International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Analysis of the risks from citizen indentifications with electronic chip

Nam Truong Dong *

Dong Nai Technology University, Bien Hoa, Dong Nai, Viet Nam.

International Journal of Science and Research Archive, 2023, 09(01), 262–268

Publication history: Received on 09 April 2023; revised on 25 May 2023; accepted on 27 May 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.9.1.0421

Abstract

In recent years, the use of electronic identification has become increasingly popular, with more and more countries implementing this technology. E-IDs are used for a variety of purposes, including accessing government services, voting, and conducting financial transactions. The electronic chip embedded in the card stores a wealth of personal information, including biometric data, residency information, and personal photographs. While e-IDs have many benefits, they also pose significant risks, particularly when it comes to the security of personal information.The aim of this research paper is to explore the risks associated with e-IDs and to identify the factors that contribute to these risks. We will examine the potential consequences of these risks, including identity theft, financial fraud, and other forms of cybercrime. In addition, we will provide recommendations on how to mitigate these risks and ensure that e-IDs are used safely and securely.

Keywords: E-Ids; Electronic Chip; Electronic identification; Biometric data; Residency information

1 Introduction

Citizen identification is an essential aspect of modern society, enabling individuals to access public services, vote, travel, and carry out transactions in a secure and reliable manner. In recent years, there has been a significant shift towards electronic identification (e-ID) systems, which use electronic chips and biometric data to verify identity. These systems offer numerous benefits, including increased security, convenience, and efficiency. However, they also present new challenges, particularly around data privacy and security [1-2].

This research paper aims to explore the topic of citizen identification, with a specific focus on e-ID systems. The paper will begin by providing an overview of the different types of citizen identification systems that are currently in use, including traditional paper-based systems and newer e-ID systems. We will then explore the benefits and challenges associated with e-ID systems, with a focus on issues related to data privacy and security [3].The paper will also examine case studies from around the world, including countries that have successfully implemented e-ID systems, as well as countries that have faced challenges in doing so. Through these case studies, we will identify best practices and potential pitfalls associated with e-ID implementation [4].

Finally, the paper will conclude with recommendations for policymakers and other stakeholders involved in citizen identification. We will consider the importance of striking a balance between the benefits of e-ID systems and the need to protect individual privacy and security. The paper will also identify areas for future research, including the potential impact of emerging technologies such as blockchain and artificial intelligence on citizen identification [3-5].

Citizen identification cards with electronic chips, commonly known as e-IDs, have become an integral part of daily life in many countries. These cards are designed to make identification and authentication easier and more secure. However, with the increasing use of e-IDs, new risks have emerged, including identity theft, fraud, and other forms of

* Corresponding author: Nam Truong Dong

cybercrime. This research paper focuses on the risks associated with citizen identifications with electronic chips and aims to identify the key factors that contribute to these risks. We will examine the potential consequences of these risks and provide recommendations on how to mitigate them, shown in Figure 1 [6-8].

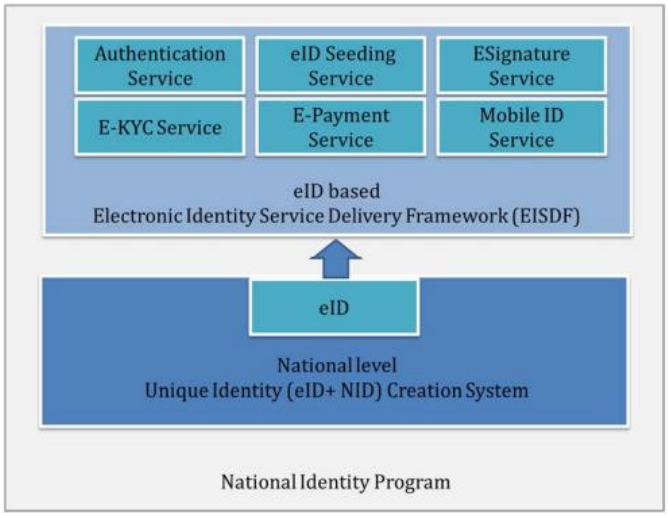

Figure 1 Technical Organization of the National eID System

Services Offered. Some of the key services that may be delivered with the implementation of the EISDF are explained below [9-10].

- The Electronic Identity Authentication Service (EISDF) has the potential to support the implementation of a nation-wide electronic service for the authentication and identification of residents, both physically and online. The service can be utilized by various service providers in both the public and private sectors to offer eID-enabled services via eID-enabled applications to their customers, beneficiaries, and subscribers. (CBS).
- The Electronic Identity Seeding Service offered by the EISDF allows for eID authentication to be used by linking the CBS profile to the individual's unique National Identity Number (NIN) that is generated at the national level during registration.
- The electronic signature service (eSignature) can be implemented through the EISDF, allowing residents to sign eDocuments when conducting transactions with both public and private sectors. By utilizing eSignatures, paperless eService workflows can be established, eliminating the requirement for physical signatures.
- Electronic Know-Your-Customer Service (eKYC). The EISDF has the potential to offer an electronic, centralized eKYC process, allowing service providers to verify their customers' identities electronically with their explicit consent. This eKYC service, based on eID, can provide instant and non-repudiable Proof of Identity (PoI) and Proof of Address (PoA), as well as the customer's date of birth and gender. Additionally, it can provide the customer's mobile number and email address to the service provider, thereby streamlining the service delivery process
- The Electronic Identity Service Delivery Framework (EISDF) has the potential to offer an ePayment service that is based on eID through the Electronic Identity Service Delivery Platform (EISDP). The ePayment service would enable government agencies to transfer public program benefits, including social pension, healthcare benefits, scholarships, and others, directly to the intended beneficiaries. This streamlined process would enable seamless Government-to-Citizen payments to the beneficiary's bank account, which can be identified through the beneficiary's electronic ID..
- The Electronic Identity Service Delivery Framework (EISDF) could offer a Mobile ID solution, which would allow residents of Vietnam to use their mobile phones as a form of electronic identification. This would significantly enhance the accessibility and timeliness of eID services for the population.

2 Details Description of e-ID Card

2.1 Details of an e-ID card with electronic chip

According to Circular No. 06/2021/TT-BCA, effective from January 23, 2021, shown in Figure 2.

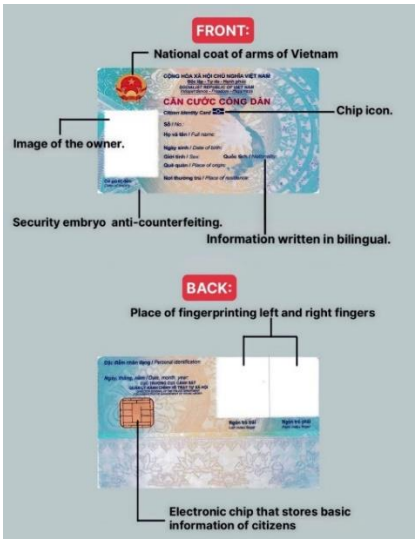

Figure 2 e-ID card template with chip

High security: Digital document management systems provide advanced security features such as encryption, access controls, and audit trails, making it difficult for unauthorized individuals to tamper with or access sensitive information.

Reduced costs for notarizing documents: Digital document management eliminates the need for physical paperwork, printing, and manual notarization processes, resulting in cost savings for organizations and individuals.

Integration of additional information: Digital systems can easily integrate various types of information, such as health insurance records, social insurance data, driver's licenses, and more. This integration improves data accessibility, efficiency, and accuracy.

Support for multiple applications: Digital document management solutions can support a wide range of applications, including digital signatures and biometric authentication. These capabilities enhance the authenticity and security of digital documents and transactions.

Prevention of document forgery: Digital document management systems utilize cryptographic techniques and other security measures that make it extremely difficult to forge or alter documents, ensuring the integrity and authenticity of the information.

Implementing a digital document management system or utilizing digital identity solutions can bring these advantages, streamlining processes, enhancing security, and reducing costs associated with document management and verification.

While electronic identification (e-ID) systems offer numerous advantages, there are also some potential disadvantages and challenges to consider. Here are the disadvantages you mentioned:

Risk of information exposure: Some individuals may unknowingly share their e-ID card information on social networks or other platforms, which can lead to the misuse of personal data by third parties. Educating citizens about the importance of protecting their personal information is crucial in addressing this risk.

Counterfeiting of e-ID cards: Despite the security measures implemented in e-ID cards with chips, there is always a possibility of counterfeiting. Sophisticated methods and technologies may be employed to replicate or forge e-ID cards, potentially compromising their integrity and undermining the trust in the system.

Limited knowledge of personal information security: Many individuals may have limited awareness and understanding of personal information security practices. This lack of knowledge can make them more susceptible to social engineering attacks, phishing attempts, or other forms of identity theft.

Misuse by virtual companies: It is possible for virtual or fraudulent companies without actual employees to acquire e-ID cards to create fake records or engage in fraudulent activities. This highlights the importance of robust verification processes and strict regulatory measures to prevent such misuse, Figure 3.

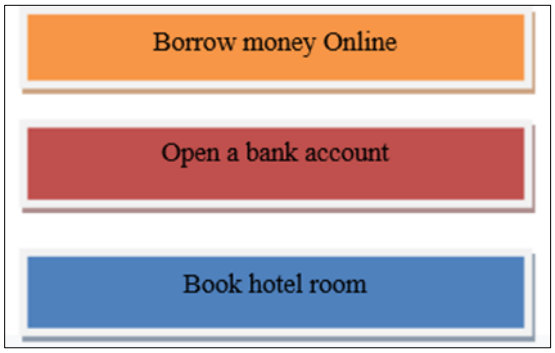

Figure 3 Fake e-ID model with chip

3 Some Applications Use e-ID Card

To clarify the risks and disadvantages of an e-ID card, some applications are used for testing as follows: using e-ID card to borrow money online, using e-ID card to open online bank accounts, using e-ID card to book hotel rooms

3.1 Use e-ID to borrow money online

Online money lending websites, all of them are required to attach an e-ID card when you apply for a borrow money online, usually the information required here is e-ID, name, occupation, hometown, personal phone number, company phone number, and OTP verification code, Figure 4.

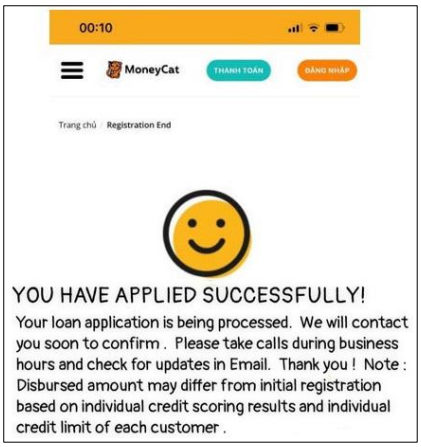

Figure 4 Using e-ID card to borrow money online

3.2 Use e-ID In Case Of Opening A Bank Account Online (Banking Apps)

In this article, I use some banking apps for testing such as VCB, BIDV, TPBank, OCB Bank, Figure 5.

+ Open a VCB Online account

Figure 5 Using e-ID card when opening a VCB account

+ Open a BIDV online account, shown in Figure 6 and wFigure 7.

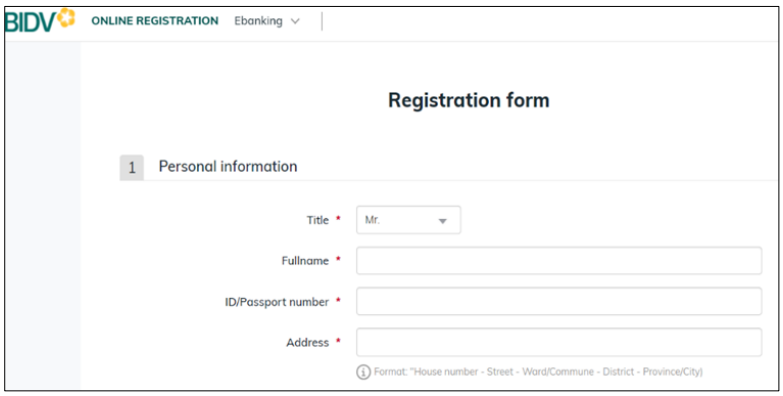

Figure 6 Using e-ID card when opening a BIDV account

Figure 7 Open a TPBank online account

3.3 Use e-ID Cards To Book Hotel Rooms

In hotels, when booking a room, customers are often required to provide e-ID cards, therefore the hotel owner/manager can save the room number, room rate, and other expenses before the guest rents the room. Some hotels also allow customers to book rooms online, one of which may require e-ID cards to reserve a room in advance. In this article, I use 2 e-ID cards to test hotel reservations at 8 hotels in Dong Nai.

Thus, through testing and comparison, the risk detection results of e-ID cards test success rate in the case of online borrowing is 100%, opening a bank account is 25%, hotel booking is 75%. This proved my original e-ID cards hazard analysis was possible. I have succeeded in checking e-ID cards. At the present time, I am the only one who has analyzed this issue and pointed out the shortcomings of the e-ID cards.

4 Conclusion

In this article, I give some typical examples which are the most realistic and associated with the lives of all citizens. The experimental e-ID cards pseudo-system can detect and alert everyone, especially social media users. Some sources of customer information are also exposed because bank insiders or third parties sell data for profit. More specifically, I have been able to use from seemingly harmless e-ID cards photos, but it has pointed out many problems about the weaknesses of e-ID cards. Up to now, only my article is able to analyze this, thereby helping the state, authorities, the Ministry of Public Security, application developers and citizens in the country, the international community has discovered the disadvantages of e-ID cards and hopes to make significant improvements. In the future, I am going to upgrade this model by testing the withdrawal functionality and the integrated papers on the e-ID cards

Compliance with ethical standards

Acknowledgments

The researchers acknowledge and appreciates all the mothers who participated in this study

Disclosure of conflict of interest

All authors contributed positively to the writing of this manuscript and there no conflict of interest as agreed to the content of this research.

Statement of informed consent

Informed consent was obtained from all individuals respondents included in the study

References

[1] Meingast, Marci, Jennifer King, and Deirdre K. Mulligan. "Embedded RFID and everyday things: A case study of the security and privacy risks of the US e-passport." In 2007 IEEE International Conference on RFID, pp. 7-14. IEEE, 2007.

[2] Tsap, Valentyna, Ingrid Pappel, and Dirk Draheim. "Key success factors in introducing national e-identification systems." In Future Data and Security Engineering: 4th International Conference, FDSE 2017, Ho Chi Minh City, Vietnam, November 29–December 1, 2017, Proceedings 4, pp. 455-471. Springer International Publishing, 2017.

[3] Akkaya, Cigdem, Petra Wolf, and Helmut Krcmar. "Factors influencing citizen adoption of e-government services: a cross-cultural comparison (Research in progress)." In 2012 45th Hawaii International Conference on System Sciences, pp. 2531-2540. IEEE, 2012.

[4] Chauhan, Sumedha, and Anjali Kaushik. "Evaluating citizen acceptance of unique identification number in India: an empirical study." Electronic Government, an International Journal 12, no. 3 (2016): 223-242.

[5] Zang, Chongzhi, Dustin E. Schones, Chen Zeng, Kairong Cui, Keji Zhao, and Weiqun Peng. "A clustering approach for identification of enriched domains from histone modification ChIP-Seq data." Bioinformatics 25, no. 15 (2009): 1952-1958.

[6] Chorley, Brian N., Michelle R. Campbell, Xuting Wang, Mehmet Karaca, Deepa Sambandan, Fatu Bangura, Peng Xue, Jingbo Pi, Steven R. Kleeberger, and Douglas A. Bell. "Identification of novel NRF2-regulated genes by ChIP-Seq: influence on retinoid X receptor alpha." Nucleic acids research 40, no. 15 (2012): 7416-7429.

[7] Chorley, Brian N., Michelle R. Campbell, Xuting Wang, Mehmet Karaca, Deepa Sambandan, Fatu Bangura, Peng Xue, Jingbo Pi, Steven R. Kleeberger, and Douglas A. Bell. "Identification of novel NRF2-regulated genes by ChIP-Seq: influence on retinoid X receptor alpha." Nucleic acids research 40, no. 15 (2012): 7416-7429.

[8] Ballinger, Carol A., Patrice Connell, Yaxu Wu, Zhaoyong Hu, Larry J. Thompson, Li-Yan Yin, and Cam Patterson. "Identification of CHIP, a novel tetratricopeptide repeat-containing protein that interacts with heat shock

proteins and negatively regulates chaperone functions." Molecular and cellular biology 19, no. 6 (1999): 4535-4545.

[9] Yang, Hong, Angela Hui, George Pampalakis, Leyla Soleymani, Fei-Fei Liu, Edward H. Sargent, and Shana O. Kelley. "Direct, electronic microRNA detection for the rapid determination of differential expression profiles." Angewandte Chemie 121, no. 45 (2009): 8613-8616.

[10] Keene, Jack D., Jordan M. Komisarow, and Matthew B. Friedersdorf. "RIP-Chip: the isolation and identification of mRNAs, microRNAs and protein components of ribonucleoprotein complexes from cell extracts." Nature protocols 1, no. 1 (2006): 302-307.