# TOWARDS AN INFORMATION SECURITY FRAMEWORK FOR GOVERNMENT TO GOVERNMENT TRANSACTIONS: A PERSPECTIVE FROM EAST AFRICA

by

CARINA KABAJUNGA WANGWE

submitted in accordance with the requirements
for the degree of
DOCTOR OF PHILOSOPHY
in the subject of
COMPUTER SCIENCE
at the
UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF. MM ELOFF
CO-SUPERVISOR: PROF. LM VENTER

October 2012

**Summary**

The need for a regional framework for information security in e-Government for the East African Community (EAC) has become more urgent with the signing in 2009 of the EAC Common Market Protocol. This protocol will entail more electronic interactions amongst government agencies in the EAC partner states which are Burundi, Kenya, Rwanda, Tanzania, and Uganda.

Government to Government (G2G) transactions are the backbone of e-Government transactions. If a government wants to provide comprehensive services that are easy to use by citizens, employees or businesses, it needs to be able to combine information or services that are provided by different government agencies or departments. Furthermore, the governments must ensure that the services provided are secure so that citizens trust that an electronic transaction is as good as or better than a manual one. Thus governments in the EAC must address information security in ways that take into consideration that these governments have limited resources and skills to use for e-Government initiatives.

The novel contribution of this study is an information security framework dubbed the TOG framework, comprising of technical, operational, governance, process and maturity models to address information security requirements for G2G transactions in the EAC. The framework makes reference to standards that can be adopted by the EAC while taking into consideration contextual factors which are resource, legislative and cultural constraints. The process model uses what is termed a 'Plug and Play' approach which provides the resource poor countries with a means of addressing information security that can be implemented as and when resources allow but eventually leading to a comprehensive framework. Thus government agencies can start implementation based on the operational and technical guidelines while waiting for governance structures to be put in place, or can specifically address governance requirements where they already exist. Conversely, governments using the same framework can take into consideration existing technologies and operations while putting governance structures in place.

As a proof of concept, the proposed framework is applied to a case study of a G2G transaction in Tanzania. The framework is evaluated against critical success factors.

**Dedication**

To Angela, Steve, Magige and the Gals.

**Acknowledgements**

I wish to thank my promoters Professor Eloff and Professor Venter for their patience and encouragement throughout my studies. I also acknowledge the help received from the administrative staff and librarians at UNISA and from the Financial Services offices of UNISA in form of bursaries.

I wish to thank all those staff in government agencies and departments in Rwanda, Tanzania and Uganda for their help in responding to questionnaire surveys, requests for interviews and in giving me the necessary information to conduct this study.

I acknowledge the support that I received from my employer, colleagues, friends and family. I would particularly like to thank Vupe, Robert, Goodluck, Irene, Kiiza, Ayeta, Donna and Magige for their help in understanding the legal environment, evaluating the framework and proof reading this thesis.

**Declaration**

I declare that "TOWARDS AN INFORMATION SECURITY FRAMEWORK FOR GOVERNMENT TO GOVERNMENT TRANSACTIONS: A PERSPECTIVE FROM EAST AFRICA" is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

## Table of Contents

**List of Figures**

**List of Tables**

**List of Acronyms**

| | |
|---|---|
| ABAC | Attribute Based Access Control |
| CAS | Central Admissions System |
| CEN | European Committee for Standardization |
| CSFs | Critical Success Factors |
| EAC | East African Community |
| FEA | Federal Enterprise Architecture |
| G2B | Government to Business |
| G2C | Government to Citizen |
| G2E | Government to Employee |
| G2G | Government to Government |
| GABAC | Governance & Attribute Based Access Control |
| GBAC | Governance Based Access Control |
| GPPS | Government Pensioners Payroll System |
| GRC | Governance, Risk and Compliance |
| GWEA | Government Wide Enterprise Architecture |
| IEC | International Electro technical Commission |
| ISMS | Information Security Management System |
| ISO | International Organization for Standardization |
| MDA | Ministries, Departments and Agencies |
| MIOS | Minimum Interoperability Standards |
| NICI | National Information and Communication Infrastructure |
| NIST | National Institute of Standards and Technology |
| OECD | Organization for Economic Co-operation and Development |
| PDCA | Plan – Do – Check – Act |
| PKI | Public Key Infrastructure |
| RBAC | Role Based Access Control |
| SAML | Security Assertion Markup Language |
| SOA | Service Oriented Architecture |
| SSL | Secure Sockets Layer |
| TISS | Tanzania Interbank Settlement System |
| TOG | Technical - Operational - Governance |
| XACML | eXtensible Access Control Markup Language |
| WS | Web Services |

## List of Publications

### Journal Paper

1. Wangwe, C K, Eloff, M.M, Venter, L.M., (2012). A Sustainable Information Security Framework for E-Government – Case of Tanzania. *Technological and Economic Development of Economy*, 18(1), 117-131.

### Conference Proceedings

1. Wangwe, C.K., Eloff M.M., Venter, L.M.; (2009) *E-Government Readiness: An Information Security Perspective from East Africa*, IST-Africa 2009 Conference Proceedings, Paul Cunningham and Miriam Cunningham (Eds), Published by IIMC International Information Management Corporation, 2009, ISBN: 978-1-905824-11-3, 06 - 08 May 2009, Uganda
2. Wangwe, C.K, Eloff, M.M., Venter, L.M., (2008) Towards A Context-Aware Access Control Framework for Web Service Transactions, Research-in-Progress papers, ISSA2008, 7 – 9 July 2008, Johannesburg, South Africa, available online http://icsa.cs.up.ac.za/issa/2008/Research_TOC.htm
3. Wangwe, C.K, Eloff, M.M., Venter, L.M., (2008) A Proposed Implementation of SAML V2.0 in an e Government Setting, in Proceedings of IST-Africa 2008 Conference & Exhibition, Windhoek, Namibia, 07 - 09 May 2008, ISBN 978 1-905824-076

# PART I: INTRODUCTION

# Chapter 1 Introduction and Background

## 1.1 Introduction

This chapter introduces the major concepts that will be referred to throughout this thesis, which are e-Government and Information Security. A background of the East African Community (EAC) which is the contextual setting to this study is outlined, together with a statement of the problem to be resolved. This chapter also lists the general and specific objectives of the study and the methodology used. The layout of the entire thesis is presented at the end of the chapter.

For purposes of this thesis, e-Government is defined as the use of information and communication technologies to enable efficient and cost effective processes in government that lead to the provision of citizen centric services through channels such as the Internet and mobile phones. The kind of transactions that take place within e-Government can be categorized as follows:

- Government to Citizen (G2C) services in which a citizen usually initiates a transaction by requesting a service such as applying for a driver's license, or requesting information through a web based portal or SMS service. A government may also publish information and electronic forms that citizens need on a website.
- Government to Business (G2B) in which governments interact with businesses, for example for tax filing. The interaction is usually through a portal.
- Government to Employee (G2E): The Government as an employer provides electronic services to employees through an intranet. Examples are online leave processing and performance appraisals.
- Government to Government (G2G): These are transactions between one government agency and another (within a country or across countries). These transactions may be as a result of a G2C or a G2B service request or simply a requirement between two agencies. Government agencies may give each other access to their information systems or publish web services that can be accessed by authorized users.

The concept of e-Government has been greatly enabled by advances in Internet related technologies and has been pushed by the need of Governments to provide efficient, effective, affordable and quick services to citizens. The need for increased accountability and transparency is another factor that has led to attempts by governments to move towards e-Government (United Nations, 2008). While many developing countries are making steady progress in terms of building infrastructure and providing access to digital information and services to their citizens (United Nations, 2010), it is important that measures to ensure the security of that information are taken as part of any e-Government initiative. Addressing Information Security is one of the critical success factors of e-Government implementations given that governments handle large amounts of confidential information (President's Office, 2009; United Nations, 2008; Conklin, 2007).

Information Security is defined in the Computer Science and Communications Dictionary (Weik, 2001) as the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. Information security management is an area that has been addressed through guidelines and standards from various organizations (NIST, 2006; ISO/IEC, 2005b; OECD, 2002). Technical, operational and management perspectives on information security have been presented in standards and guidelines. These guidelines have been put into practical use in many countries and are largely based on achieving the security goals of Confidentiality, Integrity and Availability (CIA). Furthermore, Accountability is now becoming another important principle as electronic transactions need to be traceable and parties held accountable for their actions. However, information security depends on the context in which it is being applied and the addressing of information security starts with a risk assessment and an understanding of the particular context in which security is being addressed (Hayat, Reeve, & Boutle, 2007; Siponen & Willison, 2009).

This study specifically looks at information security for G2G transactions. A G2G transaction for the purpose of this study is defined as:

*The sharing of information resources and services between government agencies in a restricted network setting with the ultimate aim of providing comprehensive, easy to access services to citizens.*

The role of G2G transactions in e-Government is illustrated in Figure 1-1.

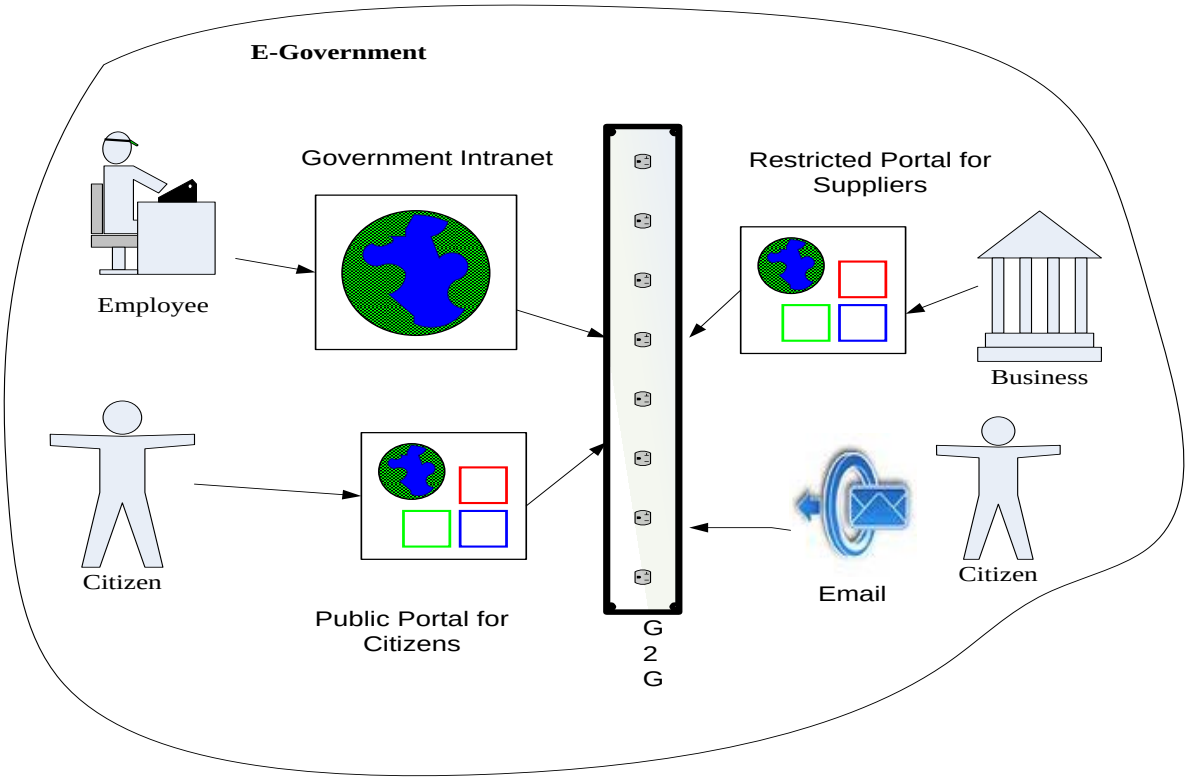



Figure 1-1 G2G in e-Government

Figure 1-1 illustrates that a transaction between a citizen, employee or business through a portal or intranet is likely to trigger collaboration amongst two or more government agencies. Thus for a government to provide efficient G2B, G2C or G2E services, a robust G2G backbone must be in place.

Consider, for example, the case of a citizen applying for a driver's license online. This request may result in a cross check of information with the government agency that deals with identification of citizens, with the government agency that deals with traffic or road safety and with an agency that deals with the establishment of the age of the citizen. While the citizen may be required to register their request at one point, the details need to be sent

electronically to all the agencies involved, the information retrieved from the agencies collated and used to trigger a response to the request. The inter-agency collaboration that will result from the citizen request, which is the G2G transaction, needs to meet the security goals of Confidentiality, Integrity, Availability and Accountability. In other words, the individual information security requirements of each agency should be preserved in the joint collaboration. This is a challenge considering that each agency may have different security policies and different technological platforms on which data is stored. Furthermore, other security risks to G2G collaboration may arise as a result of the context in which the transaction is taking place.

A typical G2G transaction can be viewed as in figure 1-2 below.

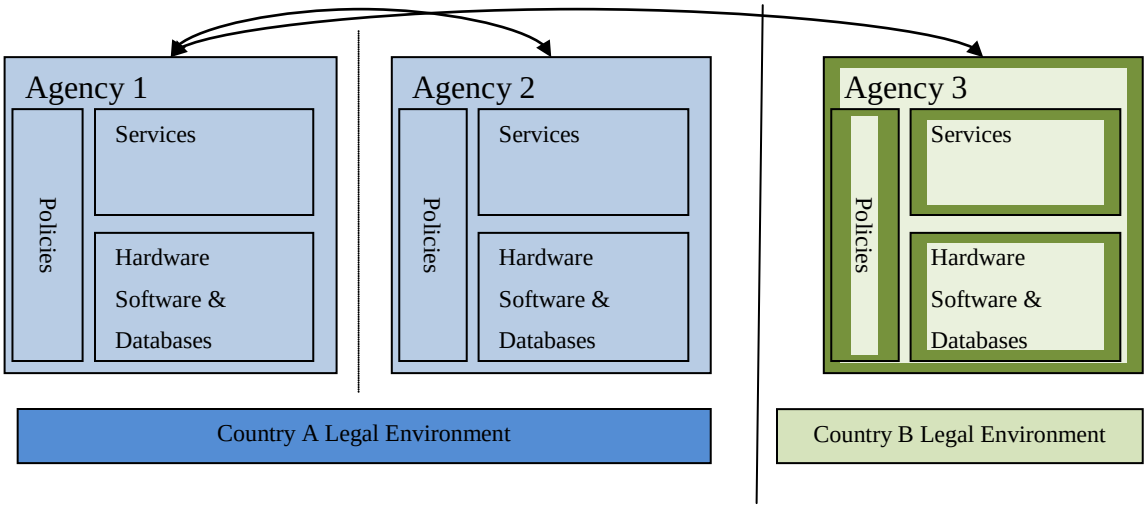



Figure 1-2 G2G Transaction

Figure 1-2 illustrates that a G2G transaction may be between two agencies in the same country or across borders. The challenges that need to be addressed in proposing an information security framework for such transactions include:

- Differences in the organizational policies in each agency.
- Differences in Hardware, Database and Software platforms in the agencies.
- For transactions going across countries, legal environments may differ, and regional laws do not necessarily exist.
- Laws and policies may change or new laws may arise. This should not affect the applicability of the proposed framework.

- The approaches to handling information security may vary due to resource limitations in the individual agencies, and organizational priorities within that agency.
- Each government agency is a potential provider and a consumer of services; in both cases they must be ready for secure collaborations.

The framework proposed must also take into consideration the contextual issues. The risks identified for a G2G transaction between government agencies in Switzerland for example, will be different from those in Tanzania because of different cultural (Chaula, Yngstrom, & Kowalski, 2006), infrastructural, resource and policy environments (Ezz & Themistocleous, 2005).

This study uses three countries in East Africa to determine what issues need to be addressed so as to come up with a robust information security framework that can be applied successfully in the East African Community.

## 1.2 Background

The East African Community (EAC), as at the beginning of 2010, comprised of a block of five countries namely, Burundi, Kenya, Rwanda, Tanzania and Uganda. The positioning of these countries within Africa is shown in the map in Figure 1-3.

The EAC has undertaken various e-Government initiatives in recent years, introducing e-Government strategy documents both at country and regional level and various legislations to enable e-transactions. Furthermore, projects towards delivery of services and citizen participation have been undertaken or are in progress in Rwanda (Ndahiro, 2009) and Uganda (De Jager & Van Reijswoud, 2007). Details of these e-Government initiatives are presented in chapter five of this thesis.

The use of e-Government promises a wealth of benefits for the countries in the EAC if implemented successfully. The countries of the EAC, namely, Burundi, Kenya, Rwanda, Tanzania and Uganda, are all ranked in the bottom 50 countries in the world in terms of e-readiness out of 175 countries surveyed (United Nations, 2010). While there are few citizens

with access to personal computers (PCs) in the EAC, there is a proliferation of mobile phones which allow citizens' access to electronic services (Hellström, 2010).

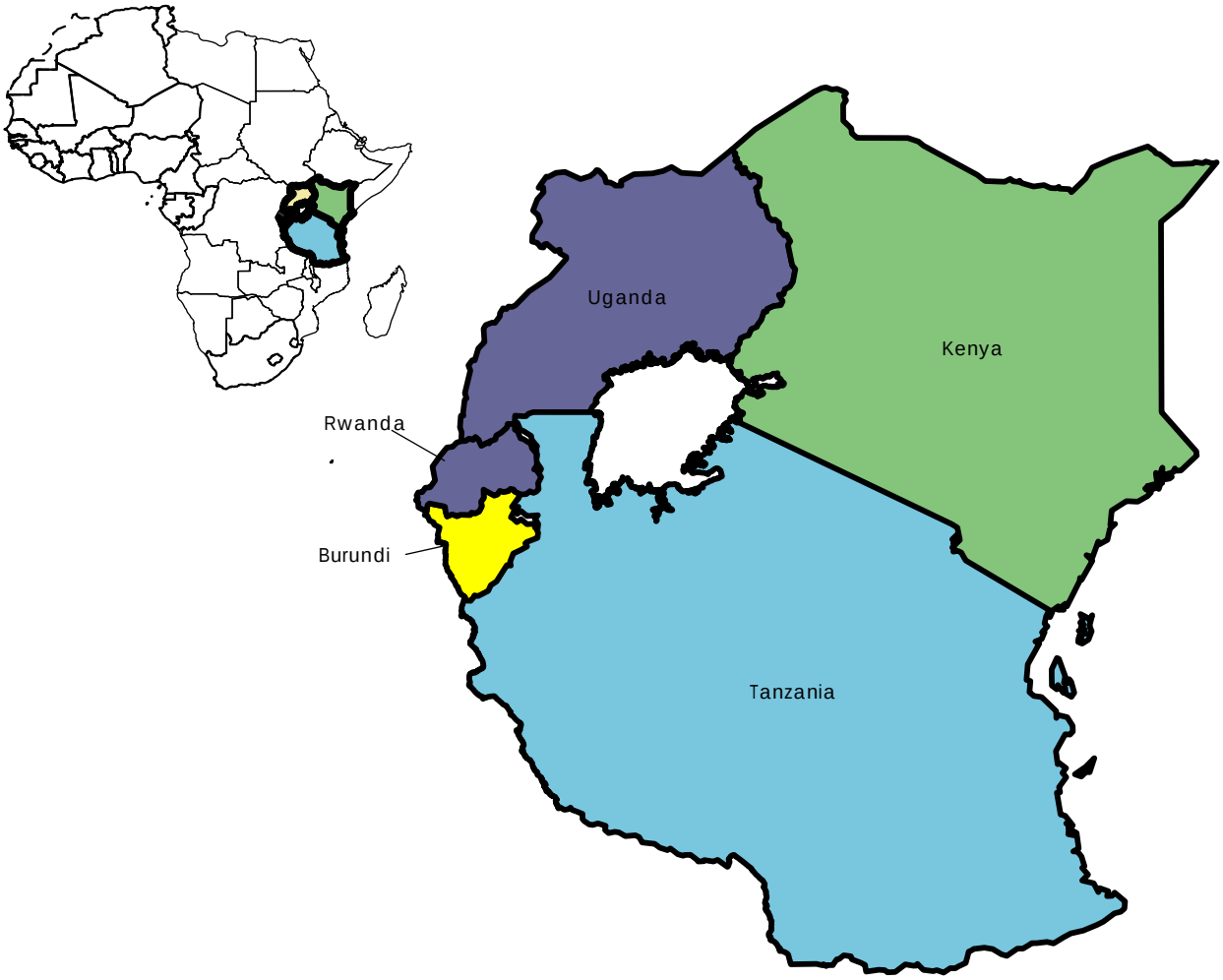



Figure 1-3 Map of the East African Community

In 2009, the governments of the EAC countries signed a common market protocol that is aimed at promoting free movement of labor, capital, goods and services; and harmonization of taxation (EAC, 2009). A successful implementation of the protocol will involve collaboration of government agencies in each country of the EAC and amongst the five partner countries.

The focus on e-Government implementations in the EAC needs to be not only on improved service delivery, but also on the underlying structures that will enable governments to offer

value added services to citizens. According to the UN e-Government Survey of 2008 (United Nations, 2008), where earlier emphasis of e-Government was mostly on developing e-services, the focus has shifted towards building and managing integrated and coordinated government services. The report also states that ICT-based connected governance efforts are aimed at improving cooperation between government agencies, allowing for enhanced active and effective consultation and engagement with citizens. The cooperation would involve multiple stakeholders regionally and internationally. In the UN e-Government Survey of 2010 (United Nations, 2010) e-readiness rankings for Tanzania and Rwanda improved since 2008, while the rankings for Uganda and Kenya declined. Burundi maintained the same ranking. The UN survey report does acknowledge that security is a major factor that hinders countries from providing more online services as the threat of fraud and identity theft is great.

Several studies have looked at the challenges of implementing e-Government and have identified the need to address technical, social and organizational factors which include the values, perceptions and key stakeholders in e-Government implementations. The studies by Heeks (2002); Chango (2007); and Schuppan (2009) which were carried out in the African context all recommend that the specific contextual issues be studied rather than adopting, without modification, solutions that have been applied in other regions of the world. In the specific EAC context, studies have been done mostly from an organizational management perspective and from the point of view of G2C transactions (Bakari, Tarimo, Yngstrom, & Magnusson, 2005; Karokola & Yngstrom, 2009). The need for a study that specifically looks at G2G transactions in the EAC is presented in the next section.

### 1.3 Motivation of the Study

This thesis focuses on Information Security for G2G transactions in the EAC context. The need to study the EAC is motivated by the EAC Mission Statement which is to "*widen and deepen Economic, Political, Social and Culture integration in order to improve the quality of life of the people of East Africa through increased competitiveness, value added production, trade and investments"* to be achieved through the implementation of e-Government as one of the strategies (East African Community, 2006).

The focus on G2G in particular is motivated by the potential role that G2G can play in the successful utilization of e-Government services, and more importantly the role that e-Government can have in the development of economy. The need for a developmental focus in ICT research in Africa is presented in a study by Thompson & Walsham (2010), who argue that without appropriate and sufficient research in the African context, it is difficult to apply ICT solutions to African contextual issues.

The specific focus on information security for G2G transactions is motivated by the influence of information security on the success of G2G and e-government implementations. A study by Ezz & Themistocleous (2005) presents ten barriers to the adoption of G2G as shown in figure 1-4.

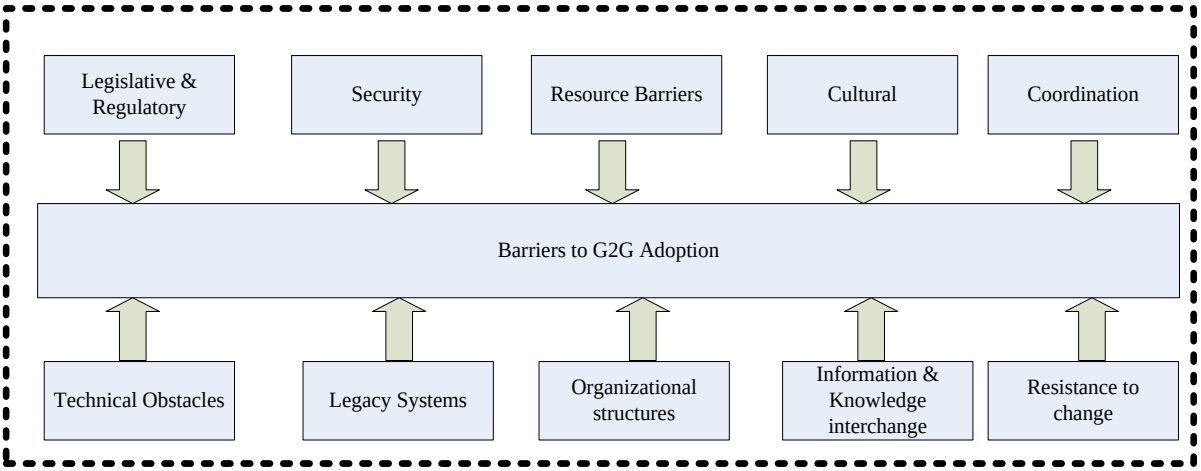



Figure 1-4 Barriers of G2G Adoption - (Ezz & Themistocleous, 2005)

These ten barriers would apply generally regardless of the context. However, in order to overcome barriers, it is necessary to study the context in which G2G is being applied. While security is presented as one of the barriers, all the other barriers have a bearing on robust information security management. The need for a specific perspective or context in information security is guided by studies cited in section 1.2 above, and other studies including Kayworth & Whitten (2010), and Loser et.al (2011) which have concluded that a

socio-technical approach is necessary for holistic addressing of information security. Thus while generic technical solutions may be applicable to information security problems, the social issues have to be addressed in the context in which the problem exists and therefore the solution is to be applied.

One of the areas to be explored is the contextual governance situation as represented by the legal & regulatory barrier. Governance is one of the major drivers of a successful e-Government implementation (Rose & Grant, 2010; OASIS, 2010a)and there is a need to propose a structured governance approach to information security that is applicable at a regional level.

Another area is to recognize and take into consideration the resource constraints, represented by the resource barrier in Figure 1-4. The resources include both financial and human resource skills related to ICT and e-government. The resource constraints in the EAC will be different from those in developed countries. Impediments to the use of ICTs and the growth of e-Government in African countries are discussed by Rezaian (2007)and Chen et al (2006) as including unreliable power sources, lack of government co-ordination, dependence on donor funding, and lack of adequate human resource skills. In a G2G setting, such impediments would be faced by government agencies and addressing these specific contextual issues would address barriers including cultural, organizational structures, and coordination.

The technical barriers identified in Figure 1-4 including technical obstacles, legacy systems, information and knowledge interchange can be overcome by applying generic technical mechanisms that will lead to technical interoperability that is needed to overcome these barriers in a G2G transactions. However there is still a need to explore the appropriate technical mechanisms for information security in the EAC given the resource constraints in this context.

Galpin (2008) suggests that in answer to African contextual issues with regards to application of ICTs, research from elsewhere in the world may be a starting point to understand how to effect change, but it must be noted that local, cultural and societal explanatory factors differ

from country to country. Solutions must, therefore, be assessed as to whether they are appropriate before they are applied. There is a need to ensure that sustainable solutions are found such as the use of open technical standards and to link these solutions to specific information security requirements.

The solution developed in this study can be extended or generalized for use in countries or regions that face similar contextual issues as in the EAC. Part III of this thesis presents the contextual issues in the EAC and points out the differences with other regions of the world. The framework developed in this study, and presented in part IV of this thesis, then specifically considers those contextual issues found in the EAC environment.

## 1.4 Problem Statement

As the EAC moves towards greater co-operation in various spheres such as common markets, common currencies and free labor movement, electronic transactions will become more pervasive and cross-border in their nature. Information security is a critical success factor in e-Government implementations, and particularly in G2G transactions. It needs to be addressed in the context of the transactions being secured, but there are no national or regional information security frameworks that have been adopted in the EAC. An Information Security Framework for G2G transactions is therefore necessary to ensure the take up of electronic transactions and successful implementations in resource-poor environments such as the EAC.

## 1.5 Objectives of the Study

### 1.5.1 General Objective

The general objective of this study is to add to the body of information security and e-Government knowledge by proposing an Information Security framework for G2G transactions in the context of the EAC. The information security framework shall be such that is can be generalized to apply in a setting with similar context to the EAC.

### 1.5.2 Specific Objectives

i. To define information security requirements in the EAC context for G2G transactions.

ii. To propose a framework that addresses the requirements identified.
iii. To evaluate the proposed framework.

### 1.5.3 Research Questions

i. What are the information security requirements for G2G transactions in the EAC context?
ii. What are the factors in the EAC that need to be addressed in an information security framework for G2G transactions?
iii. How can a sustainable information security framework for G2G transactions be achieved in the EAC context?

## 1.6 Research Methodology

### 1.6.1 Research Approach and Design

The overall approach followed in this study was largely an interpretive approach, with induction being used to draw conclusions. The reason for using this approach was the need to understand the context of the study and the researcher being part of the study process in order to fully answer the research questions. This approach is opposed to the deductive approach whereby given the dearth of readily available data in the EAC on e-government and information security – sufficient sample data for a quantitative analysis would not have been possible. The use of the interpretive approach in computer science and information systems research has been discussed by Bernsten, Sampson & Osterlie (2005) and de Villiers (2005).

Multiple methods were used to address the different facets of the research problem. The first method used is Appreciative Inquiry. Wirtenberg, Russell & Lipsky (2008) investigate the Appreciative Inquiry method as a tool towards developing sustainable processes. This method lends itself well to addressing this study's third research question, which is how sustainable framework for G2G transactions can be developed for the EAC context. However, in order to reduce bias that may result from using purely qualitative data, some quantitative data was employed for triangulation. This quantitative data was obtained through using a questionnaire survey as the method for eliciting the required information from Government Ministries, Departments and Agencies (MDAs). Furthermore, since this study

specifically addresses the EAC context, a case study from the EAC context was used as a 'proof of concept' of the information security framework that was developed.

Appreciative Inquiry is described by Olivier (2004), as starting with a discovery phase which is an appreciation of what already exists. Thus an exploration of research and practical implementations of information security in e-Government and particularly G2G was done as is presented in the next part of the thesis. The current EAC situation was also explored with regards to what e-Government initiatives and / or enabling structures are currently in place. The discovery phase is followed by the dream phase, which is what could it be. Then comes the design phase when models for improvement are developed and lastly the implementation phase.

In the discovery phase, investigation was undertaken to discover what research has been carried out on information security of G2G, what other countries have put in place in terms of information security for e-government, and what international standards exist. The discovery phase was also extended to investigate what the existing situation in the EAC is, with emphasis on the positive factors that can enable secure G2G transactions. For discovery in the EAC, a survey was carried out to obtain data on the information security practices in transactions among MDAs in three countries of the EAC, which are, Rwanda, Tanzania and Uganda, through the use of questionnaires.

The outputs of what was discovered were used in the Dream Phase to come up with a list of requirements of secure G2G transactions in the EAC. These requirements were the input for the Design phase, in which an information security framework for G2G in the EAC was developed. The framework developed comprises of five models which are a technical model; an operational model; a governance model; a process model; and a maturity model. In the Implementation Phase, the framework was applied to a case study of G2G transactions in the EAC. In keeping with appreciative inquiry approach – the focus was on a positive core, such that the framework can be implemented regardless of the factors that may not be enabling in the current EAC situation. The research approach and design is as illustrated in Fig 1-5 below.

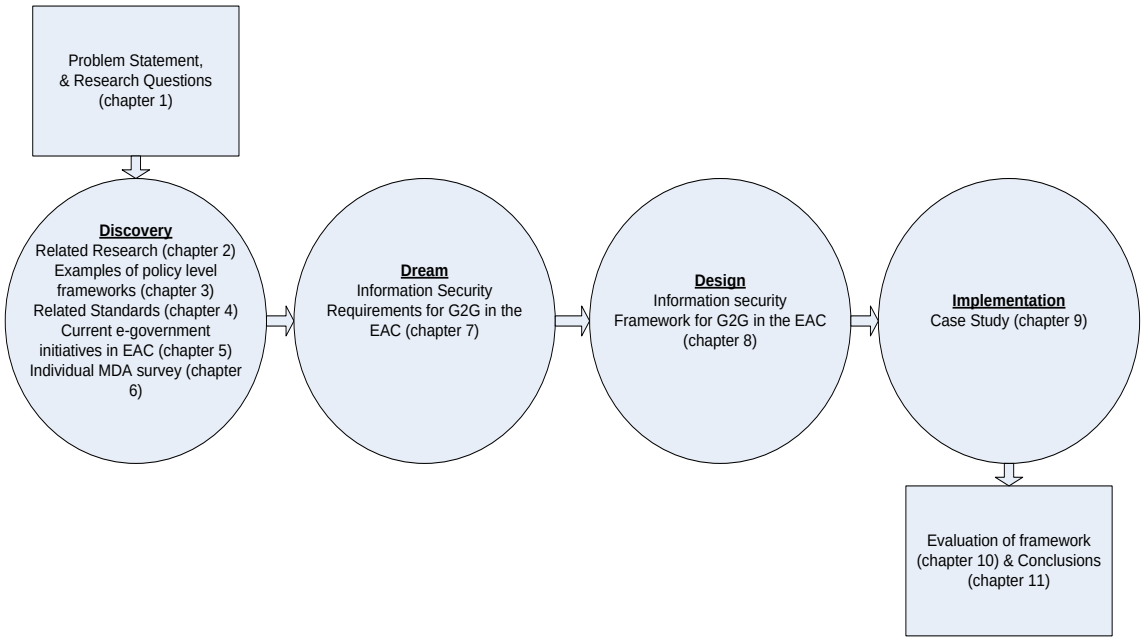



Figure 1-5 Research Approach & Design

The research approach and resultant methods were chosen on the basis of four factors which are:

i. Feasibility: The author of the thesis being a government employee in one of the countries studied and involved in e-Government projects has ample access to the necessary resources to carry out the discovery process and case study.

ii. Appropriateness: This study's main objective is to develop a framework that is applicable in the EAC context. While the framework may include a technical aspect, non-technical aspects shall be researched using the interpretive approach with appreciative inquiry. In addition, the lack of readily available data in the EAC region was another factor that influenced the choice of an interpretive approach.

iii. Validity, reliability and trustworthiness: To reduce subjectivity that may be introduced by using an interpretive approach, empirical data obtained from a survey is used to triangulate findings.

iv. Robust: The approach is likely to produce novel and significant results which are an information security framework for G2G transactions in the EAC context, which can be generalized for use in countries/ regions with similar contextual issues.

### 1.6.2 Evaluation of Research findings

The framework, which represents the novel findings of this thesis, was evaluated at the end of the study using Critical Success Factors (Bergeron & Bégin, 1989). The framework, presented in chapter eight of this thesis, is a unified framework consisting of five models. These models are a technical model, an operational model, a governance model, a process model and a maturity model. The critical success factors used to evaluate the framework are taken from one of the EAC country e-government strategy documents, and from the ISO – ISMS standard for information security management. It was found that the TOG framework addresses each of the Critical Success Factors. The extent to which the framework addresses the critical success factors is presented in detail in chapter ten of this thesis.

### 1.6.3 Research Scope and Limitations

The study was carried out in three countries of the EAC and investigated e-Government with a focus on G2G interactions. When the study started, the EAC comprised of 5 countries, namely Burundi, Kenya, Rwanda, Tanzania, and Uganda. By the time this thesis was being completed, one additional country had been admitted into the EAC, which is South Sudan.

Due to time limitations, and logistical difficulties in obtaining information, only three countries of the EAC were studied in detail, namely Rwanda, Tanzania and Uganda. At the time that information was being sought for this study from the various government agencies, Kenya was suffering from the after effects of post-election violence in early 2008, and Burundi was also experiencing upheavals that made it difficult to obtain information from government offices. At the same time, South Sudan had not yet come into existence as a country.

The information security framework proposed in this study includes both technical and non-technical (socio) mechanisms to address information security. The framework was evaluated using Critical Success Factors – which are well suited to a socio-technical framework. These are, however, not in themselves sufficient to evaluate the novel technical mechanism, which is Governance and Attribute Based Access Control (GABAC) for G2G transactions, proposed as part of the technical model of the framework. This is a limitation of the study and could be a basis for future work in the area of securing G2G transactions.

## 1.7 Significance of the Study

In section 1.3, a motivation of this study has been discussed. The findings of this study that are presented in part IV of the thesis open up new areas in the fields of information security and e-Government by:

i. Providing a new framework applicable to the EAC, that is a framework for information security in G2G transactions in the EAC context. The EAC context is investigated in detail in Part III of the thesis.
ii. Providing a process where none exists specifically that is a sustainable implementation process for the framework in the EAC context.

These contributions add to the field of information security by adding knowledge on contextual issues that face the EAC and how these can be addressed. The contributions also have a practical value of providing governments that face similar contextual issues to the EAC with a starting point for implementation of an information security framework for electronic G2G transactions which are becoming an inevitable part of government service delivery.

## 1.8 Layout of Thesis

This thesis is comprised of five parts. Part I contains the introduction and background to the thesis and consists of one chapter. This chapter describes the major concepts that are used in this study and introduces the background, problem statement and objectives of the study and the methodology used to conduct the study. It also includes a layout of the chapters in the thesis.

Part II is presents a literature study and background research, and starts off the discovery phase of our appreciative inquiry. Part II comprises of chapters two, three and four. Chapter two discusses relevant research in the fields of information security in e-Government. Chapter three examines examples of existing policy level information security and e-Government infrastructure in countries outside of EAC, while chapter four presents internationally accepted standards for information security that are applicable to G2G transactions. The motivation for Part II is to discover what proven solutions exist and identify how they can be reused to answer the research questions. Such reuse would result in reduced

costs in terms of cultivating the necessary skills and in terms of financial resources where open, non-proprietary solutions exist. This approach also contributes to answering the research question on how to achieve a sustainable framework. By looking at research from East Africa in chapter two, pointers towards the contextual differences between the EAC and other parts of the world are identified.

Part III, consisting of chapters five and six, is a situational analysis of e-Government initiatives and practices in East Africa from an Information Security perspective. Chapter five presents current e-Government practices and initiatives, while chapter six presents the findings of a survey on actual practices in government and in MDAs. Three countries were surveyed, which are Rwanda, Tanzania and Uganda. Part III concludes the Discovery phase of the study.

Part IV presents the major contributions of this study. It comprises of four chapters, namely chapter seven which represents the Dream Phase and details the information security requirements, and the components of a sustainable framework. At the end of chapter seven, the first research question has been answered. Chapter Eight presents the detailed framework while in chapter nine, a case study in which the framework is applied to a real-life G2G transaction is presented. Chapter nine thus presents the implementation phase of the study. In chapter ten, an evaluation of the framework using critical success factors is presented. At the end of part IV, all three research questions have been answered. In chapter ten, the framework is evaluated using Critical Success Factors. Thus all the three research questions are answered by the end of Part IV.

Part V, which consists of chapter ten, concludes the thesis and looks at further work. The thesis is structured as shown in Figure 1-6.

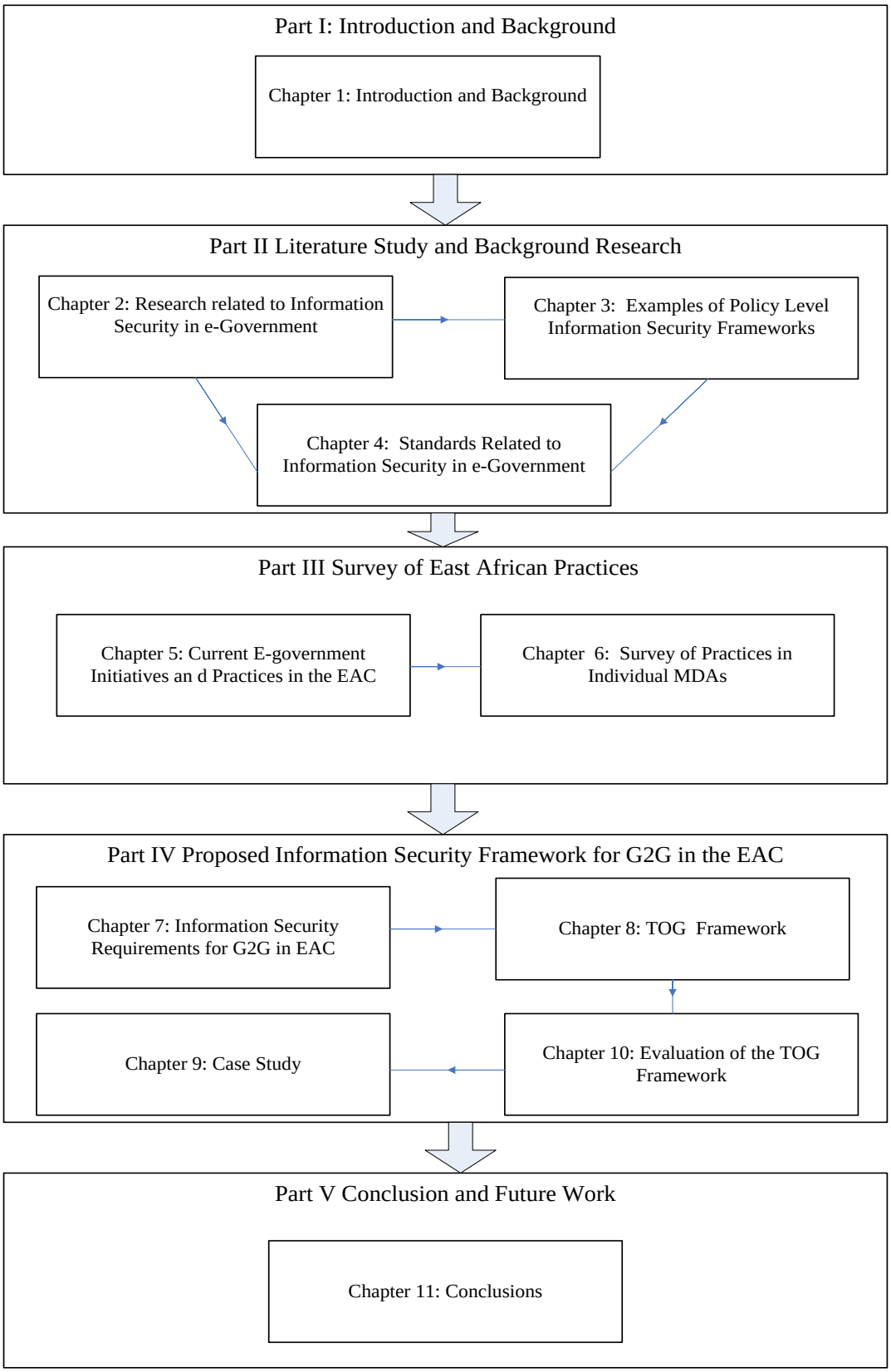



Figure 1-6 Layout of Thesis

## 1.9 Conclusion

This chapter has presented the background to the study, the problem statement, research objectives and methodology used in order to come up with the original research findings which are an extensible framework for information security in G2G transactions and a cost-effective and sustainable implementation process for the framework in the context of the EAC.

The assurance that an information system is secure is a challenge to any information system regardless of the nature of the transactions in that system. However, in meeting the challenge of addressing information security, solutions must take into consideration the context in which the proposed solution is to apply. The methodology proposed for this study is designed to address each of the research questions and ultimately meet the general objective of this thesis, which is to add to the body of knowledge in information security by proposing an information security framework for G2G transactions that takes the EAC context into consideration.

The framework proposed in this thesis is applied to a case study of a G2G transaction in one of the countries of the EAC. The framework is then evaluated using critical success factors drawn from international and national standards and policy documents.

In the next part of the thesis, a study of literature that is related to this study is presented. The purpose of the literature review is to establish what information security standards, frameworks or academic research is available and how this literature relates to the research questions. The findings of this part will be combined with the EAC contextual issues addressed in part III of the thesis and will contribute to the design of the information security framework for G2G transactions in the EAC.

# PART II: LITERATURE STUDY AND BACKGROUND RESEARCH

# Chapter 2 Research Related to Information Security in e-Government

## 2.1 Introduction

In this section of the thesis, which is the first part of the discovery stage of the appreciative inquiry, an exploration of research related to the research questions is done. The research questions are: What are the information security requirements for G2G transactions in the EAC? What are the factors to be addressed in an information security framework for G2G transactions in the EAC? and How can a sustainable information security framework for G2G transactions be achieved in the EAC context?

The three research questions focus on three areas which are information security requirements for G2G; the EAC context; and sustainable information security frameworks. The related research presented in this chapter is therefore presented along the focus areas of the research questions in three categories. These are information security requirements for e-Government in general and G2G in particular. The next category is research in the EAC context. For the EAC context, additional research was carried out during this study to obtain sufficient background information to answer the research questions. The findings are presented in chapter five of this thesis. The last category presented in this chapter addresses research related to sustainable frameworks.

## 2.2 Information Security Requirements for e-Government.

This section discusses research that has been published on information security requirements for e-Government and for technical mechanisms that may be used to meet these. The focus areas of the studies presented in this section are general security requirements, access control and security management.

### 2.2.1 Security Requirements

The security requirements for e-Government implementations are discussed by Zissis and Lekkas (2011) in five broad categories which are Availability, Confidentiality, Integrity, Authenticity, and Accountability. Durbeck, Schillinger and Kolter (2007) study a particular e-government project, which is the Access e-Gov project, and list four security requirements. They further discuss how the requirements can be addressed as follows:

- Communication Security comprising of message integrity, user authentication and confidentiality: Encryption and Digital Signatures using international standards are proposed to meet this requirement.
- Privacy: The authors identify a need to protect users' data so the citizens can trust the architecture and propose the use of a special purpose language to define privacy requirements.
- Trust: that can be met by authentication of network components amongst themselves.
- Access Control: Attribute Based Access Control is suggested to provide a flexible dynamic infrastructure that suits loosely coupled SOA.

Trust is also identified as a security requirement for e-Government transactions in Kaliontzoglou, Karantjias, & Polemi (2008). Their findings indicate that in order for an e-Government service to succeed in its business goals, it should be secure in all aspects so that all the entities involved trust it. Thus an e-Government service should make use of security services and mechanisms supported by the environment or the architecture where it is deployed. The conclusion can be related to the second research question of this study which seeks to find out the contextual characteristics in the EAC which would affect the implementation of an information security framework.

In a G2G transaction, the government agency providing a service has to address the security issues related to the service provision. The security services in electronic transactions are tackled by He & Antón (2009) through the specification of access control policies. Two major challenges of access control systems are identified, namely: defining correct and complete policies to control users' access to the system and its resources; and ensuring the resulting policies comply with the system requirements and high-level security/privacy policies. However these challenges were, to an extent, resolved in a study by Hu, Quirolgico, & Scarfone (2008) who present a method of Access Control policy composition using Semantic Web technology that leverages the pervasive capability of semantic content and the fluency of machine understandable knowledge for the management of federated resources. Beimel and Peleg (2011) introduce an improved method of Access Control policy composition which underpins access control with ontologies through the application of the

Web Ontology Language (OWL) and the Semantic Web Rule Language (SWRL). In these three studies, the electronic transactions are achieved through web services.

Many e-Government implementations are achieved through Service Oriented Architectures (SOA) with Web Services (Chunnian, Yiyun, & Qin, 2011), (Scholl & Pardo, 2010), (Simon, Laszlo, Goldschmidt, Kondorosi, & Risztics, 2010). This is because e-Government implementations involve transactions across heterogeneous systems. Web Service System security is investigated by Gutiérrez, Rosado, & Fernández-Medina (2009) who look at the use of security patterns and a standards-based approach to design a secure web service system. They use the case of a Bank Transfer system and conclude that security is a crucial aspect, if WS-based systems are to be the 'de facto' solution for inter- and intra-integrating heterogeneous systems. For this to become a reality, a software engineering-based, security engineering-centred global approach must be defined. This approach should provide developers with all the activities, tasks, tools, security artefacts and organizational structures necessary to design a secure WS-based solution. The idea of combining organizational structures with technical mechanisms to help design secure systems is an interesting point that can be applied to the EAC.

Still in the sphere of web services and service oriented architectures, O'Brien, Merson & Bass (2007) recognised that security is a major concern for Service Oriented Architectures (SOA) and Web services and suggested characteristics of SOA that need special attention as they directly impact on security. These issues include the presence of metadata in messages, services provided by third-party organizations, enforcement of access restrictions based on the identity of a user, and the use of public directories to find services. The authors cite the use of web service security standards to resolve some of these issues. The benefits of SOA/ Web services which are also applicable in security are Technical neutrality, Reusability and Formal contracts between end points (Sprott & Wilkes, 2004).

ISO 27002 requires legal and regulatory aspects to be taken into consideration when incorporating security requirements in the design of systems. To this end, Gerber and von Solms (2008) state that the escalating magnitude of national and international laws and

regulations has caused organisations to become increasingly aware of the importance of legal compliance and the obligations that arise from it. A process and a model are presented by the authors, which, when implemented, will lead to the specification of legal aspects that satisfy the ISO 27002 controls. Similarly, Guarda & Zannone (2009) state the legal requirements should be incorporated into software engineering for e-Government transactions by following existing laws and more especially those related to privacy and data protection. A practical implementation of how legal requirements can be incorporated in software system engineering is demonstrated in a study by Islam, Mouratidis & Jurjens (2011) in a framework that allows developers to elicit requirements from legislation, and track that these requirements are addressed through the system development.

The studies presented above present both information security requirements and mechanisms to meet those requirements. The mechanisms proposed include technical and non-technical requirements including legislation, and appropriate organizational structures. These requirements and mechanisms are summarised in Table 2-1, in the order of their discussion in this section.

From a technical perspective, G2G transactions are implemented through machine to machine interactions, thus the studies cited in the table above focus on access control as a requirement and web services as a mechanism for technical solutions for information security in e-government. A further exploration of studies on access control is presented in the next sub-section. The other discovery is legal compliance as a security requirement in e-government and the use of standards as a mechanism for implementing security. Access Control is investigated further in section 2.2.2., while legislation is discussed further in the investigation of the EAC context that is presented in chapter five.

Table 2-1 Focus of Studies on Information Security

| **Study** | **Requirements** | **Mechanisms for meeting requirements** |
|---|---|---|
| Zissis & Lekkas (2011) | Availability, Confidentiality, Integrity, Authenticity, and Accountability | Cloud Computing Architecture and Cryptography |
| Durbeck, Schillinger and Kolter (2007) | Authentication, integrity, confidentiality Privacy; Trust; Access Control | Encryption and Digital Signatures using international standards; Special purpose language; Attribute Based Access Control |
| Kaliontzoglou, Karantjias, & Polemi (2008) | Authentication; Integrity; Privacy and Confidentiality; Non repudiation; Availability; Trust; Need to consider implementation context | Encryption; Standards; Addressing of contextual issues such as lack of skilled staff |
| He & Antón (2009) | Access Control | Access Control Policies |
| Hu, Quirolgico, & Scarfone (2008) | Access control rules that manage dynamic trust relations amongst federated parties | Semantic Web |
| Beimel & Peleg (2011) | Access Control Policies | OWL and SWRL |
| Gutiérrez, Rosado, & Fernández-Medina (2009) | Mutual Authentication; Integrity; Confidentiality | Secure Web Services; Organizational structures; standards |
| O'Brien, Merson & Bass (2007) | Confidentiality; Authenticity; Availability; Integrity | Web Service Security Standards |
| Sprott and Wilkes (2004) | Technical neutrality; Reusability; Formal Contracts | Service Oriented Architectures; Web Services. These are discussed further in Chunnian et.al (2011); Scholl & Pardo (2010) and Simon et.al (2010) |
| Gerber and von Solms (2008) | Legal Compliance | Intellectual Property rights; Legislation; Contractual Obligations; International Treaties; Standards |
| Guarda & Zannone (2009) | Privacy; Legal Compliance | Privacy aware access control mechanisms; policies and legislation. Incorporation of legislation into system engineering process is discussed by Islam et.al (2011) |

### 2.2.2 Access Control

In implementing G2G transactions through SOA and web services, a crucial security service is access control. A description of web services and their relation to access control is given by Shen & Hong (2006) as follows:

> "A web service is a web-based loosely coupled application that can be published, located and invoked across the internet. Web services technology enables organizations to exploit software as a service. Services are accessed by method invocations. Method interfaces are

described and published and may be freely available. In web service environments, access control is required to cross the borders of security domains, to be implemented between heterogeneous systems. Interaction is between remotely located parties who may know little about each other."

Three access control models that can be applied in G2G transactions are:

- **Role Based Access Control (RBAC)**

RBAC uses roles as a basis for access control decisions and was designed specifically with enterprise organization structures in mind. RBAC allows the specification of security roles that map naturally to an organization's authorization structures (Bertino, 2003). However, RBAC does not entirely suit web service transactions and its weakness in open environments was identified by De Capitani di Vimercati and Samarati (2005). Several studies have subsequently been done to extend the RBAC model in order to address some of the weaknesses (Demchenko, Gommans, & de Laat, 2007).

- **Attribute Based Access Control (ABAC)**

In recent years, there has been a shift to looking at attributes as a basis for access control in a web services environment (Coetzee & Eloff, 2007). Attributes describe the characteristics of the requester, and may be a combination of identity and role. Attributes may be subject attributes, resource attributes or environment attributes. The ABAC model comprises of an Attribute Authority, Policy Enforcement Point, Policy Decision Point and Policy Authority.It has been recognized that there is still a need for the usage of semantics and/ or ontologies to ensure correct access control decisions with the ABAC model, and some research to that effect has been done (Warner, Atluri, Mukkamala, & Vaidya, 2007).

- **Governance Based Access Control (GBAC)**

The idea as presented by the Centre for Governance Institute – CGI (Centre for Governance Institute, 2005) is that transactions in which information is shared must be governed by the relevant legislation to which the organizations sharing the information are accountable. Thus any request for information is checked against the existing laws or regulations before it is granted. The argument presented by CGI is that traditional access control models such as RBAC, or any identity or rule based access control assumes that subjects are compliant with a single authority. This makes such models insufficient for the needs of e-Government transactions as information in such transactions is shared across not only organisational but

also jurisdictional borders. CGI defines GBAC as a method of classifying and accessing information asset holdings by directly linking them back to the specific legal measures that mandate their collection, dissemination, protection and disposition.

An analysis of the access control mechanisms leads to another discovery that regardless of the access control method used, where transactions are taking place across different security domains, it is necessary to ensure semantic interoperability so that credentials that are used in authorisation and access control decisions are interpreted in the same way by all parties involved in the transaction (Jeong & Han, 2006). In order to make correct access control decisions in transactions where attributes are passed from one security domain to another, the interpretation of the meaning of the security attributes needs to be consistent across the domains. One way to ensure this is through the use of domain specific ontologies. The use of ontologies in web services has been promoted by the World Wide Web Consortium (W3C), which has recommended the Web Ontology Language (OWL) as a general ontology for the semantic web (W3C, 2009). OWL is based on the Resource Description Framework (RDF) schema, which was an earlier specification from W3C. The ontology serves the purpose of clearly defining terms that are used in a transaction and enables a semantic evaluation of terms to determine similar meaning. For Web Service transactions, domain specific ontologies based on OWL or RDF have been proposed including ontologies for e-Government transactions (Domingue, Gutierrez, Cabral, Rowlatt, Davies, & Galizia, 2004). Ontologies can also be used to model other contextual information such as identified risks, legal requirements and operational controls.

**Analysis of ABAC, RBAC, and GBAC in G2G transactions**

The three access control mechanisms described above, each has its limitations when applied to G2G transactions. For Role Based Access Control, the organizational structures of two government organizations may be very different. What is an appropriate role in one organization, and therefore defines the access levels for a process or user may be defined differently in another organisation. If these two organisations collaborate in a G2G transaction, then there needs to be a definition of roles that hold across G2G transaction. For

Attribute Based Access Control, the challenge is being cognizant of issues such as legal compliance which is a requirement that was presented in some of the studies that were analysed in section 2.2.1. If it were possible to combine Governance Based Access Control and Attribute Based Access Control, it is likely that a more suitable Access Control model for G2G interactions would be formed. This possibility is investigated in the Design phase of this thesis where an access control model called the Governance and Attribute Based Access Control Model is proposed. This is presented in chapter eight of this thesis.

### 2.2.3 Security Management

In section 2.2.1 some of the requirements and mechanisms were non-technical ones, tending towards governance or management issues including legislation and organizational structures. In this sub section, an investigation of studies on security management studies relevant to G2G transactions is presented.

The effect of national culture on online transactions is investigated by Seidenspinner & Theuner (2007) who look at three countries which are Germany, Egypt and China, and conclude that national culture affects the way that transactions are carried out. A proposition that national culture may have an impact on e-Government security effectiveness in developing countries is made by Alfawaz, May, & Mohanak (2007). They look at the effect of legislation on security and privacy and states that many developing countries have yet to consider adopting adequate legislation related to information security management, laws that criminalize cyber-attacks and enable police to adequately investigate and prosecute such activities. In addition, many do not have privacy or network security laws or regulations which could be used to take action against the misuse of ICT resources. Zarei & Ghapanchi (2008), however, argue that e-Government development should not wait until reaching full security levels. They state that providing fully functional security for all the e-Government programs is impractical. Other security heuristic principles stated include the need for a security development and management plan, and application of security standards by a team with sufficient experience. The recommendations of the study by Zarei & Ghapanchi are to an extent validated by a study conducted in South Africa by Dagada, Eloff and Venter (2009) who conclude that while legislation that deals with information security exists, it is not used in organizational policies. It will therefore be necessary in the framework being proposed to address how organizations in the

EAC can consistently map their policies on existing and new legislation while taking into consideration international standards that are applicable. At the same time, the framework should remain implementable regardless of whether legislation is currently in place and should not require all security measurements to be in place at once.

## 2.3 Research in the EAC context

As previously presented in chapter one of this thesis, the ICT and e-Government service deployment in the EAC is the low according to the UN Survey on e-readiness conducted in 2010 (United Nations, 2010). The countries of the EAC, namely, Burundi, Kenya, Rwanda, Tanzania and Uganda, are all ranked in the bottom 50 countries in the world in terms of e-readiness out of 175 countries surveyed. This may explain why so few studies related to e-Government and/or information security have been carried out in the EAC context. In one of these, (Hellsten, 2010), an argument is presented that the technical infrastructure in the EAC is sufficient to provide e-Government services, however implementation approach towards e-Government has to be reviewed. Details of current initiatives in the EAC and in each of the three countries surveyed are presented in chapter five of this thesis. The rest of this section presents studies on e-Government and on Information security that address the EAC context.

### 2.3.1 Studies on e-Government in the EAC

Kaaya (2003) who bases her research on Kenya, Tanzania and Uganda in the EAC states that a four stage development model is used in e-Government strategies which are:

- Stage 1: Web sites are established to provide information about government functions and services
- Stage 2: Downloadable forms that can be completed and submitted offline are made available on the web site; email interaction between government officials and users may also be supported
- Stage 3: Web sites begin to support some formal online transactions such as payments or creating and submitting information online such as renewing driving license and filing tax returns
- Stage 4: Comprehensive and sophisticated government portals are developed to provide a wide range of information to users coupled with reliable security/privacy/confidentiality provisions.

The study makes two conclusions that are relevant, namely, the countries of the EAC are at stage 2 in terms of e-government services offered, and the common cultural and economic similarities of countries in the EAC are a basis for common approaches to e-Government. According to the UN e-Government survey of 2010 (United Nations, 2010), stages 1 and 2 have been achieved in all East African countries, and in some cases stage 3 has been accomplished. The challenge remains the provision of a wide range of secure services as required by stage 4.

Rwangoga and Baryayetunga (2007) propose the following measurable objectives for e-Government projects in a study based in Uganda:

i. Improved service delivery and the quality and speed of government's interaction with citizens and businesses as well as among government entities.
ii. Improved responsiveness to customer needs by using new modes of contact to provide public sector information and services.
iii. Increased government transparency by increasing the availability of information and accessibility to services.
iv. Saved time and money by improving efficiency in government processing, in part through use of common technology standards, policies and a federated architecture, as well as contributing to financial reform within the public sector.
v. Creation of positive, spin-off effects in society through the promotion of ICT skills development within government, businesses and households.

Of the above objectives, objective (iv) is of particular interest in terms of use of common technology standards, policies and a federated architecture that would enhance security in e-Government transactions.

The role of political will and human resources skills as factors that lead to successful e-Government initiatives is examined by Mwangi (2006) in the case of Rwanda. Additionally, Saidam (2007) states that lessons learnt from international experience should be applied. The roles of political will, resources and organizational culture in the EAC community efforts towards e-government are discussed by Hellsten (2010) who argues that the basic technical

infrastructure for e-Government in the EAC is in place, but what are needed are changes to implementation approaches that consider the leadership culture.

This study looks in detail at the EAC in part III of this thesis, but prior to that presents what has been done in some countries outside of the EAC with regards to information security management at national level. This is presented in chapter three of this thesis.

### 2.3.2 Studies on Information Security in the EAC

In Tanzania, a study of information security in higher institutions of learning (Bakari, Tarimo, Yngstrom, & Magnusson, 2005) led to two key conclusions, namely, the necessity of adequate planning at national and organizational level for a successful information strategy; and the need for developing countries to transform traditional information security policies into relevant policies to cater for digital information security. These conclusions give some insight on a possible way to approach the design of a sustainable information security framework and further motivate this study since a framework for e-Government security would not only ease planning at a national and organizational level, but also guide the drafting of relevant security policies.

The need for regulations to underpin Information Security is discussed by Tarimo, Yngstrom, & Kowalski (2005) who recognize the contexts in developing countries as significantly different from those in developed countries, including the slow pace of government initiatives. Tarimo et.al conclude that instead of waiting for government intervention, organizations deploying ICT can put forward their own initiatives to make sure that their systems follow standards that make provision for security, interconnectivity and interoperability with other ICTs in the country and beyond. This conclusion is supported by Zarei & Ghapanchi (2008) who state that a top-down approach to information security might not work for a developing country, since governments are slow in implementing the necessary governance structure, while a bottom- up approach may be constrained by lack of guidelines.

Karokola & Yngstrom (2009) investigated Tanzanian government institutions' requirements with regards to information security and suggested a score of the priority areas. Technical

security issues together with awareness are ranked most important. Their findings also highlight the need for strong access control mechanisms. Non-technical aspects including managerial, operational and economic factors are also considered priority areas. The findings show that legal and regulatory requirements are not high on the list of priorities. This could be explained by the fact that there are currently not many laws in Tanzania that address information security.

These studies leave some gaps that need to be filled in to address specific G2G requirements. There is a need to establish what kind of transactions take place and what are the mechanisms in place for security. This is done as part of this study and presented in chapter five.

## 2.4 Studies on Information Security Frameworks

The third research question of this thesis seeks to propose a sustainable framework for information security. A comprehensive information security framework in an organizational setting is proposed by Da Viega (2008) as comprising of six components which are: Leadership and Governance; Security Management and Organization, Security Programme Management; Security Policies; User Security Management; and Technology Protection and Operations. This framework leaves out some important aspects such as interoperability between the government agencies that are participating in a G2G transaction. A study by Lee, Yee & Cheung (2009), that is limited to data interoperability, does provide some insights into building an information security framework. These insights include the use of open standards such as XML, and the use of maturity levels to track progress in implementation of the framework.

In the next chapter, a discussion of examples of national level implementations of information security frameworks is presented before moving on to investigate the EAC situation in detail.

## 2.5 Conclusion

In this chapter, studies related to information security in e-government have been presented. The studies reviewed show that there are technical solutions that address environments in

which G2G transactions can be implemented such as use of web services and Service Oriented Architectures. For e-Government transactions, security requirements have been identified including authentication, integrity, trust, privacy, and access control. Several mechanisms for addressing access control have been found in the studies that were reviewed and a summary of the possible access control mechanisms that can be used in e-Government have been presented.

However, information security cannot be addressed solely by using technical mechanisms. Thus studies that address the management of information security have also been presented. The studies discussed in this chapter were chosen because they all stem from a developing country context albeit outside of the EAC. These studies help to point out some contextual issues that would be common across countries that may have limited resources and are just starting to put in place enabling legislation for information security practices in government.

Studies from the EAC are presented both from an e-Government and an information security perspective. These studies mostly focus on the management of information security rather than introducing new technical mechanisms for the addressing of information security requirements. These studies also give light on the EAC context and the possible need for governments not to attempt to follow a strictly top down or bottom up approach to addressing information security but to be able to do what they can with limited resources. The information from the research studies in the EAC is combined with the findings of this study presented in chapter five and used to establish the specific contextual factors that need to be addressed in an information security framework for G2G transactions in the EAC.

Finally, studies on information security frameworks are presented, and the main discovery from these is that there is a need to address interoperability as well as to use maturity levels to track progress in implementation of frameworks. All the discoveries in this chapter are summarized in chapter seven, in the build up to answering the research questions

This thesis attempts to combine both the technical and management perspective in one framework to enable implementing organizations or governments to have one reference

framework from which information security for G2G transactions can be addressed holistically. The next chapter looks at country implementations of frameworks that relate to the research questions of this study.

.

# Chapter 3 Examples of Policy Level Information Security Frameworks

## 3.1 Introduction

A G2G transaction has been defined in chapter one as “the sharing of information resources and services between government agencies in a restricted network setting with the ultimate aim of providing comprehensive, easy to access services to citizens”. G2G transactions may take place within a country or across country borders. In section 2.4 published research on information security frameworks was presented. However, this study aims at an information security framework that can be applied practically in the EAC. Thus in this chapter, examples of national policy infrastructure for achieving information security in e-Government are examined. These frameworks promote collaboration amongst government agencies within the country. Three categories of policy infrastructure are presented, which are, Information Security Frameworks, Interoperability Frameworks and Enterprise Architectures.

Interoperability Frameworks and Enterprise Architectures are addressed together with National Information Security Frameworks because they aim at achieving seamless flow of information across diverse entities, which may have different technology platforms and different policies. They thus have a bearing on information security in G2G transactions. For G2G transactions where ultimately information may need to be composed and provided to a citizen, regardless of the source of the information, it is important that the security objective of availability is achieved. Interoperability Frameworks and Enterprise Architectures are a way to ensure that information stored on different platforms is available in a convenient manner when needed. Two examples of national implementations are given in each of the categories.

The countries chosen for the examples in this chapter are the United States, Australia (Tasmania), United Kingdom, Spain and South Africa. The first four countries are ranked in the top ten in the 2010 UN e-Government development index (United Nations, 2010) and are taken to be representative of countries with good practices that the EAC can learn from. South Africa is included in the examples presented because it is ranked among the top ten in Africa in the same survey.

## 3.2 Information Security Frameworks

National Information Security Frameworks provide a holistic approach to information security covering both physical and logical security of government information assets. National frameworks usually consist of policies and practices. Policies provide general, overarching guidance on matters affecting security while practices document methods and minimum compliance activities as appropriate to ensure that policy objectives are met. The two frameworks presented are discussed from the point of view of their relevance to G2G transactions. These two frameworks were chosen because they were the most comprehensive documents found through an online search on national information security frameworks.

### 3.2.1 Her Majesty's Government (HMG) Security Policy Framework

The HMG Security Policy Framework (Cabinet Office UK, 2008) that is used by the United Kingdom government was developed with the recognition that protective security is an essential element towards making government work more efficiently. Protective Security is defined to include physical, personnel and information security. Security risks must be managed effectively, collectively and proportionately, to achieve a secure and confident working environment. Seven policy statements in the framework cover the following areas:

- Governance, Risk Management and Compliance (GRC): Sets out the roles and responsibilities of central government, departments and agencies, and states that where statutory requirements and international obligations exist, they must be complied with. Risk assessment is required at departmental level.
- Protective Marking and Asset Control: In relation to marking of information assets, departments and agencies are required to apply the government protective marking system which is aligned with the ISO 27001 standard.
- Personnel Security: This principle is designed to provide a level of assurance as to the trustworthiness, integrity and reliability of all HMG employees, contractors and temporary staff.
- Information Security and Assurance: This principle states that departments and agencies must have an information security policy that addresses both operational and technical issues.

- Physical Security: Physical security involves the appropriate layout and design of facilities, combined with suitable security measures, to prevent unauthorized access and protection of HMG assets – people, information, materials and infrastructure. This means putting in place, or building into design, measures that prevent, deter, delay and detect, attempted or actual unauthorized access, acts of damage and/or violence, and triggers an appropriate response.
- Counter – Terrorism: Departments and Agencies are responsible for reducing risk from terrorist attacks to as low a level as is reasonably practical.
- Business Continuity: Departments should aim to continue their critical business activities following a disruption and effective recovery afterwards (return to 'normal'). It is an essential aspect of securing their business.

The above framework is a very comprehensive framework that deals with various aspects of information security in government. The discoveries within this framework that directly relate to the research questions of the study include Governance, Risk and Compliance (G*RC), protective marking, information security and business continuity*. The framework relates to the UK context, based on the government structures and legislation where applicable. There is a need to do the same for EAC, but using a format that is context-specific. Clear identification of actors and their roles, and how the mapping of the outputs of one role to another can be achieved, would contribute to a sustainable information security framework.

### 3.2.2 Tasmania Government Information Security Framework

The Government of Tasmania has adopted an Information Security Framework (Department of Premier and Government, Tasmania, 2009) which provides guidance to government agencies on what Information Security Policy Principles they need to adhere to, as well as important legislative requirements and the primary roles and responsibilities for information security. The areas covered by the framework are Information Security Governance; Record Security; Physical Security; Personnel Security; General ICT; Incident Management; and Risk Management. The ISO 27000 series of standards are to be used to help the implementation of the framework.

This framework consists of a number of documents (Department of Premier and Government, Tasmania, 2009), the contents of which are summarized in Table 3-1.

Table 3-1 Tasmanian Government Information Security Framework

| Document Name | Contents Outline |
|---|---|
| Tasmanian Government Information Security Charter | • Legislative requirements<br>• Information security policy principles<br>• Information security policies<br>• Primary roles and responsibilities |
| Tasmanian Government Information Security Guidelines | • Overview of the Tasmanian Government Information security framework<br>• Information security governance<br>• Records, Physical and Personnel security<br>• General ICT<br>• Incident management<br>• Information security risk management |
| Tasmanian Government WAN and Internet Services: Information Security Policies and Standards | A whole-of-government implementation of the framework with polices and standards specific to this topic |
| Agency implementations of the Framework | Determined by each agency |

The Tasmanian framework addresses security at two levels, which are, across the whole Government and at individual agencies. This approach is an interesting one that can be adopted to provide a flexible framework that is consistent and applicable in different scenarios. This study looks at G2G transactions, which pre-supposes that more than one agency is involved. However, a framework that can also fit the individual agency needs can be achieved. This is done in the framework that is developed in this study and presented in chapter eight.

## 3.3 Interoperability Frameworks

Interoperability frameworks are a tool used by governments to ensure that e-Government implementations work, given that government agencies often have different technical platforms and different organizational processes. Two examples are presented in this section, one from South Africa and the other from Spain. While other national interoperability frameworks may exist, the two frameworks presented here are sufficient to illustrate the basic structure and purpose on interoperability frameworks in relation to this study. In addition,

one example is from the African continent – that is South Africa, while the other is taken from outside of Africa, that is, Spain.

### 3.3.1 South African Minimum Interoperability Standards (MIOS) for Information Systems in Government

The South African MIOS (SITA, 2007) are standards based on international and/or open standards that enhance interoperability. The Government of South Africa adopted MIOS in order to ensure that public sector organizations that provide e-services have the underlying infrastructure for web enabled government.

The MIOS standards have been driven by:

- Interoperability: only standards that are relevant to systems interconnectivity, data interoperability and information access are specified
- Market Support: the standards selected are widely supported in the market and are likely to reduce the cost and risk of government information systems
- Scalability: standards selected have the capacity to be scaled to satisfy changed demands made on the system
- Open Standards: the specifications for the standards documented are freely implementable and available to the public at large
- Security: all standards selected need to support a secure computing environment

The principles stated in MIOS cover interconnectivity, data interoperability, web services, information access, content management metadata, identifiers, mobile phones and biometric data interchange. For each of these a list of applicable standards is given.

The use of open and freely available standards is advocated for, one of the reasons being cost reduction. This is applicable in the EAC setting and a list of applicable standards could be compiled and updated centrally so that government agencies keep up to date on standards. The use of open standards could contribute to the sustainability of the framework, which is part of the 3$^{rd}$ research question of this study.

### 3.3.2 Spanish National Interoperability Framework

The Spanish Government has adopted a National Interoperability Framework (Ministry of the Presidency, Spain, 2010) in order to create the necessary conditions to guarantee the suitable

level of technical, semantic and organizational interoperability of the systems and applications used by Public Administrations. This framework allows the exercise of rights and the fulfillment of obligations through electronic access to public services, benefiting the efficacy and the efficiency at the same time. The framework refers to national legislation. The guidelines for achieving these levels of interoperability are summarized in Table 3-2.

Table 3-2 Spanish national interoperability framework components

| Component | Guidelines |
|---|---|
| **Organizational interoperability** | • Establish and publish access and use conditions of services and data in accordance to relevant legislation.<br>• Maintain an inventory of administrative procedures with indication of level of computerization.<br>• Maintain inventory relations among public bodies. |
| **Semantic Interoperability** | • Establish and maintain data models considered of common interest that will be used during information exchanges in Public Administrations.<br>• Establish and publish the corresponding interchange data models that will be of mandatory application for information interchanges in Public Administrations. |
| **Technical Interoperability** | • Use open standards, together with standards that are widely used by citizens, with the aim to guarantee independence in the choice of alternative technologies by the citizens and Public Administrations and adaptability to progress of technology. |

The Spanish national interoperability framework recognizes that some activities may not be computerized thus a framework would possibly include addressing operational issues that may not be tied to the use of technology. The idea of open standards for technical interoperability is also featured in this framework. Furthermore, the holistic addressing of interoperability namely, technical operational and semantic is applicable to G2G transactions as by their nature those transactions will occur across technically and organizationally disparate domains.

## 3.4 Enterprise Architectures

As mentioned in chapter two, SOA are largely used to implement e-Government. There is some overlap between SOA and enterprise architectures (Ibrahim & Long, 2007). SOA can be built on existing enterprise architectures. Implementation of enterprise architectures can result in the achievement of interoperability (Janssen & Scholl, 2007). In this section, two examples of government wide enterprise architectures are presented.

### 3.4.1 Federal Enterprise Architecture Framework

The Federal Enterprise Architecture (FEA) is a model developed by the United States Government for use by its Government Agencies (CIO Council, 1999). Information security is a component of FEA which has been successfully implemented in different government environments (http://www.whitehouse.gov/omb/E-Gov/EA-Success).

The underlying principles encompassed of FEA, as envisaged by the Chief Information Officers (CIO) Council of the USA (CIO Council, 1999), include the following:

- Establishment of Federal Interoperability Standards
- Coordination of technology investments with the Federal business and architecture
- Minimization of the Data Collection Burden
- Securing of Federal information against unauthorized access
- Functionality: Taking advantage of standardization based on common functions and customs
- Providing access to information
- Selecting and implementing proven market technologies
- Complying with Privacy Act of 1974

The FEA framework (CIO Council, 1999, p. 23) is presented in Table 3-3.

Table 3-3 FEA Framework

| Perspectives | Data Architecture (Entities = What) | Applications Architecture (Activities = how) | Technology Architecture (Location = what) |
|---|---|---|---|
| Planner's View Objectives/Scope | List of Business Objects | List of Business Process | List of Business Locations |
| Owner's View Enterprise Model | Semantic Model | Business Process Model | Business Logistics System |
| Designer's View Information Systems Model | Logical Data Model | Application Architecture | System Geographic Deployment Architecture |
| Builder's View Technology Model | Physical Data Model | System Design | Technology Architecture |
| Subcontractor's view Detailed specification | Data Definition Library or Encyclopaedia | Programs "Supporting Software Components (i.e. operating systems)" | Network Architectures |

The FEA Enterprise Architecture Framework ties organizational and technical goals together, which can be applied to get a holistic security framework by linking operational and technical activities necessary to achieve security. The FEA framework also defines views that correspond to different roles. Such views help implementers of the framework to understand how their roles affect the entire organization. A similar approach to an information security framework for G2G transactions could work as a tool for raising awareness and thus inculcating information security practices across government.

### 3.4.2 Government Wide Enterprise Architecture

The Government Wide Enterprise Architecture (GWEA) is a framework adopted by the South African Government to address the following challenges in Government:

- Inconsistent and non-standard planning frameworks
- Use of different notations and varying levels of details in plans submitted by departments
- Problems for South African Information Technology Authority (SITA) to certify plans using a consistent and government wide accepted framework
- Government unable to integrate services as a result
- Costly systems development and rampant duplication
- Low organizational maturity and stagnant service improvement

The GWEA framework is designed to meet these challenges by achieving interoperability at three levels (GITOC, 2009). The three levels are:

- Organizational level: organisational components are able to perform seamlessly together;
- Semantic level: ensuring the precise meaning of exchanged information between different kind of Information Systems; and
- Technical level: technical issues of linking computer systems and services.

This approach is similar to that proposed by the Spanish Interoperability framework that is discussed in section 3.3.2. The GWEA brings the additional value of illustrating how the enterprise architecture framework adds value to the operations of government through what is acting as a foundation to meet government objectives (Segole & Needham, 2009). These government objectives are security, interoperability, reduced duplication, economies of scale and digital inclusion. The objectives, when met, can lead to lower costs, increased productivity and citizen convenience.

As with the Spanish interoperability framework, GWEA outlines the need for interoperability which is applicable to information security in G2G transactions. In addition, the framework is presented in a way that ties it with its contribution to the overall goals of government. Since the third question of this study addresses how a sustainable framework can be achieved, it is necessary that the information security framework that is proposed also has a mechanism to address awareness amongst top leadership, and acceptability so that the value of the framework at all levels of government is achieved. These discoveries are used in chapter ten, whereby e-government critical success factors are used to evaluate the framework.

## 3.5 Conclusion

In this chapter national interoperability, information security and enterprise architectural frameworks have been presented. For each of these, relevance to the research objectives has been identified. The focus of this chapter was to see what has been done by governments round the world. All the initiatives except for the FEA framework are fairly new and thus no data on their success are available yet. The frameworks presented, however, do have relevance to this study as summarized below:

- A national information security framework addresses specific national issues such as legislation and priority areas
- Interoperability is a key issue of concern and is addressed at technical, semantic and operational levels. Open standards may be used to address interoperability
- The framework may include mechanisms to be implemented internally within an agency and also applied in a G2G transaction
- The framework may include operational mechanisms that are not necessarily directly tied to technical mechanisms
- As a means of achieving acceptability, which will contribute to sustainability, the framework may be evaluated against set government policy objectives.

For G2G transactions, national level policies and guidelines will guide the individual government agencies that participate in the transaction. However, there are two areas where

the national information frameworks described above do not address the challenges in G2G information security that were described in chapter one. Firstly, there is a need for a means for an agency to map national policies onto organizational policies and plans and technical mechanisms for information security, which should be flexible enough to incorporate changing legislation. Secondly, there is need for a means to preserve information security across a G2G transaction. The framework that is presented in chapter eight of this thesis does address these two areas through a process model that is part of the framework.

Another pertinent discovery from the frameworks presented in this chapter is that all the examples given were achieved through a concerted effort at central government level, with a particular government department spearheading the initiative. An investigation into the EAC context that is presented in chapter five will reveal that most e-Government initiatives are not centralized in the EAC. This gives a justification for the EAC not to simply adopt a framework in use in another part of the world, but to critically examine contextual factors and come up with a framework that will fit the needs of the EAC.

The framework examples presented in this chapter frequently refer to the application of standards to achieve information security. In the next chapter, an investigation of standards related to information security for G2G transactions is presented.

# Chapter 4 Standards Related to Information Security in e-Government

## 4.1 Introduction

A reference to the use of standards in addressing information security has been discovered both in the research presented in chapter two, and in the national information security frameworks presented in chapter three. This chapter describes standards that are relevant to G2G transactions in e-government. Open and freely available standards are referred to where possible. The exception is standards issued by the International Organization for Standardization (ISO) because this is the de-facto standards body recognized worldwide.

The detailed investigation into use of standards is motivated by the need to develop a sustainable framework in which the EAC governments need not "re-invent the wheel", but rather concentrate on those specific mechanisms that will address context sensitive needs, as will be presented in chapter eight of this thesis. Standards also address some of the barriers to G2G that are discussed in chapter 1 including information exchange, technical platforms and resource constraints.

The standards bodies whose standards are cited are:

- European Committee for Standardization or Comité Européen de Normalisation (CEN) is a regional body with membership of 33 nations in Europe: CEN provides a platform for European standards and other technical specifications which can be accessed at http://www.cen.eu.
- International Organization for Standardization (ISO) is an international body with a membership of 163 countries with a Central Secretariat in Geneva, Switzerland
- International Electro technical Commission (IEC) is an international organization that publishes standards for electrical, electronic and related technologies
- National Institute for Standards and Technology (NIST), an agency of the government of the United States of America, develops standards and guidelines for use by federal agencies and external bodies that deal with federal entities (http://csrc.nist.gov). The agency is also in charge of Federal Information

Processing Standard (FIPS) publications. NIST guidelines are based on the Federal Information Security Act of 2002 (United States Congress, 2002)

- Organization for Advancement of Structured Information Standards (OASIS) is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS promotes industry consensus and produces worldwide standards for security, Cloud computing, SOA, web services, the Smart Grid, electronic publishing, emergency management, and other areas. SOA and web services are mechanisms to implement G2G transactions. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology
- Organization for Economic Co-operation and Development (OECD) is an international organization with 34 member countries which provides a forum for governments of these countries to compare policy experiences, seek answers to common problems, identify good practice and coordinate domestic and international policies
- World Wide Web Consortium (W3C) is an international community which develops web standards.

In the next section, a description of standards and their relationship to information security for G2G transactions is presented.

## 4.2 Non – Technical Standards related to information security for G2G transactions

### 4.2.1 ISO/IEC 27001:2005

The ISO/ IEC 27001:2005 is named Information security management systems — Requirements (ISO/IEC, 2005a) and can be downloaded for a fee from www.iso.org. This international standard presents a process approach for information security management, which emphasizes the importance of understanding an organization's information security requirements and the need to establish policy; objectives for information security; risk management and implementation of controls; performance management and continual

improvement. The "Plan-Do-Check-Act" (PDCA) model is adopted and is applied to structure all ISMS processes.

The relevance of this standard to G2G transactions is that individual MDAs involved in a G2G transaction should have internal processes or mechanisms to address information security. The PDCA process principle be applied both for a framework that is applicable within an MDA and across MDAs participating in a G2G transaction. However the PDCA process is a generic process that does not consider contextual issues. In chapter eight of this thesis, a more appropriate process model is presented that addresses the EAC context as discovered and presented in chapter five.

### 4.2.2 ISO/IEC 27002:2005

The ISO/IEC 27002:2005 is named Code of Practice on Information Security Management (ISO/IEC, 2005b) and can be downloaded for a fee from www.iso.org. This international standard addresses information security from a traditional point of view of Confidentiality, Integrity and Availability (CIA). Confidentiality deals with ensuring that information is accessed by authorized users only. Integrity means that the information should not be altered without authorization and lastly information should be available as and when required. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities. The standard addresses 10 security domains which are security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, risk, incident and business continuity management, and compliance. The standard also states as well as critical success factors for information security management systems.

The security requirements of confidentiality, integrity and availability have been discovered in the literature presented in chapter two. The additional discovery from this standard is the description of critical success factors as part of the standard. These critical success factors

will be used to evaluate the framework that is developed in this study. The evaluation is presented in chapter ten.

### 4.2.3 FIPS PUB 200

FIPS PUB 200 is the Minimum Security Requirements for Federal Information and Information Systems (NIST, 2006). This standard can be downloaded for free from www.csrc.nist.gov. The standard specifies 17 security areas for which federal organizations are required to develop and adopt policies. Four of these that relate to this study are:

- Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.
- Identification and Authentication (IA): Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- System and Communications Protection (SC): Organizations must secure organizational communications at the external boundaries and key internal boundaries of the information systems; and techniques that promote effective information security within organizational information systems.
- System and Information Integrity (SI): Organizations must manage information system flaws in a timely manner; provide protection from malicious code; and monitor information system security alerts and advisories and take appropriate actions in response.

This standard addresses information security requirements discussed in previous sections of the thesis, but with the additional discovery of the promotion of effective information security within organizational boundaries.

### 4.2.4 Network and Information Security Standards Report, Issue 6.2

The Network and Information Security Standards Report (CEN, 2007) can be downloaded for free from http://www.cen.eu. This report identifies the increasing importance of the availability, reliability and security of networks and information systems to the economies in Europe and proposes standards to address current security threats. The standards are addressed under five categories which are referred to as Security Services. Security Services are defined as follows:

- Registration, Authentication and Authorization Services. These services provide the means to ensure that users are uniquely and unambiguously identified and granted access only to those assets for which they have been authorized.
- Confidentiality and Privacy Services. These services provide the means whereby e-business information is stored and transferred securely. They also ensure that private information is protected in accordance to legislation.
- Trust Services. These services are required to ensure that e-business transactions are properly traceable and accountable to authenticated individuals and cannot subsequently be disavowed.
- Network and Information Security Management Services: These services are required to ensure that appropriate management controls, processes and procedures are in place in addition to the technical security measures to protect the system and network infrastructure.
- Assurance Services. These services provide e-business users with confidence that all technical and non-technical security measures have been designed, configured and are being operated in a secure manner in accordance to the relevant standards.

There are two discoveries in this standard, which are the connection of accountability to trust as a requirement, and the provision of assurance that both technical and non-technical measures have been designed to meet information security requirements. These are issues that are addressed in the framework proposed for the EAC in this thesis.

### 4.2.5 OECD 81829 2002

The OECD standard number 81829 2002 is named Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (OECD, 2002). This standard can be downloaded for free from www.oecd.org

The Guidelines outline nine principles aimed at instilling a culture of security in organizations. The guidelines identify the need for the incorporation of security as an essential element of information systems and networks. The nine principles are awareness of the need for information security; responsibility for the security of information systems; response to security incidences; ethics, that is, respect for the legitimate interest of others; democracy, that is, security of information systems and networks should be compatible with the essential values of a democratic society; risk assessment; security design and implementation; security management and lastly, reassessment of information security management systems.

In chapter five of this thesis, an investigation is done as to what national culture may exist in the EAC that could influence information security practices. The discoveries of chapter five are used in the design of the information security framework and its related models to ensure that the cultural context of the EAC is taken into consideration in the solution proposed.

### 4.2.6 OECD Guidelines for Electronic Authentication

The Guidelines for Electronic Authentication (OECD, 2007) can be downloaded for free from www.oecd.org. The guideline defines authentication as a function for establishing the validity and assurance of a claimed identity of a user, device or another entity in an information or communication system. One of the recommendations in this guideline is that both public and private sectors should encourage the use of authentication schemas that are legally compatible, technically interoperable and meet business needs. Such schemas will in turn facilitate cross-sectoral and cross-jurisdictional online interactions and transactions. Furthermore, they will ensure that authentication products and services can be deployed at both national and international levels. The guideline further sets out foundation and operational principles for electronic authentication.

The discovery with this standard is the need for national level mechanisms when addressing the authentication information security requirement. This discovery leads to the investigation in chapter five, of legislation that may be in place in the EAC to address authentication, and the inclusion of national level mechanisms, which are Certificate authorities, in the information security framework for the EAC that is presented in chapter eight of the thesis.

### 4.2.7 OECD Guidelines on Privacy and Transborder Flows of Personal Data

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 1980) can be downloaded for free from www.oecd.org. These guidelines set minimum standards for protection of personal data including restrictions of collection of personal data, use of personal data, need to be complete, accurate and up to date data and protection of personal data from loss, unauthorized access, destruction, modification and disclosure. The guidelines are currently being reviewed.

This standard highlights the need for legislation on cross border transactions. G2G transactions are likely to be cross-border across the EAC partner states. The presence of legislation on privacy is investigated further in chapter five of this thesis.

### 4.2.8 NIST Special Publication 800-53 Revision 3

These guidelines are named Recommended Security Controls for Federal Information Systems and Organizations (NIST, 2009) and can be downloaded for free from www.csrc.nist.gov. The purpose of these guidelines is to help federal agencies to select and specify security controls to meet the requirements of the Minimum Security Requirements for Federal Information and Information Systems (FIPS 200). For each of the security requirement areas outlined in FIPS 200, baseline security controls are presented. Some of the controls mentioned in this document include access control policies, security attributes for authentication, access control for mobile devices, security awareness and training policy and procedures, audit and accountability policy and procedures, contingency planning, configuration management, risk assessment policy and procedures, incidence response management procedures, environment management policy and procedures, cryptography, enterprise architecture and system and information integrity policy and procedures.

The discovery in these guidelines is the use of both technical and non-technical controls in addressing information security requirements. The framework presented in this study includes both technical and non-technical requirements in addressing information security in G2G transactions.

## 4.3 Technical Standards

The standards and guidelines presented in section 4.2 mostly address the information security management process. In order to address the technical aspects of information security, a survey of current technical information security standards is presented in this section. The standards presented in this section are those related to the technical mechanisms that can be used to implement e-Government transactions. Complex e-Government transactions are largely achieved through the implementation of Service Oriented Architectures (SOA). Web services are the reference technology used to implement SOA -based information systems (Gutiérrez, Rosado, & Fernández-Medina, 2009). Web Services are software that provide a standard based approach for machine to machine interaction (W3C, 2004). The Organisation for Advancement of Structured Information Standards (OASIS) conducted a survey on e-Government (OASIS, 2010a) of which one of the findings was that there is a need to use Open Standards to underpin the delivery of e-Government online services. The reason behind the use of these standards is to help to ensure interoperability and to produce the best value for money. OASIS has proposed technical standards for web services that are applicable for e-Government implementations. These are discussed 4.3.1 to 4.3.3.

### 4.3.1 XACML

The eXtensible Access Control Markup Language (XACML) is a policy language which uses XML statements to present access control policies. XACML version 2.0 was ratified as a standard by OASIS in February 2005 (OASIS, 2010b). XACML components are as shown in Table 4-1.

Table 4-1 XACML Components

| XACML Component | Description |
|---|---|
| Policy Enforcement Point (PEP) | Forms a request (using the XACML request language) based on the attributes of the subject, action, resource, and other relevant information. The PEP then sends this request to a Policy Decision Point (PDP) |
| Policy Decision Point (PDP) | Receives and examines a request, retrieves applicable policies, evaluates the applicable policy and returns the authorization decision to PEP |
| Context Handler | Context Handler can be defined to convert the requests in its native format to the XACML canonical form and to convert the Authorization decisions in the XACML canonical form to the native format |
| Policy Information Policy | Serves as the source of attribute values, or the data required for policy evaluation |
| Policy Administration Point (PAP) | Creates security policies and stores these policies in the repository |

The need for organizational information security policies is included in many of the standards presented in section 4.2. For electronic transactions the organizational policy should be translated into an electronic format that can be read by other systems. XACML is an open standard for expressing policies and thus would be applicable in G2G transactions. A government agency (Service Requestor) that is requesting a service electronically from another agency (Service Responder) would submit their request in XACML request language. This request would be checked by the Policy Enforcement point in the service responders access control policy, and combine it with the attributes presented by the requestor. This request would then be passed on to the Policy Decision Point of the Service Responder.

In this study, an access control model, based on XACML and using SAML attributes is developed and presented as part of the information security framework for G2G transactions. This model is presented in chapter eight of this thesis.

### 4.3.2 SAML

The Security Assertion Markup Language (SAML) is an XML-based security specification schema for exchanging authentication and authorization information. SAML handles the user authentication and also carries attribute information for authorization and access control (OASIS, 2010b).

SAML assertions are of three kinds, namely, Authentication assertions, Attribute assertions and Authorization Decision assertions. An assertion is defined as a piece of data regarding either an act of authentication performed on a subject, attribute information about the subject, or authorization data applying to the subject with respect to a specified resource. Assertions are produced by a SAML authority, which is an abstract system entity in the SAML domain model. The user or web service requesting assertions from the SAML authority is called the Requester. These assertions are then used in communicating with an entity called a Responder, who utilizes those SAML assertions to respond appropriately to the Requester. In a web services environment, SAML assertions may be carried within a SOAP message. Other than assertions, SAML is also composed of protocols, bindings and profiles. Protocols allow service providers to request for assertions, authentication and name identifier registration and mapping. Bindings are the mappings from SAML request-response message exchanges into standard messaging or communication protocols such as SOAP and HTTP. A profile of SAML defines constraints and/or extensions in support of the usage of SAML for a particular application. SAML has been implemented in e-Government settings for identity management (McKenzie, Crompton, & Wallis, 2008) and studied for authentication and authorization in federated networks by Marin-Lopez, Pereniguez, Lopez, & Perez-Mendez (2011).

As part of this study, a way to implement SAML as a mechanism for meeting information security requirements in an e-Government setting was investigated (Wangwe, Eloff, & Venter, 2008a). The six information security requirements addressed were authentication, privacy, authorization and access control, data integrity and trust. The applicability of SAML to the security requirements was presented as follows:

- **Authentication**: A SAML authentication assertion simply asserts that the service requestor provided authentication, the method of authentication used, and who did the authentication. An authentication services such as Lightweight Directory Access Protocol (LDAP) can provide the actual authentication. For example, the following portion of an assertion:

  `<saml:AuthnStatement AuthnInstant=2006-04-12T16:57:30.000Z”>`

  indicates the time and date of an assertion; while

```
<saml:AuthnContext><saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
```

indicates that the authentication was done through a local server in order to acquire a Kerberos ticket for subsequent use.

- **Privacy:** SAML V2.0 defines how pseudonyms can be used between providers to represent the entity that has been authenticated. This is achieved through the Name ID element. In addition, SAML includes mechanisms to allow providers to communicate privacy policy and settings.
- **Authorization and Access Control:** SAML authorization decision assertions indicate what resources the subject is allowed to access. Furthermore, SAML attribute assertions may be used to describe the role that the subject holds in the context of the particular transaction. For example:

```
<saml:AuthzDecisionStatement
Resource=”http://civilregistry.go.tz/birthdateregister.html”
Decision=”Permit”>
<saml:Action>GET</saml:Action></saml:AuthzDecisionStatement>
```

indicates that permission has been granted to access web page birthdateregister.html. An example of an attribute assertion would be:

```
<saml:AttributeStatement><saml:Attribute>
NameFormat=http://pensions123.co.tz Name=”MemberType”
<saml:AttributeValue> pensioner </saml:Attribute>
</saml:Attribute></saml:AttributeStatement>
```

- **Data Integrity:** In SAML implementations, it is possible to confirm that data integrity has not been compromised, that is, a given message has not been altered during transmission. This is done through the use of XML signatures, and additional security related technologies such as PKI. Furthermore network protocols such as IPSec and RFC2246 can be used to secure SAML traffic.
- **Trust:** Trust is achieved by using a separate authority (trusted third party) to issue security tokens which are acceptable to all parties. In the case of a SAML implementation, the trusted authority would issue SAML assertions to confirm the authenticity and access rights for the service requester.

### 4.3.3 Web Services (WS) Security Framework

The objective of the WS Security Framework is to have a standard way of handling web services security in transactions originating from entities that may have different security environments/policies. The WS – Security framework has been adopted by OASIS as a standard (OASIS, 2010b). The standards contained in the WS – Security framework are illustrated in Table 4-2.

Table 4-2 WS Security Framework Components

| WS Security Framework component | Description |
|---|---|
| SOAP Message Security | Describes enhancements to SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies. This specification also provides a general-purpose mechanism for associating security tokens with message content. No specific type of security token is required, the specification is designed to be extensible (i.e. support multiple security token formats). |
| User Name Token Profile | Describes how a web service consumer can supply a Username Token as a means of identifying the requestor by "username", and optionally using a password (or shared secret, or password equivalent) to authenticate that identity to the web service producer. |
| SAML Token Profile | Describes how to use SAML assertions with the WS Security SOAP message specification |
| X.509 Token Profile | Describes how to use X.509 with the WS Security SOAP message specification. An X.509 certificate specifies a binding between a public key and a set of attributes that includes (at least) a subject name, issuer name, serial number and validity interval. An X.509 certificate may be used to validate a public key that may be used to authenticate a SOAP message or to identify the public key with SOAP message that has been encrypted. X.509 is an ITU-T (ITU Telecommunication Standardization Sector) standard for PKI (Public Key Infrastructure) in cryptography, which, amongst many other things, defines specific formats for PKC (Public Key Certificates) and that the algorithm that verifies a given certificate path is valid under a given PKI (called the certification path validation algorithm) (http://www.itu.int/rec/T-REC-X.509/en). |
| Kerberos Token Profile | Describes how to use Kerberos tokens with the WS Security SOAP message specification. Kerberos is a network authentication protocol developed by Massachusetts Institute of Technology (http://web.mit.edu/Kerberos/). It is designed to provide strong authentication for client/server applications by using secret-key cryptography |
| Rights Expression Language Token Profile | Describes the use of ISO/IEC 21000-5 Rights Expressions with respect to the WS-Security SOAP message specification |

## 4.4 Conclusion

In this chapter, information security standards from international, regional, technical and national organizations have been presented.

International organizations are those whose membership is open to nations worldwide. The standards from international organizations which have been presented in this chapter are standards from ISO, IEC, and OECD. Standards from one regional body, the CEN, have been presented. CEN's membership comprises of nations in the European region. For national standards, NIST that is the standardization body of the United States of America have been presented. Technical standards are those from international organizations, but whose membership is on an individual or corporate basis. The standards presented are from OASIS and W3C.

The discoveries from these standards were discussed and can be summarized as:

- The PDCA process principle as a generic process model for implementation of an information security framework, and the need to a process model that is context sensitive to the EAC situation
- Security objectives of Confidentiality, Integrity and Availability
- The presence of critical success factors for information security frameworks within ISO standard 27002:2005
- The need for promotion of effective information security within organizational boundaries
- Accountability as a security objective related to the trust requirement
- The need to include cultural considerations in an information security framework
- Legislation as a mechanism for addressing the authentication and privacy information security requirements
- Implementation of technical and non-technical mechanisms to address information security
- Use of open technical standards as a mechanism to meet information security requirements.

The standards and guidelines presented address security requirements that are applicable in many settings. However recognizing that a successful implementation must take context into consideration, standards organizations have started moving towards investigating context specific standards and guidelines, for example the ISO 27799:2008 standard for health information systems (ISO, 2008), and work done by OASIS on legal XML (OASIS, 2008). In the next part of the thesis, an EAC situational analysis is undertaken to discover what initiatives have been done with regards to e-government, what legislation is in place with regards to e-government and information security, what cultural practices may affect information security implementations and what are the related practices in individual MDAs in the EAC.

# PART III: EAST AFRICAN COMMUNITY SITUATIONAL ANALYSIS

# Chapter 5 Current e-Government Initiatives and Practices in the EAC

## 5.1 Introduction

In the second part of the thesis, a literature survey was presented that discussed international standards, existing frameworks and research related to this study. This part of the thesis consists of chapters five and six which together present a situational analysis of e-Government practices from an information security perspective in the three countries surveyed. Chapter five discusses regional and national e-Government initiatives while chapter 6 presents the detailed findings of a survey on G2G related information security practices in individual MDAs in the EAC.

This chapter starts with a discussion on regional EAC initiatives followed by the initiatives and practices in three countries surveyed, namely, Rwanda, Tanzania and Uganda. For each country, resources, policies, strategies, legislation and projects related to e-Government are presented, together with a discussion on how information security is addressed in these initiatives. The national cultural considerations that may affect information security are also discussed.

## 5.2 Regional EAC Initiatives

The EAC regional framework for e-Government (East African Community Secretariat, 2005) highlights the following areas where EAC partner states need to provide an enabling framework for e-Government:

- Legislation: Necessary legislation on data security, network security, cyber-crime, information systems and electronic transactions needs to be put in place.
- Risk Assessment: A study to identify the challenges, threats and vulnerabilities of networks and information infrastructures needs to be undertaken.
- Security standards: An investigation of data security standards and issues necessary for the exchange of classified government information of the partner countries of the EAC needs to be undertaken.

The East African common market protocol (EAC, 2009) requires partner states to establish a common standard system for issuing national identification documents to their nationals that

may be machine-readable and electronic. The protocol in article 42 also calls for the promotion and ensuring of the sustainability of an information and communications technology culture.

## 5.3 Initiatives in Rwanda

### 5.3.1 Resources

Rwanda has a population of about 10 million and a GDP per capita of USD 520 in 2009 (National Institute of Statistics of Rwanda, 2010). The central ministry responsible for ICT had a budget of RwFr. 162,992,037,193 equivalent to about USD 282,140,000 in the 2010/2011 budget(Ministry of Finance and Economic Planning - Rwanda, 2010).Internet users are estimated to be 3% of the population while mobile phone penetration stands at 13% (Hellström, 2010). Rwanda is hailed as having one of the most comprehensive integrated ICT4D plans throughout Africa, and e-Government is one of the pillars of that plan (UN Economic Commission for Africa, 2007).

### 5.3.2 Government Policies, Strategies and Standards

In 2010 the government of Rwanda unveiled the National Information and Communication Infrastructure (NICI) 2010 plan (Government of Rwanda, 2010). With regards to e-Government, the plan aims to ensure that that implementation cuts across ministries and agencies horizontally so that complete business processes are automated and not just departmental planned actions. Furthermore it is planned that core design criteria for e-Government applications in terms of portal design, look and feel, and minimal content will be identified and standardized. Another point of interest is the identification of re-usable applications and ensuring that duplication does not take place, together with implementation of standardized data dictionaries and controlled data exchange to ensure proper ownership of information.

Technical standards for e-Government were adopted in 2006 (RITA, 2006). The objective of these standards is to establish common models, frameworks and standards. The benefits expected are:

- Cost reduction by reducing duplicity and sharing administration and training expenses; economies of scale in purchasing and simpler upgrades paths

- Improved interoperability and integration
- Improved availability of accurate information whenever and wherever needed
- Improved security
- Reduced technical risk since guidelines are based on International best practices and industry.

The report covers policies and standards for Data, Communications Infrastructure, Hardware, System Administration, Security, Applications, Collaboration and Application Integration. For security, the standards are based on the OECD Guidelines for the Security of Information Systems (OECD, 2002), which has been discussed in chapter four of this thesis. Several technical security technologies are described for maintaining confidentiality and integrity of information.

### 5.3.3 Legal Environment

The following legislation in Rwanda is related to information security in e-Government:

a) The Constitution of the Republic of Rwanda (Republic of Rwanda, 2003) in Article 22 states that :

"The private life, family, home or correspondence of a person shall not be subjected to arbitrary interference; his or her honour and good reputation shall be respected. A person's home is inviolable. No search of or entry into a home may be carried out without the consent of the owner, except in circumstances and in accordance with procedures determined by law. Confidentiality of correspondence and communication shall not be subject to waiver except in circumstances and in accordance with procedures determined by law."

The clause of the confidentiality of correspondence and communication is relevant to this study since G2G transactions would be subject to adherence to this article of the consitution.

b) Other laws: The following bills and laws have been proposed and/or adopted: Information and Communication Technology Bill of 2009; E-Contracting Law of 2010; and Cyber crime bill of 2009 (UNCTAD, 2010). It was not possible to get a detailed description of the contents of these bills and law up to the time of submission of this thesis.

### 5.3.4 E-Government Implementations

A summary of e-Government implementations in Rwanda (Ndahiro, 2009) follows:

a) National Identity (ID) project:

This is an ongoing project that aims at establishing a smart card identification system that offers authentication that will allow access by citizens to different services such as insurance, banking and immigration. A description of the project is available at www.minict.gov.rw.The national ID forms an essential core for any future G2C services that will be offered by the Government of Rwanda.

b) Document Management:

This G2G project seeks to deploy an ICT system across MDAs that should be able to register all incoming and outgoing mail and to provide scanning facilities in case documents being tracked or registered need to be archived. The system would also enable secure and consistent storage of documents and a search facility. This will reduce paper based process and inefficiency in service delivery in all MDAs.

c) Gov-NET:

The key objectives of this G2G project are:

- To inter-network all the government ministries and PSOs via their organizational network into a secure GovNet, the Wide Area Network (Intranet) of Government.
- To provide a common Internet gateway for all government ministries via GovNet.
- To facilitate civil and public service-wide information access, interchange and exchange via GovNet, an important component of the overall e-Government initiative.

### 5.3.5 National Cultural Considerations

Rwanda has adopted a top down approach with strong commitment from the head of government towards the use of ICT as a tool for development of the country (Cunningham, 2007; Kanyesigye, 2011). ICT initiatives and e-Government projects fall under the mandate of the Rwanda Development Board. This strong and visible political commitment to ICT is a very good factor in ensuring that any initiatives can be adopted across the country.

## 5.4 Initiatives in Tanzania

### 5.4.1 Resources

Tanzania is a country in East Africa with a population of about 43 million people and per capita GDP in 2009 of Tanzania Shillings 693,185 or USD 522 (Ministry of Finance and Economic Affairs - Tanzania, 2010a). The government of Tanzania consists of central government ministries, departments and government agencies or parastatal organizations. The central government budget for the financial year 2010/2011 by the Ministry of Communication, Science & Technology, which is responsible for ICT, was Tanzania Shillings 3.1billion - equivalent to about USD 2million (Ministry of Finance and Economic Affairs - Tanzania, 2010b). Internet penetration stands at 11% of the population (Tanzania Communications Regulatory Authority, 2010). A shortage of ICT skills in central and local government in Tanzania has been documented in research carried out by Msuya (2010).

Despite its low GDP, low ICT spending and low numbers of internet users, mobile phone penetration in Tanzania is fairly high, standing at 31% of the population, and the private sector has introduced many services to take advantage of the high use of mobile phones. (Hellström, 2010, p. 14). Citizens expect government to keep up with these innovations and in response the government of Tanzania has come up with policies and strategies to harness the use of ICT. These are outlined in the next sub section.

### 5.4.2 Government Policies, Strategies and Standards

Tanzania's national ICT policy was adopted in 2003 (Ministry of Communications and Transport, 2003), after the Government recognized the need to harmonize independent ICT-related initiatives. The broad objectives of the policy are to provide a national framework that will enable ICT to contribute towards achieving national development goals; and transform Tanzania into a knowledge-based society through the application of ICT. Ten policy areas are articulated, including Strategic ICT leadership, ICT Infrastructure, ICT Industry, Human Capital, Legal and Regulatory Framework, Productive Sectors, Public Service, Local Content and Universal Access. Two of these are particularly relevant to this study. These are:

- Legal and Regulatory Framework: This section of the policy addresses the desire of the Government to ensure that appropriate legal regulatory frameworks are setup and to ensure that electronic transactions take place in a secure environment.

- Public Service: This section states the government's intention to be the model user of ICT to improve efficiency, reduce wastage of resources, enhance planning, raise the quality of services and access global resources.

The Tanzanian e-Government strategy (President's Office, 2009) is aimed at improving efficiency in government and providing better services to citizens. The strategy outlines seven guiding principles including: Service Innovation; Equal Access; Ease of Use; Benefit Realization and Involvement of All Stakeholders; Security and Privacy; Partnership and Outsourcing; and Interoperability. The two principles that relate directly to information security are Security and Privacy and Interoperability. The strategy states that E-Government in Tanzania's context is about "Delivering quality services to the public through technology". In particular the strategy is aimed at the use of ICT to support processes within the government (G2G) as well as for the delivery of services to beneficiaries, such as citizens, businesses and organizations. However, the strategy does not provide guidance to Government MDAs, who are the major implementers of e-Government, on how to go about addressing information security issues.

The salient features addressed by the strategy can be summarised as follows:

- Service Innovation: This involves creating new operational processes and changing current process to lead to innovative services that are sustainable
- Equal Access: Ensure that all citizens will have equal access to e-Government services through different service delivery channels
- Ease of use: Provision of user-friendly Citizen-Care and Business-Centric services for all
- Benefit Realization: Ensuring that the benefits obtained by citizens from using e-Government services will be greater than those from visiting government offices in person
- Security and Privacy: Use of security and privacy mechanisms to ensure the proper use and handling of personal information and transactions
- Partnership and Involvement of all Stakeholders: Building of strategic partnerships with private sector stakeholders and encouraging private-sector led innovations in delivering public services

- Interoperability: Ensuring that newly implemented systems leverage existing systems and are aligned to the principle of Open Access.

The strategy lists six critical success factors, and the requirements for each factor as shown in Table 5-1.

Table 5-1 Critical Success Factors in Tanzania's E-Government Strategy

| Critical Success Factors | Requirements |
|---|---|
| Political will, support and commitment | • Continuous engagement of political leaders in support to e- Government in order to maintain the momentum |
| Availability of HR capacity | • Continuous capacity development<br>• Continuous public involvement |
| Institutional and Legal framework | • Clearly defined institutional framework and supportive legislation and enforcement mechanisms |
| Financial Resources | • Recognition of e-Government as a priority area in the Government agenda |
| Commitment by all actors | • Continuous coordination and buy-in by all actors or stakeholders<br>• Active coordination among all stakeholders to develop and enforce coherent e-Government service delivery |
| Sustainable Infrastructure | • Network and information security Infrastructure to sustain e-Government services |

With regard to standards, the Government of Tanzania has not set any government wide standards related to e-Government.

### 5.4.3 Legal Environment

The legal and regulatory environment in Tanzania has some legislation that is relevant to e-Government transactions. Such legislation includes:

a) The Constitution of the United Republic of Tanzania (United Republic of Tanzania, 2000) which addresses privacy in section 16 as follows:

> "16(1) every person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications.
>
> (2) For the purpose of preserving the person's right in accordance with this Article, the state authority shall lay down legal procedures regarding the circumstances, manner and extent to which the right to privacy, security of his

person, his property and residence may be encroached upon without prejudice to the provisions of this Article."

This article of the constitution can be related to e-Government and to G2G transactions in particular in that any information provided by a citizen to a government agency should be used only for the purpose it was intended for and should be protected from unauthorized access.

b) The Written Laws – Miscellaneous Amendments of 2007 (Parliament of Tanzania, 2007). This law added section 40A to the Evidence Act which reads as follows:

> "In any criminal proceedings, information retrieved from computer systems, networks or servers; or the records obtained through surveillance of means of preservation of information including facsimile machines, electronic transmission and communication facilities; or the audio or video recording of acts or behaviours or conversations of persons charged shall be admissible in evidence."

This law is important since one of the major concerns of government departments and agencies is the possibility of fraud occuring in electronic transactions as a result of insufficient information security controls, as confirmed in the survey findings that are presented in chapter six. If fraud does occur, then the responsible MDA can be held accountable in a court of law through the provision of electronic evidence.

### 5.4.4 e-Government Implementations

Examples of e-Government implementations that have been carried out were obtained from interviews with staff of MDAs as well as requests for information from an online discussion group of Tanzanian IT professionals. This forum is called ethinktank Tanzania and is accessible at the URL http://groups.yahoo.com/group/eThinkTankTz/. The list below gives a description of four e-Government implementations.

a) Parliamentary Online Information System (POLIS)

POLIS is an open access system implemented in 2003. The system provides an index to the proceedings and publications of the Parliament of Tanzania and it includes the full text of parliamentary motions. The system also provides flexible and user-friendly forms to facilitate the searching of contents. Updates are collected from relevant government

departments offline and then updated by the parliament office. The services provided by POLIS can be categorised as Government to Citizen (G2C). POLIS project output can be viewed at www.parliament.go.tz.

b) Government Pensioners Payroll System (GPPS)

GPPS is a system that facilitates the processing of Government pensioners payroll for civil servants who retired from central government before 2004 through an outsourcing arrangement between central government and a government agency. GPPS was implemented in 2009. The service can be categorised as a government to government (G2G) transaction. The central government department responsible for pensions is linked through a secure communications link with the government agency that provides the service. An access control list has been established to guide authorization decisions to different information and functionality. Authentication is through the use of passwords. A contract under the Tanzanian law has been signed between the two parties to govern the provision of the service. This implementation is used as a case study in this thesis and is described in more detail in part IV of the thesis.

c) Central Admission System (CAS)

CAS allows students who have completed high school to apply online, through mobile phone or the internet, to public and private universities. The system was implemented in 2010. Access is granted when a valid examination number is entered. Currently the service offered is a G2C service although it is planned that the system shall be expanded to involve G2G transactions with other agencies such as the agency responsible for issuing student loans. An interface of this system can be viewed at www.tcu.go.tz.

d) Tanzania Interbank Settlement System (TISS)

TISS is a system to allow transfers of payments that involve accounts with the Bank of Tanzania (BoT). The system was first implemented in 2004 for commercial banks but use by Ministry of Finance and Economic Affairs started in 2010 (Ministry of Finance and Economic Affairs, 2010c). The services can be categorised as G2B and G2G. Access is through special terminals connected through secure communications links. For payment transfers a link provided by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) is used, while for enquiries a virtual private network has been set up. Contractual agreements are signed between participating parties which are

binding under the laws of Tanzania. The participants are financial institutions that are regulated by the Bank of Tanzania and institutions that deal in high volume large transaction payments. An example is the Tanzania Revenue Authority who the MDA with the responsbility for collection oftaxes. More information on TISS is available at http://www.bot-tz.org/PaymentSystem/NPSoverview.asp.

### 5.4.5 National Cultural Considerations

Chaula et.al (2006) investigate the role that culture plays in information security in an organization in Tanzania and suggests that the unstructured approach to information security management is a reflection of the unstructured approach to life in general in Tanzania.

## 5.5 Initiatives in Uganda

### 5.5.1 Resources

Uganda has a population of about 30 million and a per capita GDP of USD 506 (Office of the Prime Minister, 2010). The 2010/2011 budget estimates for spending on ICT is Uganda Shillings 12.15 billion (Republic of Uganda, 2010) which is about USD 5million. Internet usage stands at 8% of the population while mobile phone penetration is at 27% of the population (Hellström, 2010).

### 5.5.2 Government Policies, Strategies and Standards

As was the case with Tanzania, Uganda adopted its National Information and Communication Policy in 2003. The policy (Ministry of Works, Housing and Communications, 2003) sets out 14 policy objectives. For purposes of this study, three of the objectives that are highlighted are:

- To promote the use of ICT in the stimulation of production, storage, and dissemination of in-country information and knowledge in both the public and private sectors
- To facilitate the broadest possible access to public domain information
- To provide for establishment of an enabling and desirable legal and regulatory framework that, among other things, takes into account the convergence of technologies.

The Uganda National e-Government Strategy was drafted in 2004. The strategy (Ministry of Works, Housing and Communication - Uganda, 2004) identifies establishment of standards as one of the areas where action has to be taken. It is stated that an architecture that enables

collaboration and seamless integration of various systems is required. The key components of such architecture would be a common e-Government Portal, metadata for presenting information and services to this portal and a secure e-Government environment to ensure that the documents and information sent reaches only the intended recipients and in time.

### 5.5.3 Legal Environment

Of the three countries surveyed, Uganda has made the most strides in putting in place an enabling legal environment for e-Government. The following is legislation in Uganda that relates to e-Government and information security:

a) The constitution of the Republic of Uganda (Republic of Uganda, 1995) states in Section 27 subsection 2 that:

   "No person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property".

   This is similar to the Tanzanian constitution and relates to the need for G2G transactions to preserve the privacy of the information that is exchanged.

b) National Information Technology Authority Act (Parliament of Uganda, 2009) which defines e-Government as the use of information and communication technologies to deliver services in a convenient efficient customer-oriented and cost-effective way. The functions of the National Information Technology Authority, as stated in the Act, that have direct bearing on this study include regulation and enforcement of standards including security standards; regulation of electronic signature infrastructure and other matters related to electronic information and provision of guidance on the establishment of e-Government.

   This law could be used to address the authentication security requirement by having the National Information Technology Authority (NITA) act as the agency in charge of issuing digital certificates or electronic credentials to MDAs.

c) Electronic Transactions Bill (Ministry of Information and Communication Technology - Uganda, 2008a). Salient definitions in this bill include:

   "e-Government services" includes a public service provided by electronic means by a public body in Uganda;

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

The bill strives to create a legal framework for the facilitation of electronic transactions through recognition of electronic evidence as part of a legal process, electronic signatures and defining the authenticity of the electronic record.

d) Electronic Signatures Bill (Ministry of Information and Communication Technology - Uganda, 2008b): This bill aims to govern the use of electronic signatures and certification authorities.
e) Computer Misuse Act (Parliament of Uganda, 2010): is aimed at making provision for the safety and security of electronic transactions and information systems; preventing unlawful access, abuse or misuse of information systems including computers and making provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters.

### 5.5.4 e-Government Implementations

Examples of e-Government implementations in Uganda were difficult to come by. Information was sought by contacting staff of the ICT ministry as well as sending requests to an online discussion forum for Ugandan IT professionals, namely the iNetwork forum (www.i-network.or.ug). A few examples of e-Government implementations in Uganda are described below.

a) DistrictNet

DistrictNet is a G2G infrastructure project that is aimed at interconnecting of government districts and was started in 2002. The objective is to improve performance and productivity in local government (De Jager & Van Reijswoud, 2007). The project will allow exchange of information used in routine operations of government such as payroll information and inputs required for centralized planning and budgeting.

b) SchoolNet

This project started in 1997 as a program supported by the World Bank and the Ministry of Education and Sports of Uganda. A portal of educational resources for schools has been developed and is available at the URL www.schoolnetuganda.sc.ug. Schools are given user names and passwords to be able to access the content on the portal. The project embodies both G2C and C2C functionality, allowing Government to disseminate information electronically to schools, and for teachers and students to interact in areas of common interest.

c) e-Tax filing

In 2010, the Uganda Revenue Authority launched a portal that enables citizens and businesses to file their tax returns online and to register payments made to the authority. A user needs to register and login in using a Tax Identification Number (TIN) and a pass code. The portal is accessible at www.ura.go.ug. The e-Portal will allow both G2C and G2B transactions, and it will be expanded in the future to incorporate G2G transactions between the revenue authority and other government agencies who require some of the information filled in by tax payers for the own transactions. An example is the Ministry of Lands who require evidence of tax payments in the process of granting land titles.

### 5.5.5 National Cultural Considerations

A national ICT master plan and e-Government network feasibility study carried out in Uganda in 2006 (MEGA-TECH, Inc, 2006) states the following:

> "There is a broad range of individual, and largely uncoordinated, ICT initiatives and programs ongoing across the Government. This lack of coordination precludes a planned, managed, and adequately funded integrated approach to ICT development. Therefore, an ICT Master Plan to guide the coherent development of ICT within the government must focus on structures and processes that foster integration,

cooperation, and common objectives and processes. Even successful ICT initiatives such as the World Bank project with the Ministry of Finance to implement the Financial Management System and the Information Sharing System have not resulted in a dialogue of lessons learned with other Government entities to provide a model of ICT implementation."

The report further notes that many of the initiatives are donor funded, which are difficult to sustain. This statement points towards a national culture that does not involve cohesive planning. Since one of the research questions' being addressed in this thesis is aimed at developing a sustainable framework, the approach proposed is one that recognizes the frequent lack of co-ordination in government initiatives.

## 5.6 Discussion

The previous sections in this chapter have presented the practices at a national level in Tanzania, Uganda and Rwanda. A Strengths, Weaknesses, Opportunities and Challenges (SWOC) analysis in the context of our research question can be obtained from the information above for each country as shown in Table 5-2.

Table 5-2 SWOC analysis of e-Government practices in Tanzania, Uganda and Rwanda

| | **Rwanda** | **Tanzania** | **Uganda** |
|---|---|---|---|
| Strength | Strong policies that encompass international standards. Centrally co-ordinated initiatives | Some successful implementations | Enabling legislation is in place |
| Weakness | Few internet users/ mobile phones; lack of a comprehensive national framework for information security in e-Government | Lack of enabling Legislation; lack of a comprehensive national framework for information security in e-Government | Few implementations and lack of a comprehensive national framework for information security in e-Government; |
| Opportunities | Ongoing implementations; and ongoing drafting of legislation | Ongoing implementations | Ongoing implementations |
| Challenges | Resource constraints; | Resource constraints, culture of unstructured approach to information security | Resource constraints, culture of uncoordinated initiatives |

The challenges for the three countries surveyed are common, that is resource constraints. The culture is different from Rwanda where government initiatives are centrally coordinated, with ICT initiatives falling under the mandate of the Rwanda Information Technology Authority

(RITA) which is now part of the Rwanda Development Board. In the other two countries, Tanzania and Uganda, there are un-coordinated and unstructured initiatives. In terms of initiatives at a regional (EAC) level, the un-coordinated culture in the two countries shall have an effect on the implementation of regional initiatives, and is thus taken into consideration in the design of the framework for information security in G2G transactions that is presented in chapter eight of this thesis. A framework for the EAC would have to take into consideration that combination of factors that are firstly, resource constraints – both financially and in terms of adequate human resource skills; secondly, legal and regulatory constraints – both insufficient legislation and lack of specific national information security frameworks; and thirdly, national culture constraints – un-coordinated or unstructured approaches to ICT initiatives. These EAC contextual factors are compared against other countries in Table 5-3. The United Kingdom is chosen as representative of the four countries whose national information security frameworks are discussed in chapter three, and who are ranked in the top ten in the 2010 UN e-Government development index (United Nations, 2010). South Africa is chosen, because it is the only African country whose information security framework was discussed in chapter four.

Table 5-3 Comparison between EAC and United Kingdom and South Africa

| **Factor** | **EAC** | **United Kingdom** | **South Africa** |
|---|---|---|---|
| Resources | Average national (public sector) ICT related budgets of about USD 96 million for year 2010 | National (public sector) ICT budget of about USD 12billion for year 2010[1] | National (public sector) ICT budget of USD 2.7 billion for year 2010[2] |
| Legalisation/ Regulatory Environment | Some legislation & policies are in place; no national frameworks | Legislation in place, national frameworks in place [3] | Legislation in place, national frameworks in place[4] |
| Culture | Uncoordinated and unstructured approaches in government | Coordinated approaches towards e-Government[5] | Coordinated approaches towards e-government[6] |

## 5.7 Conclusion

The context of the EAC has, so far in this chapter, been discussed at a national or governmental level.

[1] www.directgov.uk
[2] www.treasury.gov.za
[3] Discussed in section 3.2.1 of this thesis
[4] Discussed in sections 3.3.1 and 3.4.2 of this thesis
[5] www.cabinetoffice.gov.uk
[6] www.sita.co.za

The contextual issues identified are:

- All the governments in the EAC countries surveyed are under financial resource constraints. National / Public sector ICT budgets are small. The comparison of financial resources was the EAC average against one country in Africa and one country in the developed world. A lack of adequate skills in ICT has also been identified. The framework developed must be such that it can be applied in a resource-poor environment.
- Legislation related to information security does exist and is continuing to be put in place in the EAC. In addition, although no national information security related frameworks are in place, there are some related policies such as e-government strategies and national ICT policies that include some provisions for information security in e-Government. The framework developed must recognize existing legislation and seek to raise awareness across MDAs on that legislation.
- Many e-Government initiatives are not centrally conceived and/ or coordinated. Thus any framework developed cannot presuppose coherency across governments even though national e-government strategy documents do exist.

The above contextual issues are the factors that need to be addressed in an information security framework for G2G transactions in the EAC. These factors can be summarized as resource constraints; legal and regulatory constraints and national culture constraints. Identification of these factors answers the second research question of this study.

The combination of these three factors are what distinguishes the context of the EAC from other countries, specifically the countries whose national information security frameworks were discussed in chapter three as is presented in Table 5-3. It is possible that some countries outside of the EAC have similar issues. In that case the framework developed and presented in chapter eight of this thesis could be generalized and applied to countries with a similar combination of issues.

This chapter presented national and regional EAC issues. For G2G transactions that take place in individual agencies, there is a need to discover more information on practices in individual MDAs with the EAC. This was done, as part of this study, through a survey whose findings are presented in chapter six.

# Chapter 6 Survey of Practices in Individual MDAs

## 6.1 Introduction

In chapter four, data has been obtained from secondary sources, in an attempt to analyze the context in which G2G transactions are being carried out in the EAC. This information however needs to be supplemented with empirical data on actual G2G transactions taking place if any. Furthermore data needs to be obtained on the information security practices in place that surround the G2G transactions that are taking place.

The use of empirical data in interpretive approaches is discussed in de Villiers (de Villiers, 2005) where surveys and questionnaires are one of the research strategies that overlap between the positivist and interpretivist approaches. The objective of the survey presented in this chapter was to supplement the findings from literature that are presented in chapter four by obtaining actual practices in central government (ministries and departments) and government agencies (including parastatal organisations). The survey was also aimed at triangulating some of the information obtained in chapter five, from reviewing Government initiatives in e-Government, including application of standards or specific mechanisms to ensure security.

The questionnaire included both closed and open type responses. Open responses were designed to encourage descriptive answers on what is actually being done and what the views of the MDAs are. The questionnaire used is included in this thesis as Appendix A.

## 6.2 Areas Covered by the Survey

The questionnaire covered nine areas designed to address security mechanisms/ solutions that are in place in the MDA for G2G transactions thus contributing to answering the research question on the EAC contextual issues. The areas surveyed also attempted to obtain additional information on the security mechanisms mentioned in the literature that was reviewed in chapter four. The areas that were surveyed are:

### 6.2.1 Presence of an information security policy

The East African Regional e-Government Strategy, (East African Community Secretariat, 2005) states that the EAC shall develop a secure information infrastructure in all the partner states. By implication, all participating MDAs shall have to have secure information infrastructures in place both for internal and for G2G transactions. An organizational information security policy is a tool that is useful in documenting the information security guidelines that need to be adhered to be an organization. Such a document would typically incorporate the particular contextual issues that are relevant to the organization and is usually aligned with the organizations operational activities and strategic goals. An organizational information security policy should guide both internal organizational transaction and external collaborations. For the purpose of this survey, a question was asked as to whether or not an information security policy was in place.

### 6.2.2 Mode of transaction with other MDAs

The definition used for a G2G transaction for this research was the transactions between one government agency and another (within a country or across countries). The question in the survey was aimed at establishing whether the MDA transacts manually, by email or through access to computer systems of other MDAs. It was also necessary to establish an indication of the volume of electronic transactions that are actually taking place. However, even for manual transactions, security mechanisms and practices need to be in place, so as to ease transformation to electronic transactions when it occurs. The mode of transaction would enable the design of an information security framework that takes into consideration current modes of transaction (whether manual or electronic) and provides for future changes or modifications to the mode of the transactions. Such flexibility in the framework shall enhance the sustainability of the framework, which is part of the third research question of this study.

### 6.2.3 The kind of information involved in transactions

The need for data protection for information in e-Government transactions is highlighted in the EAC Regional e-Government Framework (East African Community Secretariat, 2005), and is reflected in e-Government strategy of some of the partner countries (United Republic of Tanzania, 2009), (RITA, 2006). Additionally, as presented in chapter four, partner countries of the EAC have recently put in place legislation that is related to protection of

electronic transactions. The survey question on the kind of information involved in transactions was to establish if sensitive information such as confidential information or payment related information was being exchanged between MDAs. The aim was to establish the security requirements based on the information involved in the G2G transactions, which is the first research question of this study.

### 6.2.4 Concerns in electronic transactions

In chapter three, policy level information security frameworks (Cabinet Office UK, 2008) pointed out some concerns that are addressed by governments, including Business Continuity and Access Control. The survey question on concerns in electronic transactions was aimed at identifying areas perceived as high risk in electronic transactions. The options given in this case were fraud – that would possibly result from weak access control; network breakdowns resulting in interruption of electronic G2G transactions and any other concerns that the respondent could be aware of. In EAC, issues such as frequent power failures and poor communications infrastructure may be a major concern in implementing e-services, leading to network breakdowns and thus the need for addressing of business continuity as part of an information security framework. The responses to this question shall therefore contribute to developing the information security framework, which is the third research question of this study.

### 6.2.5 Security mechanisms in use for data exchange

The country specific e-government documents mention mechanisms that may be used to address information security (RITA, 2006). The survey question on security mechanisms in place was to establish whether these mechanisms are practically in use in MDAs. Mechanisms that are already in use would be included in the proposed framework as part of the interpretive research approach, focusing on and using the positives that are already in place to come up with a solution to security of G2G transactions in the EAC. The security mechanisms could include a wide range of technological tools such as PKI or any other encryption mechanisms, antivirus software, etc. The question was also aimed at seeking to find a correlation, if any, between the kinds of information exchanged and the mechanisms in place. This survey thus included an open ended question to allow respondents to fully describe the mechanisms in place.

### 6.2.6 Presence of binding agreements between collaborating MDAs

In a G2G, one MDA exchanges information with another MDA based on a request by one of the MDAs or perhaps as a requirement of existing legislation. The survey question of the presence of binding agreements related to the security information between the MDAs was to establish if such agreements exist. The presence of such an agreement would mean that, even in the absence of national level legislation in respect to security of information exchange in G2G transactions, the MDAs can still transact in an accountable manner. Such an agreement could be in the form of a contract or a memorandum of understanding.

### 6.2.7 Presence of common format for exchange

Interoperability is one of the challenges in electronic G2G transactions and some of the policy level information security frameworks studied have provided for standards or mechanisms to address interoperability (SITA, 2007), (Ministry of the Presidency, Spain, 2010). Since the parties in a G2G transaction may be running different applications in different computing environments with different data formats, there has to be a mechanism to ensure interoperability, to ensure successful electronic exchange of information without comprising the integrity of the information. This survey question was aimed at collecting information on formats in place that enhance interoperability.

### 6.2.8 Presence of common language or terminology or laws

Ultimately electronic G2G transactions involve machine to machine interactions enabled for example by web services as seen in some of the studies cited in chapter two of this thesis (Hu, Quirolgico, & Scarfone, 2008), (Gutiérrez, Rosado, & Fernández-Medina, 2009). In transactions that involve machine to machine communications, for example, through web services, lack of semantic interoperability can lead to incorrect authorization or access control decisions. This survey question was aimed at investigating if MDAS define standard terminology to be used in multiparty transactions. Such terminology would save as a basis for addressing semantic interoperability in G2G transactions.

### 6.2.9 Views of the MDAs on the need for standards

MDAs were requested to provide their views on the need for development and adoption of national standards related to information security. This question was to establish whether MDAs saw the need of national frameworks such as those examined in chapter three of this

thesis, and or adoption of other international / regional standards related to information security.

### 6.3 The Survey Respondents

Questionnaires were sent by email and or physical delivery to fifty MDAs in the three countries surveyed which are Rwanda, Tanzania and Uganda. Of these, 18 MDAs responded. A follow up of those who did not respond was done by telephone, email or physical visits. Eighteen of the MDAs that did not respond gave the reason that they did not have IT departments in place and as such felt they were not in a position to respond. Four of these 18 MDAs, all based in Rwanda, referred us back to the Rwanda Information Technology Authority (RITA – now part of the Rwanda Development Board) as the authority that addresses all IT related issues. RITA did respond to the questionnaire. The remaining 14 MDAs did not give a reason as to why they did not respond. The pattern of responses of the questionnaire is shown in Table 6-1.

Table 6-1 Pattern of Responses to Questionnaire

| Country | No. of questionnaires sent out | No. of MDAs that responded | No. of MDAs that gave a reason for lack of response | No. of MDAs that did not give a reason for not responding |
|---|---|---|---|---|
| Tanzania | 20 | 8 | 10 | 2 |
| Uganda | 20 | 6 | 4 | 10 |
| Rwanda | 10 | 4 | 4 | 2 |
| | 50 | 18 | 18 | 14 |

Given the difficulties in collecting data on ICT related issues as discovered in other studies (Msuya, 2010), the data collected from 18 MDAs was taken to be significant enough to represent the practices in the EAC.

Of the responses, eight were from Tanzania, six from Uganda and four from Rwanda.

Respondents were asked to state whether they were from central government (ministry or department); an agency, parastatal or any other government institution (government agency). From the 18 respondents, 5 were from ministries or departments, and 13 were from government agencies.

The respondents were also asked to state their role in the MDA as being Managerial (IT), Managerial (Other), IT Support or Operations. Of the 18 responses received, 10 were from Managerial (IT), 2 were from Managerial (other), 6 were from IT Support and none from operations. The profile of the respondents is shown in Figure 6-1 below:

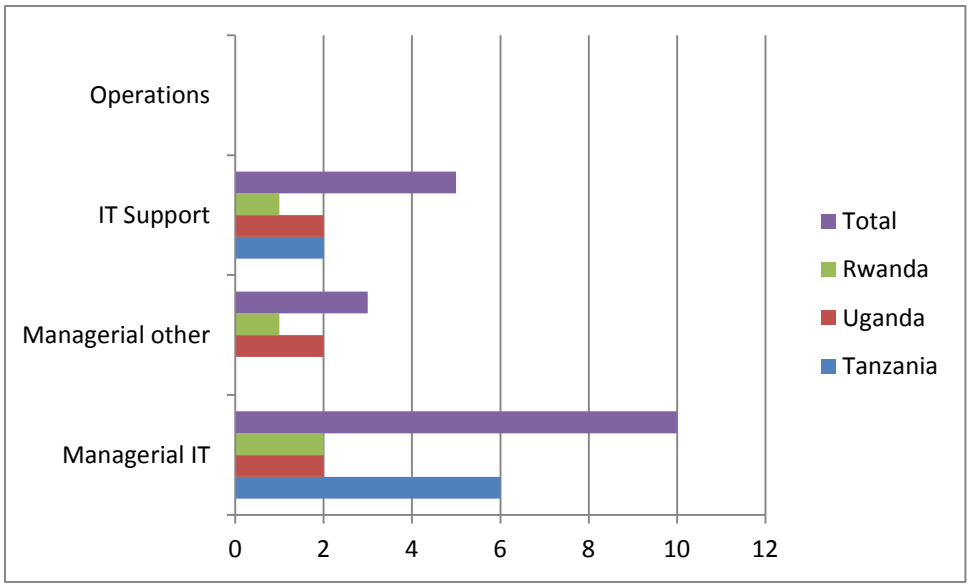



Figure 6-1 Profile of Respondents

The figure shows that over 50% of the respondents occupied a managerial role in IT. This is to be expected as the survey questions touched on both policy and technical issues.

## 6.4 Key Findings

The survey was carried out to supplement findings on contextual issues that were presented in chapter four, and to obtain some insights into how a framework can be developed for information security. The key findings from the survey are summarized in the sub sections below, while the detailed findings are presented in the next section. The three subsections are summarized based on three research questions.

### 6.4.1 Information Security requirements for G2G transactions in the EAC

G2G transactions are indeed taking place, and 44% of the respondents indicated that these interactions involved direct access to systems in the other agencies. The security requirements for such access would involve authorization and access control mechanisms and will be discussed further in chapter six. However, only 33% of the respondents indicated

that binding agreements are in place and common formats for data interchange exist. Even less, 22% indicated common terminology for data exchange between MDAs which points to a need to enhance the security mechanisms with mechanisms for semantic interoperability. Additionally over 50% of the respondents were concerned with the possibility of both fraud and network break downs thus the requirement to ensure proper access control and authorizations, as well as putting in place mechanisms to ensure availability of systems.

### 6.4.2 Contextual issues in MDAs in the EAC

The contextual issues discovered in the survey include the presence of manual interactions between MDAs. Over 60% of the respondents indicated some form of manual transactions amongst agencies. The other key discoveries from the responses are lack of cross government interoperability guidelines, as compared to the countries whose guidelines were presented in chapter three. Another discovery was that, although some agencies lack information security policies, all MDAs have some security mechanisms in place, indicating awareness of the need for information security.

### 6.4.3 Information Security Framework for G2G transactions

Respondents were unanimous in the need for standards for secure information exchange in G2G transactions. One Respondent put it this way:

> "There are many IT security solutions that institutions may deploy. Some may be stronger than the other, and some may be incompatible with the other. Then their differences may not facilitate the information exchange. That's why I think that any government needs to define standards for the security they want according to their requirements. Having the security standards will facilitate even the maintenance and the interoperability of the security systems that have been deployed in different government institutions."

However, it was interesting to note that even where governments have documents that state or prescribe specific information security standards or mechanisms for e-Government as is the case for Rwanda, 75% respondent agencies from Rwanda did not reflect these at all in their responses. Significant also was the correlation between a binding agreement being in place with the MDA having a common format of data exchange. That is, all MDAs that

indicated that a binding agreement was in place also indicated the presence of a common format of data exchange.

These survey findings are combined with the other research done to come up with an information security framework for G2G transactions.

### 6.5 Detailed Findings

The detailed findings of the survey questions are as follows for each of the survey questions:

i. Presence of information security policy: All MDAs except three have a documented information security policy.

ii. Mode of transaction with other MDAs: Most agencies transact through all the three modes specified which are, manually, email, and access to computer systems of the other MDA. Eight out of the eighteen agencies surveyed indicated transactions involving access to computer systems of the other agencies.

iii. Type of information involved in the transactions: Sixteen agencies indicated that payment information is involved in the transaction, and fifteen indicated confidential information. Other information indicated in the responses includes data for budget preparation and reports.

iv. Concerns in electronic transactions. Eleven MDAs are concerned with fraud and fourteen with network breakdowns. The other concerns raised include reconciling manual and electronic transactions where both kinds of transactions are used.

v. Security mechanisms: Varied mechanisms were listed including passwords, encryption, Secure Socket Layer (SSL) certificates and access control lists.

vi. Binding agreements: Twelve out of the eighteen MDAs surveyed do not have binding agreements. Where agreements were in place, they are in the form of a memorandum of understanding (MoU).

vii. Common format of exchange: Fourteen MDAs do not have a common format for exchange of information. The MDAs that do have a format indicated that format as being Society for Worldwide Interbank Financial Telecommunication (SWIFT) secure messaging service, system interfaces, and a national payroll standard.

viii. Common terminology/ language: Eight MDAs do not have a common basis for language or terminology. The MDAs that indicated the presence of a common terminology stated English, laws of Uganda, payroll manual and standards.

ix. Views of the need for standards: All responses indicated a need for information security standards at a government level.

The data obtained is as summarized in Table 6-2.

Table 6-2 Summary of Survey Responses

| **Area Surveyed** | **RW** | | **TZ** | | **UG** | | **TOTAL** | |
|---|---|---|---|---|---|---|---|---|
| | Y | N | Y | N | Y | N | Y | N |
| Presence of information security policy | 2 | 2 | 7 | 1 | 6 | 0 | 15 | 3 |
| Mode of transaction with other MDAs: | | | | | | | | |
| Manual | 3 | 1 | 8 | 0 | 3 | 3 | 14 | 4 |
| Email | 4 | 0 | 8 | 0 | 5 | 1 | 17 | 1 |
| Access to systems | 0 | 4 | 4 | 4 | 4 | 2 | 8 | 10 |
| Type of transactions: | | | | | | | | |
| Payment | 4 | 0 | 7 | 1 | 5 | 1 | 16 | 2 |
| Confidential | 4 | 0 | 7 | 1 | 4 | 2 | 15 | 3 |
| Other | 1 | 3 | 3 | 5 | 2 | 4 | 6 | 12 |
| Concerns in electronic transactions: | | | | | | | | |
| Fraud | 0 | 4 | 7 | 1 | 4 | 2 | 11 | 6 |
| Network Breakdowns | 3 | 1 | 5 | 3 | 6 | 0 | 14 | 4 |
| Other | 1 | 3 | 1 | 7 | 2 | 4 | 4 | 14 |
| Security mechanisms | 1 | 3 | 7 | 1 | 6 | 0 | 14 | 4 |
| Binding agreements | 1 | 3 | 3 | 5 | 2 | 4 | 6 | 12 |
| Common format of exchange | 1 | 3 | 3 | 5 | 2 | 4 | 6 | 12 |
| Common terminology/ language/ laws | 0 | 4 | 0 | 8 | 4 | 2 | 14 | 4 |
| Views on the need for standards | 4 | 0 | 8 | 0 | 6 | 0 | 18 | 0 |

RW=Rwanda TZ=Tanzania UG=Uganda

The findings show that:

i. Where a binding agreement is in place, there is also a common format of exchange.

ii. The need for standards is unanimous for all respondents.

The significance of these findings is that while no national information security frameworks have been developed in the EAC, MDAs do recognize the need for standards and have put in place some ways to ensure interoperability across MDAs that are participating in G2G transactions.

The secondary aim of this survey was to triangulate with the findings in chapter four. The areas where the survey confirms information presented in chapter five include establishment that electronic G2G transactions do actually take place as described in the examples of e-government implementations in the three countries surveyed and common formats and binding agreements are in place.

A mismatch was, however, observed in the survey response to the question on the need for national level standards in the case of Rwanda. The e-government strategy document mentions standards, but respondents from MDAs did not refer to those standards. This finding raises the need for a process model that will lead to MDAs continually checking what national level initiatives are in place, and basing their own initiatives on them. The process model that is presented as part of the information security framework proposed in this thesis addresses this need.

## 6.6 Conclusion

In this chapter, the results of a survey on the individual practices related to information security of MDAs in the EAC have been presented. These findings indicate that some practices exist, but there is a need for a common framework that addresses the gaps in the information security frameworks in individual agencies. Although responses were obtained from only 18 MDAs out of the fifty to which questionnaires were sent, the responses obtained will add significant utility to the framework that is developed as part of the study. The framework, however, should be such that it considers three factors that were identified in the situational analysis presented in chapter five which are resource constraints; legal and regulatory constraints and national culture constraints.

This chapter concludes the discovery phase of the study, and all the discoveries presented so far are synthesized in chapter seven to come up with information security requirements for G2G transactions in the EAC in answer to the first research question.

# PART IV: PROPOSED INFORMATION SECURITY FRAMEWORK FOR G2G TRANSACTIONS IN THE EAC

# Chapter 7 Proposed Information Security Requirements for G2G Transactions in EAC

## 7.1 Introduction

In parts II and III of this thesis, discoveries related to the three research questions were presented. These discoveries were firstly from a literature review of researches and implementations related to information security for e-government in general and G2G transactions, and secondly from a situational analysis and survey of practices in the EAC.

Following the appreciative inquiry process adopted as one of the methods this study, after the discoveries phase, comes the dream phase. This chapter presents the dream phase of the Appreciative Inquiry process. The dream phase involves creating a clear results-oriented vision in relation to the discovered potential. The dream phase builds upon the discoveries and extends those to come up with an ideal. This vision is translated into an implementable design in the next phase, which is the design phase. Finally in the implementation phase, the design is adopted and implemented.

In this phase, the knowledge discovered and presented in chapters 2 through 6 is analyzed to bring out the positive ideas that can be used to visualize information security requirements for G2G requirements in the EAC.

The dream phase is conducted either by using matrices or brainstorming sessions. In this study, the dream phase is conducted by presenting the discoveries in matrices. In order to build a list of information security requirements for G2G in the EAC, a set of matrices is built based on discoveries of each chapter of parts II and III. Each matrix is refined based on subsequent discoveries. At the end of the chapter, these discoveries are synthesized into a set of information security requirements for G2G transactions in the EAC.

## 7.2 Key Discoveries from Part II

Part II of the thesis covered three chapters which are chapter two – Research related to information security in e-government; chapter three – Examples of policy level information

security frameworks; and chapter four – Standards related to information security for e-government.

### 7.2.1 Discoveries from Related Research

The first set of matrices is built using discoveries in sections 2.2, 2.3 and 2.4 of this thesis. These are discoveries include requirements for information security and mechanisms for meeting the information security requirements as shown in Table 7-1 below.

Table 7-1 Mechanisms to implement information security requirements

| **Domain** | **Requirement** | **Mechanism** |
|---|---|---|
| General Information security requirements | Authentication | Encryption, standards |
| | Access Control | RBAC, ABAC, GBAC, Access control policies, semantic web |
| | Message Integrity | Encryption |
| | Confidentiality | Encryption, Standards |
| | Privacy | Encryption, Standards, Policies |
| | Non Repudiation | Legislation |
| | Trust | Contractual Obligations |
| G2G Specific Requirements | Formal Contracts | |
| | Legal Compliance | |
| | Reuse | |
| | Technical Neutrality | Web Services, Service Oriented Architectures |
| EAC Specific Requirements | Need to consider context | Open standards |
| | Need not to require full implementations | Use of maturity models for tracking progress |

There is some overlap on what is presented as a requirement and what is presented as a mechanism in some cases. A clear separation will be achieved once all the discoveries are presented and synthesized in section 7.2.4. In addition, the EAC specific requirements cited in the research studies are not sufficient to fully address the challenges stated in chapter one of this thesis. These discoveries are therefore combined with more discoveries from the other chapters in part II and with the EAC situational analysis in Part III before attempting to answer this study's research questions.

### 7.2.2 Discoveries from Policy Frameworks

The examples of policy frameworks presented in chapter three mostly add to discoveries that can adopted with modification in the design of an information security framework. The same domains used in the matrices above can be used to present the discoveries. The discoveries are presented in Table 7-2 below.

Table 7-2 Discoveries from policy frameworks

| Domain | Requirement | Mechanism |
|---|---|---|
| General Information security Requirements | Availability | Business Continuity |
| G2G Specific Requirements | Organizational structures | Clear information security roles |
| | Interoperability | Technical, operational and semantic interoperability, use of standards |
| EAC Specific Requirements | Sustainability | Governance, Risk, Compliance, mapping of outputs of roles; addressing of information security across government and in individual agencies, use of open standards, tie to overall government goals |

The sustainability requirement is part of the third research question of this study for each the use of standards is suggested as a way to meet that requirement. The discoveries from the standards discussed in chapter four are discussed in the sub section below.

### 7.2.3 Discoveries from Standards

In chapter four, non-technical and technical standards were presented. The discoveries from these add mainly to the proposed mechanisms for information security requirements that have already been discovered. These are presented in Table 7-3 below.

Table 7-3 Discoveries from Standards

| Domain | Requirement | Mechanism |
|---|---|---|
| General Information security Requirements | Accountability | Provision of assurance through, technical and non-technical measures |
| | Confidentiality, Integrity, Availability and Accountability | Use of open standards including XACML, SAML and WS Security |
| G2G Specific Requirements | Internal Processes to address information security | Promotion of effective information security within organizational boundaries. |
| | Privacy | cross border legislation |
| | Authentication | National level measures for authentication; |
| EAC Specific Requirements | Consider influence of national culture | |
| | Sustainability | Critical Success Factors |

### 7.2.4 Synthesized Requirements

The first research question of this study is to identify information security requirements for G2G transactions in the EAC, and a G2G transaction has been defined as "*The sharing of*

*information resources and services between government agencies in a restricted network setting with the ultimate aim of providing comprehensive, easy to access services to citizens."*

The discoveries presented in sections 7.2.1-7.2.3 present requirements and mechanisms at different levels of granularity. For purposes of this study, two levels of granularity are considered in answering the first research questions. At the lower level, six security requirements are derived from discoveries as being:

- Authentication
- Authorization and Access Control
- Privacy
- Data Integrity
- Availability
- Trust and Non Repudiation

The above requirements are grouped, at a higher level, into four security objectives, and the description of each objective aligned with the first research question as well as the definition of G2G transactions. The security objectives are:

i. Confidentiality: This is defined as the principle of ensuring that an MDA participating in a G2G exchange only accesses information and systems that they are authorized to and any privacy requirements are preserved during the transaction. Confidentiality, as a security objective is motivated by the nature of G2G transactions identified in the survey of MDAs that was presented in chapter six of this thesis.

ii. Integrity: This is defined as the principle of ensuring that the completeness, correctness and consistency of data are not compromised during exchange between MDAs that are participating in a G2G transaction. Integrity as a security objective is motivated by the nature of G2G transactions in which different sets of data may be obtained from different MDAs for the purpose of providing a composite service. The integrity of all the data obtained should be maintained throughout the G2G transaction.

iii. Availability: This is defined as the principle of ensuring that the systems and the data that is required by MDAs in G2G transactions are available when required. Availability as a security objective is motivated by the recognition that G2G transactions ultimately aim at achieving easy access to services to citizens when required.

iv. Accountability: This is defined as the principle of ensuring that MDAs involved take responsibility for the data, and or system access they provide to other MDAs. Accountability as a security objective is motivated by the recognition that there are already incidences reported where a G2G transaction has resulted in some fraud or foul play in the EAC (*The Guardian* Newspaper, 2009). Thus MDAs must have mechanisms to ensure that other MDAs trust the data or services that they provide.

The Confidentiality objective encompasses three security requirements which are Authentication, Privacy and Authorization and Access Control. The integrity objective encompasses the Data integrity requirement, while the Availability and Accountability objectives cover the availability and the trust and non-repudiation requirements respectively. The description of the six information security requirements is shown in Table 7-4.

Table 7-4 Security Objectives and Requirements

| Security Objective | Security Requirement | Description of Requirement |
|---|---|---|
| Confidentiality | Authentication | Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system |
| | Privacy | Control of access to information in accordance to laws, regulations or policies |
| | Authorization and Access Control | The decision to allow a user, process, or device access to information or information processing services, and the process of granting or denying specific requests for obtaining and using information and related information processing services |
| Integrity | Data Integrity | The property that data has not been altered in an unauthorized manner |
| Availability | Availability | The property that a service is available whenever required |
| Accountability | Trust and Non-Repudiation: | The attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities and not to deny any actions done |

The description of the requirements presented in Table 7-4 is a generic description that could apply to any kind of electronic transaction. Furthermore, the six requirements could be stated at a different of granularity depending on the context in which they are being applied. For instance, the trust and non-repudiation requirement may be broken down into two separate requirements or the Integrity objective could be taken to encompass more than one requirement, that is, include data, communications and systems integrity. For this study, however, the level presented is seen to be sufficient based on the definition of G2G transactions which is the exchange of information and services between government agencies in a restricted network setting. In particular:

- Authorization and Access Control are grouped together as one requirement. This is because in a G2G transaction, the user or system requesting for authorization must be requesting for a particular service from the responding system. Thus an authorization request must be responded to not only with an authorization to access a system but also to which resources or services the requester is allowed to use.
- Data integrity is the only requirement addressed under the Integrity objective. Other possible forms of integrity such as system integrity or communications integrity are

not included. The justification for this is that the valuable resource being secured in a G2G transaction is the data. While communications between two MDAs participated in a G2G transaction may be compromised, this is addressed under the Confidentiality objective with the need to ensure that any systems or communication line accesses are authenticated authorized and preserve the privacy of the data that is being communicated in the G2G transaction.

- Trust and Non-Repudiation are grouped together as one requirement. The justification for this level of granularity is that in a G2G transaction, an MDA will typically have to establish trust through an agreement, since the parties involved are both government agencies. The trust and non-repudiation requirements would form inseparable parts of such an agreement.

The security objectives and security requirements, together address part of the first research question. The motivation for the identified security objectives and requirements is tied to the EAC contextual analysis presented in part III. The discoveries in part III are analyzed further in section 7.3 in order to fully answer the study's first research question, and to build a foundation to answer the third research question.

### 7.3 Key discoveries from Part III

Part III which presented the EAC situational context consists of two chapters, which are chapters five and six. In chapter five, the EAC context was established by outlining legislation and policies related to information security and e-government, and by presenting examples of e-Government initiatives in three countries of the EAC. Chapter six presents a survey of information security practices that relate to G2G transactions in MDAs in the EAC. Since this part focused specifically on the EAC, the matrices are presented in a way that recognizes or appreciates the positives in the EAC situation. Unlike the discoveries pointed out in sections 7.1, and 7.2, this section starts to build up to the original findings of the study that bring out the EAC context.

### 7.3.1 Discoveries from EAC e-government Initiatives

The situational analysis shows that there are some examples of successful e-government implementations and legislation that address information security. The addressing of the security requirements can be summarized as:

- Mentioned (M): The need for the security requirement is recognized and mentioned in documentation.
- Described (D): Methods of meeting the security requirement are described in documentation.
- Implemented (I): Security mechanisms to meet the security requirement have been practically implemented in an e-Government initiative. The use of the security mechanisms was established from interviewing staff of MDAs involved in e-Government projects and from documentation from project websites where available.

The addressing of information security for each country surveyed is presented in table 7-5.

Table 7-5 Information Security in Tanzanian, Ugandan and Rwandan e-Government Initiatives

| Requirement Area | Authentica-tion | | | Privacy | | | Authorization and Access Control | | | Data Integrity | | | Availability | | | Trust and Non Repudiation | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | R | T | U | R | T | U | R | T | U | R | T | U | R | T | U | R | T | U |
| Policies, Strategies &Standards | D | - | - | D | M | M | D | M | M | D | M | M | M | M | M | D | - | - |
| Legal Environment | - | - | - | M | M | M | M | M | D | - | - | D | - | - | - | - | - | D |
| e-Govt Implementa-tions | I | I | I | - | - | - | I | I | I | I | I | - | I | I | I | - | - | - |

Key: R=Rwanda T = Tanzania U= Uganda

For each information security requirement identified for G2G transactions, the discoveries can be summarized as follows:

**Authentication:** All the e-Government implementations studied in the three countries have implemented authentication mechanisms mainly in the form of passwords. One way to do this would be to use a unique identifier such as a national identification number, and include a section in existing laws that would recognize that national ID as the definitive authenticator of a citizen. There is a need as well for an authentication mechanism for an MDA in order for

them to be recognized when providing or using electronic services. This could be in the form of an electronic certificate issued by an authority recognized by law.

**Privacy:** The findings indicate that privacy is not considered in any of the e-Government implementations studied although it is mentioned or described in legislation, policies and strategies. The reason for this may be that most of the current e-Government initiatives are more on presenting information to citizens rather than obtaining information from citizens, and using that information to provide a service. Thus as the implementations become more complex, there is a need for MDAs to refer to existing legislation, policies and standards.

**Authorization and Access Control:** This requirement has been fairly well covered in the legal and regulatory environment as well as in the e-Government implementations. Further analysis is required to see whether the authorization and access control mechanisms addresses all kinds of e-Government transactions, that is, Government to Government, Government to Citizen and Government to Business as the context of a transaction affects access control and authorization mechanisms implemented.

**Availability:** This requirement was addressed in e-government implementations across the three countries.

**Data Integrity:** In Uganda, data integrity has been addressed in legislation. In the other two countries, there is a need to emulate the steps that Uganda has taken in improving on the legal and regulatory environment to address this requirement.

**Trust and Non-Repudiation:** This requirement has not been met in the e-Government implementations studied. The explanation for this may be similar to that of privacy, and there is therefore a need to address it more comprehensively in the legal and regulatory environment and to tie those requirements to any future e-Government implementations.

The discoveries in part III also resulted in answering the second research question of this study by identifying 3 factors that need to be taken into consideration in an information

security framework for G2G transactions in the EAC. These factors are resource constraints; legal and regulatory constraints and national culture constraints.

### 7.3.2 Discoveries from Survey of MDAs

At the individual MDA level, the relationship between the six security requirements of authentication, privacy, authorization and access control, integrity, availaibility and trust and non-repudation are as shown in Table 7-6.

Table 7-6: Relationship Between Areas surveyed and SecurityRequirements

| Area Surveyed | Security Requirement |
|---|---|
| Presence of information security policy | All |
| Mode of transaction with other MDAs | All |
| Concerns in electronic transactions | Authorisation and Access Control, Availability |
| Security mechanisms* | All |
| Binding agreements | Authorisation and Access Control |
| Common format of exchange | Authorisation and Access Control |
| Common terminology/ language | Authorisation and Access Control |
| Views of the need for standards | All |

* The security mechanisms that were listed in the survey responses were technical mechanisms including use of passwords, encryption, SSL and access control lists.

## 7.4 Information Security requirements for the EAC

The discoveries presented in sections 7.2 and 7.3 can now be synthesized to form an answer to the first research question which was *"What are the information security requirements for G2G transactions in the EAC context?"* The information security requirements and the mechanisms to address these requirements in the EAC context are presented in sections 7.4.1 and 7.4.2.

### 7.4.1 Information Security Requirements for G2G transactions in the EAC.

The information security requirements for G2G in the EAC are Authentication, Authorization and Access Control, Privacy, Integrity, availability, trust and non-repudiation. These are generic requirements, but the EAC context and the G2G transactional nature then influences the mechanisms that meet these requirements. These mechanisms may be tried and tested methods such as international standards, or methods and tools that are adapted to the EAC context. In the framework proposed in chapter eight, some mechanisms are proposed that can be adopted by MDAs in the EAC. Ultimately, the mechanism chosen must address the

matching security requirement and meet the security objective. These mechanisms have not been generalized because they will depend on the implementing agency's resources.

### 7.4.2 EAC issues to be addressed in an information security framework

The EAC factors that will influence the addressing of the information security requirements in a framework are resource constraints; legal and regulatory constraints and national culture constraints. Five perspectives are introduced in this section to address how these constraints can be overcome, or how information security for G2G transactions can be achieved despite these constraints. The five perspectives are:

i. Technical: The technical perspective involves looking at addressing information security through mechanisms implementable at a system level (hardware or software) to meet information security requirements. Examples of these include the use of technical standards such as XACML and SAML. From the EAC context, technical mechanisms need to be "tried and tested" and based on open freely available standards. However, for G2G transactions, a novel mechanism is developed as part of this study. This is the Governance and Attribute Based Access Control (GABAC) mechanism that is described in detail in chapter eight and is based on open standards. The use of open standards, and the technical mechanisms addressed the resource constraint factor in the EAC. The use of open freely available standards means that EAC MDAs can implement robust mechanisms without having to pay much for the software used. At the same time, freely available documentation on those standards will allow the limited ICT human resources to upgrade their skills or acquire new skills without incurring high costs.

ii. Operational: The operational perspective looks at addressing information security through mechanisms implemented within organizational units of an MDA to meet security requirements. Examples of these include the implementation of risk assessments and business continuity plans within an MDA. The operational perspective addressed the culture constraint factor by ensuring that initiatives are addressed not only at a national level but also at an organizational level. So even in the case where there is no central national coordination, each MDA involved in a G2G transaction, can follow standard operational guidelines to move towards addressing of information security requirements.

iii. Governance: The governance perspective looks at addressing information security through mechanisms at policy level within MDAs, and across national and regional government to meet security requirements. Examples of these include legislation and contractual agreements between MDAs. These mechanisms address the legal and regulatory constraints factor.

iv. Process: The process perspective looks at addressing information security through a series of steps that MDAs can follow to implement a framework that will meet the information security requirements such that the resource constraints, legal and regulatory constraints and national culture constraints recognized in the EAC do not hinder the addressing of information security.

v. Maturity: The maturity perspective looks at ensuring that the information security framework used allows for continual improvement in information security practices within MDAs and across national and regional governments.

## 7.5 Conclusion

In this chapter answers to the second research question, which where presented at the end of chapter five, have been combined with the discoveries from Parts II and III of the thesis to come up with a detailed answer to the first research question of this study, which is *"What are the information security requirements for G2G transactions in the EAC context?"*. This question has been anwered by stating security objectives, requirements and perspectives that need to be addressed for G2G transactions in the EAC context. Three of the perpectives that is the technical, operational, and governance perspectives are associated with the standards and both technical and non technical mechanisms for implementation.

This chapter leads to the design of a framework to meet information security requirements for G2G transactions in answer to the final research question. The framework design is presented in chapter eight and uses the foundation of the security objectives, requirements and perspectives that are discussed in this chapter. The framework also details the mechanisms that are required to address the information security requirements for G2G transactions in the EAC.

# Chapter 8 TOG Framework

## 8.1 Introduction

In chapter seven, the first research question was answered with the stating of information security objectives and requirements as being Confidentiality with the specific requirements of authentication, privacy and authorization and access control; Integrity with the specific requirement of data integrity; Availability; and Accountability with the specific requirement of trust and non-repudiation. Mechanisms to meet these requirements need to be cognisant of the EAC context. The second research question is *"What are the factors to be addressed in an information security framework for G2G transactions in the EAC?"* This question was answered at the end of chapter five. The three factors identified were resource constraints; legal and regulatory constraints and national culture constraints.

The rest of this chapter answers the third research question which is "How can a sustainable information security framework for G2G transactions be achieved in the EAC context?" This is the Design Phase of the Appreciative Inquiry process in which a framework, dubbed the Technical, Operational and Governance (TOG) framework to address information security for G2G transactions in the EAC is designed.

## 8.2 Design Process

In chapter seven, the discoveries from earlier chapters were used to come up with information security requirements for G2G transactions. In addition, mechanisms that may address some of these requirements are discovered. Furthermore, five perspectives to capture the EAC context are presented at the end of the chapter seven.

In order to design an information security requirements framework for G2G transactions in the EAC, it is now necessary to come up with a design that meets the information security requirements. The discoveries on mechanisms and perspectives that are presented in chapter seven are used to develop design artifacts that will form elements of the framework. Design artifacts may be constructs, models, methods or instantiations (Hevner, March, Park, & Ram, 2004). In addition to developing design artifacts, the design processes bases on a proposal by Carlsson (2006) to include an object design, realization design and a process design in an

information systems research initiative in order to come up with a successful problem solution. An object design is the intervention required to solve the problem (in the case of this study, the design of a sustainable framework for G2G transactions in the EAC). The realization design is guidance on how to implement the object design, and the process design is the methods and techniques to implement the object design.

The five perspectives discovered in chapter seven form the design artifacts which are represented in the object design as models. These are a Technical Model, an Operational Model, a Governance Model, a Process Model and a Maturity Model. The first three models include components or mechanisms that address the meeting of information security requirements stated in chapter seven, in response to the first research question. The component or mechanisms also address the factors to be considered in the EAC stated in chapter five in response to the second research question. For each of the models, guidelines on implementation of the model are developed and useful resources to be used by the implementing MDAs are included. This forms the realizable design. The Process Model details a process cycle through which MDAs can implement the Technical, Operational and Governance Model while the Maturity Model outlines how the MDAs can gradually improve on their ability to meet the Information Security requirements over time. The Process Model and the Maturity Model represent the process design and are cognizant of the three factors that need to be considered in the EAC context which are resource constraints, legal and regulatory constraints and national culture constraints.

The design process is shown in Figure 8-1 and the resultant framework is discussed, starting with an overview in section 8.3 followed by a detailed description of each of the models in sections 8.4 to 8.7.

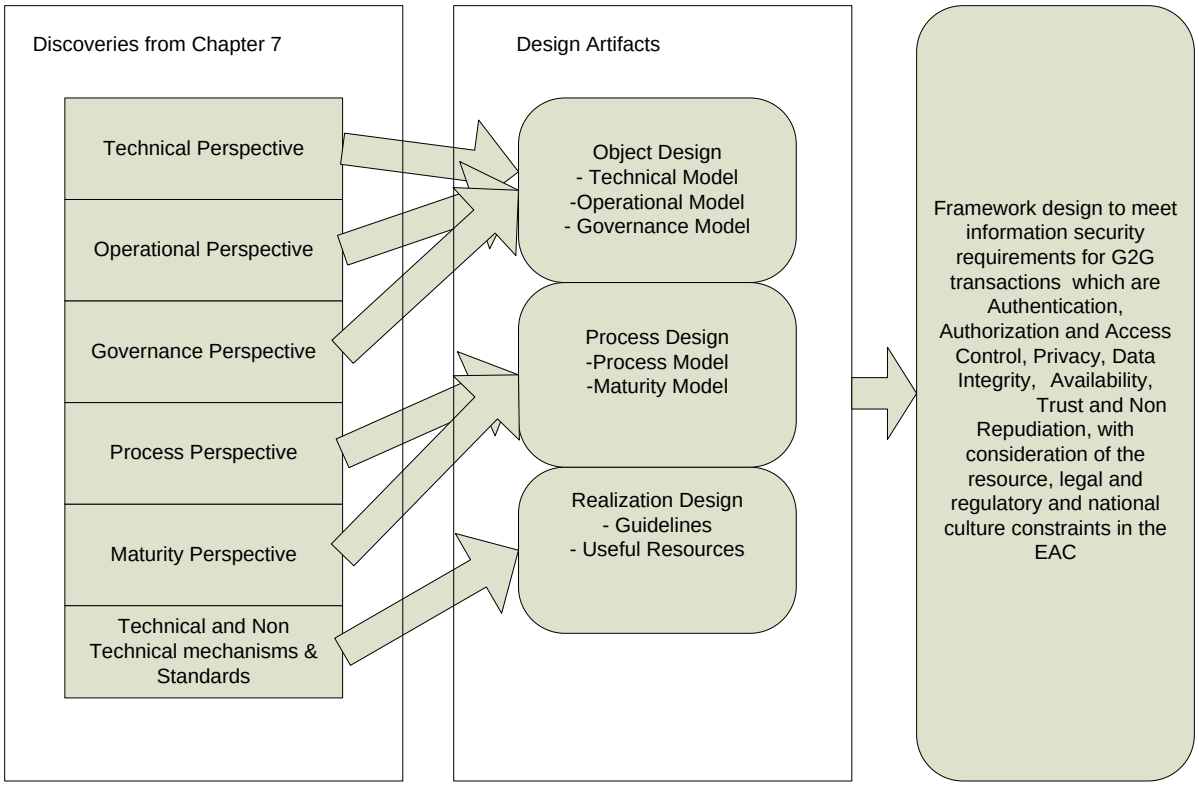



Figure 8-1 Design Process there is some double text in the middle process

## 8.3 Overview of the TOG Framework

The TOG framework is a unified framework, which consists of five models which are based on the perspectives discussed in chapter seven. These are:

i. Technical Model: The technical model presents technical mechanisms that work together to address the information security requirements for G2G transactions. As part of the technical model, a mechanism for addressing access control, the GABAC mechanism is presented. This mechanism was developed after the discovery that access control mechanisms that are discussed in literature in chapter two, can be improved upon to come up with a mechanism more suitable to meet the authorization and access control security requirement for G2G transactions. The other mechanisms presented in the technical model are not novel mechanisms, but are "tried and tested" as presented in the literature discussed in part II of this thesis. These include Service Oriented Architectures, Ontologies and PKI. In addition, mechanisms that were discovered as already in use in the survey of EAC MDAs are also included in the model. The purpose of these mechanisms is that they work together to produce part of the novel framework that

addresses the research questions in this study. For each mechanism presented, the purpose is given and useful resources that help MDAs to implement the technical model are given.

ii. Operational Model: The operational model presents operational mechanisms that need to be implemented in individual MDAs to address information security requirements. The Operational Model makes no assumptions about the technical capabilities in the MDA, or even that the transactions that are taking place in the G2G transaction are entirely electronic transactions.

iii. Governance Model: The governance model presents governance mechanisms that need to be implemented at a policy level within MDAs, amongst MDAs and across governments. The governance mechanisms include organizational policies, national and regional legislation.

iv. Process model: The process model presents the way that the TOG framework can be implemented within an MDA and amongst MDAs who plan to undertake G2G transactions. The TOG process model captures the EAC context whereby resources to carry out whole security implementations at one go may not be available and where there may be lack of coordination across governments with regards to e-government implementations.

v. Maturity model: The maturity model provides a mechanism for MDAs and governments to continually measure progress with regards to meeting information security requirements for G2G transactions.

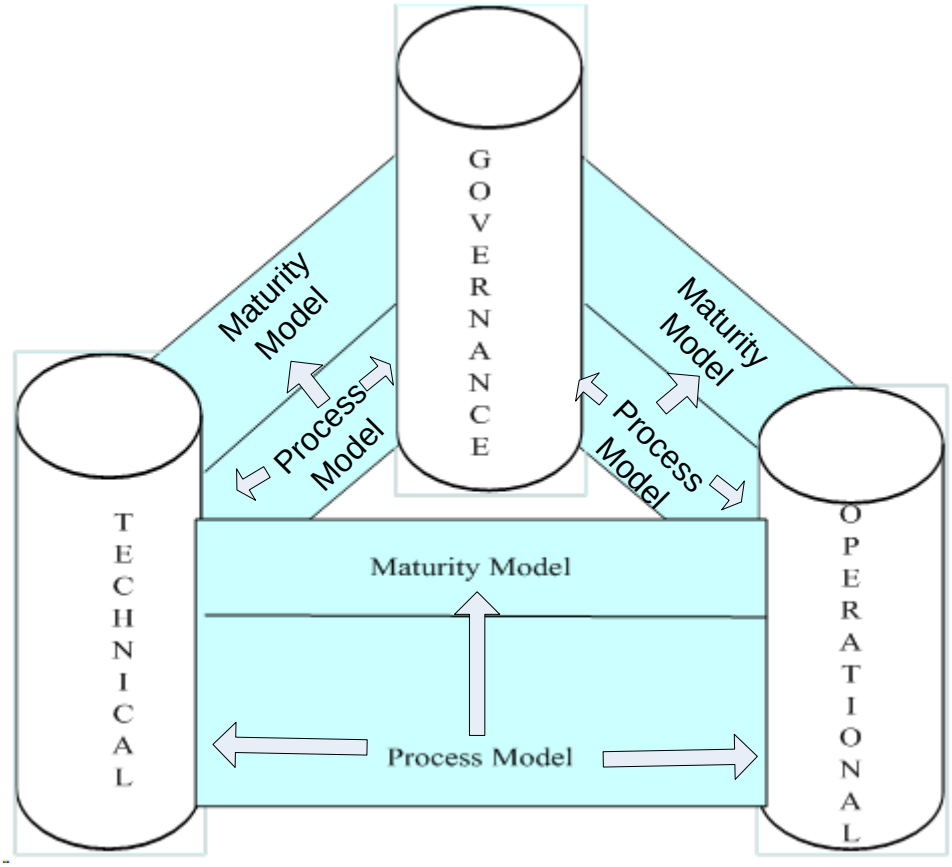



Figure 8-2 TOG Framework

Figure 8-2 depicts the five TOG models. Three of the models, which are the technical, operational and governance models, appear as pillars and the remaining two models, which are the process and maturity models, are mapping mechanisms across those pillars. This means that in each MDA, the technical, operational and governance pillars can be applied independently to meet information security requirements for G2G transactions, as and when resources are available, or when legislation is put in place. The process and maturity models help the MDAs to continually move towards a holistic information security framework, by mapping mechanisms in the technical, operational and governance models onto each other. The TOG framework thus addresses the information security requirements in a manner that recognises that the contextual issues (resources; lack of legislation or the culture) in the EAC may not permit a structured approach to implementing of an information security framework.

The actors in a G2G transaction are individual MDAs who have to comply with national and regional legislation set by the Government and with organisational policies that are set by the MDA's internal governance structures (executive management). The roles of each of the major actors determine who implements the models of the TOG Framework as shown in Table 8-1.

Table 8-1 TOG implementation by main actors in a G2G transaction

| Actor | Role | TOG Model implemented |
|---|---|---|
| Government | Establish legislation and policies that address the information security objectives and requirements; Ratify or adopt regional legislation that addresses the information security requirements. | Governance |
| MDA - Executive | Establish policies within the MDA to address the information security requirements | Governance |
| MDA - Operational | Put in place operational plans and mechanisms to address the information security requirements | Operational |
| MDA - Technical | Implement technical mechanisms to meet information security requirements | Technical |

The process model provides steps to implement the governance, operational and technical models, while the maturity model allows governments and MDAs to track how their information security practices are growing to fully meet the information security objectives.

The models of TOG are not interdependent and can be developed in parallel. This is in keeping with the previously stated discovery with regards to culture of lack of central co-ordination of e-Government initiatives in the EAC, and where governance solutions and technical solutions are not developed and applied at the same pace. The common factor is that all the models are implemented with the same security objectives and requirements in mind. The TOG process model serves as the mapping mechanism from one model to another, and the maturity model provides guidance to ensure that MDAs and governments are continually improving towards a holistic information security framework that addresses the EAC context.

The details of each of the models are presented in sections 8.4 to 8.8 below.

## 8.4 TOG Technical Model

### 8.4.1 Description of the Technical Model

The technical model of the TOG framework outlines technical mechanisms that can be used to meet the information security requirements. The technical model is motivated by the following factors:

- As established in the survey conducted in the EAC as well as the description of e-government initiatives, there are electronic G2G transactions taking place. For these technical mechanisms must be put in place.
- Any MDA that hopes to start transacting electronically should be aware of technical mechanisms available that can be applied with minimal resources to address security requirements.
- Where proven solutions exist, and where those solutions do not require major resources, the EAC should use these solutions and adapt them to their context.

Any proven solution that can address the security requirements can be included in the technical model. For now, four mechanisms that can address the security objectives are described in more detail. These can be implemented by technical staff on their own or in collaboration with operational staff. The security mechanisms described are chosen on the basis of their suitability for G2G transactions as established in the literature review done in part II. Some of the mechanisms are mentioned in existing national level policies. The four mechanisms are Governance and Attribute Based Access Control; G2G Ontologies, SOA and PKI. For each mechanism the purpose of inclusion in the framework is outlined, together with a list of useful resources that the implementer may refer to. The mechanisms may overlap in addressing the information security requirements. Of the four mechanisms proposed, three of these are based on known mechanisms with are tried and tested in Government and indeed in some of the EAC governments as established in chapter five of this thesis. This is in keeping with the objective of the third research question, which is to have a sustainable framework. The fourth mechanism, which is the GABAC, is proposed because as discussed in chapter two, current access control models do not fit quite well with G2G transactions.

The model can be extended to include any mechanisms that the actors in a G2G transaction need to meet the security requirements. The TOG technical model is as illustrated in the Figure 8-3 below.

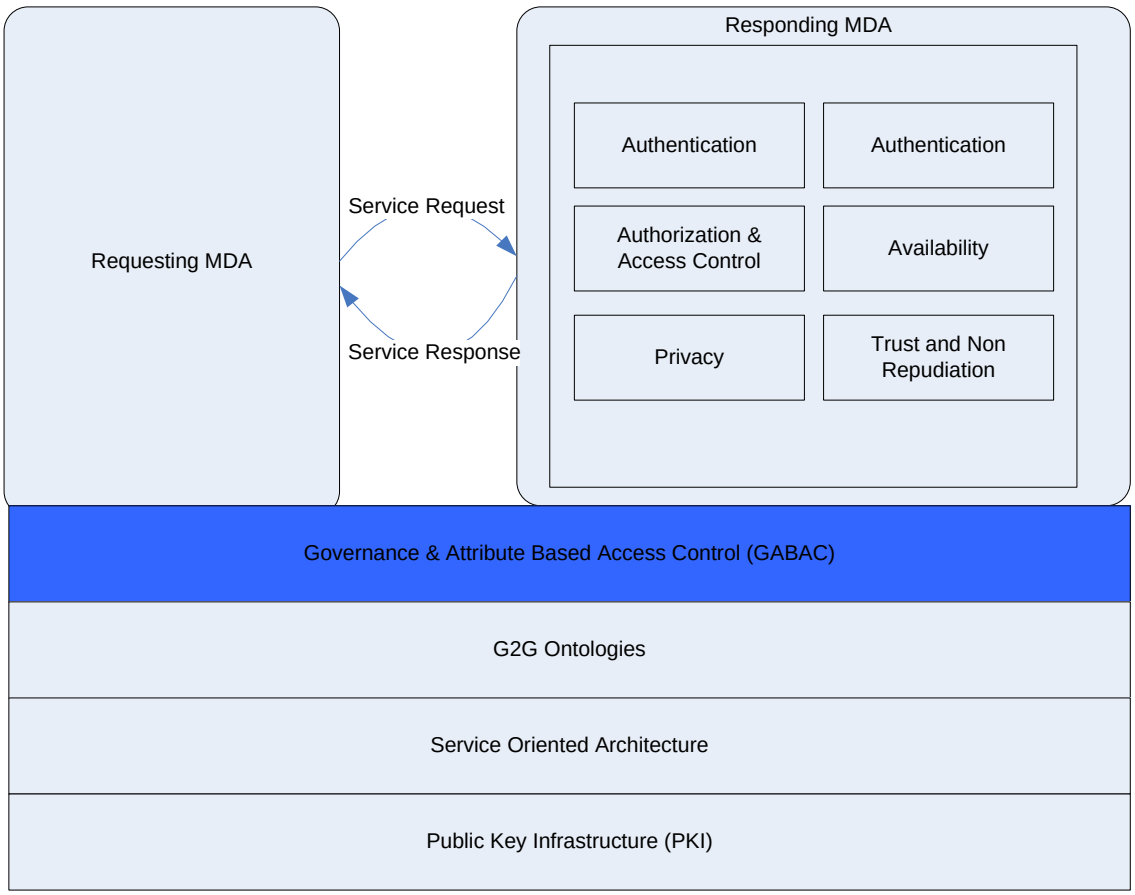



Figure 8-3 Technical Model of TOG Framework

The base of figure 8-3 shows the mechanisms to be used to meet the Information Security: requirements. GABAC is a novel mechanism proposed in this study as being particularly suited to G2G transactions. The other three mechanisms are generic mechanisms. The security model components are described in more details in the sections below, together with implementation guidelines for the technical departments of MDAs.

### 8.4.2 Technical Model Components: Governance & Attribute Based Access Control (GABAC).

GABAC is an access control model that is based on two open standards which are XACML and SAML. GABAC uses an underlying legal repository and ontology mapping service as

shown in figure 8-4 to satisfy the information security requirements for G2G transactions. The objective of the GABAC model is to meet the security requirements of authentication, authorization and access control, privacy.

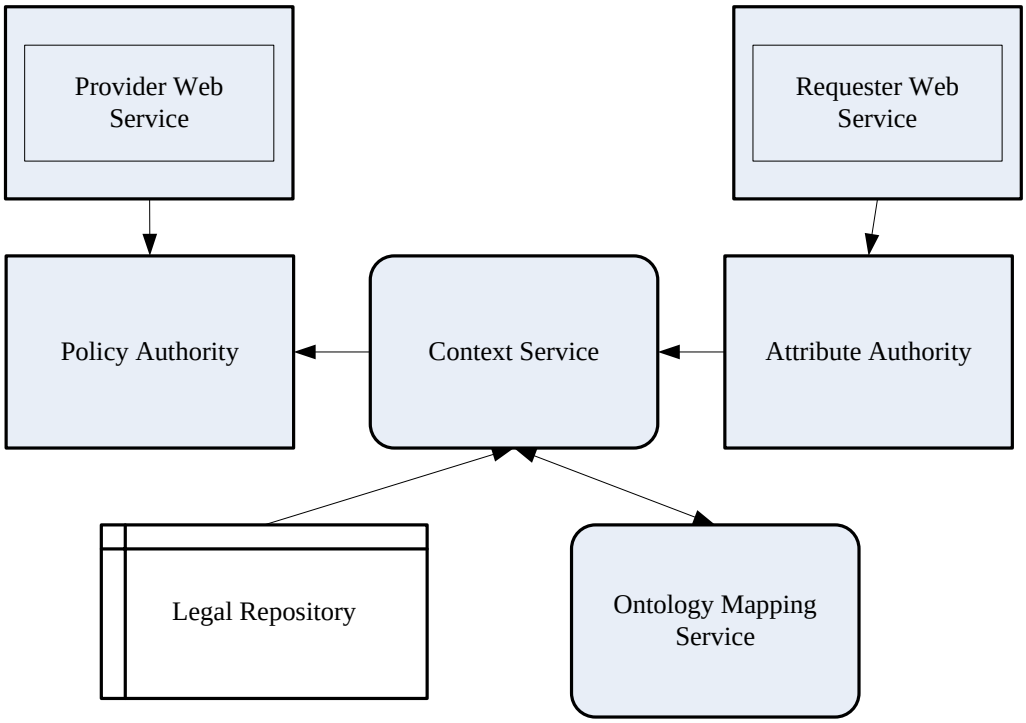



Figure 8-4 Overview of GABAC

The access control model proposed in this framework is a combination of the Attribute Based Access Control and the Governance Based Access Control methods described in chapter three of this thesis. The access control model is implemented using XACML and SAML which are open standards. Ontology is used for enhancing semantic interoperability and ensuring correct access control decisions across agencies. A legal repository (Ross, 2007) is used to represent legal requirements. The components of the GABAC model are as shown in Table 8-2.

Table 8-2 GABAC Components

| GABAC Component | Description |
|---|---|
| **Attribute Authority** | The attribute authority issues SAML assertions to the MDA that is requesting a service in a G2G transaction. The attribute assertions correspond to the subject, resource and environmental attributes of the requester. If there is a legal requirement on the requester's side that has to be complied with, this requirement is passed in a SAML condition statement. |
| **Policy Authority** | The policy authority contains the XACML Policy Decision Point (PDP) and Policy enforcement points that evaluate the requester's attributes against the providers XACML policy. In order to evaluate the compliance with legal requirements XACML is extended to include a function that accepts environment attributes and compares against relevant laws and regulations within the legal repository. This operation will be stated as a XACML obligation in the policy of the MDA that provides the service in a G2G transaction. If there is no legal requirement for a particular transaction, then the request is granted provided the other requirements of the policy are met. |
| **Ontological mapping service** | The ontological mapping services checks that the semantics of the requester's attributes match with those in the provider's policy. |
| **Legal repository** | The legal repository contains laws and regulations that apply to different transactions. The legal repository contains the conditions in which a transaction is considered legal or illegal. The legal repository is a database with several indexes to allow multiple matching by the Context Service. |
| **Context Service** | The role of the context service is to combine the results from the ontological mapping mechanism and the legal repository into an environmental attribute that is then passed to the attribute authority for authorisation and access control decisions to be made. |

The purpose of the GABAC is that it is a robust access control mechanism that addresses the authorisation, access control and privacy security requirements in G2G transactions. As discussed in section 2.2.2 existing mechanisms do not suffice. The GABAC mechanism is based on open standards i.e. XACML and SAML and takes into consideration prevailing legislation which is one of the contextual issues identified for the EAC. SAML assertions are used for authentication while XACML is used to formulate policies and to provide a rule combining algorithm and delegation in policy decisions.

This is useful in G2G transactions in cases where a service may require information that crosses legislative domains. One agency can delegate part of the authorisation decisions based on the policies and laws in the participating agencies. XACML may be used together with SAML Authentication, Authorization Decision and Attribute assertions being issued by

the Certificate Authority which is part of the operational guidelines presented in section 8.3.2.

A high level view of how GABAC works is presented in the UML Communication diagram illustrated in Figure 8-5 below.

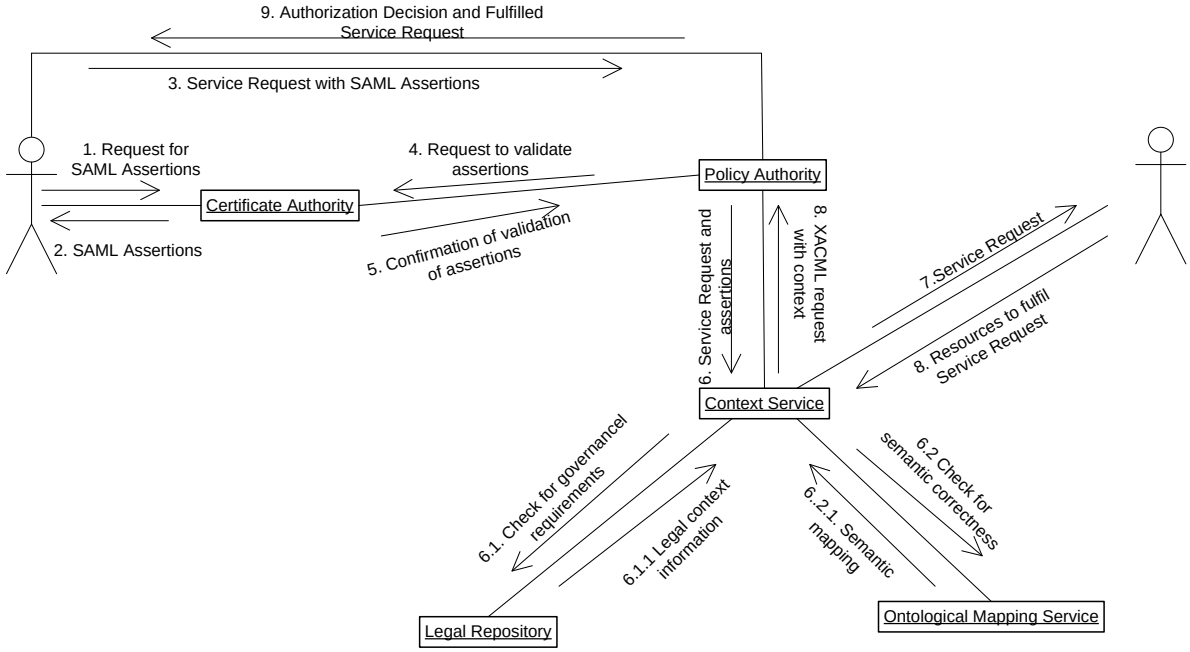



Figure 8-5 How GABACworks

Within the Policy Authority are XACML components that play specific roles. These components are:

- Policy Enforcement Point (PEP): Receives the request from the requesting MDA and sends the request to the context handler.
- Policy Decision Point (PDP): Receives the XACML request with contextual information from the context handler and returns the authorization decision.
- Policy Information Point (PIP): Receives the SAML attributes and passes them onto the Context handler.
- Policy Enforcement Point (PEP): Fulfills the obligation (Service Request) based on the authorization decision.

The context Service in GABAC is based on the XACML Context handler and has the role of

- Mapping the SAML Assertions onto XACML attributes using the SAML 2.0 profile of XACML v2.0 (OASIS, 2005).
- Mapping attributes from the legal repository onto XACML attributes using the XML Data Type Definition (DTD) for the legal repository.
- Checking that the resultant XACML attributes are semantically consistent using the ontological mapping service.

The legal repository represents governance level documents that affect information security, and are stored in XML format. The legal repository contains a complete range of laws, regulations, policies, standards, guidelines and directives to which the responding MDA is subject. There must be metadata tables that determine the matching of laws to specific information security requirements.

If, for example, there is any G2G transaction where the location of the requesting attribute is from outside of the country where the responding MDA is, and the responding MDA has legislation that restricts the countries to which a country can provide a service, then for the authorization and access control requirement, the legal repository has to have a list of restricted countries. This information is passed on to the context service so that the appropriate decision is made.

The ontological mapping service keeps track of those attributes that may have different meanings in the requesting and responding MDAs to ensure that access control decision are correctly made.

### 8.4.3 Technical Model Components: G2G Ontologies

The use of standards such as XACML and SAML as incorporated in the GABAC model addresses syntactic interoperability. Ontologies are a useful tool for achieving semantic interoperability. Ontology is a formal representation of concepts in a particular domain. The ontologies developed can be used to ensure correct access control decisions in G2G

transactions. The ontologies will be based on the common terminology in the operational model.

The purpose of a G2G ontology in the TOG technical model is to enable the definition of attributes that will be used in access control and authorization decisions. In a G2G transaction where there may be no human intervention, a wrong authorization may be made because an assertion made from the requesting machine may be interpreted differently from the consumer's policies. By using a common ontology, semantic interoperability is achieved.

### 8.4.4 Technical Model Components: Service Oriented Architecture

A Service Oriented Architecture is defined by World Wide Web Consortium (W3C) as a set of components which can be invoked, and whose interface descriptions can be published and discovered.W3C further define a Web Service as a software system designed to support interoperable machine-to-machine interaction over a network (W3C, 2004). It has an interface described in a format that machines can process. Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with XML serialization in conjunction with other Web-related standards. Web Services are used to implement service-oriented architectures.

In a G2G transaction, interactions are typically machine to machine interaction. The purpose of a SOA in the Technical Model is to achieve the availability security objective, when implemented with web services. This is because web services are technically neutral, so a web service produced by an MDA can be utilized by another MDA regardless of differences in technical platforms in the two MDAs.

### 8.4.5 Technical Model Components: PKI

PKI comprises of components that allow parties to communicate securely over public networks through the use of public key cryptography. A certificate authority issues and verifies certificates that are given to the parties in a transaction. For G2G transactions, a trusted third party could be agreed upon to act as a certificate authority for MDAs.

The use of PKI in the TOG Technical Model would allow governments to use the internet as a means of communications, thus avoiding expensive point to point secure links between MDAs.

### 8.4.6 Implementation Guidelines for the Technical Model

This section outlines guidelines that are applicable in the Technical Model that will lead to the addressing of each of the information security objectives of Confidentiality, Integrity, Accountability and Availability. The mapping of the mechanisms proposed in the Technical Model against the security requirements in shown in Table 8-3.

Table 8-3 Mapping of Requirements Against Mechanisms in the Technical Model

| **Security Objective** | **Security Requirement** | SOA, Web Services | GABAC mechanism | Ontology | PKI |
|---|---|---|---|---|---|
| Confidentiality | Authentication | | x | | x |
| | Authorization and Access Control | | x | x | |
| | Privacy | | x | | |
| Integrity | Data Integrity | x | | | x |
| Availability | Availability | x | | | |
| Accountability | Trust & Non Repudiation | x | | | x |

A government agency can choose to use other security mechanisms and map them using the same matrix to check that all security requirements are being addressed.

Two guidelines (represented with the codes T1 and T2) for implementation of the technical model in MDAs are as follows:

**T1:** The mechanisms used to address the information security requirements should, where possible, be based on free and openly available standards.

**T2:** The mechanisms used to address the information security requirements should allow for technical and semantic interoperability across MDAs.

### 8.4.7 Useful Resources for Implementation of the Technical Model

In order to have a sustainable implementation, MDAs can keep up to date advances in access control related standards or research that would be useful for G2G transactions. The list is not exhaustive but gives a direction as to where a starting point or seed for those standards and mechanisms are referred to in this model. These are shown in the Table 8-4.

Table 8-4 Useful Resources for implementing the Technical Model

| Resource | Source | Purpose |
|---|---|---|
| Organization for the Advancement of Structured Information Standards – OASIS | www.oasis.org | Source of information on updates to the XACML and SAML standards that form part of the GABAC. |
| Centre for governance institute | www.cgi.org | Source on white papers on Governance Based Access Control |
| Security Ontology developed by the United States Centre for High Assurance Computer Systems | http://www.nrl.navy.mil/chacs/publications.php | Source of a security ontology that can be used as a base ontology for G2G transactions to enhance semantic interoperability outside of the EAC region |
| Protégé Ontology development tool from Carnegie Mellon University | www.protege.stanford.edu | Free tool for development of ontologies |
| World Wide Web Consortium | www.w3c.org | Source of updates on standards related to web services and web service security |
| Rwanda Technical guidelines and standards for e-Government | Report published by Rwanda Information Technology Authority (Now part of Rwanda Development Board) in 2006 | EAC perspective on PKI implementation |
| ISO/IEC TR14516 | http://webstore.iec.ch/preview/info_isoiec14516%7Bed1.0%7Den.pdf | Source of information on updates to IT security mechanisms and techniques from ISO and IEC |

## 8.5 Operational Model

### 8.5.1 Description of the Operational Model

The Operational Model of the TOG framework outlines organizational plans and practices that an individual MDA can use to address the information security requirements.

The operational model is motivated by the following factors:

- It has been established in part III those MDAs in the EAC sometimes set their own agendas in terms of ICT in the absence of national guidelines. The TOG framework is cognizant of this practice, however it is necessary for MDAs to map their initiatives onto legislation or policies as and when they come into effect. This is through matching

organizational plans to the relevant governance components that address a specific information security requirement.

- Technical mechanisms for addressing information security should be backed by organizational plans and practices to allow for holistic addressing of information security.

### 8.5.2 Components of the Operational Model

The components of the operational model include organizational plans and programs, certificate authority agreements and common terminology for G2G transactions. The operational model is implemented by operational departments in individual MDAs and some components are implemented across MDAs as shown in Figure 8-6.

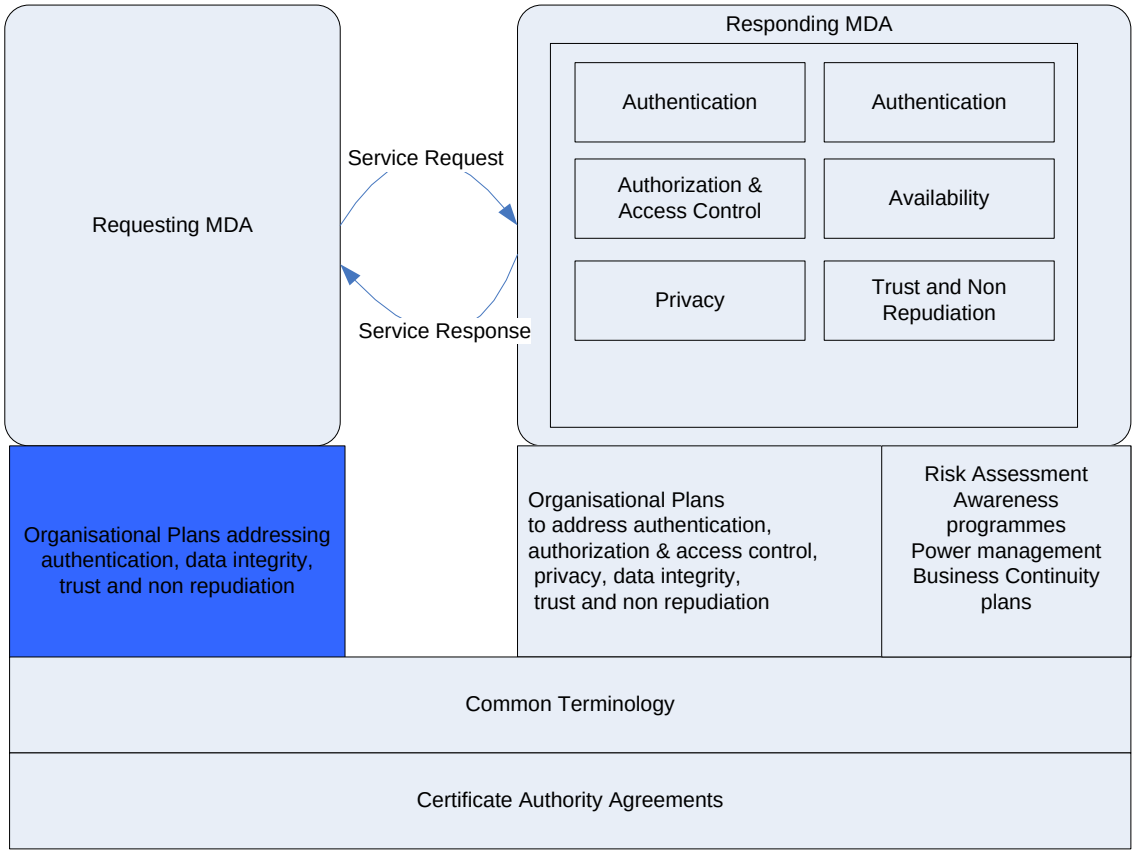



Figure 8-6 TOG Operational Model

The components of the operational model are organisational structures, plans and procedures which address the information security requirements. The Operational Model is implemented by operational or business units within government or within an MDA.

### 8.5.3 Implementation Guidelines for the Operational Model

This section outlines guidelines that are applicable in the operational model that will lead to the addressing of each of the information security objectives of Confidentiality, Integrity, Accountability and Availability. The mapping of the mechanisms proposed in the operational model against the security requirements are shown in Table 8-5.

Table 8-5 Mapping of Requirements Against Mechanisms in the Operational Model

| **Security Objective** | **Security Requirement** | Risk Assessment | Certificate Authority | Power management and Backup | Interoperability and metadata | Awareness |
|---|---|---|---|---|---|---|
| Confidentiality | Authentication | | x | | | |
| | Authorization and Access Control | x | x | | | x |
| | Privacy | x | | | | x |
| Integrity | Data Integrity | x | x | | | |
| Availability | | x | | x | | |
| Accountability | Trust & Non Repudiation | x | | | x | |

A government agency can choose to use other security mechanisms and map them using the same matrix to check that all security requirements are being addressed.

**a) Operational guidelines for achieving Confidentiality:**

The operational guidelines for addressing the confidentiality security objective are summarized in Table 8-6.

Table 8-6 Operational Guidelines to address the Confidentiality Security Objective

| **Security Requirement** | **Guideline Code** | **Guideline** |
|---|---|---|
| Authentication | O1 | Incorporate national identifier in systems design |
| | O2 | Obtain certification from Certificate Authority |
| | O3 | Conduct awareness training for potential users of services on required authentication mechanisms |
| Authorization and Access Control | O4 | Implement organisational security policies. |
| | O5 | Conduct Risk Assessment using a proven methodology |
| | O6 | Create taxonomy of terms used in organisational processes. |
| | O7 | Define required security attributes that take into consideration legal requirements and the use of standard terms. |
| Privacy | O8 | Establish privacy mechanisms<br>Establish encryption mechanisms. |

**b) Operational guidelines for achieving Integrity**

O9: Establish methods of validating data integrity.

O10: Adopt encryption standards.

**c) Operational guidelines for achieving Availability**

O11: Establish regulations for power management.

O12: Implement business continuity and disaster recovery plans.

**d) Operational guidelines for achieving Accountability**

O13: Establish auditable fields and transactions.

O14: Register with Certificate Authority and Obtain Certificate.

015: Setup incident reporting mechanism.

016: Establish regulations for use of digital signatures.

### 8.5.4 Useful Resources for implementation of the Operational Model

MDAs can assess updates on some of the mechanisms proposed for use in implementing the operational model through the useful resources shown in Table 8-7.

Table 8-7 Useful Resources for implementing the Operational Model

| Resource | URL/Source | Purpose |
|---|---|---|
| Information Systems Audit and Control Association | www.isaca.org | Source of information on standards and white papers related to audit and risk assessment of information systems |
| CERT Program, Software Engineering Institute – Carnegie-Mellon University | www.cert.org/octave | Source of information on the OCTAVE Risk assessment methodology |

## 8.6 The Governance Model

### 8.6.1 Description of the Governance Model

The Governance model of the TOG framework outlines policy level mechanisms for addressing the information security requirements for G2G transactions.

The Governance model is motivated by the following factors:

- A G2G transaction typically takes place across more than one organisation. This means that multiple organizational and security domains may be involved. Thus the handling of security must be at a level higher than just an individual organizational level.
- It has been established in Part II of this thesis that there exists some legislation in the EAC that relates to information security for G2G transactions. This legislation must be complied with in any G2G transactions. The framework must therefore take into consideration existing legislation, and at the same be flexible enough to anticipate new laws or changes to existing legislation.
- In many areas, implementation of international frameworks without adaptation has proved not to work, as developing countries need context-sensitive approaches both for e-Government and information security (Dada, 2006). This is because the countries are resource poor i.e. weak public administrations, poor institutional capacity and low financial resources.
- Governance is one of the identified pitfalls in e-Government if not properly addressed (OASIS, 2010a). There has to be top level awareness and ownership within government of any e-government related initiative.

### 8.6.2 Components of the Governance model

The components of the governance model are International standards, National and regional laws and regulations, and Organisational policies. Each of these components will have elements that apply to some or all of the information security requirements. The Governance model is implemented by top level management in government. Figure 8-7 shows the model.

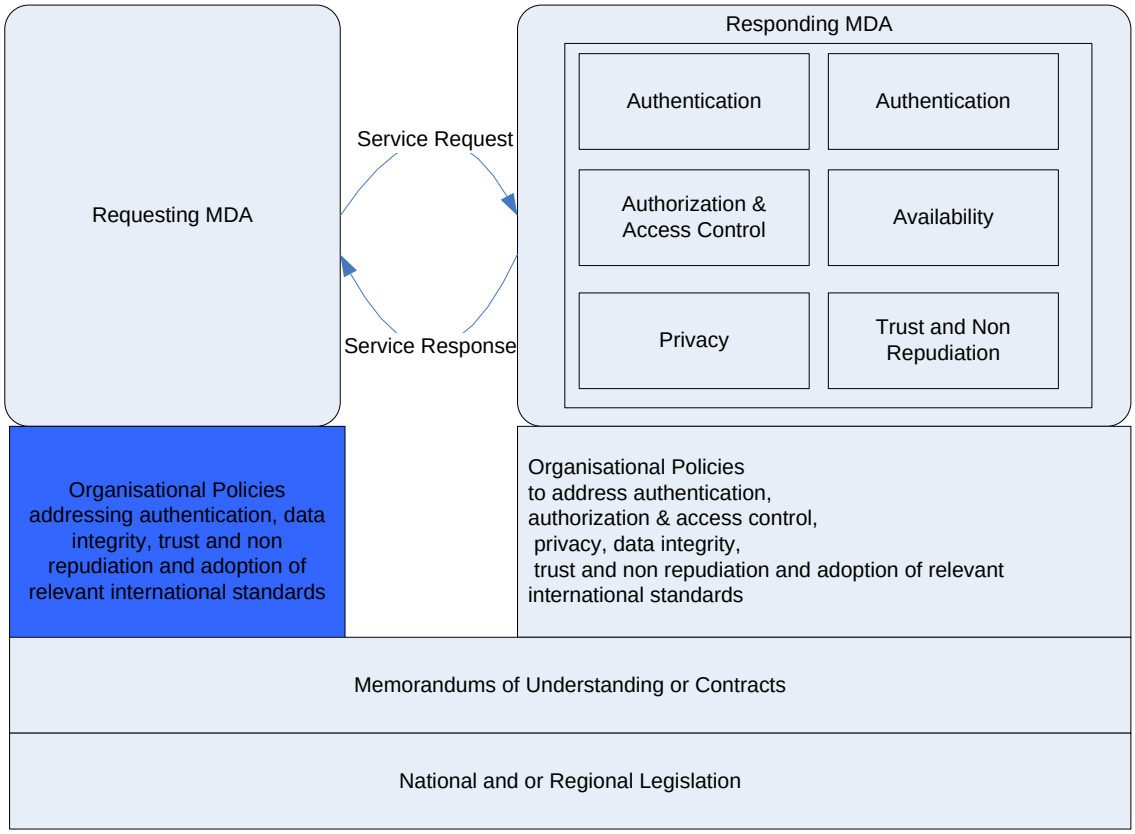



Figure 8-7 TOG Governance Model

### 8.6.3 Implementation Guidelines for the Governance Model

This section outlines guidelines that are applicable in the governance model that will lead to the addressing of each of the information security objectives of Confidentiality, Integrity, Accountability and Availability. A mapping of the mechanisms proposed in the governance model against the security requirements is shown in Table 8-8.

Table 8-8 Mapping of Requirements Against Mechanisms in the Governance Model

| **Security Objective** | **Security Requirement** | International Standards | Legislation | Organisa-tional policies | Contracts/ MoUs |
|---|---|---|---|---|---|
| Confidentiality | Authentication | x | x | | |
| | Authorization and Access Control | x | x | | |
| | Privacy | x | x | | |
| Integrity | Data Integrity | x | x | | |
| Availability | | | | x | |
| Accountability | Trust & Non Repudiation | x | x | | x |

A government agency can choose to use other security mechanisms and map them using the same matrix to check that all security requirements are being addressed.

**a) Governance Guidelines for achieving confidentiality**

For confidentiality the following three security requirements should be addressed namely authentication, authorisation and access control and privacy. The guidelines for each security requirement for confidentiality are stated in Table 8-9.

Table 8-9 TOG – Governance guidelines for achieving the confidentiality objective

| Security Requirement | Guideline Code | Guideline |
|---|---|---|
| Authentication | G1 | Establish legislation and policies that identify the primary mechanism for identification of a citizen; business or government agency:<br>• For citizens a unique national Identity number (ID number) may be used.<br>• For Businesses a Tax Identification number (TIN) may be used.<br>• For Government agencies an electronic identifier / certificate should be issued by a Certificate Authority. |
| | G2 | A certificate authority should be established by law with the role of issuing identification certificates to government agencies for electronic transactions. |
| | G3 | Identify related legislation that exists at international and regional level (EAC). |
| Authorization and Access Control | G4 | Establish legislation and policies to classify information assets. |
| | G5 | Establish policies and regulations on minimum requirements for access control decisions. |
| | G6 | Identify related existing laws and regulations at international and regional level (EAC). |
| | G7 | Establish legislation that enables prosecution of fraud carried out through electronic means and other kinds of cyber-crime. |
| Privacy | G8 | Identify articles that address privacy in national constitutions |
| | G9 | Establish laws and regulations on Data Privacy. |
| | G10 | Identify related existing laws and regulations that exist at international and regional level (EAC). |

**b) Governance guidelines for achieving Integrity**

The guidelines for achieving the integrity objective and data integrity security requirements at a governance level are:

G11: Establish legislation and policies for Computer Misuse.

G12: Establish legislation and policies to govern computer communications.

G13: Identify related existing laws and regulations that exist at international and regional level (EAC).

G14: Establish encryption policies.

**c) Governance guidelines for achieving Availability**

The governance guidelines for achieving the availability objective and security requirements are:

G15: Establish regulations for power and back up.

G16: Establish regulations on use of standards to achieve interoperability.

G17: Identify related existing laws and regulations that exist at international and regional level (EAC).

**d) Governance guidelines for achieving Accountability**

Trust and non-repudiation are the security requirements to be addressed in order to achieve the accountability objective. The governance guidelines for addressing accountability are:

G18: Establish a Certificate Authority as the trusted third party to authenticate government agencies and departments for electronic transactions.

G19: Establish standards for drafting contracts between government to government transactions.

G20: Establish Laws and Regulations for acceptability of electronic evidence.

G21: Establish regulations for publishing of breaches in electronic transactions (Incident reporting) to enable governments to identify and fix gaps in information security.

G22: Identify related existing laws and regulations that exist at international and regional level (EAC).

### 8.6.4 Useful Resources for Implementing the Governance Model

In implementation of the governance model the resources shown in Table 8-10 may be found useful in obtaining updates on mechanisms such as national legislation and international standards.

Table 8-10 Useful resources for implementing the Governance Model

| Resource | URL/Source | Purpose |
|---|---|---|
| ISO/ IEC 27000 series of security standards. | www.iso.org | Source of security standards issued by ISO and IEC |
| Legislation of the United Republic of Tanzania, Rwanda, Uganda | www.parliament.go.tz,<br>www.amategeko.net<br>www.parliament.go.ug | Sources of national legislation in the EAC |
| National Institute of Standards and Technology | www.nist.org | Information security standards and guidelines issued by the United States Government |

## 8.7 Process Model

### 8.7.1 Description of the Process Model

The three models proposed above represent distinct actors with distinct roles within each MDA. In order for the MDA to move towards holistic addressing of information security requirements, there has to be a mapping from one model to the other. The TOG process model that is proposed in this section allows an MDA to recognize what technical, operational or governance mechanisms are in place and use them appropriately in a G2G transaction.

The process model is motivated by the need to address the three contextual factors discovered in the EAC which are:

- Resource constraints: These include financial constraints due to limited national (public sector) budgets allocated to ICT/ e-Government initiatives and inadequate ICT skills;
- Legal or regulatory constraints: These include lack of sufficient legislation and national policy frameworks related to information security in e-Government; and
- National Culture constraints: These include uncoordinated or unstructured national government initiatives related to ICT or e-Government.

The addressing of these factors is done by designing the process model such that it uses a ‘plug and play’ approach, that each MDA applies the mechanisms that it can in a particular model, and maps those onto the corresponding models. Where resource or cultural constraints exist, the implementation still continues, and a maturity model is proposed to

ensure continual improvement in the MDA's efforts to comprehensively meet information security requirements.

### 8.7.2 Components of the Process Model

The process model is comprised of two layers which are formally presented using the ebXML Business Process Specification Schema Technical Specification v2.0.4, which was adopted as a standard in 2006 by OASIS (OASIS, 2006).

ebXML Business Process Specification Schema (BPSS) was developed specifically for e-business, but its basic concepts lend themselves quite well to G2G transactions. The TOG process model is applicable at two layers. The first layer is a G2G transaction between two MDAs, and the second layer represents any two actors within an MDA, or country who are putting in place mechanisms to meet the information security requirements. The TOG Process is shown using ebXML notation in figures 8-8 and 8-9 below.

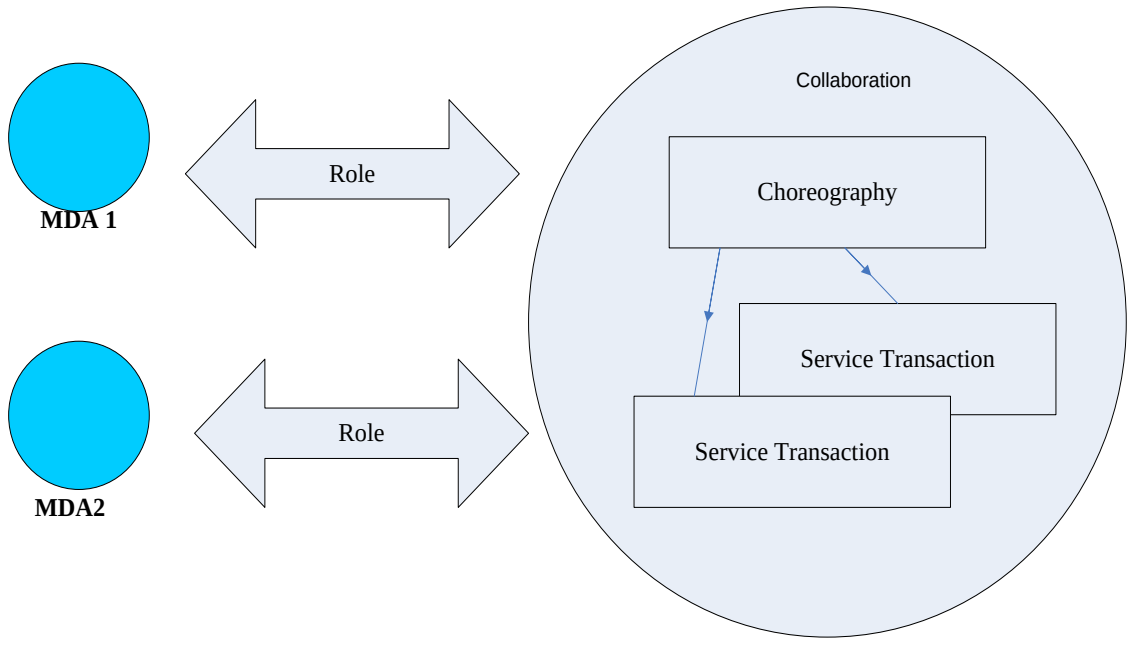



Figure 8-8 TOG Process Model - Layer 1

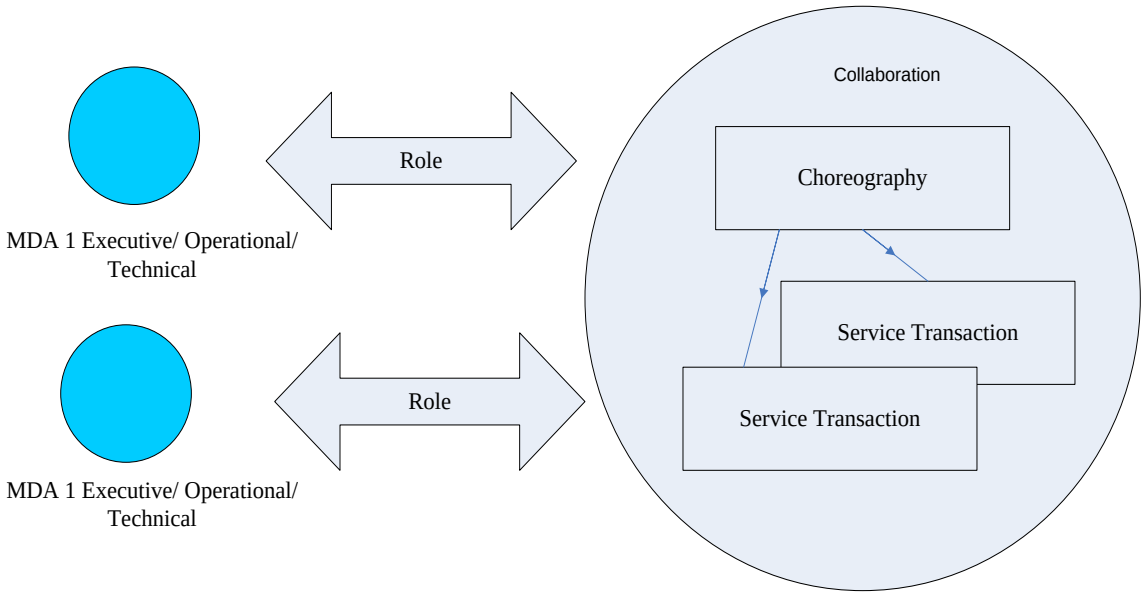



Figure 8-9 TOG Process Model - Layer 2

The concepts shown in Figure 8-8 that describe the TOG process model are:

**Service Collaboration**

A Service Collaboration is a set of Service Transactions between two individual MDAs in one government or across governments for layer 1 of the process model, and between actors within an MDA for layer 2. The ebXML Business Process Specification Schema supports two levels collaborations which are Binary Collaborations and Multiparty Collaborations. Binary Collaborations are between two roles only Multiparty Collaborations are among more than two roles, but such Multiparty Collaborations are always synthesized from two or more Binary Collaborations. For instance if Roles A, B, and C collaborate and all parties interact with each other, there will be a separate Binary Collaboration between A and B, one between B and C, and one between A and C. The Multiparty Collaboration will be the synthesis of these three Binary Collaborations.

**Service Transactions**

A Service Transaction is the atomic unit of work in a Service Collaboration. A Service Transaction is conducted between two parties playing opposite roles in the transaction. The

roles are always a requesting role and a responding role. Like a Binary Collaboration, a Service Transaction is a re-useable protocol between two roles.

A Service Transaction will always either succeed or fail. If it succeeds it may be designated as legally binding between the two partners, or otherwise govern their collaborative activity. If it fails it is null and void, and each partner must relinquish any mutual claim established by the transaction.

**Service Document flows**

A service transaction is realized as Service Document flows between the requesting and responding roles. In the case of the TOG process model, there is always a two way conversation between the MDAs therefore there is always a requesting Service Document, and a responding Service Document. Actual document definition is achieved using the ebXML core component specifications, or by some methodology agreed to by the MDAs that have roles in the service collaboration.

**Choreography**

The TOG Process Plug and Play approach is characterized definitively by the Service Transaction Choreography. The Service Transaction choreography describes the ordering and transitions between service transactions or sub collaborations within a binary collaboration. Thus the choreography in the TOG framework describes how mapping across different technical, operational and governance mechanisms is achieved.

For Layer 1 of the TOG process model, the service transaction is the G2G transaction, in which one MDA requests for a service from the second MDA. To implement the TOG framework process model in this case, means that the responding MDA will check that the request complies with the security requirements from a technical, operational and governance perspective. The particular mechanism that needs to be check against or used to implement the requirement may vary, but as a starting point, some mechanisms are summarized in Table 8-11.

Table 8-11 Proposed Mechanisms

| | | MODEL | | |
|---|---|---|---|---|
| **Security Objective** | **Security Requirement** | **Governance** | **Operational** | **Technical** |
| Confidentiality | Authentication | • International Standards,<br>• Laws and Regulations,<br>• Organisational Policies | • Risk Assessment<br>• Certificate Authorities<br>• Metadata definitions<br>• Awareness Sessions | • Ontologies<br>• Access control model based on open standards (XACML, SAML) |
| | Authorization and Access Control | | | |
| | Privacy | | | |
| Integrity | Data Integrity | • International Standards, Organisational Policies | • Certificate Authorities | • Encryption, SSL |
| Availability | Availability | • Business Continuity Policies (BCP) | • Power Management<br>• Business Continuity Plans<br>• Interoperability frameworks | • SOA, Web Services, Uninterruptible Power Supply (UPS) |
| Accountability | Trust & Non Repudiation | • Laws and Regulations,<br>• Contractual Agreements and MoUs | • Certificate Authorities | • Digital Signatures, Certificates |

For Layer 2 where the interaction is between actors in an individual MDA for purposes of continually improving the ability to meet information security requirements, the choreography is that for each mechanism implemented in one model, a mapping is done across to the models to ensure that matching mechanisms are in place or are planned for. To ensure consistency in the implementation of the process model, a PDCA cycle is proposed to be followed as shown in Figure 8-10.

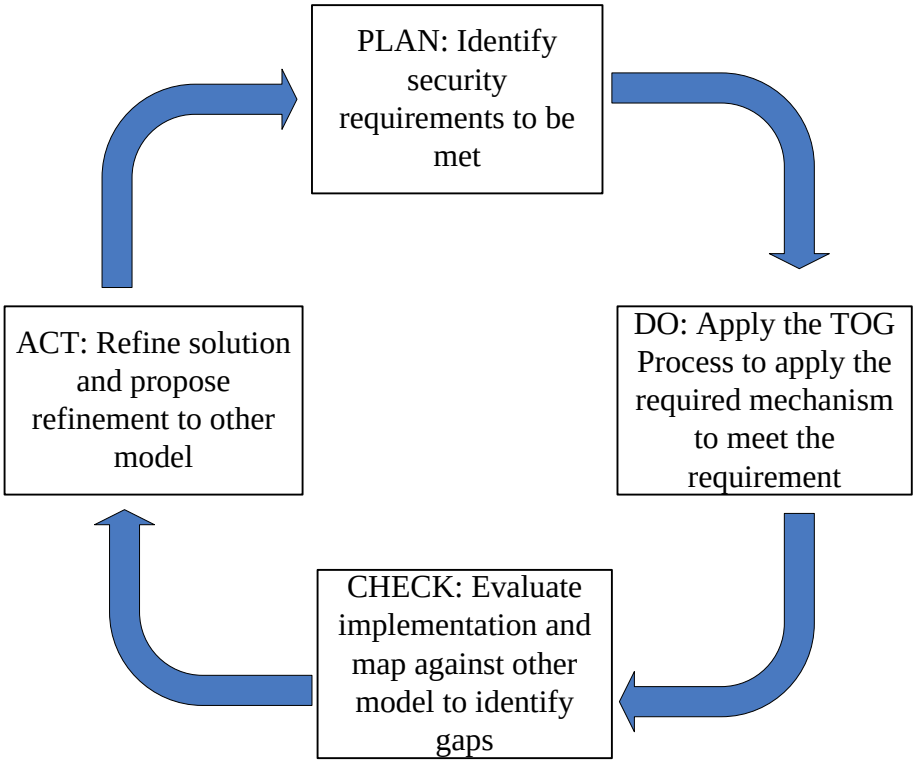



Figure 8-10 PDCA Cycle implementation of Layer 2 of the TOG Process Model

In the planning stage, the security requirement to be met is identified based on whether the implementation is triggered by a service request from an MDA (Layer 1 of the process model) or whether an MDA is putting in place more mechanisms to address information security (Layer 2 of the process model). In the Do stage, the TOG process is applied, security mechanisms to address the requirement are implemented across all the models, where those mechanisms are in place. In the Check phase, the MDA evaluates the transaction to recognize gaps, and finally acts on them to continually improve on addressing information security requirements.

### 8.7.3 Scenarios to Illustrate the Implementation the Process Model

In this section, two scenarios are presented that illustrate how MDAS can implement the process model. The use of scenarios in process modeling has been presented in several studies (Gregoriades & Sutcliffe, 2008; Barnickel, Bottcher, & Paschke, 2010) and is intended to help implementers to quickly understand how the model can be applied in their particular context. The two scenarios presented below are drawn from real situations in the

EAC. The first scenario is drawn from the Government of Tanzania, and the second, from the Government of Rwanda. The scenarios are drawn from information obtained from MDAs that participated in the survey that is presented in chapter six of this thesis.

a) Scenario 1

The Government of a country decides to provide a pension to all citizens above the age of 65. The personal details of all citizens are held in a database that is managed by an MDA that is responsible called national identification (for purpose of this scenario, referred to as MDA A). A law to facilitate the payment of the pension is passed, and the MDA tasked with paying the pension (referred to here as MDA B) is required in this law to use only personal details that are in MDA A's database. Confidentiality of the information must be maintained through this G2G transaction. MDA A currently has operational plans that address confidentiality of information but do not recognize the newly passed legislation.

Using the TOG process model- Layer 2, the first action is that MDA A needs internally to align its operational plans with the new legislation. So the first step in the service choreography between MDA A executive actor and MDA A operational actor is to align the legislation with operational procedures. Then in implementing Layer 1, MDA B submits the request to MDA A, and then MDA B compares the service documents which are the various policies/ plans that state information security requirements. MDA A then fulfills the service requests in line with the requirements of the law, and applying the appropriate mechanisms in the TOG framework. This scenario illustrates the 'plug and play' nature of the TOG process model, in that only the specific requirement for that particular scenario is plugged into the TOG framework and results in a G2G transaction that meets information security requirements. This is illustrated in Figure 8-11.

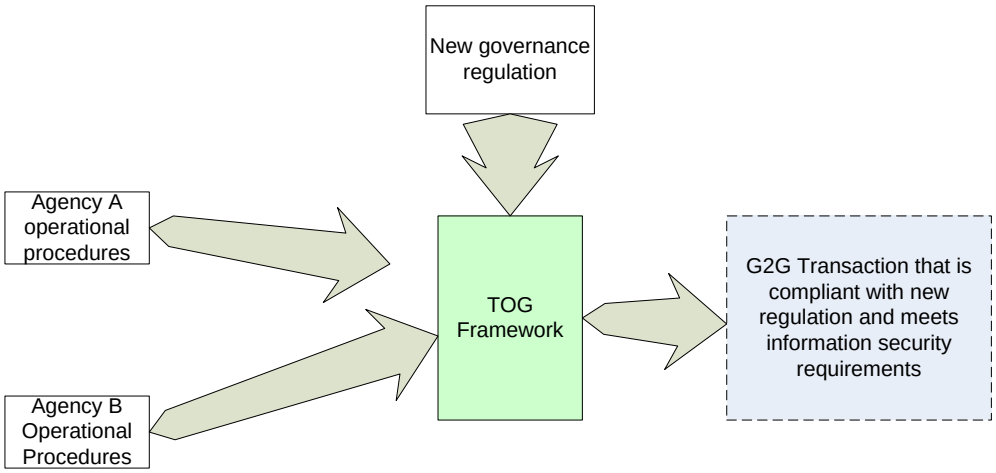



Figure 8-11 Illustration of Plug and Play approach – Scenario 1

b) Scenario 2

A MDA has invested significantly in setting up a robust information security policy that sets out the governance requirements for information security. This MDA now wants to proceed with the implementation of a new application to provide services to other MDAs. The technical team is eager to start putting together technical mechanisms that match the governance requirements stated in the information security policy without necessarily waiting for operational departments to finish putting in place operational procedures.

Implementation: The existing policy falls within the governance model, and the contents of the policy need to be mapped onto relevant technical mechanisms. This process falls within Layer 2 of the TOG process model. Once technical mechanisms are in place, the G2G transactions can take place, following Layer 1 of the process model. The operational model can be addressed when the implementers who are the MDA operational staff are ready. This implementation is illustrated in Figure 8-12.

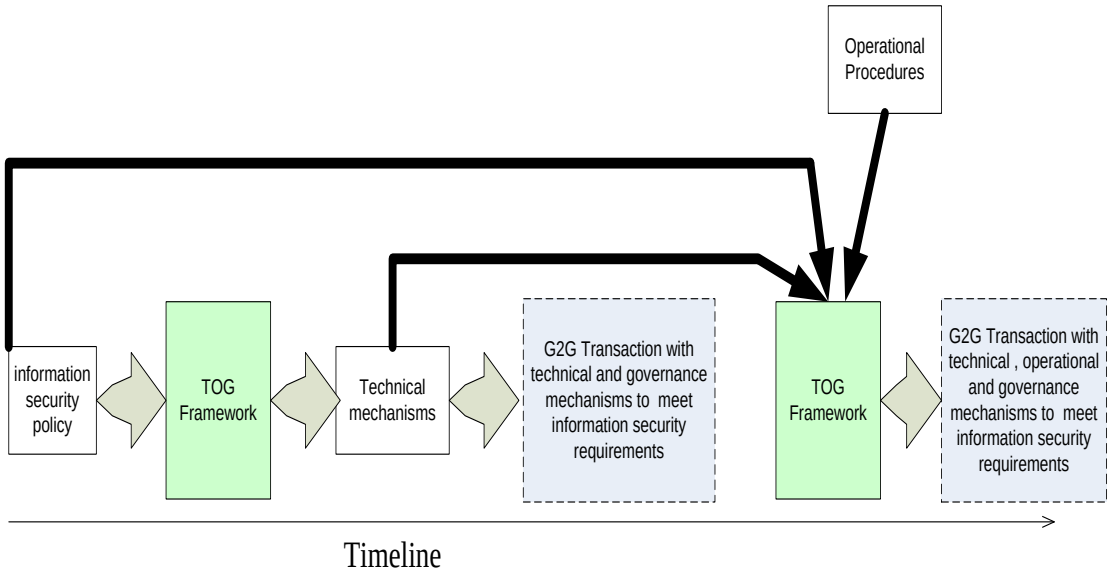



Figure 8-12 Illustration of Plug and Play Approach - Scenario 2

The two scenarios illustrated in figures 8-11 and 8-12 show that with the TOG framework, implementation can start anywhere, namely, in any model depending on the circumstances. The other model can be addressed as necessary when resources are available. It also shows that where information security initiatives are already in place, the use of TOG maps new implementations to existing ones, thus agencies do not have to start from scratch. Furthermore, not all requirements need to be addressed at once. The process can be done iteratively and a simple maturity model can be used to track progress by MDAs in adopting information security practices. The maturity model is described in section 8.8.

## 8.8 Maturity Model

The purpose of a maturity model is to propose a roadmap through which an entity can continually improve towards a set goal. The TOG maturity model is aimed at helping MDAs continually improve information security practices through the TOG framework with the goal of achieving a sustainable information security framework for G2G transactions that is applicable in the EAC context.

The TOG maturity model consists of the following levels of maturity:

Level 0: There are no information security practices within the MDAs. Characteristics of a Level 0 maturity would include lack of information security policies or even documented information security objectives.
Level 1: Some Governance, operational and technical mechanisms exist but do not map onto each other. An example of a Level 1 maturity level would be where an MDA implements technical security mechanisms but there is no accompanying operational or governance mechanisms.
Level 2: Governance, Operational and technical mechanisms are in place, and some mapping has been done across the TOG models.
Level 3: Governance, operational and technical mechanisms are in place to meet all security objectives and mapping across the TOG models has been achieved.

The levels of maturity can be used as mechanisms in the TOG framework to address the Accountability objective. Thus in a G2G transaction between two MDAs, the MDA providing a service may inform the requesting MDA as to what level of security it is at. An MDA that is providing a service may also require that a requesting MDA is at a given level of maturity in order to access information or a service, so that information security is preserved even when information is passed onto another MDA.
The TOG maturity model is illustrated in Figure 8-13.

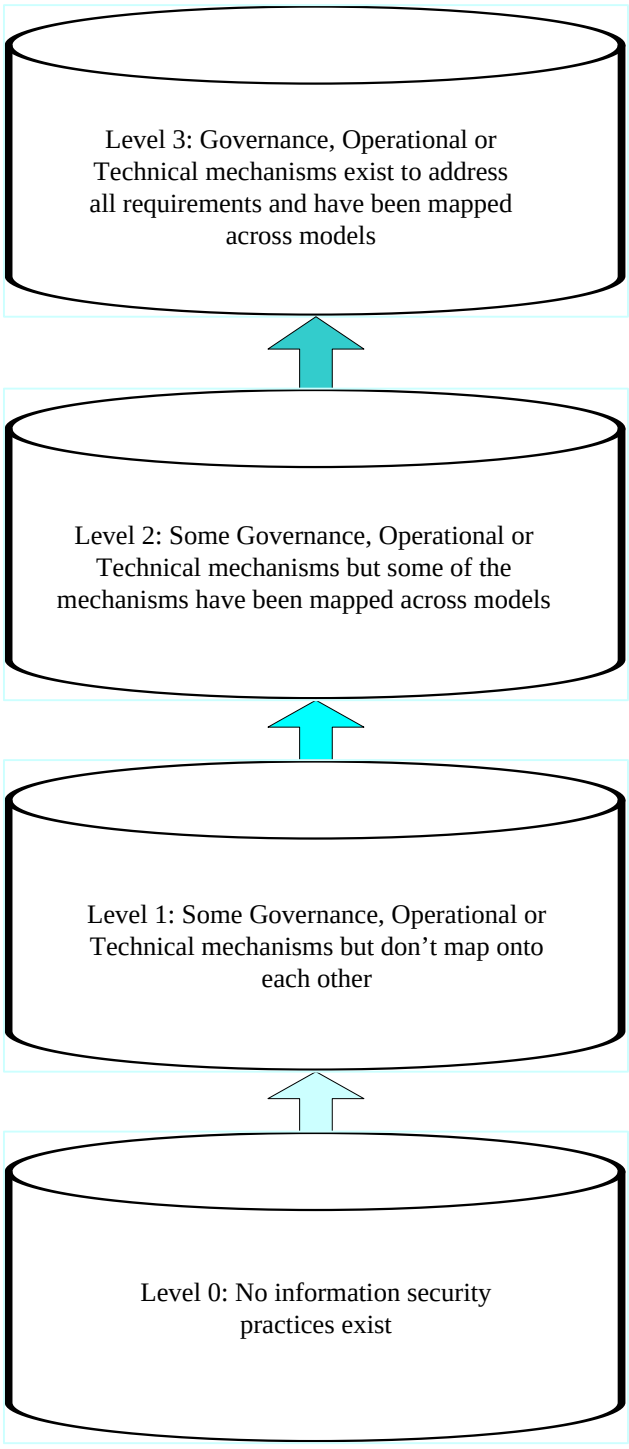



Figure 8-13 Maturity model for TOG framework

## 8.9 Conclusion

This chapter has presented an information security framework for G2G transactions in the EAC context. The framework comprises of five models which are technical, operational, governance, process and maturity models.

The basic tenets or philosophy of the TOG framework is simple – each actor in a G2G transaction must recognize their role; and do whatever is possible to address common security objectives. A mapping across roles is done whenever each actor is addressing a security requirement. This process leads to a continual raising of information security awareness and a move towards holistic handling of information security even where resources are limited and where there is little or no co-ordination within government. For the technical, operational and governance models, implementation guidelines and useful resources are presented so as to ease implementation. The mechanisms proposed in each of the models, are mechanisms that have been tried and tested in existing implementations in e-government in the EAC, with the exception of the GABAC mechanism.

The TOG process model with its 'Plug and Play' implementation approach suits the EAC context where flexibility in approach is required to take into consideration the culture of un-coordinated initiatives, and at the same time, the limited resources. The need for continual improvement in the addressing of information security remains relevant to the EAC, and the application of the TOG maturity model ensures that MDAs are continually improving on information security practices.

The next chapter describes how the framework was applied in a real life case study for a G2G transaction in one of the countries of the EAC, that is, Tanzania. This is the Implementation stage of the Appreciative Inquiry process.

# Chapter 9 Case Study

## 9.1 Introduction

In the previous chapter the TOG information security framework was presented together with guidelines on how the framework can be implemented. This chapter describes how the framework is applied to a case study of a G2G transaction in the Implementation phase of the Appreciative inquiry approach, which was one of the methods used in this study.

The purpose of undertaking the case study was to demonstrate that the proposed framework is a practical framework that can work in a real situation.

## 9.2 Case Study Description

The Tanzanian Central Government has been paying pensions to civil servants who retired before 1996 through a ministry responsible for finance. Due to concerns about the efficiency of the process, fraud and resource constraints, the ministry, in 2008, decided to outsource the process to a government agency. The government agency chosen is one that has experience in paying pensions to employees from the private sector and from other government agencies. The ministry required the government agency to run the payroll on secure software and send the payroll information electronically to banks. The banks would then debit the ministry account and credit the pensioners account. The ministry envisaged that this process would reduce human intervention which is one of the sources of fraud; ensure that pensioners are paid on time; and have an audit trail of transactions so as to follow up on any suspect cases. Furthermore, by outsourcing the arrangement to an agency that already had robust software, and a business continuity program in place, the risks arising from frequent power interruptions and lack of sufficient technical skills in the ministry would be addressed.
Information related to the processing of the payroll is classified by the Government as Confidential, and the Government ministry has put in place an information security policy that outlines some mechanisms that need to be put in place to preserve confidentiality.

The agency chosen to implement also has an information security policy in place, which includes a statement that states all interactions with external parties that involve system access must be governed by the agency's information security policy.

## 9.3 Methodology used for Case Study

In keeping with the interpretive methods used in this study, action research was chosen to apply the TOG framework to the case study. The TOG framework was applied using the action research methodology (de Villiers, 2005). The process undertaken can be viewed as illustrated in Figure 9-1.

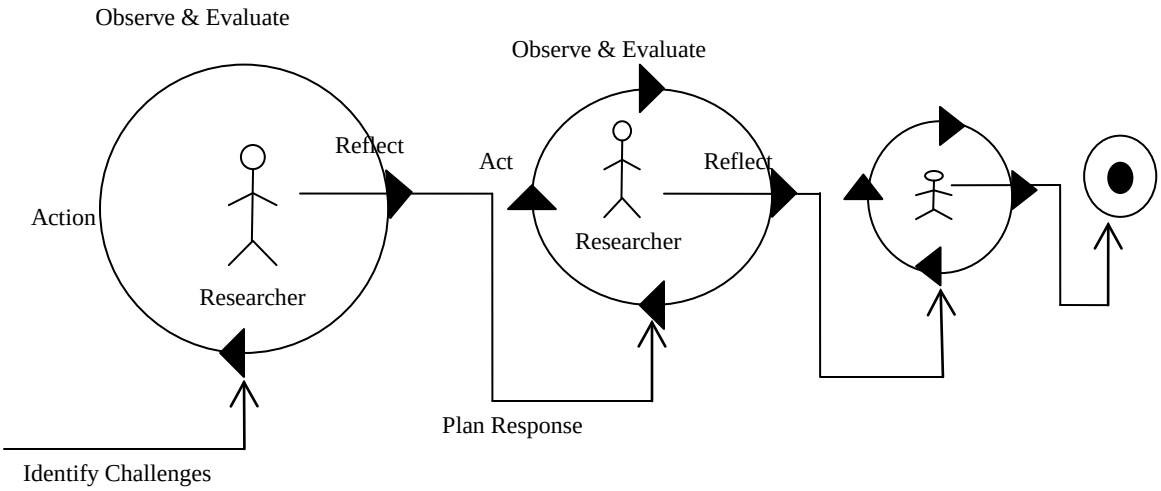



Figure 9-1Action Research: Adopted from de Villiers (2005)

It was possible to use the action research methodology which requires the researcher to be an active part of the process, because the author of the thesis was an employee of the implementing agency, heading the information systems department.

The actors who participated in the case study are as shown in Figure 9-2.

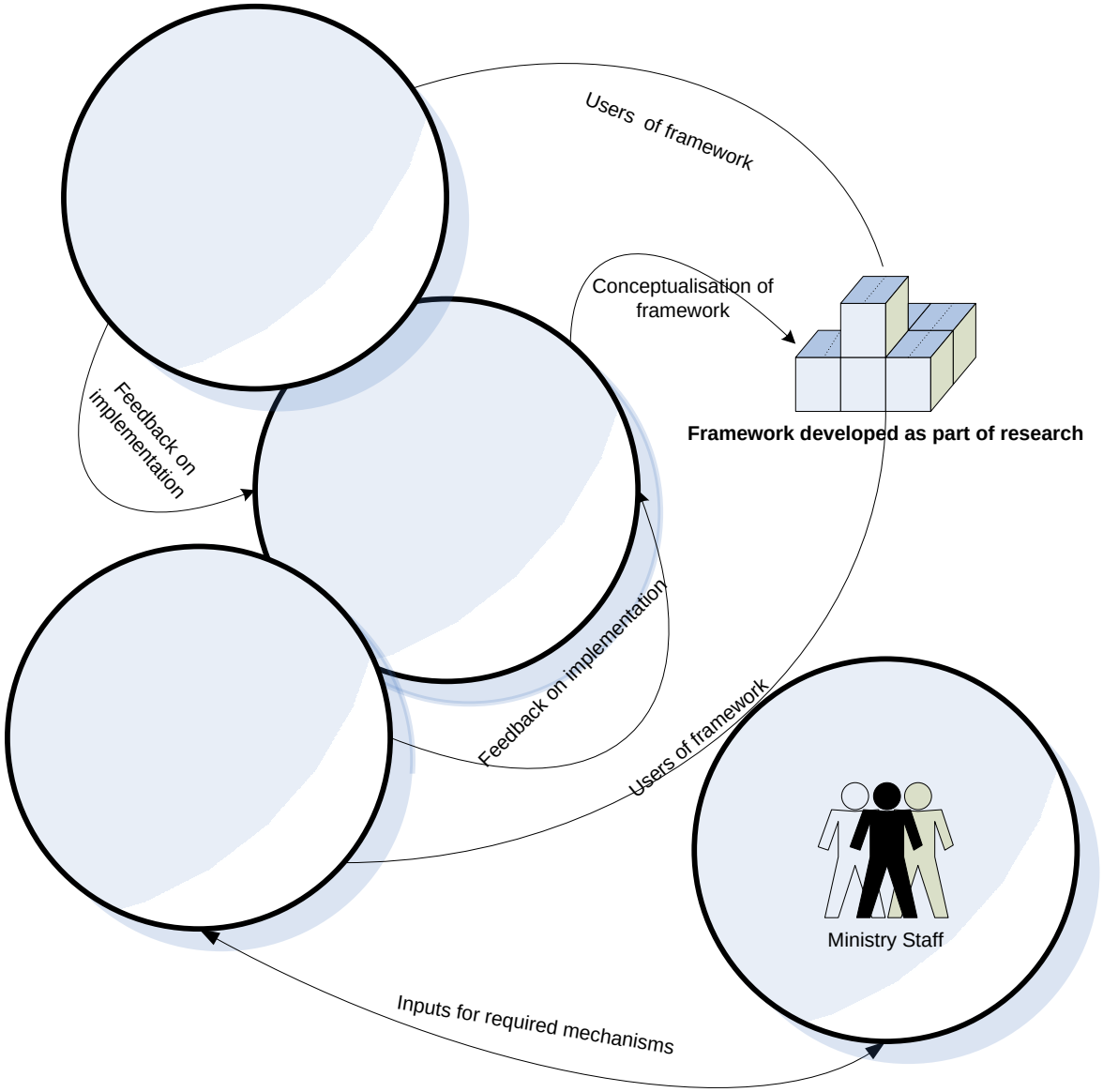



Figure 9-2 Actors in the Case Study

In terms of the roles identified for actors in the TOG framework, the author of this thesis (researcher) had a role as MDA executive and MDA technical.

The first step in the case study was to identify the challenges that application of the TOG framework was expected to address. These challenges are outlined in the next section.

### 9.3.1 Challenges identified

The process of implementing the decision began with a kickoff workshop in 2008 involving staff from the ministry responsible for finance and the agency chosen to pay pensions.

Workshop participants were drawn from all the three major actors/ roles described in the TOG framework, who are MDA executive, MDA operational and MDA technical. Several challenges were identified during the workshop and when the action plan for implementation was started. These challenges are categorized in three categories. For ease of reference the challenges are given code numbers. These are:

**a) Governance**

- C_01: Legally, the agency had no mandate to access the data held by the ministry or to pay pensions on behalf of the ministry.
- C_02: Both ministry and agency had information security policies that needed to be aligned for purposes of the transaction.
- C_03: The memorandum of understanding (MoU) signed between the Ministry and the agency did not explicitly address information security.

**b) Operational**

- C_04: Definitions of some terms were different. For example a survivor's pension in the central government ministry is different from a survivor's pension in the government agency.
- C_05: Financial resources allocated to the outsourcing project were limited.
- C_06: The ministry wanted to retain some control over updates to information
- C_07: Technical and management teams met separately during the planning process.
- C_08: The organizational culture for the two organizations was found to be different. In the agency, technical staff spearheaded most initiatives and sold ideas to management, while in the ministry the approach was more top down, with directives given by the minister, which the technical and operational staff have to implement.

**c) Technical**

- C_09: Some of the necessary data was mostly in paper files and confidentiality and privacy was observed through physical access controls such as storing the data in locked cabinets. Access lists were on paper and files containing information were issued by a person responsible for storing the files.

- C_10: The ministry was running their payroll on a COBOL based application while the government agency was using an application based on Oracle Forms. The underlying databases and operating systems were also on different platforms.
- C_11: The ministry offices and the agency offices had no direct data communication link.
- C_12: Although security policies existed in both organizations, no standard requirements for security were set out in either policy.

The above challenges show that the requesting MDA, at the beginning of the application of the case study was at Level 1 maturity on the TOG maturity model meaning that some governance operational and technical mechanisms were in place but did not map onto each other. The responding MDA was at level 2, with some mapping across operational, technical and governance mechanisms.

### 9.3.2 Applying the TOG Framework

The first action was to apply the TOG process model by identifying the requirements to be met and the mechanisms to be put place in both the requesting and responding agencies. The Agency and Ministry staff, following the implementation guidelines of the TOG framework, identified the essential mechanisms that needed to be place as shown in Table 9-1.

Table 9-1 Essential mechanisms to be put in place

| | | MODEL | | |
|---|---|---|---|---|
| **Security Objective** | **Security Requirement** | **Governance** | **Operational** | **Technical** |
| Confidentiality | Authentication | | Valid user names | Need to authenticate IP address, that it is from valid PC |
| | Authorization and Access Control | | | |
| | Privacy | | | |
| Integrity | Data Integrity | | | |
| Availability | Availability | | | |
| Accountability | Trust & Non Repudiation | Need Legislation | | |

An initial application of Layer 2 of the process model identified that there were gaps in the Governance model. Thus the initial approach by the Ministry was to deal with the issue of legislation, and propose amendments to legislation to allow the agency to process payments.

These amendments simply allowed the agency to pay pensions on behalf of the government. The challenge of data access was not addressed.

### 9.3.3 Reflection

Reflection was undertaken to identify the gaps still outstanding. This was done in the form of a workshop, with the author still in the roles of MDA executive and MDA technical. The participants in the workshop were from both the Ministry and the Agency and including both executive and technical staff.

The actions undertaken to meet the requirements in each of the three TOG models, Governance, Technical and Operational to resolve the gaps are outlined in section 9.4

## 9.4 Actions undertaken

### 9.4.1 Technical

The actions described in section 9.3.2 were the first set of actions in applying the TOG framework. The second set of actions involved the technical staff of the agency developing a payroll web service that can be invoked by the ministry if they need to do updates to data. The code for this web service is included in this thesis as Appendix B. The same web service is used to run the payroll. In addressing data integrity, privacy and confidentiality, a secure communication link has been set up between the ministry and the agency and information across the link is encrypted. The relevant information security policies were translated to XACML. Authentication has been tied to fixed IP addresses with user names and passwords. Availability has been addressed through the installation of UPS for power supply management. The agency uses an SSL certificate issued by VeriSign for its browser interfaces. The challenges that still need to be addressed include automating the issue of security assertions, by for example, implementing SAML.

### 9.4.2 Operational

In meeting the operational information security objectives, the following activities were undertaken jointly by Ministry and Agency staff at an executive and technical level:

- A risk assessment was carried out and an access control list setup
- The parties have agreed to use the Ministry definitions where terminology differs.

Challenges that still need to be addressed include compiling taxonomy of terms that relate to the payment of pensions to ensure that terms are interpreted consistently. Some of the terms have been represented in OWL ontology as shown in appendix C.

### 9.4.3 Governance

Legislation was put in place to mandate the agency to pay pensions to designated recipients on behalf of the ministry before the implementation of the framework. The role of drafting and proposing amendments was undertaken by the Ministry executive staff. Based on the amended legislation, a contract was signed between the two parties to outline the operational roles and responsibilities of each party in implementing the outsourcing of payment of pensions. Furthermore, the parties also agreed that the information security policy of the ministry would prevail. Table 9-2 illustrates how the TOG framework was applied.

Table 9-2 Application of the TOG framework to the case study

| | | MODEL | | |
|---|---|---|---|---|
| **Security Objective** | **Security Requirement** | **Governance** | **Operational** | **Technical** |
| Confidentiality | Authentication | • Ministry's Information Security Policy | | Authentication based on fixed IP addresses with user names and passwords |
| | Authorization and Access Control | • Finance Act. No. 13 of 2008<br>• Contract between Ministry and Agency | • Risk Assessment, Access Control List,<br>• Standard Terminology for transactions<br>• Awareness Sessions | • XACML policies based on Ministry's information Security Policy |
| | Privacy | • Ministry's Information Security Policy | | |
| Integrity | Data Integrity | • Ministry's Information Security Policy | | • SSL, Encryption |
| Availability | Availability | | | • Uninterruptible Power Supply (UPS);<br>• Pensioner Payroll Web Service |
| Accountability | Trust & Non Repudiation | • Finance Act No. 13 of 2008<br>• MoU between Ministry and Agency | • Access Control List | • SSL (from VeriSign)<br>• Authentication by IP address |

### 9.4.4 Improvements to Maturity

As mentioned in section 9.3.1, maturity levels when measured using the TOG maturity levels, were are Levels 1 and 2 for the requesting MDA (Ministry) and the responding MDA (pensions agency) respectively. Layer 2 of the TOG process model was applied within the pensions agency, in which the author of this thesis was employed. The TOG framework was applied to improve the existing information security framework and to represent the framework using the TOG technical, operational and governance models. The resultant framework has been included in this thesis as Appendix D.

## 9.5 Conclusion

The case study described illustrates how the TOG framework was applied in a real life situation. The lessons learnt from the application were that no additional skills were required to implement the framework, and the technical mechanisms used were those already in use in the responding agency. Thus the cost of implementation of the framework was minimal.

The case study acts as a proof of concept that the framework actually works and that the implementation is such that not all mechanisms need to be put in place at the same time in order to address a security requirement. Although not all aspects of the framework were implemented due to the nature of the case study and time constraints, the applicability of TOG to G2G transactions in the EAC context has been demonstrated through the described case study.

In the next chapter, an evaluation of the TOG framework against critical success factors is presented. While the case study presented shows how the framework can be applied in a particular setting, the evaluation in chapter ten demonstrates that the TOG framework can be applied generally to address information security requirements for G2G transactions in the EAC.

# Chapter 10 Evaluation of the TOG Framework

## 10.1 Introduction

In the previous chapter, a case study showing how the TOG can be implemented was presented. This chapter presents an evaluation of the framework to show that the framework is generally applicable to addressing of information security requirements for G2G transactions in the EAC.

The TOG framework is evaluated in two ways. Firstly Critical Success Factors (CSFs) from both Tanzania and ISO are used and secondly by matching against G2G guidelines issued by the US National Research Council. The use of critical success factors as a method for evaluating information systems is discussed by Bergeron & Bégin (1989) who identify CSFs and measure performance against those factors in a case study involving an information system in the health domain. Caralli (2004) discusses the uses of CSFs for validation of security measures within an enterprise. Furthermore, one of the discoveries from the national information security frameworks as presented in chapter three was that as a means of achieving acceptability, which will contribute to sustainability, a framework may be evaluated against set government policy objectives.

For the TOG framework evaluation, two sets of established critical success factors were chosen. These two sets were chosen because the TOG framework was designed to address information security requirements for G2G transactions in the EAC. The first set of CSFs is taken from the Tanzanian e-Government Strategy (United Republic of Tanzania, 2009). These CSFs have considered the EAC context and therefore to evaluate TOG against them shows how well the framework suits the EAC. The second set of CSFs is the ISO/IEC Information Security Management Standards (ISMS) CSFs. These are chosen because, firstly they relate to information security which is the focus of the TOG framework, but secondly because they are published by an international standards body, which is the ISO and therefore evaluating TOG against the ISMS standards is a measure of the robustness of the framework.

There, however, remains the issue of the G2G component of this study and of the TOG framework. Neither of the above two sets of CSFs addressed G2G in particular. To address this gap, the TOG framework is also evaluated against the guidelines for G2G transactions that have been issued by the US national research council (National Research Council, 2002).

## 10.2 Critical Success Factors from Tanzania's e-Government strategy

The government of Tanzania in its e-Government strategy has identified key factors that are critical to successful e-Government implementation. The factors are not specifically for information security but can be applied as information security should form an integral part of the planning process of the implementation from conception to conclusion.

The six CSFs identified in the Tanzanian e-Government Strategy are:

i. Political will, support and commitment: Continuous engagement of political leaders in support toe-Government in order to maintain the momentum
ii. Availability of HR capacity: Continuous capacity development, Continuous public involvement
iii. Institutional and Legal framework: Clearly defined institutional framework and supportive legislation and enforcement mechanisms
iv. Financial Resources: Recognition of e-Government as a priority area in the Government agenda
v. Commitment by all actors: Continuous coordination and buy-in by all actors or stakeholders. Active coordination among all stakeholders to develop and enforce coherent e-Government service delivery
vi. Sustainable Infrastructure: Network and information security; Infrastructure to sustain e-Government services.

In the context of the TOG framework, the above CSFs can be related to the five models that make up the TOG framework which are the Technical, Operational, Governance, Process and Maturity Models.

The Technical Model of the TOG framework identifies security mechanisms that enable secure G2G transactions. These mechanisms address CSF (vi); and furthermore, the TOG

technical model proposes web services to implement G2G transactions which are the backbone of e-Government Services. Sustainability is built into the TOG framework through the process model, that allows for implementations as and when resources are available, and through the maturity model that guides the implementing MDAs and governments on how to continually improve the way that they meet information security requirements for G2G transactions. The Technical Model also proposes the use of mechanisms based on open standards thus addressing CSF (ii) and (iv).

The Operational Model of the TOG Framework proposes operational plans that will enable the information security requirements for G2G transactions to be addressed. This takes care of the institutional component of CSF (iii).

The Governance Model of the TOG framework proposes the use of legislation and policies to meet the information security requirements for G2G transactions, and in this way addresses CSF (i) and (iii).

The Process and Maturity models of the TOG framework contribute to CSFs (ii), (iv) and (v) firstly by allowing MDAs to address information security requirements through a 'plug and play' approach that does not force complete solutions to be in place at once. However, the process model calls for continual mapping across the technical, operational and governance models, thus ensuring that staff at all levels in the MDA are part of the process in addressing information security requirements for G2G transactions.

The evaluation of the TOG framework against the CSFs in the Tanzanian e-Government strategy is summarized in Table 10-1.

Table 10-1 Evaluation of TOG against Tanzania CSFs

| **CSF from Tanzania's e-Government Strategy** | **TOG Solution** |
|---|---|
| Political will, support and commitment | All legislation in Tanzania is passed through the parliament. By identifying the governance model, political leaders understand the role they need to play to have successful information security in e-Government implementation. |
| Availability of HR capacity | TOG addresses availability by having a flexible structure that refers to international open standards. Therefore there is no need for MDAs to reinvent the wheel where proven standards are already in place. |
| Institutional and Legal framework | This is addressed in the Governance and Operational Models were legislation and polices have to be taken into consideration. |
| Financial Resources | TOG is a flexible framework whose 'plug and play' approach to process implementation means that the technical, operational and governance components to address each security requirement can be implemented as and when resources are available within the acceptable risk acceptance level. |
| Commitment by all actors | Implementation of the TOG framework forces the involvement of technical operational and management staff. |
| Sustainable Infrastructure | The technical model proposes the use of open standards, and service oriented architectures which address the lack of interoperability that may exist among MDAs. |

## 10.3 ISMS Critical Success Factors (ISO/IEC, 2005b)

ISO in the code of practice of information security management states critical success factors for information security management. These are applicable to the evaluation of TOG since TOG is designed to address management aspects of information security. The evaluation against the ISMS CSFs is shown in Table 10-2.

Table 10-2 Evaluation of TOG against ISMS CSFs

| **ISMS CSFs** | **TOG Solution** |
|---|---|
| Information security policy, objectives and activities aligned with objectives | TOG addresses information security policies and provides for the mapping of those policies to operational and technical activities |
| An approach and framework for designing, implementing, monitoring, maintaining and improving information security consistent with the organizational culture. | The TOG process model allows for organizational culture especially in the context of Tanzania where often it is not possible to have a strictly hierarchical or sequential process. TOG allows for various start points in any of three models which are the technical, operational and governance models and then subsequent mapping to any of the other models using the process model, provided that the security objectives are set in advance. |
| Visible support and commitment from all levels of management especially top management | Implementation of the TOG framework forces the involvement of technical, operational and management staff. |
| An understanding of information asset protections achieved through the application of information security risk management | Risk Assessment is provided for as a proposed mechanism in the operational model. |
| An effective information security awareness, training and education program informing all employees and other relevant parties of their information security obligations set forth in the information security policies and standards and motivate them to act accordingly | Awareness is provided for as a mechanism in the operational model. Furthermore, the requirement that in each model for each requirement, the actor has to see what has been done in another model ensures that technical departments, operational units, and executive management are aware of the information security initiatives across the MDA that are being carried out to achieve security objectives |
| An effective information security incident management process | An incident management process is included in the guidelines for the implementing the operational model. |
| An effective business continuity management approach | Business continuity management is provided as a mechanism in to address the Availability security objective. |
| A measurement system used to evaluate performance in information security management and feedback suggestions for improvement | The TOG maturity model allows MDAs to track their progress with regards to addressing information security for G2G transactions |

## 10.4 US National Research Council Guidelines

The US National Research Council (National Research Council, 2002) proposes some areas where G2G needs have to be addressed. These include:

- Ubiquity: Governments must provide services to all citizens. They cannot in general opt to serve only the easiest to reach customers.

  *In the TOG framework, SOA and web services are proposed as technical mechanisms. These services can be accessed through mobile phones. The penetration of mobile phones*

*is quite high the EAC region and are accessible in rural areas. Thus a citizen can launch a request from their mobile phone which would result in a G2G transaction that would be securely handled by the proposed framework.*

- Trustworthiness: Citizens expect governments to provide assurances of security including confidentiality, integrity and availability of information. For G2G transactions there is a need to ensure that there is no improper disclosure of personal information while at the same time, certain kinds of information may be derived from personal information and made available to all.

  *The framework presented addresses information security requirements at governance, operational and technical level in detail.*

- Information Heterogeneity and Semantic Interoperability: In G2G transactions, information is drawn from multiple sources. Integration is especially difficult in ad-hoc situations e.g. to respond to a crisis. But even in routine situations there is a need to provide a service based on aggregate information. The need for information heterogeneity and semantic interoperability is further underlined because government agency systems often employ different and incompatible conventions for data formats.

  *The framework makes use of open technology neutral standards, web services and ontologies to achieve information heterogeneity and semantic interoperability.*

- Providing software interfaces to services: to allow other stakeholders to easily exploit information provided by the government.

  *The framework proposes the use of Service Oriented Architectures with services published as web services thus enabling exploitation of the services to authorised users.*

## 10.5 Limitations of the Evaluation Approach

The Critical Success Factors used to evaluate the framework allow for a weighing of each critical success factor against the respective component of the framework in order to conclude as to whether the framework addresses those critical success factors. This kind of evaluation, while suitable for the overall TOG framework does not critically evaluate the technical model of the TOG framework. In particular, the GABAC mechanism proposed as part of the technical model would benefit from a more suitable way of evaluation for a technology based mechanism.

## 10.6 Conclusion

In this chapter which is the last in part IV, the TOG framework has been evaluated. The framework proposed evaluates well against critical success factors for e-Government and information security and matches G2G transactions guidelines.

The TOG framework also addresses the constraints that are currently faced by the EAC in the following way:

- Proposing a process such that the framework that can be implemented as and when resources are available at a regional, national and individual agency level.
- Basing on open standards that are available freely together with examples of implementation and guides to useful resources.
- Enabling implementation to be a 'plug and play' approach so that governments do not constantly have to keep up with technologies but rather keep focused on what has to be achieved and ensuring that technical solutions meet specific requirements and are backed by operational guidelines and governance policies. At the same time, MDAs can proceed with secure G2G transactions without waiting for legislation to be put in place, and can adapt their organizational practices when legislation comes into place.
- Enabling communication between Governance level and technical level staff by using a format that shows what other actors have done and what has to be done to meet common security objectives, thus continually raising awareness across the MDA.

In the next chapter, which is the last in this thesis, the conclusions of this study are presented, and the original contributions are highlighted.

# PART V: CONCLUSION AND FUTURE WORK

# Chapter 11 Conclusions

## 11.1 Introduction

This study set out with the general objective of adding to the body of information security and e-Government knowledge by proposing an Information Security framework for G2G transactions in the context of the EAC. The study was motivated by the observation that comparatively little information security research has been carried out using the EAC as a case study. Furthermore, given the EAC's desire to move towards a common market which will entail increased G2G transaction, an information security framework will be a helpful aid to the EAC governments as they start to increase electronic collaborations within each country and across the region.

The research questions that were to be answered by this study were:

i. What are the information security requirements for G2G transactions in the EAC context?
ii. What are the factors to be addressed in an information security framework for G2G transactions in the EAC?
iii. How can a sustainable information security framework for G2G transactions be achieved in the EAC context?

The following were the specific objectives of the study

i. To define information security requirements in the EAC context for G2G transactions
ii. To propose a framework that addresses the requirements identified
iii. To evaluate the proposed framework

The framework was arrived at by:

- Defining the key concepts of e-Government and information security in Part I of the thesis.
- Studying and interpreting literature on information security related to G2G practices adopted by international and national bodies as standards or guidelines together with related academic research. The result was a literature review presented in Part II of this thesis.

- Establishing the EAC context through a synthesis of relevant documentation and the data obtained from a survey of information security practices related to G2G transactions in MDAs; and thus answering the second research question. The EAC context was combined with the results of Part II of the thesis to establish the information security requirements for G2G transactions in the EAC, and thus answering the first research question.
- Combining the findings of Parts II and III to propose an information security framework and process that is relevant to the EAC context, and thus answering the third and final research question.

The resultant framework was applied to a case study and evaluated using Critical Success Factors.

## 11.2 Summary of findings

### 11.2.1 First Research Question: Information Security Requirements for G2G transactions in the EAC

Information security requirements for G2G transactions in EAC countries are not different to the requirements in other parts of the world and relate to the same security objectives. The security objectives and requirements are: Confidentiality (Authentication, Authorization and Access Control, Privacy); Integrity (Data integrity); Availability; and Accountability (Trust and non-repudiation). The information security requirements were detailed in chapter seven of the thesis. For the EAC, however, the mechanisms that are used to meet these requirements must address the three factors identified in the EAC context as detailed in the findings that answer the 2$^{nd}$ research question. Additionally, a specific novel mechanism suitable for meeting information security for G2G transactions, which is the GABAC mechanism, has been developed as part of this study.

### 11.2.2 Second Research Question: Factors that need to be considered in an information security framework for G2G transactions in the EAC.

Three factors were identified as being:

i. Resource constraints: These include financial constraints due to limited national (public sector) budgets allocated to ICT/ e-Government initiatives and inadequate ICT skills;

ii. Legal and regulatory constraints: These include lack of sufficient legislation and national policy frameworks related to information security in e-Government; and

iii. National culture constraints: These include uncoordinated or unstructured national government initiatives related to ICT or e-Government

### 11.2.3 Third Research Question: Sustainable Information Security framework for G2G transactions in the EAC

A unified framework – the TOG framework – was designed to address the information security requirement for G2G transactions in the EAC. The framework comprises of five models which are the technical, operational, governance, process and maturity models.

The Technical Model proposes the use of mechanisms based on open and freely available standards to address the resource constraint factor in the EAC and to contribute towards the sustainability of the model.

The Operational Model proposes mechanisms to address information security within individual MDA organizational units. This addresses both the resource and national culture constraint since each MDA, in implementing the framework can put in place non-technical mechanisms to address information security if there is a lack of technical skills to implement the technical model. At the same time, if the MDA is in a country that lacks central coordination of ICT or e-government initiatives, that MDA can still move towards addressing information security requirements through operational level mechanisms. These mechanisms can then be mapped onto governance level mechanisms as and when they are put in place by governments.

The Governance Model proposes mechanisms to address information security at regional national or policy level within MDAs. This addresses the legal and regulatory constraint by providing guidance on which gaps may exist that require legislation that will address information security requirements. The Governance model allows policy or decision makers to recognize their role in ensuring information security for G2G transactions and implementing their role as and when resources allow.

The process model provides a mechanism to map or to bring together technical, operational and governance mechanisms towards holistic addressing of information security in G2G transactions. The TOG process model, particularly addresses the EAC resource, legal and regulatory and national culture constraints, by using a 'plug and play' approach that allows MDAs and governments to implement the appropriate mechanisms to meet the set of information security requirements using the available resources, and mapping those implementations against mechanisms that are already in place. Implementing of the process model also raises awareness on gaps in information security that the government or MDA can then plan to address when resources are available. Such a process would contribute to sustainability, because it allows the MDA to work within the identified constraints, but still achieve information security for G2G transactions.

The maturity model allows the EAC governments and MDAs to monitor their progress towards improved information security addressing of G2G transactions.

## 11.3 Original contributions

The original contributions of this thesis are:

- An identification of factors in the EAC that need to be addressed for information security in G2G transactions.
- The TOG information security framework for G2G transactions which is a sustainable framework in the EAC context. The framework comprises of five models which are technical, operational, governance, process and maturity models.
- A proposed Governance and Attribute based access mechanism model which is suited to G2G transactions.

## 11.4 Limitations of the study

The findings that have been presented as a result of this research were focused on the EAC. While it may be possible to apply the findings to other countries or regions with the same contextual factors as the EAC, this study has made no conclusions on the generalizability of the findings.

The research methodology used in the study was largely an interpretive one, with the researcher involved in the implementation of the framework that was developed. This approach may introduce an element of bias in the study. This limitation however is weighed against the utility of the research findings, where involvement of the researcher resulted in a good understanding of the research questions, and especially the contextual factors.

The survey undertaken of MDAs in the EAC resulted in only 18 responses out of 50 questionnaires sent out. This is a limitation that could be addressed in future work that bases on the EAC.

The limitation of the evaluation method used for the framework, as discussed in section 10.5 of this thesis, is that the CSF method used is in itself not sufficient to evaluate the novel technical mechanism, which is Governance and Attribute Based Access Control (GABAC) for G2G transactions proposed as part of the technical model of the framework. Such an evaluation of the GABAC mechanism could be a basis for future work in the area of securing G2G transactions.

Finally, the TOG framework was specifically designed with the contextual factors that were discovered in this study in mind. These context issues including resource, legal and regulatory, and national culture constraints are not stagnant and may change with time. Such changes may result in limitations in the applicability of the framework.

## 11.5 Conclusion and Future Work

The general objective of this study was to add to the body of information security and e-Government knowledge by proposing an Information Security framework for G2G transactions in the context of the EAC. This objective has been achieved by the development and application of the TOG framework to a case study from the EAC. This work has been published in a reputable journal.

Although the TOG framework has been evaluated against both EAC and international criteria (ISMS), further work could include investigating how the framework can be generalized for

application outside of the EAC. Future work could include more detailed technical mechanisms with use cases to ease implementation in environments where resources are limited, and improvements to the GABAC mechanism. In the area of information security management, further work could build on and expand the maturity model that is outlined in this study.

## References


Alfawaz, S., May, L., & Mohanak, K. (2007). E-government security in developing countries: A Managerial Conceptual Framework. *40th Hawaii International Conference on System Sciences.*

Bakari, J. K., Tarimo, C. N., Yngstrom, L., & Magnusson, C. (2005). State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case Study. *ICALT 2005*, (pp. 1007-1011).

Barnickel, N., Bottcher, J., & Paschke, A. (2010). Incorporating Semantic Bridges into Information Flow of Cross-Organizational Business Process Models. *6th International Conference on Semantic Systems.* ACM.

Beimel, D., & Peleg, M. (2011). Using OWL and SWRL to represent and reason with situation-based access control policies. *Data & Knowledge Engineering, 70*(6), 596-615.

Bergeron, F., & Bégin, C. (1989). The use of Critical Success Factors in Evaluation of Information Systems. *Jounral of Management Information Systems*, 111-124.

Bernsten, K., & Sampson, J. O. (2005). *Interpretive Research Methods in Computer Science.* Retrieved November 30, 2011, from Norwegian University of Science and Technology: http://www.idi.ntnu.no/~thomasos/paper/interpretive.pdf

Bertino, E. (2003, September). RBAC models — concepts and trends. *Computers & Security, 22*(6), 511-514.

Cabinet Office UK. (2008, December). *HMG Security Policy Framework.* Retrieved June 14th, 2010, from Cabinet office UK: http://www.cabinetoffice.gov.uk/media/111428/spf.pdf

Caralli, R. A. (2004). *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management.* Pittsburgh: Software Engineering Institute - Carnegie Mellon.

Carlsson, S. A. (2006). Towards an Information Systems Design Research Framework: A Critical. *First International Conference on Design Science in Information Systems (DESRIST 2006)*, (pp. 192-212). Claremont.

Cavoukian, A., Taylor, S., & Abrams, M. E. (2010). Privacy by Design: essential for organizational accountability and strong business practices. *Identity in the Information Society, 3*(2).

CEN. (2007). *Network and Information Security Standards Report.* Final Version, ICT Standards Board.

Centre for Governance Institute. (2005). *Governance-Based Access Control (GBAC):Enabling Improved Information Sharing that meets Governance Requirments.* Retrieved June 14th, 2010, from CGI: http://www.cgi.com/cgi/pdf/cgi_whpr_63_gbac_e.pdf

Chango, M. (2007). Challenges to E-Government in Africa South of Sahara: A Critical View, and Provisional Notes for a Research Agenda. *ICEGOV2007* (pp. 384-393). Macao: ACM.

Chaula, J., Yngstrom, L., & Kowalski, S. (2006). Technology as a Tool for Fighting Poverty: How Culture in the Developing World Affect the Security of Information Systems. *Fourth IEEE International Workshop on Technology for Education in Developing Countries* (pp. 66-70). Iringa: IEEE.

Chen, Y. N., Chen, H. M., Huang, W., & Ching, R. K. (2006). E-Government Strategies in Developed and Developing Countries: An Implementation Framework and Case Study. *Journal of Global Information Management, 14*(1), 23-46.

Chunnian, L., Yiyun, H., & Qin, P. (2011). A Study on Technology Architecture and Serving Approaches of Electronic Government System. *Intelligent Computing and Information Science, Communications in Computer and Information Science, 134*(1), 112-117.

CIO Council. (1999, September). Retrieved September 17, 2010, from http://www.cio.gov/documents/fedarch1.pdf

Coetzee, M., & Eloff, J. (2007). A Trust and Context-Aware Control Model for Web Service Conversations. *Lecture Notes in Computer Science, 4657*, 115-124.

Conklin, A. (2007). Barriers to Adoption of e-Government. *40th Hawaii International Conference on System Sciences.*

Cunningham, E. (2007, July 4). Rwanda Leading Africa in ICT Revolution. *IPS Africa*.

Da Veiga, A. (2008). *Cultivating and assessing information security culture, PhD thesis.* Retrieved December 1, 2011, from University of Pretoria: http://upetd.up.ac.za/thesis/available/etd-04242009-165716

Dada, D. (2006). The Failure of e-Government in Developing Countries: A Literature Review. *The Electronic Journal of E-Government in Developing Countries, 26.*

Dagada, R., Eloff, M. M., & Venter, L. M. (2009). Too Many Laws but very little progress-Is South African Highly Acclaimed Information Security Legislation Redundant? *Informaton Security South Africa (ISSA09).*

Davies, J., & Jeremy, G. (2009, June). Formal Methods for Future Interoperability. *inroads — SIGCSE Bulletin, 41*(2), 60-64.

De Capitani di Vimercati, S., & Samarati, P. (2005). New Directions in Access Control. In J. Kowalik, J. Gorski, & A. Sachenko (Eds.), *Cyberspace Security and Defense: Research Issues* (pp. 279-298). Gdansk: Kluwer Academic Publishers.

De Jager, A., & Van Reijswoud, V. (2007). E-governance in the developing world in action: the case of DistrictNet in Uganda. *World Hospitals and Health Services, 43*(1), 32-41.

De Jager, A., & Van Reijswoud, V. (2007). E-governance in the developing world in action: the case of DistrictNet in Uganda. *World Hospitals and Health Services, 43*(1), 32-41.

de Villiers, M. (2005). Three approaches as pillars for interpretive Information Systems research:development research, action research and grounded theory. *Annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries* , (pp. 142-151).

Demchenko, Y., Gommans, L., & de Laat, C. (2007). Extending Role Based Access Control Model for Distributed MultiDomain Applications. In P. a. New Approaches for Security, H. Venter, M. L. Eloff, J. Eloff, & R. von Solms (Eds.), *New Approaches for Security, Privacy and Trust in Complex environments* (pp. 301-312). Boston: Springer.

Department of Premier and Government, Tasmania. (2009). *Tasmanian Government Information Security Framework.* Hobart: e-Government Office.

Domingue, J., Gutierrez, L., Cabral, L., Rowlatt, M., Davies, R., & Galizia, S. (2004). *WP 9: Case Study eGovernment D9.3 e-Government Ontology.* Retrieved March 30, 2011, from DIP: http://dip.semanticweb.org

Durbeck, S., Schillinger, R., & Kolter, J. (2007). Security Requirements for a Semantic Service-oriented Architecture. *The Second International Conference on Availability, Reliability and Security* (pp. 366-373 ). IEEE Computer Society.

EAC. (2009). *Protocol on the establishment of the East African Community Common Market.* The East African Community.

East African Community. (2006). *EAC Development Strategy 2006 – 2010.*

East African Community Secretariat. (2005). *Regional e-Government Framework.*

Ezz, I. E., & Themistocleous, M. (2005). Investigating the Barriers to G2G Adoption. *e-Government Workshop.* London: Brunel University.

Fan, J., & Zhang, P. (2007). A case study of G2G information sharing in the Chinese context. *8th annual international conference on Digital government research: bridging disciplines & domains.* Philadelphia: Digital Government Society of North America .

Galpin, V. (2008). Africa, Women in Technology in Sub Saharan. In F. B. Tan, *Global Information Technologies: Concepts, Methodologies, Tools and Applications* (pp. 1681-1688). IGI Global.

Gerber, M., & von Solms, R. (2008). Information security requirements – Interpreting the legal aspects. *Computers & Security, 27*, 1 2 4 – 1 3 5.

GITOC. (2009). *Government-Wide Enterprise Architecture (GWEA) Framework Revision 1.2.* Government Information Technology Officer's Council of South Africa. Pretoria: GITOC South Africa.

Government of Rwanda. (2010). An Integrated ICT led Socio-Economic Development Plan for Rwanda 2006 - 2010: The NICI 2010 Plan.

Gregoriades, A., & Sutcliffe, A. (2008). A Socio-technical Approach to Business Process Simulation. *Decision Support Systems, 45*(4), 1017-1030.

Guarda, P., & Zannone, N. (2009, February). Towards the development of privacy-aware systems. *Information and Software Technology, 51*(2), 337-350 .

Gutiérrez, C., Rosado, D. G., & Fernández-Medina, E. (2009). The practical application of a process for eliciting and designing security in web service systems. *Information and Software Technology , 51*, 1712–1738.

Hayat, Z., Reeve, J., & Boutle, C. (2007). Ubiquitous security for ubiquitous computing. *Information Security Technical Report, 12*(3), 172-178.

He, Q., & Antón, A. I. (2009). Requirements-based Access Control Analysis and Policy Specification (ReCAPS). *Information and Software Technology, 51*, 993–1009.

Heeks, R. (2002, August). eGovernment in Africa: Promise and Practice. *Information Polity, 7*(2,3), 97-114.

Hellsten, K. S. (2010). E-Government: A Case Study of East African Community Initiative. In T. Dumova, & R. Fiordo (Eds.), *Handbook of Research on Social Interaction Technologies and Collaboration Software: Concepts and Trends* (pp. 80-90). IGI Global.

Hellström, J. (2010). *The Innovative Use of Mobile Applications in East Africa.* SIDA.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly, 28*(1), 75-105.

Hu, V. C., Quirolgico, S., & Scarfone, K. (2008). Access Control Policy Composition for Resource Federation Networks Using Semantic Web and Resource Description Framework (RDF). *International Computer Symposium (ICS 2008).* Taiwan.

Ibrahim, M., & Long, G. (2007, February 27). *Service-Oriented Architecture and Enterprise Architecture, Part 1: A framework for understanding how SOA and Enterprise Architecture work together.* Retrieved September 19, 2010, from IBM: http://www.ibm.com/developerworks/webservices/library/ws-soa-enterprise1/

International Telecommunications Union. (2011, December 31). *The World in 2011: ICT Facts and Figures.* Retrieved October 11, 2012, from International Telecommunications Union: http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf

Islam, S., Mouratidis, H., & Jurjens, J. (2011). A framework to support alignment of secure software engineering with legal regulations. , 10(3),. *Software and Systems Modeling, 10*(3), 369-397.

ISO. (2008). *Health informatics -- Information security management in health using ISO/IEC 27002.* Geneva: International Organization for Standardization.

ISO/IEC. (2005a). *Information technology — Security techniques — Information security management systems — Requirements.* Geneva: International Organization for Standardization.

ISO/IEC. (2005b). *ISO/IEC 27002:2005 - Information technology -- Security techniques -- Code of practice for information security management.* Geneva: International Organization for Standardization.

ISO/IEC. (2009). *Information Technology- Security techniques-Information security management systesm - Overview and vocabulary.* Geneva: International Organization for Standardization.

Janssen, M., & Scholl, H. J. (2007). Interoperability for Electronic Governance. *ICEGOV2007*, (pp. 45-48). Macao.

Jeong, D., & Han, Y. (2006). Resolving the Semantic Inconsistency Problem for Ubiquitous RFID Applications. *UIC, 4159*, pp. 1134-1143.

Kaaya, J. (2003). Implementing e-Government services in East Africa: Assessing Status through Content Analysis of Government Websites. *Electronic Journal of e-Government, 2*(1), 39-54.

Kaliontzoglou, A., Karantjias, T., & Polemi, D. (2008). Building Innovative, Secure and Interoperable E-Government Services. IGI Global.

Kanyesigye, F. (2011, January 18). Rwanda: Third Phase ICT Action Plan Unveiled. *The New Times*.

Karokola, G., & Yngstrom, L. (2009). Discussing e-Government Maturity Models for Developing World - Security View. *Information Security South Africa (ISSA09).*

Kayworth, T., & Whitten, D. (2010). Effective Infomation Security requires a balance of social and technology factors. *MIS QUARTERLY EXECUTIVE, 9*(3), 163-175.

Kokolakis, S. A., & Kiountouzis, E. A. (2000). Achieving Interoperability in a Multiple-Security- Policies Environment. *Computers & Security, 19*(3).

Lee, T. Y., Yee, P. K., & Cheung, D. W. (2009). E-government Data Interoperability Framework in Hong Kong. *International Conference on Interoperability for Enterprise Software and Applications China* (pp. 239-244). Beijing: IEEE.

Loser, K., Nolte, .., Herrmann, T., & te Neues, H. (2011). Information security management systems and socio-technical walkthroughs. *1st Workshop on Socio-Technical Aspects in Security and Trust (STAST),* (pp. 45 - 51 ).

Lowery, L. M. (2003). *Developing a Successful E-Government Strategy*. Retrieved October 15, 2010, from United Nations Public Administration Network: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan000343.pdf

Marin-Lopez, R., Pereniguez, F., Lopez, G., & Perez-Mendez, A. (2011). Providing EAP-based Kerberos pre-authentication and advanced authorization for network federations. *Computer Standards & Interfaces, 33*(5), 494-504.

McKenzie, R., Crompton, M., & Wallis, C. (2008). Use Cases for Identity Management in e-Government. *Security & Privacy, 6*(2), 51-57.

MEGA-TECH, Inc. (2006). *The National ICT Master Plan and e-Government Network Feasibility Study in Uganda.*

Ministry of Finance and Economic Planning - Rwanda. (2010). *Annex II-7: State expenditure per Budget Agency and Programme 2010/2013.*

Ministry of Communications and Transport. (2003). *National Information and Communications Technologies Policy.* United Republic of Tanzania, Dar es Salaam.

Ministry of Finance and Economic Affairs - Tanzania. (2010a). *Hali ya uchumi ya Taifa katika Mwaka 2009 Jedwali Na.A.*

Ministry of Finance and Economic Affairs - Tanzania. (2010b). *Volume IV- Public expenditure Estimates, Development Votes for 2010/11.*

Ministry of Finance and Economic Affairs - Tanzania. (2010c, July). *Taarifa Kwa Umma - Mfumo Mpya wa Malipo Serikalini.* Retrieved September 30, 2010, from Ministry of Finance: http://www.mof.go.tz/mofdocs/anouncement/TANGAZO%20MAALUM-kiswahili2.pdf

Ministry of Information and Communication Technology - Uganda. (2008a). The Electronic Transactions Bill.

Ministry of Information and Communication Technology - Uganda. (2008b). The Electronic Signatures Bill.

Ministry of the Presidency, Spain. (2010). *Spanish National Interoperability Framework.*

Ministry of Works, Housing and Communication - Uganda. (2004). *E-Government Strategy and Action Plan.* Draft Version 1.1, Republic of Uganda.

Ministry of Works, Housing and Communications - Uganda. (2003, October). National Information and Communication Technology Policy.

Ministry of Works, Housing and Communications. (2003, October). *National Information and Communication Technology Policy.*

Msuya, E. (2010, August). Challenges in Data Collection, consolidation and reporting for local government authorities in Tanzania. *REPOA Brief.*

Mwangi, W. (2006). The Social Relations of e-Government Diffusion in Developing Countries: The Case of Rwanda. *International conference on Digital government research* (pp. 199-208). ACM.

National Institute of Statistics of Rwanda. (2010). *GDP Annual Estimates for 2009 based on 2006 benchmark.*

National Research Council. (2002). *Information Technology Research, Innovation and E-Government.* Washington DC: National Academy Press.

Ndahiro, M. (2009). Electronic/Mobile Government in Africa:Progress Made and Challenges Ahead. *UN Public Administration Programme.* Addis Ababa: Rwanda Development Board.

NIST. (2006). *Minimum Security Requirements for Federal Information and Information Systems.* National Institute of Standards and Technology, Computer Security Division.

NIST. (2009). *Recommended Security Controls for Federal Information Systems and Organizations.* National Institute of Standards and Technology, Computer Security Division.

OASIS. (2005). *SAML V2.0 documentation.* Retrieved from Organization for the Advancement of Secure Information Systems: http://docs.oasis-open.org/security/saml/v2.0/

OASIS. (2006). *ebXML Business Process Specification Schema Technical Specification v2.0.4.* Retrieved November 11, 2011, from OASIS: http://docs.oasis-open.org/ebxml-bp/2.0.4/OS/spec/ebxmlbp-v2.0.4-Spec-os-en-html/ebxmlbp-v2.0.4-Spec-os-en.htm

OASIS. (2008). *Electronic Court Filing Version 4.0.* Draft Committee Report.

OASIS. (2010). *OASIS Standards and Other Approved Work.* Retrieved June 15, 2010, from OASIS: http://www.oasis-open.org/specs/

OASIS. (2010a, April 12). *Avoiding the Pitfalls of eGovernment.* Retrieved June 30, 2010, from OASIS: http://oasis-egov.org/sites/oasis-egov.org/files/eGov_Pitfalls_Guidance%20Doc_v1.pdf

OASIS. (2010b). *OASIS Standards and Other Approved Work.* Retrieved June 15, 2010, from OASIS: http://www.oasis-open.org/specs/

O'Brien, L., Merson, P., & Bass, L. (2007). Quality Attributes for Service-Oriented Architectures. *International Workshop on Systems Development in SOA Environments* (p. 3). Washington DC: IEEE Computer Society.

OECD. (1980, September). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Retrieved June 11, 2010, from OECD: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

OECD. (2002). *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.* Retrieved June 13th, 2010, from Organisation for Economic Cooperation and Development: http://www.oecd.org/dataoecd/16/22/15582260.pdf

OECD. (2007, June). *OECD Recommendation on Electronic Authentication and Guideline on Electronic Authentication.* Retrieved June 11th, 2010, from http://www.oecd.org/dataoecd/32/45/38921342.pdf

Office of the Prime Minister. (2010, April). *National Development Plan 2010/2011 - 2014/2015.* Retrieved October 10, 2010, from Office of the Prime Minister, Republic of Uganda: http://www.opm.go.ug/manage/pdfs/ndp_april_2010_port.pdf

Olivier, M. S. (2004). *Information Technology Research: A Practical guide for Computer Science and Informatics* (2nd ed.). Pretoria: Van Schaik.

Parliament of Tanzania. (2007). The Written Laws (Miscellanous Amendments) Act - Part IX. Tanzania.

Parliament of Uganda. (2009). National Information Technology Authority, Uganda Act.

Parliament of Uganda. (2010). The Computer Misuse Act.

President's Office. (2009). *Tanzania e-Government Strategy.* United Republic of Tanzania.

Republic of Rwanda. (2003, May). Consitution of the Republic of Rwanda.

Republic of Uganda. (1995). Constitution of the Republic of Uganda.

Republic of Uganda. (2010). *Approved Estimates of Revenue and Expenditure (Recurrent and Development) FY 2010/11.* Ministry of Finance.

Rezaian, B. (2007). African Development: Challenges and Opportunities in Sub Saharan Africa. In M. Gascó-Hernández, F. Equiza-López, & M. Acevedo-Ruiz (Eds.), *Information Communication Technologies and Human Development: Opportunities and Challenges.* IGI Global.

RITA. (2006). *Final Report on technical standards and guidelines for e-government.* Rwanda Information Technology Authority.

Rose, W. R., & Grant, G. G. (2010, January). Critical issues pertaining to the planning and implementation of E-Government initiatives. *Government Information Quarterly, 27*(1), 26-33.

Ross, S. J. (2007). Automating Compliance. *Information Systems Control Journal, 5*.

Rwangoga, N. T., & Baryayetunga, A. P. (2007). E-Government for Uganda: Challenges and Opportunities. *International Journal for Computing and ICT Research, 1*(1), 36-46.

Saidam, S. (2007). Knowledge and E-Governance Building in Conflict Affected Societies: Challenges and Mechanisms. *1st international conference on Theory and practice of electronic governance* (pp. 341-344 ). Macao: ACM.

Scholl, H. J., & Pardo, T. A. (2010). Data-Centric Workflows in Government: A New Avenue of Research? *11th Annual International Digital Government Research Conference,* (pp. 138-146).

Schuppan, T. (2009). E-Government in developing countries: Experiences from sub-Saharan Africa. *Government Information Quarterly, 26*, 118-127.

Segole, J., & Needham, W. (2009, June 30). Retrieved September 19, 2010, from GITOC: www.gitoc.gov.za/gitoc_web/index.php?

Seidenspinner, M., & Theuner, G. (2007). Intercultural aspects of online communication a comparison of mandarin-speaking, US, Egyptian and German user preferences. *Journal of Business Economics and Management, 8*(2).

Shen, H., & Hong, F. (2006). An Attribute-based Access Control Model for Web Services. *Seventh International Conference on Parallel and Distributed Computing Applications and Technologies.* IEEE.

Simon, B., Laszlo, Z., Goldschmidt, B., Kondorosi, K., & Risztics, P. (2010). Evaluation of WS-* Standards Based Interoperability of SOA Products for the Hungarian e-Government Infrastructure. *4th International Conference on Digital Society.*

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*, 267-270.

SITA. (2007). *Minimum Interoperability Standards for Information Systems in Government.* Retrieved June 12th, 2010, from SITA: http://www.sita.co.za/standard/MIOSv4.12007.pdf

Sprott, D., & Wilkes, L. (2004, January). Understanding Service-Oriented Architecture. *Microsoft Architect Journal*.

Tanzania Communications Regulatory Authority. (2010). *Report on Internet and Data Services in Tanzania: A Supply-Side Survey.* Dar es Salaam: TCRA.

Tarimo, C. N., Yngstrom, L., & Kowalski, S. (2005). An Approach to Enhance ICT Infrastrcutures Security Through Legal, Regulatory Influence. *ISSA 2005*, (pp. 1-12).

The East African Community. (2009). *Protocol on the establishment of the East African Community Common Market.*

The Guardian Newspaper. (2009, September 27). Five men who stole TRA's $77m nailed . *Guardian on Sunday.*

Thompson, M., & Walsham, G. (2010). ICT research in Africa: need for a strategic developmental focus. *Information Technology for Development, 16*(2), 112-127.

UN Economic Commission for Africa. (2007). *National Information and Communication Infrastrcuture (NICI) e-Strategies : Beat Practices and Lessons Learnt.* Addis Ababa: UN Economic Commission for Africa.

UNCTAD. (2010, June 21). *East African community adopts framework for cyberlaws to foster regional trade, investment.* Retrieved January 15, 2011, from UNCTAD: http://www.unctad.org/templates/webflyer.asp?docid=13379&intItemID=1528&lang=1

United Nations. (2008). *UN eGovernment Survey 2008: From eGovernement to Connected Governance.*

United Nations. (2010). *2010 Global e-Government Survey: Leveraging E-government at a Time of Financial and Economic Crisis.*

United Republic of Tanzania. (2000). Constitution of the United Republic of Tanzania of 1977.

United Republic of Tanzania. (2009). *Tanzania e-Government Strategy.*

United Republic of Tanzania, President's Office. (2008). *Tanzania e-Government Strategy.* Presidents Office - Public Service Management. Dar es Salaam: -.

United States Congress. (2002). Tit. III, E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002) (superseding Tit. X, Homeland Security Act of 2002, Pub. L. 107-296 (Nov. 25, 2002)), codified at 44 U.S.C. § 3541 et seq.[2.

W3C. (2004, February 11). *Web Services Glossary*. Retrieved July 15, 2010, from W3C Working Group: http://www.w3.org/TR/ws-gloss/

W3C. (2009, October 27). *OWL 2 Web Ontology Language Guide.* Retrieved January 12, 2011, from W3C: http://www.w3.org/TR/owl2-overview/

Wangwe, C. K., Eloff, M. M., & Venter, L. (2008a). A Proposed Implementation of SAML V2.0 in an e Government Setting. *IST Africa.* Windhoek: IIMC International Information Management Corporation.

Wangwe, C. K., Eloff, M. M., & Venter, L. (2008b). Towards A Context-Aware Access Control Framework in Web Service Transactions. *ISSA08.* Johannesburg.

Wangwe, C. K., Eloff, M. M., & Venter, L. (2009). E-Government Readiness: An Information Security Perspective from East Africa. In P. C. Cunningham (Ed.), *IST-Africa.* Kampala: IIMC International Information Management Corporation.

Warner, J., Atluri, V., Mukkamala, R., & Vaidya, J. (2007). Using Semantics for Automatic Enforcement of Access Control Policies Among Dynamic Coalitions. *SACMAT*, (pp. 235-244).

Weik, M. (2001). *Computer Science and Communications Dictionary.* Springer.

Wirtenberg, J., Russell, W. G., & Lipsky, D. (2008). *The Sustainable Enterprise Fieldbook: When It all Comes Together.* Amacom.

Zarei, B., & Ghapanchi, A. (2008). Guidelines for government-to-government initiative architecture in developing countries. *International Journal of Information Management, 28*, 277– 284.

Zissis, D., & Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture. *Government Information Quarterly, 28*(2), 239-251.

## APPENDIX A Questionnaire used for Data Collection.

The following questionnaire was used to collected data from MDAs in Tanzania, Uganda and Rwanda**.**

**Carina K. Wangwe**
**P.O. Box 60049**
**Dar es Salaam**
**Tanzania**

Dear Sir/Madam,

I am undertaking a PhD research project to develop an information security framework for electronic transactions in government and related agencies. This research is being conducted in the countries within the East African Community. To this end, I kindly request you to complete the following short questionnaire. It should take no longer than 15 minutes of your time.

The information provided by you shall remain confidential and shall be reported in summary format only.

Please return the completed questionnaire to me by email (carina.wangwe@gmail.com) or to the person who handed it to you.

Should you have any queries or comments regarding this questionnaire, please contact by phone on +255 754 600512 or email: carina.wangwe@gmail.com.

Yours sincerely

Carina K. Wangwe
PhD Student

University of South Africa

1. What is the nature of your organisation

Central Government ☐

Government Agency ☐

Parastatal Organisation ☐

Other ☐

2. What is your role within your organisation

Managerial (IT) ☐

Managerial (Other) ☐

IT Support ☐

Operations ☐

3. Does your organisation have a documented Information (or ICT) Security Policy?

Yes ☐

No ☐

4. How does your organisation transact with other agencies/ government departments (You can choose more than one answer)

Manually ☐

Email ☐

Access to Computer Systems of other agencies (Online or remotely) ☐

Other _____

_____

5. What kind of information is involved in the transactions (You can choose more than one answer

Payment/ financial ☐

Confidential information ☐

Other _____

_____

6. What are the main concerns with electronic transactions

Fraud ☐

Network breakdowns ☐

Other _____

7. For data exchange what security e.g. encryption is in place

_____

_____

_____

8. Does your organisation have any binding agreements with regards to security of information with other transacting partners

Yes ☐

No ☐

9. a) Is there a common format for data exchange is used e.g. SWIFT for financial transactions?

Yes ☐

No ☐

b) If Yes, what common format is used?

_____

_____

_____

10. a) Is there a common basis for terms/ language used in transactions e.g. a law or regulations that define terms?

Yes ☐

No ☐

b) If Yes, what is the common basis?

_____

_____

_____

11. Please enter your views about the need for standards for security of information exchanges within government or between government agencies and other parties.

_____

_____

_____

**Thank you for your co-operation.**

## APPENDIX B Web Service Using WS-Security for Case Study Transaction

The following are three files used to implement a web service for the G2G transaction described in the case study in chapter nine.

i) Configuration File:

```
<?xml version="1.0" ?>

- <!--

            Coded & Tested by G. Msangi, R.Mtendamema &C.K.Wangwe.

  -->

- <configuration>

- <configSections>

- <sectionGroup name="system.web.extensions"
type="System.Web.Configuration.SystemWebExtensionsSectionGroup,
System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35">

- <sectionGroup name="scripting"
type="System.Web.Configuration.ScriptingSectionGroup,
System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35">

<section name="scriptResourceHandler"
type="System.Web.Configuration.ScriptingScriptResourceHandlerSection,
System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35" requirePermission="false"
allowDefinition="MachineToApplication" />

- <sectionGroup name="webServices"
type="System.Web.Configuration.ScriptingWebServicesSectionGroup,
System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35">

<section name="jsonSerialization"
type="System.Web.Configuration.ScriptingJsonSerializationSection,
System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35" requirePermission="false"
allowDefinition="Everywhere" />

<section name="profileService"
type="System.Web.Configuration.ScriptingProfileServiceSection,
System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35" requirePermission="false"
allowDefinition="MachineToApplication" />

<section name="authenticationService"
type="System.Web.Configuration.ScriptingAuthenticationServiceSection,
System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
```

```
PublicKeyToken=31BF3856AD364E35" requirePermission="false"
allowDefinition="MachineToApplication" />

<section name="roleService"
type="System.Web.Configuration.ScriptingRoleServiceSection,
System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35" requirePermission="false"
allowDefinition="MachineToApplication" />

</sectionGroup>

</sectionGroup>

</sectionGroup>

</configSections>

<appSettings />

<connectionStrings />

- <system.web>

- <!--

            Set compilation debug="true" to insert debugging

symbols into the compiled page. Because this

affects performance, set this value to true only

during development.



  -->
```

```
- <compilation debug="false">

- <assemblies>

<add assembly="System.Core, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=B77A5C561934E089" />

<add assembly="System.Data.DataSetExtensions, Version=3.5.0.0,
Culture=neutral, PublicKeyToken=B77A5C561934E089" />

<add assembly="System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35" />

<add assembly="System.Xml.Linq, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=B77A5C561934E089" />

</assemblies>

</compilation>

- <!--             The <authentication> section enables configuration
```

```
of the security authentication mode used by

ASP.NET to identify an incoming user.



  -->

<authentication mode="Windows" />

- <!--              The <customErrors> section enables configuration

of what to do if/when an unhandled error occurs

during the execution of a request. Specifically,

it enables developers to configure html error pages

to be displayed in place of a error stack trace.



<customErrors mode="RemoteOnly" defaultRedirect="GenericErrorPage.htm">

<error statusCode="403" redirect="NoAccess.htm" />

<error statusCode="404" redirect="FileNotFound.htm" />

</customErrors>



  -->

- <pages>

- <controls>

<add tagPrefix="asp" namespace="System.Web.UI"
assembly="System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35" />

<add tagPrefix="asp" namespace="System.Web.UI.WebControls"
assembly="System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35" />

</controls>

</pages>

- <httpHandlers>

<remove verb="*" path="*.asmx" />

<add verb="*" path="*.asmx" validate="false"
type="System.Web.Script.Services.ScriptHandlerFactory,
System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35" />
```

```
<add verb="*" path="*_AppService.axd" validate="false"
type="System.Web.Script.Services.ScriptHandlerFactory,
System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35" />

<add verb="GET,HEAD" path="ScriptResource.axd"
type="System.Web.Handlers.ScriptResourceHandler, System.Web.Extensions,
Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35"
validate="false" />

</httpHandlers>

- <httpModules>

<add name="ScriptModule" type="System.Web.Handlers.ScriptModule,
System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35" />

</httpModules>

- <webServices>

<soapServerProtocolFactory
type="Microsoft.Web.Services3.WseProtocolFactory,
Microsoft.Web.Services3, Version=3.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35" />

</webServices>

</system.web>

- <system.codedom>

- <compilers>

- <compiler language="c#;cs;csharp" extension=".cs" warningLevel="4"
type="Microsoft.CSharp.CSharpCodeProvider, System, Version=2.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089">

<providerOption name="CompilerVersion" value="v3.5" />

<providerOption name="WarnAsError" value="false" />

</compiler>

</compilers>

</system.codedom>

- <!--

        The system.webServer section is required for running ASP.NET
AJAX under Internet

Information Services 7.0.  It is not necessary for previous version of
IIS.
```

```
  -->

- <system.webServer>

<validation validateIntegratedModeConfiguration="false" />

- <modules>

<remove name="ScriptModule" />

<add name="ScriptModule" preCondition="managedHandler"
type="System.Web.Handlers.ScriptModule, System.Web.Extensions,
Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" />

</modules>

- <handlers>

<remove name="WebServiceHandlerFactory-Integrated" />

<remove name="ScriptHandlerFactory" />

<remove name="ScriptHandlerFactoryAppServices" />

<remove name="ScriptResource" />

<add name="ScriptHandlerFactory" verb="*" path="*.asmx"
preCondition="integratedMode"
type="System.Web.Script.Services.ScriptHandlerFactory,
System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35" />

<add name="ScriptHandlerFactoryAppServices" verb="*"
path="*_AppService.axd" preCondition="integratedMode"
type="System.Web.Script.Services.ScriptHandlerFactory,
System.Web.Extensions, Version=3.5.0.0, Culture=neutral,
PublicKeyToken=31BF3856AD364E35" />

<add name="ScriptResource" preCondition="integratedMode"
verb="GET,HEAD" path="ScriptResource.axd"
type="System.Web.Handlers.ScriptResourceHandler, System.Web.Extensions,
Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" />

</handlers>

</system.webServer>

- <runtime>

- <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">

- <dependentAssembly>

<assemblyIdentity name="System.Web.Extensions"
publicKeyToken="31bf3856ad364e35" />

<bindingRedirect oldVersion="1.0.0.0-1.1.0.0" newVersion="3.5.0.0" />

</dependentAssembly>
```

```
- <dependentAssembly>

<assemblyIdentity name="System.Web.Extensions.Design"
publicKeyToken="31bf3856ad364e35" />

<bindingRedirect oldVersion="1.0.0.0-1.1.0.0" newVersion="3.5.0.0" />

</dependentAssembly>

</assemblyBinding>

</runtime>

- <!--  Configuring Policy: The entry must be placed here in

    Web.config for WSE Policy statement to be used in this virtual
directory



  -->

- <microsoft.web.services>

- <policy>

- <receive>

<cache name="PensionerPayrollPolicy.xml" />

</receive>

</policy>

</microsoft.web.services>

</configuration>
```

ii) Policy File

```
<?xml version="1.0" encoding="utf-8" ?>
<policies
xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility"
xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/12/secext"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy"
xmlns:wse="http://schemas.microsoft.com/wse/2003/06/Policy">

<wsp:Policy wsu:Id="GovtPension.asmx">
<Integrity wsp:Usage="wsp:Required"
xmlns="http://schemas.xmlsoap.org/ws/2002/12/secext">
<TokenInfo>
<SecurityToken>
<TokenType>UsernameToken</TokenType>
</SecurityToken>
<Claims>
<!-- Role Value Interms of value="MACHINE_NAME\Group Name" />  --
>
<wse:Role value="GovtPenSrv\PRegistration" />
<wse:Role value="GovtPenSrv\PRunPayroll" />
```

```
<wse:Role value="GovtPenSrv\PEditDetails" />
</Claims>
</TokenInfo>
<MessageParts
      xmlns:rp="http://schemas.xmlsoap.org/rp"
Dialect="http://schemas.xmlsoap.org/2002/12/wsse#part">
wsp:Body()
</MessageParts>
</Integrity>
</wsp:Policy>

<policyDocument
xmlns="http://schemas.microsoft.com/wse/2003/06/Policy">
<!--<mappings> element maps a resource to a policy assertion by
policy ID />  -->
<mappings>
<map to="http://localhost/GovtPension.asmx">
<default policy="#GovtPension.asmx" />
</map>
</mappings>
</policyDocument>
</policies>
```

iii) Web Service

```
using System;
using System.Collections;
using System.ComponentModel;
using System.Data;
using System.Linq;
using System.Web;
using System.Web.Services;
using System.Web.Services.Protocols;
using System.Xml.Linq;
using System.Data;
using System.Data.SqlClient;

using Microsoft.Web.Services3.Security;
using Microsoft.Web.Services3.Security.Tokens;

namespace govtpensioner
{
    /// <summary>
    /// Summary description for Service1
    /// </summary>
    [WebService(Namespace = "http://tempuri.org/")]
    [WebServiceBinding(ConformsTo = WsiProfiles.BasicProfile1_1)]
    [ToolboxItem(false)]
    // To allow this Web Service to be called from script, using
ASP.NET AJAX, uncomment the following line.
    // [System.Web.Script.Services.ScriptService]

        //CLass to Authenticate Web Service Consumers
public class WseSecurityHelpers
         {

public static UsernameToken GetUsernameToken(SoapContext context)
```

```
              {
if (context == null)
throw new Exception("Only SOAP requests are permitted.");

                  // Make sure there's a token
if (context.Security.Tokens.Count == 0)
                    {
throw new SoapException("Missing security token",
SoapException.ClientFaultCode);


                     }
foreach (UsernameToken tok in context.Security.Tokens)
return tok;
throw new Exception("UsernameToken not supplied");
                }
         }



//Classs to create new Pensioner. This class is used by
webservice Method called
        //[Create Pensioner] to actual create a Pensioner.

public class NewPensioner
    {
private string CHQNo;
private string FName;
private string MName;
private string SName;
private char Gender;
private string Acno;
private int Brno;
private float Amount;
public NewPensioner(string CHQNo,string FName, string MName,
string SName, char Gender, string Acno, int Brno, float Amount)
        {
            this.CHQNo = CHQNo;
            this.FName = FName;
            this.MName = MName;
            this.SName = SName;
            this.Gender = Gender;
            this.Acno = Acno;
            this.Brno = Brno;
            this.Amount = Amount;
        }
public string NP()
        {
            //CODE TO CONNECT AND CREATE PENSIONER HERE
            SqlConnection con = new SqlConnection("connection
string");
            SqlCommand cmd = new SqlCommand();
            cmd.Connection = con;
            cmd.CommandType = CommandType.StoredProcedure;
            cmd.CommandText = "SP_NEW_PENSIONER";
```

```
            SqlParameter par1 = new SqlParameter("CHQNo",
SqlDbType.Int, 10);
            par1.Value = this.CHQNo;
cmd.Parameters.Add(par1);
//more parameters here.
con.Open();
cmd.ExecuteScalar();
con.Close();

        }
    }

//Classs to run Payroll. This class is used by webservice Method
called
    //[Run Payroll] to actual create run a Payroll.

public class RPayroll
    {
private int Month;
private int Year;

public RPayroll(int Month, int Year)
        {
            this.Month = Month;
            this.Year = Year;
        }

public string RunP()
        {
            SqlConnection con = new SqlConnection("connection
string");
            SqlCommand cmd = new SqlCommand();
            cmd.Connection = con;
            cmd.CommandType = CommandType.StoredProcedure;
            cmd.CommandText = "SP_RUN_PENSION";
            SqlParameter par1 = new SqlParameter("pMonth",
SqlDbType.Int, 2);
            par1.Value = this.Month;
cmd.Parameters.Add(par1);
            SqlParameter par2 = new SqlParameter("pYear",
SqlDbType.Int, 4);
            par1.Value = this.Year;
cmd.Parameters.Add(par2);
con.Open();
cmd.ExecuteScalar();
con.Close();
        }
    }

//Classs to Edit Pensioner. This class is used by webservice
Method called
//[Edit Pensioner] to actual edit a Pensioner.
public class EPensioner
    {
private int PNo;
private string Acno;
private int Brno;
```

```
private float Amount;

public EPensioner(int PNo,string Acno,int Brno,float Amount)
        {
            this.PNo = PNo;
            this.Acno = Acno;
            this.Brno = Brno;
            this.Amount = Amount;
        }

public string EP()
        {
            //Code to edit pensioner details will be coded here
        }
    }

//Classs to change Pensioner Status. This class is used by
webservice Method called
//[ChangePenStatus] to actual change Pensioner status.
public class CPStatus
    {
private int PNo;
private char status;
private string reason;

public CPStatus(int PNo,char status,string reason)
        {
            this.PNo = PNo;
            this.status = status;
            this.reason = reason;
        }

public string CS()
        {
            //Code to change pensioner status will be coded here
        }
    }

public class Service1 : System.Web.Services.WebService
    {
        //Webservice Method to Create new Pensioner.
        //The Particular to pass is as indicated in the Method
Parameter.
        [WebMethod]
public string CreatePensioner(string CHQNo, string FName, string
MName, string SName, char Gender, string Acno, int Brno, float
Amount, int AuthorizationCode)
        {
            UsernameToken tok =
WseSecurityHelpers.GetUsernameToken(RequestSoapContext.Current);

            //Check if the Web Service Consumer is Allowed to
create new Pensioner as defined in the web Policy
if (!tok.Principal.IsInRole(string.Format("{0}\\CreatePensioner",
Dns.GetHostName())))

throw new Exception("access denied");
```

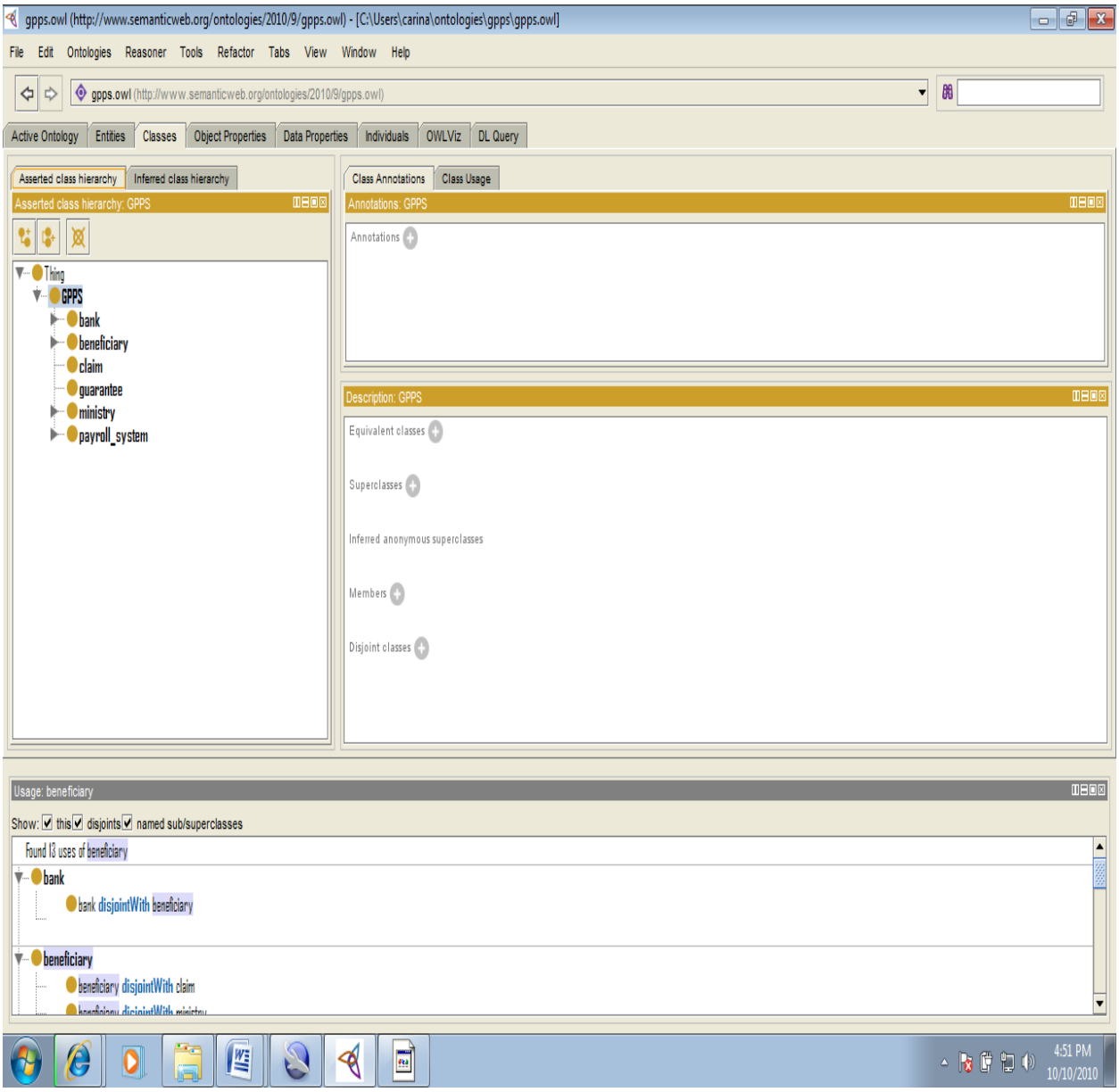
```
            NewPensioner Pensioner = new NewPensioner(CHQNo,
FName, MName, SName, Gender, Acno, Brno, Amount);
success = Pensioner.NP(); //Call Method to Create New Pensioner.
return success;

        }

        //Webservice Method to Edit Pensioner Deatils
        //Details to Edit includes:Account Number,Account
Name,Branch Number
        //and Amount for a given Pensioner.
        [WebMethod]
public string EditPensioner(int PNo, string Acno, int Brno, float
Amount, int AuthorizationCode)
        {
            UsernameToken tok =
WseSecurityHelpers.GetUsernameToken(RequestSoapContext.Current);

            //Check if the Web Service Consumer is Allowed to
change Pensioner Details as defined in the web Policy
if (!tok.Principal.IsInRole(string.Format("{0}\\Edit Pensioner",
Dns.GetHostName())))

throw new Exception("access denied");

            EPensioner edit = new
EPensioner(PNo,Acno,Brno,Amount);
success = edit.EP(); //Call Method to Edit Pensioner Details
return success;
        }

        //Webservice Method used to change the Pensioner
Status.Reason must also be passed
        [WebMethod]
public string ChangePenStatus(int PNo, char status, string
reason, int AuthorizationCode)
        {
            //Authenticate Webservice Consumer
            UsernameToken tok =
WseSecurityHelpers.GetUsernameToken(RequestSoapContext.Current);

            //Check if the Web Service Consumer is Allowed to
change Pensioner Status as defined in the web Policy
if (!tok.Principal.IsInRole(string.Format("{0}\\ChangePenStatus",
Dns.GetHostName())))

throw new Exception("access denied");
            CPStatus   CPS = new CPStatus(PNo,status,reason);
success = CPS.CS(); //Call Change Status for Pensioner
return success;
        }

        //Webservice Method to run Peyroll.You must pass
particular Month and Year
        //for the Payroll to run.
        [WebMethod]
```

```
public string RunPayroll(int Month, int Year, int
AuthorizationCode)
        {
            UsernameToken tok =
WseSecurityHelpers.GetUsernameToken(RequestSoapContext.Current);

            //Check if the Web Service Consumer is Allowed to run
Payroll as defined in the web Policy
if (!tok.Principal.IsInRole(string.Format("{0}\\RunPayroll",
Dns.GetHostName())))

throw new Exception("access denied");

            RPayroll Payroll = new RPayroll(Month, Year);
success = Payroll.RunP();
return success;

        }

    }
}
```

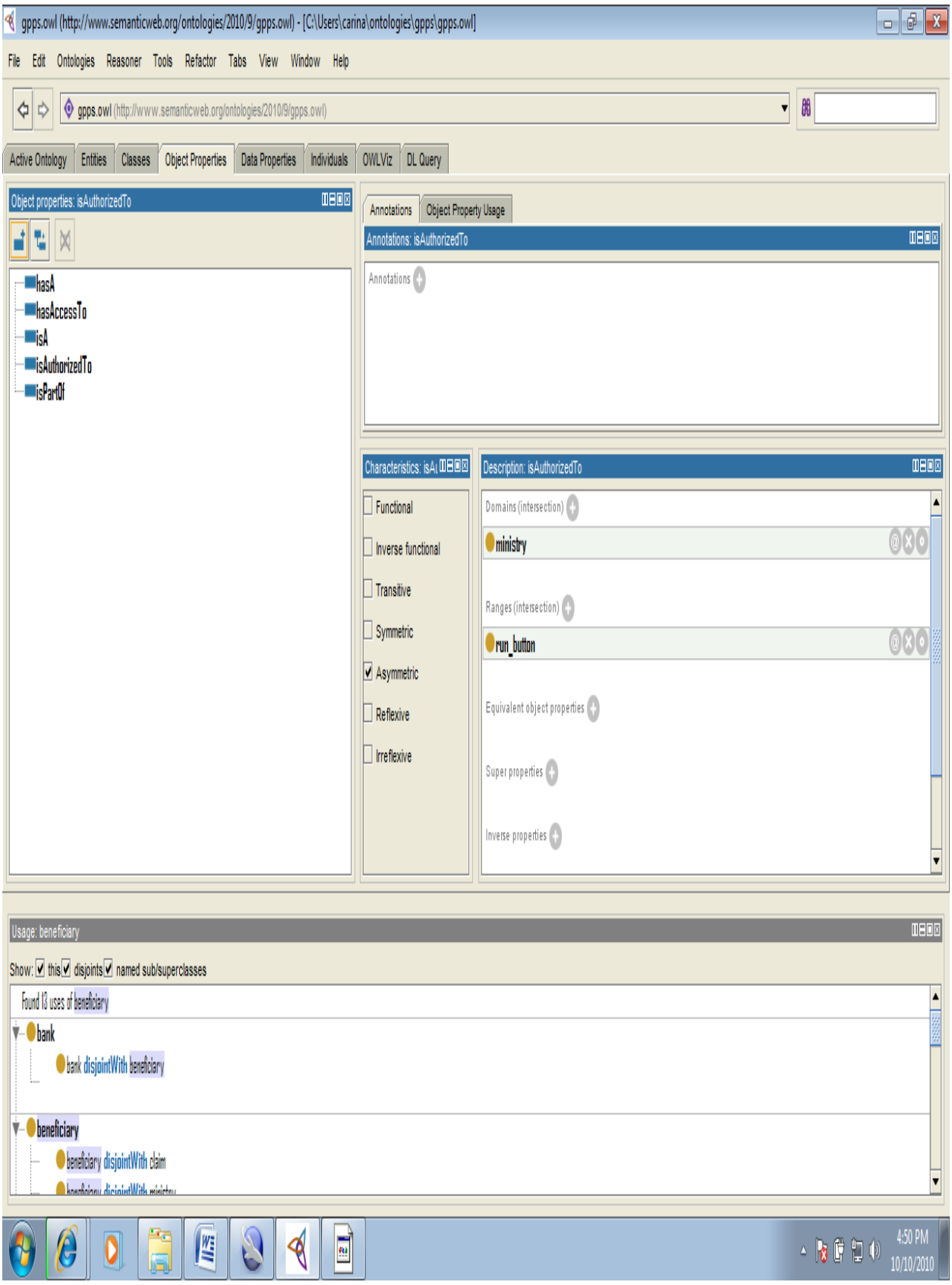
# APPENDIX C Ontology for G2G Transactions in Case Study

Some work was done as part of this study towards building an ontology for the case study described in chapter eight. The language used was OWL and the ontology was built using the Protégé tool. Below are screenshots showing the class hierarchy and the object and data properties.

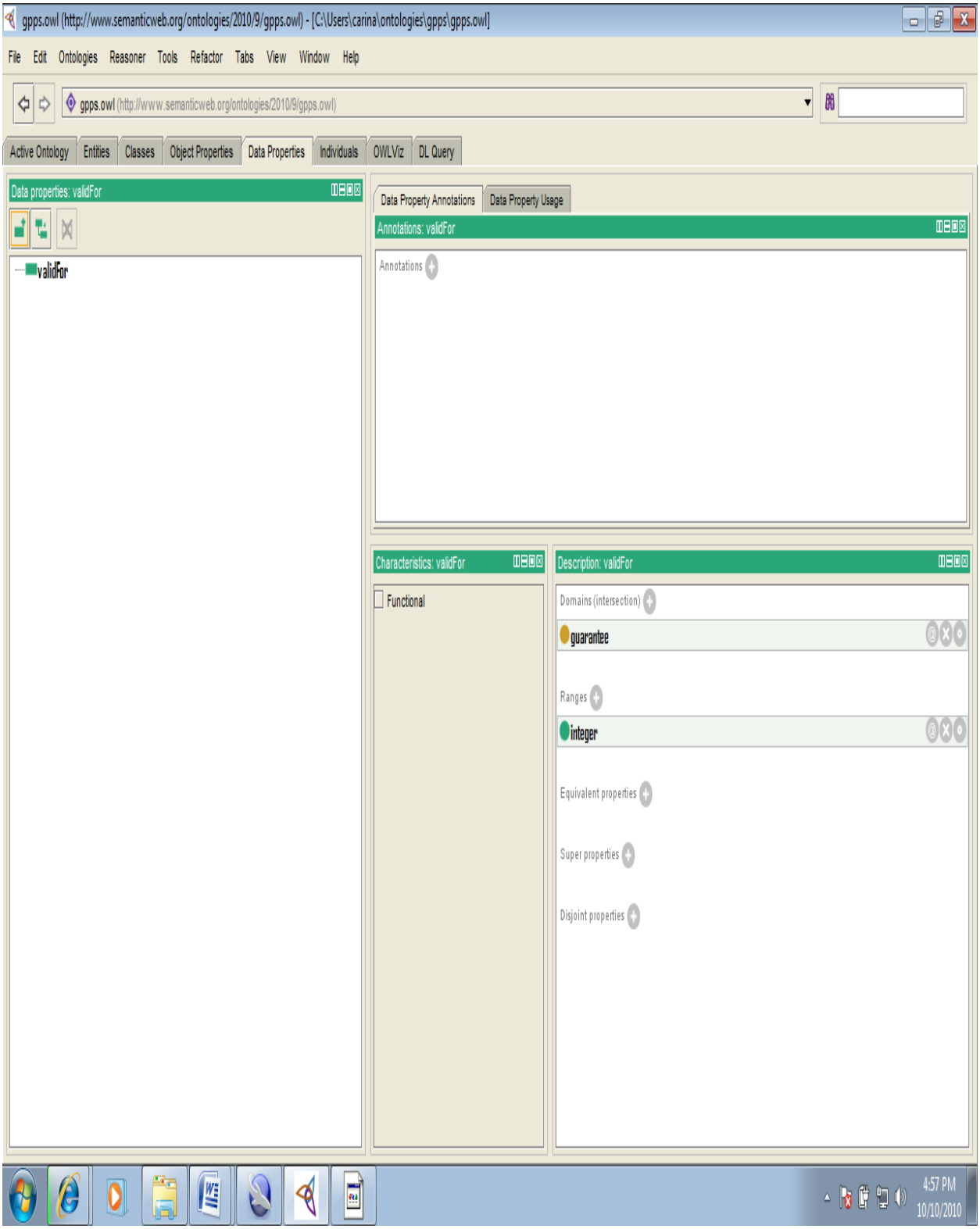
Classes in the Case Study domain ontology in the domain are bank, beneficiary, claim, guarantee, ministry and payroll system.




The object properties are: hasA; hasAccessTo; isA; isAuthorisedTo and isPartOf.


gpps.owl (http://www.semanticweb.org/ontologies/2010/9/gpps.owl) - [C:\Users\carina\ontologies\gpps\gpps.owl]
File Edit Ontologies Reasoner Tools Refactor Tabs View Window Help
gpps.owl (http://www.semanticweb.org/ontologies/2010/9/gpps.owl)
Active Ontology Entities Classes Object Properties Data Properties Individuals OWLViz DL Query
Object properties: isAuthorizedTo
hasA
hasAccessTo
isA
isAuthorizedTo
isPartOf
Annotations Object Property Usage
Annotations: isAuthorizedTo
Annotations
Characteristics: isA
Functional
Inverse functional
Transitive
Symmetric
Asymmetric
Reflexive
Irreflexive
Description: isAuthorizedTo
Domains (intersection)
ministry
Ranges (intersection)
run_button
Equivalent object properties
Super properties
Inverse properties
Usage: beneficiary
Show: this disjoints named sub/superclasses
Found 13 uses of beneficiary
bank
bank disjointWith beneficiary
beneficiary
beneficiary disjointWith claim
4:50 PM
10/10/2010

The only data property in the domain is validFor



## APPENDIX D Improving organizational maturity with TOG Framework.

The TOG framework application to the case study presented in chapter nine, resulted in improvement in the information security policy with the implementing agency. A mapping of the requirements of the information security policy was done against 3 models of the TOG framework. This was done to guide implementation of the information security policy and to raise awareness for all staff of what their role at a governance, operational and technical level is in complying with the policy and any related governance requirements related to information security. The framework used is shown in the table below.

| | | **MODEL** | | |
|---|---|---|---|---|
| **Security Objective as per policy** | **Security Requirement** | **Governance** | **Operational** | **Technical** |
| Systems Resources Classification & Control | Authentication and access control | Board Directive of n$^{th}$ Board Meeting –on auditor's recommendations | • HR/ Payroll as source of identification of staff;<br>• Physical controls on access to offices | • Domain controller access controls i.e. password management.<br>• Lock account for 3 unsuccessful log in attempts.<br>• Encryption (email & access to Member self help)<br>• Terminals should time out in 10 minutes if left inactive. |
| Personnel Security | Confidentiality/ privacy and accountability | Staff & Admin Regulation;<br>Board directive of nn$^{th}$ Board meeting on review of audit trails | • Standard user name – initial followed by surname;<br>• Regulation on review of audit trails<br>• Password policy | • Software (Microsoft server 2008) Use of the list privilege principle to Information systems |
| Software Security | Integrity and Availability | Board Directive of nth meeting on IT risk register | • Maintenance agreement for software<br>• Documentation of software (functionalities and roles) | • ICT service level agreement which aims to ensure the availability and integrity of systems.<br>• Access controls (only administrator can install and do authorised modifications to software |

| | | MODEL | | |
|---|---|---|---|---|
| **Security Objective as per policy** | **Security Requirement** | **Governance** | **Operational** | **Technical** |
| Physical and Environmental Security | Authorization | • Risk recommendation on Physical security of server room<br>• Auditors recommendation | • Insurance<br>• Risk Register<br>• Fixed Asset Register<br>• Financial Regulations | • CCTV (Closed-circuit television)<br>• Biometric access to server room<br>• Infrastructure management system<br>• Installation of fire extinguishers, smoke detector and water detectors. |

# APPENDIX E Papers Published

# A SUSTAINABLE INFORMATION SECURITY FRAMEWORK FOR E-GOVERNMENT – CASE OF TANZANIA

**Carina Kabajunga Wangwe[1], Maria Margaretha Eloff[1], and Lucas Venter[2]**

*[1]University of South Africa, P O Box 392 UNISA 000, South Africa*

*[2]North WestUniversity, Private Bag X1290, Potchefstroom 2520, South Africa*

carina.wangwe@gmail.com (corresponding author), eloffmm@unisa.ac.za, *lucas.venter@nwu.ac.za*

***Technological and Economic Development of Economy Journal Volume 18, Issue 1, 2012, p 117-131***

**Abstract**

The government of Tanzania adopted an e-Government strategy in 2009 that is aimed at improving efficiency in government and providing better services to citizens. Information security is identified as one of the requirements for a successful e-Government implementation although the government has not adopted any standards or issued guidelines to government agencies with regards to information security. Comprehensive addressing of information security can be an expensive undertaking and without guidelines information security implementations may be more prone to failure. In a resource poor country such as Tanzania, there is a need for a cost effective and sustainable means of addressing information security in e-Government implementations. In this paper the authors present a case study of an e-Government interaction between a ministry and a government agency and the information security challenges identified in the implementation. In order to

address these challenges an information security framework is conceptualized using action research. The framework is applied in the case study to address the identified challenges and the means to address future challenges in a sustainable manner is identified. Finally, the proposed framework is evaluated against Tanzanian and international metrics.

**Keywords**
Information Security Framework, e-Government, information security, e-Governance, e-Government in Tanzania,

JEL Classification: O14, O33, O38

## 1. Introduction

Tanzania is a country in East Africa with a population of about 43 million people and per capita GDP in 2009 of Tanzania Shillings 693,185 or USD 522 (Ministry of Finance and Economic Affairs, 2010a). The government of Tanzania consists of central government ministries, departments and government agencies or parastatal organizations. These are commonly referred to by the acronym MDAs. Tanzania has recognized information and communication technologies as a tool for development of the country. There is a national ICT Policy (Ministry of Communications and Transport, 2003) that was adopted in 2003 with the intention to guide national ICT initiatives. However each ministry within central government and each municipality within local government set their own agenda in relation to ICT. The central government budget for the financial year 2010/2011 by the Ministry of Communication, Science & Technology which is responsible for ICT was Tanzania Shillings 3.1billion which is equivalent to about USD 2 Million (Ministry of Finance and Economic Affairs, 2010b). Despite its low GDP and low ICT spending, mobile phone penetration in Tanzania is fairly high, standing at 31% of the population, and the private sector has

introduced many services to take advantage of the high use of mobile phones. (Hellström, 2010, p. 14). Citizens expect government to keep up with these innovations and in response the government of Tanzania has come up with policies and strategies to harness the use of ICT including an e-Government strategy.

This Tanzanian e-Government strategy (President's Office, United Republic of Tanzania, 2009) is aimed at improving efficiency in government and providing better services to citizens. The strategy outlines seven guiding principles including: Service Innovation; Equal Access; Ease of Use; Benefit Realization and Involvement of All Stakeholders; Security and Privacy; Partnership and Outsourcing; and Interoperability. The two principles that relate directly to information security are *Security and Privacy* and *Interoperability*. The strategy lists six critical success factors, one of which is sustainable infrastructure, and goes further to state one of the requirements of a sustainable infrastructure as being network and information security. However, the strategy does not provide guidance to MDAs, who are the major implementers of e-Government, on how to go about addressing information security issues. Furthermore, there are no other government-wide policies, guidelines or standards that have been issued with regards to information security. In order for citizens to benefit from e-Government, MDAs must collaborate and cooperate to come with comprehensive services that are efficient and secure.

Implementation of robust information security can be an expensive undertaking. Since Tanzania is a country with limited resources, it is important for MDAs to have a framework which allows them to plan for and implement information security in e-Government implementations, but at the same is cognizant of the limited resources that are at the MDAs disposal. This paper presents such a framework and uses a case study of an e-Government implementation in Tanzania to illustrate how the framework can be applied.

This paper aims at answering the research question “How can a cost effective and sustainable information security framework for e-Government be developed for Tanzanian MDAs?” Action research is used as the methodology for a case study involving an e-Government transaction between a government ministry and a government agency. The observations resulting from the study are combined with secondary data from the literature review resulting in an information security framework that answers the research question.

The remainder of this paper is structured as follows: section 2 presents the case study of a Government to Government implementation and the approach to solve the identified information security challenges. Section 3 discusses literature that is relevant to the study that is used to gain insights on how to solve the identified challenges. In section 4 a conceptual framework is proposed and then applied to the case study. Section 5 presents an evaluation of the frameworks using Critical Success Factors. The paper ends with a conclusion in section 6.

## 2. Case Study

### 2.1. Background

The Tanzanian Central Government has been paying pensions for civil servants who retired before July 2004 through a ministry responsible for finance. Due to concerns about the efficiency of the process, fraud and resource constraints, the ministry decided to outsource the process in 2008 to a government agency. The government agency chosen is one that has been dealing with pension payments for over 30 years for employees from the private sector and from other government agencies. The ministry required the government agency to run the payroll on secure software and send the payroll information electronically to banks. The banks would then debit the ministry account and credit the pensioners account. The ministry envisaged that this process would reduce human intervention which is one of the sources of fraud; ensure that pensioners are paid on time; and have an audit trail of transactions so as to follow up on any suspect cases. Furthermore, by outsourcing the arrangement to an agency that already had a robust software, and business continuity program in place, the risks arising from frequent power interruptions and lack of sufficient technical skills in the ministry would be addressed.

### 2.2. Challenges identified in implementing the decision

The process of implementing the decision began with a kickoff workshop involving staff from the ministry and the agency. Several challenges were identified during the workshop

and when the action plan for implementation was started. These challenges are categorized in three pillars. For ease of reference the challenges are given code numbers. These are:

**a) Governance**

- G1: Legally, the agency had no mandate to access the data held by the ministry or to pay pensions on behalf of the ministry.
- G2: Both ministry and agency had information security policies that needed to be aligned for purposes of the transaction.
- G3: The memorandum of understanding (MoU) signed between the Ministry and the agency did not explicitly address information security.

**b) Operational**

- O1: Definitions of some terms were different. For example a survivor's pension in the central government ministry is different from a survivor's pension in the government agency.
- O2: Financial resources allocated to the outsourcing project were limited.
- O3: The ministry wanted to retain some control over updates to information
- O4: Technical and management teams met separately during the planning process.
- O5: The organizational culture for the two organizations was found to be different. In the agency technical staff spearhead most initiatives and sold ideas to management, while in the ministry the approach was more top down, that is directives are given by the minister, which the technical and operational staff have to implement.

**c) Technical**

- T1: Some of the necessary data was mostly in paper files and confidentiality and privacy was observed through physical access controls such as storing the data in locked cabinets. Access lists were on paper and files containing information were issued by a person responsible for storing the files.
- T2: The ministry was running their payroll on a COBOL based application while the government agency was using an application based on Oracle Forms. The underlying databases and operating systems were also on different platforms.
- T3: The ministry offices and the agency offices had no direct data communication link.
- T4: Although security policies existed in both organizations, no standard requirements for security were set out in either policy.

The initial approach by the Ministry was to deal with the issue of legislation, and propose amendments to the law which were passed by the Parliament (Parliament of Tanzania, 2008). These amendments simply allowed the agency to pay pensions on behalf of the government. The challenge of data access was not addressed. A technical team headed by one of the authors of this paper, was set up by the agency to coordinate the project implementation. This team decided to adopt a structured approach to address the challenges mentioned above. The process which is an ongoing iterative process uses the action research methodology (de Villiers, 2005) as shown in Figure 1.

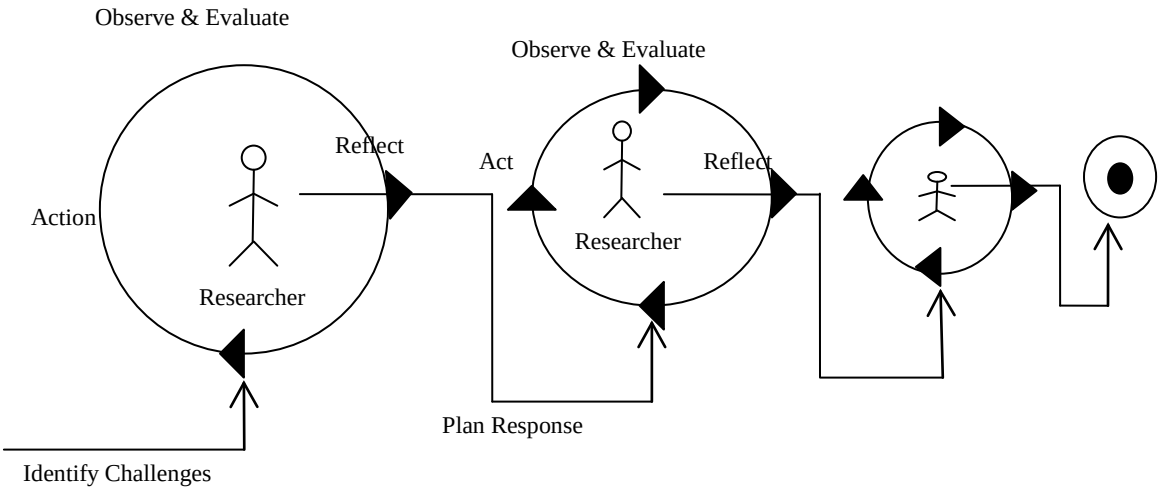



Figure 1: Action Research process: Adopted from de Villiers (2005)

Early in the process, the authors observed that some of the challenges identified have been addressed by studies already published in journals or conferences proceedings. The reuse of solutions or components of the solutions presented in such studies could be beneficial to the case study. This resulted in literature surveys that identified some relevant studies. These studies are outlined in the next section and how they meet the challenges identified is discussed.

## 3. Literature Survey

The starting point for the literature survey was existing international standards on information security. The International Organization for Standardization (ISO) defines

information security as the preservation of confidentiality, integrity and may also involve authenticity, accountability, non-repudiation and reliability (ISO/IEC, 2009, p. 3). Information security has been studied comprehensively from a technical and a management perspective. A few studies have also been done on information security in Tanzania. In this section, studies related to information security in e-Government are discussed in relation to the challenges observed in the case study. The studies are presented in three categories, which are, technical, management and studies based in Tanzania.

### 3.1. Technical Studies on Information Security in e-Government

Many e-Government implementations are achieved through Service Oriented Architectures (SOA) with Web Services (Chunnian et al. 2011), (Simon et al. 2010), (Scholl and Pardo, 2010). This is because e-Government implementations involve transactions across heterogeneous systems.

The security requirements for e-Government implementations are discussed by Zissis and Lekkas (2011) in fiver broad categories which are Availability, Confidentiality, Integrity, Authenticity, and Accountability. The security requirements of a particular e-Government project, the Access e-Gov project (Durbeck et al. 2007) are listed as Communication security that can be achieved through standards-based encryption and digital signatures; Trust; Privacy; and access control: whereby Attribute Based Access Control is suggested to provide a flexible dynamic infrastructure that suits loosely coupled SOA. Beimel and Peleg (2011) introduce an improved method of Access Control policy composition which underpins access control with ontologies through the application of the Web Ontology Language (OWL) and the Semantic Web Rule Language (SWRL).

The use of the Security Assertion Mark-up Language (SAML) as a mechanism for handling access control in an e-Government transaction was addressed in a study by Marin-Lopez et al. (2011) and by Wangwe et.al (2009). SAML is one of several open technical standards adopted by the Organization for the Advancement of Structured Information Standards (OASIS). Other standards from OASIS include XACML which is designed for access control and the WS family of standards for web service security (OASIS, 2010).

### 3.2. Information Security Management

ISO 27002, which is an internationally accepted standard, requires legal and regulatory aspects to be taken into consideration when incorporating security requirements in the design of systems (ISO/IEC, 2005). To this end, Guarda & Zannone (2009) state that legal requirements should be incorporated into software engineering for e-Government transactions by following existing laws and more especially those related to privacy and data protection. A practical implementation of how legal requirements can be incorporated in software system engineering is demonstrated in a study by Islam et.al (2011) in a framework that allows developers to elicit requirements from legislation, and track that these requirements are addressed through the system development.

A study by Seidenspinner and Theuner (2007) investigates different cultural environments and concludes that the cultural environment of users affects their online behaviour. This conclusion is extended to governments in a proposition by Alfawaz et al. (2007) that national culture may have an impact on e-Government security effectiveness in developing countries. Their study looks at the effect of legislation on security and privacy and states that many developing countries have yet to consider adopting adequate legislation related to information security management which could be used to take action against the misuse of ICT resources. Zarei and Ghapanchi (2008) however argue that e-Government development should not wait until full security levels are reached. They state that providing fully functional security for all the e-Government programs is impractical. Other security heuristic principles include the need for a security development and management plan and application of security standards by a team with sufficient experience. The recommendations of the study by Zarei & Ghapanchi are to an extent validated by a study conducted in South Africa by Dagada et al. (2009) who conclude that while legislation that deals with information security exists, it is not used in organizational policies.

Several governments have put in place mechanisms at a national level to govern information security. For instance, the government of the United Kingdom adopted Her Majesty's Government (HMG) Security Policy Framework that sets out policy areas to guide information security management in government departments (Cabinet Office UK, 2008). The Government of Tasmania has adopted an Information Security Framework which

provides guidance to government agencies on what Information Security Policy Principles they need to adhere to, as well as important legislative requirements and the primary roles and responsibilities for information security (Department of Premier and Government, Tasmania, 2009). A slightly different approach has been adopted by the Spanish and South African Governments, who have adopted interoperability standards for government agencies that address security among other issues (Ministry of the Presidency, Spain, 2010; SITA, 2007).

### 3.3. Information Security and e-Government in Tanzania

In Tanzania, a study of information security in higher institutions of learning (Bakari et al. 2005) led to two key conclusions, which were, the necessity of adequate planning at national and organizational level for a successful information strategy; and the need for developing countries to transform traditional information security policies into relevant policies to cater for digital information security. These conclusions further motivate this study since a framework for e-Government security would both ease planning at a national and organizational level, and also guide the drafting of relevant security policies.

The need for regulations to underpin information security is discussed by Tarimo (Tarimo et al. 2005) who recognizes contexts in developing countries as significantly different from those in developed countries, and the impact on information security. Tarimo et.al conclude that instead of waiting for the government intervention, organisations deploying ICT can put forward their own initiatives to make sure that their systems follow standards that allow for security, interconnectivity and interoperability with other ICTs in the country and beyond. This conclusion is supported by the study Zarei and Ghapanchi (2008), which is to say that for a developing country; a top-down might not work since governments are slow in implementing the necessary governance structure, while a bottom- up approach may be constrained by lack of guidelines.

Karokola (Karokola and Yngstrom 2009) study Tanzanian government institutions' requirements with regards to information security and come up with a score of the priority areas. Technical security issues are ranked most important together with awareness. Non-technical aspects including managerial, operational and economical factors are also

considered priority areas. This study shows that legal and regulatory requirements are not high on the list of priorities. This could be explained by the fact that there are currently not many laws in Tanzania that address information security.

### 3.4. Reflection on the Literature Survey

The literature survey provided useful insights to addressing the information security challenges that were identified in the case study, and in particular in highlighting areas where solutions to similar challenges have already been found and how other governments have approached information security management. The insights to some of the challenges obtained from the literature survey are summarised in Table 1. For challenges, G2, O2, O4 and T3 which are very specific to the case study, ways to address the challenges were obtained through brainstorming sessions, and the findings incorporated in the framework that is presented in section 4.

Table 1: Insights from Literature Surveyed

| **Identified Challenges** | **Insights from studies surveyed** |
|---|---|
| **Governance** | |
| G1 | Where legislation exists, it should be reflected in policies. International Standards should be used to guide implementations. |
| G3 | Technical and operational solutions can and should be used in the absence of governance structures. |
| **Operational** | |
| O1 | Semantic interoperability can be achieved through common taxonomies |
| O3 | Robust Access control mechanisms are important for secure government to government transactions. Attribute Based Access Control is a mechanism that can be used with SOA to ensure controlled access to information assets |
| O5 | Culture has an impact on web usage in general, and specifically on information security for online transactions. The implementation of successful information security implementations should thus include addressing of culture |
| **Technical** | |
| T1 | Access control lists can be translated into electronic polices using open standards such as XACML and implemented using SAML |
| T2 | Service Oriented Architectures and Web Services can be used for technical interoperability; in addition semantic interoperability can be achieved through use of ontologies. |
| T4 | In general, Security Objectives are Confidentiality which includes authentication, authorization and access control and privacy, Integrity, Availability and Accountability which includes Trust and Non repudiation |

## 4. Proposed Framework

The insights obtained from the literature survey were combined with data collected through observations of current information security practices in both the ministry and the agency, and interviews with staff involved in the implementation of the case study. From these, the authors conceptualized an information security framework that is referred to by the acronym TOG (Technical, Operational and Governance). The TOG framework recognizes the need for e-government transactions to be cognizant of national legislation, and policies, will at the same time complying with organizational policies. At the technical level, for a country that has limited resources such as Tanzania, the technical pillar recognizes the existence of tried and test mechanisms, particularly those based on open internationally accepted standards.

The TOG information security framework consists of three pillars which are Technical, Operational and Governance pillars. The governance pillar includes legislation, internationally acceptable standards, national and regional standards and guidelines and operational policies. This pillar will be typically implemented at national level by inter-ministerial committees together with legislative bodies such as parliament, while at MDA level it will be implemented by executive management and or Boards of Directors. The operational pillar includes organizational plans and operational procedure and is implemented by organizational units within MDAs. The technical pillar includes technical mechanisms to address the security requirements and is implemented by Information Technology departments within MDAs. The components of each pillar are gleaned from the literature study done of researches on information security for e-government and matched to security objectives and requirements that are applicable to the e-government transaction.

The detailed TOG framework is depicted in Table 2.

Table 2. TOG Framework

| | | PILLAR | | |
|---|---|---|---|---|
| **Security Objective** | **Security Requirement** | **Governance** | **Operational** | **Technical** |
| Confidentiality | Authentication<br>Authorization and Access Control<br>Privacy | • International Standards,<br>• Laws and Regulations,<br>• Organisational Policies | • Risk Assessment<br>• Certificate Authorities<br>• Metadata definitions<br>• Awareness Sessions | • Ontologies<br>• Attribute based Access control using XACML & SAML attributes<br>• Passwords |
| Integrity | Data Integrity | • International Standards, Organisational Policies | • Certificate Authorities | • Encryption, SSL |
| Availability | Availability | • Business Continuity Policies (BCP) | • Power Management<br>• Business Continuity Plans<br>• Interoperability frameworks | • SOA, Web Services, Uninterruptible Power Supply (UPS) |
| Accountability | Trust & Non Repudiation | • Laws and Regulations,<br>• Contractual Agreements and MoUs | • Certificate Authorities | • Digital Signatures, Certificates,<br>• PKI |

### 4.1 Application of the Framework

The application of the framework was done by the ministry and the agency with activities often taking place in parallel, and with the top management being responsible for governance, operational staff for the operational pillar and technical staff for the technical pillar. Mapping across the pillars was undertaken in workshops where management and technical staff met to discuss their activities and map them against activities being done in other pillars. This approach was termed a ‘plug and play’ approach in contrast to a top-down or bottom up approach, although for each activity a Plan-Do-Act-Check cycle was followed

as shown in Figure 2. The plug and play approach recognises that resources in the Tanzania government for one big initiative may not be available, but it is still possible for a department to start to address information security for an e-government transaction by focusing first on one pillar of the framework – depending on what the role of the department is, and what resources are available. A mapping onto the other pillars can be done from time to time, as resources become available. Each mapping recognises the initiative already in place and gradually the government moves towards a holistic addressing of information security requirements.

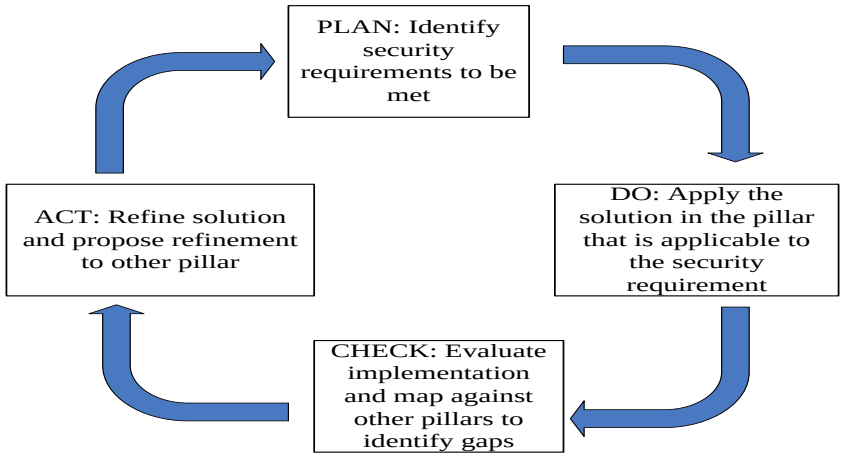



Figure 2: PDCA Cycle for application of the TOG framework

The specific activities carried out so far in implementing the framework and addressing the challenges stated in section 2.2 are:

**a) Governance**

Legislation (Parliament of Tanzania, 2008) was put in place to mandate the agency to pay on behalf of the ministry before the implementation of the framework. Based on the amended legislation a contract signed between the two parties to outline the roles and responsibilities of each party in implementing the outsourcing of payment of pensions. Furthermore the parties agree that the information security policy of the ministry would prevail.

**b) Operational**

In meeting the information security objectives, the following activities have been done:

- Risk assessment has been carried out and an access control list setup
- The parties have agreed to use the Ministry definitions where terminology differs.
- Joint awareness sessions between technical and management teams are held every six months to review activities in each team and determine where solutions need to be mapped to each other.

Challenges that are still to be addressed include coming up with taxonomy of terms that relate to the payment of pensions to ensure that interpretation of the terms is consistent.

**c) Technical**

The technical team has developed a payroll web service that can be invoked by the ministry if they need to do updates to data. The same web service is used to run the payroll. In addressing data integrity, privacy and confidentiality, a secure communication link has been set up between the ministry and the agency and information across the link is encrypted. The relevant information security policies translated to XACML. Authentication has been tied to fixed IP addresses. Availability has been addressed through the installation of UPS for power management. The agency uses an SSL certificate issued by VeriSign (www.verisign.com) for its browser interfaces. Thus VeriSign was used as a trusted third party in the absence of a certificate authority set up by government. The challenges that still need to be addressed include automating the issue of security assertions, by for example, implementing SAML. Table 3 illustrates how the TOG framework has been applied.

Table 3. Application of TOG framework to payroll application

| | | PILLAR | | |
|---|---|---|---|---|
| **Security Objective** | **Security Requirement** | **Governance** | **Operational** | **Technical** |
| Confidentiality | Authentication | • Ministry's Information Security Policy | | |
| | Authorization and Access Control | • Finance Act. No. 13 of 2008<br>• Contract between Ministry and Agency | • Risk Assessment, Access Control List,<br>• Standard Terminology for transactions<br>• Awareness Sessions | • XACML policies based on Ministry's information Security Policy |
| | Privacy | • Ministry's Information Security Policy | | |
| Integrity | Data Integrity | • Ministry's Information Security Policy | | • SSL, Encryption |
| Availability | Availability | | | • Uninterruptible Power Supply (UPS);<br>• Pensioner Payroll Web Service |
| Accountability | Trust & Non Repudiation | • Finance Act No. 13 of 2008<br>• Contract between Ministry and Agency | • Access Control List | • SSL (from VeriSign)<br>• Authentication by IP address |

### 4.2. Addressing Future Challenges

The TOG framework allows MDAs to include any technical, operational or governance solutions or practices that are applicable in the context of the transactions being addressed. Once a solution has been adopted in one pillar, mapping will be done across the other pillars to ensure that comprehensive information security is achieved.

## 5. Evaluation

The TOG framework is evaluated using critical success factors (CSFs). The evaluation is shown in Table 3. CSFs have been used as a method for helping organizations guide the development and management of security strategies and across their enterprises and for evaluation of information systems (Caralli, 2004) (Bergeron, Bégin, 1989). The TOG framework is evaluated in two ways. Firstly Critical Success Factors (CSFs) stated in the

Tanzania e-Government strategy are used. Although the CSFs are stated in relation to e-Government they can also be applied to information security in e-Government since information security should form an integral part of the planning process for e-Government implementations conception to conclusion. Secondly CSFs stated in the ISO 27002 information security management standard are used. This is done in order to determine how the TOG framework measures up against an international standard. ISMS Critical Success Factors have been adopted by ISO in the ISO/IEC Code of practice of information security management (ISO/IEC, 2005, p. 11). These are applicable to the evaluation of TOG since TOG is designed to address management aspects of information security.

The evaluation of the TOG framework against the Tanzania e-Government Strategy and the ISO ISMS CSFs are presented in Table 4 and Table 5 respectively.

Table 4: Evaluation of TOG against Tanzania e-Government Strategy CSFs

| **CRITICAL SUCCESS FACTOR** | **TOG solution** |
|---|---|
| Political will, support and commitment | All legislation in Tanzania is passed through the parliament. The Governance pillar of TOG which includes legislation enables political leaders to understand the role they need to play to have successful information security in e-Government implementation. |
| Availability of HR capacity | TOG addresses HR capacity by its flexible structure that refers to international open standards. So there is no need for MDAs to reinvent the wheel where proven standards are already in place. In addition, the PDCA implementation process helps the existing HR resources to continually check where gaps in implementation are and focus the upgrading of skills or looking for new resources on the areas where skills are lacking. |
| Institutional and Legal framework | The TOG governance pillar includes all relevant legislation and organizational policies that address how a security requirement is to be met. These are then mapped onto organizational plans and procedures in the operational pillar. |
| Financial Resources | TOG is a flexible framework whose 'plug and play' of 'start anywhere' nature means that the technical, operational and governance components to address each security requirement can be implemented as and when resources are available within the identified risks acceptance level. |
| Commitment by all actors | Implementation of the TOG framework forces the involvement and collaboration of technical operational and management staff. Every technical implementation needs to be mapped back onto an operational procedure and or governance structure and vice versa. |
| Sustainable Infrastructure | The technical pillar emphasizes the use of open standards, and service oriented architectures which address the lack of interoperability that may exist among MDAs. In addition the 'start anywhere' and flexible approach to implementing TOG means that each MDA can start with addressing the requirements in a manner that takes the context of the implementation into consideration then build upon that implementation as resources improve, or review and change the implementation if necessary. |

Table 5: Evaluation of TOG against ISMS CSFs

| **ISMS CRITICAL SUCCESS FACTORS** | **TOG Solution** |
|---|---|
| Information security policy, objectives and activities aligned with objectives | TOG addresses information security policies and provides for the mapping of those policies to operational and technical activities |
| An approach and framework for designing, implementing, monitoring, maintaining and improving information security consistent with the organizational culture. | The TOG framework allows for organizational culture especially in the context of Tanzania where often it is not possible to have a strictly hierarchical or sequential process. TOG allow for various start points in any of the pillars and then subsequent mapping to any of the other pillars, provided that the security objectives are set in advance. |
| Visible support and commitment from all levels of management especially top management | Implementation of the TOG framework forces the involvement of technical operational and management staff. |
| An understanding of information asset protections achieved through the application of information security risk management: | Risk Assessment is provided for in the operational pillar of TOG. |
| An effective information security awareness, training and education program information all employees and other relevant parties of their information security obligations set forth in the information security policies, standards etc. etc, and motivate them to act accordingly | Awareness is provided for in the operational pillar of TOG. |
| An effective information security incident management process | TOG does not address this. Such a process however, can be included in the Operational Pillar. |
| An effective business continuity management approach | Business continuity management is provided for in the TOG framework in order to address the Availability security objective. |
| A measurement systems used to evaluate performance in information security management and feedback suggestions for improvement: | The PDCA cycle approach can be used to implement TOG. |

The evaluation of the TOG framework shows that it is a robust framework since it addressed most of the factors in an internationally accepted standard, which is ISO/IEC 27002. At the same, it is a sustainable framework for Tanzania as it addresses all the critical success factors stated in the Tanzanian e-Government strategy.

## 6. Conclusion and Further Work

This paper aimed at answering the research question “How can a cost effective and sustainable information security framework for e-Government be developed for Tanzanian MDAs?” To answer the question, a framework that identifies security objectives and requirements has been presented. The framework, dubbed the TOG framework, consists of three pillars, namely governance, operational and technical. Together these pillars allow an

MDA to addresses information security comprehensively while at the same time allowing flexibility in the implementation to cater for resource and other constraints. The framework is sustainable in that it proposes the use of open standards and service oriented architectures while meeting any legal or regulatory requirements. TOG also allows a 'plug and play' approach so that MDAs can start with a solution in any of the pillars for which resources are available and then move towards a comprehensive solution by mapping solutions from one pillar to another. The framework has been successfully applied to a case study. The evaluation of the framework shows that TOG addresses all the CSFs stated in Tanzania's e-Government strategy while meeting all except one of the CSFs proposed by the ISO in its information security management system standard. This evaluation leads to the conclusion that the proposed framework is a robust, sustainable and cost effective framework that is applicable to MDAs in Tanzania. The proposed framework adds to the body of knowledge in the field of information security as it shows how the Tanzania context of e-Government transactions can be addressed. While the mechanisms presented within the framework are tried and tested, the framework shows how these can be combined, as and when resources allow, going towards a holistic addressing of the information security This is the innovation of this approach rather than the government adopting without modification either a standard or copying another countries' framework. At the same time the framework enables different levels in government to address the same requirements through different mechanisms depending on their areas of expertise and then provides a means for the others to map these onto their initiatives.

The authors intend to extend the study to determine whether the framework would be applicable in the East African Community, as the countries in the EAC have similar challenges in terms of information security as those in Tanzania.

**References**


1. Alfawaz, S., May, L., and Mohanak, K. 2007. E-government security in developing countries: A Managerial Conceptual Framework. 40th Hawaii International Conference on System Sciences.
2. Bakari, J. K., Tarimo, C. N., Yngstrom, L., and Magnusson, C. 2005. State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case Study. ICALT 2005, 1007-1011.
3. Beimel, D and Peleg, M. 2011. Using OWL and SWRL to represent and reason with situation-based access control policies. Data & Knowledge Engineering, 70(6), 596-615.
4. Bergeron, F., & Bégin, C. 1989. The use of Critical Success Factors in Evaluation of Information Systems. Jounral of Management Information Systems, 111-124.
5. Cabinet Office UK. 2008. HMG Security Policy Framework. Available on Internet <http://www.cabinetoffice.gov.uk/media/111428/spf.pdf>.
6. Caralli, R. A. 2004. The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management. Software Engineering Institute - Carnegie Mellon, Pittsburgh.
7. Chunnian, L., Yiyun, H. and Qin, P. 2011. A Study on Technology Architecture and Serving Approaches of Electronic Government System. Intelligent Computing and Information Science, Communications in Computer and Information Science, 134(1) 112-117.
8. Dagada, R., Eloff, M. M., and Venter, L. M. 2009. Too Many Laws but very little progress- Is South African Highly Acclaimed Information Security Legislation Redundant? Informaton Security South Africa (ISSA09).
9. de Villiers, M. 2005. Three approaches as pillars for interpretive Information Systems research: development research, action research and grounded theory. SAICSIT, 142-151.
10. Department of Premier and Government, Tasmania. 2009. Tasmanian Government Information Security Framework.

11. Durbeck, S., Schillinger, R., and Kolter, J. 2007. Security Requirements for a Semantic Service-oriented Architecture. The Second International Conference on Availability, Reliability and Security, 366-373. IEEE Computer Society.
12. Guarda, P., and Zannone, N. 2009. Towards the development of privacy-aware systems. Information and Software Technology, 51 (2), 337-350.
13. Hellström, J. 2010. The innovative use of mobile applications in East Africa. SIDA.
14. Islam, S., Mouratidis, H.,and Jurjens, J. 2011. A framework to support alignment of secure software engineering with legal regulations. Software and Systems Modeling, 10(3), 369-397.
15. ISO/IEC. 2009. Information Technology- Security techniques-Information security management systems - Overview and vocabulary.
16. ISO/IEC. 2005. ISO/IEC 27002:2005 - Information technology -- Security techniques -- Code of practice for information security management.
17. Karokola, G., and Yngstrom, L. 2009. Discussing e-Government Maturity Models for Developing World - Security View. Information Security South Africa (ISSA09).
18. Marin-Lopez, R.,Pereniguez, F.,Lopez, G. and Perez-Mendez, A. 2011. Providing EAP-based Kerberos pre-authentication and advanced authorization for network federations. Computer Standards & Interfaces, 33(5), 494-504.
19. Ministry of Communications and Transport. (2003). National Information and Communications Technologies Policy. United Republic of Tanzania, Dar es Salaam.
20. Ministry of Finance and Economic Affairs. 2010a. Hali ya uchumi ya Taifa katika Mwaka 2009 Jedwali Na.A. [State of the Economy of the Nation in 2009, Document no. A].
21. Ministry of Finance and Economic Affairs. 2010b. Volume IV- Public expenditure Estimates, Development Votes for 2010/11.
22. Ministry of the Presidency, Spain. 2010. Spanish National Interoperability Framework.
23. OASIS. 2010. Available from Internet <http://www.oasis-open.org/specs/>.
24. Parliament of Tanzania. 2008. Finance Act No.13.
25. President's Office United Republic of Tanzania. 2009. Tanzania e-Government Strategy.

26. Scholl, H. J., and Pardo, T. A. 2010. Data-Centric Workflows in Government: A New Avenue of Research? 11th Annual International Digital Government Research Conference, 138-146.
27. Seidenspinner, M and Theuner, G. 2007. Intercultural aspects of online communication a comparison of mandarin-speaking, US, Egyptian and German user preferences. Journal of Business Economics and Management, 8(2).
28. Simon, B., Laszlo, Z., Goldschmidt, B., Kondorosi, K. and Risztics, P. 2010. Evaluation of WS-* Standards Based Interoperability of SOA Products for the Hungarian e-Government Infrastructure. 4th International Conference on Digital Society, 118-123.
29. SITA. (2007). Minimum Interoperability Standards for Information Systems in Government. Available from Internet < http://www.sita.co.za/standard/MIOSv4.12007.pdf>.
30. Tarimo, C. N., Yngstrom, L., and Kowalski, S. 2005. An Approach to Enhance ICT Infrastrcutures Security through Legal, Regulatory Influence. ISSA 2005, 1-12.
31. Wangwe, C. K., Eloff, M. M., & Venter, L. 2008. A Proposed Implementation of SAML V2.0 in an e Government Setting. IST Africa. Windhoek: IIMC International Information Management Corporation.
32. Zarei, B., & Ghapanchi, A. 2008. Guidelines for government-to-government initiative architecture in developing countries. International Journal of Information Management, 28, 277– 284.
33. Zissis, D and Lekkas, D. 2011. Securing e-Government and e-Voting with an open cloud computing architecture. Government Information Quarterly, 28(2), 239-251.

**Carina K. Wangwe** is a PhD student at University of South Africa (UNISA) and works for a government agency in Tanzania. Four articles that she wrote as the primary author have been published in peer reviewed conference proceedings.

**Mariki Eloff** is a Professor at School of Computing UNISA who holds a PhD from Rand Afrikaans University. She has published extensively in the field of information security.

**Lucas Venter** is a Professor and Director: Research support at North Western University, and a Professor Extraordinaire at UNISA. He has published extensively on information security, mobile agents and curricula for computing.

# e-Government Readiness: An Information Security Perspective from East Africa

*In proceedings of IST-Africa 2009 Conference Proceedings, Paul Cunningham and Miriam Cunningham (Eds), Published by IIMC International Information Management Corporation, 2009*

Carina K. WANGWE[1], Mariki M. ELOFF[2], Lucas M. VENTER[2]

[1]*University of South Africa, P.O.Box 60049,Dar es Salaam,Tanzania*

*Tel: +255 754 600512, Fax: + 255 22 2117772, Email:carina.wangwe@gmail.com*

[2]*University of South Africa, P.O.Box 392 UNISA 0003 South Africa*

*Tel: +27 12 4296330 Fax: + 27 12 4296771, Email:eloffmm@unisa.ac.za*

**Abstract:** e-Government readiness is the measure by which a government is positioned to provide e-services to its citizens. In order to achieve e-readiness, governments must among other factors, set up efficient collaborations between government agencies. Such collaborations should take into consideration information security requirements. Our study looks at e-government readiness in three East African countries namely, Tanzania, Uganda and Rwanda from an Information Security perspective. Data was gathered through questionnaires and by reviewing country and regional e-government polices, as well as evaluating government agency websites. The results of the study are discussed based on findings by other researches on Information Security and or e-government in the East African region.

**Keywords:** Information Security, e-Government

## 1. Introduction

e-Government readiness is the extent to which a government has positioned itself to apply information and communication technologies to provide better access to and delivery of services to citizens, improved interaction with citizens and business, and the empowerment of citizens through access to information. In the East African Community (EAC), which consists of five countries, that is, Uganda, Kenya, Tanzania, Rwanda and Burundi, various initiatives towards delivery of services and citizen participation have been undertaken or are in progress. e-Government Policy documents have been drafted in all these countries except

Burundi, and various legislations are being introduced in the arena of e-Government and e-Business[1][6][7][8]. Furthermore an East African e-Government Secretariat has been set up to develop regional policies.

However according to the UN e-Government Survey of 2008 [1], whereas earlier emphasis of e-government was mostly on developing e-services, the focus has shifted towards building and managing integrated and coordinated government services. This is critical since a lack of coordination in policy decisions and announcements can play a considerable role in undermining policy objectives and also weakening the credibility of institutions and policies. Furthermore the report states that ICT-based connected governance efforts are aimed at improved cooperation between government agencies, allowing for an enhanced active and effective consultation and engagement with citizens and a greater involvement with multi stakeholders regionally and internationally. For the case of East Africa, since key infrastructure projects are underway such as the Fibre Optic Backbone projects in Rwanda, Tanzania and Uganda, as well as national ID projects, a good foundation is being laid for government agencies and departments to provide integrated services to Citizens. This step however requires the addressing of information security, to ensure confidentiality and integrity of information passed from one agency to another for the purpose of providing a service.

The objective of this study was to evaluate e-Readiness in the EAC from an information security perspective, based on e-government policy documents, cross agency collaborations and government agency websites. Such an evaluation should act as a basis for recommendations as to how government agencies can plan for and address information security in future. The remainder of the papers is structured as follows:

Section 2 gives a brief overview of the information security requirements as indicators of e-readiness. Section 3 explains the methodology used and presents the results obtained. This is followed by a critical analysis of the results with a conclusion and further research in the last section.

## 2. Information Security e-readiness indicators

The security requirements for e-Government can be considered to be:

- Authentication;
- Privacy;
- Authorization and Access Control;
- Data integrity and
- Trust.

The above requirements apply both to transactions between citizens and government agencies and also to inter – agency collaborations. In order to gauge e-readiness from an Information Security perspective, the following factors should be evaluated.

i) The agency should have a information security policy that outlines how and when its systems should be accessed, how trust is established and what standards are there for ensuring privacy and integrity of data. Furthermore there needs to be an enabling environment at country and or regional level in the form of security polices statements incorporated in e-government policies.

ii) The agency should establish standard terminologies for automated transactions to ensure that no misunderstandings arise when dealing with another agency, that is, semantic interoperability is achieved.

iii) The context of the transactions should be taken into consideration and in particular, risks in the inter-agency collaborations should be identified such as the possibility of fraud and network breakdowns.

iv) The incorporation of security requirements in interfaces with citizens, for example, web pages.

Our study therefore investigated whether EAC government agencies or departments have addressed the above factors.

## 3. Methodology and Results

### 3.1 Structure of the Study

The methodology used for this study was Grounded theory [2]. The study was conducted between December 2007 and February 2008. Data was collected from three of the five countries forming the EAC, namely, Uganda, Tanzania and Rwanda. Information from Kenya and Burundi was not obtained because of difficulties in communication at the time the data collection was undertaken. Data was collected from three sources i.e.

Government Department websites: A review was done of web sites to investigate services offered and any information security related requirements e.g. authentication for e-services.

National e-Government policies: A review was done for of e-government and or related documents was done with focus on Information Security.

Questionnaires issued to staff of Government Agencies/ Departments. The agencies included in the study were those which as per their operational mandate need to collaborate with other agencies in order to provide a service. The questions designed to address information security requirements identified by several studies including Bakari &Tarimo[3], Chaula et. al[4] both of which were carried out in Tanzania, and from Bakari et.al[5] which is written from a developing countries' perspective. Questionnaires were distributed to Government agencies or departments that typically undertake cross agency transactions.

### 3.2 Results and Discussion

#### 3.2.1 Web Sites

Twelve websites were examined from government departments/ agencies in the three countries i.e. 4 each. The Criteria for examining web sites was based on the study by Kaaya [6]. The results are represented in Table 1 below:

*Table 1: Websites from EA*

| | Country | | |
|---|---|---|---|
| Level ( Adopted from Kaaya [5]) | Tanzania | Rwanda | Uganda |
| Initial Level: Web sites are established to provide information about government functions and services | 100% | 100% | 100% |
| Intermediate Level: Downloadable forms that can be completed and submitted offline are made available on the web site; email interaction between government officials and users may also be supported. | 100% | 100% | 100% |
| Advanced Level: Web sites begin to support some formal online transactions such as payments or creating and submitting information such as renewing driving license and filing tax returns. | 25% | 25% | 25% |
| Comprehensive Level: Comprehensive and sophisticated government portals are developed to provide a wide range of information to users coupled with reliable security / privacy/ confidentiality provisions. | 0% | 0% | 0% |

The results from the table above show that in all three countries although government agency web sites are available, they have not yet reached the comprehensive level. Thus government agencies need to address how provisions for security, privacy and confidentiality are being made in order to efficiently provide a wide range of e-services to citizens through inter agency collaborations.

### 3.2.2 Review of Policies

A review of Policy/ Strategy documents related to e-government was undertaken to investigate how information security requirements are addressed. The results were as follows:

i) Rwanda: The Rwanda e-Government Policy Report [7] outlines minimum standards for security both hardware and software and includes also a certification server standard. Furthermore the report states that there shall be a root Certificate Authority (CA) to security certificates to government agencies. The root CA must be trusted by all other CAs. The report does not however state how that trust will be established.

ii) Uganda: The Uganda e-Government Strategy [8], addresses security under the infrastructure component by proposing that a security infrastructure be setup for secure online transactions. A PKI infrastructure is mentioned including a Certificate Authority. Cross Agency collaboration is mentioned as the last phase of the e-government transformation during which agencies will take a whole-of-government perspective when designing and implementing services. Furthermore, the strategy recognises the need to incorporate, within current systems design, the need for among agencies to collaborate in the future.

iii) Tanzania: The National Information and Communication Technologies Policy [9] recognises a need for an e-government infrastructure through which the public service (government departments and agencies) can communicate internally. The policy includes statements that address security in terms of legal framework and infrastructure.

iv) East Africa: The Regional e-Government framework [10] recognises security as a challenge that needs to be addressed in e-government projects. Furthermore, Information Security is recognised as a cross cutting issue and

declares that the operational efficiency of any e-government strategy will need strong backup support of necessary legislation on data security, network security, cyber crime, information systems and electronic transactions.

It was found that, all the e-government documents mention information security requirements for inter agency collaborations, although the factors listed in Section 2 of this paper have not been addressed in detail.

### 3.2.3 Results obtained from Questionnaires

Questionnaires were distributed to government agencies with the objective of soliciting information about information security practices in cross agency transactions. The respondents were managers responsible for technology functions in agencies that engage in cross agency transactions by the nature of their work. Twelve questionnaires were sent out and eight responses were obtained with 4 responses being from Tanzania, and 2 each from Uganda and Rwanda. The questions asked and the responses received are summarized in Table 2 below.

*Table 2: Survey Results for Information security in cross-agency transactions*

| | **Country (No of Respondents)** | | | |
|---|---|---|---|---|
| **Question - Response** | **Tanzania (4)** | **Rwanda (2)** | **Uganda (2)** | **Overall(8)** |
| Presence of Information Security policy - Yes | 75% | 100% | 100% | 87.5% |
| Type of cross agency transactions- Manually | 100% | 100% | 100% | 87.5% |
| Type of cross agency transactions -Email | 100% | 100% | 100% | 100% |
| Type of cross agency transactions -Access to Computer Systems | 50% | 0% | 50% | 37.5% |
| Information involved in transactions - Payment/ Financial | 75% | 50% | 50% | 62.5% |
| Information involved in transactions - Confidential | 75% | 50% | 100% | 87.5% |
| Main concerns in cross agency transactions - Fraud | 100% | 0% | 50% | 87.5% |
| Main concerns in cross agency transactions - Network Breakdowns | 50% | 0% | 100% | 50% |
| Security measures such as encryption - Yes | 75% | 100% | 100% | 87.5% |
| Binding agreements with regards to information security with partners - Yes | 50% | 0% | 0 | 50% |
| Common format for Data Exchange - Yes | 50% | 0% | 50% | 37.5% |
| Common terminology for transactions - Yes | 0% | 0% | 50% | 12.5% |
| Need for standards for cross agency transactions - Yes | 100% | 100% | 100% | 100% |

### 3.2.4 Discussion

From the above results the following observations are made:

- There is no significant difference in results between the three countries.
- There appears to be a correlation between the presence of an information security policy and the use of security for transactions. The agency without a security policy has no security measures in place for transactions.
- Fraud is a major concern in over 50% of the respondents
- Fraud is a bigger concern than network breakdowns.
- A need for standards is recognized by all agencies although only 37.5% and 12.5%of the respondents have common terminology for transactions and common data format exchange respectively.
- Although in the case of Rwanda the e-government report mentions that requirements/ standards of security, the questionnaires returned do not refer to the document, thus posing the question of whether government agency are aware of the standard.

## 4. Conclusions and Further Work

The results of our study show that from an Information Security perspective, some steps have been taken towards improving e-readiness in the East African community at an agency, country and regional level. However the of the factors outlined in section 2 of this paper are yet to be fully addressed. It can be concluded that the EAC has not fully reached e-readiness. The results of this study can also be related to work done by Rwangoga & Baryayetunga [11] who discuss e-Government in Uganda and describe successful delivery on institutional frameworks, legal frameworks, and ICT infrastructure.

In order to enhance e-readiness for an Information Security perspective, the following recommendations are made for East African countries:

i) The establishment of government – wide guidelines that encourage the establishment of Information Security policies in all government departments and agencies. The policies should address both inter and intra agency transactions as well as security requirements for interfaces with citizens.

ii) The establishment of Risk Management Frameworks for e-government transactions. The risk frameworks should identify risks and how to mitigate those risks.

iii) The establishment of an e-government security ontology for East Africa to ensure semantic interoperability. This could be modelled on the e-government ontologies that have been developed in the European Union [12] and United States[13].

In future research, we plan to look further at the development of a holistic framework to address Information Security in e-government. Such a framework would address standards, common terms, infrastructure and policies, all from the context of developing countries, and in particular, East Africa.

**5. References**


[1] UN E-Government Survey 2008: From E-Government to Connected Governance. 2008.

[2] R. M. De Villiers, Three Approaches as pillars for interpretive Information Systems Research: development research, action research and grounded theory. In proceedings of SAICSIT, 2005. ACM.2005

[3] J.K. Bakari, C.N. Tarimo, L.Yngstrom, and C. Magnusson, State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case Study, In Proceedings of the Fifth IEEE International Conference on Advanced Learning Techniques (ICALT'05). IEEE. 2005, pp 1007-1011.

[4] J.A. Chaula, L. Yngstrom, and S. Kowalski, Technology as a tool for Fighting Poverty: How Culture in the developing world affect the Security of Information Systems. In proceedings of the 4th IEEE International Workshop on Technology for Education in Developing Countries. IEEE. 2006, pp 66-70.

[5] J.K. Bakari, C.N. Tarimo, and B. Mutagahywa, Issues and Challenges to be Addressed in e-Government from an Information Security Point of View, In Proceedings of IST-Africa 2006 Conference, IIMC, 2006.

[6] J. Kaaya, The Emergence of E-Government Services in East Africa: Tracking Adoption Patterns and Associated Factors. In proceeding of Sixth International

Conference on Electronic Commerce. ACM. 2004, pp 438-445.

[7] Rwanda Information Technology Authority: Technical Standards and Guidelines for E-Government: Final Report, February 2006

[8] Republic of Uganda, Ministry of Works, Housing and Communications, E-Government Strategy and Action Plan Ver 1.1, Mar - 2004

[9] The United Republic of Tanzania, Ministry of Communications and Transport, National Information and Communications Technologies Policy, March 2003

[10] East African Community Secretariat, Regional e-Government Framework (Final Draft), December 2005

[11] N.T. Rwangoga, and A.P Baryayetunga. E-Government for Uganda: Challenges and Opportunities. International Journal of Computing and ICT Research, Vol.1 No. 1 June 2007, pp 36-46.

[12] European Union, Access e-Gov Project, http://www.accessegov.org/acegov/web/uk/index.jsp?id=50024, accessed 4 Feb 2009.

[13] Federal Enterprise Architecture Reference Model Ontology, http://web-services.gov/fea-rmo.html, accessed 4 Feb 2009

# TOWARDS A CONTEXT-AWARE ACCESS CONTROL FRAMEWORK IN WEB SERVICE TRANSACTIONS

**Carina K Wangwe, Mariki M Eloff, Lucas M Venter**

University of South Africa

carina.wangwe@gmail.com, +255 754 600512, Box 60049 Dar es Salaam

eloffmm@unisa.ac.za, +27 12 4296330, Box 392 UNISA 0003 SA

ventelm@unisa.ac.za, +27 12 4296330, Box 392 UNISA 0003 SA

***In proceedings of ISSA 2008 Conference, 7-9 July 2008 Johannesburg***

ABSTRACT

Interoperability across heterogeneous domains has become a reality through technologies such as Service Oriented Architectures and Web Services. These technologies have been put to use in e-Government and e-Business, enabling services to transact without human intervention. Such transactions, however, raise security concerns, as a human response to an authorization or access request can take into consideration semantics and the context in which the request is being made, while a machine to machine decision to grant access would rely on how well the XML based security policies have captured all semantic and contextual considerations.

This paper proposes a context-aware access control framework in a web services environment. The framework is based on the Organization for Advancement of Structured Information Standards (OASIS) for web services security and access control and extends these to include semantic interpretation of security attributes. Furthermore, the framework addresses contextual information that would affect an access control decision, in a web service transaction, such as legal or regulatory requirements.

KEY WORDS

Access Control

# 1 INTRODUCTION

With any collaboration, it is crucial to have unambiguous communications between the collaborators, to ensure that no information is either wrongly withheld or provided based on an ambiguous request.

For Web Service transactions, one way to achieve such communication is the use of a semantic framework to provide a basis for interpretation of access control requests depending on the context of the transaction within a given domain. Furthermore, where laws and regulations exist that govern the transaction, these have to be taken into consideration when applying the access control or authorisation policy. The framework would thus include an access control mechanism, semantic interpretation of access requests, a context service and a repository of relevant laws and regulations.

The Organisation of Advancement of Structured Information Standards (OASIS) has adopted standards such as the Extensible Access Control Markup Language (Oasis 2005a) and the Security Assertion Markup Language (Oasis 2005b) to address access control across heterogeneous domains. The Extensible Access Control Markup Language (XACML) is a policy language which uses XML statements to present access control policies while the Security Assertion Markup Language (SAML) is an XML-based security specification schema for exchanging authentication and authorization information. XACML and SAML both have extensibility mechanisms which allow them to be used for different implementation. Use of these standards alone does not however ensure the correct access control decisions in interacting web services. There is a need to ensure that those XML tags passed to request access are correctly interpreted in the context of the transaction.

The use of ontologies in web services has been promoted by the World Wide Web Consortium (W3C) which has recommended the Web Ontology Language (OWL) as a general ontology for the semantic web (W3C, 2004). OWL is based on the Resource Description Framework (RDF) schema which was an earlier specification from W3C. The ontology serves the purpose of clearly defining terms that are used in a transaction, and enables a semantic evaluation of terms to determine similar meaning. Specific ontologies

based on OWL or RDF have been proposed by Ceravolo (2003), Domingue et.al. (2004), and Dritsas et.al.(2005) for the e-Government domain.

For a specific ontology to be used, the context of the transaction must be taken into consideration. Context defines the conditions that must or must not hold in order for an authorisation policy to apply (McDaniel, 2003). Contextual information may include the location of the requester and the provider of the service or the time when the transaction is taking place. For transactions that are taking place in an E-Government or E-Business environment, the legal context may also be necessary. All contextual information needs to be captured and combined so as to act as input into the access control decision.

This paper presents a framework that comprises of a context service, ontological mapping mechanism and a legal repository which together with extended markup languages, support correct access control decisions in interacting web services. The remainder of the paper is structured as follows: Section 2 describes existing access control models for web services. Section 3 proposes a context –aware framework while section 4 looks at related work in this area and we conclude and look at further work in Section 6.

## 2 ACCESS CONTROL IN WEB SERVICE TRANSACTIONS

A major requirement of an access control model for web services is the handling of the dynamic nature of the transactions. Web services interact across disparate computing platforms, in different geographical locations and with different regulatory compliance requirements. In subsequent sub sections, we describe some access control models that have been proposed or implemented for web services.

### 2.1 Role Based Access Control (RBAC)

RBAC uses roles as a basis for access control decisions and was designed specifically with enterprise organisation structure in mind. RBAC allows the specification of security roles that map naturally to an organisation's authorisation structures. However RBAC does not entirely suit web service transactions and its weakness in open environments were identified by De Capitani di Vimercati and Samarati (2005). Several studies have subsequently been

done to extend the RBAC model in order to address some of the weaknesses (Demchenko et.al, 2007).

## 2.2 Attribute Based Access Control ABAC

In recent years, there has been a shift to looking at attributes as a basis for access control in a web services environment. (Coetzee and Eloff, 2007; Damaini et. al, 2005; Shen and Hong, 2006; Yuan and Tong, 2005). Attributes describe the characteristics of the requester, and may be a combination of identity and role. Attributes may be subject attributes, resource attributes or environment attributes. The ABAC model comprises of an Attribute Authority, Policy Enforcement Point, Policy Decision Point and Policy Authority.

It has been recognized that there is still a need for the usage of semantics and or ontologies to ensure correct access control decisions with the ABAC model, and some research to that end has been done. (Preibe et.al; 2006; Warner et.al, 2007).

## 2.3 Context Aware Access Control

Both RBAC and ABAC paradigms do provide ways to include contextual information (Bacon et.al, 2002; Huselboch et.al., 2005; Strembeck and Neumann, 2004). However other access control models that focus primarily on context have been proposed. These include:

### 2.3.1 Governance Based Access Control

The idea as presented by the Centre for Governance Institute (2005) is that transactions in which information is shared must be governed by the relevant legislation to which the organizations sharing the information are accountable. Thus any request for information is checked against the existing laws or regulations before it is granted.

### 2.3.2 Session Based Access Control (SBAC)

In session based access control, the context of a transaction is limited to a session. Access to resources is based on the attributes of the subjects and the properties of the objects but the rights that can be applied at a given time are limited based on the context defined by the access session (Fernandez and Pernul, 2006)

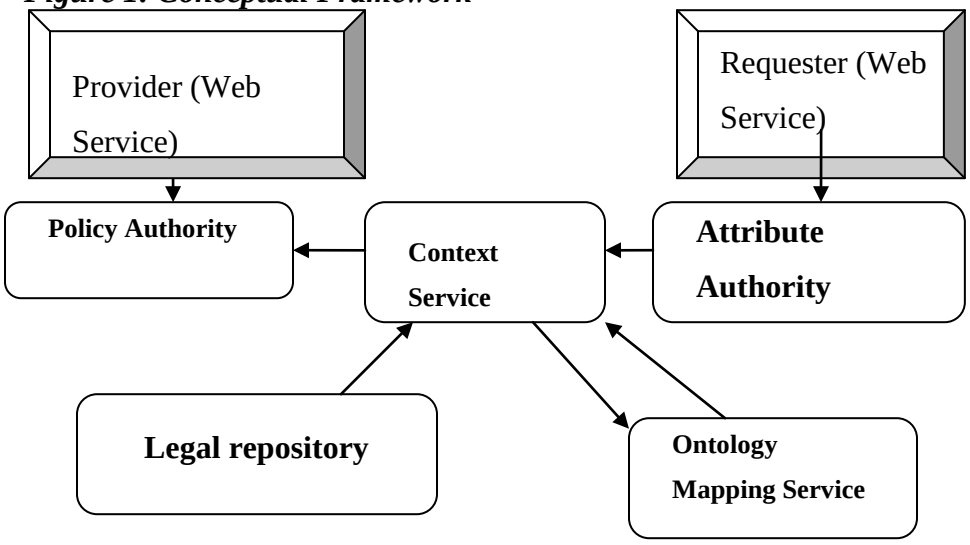
### 2.3.3. Location-Based Access Control (LBAC)

LBAC takes requester's physical location into account when determining their access privileges. The physical location may be combined with other attributes related to identity or role of the requester. Ardagna et.al (2006) propose combining location with user credentials to support access control decisions.

## 3 PROPOSED FRAMEWORK

In order to achieve correct access control decisions in the context of a web service transaction, we propose a framework based on the ABAC model. The proposed framework is illustrated in Figure 1 below:

***Figure 1: Conceptual Framework***




Each of the components of the framework works as follows:

### i) Policy Authority

The policy authority contains the Policy Decision Point (PDP) and Policy enforcement points that evaluate the requester's attributes against the providers XACML policy. In order to evaluate the compliance with legal requirements XACML is extended to include a function that accepts environment attributes and compares against relevant laws and regulations within the legal repository. This operation will be stated as a XACML obligation in the

Provider's policy. If there is no legal requirement for a particular transaction, then the request is granted provided the other requirements of the policy are met.

**ii) Attribute Authority**

The attribute authority issues SAML assertions to the requester. The attribute assertions correspond to the subject, resource and environmental attributes of the requester. If there is a legal requirement on the requester's side that has to be complied with, this requirement is passed in a SAML condition statement.

**iii) Ontological mapping service**

The ontological mapping services checks the semantics of the requester's attributes match with those in the provider's policy. A mechanism to conduct such a mapping has been described by Patil et.al (2007). If unknown vocabularies are used, ontology mediators may be used (Kolter, et.al, 2007).

**iv) Legal repository**

The legal repository contains laws and regulations that apply to different transactions. The legal repository contains the conditions in which a transaction is considered legal or illegal. The legal repository is a database which with several indexes to allow multiple matching by the Context Service.

**v) Context Service**

The context service is a key element of the framework and is adapted from Lei et.al. (2002). The role of the context service is to combine the results from the ontological mapping mechanism and the legal repository into an environmental attribute that is then passed to the attribute authority for authorisation and access control decisions to be made. To illustrate how the framework could be applied, consider the following illustrative example:

A request for information is made in a criminal investigation where a national of Country A is suspected of committing a crime in Country B; and the suspected criminal is now in resident in Country C. In order for the service in Country C to decide whether to authorise access to the information the following requirements must be met:

- The penalty for the crime in Country C must be evaluated against the penalty for the crime in country A. If conviction may result in a death penalty, then Country C must refuse to provide information.
- The crime committed in Country B must be interpreted in the context of the laws of country C.
- Laws of country A must be examined to see if they have any relevance in the crime and or penalty for the crime

Thus for this example the service provider would need access to a legal repository of the countries' laws and also to the ontological mapping mechanism to make semantic comparisons as to whether or not all necessary conditions to grant the requested information hold.

## 4 Related work

There are various studies that have been done in relation to context – aware and or semantic – aware authorisation and access control. The studies that are pointed out below are those that address context in access control decisions with some reference to semantics.

Demchenko et al. (2007) use XACML to handle policy and base on RBAC with a Domain Resource Management model. The study argues that domain based access control provides several benefits including dynamic context management. However interpretation of attributes is not addressed by the study. Toninelli et.al (2006) also draw inspiration from the RBAC model and associate the context in which a subject transacts directly with the role that the subject plays in that transaction.

Hu and Weaver (2006) look at the healthcare domain and provide a formal definition of context and context constraints. The definition of context is restricted to time, location, user type, object type and object ID. Context is built into the policy language and WS policy is used for the implementation.

Kolter et al. (2007) describe a semantic aware security architecture which includes an ontological mapping mechanism. The architecture is based on the ABAC model, but does not specifically address how contextual attributes would be handled.

Our work, as presented in Section 3 above, takes into consideration both semantics and contextual information with emphasis on legal requirements.

## 5 Conclusion and Further Work

We have presented a framework that comprises of a context service, ontological mapping mechanism and a legal repository which together with extended markup languages support corrects access control decisions in interacting web services. The inclusion of a legal repository make the framework especially useful for e-Government or e-Business transactions that take place across two or more legal domains where different regulations may apply to the transaction. Thus combine with the ontologically mapping mechanism that address semantic interpretation of attributes, the framework lays a basis for correct access control decisions based on the context of the transaction.

Future work shall include formalising a model based on the proposed framework and evaluating the framework in against requirements for access control architectures (Keromytis and Smith, 2007) when the framework is implemented in a practical setting.

## 6 References

Ardagna, C.A., Cremonini, M. & Damiani, E. (2006). *Supporting Location – Based Conditions in Access Control Policies.* Proceedings of ASIACCS'06 held in Taipei. ACM.

Bacon, J., Moody, K. & Yao, W. (2002).A Model of OASIS Role-Based Access Control and Its Support for Active Security. *ACM Transactions on Information Security and Systems Security*, 5(4): 492:540.

Centre for Governance Institute (CGI). (2005). Governance Based Access Control (GBAC): Enabling improved information sharing that meets compliance requirements. Available from http://www.cgi.com/cgi/pdf/cgi_whpr_63_gbac_e.pdf.(Accessed 1 April 2008).

Ceravolo, P. (2003). *Managing identities via interactions between ontologies.* Proceedings of the OTM Workshop held in Catania.

Coetzee, M & Eloff, JHP. (2007). A Trust and Context Aware Access Control Model for Web Service Conversations. *Lecture Notes in Computer Science*, 4657:115:124

Damiani, E., de Capitani di Vimercati, S., & Samarati, P. (2005). *New Paradigms for Access Control in Open Environments*, Proceedings of the fifth IEEE International Symposium on Signal Processing and Information Technology. IEEE.

De Capitani di Vimercati, S. & Samarati, P. (2005). New Directions in Access Control. In Cyberspace *Security and Defense: Research Issues*. Edited by Kowalik, J & A Sachenko, A. Kluwer Academic Publisher.

Demchenko, Y., Gommans, L., & de Laat, C. (2007). Role Based Access Control Model for Distributed Multidomain Applications. In *New Approaches for Security, Privacy and Trust in Complex Environments*.Edited by Venter, H. Eloff, M., Labuschagne, I.., Eloff, J., & von Solms, R. IFIP International Federation for Information Processing.

Domingue, J., Gutierrez, L., Cabral, L., Rowlatt, M., Davies, R., & Galizia, S. (2004,). WP9: Case Study eGovernment D9.3 e-Government Ontology. Available from http://www.dip.deri.org/documents/D9-3-improved-eGovernment.pdf (Accessed 14th March 2008)

Dritsas, S., Gymnopoulos L., Karyda M., Balopoulos, T., Kokolakis, S., Lambriniudakis C., & Gritzalis S. (2005). *Employing Ontologies for the Development of Security Critical Applications: The secure e-poll paradigm*. Proceedings of the International Conference on eBusiness, eCommerce and EGovernment held at Turku. IFIP.

Fernandez & Pernul, (2006) *Patterns for Session Based Access Control.* Proceedings of Pattern Languages of Programming Conference held at Portland.

Keromytis, A.D & Smith J.M. (2007).Requirements for Scalable Access Control and Security Management Architectures.*ACM transactions on Internet Technology (* 7) 2.

Hu, J. & Weaver A.C. (2006) Dynamic , Context – Aware Access Control for Distributed HealthCare Applications . Available at http://www.cs.virginia.edu/papers/p1-hu-dynamic.pdf

Huselbosch, R.J., Salden, A.H., Bargh, M.S., Ebben, P.W.G, & Reitsma, J. (2005) *Context Sensitive Access Control*. Proceedings of SACMAT'05 held in Stockholm. ACM.

Lei, H., Sow, D.M. Davis, J.H., Banavar, G. & Ebling, M.R. (2002).The Design and Applications of a Context Service.*ACM SIGMOBILE Mobile Computing and Communications Review* (6) 4: 45:55.

McDaniel, P. (2003). *On Context in Authorization Policy.* Proceedings of SACMAT 2003 held at Como, Italy. ACM.

OASIS, (2005 a), XACML v2.0 Documentation. Available at http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml (Accessed 15th March, 2008)

OASIS, (2005 b) SAML v2.0 Documentation. Available at http://docs.oasis-open.org/security/saml/v2.0/ (Accessed 15th March 2008).

Patil, V., Mei, A. & and Mancini, L. (2007). *Addressing Interoperability issues in access control models.* Proceedings of ASIACCS'07 held at Singapore. ACM.

Priebe, T., Dobmeier, W. & Kamprath, N (2006), *Supporting Attribute-based Access Control with Ontologies.*Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06) held at Vienna. IEEE Computer Society.

Shen, H & Hong, F (2006).*An Attribute – Based Access Control Model for Web Services*. Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06) held at Taipei.

Strembeck, M. & Neumann, G, (2004).An Integrated Approach to Engineer and Enforce Context Constraints in RBAC Environments.*ACM Transactions on Information and System Security*, ( 7) 3: 392:427.

Toninelli, A., Montanari, R., Kagal, L., & Lassila, O. (2006).A Semantic Context – Aware Framework for Secure Collaborations in Pervasive Computing Environments.*Lecture Notes in Computer Science*, (4273): 473-486

Warner, J., Atluri, V., Mukkamala, R., &Vaidya, J. (2007). *Using semantics for automatic enforcement of access control policies among dynamic coalitions*, In Proceedings of SACMAT 2007.

W3C (2004).OWL Web Ontology Language Overview. Available from http://www.w3.org/TR/owl-features (Accessed 2nd May 2008)

Yuan, E. & Tong, J. (2005).*Attribute Based Access Control (ABAC) for Web Services.* In Proceedings of the IEEE International Conference on Web Services (ICWS'05) held at Orlando. IEEE Computer Society.

# A Proposed Implementation of SAML V2.0 in an e-Government Setting

**Carina K. WANGWE[a], Mariki M. ELOFF[b], Lucas M. VENTER[b]**

[a]*University of South Africa, P.O.Box 60049,Dar es Salaam,Tanzania*

*Tel: +255 754 600512, Fax: + 255 22 2117772, Email:carina.wangwe@gmail.com*

[b]*University of South Africa, P.O.Box 392 UNISA 0003 South Africa*

*Tel: +27 12 4296330 Fax: + 27 12 4296771, Email:eloffmm/ventelm@unisa.ac.za*

***In proceedings of IST-Africa 2008 Conference Proceedings, Paul Cunningham and Miriam Cunningham (Eds), Published by IIMC International Information Management Corporation, 2008***

**Abstract:** Developing countries are increasingly undertaking e-government initiatives in order to provide more efficient and cost-effective services to citizens. Such initiatives involve collaboration within government agencies and with other organisations in order to access information and to exchange data for transactions. One of the issues that need to be addressed in any e-Government initiative is Information Security. The Organization for the Advancement of Structured Information Standards (OASIS), a non-profit International consortium, that drives the development and adoption of e-business standards, adopted the Security Assertion Markup Language Version 2.0 in March 2005 (SAML V2.0). SAML is an XML-based framework for exchanging security assertions about authentication, authorization and attributes. SAML is particularly suited to e-Government transactions because it is platform independent and can be used with other security related technologies such as PKI, Smartcards and Biometrics in order to provide end to end security for transactions in an e-Government collaboration. This paper discusses a proposed SAML implementation in an e-government setting with specific focus on pensions administration.

**Keywords:** e Government, Security, Web Services, Access Control

## 1. Introduction

The concept of e-Government has been greatly enabled by advances in Internet related technologies and has been pushed by the need of Governments to provide efficient, effective, affordable and quick services to citizens. In order to provide e-Government services information security is one aspect that needs to be addressed. While developing countries are making steady progress in terms of building infrastructure and providing access to digital information and services to their citizens, it is important that measures to ensure the security of that information are taken as part of any e-Government initiative.

The security requirements for e-Government that are considered in this paper are

- Authentication;
- Privacy;
- Authorization and Access Control;
- Data integrity and
- Trust.

The objective of this work is to illustrate how SAML v2.0 can be used to meet the security requirements in an e-Government implementation using the case of pensions administration.

The remainder of the paper is structured as follows: Section 2 outlines the motivation for this work; Section 3 contains an overview of related work on information security in e-Government followed by a brief overview of SAML V2.0, in Section 4. The fifth section describes how the Security Assertion Markup Language can be used to meet the e-government security requirements. Section 6 illustrates the usage of SAML in the processing of a benefit by a pensions administrator in collaboration with other government agencies. Section 7 outlines the limitations of the proposed implementation in meeting all security requirements that are envisaged for an e-government setting. The paper concludes with a summary.

## 2. Motivation

In most developing countries, Governments are faced with resource constraints in providing services to citizens. While e-Government is a tool that can promote better and more efficient

services, it is also expensive and requires good planning. In East Africa, for example, a regional e-Government framework has been drafted [1] but implementation of the various initiatives has been slow. The measure of how ready a country is for E-government is based on criteria such as connectivity, political priorities, information security, human capital and e-Business climate. The implementation of a platform independent standard such as SAML is a way to reduce the cost of addressing the information security component of an e-Government initiative and thus contributing to the success of an e-Government implementation.

## 3 Related Work

Several studies have been done in relation to security requirements in an e-government setting. The areas of research include general approaches to security requirements engineering, architectures for trust models and security management. Kalloniatis [2] analyses frameworks for security requirement engineering in e-government applications and concludes that the current frameworks do not adequately cater for security requirements for users to keep information safe and secure.

Specific projects in the e-government arena have been described such as the eMayor project where Oikonomidis et.al [3] propose a trust model for web service interaction among different government agencies. Within the same eMayor project, Meneklis et.al [4], describes the use of SAML for identity management, so as to provide standardized administration and transfer of authentication attributes by embedding them in SOAP messages. Arcieiri et.al [5] proposes an architecture for communication of digital personal data amongst government agencies, although the approach here uses PKI rather than SAML.

This paper describes how the Security Assertion Markup Language, in itself, and together with other technologies can be used to address the security requirements for e-government.

## 3 An Overview of SAML V2.0

The Organization for the Advancement of Structured Information Standards (OASIS), a non-profit International consortium, that drives the development and adoption of e-business standards, adopted the Security Assertion Markup Language Version 2.0 in March 2005 (SAML V2.0). SAML is an XML-based framework for exchanging security assertions about authentication, authorization and attributes. SAML defines the syntax and processing semantics of assertions made about a subject by a system entity [6].

An assertion is defined as a piece of data regarding either an act of authentication performed on a subject, attribute information about the subject, or authorization data applying to the subject with respect to a specified resource [6]. Assertions are produced by a SAML authority, which is an abstract system entity in the SAML domain model. The user or web service requesting assertions from the SAML authority is called the Requester. These assertions are then used in communicating with an entity called a Responder, who utilises those SAML assertions to respond appropriately to the Requester.

SAML assertions are of three kinds i.e. Authentications, Attribute and Authorization Decision. In a web services environment, SAML assertions may be carried within a SOAP message. Other than assertions, SAML is also composed of protocols, bindings and profiles. Protocols allow service providers to request for assertions, request for authentication and to request for name identifier registration and mapping. Bindings are the mappings from SAML request-response message exchanges into standard messaging or communication protocols such as SOAP and HTTP. A profile of SAML defines constraints and/or extensions in support of the usage of SAML for a particular application [7]. SAML V2.0 comes as an improvement on SAML 1.1, by incorporating new attribute profiles and metadata specifications to improve communications among businesses in a federation. In particular, SAML V2.0 provides Convergence, Federated Identifier Management, Privacy Mechanisms and Session Management as additional functionality [8].

## 4 Application of SAML V2.0

SAML V2.0 addresses the security requirements for an e- government setting as outlined in Section 1 above, in the following manner:

- **Authentication**: A SAML authentication assertion, simply asserts that authentication was indeed provided by the service requestor, the method of authentication used, and who did the authentication. An authentication services such as LDAP has to provide the actual authentication. For example, the following portion of an assertion:

  <saml:AuthnStatement AuthnInstant=2006-04-12T16:57:30.000Z”>

  indicates the time and date of an assertion; while

  <saml:AuthnContext><saml:AuthnContextClassRef>

  urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos

indicates that the authentication was done through a local server in order to acquire a Kerberos ticket for subsequent use.

- **Privacy:** SAML V2.0 defines how pseudonyms can be used between providers to represent the entity that has been authenticated. This is achieved through the NameID element. In addition, SAML includes mechanisms to allow providers to communicate privacy policy and settings
- **Authorization and Access Control:** SAML authorization decision assertions indicate what resources the subject is allowed to access. Furthermore, SAML attribute assertions may be used to describe the role that the subject hold in the context of the particular transaction. For example:

  <saml:AuthzDecisionStatement
  Resource="http://civilregistry.go.tz/birthdateregister.html"
  Decision="Permit">
  <saml:Action>GET</saml:Action></saml:AuthzDecisionStatement>

  indicates that permission has been granted to access web page birthdateregister.html. An example of an attribute assertion would be:

  <saml:AttributeStatement><saml:Attribute>
  NameFormat=http://pensions123.co.tz Name="MemberType"
  <saml:AttributeValue> pensioner </saml:Attribute>
  </saml:Attribute></saml:AttributeStatement>

- **Data Integrity:** In SAML implementations, it is possible to confirm that data integrity has not been compromised, that is, a given message has not been altered during transmission. This is done through the use of XML signatures, and additional security related technologies such as PKI. Furthermore network protocols such as IPSec and RFC2246 can be used to secure SAML traffic.
- **Trust:** Trust is achieved by using a separate authority (trusted third party) to issue security tokens which are acceptable to all parties. In the case of a SAML implementation, the trusted authority would issue SAML assertions to confirm the authenticity and access rights for the service requester.

## 5 SAML Implementation

The case used to illustrate the use of SAML is the processing of a death/ survivors pension. In many developing countries, mandatory pensions are governed by law and administered directly by Government or through Government Agencies. Pensions Administrators typically handle large volumes of confidential data and fraud is a common problem, with a high proportion of fraud resulting from claims for benefits based on forged information.

Web services are increasingly being adopted in pensions administration [9,10]. The use of web services enables Pensions Administrators to reduce human intervention in the processing of claims and to reduce the dependence on documents submitted by the intended beneficiary, thus reducing the possibility of fraud. These transactions require interaction between several external agencies and thus there arises a need to have trusted ways to provide identification, authentication and authorization for the users and or services that access the data.

In the implementation of SAML, the agencies involved need a trusted third party, also called a SAML authority to issue SAML assertions. In order for the Pensions Administrator's web service to access the web services and servers of the other agencies, the Pensions Administrator must have valid authentication and the appropriate authorizations. Rather than negotiate for access permissions with each of the agencies individually, the Pensions Administrator would request for assertions from the SAML authority who is trusted by all the other agencies. In an e-Government setting, this could be the agency that regulates the Financial and Pensions Industry.

The trusted third party would produce the SAML assertions to be issued to the Pensions Administrator and perform the initial authentication for the Pensions Administrator. Trust between the third party and each of the collaborating agencies would be pre-established. The trust relationship could be both credential and reputation based [11]. Figure 1 below shows how a death (survivors) benefit would be processed.

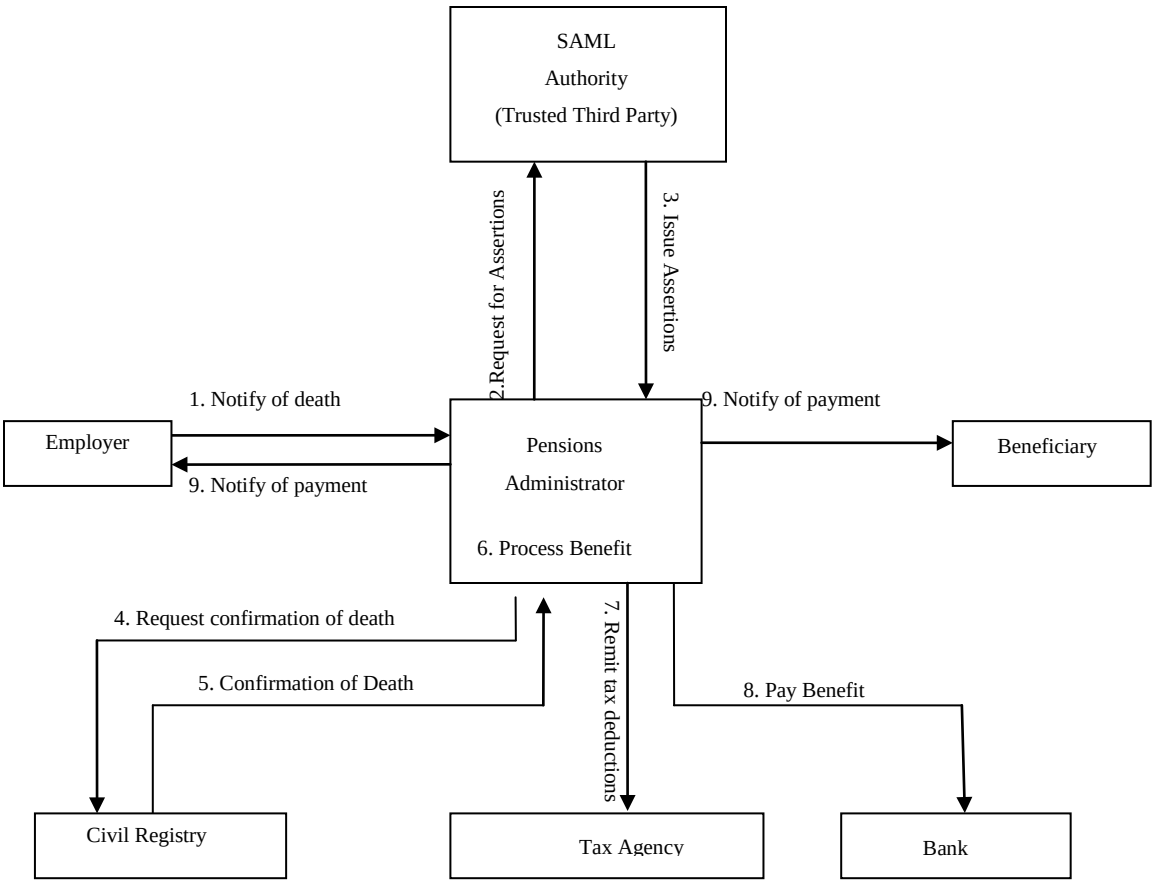



Figure 1 **Death Benefit Scenario**

The assertions issued to the Pensions Administrator would be passed from service to service, with the role changing if necessary, through the use of Attribute Assertions, for each interaction. For example, the role of the Pension Administrator when interacting with the Civil Registry is different from the role with the Bank. With the Civil Registry, the Pension Administrator would simply be performing an enquiry on the data, while with the Bank, the Pension Administrator should be able to authorise a transfer of funds from one account to another. The assertions for the Death/ Survivors benefit scenario could be as shown in table 1 below.

**Table 1. Assertions issued to Pensions Administrator in Death Benefit Scenario**

| Responder | Assertion | | |
|---|---|---|---|
| | Authentication | Attribute | Authorization Decision |
| Civil Registry Office | Pensions Administrator is identified as a trusted client who can access the local server of the Civil Registry office | The role of the Pensions Administrator is an Enquirer i.e. can query the Death register in order to confirm details as submitted by the employer. | Permit access to Death Register |
| Tax Agency | Pensions Administrator is identified as a trusted client who can access the local server of the Tax Agency | The role of the Pensions Administrator is a Tax Payer i.e. can transfer deductions from benefits into the Tax Agency Account | Permit execution of transfer to payment to Tax Agency account |
| Bank | Pensions Administrator is identified as a trusted client who can access the local server of the Bank | The role of the Pensions Administrator is a bank client i.e. can transfer benefit payments into beneficiary accounts. | Permit execution of transfer from Pensions Administrator's Account into Beneficiary's account. |

In particular, the interaction between the Pensions Administrator and the Civil Registry could be achieved as illustrated in the SAML code below:

<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0" IssueInstant="2006-04-12T17:20:32">

<saml:Issuer>http://authority.go.tz/</saml:Issuer><ds:Signature>.</ds:Signature>

<saml:Subject><saml:NameID format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"> pension123 </saml:NameID></saml:Subject>

<saml:AuthnStatement AuthnInstant="2006-04-12T17:21:00" SessionIndex="1000001">

<saml:AuthnContext><saml:AuthnContextClassRef>

urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransportKerberos

</saml:AuthnContextClassRef></saml:AuthnContext>

</saml:AuthnStatement>

<saml:AttributeStatement><saml:Attribute> NameFormat="http://civilregistry.go.tz" Name="ClientType" <saml:AttributeValue> Enquirer </saml:AttributeValue>

</saml:Attribute></saml:AttributeStatement>

<saml:AuthzDecisionStatement

Resource="http://civilregistry.go.tz/deathregister.html"

Decision="Permit"><saml:Action> GET </saml:Action>

</saml:AuthzDecisionStatement>

</saml:Assertion>

## 6 Limitations

The SAML implementation proposed in this paper, assumes that there exists a pre-established trust framework between the Government agencies involved in the e-Government transaction. Furthermore, the implementation only addresses agency to agency collaborations through web services, and not how the citizen shall finally receive the service. In order to fully address trust issues, an extension to SAML could be developed, based on a trust model described by Thomas A. and Venter L. [12], for the establishment of a trust relationship between a user and a complex web service. Other approaches to trust establishment have been described in various studies [13, 14]. Furthermore, SAML can be extended to cover various scenarios as described by Bertino and Squicciarini [15] for partial authorisations, and by Canovas [16] for handling non- SAML complaint credentials. Additional authentication mechanisms could be implemented for the human to service interfaces such as Biometrics.

## 7 Conclusion

A successful e-Government implementation requires the confidence of the key users of e-government systems, that is, citizens and service providers (government agencies). Such confidence can be obtained through providing secure transactions in a trusted environment. SAML v2.0 as described in this paper, addresses the security requirements for e-government, in itself or together with other technologies. As a standard, SAML would provide a platform independent and proven way to implement information security requirements in an e-government initiative.

For developing countries, e-Government initiatives can be boosted through the use of a standard such as SAML to address Information Security requirements. Further work however needs to be done to incorporate the proposed SAML implementation into a framework based on existing information security policies of government agencies and placed in the context of existing legal and regulatory requirements with regards to information security.

## 8 References


[1] East African Community Secretariat, Regional e-Government Framework, Final Draft (December 2005)

[2] C. Kalloniatis, E.Kavakli, and S.Gritzalis, Security Requirements Engineering for e-Government Applications: Analysis of Current Frameworks, *Lecture Notes in Computer Science,* 3183 66 – 71 (2004)

[3] N. Oikonomidis, S.Tcaciuc and C.Ruland, Provision of Secure Policy Enforcement Between Small and Medium Governmental Organizations, *Lecture Notes in Computer Science,* 3592 141 -150 (2005)

[4] B. Meneklis, A.Kaliontzoglou, C.Dougligeris. and D.Polemi, Engineering and Technology Aspects of an e-Government Architecture Based on Web Services, In: *Proceedings of the Third European Conference on Web Services (ECOWS'05),* 118 – 129. (2005)

[5] F. Arcieiri, F. Fioravanti, E. Nardelli, and A. Talamo, A Layered IT Infrastructure for Secure Interoperability in Personal Data Registry Digital Government Services, In: *Proceedings of the 14th International Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications* , 95-102 (2004)

[6] OASIS, SAML v2.0 Documentation,(December 12,2005), http://docs.oasis-open.org/security/saml/v2.0/

[7] OASIS, SAML V2.0 Executive Overview, (April 12, 2006), http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf

[8] P. Madsen, SAML V2.0 : the building blocks for federated identity, (February 22, 2006), http://www.xml.com/pub/a/2005/01/12/saml2.html.

[9] International Social Security Association (ISSA), Implementing electronic services in social security: Transnational Guidelines and Perspectives, (October 16, 2006), http://www.issa.int/pdf/marrakech06/2franke.pdf

[10] D. Spadaccia, INPS Replatforming: Migration of the Front-End Applications from AS/400 Legacy Environment to Microsoft.Net, (March 17, 2006), http://www.issa.int/pdf/IT/2spadaccia.pdf.

[11] D. Artz and Y. GIL, A Survey of Trust in Computer Science and the Semantic Web, (March 20, 2006); http://www.isi.edu/~dono/pdf/artz06survey.pdf.

[12] A. Thomas and L.Venter, Propagating Trust in the Web Services Framework. In: *Proceedings of the ISSA 2004 enabling tomorrow Conference*,( 2004.)

[13] Z. Wu. and A.C. Weaver, Dynamic Trust Establishment with Privacy Protection for Web Services, In: *Proceedings of the IEEE Conference on Web services (ICWS'05)*, 811-812 (2005)

[14] E.R. De Mello and J.S. Fraga, Mediation of Trust across Web Services, In: *Proceedings of the IEEE Conference on Web services (ICWS'05)*, 515-522 (2005)

[15] E. Bertino and A.C. Squicciarini, A Flexible Access Control Model for Web Services, *Lecture Notes in Artificial Intelligence*, 3055 13-16 (2004)

[16] O. Canovas, G. Lopez and A.F. Gomez-Skarmeta, A Credential Conversion Service for SAML –based Scenarios, *Lecture Notes In Computer Science*, 3093 297-305. (2004)