ENCRYPTION TECHNOLOGY TO ADDRESS VALIDITY IN TRANSACTIONS USING THE GII

BY

ANTON HENDRIK GERBER

SHORT DISSERTATION

SUBMITTED FOR THE PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE

MASTER OF COMMERCE

IN

COMPUTER AUDITING

IN THE

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

AT THE

RAND AFRIKAANS UNIVERSITY

STUDY LEADER: PROF A DU TOIT

JOHANNESBURG

NOVEMBER 1997

ACKNOWLEDGEMENTS

Opinions expressed are those of the author. I also declare that this short dissertation has not been submitted for any other degree to any other university.

I wish to thank the people closest to me for their moral support and encouragement during my studies.

I would like to thank my study leader, Prof Du Toit, and also Prof Boshoff for their guidance and assistance and for introducing me to this fascinating field of research.

INDEX

AFRIKAANSE OPSOMMING

TITEL

ENKRIPSIETEGNOLOGIE OM DIE GELDIGHEID VAN TRANSAKSIES OP DIE GLOBALE INLIGTINGS INFRASTRUKTUUR TE VERSEKER

DEUR

ANTON HENDRIK GERBER

OPSOMMING VAN DIE SKRIPSIE INGEDIEN TER GEDEELTELIKE VERVULLING VAN DIE VEREISTES VAN DIE GRAAD MAGISTER COMMERCII IN REKENAAROUDITERING IN DIE FAKULTEIT EKONOMIESE EN BESTUURSWETENSKAPPE AAN DIE RANDSE AFRIKAANSE UNIVERSITEIT

STUDIELEIER: PROF A DU TOIT

JOHANNESBURG

NOVEMBER 1997

PROBLEEMOMSKRYWING EN DOEL VAN NAVORSING

Die ontwikkeling van elektroniese sake het tot gevolg dat al hoe meer transaksies in die sakewêreld deur elektroniese data interskakeling en die Internet gedoen word. Die ontwikkeling het die vraag laat onstaan of daar 'n sekuriteits tegnologie beskikbaar is wat sal verseker dat geldigheid en integriteit van transakies verseker kan word .

Die noodsaaklikheid van so 'n tegnologie het belangriker geword met die aankondiging dat 'n Globale Inligting Infrastruktuur (GII) die volgende doelwit in die ontwikkeling van kommunikasie gaan wees. Die infrastruktuur sal nie net gebruik word vir elektroniese sake nie, maar sal ook as medium gebruik word in die onderwys, gesondheid, ontspanning en sal verskillende wêreldwye netwerke insluit.

Enkripsie is een van die tegnologieë wat beskikbaar is om data transaksies' te beveilig gedurende die versending oor kommunikasie lyne of media en kan selfs gebruik word om ongemagtigde toegang te verhinder gedurende die stoor van data. Enkripsie behels die omskakeling van transaksies deur middel van sleutels tot onverstaanbare "geheime skrif" voor versending en dan weer die omskakeling na die volledige inligting by ontvangs.

Die volgende probleme bestaan tans wat aangespreek moet word:

- Wat die beste en koste doeltreffendste oplossing is om die sekeriteits behoeftes van besighede aan te spreek;
- Die regsgeldigheid en wetlike aspekte van privaatheid en sekuriteit van transaksie oor die GII moet aangespreek word;
- Die versending van die geheime sleutels wat tot enkripsie lei sal in die toekoms deur elektroniese en digitale mediums aan die ontvanger gestuur word wat sal noodsaak dat die sekuriteit gedurende versending baie belangrik sal word;
- Standaarde en infrastrukture sal in plek gestel moet word om die suksesvolle ontwikkeling van die GII te verseker; en

- Huidige interne en eksterne oudit modelle sal die ontwikkeling van die nuwe tegnologie kan hanteer maar die toepassingsbenaderings en toetse wat uitgevoer sal word om geldigheid, volledigheid, akkuraatheid en bestendigheid van data transaksies te verseker, sal verander, ontwikkel en nagevors moet word.

Al bogenoemde punte behalwe die regsgeldigheid and wetlike aspekte, word in the skripsie aangespreek. Elkeen van die punte kan egter dien as 'n onderwerp vir verdere detail navorsing.

Die skripsie word toegespits op die enkripteringstegnologie wat beskikbaar is om die geldigheid van transaksies wat deur die GII versend word, te verseker. Die doel van die skripsie is om 'n vraelys saam te stel wat die ouditeur kan gebruik as riglyn wanneer 'n oudit uitgevoer word in 'n besigheid wat the GII of internet gebruik.

NAVORSINGSMETODIEK EN BEPERKINGS

Die navorsing is gedoen deur middel van 'n literatuurstudie van boeke, tydskrifte en die Internet oor kriptering, elektroniese sake, GII en oudit modelle wat tans beskikbaar is, asook die verwagting van toekomstige ontwikkelings, soos vervat in die literatuur.

Die navorsing is beperk tot kriptering van finansiële transaksies gedurende versending. Die wiskundige modelle en grondslae van kripterings modelle is nie nagevors nie. Die ander beveiligings meganismes wat as totale sekuritietspakket gebruik moet word om 'n besigheid se data te verseker, is nie ingesluit by die navorsing nie. Daar is ook net gekyk na die versekering van geldigheid van transaksie en nie na die ander oudit doelwitte nie.

RESULTATE

Die GII sal ontwikkel tot die infrastruktuur van die toekoms wat die medium sal wees van menigte, indien nie alle elektroniese sake en vele ander gebruiksvelde, nie. Die potensiaal en markdeurdringing wat bereik kan word kan nou al reeds gesien word in die gebruik van die Internet wat maar net 'n deel van die GII sal uitmaak.

Enkriptering tegnologie is beskikbaar en ontwikkel nog steeds wat verseker dat die volledigheid van transaksies gedurende versending gewaarborg kan word. Die standaarde van kriptering wat benodig word, word al hoe meer wêreldwyd aanvaar en is ingesluit by die kommunikasie beleid vir die GII. Die sekuriteit van enkriptering word as gegewe aanvaar omdat die pogings benodig om 'n sleutel te breek groter is as die waarde van die transaksie self.

Finansiële transaksies kan beveilig word en volledigheid verseker word deur kriptering mits die bestuur en sekuriteit van die dekoderings sleutels verseker word. Die wye verskeidenheid van besigheids onsekerhede oor sekuriteit van transaksies oor die GII kan aangespreek word deur gebruik te maak van kriptering en ander sekuriteitstegnologieë.

'n Kort vraelys van items wat die sakeman en die ouditeur kan gebruik om seker te maak dat aandag gegee is en beleide intern ontwikkel is om beveiliging van transaksies deur enkripsie te verseker, is ook ontwikkel. Dit dien slegs as 'n riglyn en verskeie ander aspekte van sekuritiet moet ook oorweeg word.

GEVOLGTREKKINGS

Die beheer van die sleutels is van kardinale belang. Enkripsie verseker dat transaksies oor onveilige kommunikasiemedia gestuur kan word sonder dat die data verstaan sal kan word al word dit onderskep. Enkripsie bied een van die belangrikste sekuriteit tegnologieë wat gebruik kan word, saam met ander

beveiligingsmaatreëls om die vrese van besighede en regerings aan te spreek solank 'n wêreldwye aanvaarding van GII beleide en standaarde verlang word.

Verskeie ander aspekte soos in die probleemomskrywing uiteengesit is nie aangespreek in die navorsing nie en kan gebruik word vir verdere navorsing veral in die veld van die oudit van transaksies en die daarstelling van 'n totale sekuriteits pakket vir die besigheidsman wat doelmatig en effektief, maar ook bekostigbaar, is.

ENGLISH SYNOPSIS

PROBLEM DESCRIPTION AND OBJECTIVES OF THIS SHORT DISSERTATION

The development of electronic commerce resulted in the development of EDI and the use of the Internet to transact these data. This led to the question of whether a security technology existed that could ensure the validity and integrity of transactions.

The development of the GII which will not only be used for EDI and other financial transactions, but also in the medical and educational fields, has emphasised this concern of business.

Encryption is one of the technologies available which can ensure the validity of transaction during transmission and even during storage. Cryptology entails the encoding and decoding of transaction data before and after transmission through the use of secret and public keys.

The following questions should be addressed:

- The most cost effective solution to business' security concerns;
- The legal and regulatory issues concerning privacy;
- Transmission of keys through digital and electronic media resulting in the possible breach of security in the keys themselves;
- Standards and infrastructures which must be agreed upon and implemented to secure the development of the GII; and
- Existing internal and external audit methodologies can cater for the audit of the completeness, accuracy, validity and continuity of transactions but the methods and tests to substantiate these objectives will have to change.

All of the above points are addressed in the research, except those on the legal and regulatory issues. Each of these points can, however, still be the topic for detailed future research.

The objective of this dissertation is to research encryption technology to provide a questionnaire to the auditor ensuring the validity of transactions on the GII. A questionnaire or checklist is presented that could be serve a guideline for auditors when addressing risks in a GII environment.

RESEARCH METHODOLOGY

The research was conducted through a literature survey of existing textbooks, articles and Internet information in the fields of encryption, GII, EDI and audit models.

SCOPE AND LIMITATIONS

The research and the scope were limited to financial transactions during transmission. The mathematical models used in encryption were not researched. Other technologies available which should be used to ensure a total security package have also not been included in this research. The validity objectives of transactions were researched and not the other audit objectives.

RESULTS

The GII will develop into the infrastructure of the future through which EDI and electronic commerce will be conducted by most if not all businesses. The market potential can already be seen in the use of the Internet which will form a part of the GII.

Encryption technology is available and is developing to ensure validity of transactions during transmission through these infrastructures. The standards are increasingly becoming more acceptable and conventions and agreements are being developed and signed worldwide. Encryption technology is accepted as a secure method to ensure data privacy as the effort required to break the stronger keys is exponentially higher than the value of the data itself.

Financial transactions can be secured by encryption only if the keys are managed and secured in a responsible manner. This should then address the privacy concerns of businesses.

A short questionnaire has been developed to use as a guide to ensure that consideration is given to aspects that will impact on the decision of which security mechanism and policy to select.

CONCLUSION

The control of the keys is even more important than the encryption itself. Encryption ensures that data can be transmitted and will be of no value even if it is intercepted without the keys. This technology is one of the most important mechanisms that can address the validity concerns of businesses and which will lead to the development of the GII.

Many other fields of research as indicated in the problem description must also be addressed to ensure the acceptance of the GII for conducting electronic commerce. A specific audit technology and approach should be researched as well as the formulation of a complete security package that is effective and efficient but also cost effective.

1. INTRODUCTION

This chapter provides an introduction into the research conducted and the results of the research. This is discussed under the following headings:

1.1 BACKGROUND

The development of new technologies over the past few years has accelerated at an ever increasing rate. This has resulted in a rapid change in the business environment and even electronic data interchange (EDI) and the Internet will be replaced in the near future by the further development of the Global Information Infrastructure.

"The global information society has arrived. It is borderless, unconstrained by distance and time. Our economies, politics and societies are based less on geography and physical infrastructure than previously, and increasingly on information systems infrastructures" (OECD, 1992:8).

The concept of *"using technology to control technology"* is researched and user controls are only investigated as compensating controls. The

concepts of user and integrity controls are well documented by the institutes governing auditing standards, such as the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA) and the South African Institute of Chartered Accountants (SAICA). The controls objectives are as follows (Damianides, 1991:5):

- COMPLETENESS of input, processing, updating and output
- ACCURACY of data both in transient and static state
- AUTHORITY/VALIDITY of business processing
- CONTINUITY to ensure it is working and continues to work as intended.

The objectives of confidentiality, integrity and availability must be balanced against priorities of the business such as cost, efficiency and risks associated with breaches of information technology. The controls and policies should be sufficient to ensure that the cost spent in implementing and maintaining security is less than the potential loss of an intrusion or loss of data (OECD, 1992:4).

With the development of new technologies such as the Internet and the Global Information Infrastructure, the distinction between the physical world and the digital world is becoming less clear. Technology is starting to drive changes in the business environment and this results in the evolution and re- engineering of businesses across the world. The correlation between the development of the business environment and the development of technology is depicted in figure 1.1 where the vertical axis represents the movement in time and the horizontal axis the development in business and information technology. The rapid development of technologies particularly in the information field has paved the way for business re-engineering and transformation. The typical business processes driving an organisation have developed from being based on individual actions to the current (and future) virtual

organisations and the accompanying technology from host centric computers to networks to the GII.

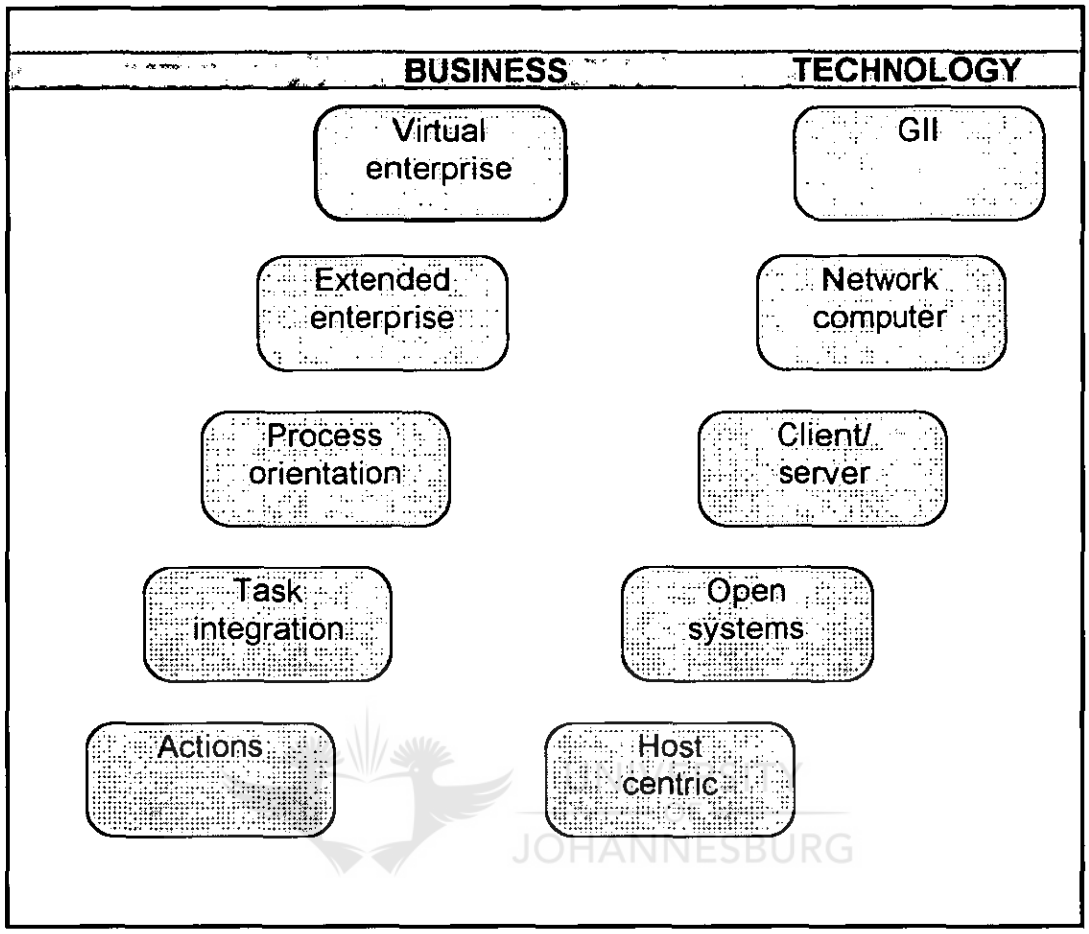

Figure 1.1 *Relationship between business and technology development.*

1.2 PROBLEM DESCRIPTION

With this rapid development and change in the business environment, the growing concern of businesses and auditors is the validity of transactions created by this change. Technologies have been developed to address these risks and concerns and an evaluation is required to determine whether encryption technology, as one of the control measures, is adequate, efficient and effective to deal with the

validity of transactions using the Global Information Infrastructure (GII). Security of communication and transactions starts with authentication and encryption (Kosiur, 1997:1).

Computer auditing will increase in importance and the computer model will change due to the development of the Internet and the GII. Management involved in businesses exploring the possibility of employing Internet and GII technologies in the running of their enterprises will have to address the risks and controls necessary to ensure that the above audit objectives are met. This must match the needs of the organisation and a planned approach should involve the following steps identified by the European Security Forum (1995:14):

- Establish goals for use of GII;
- Perform a risk assessment;
- Develop a policy;
- Determine appropriateness of technical solutions;
- Implement the solution/s;
- Verify the solution/s; and
- Maintain the solution/s.

By following this structured approach businesses can address the opportunities and risks associated with transactions on the GII.

The following problems currently exist in the field of technologies that will address the validity of transactions:

- What is the best and most cost-effective solution to business' security needs. There is a range of products and technologies available but which technology can address validity concerns even if the channels over which transactions are transmitted are insecure. To achieve confidentiality and integrity (defined as

validity) of information whilst in transit it will be necessary to use cryptographic techniques such as data encryption;

- There are legal and regulatory issues to be considered when using encryption and different laws are imposed by countries importing and exporting these technologies;

- At present the distribution of keys used in the encryption is performed manually but a number of alternatives are in various stages of development. (European Security Forum, 1995:18). Distribution can be provided through a TELNET connection with encrypted software, Dial-up connection via modem and terminal emulation software which are encrypted or even cellular phone connectability;

- Standards and frameworks must be in place to ensure a co-ordinated approach and uniform trading rules for all parties using the GII. There should be no barriers for transacting securely on the GII; and

- Either current internal and external audit models must be able to address the new technologies or new audit approaches and tools should be developed to cater for the needs of businesses transacting on the GII. Although methodologies would not change the approach and audit skills would have to progress into this new field.

The relative effectiveness of the solutions against individual threats, as well as the cost and maintenance requirements for the various technologies is summarised in figure 1.2.

SOLU-TION	DISCLO-SURE	UNAU-THO-RISED ACCESS	LOSS OF INTE-GRITY	DENIAL OF SERVICE	COSTS	ON-GOING MAINTE-NANCE
	RISKS					
Increase security of individual computers	**	****	***	*	$$$$	$$$$$
Firewalls	***	*****	*	***	$$	$$$$
Strong authenti-cation devices	*	*****	*	*	$$$$$	$$$
Internal network partitioning	**	*****	*	***	$$$$	$$$$$
Data encryption	*****	***	*****	**	$$$	$$
Digital signatures	*	**	*****	*	$$$$$	$$$

Figure 1.2 *Relative effectiveness of specific solutions in protecting against vulnerabilities. The more ***** the more effective the solution and the more $$$$$$ the more expensive the solution (European Security Forum, 1995:19).*

From figure 1.2 it can be seen that data encryption is most effective in mitigating disclosure and loss of integrity risks whilst at the same time it is not the most expensive technology to install and maintain. The table also indicates that data encryption and digital envelopes are the most effective to deal with the risk of loss of integrity or validity of data.

Due to the variety of technologies available and due to the uncharted waters opened up by the GII initiative as an expansion of the current Internet and EDI, I believe it is important to research the topic of this short dissertation to address the problems listed above.

1.3 OBJECTIVES OF RESEARCH

The research in this short dissertation will focus on encryption technology which is part of the cryptology technology available to secure validity of transactions on the GII.

The objective of this short dissertation is to determine what encryption technologies are available in the market today and to establish how effectively and efficiently they address the audit risk of validity of transactions within the framework of the Global Information Infrastructure (GII).

From this , a guideline or checklist is developed for the use by internal and external auditors and even business managers concerned with risks associated with transacting on the GII with specific reference to validity concerns of transactions.

1.4 SCOPE, LIMITATIONS AND EXCLUSIONS

"The GII is a new development in the thinking of global political and technological leaders and the potential for human and economic development is vast and disparate populations will experience these changes as part of the global community." (Gore, 1994). This development is the next step in the technological advancement from

closed systems to EDI to electronic commerce to Internet to GII (See figure 1.1).

The development of electronic transactions to electronic data interchange (EDI), to electronic commerce (EC), to the current Internet, and the next phase in technological development, the GII, can be graphically depicted in Figure 1.3. The Internet will be a part of the GII and so will EDI which can operate in the Internet, in the GII, by itself or in any of these infrastructures. The same can be said for electronic commerce of which EDI is but one part.

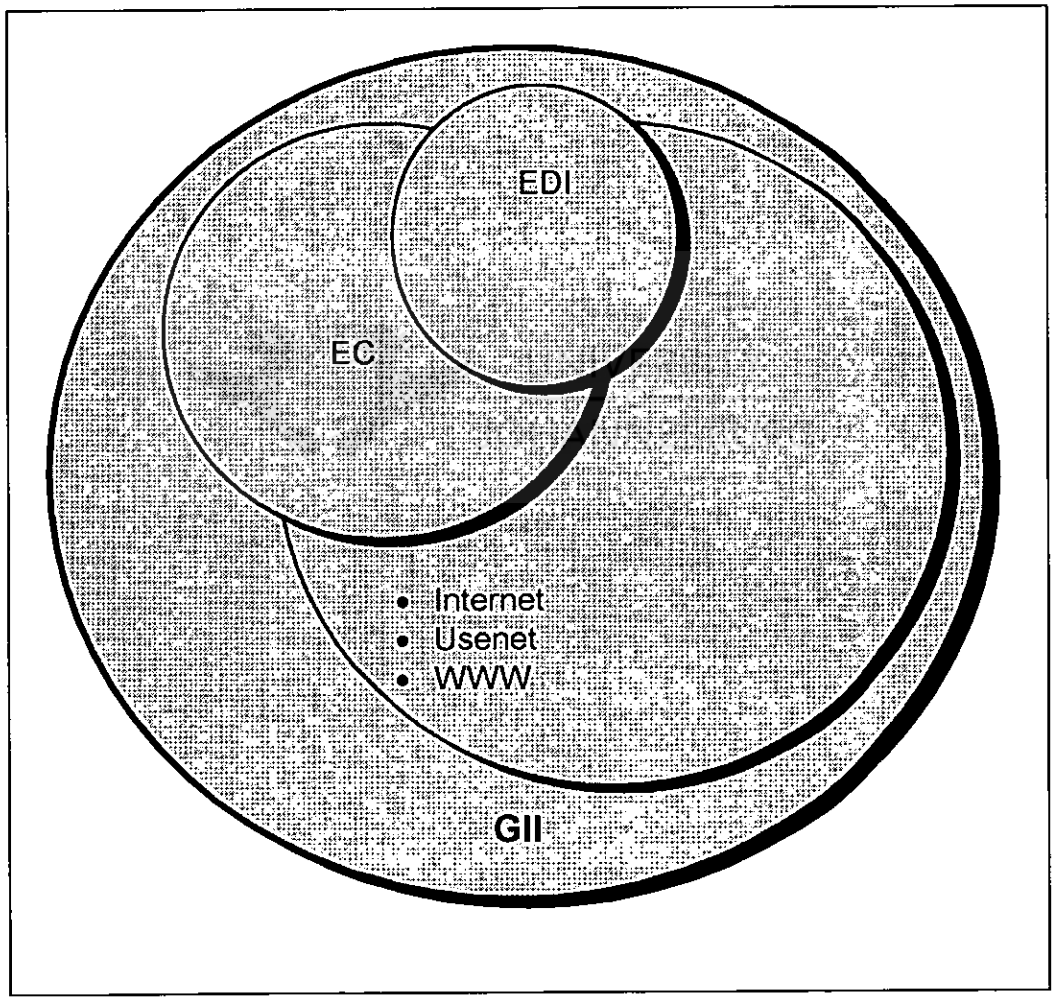

Figure 1.3 *Relationship between EDI, EC, Internet and GII.*

A transaction is part of EDI which is part of all the electronic trade tools which is again part of the EC which can operate on the Internet that will

become part of the GII (Van Aardt, 1995:8).

The scope of technologies that can address security risks of transacting on the Internet and the GII is wide and so are all the audit controls that need to be addressed in such an environment.

There is no one control measure built into the current Internet or GII infrastructure that will address all the risks associated with performing transactions (European Security Forum, 1995:19). The Internet and the GII rely on a combination of the following security measures (either hardware or software solutions) to address the risks:

- Passwords;
- Encryption;
- Screening routers and packet filtering;
- Dual homed hosts;
- Bastion hosts;
- Screened subnets;
- Application level gateways; and
- Firewalls.

Most of the solutions listed above deal with controlling the flow of information from one location to the other. A combination of all these techniques will be the most appropriate and will depend on a cost/benefit analysis linked to the perceived risks attached to each access program and hardware into the Internet.

This short dissertation will only focus on the following areas:

- Encryption technology;
- Validity of business transactions; and
- Global Information Infrastructure.

The scope of encryption technology is wide ranging and concentrates on the mathematical calculations of algorithms and standards. There are also detailed discussions in literature on the history and development of algorithms and their advantages and disadvantages. This will be summarised in this research and some of the latest frameworks will be discussed. The research will be concentrated on the practical functions required from a business and audit point of view to ensure validity in transactions. The calculation of algorithms falls outside the scope of this research and the detailed working of algorithms and the breaking of them are not researched.

A financial transaction relating to electronic commerce operating on the GII will be researched. This will only include the framework of the GII with its associated risks and not specifically any Internet protocols and security features. Technology will be limited to encryption only and not to other technologic tools available, even if they address validity of transactions to a certain degree. The research into encryption will be limited to the framework and models available and will not be an in-depth research into a specific product available. The effect of these technologies within the framework of the GII will be limited to validity risks and solutions even if some or all of the other audit control objectives are met by encryption. The mathematical science behind encryption algorithms will not form part of this research.

1.5 DEFINITIONS

The key words for this short dissertation can be defined in the context of this research as follows:

- **Encryption**

"The process of making information indecipherable to protect it from unauthorised viewing or use, especially during transmission or when it is stored on a transportable medium." (Microsoft ® Encarta 1994).

"To put into code or cipher. To scramble access codes to (computerized information) so as to prevent unauthorised access." (The American Heritage Dictionary of the English Language, 1992).

"Encryption (cryptography) defines the principles, generalised methods and technologies for making information unintelligible to unauthorised individuals or processes (Deloitte & Touche, 1996:1).

Encryption is the methods and tools that can be used to secure data whilst in transfer on the GII, by encoding and decoding of information with the use of keys, to ensure the validity of transactions.

- **Technology**

"The application of scientific discoveries to the production of goods or services that improve the human environment." (The Concise Columbia Encyclopedia, 1991)

- **Validity**

"Producing the desired results: efficacious: valid methods. Having legal force: effective or binding. What is valid is borne out by the truth or fact." (The American Heritage Dictionary of the English Language, 1992). Validity includes integrity and confidentiality.

- **Transactions**

  "Communication involving two or more people that affects all those involved. Something transacted, especially a business agreement or exchange." (The American Heritage Dictionary of the English Language, 1992).

- **GII**

  Global Information Infrastructure. A global network of networks interacting on all human development through various forms of electronic and digital mediums (GIIC, 1997).

- **Continuity**

  Continuity can be defined as the availability of your information and processing resources when required. This can no longer be artificially divided into organisational and technological segments as the two are interdependent and interrelated.

- **Integrity**

  Integrity can be defined as trustworthiness. There is a relationship between continuity and integrity as the loss of integrity of data is the same as having no data available.

- **Confidentiality**

  Confidentiality relates to intellectual property and individual privacy (Deloitte & Touche, 1995:16).

- **Electronic commerce**

  Electronic commerce can be defined as any electronic communication made in support of business initiatives and has been done for years on a limited scale using email, EDI and EFT which are increasingly resulting in a paperless transaction flow.

- **Cryptology**

  Cryptology originates from the Greek words "kryptós" and "logós" meaning "hidden word" and involves the science of secure communications and has been used for many centuries from unsophisticated forms to current day mathematical science (Simmons, 1991:4). The reason for cryptography stems from the need for privacy and authentication (Van Tilborg, 1989:1).

  Cryptography is a practical method for protecting information through communication networks that use land lines, communication satellites and microwave facilities and could even be used to protect stored data. It is also used for message authentication, digital signatures, personal identification for authorising electronic fund transfers and credit card transactions.

- **Information privacy**

  Information privacy is defined by Alan Westin (1976) as the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others. The GII complicates this issue but facilitates low cost, and dissemination of information to the broadest audience possible (National Information Task Force, 1997:7).

- **Security**

  Security, and specifically computer security, can be described as the degree of protection offered by the safeguards and procedures which can be applied to computer hardware, programs and data and includes system controls.

1.6 RESEARCH METHODOLOGY

The methodology followed in this short dissertation will be as follows:

- Chapter 2 will be a research into the goals and objectives of the Global Information Infrastructure, its establishment, future and impact on business transactions. The agreed-upon standards that already exist will be discussed but will be limited to the security concerns of businesses. The risks associated with transacting on the GII are documented, as well as proposed solutions.

- In chapter 3, a short history of encryption technology is provided. This will be followed by a description of the technologies available and agreed-upon standards in force within this scientific field. The different types of encryption methods will be detailed, as well as future developments envisaged. Current products available will only be mentioned and a conceptual structure for implementing encryption technologies will be detailed. The risks and concerns of businesses and auditors relating to electronic trade and transacting on the GII are researched and an evaluation will be done to determine if encryption technology offers solutions to validity risks in particular. The importance of encryption technology in future developments in the Global Information Infrastructure and audit environment is discussed.

- In chapter 4, a checklist for the auditor involved in such a business environment is developed to assist the auditor in addressing validity risks that prevail in a GII environment and which can serve as a guide for future research and discussion.

- In chapter 5, a conclusion is reached as to whether the research conducted indicated that validity concerns can be addressed through the use of encryption technology. This indicates whether

the objectives of this short dissertation are met. An indication is also provided for areas of future research that can be conducted based on this short dissertation or on other issues not yet covered by detailed research.

1.7 RESEARCH APPROACH

The approach used in the research of this short dissertation will be in the form a literature survey of the topics to address the objectives of the research. The research will be focused on the risks and controls in place to address these risks from an audit perspective with specific reference to transactions using the Global Information Infrastructure. As this field of research is a fast developing one, the newest information will be obtained from digital sources such as CD-ROM and the Internet. Current available research and literature on electronic commerce and cryptology will also be researched.

1.8 SUMMARY OF RESULTS

The GII is envisaged as the network of networks that will influence not only the financial and business markets but also everyday lives of ordinary people. Several initiatives and organisations are actively involved in developing and enhancing international co-operation and standards that will be applied globally to cater for these global initiatives. Freedom of development, and transaction and trade in technologies, are encouraged.

Transactions will be secured by way of encryption algorithms that are secure from normal attack and any security measure should not be

applied in isolation but also in context of the cost to the corporation and the perceived risk of loss of information, financial losses and loss of reputation. Key management is the vital link in the strength of encryption and key recovery is a contentious field that should be researched further.

A short checklist has been constructed to address the risks and concerns of businesses from an audit point of view. This checklist concentrates on the validity issues of transactions, and encryption as the means of securing the privacy, integrity and confidentiality of transactions during transmissions.

Certain fields for further research have also been defined which could lead to the development of a specialised field within auditing, namely GII auditing. Others include the legal, taxation, standards and protocols and comprehensive security packages disciplines.

1.9 CONCLUSION

The result of the research conducted supported the objectives of this short dissertation. Support was found in the literature surveyed for the theory that encryption is the best security measure to ensure validity of transactions during transmission in unsecured channels such as the Internet and GII.

The strengths and benefits of this technology within the GII will be dependent on:

- internal controls within the organisation;

- other security controls implemented;
- management of key security;
- adherence to international cryptographic standards; and
- development of international standards and agreements on electronic trade on the GII.

2. THE GLOBAL INFORMATION INFRASTRUCTURE AND ELECTRONIC COMMERCE

This chapter discusses infrastructure and applications identified through the use of electronic commerce under the following headings:

2.1 OBJECTIVE

The objective of this chapter is to research the goals and objectives of the Global Information Infrastructure, its establishment, future and

impact on business transactions. The agreed-upon standards that already exist are discussed but are limited to the security concerns of businesses. The risks associated with transacting on the GII are documented, as well as proposed solutions.

The relationship and impact of electronic commerce are also researched to highlight the standards, risks and benefits of this emerging technology to businesses.

2.2 NATURE OF LITERATURE SURVEY

The Internet was searched for the latest information on the GII as there is no authoritative literature available. Documentation and standards issued by various government and international organisations were researched as well as information contained in articles available on CD-ROM and other media. No interviews were conducted or questionnaires circulated.

The nature of the literature survey conducted in this chapter focused on literature work on the basics of encryption and recent opinions of how this technology can be utilised in the GII. The current frameworks of encryption standards were also studied.

2.3 SCOPE, LIMITATIONS AND EXCLUSIONS

"We are on the verge of a revolution that is just as profound as the change in the economy that came with the industrial revolution. Soon electronic networks will allow people to transcend the barriers of time and distance and take advantage of global markets and business opportunities not even imaginable today, opening up a new world of economic possibility and progress" Vice President Albert Gore, Jr (Gore, 1994).

Certain controls can be brought into place and should be planned, implemented, maintained and reviewed at the appropriate level and at appropriate intervals by professional people and experts. These controls could include the following:

- good business relationships;
- legal agreements;
- exception reporting in executive information systems;
- trading agreements relating to the use of electronic media;
- network user forums;
- service agreements with service providers;
- encryption;
- governmental legal requirements and directives;
- testing of third party systems;
- control totals attached to each message;
- sequential numbering; and
- parity and packet sequence protocols.

Efforts to protect the privacy of personal and business transactions will be futile, unless technologies are available and policies in place to ensure security and integrity of on-line data (Clinton & Gore, 1996:11).

The development of the GII will result in the network of networks and will endeavor to create a global village in the commercial, social and educational spheres of human development (National Information Infrastructure, 1997:1). The GII represent the world-wide infrastructure that supports the transmission and delivery of electronic content, including the goods and services involved in electronic commerce (Clinton & Gore, 1996:17).

So wide are the scope and possibilities of the GII that the research will be limited to electronic commerce and, in particular, electronic financial transactions conducted on the GII. The security issues, standards and solutions of transacting on the GII will be researched.

2.4 DEVELOPMENT OF THE GLOBAL INFORMATION INFRASTRUCTURE

The Global Information Infrastructure (GII) concept was introduced by the Vice President of the United States in 1994 at the World Telecommunication Development Conference.

The GII will depend on the development of technologies and products currently available and new technologies not yet envisaged. It will extend beyond the hardware and software and will include systems of applications, activities and relationships as well as standards, interfaces and transmission codes that will facilitate interpolarity between networks and ensure security and privacy of the information transmitted. But above all the GII involves people and the development of peoples across the globe (National Information Infrastructure, 1997:1) (Computer Systems Policy Project, 1997:10). The current Internet is not the GII but will be a critical part and starting point of the GII. The GII will

involve the widest possible spectrum of information services, delivery mechanisms and participants (Deloitte & Touche, 1995:6).

The GII will revolutionise electronic commerce and government, and will provide open access to the information society. The need for information security will be required otherwise companies and individuals will become reluctant to move any business or information on to the GII. New and advanced uses of the GII will include:

- private and business communications;
- fax messages;
- electronic mail;
- electronic fund transfers and other financial transactions;
- business information and trade secrets storage and transmission;
- air traffic control operations;
- telephone networks;
- health records; and
- personnel files and other personal information.

The GII will continually evolve but industry (private and governmental) will have to take action to address complex technological issues and to eliminate regulatory and policy barriers to its deployment and use (Computer Systems Policy Project, 1997:10).

The following changes can be brought about by the development of the GII:

- education available to all students regardless of geography, distance, resources or disability;
- art, literature and science available everywhere;
- improved health care facilities available when required;
- virtual offices enabling working from home for your corporation;

- transmitting and receiving orders from any business directly to manufacturing lines;
- entertainment and personal finance available from your home;
- availability of government information on line; and
- exchange of information electronically and the resultant reduction in paper usage (Sunsite, 1997:1).

2.5 COMMERCIAL APPLICATION OF GII

As can be seen from the above the GII will cater for a lot more than just financial transactions. A framework for the development of global electronic commerce must be developed and include the following issues that must be agreed upon globally to ensure the success of the GII initiative. All of these issues will be present in any one transaction conducted on the GII (Clinton & Gore, 1996:4):

Financial issues

- customs and taxation; and
- electronic payment system.

Legal issues

- uniform commercial code;
- intellectual property protection;
- privacy; and
- security.

Market access issues

- telecommunications infrastructure and inter-operatability;
- content; and
- technical standards.

Certain principles were laid down in the framework for the development of the GII (GIIC, 1997:6) which relayed the view of the US government on trading on the GII. The development of the GII is based on five principles:

- encouraging private investment;
- promoting competition;
- providing open access;
- creating a flexible regulatory environment; and
- ensuring universal service.

2.6 GII POLICY

To facilitate the development and growth of the GII certain policies and fundamental principles had to be agreed upon. This has been done in conjunction with private sector firms, universities and governmental organisations and is driven by world wide forums such as the OECDC, WTO, IISP (ANSI) and GIIC.

There are several organisations involved in the standard setting and policy decision making of issues relating to the GII (GIIC, 1997:23):

- World Trade Organisation (WTO) will have to regulate the trading environment and provide legislation for international tax issues;

- Organisation for Economic Co-operation and Development (OECD) will introduce co-operation on international tax issues and has issued guidelines for security and encryption policies;

- Central Banks and the Basle Committee for standards on electronic banking and settlement;

- United Nations Commission on International Law is preparing a model law to support electronic commerce;

- World Intellectual Property Organisation is establishing new international agreement on this subject;

- The European Union has issued guidelines on privacy issues;

- The Information Infrastructure Task Force of the US government is formulating privacy policies;

- Information Infrastructure Standards Panel is sponsored by ANSI and has been established to develop standards on security; and

- Global Information Infrastructure Commission (GIIC) is an independent initiative with the objective of fostering global knowledge on GII issues.

The immediate concerns and areas that have to be covered by agreed upon policies are (Computer Systems Policy Project, 1997) :

- **Launching of the GII;**

  The development of the GII should not wait for government. Across the world private companies are taking the lead in developing technologies and applications that can be used in the GII. The greatest concerns are the global interaction and standardisation of these developments.

- **Private sector involvement;**

  The private sector is taking the lead in the development of the infrastructure. The government's role is to nurture the GII and to

ensure that private sector views are represented in any international discussions and agreements.

- **More than telecommunications;**

  The GII is the integration of networks, information appliances, information resource applications and people, and requires policies beyond those applicable only to the telecommunications industry. There also needs to be a harmonisation of treatment and policies across the globe.

- **Competition and deregulation;**

  Private sector initiative and competition are the building blocks for the development of the GII. In the competitive global market, this will ensure the development and survival of the best technology and the most efficient and economic scale for all the peoples of the world. Governments should ensure co-operation amongst themselves and should try to remove all trade and economic barriers to ensure the flourishing of a deregulated market.

- **Availability and affordability;**

  As the GII is in the development stage, the best "medicine" at this stage will be to encourage competition to ensure the eventual provision of a universal service selected by the users on the basis of affordability and availability.

- **Substantive priorities; and**

  It must be ensured that the GII develops as a global tool, and the following issues must be addressed by governments and the private sector:

  - interoperatability to ensure globally accepted standards and key interfaces;

- achieving open and competitive markets in a deregulated environment;
- developing and adopting security mechanisms such as encryption standards;
- protecting sensitive and personal information and providing such information on accepted guidelines; and
- protecting intellectual property.

- **Testbeds.**

  Engaging in international pilot projects will increase the knowledge and support research and development of new technologies that will focus on the enhancement and global implementation and availability of the GII (Computer Systems Policy Project, 1997:4).

2.7 SECURITY AND PRIVACY CONCERNS

Security is defined as the combination of methods, procedures, hardware, firmware and software used by a system to minimize the vulnerabilities of assets and resources (Information Infrastructure Standards Panel, 1997:1). The GII will require an effective set of mechanisms to protect commercial and other transactions. Providers and purchasers of the goods and services provided on the GII will have to be assured and be confident that their transactions are conducted in a secure manner. The transactions will have to be confidential, origin of messages should be verifiable, personal privacy should be protected and these security measures should not impede the flow of electronic data.

All countries should adopt standards that support these security goals and governments will have to play a role to enforce laws different to those for national security and diplomatic purposes. Encryption mechanisms should be freed from existing laws restricting export and

development outside the United States, as this is seen as one of the most powerful tools to ensure security on the GII (Computer Systems Policy Project, 1997:7)(SAICA, 1996:22). International conferences and cooperation in this field are vital to develop a global strategy that will be acceptable to all nations. Information security is essential and includes encryption and cryptographic methods that should be determined by the market in an open and competitive market environment. Key contributors to policy guidelines are the Commission of European Union's (EU) draft Green Book on security information systems, the Organization for Economic Cooperation and Development's (OECD) guideline on security systems and the International Chamber of Commerce's (ICC) position paper on international encryption policy (Information Infrastructure Standards Panel, 1997:2).

A set of 32 security needs have been agreed upon by the IISP (Information Infrastructure Standards Panel, 1997). A list of these needs is:

- **Anonymous features**
  - secure message format;
  - cryptographic functions; and
  - mechanisms for electronic cash transactions.

- **Confidentiality**
  - negotiating cryptographic attributes at connection establishment; and
  - renegotiating cryptographic attributes during the connection.

- **Prevention of theft, tampering and destruction**
  - non-repudiation mechanisms for operating mediation of resource system access;
  - non-repudiation mechanisms for application mediation of resource access;

- a framework for application layer protocols;
- security aware entity naming systems; and
- secure payment protocols.

- **Quality of service**
  - application features for security;
  - secure application architecture;
  - secure application portability;
  - secure operating system architecture; and
  - standard overall security framework.

- **Authentication, authorisation, delegation and administration**
  - methods of operating system level authentication;
  - methods of application level authentication;
  - methods of operating system level authorization;
  - methods of application level authorization; and
  - delegation of security attributes.

- **Security classification**
  - security levels for data processing;
  - security compartmentalisation for processing data;
  - security levels for data; and
  - methods to support non hierarchical compartmentalisation security classification for data.

- **Interoperable encoding of security attributes**
  - conversion of security attributes to and from text; and
  - user interface security labeling.

- **Secure methods for security administration**
  - standardisation of levels of assurance for application integrity.

- **Evaluation methods and criteria**
  - standardisation of evaluation criteria for operating system security services;
  - standardisation of evaluation criteria for application security services;
  - evaluation criteria for security enforcement;
  - standard evaluation criteria for network security services; and
  - evaluation criteria for security architectures and frameworks.

These needs are the basis for further development of policies and incorporate several needs directly related to one of the main areas of this research, namely encryption. Standards are required for the secure exchange of information through the use of cryptology to authenticate, encrypt, decrypt, digitally sign and to perform key management functions. Standards are also needed to specify components of communications protocols used to negotiate cryptographic algorithms at establishment and during a session (Information Infrastructure Standards Panel, 1997).

New risks will be present when using the GII, such as the degradation of the service, errors during the transmission of messages and manipulation of messages during the transmission. The latter will be the focus of this short dissertation as this entails the ensuring of the validity of the data when the GII, or for that matter any electronic communication, is used (SAICA, 1996:12).

Third parties could:

- alter some , all or part of a message;
- delete a message;
- send a duplicate message;
- pre send a message or
- send an acknowledgement.

2.8 ELECTRONIC COMMERCE

As financial transactions in particular is one of the objectives of this research it is important to relate it to electronic commerce on the GII. This relationship has been depicted in figure 1.3. Electronic commerce requires changes to internal processes as well as the invention of new ones. There is a global move to transact electronic commerce on the Internet and ultimately on the GII as a result of the lower overheads and potential exposure to the global marketplace (Coopers & Lybrand, 1996a:2).

The relationship between electronic commerce (EC), electronic trading (ET) and electronic data interchange (EDI) is depicted in figure 2.1. Electronic commerce encompasses electronic trade which focuses on a specific trading cycle, whilst EDI only deals with transfer of data which is aimed at leading the business world to a paperless society.

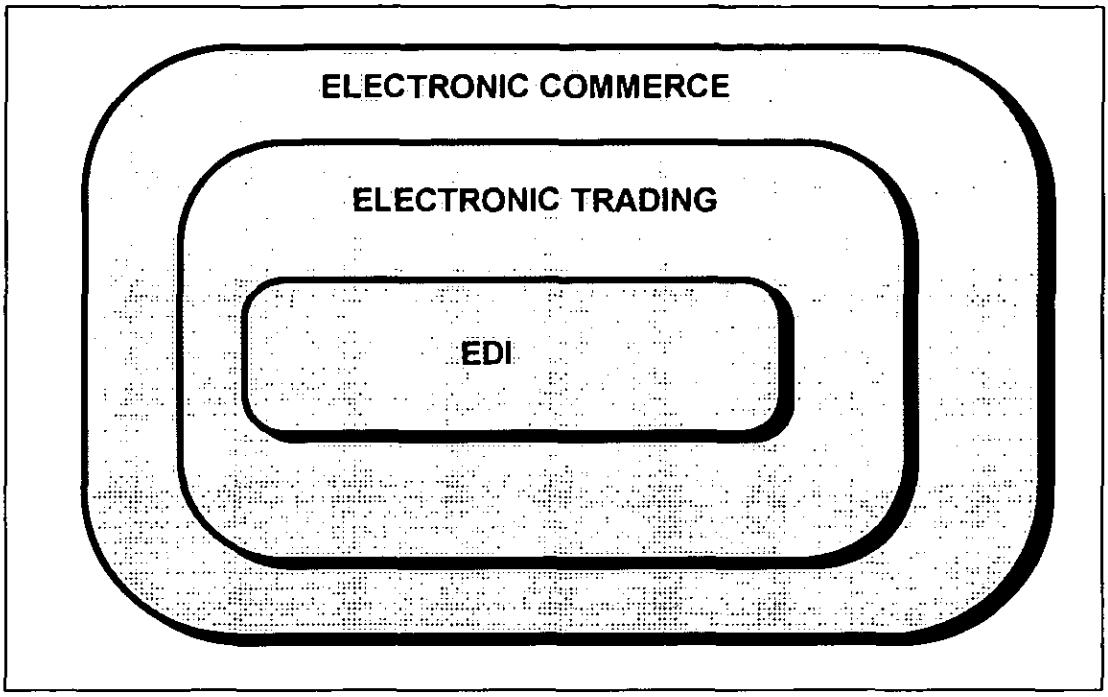

Figure 2.1 *The relationship between EC, ET and EDI (Van Aardt, 1995:8).*

Electronic commerce will force the organisation to rediscover its mission as electronic commerce will affect all aspects of the organisation. This necessitates a coherent strategy for the implementation of electronic commerce to limit risks but also to explore effectively and efficiently all the opportunities that it brings.

Electronic trading tools include EDI, electronic mail, bulletin board systems, office automation and tele-conferencing. With these tools additional security concerns evolve that should be addressed.

The effect of the introduction of EDI into an organisation can be described as a ripple effect (Van Aardt, 1995:134) and the upward evolvement of activities within the organisation is shown in figure 2.2.

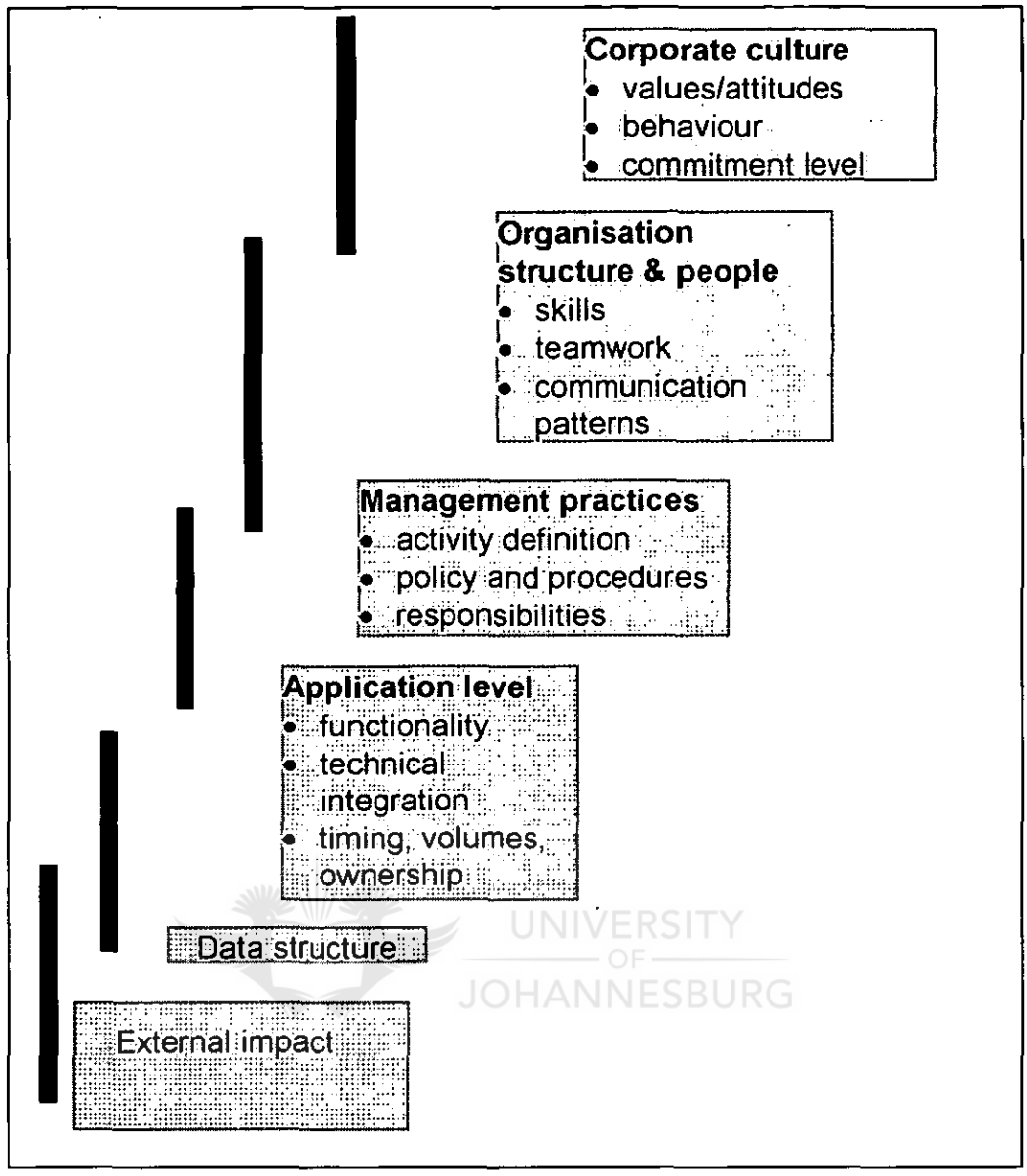

Figure 2.2 *The EDI ripple effect (Van Aardt, 1995:120).*

The following steps are usually taken by a business when it explores transactions and does business on the Internet and GII (Van Aardt, 1995:212):

- Allowing access through email and the construction of home pages on the web. Security management requires secure browsers and servers, single sign on, access control, secure email, anti virus protection, firewalls, ethical hackers and emergency response plans;

- Integration with existing systems where transactions are conducted with customers and suppliers and confidentiality, integrity of data and authentication on both sides are supported by public key based encryption, certification and gateways;

- Electronic commerce where two way transactions are performed inside and outside the corporation. Secure payment infrastructures are also now required, a non repudiation facility and a trusted environment for secure end to end transaction; and

- Electronic interactive phase where more complicated and interactive conducting of business using sound, videos and voice are used.

The impact of electronic commerce is summarised in table 2.1, although all the possible benefits and impact will be too long to list (Van Aardt, 1995:120). The change in management focus required when trading through electronic commerce on the Internet and the GII can clearly be seen.

AREA OF IMPACT	MANAGEMENT FOCUS
Information flows	Pro active vs reactive
Delays and overheads	Optimisation of time
Better service and efficiency	Improved efficiency
Capital expenditure	Reduction in working and start up costs
Corporate benefits	Quick response to market changes
Market competitiveness	Market share
Administration and cost benefits	Cost savings and increased accuracy
Trading relationships	More leverage
EDI as a prerequisite	The cost of not doing EC
Market forces	Market share
Market competitiveness	Market share

Table 2.1 *Summary of impact of EC (Van Aardt, 1995:120).*

The risks, benefits, standards and future of developments will now be discussed.

2.8.1 Risks

Traditional data security involves a comprehensive data security policy and this must be expanded now to include and address risks associated with electronic communications (Van Aardt, 1995:385). Controls should be implemented to achieve the following objectives:

- only authorised messages are sent and received by the organisation;
- no messages are misdirected or re-routed;
- no messages are lost, changed, duplicated or disclosed during transit;
- downtime of communication networks are eliminated; and
- unauthorised access leading to interruptions and losses are prevented.

Several unique risks are present in electronic commerce on the Internet and the GII (Coopers & Lybrand, 1996b:2) such as:

- Intrusion and external invasion by unauthorised users and the misuse of internal users are the biggest risks in electronic commerce. Any user names and passwords sent in the clear are vulnerable to attack;

- The pretense of running a legitimate business on the web is greater because the lack of traces to the actual owners could lead to fraudulent gathering of information and its use in transactions that lead to a loss of resources without the

possibility of tracing and placing responsibility on the originators;

- Viruses and Trojan horses could be resident in any software that is offered for download on the web and the greater risk is that an apparently legitimate site or software could have been created just to entice you to download it to enable the virus to be deployed in your system; and

- Other risks such as intercepting of account information and misuse of internal access to confidential information also exist.

2.8.2 Benefits

From the above it can be seen that EDI is part of electronic commerce and as it evolves with the Internet and the GII the following benefits can be achieved by a typical business organisation (Van Aardt, 1995:387):

- streamlined information flows;
- reduction in delays and overheads;
- better service and higher efficiency;
- reduction in capital expenditure over the long term;
- rapid and efficient modification of corporate policies;
- better utilisation of staff;
- market competitiveness;
- administration and other cost benefits; and
- enhanced and global trading relationships.

EDI has already become a prerequisite in certain sectors as the deployment of this tool in a particular organisation will require

its suppliers and customers to follow a similar route for it to achieve the best benefits from the electronic commerce environment. This will have a snowball effect as one of the suppliers will follow a similar route requiring its suppliers and customers to switch over to EDI and electronic commerce and so on. Market forces will also force businesses to change to electronic commerce because of the benefits as listed above for one link in the trading chain in the business sector or even within government administrations and policies (Van Aardt, 1995:94).

2.8.3 Standards

There are still numerous legal implications and interpretations that will have to evolve to take cognisance of electronic commerce as this is a new discipline and several national, and especially international, law enactments and amendments will be required. Most of the laws applicable to commerce have their roots in paper based transactions which will now disappear in electronic commerce. Issues such as document/information retention, legal enforceability, taxation issues, rights and obligations, technology exports of encryption techniques are only some of the issues that will have to be addressed in law (Coopers & Lybrand 1996a:2).

Although from a legal point of view there are several questions to be addressed this could be overcome by an interchange agreement. This has many shortcomings and the wider legal environment dealing with the law of evidence, contract, delict, criminal law, tax law, insurance law, administrative law, procedural law, data protection law, law of prescription, copyright and international law have to be expanded to address

electronic commerce issues adequately (Van Aardt, 1995:100).

2.8.4 Future developments

The profit motive will be one of the driving forces in the future development of electronic commerce. Technology will be one of the enablers but the business community must perceive the GII and the Internet as a viable alternative as well as a cost effective medium to conduct business. New developments to accommodate electronic commerce can be foreseen in (Coopers & Lybrand, 1996c:1):

- Business presence just for the sake of being there (perception);
- Demographics of target markets;
- Advertising;
- Payments electronically and secure;
- Hardware development and cost;
- Java self contained program applets;
- Interactive web pages using for example AxtiveX;
- Digital agents;
- Network computers;
- Personal digital assistants;
- Intranets; and
- Process automation.

The changes introduced by electronic commerce will affect the ability to perform and the strategies in place within the corporation and result in a change in business strategies. The external environment in which the organisation operates will also change. More time will be available and the production and operations of the organisation will change, which could lead to a

comparative advantage over competitors. Management can become more proactive than reactive in decision making based on more accurate and timeous information.

2.9 BUSINESS CONCERNS

The more exposed your data is the more secure encryption and other protection you require. Encryption can support the following objectives of businesses:

- Confidentiality which prevents unauthorised viewing of data;
- Integrity where any tampering with an encrypted message would make it illegible and would indicate the attempt to invade the privacy of the message;
- Continuity which should ensure that the business can operate without disruption and so also the data; and
- Non repudiation which ensures that responsibility can be attributed to the correct parties. This will ensure that you can determine from whom the data was received and that the sender is who he claims to be (Deloitte & Touche 1996:2).

The top security issues faced in electronic commerce are (Coopers & Lybrand 1996b:1):

- system intrusion;
- theft of credit card information;
- user authentication;
- vendor authentication;
- modification of transactions;
- confidentiality of transactions;
- industrial espionage;

- software piracy;
- password sniffers; and
- other credit card fraud.

The risks present in an electronic commerce environment can be summarised as in table 2.2. The management of these risks is the responsibility of management and the responsibility of internal and external auditors is to express an opinion on the adequacy of controls implemented. These are only the major risks (SAICA, 1995:6).

GENERAL	INTERNAL	EXTERNAL
Increased dependence on trading partners	Internal security failures	Trading partner controls
Increased dependence on technology	Implementation risks	Loss of confidentiality of sensitive information
Reduced human involvement	Processing risks	Legal trading requirements
Dependence on service providers		Loss or degradation of EDI service
Legal uncertainty		Errors during the transmission of messages
		Manipulation of messages during transit

Table 2.2 *Risks present in electronic commerce (SAICA, 1995:6).*

Validity of transactions on the GII is concerned more with the latter two external risks of errors and manipulation of transactions during transit. These include the following risks which could result in incorrect business decisions and possible subsequent loss to the corporation (SAICA, 1995:12):

- loss of all or part of a transaction
- delivery of message to the wrong person
- corruption of the message
- delays in the delivery of a message
- alteration of some or all of the content
- deletion of a message
- duplication of messages

2.10 SECURITY SOLUTIONS

If there is no coordination between the components of electronic commerce and specifically the trading cycles, then advances in technology will increase the risks and controls required to address the risks of transacting on the GII. An organisation always operates in a particular environment that influences its actions and the base of societal controls already in place or the inherent difficulties in enforcing globally accepted societal controls (Van Aardt, 1995:220).

The GII will incorporate the Internet and many of the technologies utilised to secure transactions on the Internet. The communication protocol of the Internet - TCP/IP (transmission Control Protocol/Internet Protocol) provides the rules for addressing and directing packets of transactions and data on the Internet. The transmission protocol breaks the message down to manageable packets whilst the Internet protocol addresses them (Deloitte & Touche 1995:6).

The layers of information data protection, work in conjunction with one another to minimise the overall risk inherent in the use of information technology in processing data and transactions. This can be depicted as in table 2.3 where the overall control remains with the mental attitude and culture of the organisation and the society as the base of all

controls. Then only can additional administrative, physical and technical controls be built into the system with the constant threat that a deterioration in societal control affects all other controls (Security and Control, undated).

SOCIETAL CONTROLS Laws , legal framework, morality		
ADMINISTRATIVE CONTROLS Staff procedures Operational controls	**PHYSICAL CONTROLS** Locks, alarms, guards, secure cables, fire precautions	**TECHNICAL CONTROLS** Input and output controls Processing controls System security

Table 2.3 *Societal controls (Van Aardt, 1995:220).*

- **Secure socket layer (SSL)**

  This method protects communications by server authentication, encryption, and maintaining data integrity and was developed by Netscape. The SSL only functions in environments where security is present in both the client and server sides of the communication. It requires a security certificate and operates below the application level of the system.

- **Secure hypertext transfer protocol (SHTTP)**

  Developed by the W3 Consortium and uses cryptography and message based encryption at application level but does not require a security certificate at the client system.

- **Digital signatures**

  Digital signatures identify each use of such signatures on a document, transaction or message. If secured in transmission the user can be assured that the information has not been altered and that the person whom signed the item is the sender.

- **Certificate authorities and authenticode**

  This secures the download of software and prevents viruses and Trojan horses. Certificates are issued to the users.

- **Encryption**

  Several access and authentication technologies use encryption which provides for privacy, authentication, message integrity and non repudiation.

A common set of rules to enable security can only be voluntary since the laws of the countries of the world are not similar regarding data security and networking. Certain security guidelines (Network Working Group, 1991:2) are:

- Users are individually responsible for understanding and respecting the security policies of the system;
- Users have the responsibility to employ available security mechanisms to protect their data;
- Computer and network providers are responsible for maintaining security in their systems;
- Vendors should ensure that what they sell has adequate security controls embedded;
- All parties are responsible for co-operating to provide security; and

- Technical improvements should be sought on an ongoing basis.

Any protective measures taken should not be implemented or evaluated in isolation or individually but the aggregate effect should be considered together with the efficiency and effectiveness against cost and risk concerns of the corporation. Access control includes the functions of identification, authentication, authorisation, access mediation, monitoring, enforcement and incident reporting and logging of event. This can be achieved by logon scripts and support services, password management, authentication subsystems, path control through router switch management and protection, encryption of network traffic, authorisation management, firewalls and proxies (Deloitte & Touche, 1995:24).

The private sector has researched various solutions to privacy concerns in using the GII and Internet and these include the following projects (Information Technology Industry Council, 1997:2):

- The "cookie" solution to allow the user to decide where cookies or traceability of the browser's address will be deposited;
- Privacy profiles preferences that will allow the user to specify what information can be disclosed and he will be warned if a web site does not fit into his profile;
- The platform for Internet content selection (PICS) which accommodated parent control will be developed to include code signing, privacy and intellectual rights management;
- Project OPEN is an educational project that will educate Internet users on how to transact in a responsible manner on the net;
- Certain logos that signify privacy protection will be incorporated into a web site to indicate that the site is "privacy" compliant;
- An open profile standard is encouraged by the major Internet developers to enhance privacy without limiting the information gathering process;

- Anonymiser technologies are developing that will prevent the depositing of cookies; and
- Industry agreed self regulation that will prevent the distribution of non public information such as private information of individuals.

2.11 AUDIT CONCERNS

A change is required as a result of the change in the business environment caused by the evolution of electronic commerce, the Internet and GII. This creates a change in risks and the internal and external auditors have the task of analysing the risks and evaluating the control measures put in place by the organisation to address the risks. This remains a management issue as the auditor only evaluates the risks, recommends corrective actions and expresses an opinion on the adequacy of the risks (Van Aardt, 1995:106).

The risks can be divided into administrative and environmental controls. The traditional approach to application controls includes controls such as editing and validity checks, accountability for unauthorised transactions, reconciliation, sequence checks, review and follow up of exception reports and this should still be implemented. Electronic commerce has however also introduced the following additional EDI controls to ensure adequacy, accuracy, completeness and authorisation of transactions:

- the transactions are processes and received in all appropriate applications and only those;
- adequate and timely reporting must occur and could be on line flags that report exceptions;
- there is a differentiation between a processed transaction and a transmitted processed transaction;

- temporary files are secure from unauthorised access;
- correct message header, trailer, identification information and structure are applied;
- repeat counts are within limits, individual transactions can be controlled by check digits on control fields and document standards are used;
- changes from VANS can be traced on transaction histories;
- formal and effective policies and procedures to validate business partners exist;
- the source of the transactions must be authenticated;
- confirmation of high risk transactions must be requested; and
- encryption techniques should be considered.

Communication security and VANS security over communications and communication lines should be ensured (Van Aardt, 1995:67).

Errors during transmissions can be addressed by controls totals attached to each transaction, sequential numbering for each type of transaction and parity and packet sequence checks should be incorporated into the communications using the specified protocols listed above. The most effective control over the manipulation of transactions during transmission is the use of encryption (SAICA, 1995: 24). This ensures, as detailed in chapter 3, that a message can not be read if intercepted and also that the validity of the sender can be confirmed.

2.12 CONCLUSION

This chapter indicates the changes and opportunities that are now available when conducting electronic commerce through the GII. There are a lot of security issues and development work that must still be

conducted through international co-operation, agreements and research. One of the major concerns is security and in particular the validity of transactions that are sent through the GII.

3. ENCRYPTION TECHNOLOGY

This chapter will indicate the results of the research into encryption technology under the following headings:

3.1 OBJECTIVE

The objective of this chapter is to discuss the history, current status of encryption technology, the science and the developments as seen by the researchers and experts in the field. The research will also indicate the strengths and benefits of using encryption technology.

3.2 BACKGROUND

The growth of the Internet and digital global economies has bred a new attack from electronic vandals that forever try to break into the privacy of individuals and corporations. Although one is aware that an attack is always possible one does not always know what counter measures to launch. Encryption is one of such measures that can be used and is gaining support as the more robust technology for transmitting and storing data even if the transport medium and other controls are weak and open to abuse and hacking (Dellino, 1996:1).

A Dial-up connection for Serial Line Internet Protocol (SLIP) or Point To Point Protocol (POP) can provide for an encrypted TCP/IP session using encryption software and modems. Encrypting routers provide for encryption of all IP packets between the networks. The benefit is that no data is ever sent in the clear or untrusted paths and that the two networks are joined as one. This is the basic control in an Internet environment. As can be seen in chapter 2, the Internet is part of the GII and both support electronic commerce.

The current TCP/IP protocols solve many of the communication risks but are not designed to offer security. Additional securities are required and the only technology that can provide for most of the security needs are cryptology which is incorporated in security protocols such as SSL

(secure sockets layer), SET (Secure electronic transactions) and S/MIME (secure multipart Internet mail encoding). As can be deduced from the acronyms these protocols are the foundation for most of the transactions of electronic commerce on the GII. Cryptology provides security services such as message encryption, message integrity, digital signatures and strong authentication (Netscape, 1997:2).

3.3 ENCRYPTION

The process of developing a cryptographic algorithm includes the design where the criteria and invention of the algorithm take place and the validation where the algorithm is tested for strength from attack (Meyer & Matyas, 1982:8).

Encryption is based on an algorithm and a key. Cryptology defines principles, methods and technologies for making information unintelligible to unauthorised individuals or processes (Deloitte & Touche, 1996:1). Decryption is the restoration of encrypted messages to a readable form. Cryptoanalysis is the science of breaking encrypted messages.

Cryptology can be divided into cryptographic and cryptoanalysis fields of science where the first relates to the science of encoding and decoding of algorithms and the building of algorithms and the latter to the science of trying to break the algorithms used in encryption. The original data is called plaintext and once it has been encrypted it is called cipher text or a cryptogram (Simmons, 1992:4). A universal assumption is that the strength of a cipher lies in the key as the intruder does have access to the cryptogram, the *Kerckhoff's assumption* first enunciated by A Kerckhoff (1835 - 1903)(Simmons, 1992:4).

This technology can protect either transmitted or stored data. The stored data require a longer management cycle than the transmitted data where the keys could be disengaged as soon as the message is received and deciphered. There is end to end transmission encryption where the message originates in encrypted form and ends in encrypted form, or a link transmission where the message is decrypted and encrypted at some or all the switch points en route to the receiver (Deloitte & Touche, 1996:3).

3.4 ENCRYPTION ALGORITHMS

The method of encryption and decryption is through ciphers which are a key to control the process. Block ciphers result in the same plaintext to be encrypted into the same cipher text whilst a stream cipher results in different cipher text even for the same plaintext as the encryption changes from unit to unit (Simmons, 1992:22).

Algorithms are today executed by computers and specialised hardware and software packages. Generally the public key algorithm is used to encrypt a randomly generated encryption key and this key is used to encrypt the message using a symmetric algorithm (Ylönen, undated:2). An algorithm is the mathematical formula which with the other unique string or key will create an encrypted message. This could be in software or hardware form and could be private or public (Deloitte & Touche, 1996:1).

The encryption key and the function are crucial as the same key used in two different encryption functions will produce two different results and is dependable on the key size (Kosiur, 1997:3). Encryption keys are the string of secret data used to encrypt the readable message. The choice of key, key length, unpredictability of key content and the protection of the key are critical.

The following list of encryption technologies are a summary of what is available today:

- **DES (Data Encryption Standard);**

  This is a block cipher created by IBM and endorsed by the US government using a 56 bit key operating on a block of 64 bits which is relatively fast and used to encrypt large amounts of data at one time. The algorithms have been made public and have been built into a chip. A disadvantage of the algorithm is that the same input will yield the same output that will enable an eavesdropper to predict a message response (Van Tilborg, 1989:55)(Kosiur, 1997:8).

- **Triple DES;**

  Based on DES and encrypts a block of data three times with three different keys.

- **RC2 and RC4;**

  Designed by Ron Rivest and are variable key size ciphers used for very fast bulk encryption which is faster than DES and can be made more secure by selecting a longer key. RC2 is a block cipher and RC4 is a stream cipher.

- **IDEA (International Data Encryption Algorithm);**

  Created in 1991 is efficient in software and offers secure 128 bit key encryption.

- **RSA;**

  A public key algorithm supported by a variable length key and a variable block size of text that can be encrypted.. The plain text block must be smaller than the key length with a common length of 512 bits.

- **Diffie-Hellman; and**

  The oldest public key cryptosystem still in use but does not support encryption or digital signatures.

- **DSA (Digital Signature Algorithm)**

  Developed by NIST using a similar scheme as Diffie-Hellman which can create signatures faster than RSA (Kosiur, 1997:3).

3.5 KEY MANAGEMENT

The administrative and technology based techniques used to create, disseminate, control, maintain and destroy encryption keys form part of key management. This process is critical to the success of the encryption and could lead to costly failures if not managed properly. Careful planning and management are required (Deloitte & Touche, 1996:1).

The activities involved in key management are described in FIBS 140-1 (National Institute of Standards and Technology, 1994) as the handling of keys and other related security parameters during the following stages in the entire life of the key:

- generation;
- storage;
- distribution;
- entry and use;
- deletion or destruction; and
- archiving.

3.6 MODES OF ENCRYPTION

There are several ways in which encryption can be achieved such as:

- Message or record encryption results in the actual encryption of the content of the message or transaction (Deloitte & Touche, 1996:1).

- Digital envelopes are encryption techniques where the message is left as is but is sent in an encrypted appendage which serves as an indicator of the integrity of the message (Deloitte & Touche, 1996:2).

- Digital signature is where the encrypted appendage includes sufficient information to identify the sender or the sending process as well as other data. This serves the objectives of integrity and non-repudiation (Deloitte & Touche, 1996:3). The signature or certificate establishes your identity and servers may be configured to accept only certain signatures which will ensure the security of the transaction. The certificate presenter must digitally sign the data exchanged and the protocol data to prove that he is the legitimate owner of the certificate. The combination of the certificate and the correct private key authenticates the transaction. Certificates are verified by checking validity dates and verifying that the certificate bears the signatures of a trusted certificate authority (Netscape, 1997:3). Digital signatures are generated by public key algorithms that can verify through a corresponding private key the public key to ensure that the message did originate from the sender (Ylönen, undated:2).

- Digital certificates can include the name of the certificate authority, a public key for cryptographic use and a time limit for the use of a certificate and can also include an indication of the verification level of the holder. The development of a hierarchy of certificate

authorities and standardised infrastructure is in progress by the US government in its drive to set up a Public Key Infrastructure (Kosiur, 1997:5).

3.7 TECHNIQUES OF ENCRYPTION

There are several techniques that can be used when data is encrypted. The technique, its problems and benefits are now discussed.

3.7.1 Symmetric

This is the oldest form of encryption and both the sender and the receiver possess the same key and both can encrypt and decrypt data with that key. Both parties have to agree to the key and know the same key (Kosiur, 1997:2). The same algorithm or key is used for encryption and decryption. Also called private key algorithms for example DES, RC4 (stream cipher), RC5 (block cipher) or IDEA. The key is uniquely associated with an entity and not made public (National Institute of Standards and Technology, FIBS 140-1, 1994).

Problems include security of keys, number of keys required (the number of keys tends to be much larger than the number of nodes), distribution of keys, no support for digital signatures and there is no proof of non repudiation.

Benefits are that it is fast and can be easily implemented in hardware.

3.7.2 Asymmetric

A key pair is used. One key is used for encryption and another key is used for decryption. Each person has his own pair of keys (Netscape 1997:2). One part of the key pair is private and only known to the owner and the other public part of the key is published widely but still belongs to the owner. Data encrypted by one key can be decrypted by the other key in the pair (Kosiur, 1997:2).

Public key algorithms are for example Diffie-Hellman, RSA, DSA. The keys are also uniquely associated with an entity but are made public (National Institute of Standards and Technology, FIBS 140-1, 1994).

Benefits are that one side of the process can be public and only the other side requires secrecy and key management, distribution of keys is relatively easy and it allows you to authenticate the integrity of the sender for purposes of non repudiation through digital signatures.

The problems that the process is slow and computationally intensive can be solved by using a message digest generated by one-way hash functions.

3.7.3 Other

Proprietary encryption algorithms developed by individuals and companies are usually secret and relatively unsecured.

3.8 ENCRYPTION STANDARDS

The following encryption standards have been issued by industry and government agencies and are regarded as de facto standards against which all encryption techniques and management must be measured.

3.8.1 FIBS140-1

The objective of this standard (National Institute of Standards and Technology, FIBS 140-1, 1994:1) is to ensure the secure design and implementation of the cryptographic module by meeting the following objectives:

- protection from unauthorised operation or use;
- prevent unauthorised disclosure of non public contents and critical security parameters;
- prevent the unauthorised and undetected modification of keys;
- employ FIBS approved security methods;
- provide indication as to the operational state of the key;
- ensure proper operation of module; and
- detect errors in the operation and to prevent compromise of sensitive data.

The following documentation is the minimum required by the standard indicating which areas and requirements for security are governed by the standard (National Institute of Standards and Technology, FIBS 140-1, 1994:4):

- **Cryptographic modules**

  Specification of the hardware, software and firmware with a block diagram must be documented indicating any exclusions together with the security policy.

- **Module interfaces**

  Specifications of interfaces , maintenance procedures and data paths must be documented.

- **Roles and services**

  Documentation of all the authorised paths, services and functions that can be supported by the module.

- **Finite state model**

  Specifications of all state and transitions with a finite state diagram must be documented.

- **Physical security**

  Specifications of the physical embodiment and security level and environmental failure protection procedures must be documented.

- **Software security**

  Exclusion of specification not adhering to the requirements must be documented with software design, source code and formal model of the cryptographic module security policy.

- **Key management**

  Documentation of FIBS approved key generation procedures and techniques.

- **Cryptographic algorithms**

  Documentation of the specifications of the FIBS approved cryptographic algorithm.

- **Self tests**

  Documentation of possible error conditions and all critical functions.

- **Assembly language**

  Documentation of assembly language code and adherence to requirements.

The security requirements set out in this standard can be summarised in table 3.1 as follows where the NIST (1994:2) have divided the security requirements into four levels.

- **Level 1** provides the lowest level of security and specifies the basic requirements for encryption without any physical requirements.

- **Level 2** requires physical security for identifying tampering and role based authentication.

- **Level 3** requires enhanced physical security using coatings and identity based authentication.

- **Level 4** requires the highest level of security and provide an envelope of protection around the cryptographic module.

	LEVEL ONE	LEVEL TWO	LEVEL THREE	LEVEL FOUR
Operator authentication	No access control required	Role based or identity based	Identity based	Identity based
Single chip modules	Product grade quality with sealing coat	Level 1 plus opaque coat	Level 1 and 2 plus opaque tamper evident coat	Levels 1,2 and 3 plus removal resistant opaque coat

	LEVEL ONE	LEVEL TWO	LEVEL THREE	LEVEL FOUR
Multiple chip embedded modules	Product grade quality with sealing coat	Level 1 plus opaque tamper evident coat	Level 1 and 2 plus opaque potting material and non removable enclosure	Levels 1,2 and 3 plus removal detection envelope, tamper response and zeroisation circuitry plus EFP or EFT
Multiple chip standalone modules	Product grade quality with sealing coat	Level 1 plus opaque coat	Level 1 and 2 plus opaque potting material and non removable enclosure	Levels 1,2 and 3 plus removal detection envelope, tamper response and zeroisation circuitry plus EFP or EFT
Software security	Detailed documents of the designs	Detailed documents of the designs	Level 1 and 2 plus written in high level language	Levels 1,2 and 3 plus module security policy
Operating system security	Installed only on executable code	Level 1 plus all software must be under controlled access	Levels 1 and 2 plus software labeled and under labeled protection	Levels 1, 2 and 3 plus under structured control
Key entry and output	Manual keys in plaintext and electronic key encrypted	Manual keys in plaintext and electronic key encrypted	Manual encrypted or split knowledge and electronic encrypted	Manual encrypted or split knowledge and electronic encrypted
EMI/EMC	Minimum requirements FCC Part 15 Class A	Minimum requirements FCC Part 15 Class A	Minimum requirements FCC Part 15 Class B	Minimum requirements FCC Part 15 Class B

Table 3.1 *Security requirements (NIST, 1994:2).*

3.8.2 DATA ENCRYPTION STANDARD (DES) FIBS 46-2

This standard sets out the mathematical detail for the algorithm to be used as standard to provide cryptographic protection to binary coded data. The algorithm is designed to encipher and decipher blocks of 64 bits under control of a 64 bit key and the same key should be used (National Institute of Standards and Technology, FIBS46-2, 1993:1).

3.8.3 SAFE ACT of 1997

Security and Freedom through Encryption Act of the United States of America which enforces the freedom to use and sell of any type of encryption finally broke the government enforced ban on the export of technology required to enable the encryption of electronic commerce transactions on a global basis (United States of America Acts, 1997).

3.8.4 OECD GUIDELINES FOR CRYPTOGRAPHY POLICY

The body recommended that member countries establish new or amend existing policies, methods, measures, practices and procedures to adhere to guidelines aimed at :

- promoting the use of cryptography to raise confidence in the infrastructures and to help ensure the security of data and privacy;
- promoting the use without impinging on national security;
- raising awareness of the need for policies;
- assisting decision makers to develop a coherent policy and procedures;
- promoting co-operation between public and private sectors;
- facilitating international trade; and

- promoting international cooperation between governments to achieve uniform use of cryptography.

The principles set out in the guideline are (OECD, 1997:2):

- Cryptographic methods should be trustworthy and generate confidence in the use of information and communication systems;
- Freedom of choice relating to the method used should be allowed within the law;
- Methods should be developed responding to the needs of individuals, businesses and governments;
- Technical standards, criteria and protocols should be developed and enforced at national and international level;
- Rights to privacy and secrecy should be respected;
- Lawful access to keys and plaintext of encrypted data should be allowed;
- Obligations of cryptographic service and key providers should be clearly defined and agreed upon by all parties involved; and
- There should be a coordinated approach by governments relating to policies and no policy should hinder trade between countries.

3.8.5 OTHER

There are other NIST Federal Information standards on computer security that relate directly to encryption technologies such as FIPS 74, 81,180-1, 181, 185, 186,190 and 196. In the USA privacy is also entrenched in the Privacy Act of 1974, The Computer Matching and Privacy Protection Act of 1988, The Freedom of Information Act, statutory limits applicable to federal agencies, the privacy principles of 1995 and federal law regulating state sale of government data . There is however no uniform international law and there are many conflicts in

law between different governments (National Information Task Force, 1997:4).

3.9 STRENGTH OF ENCRYPTION

In theory any key can be broken by using brute force or all possible combinations in sequence but with the mathematical assurance that the computing power required to break the key increases exponentially with the length of the key. It is always possible but the larger keys such as 128 bit keys are safe for the time being as there is a limit to the energy consumable to the point of infinity.

It is possible to break ciphers without using brute force but the problem is to guess the matching secret key from the public key. The strength of an algorithm is equal to its weakest point (Ylönen, undated:4).

An encryption algorithm's security is dependent on its key length as knowing the length of the key only gives you an idea of how much time it will take to break the code - eg. 8 bits have 256 possible keys (Kosiur, 1997:5).

If the cost and time factors are the only consideration to determine the strength of a key algorithm, then a comparison was made by Bruce Scheinder (1996) as quoted by Kosiur (1997:4) in table 3.2.

LENGTH OF KEY IN BITS					
COST	**40**	**56**	**64**	**80**	**128**
$100000	2 secs	35 hours	1 year	70000 years	10^{19} years
$1 million	0.2 secs	3.5 hours	37 days	7000 years	10^{18} years
$100 million	2 msecs	2 minutes	9 hours	70 years	10^{16} years
$1 billion	0.2 msecs	13 secs	1 hour	7 years	10^{15} years
$100 billion	2 microsec	0.1 secs	32 secs	24 days	10^{13} years

Table 3.2 *Strength of key algorithms (Kosiur, 1997:4).*

This table indicates, that if you have a key with a strength of 64 bits, it will take an intruder one year to break the code at a cost of $100 000. He also compared the resistance to brute force attack which indicated that public keys are much safer than secret keys from these attacks.

3.10 BENEFITS OF ENCRYPTION

Transaction privacy is achieved by using both public and private key encryption when the traffic between the SSL server and client is encrypted and negotiated during the SSL handshake. Even if packet sniffers are used successfully the message will still be unreadable.

The message integrity service ensures that the SSL session traffic is not accessed en route to its final destination by using a combination of shared secret and mathematical hash functions and identities are confirmed by public key certificates.

During an SSL handshake the client and server exchange X.509 certificates to prove their identities, the client generates a random set of keys to encrypt the transaction through the server's public key and a message algorithm for encryption and a hash function for integrity are negotiated (Netscape, 1997:8).

3.11 CRYPTOGRAPHIC INFRASTRUCTURES

The IBM SecureWay cryptographic infrastructure (IBM, 1996:4) is discussed below to illustrate the cryptographic infrastructure and configuration to ensure encryption for secure data transactions over the present Internet and the GII. The infrastructure is open and supports industry standards and provides a choice of toolkits and services. Through the supporting services, the infrastructure provides for a cryptographic programming environment which can be utilised in a broader business environment.

Business must be assured that it can use its applications in a secure and efficient manner independent of any platform (IBM, 1996). Cryptographic services can be utilised in layers from the applications down to the cryptographic engines with an option for application access at the appropriate level. This reduces the level of awareness required but increases the portability of applications through the use of standard APIs. The algorithms can be embedded in the applications and this layered approach assists in the identification and management of the infrastructure.

The four conceptual layers are depicted in figure 3.1. Layers describe the functions within a layer that are complementary, related and cross functional between layers resulting in an open infrastructure.

APPLICATIONS			
IBM CommercePOINT	Messaging	Firewall	IBM Info Market
Digital library	Health village	Lotus notes	Home banking
SUPPORTING SERVICES AND SUB SYSTEMS			
Credential services	Authentication services	Security context services	Access control services	Audit services
Key recovery services	Secure content distribution services		Secure electronic transactions (SET)	Applet security
CRYPTOGRAPHIC SERVICES			
API's toolkits			**Crypto engines**
BSAFE	C-API	CCA	GSS-API	GCS-API
HARDWARE/ SOFTWARE PLATFORM			
Transaction security system	Software		CMOS cryptographic co processor (chip)
Smart cards	Smart cards		PCMCIA

Figure 3.1 *Cryptographic infrastructure conceptual layers (IBM, 1996:4 and IBM, 1997:8,12).*

The application layer can use the supporting layer directly depending on the level of cryptographic awareness required by the application. The supporting services layer consists of an extensible set of services that invoke and exploit the APIs according to the cryptographic knowledge required by the service.

The cryptographic toolkit and engine layer consists of industry standard sets of calls to the engines or routines that incorporate the algorithms into the above two layers.

3.11.1 APPLICATIONS

Electronic commerce applications are listed in figure 3.1 and encryption services, APIs and cryptographic engines are all used by these applications. The applications are there to solve business problems.

Applications can provide the following range of security services to a business application:

- **Credential services**

  The management of user identifications and certificates which have been created and signed by a trusted authority to present a person's right to access the information. The service includes the issue and revoking of credentials, the validation, the mapping between systems and the provision of protection mechanisms.

- **Authentication services**

  The establishment and proving of identities are managed by this service.

- **Security context services**

  The service remembers that a user has already been authenticated on the system and reduces overheads.

- **Access control services**

  Checks the authority of a user to access a specific resource and up to what level.

- **Cryptographic services**

  This service provides for the encryption and decryption of transactions and data using a pair of keys to provide security functions such as data confidentiality, integrity, authentication and non repudiation.

- **Key recovery service**

  This service provides mechanisms to reconstruct cryptographic keys in case of loss or destruction or the legitimate need of a government law enforcement agency to decrypt a message. The development of key recovery infrastructures leads to new risks such as alternative paths to plaintext, insider abuse, new external attacks and forward secrecy as well as new complexities to the control environment due to the scale, operational complexity, authorisation of key recovery and new costs for designers, end users and authorisation agencies. (Abelson, Anderson, Bellovin, Blaze, Diffie, Gilmore, Neuman, Rivest, Schiller, Schneier, 1997:3)

- **Secure content distribution service**

  This service ensures that copyrighted material can be distributed without the loss of control and is usually sent through cryptolopes.

- **Secure electronic transaction (SET)**

  This enables the routing of payment information between users, suppliers and banks and is a set, agreed-upon protocol including cryptographic devices and algorithms.

- **Applet security**

  Securing that the Java applets used in browsers and web pages that provide links are secure.

  Examples of products available are:

  - Internet shopping;
    The user would select merchandise on the web page and supply the credit card information for payment. The application invokes the secure payment cryptographic service using the SET protocol. The protocol for payment negotiation will be invoked. Integrity and confidentiality of credit and payment information and verification of the merchant are ensured as well as non repudiation of the transaction.

  - Internet banking;
    Customers will be authorised to use the service through the use of certificate management services. The certificate will authenticate the client and select the level of confidentiality and integrity appropriate to the application. Public key infrastructure services, APIs and encryption algorithms are used by the application.

  - Information services; and
    Intellectual property requires control and this is provided through encryption.

  - Health care
    Patient records must be kept in the strictest confidence but also require immediate availability by authorised personnel. Confidentiality, integrity and authentication are invoked by the application, and the use of smart cards is envisaged.

3.11.2 SUPPORTING SERVICES AND SUB SYSTEMS

This layer has a set of services that can invoke and exploit the APIs. Each service will now be discussed.

- **Key recovery services**

  The service must support existing key distribution schemes and encryption algorithms.

- **Secure content distribution**

  Cryptolope containers will be used to secure the copyrighted and digital information. This can also be used to penetrate new markets where products can be sold directly from the infrastructure where the container will hold the encrypted version of the text document or electronic commodity. Attached to this will be a description of the product, its price and terms and conditions of use. The customer will purchase the item and a key (using DES and RSA technology) will be provided to open the cryptolope container which is directly off loaded from the web page.

- **Virtual private network**

  This enables business partners to conduct business over the net and confidential communications are ensured by the use of firewalls. It encrypts the IP packet, creating a secure channel for transmitting the transaction.

- **Applet security**

  Java applications are run on the browsers without any insight by the browser into the application. The applet is however seen by the

user as a possible intrusion or virus and cryptographic services and code signing are combined by the applet to control access, identification and authentication of the applet.

- **Certificate management**

To ensure the confidential transmission of transactions and data public key infrastructures must be developed to supply, publish, maintain, revoke and renew digital certificates and to distribute them to their destinations. This will provide communications transport over public and private networks. The certificate is issued by a trusted authority and includes the public key, global name, expiration date and application unique information.

- **SET**

This is the technology standard used by credit card companies that encrypts and secures credit card transactions. Payment information is automatically routed between users, merchants and banks. The client and server application has no knowledge of the encrypted credit card information.

3.11.3 APIS AND TOOLKITS

API toolkits and crypto-engines are specific programs available for the use by a service and through the hardware and software platforms.

- **PICA**

The platform independent cryptography API allows open, cross platform security and cryptographic functions to applications regardless of the platform on which they reside.

- **CCA**

  The common cryptographic architecture is a cryptographic API for secret key algorithms such as DES and public key algorithms such as RSA. It provides services for data privacy, data integrity, key generation, distribution, installation and PIN number generation. It provides interoperability between products regardless of platform.

- **BSAFE**

  A portable C programming toolkit that provides a code that supports a complete range of the most popular cryptographic and hashing algorithms and a random number generator without the programmer having access to the API.

- **GSS-API**

  A session orientated interface to facilitate secure communications and supports mutual authentication which requires a low level of security awareness by the application.

- **GCS -API**

  A generic algorithm independent cryptographic API providing a single multi vendor standard.

- **C-API**

  Provides system level access to common cryptographic functions such as encryption, hashing and digital signatures.

3.11.4 CRYPTOGRAPHIC ENGINES

These engines include the hardware and the software installations that utilise encryption technology and which will be used in electronic commerce and by the public.

- **Smart cards**

  The new way of the future. They are tamper resistant, cost effective and a simple means to authenticate users. The use of these cards will enhance the SET protocol by storing user certificates that could be read by a secure browser which will enhance the portability of security. The microprocessor and tamper resistant enclosure can store cryptographic keys, certificates and other data.

- **Workstation interface adapters**

  This co-processor will have a general purpose PC compatible subsystem, random number generator, cryptographic functions within a tamper resistant enclosure.

- **CMOS cryptographic co-processor**

  A single CMOS chip with a co-processor feature and integrated cryptographic service facility to support high volume transaction rates and bulk data security needs and provides all the cryptographic functions.

- **Transaction security system**

  A range of products that supports DES and RSA based cryptographic processing and offers interoperability across all workstations and host environments.

3.12 CONCLUSION

The objective of this chapter has been met, as the detail research indicated all the technologies available, although the detailed mathematical science has not been researched in this chapter. This chapter provides a summary of what is available and evaluates the strengths and weaknesses of encryption technology.

It is important to note that this is only one of the security techniques available but it is the best and most comprehensive one that will ensure validity of transactions and communications even if the channels are insecure.

4. AUDITING VALIDITY ISSUES

This chapter will introduce my findings from the research and introduce a proposed questionnaire or checklist that can be used to audit validity issues. This is discussed under the following headings:

4.1 Objective
4.2 Background
4.3 Checklist
4.4 Conclusion

4.1 OBJECTIVE

The objective of this chapter is to assess if validity issues can be addressed by the use of audit techniques. A checklist for use by the auditor (both internal and external) will be developed to highlight the points that must be considered when a business transacts electronic commerce in the GII.

4.2 BACKGROUND

New business applications have emphasised the need for far more than encoding and decoding; functions such as user identification and authorisation, access control to resources and services, confidentiality, data integrity, non repudiation of transactions, security management and audit are all critical functions that must be addressed by technology and encryption supports all of these technologies (IBM 1996:2).

Validity is one of the risks and includes integrity and confidentiality of transactions and is the major concern of doing business on the GII. Traditional data security should still be kept in place but should be extended to cater for electronic commerce. Logical and physical security should ensure that transactions even in transmission mode are secure. Controls to ensure communication security should be in place (SAICA, 1995: 12).

Any auditing procedures will depend on the nature of the computer environment but the nature of auditing procedures will not change. However the nature of audit evidence, procedures to obtain such evidence, timing of procedures and extent of these procedures may change (SAICA, 1989: para 89). The audit opinion expressed by external auditors in their independent report to the shareholders of a company expresses an opinion on the fairness and reasonableness of the presentation of the annual financial statements and the internal auditors' report expresses their opinion on whether the internal controls functioned adequately, effectively and efficiently.

The internal and the external auditor should be involved in the change in business processes to accommodate electronic commerce and the use of the Internet at the earliest possible stage, and workshops should be held to address the issues of controls, security and auditing and accounting procedures. This should be done before the business plan is developed to facilitate specific controls and procedures that should be included in the plans and programs. The auditors will then be actively involved in the implementation process to ensure that the final system conforms to auditing and control requirement to minimise and identify risks (Van Aardt, 1995:212).

The internal auditors must stay abreast of the development of the latest techniques and advances on the GII and should be able to advise the corporation on the best control measures that can be implemented

within the cost restraints of the company. A more proactive and advisory role should be played by the internal and external auditors.

Their audit techniques will now also change to the use of more CAATS and BEASTS to cater for the large volumes of data that require scrutiny and to gain a quick understanding of the information environment of their client.

4.3 CHECKLIST

The following is a proposed checklist that can be utilised by the internal and external audit and the business manager concerned by the risks involved when transactions and electronic commerce are conducted over the Internet or GII. This list is a starting point for questions that should be raised, and must be expanded and adapted for the specific circumstances and environments present within the particular business. It also only addresses some of the general controls required and focuses on transmission security and secrecy of transactions. The internal controls over the internal information system environment are not covered but this checklist could be an extension of the controls that should be present in this environment.

This checklist set out in table 4.1 could form the basis for a long term audit plan to be conducted by the internal and/or external auditors based on their risk assessment of the environment. A variety of tests can then be performed to check the controls over these risks over a period of time. If a control is not in place and there is no compensating control then this should be brought to the attention of management and appropriate corrective action taken. The recommendation and agreed action should be tested in a follow up to ensure that the

recommendation has been implemented and that the risk is now controlled in a satisfactory manner on a consistent basis.

This checklist assumes that the change to electronic commerce and GII has already been done and that this process has been adequately managed and controlled. The reference is to the specific paragraphs in the dissertation.

NO	CONTROL MEASURE	REF
	General controls	
1	Obtain and document information on the current control environment and structure of the information services division.	
2	Ascertain the assessment of risk by management and their perception of the adequacy of the controls in place. Ensure that all the risk were identified and are addressed.	2.8
3	Obtain the assessment of risks and controls from the internal or external auditors or both. Evaluate control testing procedures.	2.9
4	Evaluate the adequacy of hardware used in relation to the volume and sensitivity of business transactions.	
5	Evaluate the interchangeability/ transferability of information between the EC/ GII external link with that of the internal information infrastructure and architecture of the corporation.	
6	Evaluate the documentation of procedures and ensure that it has been approved at the appropriate level.	
7	Ensure that approval has been obtained from the appropriate authority to ensure documentation and data storage are acceptable.	
8	Ensure that alternatives for trading partners which do not trade at the same level of sophistication (not on EDI/GII) are in place and are efficient and effective.	2.8

NO	CONTROL MEASURE	REF
9	Ensure that the agreements with trading partners clearly define the roles and responsibilities of all parties and that these are up to date and signed by the appropriate authority.	2.9
10	Evaluate whether the information services' mission, goals and long term plan are in line with the business objectives and mission to ensure that effective use is made of all business processes.	
11	Ensure adherence to GII policies on a test basis.	
12	Evaluate the disaster recovery plan of the EC/ GII platform and data information and continuity of business in case of a disaster.	
13	Ensure that the trading partner's internal controls have been assessed.	
	GII transaction controls	
14	Evaluate the access controls and authority for the release of transactions over the Internet or GII.	
15	Evaluate the risks and controls implemented in particular categories of transactions and/or transactions conducted with particular trading partners.	1.4 2.7 2.8 2.9
16	Evaluate the public liability and other insurance cover of the company and ensure that this includes transactions over the GII and the exposure of loss of confidentiality during transmission.	
17	Ensure that all laws and regulations are adhered to.	2.3 2.5
18	Ensure that the internal networks of the corporation are protected against intrusion and viruses by the appropriate mix of software and hardware security such as firewalls.	1.2
19	Ensure that a reporting policy of any intrusions or breach of controls is in place and that the appropriate corrective actions have been taken in the case of such events.	2.10

NO	CONTROL MEASURE	REF
20	Ensure that the appropriate encryption technology has been purchased from a reputable dealer and that all the requirements of the management of that technology have been adhered to.	3.11 3.8
21	Ensure that the supplier and the product adhere to international standards such as FIBS 140-1.	3.8
22	Ensure that a proper key management policy and procedures are in place and are being followed.	3.5
23	Ensure that confidentiality and security of private keys are managed.	3.5 3.9
24	Ensure that appropriate management review and audit logs are in place specifically relating to the identification of transactions outside the scope of the norm.	
25	Evaluate management's active involvement in and commitment to security issues and fostering of a "fraudless" corporation.	
26	Ensure transmission service provider adheres to similar technologies and security frameworks.	
26	Ensure that a policy exists that identify the transactions and data that must be encrypted.	
28	Ensure that all international and local initiatives on the GII be brought to the attention of management to keep them abreast of the latest developments and standards.	2.6

Table 4.1 *Audit checklist.*

4.4 CONCLUSION

This chapter highlighted the audit risks and a checklist has been developed to focus on issues that should at least be addressed by a corporation. It is important that the auditor use very tool available to ensure that the risks are addressed and that a detailed knowledge is

obtained and maintained on the client's procedures and the technology used by the client. The checklist is one of the tools that can be used. The objectives have thus been achieved.

5. CONCLUSION

In this chapter, the conclusion of the research is reached and areas for further research and study identified under the following headings:

5.1 Achievement of objectives
5.2 Applicability of results of research
5.3 Future research

5.1 ACHIEVEMENT OF OBJECTIVES

This short dissertation set out to achieve through a literature survey whether encryption technology can address validity concerns of a business when conducting transactions and data transfers through the GII, or its present form, The Internet. A checklist of controls within this framework has also been developed as an indication of the risks and controls that should be looked at by the corporation and its auditors. The research has focused on these key issues.

Although there are many other factors, risks and controls that should also be addressed and considered, these fell outside the scope of the research conducted. The GII and its development are still in a developing phase and many key issues still have to be agreed upon by the global nations and within each country on the political, economic, legal and taxation environments. A co-ordinated approach will have to be followed and all countries should follow international agreements and conventions as the GII will transcend all borders and even, "for better or for worse", any legal restrictions.

The development of encryption technology, although in existence for many years and well established, is changing at such a rapid rate due to the potential breaking of ciphers that continued research and development will take place. Standards will have to be adopted by all the suppliers of such technologies and customers should ensure that the appropriate level of security is achieved by the technology and key strength they buy and implement in their corporation.

The control and measurement of the effectiveness, efficiency and adherence to controls to minimise risks within the GII are the domain of the internal and external auditors. They will also have to ensure that their methodologies and audit approaches are risk orientated and in tandem with the development of new technologies. This will only be achieved by ongoing research and education. Their primary role should shift from reporting weaknesses to a more proactive value added role of identifying risks and recommending prevention controls before security, integrity, confidentiality and validity of transactions are compromised.

The employees and public in general should also be kept informed of developments in this field as the GII will have a direct impact on their lives. If a sense of security can not be instilled in and proven to them, the failure of the GII initiative and any expansion of electronic commerce beyond only governments and selected organisations will be inevitable.

5.2 APPLICABILITY OF RESULTS OF RESEARCH

The research conducted in this short dissertation indicated that the validity of a transaction can be securely conducted on the GII. This should give comfort to businesses and the public at large that there is a technology available that will secure the privacy of transactions on the GII and that this technology is sound and well developed.

Security is however only as strong as the weakest link in the chain and it should always be ensured that there is the maximum improvement in local security within an organisation which should include (Network Working Group, 1991:6):

- Statement of local security policy which must be communicated to all parties transacting with a corporation. This must be in writing and on file;
- Adequate security controls must be implemented via access controls and system configurations;
- Monitor security compliance and respond to violations. Record activity in logs and audit these regularly;
- Establish a chain of communication to handle security matters; and
- Respond in a timely and effective manner to security incidents through tough and uniformly applied disciplinary procedures.

5.3 FUTURE RESEARCH

The research of this short dissertation indicates several other fields where research and dissemination of information must still be conducted and which could lead to a specialised field within the audit and technology disciplines within academia and in business.

The development and adequacy of law of electronic commerce and transacting on the GII require urgent attention and will affect local, common and international law on a wide range of subjects affected by the GII.

Taxation treatment of transactions will have to be incorporated in international tax treaties and local tax laws and certain countries such as South Africa will have to consider the fundamental principles of their tax law such as the source principle when transactions are subject to tax on the GII.

Uniform standards and protocols will have to be implemented on a global basis and the acceptance of these protocols without any legal or governmental enforcement should be researched.

The complete security package for model organisations should be researched to define a framework that will address all the security and risk needs of a specific or generic organisation conducting the full scope of business on the GII. This should not only include financial aspects but also issues such as marketing, training, virtual offices etc. This should result in a matrix that could show the relative effectiveness, interrelationships and the best combination of security controls such as firewalls, encryption for Intranets, LANs and VANS.

A detailed audit plan that can address all the business risk issues from a financial point of view should be developed. This short dissertation only focused on validity concerns and concluded in a short checklist that could be followed but a deeper analysis of all audit risks and the impact of the GII, should be considered for research on auditing of GII transactions. This could also lead to the development of specific CAATS tools for use by the auditor and business.

6. BIBLIOGRAPHY

1. CLINTON, WJ & GORE A 1996: A framework for global electronic commerce. [Online]. Available URL address: http://www.iitf.nist.gov/ipc/.

2. COMPUTER SYSTEMS POLICY PROJECT 1997: Perspectives on the global information infrastructure. [Online]. Available URL address: http://www.cspp.org/reports/perspectives.html.

3. COOPERS & LYBRAND LLP 1996a: Future trends: Business models as enablers to electronic commerce. [Online]. Available URL address: http://raw.rutgers.edu/raw/iia/ec.trnd.htm.

4. COOPERS & LYBRAND LLP 1996b: Security issues to consider in developing EC systems on the Internet. [Online]. Available URL address: http://raw.rutgers.edu/raw/iia/.

5. COOPERS & LYBRAND LLP 1996c: Today's security solutions. [Online]. Available URL address: http://raw.rutgers.edu/raw/iia/ec.tss.htm.

6. DAMIANIDES, M 1991: a control model for the evaluation and analysis of control facilities in a simple path context model in a MVS/XA environment. Johannesburg: RAU (M.Com research essay).

7. DELLINO, DJ 1996: An introduction to CryptoSystems of the Internet.

8. DELOITTE & TOUCHE 1995: Information protection, your business and the Internet New approaches for new environments. Deloitte & Touche LLP. [Online]. Available URL address: http://www.dttus.com/publish/briefing/internet/intern01.htm.

9. DELOITTE & TOUCHE 1996: Taking the mystery out of encryption. Information Protection brochure. [Online]. Available URL address: http://www.dttus.com/publish/mystery/encrypt.htm.

10. EUROPEAN SECURITY FORUM 1995: The Internet and security. A guideline for managers. London.

11. GIIC 1997: Global Information Infrastructure Commission: "Platform Service Business" Encryption, security and self-expression on the battlegrounds of the information revolution. [Online]. Available URL address: http://www.gii.org/egi00250.html, http://www/gii.org/egi00263.html.

12. GORE, A 1994: GII Buenos Aires Speech. [Online]. Available URL address: http://icg.stwing.upenn.edu/cgi-bin/mfs/02/0949.html.

13. IBM 1996: IBM SecureWay cryptographic infrastructure. IBM Corporation. [Online]. Available URL address: http://www.ibm.com/security/html/wp_sc.html.

14. IBM 1997: IBM SecureWay internet technical direction; IBM Corporation. [Online]. Available URL address: http://www.ibm.com/security/html/wp_techdir.html.

15. INFORMATION INFRASTRUCTURE STANDARDS PANEL 1997: IISP security standards needs. [Online]. Available URL address: http://www.ansi.org.

16. INFORMATION TECHNOLOGY INDUSTRY COUNCIL 1997: Response of the Information Technology Industry Council to the Information Infrastructure Task Force's paper "Options for promoting privacy".

17. KOSIUR, D 1997: Keep your data secure from prying eyes: An encryption primer. SunWorld. [Online]. Available URL address: http://www/sun/com/sunworldonline/swol-03-encrypt.html; Web Publishing Inc.

18. MEYER, CH & MATYAS SM 1982: Cryptography: a new dimension in computer data security. New York: John Wiley & Sons.

19. MICROSOFT ® ENCARTA 1994. Microsoft Corporation.

20. NATIONAL INFORMATION INFRASTRUCTURE 1997: What is the GII. [Online]. Available URL address: http://nii/nist.gov/whatgii.html.

21. NATIONAL INFORMATION TASK FORCE 1997: Options for promoting privacy on the National Information Infrastructure Information. Policy Committee draft for public comment.

22. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 1993: Data Encryption Standard (DES). Federal Information Processing Standards Publication FIBS 46-2. US Department of Commerce.

23. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 1994: Security requirements for cryptographic modules. Federal Information Processing Standards Publication FIBS 140-1. US Department of Commerce.

24. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 1997: Federal Information Processing Standards on computer security. US Department of Commerce. [Online]. Available URL address: http://csrc.ncsl.nist.gov/fips/.

25. NETSCAPE 1997: Cryptography is the key to Internet security needs; White paper. Computer Reseller News.

26. NETWORK WORKING GROUP 1991: Guidelines for the secure operation of the Internet; rfc1281. [Online]. Available URL address: http://cgi.gnacadamy.org.

27. OECD 1992: Guidelines for the security of information systems. [Online]. Available URL address: http://www.oecd.org/dsti/iisp/.

28. OECD 1997: Cryptography Policy guidelines recommendations of the council concerning guidelines for cryptography policy. [Online]. Available URL address: http://www.oecd.org/dsti/iisp/crypto/e.html.

29. SAICA 1989: Auditing in a computer environment. Johannesburg.

30. SAICA 1995: Paperless business transactions, an introduction to the risks and controls. Kengray.

31. SAICA 1996: Controlling paperless business transactions. Kengray.

32. SECURITY AND CONTROLS: Security and controls the linear system development lifecycle. [Online]. Available URL address: http://dingo.vut.edu.au/~pauld/sdesign/notes7.htm.

33. SIMMONS, GJ ed 1991: Contemporary cryptology. New York: Institute of Electrical and Electronics Engineers, Inc.

34. SUNSITE 1997: The administration's agenda for action. [Online]. Available URL address: http://www.sunsite.unc.edu/nii/NII.

35. THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 1991. Third edition.

36. THE CONCISE COLUMBIA ENCYCLOPEDIA 1991.

37. UNITED STATES OF AMERICA. Acts: SAFE Act of 1997: Summary of the security and freedom through encryption (SAFE) Act of 1997 HR 695; Bill summary & status for the 105th Congress.

38. VAN AARDT, AH 1995: The strategic implications of electronic commerce on management. Johannesburg: RAU (D.Com thesis).

39. VAN TILBORG, HCA 1989: An introduction to cryptology. Norwell, Massachusetts, USA: Academic Publishers.

40. YLöNEN, T: Introduction to Cryptography. [Online]. Available URL address: http://www.cs.hut.fi/ssh/crypto/intro.html.