Cloud Based Citizen Identity Management Architecture Towards Seamless e-Government: The Case of Ethiopia

Ebisa Asfaw
HiLCoE, Computer Science Programme, Ethiopia
Meles Zenawi Leadership Academy
myhilcoegroup@yahoo.com

Mesfin Belachew
HiLCoE, Ethiopia
Ministry of Communication and Information Technology
mesfinbelachew@mcit.gov.et

Abstract

Identity is the new internet edge for re-engineering security thinking in today's technology realities. Today's web based service is expected to provide efficient, stable, reliable, and on demand services. In recent years, the introduction of e-Government and service oriented architecture held out the promise of web based service. However, in practice, there remain significant barriers in identity management and service integration. Attempts to enable cross-government efficiencies and service improvements for citizens have often been met with mistrust and suspicion by citizens and service consumers. In this paper we have identified the core issues hindering digital identity management for service integration in Ethiopian e-Government case, and developed an architecture that can solve the problem. We proposed cloud based identity as a service architecture, which solves digital identity management problems while addressing the relevant security and privacy concerns. In this architecture, the common cloud computing models (Software as a Service, Platform as a Service, and Infrastructure as a Service) are adopted to form identity as a service model. This service model is identified as a central identity provider including directory, federated, identity creation, authentication, and authorization. This reduces operation cost, increases government efficiency and citizen service, and simplifies identity management and maintenance effort. We have identified different identity authentication tools including Single-Sign-On, Identity Federation, National ID, Biometric Data, and Tokens.

Keywords: Cloud Computing; Citizen Identity Management; Identity Architecture; Seamless e-Government

1. Introduction

The Internet provides ample of merits for agencies to upgrade their e-Service efficiencies. Today service components are providing web-based services such as banking, shopping, and administrative services that are accessible anytime and anywhere. This is cost saving for the e-Services components. This also enables the agencies to deliver value-added services.

Every user must be authenticated and authorized before the user can get any service. Agencies require an initial registration procedure in which the user is asked to provide personal information such as name and address to issue an account. To protect users' personal information, agencies require every user to have credentials. Users must be authenticated and authorized with their credentials prior to access to any web-based services.

Each service provider issues a digital identity for each user. The user must be identified and authenticated with his/her security credentials such as a password. This establishes trust requirements between the user and the service provider [1]. This approach does require a service provider that has an identity management system to handle the identity lifecycle such as creation, management, usage, and decommissioning [2].

Efforts are made by e-Government initiatives to improve the internal efficiencies within the government agencies, and digital access to government services by citizens. SOA (Service Oriented Architecture) and many government portal applications were in place by governments to build e-Government infrastructures and services.

But in practice, there are limitations in ensuring e-government efficiency, citizen authentication and authorization for resources in a trustworthy manner. This is partly due to lack of citizen identification and identity management. In this paper we have examined and come up with solutions for the following research questions: (1) How identity data is stored for Ethiopian citizens? (2) What is the level of authentication for Ethiopian citizens to get access to web based e-Government transactions? (3) How can the identity of citizens be easily traceable anytime and anywhere in Ethiopia?

To survey and come up with the design solution, we used purposive sampling. The survey techniques mainly employed are questionnaire, document analysis, expert interview, and observation.

Purposive Sampling technique is employed to select the organizations and the research participants under the study. For this study, four ministry level organizations, four agencies, and three woredas in Addis Ababa are purposely selected. Two participants are selected to participate on the interview and survey questionnaire from each agency which is a total of 22, from which 16 participated.

For fact-finding, qualitative research approach followed by inductive reasoning technique is used. This is to get insight views of the participants. Intensive analysis of documents and literature are made and conclusion is drawn.

Design Science approach is employed for the system architecture design. The general system architecture, which is a common 3-tier architecture (data storage, application logic and presentation tier) is used. At the data center, a simplified virtual cloud architecture addressing the security issues at each abstraction layer is used. At the application logic layer, application integration middleware are used to design backend solutions. At presentation layer, tools and technologies like identity federation, web application services, SAML (Security Assertion Markup Language), and other service virtualization frameworks are used.

2. Literature Review

2.1 Citizen Identification System in Some Selected Countries

There are a number of systems and applications as identification tools used in most countries. National ID, SSS (Social Security Number), Driving License, and biometric enabled smart cards [3] are the most common ones. In most cases, identification document is issued to citizens at birth or when they reach a legal age (typically 16 or 18). Non-citizens may be issued such numbers when they enter the country, or when granted a temporary or permanent residence permit. Many countries issue such numbers for a singular purpose, but over time, they become a bona fide national identification number.

The following are typical countries which implemented electronic identity solution.

A driver license is the widely accepted form of identification in Australia. Driver licenses are issued by the States and territories and are the most widely used personal identification documents. A driver license lists a person's full name, date of birth, current address and contains a photograph. It can commonly be used for personal identification for various purposes such as obtaining various government permits and documentation (for example, passport or Tax File Number) as well as for opening bank accounts or applying for credit cards.

The Belgian Personal Identity Card (BELPIC) [4] is a highly secure, easy-to-use, and affordable digital identity system for all citizens to use to file taxes, open bank accounts, and make purchases online. It is based on Oracle WebLogic Server. Citizens can use their e-ID through the Belgian government’s portal that runs on Oracle WebLogic Portal. Oracle Service Bus provides the underlying services bus to back-end platforms across the various government agencies. Belgian citizens can already use the new e-ID card for identification, authentication, and authorization for many public services, including secure online tax form declaration, official document requests,

electronic submission of court case conclusions and other public services.

It is compulsory for all Egyptian citizens of age 16 or above to possess ID card. It is used for opening or closing a bank account, registering at a school or university, registering the number of a mobile or leased line telephone, and interacting with most government agencies, including applying for a driver's license, a passport, any social services, registering to vote, and voting in elections, and registering as a taxpayer. Egyptian ID cards expire after 7 years from the date of issuance.

Finland is spearheading on SOA-driven shared services delivery. The Finnish government was challenged with the need to create a flexible means of issuing and authenticating identities to customers, organizations, and citizens [5]. It also needed to reduce the cost of supporting customers at the point of service and implemented a solution for role-based access control and organizational authentication. The outcome is Katso -a nationwide identity management, authentication, and authorization system. Katso is already used by the Finnish Tax Administration and the Social Insurance Institution. As part of the development of government services, the Katso system will become the de facto authentication and authorization solution for online government services in Finland. The Katso system resides on Oracle WebLogic Server, an open, service-centric application server authentication and Liberty Identity Web Services Framework for Web-based applications.

A compulsory and universal ID system based on personal ID cards has been in place in Greece since World War II. ID cards are issued by the Police and display the holder's signature, standardized face photograph, name and surname, father's name and surname, mother's name and maiden surname, date and place of birth, height, municipality, and the issuing police district. Fields included in previous ID card formats, such as profession, religious, domiciliary address, name and surname of spouse, fingerprint, eye and hair color, and ethnicity were removed permanently as being intrusive of personal data and/or superfluous for the sole purpose of personal identification. In addition to being equivalent to passports within the European Economic Area, Greek ID cards are the principal means of identification of voters during elections since 2005.

Multi-purpose national identity cards, carrying 16 personal details and a unique identification number are issued to all Indian citizens since 2007. Biometric data such as fingerprints and a digital signature are contained in a microchip embedded in the card. On it are details of the holder's date and place of birth and a unique 16-digit National Identification Number. The card has a code embedded, through which all the details on the card are accessible.

The challenge facing the Italian Ministry of the Interior was to develop a national identity card. The solution needed to offer a greater degree of security and availability than the previous methods of identification [6]. The solution, called the Carta d'Identità Elettronica (CIE), currently supports, integrates, certifies, and tracks more than 70 million national identity cards. To obtain the CIE, Italian residents in the municipalities simply provide identity information that is checked against a central infrastructure at the Ministry of the Interior, which authenticates the information, generates a signature and digital certification, and then the municipality produces the actual e-ID card. Oracle WebLogic Server supports the CIE infrastructure. The Italian Ministry of the Interior is able to identify and authenticate all citizens on the Web using digital certificates.

In Malaysia, the MyKad is the compulsory identity document for Malaysian citizens aged 12 and above. Introduced by the National Registration Department of Malaysia on 5 September 2001, Malaysia became the first country in the world to use an identification card that incorporates both photo identification and fingerprint biometric data on an in-built computer chip embedded in a piece of plastic [7]. All newborn babies are issued with a MyKid and it will later be upgraded to a MyKad on the 12th birthday. The MyKad must be replaced when a person reaches 18

years old, as it is a requirement that the photograph must be up to date. A record of all Malaysian cardholders is kept by the National Registration Department of Malaysia, which operates the MyKad system [3].

Nigeria first introduced a National Identity Card in 2005. The country is now in the process of introducing a new biometric ID card complete with a Smartcard and other security features. The National Identity Management Commission (NIMC) [8] is the Federal Government Agency responsible for the issuance of these new cards as well as the management of the new National Identity Database. The Federal Government of Nigeria announced in April 2013 that after the next General Election in 2015, all subsequent elections will require that voters will only be eligible to vote provided that they possess a NIMC-issued Identity Card. The Central Bank of Nigeria is also looking into instructing banks to request for a National Identity Number (NIN) for any citizen maintaining an account with any of the banks operating in Nigeria.

The United States developed its Social Security Number (SSN) system as a means of spending Social Security benefits. However, due to function creep, the number has become used for other purposes like to open a bank account, obtain a credit card, or drive a car, for instance. For most people, driver's licenses issued by the respective state and territorial governments have become the actual identity cards, and are used for many identification purposes, such as when opening bank accounts and boarding planes. Individuals who do not drive are able to obtain an identification card with the same functionality. In addition, many schools issue student and teacher ID cards. The passport card can also be used as a valid proof of citizenship and proof of identity both inside and outside the United States

From the above country surveys, we can generalize the following best practices for this study:

Identity documents in these countries, besides identification, help to get derived identity documents and other government services. Katso, as it is identified as a model of standard adoption for large-scale government infrastructure, services around the world, can also be best suited for the Ethiopian case. The Malaysian MyKad is the best identification practice for identifying citizens.

2.2 Citizen Identification System in Ethiopia

In Ethiopia manual ID system given by every Kebele was the only unique identifier tool available to citizens for decades. Latter attempts were made by different institutions toward strengthening citizen's uniqueness. The introduction of finger print by police commission offices was one footstep. Driving License issued to citizens by transport authority is another attempt toward the realization of uniqueness. The better organized citizen unique ID is introduced by Taxpayer Identification Number (TIN) by Federal Custom and Revenue Authority, which is a better integrated system for tax payers. This system is being utilized to uniquely identify individuals and organization taxpayers at national level. Moreover, Private Organizations Employees Social Security Agency (POESSA) is probably the first to inherit TIN as a unique ID to citizens - and this pinpointed the integration of citizen ID in the history of Ethiopia.

An attempt is also made by the research community toward the transformation of citizen ID. The studies on Citizen Identification System that contributed to automatic national ID generator [9], Semantic Knowledge Oriented Electronic Health Record Integration System that contributed to integrated patient ID generator [10], and Federated e-Identity Management across the Gulf Cooperation Council (GCC) [11] that describe the concept of federated e-identity in gaining attention worldwide in light of evolving identity management challenges, are among the major efforts.

However, the current systems have problems dealing with personal information, ensuring user's permission, and resolving multiple identity conflicts. Today, there are more and more inter-service integration solutions through cooperative systems.

2.3 Technologies for Identity Management

Oracle Identity Manager runs on leading Java EE compliant application server platforms [12], including Oracle WebLogic Server, to take advantage of the performance and scalability features inherent in these servers. It also supports application server clustering for increased performance and virtually automatic failover in mission-critical computing environments.

Microsoft is focusing on enhancing Windows Azure AD (Active Directory) over Windows Server AD [13]. As Windows Azure AD is a web service, Microsoft has rapidly deployed new features to it. The Microsoft offering bridges single-sign-on technology from the datacenter to the cloud.

Windows Authentication provides single sign-on for all applications, as well as details of the authenticated user and group membership. The application is no longer required to make authentication decisions, and the same authorization logic applies for applications deployed on the intranet or as a cloud service

Oracle Web Logic Server implemented by countries like Belgium, Finland, and Italy as identity middleware solution, is identified in this work as the best option for the Ethiopian condition, since it supports large scalability, security and easy integration.

3. The Proposed ECIM (Ethiopian Citizen Identity Management) Architecture

Based on the findings so far, we come to the proposed designs for ECIM, called Identity as a Service (IDaaS) Architecture.

IDaaS offers management of identity as a digital entity. IDaaS can be implemented as an application on top of virtual cloud government infrastructure. This service center is proposed to be the legitimate identity authentication center for e-services and electronic transactions.

We have assessed different cloud models and proposed a virtual cloud model as best suited for ECIM architecture. Virtualization is a technique which allows to share single physical instance of an application among multiple agencies or service components as depicted in Figure 1. It does this by assigning a logical name to a physical resource and providing a pointer to that physical resource when demanded.

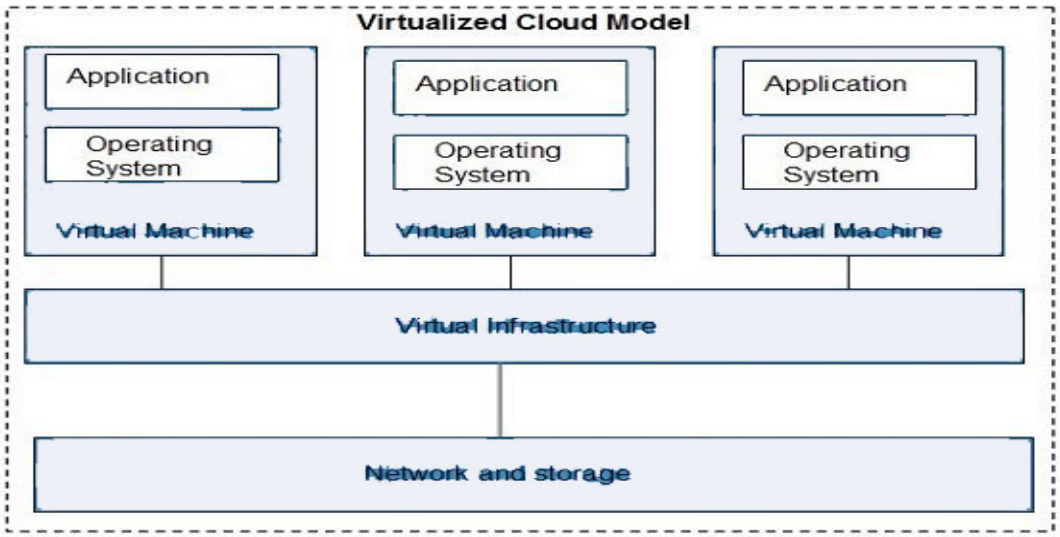

Figure 1: Virtual Cloud Infrastructure model for Identity Management

Creating a virtual machine over existing operating system and hardware is referred to as Hardware Virtualization. This virtual machine is managed by a software or firmware. The architecture can be implemented in Ethiopian e-Government applications as follows. There are government infrastructures, datacenters and applications implemented at the center. That datacenter is already forming central Government Cloud. What we need to extend further is to implement a middleware (virtual machine) with all

its security features. Different operating systems are installed on each instance of virtual machine which are separated by static IP addresses. Then applications (services) from different partners are implemented on logically separated operating systems.

Therefore, identity management is implemented as an application in a similar fashion, which integrates the identity of the same citizen (customer) in different applications.

Figure 2 shows the main form for initial user registration. The user who registered by this form with the basic personal details and stored in the authoritative data source will be available for latter authentication and authorization. Every citizen in the country is required to be registered using the form into a central authoritative data source. Thus, when requesters (service providers) want to give any service to citizens, the citizen must be authenticated and authorized for the required service against this initial personal data. If update is needed about the registered person, the update can be done by mutual agreement between the service provider and the identity provider.

Figure 2: User Initial Registration Form for Ethiopian Citizen Identity Management

The proposed Architecture for ECIM Identity Lifecycle Management

The architecture comprises the process of Identity Creation (Registration), Authentication, Authorization and decommissioning of digital identities of entities for different service and application domains.

Figure 3 shows a simplified Architecture of Identity and access management. In this architecture, a client (user) presents her/his credentials to the service provider (SP) _ECIM. Then ECIM checks the credentials (embedded in digital ID) in its data repository, and if it matches with the credentials that was captured during the initial registration, then the IP successfully authenticates the user. Then, the requester will be authorized to access the resource, which s/he claims from the service provider.

The registration process can be twofold. First the user can register her/his own profile in ECIM using registration form and then the administrator approves the user. Second, the administrator can register the user directly. By the identity management services center, the administrator can also update the user profile and may also decommission a user from the service when the user is no longer needed.

After registration, the user profile is stored in the directory service. Then the access management

component authenticates the user based on the user profile and policy store. Finally, the provisioning service authenticates the user for various resources and applications, based on successful authentication of users.

This architecture is assumed to be built for Ethiopian condition as a single datacenter to provide identity data from one authoritative data source. We have seen the cases of Belgium, Finland, Italy, Malaysia, and Nigeria, in which case one central agency issues and authenticate digital ID for every citizen, from one authoritative data source, for various services. Thus, Ethiopia has to build digital ID issuance, authorization, and management on top of e-Government cloud infrastructure.

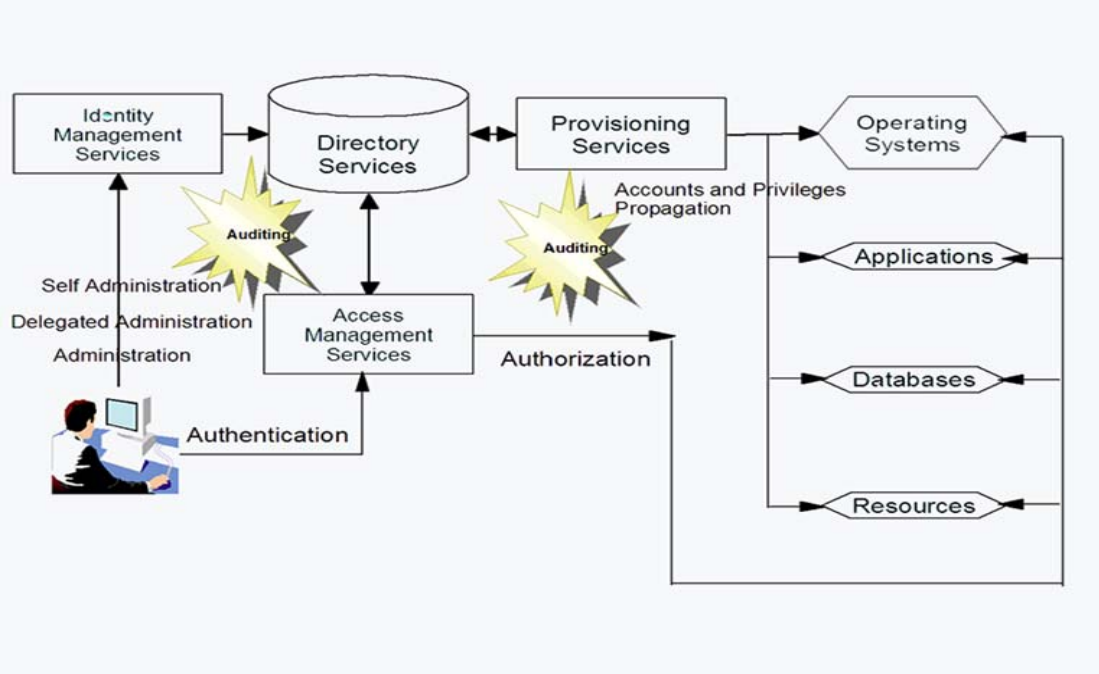

Figure 3: A Simplified Architecture for Identity Management

4. Conclusion and Recommendation

As a result of findings from this study, the following conclusions are drawn.

We identified that personal ID is the principal identity document in Ethiopia. We analyzed that the personal ID document is just given on ordinary card with basic attributes. Our study also shows that no digital identity document processing system is yet in place. Digital Identification/e-ID, or biometric data enabled smart card system is not yet implemented in Ethiopia.

In the current Ethiopian system, citizen identity and identity attributes are not integrated across e-Government services and applications. There are also many legal and policy limitations regarding ID card standards, data repository, and identity management.

In this work, we have assessed citizen identification system and smart card technologies being practiced by many countries. Most of these smart cards are unique, biometric enabled, and multipurpose. Thus, we propose microchip embedded Smart card, like Katso, as in Finland, as identification tool for Ethiopian citizens.

We have identified cloud computing service and deployment models and come to the design that virtual cloud architecture is the best solution for Ethiopian case. IDaaS architecture, the artifact of this work, is proposed for ECIM. We believe virtual cloud computing and service virtualization will dramatically cut cost needed to build the necessary infrastructures.

We propose biometric enabled smart card national ID for security and its versatility reasons. The national ID card will be used as the primary identification

credential within the e-Government services to access resources.

We also recommend that there should be a central authoritative agency for ECIM that is responsible for the identity implementation and administration services. A common standard and policy have to be devised by MCIT, or other designated body, on a set of comprehensive international and/or company specific guidelines for personal identification and management including data storage, secured electronic data exchange, identity attributes, etc.

We also propose the implementation of virtual cloud infrastructure and web-based applications for easy integration and authentication of identity data.

References

[1] Audun Jossang and Jonh Fabre, “Trust Requirements in Identity Management”, Australian Computer Society, Inc., 2005.

[2] Uciel Fagoso-Rodriguez, Maryline Laurent-Maknavicius, and Jose Incera-Dieguez, “Federated Identity Architecture Evaluation”, Instituto Tecnologico Autonomo de Mexico, Mexico.

[3] National identification number, http://en. wikipedia.org/wiki/National identification number, last accessed on March 18, 2014.

[4] Danny De Cock, Christopher Wolf, and Bart Preneel Katholieke, Universiteit Leuven, Department of Electrical Engineering, Kasteelpark Arenberg 10, B-3001 Heverlee-Leuven, Belgium.

[5] Teemu Rissanen, Electronic identity in Finland: ID cards vs. bank IDs, Published online: 6 March 2010, http://link.springer.com /article/10.1007 %2Fs12394-010-0049-8, last accessed Nov 2015.

[6] Ali M. Al-Khouri: Optimizing Identity and Access Management, International Journal of Engineering Research and Applications (IJERA), Vol. 1, Issue 3.

[7] “MSC Malaysia Flagship Applications". http://web.usm.my/aamj/17.1.2012/AAMJ17.1. 4.pdf, Last accessed on March 18, 2014.

[8] "National Identity Management Commission", Nimc.gov.ng, Last accessed on March 18, 2014.

[9] Tewodrose Nigussie, “Citizen Identification System”, Unpublished Master’s Thesis, Addis Ababa University, 2007.

[10] Winta T. Zibello, “Semantic Knowledge Oriented Electronic Health Record Integration System”, Unpublished Master’s Thesis, HiLCoE School of Computer Science & Technology, 2012.

[11] Ali M. Al-Khouri, “Federated E-Identity Management across the Gulf Cooperation Council”, International Journal of Public Information Systems, Vol. 2013

[12] Oracle Identity Management Concepts and Architecture: http://docs.oracle.com/cd/ B14099_19/idmanage.1012/b14084/ concepts.htm, last accessed on April 23, 2014.

[13] http://www.windowsazure.com/enus/solutions/ identity/, Last accessed April 25, 2014.