GLOBAL JOURNAL OF PURE AND APPLIED SCIENCES VOL 16, NO. 2, 2010: 269- 275
COPYRIGHT© BACHUDO SCIENCE CO. LTD PRINTED IN NIGERIA. ISSN 1118-0579
www.globaljournalseries.com; Email: info@globaljournalseries.com

DESIGNING A FRAMEWORK FOR A UNIFIED ELECTRONIC IDENTITY SYSTEM: NIGERIA A CASE STUDY

C. K. AYO

(Received 30, October 2009; Revision Accepted 4, January 2010)

ABSTRACT

The advent of the Internet has popularized online transactions, particularly eCommerce, eGovernment, and ePayment among others. However, identity theft is one of the major problems inhibiting the successful adoption of this medium of business transaction because it is public in nature and devoid of face-to-face (F2F) interaction.

Each platform of business transaction is associated with a unique identification system and presently an individual may be carrying a barrage of ID cards such as: the Driver's License (for driver's identification); the National ID Card (for national identification); the International passport (for International travels); and several payment cards depending on the number of bank accounts an individual operates: Personal, Salary and Business among others.

In this paper, a Unified Identity System is proposed where single electronic identity (eID) is issued that can be used across the various platforms of business transaction. The activity/state diagram of the model is presented, and the means of authentication is based on the Secure Assertion Markup Language (SAML) framework.

KEYWORDS: eIdentity, SAML, eCard, ATM, and Identity Management

INTRODUCTION

Identity Management is a broad administrative area that involves providing a means of identifying individuals in any system such as country, network or enterprise with a view to granting them access to resources within that system (ID, 2008). The Extensible Name Service (XNS) is a standard that is being developed for identity management within and outside an organization.

Tacking an "e" into any business model is no longer a luxury or a novelty but a necessity. It requires granting system access to users, customers, business partners and the supply chain. As organisations create virtual enterprises and create more collaboration with trading partners, there is much demand for an automated process to manage the resources by restricting access to authorized individuals (Mimoso, 2002).

The Security Assertion Markup Language (SAML) is an eXtensible Markup Language (XML)-based framework for communicating user authentication, entitlement and attributes information (OASIS, 2005). SAML enables organizations to make assertions regarding the identity, attributes and entitlements of a subject, particularly human users, to other entities such as other organizations.

SAML is primarily used for Internet Single-Sign-On (SSO). It eliminates the use of multiple authentication credentials, and phishing opportunity by reducing the number of times a user logs on to the Internet.

The operation of SAML revolves around three major actors: the Users, the Identity Provider, and the Service Provider. The service providers are organizations that host numerous services that users need while the identity provider are organizations that maintain the directory of users' identities.

The practical representation of SAML is shown figure 1.

C. K. Ayo, Dept of Computer and Information Sciences, Covenant University, P.M.B 1023, Ota, Ogun State, Nigeria

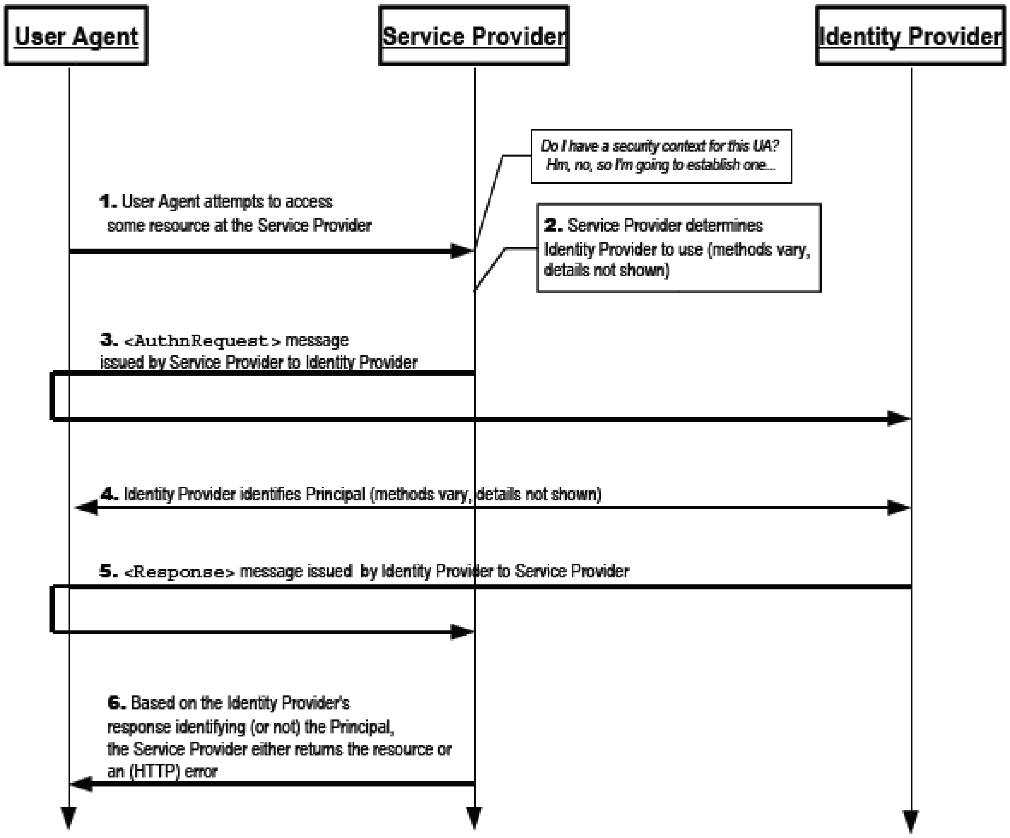
User Agent
Service Provider
Identity Provider
Do I have a security context for this UA? Hm, no, so I'm going to establish one...
1. User Agent attempts to access some resource at the Service Provider
2. Service Provider determines Identity Provider to use (methods vary, details not shown)
3. <AuthnRequest> message issued by Service Provider to Identity Provider
4. Identity Provider identifies Principal (methods vary, details not shown)
5. <Response> message issued by Identity Provider to Service Provider
6. Based on the Identity Provider's response identifying (or not) the Principal, the Service Provider either returns the resource or an (HTTP) error

Figure 1: Overview of Security Assertion Markup Language (SAML)
Source [Copyright © OASIS Open 2005.]

A user attempts to access services offered by a provider (Service Provider), the identity of the user is sought from the identity provider after which access is either granted or denied based on the outcome of the authentication request.

Google Applications offers a SAML-based Single Sign-On service that provides partner companies with full control over authorization and authentication of hosted users account that can access web-based applications like gmail. In this instance, Google acts as the service provider and provides services to users; Google Partners acts as identity providers and control usernames, password and other details needed to identify, authenticate and authorize users for web applications that Google hosts (see figure 2).

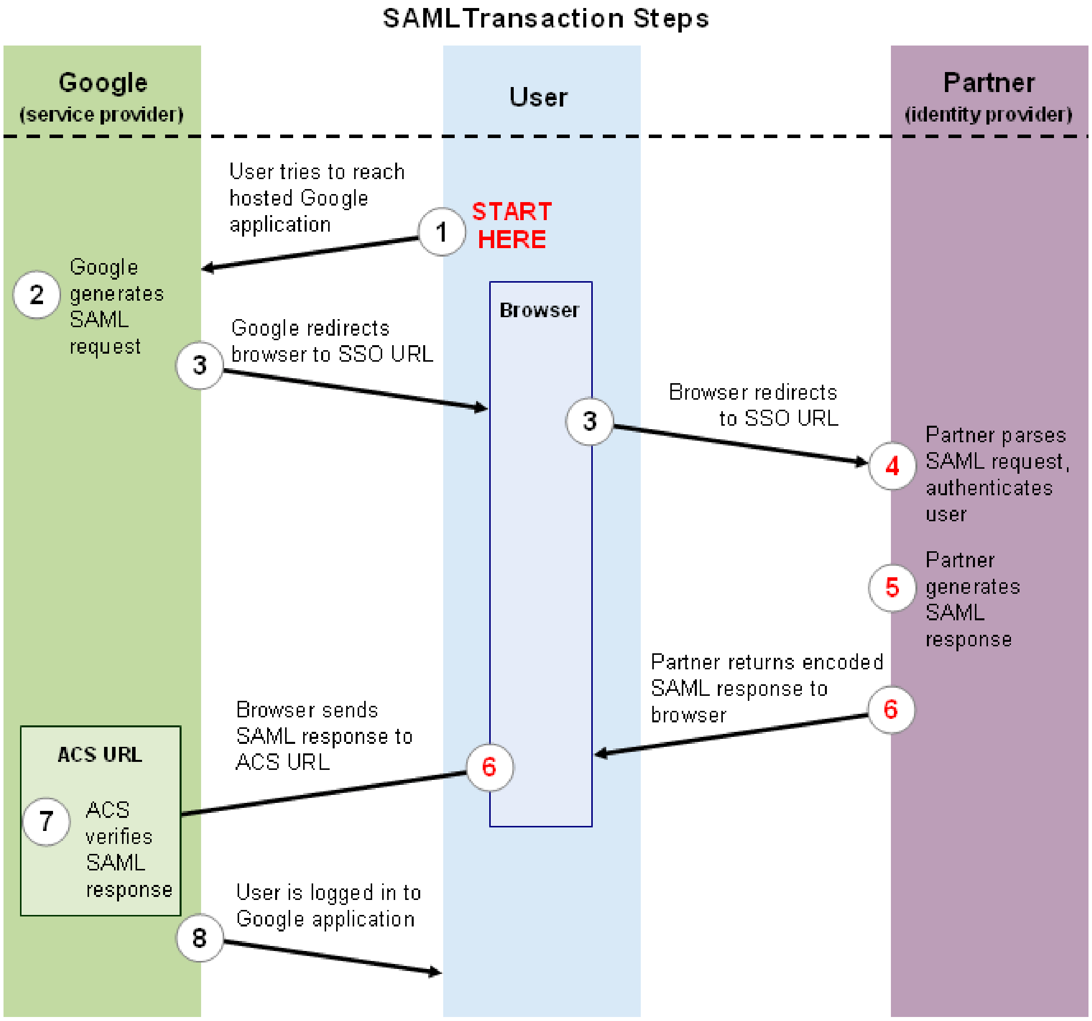
SAMLTransaction Steps
Google
(service provider)
User
Partner
(identity provider)
User tries to reach hosted Google application
1
START HERE
2
Google generates SAML request
Browser
3
Google redirects browser to SSO URL
3
Browser redirects to SSO URL
4
Partner parses SAML request, authenticates user
5
Partner generates SAML response
Partner returns encoded SAML response to browser
6
Browser sends SAML response to ACS URL
6
ACS URL
7
ACS verifies SAML response
8
User is logged in to Google application

Figure 2: SAML Single Sign-On (SSO) Service for Google Apps
Source [http://code.google.com/apis/apps/sso/saml_reference_implementation.html]

The steps are similar to the presentation in figure 1. The user requests for services from the service provider, which in turn seeks clarification on his identity from the identity provider before granting access or otherwise.

Electronic identity has become a major issue in online commerce and public sector organizations. Because of the faceless nature of customers, suppliers and organizations, verifying identities online requires a proof of identity relationship with government entities and not just a third party if it is to be trusted, or at best, a combination of government and the third party, or through public private partnership (PPP).

The problem of identity verification and management will continue to increase in magnitude and importance, thus relying on passwords and asking customers to remember them may neither be sufficient nor efficient. Any system that relies on password is insecure because there are several software tools around that are used to defeat password security (Ayo, 2009).

Similarly, the barrage of cards carried by users can be reduced to one through which access can be granted to all platforms of business transaction (voting, banking, driving, etc.).

eGovernment applications typically require the need for citizens to use a consistent single online electronic identity as against the multiplicity of existing ones that are used for different platforms. Therefore, an eIdentity should be such that offers a consistent and reliable means of identifying online users in some areas of applications such as banks, employers, utility companies, airlines, eGovernment and eBusiness outlets.

In Nigeria, the issue of identity is still a major challenge. There is no acceptable census figure, the previous national ID projects were flawed, and revision/update of voters' registers was marred with irregularities. All these issues would be solved through the proposed eID framework.

Therefore, the objective of this paper is to design a unified electronic identity card that can be used across all platforms of business transactions. The rest of the paper is arranged as follows: section 2 presents a review of related works; section 3 presents the design framework; section 4 presents the operational framework, while the conclusion of the work is presented in section 5.

RELATED WORK

There are a number of identity management initiatives in the world. In Africa, Angola is leading the first national eIdentity project while other countries are following suit, particularly Nigeria. In Europe and America however, Belgium had started her eID roll-out while UK and the

US are fast concluding the legal framework needed for their implementations.

The Italian electronic Identity Card (EIC) is a polycarbonate smart card equipped with microchip and a laser band. It contains both personal and biometric data of citizens. According to the Italian laws, the card serves dual purposes. It can be used as a traditional paper-based ID card on one hand and as an authentication credentials, allowing access to network enabled government services (Arcieri et al, 2009).

There are established laws governing the adoption and operations of eID. The national database or databank contains the personal data of persons, particularly those with established residence and new born babies. Similarly, after death or when an individual establishes the residence outside the countries through naturalization, the data of such persons are deleted from the databank (Arcieri et al, 2009).

There are established security infrastructures already in operation. The Italian (EIC) offers a security backbone that provides all security services. The infrastructure is composed of functional subsystem such as: (i) confidentiality and integrity services, (ii) authorization service (iii) authentication service (iv) access policy management, (v) quality of service monitoring.

Belgium was the first European country that issued electronic identity (eID) card to all its citizens from age 12 and above. Similarly, there are frantic efforts made in Estonia, Austria, Italy and Spain (Danny et al, 2009)

The Belgian eID card is a normal smart card that offers both F2F and electronic features. It contains name, title, nationality, place and date of birth, gender and photograph of the holder. The chip on the card performs digital signatures and key generation. The Belgian eID card model was not integrated with the social security card or the driver's license or the national identity card because of incompatibilities with the legal framework. However, the card can be used for citizen-to-citizen (C2C), citizen-to-business (C2B), and citizen-to-government (C2G) transactions. The major concern with the eID is that there is no privacy enhancing technologies incorporated to it.

The Belgian eID card employs three different 1024-bit RSA private signing keys: one to authenticate holders, another for non-repudiation signatures and the last is to identify the card itself. The eID card is able to complete digital signature with all the three keys. Each of the first two key pairs is accompanied by a certificate that is issued to the citizen. One certificate is used to authenticate the client with secure socket layer (SSL) and the transport layer security (TLS) security; the second binds the non-repudiation key to the card holder.

The new German national ID card preserves all visual identity card functions such as photograph, name, signature etc but incorporates additional security features. It combines both traditional card and electronic features and there are biometrics presentation of photograph and fingerprint (Andreas, 2009).

The benefits the eID card offers include: automated fill-in functions (single-sign-on), quicker age verification, address verification, reliable authentication for social eCommunities as well as access verification among others.

In the German model, there is mutual authentication between the parties. That is, the citizen and the service providers authenticate themselves. The citizens identify themselves with the eID card while the service providers identify themselves with an authorization certificate. The mode of operation of this model is based on the SAML where the eID card holder is the citizen, the eBusiness/eGovernment providers are the service providers.

DESIGN FRAMEWORK

In developing a digital identity model, debates are ongoing about the need for identity laws or principles to guide its operations. Kim Cameron presented the seven laws of identity as the emergent framework for effective identity management in an online world (Ayo, 2009). The proposed framework varies in scope and scale, from the traditional public key infrastructure (PKI) style projects using smart cards with embedded chips to those that include biometrics. A general design is shown in figure 3.

The various attributes of the ID cards in Nigeria under consideration are shown in table 1. The cards include National ID card, Driver's license, Voter's card and ATM card.

Table 1: Attributes of the ID Cards

National ID Card	Driver's License	Voter's Card	ATM Card
▪ Name of the country. ▪ Identity number. ▪ Name. ▪ Surname. ▪ Other Names. ▪ Sex. ▪ Date of birth. ▪ State of origin. ▪ Height. ▪ Signature. ▪ Thumb print. ▪ Address. ▪ Father's Name ▪ Mother's name. ▪ Profession. ▪ Period of validation. ▪ Picture of person	▪ Name of country. ▪ License No. ▪ Class of License. ▪ Picture of person. ▪ Issue date. ▪ Expiry date. ▪ Name of individual. ▪ Address. ▪ Blood group. ▪ Sex. ▪ Date of birth. ▪ Height. ▪ Holder's signature.	▪ Name of country. ▪ Voter's identification number. ▪ Surname. ▪ First name. ▪ Sex. ▪ Age. ▪ Date of birth. ▪ Delimitation/Location ▪ Date of issue. ▪ Picture.	▪ Authorized signature ▪ Name of bank. ▪ Account No. ▪ Instruction on how the card is to be used. ▪ Expiry date. ▪ Name of owner.

To create a unified database for all the cards, it is sufficient to use the union of all attributes of the cards viz: A ∪ B ∪ C ∪ D for the National ID card, Driver's license, Voter's card and ATM card respectively. Therefore, nE = {A ∪ B ∪ C ∪ D} = 24 fields.

In the database design, the system will be able to accommodate several bank accounts. There will be automatic update of the database so that the current changes are incorporated, particularly whenever new bank accounts are created.

The Proposed Unified ID Card.

This is a credit card sized plastic card that contains: ID Number, Name, Gender, State of Origin, Date of Birth, Class of License, Blood Group, Height, Passport and signature. The chip contained on the card will carry both personal information and biometric identities such as any of fingerprints, iris scanning, pattern of blood vessels in the retina or hand, voiceprints, etc. The contents of the chips are verifiable at any terminal.

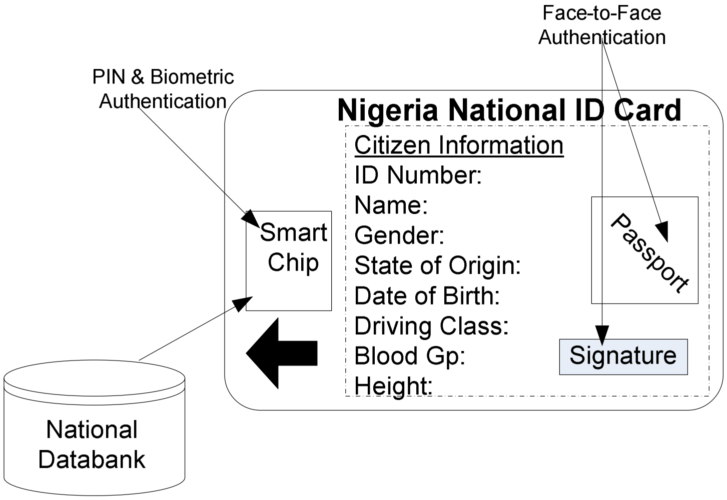

Figure 3: Smartcard-based eIdentity Card

The information contained on the card will serve dual purposes namely F2F identification and electronic authentication at any terminal. For F2F authentication, the name, passport and signature are sufficient, while for electronic authentication the supply of PIN and fingerprint will be at the instance of the terminal, particularly when the card is to be used for voting, banking, etc purposes. It is important to note that for driving offences, or accident, the name, passport, driving class, and blood group are sufficient to handle any situation that may arise.

OPERATIONAL FRAMEWORK

From the design in figure 4, the basic operational codes are V for Voter's ID, D for Driver's ID, N for National ID, and B for banking identification. Upon the entry of valid codes for all transactions except banking, the user's identity is authenticated using both personal identification number (PIN) and fingerprint before granting access, while for banking transactions, the user is expected to enter the code for the particular bank where business is to be transacted. It is after this point that the user is authenticated and access granted.

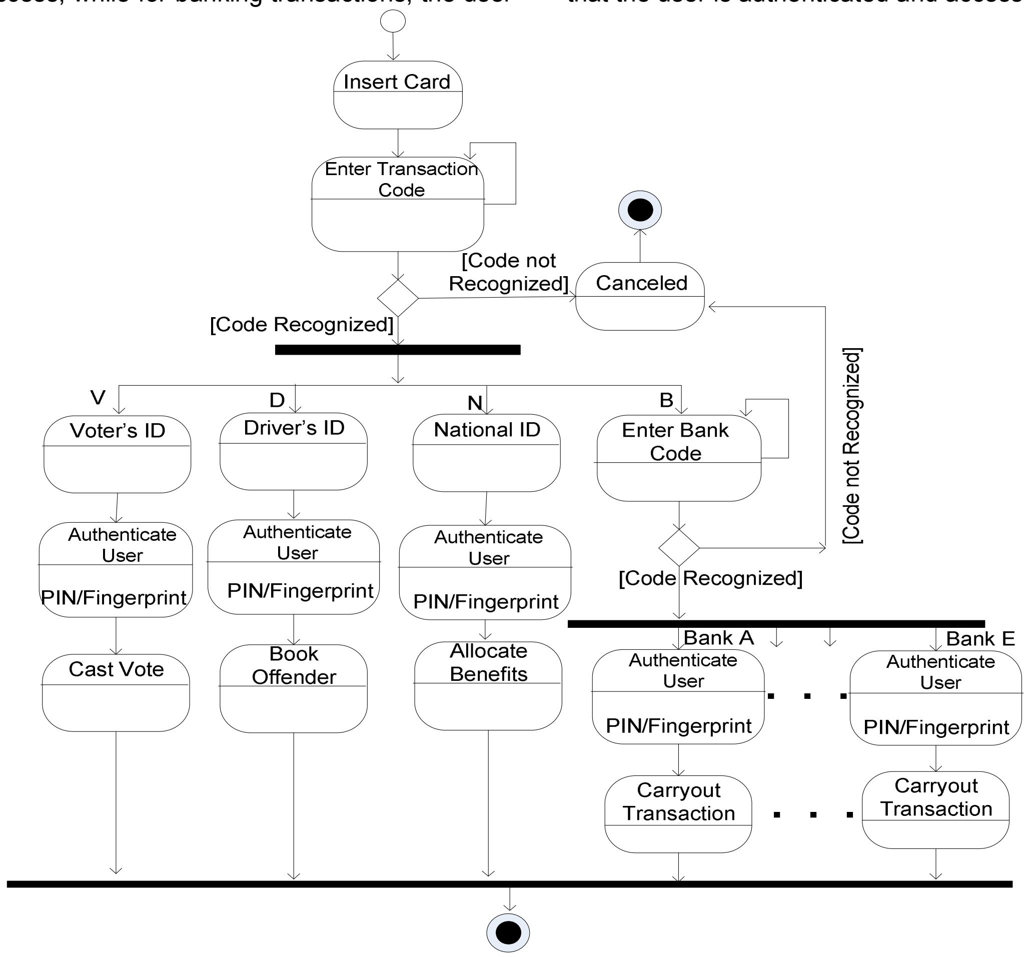

Figure 4: Activity Diagram for a Unified eID System

It is important to note that the design framework can be implemented on the existing ATM platforms with minimal cost. All the available terminals accept ATM cards from different banks, therefore, they are interoperable. However, beyond banking the other medium of identification can adopt this approach. Similarly, the existing ATM keypad has a blank key (button) probably for future development, which can be used for the fingerprint reader (see figure 5).

Therefore, for non banking transactions, particularly voting, driving and national identifications, a navigation system with miniaturised keypad with card reader will be a sufficient platform of operation. The device can be fitted on any patrol van or used as a palmtop and the virtual private network (VPN) provided by the Telecommunications companies – Glo, Zain, MTN, etc.

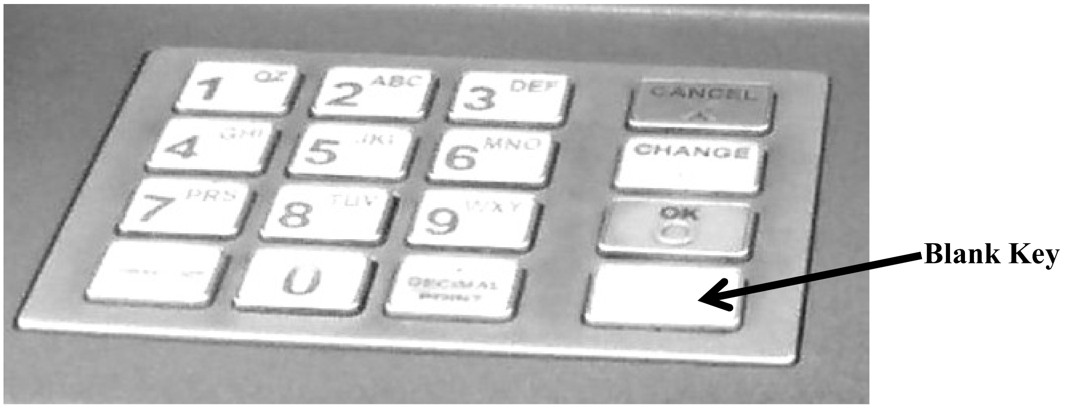

Figure 5: The Existing ATM Keypad

CONCLUSION

This paper has provided a framework for a unified eID card for all platforms of business transactions (Voting, Driving, National identification, and Banking) in Nigeria. Similarly, this framework should serve as a guide to the Federal Government of Nigeria on the proposed biometrics-based National identity card project with a view to evolving a workable identity system and preventing the colossal waste of funds associated with such projects in the past.

The means of authentication is through SAML, which will help a great deal to solve a number of other problems in the country. Presently, e-Payment cards that originated from Nigeria are not accepted internationally on accounts of fraud because the nation had been blacklisted. However, with the unified eID and the associated databank, there is the assurance that the identity of all card carrying Nigerians can be verified by the identity provider and this will help reduce crime rate, particularly identity theft since all users' identity can be ascertained.

Furthermore, the national databank will serve as a repository of all records of citizens. On it, births, deaths are registered and or updated and the revision of voter's list before any election may not be necessary as these records can be updated automatically and reports generated as required. In addition, the security features as demonstrated in the Italian, Belgian and German models are sufficient to guarantee privacy, integrity and non-repudiation of transactions.

Generally, there is reduced cost of producing cards, improved security of transaction and improved level of participation and trust in eCommerce and eGovernment. A single card is issued to every citizen whose identity can easily be verified and access granted as at when needed to whatever transaction.

REFERENCES

Andreas, R., 2009. Technologies for electronic identification, Access date Sept. 2009. Available at:http://www.e-identify df.de/documents/presentations/04-herr-reisen

Ayo, C. K., 2009. Information Systems and technologies, McKAY Educational Series, First Edition, 649p.

Danny, D. C., Christopher, W., and Bart, P. The Belgian Electronic Identity Card (Overview), Access date Sept. 2009. Available at: http://www.cosic.esat.kuleuven.be/publications/article-769.pdf

Franco, A., Mario, C., Andrea, D., Fabio, F., Enrico, N. and Maurizio, T., 2009. The Italian electronic identity card: Overall architecture and IT Infrastructure, Access date Sept. 2009. Available at: http://www.mat.uniroma2.it/~nardelli/publications/CSES-04.pdf

Google Apps APIs, 2009. SAML Single Sign-On (SSO) Service for Google Apps, Access date Sept. 2009. Available at: http://code.google.com/apis/apps/sso/saml_reference_implementation.html
ID Management, 2008.

SearchUnifiedCommunications.com Definitions, Access date Sept. 2009. Available at: http://searchunifiedcommunications.techtarget.com/sDefinition/0,,sid186_gci906307,00.html

Mimoso, M. S., 2002. Identity management a must for the virtual enterpriseAvailable at: http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci822376,00.html

OASIS, 2005. saml-profiles-2.0-os, Access date Sept. 2009. Available ate: http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf