Journal of Physics: Conference Series

PAPER • OPEN ACCESS

A Proposed Unified Digital Id Framework for Access to Electronic Government Services

To cite this article: V. Geteloma *et al* 2019 *J. Phys.: Conf. Ser.* **1378** 042039

A Proposed Unified Digital Id Framework for Access to Electronic Government Services

V. Geteloma [1*], C. K. Ayo [1], and R. N. Goddy-Wurlu [1]

,
[1]Department of Computer and Information Science, Covenant University, Ota, Nigeria
Corresponding Author; victor.geteloma@stu.cu.edu.ng

Abstract-
The concept of identification has always been of great significance in terms of connecting an individual to his/her community. Verifying the identity of a person (card or number) is vital for granting the right and secure access to numerous services embedded within an Electronic Government (e-Government). e-Government applications typically require the need for citizens to provide a form of digital identity (card or number) for access to numerous services, as against the multiplicity of existing ones that are used for different platforms in Nigeria today. Nigeria and other developing nations have not taken the optimum advantage of utilizing an all in one digital identity card for providing citizens with an array of e-Government services, as well as proper authentication methods for security, as recorded in highly innovative nations in the world today. This paper addresses two major challenges of identity management in Nigeria, which are poor authentication methods for access to services and inadequate management of multiple identification systems. Therefore, the objective of this paper is to propose a web-based digital identity system framework for accessing multiple e-Government services, which includes Electronic Voting, driver's licence, Electronic Passport, Electronic Health and Electronic Payment. Also included in the framework is the authentication services, which utilizes Near Field Communication (NFC) smart cards, biometric data, and One Time Password (OTP) as a consistent and reliable means of identifying and authenticating the user's access to the embedded e-Government services.

Key words: Digital Identity, Multifactor Authentication, NFC, Smart Card, OTP and e-Government.

1. Introduction

Digital identity is the representation of an individual within a specific setting, thus enabling the individual to assume a range of distinctive identities for every service rendered in either the public or private sectors with which he or she engages in [1]. Nowadays, technology has become more pervasive and affordable [2], which has resulted in inclusive digital identification systems in some part of the world today. For example, Estonia has created a digital legal representation of an individual, whereby personal identification numbers (PINs) are utilized for authenticating individuals against the credential of a digital card, which enables the individual to remotely access public services, and also allows them to sign authoritative documents or contracts with a similar lawful legitimacy as though they were signed in person [3]. Digital identity systems have opened a new area of development for civil participation and have increased the efficiency of public services as evident in Belgium, Estonia, Finland, France, the Republic of Korea and Singapore, where citizens can pay taxes or request official documents online [4]. With the advances in technology every day, the preferences of identity mechanisms have already made a large impact on the social, cultural, business, and political aspects of human lives [5], [6]. The ability to access and use digital identities on the go (anywhere and anytime), has become a prerequisite for a dynamic information society [6].

1.1 The Need for a Digital Inclusive Identification System

In 2015, the World Bank acknowledged the likelihood of using digital identity cards as a medium for connecting conventional national identity cards to multiple functional applications [7]. The mission of the World Bank's Identification for Development initiative is to foster inclusive development by helping countries to build secure and efficient identification systems. In their investigations, they discovered that over 1.1 billion people worldwide, most of whom belong to developing or low income nations, lack the official identification needed to access basic services and opportunities which includes casting of votes, accessing health care services, getting jobs, accessing financial services, and other social benefits [8]. Digital identity is now seen as a need for developing or low income nations to develop essential primary forms of identification, and as a chance to cultivate digital inclusion by linking trusted and secured e-government services to digital identity systems [9]. Although most developing nations already have a type of digital identity system which is attached to specified services and is serving a subset of the populace, just a couple have a multipurpose digital identification system that covers the whole populace [3]. According to [10], amongst the developing nations in the world today:

- 24% have no form of a digital identification system,
- 18% have a system that is aimed at providing only identification services,
- 55% have a system that is utilized for identification services, as well as for accessing a limited amount of offline services, and
- 3% have a foundational multipurpose digital identification system utilized for providing both identification services, and for accessing a variety of online and offline e-Government services.

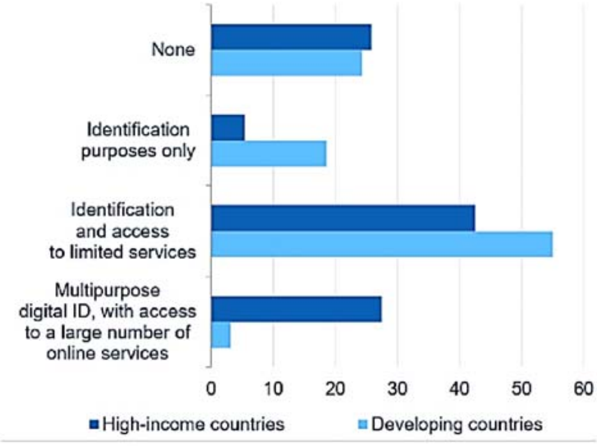

Figure 1: Digital Identity Penetration

The importance of digital Identities has now been acknowledged in the post 2015 development agenda by the united nations, solely as a Sustainable Development Goal (SDG) target to "promote peaceful and inclusive societies for sustainable development, provide access to justice for all, and build effective, accountable, and inclusive institutions at all levels" [11]. A key indicator of the SDG target is to "provide legal identity for all, including birth registration, by 2030". Achieving this goal in the best way possible can be done by building a unified digital identity system for all, which results in utilizing a solitary digital identity card for access to multiple e-Government services and relies on the digital rather than the physical attributes of an individual for authentication.

1.2 Early Adopters of Unified Digital Identity Systems

As of recent, advancements in digital identification systems have been achieved by different worldwide governments [12], [13]. Adopting digital technologies (such as smart cards, mobile devices, etc.) for digital identity solutions, presents an opportunity for Governments to drive transformational change for citizens, businesses and public administrations, enhance the performance and delivery of numerous e-Government services, and promote a more connected digital society both at the national and cross-border level [9], [14]. Other key drivers of the digital identity evolution, which includes strengthening essential identity allocation procedures, upgrading border security measures, and improving the conveyance of social benefits for individuals, have assumed a noteworthy role in the developing various national identity frameworks in various parts of the world, thus creating digital identity systems [15]. Following the global trend towards a unified digital identity implementation, Table 1 lists some countries that have successfully adopted smart identity cards embedded with multiple applications.

Table 1: Some Successful Adoptions of Unified IDs

COUNTRY	*NAME OF ID CARD*	*YEAR INTRODUCED*	*USES*	*REFERENCES*
Austria	Citizen Card	2002	National ID Card E-Government Services E-Banking E-Education	[16]
Belgium	eID Card	2003	National ID Card E-Government Services E-Banking E-Health E-Commerce	[17]–[20]
Finland	Finnish eID Card	1999	National ID Card E-Government Services E-Banking (Online) E-Health European Travel	[19]–[21]
France	French National Identity Card	2007	National ID Card E-Banking E-Education E-Voting E-Health European Travel	[20]

Estonia	eID Card	2010	National ID Card E-Banking E-Education E-Voting E-Health European Travel	[17], [22]–[24]
Germany	German Identity Card	2010	National ID Card E-Government Services E-Business European Travel	[17], [20], [25]
Malaysia	MyKad	2001	National ID Card Driver's License E-Banking E-Health Transportation Card	[20], [26]–[28]
Spain	eID Card	2006	National ID Card E-Government Services E-Commerce European Travel	[17], [20], [29]
UAE	Smart ID Card	2003	National ID Card E-Commerce E-Voting	[15], [30]

1.3 Authentication Technologies & Digital Identity Systems

Digital identity is vital for accessing and engaging in systems, which requires the use of appropriate authentication techniques for guaranteeing the privacy, integrity and security of the user's identity [31]. Authentication is the utilization of at least a mechanism to verify the identity of a person or other entity requesting access under security constraints [32]. Nowadays, digital identity management systems are inclined to establishing single digital identities for individuals based on three distinct factors of authentication: The Knowledge Factor (What the user knows), The Possession Factor (What the user has), and The Inherence Factor (What the user is) [10], [33].

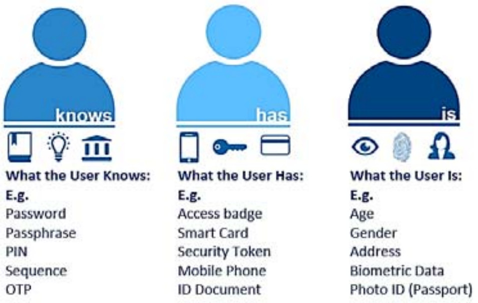

Figure 2: Authentication Factors

By combining at least two of these factors together (Multi-factor authentication), the optimal security of the individual's identity is guaranteed, thus minimizing vulnerabilities, which includes; Brute Force Attacks, Fake Alerts, Phishing/Vishing Attacks, Key Logger Attacks, Man in the Middle Attacks, Image capture and replay attacks, etc. [34].

Establishing the digital identity of an individual means to verify the authenticity of the presented authentication technology, which is the key features that guarantees the security of the individual's identity. Authentication technologies are utilized for providing filters that verifies the attributes of digital identities and grants permissions for legitimate individuals to access services [35].

Contactless Smart Cards: Smart cards are widely recognized as a robust solution for authentication because they can be used to authenticate an individual's identity using multiple authentication factors for varying levels of assurance [8]. Although the original design of smart cards was contact based, the present necessities for expanded data transmission speed and expediency of smart cards has driven the market towards contactless approaches. According to [36], contactless smart cards are advantageous to digital identity systems over contact-based ones, in terms of:

- Speed: Contactless smart cards provides quicker transaction time for card holders.
- Convenience: The operation and transaction of contactless-based smart cards requires little to no effort from the card holder. All the card holder needs to do to start a session is to swipe his or her card.
- Low Maintenance: Contactless cards require less maintenance because the components of the card are not exposed to natural elements, and to the friction of contact scenarios, thus preventing most of the wear and tear that damages contact cards.

NFC: Integrating contactless smart cards with NFC technology offers vital advantages in the amount and type of data that can be stored, the incorporation of multiple-independent applications (aka applets), and the flexibility for multipurpose digital identity programs [37]. NFC is a short range wireless communication technology, which provides safe yet straightforward and instinctive data transmission techniques amongst electronic gadgets [38]. NFC is a subdivision of Radio frequency identification (RFID) systems, which uses a carrier frequency of 13.56 MHz, a data transfer rate of 424kbps, and operates within an extended communication protocol and data exchange format of ISO/IEC 14443 standards [39]. Also, NFC supports secured data transmissions over distance rates of at least 10 cm through a combination of RFID and contactless smart card standards [40]. NFC technology has two goals, which are simplicity and security. By using near-field electromagnetic waves, communication can be initiated by reducing the proximity between electronic devices [41]. The combination of NFC technology and contactless smart card for digital identity solutions presents an opportunity for governments to: Drive transformational change for citizens, businesses and public administrations, Enhance the performance and delivery of its services, and Promote a more connected digital society both at the national and cross-border level [9], [14].

Biometrics: Biometrics is commonly defined as a quantifiable behavioral trait of individuals that can be captured and utilized for authentication purposes [42]. Various forms of biometric data utilized for authentication purposes includes fingerprints, iris scans, retina scans, hand geometry, face recognition, voice recognition, signature recognition and keystroke patterns [20]. According to [43] utilizing biometric technology for digital identification and authentication of individuals involves employing three (3) distinct phases such as:

1. Sampling Phase: This involves capturing a set of biodata samples of an individual and subsequently utilizing the average measurement to produce the individual's digital template.

2. Storage Phase: This involves encrypting the digital template and storing it on either a hardware token (smartcard), on a database or remotely on a cloud [44].
3. Recognition Phase: This involves utilizing the stored digital template on an authentication mechanism in order to gain access into a system. Gaining access requires making a match between the biodata read from the authentication mechanism against the stored digital template of the individual.

The key to the utilization of biometrics as an authentication technology for digital identities, is the multiplicity contained in an individual's biodata. This makes biometrics a core process for digital identification and authentication, whereby the biodata of an individual is used to match the individual's identifier or attribute data [20].

One Time Password: One Time Password (OTP) is a unique passcode that is generated using algorithms, which combines random characters and symbols to form strong passwords each time they are requested. Once an OTP is used, it becomes invalid and cannot be reused [45]. Amongst the various methods of sending OTPs for authentication processes, a simple method involves the use of mobile phones for receiving OTPs via SMS. The idea of using mobile phones as a possession factor for OTPs was developed to provide an alternative method of using hardware tokens. The method is advantageous because it eliminates the for additional dedicated tokens, as users tend to carry their mobile devices around at all times [46]. Nigeria has witnessed an increase in mobile phone penetration due to more affordable means of acquiring these devices, and has been recognized as the most mobilized country in the world with most of the internet traffic coming from mobile devices [47], [48]. Thus, a mobile first approach is necessary in order to engage Nigerians in a more digital inclusive environment, which makes it very easy and efficient for individuals to access e-Government services remotely [47].

Several works have been published in relation to this study, which is focused on multipurpose digital identification systems, with emphasis on the smart card technology and the authentication methods utilized for identification purposes, and access to multiple applications. The design of an identification system that utilizes RFID (Radio Frequency Identification) smart cards and NFC (Near Field Communication) mobile device readers for identity recognition and access to integrated services, was proposed in [49]. The authors developed an NFC based identification system framework, which utilizes a combination of RFID smart cards, finger print technology, and NFC enabled mobile device readers for identity recognition. The smart card and the user's finger print is utilized as the forms of authentication (two factor authentication).

The authors in [50] proposed a model to eliminate the conflict issues that arises with the use of multiple identities in India such as Forgery, Privacy, Security, data Theft, and Loss of Cards. They developed a Secured multipurpose Unique System Identity (USID) card framework using integrative approaches with the help of RFID technology and biometrics. The framework is designed to utilize the user's biometric data embedded in a smart card as the only form of authentication (single factor authentication).

An identification system was developed in [51], which is designed based on Smartphones and NFC technology, as it allows for the utilization of mobile phones as a form of secure electronic ID. The authors examined the idea of combing the characteristics of an electronic ID card with

NFC technologies using the mobile phone. They Developed a Mobile-ID system, which is an extension of an eID system, designed for the identification of users to access multiple government services. The Mobile-ID is utilized as the only form of authentication (single factor authentication).

The authors in [52] proposed an authentication system based on the Spanish multipurpose ID card and NFC technology. The multipurpose ID card is used for accessing e-Government, e-Commerce, and e-Passport services, while the NFC technology is used to establish wireless ad hoc communications. They developed a network-oriented architecture using cryptography techniques and authentication certificates to establish secure communications between two interlocutors. The network-oriented architecture also enables the proposed authentication system to operate in both local and remote modes. The multipurpose ID card was utilized as the only form of authentication (single factor authentication).

[53] designed and implemented a multipurpose smart card for access to e-health, e-passport and e-payment systems, and an encryption method for its security. They developed an effective encryption system for a multipurpose smart card using Data Encryption Standard (DES) and Elliptic Curve Cryptography (ECC) algorithms to secure the user's data and privacy. The multipurpose smart card was utilized as the only form of authentication (single factor authentication).

2. Methodology: The Proposed Framework

The proposed unified digital ID framework is an adaptation of the German eCard-strategy, which is the harmonization of various government projects issuing smart cards for authentication and signature purposes. The German government developed the eCard API-Framework, which aims at supporting arbitrary smart cards and facilitating the integration of them into various eID-applications [54]. As shown in Figure 3, the proposed framework distinguishes between three layers, which represent the abstract view of applications down to the physical connection to a smart card. The crucial factors of the framework are the electronic authentication of the card holder, the qualified digital signature supported on the smart card, and the secure authentication methods utilized in accessing the card holder's personal and sensitive data, as well as accessing the embedded applications. The Framework provides a simple and uniform access to various applications through a standardized NFC smart card interface. The framework is divided into three (3) layers; Application Layer, Identity Layer, and Authentication Layer.

2.1 Application Layer

The application layer provides a web interface for interaction with the framework by connecting via a web browser on computing devices (PC, laptop, or mobile). This layer contains various applications, functions and services, which are only accessible via the utilization of an NFC smart card against its equivalent card reader. The accessible applications include e-Voting, driver's license, e-passport, e-health and e-payment.

2.2 Identity Layer

The Identity layer provides the management interface and the electronic card interface, which is utilized by various applications with appropriate permissions. The management interface offers functions for updating and managing trusted identities from the database, as well as smart cards and smart card readers. To manage the user's identity on the framework, functions to initialize, update, as well as terminate identities (and its appropriate sessions) are included in this interface. The management interface also offers functions to add or remove Card Info files to or from the database.

The electronic card interface encapsulates cryptographic functions for encryption and digital signature of the user's interaction within the system. Digital signatures require certificates for verification, thus the interface includes functions for identity management to manage a database of trustworthy identities and services.

2.3 Authentication Layer

The Authentication layer provides the security functionality required for authenticating the user within the system. The ISO/IEC I4443 and ISO/IEC 18092 Interface provides standardized support for the NFC smart card and the equivalent card reader, the biometric interface provides support for the user's bio data (fingerprint), and the passcode generator provides support for generating OTPs.

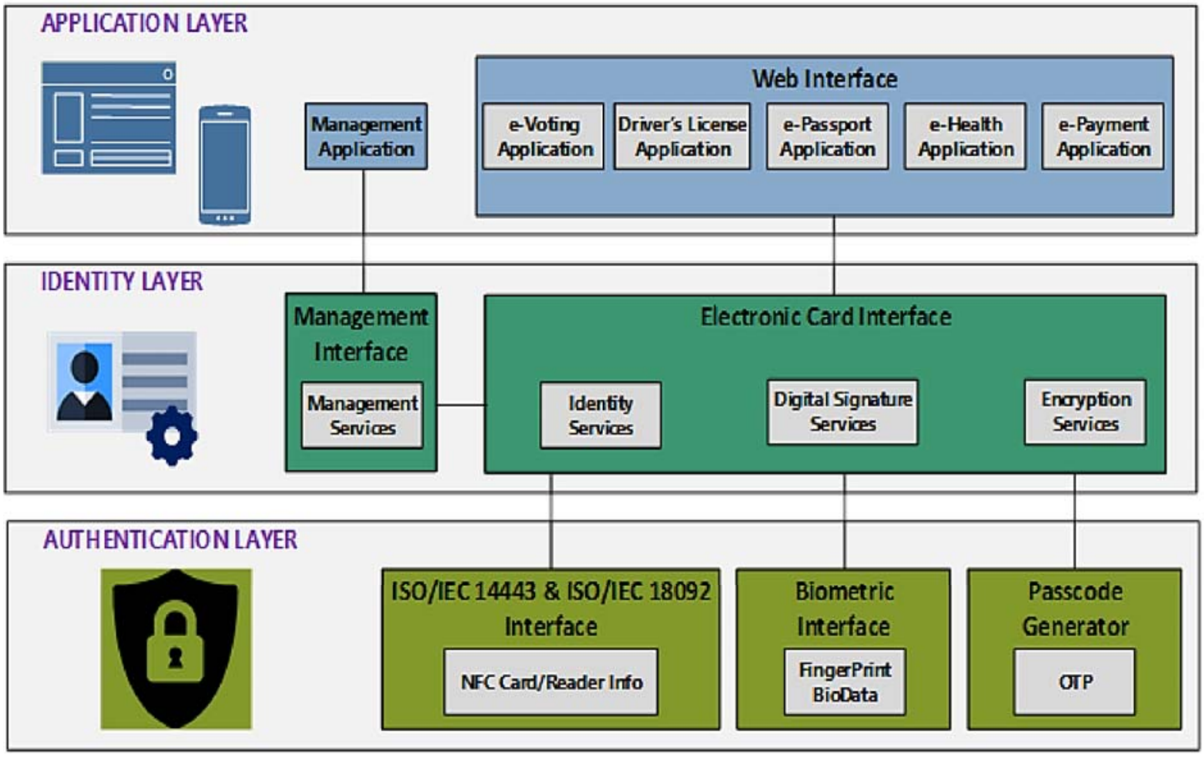

Figure 3: The Proposed Unified digital ID Framework

3. Discussion

This study is part of an effort to mitigate the multiplicity of identification systems in Nigerian today by providing an alternative to the already existing system. In this study, a 3-tier system framework is proposed, which supports the use of authentication technologies on web applications and is a clear distinction between it and the current identification systems utilized in Nigeria today. Figure 4 below shows the authentication flowchart of how the proposed framework system works. The utilized authentication factors are: The NFC Smart Card, Biometric data (fingerprint), and OTP. To log into the web interface of the system, the users are required to either swipe their NFC smart card against a smart card reader or scan their fingerprint against a fingerprint reader. Once the user is authenticated, the ID information is generated from the database and the user is granted access to the ID system, where he/she can transact with either the voting, driving, passport, healthcare or payment services. At the point of processing any of the selected service, an OTP is generated and sent to authenticate the user, which is required before any of the selected service is confirmed.

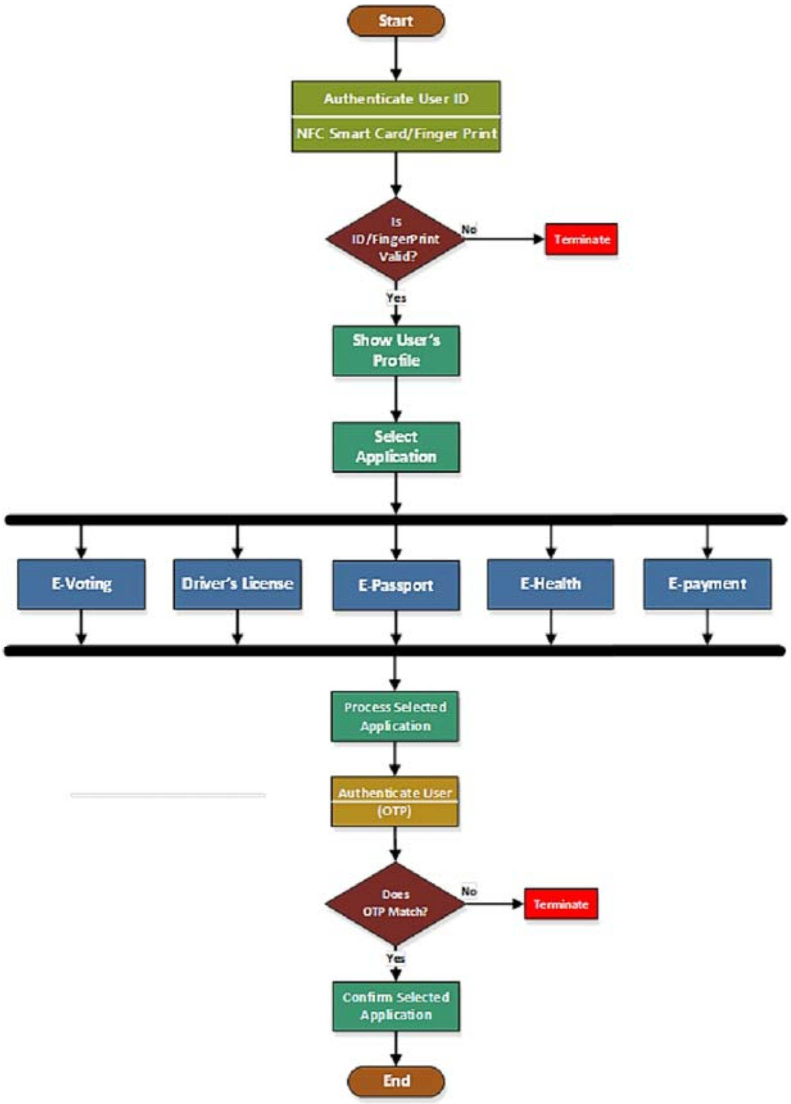

Figure 4. Authentication Flowchart of the Proposed Framework [55], [56]

Although, a lot of Nigerians have various forms of cards for identity, voting, payment, and other purposes, the concept of utilizing just a single smart card for access to all e-Government services, provides significant advantages to better the delivery of services, and also eliminates the possibility of registering multiple times for access to services. In an electoral scenario, voting via the web interface has a significant gain over the ballot/paper voting approach in terms of speed, cost and accuracy, and it also provides an easy and assessable method of voting for Nigerians who are unwilling to leave the comfort of their homes to participate in electoral processes.

Additionally, this initiative results in the development of a central database of Nigerians, which will serve as a repository of all records. On it, the personal information of citizens will be registered and subsequently updated. For example, 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 of the developed system are sufficient enough to guarantee the privacy, integrity and non-repudiation of the individual's identity and subsequent access to services, which will increase the level of trust in Nigeria's identification system and improve the level of participation by Nigerians.

4. Conclusion

Developing a unified digital ID system for all has the potential to advance many key elements of the SDGs, including digital inclusion, social protection, human empowerment, financial inclusion, governance, healthcare, education, digital development, and humanitarian assistance. In addition to reducing a basic barrier to accessing services, unified IDs can decrease wastes and leakages in public administration, facilitate innovation on how services are delivered, and empower the most poorest and vulnerable individuals in society by granting them access to critical services (voting, education, healthcare, and finance), while also advancing their legal and political rights, thus ensuring that no one is left behind in the digital age.

Furthermore, combining the e-Voting, driver's license, e-Passport, e-Health and e-Payment systems in Nigeria, will greatly enhance the overall digital identity management of each citizen, which includes simplifying the current healthcare delivery methods, proper Issuance and management of driving licenses and passports, conducting trusted electoral exercises, and performing payment transactions securely. Thus, improving the socio-economic life of Nigerians with the utilization of a single digital identity card.

Acknowledgements

We would like to acknowledge the support and sponsorship provided by Covenant University through the Centre for Research, Innovation, and Discovery (CUCRID).

Reference

[1] Seigneur, J. M., and Maliki, T. El. (2009). Identity Management. Computer and Information Security Handbook. Elsevier Inc. https://doi.org/10.1016/B978-0-12-374354-1.00017-0

[2] Ojaide, C. L. (2010). INFORMATION FLOW IN A RESTRUCTURED NIGERIA NATIONAL IDENTIFICATION SYSTEM: Election and Census Fraud Solution. Blekinge Institute of Technology.

[3] Atick, J., Dahan, M., Gelb, A., and Harbitz, M. (2016). Digital identity. World Development Report, 194–197.

[4] UNDP. (2016). Human Development Report 2016: Human Development for Everyone. 1-286.

[5] Maliki, T. E., and Seigneur, J. (2007). A Survey of User-centric Identity Management

Technologies Requirements. International Conference on Emerging Security Information, Systems and Technologies, 12–17.Retrieved from https:// doi.org/10.1109 /SECURWARE.2007.6

[6] Maliki, T. El, and Seigneur, J. (2013). Online Identity and User Management Services. Computer and Information Security Handbook. Elsevier Inc. 985-1009. Retrieved from https://doi.org/10.1016/B978-0-12-803843-7.00071-5

[7] Olaniyi, O. E. (2017). The Role of National Electronic Identity Cards in Enhancing Public Service Effectiveness: The Nigerian Case. TALLINN UNIVERSITY OF TECHNOLOGY.

[8] WorldBankGroup. (2017). The World Bank Annual Report 2017, 1–87. https://doi.org/10.1596/978-1-4648-1296-5

[9] Lenco, M. (2016). Digital identity as a key enabler for e-government services. Mobile Connect - GSMA. 1-8.

[10] Domingo, S. A. I., and Enríquez, M. (2018). Digital Identity: the current state of affairs. BBVA Research, 1–46.

[11] Dahan, M., and Gelb, A. (2015). the Role of Identification in the Post-2015 Development Agenda. World Bank Working Paper, 15(July), 20. Retrieved from http://www.cgdev.org/publication/role?identification?post?2015?development?agenda %0Ahttp://documents.worldbank.org/curated/en/600821469220400272/Digital-identity-towards-shared-principles-for-public-and-private-sector-cooperation%0Ahttp://documents.worldb

[12] Griffin, D., Trevorrow, P., and Halpin, E. (2007). Introduction. e-Government: A Welcome Guest or Uninvited Stranger? In D. Griffin, P. Trevorrow, & E. Halpin (Eds.), DEVELOPMENTS IN E-GOVERNMENT, (13), 1–224. Amsterdam: IOS Press.

[13] Seifert, J. W. (2003). A Primer on E-Government : Sectors, Stages, Opportunities, and Challenges of Online Governance. Report for Congress, 24. Retrieved from https://doi.org/RL31057

[14] WorldBankGroup. (2016). DIGITAL DIVIDENDS. World Development Report, 1–359.

[15] Al-khouri, A. M. (2012). PKI in Government Digital Identity Management Systems. European Journal of EPractise, 4–21.

[16] Aichholzer, G., and Straub, S. (2010). The Austrian case: multi-card concept and the relationship between citizen ID and social security cards, 3, 65–85. https://doi.org/10.1007/s12394-010-0048-9

[17] Zwilling, A. H. (2017). Electronic Identity Management Systems in the European Union. Radboud University.

[18] Cock, D. De. (2006). Belgian eID Card Technicalities. 1-78.

[19] Gemalto. (2018). eID card - eID programs. Retrieved from https://www.gemalto.com/govt/identity

[20] Beynon-davies, P. (2007). Personal identity management and electronic government: The case of the national identity card in the UK. Journal of Enterprise Information Management, 20(3), 244–270. https://doi.org/10.1108/17410390710740727

[21] Rissanen, T. (2010). Electronic identity in Finland: ID cards vs. bank IDs, 3, 175–194. https://doi.org/10.1007/s12394-010-0049-8

[22] Martens, T. (2010). Electronic identity management in Estonia between market and state governance. Identity in the Information Society, 3(1), 213–233.

https://doi.org/10.1007/s12394-010-0044-0
[23] e-Estonia. (2015). e-identity. Retrieved from https://e-estonia.com/
[24] Gemalto. (2015). Case Study Estonia: e-ID card - Key enabler for advanced e-services. Retrieved from https://www.gemalto.com/govt/identity
[25] Gemalto. (2017). Overview of the German identity card project and lessons learned. Retrieved from https://www.gemalto.com/govt/identity
[26] Yeow, P., and Loo, W. H. (2009). Acceptability of ATM and Transit Applications Embedded in Multipurpose Smart Identity Card: An Exploratory Study in Malaysia. International Journal of Electronic Government Research, 5(2), 37–56.
[27] Neo, H. F., Yeow, P., Eze, U., and Loo, H. S. (2012). Organizations Adoption of MyKad Initiative, 1–9. https://doi.org/10.5171/2012.542549
[28] Loo, W. H., Yeow, P., and Chong, S. C. (2011). Acceptability of Multipurpose Smart National Identity Card: An Empirical Study. Journal of Global Information Technology Management, 14(1), 35–58. https://doi.org/10.1080/1097198X.2011.10856530
[29] Heichlinger, A., and Gallego, P. (2010). A new e-ID card and online authentication in Spain. Springer, 3, 43–64. https://doi.org/10.1007/s12394-010-0041-3
[30] Al-khouri, A. M. (2012a). eGovernment Strategies The Case of the United Arab Emirates (UAE). European Journal of EPractise, 126–150.
[31] Ayo, C., and Ukpere, W. (2010). Design of a secure unified e-payment system in Nigeria: A case study. African Journal of Business …, 4(9), 1753–1760.
[32] Akinola, K. E., Amanze, R. C., Somefun, O. M., Okonji, C. N., Esomu, S. E., Nwala, K. T., and Odunayo, Y. (2017). Internet Banking In Nigeria: Authentication Methods, Weaknesses and Security Strength. American Journal of Engineering Research (AJER), 6(9), 226–231.
[33] Nwabueze, E. E., Obioha, I., and Onuoha, O. (2017). Enhancing Multi-Factor Authentication in Modern Computing. Communications and Network, 09(03), 172–178. https://doi.org/10.4236/cn.2017.93012
[34] UCSC. (2019). What type of attacks does Multi-Factor Authentication prevent? Retrieved May 9, 2019, from https://its.ucsc.edu/mfa/cyber-attacks.html
[35] CIO. (2018). What is Authentication Technology. Retrieved February 5, 2019, from https://whatis.ciowhitepapersreview.com/definition/authentication-technology/
[36] SmartCardAlliance. (2012). Benefits of Smart Cards versus Magnetic Stripe Cards for Healthcare Applications, 1–4.
[37] AlphaCard. (2018). Smart Card & RFID Encoding. Retrieved from https://www.alphacard.com/
[38] Kumar, A. (2010). Near Field Communication. COCHIN UNIVERSITY OF SCIENCE & TECHNOLOGY. Retrieved from http://123seminarsonly.com/Seminar-Reports/023/52532252-NEAR-FIELD-COMMUNICATION.docx
[39] NFC-Forum. (2018). What Is NFC? Retrieved from https://nfc-forum.org/
[40] Madlmayr, G. (2008). A mobile trusted computing architecture for a near field communication ecosystem. In Proceedings of the 10th international conference on information integration Web-based applications & services (pp. 563–566).
[41] Antonopoulou, A. (2011). Near Field Communications (NFC) – Case Study : Mobile Banking in South Africa.
[42] Austin, J. H., and David, C. Y. (2002). Biometric authentication: assuring access to information. Information Management & Computer Security, 10(1), 12–19.

[43] Camp, L. J. (2004). Digital identity. IEEE Technology and Society Magazine, 23(3), 34–42.

[44] Odun-Ayo, I., Ajayi, O., and Misra, S. (2018). Cloud Computing Security: Issues and Developments. Proceedings of the World Congress on Engineering, 1, 1-8.

[45] Aloul, F., Syed, Z., and El-Hajj, W. (2009). Two Factor Authentication Using Mobile Phones. Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference On, 641--644.

[46] Patil, G. (2013). What is a Hardware Token? Quora.

[47] Terragon-Group. (2018). Digital Trends for Nigeria in 2018.

[48] Twinpine. (2017). 2017 Nigeria Mobile trends report.

[49] Zhang, Y., Xin, C., Liu, W., Ding, J., and Zhu, Q. (2015). Identification System Based on Near Field Communication and Fingerprint Technology for Android Mobile Devices, 2232–2235.

[50] Pal, Y., Tiwari, N. K., and Mishra, S. N. (2016). An Integrative Approach for Multipurpose USID Framework Using Radio Frequency Identification : Securities and Challenges, 5(4). https://doi.org/10.17148/IJARCCE.2016.5467

[51] Maazouz, K., Benlahmer, H., and Achtaich, N. (2014). Identification System using Mobile Device Enabled NFC, 10(7), 37–39.

[52] León-Coca, J. M., Reina, D. G., Toral, S. L., Barrero, F., and Bessis, N. (2013). Authentication systems using ID cards over NFC links: The Spanish experience using DNIe. Procedia Computer Science, 21(November 2014), 91–98. https://doi.org/10.1016/j.procs.2013.09.014

[53] Savari, M., Montazerolzohour, M., and Thiam, Y. E. (2012). Combining Encryption Methods in Multipurpose. In Proceedings of The International Conference on Cyber Security, Cyber Warfare and Digital Forensic, 43–48).

[54] Horsch, M., and Stopczynski, M. (2011). The German eCard-Strategy.

[55] John, S. N., Ayo, C. K., Ndujuiba, C., and Okereke, E. C. (2013). Design and Implemenation of a Unified e-ID Card for Secure e-Voting System (MUSES). International Journal of Computer and Information Technology, 2(06), 1131–1135.

[56] Ayo, C. K. (2011). Designing a framework for a unified electronic identity system: Nigeria a case study. Global Journal of Pure and Applied Sciences, 16(2), 269–275. https://doi.org/10.4314/gjpas.v16i2.62851