

An Interoperable Identity Management Solution for Kenya E-Government

Christian Alemayehu
John Mwangi

Master program
Master of Science in Information Security

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering

Acknowledgement

We would like to praise God the Father, for His infinite merciful Love. We would also like to thank our supervisor, Professor Ann Hägerfors for a very grateful advice and expertise throughout the year. Ultimately and most importantly, the cheers go to our families for their support and encouragement throughout the year.

Christian Alemayehu

&

John Mwangi

Abstract

Identity management and the integrated technologies plays a big role to recommence administrative processes and promote e-government development by bringing services closer to citizens and the economy. It is a means of providing interoperability of records and the integration of data sources. Business processes, policies and current practices supports such administration. It comprises the competence and integrity of public authorities, personal privacy principles, legal and regulatory issues, systems and technology. Several technologies and frameworks have been developed to carry out the necessary activities related to identity management. In this thesis, we propose a framework for Kenya e-Government initiative with the most important solutions currently available, namely the Security Assertion Markup Language, the Liberty Alliance framework, web services and virtual private networks. We first identify what identity management is and the integrated disciplines and technologies in general. We then identify and analyse the perceptions of citizens' which is the single most significant obstacle to the widespread adoption of electronic identity management. Finally, we produced a model that can be used as a framework for addressing privacy protection and security issues and for choosing the technology to be used by the government for identity management with respect to the Kenyan identity policy, legislation, culture, and existing infrastructure.

KEYWORDS: Identity management, Federated identity, Security Assertion Markup Language (SAML), Liberty Alliance, Web Services, Virtual Private Network (VPN).

Table of Contents

Chapter 1

1.1.	Introduction.....	1
1.2.	Background.....	2
1.2.1	Short term initiatives.....	3
1.2.2	Middle term initiatives.....	3
1.2.3	Long-term initiatives.....	3
1.3.	Problem definition.....	4
1.4.	Research objective.....	5
1.5.	Research question.....	6
1.6.	Delimitations.....	6
1.7.	Thesis project outcomes.....	7
1.8.	Thesis chapter structure.....	7

Chapter 2

2.1.	Overview of Identity Management.....	9
2.2.	Approaches to identity management.....	11
2.2.1	Silo or Isolated Identity System.....	11
2.2.2	Centralized Identity System.....	12
2.2.3	Federated Identity System.....	13
2.2.4	User Centric Identity System.....	14
2.3.	E-Government portal of Kenya.....	16
2.4.	Infrastructural connection between government agencies in Kenya.....	21
2.5.	Comparison of Identity Management with other jurisdictions.....	21
2.5.1	Australia.....	22
2.5.2	New Zealand.....	23
2.5.3	Mauritius.....	25
2.5.4	Austria.....	25
2.6.	Cultural, legal and social impacts of Identity management.....	27
2.7.	Challenges.....	28
2.8.	Conclusion.....	29
2.9.	Research findings.....	30

Chapter 3

Integrated technologies in identity management.....	31
3.1 Introduction.....	31
3.2 Web Services	33
3.3 Liberty Alliance project.....	39
3.4 Security Assertion Markup Language (SAML)	41
3.5 Virtual Private Network (VPN)	44
3.6 Conclusion.....	45
3.7 Research findings.....	46

Chapter 4

Methodology	47
4.1 Research Purpose.....	47
4.2 Research Approach	48
4.3 Research Strategy.....	50
4.4 Sample selection.....	51
4.5 Data Collection Methods	52
4.5.1 Primary data Collection	52
4.5.2 Secondary Data Collection.....	53
4.6 Methods Problem	53
4.6.1 Reliability.....	53
4.6.2 Validity	54
4.7 Conclusion.....	55

Chapter 5

Citizens' Perception of Identity Management	56
5.1 Introduction.....	56
5.2 Survey statements	57
5.3 Results and Analysis.....	57
5.3.1 Demographics.....	57
5.3.2 Overall results and Analysis.....	57
5.4 Conclusion and key findings.....	62

Chapter 6

System Model.....	63
6.1 Introduction.....	63
6.2 Business Modeling Domain.....	63
6.2.1 Legislation.....	64
6.2.2 Common disciplines.....	64
6.2.3 Projects and initiatives.....	65
6.2.4 National Governance.....	65
6.2.5 Local governance.....	65
6.3 System model portal.....	65
6.3.1 Identity management process.....	66
6.3.2 Types of Identity.....	66
6.3.3 Identity Technologies.....	66
6.3.4 Identity Lifecycle.....	67
6.3.5 System model interfaces.....	67
6.3.6 Sample Use Case for Searching Citizen's Information.....	69
6.4 Conclusion.....	70

Chapter 7

Evaluation and Conclusion.....	72
7.1 Introduction.....	72
7.2 Integration of the research to the System Model development.....	72
7.3 Evaluation against Aims and Objectives.....	73
7.3.1 Objective 1.....	73
7.3.2 Objective 2.....	73
7.3.3 Objective 3.....	74
7.4 Limitations and future work.....	74
7.5 Lessons learned.....	75
7.6 Conclusion.....	75

References.....	77
-----------------	----

Appendix A	85
------------------	----

List of Tables

Table 2.1 - Selected country comparison of technologies used by governments to deliver online services to their citizens 27

Table 3.1 - Comparison among different approaches to Federated Identity Management..... 43

List of Figures and Illustrations

Figure 2.1: The Silo Model	12
Figure 2.2: The Centralized Model	13
Figure 2.3: Multi-organization Single-Sign-On in the Federated Model	13
Figure 2.4: Enterprise centric Federated Identity Model	14
Figure 2.5: User centric Identity Model	15
Figure 2.6: Snapshot of e-Government portal	18
Figure 2.7: Snapshot of the Kenya Revenue Authority page	19
Figure 2.8: Snapshot of Immigration Department webpage	20
Figure 2.9: Snapshot of Australian Government agency personnel's login interface for cross - agency information access and sharing	23
Figure 3.1: Web services architecture	33
Figure 3.2: Web Services Standards Stack	35
Figure 3.3: Web Services Security Standards	38
Figure 3.4: Security considerations for a Web service application	39
Figure 3.5: Liberty Alliance Architecture	41
Figure 6.1: Business Model Domain for e-identity management system	64
Figure 6.2: Portal structure of e-identity management system model	65
Figure 6.3: Login Interface	68
Figure 6.4: Search Criteria Interface	69
Figure 6.5: Results Interface	70

1.1. Introduction

Globalization and information and communication revolution are the main reasons for governments to transform the way of using information and delivering public goods and services to citizens by orchestrating services and systems. This transformation demands the ability of sharing vast amount of data and information spotted across a wide range of internal and external computing systems and managing its access. The realization of this transformation mainly depends on Electronic Government which in turn relies on regulatory, organizational and technical components. As defined by (Gartner group, 2000) e-government is ‘the continuous optimization of service delivery, constituency participation and governance by transforming internal and external relationships through technology, the Internet and new media.’

Electronic Government is all about the use of Internet based information technologies and IT applications by the government for the delivery of smooth electronic services and information to the public, businesses or another government agencies by integrating processes. Moreover, it demands safe channels for information exchange without compromising security or exposing sensitive information between government agencies, citizens and structured organizations. In line with OECD (2005) the determinants for the success of E-Government are ‘available technologies and their interoperability, level of access that citizens and business will have, citizens’ attitude and awareness of e-Government services, the overall trust in electronic channels by citizens and business, and their expectations of the types of services that should be delivered and how they should be delivered.’

As E-Government basically rely on personal information (Lips et al., 2007) the level of access that government agencies, citizens and businesses will have is basically determined by the Identity Management (IdM) employed in the E-Government system. Electronic Identity Management (eIdM) refers to the management of digital identities or digital identity data by maximizing security (information protection) and minimizing cost and redundant effort. Furthermore, it refers to the rules and procedures followed for manipulation of different digital identities (EUC Workshops et al, 2007). The implementation and use of reliable system of electronic Identity Management helps citizens, businesses and government agencies to effortlessly identify themselves and certify their transactions accurately and quickly.

The benefits of adopting electronic Identity Management comprise storing information in digital form where it can be easily accessed and transferred whenever needed, ensuring a secure, convenient and effective way of identifying both an individual and service provider identities, and safeguarding and protecting access to sensitive information. Furthermore, it improves the quality of services to be delivered, minimizes management cost, and increases confidence in reliable identification and authorisation of users which in turn enables secure and effective day to day information transactions between public agencies. Moreover, cost savings generated from these efficiencies could enable the government to provide additional free services elsewhere. Consequently, by adopting efficient identity management in e-governance; governments can overhaul their processes and systems and turn them from a red tape nightmare to customer friendly systems.

1.2. Background

The Republic of Kenya is a country in Eastern Africa bordered by Somalia to the east, Uganda to the west, Ethiopia to the north, Tanzania to the south, Sudan to the northwest and with the Indian Ocean running along the southeast border. According to the 2009 World Bank report of World Development Indicators and CIA World Fact Book, the population of Kenya is 39,802,015 of which 42.81% are (0-14 age), 54.56% are (15-64 age) and 2.64% are 65 and above. There are 3,995,492 Internet users which are around 10% of the population and 105 secure internet servers. 87% of the people aged 15 and above are literate adults.

Kenya's directorate of e-government initiative was started in the year 2004 with the objective to 'facilitate better and efficient delivery of information and services to the citizens, promote productivity among public servants, encourage participation of citizens in government, and empower all Kenyans' through the use of Information technologies with the goal of "making government more result oriented, efficient and citizen centered." (e-Government, 2004, pp. ii,3) The main aim is to develop functional communication within government services (G2G), businesses (G2B) and citizens (G2C). (ibid) The implementation matrix is divided into three initiatives namely:

1.2.1 Short term initiatives

Implementation of the short term initiative was started on June 2004 aiming "to achieve creation of a firm foundation for the overall e-Government initiative" (e-Government, 2004, p. 6) by developing ICT policy and e-Government strategy, expansion of information infrastructure, initiating integration of internal government processes, increasing internal operational efficiency and effectiveness, developing information Websites for ministries and capacity building. Infrastructure development is still going on to date.

1.2.2 Middle term initiatives

Implementation of the middle-term initiative was started on June 2007 focusing on the concerted automation and integration of Government information and records, finalizing the information infrastructure within Government, the development and implementation of web-enabled databases and integrating different networking technologies and management systems. Developing websites for different Government ministries have been started and the interactivity of the websites is still in progress.

1.2.3 Long-term initiatives

The long-term initiative includes enhancing:

- E-policing: using the related technology and Internet to administer police operations
- E-voting: polling and counting of votes by using electronic means.

- Link payments of utility bills
- Electronic advertisement, electronic application of jobs and e-interviewing to enable equal opportunities for all Kenyan citizens either locally based or internationally based.

For the long-term initiatives to be achieved interoperability of data to enable access and sharing of information and the adoption of efficient identity management should be addressed. In addition, the government should create a common framework across government agencies and corporations for cost effective delivery of e-government to the public and business sectors.

1.3. Problem definition

The idea of e-government bases on the identity policy through data and identity protection legislation. Moreover, the interaction between government agencies across the e-government information systems is mainly supported by identity management which covers what constitutes private/personal data and how it is identified, accessed, shared, used and managed based on regulations, policies, trust, collaboration, interoperability and access management.

Identity management is a broad concept that revolves around personal information and authentication mechanisms, legal and regulatory factors, technical implementations and management, passes through public and private sectors and touches many aspects of contemporary life. Researches (e.g. Lips, M. et al. 2007; Kumar, V. et al. 2007; Fioravanti, F. & Nardelli, E. 2008) have revealed that identity management is the most important foundation for the success of e-government agenda.

In the government of Kenya, ministries and agencies develop, maintain and archive several fragmented citizens' information. For example, the Kenya police keep details about a person, the Kenya revenue authority keeps other details about the same person, and the immigration and registration of births and deaths department also keep different details about the same person/citizen. Apart from storing fragmented information, citizens carry different forms of identity cards to be identified in a particular government agency or public institution.

According to the initiatives discussed in section 1.2, the government of Kenya requires a computer system that addresses the long-term initiative in the implementation matrix. The objectives are:

- To use electronic identity management to improve collaboration between government agencies through reduction in the duplication of efforts, and enhance efficiency and effectiveness of resource utilization.
- To reduce transaction costs for the government, citizens and the private sector through the provision of products and services electronically.

As the government has fragmented identity information in different public institutions and government agencies: accessing and sharing this data i.e. interoperability becomes an issue. Integrating and interfacing different government agencies and public institutions where fragmented information is kept is also a fundamental topic to be addressed. In addition, privacy protection and security issues regarding citizens' identity information must be addressed and the exchange of this information through secured channels to ensure confidentiality and integrity is also a major concern.

1.4. Research objective

This thesis will research identity management and the integrated technologies, assess citizens' perception regarding identity management, and ultimately produce a model that can be used as a framework for addressing privacy protection and security issues and for choosing the technology to be used by the government for identity management with respect to the Kenyan identity policy, legislation, culture, and existing infrastructure.

Specifically, the research will:

- Explore electronic identity management and the integrated technologies:
 - That improves collaboration, guarantee interoperability and the efficient access and sharing of data across government agencies and public institutions.
 - That ensures the secure exchange of citizens' identity information across the agencies in order to maintain availability, continuity of service, and integrity of client's data and information.

- Explore citizens' perception regarding identity management which directly influences privacy protection and security legislations and is the single most significant obstacle to the widespread adoption of electronic identity management. These findings are included in the proposed model and will be used as a guiding factor in implementing electronic identity management in e-governance of Kenya.
- Finally will produce a model that will highlight the interoperability of fragmented identity data, how agencies are integrated and interfaced using identity management technologies, and how citizens' perception in the form of policies and legislations is incorporated in the e-governance.

1.5. Research question

The research question is:

- How can the government of Kenya integrate and share for use the fragmented identity information of citizen's using a suitable identity management technology which is kept in different public agencies?
- How can the identity information of a specific citizen be identified, accessed and shared across the public agency systems under e-government model?
- How the perceptions of citizens' regarding identity management can be incorporated in the e-governance?

1.6. Delimitations

- The issue of personal identity management underrepresented in the Information Systems and Information Management literature.
- Focusing only on the public sector i.e. the e-government model only.
- Focusing on the technical interoperability only
- Limited number of people to discuss with as we will only deal with the ICT board

- Survey to collect citizens' perception will only be held in the capital Nairobi due to time and financial constraints

1.7. Thesis project outcomes

The study provides a detailed study of features of Identity management, citizens' perception, virtual private network and web services.

1.8. Thesis chapter structure

The thesis consists of seven chapters and an appendix. The following section will give a brief overview of the thesis project outline.

Chapter 1: Introduction

It introduces the area of study and problem definition; in addition it describes the research objective, research question and delimitation.

Chapter 2: Identity Management

It covers what constitutes personal data and how it is identified, used and managed. The idea of e-government as central to identity policy through data and identity protection legislation is discussed. Challenges, risks and proposed trends in the personal e-identity management are also explored. The chapter also looks at what is technologically, legally and operationally possible using e-identity in Kenyan context.

Chapter 3: Integrated Technologies

The chapter looks at Virtual private networks, Security Assertion Markup Language, Liberty Alliance and Web services technologies that will be incorporated into the proposed identity management solution. How data securely traverse across different government agencies is discussed through the

implementation of virtual private networks (VPNs). Interoperability of data is highlighted using the web services.

Chapter 4: Methodology

The research purpose, approach, strategy, data collection methods and data analysis is discussed.

Chapter 5: Citizens' perception on electronic identity management

The social aspects concerned with data sharing especially personal information in the electronic identity management system is analyzed.

Chapter 6: Sample Model

The chapter presents the model which implements research analysis and findings. The model is an interface that demonstrates interoperability of data during retrieval of identity and related information stored in independent databases.

Chapter 7: Evaluation and Conclusion

The chapter discusses the evaluation and conclusion of the entire thesis with suggested future researches.

2.1. Overview of Identity Management

Information technology has led the world into being a global village, this is because one can be able to communicate or transact business in real-time with people in other parts of the world without physically traveling to where they are, for example it is possible to use video conferencing technology to accomplish the MSC in Information Security program in Luleå University of Technology.

This is the same for the governments that need to bring services to the people; however several challenges emerge as we utilize information systems to bring service to the people, the greatest challenge for the government of Kenya is identity management for the purpose of information sharing and security between government agencies.

The central part in the information exchange between government to government, government to business and government to citizens' is identity-mainly associated with an individual (Windley, 2005). The dictionary meaning of identity is “the individual characteristics by which a person or thing is recognized, the state or fact of remaining the same one or ones, as under varying aspects or conditions.” Among several features that an identity consists the primary aspects are:

- *Cultural identity* – refers to “the common historical experiences and shared cultural codes”, for a given individual (Brazier et al., 2003, p.223) for example what makes a Kenyan-man Kenyan.
- *Digital identity* – an electronic representation of personal information (Windley, 2005) mainly concerned with how people are identified on computer systems and the internet (Glasser & Vajihollahi, 2008).
- *Biometric identity* - individuals physiological and/or behavioral characteristics (Jain et al., 2004) unique to a person such as gait, DNA profile, fingerprints, hand geometry, facial structure, voice, retina (Iris recognition) etc.

The main concern of e-Government is digital identity (Fioravanti & Nardelli, 2008) which is very helpful to exactly recognize with whom to communicate. In the provision of online services Digital Identity must be managed efficiently not only for the purpose to meet the basic requirement but for “security, privacy, and reliability” reasons (Windley, 2005, p. xi). Consequently identification, authentication and authorisation are the principal concepts in contemporary identity management. Bhargav-Spantzel et al, (2007) argued that “enrollment, storage, retrieval, provisioning and revocation of identity attributes” are the life cycle of an identity.

In line with Arabo et al., (2009) Identity Management (IdM) refers “an integrated system of business processes, policies and technologies, which enables organizations to facilitate and control user access to critical online applications and resources while protecting confidential personal and business information from unauthorized users.” It signifies “the behaviour of persons in everyday activities” in the electronic sphere (Claus, 2001, p.205) and requires effective systems integration and interoperability (Windley, 2005).

Identity management systems are “programs or frameworks that administer the collection, authentication, or use of identity and information linked to identity” (Hansen et al., 2007, p. 38) which deals with the management of digital identities and the corresponding authentication, reachability (a notion for user identification and the way users handle identity functions), authenticity, anonymity and pseudonymity (identifying subjects or sets of subjects i.e. the users of a service) and the organization of personal data management. It comprise the authentication, authorisation (access control), accounting and user management processes (ibid) hence, for the successful set up of e-Government and e-Business services the organization of a robust and interoperable Identity Management system is a decisive factor (Fioravanti & Nardelli, 2008).

In the selection of an identity management technique to be used to identify an individual there are several factors that needs to be considered such as: availability and integrity of information being accessed, confidentiality, continuity of service, security and legal requirements (Burr & NIST, 2006) in addition, technical issues or what is technically legal and operable also needs to be considered (Maler & Reed, 2008).

In this chapter we will discuss approaches to identity management, examine the e-Government portal of Kenya (check how far the government has reached in the development of the e-Government structure and what needs to be done for proper identity management), comparison of Identity Management with other jurisdictions, cultural, legal and social impacts of Identity Management, challenges to Identity Management, a conclusion and research findings.

2.2. Approaches to identity management

The aim of identity management is to enhance security and productivity, at the same time decreasing extra administration costs. It consists the issuing of credentials and identifiers to users at the time of initial registration phase which includes creating, modifying and deleting user accounts and the authentication and controlling of access rights to use the system resource based on the established credentials and identifiers. Thus, privacy and interoperability are decisive factors or requirements for triumphant Identity Management system.

2.2.1 Silo or Isolated Identity System

This is the most common type of Identity Management system designed and functions independently without connecting with other identity systems (OECD, 2009). Usually implemented in a single firm where identity and services are provided and managed by the service provider alone (Brankovic et al., 2007). The organization plays a role of service provider and Identity Provider by issuing IDs and managing information on its own domain (IEEE, 2009).

Siloed systems are simple to deploy from the service provider perspective but inefficient since it creates “identity overload and password fatigue” (Brankovic et al., 2007, p.3) and identity data has to be maintained in multiple accounts within the organization (OECD, 2009). Furthermore, as there is no link with other domain identity theft and corruption are extremely limited hence, if the domain encounters any security or system failure the consequence is severe (ibid).

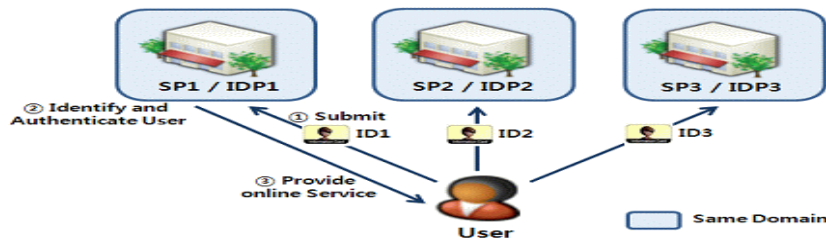


Figure 2.1: The Silo Model (adopted from IEEE, 2009)

2.2.2 Centralized Identity System

The centralized identity system is designed to alleviate the inconveniences of Silos model by centralizing the identity information. The model offers Single-Sign-On (SSO) services and with this model the user accesses and utilize the resource (applications, websites) within the same domain after authenticated by providing a single ID (OECD, 2009). Identities of users are stored in a directory independently of the web services provided and authentication is administered across the services by a single identity provider or authority (IEEE, 2009).

The Passport authentication service introduced by Microsoft in 1999 is a good example of this model. The service is designed to be an identity provider for the Internet but mistrust and critic has risen for giving Microsoft too much control over the identity information of Internet users' such as credit card numbers as websites that participate in the initiative rely on Passport for the authentication of users (Camenisch et al., 2011). Windows Live ID (the former Passport) beginning from 2006 operates as authentication server for online services controlled by Microsoft such as Hotmail (Brankovic et al., 2007). Microsoft .Net Passport and Kerberos based authentication solutions, where the Kerberos Authentication Server acts as the centralized identifier and credential provider, are in this category (ibid).

In addition to the problem with link-ability, potential security vulnerabilities such as cracking the authentication information of a user's single ID will enable an attacker to pretext and access all services in the domain. Moreover, the single identity provider that all service providers rely on for their identity service provision can become the single point of failure (Camenisch et al., 2011). Researchers like (Fioravanti & Nardelli, 2008) argued that the centralized approach addresses secure interoperability issues in strictly hierarchical environments e.g. multinational companies.

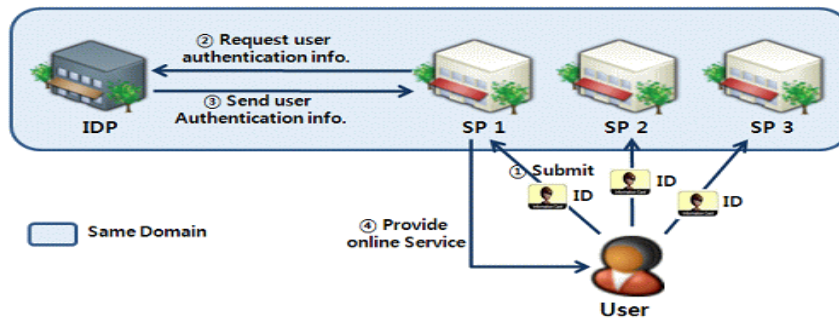


Figure 2.2: The Centralized Model (adopted from IEEE, 2009)

2.2.3 Federated Identity System

A federation is “a group of organizations which trust certain kinds of information from any member of the group to be valid” (Bhargav-Spantzel et al., 2006, p.271). In Federated model there exists Multi-organization single sign-on (e.g., Microsoft .Net Passport) where identification and authentication is subcontracted to a trusted identity provider, and Enterprise centric federated identity management (e.g., Liberty Alliance) (Camenisch et al., 2011) where more than one identity and service providers federated with an agreement concerning security and authentication hence, assumed that all entities in the federation are completely trusted (OECD, 2009).

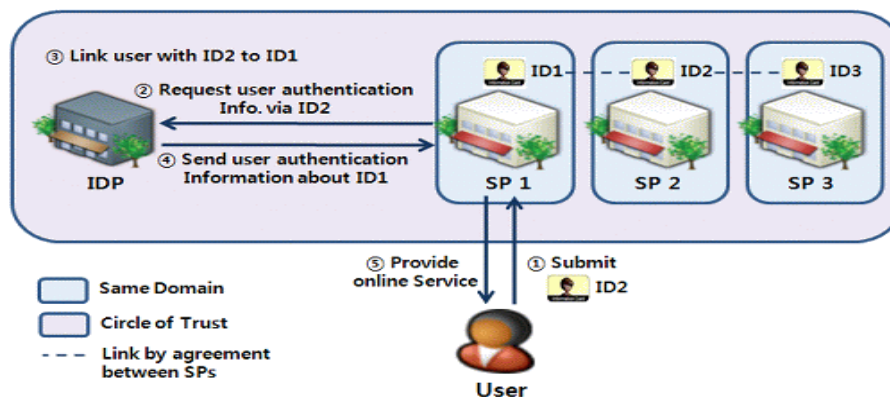


Figure 2.3: Multi-organization Single-Sign-On in the Federated Model (adopted from IEEE, 2009)

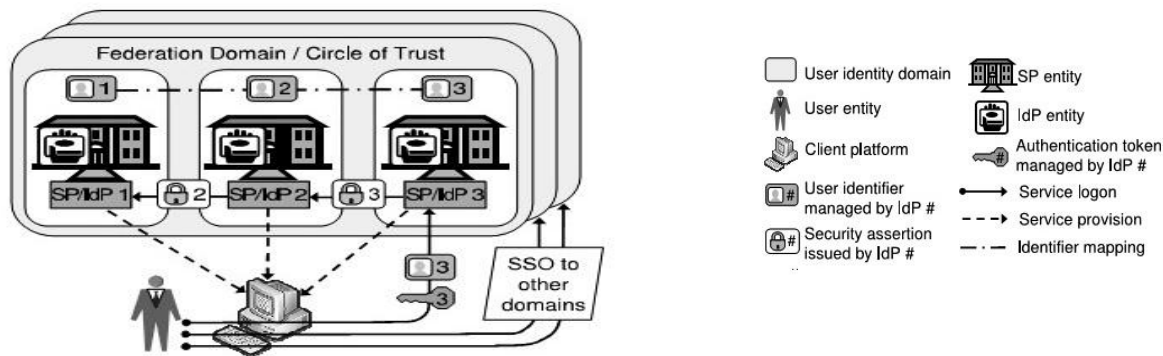


Figure 2.4: Enterprise centric Federated Identity Model (adopted from Brankovic et al., 2007)

As there exist many service providers and the model is capable to provide Single-Sign-On (SSO) service, after authenticating herself to the central identity provider a user can access services in the federation domain since her primary account is distributed among the service providers (Camenisch et al., 2011). Besides, the model is easily compatible with the traditional silo and the centralized model that lets service providers to benefit from its compatibility and efficiency to manage accounts it is also more convenient for users too(OECD, 2009).

The three most widely adopted identity federation protocols are the Security Assertion Markup Language (SAML), the Liberty Alliance protocols (ID-FF) and the WS-* (“WS-star”) suite of specifications (Clemm et al., 2005). Communication security is only considered in the standards and users are responsible to control which information about them is allowed to be shared (ibid). Moreover, the Shibboleth initiative is another federated framework that supports cross-domain SSO (IEEE 2009).

2.2.4 User Centric Identity System

In the User-centric model, users’ are in control of the management of their ID entitled by the identity provider also, the system requires the users’ consent specifically before transmitting and sharing their IDs, personal and authentication information (Arabo et al., 2009, Paci et al., 2009,

IEEE, 2009). Focusing on users' perspective it lets users' "to choose identity providers independently of service providers and do not need to provide personal information to service providers in order to receive services" (IEEE, 2009).

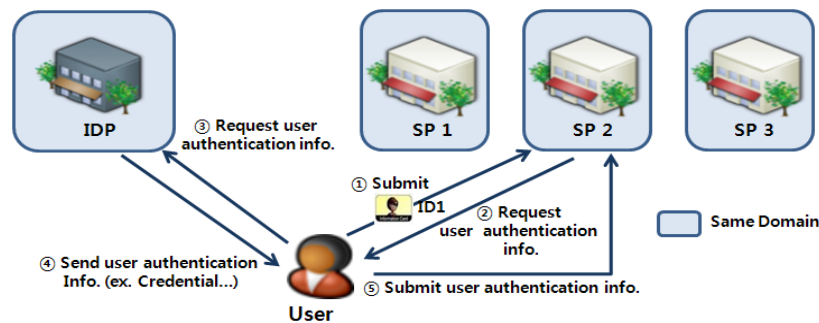


Figure 2.5: User centric Identity Model (adopted from IEEE, 2009)

In line with OECD (2009), IEEE (2009) and Bramhall et al., (2007), in this model user are fully responsible to choose an identity provider and make the initial registration. They are not obliged to present their identity to the service providers in order to get the service but the identity providers are responsible to store information regarding the user and do the authentication. The identity providers are not part of the federation but works as a third trusted party between the users' and the service providers mainly targeting in the interest of users. (ibid)

The model is very compatible with the federated paradigm rather than purely centralized approaches (Bramhall et al., 2007) compared with the other models it is considered to be efficient to protect the security of users' personal information (IEEE, 2009). Josang & Pope (2005) argued the benefits of this architecture are:

- The user only needs to remember one credential (e.g. the PAD PIN)
- The possibility of implementing Virtual SSO
- The compatibility with traditional legacy identity management models

Higgins, CardSpace, Credentia, Liberty alliance and OpenID are the standard frameworks for user-centric identity management model (Paci et al., 2009; IEEE, 2009; OECD, 2009).

2.3. E-Government portal of Kenya

There are five stages in the development of e-government (United Nations, 2008). Namely;

Stage 1: This is *emerging stage*. A government's online presence comprises of a web page and an official website. There is little interaction with citizens and information is static.

Stage II: This is *enhanced stage*. Governments have created links to archived information that is easily accessible to citizens e.g. documents, forms, laws and regulations etc. There is more information on public policy and governance.

Stage III: *Interactive Stage*. There is a basic interactive portal with services to enhance the convenience of citizens. Governments deliver online services such as downloadable forms for tax payments and applications for license renewals.

Stage IV: *Transactional stage*. Governments begin to transform themselves by introducing two-way interactions between citizen and government. It includes options for paying taxes, applying for ID cards, birth certificates, passports and license renewals. All transactions are conducted online.

Stage V - *Connected Stage*. Governments transform themselves into a connected entity that responds to the needs of its citizens by developing an integrated back office infrastructure. It is characterized by;

1. Horizontal connections (among government agencies)
2. Vertical connections (central and local government agencies)
3. Infrastructure connections (interoperability issues)
4. Connections between governments and citizens
5. Connections among stakeholders (government, private sector, academic institutions, NGOs and civil society).

The e-Government in Kenya is in stage III. The governmental portal provides a framework to interlink all the ministries and government agencies. The portal provides government to citizen communication through which government information such as policy documents, legislation, report and case law are made available direct to the public.

In the e-Government of Kenya implementation matrix highlighted in previous chapter, short term initiatives have been implemented. Mid-term initiative has been done limitedly and long-term

initiatives are yet to be implemented. Below are several examples of government portals and websites which depict how government has developed fragmented systems, which will eventually have an impact on the identity management systems that they will pick.

The e-Government portal snapshot is shown in figure 2.6 and 2.7 (egovernment.go.ke, 2011) and the Kenya revenue authority figure 2.8 (kra.go.ke). The government portal shows information and service dissemination from government to citizen. The e-Government portal contains links to other ministerial websites, state corporations and investment opportunities i.e. from the e-Government portal there are links to immigration and the KRA. Citizenry interaction with the website is at an advanced stage. The Kenya Revenue Authority website shows some interactivity with the citizen by virtue of it have online services which include the following;

- Taxpayer Registration
- File Tax Returns
- Import
- Declaration (IDF)
- Application Tax Return Processing
- Goods Declaration
- PIN Checker
- TCC Checker
- KRA FAQ
- WCO E-Learning

Government services can be delivered in several level of interaction in web portals, the levels are basically communication, information and transactions. In information level the government present the necessary and relevant information through static websites, this is usually meant for citizen's knowledge, businesses and tourists. It is basically meant for informing only. The other is the communication level where issues to perform communication with citizens like email comes to life and finally the transaction level where there is interaction which involves filling of online forms for the purpose of transacting.

As can be seen in the e-Government portal (e-gouvernement.go.ke) it has met all the above criteria and the question still remains, how do you identify a citizen filling a form across all this fragmented systems.

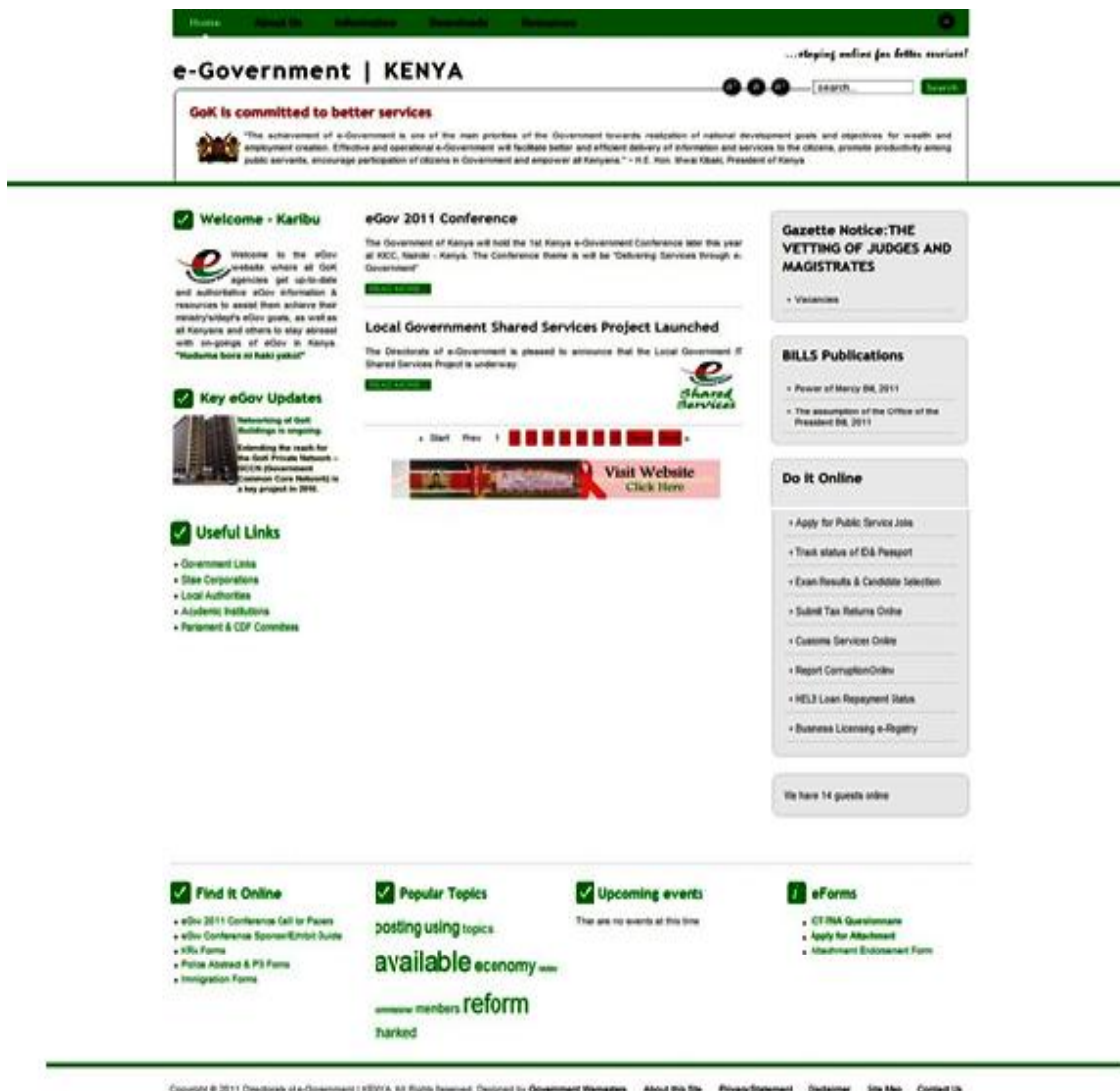


Figure 2.6: Snapshot of e-Government portal

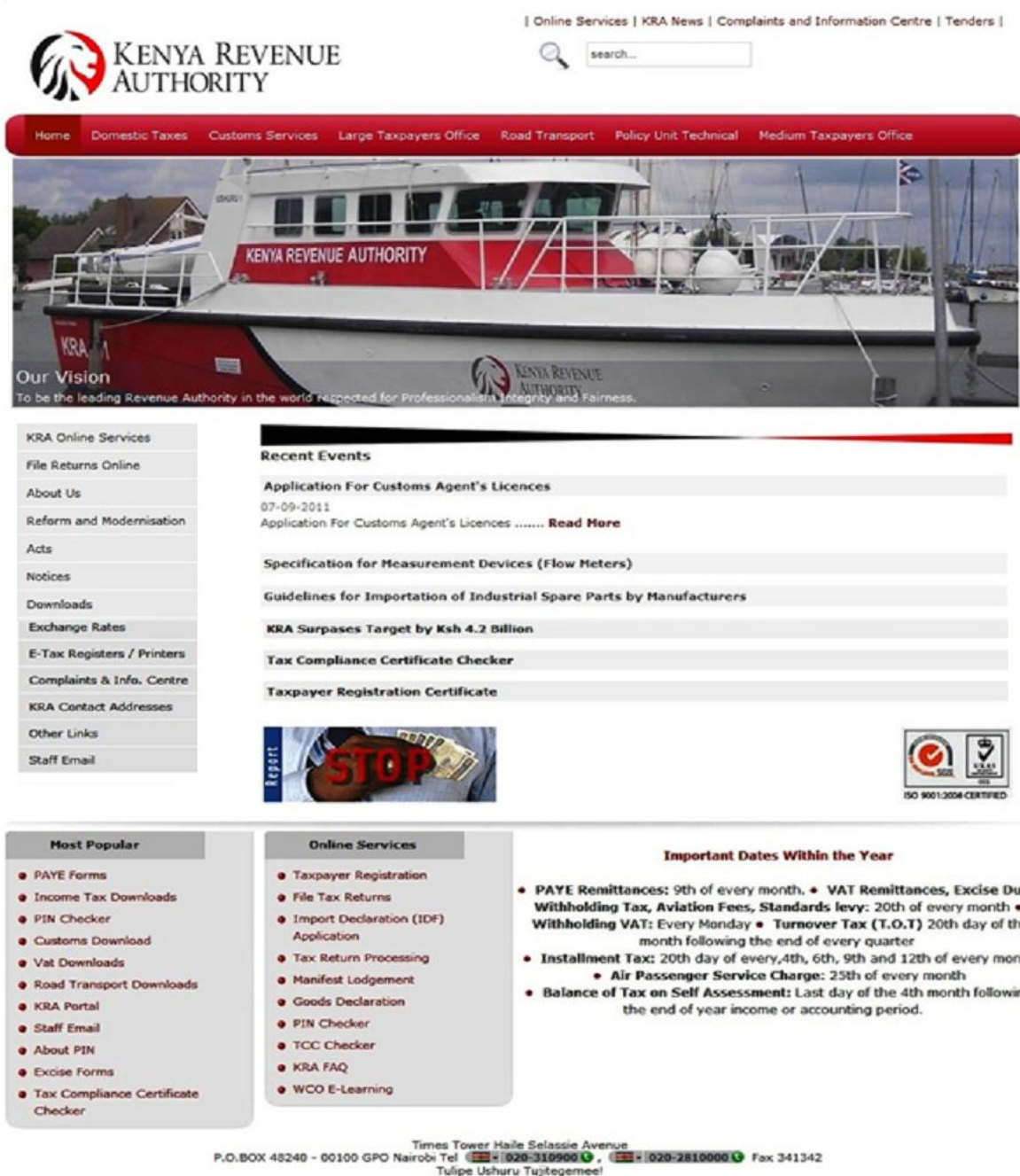


Figure 2.7: Snapshot of the Kenya Revenue Authority page

Other government websites such as the immigration ministry only provides forms for download, filling and returns to the ministry however, after returning the forms the site provides for checking

status i.e. whether it has been processed or not below is the snapshot. The website also provides information on government policies, on immigration and other requirement for people wishing to visit the country; this means you do not require calling or walking in the embassy to obtain this kind of information.

The main question here is how will we manage identity if we make the entire process online? Can anyone there steal electronic identity of a person and fill the forms and therefore obtain a Kenyan passport illegally with issues of terrorism on the rise? These are some of the critical questions that the ICT board would want to answer in identity management.

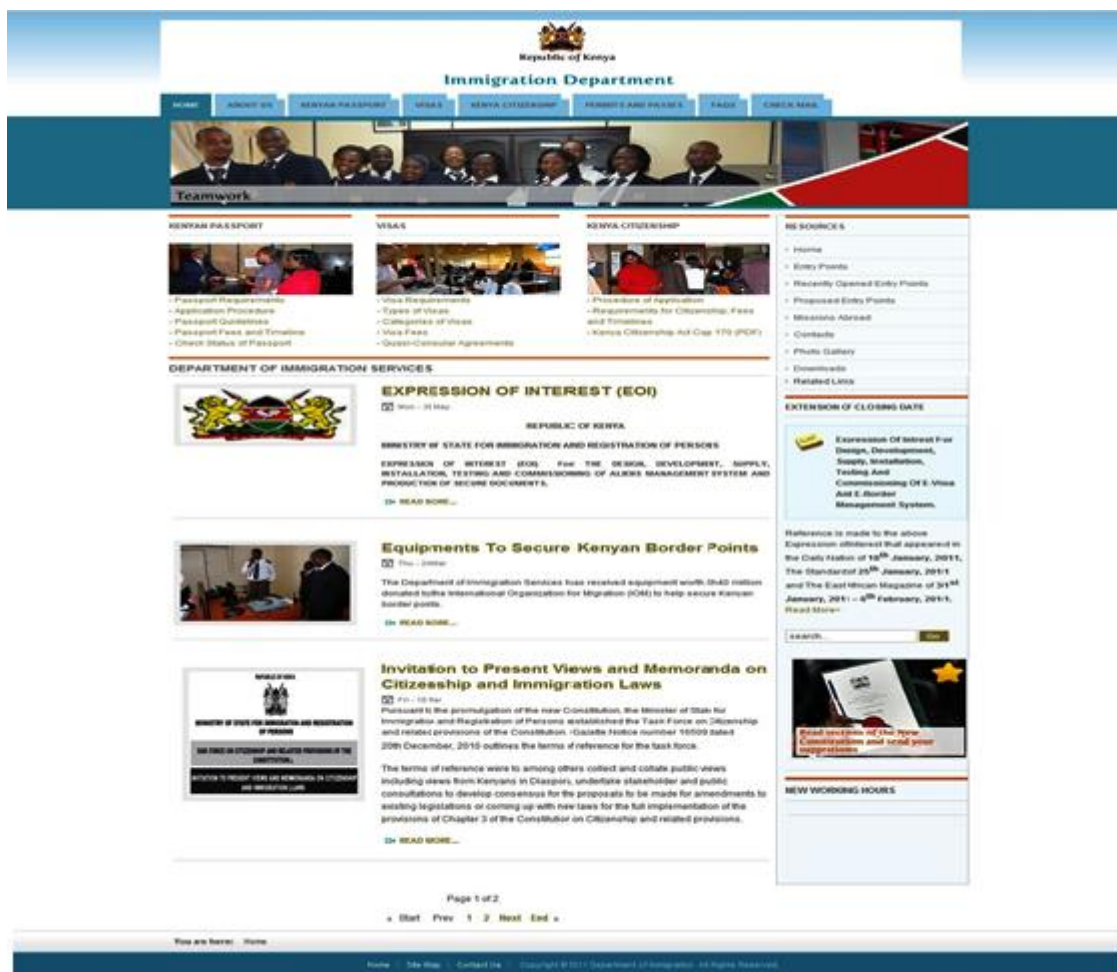


Figure 2.8: Snapshot of Immigration Department webpage

2.4. Infrastructural connection between government agencies in Kenya

Until late 2004 Kenya had been relaying on satellite bandwidth, during this period internet was slow and expensive and only few institution could access internet connection and WAN. Connection between different branches of organization and different government ministries was also very expensive and therefore not feasible, however the government of Kenya liberalized the telecommunications sector and this allowed very many players to come in to play, these players included data communication providers, ISP and Mobiles services providers.

Kenya has currently more than 100 data communication operators and ISP; the major ones include Safaricom (which provides both data and mobile phone service), Accesskenya, Wananchi online, UUNET, KDN (Kenya data networks), etc. These players have helped the country and made the ICT sector to grow at a very high rate, the companies have also laid fiber optic cables interconnected together (Mesh topology) in all districts in Kenya.

The cables are also connected to the undersea fiber optic cables connecting the east Africa and Europe (such as teams, adn, seacom). In turn this has reduced the cost of bandwidth and interconnectivity between government agencies and ministries. It is against this background that the Kenya government utilizes this infrastructure to connect ministries and government agencies; even though there is a price tag associated with use of this infrastructure the price is very affordable. In areas where there is no fiber connection the government agencies use last mile microwave link for connection and in very few place does the government use VSAT.

In conclusion internet and network infrastructure have grown tremendously over the last few years to make Kenya one of the best country in this region with regard to fiber infrastructure.

2.5. Comparison of Identity Management with other jurisdictions

The collection, storage and management of personal data (digital identity) is a concern for both governments and private sectors as they both work together in an attempt to have control over the security of their customer's identity, improve the provision of online services and effectively

utilize and manage the underlying technology. The effect is that they learn from each other and produce guidance for best practice and governing frameworks or initiatives that support collaboration, standards, and interoperability to achieve consistency. The subsequent subsections highlight the type and level of identity management implemented in the selected countries.

2.5.1 Australia

The Australian Government Information Management Office (AGIMO) has developed The National Authentication Framework (NeAF) in 2009 by replacing the earlier Australian Government Authentication Framework for Businesses and Australian Government Authentication Framework for Individuals (AGAF-B and AGAF-I) that was developed in 2003 (Australia, 2009). The framework aimed at achieving consistency by providing guidance and principles, trust and confidence, cost effectiveness and convenience, “fit-for-purpose authentication solutions” for individuals, businesses and government websites, responsiveness and accountability, privacy controls and interoperability based on federation (ibid, p.1). This has enabled it to gain a wider community acceptance (McKenzie et al., 2008).

The e-Government Interoperability Framework (e-GIF) known as Australian Government Authentication Framework for Individuals is a fundamental initiative or strategy to rationalize electronic processes that enable the transaction of appropriate information between government agencies and the delivery of government services to the community (UNDP, 2007).

The Whole-of-Government online services is a federated system designed towards the integration of government services by facilitating cross agency information sharing with an access controlled collaboration environment. “Govdex” is a secure web-based space (service) designed to integrate and interoperate government agencies in order to manage projects and share ideas, documents and information. The service of “Govdex” an online communications platform; includes authenticating and authorizing registered agency users in order to restrict access and/or edit permission for specific pages within a shared workspace. It also provide mechanisms to support private, secure cross-agency and cross-jurisdictional: document and information sharing, collaborative authoring, issues management, communications and engagement with project stakeholders. The Department of

Finance and Deregulation (Finance) provides the hosting, infrastructure, software applications and information storage and disaster recovery for the service. (finance.gov.au, 2011)



Figure 2.9: Snapshot of Australian Government agency personnel's login interface for cross-agency information access and sharing

2.5.2 New Zealand

Based on the literature McKenzie et al. (2008), The United Nations e-Government Survey (2010), online resources from Government ICT Directions and Priorities (<http://www.e.govt.nz/>) and Guide to Authentication Standards for Online Services (<http://www.e.govt.nz/guidance-and-resources>) we found that the New Zealand e-Government Interoperability Framework (NZ e-GIF) defines set of standards and guidelines to ensure coherent flow of information across ICT systems and serve as a basis for the design and efficient interactions of e-government services. It complies with all relevant NZ legislation and Government policy particularly on personal privacy, and the security and transaction of data and information held by government. The main purpose of the Interoperability framework is to: facilitate the collection and exchange of data, documents, business processes and metadata across government agencies, organize government agencies around citizen-centered service delivery and create joined-up government system.

In creating technical interoperability, the framework encourages the application of open standards to a greater level. The country's all-of-authentication Programme began in 2000 by identifying key policy and implementation principles to guide the authentication approach's design based on the

principles of federated user-centric Identity Management which is affordable, easy to use, technology neutral, secured and fit for the purpose.

The Government of New Zealand Web Community uses two different sets of restricted access collaboration tools, a Shared Workspace and a Yammer feed (Public Sector Intranet). SEEMail is an Internet based technology used for secure exchange of email and attachments by government agencies. This technology has been extended to include secure email communications between government, businesses and citizens'. Shared Workspace is a suite of online tools and processes to support information sharing and working between government agencies and the functionality has also extended to incorporate partners outside the government. This web services technology is designed to support interagency collaboration and to share documents and project work. It utilizes Internet browser technology (http) as the primary transport channel with SSL for security (https).

Focusing on user centricity, privacy, and security the authentication approach (browser-based logon management) follows all-of-government authentication services (centralized shared services) - the Government Logon Service (GLS) and the Identity Verification Service (IVS). The igovt logon service (a web site) is used to access all participating government service provider's online services and igovt identity verification service is used to verify users' identity to participating government service providers via the Internet by implementing the Security Assertion Markup Language (SAML 2.0), an open standard for communicating security assertions in real time. The igovt logon service operates in line with SAML's single-sign-on profile. The technology effectively identifies a customer and sends minimal identity attributes that are very useful to Service Providers for access control, personalization, and other purposes.

The igovt logon service works also for identifying and authenticating citizens in order to access public electronic services. Citizens do not need to prove their identity to multiple departments instead can log on to the centralized IVS via the GLS to choose their verified core identity attributes (real or pseudonymous) electronically stored in a centralized database and release to other agencies they wish to receive service from. Identity assertion to government agency service providers is performed completely under a user-controlled manner.

2.5.3 Mauritius

The information we provide is extracted from sources including United Nation (2007), Kitaw, Y. (2006, November), Government of Mauritius (<http://www.gov.mu>) and Minges, Gray & Tayob (2004).

E-Government initiatives to put all ministerial offices on the web, so as to render online access to their new acts, publications and events was forwarded early in 1996 for Mauritius. This is followed by The National IT strategic plan (NITSP) of 1998 and an Electronic Transaction Act in July 2000. The country has an integrated portal that provides a lot of information to the citizens in one single place.

There exists Government to Business (G2B) initiative that allows electronic payment of tax for all employers in the country. This is done through secured networks and ICT applications allowing a fully electronic tax collection. 43 e-Services are enabled ranging from transaction-based services to static information which is important to civil servants, businesses, tourists and citizens.

The electronic submission of returns is done using the front end electronic Data Interchange (EDI) software. The processed standard EDI messages are routed to the relevant government agencies through the Value Added Network (VAN) - a secure private network connecting government agencies and commercial banks. A harmonized identity management has been adopted and security is ensured through implementation of firewall controls and data encryption through Secure Socket Layer (SSL). There exists a Government Sub-Portal that provides comprehensive information on the Government services to the public and serves as a gateway for Government employees to access the various online services by using a government-to-government login identification and verification service.

2.5.4 Austria

Based on the information extracted from Aichholzer & Strauß (2010), Romansky, EG&DP, & International Workshop on e-Government and Data Protection (2006) and Fioravanti & Nardelli (2008) the Austrian Citizen Card concept (Bürgerkarte) was initiated by the government on the year

2000 after adopting the Austrian Signature law and European Directive for Electronic Signatures (1999/93/EC) act intending the use of secure and reliable digital signatures in e-Government with the help of open standards. Issuing electronic cards has started by 2004 embedded with an electronic signature and a digital certificate that makes Austria the second country after Finland introducing a fully functional smart card in Europe. At present, Austria is the leading country in the European Union Benchmark for e-government services for citizens and businesses by using a standard Citizen Card approach to identity management.

On the federal level a direct secure electronic message exchange system handles the administration of documents exchange between all ministries. The Austrian e-government system entirely relies on web based communication. Role based access control system helps agency workers to identify themselves and access data bases, which is an important feature of e-government procedures. A Citizen Card contains an electronic assertion (Identity Link - an XML-document signed by an appointed authority) that binds the citizen's public key to a sourcePIN i.e. a unique governmental identification number derived from the Central Register of Residents by a strong encryption. This helps to uniquely identify a citizen by comparing the certificate (sourcePIN plus public key) signed by registration authority included with the key (sourcePIN stored in every citizen card) contained in the Identity Link.

The associated data of all persons registered in Austria is contained in a central database called ZMR (Zentrale Melderegister) created by the Federal Ministry of the Interior where authentication is obtained by matching the card's data with the data from this repository. There are more than 100 different federated public services available to access using the citizen card like file applications and online payment using "EPS (Electronic Payment Standard) online" electronic payments for e-Government services.

To increase the functionality of the smart card, upon obtaining users need to activate to use it on their mobile phone or with a card reader. For instance, if we take a case when a citizen wants to access public e-Services by using her mobile-phone she directly browse the start page. Click on the option Mobile phone and enter her mobile phone number and signature password (the password chosen upon activation). An SMS will be sent on her mobile phone called TAN for comparison and only need to enter the TAN in the input field and click Sign. The table below shows selected countries that use technologies highlighted in identity management.

	PORTAL/DASHBOARD	NATIONAL ID	SAML	DIGITAL CERTIFICATES
Austria	X	X	X	X
Canada	X			X
Catalonia/Spain		X	X	X
Finland		X	X	X
France	X		X	
New Zealand			X	
Netherlands	X	X	X	
Norway	X	X	X	X
UK	X		X	X

Table 2.1 : Selected country comparison of technologies used by governments to deliver online services to their citizens (adopted from McKenzie et al., 2008).

According to McKenzie et al. (2008) Austria, Spain, Finland, Netherlands and Norway developed their electronic identity management systems based on existing national identity numbers and digital certificate system (Citizen card). A portal or dashboard is a browser-based logon management system. Security Assertion Markup Language (SAML) is an XML framework or security standard developed by OASIS, for exchanging authentication and authorization information.

2.6. Cultural, legal and social impacts of Identity management

Identity management requires high levels of trust from the identity provider such as government for it to be accepted by citizens but there exists a problem in the efficiency and levels of trust (Kumar et al., 2007). Citizens seek trust and control of their private information as it is shared online and Governments are trying their best to get a right solution by approaching identity management in considerably different ways.

McKenzie et al, (2008) argued that “Culture and history strongly affect the nature of the identity management system that might be acceptable to citizens in particular circumstances, with levels of trust in government being a key factor.”(p. 51). There is a great difference between nations in the citizens’ interaction and relationship with their governments. Where the citizens are confident that their government is trustworthy and has their information under appropriate control, they are less likely to demand direct control over their private information like the case of Singapore and Scandinavian countries. On the other hand, unique challenges will rise like the case of UK, US,

Canada and Australia and this has a direct impact on the type of identity management systems to be implemented (ibid).

Identity management systems are also affected by social policy (Landau & Mulligan, 2008) and society's values can limit the type of an identity management system that is viable and hence each country's identity management system is unique to another. Kenya has diverse cultural beliefs and the ideal electronic identity management system must comprise joint public-private agreements.

In Kenyan context, there are gaps in the legislation on data and personal privacy protection. There is a draft data protection act that will be tabled in parliament for debate. ICT policy is being reviewed and updated to include electronic security measures. An e-security structure will be developed in collaboration with relevant institutions. Mechanisms should also be established for international cooperation to combat cross-border crimes. This is in contrast to countries such as Denmark that have protection of privacy through Personal Data protection Act, EU data protection Directive, Law on Digital signatures and Data protection Agency (Hoff & Hoff, 2010). This has resulted to higher levels of trustworthiness from the citizens. The trustworthiness the citizens have for the government is that of optimism and hope. These are the issues that the Kenyan draft data protection and privacy act must address.

2.7. Challenges

Identity management is an issue with legal and policy implications hence, what is legal to collect or disclose in one jurisdiction might not be legal to collect in another. As legislation and public policy evolve, new technical issues arise and expectations from citizens and users increase; citizens expect that electronic transactions should be regulated by law and those transactions to be conducted must be accomplished in accordance with the regulations.

Governing information "when the entities that need to access it are dispersed and diverse" (Buell *et al.*, p.26, 2003) and the desire to have a single sign-on (SSO) access to a collection of resources that might have different access-protection rules (Benantar, 2006) are the main challenges to effective electronic identity management moreover, databases may also have different access protection rules and hence it would be challenging to have a single sign-on access and ability to verify an electronic SSOs authenticity.

The social and human factors (Dhamija & Dussault, 2008) must also be considered as there are citizens who are new to the domain of electronic transactions and others who resist when compared to existing behaviors in traditional situations. This makes the task more challenging since technology alone will not make the system be accepted but also the diversity of human beings must be considered.

Predominantly, interoperability, privacy and data protection are challenging issues in a system where multiple parties collaborate (Pacci et al., 2009). In addition, the characteristic tension between the desires to provide seamlessly integrated services and the importance of providing the end-user with the understanding to take informed decisions (Olsen & Mahler, 2007) is another additional challenge.

2.8. Conclusion

Governments can enhance service delivery to its citizens by incorporating identity management systems in governance. Governments use different technologies to implement their identity management strategies. The approaches depend on cultural, legal and historical differences. Hence, using a single standard for identity management presents a significant challenge. E-government and its connection with identity management are still immature to conclusively say that one approach is better than another. This is highlighted in the research that selected governments studied have their own way of implementing identity management systems. Whatever approach is adopted, its success is judged by citizens' acceptance.

The citizens' must be certain about their government trustworthiness and ensured that they do not suffer from associated risks such as disruption through loss of identity credentials or fraudulent misuse of those credentials, financial loss by interacting with a fraudulent entity etc. Kenyan government has different autonomous systems that contain part of the credentials of a citizen. Linking the autonomous systems is the first step in achieving a single sign-on or federated online identity management system. Interoperable identity management is seen as a key and critical tool for electronic administration along with trust, document authentication and the electronic archive.

Different government ministries and agencies will have to collaborate (managerial and technical) in order to fetch out aggregate information regarding an individual in a single sign-on through the directorate of e-government. A federated model is an ideal solution for the interoperability and

portability of identity information which leads to the provision of citizen-centered, result-oriented and market-based services. In this model responsibilities and accountabilities with the operation is spread over distinct agencies. A continued development of data protection law is very crucial. The Kenyan draft data protection and privacy act must be enacted into law for the citizens to gain confidence, trust and acceptance in using the identity management system. This will aid into the success of the project.

2.9. Research findings

The lessons learnt from the research are:

- There exist traditional, hierarchical, and silo-based model of management and fragmented systems in the Kenya government. Developing a consistent system across the silos that will able them to talk to each other is necessary. The fragmented systems should be linked with an external interface to make them interactive and interoperable. An external interface should have to be developed to interlink National Hospital Insurance fund (NHIF), Immigration and Registration of Person's system (MOI) and Kenya Revenue Authority (KRA) Simba system. These ensures that the fragmented systems to be interactive and interoperable.
- Countries that are using electronic Identity Management System have employed interoperability and security frameworks to ensure that different autonomous systems are integrated and shared. Security frameworks provide benchmarks to ensure a citizen's personal information is safe. Interoperability and security frameworks will be used in developing the system model.
- Citizens' participation to the overall success of identity management is emphasized. Singapore and other Asia countries have managed to implement the system successfully unlike UK, US, Canada and Australia where there is mistrust. A survey will be carried out in Kenyan context to determine views from citizens' regarding electronic identity management. The research only implements technology (Technical Interoperability) aspect of electronic identity management. Analysis from the survey on social and cultural aspects of electronic identity management will be given to client for future consideration and research.

In the next chapter integrated technologies in identity management is discussed.

Integrated technologies in identity management

3.1 Introduction

Identity Management technologies can help government and business enterprises to realize the potential of the digital age by: providing technologies and expertise to make seamless critical business information exchange, creating ways of integrating multiple devices to function interoperable, creating mechanisms of combating fraud attacks and creating unimagined services. Identity management systems comprise organizational processes and several technologies that are used to manage entities' attributes including authorization, authentication and the accounting of information (Pfitzmann and Hansen, 2008). Identity management is always complemented with privacy policies and legislation to protect individuals and service providers (government agencies or business firms) from online security related risks (attacks) and mismanagement of private information. Moreover policies and legislations create ways to provide consumers with better information security assurance and data integrity.

Identity management system can be federated or user-centric (Maler & Reed, 2008). User-centric identity management systems are designed for users to establish their identity and choose what personal information to disclose to which party and for what reason under various circumstances. This will put the management of personal information under the consent of users - knowing the consequence of sharing their personal data and effectively utilize the full range of services in the cybernetic world. In a federated context it specifies how elements of an individual's identity are linked and shared across multiple federated and autonomous data sources hence, increased portability of digital identities (Bhargav-Spantzel et al., 2007).

In the case of Kenya government systems user's personal information, access policies and databases are fragmentally stored across different IdM systems. Typical Silo or Isolated Identity Systems which requires multiple logins for users that creates "identity overload and password fatigue" (Brankovic et al., 2007, p.3). One approach to the problem is centralizing access control information into one server (Centralized Identity System) that requires single-sign-on (SSO) and single identity provider which in turn have a problem of linkability, potential security vulnerabilities and single point of failure (Camenisch et al., 2011).

Implementing a user centric identity management system would make the existing government systems to be modified in order to suit a central database. This would make the exercise costly and not viable. A federated system is ideal because of its ability to link and share distributed applications and since systems are already in place. As argued by Windley (2005) it is an ideal and appropriate approach "for handling authentication and authorization in a cooperative autonomous system where each local system has its own IdM with independent identity schema and with the ownership on the identities it possesses".

In the standardization and development of Identity Management approaches standard bodies like Liberty Alliance, OASIS (Organization for the Advancement of Structured Information Standards), W3C (World Wide Web Consortium), Web Services Interoperability (WS-I), The Internet Engineering Task Force (IETF), The Open Group, Internet2 – (Shibboleth), IDsec, ITU Focus Group on Identity Management (FG IdM), ICANN (Internet Corporation for Assigned Names and Numbers), and DDI (Data Documentation Initiative) can be mentioned. Liberty Alliance specification, SAML (Security Assertion Markup Language), SPML (Service Provisioning Markup Language), XACML (eXtensible Access Control Markup Language) and XKMS (XML Key Management Specifications) are among the widely accepted and implemented standards. The four main standards being used in Identity Federation are Liberty Alliance, SAML, Shibboleth and WS-Federation.

The chapter discusses the technologies appropriate for the implementation of the project. Section 3.1.2 highlights the Web Services 3.1.3 Liberty Alliance project. Section 3.1.3 discusses Security Assertion Markup Language (SAML) and Section 3.1.5 and 3.1.6 highlights Virtual Private Network (VPN). Section 3.2 and Section 3.3 discusses findings from the research and conclusion.

3.2 Web Services

Services are intangible commodities and economic activities that require specialized knowledge and skills and are offered by service providers over a communication media to service consumers. These self-describing, open components are being communicated over the Internet hence, e-Services - the delivery of services by employing Information and Communication Technologies and infrastructures Bean (2010).

The World Wide Web Consortium (W3C) defined Web services as “software systems that support interoperable machine-to-machine interactions over a network. They provide universal glue between different applications within the enterprise or between different companies and they enable fast development of distributed applications in heterogeneous systems.” ORACLE defines Web services as “Web-based applications that use XML standards and transport protocols to exchange data with clients. Web Service Definition Language (WSDL) is used to describe the available services and Simple Object Access Protocol (SOAP) is used to transfer the data in a request and response model over HTTP. XML is used to tag the data.”

The World Wide Web Consortium (W3C) has developed web service architecture to show the basic functionalities and core technologies which are very helpful to aid conceptualization. The following picture shows the basic architecture.

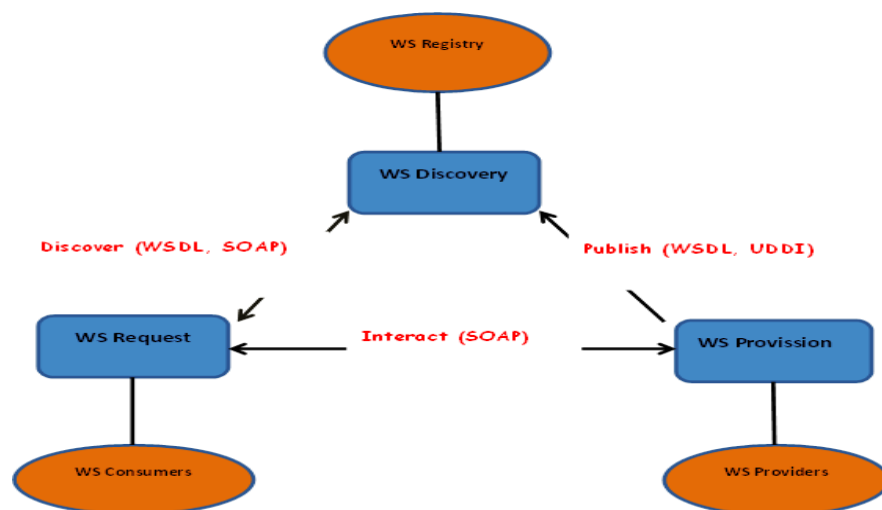


Figure 3.1 Web services architecture (Reproduced from Austin et al., 2004)

Publish signifies describing or making available the services for use by service consumers over an Internet or Intranet by using Web Services Description Language (WSDL). **Discover** signifies making the service discoverable to the service consumers. The discovery request and response with the registry is done by the help of WSDL through the use of Simple Object Access Protocol (SOAP) protocols. **Interact** signifies the communication with clients through the use of SOAP. **WS Registry** stores and renders the capability of listing and searching of services, contact details and quality of service information and all the necessary data about a service based on Universal Description, Discovery and Integration (UDDI) standards (ibid).

There are four architectural models associated with Web services:

- **Message Oriented Model** deals with the structure and mechanisms of transporting the message;
- **Service Oriented Model** deals with the actions associated with the service and user;
- **Resource Oriented Model** deals with the ownership and policy associated with resources;
- **Policy Oriented Model** deals with aspects of security and quality of service (Booth et al., 2004).

Bean (2010) argued Web Services as a kind of SOA (Service Oriented Architecture) service type that depends on rigorous set of standards and the most preferable service type because of its interoperability i.e. having a capability of harmonizing services that runs from different platforms by abolishing the challenges associated with system integration.

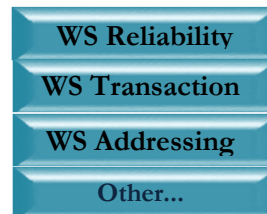
According to Singh et al., (2009), Yu et al., (2008) and Austin et al., (2004) the Web service stack (conceptual and technical standard) contains - Communication, Messaging, Description, Discovery and Process layers while Security, Management and Quality of Services are the associated key functionalities. The **Communication layer** deals with the technologies and concepts focusing on the actual physical exchange of information (network transport) considering HTTP as a de facto network protocol standard. The **Messaging layer** deal with message exchanges and SOAP is the standard under HTTP/HTTPS as an underlying communication protocol. The **Description layer** deals with describing Web services using XML Schema and considering Web Services Description Language (WSDL) as a base standard. The **Discovery layer** deals with the service publication and discovery of service information in the registry to service requestors through the use of UDDI.

The Web Services Technologies offers interoperability between service providers, applications and internal Information Systems within and among organisations. According to Bean (2010) the core Web Services Technology standards are: **Web Service Description Language (WSDL)** the current industry standard for service description i.e. from where and how the functionality is offered, **Simple Object Access Protocol (SOAP)** for communication protocol definition and exchanging structured information between service collaborators (decentralized, distributed), **Universal Description, Discovery and Integration (UDDI)** that renders a registry service which acknowledges advertisement and discovery of Web services and **XML standards** such as XML Schemas Definition Language (XSD) to define facilities and data types and Extensible Markup Language (XML) to store and exchange (transport) data on the Web by supporting wide variety of applications. The picture below describes the standards briefly.

Web Services Communication Protocol



Web Services Management



Web Services Security



Core Web Services Standards Stack



Figure 3.2 Web Services Standards Stack (reproduced from Bean, J. 2010)

Web Services technologies allow applications to pass standardized messages (SOAP messages) over composite computing systems, (Bertino et al., 2010). These programming language, operating system and hardware platform independent software systems are shared and easily be accessed over standard Internet protocols offering richness, flexibility and scalability features needed by service providers (Lé cué et al., 2008). An immigration system for example, passes a standard message informing Kenya Revenue System to "register employee Sara Jane in Income Tax returns system." The Kenya Revenue Authority Systems might respond back, telling the Immigration Department System that it had "successfully added Sara Jane to Income Tax returns.

Web Services technology can be deployed either with other technologies and software design approaches or progressively without requiring structural modification of the legacy system (Bertino et al., 2010). Moreover, the adoption of Web services entails dealing with the issues of frameworks (standards), quality, management and security/privacy. As standards have a capacity to facilitate the adoption and deployment of a system, Web services must be constructed based upon the established and implemented Web Services framework and communication standards created by organizations like Organization for the Advancement of Structured Information Standards (OASIS), Liberty Alliance, and the World Wide Web Consortium (W3C).

As there exists multiple programming languages, operating systems, database, and middleware technologies; delivering a functional and successful web service and maximizing the required payback mainly depends on adopting a common framework thus, benefits achieving seamless integration of various components work in harmony by removing overlaps and conflicts. (Bertino et al., 2010)

Commonly adopted Web Services frameworks are OASIS Framework for Web Services (OWSM), Liberty Alliance Web Services Framework: (Identity Web Services Framework (ID-WSF) and the Identity Service Interface Specifications (ID-SIS)), ORACLE (Oracle Dynamic Services), W3C (Web Services Policy 1.5 - Framework) Microsoft .Net framework, Apache Axis Web Services, and WSO2 Web Services Framework/PHP (WSO2 WSF/PHP) (Papazoglou, 2008).

Value added standards include WS-Security, WS-Policy and WS-Management. WS-Security addresses how to maintain a secure context over a multi-point message path whereas, WS-I addresses interoperability issues, WS-Reliability and WS-Reliable Messaging standards guarantees the Quality of Service (QoS). Moreover, in selecting an appropriate Web Services Framework (WSF) in

addition to the thoroughly discussed points, criteria's such as interoperability and integration, licensing policies and ease of deployment, performance and reputation, must also be considered (Léclercq et al., 2008) the main criterion to use for this research is interoperability.

In the context of e-Government Interoperability can be defined as: *“the ability of information and communication technology (ICT) systems and of the business processes they support to exchange data and to enable sharing of information and knowledge.”* (IDABC, 2004) interoperability signifies the extent to which the federated services would collaborate to undertake a common objective. As interoperability is one of the main challenges of Web services, the application of core Web services technology with the required policy and expertise and the utilization of best practices like the Web Services Interoperability Organization (WS-I) WS-I Basic Profile 1.1 would alleviate the problem.

The UK's e-GIF technical specification details the implementation of SOAP and WSDL specifications and UDDI-compliant systems for registry functions. The adoption of universally accepted common specifications used on the Internet and World Wide Web, and W3C's XML schema i.e. XML (Extensible Mark-up Language) and XSL (Extensible Stylesheet Language) has been taken as a primary standard for the government data interoperability, management and integration strategy. The interface between the intermediaries and government systems conforms to WS-I initiatives and Organization for the Advancement of Structured Information Standards (OASIS) standards. The e-GIF of New Zealand has also adopted UDDI for discovery, WSDL for description, SOAP for Web services transport and security, E-Business Extensible Markup Language (ebXML MSG) for messaging services and Web Services Security (WSS) for the security aspect. The government of Mozambique has also accepted and implemented the core Web Services Technology in its e-Government implementation (Shvaiko et al., 2009).

The other major challenge is safeguarding the security of Web Services which requires ensuring the discovery and availability of services, maintaining the confidentiality and integrity of a message, and enhancing the security mechanisms with appropriate security frameworks. The picture below depicts the security standards offered by NIST (National Institute of Standards and Technology).

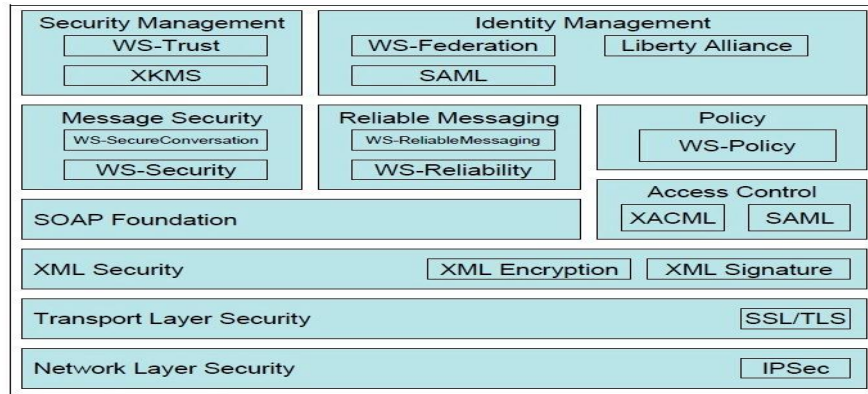


Figure 3.3 Web Services Security Standards (adopted from Winograd et al., 2007)

Security must begin at the network level as messages (request and response) in XML format traverse via Hyper Text Transport Protocol (HTTP) across the network to carry out transactions. (Blaze et al., 2000) Network layer security addresses protecting the traffic between hosts, links, trusted and untrusted networks. End-to-end message integrity, confidentiality and authentication can be achieved through SSL/TLS (point-to-point). (ibid)

The World Wide Web Consortium (W3C) specification called XML Encryption provides a mechanism of encryption to maintain the confidentiality and privacy of SOAP messages. Integrity and non-repudiation can be maintained by applying XML Signature standards to SOAP messages. XML Signature is a specification of W3C and the Internet Engineering Task Force (IETF). Organization for Advancement of Structured Information Standards (OASIS) recommends the application of Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML) with XML Signature for authentication and authorization. Management and monitoring solutions are able to alleviate the problem with service performance and availability issues for example can keep from DoS (Denial of Service) attacks. (Winograd et al., 2007)

Organizations like The World Wide Web Consortium (W3C), Organization for Advancement of Structured Information Standards (OASIS), Web Services Interoperability Organization (WS-I), and Java Community Process (JCP) work on web services security requirements, strategies, and tools both at transport and application level. Requirements such as confidentiality, auditing, trust, authorization, authentication and integrity of SOAP messages as they transverse across networks

should be considered when deploying an identity management system. The figure below highlights security requirements of a web service in an identity management system.

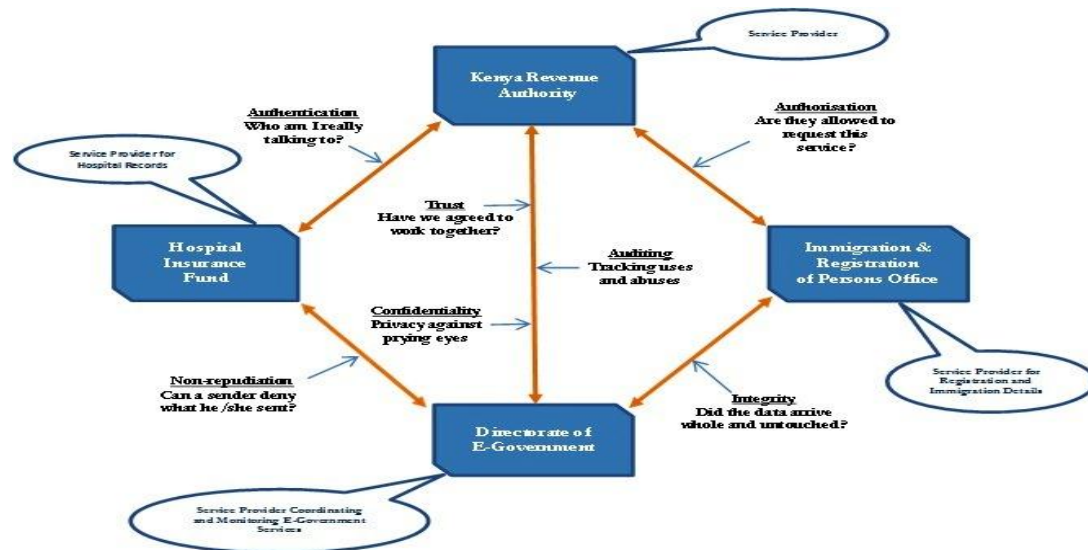


Figure 3.4 shows security considerations for a Web service application

Prevalent standards for identity management solutions include the Liberty Alliance, Security Assertion Markup Language (SAML), Shibboleth and WS-Federation.

3.3 Liberty Alliance project

Liberty alliance is a global identity consortium that incorporates more than 170 companies commenced in 2001. The consortium is dedicated in developing an open standard or specification, guidelines and best practices capable of incorporating other industry standards for federated identity management (Alsaleh & Adams, 2006). The main goal of the project is to provide a level playing field for users and vendors to come together and share ideas on how to incorporate identity management techniques in an organization infrastructure “while respecting the privacy and security of shared identity information”. The consortium creates frameworks and interoperable standards for a trusted network that are open to promote innovation and solve global identity management needs based on circle of trust concept. (Geihs, 2003)

The Liberty architecture is made up of three main components: *identity federation framework (ID-FF)*, the *web services framework (ID-WSF)* and the *services interface specifications (ID-SIS)*. **Identity Federation Framework (ID-FF)** proposes a feasible method for implementing single sign-on and account linking between federated network identities with established trust relationships and Liberty enabled technologies. The objective incorporates building "network identity infrastructure that supports all current and emerging network access devices" and a mechanism for "decentralized authentication and authorization from multiple providers".(Wason & IEEE-ISTO, P.4, 2004-2005). The final version of the framework is ID-FF 1.2 which includes SAML 2.0 of OASIS.

Identity Web Services Framework (ID-WSF) specifies the interaction of trusted partners and the consent of users in releasing and controlling the sharing of their personal information (Cahill et al., 2009). The specifications standardize common functionality features that include authentication, message and privacy protection, service discovery and addressing, policy requirement, data access and management, describing and managing social identity and transport protocols i.e. binding messages to SOAP in order to be carried over HTTP (ibid). Liberty's Identity Web Services Framework (ID-WSF) uses SAML, WS-Discovery services to discover and invoke the service instance, WS-Security and SOAP. The final version of the framework is Liberty Alliance ID-WSF 2.0.

The Liberty Identity Service Interface Specification (ID-SIS) employs ID-WSF and ID-FF specifications to define, design and provide interoperable networked identity services, such as storing and querying personal profiles and wallet services (Kellomäki et al., 2005). The framework consists:

Liberty ID-SIS Personal Profile Service Specification (ID-SIS-PP) to define an identity-based web service that keeps, updates, and manage basic profile information regarding a Principal (user).

Liberty ID-SIS Employee Profile Service Specification (ID-SIS-EP) to define an identity-based web service that keeps, updates, and manage profile information regarding an employee.

New Zealand has incorporated Liberty alliance conformance products in its effort to raise the level of citizen participation and engagement via online channel (NZ e-GIF, 2008). This was achieved by incorporating Liberty web based specifications and Liberty enabled technologies during implementation from vendors. The UK Government Authentication Gateway has also employed Liberty Federation and Liberty Web services specifications to its digital identity management deployments (UK e-GIF, 2005). Countries like Sweden (Stockholm portal), Portugal (Citizen and agency e-government services), Germany's "Citizen Portal", California (Local Government), China: National Development and Reform Commission and Australia: Australian Department of Human Services (DHS) has adopted Liberty federation based upon SAML for their e-Government solution (Liberty Alliance Resource Center, 2011).

Liberty runs comprehensive interoperability conformance tests to ensure that different vendors interoperate and for companies to obtain interoperability certification (Wason & IEEE-ISTO, 2004-2005). This removes the burden of organizations in ensuring that the products being implemented by vendors are interoperable. Organizations just need to check on the liberty mark on the products they want to purchase. Liberty also incorporates a standard that provides a way to define user attributes, entitlements and authentication information in XML document (Kim & Han, 2008).

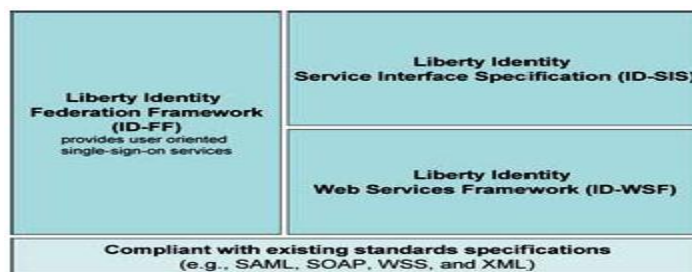


Figure 3.5 : Liberty Alliance Architecture (adopted from Bertino, E. et al, 2010, p.85)

3.4 Security Assertion Markup Language (SAML)

Security Assertion Markup Language (SAML) is an XML-based open standard framework for exchanging authentication and authorization (security) information among systems and applications

(Gupta & Sharman, 2008). The standard is developed by OASIS-Security Services Technical Committee to enable Identity Federation integration by focusing on the security of SOAP messages.

SAML describes a set of XML data formats for representing and exchanging identity attribute information and protocols for access control among security systems (Bertino et al., 2010). It is designed to alleviate the shortcomings and drawbacks of Web Single-Sign-On (SSO) by creating an open standard (protocol and platform independent) and authenticating and authorizing mechanism which works with all type of identity management environments based on XML framework (Liberty Alliance, 2009).

There exist three entities in a SAML information exchange: a subject (the principal that can be a human or a computer) that has an identity in some security domain, the asserting party an authority that issues an assertion regarding a subject (identity provider) and the relying party the consumer (service provider or receiver) of the assertions made by an asserting party. Assertion refers to the identity attributes of a subject or the authentication or authorisation information about a subject. It is a small data produced by SAML [SAMLProf, 2005].

Security related acts or transactions are represented by SAML-assertions; the request communication of such acts or the interaction between the asserting and relying parties is made by SAML-protocols; and the transportation or mapping of request-response messages is made by SAML-bindings and SAML-profile dictates how the interaction works together to provide Single-Sign-On (SSO) [OASIS-sstc-saml-tech-overview-2.0]. An individual application does not need to have a direct access to user repository it only requires knowing and trusting an assertion source. The assertion in SAML is also used in providing audit trail (Lewis & Lewis, 2009). The audit trail includes an evidence chain that is used to make access control decision. The evidence chain gives information such as who accessed what, what time, why and on whose authority. This is used as a legal record which gives additional accountability and security for web service transactions. Moreover, SAML is a standard for encoding authentication declarations that describes the authentication status of a given subject (human or machine) (Bertino et al., 2010).

SAML interfaces can be incorporated to a web service application to link separate access control systems but does not describe the implementation on how local authentication services are provided to the subject (Winograd & NIST, 2007). When a subject requests a service the asserting party

(identity provider) will provide the assertion to the relying party (service provider) and the service provider will provide the service by trusting the assertions made by the asserting party (ibid).

The current version SAML 2.0 is a combination of SAML 1.1, Liberty ID-FF 1.2, and Shibboleth identity federation standards. In addition it has included functionalities of W3C XML encryption, web single sign-on (SSO) and “Single Logout” functionality. SAML eGov-profile is designed for approved e-Government federations and deployment based on the SAML 2.0 specifications. Above all SAML is a preferred XML standard protocol that delivers message-level authentication and integrity services (Chuvakin & Peterson, 2009) for communicating identities across the Internet.

A renowned expert on the field Roberto Baldoni, has made a research on current IdM standards (Baldoni, 2009) on the context of federated identity management and selected SAML as a recommended standard based on platform neutrality, loose coupling of directories, improved online experience for end users, reduced administrative costs for service providers, and risk transference rationale. The table below describes the review of standards.

	Microsoft Passport	SAML	Liberty Alliance	WS-Federation	Open-ID	Shibboleth
Type of Distribution	Specs, implementation and distribution are not free	Specs are free to implement in products and services	Specs are free to implement in products and services	Specs free to review. Implementation and distribution costs unknown	Specs, implementation and distribution are free distributed by the community	Specs are free to implement in software and services
Services	<ul style="list-style-type: none"> • Single-sign-in wallet 	<ul style="list-style-type: none"> • Single-sign-on • Single logout • Opaque identifiers for privacy 	<ul style="list-style-type: none"> • Single sign on based on SAML token • Single logout • Opaque identifiers for privacy • Trust based on legal and business agreements 	<ul style="list-style-type: none"> • Single sign on based on WS trust token • Single logout • Opaque identifiers for privacy • Information sharing based on UDDI 	<ul style="list-style-type: none"> • Single sign on • Single logout • User controlled privacy 	<ul style="list-style-type: none"> • Single sign on based on SAML trust token • Single logout • Attribute check for licensing of software application
Scalability	Small federations	Fully scalable	Fully scalable from Liberty 2	Fully scalable	Fully scalable	Small federations
Attribute exchange	Available	Available	Available from Liberty 2	Available	Available	Available
Third party for attribute certification	Not available	Available	Available from Liberty 2	Available	Available	Available

Table 3.1 : Comparison among different approaches to Federated Identity Management
(adopted from Baldoni R., 2009, p.7)

3.5 Virtual Private Network (VPN)

The National Institute of Standards and Technology (NIST) defines Virtual Private Network (VPN) as “*a virtual network, built on top of existing physical networks that provide a secure communication mechanisms for data and other information transmitted between two endpoints*” (Frankel & NIST, 2008). The Virtual Private Network Consortium (VPNC) has also defines a VPN as “*a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of tunneling protocol and security procedures*” (VPN Consortium, 2008). This networking technology creates a way of securely transmitting sensitive information over private or public networks such as the Internet. Organizations having branch offices across a given geographic location can extend their internal network connection with the help of VPN to securely authenticate the user and transact company sensitive financial information using encryption technologies to remote locations (Carmouche, 2007). In addition, VPN creates a flexible solution for mobile workers to maintain a secure connection to their corporate network in order to share resources and information.

Trusted VPNs, secure VPNs, and hybrid VPNs are the three VPN technologies currently used on the internet (VPN Consortium, 2008; Whiteman & Mattord, 2009). Trusted VPN or legacy VPN uses a leased circuit from the Internet Service Provider for private communication. The line is dedicated for the customer only. A trust between the communications service provider and the customer is mandatory. Secure VPN uses an encryption technology and cryptographic tunneling protocols to communicate with other party through the public network. Cryptographic tunneling protocols include: IPsec (Internet Protocol Security), Transport Layer Security (TLS/SSL), Datagram Transport Layer Security (DTLS), Microsoft Point-to-Point Encryption (MPPE), Secure Socket Tunneling Protocol (SSTP), and Secure Shell (SSH) VPN. The hybrid VPN uses the encryption mechanism and security protocols over a leased line. It simply combines the two technologies (ibid).

As web services are application programs that can be published, located and invoked across the web the need of dynamic management is indisputable. The process of invoking and discovery is taking place in an untrusted network such as Internet hence; security is a great concern for the integrity and confidentiality of the transactions (Bertino et al., 2010). VPN security addresses the external environment processes i.e. the end to end communication of application data between the web service provider and the client environment (web browser). It can be used to establish secure end to

end connections over HTTP using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) the de facto standards used to ensure transport level security for Web applications (Frankel & NIST, 2008; Whiteman & Mattord, 2009).

Secure Socket Layer VPN (SSN VPN) or Transport Layer Security VPN (TLS VPN) is a secure way of communicating applications connected through the Web using VPN (Frankel & NIST, 2008). It does not need a dedicated device or software to be installed on client machine but it can be used with any standard Web browsers like Internet Explorer, Google Chrome and Firefox. Secure Socket Layer VPNs are of two types: SSL portal VPN is a secure SSL way of connecting a user to a Web site in order to access multiple network services over protected HTTP. To access the SSL portal VPN the user will be redirected to a secured URLs typically https. SSL tunnel VPN allows a user to securely communicate and access network resources with the help of a typical Web browser through a tunnel (ibid).

The dominant protocol in Virtual Private Networking (VPN) is IPsec that uses a transport mode or a tunnel mode (Whiteman & Mattord, 2009). The transport mode deals with encrypting the data in an IP packet without encrypting the header information and the delivery of end-to-end transport. The tunnel mode in contrast deals with encrypting all the traffic in an IP packet and traversing in an unsecured network (ibid).

3.6 Conclusion

Web services play critical role in identity management. It enables different systems to integrate and be interoperable. However, there are many challenges in securing web services and reliable authentication of end users which is a fundamental requirement. For our proposed model WS-Security, SAML, and VPN are used to provide strong authentication, authorization, integrity and confidentiality.

SAML is the dominant web services standard for federated identity management and can provide audit function which can be used as a legal record. Virtual Private Network (VPN) provides infrastructure over which to transport sensitive information among service providers or between a service provider and an identity provider to take place. The management operation point manages security policy configurations, client authorization and authentication. VPN does not hinder other

security technologies such as SAML and WS-Security from being implemented. It is important that the simplicity of web services should not be compromised when there is added security.

This requirement is achieved well by web services. The bringing together of Web services, SAML and VPN strengthens these technologies to be used in identity management. However, these technologies should be carefully designed to ensure overall security is improved and no additional vulnerabilities are introduced. The synergy of web services and security technologies offers exciting prospects of a new range of cost-effective and secure applications.

3.7 Research findings

The lessons learnt from the research are;

- Web services address the issue of integration and interoperability. As there exists fragmented systems in the Kenya government ministries, Web services can provide an interface to link these systems. Henceforth, Web service technology will be implemented in the system model.
- Web services have security vulnerabilities which have to be addressed properly. The usage of SAML and VPN mitigates these vulnerabilities. SAML will be incorporated in the system model. The Client Internet Service Provider (ISP) will be requested to setup a Web Service Virtual Private Network (VPN).

The next chapter surveys and analyses the social and cultural aspects of electronic identity management in Kenyan context.

Methodology

This chapter will discuss and justify the research methodology, information gathering (data collection) and processing methods selected.

4.1 Research Purpose

Researches can be classified according to their purpose or function “to understand how the nature of the problem influences the choice of research method” (Zikmund, 2000, p.50) hence, Exploratory, Descriptive and Causal.

Exploratory research is used mainly to gain or discover general information and a deeper understanding of a phenomenon or a topic. It is very helpful to analyze “the general nature of the problem, the possible decision alternatives, and relevant variables that need to be considered” (Aaker et al., 2004, p.75). With the purpose of diagnosing a situation, screening alternatives and discovering new ideas, the method takes several forms: pilot studies, experience surveys, secondary data analysis, case analysis, and focus groups (Zikmund, 2000). The main goal of exploratory research is to provide background information, “the production of inductively derived generalizations about the group, process, activity, or situation under study” (Given, 2008, p.327). In most exploratory studies, qualitative data is interpreted by using descriptive statistics such as indexes, percentages, and frequency distributions. Literature search, analysis of selected cases, experience surveys and focus groups are the main types of exploratory study.

Descriptive research is designed to present an explanation for the current status of the phenomena or population characteristics by answering the question ‘what is going on?’ It is conducted “to provide information about the physical, social, behavioral, economic, or psychological characteristics

of some group of people” (Leary, 2001, p.104) and tries to determine the answers to who, what, when, where and how questions. By implementing observation, data review, questionnaire, interview and survey data collection strategies it seeks to describe ‘what exists’ in the situation and determine “the extent of differences in the needs, perceptions, attitudes, and characteristics of subgroups” (Zikmund, 2000, p. 51). Cross-Sectional Study and Longitudinal Study are the main types of descriptive study.

Causal research (Explanatory) is conducted in order to identify and explain the cause and effect relationships between variables (ibid). It could be carried out through using questionnaires, group discussions, interviews, and random sampling to explain a social phenomenon and find an answer to a problem that put forward a ‘why is it going on?’ question (McNeill & Chapman, 2005). Experiments are the best way to suit constituents of causation.

We will employ exploratory research purpose to gather as much information as possible, discover general insight and get a deeper understanding of electronic identity management systems that uses web services and other integrated technologies. With this method we will come up with a clear understanding of the problem under the study. Furthermore, we will utilize descriptive method to collect and present citizens’ perception about trustworthiness of their government in managing their sensitive personal information and their understanding the usefulness of electronic identity management which will be very helpful to make electronic identity management system successful in its implementation.

4.2 Research Approach

The methodology adopted to conduct a research refers a research approach which involves the selection of research question and appropriate research method. Each approach has its own strength and weaknesses and each is particularly suitable for a particular context hence, the approaches adopted and the method of data collection selected will depend on the nature of the inquiry and the type of information required (Bell, 2010).

Inductive or deductive research approach

The purpose of inductive approach is to briefly summarize extensive raw text data, to establish a link between the research objective and the summary findings, and to develop a model or theory (Thomas, 2007) the research starts with raw data collection and continue to develop a theory as a result of the data analysis. This approach is more credible for grounded theory which is used as an instrument to understand the meaning of complex data through summary or data reduction (ibid). An inductive approach means that from the reality of the case one draws conclusions and creates new theories and models (Bell, 2010). This is to mean that the researcher begins with collecting facts, examines it for patterns and formulates a hypothesis.

The deductive approach begins with the development of theory and hypotheses, followed by hypotheses testing (Brewerton & Millward, 2001). Most commonly, a deductive method is regarded as a highly structured scientific research approach compared to the inductive. Understanding the nature of the research is a major factor in the selection of a research approach to use (ibid). If the area of research is unexplored and there is a lack of relevant literature, an inductive research approach will be preferable. If the area of research holds a wealth of literature that can help to define theory and hypotheses, a good choice is to use a deductive research approach (Saunders et al., 2009).

With this in mind, a deductive research approach seems to be well suiting for our research. As we are focusing on electronic identity management; a number of research have been done on the area and it will be a base theory. So, the research approach used in this study is deductive.

Qualitative or Quantitative research approach

There are broadly two research approaches: quantitative research and qualitative research.

Qualitative research is intended to acquire or explore an in-depth opinion, attitudes, behavior and experiences from participants through such methods as interviews or focus groups (Dawson 2002). The findings in qualitative research are not arrived by means of statistical procedures or any other means of quantification (Strauss and Corbin,1990) it mainly describes a social phenomenon as it occur naturally, by promoting “inductive reasoning and the construction of theory and meaning of phenomena” (Nicholls, 2009, p.533). It provides a more holistic or general examination of a

phenomena relying on observation and participant observation (fieldwork), interviews and questionnaires, documents and texts, and the researcher's impressions and reactions (Myers 2009). It often involves a smaller number of participants or samples as is intended not to obtain information which can be generalized to other larger groups. Examples of qualitative methods are action research, case study research and ethnography (ibid).

Quantitative research is employed to answer questions about “relationships among measured variables with the purpose of explaining, predicting, and controlling phenomena” (Leedy & Ormrod, 2005, p. 94). The process involves objectively measuring variable(s) of interest using standardized instruments by taking representative large sample and drawing unbiased conclusion by detaching oneself from participants. Furthermore, numeric data are collected and analyzed statistically by employing deductive reasoning and the findings are usually communicated using statistics, aggregated data, and numbers (ibid).

Based on the explanation by Berg (2001, p.3) quality refers to “the what, how, when, and where of a thing - its essence and ambience”. Thus, qualitative research refers to the meanings, concepts, definitions, characteristics, metaphors, symbols, and descriptions of things. A qualitative research try to see the phenomena as a whole, within the existing context and serve as an aid instrument to understand how people view things differently as there are many realities. It will strive for a deep knowledge and understanding to answer a research question (ibid).

In order to meet the research objectives, the exploratory nature of our problem statement, and as we intend to study the general nature of electronic identity management and the integrated technologies, we employed a qualitative research approach based on direct observation and document analysis. In addition, to provide a more holistic explanation about the subject, understanding the social and cultural aspect of electronic identity management is mandatory therefore, qualitative research approach helps us to determine citizens' perception and insight which have a major role to play in decision and policy making.

4.3 Research Strategy

Research strategy is a way of collecting and analyzing empirical evidence by following some logic. In accord with Rowley (2002, p.16) “a research design is the logic that links the data to be collected and

the conclusions to be drawn to the initial questions of a study; it ensures coherence”. According to Yin (2003) there are five major research strategies: experiments, surveys, archival analysis, histories and case studies. Having distinctive characteristics, each strategy has its own strength and weaknesses and can be utilized for all the three research purposes: exploratory, descriptive, or explanatory (ibid).

Identifying the type of research question (how, why, who, where, how many and how much), the extent of control of behavioral events, and the degree of focus on contemporary events determines when to use each strategy moreover, a researcher can employ multiple strategies in any given study (ibid). Leary (2001), when explained about the purpose of qualitative exploratory research he emphasized that it is mainly conducted “to obtain basic information about the group of interest or to provide information about the physical, social, behavioral, economic, or psychological characteristics of some group of people” (p.104) thus, a survey strategy best fit for our research and will be conducted for the empirical part.

As surveys are mainly concerned with the demographic characteristics, the social environment, the activities or the opinions or attitudes of some group of people (Moser & Kalton, 1972) with a goal to provide a description of people's behaviors, thoughts, or feelings (Leary, 2001), a researcher asks the same question to chosen people in a written questionnaire and summarizes answers to questions in percentages, tables and graphs by taking a sample or a smaller group of selected people (Neuman, 2000). As a "survey" can be anything from a short paper-and-pencil feedback form to an intensive one-on-one in-depth interview (Trochim, 2008) we have employed a paper based questionnaire as a strategy to collect the empirical evidence.

Thus the next sections will briefly describe the way of sample selection and data collection approaches.

4.4 Sample selection

A process of choosing definite data sources from a larger set of possibilities is known as sampling, a two-step process which includes defining the population and choosing the actual sample. Probability and non-probability sampling are approaches to selecting sample. The most common

form of sampling technique in quantitative research where each participant has the same chance of being selected is a probability sampling whereas convenience sampling, snowball sampling, and purposive sampling are techniques of non-probability sampling in a qualitative research (Bell, 2010).

As purposive sampling involves the selection of informants based on some important characteristic (Leary, 2001), we employed purposive sampling as our problem is related to citizens and their basic identity information and our focus group is any Kenyan citizen who is above 17 years of age. Additionally, the selected public agencies have major communication with every citizen related to identity information and the model incorporates only Ministry of Immigration, Kenya Revenue Authority and National Insurance Fund, we selected informants from these three departments located on capital Nairobi.

4.5 Data Collection Methods

Qualitative research is often preliminary and emphasizes the human factor to understand their behavior, knowledge, attitudes and fears. Characteristically, qualitative research involves qualitative data, i.e., data expressed as words, pictures or objects obtained through methods such as survey/interviews, on-site observations, and focus groups.

In all type of research, the methods selected for data collection is influenced by the nature of the data required (Bell, 2010). Data are “the empirical evidence or information one gathers carefully according to rules or procedures” (Neuman, 2000, p.7). When explaining about data collection strategy, Bell (2010) argued that, the aim of a data collection strategy is to obtain answers from different sources and this will let the researcher to describe, compare and relate one characteristic to another and demonstrate that certain features exist in certain categories. Basically, there are two types of data collection methods Primary and secondary data collection methods.

4.5.1 Primary data Collection

A primary data collection method possesses three different types of data collection strategies: interview, questionnaire and observation. Observation requires the ”systematic noting and recording

of events, behaviors, and artifacts (objects) in the social setting chosen for study” (Marshall & Rossman, 1989, p.79). It is mainly applied when the concern is to record and extract information while being part of a group. It is the most substantial method in all qualitative inquiry. Questionnaires are the very vital part of the survey process often used when a survey strategy is being selected. An interview is a discussion with a purpose between at least two people.

To study the social and cultural aspect of electronic identity management, and to determine citizens’ perception a paper based questionnaire will be distributed at Ministry of immigration, Kenya Revenue Authority and National Hospital Insurance Fund (NHIF) for three weeks’ time. The Directorate of e-government will facilitate the collection and distribution of the survey. Citizens’ will be asked to complete and submit the paper based questionnaire so that the researchers can understand and present the overall citizens’ perception about trustworthiness of authorities in terms of managing identities, the security of citizens’ identity, and understanding the usefulness of electronic identity management which is very helpful to make electronic identity management system successful in its implementation.

4.5.2 Secondary Data Collection

Secondary data is data that has been collected and processed by other researchers for different purposes than what it is used for. It is a very common practice to collect, process, utilize and store data by companies and organizations for the support of their operations. This documented data will serve as a secondary data when used to answer another research question. Secondary data are mostly collected from sources such as megazine, news paper, TV, internet, reviews and research articles.

In order to collect the secondary data or necessary information for the theoretical part, services of Google scholar and databases like EBSCO, SCOPUS (Elsevier) and PubMed - LTU will be used. Books, journal articles, proceedings, and online documents are going to be used for explanation without any publication year’s limitation.

4.6 Methods Problem

In this part of the document the validity and reliability of the research will be discussed and the strengths and weaknesses in the research will be highlighted and pointed out.

4.6.1 Reliability

Reliability is concerned with the question of the degree to which one's findings will be found again (Merriam, 1995); the extent to which a measurement procedure or data collection technique yields the same answer or findings however and whenever is carried out (Kirk & Miller, 1986). There may be four threats to reliability. These threats are: subject or participant error, subject or participant bias, observer error, and observer bias (Trochim, 2008).

Subject or participant error considers how the respondent or informant is set for the research affects the usefulness and generalizability of the results. Such type of error can be reduced through the confidentiality of a questionnaire. Subject or participant bias implicates the influence made by the researcher to participants in some way or the other, in order to portray a certain outcome. Observer error happens when the researcher stimulated answers to prove his/her hypothesis through the format of the question or layout of the questionnaire. Eliminating the human observer with automated instruments or reducing the role of the observer will minimise such an error. Observer bias creates an error when the observer records what he/she expects that participants will do rather than what participants are actually doing. Observer error and bias get reduced by a high degree of structure on the study (ibid.).

Reliability is often at risk when valuations are taken over time and executed by different people (Saunders, Lewis, & Thornhill, 2009). We have selected the most appropriate research design for our study. Extensive literature review from trusted resources has been done on the current technology. The conditions under which measurements are made makes our data more reliable as the respondents are actually waiting to be served and it takes a three weeks' time. The main objective of the survey is to understand citizens' perception towards the capability, efficiency and trustworthiness of the government in managing their personal information. It is possible that the output will vary through time but the intention was to understand the current perception of citizens'. We have tried to reduce the risk of losing any information through observer error and bias of the collected data.

Since the respondents are those who have sensitive personal information at the selected institutions, they have good knowledge, experience and interaction with the institutions, and they are the one who will be benefited from the outcome and speak freely about the topic. This will reduce the subject or participants' bias and error.

4.6.2 Validity

Validity is the “degree to which instruments truly measure the constructs that they are intended to measure”, (Peter, 1979, p. 6). Validity asks how congruent are one’s findings with reality (Merriam, 1995) by this definition the strength of validity becomes lively for the believability of the analysis in measuring what it is intended to measure. Judging by the content of this particular study there are three major types of validity that must be taken into account: content, criterion and construct validity.

Content validity refers to the sufficiency of the coverage of the content in the measurable components (Saunders, Lewis, & Thornhill, 2009). Criterion validity refers to whether a particular measure performs as expected in relation to other variables, also meaning a construct’s ability to estimate other constructs (Trochim, 2008). Construct validity refers to the ability of a measurement tool (in our case a survey) to actually measure the psychological concept being studied (ibid).

There is no problem with the criterion and construct validity of this study as the instrument used in the research (survey) has the ability and properly measures the perception of citizens’ but the sample size may not represent all the population as it is only based on the focus group to collect the data. This might be the method problem that the research faces. However; all the necessary effort will be exerted to collect the available data from the survey conducted.

4.7 Conclusion

This thesis is expressed by theoretical and empirical parts. The theoretical part focuses on reviewing of literatures and briefly describing electronic identity management technologies based on web services and other integrated technologies which are very supportive to make fragmented public sector systems to become interactive and interoperable for data access and sharing. The empirical part focuses on a study in which document analysis is done from ICT board of Kenya and a survey for the explanation of the social and cultural aspect of electronic identity management from citizens’ waiting to be served at Ministry of Immigration, Kenya Revenue Authority and National Hospital Insurance Fund (NHIF).

Citizens' Perception of Identity Management

5.1 Introduction

The previous chapters have tackled technological aspects of electronic identity management and mentioned in brief the social aspects. To ensure the e-Government is actually working a way to monitor and measure citizens' participation and satisfaction is very crucial hence, the survey is intended to investigate attitudes involved in making electronic identity management system (eIDs) successful in its implementation. The survey questionnaire addresses issues such as trustworthiness, security, understanding and usefulness of electronic identity management.

The findings will be forwarded to Directorate of e-government for further action and research. The survey revealed that the majority of the respondents does not trust the institutions and are critical about the competence of the authorities and how they will handle personal data. These negative attitudes should be addressed for the success of implementing electronic identity management in Kenya for the reason that these perceptions may translate into consequent behavior of resistance. A questionnaire was given out in the Ministry of Immigration, National Hospital Insurance Fund offices and Kenya Revenue Authority for a period of three weeks. The Questionnaire was given to citizens' to fill as they wait to be served.

The report is organized as follows: Section 5.2 describes the survey and provides information about the structure and the questions. Section 5.3 describes results of the survey; demographics and results pertaining to survey statements are provided and analyzed. Section 5.4 concludes the key findings and conclusion.

5.2 Survey statements

The survey statements

- I will reveal my identity data and other personal information to be shared across government institutions and agencies.
- I will have little control over my data but will rely on the authorities to manage it.
- Electronic identity management authorities will prevent unauthorized access to my identity and personal information
- There is need to exchange an individual identity data across different government agencies and institutions
- The electronic identity management system will not be technically secure
- The exchange of an individual's identity will be monitored by competent authority
- An individual's interest will be represented in deciding how their identity data is exchanged.
- An appropriate legal environment exists to regulate how an individual's electronic identity data will be exchanged.

5.3 Results and Analysis

5.3.1 Demographics

Overall, there were 1000 responses (57%) to the survey from the 1750 questionnaires distributed to citizens'. After omitting those that were incomplete or did not follow instructions, the number of responses was reduced to 600 (N=600). The percentage of male is 53% and female is 47 %. Males are slightly more than female in the survey. 62% of the respondents were in the population range 16-25, 29% in the population range 26-35, 6% are in the 36-45 and 3% are over 45 age range. The survey respondents comprises of a relatively young population.

5.3.2 Overall results and Analysis

The figures below represent overall results as they relate to 14 statements in the survey. For each statement, the distribution of responses in terms of level of agreement is indicated in percentage. Results pertain to the entire sample that include a total of N=600 valid completed questionnaires.

Analysis of survey data

Some respondents showed willingness for their personal data to be shared across government institutions with a percentage of 43%. Majority expressed their unwillingness.

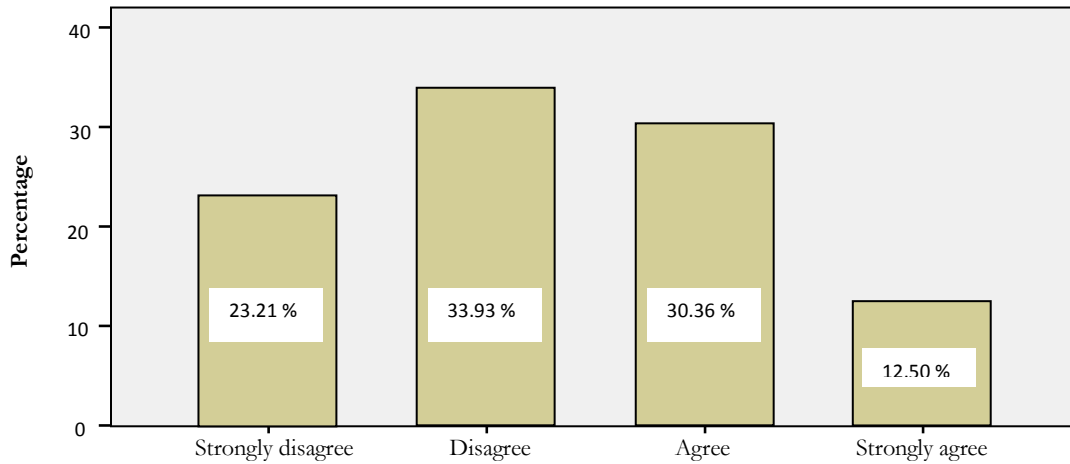


Figure 5.3.1: I will reveal my ID data and other personal information to be shared across government institutions and agencies

The questions about trust received a negative overall evaluation. 44% of the respondents want to have control over their data and manage it.

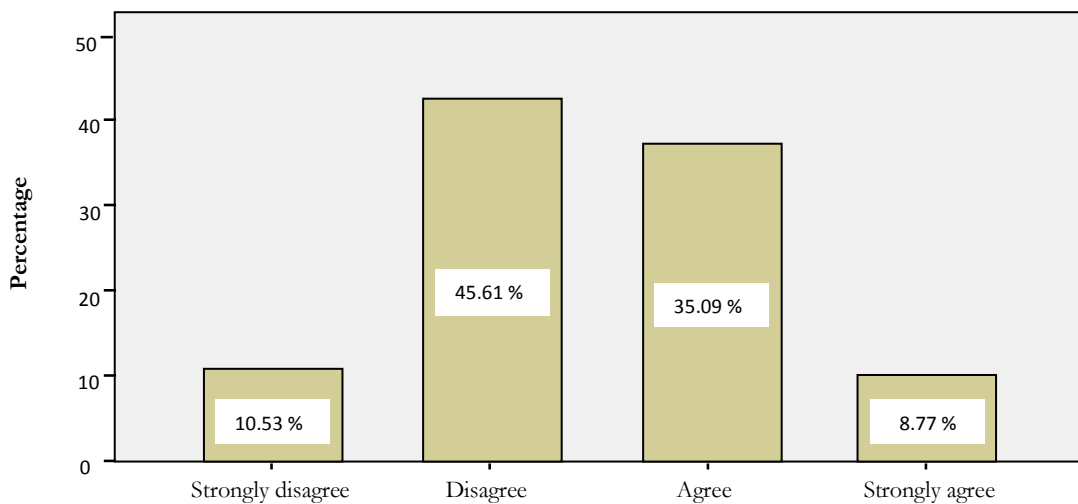


Figure 5.3.2: I will have little control over my data but will rely on the authorities to manage it

52% of the respondents disagree that the electronic identity management authorities will dedicate adequate time and effort in prevention of unauthorized access to personal information. However 47% agree.

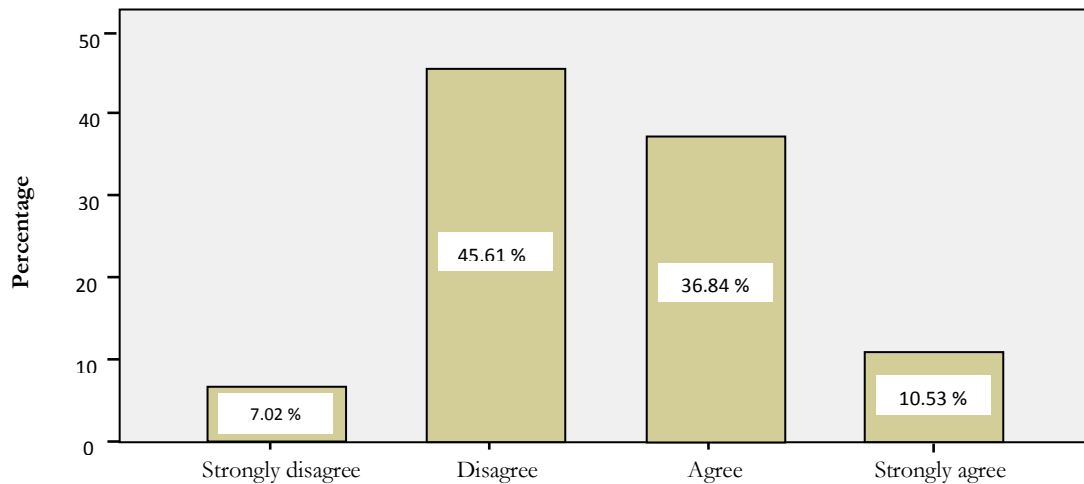


Figure 5.3.3: Electronic identity management authorities will prevent unauthorized access to my identity and personal information

64% of the respondents expressed the need to exchange personal identity data across different government agencies and institutions. Therefore, electronic identity management concept is accepted by the citizens.

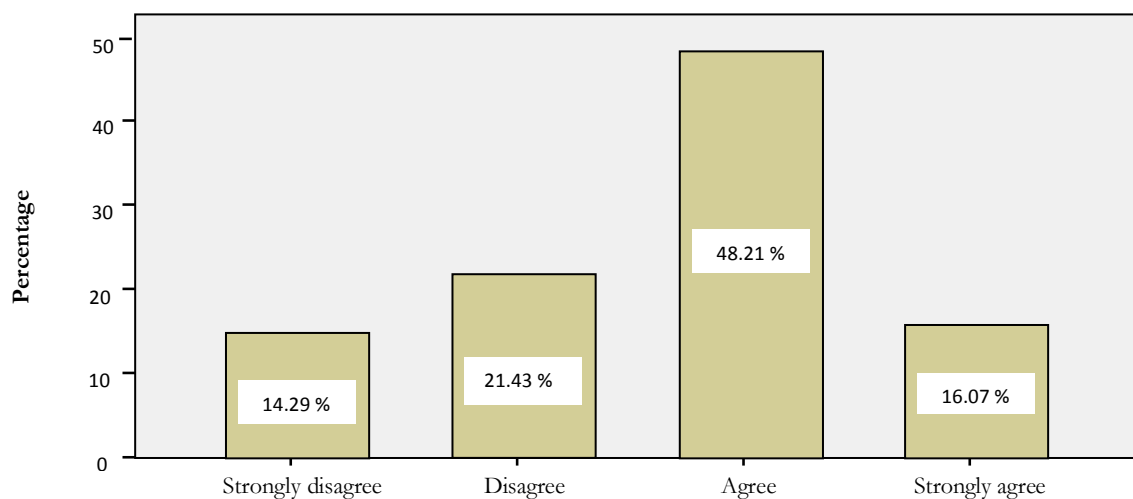


Figure 5.3.4: There is need to exchange an individual identity data across different government agencies and institutions

48% of the respondents consider that forthcoming electronic identity management systems will be technically secure and 51% of the respondents disagreed.

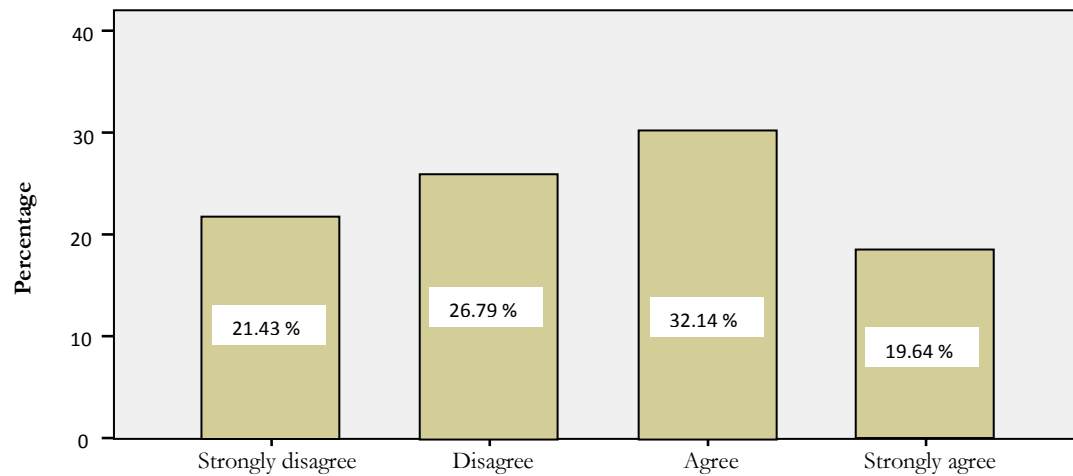


Figure 5.3.5: The electronic identity management system will not be technically secure

The competence of ID authorities in dealing with or managing ID data received a positive overall evaluation. 84% of the respondents agreed.

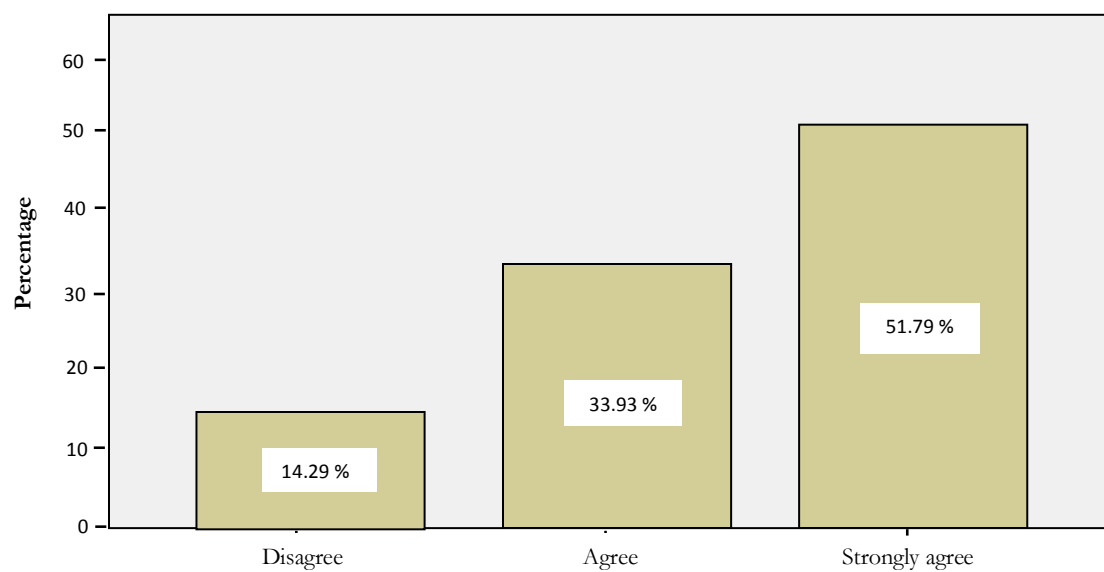


Figure 5.3.6: The exchange of an individual's identity will be monitored by competent authorities

55% of the respondents' disagreed that their interests will be represented in deciding how ID data will be exchanged. 45% of the respondents agreed.

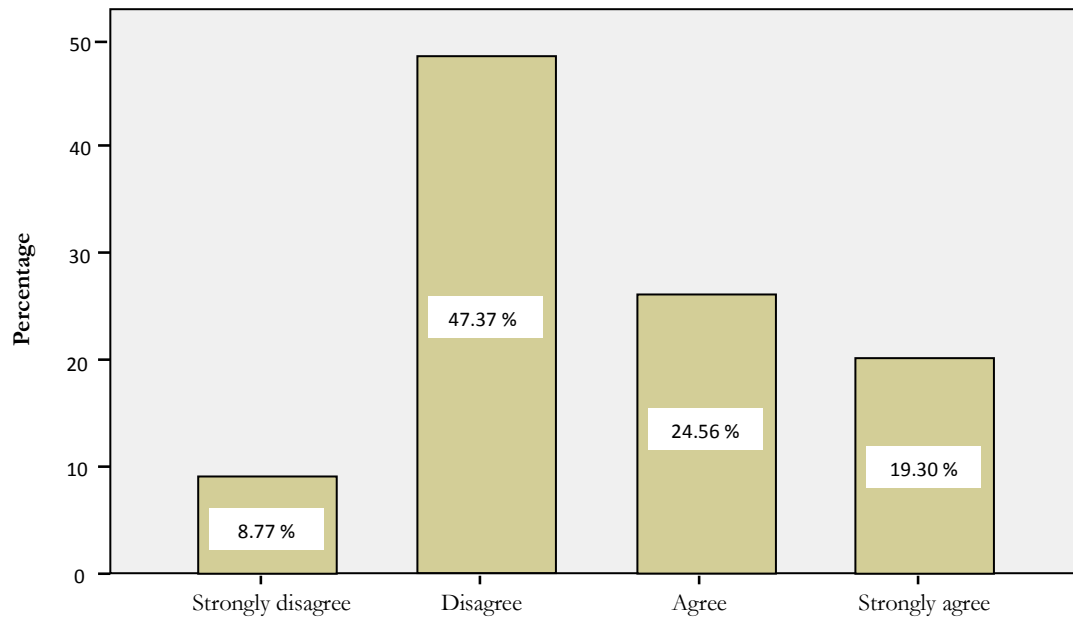


Figure 5.3.7: An individual's interest will be represented in deciding how their identity data is exchanged

The majority of respondents disagreed that there exists an appropriate legal environment for regulating the exchange of identity data. 19% of the respondent agreed and 79% disagreed.

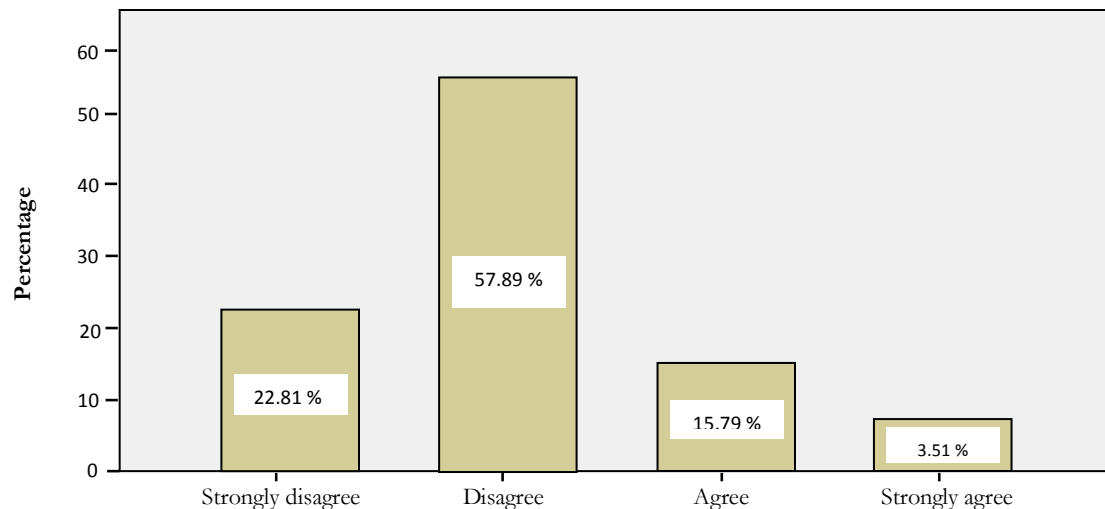


Figure 5.3.8: An appropriate legal environment exists to regulate how an individual's electronic identity data will be exchanged

5.4 Conclusion and key findings

The survey forms part of a research effort to deepen understanding of the social and cultural questions associated with electronic identity management systems. A three week schedule for the survey was agreed with the Directorate of e-government. They facilitated issuing of the survey to Ministry of immigration, Kenya Revenue Authority and National Hospital Insurance Fund (NHIF). The survey was only carried out within Nairobi and therefore, other regions within Kenya should be covered to give accurate results. The citizens waiting to be served were given the questionnaire to fill. (Refer to Appendix A1).

Findings arising from the analysis of the survey point to an overall negative perception of the electronic identity management in Kenya. The vast majority of the respondents do not trust the institutions, there are mixed reactions regarding the competence of the authorities, and their ability to handle identity data and how technical the identity system is. The respondents were evenly balanced. However, the respondents expressed the need to have an electronic identity management system for exchange of an individual's identity data across government institutions and agencies. The lack of appropriate legislation on electronic identity management has an influence on the perceptions being expressed by the citizens. These perceptions may be translated into consequent behavior i.e. resistance to use or non-use. Therefore, this has a direct implication on successful implementation of electronic identity management in Kenya.

Social and cultural aspects should be looked into in implementing an electronic identity management system. Further research and awareness should be undertaken on citizens' feelings and perceptions for a successful electronic identity management system. Also draft legislation on electronic identity management should be produced for debate in parliament.

The recommendations arising from survey includes;

- Respondents acknowledge the need for an electronic identity management system
- The respondents had mixed reactions about the technical security of the system

However, social and cultural security to gain trust in the system should be addressed but, the research scope does not cover social aspects of electronic identity management system in depth.

In the next chapter a system model based on research findings is discussed.

System Model

6.1 Introduction

The main objective of this thesis is to propose a solution for federating government agencies in order to make them integrate in administering and sharing citizen's identity information in their identity management system, based on the research findings. The system will enable fragmented autonomous systems located in the Kenyan e-government to integrate to an overall external interface through the directorate of e-government. By employing Microsoft SQL Server, MySQL and Oracle 11g DBMS databases it aims achieving a federated identity management (refer to section 2.2.3). The interoperability and interactivity is offered by Php Dom and XML. Security of web services is implemented in SAML and VPN. PHP DOM/XML class library is used in creating, extending and manipulating XML application.

The National Hospital Insurance fund (NHIF), Immigration and Registration of Persons System (MOI) and Kenya Revenue Authority (KRA) Simba System are included by the system. Only a citizen's tax returns section of the KRA system is used and does not cover corporate and institutional tax returns. Business modeling domain and activity chart that shows elements addressed in research findings are discussed in section 6.2. System portal structure with the elements used and the design and implementation of the model is highlighted in section 6.3. Section 6.4 discusses conclusion.

6.2 Business Modeling Domain

From research findings, figure 6.1 shows a business model domain that consists of elements that are addressed for the electronic identity management system.

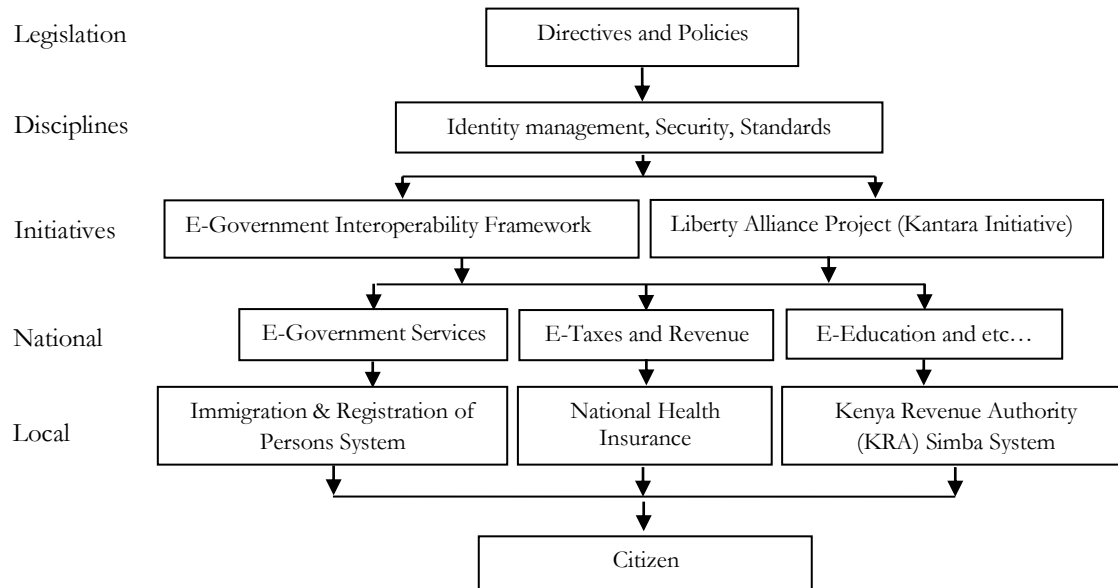


Figure 6.1 Business Model Domain for e-identity management system

The subsequent section discusses the elements in the business model domain.

6.2.1 Legislation

Kenyan governance is directed at the highest level through the Kenyan parliament. The parliament should make policies and directives regarding identity management. The aim is to protect citizens with regard to personal information and free movement of their data.

6.2.2 Common disciplines

Identity management technology cannot be deployed alone. The system need to incorporate other disciplines such as data protection, information management and security. Kenya can learn greatly from other countries (refer to section 2.4) that have written standards and records management on identity management systems. International bodies such as OASIS and Liberty Alliance Initiatives can also be of great assistance.

6.2.3 Projects and initiatives

Projects that are currently tackling electronic identity management should be taken into account to aid in understanding and implementation. Such projects include Liberty Alliance project (Kantara Initiative), Concordia Project, European interoperability Framework, and electronic-Government Interoperability Framework (e-GIF). (Refer to section 2.3).

6.2.4 National Governance

The directorate of e-government should work with other government ministries, agencies and institutions to put guidelines, monitor participant's compliance, regulate and direct strategies for the ongoing development and assistance in deploying and managing electronic identity management.

6.2.5 Local governance

Government agencies and institutions should put policies and departments to administer electronic identity management (responsibilities and accountabilities associated with operations) under the guidance and control of directorate of e-government.

6.3 System model portal

The portal structure of electronic identity management system model, shown in figure 6.2, consists of an activity chart that highlights the steps to be followed. The activity chart is divided into five parts which are then divided into elements. The elements are described below.

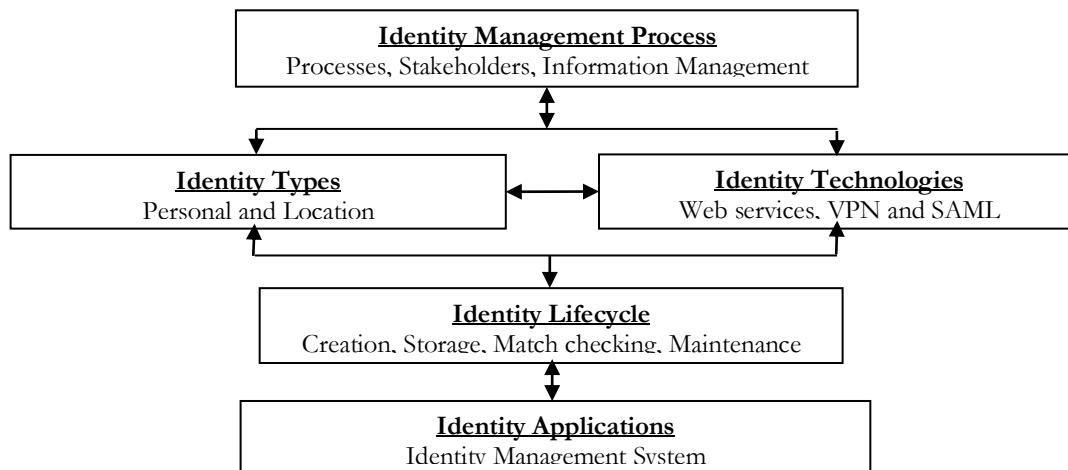


Figure 6.2: portal structure of e-identity management system model

6.3.1 Identity management process

The process is sub-divided into the following elements.

6.3.1.1 *Processes*

Processes and information models are developed to show how identities are managed within each stakeholder.

6.3.1.2 *Stakeholders*

The stakeholders are directorate of e-government and government institutions. The government institutions involved includes Ministry of Immigration (MOI), National Hospital Insurance Fund (NHIF) and Kenya Revenue Authority (KRA). The directorate of e-government will have the overall mandate of the identity management system. However other stake holder's roles and responsibilities should be specified in an identity policy document.

6.3.1.3 *Information Management*

Information management of existing systems must ensure that right information is delivered at the right place and right time.

6.3.2 Types of Identity

The identities incorporated are personal and location. Biological identities will be developed in the next phase. Personal identities include Personal Identification Number (PIN), National Identification Number (NIN) and Name. Location identities include physical address; email address, mobile telephone contacts etc.

6.3.3 Identity Technologies

The identity technologies implemented are interoperability and security techniques. Federating identities is mandatory for the interoperability, collaboration, sharing, and exchange of information across the different platforms. A mutual trust and agreement between the client and other

stakeholders has to be carried out in order to determine their roles and responsibilities towards the system. SAML and Virtual Private Networks (VPN) are used in developing the model. Biometrics can be integrated and used to authenticate the person using the system but not included in this phase.

6.3.4 Identity Lifecycle

The identity lifecycle consists of the following stages;

6.3.4.1 *Creation*

Extreme care must be taken when linking and creating citizen identities from the different autonomous systems. The digital identities must be accurate, complete, authentic and unique.

6.3.4.2 *Storage*

The current model addresses aspects such as automatic backups in the different interfaced databases. However, adequate assurance against information risks should have to be developed for the citizenry to build trust on the system.

6.3.4.3 *Maintenance*

It is critical that all identity databases and processes interlinked must be up to date. The databases should be synchronized and updates be done by authorized personnel. The external web interfaces does not update the different databases. This has been left to the different government agencies and institutions systems.

6.3.5 System model interfaces

The model is based on the use of identities throughout their lifecycle in e-government. The Identity management model has the following custom interfaces;

6.3.5.1 Login Interface

SAML's flexible specifications offers the opportunity to implement many customized deployment and integration of application options. Hence, the authentication mechanisms is based on the concept of credentials. A widely used common internet standard Username/password authentication is applied. The login interface will integrate Shibboleth 2.0 based on SAML 2.0 standards as it is an open-source and ideal for federated identity authentication and authorization purpose. It also supports Single Sign-On and Single Sign-Off functionalities. The login page will have the option of using the username and password interface to gain access into the system. Users log in to access information situated and stored in federated agencies. Figure 6.3 shows the login interface.

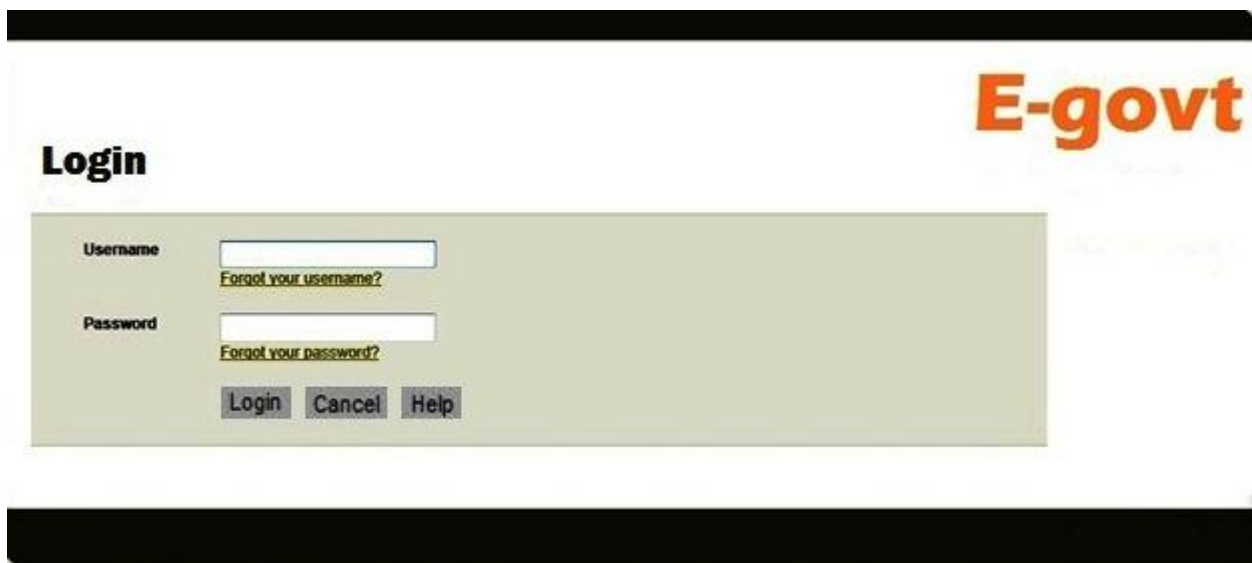
The image shows a web browser window with a black header and footer. The main content area has a white background. In the top right corner, there is a logo that says "E-govt" in orange. On the left side, the word "Login" is written in bold black text. Below it, there is a light green rectangular box containing the login form. Inside the box, there are two input fields: "Username" and "Password". Below the "Username" field is a link that says "Forgot your username?". Below the "Password" field is a link that says "Forgot your password?". At the bottom of the box, there are three buttons: "Login", "Cancel", and "Help".

Figure 6.3: Login Interface

The authorization is targeted to users using the system in the different government agencies and institutions. After login is successful processes such as search a person will be available. Several functions can be selected using the push buttons. By selecting search person, search.html page will be loaded from the host application.

6.3.6 Sample Use Case for Searching Citizen's Information

The different text fields provided will enable the user to input information located in different database management systems (DBMS) situated in the specified government agencies and institutions. The interface provides a way of interacting with data where for example, name is located in MSSQL database table that holds information of the Ministry of Immigration department. ID number field is available on the NHIF database table located in the NHIF Schema on Oracle 11g DBMS. Personal Identification Number (PIN) and Employer are found on the Kenya Revenue Authority table on the KRA database running on MySQL DBMS. Figure 6.4 shows the search criteria interface.

The screenshot displays the 'E-govt Identity Management System' search interface. On the left, a vertical menu contains buttons for 'Home', 'Search Person', 'Log Out', and 'Exit System'. The main content area has a title 'Identity Management System' and a subtitle 'Fill with Proper Search Criteria'. Below this, there are input fields for 'Name', 'ID Number' (containing the value '8904152236'), 'Passport Number', 'Date of Birth', 'PIN Number', and 'Employer'. A 'Search' button is positioned at the bottom right of the form.

Figure 6.4 Search Criteria Interface

For instance, by providing an Id Number and clicking the search button, the system will search the Id Number from the MySQL database. By use of PHP DOM, an xml file called kra.xml will be generated at the backend and selects Id number from the KRA record that has been retrieved and uses it to obtain same person's data from the Oracle database (NHIF) and a nhif.xml file will be

generated. The Oracle database has an Id Number of the same person's which then retrieves the same person's data from MSSQL database (MOI). An immigration.xml file will be generated.

The system will load eXtensible Markup Language (XML) files generated, read the data in them and write it to the user interface as an html file. This ensures uniformity and consistency of the output. After we provide the Identity number for example, and then press on the Search button within the browser component, it will load a page with the person's details from the different databases. The engine that does the processing of what to display is PHP. The ideal output is shown in the results interface in figure 6.5 below. The browse component of Visual Basic can be used to load the web based pages of the System.

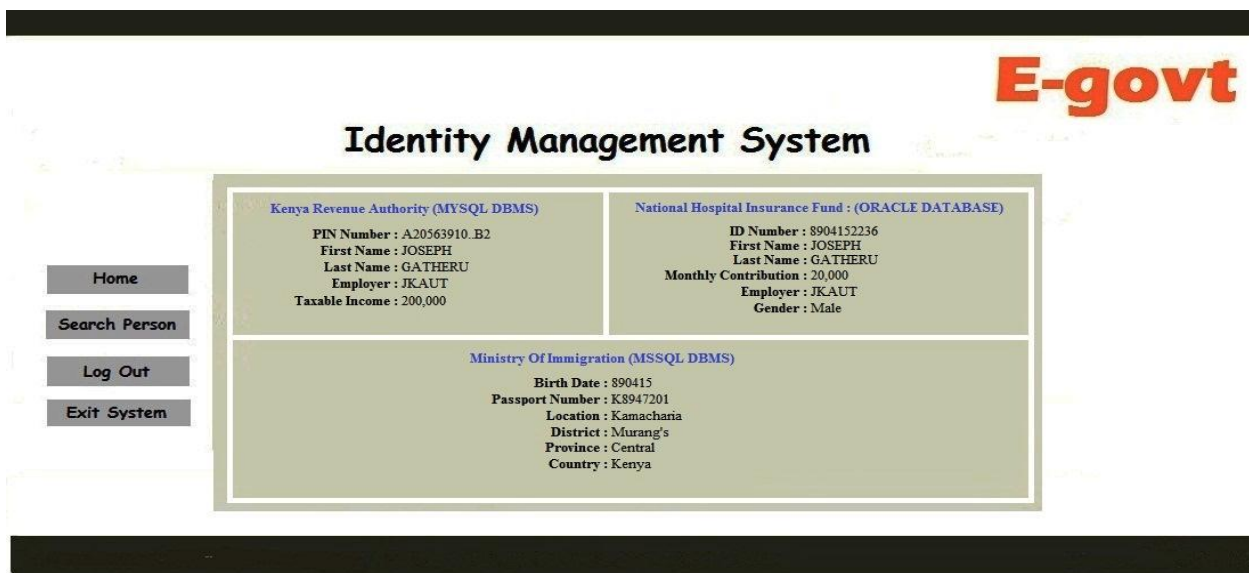


Figure 6.5: Results Interface

6.4 Conclusion

To enable interoperability across government agencies one does not start with technology but with a government interoperability framework (GIF), collaboration, clearly defined policies and trust. A government wide policy is very crucial for public agencies coordination and identity, credential, and

access management; as these activities improves access to electronic government services internally with other government associates, with business partners, and with citizen constituency. Regarding technology, the adoption of open standards for their availability, take full advantage of end users choice, no discrimination and royalty fee, and circumvention of vendor lock-in gives the government to possess a free choice of technology and vendors.

Each organization plays both roles of being a service provider and identity provider based on trust and federation. Assigned or delegated users from each agency office should have to be registered and given a unique identifier. The authorisation and access control is (SSO) maintained by directorate of e-government.

Every office is responsible to manage the lifecycle of user identities. Every office is also responsible to authenticate a user and act as an issuing party for that specific user while the others became relying parties. A federated gate way that functions as a single point of contact for all resource access based on Proxy SAML/SAML Gateway is necessary for effective interaction between agencies. Hence the authentication interface will be integrated in the existing e-government portal and at agencies web pages. The integration of identities is done through the interface as it supports SAML 2.0.

The model has incorporated every aspect through the use of Web service, relational database management technology, SAML, and VPN, and has achieved the objective of data interoperability and integration. An integrated e-government identity management system brings together citizens, professionals and service providers. This ensures there is continuous improvement on the system throughout its lifecycle. Authorised users can also be authenticated through the use of username and password included in the login interface. There is also a potential to include a biometric identification but not included at this stage. The business model domain shows more initiatives need to be done such as legislation and citizen acceptance to make the system a success. Technology alone cannot be used to measure the level of success in identity management systems.

Evaluation and Conclusion

7.1 Introduction

The purpose of this chapter is to critically evaluate the completed research project against its terms of reference as set out at the start. Evaluation and conclusions are presented for each of the objectives and how they have demonstrated through the research and model development. Attention is accorded to the integration of the research to the proposed model development. The final outputs of the research are compared against the objectives of the research to assess how far these objectives have been achieved. Finally, lessons learned from the project experience are presented and future research discussed.

The evaluation is divided into four major parts. Integration of the research to the system model development is given in section 7.2. An assessment of outcomes against objectives and evaluation is given in Section 7.3. Section 7.4 discusses Limitations and future work. Section 7.5 and 7.6 discusses lessons learned and conclusion respectively.

7.2 Integration of the research to the System Model development

Chapter 2 described identity management and the findings, (refer section 2.8) that assisted in the development of the system model. The chapter also illustrated the level of e-government in Kenya and compared it with other countries. The frameworks for electronic identity management used in other countries and their applicability in Kenyan context are also illustrated. The chapter also reviewed cultural, legal and social aspects of electronic identity management. This provided a framework to establish a survey in order to determine the perception of electronic identity

management among citizens in Kenya (refer chapter 5). The recommendations (refer section 2.8) were considered during system model development. Chapter 3 discussed integrated technologies in identity management like Web services, Security Assertion Mark-up Language (SAML), and Virtual Private Network (VPN) technologies. These technologies are used for developing electronic identity management systems. They formed as a guide and point of reference in the developing the system model. The research findings (refer section 3.3) have aided in the system model development.

7.3 Evaluation against Aims and Objectives

7.3.1 Objective 1

The first objective was to research technologies and approaches to electronic identity management, best practices and challenges. During the project, literature review on current technologies and practices on identity management was carried out including approaches of identity management in other e-governments such as Australia, Mauritius, and New Zealand etc. This review, given as Chapter 2 and Chapter 3 in the thesis, enabled us the identification of approaches and comparison of identity management with other jurisdictions in e-government and the integrated identity management technologies. However, due to the limit on the time and length of the MSc. thesis, the literature review only briefly outlines the approaches and practices of identity management within e-government. It does not go further to highlight risks and mitigation measures that different countries have put in adopting identity management. Hence, this objective has been achieved.

7.3.2 Objective 2

The second objective was to explore citizens' perception on electronic identity management. Survey and analysis was carried out in chapter 5. The challenges for future direction were identified in the survey and hence the objective has been achieved.

Evaluating the key findings from the survey and their implications for the future are discussed in the final chapter of this thesis, thus achieving this objective. Despite their busy schedule, Directorate of e-government staff members have helped us in the distribution of questionnaires to selected government institutions and agencies to understand the electronic identity management system limitations and strengths from citizen's perception. Though the questionnaire was distributed within Nairobi, the findings is hoped to assist the client in ensuring electronic identity management system success.

The survey was carried out by means of a structured questionnaire to make it easy for respondents to reply. A three week schedule for the survey was agreed with the Directorate of e-government. They facilitated issuing of the survey to the Ministry of immigration, Kenya Revenue Authority and National Hospital Insurance Fund (NHIF). The survey was only carried out within Nairobi and therefore, other regions within Kenya should be covered to give accurate results. The citizens waiting to be served were given the questionnaire to fill.

7.3.3 Objective 3

The third objective was to develop a model/framework for identity management system. This objective has been achieved in Chapter 6 which details the technologies and strategies taken to develop an identity management solution for the integration and interoperability of fragmented citizen's identity information situated in three different public agencies.

7.4 Limitations and future work

Due to limitations in time and expertise, the electronic identity management has few limitations. The major limitations are;

- 'The system model has not addressed risks and mitigation measures in the event of failure or incorrect matching of identity persons'.

- Backup and restore mechanisms was not covered in the research. Comparisons with other jurisdictions should be undertaken for an effective backup and restore procedures for an interoperable and distributed electronic identity management system.
- Social and cultural aspects of electronic identity management have not being discussed at length in the thesis. Draft legislation on electronic identity management should be the deliverable. The draft can then be debated in parliament.
- The survey was carried out within Nairobi and therefore, other regions within Kenya were not captured. The survey should cover all regions to give a broader representation.

7.5 Lessons learned

The thesis work enhances our knowledge and expertise in realizing what electronic identity management and related technologies are such as Web services and VPN's. It also enabled us to increase our realization of the numerous functionalities these technologies can offer in the course of the model development, the project has also provided us with ample knowledge on federated identity management and user communication. Further implementation of the model and the participation of system users is an influential factor towards the system success since they will be the final operators of the system. The citizens will also have a final word to the system since they are the 'customers.' Adherence to stated principles and guidelines is also not an easy undertaking, but eventually it is worth every effort. All aspects of the thesis have provided us with a lot of experience that will be valuable to future project undertakings.

7.6 Conclusion

The research has demonstrated that systems and services can be connected and work together easily and effectively, while maintaining confidentiality, privacy and security. Common policies and related initiatives concerning identity management and interoperability have been identified and discussed.

There is need to participate in developing standards for federated identity management and liaise with other research initiatives and projects. The initiatives include Future of Identities in the Information Society (FIDIS) research. This ensures adherence to standards and best practices while developing a federated identity management system.

The ability to federate identities across organizations while maintaining clear trust, liability and cost responsibilities is a major challenge for governments and enterprises as they pursue efficiency and cost savings in cross-organizational business and customer-relationship processes.

There are many research and development challenges to address before seamless identity management becomes a reality. The end consumers and citizens need assurances regarding privacy of sensitive information. Further research should be undertaken to elaborate the interplay between authentication and authorization in federated identity management. We must also refine existing access-control models to reflect the obligations on the provider and consumer of identities in multiparty transactions. We need lightweight and user transparent protocols with zero, or very small, footprints to run on end users' machines. There is also need to look at emerging client-side platforms that permit some degree of trust in the end systems themselves.

References

- Aaker, D. A., Kumar, V., & Day, G. S. (2004). *Marketing research*. New York: Wiley.
- Arabo, A., Shi, Q., & Merabti, M. (October 01, 2009). Context-Aware Identity Management in Pervasive Ad-hoc Environments. *International Journal of Advanced Pervasive and Ubiquitous Computing*, 1, 4, 29-42.
- Aichholzer, Georg & Strauß, Stefan (2010). The Austrian case: multi-card concept and the relationship between citizen ID and social security cards. *Identity in the Information Society* 3 (1):65-85.
- Alsaleh, M., & Adams, C. (January 01, 2006). Enhancing Consumer Privacy in the Liberty Alliance Identity Federation and Web Services Frameworks. *Lecture Notes in Computer Science*, 4258, 59-77.
- Austin D., Barbir A., Ferris C. and Garg S. eds. Web Services Architecture Requirements (W3C Working Group Note, 11 February 2004). Online at: <http://www.w3.org/TR/wsa-reqs/#id2604831>
- Australia. (2009). *National e-Authentication framework*. Canberra: Dept. of Finance and Deregulation.
- Austria (2011), <http://www.digital.austria.gv.at>
- Baldoni R. (2010). 'Federated Identity Management Systems in e-Government: the Case of Italy', *Electronic Government: An International Journal*, Vol. 8, No. 1, 2010.
- Bean, J. (2010). *SOA and web services interface design: Principles, techniques, and standards*. (SOA and web services interface design.) Amsterdam: Elsevier/Morgan Kaufmann.
- Bell, J. (2010). *Doing your research project: A guide for first-time researchers in education, health and social science*. Maidenhead: McGraw-Hill Open University Press.
- Benantar, M. (2006). *Access control systems: Security, identity management and trust models*. New York: Springer Science+Business Media.
- Berg, B. L. (2001). *Qualitative research methods for the social sciences*. Boston: Allyn and Bacon.
- Bertino, E., Martino, L., Paci, F., & Squicciarini, A. (2010). *Security for Web Services and Service-Oriented Architectures*. (Security for web services and service-oriented architectures.) Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg.

- Bhargav-Spantzel, A., LaCamenischst, J., Gross, T., & Sommer, D. (2007). User centrlicity: a taxonomy and open issues. *Journal of Computer Security*, 15, 493–527.
- Bhargav-Spantzel, A., Squicciarini, A. C., & Bertino, E. (January 01, 2006). Establishing and protecting digital identity in federation systems. *Journal of Computer Security*, 14, 3, 269-300.
- Booth, D., Haas, H., McCabe, F., Newcomer, E., Champion, M., & Ferris, C. (Eds.). (2004, February 11). Web services architecture [W3C Working Group Note Retrieved September 21, 2011, from <http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/>
- Bramhall, P., Hansen, M., Rannenber, K., & Roessler, T. (January 01, 2007). User-Centric Identity Management: New Trends in Standardization and Regulation. *Ieee Security & Privacy*, 5, 4, 84-87.
- Brankovic, Ljiljana, Coddington, Paul, Roddick, John F., Steketee, Chris, Warren, Jim, Wendelborn, Andrew, Josang, Audun, ... Suriadi, Suriadi. (2007). *Usability and privacy in identity management architectures*. Australian Computer Society.
- Brazier, J. E. and A. Mannur, (2003) (eds) *Theorizing Diaspora: A Reader*, Malden, Massachussets: Blackwell.
- Brewerton, P., & Millward, L. (2001). *Organizational research methods: A guide for students and researchers*. London: Sage Publications Ltd.
- Buell, D. A., Sandhu, R., & IEEE Computer Society, (2003). *Identity management*. Los Alamitos, Calif.
- Burr, W. E., & National Institute of Standards and Technology (U.S.). (2006). *Electronic authentication guideline: Recommendations of the National Institute of Standards and Technology*. Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology.
- Cahill C., Canales C., Le Van Gong H., Madsen P., Maler E., and Whitehead G. (2009, January). Liberty alliance web services framework: A technical overview, Liberty Alliance Project. [Online]. Available:<http://www.projectliberty.org/specs>.
- Camenisch, J., Leenes, R., & Sommer, D. (2011). *Digital privacy: PRIME-- privacy and identity management for Europe*. Berlin: Springer.
- Carmouche, J. H. (2007). *IPsec virtual private network fundamentals*. Indianapolis, Ind: Cisco Press.

Chuvakin, A., & Peterson, G. (January 01, 2009). Logging in the Age of Web Services. *Ieee Security & Privacy*, 7, 3, 82-85.

Claus, S. (October 01, 2001). Identity management and its support of multilateral security. *Computer Networks*, 37, 2, 205-219.

Clemm, A., Festor, O., & Pras, A. (January 01, 2005). Managing New Networked Worlds: A Report on IM 2005. *Journal of Network and Systems Management*, 13, 3, 351-354.

Dawson, C. (2002). *Practical research methods: A user-friendly guide to mastering research techniques and projects*. Oxford: How To Books.

Denmark (2011), <http://www.denmark.dk>

Dhamija, R., & Dussault, L. (March 01, 2008). The seven flaws of identity management: Usability and security challenges. *Ieee Security and Privacy*, 6, 2, 24-29.

E-government–Kenya. (2004). *E-Government priorities and implementation strategy*, <http://www.e-government.go.ke>. Accessed 15 July 2011.

EUC Workshops, Denko, M. K., & International Federation for Information Processing. (2007). *Emerging direction in embedded and ubiquitous computing: EUC 2007 Workshops, TRUST, WSOC, NCUS, UUWSN, USN, ESO, and SECUBIQ, Taipei, Taiwan, December 17-20, 2007: proceedings*. Berlin: Springer.

Fioravanti, F., & Nardelli, E. (2008). Identity Management for E-government Services. In Chen, H. (eds.). *Digital government: e-government research, case studies and implementation*. (pp. 331-352). Berlin: Springer.

Frankel, S., & National Institute of Standards and Technology (U.S.). (2008). *Guide to SSL VPNs: Recommendations of the National Institute of Standards and Technology*. Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology.

Gartner Group, *Key Issues in E-Government Strategy and Management, Research Notes, Key Issues*, 23 May 2000.

Geihs, K., Kalcklosch, R., & Grode, A. (January 01, 2003). Single Sign-On in Service-Oriented Computing. *Lecture Notes in Computer Science*, 2910, 384-394.

Given, L. M. (2008). *The Sage encyclopedia of qualitative research methods*. Los Angeles, Calif: Sage Publications.

Glasser U, & Vajihollahi M (2008) Identity management architecture. In: Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on, pp 137-144, DOI f10.1109/ISI.2008.4565043g

Gray, V., Michael, M., and Marcelino T. (2004). The Fifth Pillar: Republic of Mauritius ICT Case Study.

Gupta M. and Sharman R., (September 19, 2008). Dimensions of Identity federation: A Case Study in Financial Services. *Journal of Information Assurance and Security* 3, 244-256.

Hansen, M., Schwartz, A. and Cooper, A. (2007). "Privacy and Identity Management", IEEE Security & Privacy, 10(6), pp.13-20.

Hoff, Jens & Hoff, Frederik (2010). The Danish eID case: twenty years of delay. Identity in the Information Society 3 (1):155-174.

IDABC (2004) European Interoperability Framework for pan-European e-government Services. Luxembourg, European Communities.

Institute of Electrical and Electronics, & Falk, R. (2009). *Third International Conference on Emerging Security Information, Systems, and Technologies (Securware 2009)*. IEEE

Jain, A. K., Ross, A., & Prabhakar, S. (January 01, 2004). An Introduction to Biometric Recognition. *Ieee Transactions on Circuits and Systems for Video Technology*, 14, 1, 4-20.

Jick, T. D. (January 01, 1979). Mixing Qualitative and Quantitative Methods: Triangulation in Action. *Administrative Science Quarterly*, 24, 4, 602-611.

Jøsang A. and Pope S. User Centric Identity Management. *Proceedings of AusCERT*, Gold Coast, May 2005.

Kirk, J., & Miller, M. L. (1986). *Reliability and validity in qualitative research*. Beverly Hills: Sage Publications.

Kitaw, Y. (2006, November). E-Government in @frica: Prospects, challenges and practices (Master's thesis). Available from <http://hdl.handle.net/1850/6274>

- Kumar, V., Mukerji, B., Irfan, B. and Ajax, P. (2007) Factors for Successful e-Government Adoption: A Conceptual Framework. *The Electronic Journal of e-Government*, 5, 1, 63-77
- Landau, S., & Mulligan, D. K. (March 01, 2008). I'm Pc01002/SpringPeeper/ED288l.6; Who are you?. *Ieee Security and Privacy*, 6, 2, 13-15.
- Leary, M. R. (2001). *Introduction to behavioral research methods*. Boston: Allyn and Bacon.
- Leedy, P. D., & Ormrod, J. E. (2005). *Practical research: Planning and design*. Upper Saddle River, N.J: Prentice Hall.
- Lé'cué', Freddy, Silva, Eduardo, & Ferreira Pires, Luis. (2008). *A Framework for Dynamic Web Services Composition*. Springer-Birkhauser.
- Lewis, K. D., & Lewis, J. E. (2009). Web Single Sign-On Authentication using SAML. *IJCSI International Journal of Computer Science Issues*, Vol. 2, 2009 , 41-48.
- [LibertyProtSchema] Cantor, Scott, Kemp, John, eds. "Liberty ID-FF Protocols and Schema Specification," Version 1.2-errata-v3.0, Liberty Alliance Project (14 December 2004).
<http://www.projectliberty.org/specs>
- [LibertyIDWSFOverview] Tourzan, Jonathan, Koga, Yuzo, eds. "Liberty ID-WSF Web Services Framework Overview," Version 2.0, Liberty Alliance Project (30 July, 2006).
<http://www.projectliberty.org/specs>
- [LibertyIDPPGuide] Kellomäki, Sampo, Lockhart, Rob, eds. "Liberty ID-SIS Personal Profile Service Implementation Guidelines," Version 1.1, Liberty Alliance Project (29 September, 2005).
<http://www.projectliberty.org/specs>
- Lips, M., Taylor, J. A., & Economic and Social Research Council (Great Britain). (2007). *Personal identification and identity management in new modes of e-government*. Swindon: Economic & Social Research Council.
- Maler, E., & Reed, D. (March 01, 2008). The venn of identity: Options and issues in federated identity management. *Ieee Security and Privacy*, 6, 2, 16-23.
- Marshall, C., & Rossman, G. B. (1989). *Designing qualitative research*. Newbury Park, Calif: Sage.

- Mason, J. (1996). *Qualitative researching*. London: Sage.
- McKenzie, R., Crompton, M., & Wallis, C. (March 01, 2008). Use cases for identity management in e-government. *Ieee Security and Privacy*, 6, 2, 51-57.
- McNeill, P., & Chapman, S. (2005). *Research methods*. London: Routledge.
- Merriam, S. B. (January 01, 1995). What Can You Tell from an N of 1?: Issues of Validity and Reliability in Qualitative Research. *Paace Journal of Lifelong Learning*, 4, 51-60.
- Minges M., Gray V. and Tayob M. (February 2007). The Fifth Pillar: Republic of Mauritius ICT Case Study. *ICT 2007*.
- Moser, C. A., & Kalton, G. (1972). *Survey methods in social investigation*. New York: Basic Books.
- Myers, M. D. (2009). *Qualitative research in business & management*. Los Angeles: Sage.
- Neuman, W. L. (2000). *Social research methods: Qualitative and quantitative approaches*. Boston: Allyn and Bacon.
- New Zeland, “e-Government Interoperability Framework” (NZ e-GIF), February 2008. <http://www.e.govt.nz/standards/e-gif/e-gif-v-3-3/e-gif-v-3-3-complete.pdf>
- Nicholls, D. (2009). Qualitative research: part one -- philosophies. *International Journal of Therapy & Rehabilitation*, 16(10), 526-533.
- Olsen, T., & Mahler, T. (2007). *Privacy & identity management: Data protection issues in relation to networked organisations utilizing identity management systems*. Oslo: Senter for rettsinformatikk.
- ORACLE (2011). Oracle Enterprise Manager Cloud Control Extensibility Programmer's Guide, 12c Release 1 (12.1.0.1). Oracle® Enterprise Manager.
- [OASIS-sstc-saml-tech-overview-2.0] Ragouzis, Hughes, Philpott, Maler, Madsen, Scavo, eds.”Security Assertion Markup Language (SAML),” Version 2.0, Technical Overview, Committee Draft 02 (25 March 2008)
- Organisation de coopération et de développement économiques. (2005). *OECD e-government studies: Mexico*. Paris: Organisation for Economic Co-operation and Development.

- Otjacques, B., Hitzelberger, P., & Feltz, F. (January 01, 2007). Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing. *Journal of Management Information Systems*, 23, 4, 29-51.
- Paci, F., Ferrini, R., Musci, A., Steuer, J. K., & Bertino, E. (July 10, 2009). An interoperable approach to multifactor identity verification. *Computer*, 42, 5, 50-57.
- Papazoglou, M. (2008). *Web services: Principles and technology*. Harlow, England: Pearson/Prentice Hall.
- Patton, M. Q., & Patton, M. Q. (1990). *Qualitative evaluation and research methods*. Newbury Park, Calif: Sage Publications.
- Romansky, R., EG&DP-2006, & International Workshop on e-Government and Data Protection. (2006). *Proceedings of the 2nd International Workshop on e-Government and Data Protection, (EG&DP-2006), 22 September 2006, Varna - St. St. Constantine and Elena Resort, Bulgaria*. Sofia.
- Rowley, J. (January 01, 2002). Using Case Studies in Research. *Management Research News : Mrn*, 25, 16-27.
- Saldana, J. (2011). *Fundamentals of qualitative research*. New York: Oxford University Press.
- [SAMLProf] S. Cantor et al, "Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS SSTC (March 2005), <http://docs.oasisopen.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>.
- Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students*. New York: Prentice Hall.
- Shvaiko, P., Villafiorita, A., Zorer, A., Chemane, L., Fumo, T., & Hinkkanen, J. (January 01, 2009). eGIF4M: eGovernment Interoperability Framework for Mozambique. *Lecture Notes in Computer Science*, 5693, 328-340.
- Singh, Inderjeet, Brydon, Sean, Murray, Greg, Ramachandran, Vijay, & Violleau, Thierry. (2009). *Designing Web Services With the J2ee 1.4 Platform: Jax-rpc, Soap, and Xml Technologies*. Prentice Hall.
- Strauss, A. L., & Corbin, J. M. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Newbury Park, Calif: Sage Publications.

The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers. (2009). Paris: OECD.

Thomas, D. (January 01, 2007). A general inductive approach for analyzing qualitative evaluation data. *Educational Administration Abstracts*, 42, 1.)

Trochim, W. M. K. (2008). *Research methods knowledge base*. Cincinnati: Atomic Dog.

United Kingdom, “E-Government Interoperability Framework” (UK e-GIF) Version 6.1, March 2005, [http://www.govtalk.gov.uk/documents/eGIF%20v6_1\(1\).pdf](http://www.govtalk.gov.uk/documents/eGIF%20v6_1(1).pdf)

United Nations. (2007). *E-strategies: National Information and Communication Infrastructure (NICI): best practices and lessons learnt*. Addis Ababa: Economic Commission for Africa.

United Nations Development Programme (2007). *e-Government Interoperability: A Review of Government Interoperability Frameworks in Selected Countries*. Bangkok, Thailand.

United Nations., & United Nations. (2010). *United Nations e-government survey: 2010*. New York: United Nations.

VPN Consortium (2008) VPN Technologies: Definitions and Requirements. July 2008. Accessed 26 August 2011 from <http://www.vpnc.org/vpn-technologies.html>

W3C and Dardailler D. (2011). *W3C Web Services Package* (PAS Explanatory Report). Retrieved September 21, 2011, from <http://www.w3.org/2010/08/ws-pas.html>

Whitman, M. E., & Mattord, H. J. (2009). *Principles of information security*. Boston, Mass: Thomson Course Technology.

Windley, Phillip J. (2005). *Digital Identity*. Sebastopol, CA: O'Reilly.

Winograd, T., Kent, K., Singhal, A., & National Institute of Standards and Technology (U.S.). (2007). *Guide to secure Web services: Recommendations of the National Institute of Standards and Technology*. Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology.

Yu, Q., Liu, X., Bouguettaya, A., & Medjahed, B. (January 01, 2008). Deploying and managing Web services: issues, solutions, and directions. *The Vldb Journal*, 17, 3, 537-572.

Zikmund, W. G. (2000). *Business research methods*. Fort Worth: Dryden.

Appendix A1

ELECTRONIC IDENTITY MANAGEMENT QUESTIONNAIRE

The questionnaire aims at understanding citizens' perception on electronic identity management to be implemented in Kenya government.

PART A: BIODATA

Gender

☐ Male

☐ Female

Age Group

☐ 16-25

☐ 26-35

☐ 36-45

☐ Over 45

PART B: PLEASE ANSWER ALL QUESTIONS PROVIDED BELOW.

1. I will reveal my identity data and other personal information to be shared across government institutions.

☐ Strongly disagree

☐ Disagree

☐ Agree

☐ Strongly agree

2. I will reveal my identity data and other personal information to be shared between government and businesses.

☐ Strongly disagree

☐ Disagree

☐ Agree

☐ Strongly agree

3. I will have little control over my data but will rely on the authorities to manage it.

☐ Strongly disagree

☐ Disagree

☐ Agree

☐ Strongly agree

4. Electronic identity management authorities will prevent unauthorized access to my identity and personal information.

☐ Strongly disagree ☐ Disagree ☐ Agree ☐ Strongly agree

5. There is a need to exchange an individual identity data across different government agencies and institutions.

☐ Strongly disagree ☐ Disagree ☐ Agree ☐ Strongly agree

6. The electronic identity management system will not be technically secure.

☐ Strongly disagree ☐ Disagree ☐ Agree ☐ Strongly agree

7. Exchange of identity data will be monitored by competent authorities.

☐ Strongly disagree ☐ Disagree ☐ Agree ☐ Strongly agree

8. An individual interest will be represented in deciding how their identity data is exchanged.

☐ Strongly disagree ☐ Disagree ☐ Agree ☐ Strongly agree

9. An appropriate legal environment exists to regulate how an individual's electronic identity data will be exchanged

☐ Strongly disagree ☐ Disagree ☐ Agree ☐ Strongly agree