Biometric Verification on e-ID-Card Secure Access Devices: A Case Study on Turkish National e-ID Card Secure Access Device Specifications

Atila Bostan[‡], Gökhan Şengül, K.Murat Karakaya

Computer Engineering Dep., Engineering Faculty, Atılım University, Kızılcaşar Mah. İncek-Gölbaşı/Ankara-Turkey

[‡] e-mail: atila.bostan@atilim.edu.tr

Abstract- Biometric verification on e-ID cards requires clear procedures and standards be defined, especially when the access devices are anticipated to be produced commercial companies. Turkish national e-ID card project has reached the dissemination step. Now the commercial companies are expected to produce and market e-ID card access devices which will conduct secure electronic identity verification functions. However, published standards specifying e-ID card-access-device requirements are ambiguous on biometric verification procedures. In this study, we intended to attract scientific interest to the problems identified in the current design of biometric verification on Turkish national e-ID cards and proposed several verification alternatives which enables the production of e-ID card access devices in a commercial-competition environment.

Keywords- e-ID cards; biometric verification; Turkish national e-ID cards.

1. Introduction

Electronic Identification Cards (e-ID) are getting prevalent in most of the countries worldwide. Especially EU member countries are speeding up on the transition to e-ID, since the recognition of e-IDs in EU member counties will be mandatory as of 29 September 2018 [1]. Turkey has started handling of national e-ID cards to citizens in early 2017 and plans to complete initial distribution until 2018 [2].

The motivations behind Turkish transition to e-ID cards are listed as; [2]

- providing means for secure identity verification
- preventing citizens from unjust-treatment as a result of identity fraud
- easing the access to e-government services
- be used for travel document (for the destinations exempt from visa)
- be used in e-signature process
- increasing the citizen satisfaction and service quality in community services
- reducing the amount of financial loss due to the personal incompetency in identity

Turkish e-ID cards support three discrete identity verification alternatives, namely visual, electronic and biometric verification methods. Hence, they should have secure and enough number of evidences in order to assure these verification alternatives.

On the other hand, secure card access devices need to be developed and produced, in order to have functional and widespread usage of e-ID cards. Card access devices should guarantee certain level of security and should support different methods for identity verification. Additionally, for some financial, maintenance and commercial reasons, they are preferred to be produced by the companies in the industry. So that there is a strong requirement for descriptive, functional and measurable standard specifications, since these devices are expected to use e-ID cards which is developed and produced by the General Directorate of Civil Registration Services and should guarantee certain security levels. In order to design and produce a compatible e-ID card access device, companies need to know supported communication alternatives by the e-ID card and the structure of the data which can be accessed. Furthermore, companies should know the security requirements to support the demanded security levels. With the intention to meet these industry requirements, Turkish Standards Institute published four standards explaining the specifications for secure e-ID card access devices in 2013 and updated in in 2017 [3,4,5,6]. Although, the physical and electronic specifications of the smart cards which are referred by e-ID card access device standards are specified in another series of standards [7,8,9], they are not scrutinized in this study.

In secure e-ID access device specification standard series, there are 11 identity verification alternatives listed [10]. Depending on the assurance requirements of the application, the choice in between these verification alternatives is expected to be made by the verifier or be imposed by verification-policy server. Biometric data on e-ID is to be used in 3 out of 11 identification verification alternatives [10]. Even though a passport-size photograph of the card holder is stored in the e-ID card content, it is not referred as biometrics in the standard series, since it is planned to be used only for visual verification alternatives. These 3 biometric verification methods are named and listed as follows in the standard series [10].

- Method 5: Verification on secure access device by using biometrics.
- Method 10: Verification on secure access device by using PIN and biometrics.
- Method 11: Verification on secure access device by using PIN, biometrics and photograph of the card holder.

However, 3 identity verification methods are defined in the standards, the structure for the biometric data in the e-ID card is not mentioned [5,6]. Hence the device developers face a compatibility problem in design.

In this study, we propose solution alternatives with a comparison on advantages and disadvantages for biometric information storage and retrieval in e-ID cards. Because no rationale is published on the effective policy requirements in designing and in texting the standards, we interpret our predictions as the reasoning.

2. Privacy and Security Considerations

The design of Turkish national e-ID cards was conducted by The Scientific and Technological Research Council of Turkey (TÜBİTAK). Following the technological feasibility, functionality, pilot usage and security studies, actual production and dissemination of e-ID cards were commenced. Published standards are one of several outcomes of these studies as well. So that, the definitions, methods and specifications in standards were assumed to be well studied and tested.

Apparently, e-ID cards are instruments with high privacy and security requirements. The content of the card is strongly private and sensible to exploitation. It goes without saying, security and privacy considerations should take precedence in e-ID card specifications.

In line with the specifications in current secure e-ID card-access-device standards, we consider the rationale in not specifying the biometrics data structure and feature sets which are used in Turkish national e-ID cards is the secrecy. Since keeping these parameters secret, would bring significant level of a support for the security of the biometric information, without doubt, until those are discovered. Furthermore, if biometric feature data are accessed then it is possible to use them for malicious or fraudulent purposes either as feature data or by reproducing the biometric input from them.

Nevertheless, the most important security risk in biometrics is their unsuitability for revocation and cancellation. In all of the identification instruments used in security domain, biometrics has the hardest problem in cancellation and revocation. It is typically easy to cancel or revoke passwords, tokens or digital-certificates when needed. But it is not the case for the biometrics. It is impractical for one to revoke his finger-print and change to a new alternative. This characteristic increases the privacy and security requirements for the biometrics. Anyhow, people have limited number but static biometric information. One can change his password, token or digital-certificate to any one he chooses from a theoretically infinite alternative pool. But for the biometrics, options are limited especially for hand and retina vein maps.

3. Problems with The Current Design

Turkish national e-ID card access devices should meet a set of security requirements, such as blocking the remote access, keeping specific event/user logs and being temper resistant etc. In order to certify whether the devices meet these requirements, they are obliged to Common Criteria (CC) tests with a predefined protection profile [11]. In short, e-ID card access devices should be secure and resistant to a set of predefined security attacks. By their specification, they are bind to use an embedded cryptographic smart card (referred as Secure Access Module-GEM) to store security sensitive data such as private keys, signature certificates and perform several security operations such as authentication, signing etc. Secure Access Modules are planned to be provided by TÜBİTAK following the CC certification.

In all 3 identity verification methods that are specified by the standards, biometric verification is planned to be conducted either on e-ID access device or in biometric sensor. Although implementing one way of the verification is adequate for meeting the standards, both ways are supported. However, these biometric verification alternatives are problematic from the point of card access device production.

If the producer opts for on-device verification alternative, then the data structure and feature notation of the biometrics should be known by the designer. Since, with the purpose of verifying the identity, the device is supposed to compare the scanned biometrics with the biometric data which is read from e-ID card, assuming proper access rights such as PIN and/or certificates are provided. Nevertheless, the data structure and the feature notation used in e-ID card for biometrics is not published. This means, e-ID card access device producers will not be able to develop a verification system running on the device.

On the other hand, if the producer opts for verification on biometric sensor, then acquiring a sensor which can process biometric-data with the structure used in e-ID cards will be needed. As it is with the previous option, without the knowledge of the data structure used in e-ID cards, acquiring a proper sensor is problematic.

Moreover, cancellation or revocation of biometric data is not supported with the current verification and usage. Even though biometric data is problematic in cancellation and revocation processes, there can be several algorithmic alternatives to support these procedures as well.

4. Proposed Alternatives to Biometrics Storage and Processing

We are quite aware of the fact that finding a solution that would solve all the listed problems without bringing about new ones is not realistic. However, in this study, we wanted to list several alternatives that can be commercially implemented and produced by no additional security risks but with some functionality and processing degradation. In brief, we focused on commercially productivity of e-ID card access devices. Below the alternatives for biometric verification of e-ID card-holder are listed with some basic explanations on each of them. In the next section, advantages and disadvantages (additional requirements) are given to help in comparison and decision making.

4.1. Alternative 1: Verification on a remote server

In this alternative, biometric verification will be conducted on a government-controlled server. E-ID access devices will transmit citizen (or card identity) along with the scanned biometrics without processing (as a digital image) to a secure biometrics-verification server and receive the verification result. No biometrics will be stored on e-ID card. Access device and the sensor do not need to process biometrics.

4.2. Alternative 2: Encrypted storage of biometrics

This alternative requires the knowledge of biometric data structure. However, getting access to the biometrics will necessitate another security step other than PIN. For the encryption a symmetric key which is encrypted by card-holder's public-key may be utilized for computation convenience, otherwise encrypting biometrics by the public-key can be an option. This encryption will enable an indirect cancellation and revocation of biometrics when public-private keys are updated.

4.3. Alternative 3: Provision of a dynamic library

A dynamic library code can be provided by the government agency (namely TÜBİTAK) to process the biometrics and run verification algorithm to the access device producers. In this alternative, biometric data structure used in e-ID cards does not need to be known by the access device producers and several types of sensor data formats and biometric features can be supported. Biometrics storage structure and verification details will be hidden to access device producers. The dynamic library can be stored and run on the Secure Access Module (GEM) card or otherwise on access device itself.

4.4. Alternative 4: Biometric hash usage

A combination of alternative 1 and 2 with some modifications can be used in e-ID biometric verification process. In this alternative biometric data structure is publicly shared with the access device producers, so that access devices can verify the scanned biometrics. But a central validity check is introduced to the process steps with a minimum network and communication overhead. For central verification a hash of the biometric data on e-ID card is to be transmitted to a government controlled validation server and validity result is received. This mode of operation enables the cancellation and revocation of biometrics.

5. Comparison of the Alternatives

As we have mentioned in the previous section each biometric verification algorithm has its own advantages and disadvantages. In this section we list the advantages and disadvantages of the current and proposed mode of operations in biometrics verification by using e-ID cards. Listed advantages and disadvantages are due collection of the reviews of the authors.

5.1. Current running mode

Advantages;

- Local verification of biometrics
- No need for a network connection
- No need for a central service
- Biometric data storage structure s hidden from access devices

Disadvantages

- Access devices cannot be produced by commercial companies without sharing the biometric data and verification algorithm specifications
- Biometrics cannot be cancelled or revoked
- Parameters for sensor acquisition is not set. Suitable sensors cannot be acquired.
- Commercial competition is not supported among access device producers

5.2. Alternative 1

Advantages

- No need to sore biometrics on e-ID cards
- No need to share biometrics storage structure
- No need to share the verification algorithm specifications
- Sensor specifications can be shared with a minimum set of requirements
- Cancellation and revocation of the biometrics are enabled
- Access devices can be produced by commercial companies
- Supports commercial competition among access device producers

Disadvantages

- No local biometric verification

- Requires a secure central high performance service
- Requires a network connection

5.3. Alternative 2

Advantages

- Biometric storage structure can be shared
- Getting access to biometrics requires an additional security procedure
- Fraudulent usage risk of biometrics is reduced, especially without existence e-ID card
- Local biometric verification
- No need for a network connection
- No need for a central service
- Sensor specifications can be shared with a minimum set of requirements
- Cancellation and revocation of the biometrics are enabled by the change of encryption key
- Access devices can be produced by commercial companies
- Supports commercial competition among access device producers

Disadvantages

- Requires a decryption step in biometric verification process
- Biometric storage structure will be revealed
- Verification algorithm specifications should be published

5.4. Alternative 3

Advantages

- Biometric storage structure is hidden
- Verification algorithm specifications is hidden
- Local biometric verification
- No need for a network connection
- No need for a central service
- Sensor specifications can be shared with a minimum set of requirements
- Access devices can be produced by commercial companies
- Supports commercial competition among access device producers

Disadvantages

- Requires a dynamic library and communication parameters be developed
- Requires secure and reliable distribution of dynamic library
- Additional measures are needed to enable cancellation and revocation of biometric data

5.5. Alternative 4

Advantages

- Cancellation and revocation of the biometrics are enabled by the usage of central verification server

Disadvantages

- Biometric data structure will be revealed
- Verification algorithm specifications should be published
- Requires a secure central verification service
- No local verification
- Requires a network connection

6. Conclusions

Developing secure e-ID card is not always a simple process. It necessitates a series of critical decisions to be made, tests to be conducted and production to be coordinated. Turkey is about the end of her transition to national e-ID card usage. Distribution of e-ID cards to citizens started in 2017 aside from some previous and local pilot studies. At the current step, commercial production of e-ID card access devices are anticipated, following the standards publication. But this step is not problematic with the current design of usage which is specified in the standards.

The most important problem in the current specifications is in the biometric verification process, since the ambiguity in this process blocs the production of secure e-ID access devices. In this study, we proposed 4 alternatives for the biometric verification process on e-ID cards. Our focus is to enable the production of access devices while enabling commercial competition. We have listed our proposed mode of operations with their respective advantages and disadvantages.

We fairly admire the existence of several administrative, financial and technical constraints. In this kind and size of a projects firm constrains are generally inevitable. However, the current running mode as it is depicted in the standard series does not enable commercial development of the Turkish national e-ID card secure access devices. With the intention to attract focus on the problem and provide several plausible solutions we have conducted this research. Excluding the other possible considerations, from a technical perspective, our evaluation points to alternative 3 for a plausible solution.

Acknowledgements

This paper was presented at International Security and Cryptology Conference Turkey 2017 (ISCTurkey 2017).

References

[1] European Commission, Digital single market - e-Identification, accessed online from https://ec.europa.eu/ digital-single-market/en/e-identification, on 12.08.2017

[2] Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, Yeni Kimlik Kartları, accessed online from http://www.ekds.org/, on 12.08.2017

[3] Turkish Standards Institute, TS 13582 Secure card access devices for Turkısh national identity cards- overview.

[4] Turkish Standards Institute, TS 13583 Secure card access devices for Turkish national identity cards- interfaces and their characteristics.

[5] Turkish Standards Institute, TS 13584 Secure card access devices for Turkish national identity cards- security specifications.

[6] Turkish Standards Institute, TS 13585 Secure card access devices for Turkish national identity cards KEC application software specifications.

[7] Turkish Standards Institute, TS 7246 EN ISO IEC 7810 Identification cards- Physical characteristics.

[8] Turkish Standards Institute, TS ISO/IEC 14443-1 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics.

[9] Turkish Standards Institute, TS ISO/IEC 14443-2 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 2: Radio frequency power and signal interface.

[10] Turkish Standards Institute, TS 13678 Electronic identity verification system - Part 1: Overview.

[11] National Research Center of Electronics and Cryptography, eID Applications Unit, Common Criteria Protection Profile for Application Firmware of Secure Smartcard Reader for National Electronic Identity Verification System.