South African Egov: Secure E-Services

Innocentia Z, DLAMINI[1], Sipho J. NGOBENI [2], Murimo B. MUTANGA[3]
[1,2]*CSIR-DPSS (CCIW), P O Box 395, Pretoria, 0001, RSA*
Tel: +2712 841 4410[1]*/2678*[2]*, Fax: + 2712 841 4057,*
[1]*innozie@gmail.com*, [2]*sngobeni@csir.co.za*,
[3]*University of Zululand, Department of Computer Science, KwaDlangezwa, 3886, RSA*
[3]*Tel: +2735 902 6706, Fax: + 2735* 902 6750,
[3]*bethelmutanga@gmail.com*

Abstract: Electronic government and e-services development in South Africa is moving at a snail-pace but has potential to improve. Nothing much has been done regarding the implementation of e-government applications. There are bits and pieces for different unrelated services, as different departments are yet to be integrated. There is still a lot of work to be done, especially on the security issues of the current used e-government architecture. This paper reviews the current state of SA e-government architecture and then suggests improvements. We also make some recommendations to the security mechanisms of the existing egov architecture. We believe that our contribution will stimulate further research in this area and also increase user confidence.

1. Introduction

Although internet proliferation in South Africa (SA) and the African continent as a whole is growing immensely, accessing government services electronically inSA is still a challenge.

Apart from the very slow progress on the implementation and usage of these government services electronically, some of the requirements that need to be addressed e.g. security (privacy, integrity and confidentiality) are yet to be solved.

Currently, the SA's government departments that sufficiently utilizethe e-services, includes: South African Revenue Service (SARS); Department of Home Affairs (DHA); South African Police Service (SAPS); Department of Justice (DoJ) including National Prosecuting Authority (NPA), Department of Correctional Services (DCS) and Department of Social Development (DSD); South African Defence Force (SADF), and Department of Human settlements (DHS) [1].

The SA's egov consortium and steering committee, includes: Department of Communications (DoC), which is responsible for information infrastructure and security policy; Electronic Communications Security (ComSec) is responsible for securing national and governmental communication mechanisms and infrastructures.

State Information Technology Agency (SITA) on the other side is in charge of egov services delivery and secure implementation. DHA and SARS are regarded as the major departments in utilizing egov services.

The DPSA was mandated to promote the use of Information Technology (IT), Information Management and to improve IT service delivery to the public service within the country. The complete egov road map have four stages, i.e. Connected Government

(cgov), Mobile & Multichannel Government (mgov), Ubiquitous Government (ugov), and Transformed Government (tgov) [2].

This paper reviews the current state of SA egov architecture; extends it and further makes recommendations on what could be done to solve the identified gaps, especially on security framework of the existing egov architecture. We propose a model for securing e-services, derived from the existing SA egov architecture and other architectures that have been proposed and implemented globally. Our model is aimed at bringing trust and confidence to the South African public and international partners.

Nevertheless, the agency that is responsible for secure implementation of egov services in SA, SITA, received the SA cabinet's approval to restructure in to a holding company. One important division in SITA is the SITA e-services. This division has a big responsibility of transforming the way in which government conduct its business. It is also a conduit for the procurement of government IT and related services through its IT Acquisition Centre.

The benefits of restructuring SITA focuses on service delivery, to its base through adherence to the principle as embedded on the IT "House of Values" (details on Figure 1, below). Improved coordination of requirements and interoperability will be one of the major benefits. This will also result in the elimination of duplication and leveraging the buying power of government [3].

The rest of the paper is structured as follows: Section two briefly discusses the objectives of this work, while the description of the technology is given on Section three, in Section five, we explain the current developments, and the results of this work are presented in Section six, Section seven concludes this work and also draws the recommendations on what could be done in order to successful achieve secure egov.

2. Objectives

According to Farelo (2006), the vision of accomplishing egov in SA is to deliver services around life cycle of the citizens which follows a sequence of events, from birth to death.

These services must be accessible to all citizens without any limitations, using various access devices and media [4].The objectives of this work include:

- To investigate current SA egov architecture and find the ways to improve it into a comprehensive secure egov model,
- To analyse security issues on the egov architecture services,
- To draw proper recommendations that will improve security of the egov services, and
- To propose a security improved SA's egov Architecture.

Digital Philippines [5] and Web Measure Model [6] believe that there are five stages of egov. Using their description, South Africa would currently be on their fourth stage; consists of the confidence of the users, constructing secure channels, developing the security and privacy policy.

3. Technology Description

There are several challenges that threaten the success of egov services provisioning. These challenges include lack of regulation and policy in government i.e information governance, information security, standard procedures, information usage and sharing; capacity of the departments of successfully interacting with each other; management of related data for the citizens [3].

According to SITA [3], the main aim of the ICT House of Values (Figure 1), is to reduce ICT costs for the government, improve government's efficiency and effectiveness of e-government service delivery and make it convenient to safely access government services.

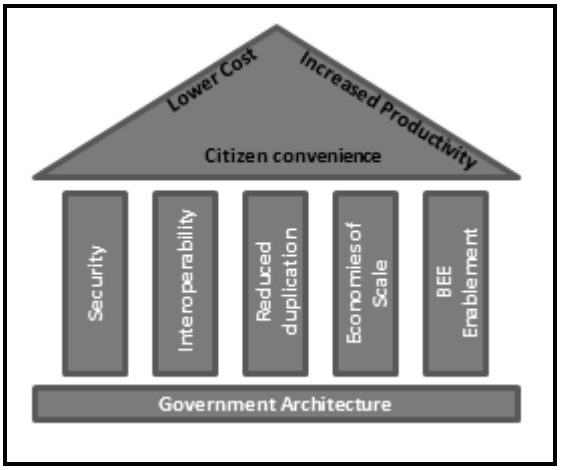

Figure 1: The house of Values

These goals can be achieved when all government processes are viewed explicitly; together with the ICT products; services and projects; which simultaneously:

- Reduce duplication, to ensure that there is reuse and sharing of existing solutions;
- Leverage on Economies of Scale, i.e. using government's buying power to procure ICT products and services for government centrally;
- Make sure that all products and services are secure;
- Ensure that all ICT solutions within government can Integrate and Interoperate;
- Guarantee that government empower the previously disadvantaged by: Providing them with access to economic opportunities; Providing them with a cost-effective way of accessing government services via different channels – anywhere, anytime, anyhow; and Providing them with training and overall skills development to understand and to use the different channels available to them to access government services.

It is therefore imperative to explore the existing models. The following subsection discusses egov in details aligned with SA standards, laws and regulations.

3.1 – What is egov?

Electronic government (egov) or digital government or online government, is the government's utilisation of information communication technology in exchanging both the information and services with its citizens and the corporate world [7].

In simple terms, egov is the use of information technologies together with the new business processes in transforming the government's interaction with its citizens and the corporate world [8].

Moosa and Alsaffar [9] argue that egov is customer-centric, and that it emphasizes the coordinated network building, together with external collaboration and customer services. While egov is often thought of as an online government or Internet-based government, many non-Internet "electronic government" technologies can be used in this context.

Egov is oftenly thought of as "online government" or "Internet-based government," Some non-internet forms include; telephone, fax, SMS text messaging, MMS, wireless

networks and services, Bluetooth, CCTV, tracking systems, RFID, biometric identification, road traffic management and regulatory enforcement, identity cards, smart cards and other NFC applications; polling station technology (where non-online e-voting is being considered), TV and radio-based delivery of government services, email, online community facilities, newsgroups and electronic mailing lists, online chat, and instant messaging technologies.

There are also some technology-specific sub-categories of egov, such as: m-government (mobile government), u-government (ubiquitous government), and g-government (GIS/GPS applications for egov) [7].

These scenarios are likely to result in a situation where there is no guarantee of privacy and security in the use of egov services. On the other hand, the governments have much interest in developing and sustaining the trust of the public (e.g. the DHA must ensure that private information preserved in this department will not leak).

The following subsection discusses the SA egov policy.

3.2 South African Egov policy

The current draft of the cybersecurity policy outlines the mission and vision of the South African government with regards to electronic service delivery, challenges and mechanisms of effective service delivery based on citizens' life expectations/events and the necessary institutional framework to realize egov [9].

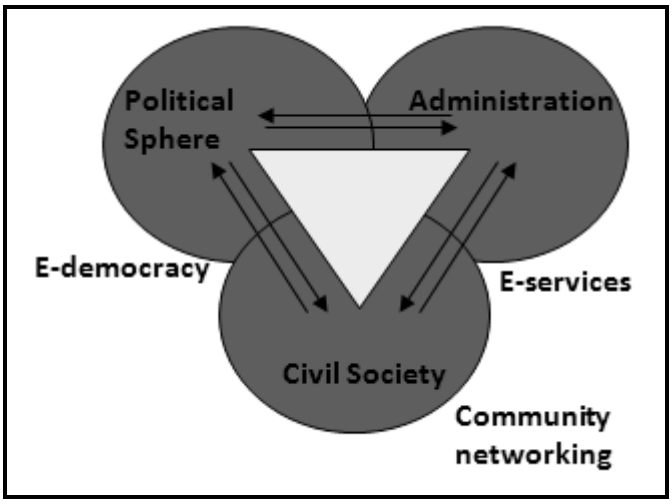

Figure 2: A model for egov

The egov policy has been a draft since 2001till this day [13]. Lack of policies, standards, laws, regulations etc, leads to slow progress of the egov services in SA, which if included on the egov model, and that this point out the SA egov model from other egov models [14].

The government agency, SITA, has a major responsibility of transforming the way in which government conduct its business and also be the single channel for the procurement of government IT and related services through its Information Technology Acquisition Centre [3]. Grönlund (2005) believes that there are three key role players (or spheres) on the egov process (Figure 2) [15].

The political sphere requires e-democracy, e-voting, e-advertising, etc. the administration on the other side involves e-service and community society. If one sphere does not perform its duties, then the success of egov would be adversely affected. The

continuous support of each other is crucial [16]. The following section discusses the current egov architecture and further suggests ways in which its security mechanisms could be improved.

4. Developments

The development of the government portal is viewed as the key component of the egov programme [13]. The portal is meant to offer a general information resource on government activities, all the national Programme of Action together with the specific information about different government services structured according to the life cycle of the citizens.

The portal is currently being enhanced to incorporate services from all the three spheres of SA government (Local, Provincial and National government) and is being translated to all eleven South African official languages [4]. However, the more the usage rate increases, the higher the security risks.

This development could potentially lead to lack of privacy for citizens as their government obtains more and more information about them. In the worse case scenario, with so much information being passed electronically between government and civilians, a totalitarian-like system could develop. When the government has easy access to countless information on its citizens, personal privacy is lost [10] and [11]. It is therefore imperative to review the SA egov architecture.

The architecture for securing the e-services is proposed on the following section. In Figure 3, the SA egov Architecture is presented.

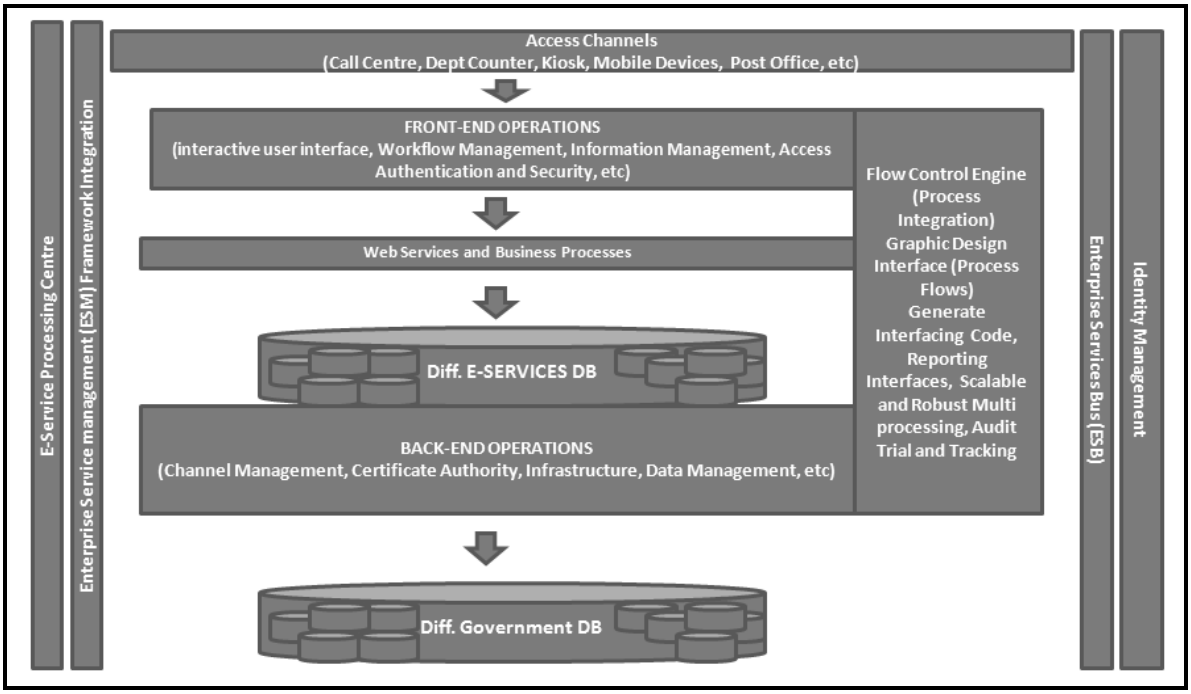

Figure 3:The SA egov Architecture

The architecture is composed of the e-service processing centre; Enterprise Service Management (ESM) Framework integration; Identity Management; and Enterprise Service Bus (ESB). All these componentsare served as the continuous systems that need to be sustained on an up and ongoing state, with no vulnerability or failure.

The architecture consists of four layers, namely: the Access layer, which defines all the places, gadgets and devices that can be used to access e-services; the Front-end Operations layer, which includes user interface, the management of the workflow and the security of access, which is basically an interactive interface between the user and the egov; the Web Services and Business Processes layer, which serves as a mediating layer between the technical- back-end operations and the front end operations.

Before this layer can interact with the back end layer, every necessary details need to be stored in the e-service database for different services provided on the egov (e.g. grant, birth certificates, marriage certificates, etc). The last layer is the Back-end Operations layer which consists of the technical operations (e.g. Channel Management, Certificate Authority, Infrastructure, Data Management, etc) which stores their data in the different departmental databases.

In order for this architecture to be secure enough, security features need to be added on the model and the integration of the departmental databases needs to be taken into consideration in order to avoid security attacks [17]. On the following section, the components that require security enhancements are discussed further.

5. Results

In figure 4 below we present the proposed egov architecture, which is an enhancement of the current egov architecture given in Figure 3

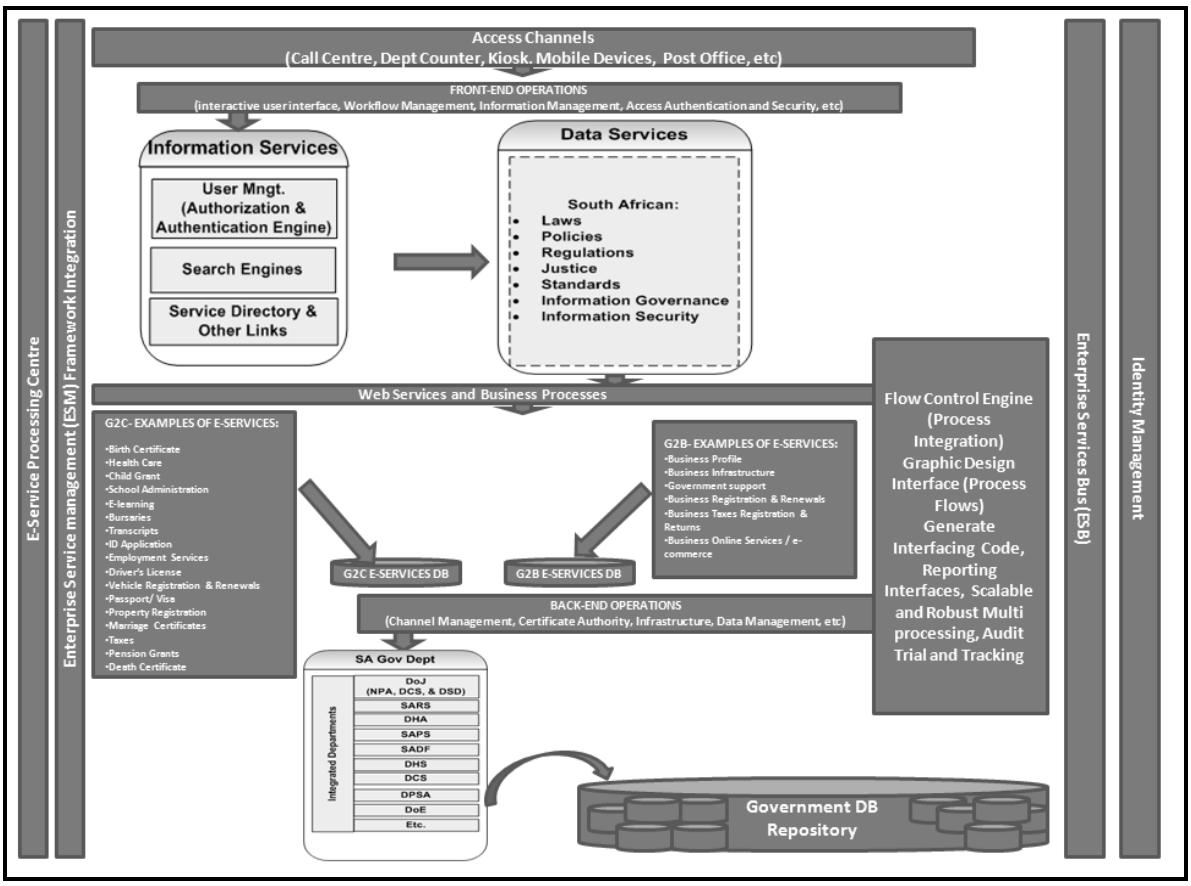

Figure 4: The Proposed Secure SA Egov Architecture

Just after the Front-end layer, there is a need to add the country's information services which include user management (e.g. authorization & authentication engine), search

engines, service directory and other links, some of these services may already have been included of the Front-end layer, but it is significant that they are made.

Furthermore, there should be data services which include South African: laws, policies, regulations, justice, tax system, fees, fines, loans, grants, addresses, individual updates, etc, which specifies the country's procedure when needs to alter with electronic data services, before this data is passed on via Web services on different business processes.

Web services and Business processes layer should report to either G2C or G2B or any other egov model which in turn is associated with its own database; and lastly the Back-end operations must search through the integrated cluster of SA government department's which leads to the specific department's database repository.

There is still a need for integration of different departments in order to properly share the services in a proper manner. The formulation of policies and standards is also important in order to see the successful egov in South Africa [18]. The following subsection summarise the business benefits of the improved model.

6. Business Benefits

More security measure needs to be taken into consideration in future as more applications and services are made available to the public.

Egov is suppose to be an ongoing process, and for it to be easily sustained, proper frameworks and structure should be in place and reviews from time to time are required to improve it; also the feedback from the users may also make difference on its enhancements.

Secure egov is the most convenient and cost-effective for the users of the e-services provided by the government. It provides easy access to mainly all the recent available than going around each department in person.

It is not easy to convince the users into using the technological services, as they come with lots of vulnerabilities. It is therefore significant to present the reliable and trustworthy system in order to buy their trust and to build more confidence on the use of the e-services.

7. Conclusions

Egov use of services is growing rapidly all over the world; and so are the security and privacy concerns. This therefore requires proper considerations especially on security issues of e-services from time to time as new threats, viruses or attacks are generated everyday. Adequate trainings and awareness programmes on secure egov will make it possible to operate it at social level of the government.

This paper reviewed the security and privacy matters of the current egov architecture and propose security improved SA egov architecture. Before the implementation of the egov goes any further, we feel that it will be better if the publication of the standards, regulations and policies for cybersecurity and use of digital resources nationally is taken seriously, executed and implemented properly, and further updated more often.

References

[1] Department of Public Service Administration, available online from: http://www.dpsa.gov.za/, accessed on the: 23 April 2010

[2] The Working Group on Egov in the Developing World, 2002, Roadmap for Egov in the Developing World, 10 Questions Egov Leaders Should Ask Themselves.

[3] Sita Strategy, (March 2010), available online from: http://www.google.co.za/#hl=en&q=sita+e+government+2010&meta=&aq=f&aqi=&aql=&oq=&gs_rfai=&fp=e0435f80f5e44ad9, accessed on: 21 April 2010

[4] Farelo, M and Morris, C., 2006, The Status of Egov in South Africa , pp 1 – 12, available online from: http://researchspace.csir.co.za/dspace/bitstream/10204/966/1/Farelo_2006_D.pdf, accessed on the: 24 April 2010

[5] Digital Philippines, Appendix I-UN-ASPA Five Stages of Egov, available online from: http://www.aijc.com.ph/PCCF/observatory/pfd%20files/directory/UN-ASPA%205%20Stages%20of%20Egov.pdf, accessed on the: 24 April 2010.

[6] Web measure model: stages of egov evolution, United Nations Global Egov Readiness Report 2005, p. 16, (2005), available online from: http://www.access2democracy.org/papers/web-measure-model-stages-egov-evolution, accessed on the: 23 April 2010

[7] Wikipedia, egov, http://en.wikipedia.org/wiki/Egov, accessed on the: 19 April 2010.

[8] Ryan, O. Building the Infrastructure for egov, available online from: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan004277.pdf, accessed on the: 23 April 2010

[9] Moosa, A. and Alsaffar, E.M., 2008, Proposing a hybrid-intelligent framework to secure egov web applications, available online from: http://delivery.acm.org/10.1145/1510000/1509109/p52-moosa.pdf?key1=1509109&key2=8279471721&coll=GUIDE&dl=GUIDE&CFID=86971269&CFTOKEN=10481693 , accessed on: 19 April 2010.

[10] Singel, R., 2007, Analysis: New Law Gives Government Six Months to Turn Internet and Phone Systems into Permanent Spying Architecture, available online from: Wired. http://blog.wired.com/27bstroke6/2007/08/analysis-new-la.html. Accessed on: 19 April 2010. .

[11] Lyman, J., 2006, AT&T Sued for Role in Aiding US Government Surveillance, TechNewsWorld, available online from: http://www.technewsworld.com/story/48629.html?wlc=1235202183. Accessed on: 19 April 2010.

[12] Presidential National Commission on Information Society & Development, Towards An Inclusive Information Society for South Africa, A Country Report to Government,

[13] Department of Public Service Administration, "South African Egov Policy Framework", 2005.

[14] Department of Home Affairs, available online from: http://www.home-affairs.gov.za/projects.asp, accessed on the: 23 April 2010

[15] Grönlund, Å. 2005. What's in a field—exploring the egovernment domain, Paper read at the 38th Hawaii International Conference on System Sciences (HICSS), 2005, Hawaii.

[16] Department of Government Communication and Information System, available online from: http://www.gcis.gov.za/mpcc/index.html, accessed on the: 25 April 2010

[17] Robert, A.D. and Daniel, C., 2008, The Information Technology and Innovation Foundation, Digital Quality of Life, pp. 137–145

[18] Unknown, 2009, Electronic Surveillance- Congress Grants Telecommunications Companies Retroactive Immunity From Civil Suit for Complying with NSA Terrorist Surveillance Program, Harvard Law Review, available online from: http://proquest.umi.com.proxy.cityu.edu/pqdweb?index=15&did=1647275451&SrchMode=1&sid=6&Fmt=2&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1267543120&clientId=8931. Accessed on the: 01 March 2010