on particular issues of privacy, vulnerability, effectiveness and costs*
   * ***Direct access to session keys****: This is the simplest strategy to employ: under a suitable court order the user, the user or his CA or the other Trusted Third Party would be required to relinquish the key. Whether established by contract or legislation, the liability of individual or entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated.*
   * ***Flexible approach****: The user has the right to use any cryptographic method, as long as it is within the realms of applicable law.*

1. *Is it entirely possible to use the traditional statutory tools to prosecute an offender who has committed an Internet crime, if not what changes should be made to the legal system to accommodate such a crime?*
2. *In all crimes, including cyber crimes, the defendant's guilt must be proven beyond reasonable doubt, but global networks lack effective identification mechanisms for individuals. How can society put in place law that circumvents such a problem?*
3. *Should the issue of cybercrime (including viruses and hacking) be dealt with at the same time as general e-commerce legislation, or should the latter be dealt with first in order to hasten the process (as was decided during the UK e -commerce initiative)?*
4. *What types of international agreement should South Africa pursue to ensure that cyberfraud and similar practices could be policed on a worldwide basis, through co-operative investigation and prosecution?*

8. CONSUMER PROTECTION

8.1 INTRODUCTION

The electronic market place offers consumers unprecedented choice and twenty-four hours accessibility and convenience. It gives established marketers and new entrepreneurs low-cost access to a virtually unlimited customer base. With these benefits also comes the challenge of ensuring that the virtual marketplace is a safe and secure one to purchase goods, services and access electronic information. Consumers must be confident that the goods and services offered online are fairly represented and that the merchants with whom they are dealing (many of whom may be located in another part of the world), will deliver their goods in a timely manner and are not engaged in illegal business practices such as fraud or deception.

Consumers must be protected against the following dangers:

- Unsolicited goods and communication;
- Illegal or harmful goods, services and content (e.g. pornographic material)
- Dangers resulting from the ease and convenience of buying on-line;
- Insufficient information about goods or about their supplier; since, the buyer is not in a position to physically examine the goods offered;
- The abundantly accessible nature of a website;
- The dangers of invasion of privacy, as discussed in the section below.
- The risk of being deprived of protection through the unfamiliar, inadequate or conflicting law of a foreign country being applicable to the contract.
- Cyber fraud

On the other hand, suppliers are in some danger themselves, through exposing themselves to unknown liabilities, especially in view of the fact that the law on Internet commerce is as yet poorly defined, and differs from country to country.

Consumer confidence also requires that consumers have access to fair and effective redresses if they are not satisfied with some aspects of the transaction. To ensure strong and effective consumer protection in an online environment and obviate the need for a long and arduous litigation process, alternative and easy-to-use mechanisms for consumer dispute resolution, redress and enforcement mechanisms are required. Again beyond enforcing current law and developing strong consumer protection policies, consumers must be made aware of the availability of instruments to help them use Internet safely.

8.2 INTERNATIONAL SITUATION

Any consumer, regardless of whether he or she is a South African or a foreigner, who accesses a commercial website, should feel comfortable dealing with any South African supplier of goods or services. While the physical location of such a supplier may be hard to determine, it is deemed to be an essential feature of any fair distance selling that the supplier provide such a physical address. This presents South African business with an opportunity to establish a reputation for sound e-commercial practices, not only locally or within the SADC but also worldwide.

Provisions of the European Directive on distance contracts. The EU Directive applies to any "distance contract", i.e. to any contract regarding goods or services which is concluded at a distance. This includes traditional forms of business such as mail orders and the supply of financial services. The salient features of the EU provisions are as follows:

1. **Prior Information:** The supplier must provide, in a clear and comprehensible manner, the consumer with his identity, including his physical address; the main characteristics of the goods or services; the price including all relevant taxes; the costs of delivery; the arrangements for payment and delivery or performance; the existence of a right of withdrawal and the period of time for which the offer remains valid.
2. **Written confirmation**: At the latest at the time of delivery, the consumer must be informed, "in writing or on another durable medium", of the conditions and procedures for exercising the right of withdrawal; the geographical address to which the consumer may address any complaints; information on after sales service, and guarantees and the conditions applicable to cancellation of the contract.
3. **Right of Withdrawal**: The main provision is that the consumer can withdraw from the contract, without giving any reason, within the first seven days of conclusion of the contract.
4. **Performance**: Unless otherwise agreed, the supplier must honour his side of the contract within thirty days.
5. **Indemnity:** The consumer may not be held liable in the case of fraudulent use of his or her card.
6. **Inertia selling:** Supplying unsolicited goods and assuming that the absence of a response signifies consent is prohibited.
7. **Communication means**: Some means of communication, such as automatic calling machines and fax machines, may only be used if the consumer has given prior permission.
8. **Judicial or administrative redress**: Among the various requirements under this heading is Article 11 3(a) which reads thus: "Member States may stipulate that the burden of proof concerning the existence of prior

information, written confirmation, compliance with time limits or consumer consent can be placed on the supplier."

9. **Binding nature**: "The consumer may not waive the rights conferred on him.

Consumer protection principles in Australia. EU principles may be compared with those proposed by the Australian National Advisory Council on Consumer Affairs (NACCA). These are as follows:

1. Consumers using electronic commerce are entitled to at least the same levels of protection as provided by the laws and practices that apply to existing forms of commerce.
2. Consumers should be able to establish the identity and location of businesses with which they deal.
3. Consumers should have readily available clear and comprehensive information before and after any purchase of goods and/or services.
4. Sellers must state contract terms in clear, simple language.
5. Sellers should ensure they received confirmed meaningful consent from consumers for a purchase of goods and/or services.
6. Consumers are entitled to receive clear information about the types of payments, which will be accepted by the merchant or the payment provider.
7. Consumers are entitled to have their complaints and inquiries dealt with fairly and effectively.
8. Sellers should provide information to consumers about affordable and effective dispute resolution arrangements, where they are available.
9. Sellers must respect customer privacy.
10. Industry code administration bodies must closely monitor the application and effectiveness of their codes and be able to correct any deficiencies, which are identified.
11. Each code operating body should strive to maintain and promote consumer confidence in the global marketplace.
12. Governments should actively develop their consumer protection responsibilities.

In line with international standards, South Africa should consider developing adequate measures for consumer protection, which include the following:

1. Legislation on consumer rights needs to be reviewed, to ensure that this adequately applies to e-commerce, and where necessary that the relevant definitions are widened;
2. The creation by industry of Codes of Practice must be encouraged; industry needs to be cognisant of generally accepted principles such as those of the EU Directive and of NACCA, and possible other examples.
3. Industry should be encouraged to institute "Seal of Approval" programs.

4. Industry and Government should collaborate on educating consumers on their rights and on the meaning of the “Seals of Approval”.
5. Only if the above measures are seen to fail in their purpose, should additional legislation be considered.

Awareness. At the same time e-communications and e-commerce must be seen as providing new opportunities for small, medium and micro enterprises. As part of its educational activities, the Government should, (recognising the vulnerabilities of possible new and inexperienced entrepreneurs), make them aware of their responsibilities and liabilities. These responsibilities include, apart from the matters touched upon above, such matters as checking and confirming incoming e-mail; confirming orders; checking links to and from their Website, and maintaining control over their own content as well as over that of sites to which they are linked, and if necessary disclaiming links.

QUESTIONS FOR POLICY CONSIDERATIONS

1. *How should South Africa embrace these principles in its consumer protection laws or legislation?*
2. *Are these guidelines adequate? If not what else needs to be added?*
3. *To what extent should law regulate consumer protection, and to what extent can commerce be trusted to regulate itself?*
4. *What new or amended consumer laws and regulations need to be established or adopted to re-inforce the rights of the public in the context of e-commerce?*
5. *How can the role of the existing consumer protection bodies be enhanced to effectively accommodate electronic communications and commerce?*
6. *Should there be new bodies established particularly to generate awareness.*
7. *How should current bodies be enhanced to deal with consumer issues and e-commerce.*

8.3 PROTECTION OF PRIVACY AND PERSONAL INFORMATION

Privacy can be generally defined as the right to be left alone, free from intrusion or interruption. Privacy or the lack thereof, is a major concern for individuals in the use of the electronic medium in commerce. This includes not only the privacy of the communication between the parties in a transaction e.g. the protection of credit and debit card numbers while traversing the Internet, or of other personal details, which can be solved through the use of encryption; but also the accumulation of personal data at Websites visited, for example through the use of “cookies” or the introduction of Customer Relationship Management Tools (CRMs). In the nature of any distance-contract, the supplying party must collect a certain amount of personal information, even if this is only the name and address, and the credit card number, of the buyer. However, it is possible, as noted in the document "*Privacy Online: A Report to Congress* (June 1998) from the U.S. Federal Trade Commission makes clear" that information of a much more personal nature, such as race, health, financial standing, sexual orientation, is collected, frequently without any indication of how this information is subsequently to be used. In particular, the disclosure of such information to other parties must be controlled, if not prevented altogether.

QUESTIONS FOR POLICY CONSIDERATION

1. *Given the ease of access and problems associated with lack of protection from information, what would be appropriate for South Africa?*
2. *What policies need to be put in place regarding administration of private information collected on line?*

8.4 OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA.

These requirements are covered by the OECD *Guidelines on the Protection of Privacy and transborder Flows of Personal Data.* These establish the following eight principles:

1. ***Collection Limitation Principle***: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. ***Data Quality Principle***: Personal data should be relevant to purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and up to date.
3. ***Purpose Specification Principle***: The purposes for which personal data are collected should be specified not later than at the time of collection, and the subsequent use limited to those purposes or such others as are not incompatible with those purposes and are as specified on each occasion of change of purpose.
4. ***Use Limitation principle***: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except with the consent of the data subject or by the authority of law.
5. ***Security Safeguards Principle***: Personal data should be protected by reasonable security against such risks as loss or unauthorised access, destruction, use modification or disclosure of data.
6. ***Openness Principle***: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and

nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. ***Individual Participation Principle**: An* individual should have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; to have communicated to him, data relating to him, within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner and in a form that is readily intelligible to him; to be given reasons if a request is denied, and to be able to challenge such denial; and last, to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
8. ***Accountability Principle**:* A data controller should be accountable for complying with measures, which give effect to the principles stated above.

It should be noted that the members of the EU recommend different approaches to how the Directive should be implemented. Thus it is recommended that a combined government and industry database be set up to enable South African businesses to establish practices in any EU member country from which they may acquire personal data, for example, to establish profiles of their customers in that country.

While self-regulation of privacy matters would be preferable, experience indicates that such self-regulation has not been effective enough, for the simple reason that an organisation which does apply a stringent privacy policy is at a competitive advantage over another one which does not.

The current Promotion of Access to Information Act emphasises more the obligations of the state in the protection of personal data held by it, and less on the collection, use and dissemination of personal data by the private sector. There is a significant difference between the U.S.A. and Europe in their approach toward privacy. The U.S. legislation is mainly based upon its Bill of Rights, which primarily serves to protect the individual from the state. Legislation to protect the individual from undue invasion of privacy by other legal persons is minimal and fragmented. Europe, on the other hand, is more concerned about the latter. The first draft of the Open Democracy Bill conformed more closely to the U.S. pattern. It is understood that either a new bill, or a second one, will deal with the protection of privacy against undue invasion by business or other individuals. The necessity of covering both aspects is clear from Section 32(1) of the Constitution, which states that "Everyone has the right of access to any information held by the state; and any information that is held by another person and that is required for the exercise or protection of any rights."

QUESTIONS FOR POLICY CONSIDERATION

The OECD Guidelines and the EU directive on protection of personal data pose the following policy challenges for South Africa:

1. *Given the above background, should the privacy legislation be enacted, and if so, to what extent should the above OECD guidelines on data protection be taken into account.*
3. *How should the requirements of the EU Directive on Data Protection be met, if necessary? What could be the implications if not met?*
4. *What new or amended consumer protection laws and regulations need to be established or adapted to reinforce the rights of the public in the context of e-commerce?*
5. *How should the issue of liability for the perpetration of illegal activities via the Internet be addressed, including the roles and accountabilities of ISPs, merchants, banks, web hosting and design services, and end-users?*
6. *Should consumer protection and law enforcement issues form part of the subject matter in this Green Paper, or should their respective ministries and government departments address them, from time to time?*
7. *What role should other consumer protection bodies (for example the Consumer Council) play in this regard?*
8. *Should South African laws be established independently, or should the initiative come from international treaties?*

9. INFRASTRUCTURE, ACCESS AND CONVERGENCE

9.1 INTRODUCTION

This section deals with the infrastructural requirements for e-commerce. The section is divided into three categories viz.: infrastructure access, telecommunications competition and convergence.

The growth of e-commerce depends on broad and affordable access to infrastructure, enabled by convergence of technologies, forward looking telecommunications policy, robust network infrastructure; sufficient bandwidth and support for targeted applications. The infrastructure foreseen for e-commerce in South Africa, against the background of globalisation, should be capable of handling many services and applications. The availability of and access to broadband infrastructures will be important in driving the necessary innovation in e-commerce services.

Information Communications Infrastructure that underlies the emergence of e-commerce is multi-faceted and can be integrated in many ways including: transmission network, hardware and software components of infrastructure. It is the advancement and the integration of the essential infrastructures of these technologies that has fuelled e-commerce growth world-wide. At the same time, the comparative lack of such infrastructure throughout many parts of the developing world is what most impedes the opportunities for e-commerce to flourish in those countries.

With the convergence on Broadcasting, Telecommunications and Information Technologies, the infrastructure capable of supporting e-commerce has become almost ubiquitous in developed countries. Electronic services infrastructures must converge to support electronic commerce applications. Convergence will have broad consequences for domestic policies such as technology and innovation policies, trade policy, telecommunications policy, Broadcasting policy and competition policy.

The challenge confronting South Africa is to create an ideal market structure for e-commerce that will stimulate and modernise network development and infrastructure; accelerate universal access; support affordable access; encourage investment and innovation. Because of the critical nature of these issues, government and the business community are faced with the challenges of developing strategies and policies that will strengthen the infrastructure needed to support effective use of e-commerce.

The topics discussed below focus on the main issues and options confronting South African business and government in their efforts to address the above goals and to bring the opportunities of e-commerce to the entire population. This section addresses issues around infrastructure development and deployment; access and affordability; telecommunications market structure, competition and interconnection; and convergence. It also suggests options to promote the rollout of e-commerce infrastructure in South Africa and poses questions that could lead to new policy direction in these areas in the near future.

9.2. COMPONENTS OF INFRASTRUCTURE

The Infrastructure required to enable e-commerce has many components and comprises backbone networks, end-user equipment and access services. The success of e-commerce will depend on the availability of speedy access infrastructure; high quality of service within the backbone network; and affordable prices. Access will not only be through fixed networks (terrestrial, wireline and cable TV) but also through wireless networks (cellular, satellite, and digital broadcast spectrum).

End-user equipment and access devices include hardware (devices) and software, which control access to services and handheld devices. Examples of such devices include personal computers, TV set-top boxes, cellular phones, and other smart handheld devices. Lack of access and cost of hardware and software components of infrastructure, especially to consumers and small businesses lowers, the possibility of participating in the global electronic marketplace for much of the country's population. Software infrastructures are as important as network infrastructures. Since software provides the bridge between the network infrastructure and applications.

QUESTION FOR POLICY CONSIDERATION

How can regulation be used to promote the development of these components of infrastructure?

9.3 BANDWIDTH

Infrastructure needed for e-commerce should have adequate capacity, that is, it should be fast and reliable. The demands made by users in South Africa on the infrastructure capacity (bandwidth especially for combined data, video, voice and other services) are growing exponentially as the usage of Internet expands. Currently, analogue modems are the most common method of access to the Internet and data services by residential wireline users because of lower price. However, much of this access is at very slow speeds. It is presumed that this lack of capacity constrains what services these users can get from the Internet. With wireline technologies, all the capacity is rigidly dedicated to a particular end user, whether he needs it at that moment or not. While wireless technologies, including satellites systems offer bandwidth on demand and can provide a more economic access technology in a wide range of settings by dedicating only the bandwidth required by a particular application at a particular moment in time.

The infrastructure deployed in South Africa at the moment will not only need to be expanded into under serviced areas with the appropriate capacity, but at the same time capacity in serviced areas will have to be increased.

QUESTIONS FOR POLICY CONSIDERATION

1. *What incentives and obligations should be put in place to encourage the investment in new carrier networks in all geographic areas and new services, in a manner that will be both commercially viable and socially beneficial?*
2. *What competitive and legal environment will be most effective in creating and encouraging new investments (in transmission networks), innovation, technological leapfrogging to encourage the evolution of net works where customers have a choice of service? (Broadband multimedia, multiservice converged wireline, wireless satellite, fixed and mobile capacity)*
3. *Wireless broadband has great potential for e-commerce so it is important to study spectrum allocation mechanisms. What mechanisms can be used to allocate spectrum without increasing the cost of access?*
4. *Is the user access bandwidth requirement in the future likely to outstrip the network capability? Which mechanisms should be utilised in the broadband access technology to ensure that users access bandwidth requirements does not outstrip the network capability? (Over subscription)*

9.4. UNIVERSAL ACCESS AND AFFORDABILITY

Although South Africa has the most developed infrastructure in Africa, with over five million telephone lines with teledensity of approximately 12%, it is still a dream for the majority of citizens to have access to telephones and computers. For vast segments of the population, in rural areas, teledensity stands slightly over two percent, and infrastructure is typically unaffordable. In major cities and other urban centres, however, high technology facilities and services are widely available to those portions of the population, which can afford them.

Access includes both access to low-cost telecommunications infrastructure and networks (such as Internet) and economic access (costs to access Internet hence e-commerce). The principal goal is to ensure that the infrastructure and services are available to the wide range of potential users so that they can access and distribute information from both local and global sources.

A significant barrier to the development of electronic commerce in South Africa is the lack of access. Government made a policy decision that the roll-out of infrastructure will be better achieved through a period of exclusivity for Telkom which allows it the opportunity to roll out services, especially in places where services have not been available in the past, and modernise network infrastructure. However, Telkom's efforts alone are not sufficient to achieve all of the infrastructural needs for e-commerce. Furthermore, the deployment of appropriate technology that has adequate data capability must be accelerated in areas where it is needed.

Access to the Internet is as important as access to basic telecommunications network facilities if end users and small businesses are to be able to take advantage of Internet–based e-commerce opportunities. ITU has ranked the country 18th in terms of Internet usage. Although there are now some 120 Internet Service Providers (ISPs) in South Africa access to the Internet remains highly restricted to particular geographic locations and segments of the population (mainly business). The problem of access to ISP services in the most rural areas has yet to be fully addressed. Government needs to reflect on how to ensure access to e-commerce for communities, disadvantaged population, people with disabilities, SMMEs and ordinary citizens.

Initiatives such as the establishment of Multipurpose Community Centres (MPCCs), telecentres, Department of Communications Internet Laboratories, "dotza", public information terminals have been started to promote universal access to technologies that would be expensive if the volumes are low and unavailable to most citizens beyond the higher income group.

The prices charged by telecommunications operators for access to crucial services can be a major factor determining the effectiveness and affordability of e-commerce opportunities on the whole. These prices become burdensome for smaller entrepreneurs, Internet Service Providers and public operations such as telecentres to afford to connect to the global backbone. Broadband access for the last mile for residential customers needs to be based on a significantly lower pricing structure so as to change how small businesses and citizens use networks.

QUESTIONS FOR POLICY CONSIDERATIONS

1. *What policies could facilitate and help reduce the price of access and facilitate access?*
   Suggest other pricing approaches/models/*packages for consideration*.
2. *In complementing the above stated initiatives, how else can we ensure access?*
3. *What options are available to accelerate access to Internet to the rest of the South African population? What means, technical and financial, should be employed to promote new ISP services in rural areas?*
4. *E-commerce requires costly infrastructure. Some kind of incentive should be provided to speed up the e-commerce deployment drives in South Africa.*

   What kind of partnership should be developed between private sector and public sector with a view to assisting SMMEs and communities to access the Internet and adopt e-commerce?
5. *How do we ensure access (including appropriate facilities) for disabled people?*
6. *In some countries, pricing for local loop access is regarded as the key to e-commerce. Is the unbundling of local loop (local end of transmission networks) likely to play an important role in addressing affordability problems for access customers in South Africa? If so, what mechanisms should be used to ensure speedy unbundling of the local loop?*

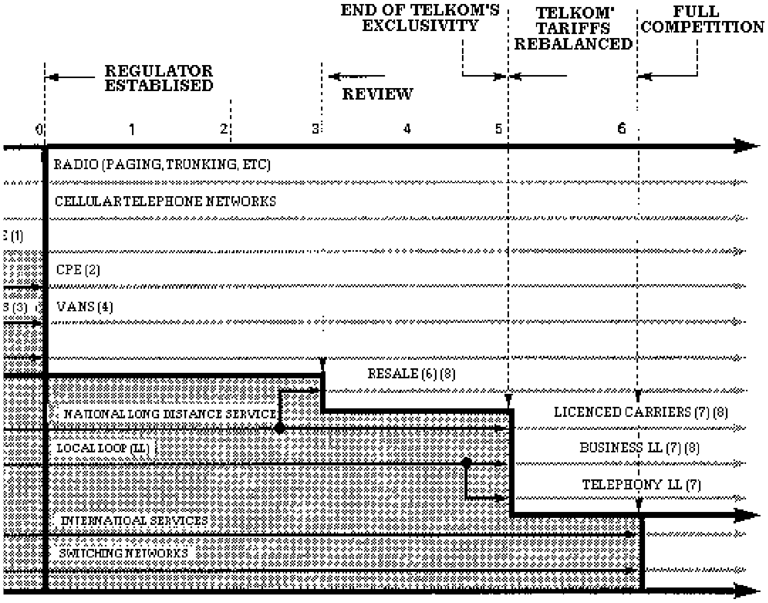
9.5. TELECOMMUNICATIONS REGULATION AND COMPETITION

Telecommunications regulation and policy need to foster effective and efficient competition while at the same time recognising social policy goals such as universality and affordability. In many countries, the transition to competition from a monopoly market structure has been a challenging exercise. It is generally recognised that the introduction of competition in telecommunications requires transitional measures to maximise the benefits of a fully competitive market.

Even in countries where open competition in telecommunications has become relatively widespread, regulation of the industry remains an important public responsibility, both to support fair competition and to oversee appropriate pricing and service responsibilities in those market segments where competition is not fully developed. Such economic regulation is even more crucial in developing countries, as market forces are not likely to emerge strongly enough to constrain dominant operator actions in the near future. This will become an increasingly important responsibility as the South African market is opened to competition. The South African telecommunications sector has undergone some changes in recent years, with the enactment of the new Telecommunications Act of 1996; partial privatisation of Telkom; and the establishment of the regulatory authority, the South African Telecommunications Regulatory Authority (SATRA), under the mandate of the Telecommunications Act of 1996, which has been recently replaced by the Independent Communications Authority of South Africa (ICASA).

The Act provides Telkom with an exclusive right to provide public switched telecommunication services for a period of time and to provide telecommunication facilities to other service providers, until May 2002. It is the intention of government to introduce facilities based competition in order to enhance the provision of infrastructure and services at the end of Telkom's period of exclusivity. The aim is to create a competitive basic market structure in the provision of telecommunications, which may have a significant impact on the markets, affected by e-commerce.

Please see the timing diagram as depicted also in the White Paper on Telecommunications overleaf:


END OF TELKOM'S EXCLUSIVITY
TELKOM' TARIFFS REBALANCED
FULL COMPETITION
REGULATOR ESTABLISED
REVIEW
0
1
2
3
4
5
6
RADIO (PAGING, TRUNKING, ETC)
CELLULAR TELEPHONE NETWORKS
E (1)
CPE (2)
S (3)
VANS (4)
RESALE (6) (8)
NATIONAL LONG DISTANCE SERVICE
LICENCED CARRIERS (7) (8)
LOCAL LOOP (LL)
BUSINESS LL (7) (8)
TELEPHONY LL (7)
INTERNATIOAL SERVICES
SWITCHING NETWORKS
▨ Exclusively provided by Telkom
┈ Licenced competitive provision

Excluding the basic telephone instrument

Including the basic telephone instrument

Licences issued by Telkom

Licences issued by the Regulator

Both Voice and Data on facilities leased from Telkom, no break-out / resale until year 4

Licenced resale of facilities leased from Telkom

Interconnect with Telkom's switching network

Contribution to Universal Service Fund

FIGURE 1 - Telkom's exclusivity and gradual introduction of competition

QUESTIONS FOR POLICY CONSIDERATION:

1. Is the existing telecommunications regulatory framework adequate to deal with the challenges posed by e-commerce?

2. How could regulator's role be enhanced in this new competitive environment of electronic commerce/communications?

3. What should be the priorities and objectives for telecommunications market development in South Africa and how will they be achieved?

4. What incentives and conditions could be put in place to attract new entrants, particularly small operators in the context of black economic empowerment?

5. What are the implications of unbundling for competition *and consumers?*

6. Certain licensing requirements are seen to have a tendency to prevent innovation, competition, and hence limiting efficient operation. Should the existing licensing conditions and requirements be reviewed in South Africa, given the advent of convergence*?*

9.5.1 INTERCONNECTION – POST EXCLUSIVITY PERIOD

The ability of entrants to interconnect with dominant operator's network is a fundamental requirement which, if completely unregulated, could forestall the development of competition through the dominant operator's refusal to allow interconnection or to allow it only under prohibitive conditions or prices. Most administrations have implemented some framework to address such abuses from ex post dispute resolution to rates, terms and conditions for interconnection approved by the regulator. In South Africa, ICASA still has to finalise the interconnection regulations.

1. *To what extend have new regulations on interconnection addressed the new challenges posed by e-commerce especially in the deregulated market in which a consumer would have a choice of the carrier in different market segments?*

2. *Should these guidelines be extended to other networks (broadcasting) in their present form or should other principles be developed?*

3. How can new carriers, especially small local operators, be assured that they will be able to interconnect affordably to the national network?

9.6. CONVERGENCE

Convergence is the ability of different network platforms to carry essentially similar kinds of service, or the coming together of consumer devices such as telephone, television and personal computer. These services include voice, data, sound and video and the convergence will make them available through one access point in the user premise via any type of infrastructure whether fixed line or wireless. For instance, while of more limited utility for e-commerce than the telecommunications networks, traditional radio and TV broadcasts have a fair high level of penetration in South Africa and this likely to be of importance to some e-commerce strategies.

Convergence occurs at three levels: technology and network platforms; at the industry and at the services/markets level. One aspect of market convergence occurring within the telecommunications sector is that between fixed and mobile telephony mostly in developed countries. This is only part of a wider trend towards the full integration of wired and wireless technologies. Many studies indicate that radical changes to Telecommunication Act, Broadcasting and Spectrum allocations laws are necessary because of convergence.

The impact of the new services resulting from convergence will be felt in the economy as a whole as well as in the relevant sectors themselves. These are telecommunications services and equipment, computer hardware, computing services, electronic information services, publishing, audio-visual services and consumer electronics. Electronic commerce illustrates those potential opportunities for consumers and businesses, although its impact in South Africa is still not significant. South Africa is however, witnessing and experiencing convergence at the regulatory, market and industry levels. For instance, it is now possible to deliver telecommunications services through electricity networks. Companies in the relevant sectors are also merging. At the regulatory level, we have seen the emergence of ICASA with the relevant amendments to the Act incorporated.

The following barriers to the development of convergence were identified by the European Green paper on ecommerce: access to users; regulatory restrictions on use of infrastructure; prices for telecommunications services; availability of content; regulatory uncertainty; market entry and licensing; access to networks, access systems and content; allocation of radio frequency and other resources; public confidence in new environment; lack of standards supporting interoperability.

As e-commerce changes the ways in which enterprises work, produce and deliver, as traditional market boundaries blur, and as technology undermines the rationale for the monopoly privileges granted to manyservice activities, competition policy will have to address new types of anti-competitive practices. As South Africa begins to experience convergence at market and service levels, we will begin to see increasing mergers and acquisitions. These factors will create an environment where producers may engage in practices that permit them to establish themselves in the de facto standard. This will have serious implications on innovation and competition and will pose a challenge to the Competition Commission and its enforcement responsibilities. The Commission should therefore guard against competition distortions and abuse of dominant market positions.

QUESTIONS FOR POLICY CONSIDERATION

1. *Convergence is seen to have significant impact on society, on employment, growth and competitiveness of business in developed countries, and on the way people access a range of services, information, entertainment and culture.*

   a) *To what extend are the effects of convergence already being felt in South Africa and in what way? What initiatives should be undertaken in order to take full advantage of convergence?*
   b) *Should telecommunications companies provide broadcasting services and vice versa.*
   c) *Regulation in terms of ownership of broadcast facilities – should this continue?*

2. *Free marketers argue that in the converged marketplace, more emphasis and reliance should be placed on market forces for achieving wider social, economic and policy objectives.*

   a) *To what extent would market forces protect consumers and safeguard public interest objectives?*

3. What are the implications of convergence and e-commerce on competition policy?

9.7 TECHNICAL STANDARDS

Standards are rules, and serve as a basis for comparison and a form of order. The major objective for standardisation is to achieve interoperability between networks and services and ensure compatibility. Users may want access from any terminal to any service, independent of the technology used, or the geographical point of such access, within a multi-vendor environment. Standards are needed for long-term commercial success of the Internet since they can allow products, services and applications from different firms to work hand in hand. Standards encourage competition and reduce stress or uncertainty in the market place. Standards can also be employed as de facto non-tariff trade barriers to "lockout" non-indigenous business from a particular national market.

Like EDI, e-commerce needs a standard platform. However, EDI has been trying to gain acceptance in the market since the 1970s, but the complexity of the standard for business transactions and the emergence of the confusing array of industry-specific subsets have made this an uphill battle. A similar lack of agreement on standards will also hinder the development of e-commerce.

An attempt therefore to develop standards in an environment in which technology is developing rapidly may be counter productive at this stage of e-commerce. It is, however, important to participate in international bodies that are currently involved in standards generating and maintenance such as the International Standards Organisation (ISO), International Telecommunications Union (ITU), International Electro-technical Commission (IEC), etc. The ITU has had a long-standing role in the development of communications standards and continues to play a lead role in producing standard sets that seek to ensure interconnection and interoperability of telecommunication networks. ITU is currently working on the development of standards on privacy, security and encryption techniques for multimedia terminals and digital certificate/certification authority issues.

Standards may be divided into three categories viz.

i. **Operational standards.** These deal with the operational aspects of the e-commerce processes and equipment.
ii. **Legal standards**. Standards by definition do not belong to the legal document type. However, should technical requirements have impact on the contractual aspects of the process then such standards may be developed. An example is the recent development on the electronic signature.
iii. Security of information standards. These cover most importantly for e-commerce, data security and process integrity requirements.

QUESTIONS FOR POLICY CONSIDERATION

1. *What factors affect the competitive position of standards in global markets?*
2. *Should the market place determine technical standards and other mechanisms for interoperability?*
3. *How should South Africa influence the work of ITU and other international standard setting bodies in the development of e-commerce related standards?*

10. DOMAIN NAMING

10.1 INTRODUCTION

Domain names are Internet addresses allocated to users on application to the relevant institutions assigned with the responsibility of allocating these addressees locally and worldwide. There are two main forms of domain names classified as, first, country top-level domains and denoted by cc TLD's, and second, the sub-domains or generic top-level domains denoted by the abbreviation: g TLD's.

To find an orderly manner in which the Internet can be accessed, a system that associates names with each user referred to as a Domain Name System (DNS) was established.

While designed to serve the function of enabling users to locate computers and other devices in an easy manner, domain names have further significance as business identifiers and, as such, have come into conflict with the system of business identifiers that existed before the arrival of the internet and that are protected by intellectual property rights. Details on this new conflict, known as 'cybersquatting', will be discussed under the heading 'DNA Dispute Resolution'.

Internet governance issues have generally fallen outside the ambit of national policy, largely because of the complexities of Internet regulation. International processes and structures overwhelmingly influence the domain name space issue. In developing policy, South Africa's overall governance goal should be to enhance the welfare of all those who operate and use the Internet and to extend the Internet to a wider population of users. A balance between the need for a technically sound, efficient and secure operation should, however, be struck while desiring to open the market to a broad range of potential players in this area.

10.2 INTERNATIONAL SITUATION

A number of governments believe that they have the right to manage the domain for their country, top-level domain (for example .za). From the outset, the registration and management of Internet naming and addressing was the responsibility of the Internet Assigned Numbers Authority (IANA), a US government funded body. Later it became clear that governance of the addressing schemes and domain name space could not be seen as a global and independent initiative if it was funded by the US government. Therefore the US government created an "independent structure", the Internet Corporation for Assigned Names and Numbers (ICANN) which replaced IANA. This new structure has yet to establish credibility as a truly independent player in the international context to remove the perception that it is a US voice. To this end, ICANN has embarked on an informal membership recruitment drive through its "at large" membership Programme. There is a danger that only the connected society, those with access to the Internet, will join and only their voices will be heard. The voice of developing countries, which have typically few people with access to the Internet, may be poorly represented and policy decisions may be made without adequate inputs that take cognisance of needs of developing countries into account. A regional body to represent Africa in ICANN, called AfriNIC (a private sector initiative), is in the process of being formed to have inclusivity in ICANN.

10.3 ISSUES OF CONCERN

There have been discussions and disputes over domain name management internationally and nationally. There is concerted effort to resolve these disputes with varying levels of success. Of greatest concern are cybersquatting, trademarks Vs domain names and potential security concerns.

10.3.1 Dispute Resolution: Trademarks Vs Domain names

The fact that in electronic commerce businesses can exist entirely as virtual entities with only an electronic presence, the relationship between intellectual property, usually protected through trademarks and branding, and domain names becomes an issue that require attention. At this stage, registrars of domain names are not required to verify whether names that are to be registered are protected through trademarks. Therefore it means anyone can register a trademark as a domain name irrespective of whether he or she owns the trademark. This situation has led to abuse by citizens of cyberspace who see potential profit making opportunity through registering a domain name and selling it to any company that would want to use it. In response to this concern, the World Intellectual Property Organisation, undertook an extensive study of the issues, which culminated in recommendations on the governance of allocation of addresses and domain names. The salient features of the recommendations are as follows:

- Collection and availability of reliable information regarding the contact details of domain name holders is viewed as an essential tool for protection of intellectual property and is therefore seen as a crucial component of the best practices that must emerge among registrars.
- Introduce non-commercial, use-restricted domains, where public availability of the contact details of those domain name holders would be unnecessary.
- Registration of domain names should continue to be a speedy process and therefore searches of trade names before permitting domain name

registration is not recommended, instead, a thorough process of dispute-resolution is to be adopted and ICANN be the custodian of this process.

10.3.2 Potential security concerns

In older versions of the DNS system, security problems related to an organisation's domain name could be falsely "taken over" by another organisation. The effect would be that when browsing the web, a user would think that he/she have gone to a particular organisation's web site, but might have been diverted to another site masquerading as the original one. This type of problem has been addressed in newer versions of the system, but it is important that all registrars of the DNS, who operate and administer the system on behalf of the users of the Internet, be competent and able to administer the system correctly. This would include ensuring regular upgrade of software used in servers to maintain adequate levels of security. Therefore it is necessary that minimum criteria be set for registrars to meet and adhere to, so that security concerns can be adequately managed.

10.4 CURRENT SITUATION IN SOUTH AFRICA

In South Africa, the .za domain has until now been administered by UNINET, which was the domain name register for the .za domain as designated by IANA. The most commonly used name address in South Africa, and probably in Africa, is co.za domain and a section 21 company, called Uniforum, manages it. Fees for registering the domain are applicable. Inrecent years, it has become clear that a new governance structure for domain names in South Africa will be required. A discussion document commissioned by the Internet Society was issued (www.isocSOC.org.za). This paper seeks views from stakeholders on what type of management structure would be ideal in South Africa. The document also made a number of recommendations. These include establishing section 21 company with open membership. The Department of Communications has also proposed that an independent Domain Name Authority (DNA) be established (Discussion Paper on the Establishment of an Independent Domain Name Authority, April 2000 – www.ecomm-debate.co.za). This non-profit making organisation will be run by a Board of Directors representing all stakeholders within the Information Communication Technologies (ICT) private sector, public sector and civil society, in general. This thinking is in line with developments in countries where transformation of domain naming has occurred. In these countries a common understanding has been reached on varying principles such as:

1 An acknowledgement that responsibility for the country-level domain is a national asset within the emerging economy.

2 That the government and private sector have a key role to play in the emerging information economy, both as model-user/ consumer of

Internet services and secondly, in creating a climate conducive to the smooth growth of the economy, especially in resolving various Internet-related disputes at national and international levels.

3 That the policy formulation process within the information communications technology arena should be inclusive of all stakeholders or representatives of stakeholders and the public, in general.

4 That the new economy, like all other free market economies, was not perfect, and therefore required the intervention of government on a policy formulation basis to intervene in extending services to both public institutions and citizens who wish to access the services offered.

The DNA would among other things look at issues such as provision of universal Internet addresses; deal with the question of dispute resolution and trademark "cybersquatting"; find appropriate means for deregulation of registration and competition in registry in order to introduce and encourage competition in all activities related to registration. Lastly, such a body will acquire accreditation from an international body such as ICANN.

10.5 POSSIBLE SCENARIOS FOR GOVERNANCE

- In the case where it is decided that government needs to play a role in Internet governance, it could establish a policy framework and structures necessary for government to take responsibility for the governance structures, more specifically the domain name service.
- An entirely private solution for the creation of the registry. This might have the advantage of dissociating the South African registry from the public authorities, but this may give rise to issues under competition policy.
- If it is assumed that few or no policy or governance intervention is necessary. Government may choose to participate in any governance structures that exist, and influence their direction to whatever extent possible, but not create any further policy or governance regulations.

QUESTIONS FOR POLICY CONSIDERATION

1. *What should be South Africa's position regarding international processes that are underway and structures being put together to effect governance of the Internet, for example ICANN and AfriNIC? Should South Africa support those structures?*
2. *Given the above discussion, what should be the role of the private sector and government in the management of domain names in South Africa?*
3. *Is the proposed organisational framework to administer domain naming in South Africa an adequate one? How should such a structure be financed?*

4. *What kind of criteria should be applied for the business, technical environment and processes of registration so that stability of the DNS is maintained while at the same time encouraging robust competition in the delivery of registration services?*
5. *What suggestions do potential users (notably SMMEs) have as to how the domain names in South Africa might be managed in order to promote access to the Internet addresses and encourage competition.*
6. *What would be the barriers of entering the market at the registry level?*
7. *How should we promote access to Internet addresses?*
8. *In order to preserve heritage and promote the South African culture and tourism, particular attention should be paid towards creating, naming and registering heritage and cultural websites for South Africa. Should there be a dedicated institution mandated to performing this task?*

11. ELECTRONIC PAYMENT SYSTEMS

11.1 INTRODUCTION

Payment systems, in the electronic commerce environment, refer to methods or instruments of effecting payment through electronic means. E-commerce transactions/payments rely on the intermediary role of banks, credit card companies and other financial institutions.

The challenges we face in this environment relate particularly to emerging payment mechanisms which can either be network-based or be stored-value cards smart cards since some have the potential *to exchange* value (payment) without the necessity of direct linking to bank accounts. The legitimacy and security of electronic money payment systems may "make or break" electronic commerce growth in South Africa. For instance, if payment systems are too complex or expose consumers to on-line fraud and theft, the viability of electronic commerce may suffer a material blow.

11.2 GUIDING PRINCIPLES

For consumers, electronic payment can readily be made using traditional credit and debit cards and new types of credit instruments that are being introduced. Questions surrounding the security of these forms of payment are among the key concerns involved in building trust in Internet-based transactions (see earlier sections). In the USA, some businesses are finding that as many as 60 per cent of their Internet credit card transactions are fraudulent. Even if these mechanisms can be made secure and effective from the consumer's perspective, however, they may not always be the most efficient ways of transferring funds around the world over the Internet. Other alternatives being considered within the industry include so-called "digital cash" (also referred to as "electronic money") and prepaid accounts. Some of these ideas might also be applied directly to the challenge of serving customers who lack access to full banking services.

In summary, most digital cash proposals involve the establishment of a virtual bank account into which the user deposits some amount of funds, or through which he or she establishes a line of credit. The account operator (which could be a bank, credit card Company, or retailer) establishes relationships with on-line merchants that allow for payments to be made directly from the subscriber's virtual account for purchases from those merchants. When selecting a product for purchase, the user may authorise payment by means of a secure, coded transmission, similar to a digital signature. This instructs the account operator to effect a transfer of funds from the user's account to the merchant's (including a transaction-processing fee to the intermediary). Although this system exists in various forms, particularly for certain well-established on-line merchants, there is no single standard or worldwide coalition of providers. Issues of security and trust, and also of competing interests by the financial and retail firms involved, have slowed acceptance of these types of services to date, but they are likely to continue to gain acceptance in the future. Proposing new and secure online solutions for electronic payments will be one of the most important challenges to financial operators.

Another mechanism that has been gaining popularity with companies and consumers is integrated circuit cards, commonly known as "smart cards." Smart cards contain programmable microchips, which can be set to identify the total value of the card (in the case of "pre-paid" cards), or the amount of funds on deposit in the user's associated bank or virtual cash account.

The cards can be issued by a specific merchant or service provider (telephone smart cards are especially popular), or can serve as general-purpose payment vehicles. The cards can be used to make regular transactions, with the amount of the payment deducted automatically (by a point-of-sale device, public telephone, or other device) from the total available on the card.

Although some smart cards are disposable once the value on the card has been expended other smart cards are re-loadable and allow the user to replenish the value on the card at an authorised agent.

Smart cards or similar ideas might be especially useful for providing financial services and access to electronic payment systems for the so-called "unbanked" consumers in rural areas or others without access to bank accounts and credit cards. Instead of paper pay cheques, for example, the general public could receive payment for their jobs or transfer payments via electronic transfers, by loading the correct amount to their personal smart card. The benefit could include reduced risk of theft and fraud, and much wider access for the general public to both electronic and traditional products and services.

Other chip card based instruments that would have to be considered in terms of electronic commerce include:

- Cellular phones, which are popular electronic communications devices, since they remove the traditional restrictions of geographical location and high entry costs. With the rapid expansion of WAP-enabled cellular phones, the Internet will be available to all. Even phones that are not WAP-enabled would be capable of being used as payment instruments.

- A Set-top Box is a device which enables the owner of a television set to receive digital television signals. These boxes will give users access to the Internet, e-mail, various other interactive channels and as a result could be used as a channel for payment.

11.3 CURRENT POLICY AND INITIATIVES IN SOUTH AFRICA

South Africa's financial services sector is well advanced, especially for providing business services in the urban areas. The South African Multiple Option Settlement (SAMOS) System was developed by the South African Reserve Bank and has been operational since 1998. This system links all the settlement banks in the country and allows real-time settlement between the banks. Major South African banks have data networks connecting their branches and large corporate customers.

These accomplishments mean that the South African financial sector is well positioned, especially with regard to large corporate businesses, to support widespread applications of e-commerce.

The South African Reserve Bank has published a document which gives an overview of emerging electronic money and commerce models. Traditional and new options for making electronic payments, including digital cash and smart cards, authentication and technical implementation issues surrounding them *are* discussed in this document. At this stage, there is no intention that the Reserve Bank should itself issue stored-value cards, or provide other forms of electronic money to the public.

The South African Reserve Bank also published a position paper in April 1999 on "Electronic Money"*.* This paper highlights certain criteria applicable for the implementation of electronic money, products and schemes.

Steps are also being taken by government, banks and the private sector to find a common standard for smart cards in South Africa, which will be acceptable both nationally and internationally.

Although the South African Reserve Bank has taken the lead in publishing its position paper on electronic money in April 1999, it is proposed that the following issues be investigated.

- Many countries are currently in the process of adopting "digital cheques" purporting to fulfil the same function as traditional paper-based cheques. It is submitted that the Bills of Exchange Act 34 of 1964, in its current form, is incapable of applying to and/or regulating "digital cheques". The inability of the Act to apply to digital cheques constitutes a material barrier to electronic commerce due to the absence of adequate consumer protection and commercial certainty of payment provided for by the Act. The Reserve Bank is however of the opinion that the use of credit push instruments for low value retail payments should be encouraged instead of debit pull instruments. With “credit push” the payer initiates the transfer of funds to the payee whereas the “debit pull” requires the recipient to collect the funds from the payer’s bank.

- The Prevention of Counterfeiting of Currency Act No. 16 of 1965, in its current form, is incapable of being applied to the "counterfeiting" of electronic money.

- The issuance of electronic money may fall outside the definition of "business of a bank", as defined in the Banks Act 94 of 1990. Accordingly, issuers of electronic money may find themselves "unregulated" and consumers "unprotected". However, in terms of the position paper, only banks would be allowed to issue electronic money from now on. Primary and intermediary issuers of electronic value will therefore be subject to regulation and supervision by the South African Reserve Bank. Although single purpose schemes will generally fall outside the definition of electronic money, the South African Reserve Bank will determine whether multi-purpose schemes fall within the definition or not.

In terms of the South African Reserve Bank Act, 1989 (Act No. 90 of 1989), the Banks Act, 1990 (Act No. 94 of 1990), the National Payment Systems Act, 1998

(Act No.78 of 1998) and the position paper on “Electronic Money”, the South Africa Reserve Bank is in a position to regulate electronic money. However, the Reserve Bank does not want to discourage innovative new technological developments by pre-regulating electronic money but instead wishes to familiarise itself with electronic money schemes generally, the effect of electronic money on monetary aggregates and the potential risks that electronic money might pose for the national payment system.

QUESTIONS FOR POLICY CONSIDERATION

1. *What steps need to be taken to further upgrade and integrate national financial services infrastructure so as to facilitate e-commerce?*
2. *How can basic banking services be extended to the broader population, to allow use of electronic payments, credit, and funds transfers?*
3. *What types of electronic payment systems and technology are most appropriate and practical? How can these be developed effectively on a national level, in co-ordination with international industry efforts?*
4. *How should the government support these development efforts, both logistically and financially? Which agencies should be responsible? Are these legislative actions that need to be considered?*
5. *Should non-banking institutions be allowed to issue e-money? How can the Reserve Bank ensure that such non-banking institutions are licensed, regulated and prudentially secured?*

12. MAXIMISING BENEFITS

12.1 INTRODUCTION

The positive effects of the Internet permeate every aspect of society ranging from social, economic, technology, education, health, and welfare to the business and academic fields with a common outlook for development and growth. To date much emphasis of the benefits of e-commerce are those directed at big business. Therefore there is a need to extend such benefits to communities and previously disadvantaged individuals as well, through appropriate policy measures.

Most of the policy debates around "Maximising Benefits" are geared toward removing barriers; developing strategies that would enhance and exploit the opportunities brought by e-commerce; and designing programmes to spur economic growth. A critical policy challenge is how to accelerate and enhance the development of the infrastructure necessary to extend the benefits of e-commerce to all South Africans.

The purpose of this chapter is to highlight the benefits that can be gained from e-commerce especially with successful strategies and the contribution e-commerce can make to the sustainable socio-economic growth. The following issues will be addressed:

- Economic and social impact of e-commerce
- Developing and growing the market for e-commerce applications and solutions
- Raising awareness of e-commerce
- Training and education
- Jobs and Skills

12.2 ECONOMIC AND SOCIAL IMPACT OF E-COMMERCE

E-commerce presents unique opportunities for less developed countries to greatly expand their markets both internally and externally. Externally, the Internet and other technologies may allow for low cost international trade, even for small, local businesses. Internally many groups of citizens who had been "marginalised" and "unbanked" may gain affordable access to financial services, and may thus participate more readily in all aspects of the economy.

E-commerce technologies carry the potential to reshape the geographic boundaries and the location of commercial business centres may become less relevant, as companies and workers conduct business with equal effectiveness from almost any location.

Electronic commerce will transform and help to shape society as a whole especially in the areas of education, health and government services. From a public policy standpoint, there is a need to establish the social conditions that allow e-commerce to reach its full economic potential and to ensure that its benefits are realised by society as a whole. The necessary elements or conditions are access, as determined by income and availability, confidence and trust. Access to the physical network will affect the adoption of e-commerce particularly among consumers and small, micro and medium sized enterprises (SMMEs).

The digital divide challenge

Digital divide refers to inequalities in ICTs distribution between developing and developed economies. North-South digital divide is real and needs to be addressed. It also refers to the gap in the information sphere between most developed parts of the country and underdeveloped rural parts, including disadvantaged groups. The challenge is how to narrow down the gap between “information haves” and “information have-nots” through addressing inequalities and inequity. If this matter is not urgently addressed, the benefits of e-commerce will be enjoyed by the few only and the expansion of e-commerce would indeed contribute to broaden rather than reduce a possible digital divide.

12.3 THE SOUTH AFRICAN E-COMMERCE MARKET OVERVIEW

When sizing the electronic commerce market, a distinction needs to be made between the value of the commerce transactions, which is potentially large, and the revenues that can be earned by third party commerce facilitators. Another important dimension is revenue that can be earned by aggregators through online advertising. Distinction should also be made between web-centric e-commerce and e-commerce using other networks such as electronic data interchange (EDI).

Projected e-commerce (web-commerce) turnover in South Africa

	1999	2000	2001	2002	2003
	Rands	Rands	Rands	Rands	Rands
B-B	3.9bn	8.0bn	17.0bn	27.4bn	37.2bn
B-C	2.7bn	5.3bn	8.3bn	11.8bn	18.8bn
Total	6.6bn	13.3bn	25.3bn	39.2bn	56.0bn

Source: Media Africa com. 2nd SA Web Commerce Survey 1999

South African business, particularly large companies claim to be conducting commercial transactions via electronic networks. Furthermore, e-commerce is now the leading investment area in the Top 200 IT users in South Africa. Although only 6 % of large companies interviewed could estimate the exact revenue accruing from their web site in 1999, nearly 30% believe their web sites are already influencing customer-purchasing behaviour (BMI-T survey 1999). Small to medium sized companies appear to be slow in embracing the use of the Internet and thus the ability to benefit from an increased global market

The rate of adoption of e-commerce by South African citizens shows a relatively high rate compared with other developing countries. A survey by BMI-T indicates that approximately 10 % of all high-income households have adopted e-commerce. This allows these consumers to have access to a range of services available on the Internet such as banking services, online shopping e-ticketing, etc. Travel and accommodation is by far the largest category in the BMI-T forecast model, which indicates that by 2004, more than R13 billion worth of consumer transactions will be influenced by the Web, of which R4 billion will be directly completed on the Web. The outlook in the financial services sector is equally impressive.

Despite increasing evidence of the global explosive growth of e-commerce and its revenue generating and job creating potential, many governments outside of the US are concerned about:

(i) The slow adoption of e-commerce strategies by their own firms

(ii) The lack of urgency expressed by company executives in respect of the potential threats and opportunities posed by e-commerce;

(iii) The lack of responsiveness by domestic companies in meeting domestic and international online demand for goods and services.

A recent Canadian study illustrates point three above by revealing that 60 % of Canadian on-line demand is supplied by US firms; 2 % by European firms and only 38 % by domestic firms. The report suggests that Canadian business needs to be more aware of the growth in domestic on-line demand and actively seek to capture a greater market share of local on-line demand as well as international demand for on-line goods and services.

The above concerns give reason for the South African government to develop a policy that ensures access for all its citizens in order to speed up the adoption of e-commerce in the country.

The sections that follow attempt to seek ideas on how to deal with this problem in South Africa and what strategies should be developed.

QUESTIONS FOR POLICY CONSIDERATION

1. *Did we see as much new growth in 1999 as we expected? If not, what are the reasons behind this slow growth?*
2. *What should be done to accelerate the adoption of e-commerce by both businesses and consumers in the marketplace?*

12.4 MARKET DEVELOPMENT

In producing a market development strategy, three key elements are relevant, namely, positioning the South African industry in the global e-commerce marketplace more competitively, supporting SMMEs, and developing public private partnerships.

Improving South Africa's industry competitiveness. E-commerce is rapidly transforming the terms of competition in global and national economies in new and unpredictable ways. The unfamiliarity and unknowns of e-business represent an unprecedented competitive uncertainty for firms, supply chains, national export positions and, ultimately, to economic competitiveness. The fact that e-business is creating new value propositions in and between global supply chains poses a fundamental strategic challenges for SA firms in relation to where these firms should aim to position themselves within these evolving global supply chains so as to obtain best comparative advantage and capture value. The core challenge is to identify measures that enable South African firms of all sizes to quickly understand ‘what e-commerce is all about and, with such knowledge, turn e-business threat into e-business opportunity.

While the application of e-commerce in conventional business certainly represents the bulk of activity and investment, whole new business opportunities are emerging, such as shown in the table below.

Internet Intermediaries	**Internet Applications and Services**	**Internet Backbone Providers**
Market makers in vertical industries	Internet Consultants	ISP's
On-line travel agents	Internet Commerce Applications	Networking, hardware and software companies
On-line brokerages	Multimedia Applications	PC and services manufactures
Content Aggregators	Web development software	Security vendors
Portal/Content Providers	Search Engine software	Fibre optic makers
Internet Ad brokers	Online Trading	Line Accelerators
	Web enabled databases	
	Customer relationship management	

A number of challenges that need to be considered for policy formulation are the following:

- Lack of capital for investment
- Insufficient capacity in the domestic IT industry to satisfy rising domestic e-business services demand
- Lack of competitive e-business knowledge and skill by industry players.– Skills are largely located in the IT industry with the exception of the banking sector
- No or lack of alignment of e-business strategy to the overall company's business strategy
- Lack of access to both infrastructure and to e-business services by small firms
- Prevailing low levels of awareness about e-business among firms and lack of preparedness by public business sector.

Supporting SMMEs: E-commerce has the potential to facilitate growth of small, medium and micro enterprises. According to reports, in the US, one out of three jobs are created by SMMEs. It is therefore evident that a faster adoption of e-commerce by SMMEs can potentially create some employment in South Africa. A recent study conducted by BMI-TechKnowledge group states that of the 600 000 registered SMMEs in South Africa, only 16% of them are conducting e-commerce. What is even sadder to notice is that 31% of these SMMEs believe they will never use the Internet for business. The challenge therefore is to empower the SMME sector to take advantages of e-commerce and increase their capacity to participate in the e-driven trading environment.

UNCTAD has cited the necessary conditions that need to be met for SMMEs to realise the potential of e-commerce:

- Access to reliable cost effective telecommunications infrastructure and Internet connectivity.
- Skills and Human Resources (vigorously introduce e-literacy).
- Content - the ability of SMMEs to produce content on the web that will be a key ingredient for broader success
- Trust in the electronic environment.

Public private partnership approach in market development: Partnerships are key to creating the enabling environment necessary for the growth of electronic commerce and in implementing e-commerce. Hence the reason why government is consulting with business, consumers, trade unions, interest organisations and communities in addressing e-commerce issues. The government acknowledges the leading role of the private sector in implementing e-commerce in terms of applications. Various mechanisms have to be employed at discussion level, advisory, applications, infrastructure and networking, research and development. Countries like USA are good examples of partnership programmes initiated to realise the benefits of e-commerce by enterprises of all sizes.

QUESTIONS FOR POLICY CONSIDERATION

1. *What policies, programmes or partnerships can government develop or leverage to support and encourage the growth of the local industry?*
2. *How successful are South African firms in creating and meeting the demand for local and international on-line goods and services and how should companies position themselves to capture a growing share in this expanding market?*
3. *What are the current constraints and how, could government create a more enabling environment for South African firms.*
4. *What steps or interventions are required to systematically expand the pool of e-commerce expertise and help resolve the skills-gaps or leakages within companies? What, if any specific interventions are required to foster entrepreneurship and innovation in the sector? And what manner of intervention would encourage the participation of formerly marginalised black entrepreneurs and women in particular?*
5. *What level of Research and Development (R&D) is required for the SMMEs? What institutional support framework should be put in place to assist SMMEs in the adoption of e-commerce? How could the existing structures/organisations be enhanced to encourage and promote the faster adoption of e-commerce by SMMEs?*

6. *What mechanisms should be put in place to develop and strengthen public private partnerships in order to enhance the economic and social benefits identified in this section?*
7. *What kind of public investment is required to foster industry development for the proliferation of e-commerce?*

12.5 HUMAN DEVELOPMENT

Skills and Human Resources: It is clear that the availability of sufficient human resources will continue to be an overriding issue in many areas of global e-commerce. There is a need to develop human infrastructure with skills, ability, training and knowledge to leverage ICT potential benefits. The Human Resources Research Council (HSRC) states that there is a chronic shortage of highly skilled human resources in various segments of the market. The scarcity of technical expertise and skills, in the country is further exacerbated by the "brain drain". The South African Information Technology Industry Strategy (SAITIS) Baseline Studies identified more reasons for shortage of highly skilled human resources including ICTs workers.

Digital literacy: Digital literacy is required for business and consumers to use and develop electronic commerce. At present, Internet users tend to be more educated, affluent and located in urban centres and Internet usage is higher in larger companies. The challenge is to expand to a wider range of consumers and all sizes of business. There is a need to bridge computer illiteracy since it is an important impediment to the facilitation of e-commerce.

Digital skills for all South Africans: In a country where literacy remains a huge and seemingly intractable problem, what resources and programmes are required to develop an awareness of the potential benefits of the information age; related technologies and e-commerce in particular. Adult and life-long learning programmes, tertiary and higher education schools and in some countries even early learning centres are the focus of review and attention. Policy makers should institutionalise ICT awareness and skills development within the labour market and prepare school leavers for an increasingly knowledge-based society.

Skills for Business: Internationally, the use of the Internet by small and medium enterprise is growing and actively encouraged by a range of government initiatives designed to foster this growth; and ensure that business owners understand the business opportunities that e-commerce presents.

Skills for the future: As elsewhere, the issue of (high-tech) skill shortages is a concern to both the private sector and government. Especially in South Africa where unemployment is high and a growing number of school-leavers enter the labour market with limited prospects of employment. There is a need for a research to inform what skills are required in the future. The Department of Arts, Culture, Science and Technology's Foresight programme in one way or the other raises and addresses the issue of skills for the future.

12.6 EDUCATION AND TRAINING

Distance education, virtual campuses and technological training will dominate the education sector in the future. Institutions of higher learning need to take a lead role in developing and implementing e-commerce based curricula. The proposals and recommendation for partnerships include the provision of education and training to local entrepreneurs, knowledge workers, users, businesses, policy makers and regulators. The development of educational training content should be inclusive and cater for known learning barriers such as with disabled people.

12.7 JOBS

The labour market is one of the areas likely to feel the most profound impact of the economic transformation being brought about by e-commerce. On the one hand, if e-commerce generates significant economic growth in general, should lead to improved employment opportunities generally. However, the exact nature of employment, and of the skills and experience required to benefit directly from e-commerce, could be significantly different in some industries. For instance many workers could become displaced, temporarily or permanently as a result of this transformation. Some displaced workers might need to be re-skilled/retrained to prepare them for new jobs in the marketplace. Clearly there is need for research in this area to evaluate the nature and number of jobs that could be created by e-commerce and lost or displaced due to efficiencies brought about by new ways of doing business. Although it can be argued that some jobs are lost due to e-commerce replacing intermediaries between business and consumers, a new breed of e-commerce firm “the infomediary” is being created to exploit the Internet.

12.8 AWARENESS STRATEGY

Central to this issue is educating the wider population about both the opportunities and potential, threats of e-commerce. Coupled with that is the need to popularise or publicise an e-commerce policy process so as to invite participation. The creation of awareness and other related initiatives by government and its partners from the academic and business sectors to promote technological development should be done on an integrated approach. We need to build a new e-community that can take effective advantage of the e-commerce opportunities.

QUESTIONS FOR POLICY CONSIDERATION

1. *What is the potential of e-commerce to create jobs? How can job creation be maximised? What strategies should both employers and government devise to minimise the effects of perceived job losses or displacements?*
2. *How can we leverage the available resources to maximise their benefits and focus to harness these skills?*
3. *How do we expand the current capacity to maximise e-commerce benefits?*
4. *What strategies and programs should be deployed to inform the process of targeting relevant stakeholders and the level of education required?*
5. *What should be the responsibilities of the institutions of higher learning and that of the Department of Education in the educational, training and awareness sector?*
6. *In what way would the private sector, in partnership with government, be involved in the awareness campaign and training programmes on e-commerce?*
7. *Funding is one of the critical success factors in the implementation of e-commerce strategies. What other innovative funding options are available except government resources?*
8. *What organizational framework should be put in place to continuously promote awareness?*
9. *How can brain drain be minimized?*
10. *How should the educational content be implemented to accelerate e-commerce?*

13. FRAMEWORK FOR E-GOVERNMENT

13.1 INTRODUCTION

Today governments are moving from old economy government, organised around agencies and bureaucracies that operated like "stove pipes", to new economy government which will be organised around the functions and the needs of citizens with ICTs as a key enabler. Leading-edge governments are rethinking their web strategies from their citizens' perspectives. The trend toward a greater level of interactivity, which allows users to obtain services and conduct transactions, continues. The Government service model will shift from the traditional relationship of a citizen interacting with a worker who turns to the IT infrastructure in the background, invisible to the user. Instead the citizen will interact directly with the IT infrastructure and the worker will serve as a problem solver for more complex issues. Being freed from routine, repetitive tasks will allow the government worker to solve problems more effectively. Citizens will, in turn, have more rapid results from routine transactions, as well as 24 hour 7 days' service.

The long-term goal for the South African government should be to take the reigns and lead the charge with regard to the deployment of ICTs and e-commerce into its business model. If government is to obtain the real benefits of the information age, for better service delivery, better procurement, efficient working and better communication with citizens and businesses, a comprehensive system needs to be formulated and implemented. Public services should be responsive to the needs of citizens and be of high quality. This chapter will identify some of the challenges facing the South African government in transforming conventional government into e-government. The chapter seeks to answer the following questions:

- What is e-Government?
- Why e-Government (challenges and opportunities)?
- What does it take to become an electronic government?
- How should we move from the traditional government to electronic government?

13.2 BENCHMARKING: INTERNATIONAL COMPARISONS

Many countries are or have already launched comprehensive client-driven e-government strategies. These countries include Canada, United States of America, Britain, Australia and Singapore. They have established clear goals and discrete targets for e-government. Their efforts to implement these strategies are supported by high-level leadership, an enabling policy and legislative framework on e-commerce, and an appropriate investment strategy.

Visions and targets

	US	**UK**	**Australia**	**Singapore**
Vision	Access America	Modernising Government	Strategic Framework for the Information Economy	Public Service for the 21st Century
Political Champion	Vice President	Prime Minister	Prime Minister	Deputy Prime Minister
Targets	2003; "where practicable"	100% by 2008	2001; "where appropriate"	2001; "for key services"
Investment	Modest	Large	Large	Large
Legal Framework	Draft legislation	Fall legislation	Legislation pending	1998 Law
Infrastructure	Departmental strategies	Corporate IT strategy	Corporate IT strategy	Broadband strategy

Source: Industry-Canada

Given the above comparisons, the crucial question that needs to be answered is "Where is South Africa" in this picture.

13.3 WHAT IS ELECTRONIC GOVERNMENT?

Electronic government can be defined as government use of information communication technologies to offer citizens and businesses the opportunity to interact and conduct business with government by using different electronic media such as telephone touch pad, fax, smart cards, self-service kiosks, e-mail / Internet, and EDI. It is about how government organises itself: it's administration, rules, regulations and frameworks set out to carry out service delivery and to co-ordinate, communicate and integrate processes within itself.

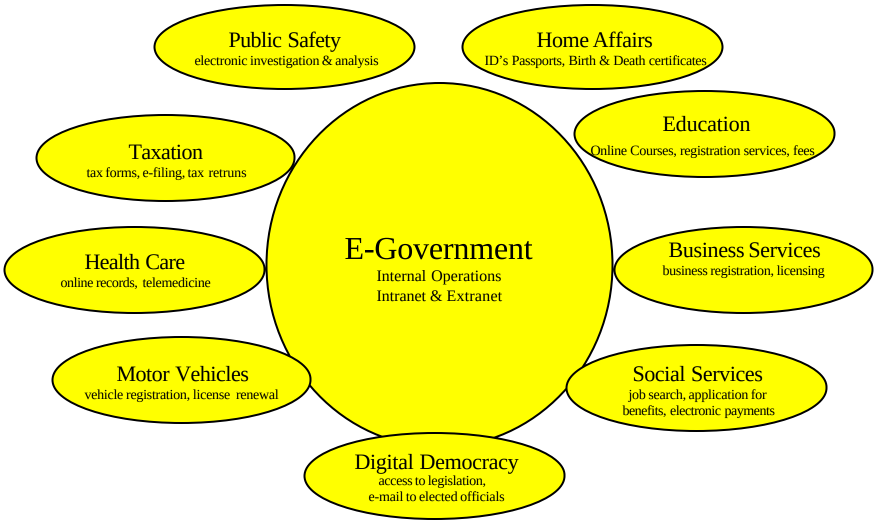
In understanding e-government, one needs to define:
"Customer" – includes the public, business, other employees, other agencies and other levels of government
"Electronic Business" –use of the Internet to create new business models; new ways of serving customers; new ways of generating profits
"Electronic Commerce" – use of electronic networks to replace paper-based transactions; the transactional part of e-business or e-government
"Electronic Government" – a vision of how government can operate in the 2000s; much broader than just e-commerce or e-business for government

13.3.1 Components of e-government

In modernising government, the following issues must be addressed:

Electronic Service Delivery – government of the future that entails a shift to a citizen-and customer focussed thinking where citizens must be able to access more and more public services, delivered online, anytime, anywhere. Moving citizens from ' standing in line' to online. These services must be integrated and customer-centric. This should be aligned to Batho-Pele service delivery framework.
E-business for e-government – government purchasing of goods and services and payments electronically
E-governance – this is about public participation in decision making, the reshaping of policy and evaluating of administrative effectiveness and service delivery efficiency
Governance, Information Sharing and Exchange – reducing number of paper transactions involved in government operation. Use of Intranet and extranet between government departments and among employees.

E-commerce Policy – e-government requires a regulatory and public policy environment that is conducive to e-commerce
Technology behind the scenes - Leaders (Chief Information Officers need to understand the capabilities of the technology infrastructure essential to translate vision to reality.

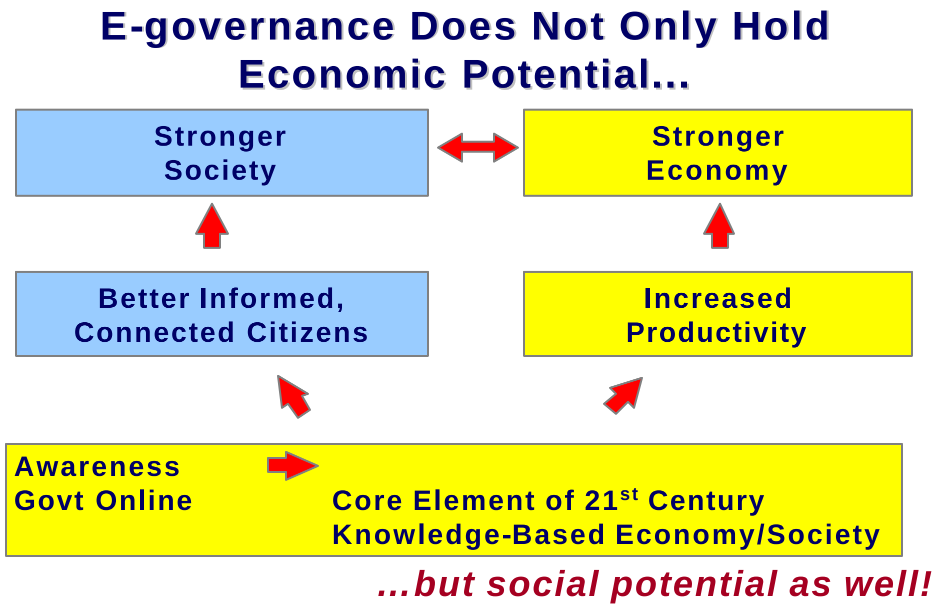

Public Safety
electronic investigation & analysis
Home Affairs
ID's Passports, Birth & Death certificates
Taxation
tax forms, e-filing, tax retruns
Education
Online Courses, registration services, fees
E-Government
Internal Operations
Intranet & Extranet
Health Care
online records, telemedicine
Business Services
business registration, licensing
Motor Vehicles
vehicle registration, license renewal
Social Services
job search, application for
benefits, electronic payments
Digital Democracy
access to legislation,
e-mail to elected officials

13.3.2 Examples of On-line Services

13.5 WHY E-GOVERNMENT?

Increasingly governments are playing a key role in demonstrating the advantages of electronic service delivery. E-government presents with it both opportunities and challenges to governments. There are both environmental pressures and business drivers that necessitate a transformation to e-government. These pressures include shrinking budgets, "do more with less", rapid technology advances, shifts in customer expectations, labour pool limitations. Business drivers include improving customer focus and service, focussing resources on core mission areas, increasing competitiveness in the marketplace. By transforming to e-government, the government will foster entrepreneurial government based on more business-like practices, cost savings and enhanced environment - improved response. The government needs to play a 'catch up' role to that of the private sector in terms of e-commerce and to that of other countries.

The ultimate benefits of e-government are illustrated as follows:



E-governance Does Not Only Hold Economic Potential...

Stronger Society

Stronger Economy

Better Informed, Connected Citizens

Increased Productivity

Awareness Govt Online

Core Element of 21st Century Knowledge-Based Economy/Society

...but social potential as well!

13.5.1 E-Procurement:

By using e-commerce applications, for instance in procurement, it has been observed that the impact on operations and service delivery will be considerable.

Given that government is the largest purchaser of products and services to the value of more than R65 billion a year

, Internet-based e- procurement solutions will present the following benefits:

- reduced prices of materials
- shortened acquisition and fulfilment cycle
- decreased administration burdens and cost
- improved inventory practices; and increased control over maverick purchases

13.6 WHAT ARE THE SUCCESS FACTORS

Ingredients for Success:

- A clear vision
- Achievable targets
- String political and bureaucratic leadership
- Incentives to encourage take-up and adoption
- Investment
- Partnerships
- Enabling infrastructures
- Common branding and marketing

Political and Bureaucratic Leadership

Leadership is essential to ensure success in developing e-government initiative. The grade scale and horizontal nature of the initiative requires strong, high-ranking political and bureaucratic leadership, as evident in the approach taken by the US, UK, Australia and Singapore. Each of these countries has high ranking political leadership – being either the head of state (i.e. Prime Minister) or the second in command (i.e. Vice President) as leader.

Investment

Implementing the government on-line strategy will require a sustained government-wide effort over a number of years in collaboration with provinces, municipalities and third party delivery partners. Departments will have to re-engineer programs and processes in the transition to electronic service delivery, while maintaining all other delivery channels. Success will depend on major investments of both time and money.

Partnerships

There is a need to develop solutions and policies collaboratively with government, citizen and industry partners. Need to address digital divide between government (which is only moving tentatively into digital operations) and the commercial sector into e-commerce)

13.7 HOW TO ACHIEVE E-GOVERNMENT

To transform government into information age government a range of new frameworks and strategies across government need to be developed:

Knowledge-based Workplace: Public servants at all levels must be info-communication literate and tap the power of ICTs to improve work processes, service delivery and teamwork

Change Management – Employees need to change attitudes – for employees to change, they must understand what e-government is; be equipped with skills to implement e-government; must be willing to implement e-government solutions.

Upgrading of the government's common Information Management/IT infrastructure and an integrated and coherent IT Strategy for government: - IT systems have tended to be developed separately by different Departments. They should converge and inter-connect.
Adaptive and Robust Info-communication infrastructure: A well-designed, reliable and scalable infrastructure is critical for supporting e-government.

Data Standards – standards should be developed to present the data the systems hold in a common way (interoperability).

Roll-out of government Public Key Infrastructure – This is critical for providing security and therefore building trust among users. Digital signatures can provide a means of identification and authentication when conducting business with government and when transmitting sensitive and confidential information over networks. Legislation in this respect is important to ensure legal equivalence between digital and paper signatures and to enable government transactions

Electronic Service Delivery: All public services that are suitable for electronic delivery should be identified and re-engineered accordingly. The starting point is to do an audit of the existing services that are currently being offered by various departments and work out savings that can be accrued to government if the same service was to be offered electronically.

Access points: Government services which can be electronically delivered will be accessed through call centres, mobile phones, digital TV, MPCCs, telecentres, kiosks, smart cards as well as through personal computers.

Websites – to bring a more coherent and uniform approach for presenting and giving government information to the public (same look and feel). Government Communication and Information System (GCIS) needs to develop and publish guidelines and standards for government websites.

Government gateways and portals – Instead of launching online services on a department-by-department basis, they can be aggregated across departments, accessible by using a common portal.

13.8 WHERE WE ARE - EXISTING E-GOVERNMENT INITIATIVES

Government departments have set up web sites and employees have PCs and connectivity to each other and globally through the Internet. Departments have separately begun projects aimed at facilitating e-government. However, much still has to be done As a starting point, government has to articulate clear vision, mission, goals and set up achievable targets in the e-government strategy to be developed.

Below is a list of some of the projects being undertaken by various departments:

- Department of Communication (DoC): Info.Com 2025 Strategy
- DoC: Public Information Terminal
- E-commerce Policy
- E-procurement Portal
- DoC Public Key Infrastructure Pilot
- 107 Communications Emergency Centres
- SA Portal (Tourism)
- Government Call Centre
- Department of Home Affairs: Hanis Project – Smart Cards
- DTI: SAITIS
- GCIS Website- Government –on-line
- GCIS Extranet Project
- Department of Justice electronic database of criminal records and procedures
- South African Revenue Service on-line tax system
- Department of Labour Electronic One Stop Service Infrastructure
- Department of Arts, Culture, Science and Technology White paper on Science & Technology
- Department of Welfare: Re-engineering of Welfare payment system – Free State
- Department of Health: Telemedicine Project
- Gauteng Provincial Government: e-Procurement Pilot Project
- State Tender Board Office (national): e-Procurement Initiative
- Other Departments projects/initiatives to be listed

Departments are requested to list other government-related initiatives toward e-government.

QUESTIONS FOR POLICY CONSIDERATION

1. *Should government establish explicit e-government targets?*
2. *What should government do to accelerate the transformation to e-government?*
3. *What types of services do citizens and businesses want to see on-line?*
4. *What more should government be doing to use e-commerce to enhance its service delivery and administration?*
5. *How can the private sector contribute toward creating e-government?*

GLOSSARY OF TERMS

Application: a computer program, which performs a set of tasks forming a defined function or service.

Authentication: a mechanism of using information resources to verify the claimed identity of a party to a transaction or an entity involved in a transaction.

Authorisation: an authentication process whereby predetermined rights, including access to information resources, are granted to users or entities

Bandwidth: measure of the capacity of a communications channel, expressed in bits per second

Broadband: this transmission medium allows transmission of voice, data and video simultaneously at higher transfer rates. Broadband transmission media generally can carry multiple channels.

Browser: software on the client's PC used to fetch/read documents from the Web, display them on-screen and print them, jump to others via hypertext, view images and listen to audio files

ccTLD: country code Top Level Domain refers to a high level Internet Protocol address to identify a country e.g, za for South Africa

Confidentiality: reasonable assurance that online or stored data cannot be viewed and interpreted by any person other than an authorised one.

Connectivity: The capability to provide, to end users, connections to the Internet or other communications networks

Cyberspace: the Internet/ electronic/ digital environment

Certification Authority: a secure third party organisation or company that issues digital certificates used to create digital signatures and public key pairs. Certificate authorities guarantee that the two parties exchanging information are really who they claim to be.

Certificate: a certificate is a public key that has been digitally signed by a trusted authority to identify the user of the public key. SET uses certificates to encrypt for example payment information.

Click wrap contracts: Contracts concluded in an online environment, usually the Internet, where the terms of a contract are set out and "offered" by one party on a website and the other party indicates "acceptance" of those terms by for example clicking on an "accept" button or icon and hence concluding the contract

Copyright: the right to retain or sell the rights to an artistic work. Copyright is a form protection to the authors or "original works of authorship" including literary, dramatic, musical, artistic, and certain other intellectual works.

Cryptography: practice of digitally "scrambling" a message using a secret key or keys.

Device: any electronic gadget with an ability to receive input (via a keyboard, or voice) or give output (via screen, or voice, etc.)

Digital: the representation of data by the bits and bytes of binary code. Vinyl records and cassette music tapes carry analogue media

Digital Divide: a term used to reflect the technological gap between countries that have fully exploited ICT and those that have not. The digital divide is often associated with the resulting gap in terms of economic development.

Digital Certificate: See Certificate

Digital Signature: Digital codes that can be attached to an electronically sent message to uniquely identify the sender.

Domain name: A unique name, which represents each computer on the Internet.

Domain Name System: The technical administration and allocation of domain names

EDI: Electronic Data Interchange - is a de facto standard format for exchanging business data between companies computer application in a standardised form, but usually refers to as proprietary system of delivery.

Electronic Fund Transfer - the electronic movement of money over secure private networks between banks' accounts

Electronic Money: means of retail payments executed over Internet, which leaves other traditional electronic payments outside of its scope. Alongside with most commonly used smart card the term include: e-cards, trade cards, traditional credit, debit and stored value cards, as well as e-cash, digicash, digiwallet, e-credit, e-loans etc.

Electronic payments system: an array of institutions and mechanisms ensuring the cash flow through electronic communications and timely provision of credit and settlements of debts at much less than traditional system could provide costs

Extranet: a website links businesses to customers, suppliers, etc. for electronic communications.

Encryption: the coding of data for the purpose of security or privacy

Gateway: the link between networks and computers which allows messages to be routed across. Often associated with security measures.

Hardware: the physical pieces of computer equipment needed to make up a system.

Hosting: the storage and maintenance of the data making up the content of Websites.

Hyperlink: a reference link that can be made from a point in one web page (traditionally in blue and underlined) to any other point on any web page on the World Wide Web.

ICT: Information and Communication Technologies – a generic term used to express the convergence of information of information technology and communications. One prominent example is the Internet

Information-based economy: refers to a country or region where ICT is used to develop economic foundation and market transactions

Interconnection: The connection with each other of the telecommunications networks of different operators so that signals or services are transported over such interconnected networks.

Intellectual Property: comprise two main branches: industrial property, which is chiefly in inventions, trademarks, and industrial designs and appellations origin; and copyright; chiefly in literary, musical, artistic, photographic and audiovisual works.

Integrity: reasonable assurance that stored or online data which its intended destination without being modified in any unauthorised manner.

Internet: the Worldwide collection of networks communicating through common languages and protocols. Also the basic infrastructure for the new economy over which information can be transferred, transactions made and work done

Internet Service Provider: companies that specialise in linking organisations and Individuals to the Internet as well as providing services to them

Intranets: using the same Internet technology, but hosted by private servers not accessible by the public over the Internet. Companies are using Intranets to facilitate their internal knowledge management, communication, collaboration on projects, HR functions, etc.

IP address: the address which all computers and websites have to have on the Internet

Knowledge-based economy – refers to a country or region where ICT is extensively used to enhance knowledge of society in general so that higher human capital brings further improvement to the economy

Local loop: this portion of the telecommunications network physically connects end users to the central office network and generally is dedicated to that particular user.

Multimedia: an interactive combination of text, graphics, animation, images, audio and video displayed by and under the control of a PC

Public key cryptography: this encryption method requires two unique software keys for decrypting data, one public and one private. Data is encrypted using the published public keys and the unpublished private keys are used to decrypt the data.

Portal: website which aims to be the starting point though which one enters the Web.

Personal data: is any data, which refers to an identified or identifiable individual, which is not otherwise readily available via a public source(s).

Permanent Establishment: a fixed place of business through which the business of an enterprise is wholly or partly carried on.

Repudiation: when a customer in a credit card transaction denies having been a party to that transaction.

Server: usually computer hub of a network, fulfilling servers' functions to client computers connected to it, such as storing files and databases and running applications.

Shrink wrap contracts: Same as click wrap contracts except for the fact that the accept icon is actually a shrinked box containing the actual product or service itself e.g. software. Accepting this type of a contract results in an immediate on-line consumption

Smart Card: card containing memory and a microprocessor, that can serve as personal identification, credit card, ATM card, telephone credit card, critical medical information record and as cash for small transactions.

Software: computer programming which gives the hardware its usefulness through various functions the software can perform.

Teledensity: teledensity refers to the number of telephone lines per 100 people, s rough measure of the ubiquity of the public switched telephone network in a country.

VPN: Virtual Private Network - a VPN is a part of the public Internet to which access is controlled by firewalls and secure tunnels to enable private and secure use by authorised users

Website: pages of information linked to one another by hyperlinks (usually organised around a menu), with the main page (usually including the menu) bearing the domain address. These pages are on a Web server and are accessible from any browser on the World Wide Web.

World Wide Web: a collection of information located in many Internet servers that can be accessed with a browser or by navigating via hyperlinks.

World Wide Web and other References

The following references identify key resources, documents, and policy information on the World Wide Web, concerning each of the main issues and sub-issues involved with the development of National Electronic Commerce Policy for South Africa. In most cases, the main referenced sites also point to other documents and resources on the Web, which further elaborate the issues, from the perspective of various governments, international organizations, and individuals.

UNCITRAL Model Law on Electronic Commerce
http://www.un.or.at/uncitral/texts/electcom/ml-ec.htm
Text and references for the UNCITRAL Model Law, adopted and proposed in numerous countries.

ECEG (1998) ‘Electronic Commerce: Building the Legal Framework’ Electronic commerce Expert Group, Commonwealth Attorney-General’s Department 31 March 1998 at
http://www.law.gov.au/aghome/advisory/eceg/

Law and the Internet: Electronic Contracting
http://www.ljx.com/internet/zammit.htm
New York Law Journal article on legal aspects of electronic contracts.

Report on Electronic Commerce Legal Issues by Edward Nathan and Friedland
www:ecomm-debate.co.za/docs/report.html

OECD Ministerial Conference (Ottawa) Tax Policy Home Page
http://www.oecd.org/daf/fa/e_com/ottawa.htm
Links to all major papers and policy discussions of the 1998 Ottawa OECD Ministerial Conference that focused principally upon e-commerce tax issues.

U.S. Internet Tax Freedom Act
http://www.ljx.com/internet/hr1054_105.html
Full text plus relevant links for U.S. law restricting application of new taxes to Internet-based commerce.
Australian Tax Office Electronic Commerce Project
http://www.ato.gov.au/ecp/index.html
Home Page for the 1996 ATO initiative which conducted a comprehensive review of Australian tax laws as related to electronic commerce.

Veritex "Tax Cybrary" Cyber Tax Channel
http://www.vertexinc.com/taxcybrary20/CyberTax_Channel/taxchannel_70.html
Summary and links for U.S. state-level tax policies and information relating to Internet commerce.
World Trade Organization Declaration on Global Electronic Commerce
http://www.wto.org/anniv/ecom.htm
Text of 1998 WTO Declaration of intent to institute a comprehensive work programme on trade-related aspects of global electronic commerce.

Europe proposes a customs free web
http://www.techweb.com/wire/story/TWB19980222S0001
Article about European Union proposal to prohibit customs duties on Internet transactions.
World Intellectual Property Organization (WIPO) Electronic Commerce Home Page
http://www.wipo.org/eng/internet/ecommerc/index.htm
Home page for WIPO treatment of e-commerce issues, with comprehensive background and reference information.
World Trade Organization (WTO) Intellectual Property Home Page
http://www.wto.org/wto/intellec/intellec.htm
Home page for WTO treatment of intellectual property issues and trade, including the global treaty on Trade Related aspects of Intellectual Property rights (TRIPS) Agreement.
"Business on the Internet is Laden with Intellectual Property Risks"
http://www.ljx.com/internet/0318inbiz.html
New York Law Journal article on Intellectual Property concerns involved with electronic commerce.

Australian National Advisory Council on Consumer Affairs (NACCA).
http://www.isr.gov.au/consumer/eleccomm/html/protect.html .)

Australian Review of Policy relating to Encryption Techniques (The "Walsh Report", 1992), section 3.7.6:

Dorothy E. Denning in her paper *CFP '93 – To Tap or not to Tap* (ACM **36** (1993), pp 24 – 30), the report of the Electronic Privacy Information Center (EPIC) entitled *Cryptography and Liberty 1999*
http://www.oecd.org/dsti/sti/it/secur/prod/crypto2.htm

UK government has taken: According to a *Draft Regulatory Impact Assessment* of the *Draft Electronic Communications Bill* (DTI, July 1999, Unique Reference Number URN99/1020):

U.S. *Cyberspace Electronic Security Act* of 1999

American Bar Association's Digital Signature Guidelines *(1996)*

Privacy Protection on Global Networks
http://www.oecd.org/dsti/sti/it/secur/act/privnote.htm
Official source for OECD positions on privacy issues in global telecommunications. Refers to seminal 1980 policy guidelines on privacy and transborder data flows. Offers summaries of, and links to, all recent OECD position papers, discussion documents, and work group outputs from conferences dealing with privacy issues.
Privacy and the National Information Infrastructure
Safeguarding Telecommunications-Related Personal Information
http://www.ntia.doc.gov/ntiahome/privwhitepaper.html
Official Paper of the Unit ed States National Telecommunications and Information Administration (NTIA) of the Department of Commerce, issued in October 1995. Emphasise issues of privacy in relation to personal data obtained through use of telecommunications and information services. Seeks minimum industry standards, largely through self-regulation, to require notification of users by service providers about their privacy policies, and consent of users for dissemination of their personal data.

Privacy and Electronic Commerce
http://www.doc.gov/ecommerce/privacy.htm
More recent policy paper (June 1998) by the United States Department of Commerce on privacy issues generally involved with e-commerce. Describes international consensus on principles for privacy protection, and options for implementing those principles (legislative vs. self-regulation). Identifies the U.S. policy approach as a combination of these methods. Also includes useful international examples and survey of basic questions to be raised in establishing a national policy.

Electronic Privacy Information Center (EPIC)
http://www.epic.org/
Home page of the EPIC, an advocacy group based in the U.S. Takes strong positions in favour of protecting privacy and consumer rights in Internet and related technology settings. Links to other international privacy advocacy organisations.

Security, Privacy and Intellectual Property Protection in the Global Information Infrastructure
http://www.nla.gov.au/archive/gii/oecdconf.html
Proceedings of a joint conference between the OECD and the government

of Australia on privacy and other Internet data protection issues, held in 1996. Links to papers and other resources discussing these issues.
Consumer Protection in the Electronic Marketplace
http://www.oecd.org/subject/e_commerce/ebooks/ecomm1_4.pdf
An OECD summary document (in .pdf format) concerning consumer protection issues relating to electronic commerce.
Germany Information and Communication Services Act
http://www.ljx.com/internet/11-12germany.html
Detailed summary of comprehensive 1997 German legislation on all forms of electronic communication. Contains a variety of consumer protection provisions, including liability of ISPs, prohibition of certain content (hateful, inciting violence, etc.), and protection of children.
Consumer Protection and Private International Law in Internet Contracts
http://rw20mit4.jura.uni-sb.de/RSchu/public/essay.htm
Academic research paper on consumer protection issues relating to the Internet, specifically in the context of international commerce.
Unsolicited Commercial Electronic Mail Choice Act of 1997
http://www.lclark.edu/~loren/cyberlaw97/avison/s771.htm
Summary of and reference to a draft U.S. legislative bill concerning "spam" or unsolicited electronic mail advertising.
Law Journal Extra, on e-mail legislation and litigation
http://www.ljx.com/internet/iremail.html
An on-line law journal focusing specifically on laws and litigations surrounding electronic mail and consumer protection issues, principally in the United States. Links to details of many laws and cases.
The OECD Cryptography Policy Guidelines and the Report on Background and Issues of Cryptography Policy
http://www.oecd.org/dsti/sti/it/secur/prod/e-crypto.htm
Two reports, on background information and issues surrounding cryptography policy, and the official guidelines developed by the OECD for member countries to design cryptography laws. Dated March 1997.
EU Data Protection Home Page
http://www.ispo.cec.be/ecommerce/dataprotect.html
Links to the most recent Directives of the European Commission on data protection policy.
U.K. Proposals for Encryption on Public Telecommunications Networks
http://www.coi.gov.uk/coi/depts/GTI/coi9303b.ok
Summary of proposals released by the Government of the UK (June 1996) for addressing data protection and encryption issues. Includes discussion of "regulatory intent" for the use of encryption in public networks.

Utah (1998) 'Frequently Asked Questions Regarding Digital Signatures' at http://www.commerce.state.ut.us/web/commerce/digsig/dsfaq.htm

Digital Signatures and Digital IDs
Verisign, Inc.'s overview of Digital signatures and IDs, technology and options.
Digital Signature Law Survey
http://cwis.kub.nl/~frw/people/hof/DS-lawsu.htm
A survey of digital signature legislation around the world.
EU Digital Signatures and Encryption Home Page
http://www.ispo.cec.be/eif/policy/Welcome.html#digital
Includes policy papers of the European Internet Forum, and the Proposal of the European Commission for a European Parliament and Council Directive on a common framework for electronic signatures.
Legal and Regulatory Issues concerning the TTPs and Digital Signatures
http://www.cordis.lu/infosec/src/study2.htm
A study sponsored by InfoSec of Europe to survey and evaluate the status of laws regarding digital signatures and trusted third parties in all European Union member states.
Japan Certification Authority Guidelines
http://www.ecom.or.jp/eng/output/ca/eng-guideline.htm
Document issued by the Electronic Commerce Promotion Council of Japan, which presents guidelines for the operation of a certification authority.
Certification Authorities for E-commerce - Public or Private?
http://www.uniforum.org.nz/conferences/1998/papers/bradshaw.html
Paper by Roger Bradshaw, New Zealand discussing the merits of public versus private sector control of certification authorities.
The Role Of Certification Authorities In Consumer Transactions
http://www.ilpf.org/work/ca/draft.htm
A report of the Internet Law and Policy Foundation (ILPF) Working Group On Certification Authority Practices; draft dated April 14, 1997
An Introduction to Certification Authorities and Public Key Cryptography
http://www.anl.gov/ECT/certify/CA-Overview.html
Paper prepared by Bill S. Halsey, Argonne National Laboratory (U.S.); revised October 2, 1996. Describes the main functions of Certification Authorities and the role of public

Department o f Communications (South Africa)
http://www.ecomm-debate.co.za
United States Government E-Commerce policy
http://www.ecommerce.gov/internat.htm
European initiative on E-Commerce
http://www.cordis.lu/esprit/src/ecomcom.htm
Organisation for Economic Co-operation and Development (OECD)
http://www.oecd.org

World Trade Organisation (WTO)
http://www.wto.org
International Telecommunication Union (ITU)
http://www.itu.int
World Intellectual Property Organisation
http://www.wipo.int/index-eng.html
Internet Engineering Task Force (IETF)
http://www.ietf.org/
Canadian Model
http://e-com.ic.gc.ca/english/index.html
Singapore Model
http://www.ec.gov.sg/
E-commerce in Japan
http://www.ecom.or.jp/ecom
New Zealand Ministry of Foreign Affairs and Trade
http://www.mfat.govt.nz
APEC E-com Legal Guide
http://www.bakerinfo.com/apec/Apecpar1.htm
Afrinic
www.afrinic.org
Internet Society of South Africa
http://www.isoc.org.za

Off-line References:

1. Media Africa com. 2nd SA Web Commerce Survey 1999

2. The 1999 South African Electronic Commerce Survey by BMI-TechKnowledge Group

3. Building Confidence: Electronic Commerce and Development, United Nations Conference Trade and Development, 2000

4. Knowledge Societies: Information Technology for Sustainable Development, by Robin Mansell and Uta Wehn, 1998

5. OECD document: A Global Action Plan for Electronic Commerce, October 1999

6. Jeffrey Reisner, in an article in The Internet Newsletter (January 1997)

7. The EU Directive 97/7/EC on The Protection of Consumers in Respect of Distance Contracts

8. Article: Development of a Secure Electronic Marketplace for Europe by M. Waidner.
   ESORICS '96 (4th European Symposium on Research in Computer Security), Rome, INCS 1146, Springer-Verlag, Berlin 1996,1-14

9. Article: State of the Art in Electronic Payment Systems by N Asokan, P Janson, M Steiner, M Waidner
   IEE COMPUTER 30/9 (1997) 28-35

10. Report on Digital Rights Management Technologies for the International Federation of Reproduction Rights Organizations

11. Germany's Digital Signature Act: Federal Bill establishing the General Conditions for Information and Communication Services: Bundestagsdrucksache 13/7934 vom 11.06.1997

Local Academic Papers Commissioned by the Department of Communications:

The Department of Communications had invited members of the academic community and other experts in the field of e-commerce to provide in-depth perspectives on various aspects of e-commerce. The ten papers were prepared and will provide readers or individuals with detailed information on each subject. The papers are available at the following website: **http://www.ecomm-debate.co.za**

1. Select Intellectual Property Implications of Electronic Commerce and Global Information Networks: Copyright, Trade Marks, and Databases by Coenraad Visser (**vissercj@unisa.ac.za**)
2. Domain Names: A Legal Model for their Administration, and their Interplay with Trademarks by Coenraad Visser and Brian Rutherford
3. Contracting on the Internet: The Formation of Contracts, Trade Practices and Online Dispute Resolution by Tana Pistorius (pistot@unisa.ac.za)
4. A Comparative Survey of Legislative Initiatives on Select Aspects of Electronic Commerce by Tana Pistorius.
5. E-commerce and issues in the law of privacy by Julian Hofman (hofman@law.uct.ac.za)
6. Cryptographic Dilemma: Possible Approaches to Formulating Policy in South Africa by Vivienne Lawack-Davids (**lwaval@upe.ac.za**)
7. In the Technology and Economics of the Next Generation Public Network: Regulatory Implications by John Joslin (**johncj@icon.co.za**)

8. Evolution of the Electronic Communications Regulatory Framework in the European Union by John Joslin
9. E-commerce and Poverty Alleviation in South Africa by Aki Stravrou, Julian May and Peter Benjamin (akidra@iafrica.com).
10. Electronic Commerce Strategies for Small, Medium and Large Businesses by Andy Bytheway (abytheway@uwc.ac.za) and Yvette Goussard