Potential Security and Privacy Issues in Novel Taiwanese National Electronic Identification system

Ming-Yang Ho*, Jing-Jie Wang§, You-Shin Tsai§, and Tang-Wei Wang§
*Graduate Institute of Biomedical Electronics and Bioinformatics, and §Department of Computer Science and Information Engineering, National Taiwan University, Taipei, Taiwan.
{r08945027, b06902035, b06902054, b06902007}@ntu.edu.tw

ABSTRACT

As the imminent issuing of Taiwanese electronic identification (eID) system, recently, several privacy and security issues are actively discussed. However, there is actually no eID guideline or a general eID survey to evaluate the eID system. This study first investigates the eID issuing status all over the world and inspects existing eID system in Estonia, Belgium, Germany, and Croatia. Threat model and potential risks in the eID system are subsequently elucidated. Finally, an unprecedented eID guideline is established to evaluate all the above eID scheme as well as the Taiwanese one. In conclusion, it is obviously that the Taiwanese government should release more related information and ensure sufficient legitimacy before rashly issuing eID.

Keywords: *Electronic Identification, Security, Privacy, Guideline*

I. INTRODUCTION

While the Taiwanese government is going to issue national electronic identity card (eID) within a few months, little related information was released and the non-transparency totally agitated the public [34]. On the other hand, the spread of COVID-19 inevitably hinder its progress, which eventually deferred its release [33].

Besides, there is actually no criterion or guideline to be complied with or to evaluate the privacy and security properties of the national eID system. Several adversarial attacks events against national eID [9, 24] and security vulnerabilities in eID per se [14] aggravate the distrust of eID.

Accordingly, it is urgent to establish a guideline for the national eID system enabling effective evaluation. We, first, inspected a operational eID system in several countries and analyzed the advantages or disadvantages of different strategies. The threat model, assumption, and potential risks were then investigated. Finally, a guideline for national eID system was proposed and the scheme of Taiwanese eID system was subsequently evaluated to fairly claim its pros and cons.

This is definitely the first research that proposes a general guideline for eID system, whereas the previous ones either merely focus on few regions [16] or small topics [23] that lack general analysis.

II. PROBLEM DEFINITION

A. The eID system

Taiwanese government expected to fully substitute its traditional national ID card for the eID system in October this year although it is postponed due to the COVID-19 and public suspicion. However, neither the technical details nor an explicit description of the scheme was announced, which might increase the uncertainty of promised privacy and security properties without the inspection from the public. Thus, we are interested in whether this system can achieve the security level they claimed and whether it provides privacy preservation on cross-platform services with a small amount of available information published by the government. Besides, some researches showed that there are some potential vulnerabilities in eID systems [31, 35]. We will survey some eID systems of other countries and the security issues they encountered. In the end, we will propose a guideline that all eID systems should obey.

B. Attacker model and assumption

The attack model is assumed to be a state-level attacker, who has the newest supercomputer. Because one eID system may contain many sensitive data and support many important services, other countries, especially those aggressively expanding their power, will be very willing to compromise the lucrative eID system. The following are the security properties required to be achieved:

1) *Confidentiality, Integrity, and Availability (CIA).*
2) *Privacy: disclose only necessary information among each service; do not record any user's log.*
3) *Digital signature: for Citizen Digital Certificate.*
4) *IC card security*

TABLE I. CHRONOLOGICAL TABLE OF EID ISSUING

Year	Compulsory	Non-compulsory
1999	-	Finland
2001	Malaysia	-
2002	Estonia	Mexico
2003	Belgium	Netherlands
2006	Spain	-
2008	Morocco	-
2009	Latvia	Lithuania
2010	Bulgaria, Germany, Guatemala	-
2011	Indonesia	-
2012	Chile, Mongolia, Pakistan	-
2013	Israel, Mauritius, Nigeria, Slovakia	-

Year	Compulsory	Non-compulsory
2014	Djibouti, Luxembourg, Malta, Portugal, Somalia	-
2015	Croatia, Honduras, Tajikistan, Japan Uruguay	-
2016	Algeria, Bhutan, Iraq, Sri Lanka	Italy
2017	Turkey	Fiji
2018	Afghanistan, Cape Verde	-
2019~	Poland	-
2021	Romania	-
Other	Denmark, Norway, Sweden (Non-compulsory)	

III. RESULTS

A. Popularity of eID

Since the government of Malaysia issued the first national eID around the world in 2001 [28], a large number of countries subsequently issued their eID, and totally up to 47 countries have built their eID system until now [32]. See TABLE 1. 44.7%, 27.7%, 14.9%, 6.4%, 4.3% and 2.1% of them are countries in Europe, Asia, Africa, South America, North America, and Oceania, respectively. Obviously, eID is almost popular and ubiquitous utilized in European countries whereas others are gradually implementing this system.

B. Case study in Estonia

1) Basic Information: Citizen in Estonia who is older than 15 years old [15] have to hold an ID-card compulsorily, and this ID-card enable the holder to authenticate him/herself on the internet. Both card itself and the certificates stored in it are valid for five years [13]. The card is manufactured by IDEMIA and personalized by Hansab while the certificates are issued by SK Solution [3].

2) Information written on card: Surname, given name, gender, personal code, citizenship, date of birth, date of expiry, document number, cardholder's signature (hand written), photo, date of issuance, and place of birth are written on the card.

3) Data stored in chip: The chip stores personal information and two 384-bit ECC key pairs [8], one for authentication and another for digital signature. The personal information stored in the chip is congruous with the information written on the card except for photo and cardholder's signature. Personal information is not protected by any PIN code while the user has to enter PIN1 code to perform authentication and PIN2 code to perform digital signature [19]. If the user enters incorrect PIN1 or PIN2 code three times, the card will be blocked but can be unlocked with user's PUK code.

4) Usage: Estonia government provides a large number of online services with their ID-cards, and the following are some examples of how they are regularly used in Estonia: (1) Legal travel ID for Estonian citizens travelling within the EU; (2) National health insurance card; (3) Proof of identification when logging into bank accounts; (4) For digital signatures; (5) For i-Voting; (6) To check medical records, submit tax claims, etc.; (7) To use e-Prescriptions; (8) Encryption and decryption for data transfer.

The government provides a software called DigiDoc for cardholders to manipulate their eID card. It has three main functions: (1) Changing PIN1, PIN2 or PUK code; (2) Signing files; (3) Encryption/Decryption for data transfer.

5) X-Road: X-Road is a data exchange platform launched by the Estonia government. It provides confidentiality and integrity data exchange between data exchange parties and is the backbone of Estonian e-Government. One of the most important features of X-Road is that it makes sure the e-government system fulfills once-only police, which means citizens only have to provide certain standard information to the authorities or administrations once because each public or private sector can easily exchange its data.

6) Related products: There are several products similar to ID-card. TABLE 2 shows three of them.

TABLE II. TABLE OF RELATED PRODUCT

Product	Introduction
Mobile ID	Use a mobile phone as a form of secure digital using special SIM card.
Digi ID	Digital document that can be used in an electronic environment but cannot be presented to identify a person.
Smart ID	Use a mobile phone as a form of secure digital without SIM card.

C. Case study in Belgium [5]

Belgian first eID card was issued in 2004. Citizens could use it to perform digital signature and key generation. Every ID-card is valid for 10 years. Cardholders have to enter self-defined PIN code to access the functions related to authentication and digital signature (RSA 2048-bit). There is a randomly generated PUK code for each cardholder to change his/her PIN code. The content written on the card are name, title, nationality, place of birth, date of birth, gender, photo, ID card number, written signature, and marital status (optional).

The content stored in the chip includes two sections, PKI and Citizen identity data. The first section contains two distinct key pairs for authentication and digital signature, and the certificates of some important CA. The second section contains personal photo, ID number, and address. Citizen identity data will be signed by government so it would be arduous to forge.

D. Case study in Germany [11]

1) Stored data and function: The German eID card, issued on 1st November 2010 by the government, is mainly used for the electronic identification of a natural person. Besides, it can also be used as a passport substitute for traveling to certain countries, and the digital signature function can also be activated. The eID card contains the following personal data of the cardholder, and all of them excluding height, eye color, and signature are also stored in the RF chip: (1) Surname and name at birth; (2) First name(s); (3) Doctoral degree;(4) Date and place of birth; (5) Photograph; (6) Signature; (7) Height; (8) Eye color; (9) Address; (10) Nationality; (11) Serial number; (12) Religious name, pseudonym.

2) Security mechanism: The security mechanism is held to protect the personal data in the card from being accessed without authorization. Besides, it is also required to ensure the authentication of the cards to protect against forgery. There are four basic protocols adopted during the general authentication procedure:

a) Password Authenticated Connection Establishment (PACE): the bearers need to verify themselves by entering the six digits secret "Personal Identification Number" (PIN)

b) Passive Authentication (PA): it is used to check if the data on the chip is authentic and unforged.

c) Terminal Authentication (TA): the readers need to transmit their access permission to the chip for reading sensitive data. Otherwise, they cannot read those data

d) Chip Authentication (CA): it will establish a secure connection between the chip and the reader for the following communication.

E. Case study in Croatia [20]

Croatian eID system, eOI, was issued on 8th Jun. 2015, which comprises national identification and authentication system (NIAS), OIB system, eID card, and the Croatian eID Identity Provider (HR eID IdP). The eID card, manufactured by state-owned company AKD d.o.o, contains name, gender, citizen, birthday, picture, signature, residence, personal ID of the owner with other information about the issuer and expiry date on its surface, while its chip stores the authentication certificate (RSA 2048 key), signature certificate (RSA 2048 key), respectively protected by one PIN code. The afore- mentioned personal information enables proof of identity, digital signature, and access to all of the e-citizen services.

Besides two RSA 2048 keys, the card in ID1-Format with the chip achieving ISO 7816, ISO/IEC 7810, and EN 419 211 criteria also guarantee the security properties of the eID system. Furthermore, the Identity Card Act enforced on 2nd Jun. 2015 with other Acts (e.g. Personal Data Protection Act) assure the public of the privacy and sufficient legitimacy.

1) Application: Croatian citizens should first go to the designated police office with certain identification documents and fill out a specific form, as well as consent to the obligation of the eID system. Different certificates and functions could be selected dependent on different age groups. Applicant data will further be tackled by the government and manufacturer with a secure channel. Finally, the eID card with an initial PIN code could be retrieved from the police officer. Users should utilize initial PIN code to log in the OIB system and set their two PIN codes for the two certificates as well as one PUK code as the password for the whole system.

2) NIAS Authentication. When the user requests authentication to NIAS, NIAS would first require the user to select one credential utilized to authenticate. NIAS then sends a SAML request to an authentication provider containing that credential. After authentication, the provider would return a signed SAML Response package to the NIAS with OIB, which could be leveraged to retrieve other user attributes from OIB Register. Eventually, the user gets access to the requested service. All the above communications are encrypted with TLS protocol and some with symmetric encryption by 3DES keys, which definitely guarantee the security of the eID system.

3) e-citizens services: With the eID, a large number of ser- vices provided by e-citizens are accessible to the Croatian [22], such as tax service, e-certificate application, public consultation participation, and prescription reviewing. Interestingly, parents are capable to check their children's grades with the eID.

F. Potential Risks

The main reason that makes people be doubtful of eID is security and privacy hazards. The governments must ensure every aspect, such as IC card, card reader, and web application, is under security guarantees. Middleware is a program that provides single APIs to interact with the card reader. Many potential risks are related to middleware. The following are some common security breaches of eID systems [31]:

1) Single sign-on authentication: Because some implementations of eID cards only require PIN code for the first authentication. This is especially dangerous when clients use the same device to access different services simultaneously.

2) Unrestricted release of personal data: Some IC cards did not use PIN code to protect sensitive information, e.g. identity, address, and picture files on the cards.

3) Identity theft: If the identity file is not well-protected, malicious applications can copy the file to another smart card. Moreover, some middleware stores the authentication and signing certificates in persistent memory, which can be stolen by malicious programs.

4) Fake signature: IC card cannot execute the hash function by itself. After middleware authorizes and calculates hashes on the document, the card just blindly signs the data. This means that malicious middleware can let the card sign whatever it wants.

Another risk occurs in eID Online Authentication, which was proposed in [4]. They made the following assumptions:

1) The attacker does not have local-system-leveled access to the user's system, eID server and web application server.

2) The attacker can trigger the client application to connect to a destination specified by the attacker (via social engineering or DNS spoofing).

3) The attacker is in the middle of the connection between the victim, the web application server, and the eID server.

Under these assumptions, they proposed two kinds of attacks: attacker between web browser and web application, and between middleware and eID server.

G. Real-world attack events

The following are some well- known attack events:

1) 2007: DDoS attack from Russian Government toward Estonian eID system [36].

2) 2010: Security flaw discovered in German eID card software (spoof attack) [37].

3) 2017: In Estonia, 760,000 state-issued eID cards with faulty chips were vulnerable to malware (identity theft) [38].

H. Challenge of eID

To evaluate an eID system, the usage rate and popularity are most representative. However, security and privacy issue is not the only factor that affects the system. We refer to some articles online [30] and sort out a few possibilities to make a more comprehensive understanding of the eID.

Firstly, in some countries, such as the U.S., Mexico, and Brazil, the eID systems are not held officially. That is to say, various eID systems may coexist and disperse the user population and lead to bad usability. Secondly, many eID systems in progress have limited functionality, which may reduce the user's frequency of use and makes itself not easy to

use for the users. Lastly, the policy of application may also influence the utilization of the eID system. If the users need to spend a lot of effort to get the new card, then many of them may give up.

These are not the only challenges the eID system may encounter, yet they point out the primary threat we need to handle rigorously.

I. eID in TAIWAN

Due to the insufficiency of security and the excessive disclosure in old ID cards as well as the low application rate of Citizen Digital Certificate [21], the Taiwanese government determines to issue national eID in 2020. Although the issuing is deferred owing to widespread criticism and the outbreak of COVID-19, a lack of declaration of eID-related information triggers vexation in public.

The explicit content on the surface of the Taiwanese eID card includes name, ID number, date of birth, residence, and marital status of the owner. Other personal information, encompassing the name of spouse, parents' name, birthplace, gender, and picture, with signature certificate (RSA 2048 key) are protected by disparate PIN code and stored in the chip. The eID card also reaches ISO 7816, iso 29115, and FIPS140-2 criteria with no expiry date. The whole system is composed of T-road, eID card, Ministry of the Interior (MOI), and Household Registration Office [21, 29].

However, merely two Articles in the Household Registration Act support the Taiwanese eID scheme [39]. Besides, the anonymity of the manufacturer and the ambiguous description of T-road lead to the uncertainty of security and privacy properties.

J. eID Guideline

After comprehensively analyzing the eID systems in four mentioned countries, we eventually propose an eID guideline. See Table 3. The eID schemes of these four countries with the one in Taiwan are all re-evaluated by our guideline. Noticeably, Taiwanese eID reaches none of the criteria in the section of system and others, which definitely demonstrates the insufficient preparation of eID issuing.

Card related criteria

1) Contain necessary information only. The eID card should not contain unnecessary information to avoid excessive disclosure. For example, the "marital status" and the "parents' name" in Taiwanese eID cards as well as the "eye color" and "pseudonym" in German eID cards, seem redundant. However, if they are domestically necessary, saving them in the chip with PIN code protection may be a solution.

2) Save other important information in chip. Important and sensitive personal information would be recommended being saved in the chip but not directly shown on the surface of the eID card. Only Taiwanese eID cards achieve this property.

3) Require PIN code to access information in chip. A self- defined PIN code should be required to access the information in the chip to avoid any disclosure when the eID card is found by strangers.

4) Require PIN code to use Digital Signature. A self-defined PIN code is necessarily required to perform digital signature. This the definitely the basic security property that an eID card should achieve.

5) Allow user to set PIN code privately. It is necessary for citizens to set their own PIN code privately but not at a public location such as Household Registration Office or police office.

6) Expire in a well-defined time. Although the key would not be compromised easily, it is recommended that the eID card should expire in a well-defined time to prevent any damage of hardware, which could be regarded as the periodical inspection.

7) Utilize safer key. The key utilized in the eID system should be cryptographically secure, for example, an RSA 2048 bits key, avoiding to be compromised easily.

8) Allow different function choice. It is recommended that there should be different choices of function for different age groups. For example, the digital signature is actually unnecessary for adolescence.

9) Credible manufacturer. A credible manufacturer is paramount for an eID system to be trustworthy enough to the public.

System related criteria

10) An open-source system. The whole eID system is recommended to be overt enabling the examination from specialists. For instance, Estonia did divulge the implementation of all their eID system on GitHub.

11) Communication with encrypted data. All the compartments in the eID system should communicate with each other with encrypted packages. This is definitely a necessary property that should be achieved.

12) Controllable permission between departments. The citizens should fully have control over the permission of their personal data. Any department within the government could not access to those data without personal agreement.

13) Credible database and server. The server storing all the personal sensitive data should be credible enough, or will definitely compromise both security and privacy.

14) Not accessible outside government. Any institution out- side the government, such as the banks, should not be able to access those personal data to guarantee enough security and privacy properties.

Other criteria

15) Versatility. The eID system is recommended to be versa- tile that could combine many systems making life more convenient, or it will be not attractive enough for citizens to accept this new technology. For example, eID can combine with application in a mobile phone.

16) Usability. Usability is similar to versatility, but this property focuses on if citizens would consider the eID actually trouble. Citizens would not accept the eID if any process within the system is too complicated and confusing. For example, the eID system in Mexico was terminated due to atrocious usability.

17) Sufficient legitimacy. Sufficient legitimacy is necessary to support the eID system. Related regulations could guarantee and ensure the security and privacy properties of the eID system.

18) Penalty and obligations. There should be penalties if citizens violate any obligation that they agreed to when applying the eID, which might, for example, preclude the citizens from illegally selling their eID and compromise all the system.

19) Transparency. It is recommended that all the eID systems or related regulations and information should be transparent enough for everyone to inspect the system and avoid suspicion from the public.

TABLE III. EID GUIDELINE

Card related criteria	**EE**	**BE**	**DE**	**HR**	**TW**
Contain necessary information only	O	△	△	O	△
Save other important information in chip	X	X	X	X	O
Require PIN code to access information in chip	X	X	O	O	O
Require PIN code to use digital signature	O	O	O	O	O
Allow user to set PIN code privately	O	O	O	O	NA
Expire in a well-defined time	O	O	O	O	X
Utilize safer key (e.g. RSA 2048)	O	O	O	O	O
Allow different function choice	O	O	NA	O	NA
Credible manufacturer	O	O	O	O	NA
System related criteria	**EE**	**BE**	**DE**	**HR**	**TW**
An open-source system	O	△	X	X	X
Communication with encrypted data	O	O	O	O	NA
Controllable permission between departments	△	NA	NA	NA	NA
Credible database and server	O	O	O	O	X
NOT accessible outside government	O	O	O	O	X
Other criteria	**EE**	**BE**	**DE**	**HR**	**TW**
Versatility (e.g. combine with app)	O	O	O	O	X
Usability	O	O	O	O	NA
Sufficient legitimacy	O	O	O	O	X
Penalty & Obligations	O	O	O	O	X
Transparency	O	O	△	△	X

EE: Estonia; BE: Belgium; DE: Germany; HR: Croatia; TW: Taiwan

K. Issuing Taiwanese eID or not

Absolutely, the Taiwanese would live a more convenient life after eID issuing. Other advantages, for example, reduction of direct disclosure from ID card, embedded digital signature function, alleviation of the risk of identity spoofing, are also beneficial to the public. However, the convenience should not compromise any of the security and privacy properties, and several potential problems, for instance, unknown application process, insufficient legitimacy, and scarce of information disclosure, still exist. With the aforementioned eID guideline, it is obviously urgent and paramount for the Taiwanese government to elucidate and explain every implementation detail to the public before issuing eID rashly.

IV. RELATED WORK

Recently, there are several studies investigating the popular eID system as this study. However, most of them either focus on the privacy or security issues theoretically without considering what schemes are actually implemented in different countries or specifically inspect the scheme in one or few countries without transnational analysis [39, 40, 41, 42, 43, 44].

A large number of studies focus on introducing the eID scheme in a specific country such as [7, 12, 15, 18, 26] investigating the eID system in Estonia, Finland, Germany, Belgium, Spain, respectively, which would be helpful to comprehend the eID scheme in those counties with the disadvantage of no comparison.

Reference [1] summarized several eID systems implemented in European countries including the UK, Austria, and Belgium. Strangely, Estonia, the earliest country implementing national eID, was not mentioned at all, which definitely compromised its credibility.

Reference [16] conducted a general survey that theoretically presented privacy features of national eID systems discussing several ways to protect personal information, such as encryption, authentication, and verification-only mode. Nevertheless, it didn't mention which cryptographic methods could be utilized to achieve those privacy features and either the pros and cons when using each cryptographic mechanism.

An in-depth study scrutinizing the privacy issues of the eID system with e-service was presented by [27]. This study disclosed several problematic unbalanced aspects of the Estonian e-service, e-residency, that some privacy properties were compromised by ensuring the security, which did also conflict Estonian national regulatory framework. Albeit only the Estonian scheme was discussed, this was the first study that deeply investigated the legitimacy issues of eID.

Several attacks against eID are also investigated recently, for example, the Coppersmith's attack proposed by [2]. In Taiwanese eID system (Citizen Digital Certificate), there was a fatal flaw in key generation function, leading to a remarkable loss of entropy in 1024-bit public and private key pairs. 184 keys could be broken in hours by combinations of Coppersmith's attack and some other methods.

Another vulnerability was disclosed in 2017 by [17]. Because of the flaw in the Infineon RSA public-key cryptography library, which is used in many countries' eID systems, adversaries could break 1024-bits key in three months and 2048-bits key in less than 100 years, respectively. After the discovery of this vulnerability, Estonia transferred to use an elliptic-curve crypto-system, whereas Slovakia moved on to generate RSA keys longer than 2048-bits.

Unfortunately, there are few studies comprehensively discussing the privacy and security issues outside cryptography, which is too limited when it comes to national eID. Besides, it is definitely urgent to establish a general guideline to evaluate those eID schemes and provide recommendations for those governments intending to issue eID.

V. CONCLUSION AND FUTURE WORK

By investigating the implementation detail of the eID system in several countries, we propose an eID guideline that could be utilized to evaluate any eID scheme and enable the perception of potential security and privacy problems. As the progress of technology, the government of many countries, including Taiwan, start to issue eID to allow many e-services that substitute in-person process for e-service. This unprecedented guideline would definitely be beneficial to those governments to evaluate their eID scheme before issuing. Revealed by this guideline, the Taiwanese eID scheme requires more improvement due to several potential security and privacy issues.

Besides, the Taiwanese government should release more related information to allow comprehensive evaluation.

However, in this work, only four countries are involved and explored to establish the guideline. Furthermore, all these four countries are in Europe, which might curtail the generality and make the guideline ineffective. In the future, more case studies with enough variety should be executed for constructing a general eID guideline.

ACKNOWLEDMENTS

Thanks Ms. Antonela Basic for providing the personal experience of using Croatian eID system.

REFERENCES

[1] Arora, Siddhartha. “National e-ID card schemes: A European overview.” Information Security Technical Report 13.2 (2008), pp. 46-53.

[2] Bernstein, Daniel J., et al. “Factoring RSA keys from certified smart cards: Coppersmith in the wild.” International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2013.

[3] Chen, Jhang, Yan, Sie, and Li. “Ministry of the Interior went to Estonia to investigate the smart government digital services,” 2019. https://report.nat.gov.tw/ReportFront/ReportDetail/detail?sysId=C10801167.

[4] Dietrich, Christian J., Christian Rossow, and Norbert Pohlmann. “eID online authentication network threat model, attacks and implications.” 19th DFN Workshop 2012.

[5] De Cock. “eID Security,” KU Leuven ESAT/COSIC, 2019.

[6] Danny De Cock. Belgian eID cards and ePassports. 2014. https://homes.esat.kuleuven.be/decockd/slides/20140424.belgian.eid.cards.and.epassports.pdf.

[7] De Cock, Danny, Karel Wouters, and Bart Preneel. “Introduction to the Belgian EID card.” European Public Key Infrastructure Workshop. Springer, Berlin, Heidelberg, 2004.

[8] E-estonia. id-card, 2019. https://e-estonia.com/solutions/e-identity/id-card/.

[9] Wolfgang Ettlinger. My Name is Johann Wolfgang Von Goethe-I can prove it. SEC Consult, 2018. https://doi.org/en/blog/2018/11/my-name-is-johann-wolfgang-von-goethe-i-can-prove-it/

[10] Bundesamt für Sicherheit in der Informationstechnik. The electronic ID card, 2020. https://www.bsi.bund.de/EN/Topics /ElectrIDDocuments/-eIDcard/ eIDcard_node.html

[11] Bundesamt für Sicherheit in der Informationstechnik. Electronic ID documents, 2020. https://www.bsi.bund.de/EN/Topics/ ElectrIDDocuments/EIDnode.html

[12] Heichlinger, Alexander, and Patricia Gallego. "A new e-ID card and online authentication in Spain." Identity in the Information Society 3.1 2010, pp. 43-64.

[13] ISA. What are certificates? 2012. https://www.id.ee/index.php?id=31015.

[14] Lips, Silvia, et al. “Key factors in coping with large-scale security vulnerabilities in the eID field.” International Conference on Electronic Government and the Information Systems Perspective. Springer, Cham, 2018.

[15] Martens, Tarvi. “Electronic identity management in Estonia between market and state governance.” Identity in the Information Society 3.1, 2010, pp. 213-233.

[16] Naumann, Ingo, and Giles Hogben. “Privacy features of European eID card specifications.” Network Security 2008.8, pp. 9-13.

[17] Nemec, Matus, et al. “The return of coppersmith's attack: Practical factorization of widely used rsa moduli.” Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017.

[18] Noack, Torsten, and Herbert Kubicek. “The introduction of online authentication as part of the new electronic national identity card in Germany.” Identity in the Information Society 3.1, 2010, pp. 87-110.

[19] Republic of Estonia Police and Border Guard Board, Estonian eID scheme:ID card, 2018.

[20] Ministry of Public Administration, Overview of the Croatian eID scheme. Ministry of Public Administration Republic of Croatia, 2018.

[21] Ministry of the Interior, R.O.C (Taiwan), electronic identity card, 2019.

[22] Government of the Republic of Croatia, The e-citizens system, 2020. https://vlada.gov.hr/the-e-citizens-system/15215.

[23] Ong, Sean, “Evaluating the Security of National Electronic Identification Programs,” 2018.

[24] Ottis, Rain. “Analysis of the 2007 cyber attacks against estonia from the information warfare perspective.” Proceedings of the 7th European Conference on Information Warfare, 2008.

[25] Estonian Police and Border Guard Boar. Applying for an ID card for an adult, 2020. https://www.politsei.ee/en/instructions /applying-for-an-id-card-for-an-adult.

[26] Rissanen, Teemu. “Electronic identity in Finland: ID cards vs. bank IDs.” Identity in the Information Society 3.1, 2010, pp. 175-194.

[27] Särav, Sandra, and Tanel Kerikmäe. “E-residency: a cyberdream embodied in a digital identity card?.” The Future of Law and eTechnologies. Springer, Cham, 2016, pp. 57-79.

[28] Stalder, Felix, and David Lyon. Electronic identity cards and social classification. London: Routledge, 2003.

[29] National Development Council (Taiwan), T-road explanation, 2019.

[30] Trulioo. A Snapshot of Digital ID in the 10 Most Populous Countries-Part2, 2019. https://www.trulioo.com/blog/digital-id-populous-countries-2/.

[31] Gritzalis, Dimitris, and Javier Lopez. Emerging Challenges for Security, Privacy and Trust: 24th IFIP TC 11 International Information Security Conference, SEC 2009, Pafos, Cyprus, May 18-20, 2009, Proceedings. Vol. 297. Springer, 2009.

[32] Wikipedia. List of national identity card policies by country. Online; accessed 01-June-2020, https://en.wikipedia.org/wiki/List-of-national-identity- card-policies-by-country.

[33] Ministry of the Interior, R.O.C (Taiwan). 內政部：因應疫情調整數位身分證換發時程, 2020. https://www.moi.gov.tw/chi/chi_news/news_-det-ail.aspx?sn=17841.

[34] Taiwan Association for Human Rights. 【連署】反對全面換發晶片身分證, 2020. https://www.tahr.org.tw/news/2648.

[35] Verhaeghe, Pieter, et al. "Security and privacy improvements for the belgian eid technology." IFIP International Information Security Conference. Springer, Berlin, Heidelberg, 2009.

[36] Kertu Ruus. “Cyber War I: Estonia Attacked from Russia”. European Affairs: Volume number 9, Issue number 1-2 in the Winter/Spring of 2008.

[37] Pierluigi Paganini. Flaw allowing identity spoofing affects authentication based on German eID cards. Securityaffairs, 2018. https://securityaffairs-.co/wordpress/78314/hacking/german-eid-cards-hack.html

[38] Silver Tambur. Possible security risk affects 750,000 Estonian ID-cards. Estonian world, 2017. https://estonianworld.com/technology/possible-security-risk-affects-750000-estonian-id-cards/

[39] Ministry of the Interior, R.O.C (Taiwan), 數位身分識別證(New eID)簡易問答集, 2019.

[40] W. J. A. Al-Nidawi, et al. "Review on national electronic identification system," in proceeding of the international conference on advanced computer science applications and technologies, 2015, pp.228-233.

[41] ITU-T Focus Group Technical Report, "Review of National Identity Programs," International Telecommunication Union, 2016.

[42] Technical Report, "Study on the use of Electronic Identification (eID) for the European Citizens’Initiative," everis, 2017.

[43] A. Windisch and A. Müller. "E-Identity Solutions in Europe - An european overview," ASQUARED, 2018, pp.1-16.

[44] V. Tsap, et al. "Factors Affecting e-ID Public Acceptance: A Literature Review," in proceeding of the international conference on electronic government and the information systems perspective, 2019, pp.176-188.

[45] S. Hohmann, et al. "Identifying factors of e-government acceptance - A literature review," in proceeding of the international conference on information systems, 2012, pp.1-19.