Privacy Features of European eID Card Specifications

Authors: **Ingo Naumann, Giles Hogben**

European Network and Information Security Agency (ENISA)
Technical Department
P.O. Box 1309, 71001 Heraklion, Greece

E-Mail: ingo.naumann@enisa.europa.eu, giles.hogben@enisa.europa.eu

This article originally appeared in the Elsevier Network Security Newsletter, August 2008, ISSN 1353-4858, pp. 9-13

1 Introduction

Following the introduction of ICAO-compliant electronic passports electronic national identity cards are now being planned and deployed on a large scale in Europe as well as world-wide. Whereas electronic passports contain a contactless chip in the booklet, electronic ID cards are usually plastic cards the size of a regular ATM card, using a chip with a contactless and/or contact interface. Like the data page of a passport, an ID card is personalized with at least a serial number, a photo and the owner's name and date of birth. Some EU countries, including Austria, Belgium, Estonia, Finland, Italy, the Netherlands, Spain and Sweden have already started issuing electronic ID cards. Others, like Germany, France and UK, are currently drafting technical specifications for their future ID card schemes. Besides national ID cards, there are many other government and commercial eID card schemes, like electronic health cards or chip and signature cards.

All ID cards contain sensitive information. We refer to sensitive information in a broad sense, i.e. to include all kinds of personal, biometric, statistical and administrative information, all of which may potentially disclosed by ID cards.

Therefore, electronic identity documents might infringe the holder's privacy. In this article, we explore privacy-enhancing technologies ("Privacy Features") which can be found in existing technical specifications and European standards. We now list different types of privacy features and distinguish clearly between them even though they are usually used in combinations.

2 Cards without privacy features

If an electronic ID card does not make use of any privacy features, it contains unprotected sensitive information, accessible by any reading device (see Figure 1). In the worst case scenario, during a transaction with the reader, the service provider has unlimited access to this information.

Figure 1: ID Card without Privacy Features

3 Encrypted information

Encryption remains the most obvious way to protect the sensitive information stored on the card. In this case, the reader and the card share a secret key which the reader software might derive from a unique identification number of the card and secret system key. All personal information, or some parts of it, are stored on the card in encrypted data blocks. Every off-the-shelf system can read these data blocks but only with the knowledge of the secret key is it possible to decrypt them.

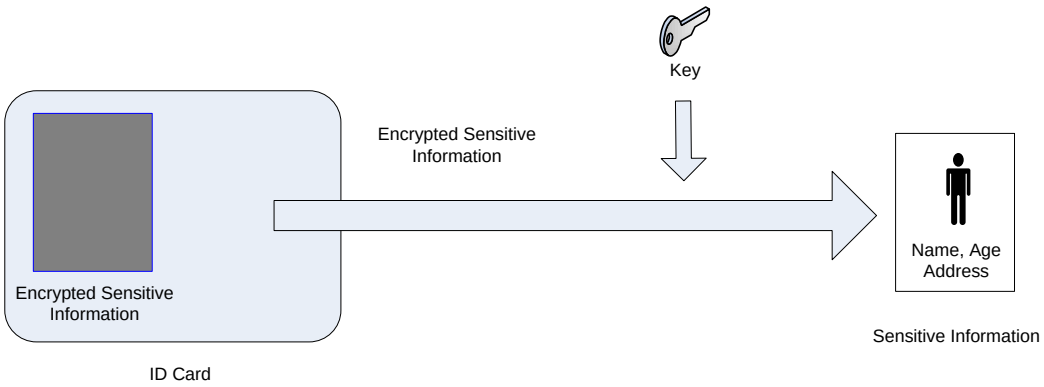

Figure 2: Encypted Data on Card

4 Access control

Another means of preventing unauthorized access to sensitive information is by applying access-control mechanisms. Typically, the card carries the data as plain text[1] but the service provider[2] only gets access to the contents after a successful authentication of the service provider and/or the cardholder. Authentication usually consists of proving the knowledge of a PIN or a secret key (see Figure 4). By entering a PIN, the cardholder authenticates themselves and also gives their consent to the access of his card. On the service-side, by proving knowledge of a secret key, the service provider is deemed authorized for the transaction (see Figure 3). The secret key may either be shared between the chip and the service provider (symmetric-key cryptography) or be the private part of a private/public key pair (asymmetric-key cryptography). In the latter case, a certificate with the public key signed by a Certifying Authority (CA) is usually sent to the card as part of the authentication. Key distribution and storage, however, very often turns out to be a tricky matter.

Some specifications define protected and unprotected areas of memory. This facilitates the deployment of many applications which do not necessarily need to have access to sensitive

[1] The data might be encrypted internally in order to protect the chip agains physical attacks [19] but this topic is not covered in this paper.

[2] In some cases, e.g. offline applications, it might be appropriate to replace “service provider” by “reading device” here; in the following, we will always refer to this entity as “service provider” and do not make this distinction.

information. The memory of a Spanish eID Card [7], for example, is divided into three areas: 1) a public zone (*zona pública*), which is accessible without restrictions, 2) a private zone (*zona privada*), which is accessible after the user has entered his secret PIN, and 3) a protected zone (*zona de seguridad*) which can only be accessed by card readers of the public administration. Sensitive personal data, like the facial image, is stored in the protected zone and therefore cannot be used by business applications.

The degree of secrecy of secret keys depends a lot on the mechanism and the assets (the "What has to be protected?"). Basic Access Control (BAC) authentication keys, for example, are derived from the Machine Readable Zone (MRZ) printed on the data page of an electronic passport (see chapter 9). In other systems, the secret keys are stored in the reading devices (for example, of the police) or in Hardware Security Modules (HSM) of background systems.

An interesting emerging area of access control mechanisms is smartcard-to-smartcard protocols. The specifications of some European Health Insurance Card systems distinguish between the Health Insure Card (HIC) of the patient and the Health Professional Cards (HPC) of the doctor [13]. The HPC needs to authenticate itself to the HIC in order to get access to the medical files stored on the card. This way, the access to the patient's health information is limited to medical personnel.

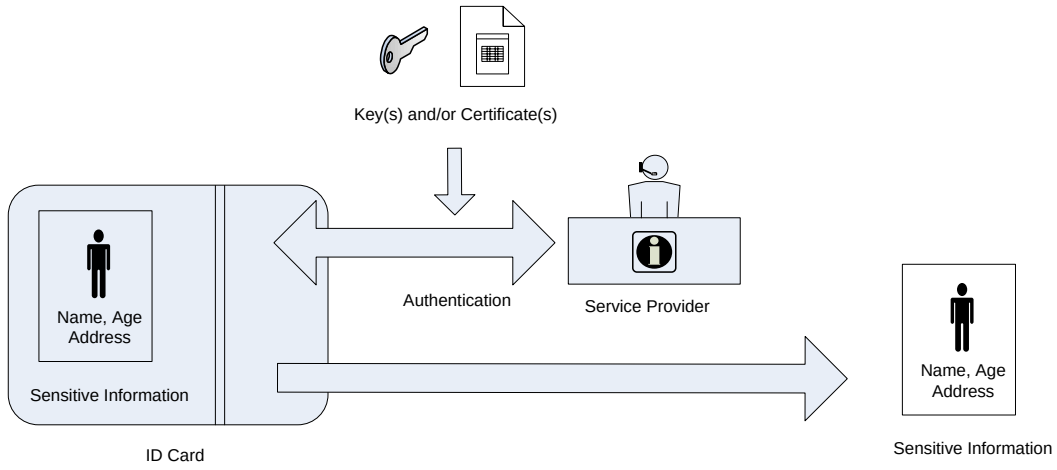

Figure 3: Access Control: Authentication of Service Provider

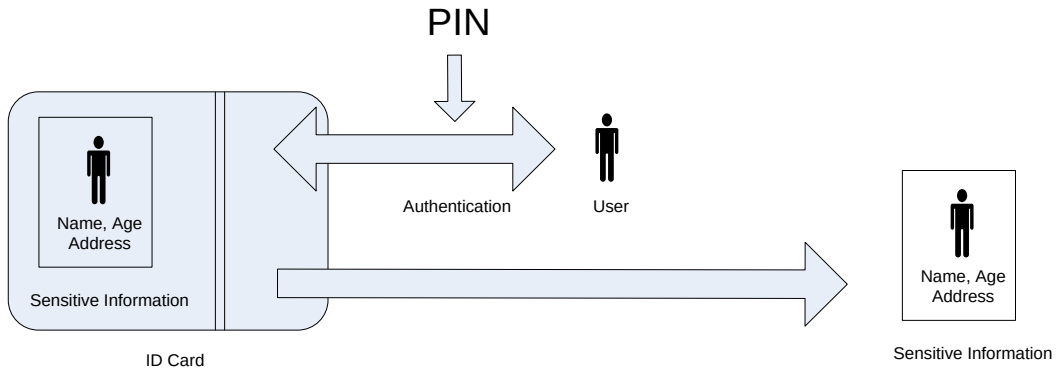

Figure 4: Access Control: Authentication of User

5 Linkability control – use of identifiers

The careful use of identifiers is crucial to controlling privacy risk. Some cards refer to citizens using UID (Unique IDs) in order to avoid the use of more privacy-invasive information like a social security number[3]. Usually, UIDs link to more information stored in a background data base.

On the other hand, a generally accessible card UID is a privacy risk even if the personal information on the card is protected by access control or encryption mechanisms. Whenever there is static data stored on the card, like a public key[4] or even an encrypted data block this might serve as an UID if it is unique. Other kinds of data, such as data exchanged during card identification and handshake with readers may also contribute to identifying card holders either uniquely or to within a small set of individuals. For example handshake protocols are able to identify the issuing country of an e-Passport. Stronger identification using combinations of such weakly identifying features should be considered in managing linkability. Furthermore, if pseudonymous identifiers are used, the size and trustworthiness of the group of parties able to resolve those identifiers should be considered.

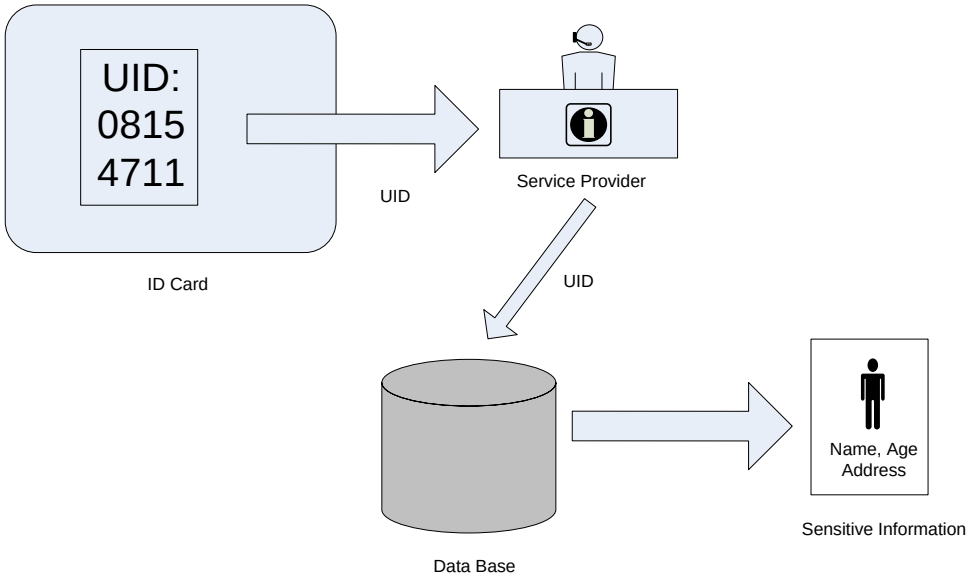

Figure 5: UIDs

6 Verification-only mode for transactions

Another way to protect sensitive information is for the card not to reveal it at all but just to *verify* certain assertions. A typical example for this approach is the match-on-card method for fingerprint information. For verification, the ID card has to be connected with a control system which scans the card holder's fingers,, generates a template and sends it to the card for verification. The card answers with a probability value that the two templates match.

A service provider (or a vending machine) might require the users to confirm they are of a certain age before providing a service or product. Typically, the card provides the date of birth in this case. A less privacy-invasive method is that the service provider "asks" the card whether the cardholder was born before a certain date which corresponds to the age to be verified. The chip compares the date of birth with the given value and responds to the service provider. Similar methods might be applied to other data objects on the chip, like address, city, region or nationality.

Besides providing a secure channel in order to prevent man-in-the-middle attacks, in all these cases the control system has to be assured of the trustworthiness of the card. If this step fails, the

[3] For example, this is, the case in Finland where a national UID (called "FINUID") serves as a reference to the population register [4].

[4] The possibility of assigning the same public key to more than one user in order to avoid unwanted UIDs is currently being discussed within the eID card community.

verification is worthless because the card might have been produced by the attacker himself. Another possible attack is to extract the data from the card by performing a lot of verifications (using, for example, a guessing game protocol). Age verification is particularly vulnerable to this attack and it is necessary to limit the number of allowed verifications (e.g. only one comparison allowed after typing the PIN).

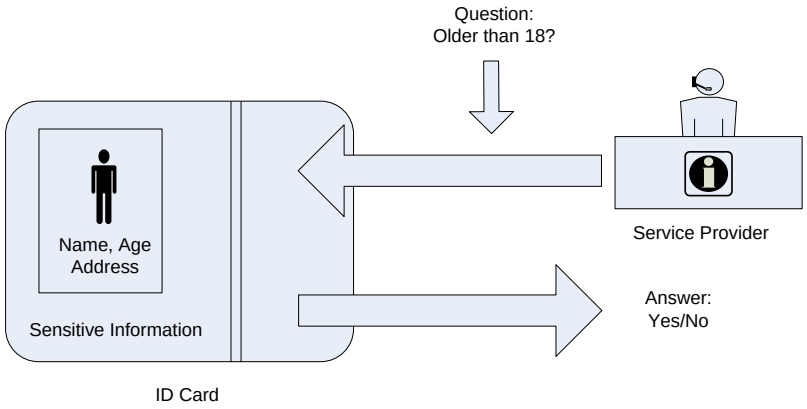

Figure 6: Age Verification

7 Hashed values

A cryptographic hash function is a mathematical function which maps a data block (including *keys*) to a relatively small, fixed length number in such a way that it is difficult to learn any information about the original data given only the hash value (digest). An important property of hashes is that it is computationally hard to find other values of data leading to the same hash. This property provides an integrity guarantee for data without revealing the data (see [18], chapter 1.9 – Hash functions).

Applied to the concatenation of a UID and another domain-specific identifier, the hash-value represents a *domain-specific UID* (or *sector-specific* UID or sector-specific personal identifiers). Applied to customer IDs this strategy may for example prevent the merger of customer databases by large industry branches. In order to receive the customer ID, the service provider sends the identifier of the company to the card, which concatenates it with a secret, unique identifier of the card holder, hashes the result and sends the digest back to the service provider. A malicious service provider who uses another companies identifier could easily be detected (and would need to hold another set of unique identifiers as database keys). Different flavours of this mechanism can be found in the eID card specifications of Austria [1][2] and Germany [6]. One general problem in such cases is how to organize the revocation of the ID documents since simple revocation lists will not work.

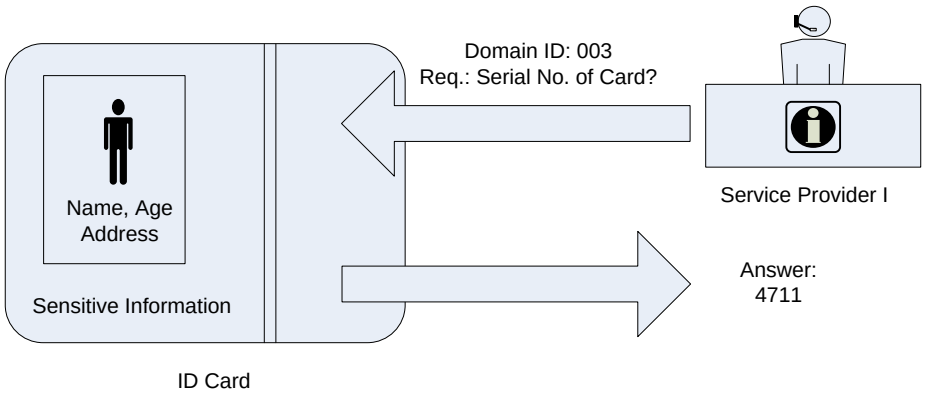

Figure 7: Domain-specific UID

Biometric templates may also be considered to be equivalent to hash values. That is, they can provide a function which maps the image of a fingerprint to a relatively small number (template), in a way that a person's fingerprint can be matched against this number. Biometric templates require much less storage space than the original images and offer better matching performance. The main disadvantage is that they offer less flexibility; for example, using the original images facilitates the migration from legacy systems to more sophisticated matching algorithms.

From the privacy point of view, the important feature in this case is whether the original image can partly recovered from the template. If not, then we refer to the templates as *hashed biometric templates*. However, even in that case, hashing the biometric information only protects against generating the original image. An attacker, for example, who has access to a database containing biometric and additional personal information can still identify a person whose fingerprints he found in a supermarket simply by generating templates and matching them against all entries in the database[5].

8 Authentication vs. electronic signature

A cardholder might demonstrate the knowledge of their private key in one of two ways:

- the card signs a randomly generated nonce, so-called *challenge*, of the service provider; the card's (qualified) electronic signature feature might be used to do this
- the card establishes a secure channel to the service provider via a Diffie-Hellman key exchange protocol or something similar

Both approaches fulfil the requirements for secure authentication but the first approach might infringe the cardholder's privacy. For the card it is usually not possible to check whether the challenge to sign has been randomly generated or whether it contains some hidden information.

A malicious, non-random challenge, however, enables the service provider to prove the establishment of the connection by the cardholder (or, for example, admission into a building) to a third party. A simple analogy is showing somebody your ID card, saying "Hi! It's me." (Diffie-Hellman) vs. signing a letter "I was here today." (signing a challenge). By signing a challenge, the cardholder potentially reveals more information than necessary for the authentication [5][17].

A similar situation occurs, if the card provides the service provider with personal data which is signed by some CA. This again allows the service provider to prove the authenticity of that data to a third party. From a privacy perspective, it is better that the card just proves its own trustworthiness and then delivers the personal information without a signature. However, depending on individual system circumstances this technique can result in inadequate security regarding document and identity fraud. Just proving that a card belongs to a set of trusted cards means that one single compromised private key can undermine the trustworthiness of all transactions if no signature exists that ties the public key to the personal information.

9 Privacy features for contactless cards

Contactless chip cards require additional security mechanisms. At least the following issues should be addressed:

- Skimming: an attacker opens a clandestine connection to the chip and gains access to the data,
- Eavesdropping: an attacker intercepts the communication between the chip and an *authorised* reader,
- Location Tracking: an attacker generates person or card-specific movement profiles

As mentioned above, BAC protects electronic passports against skimming attacks while, for example, the passport holder carries his passport in the pocket. During the border control procedure, the reading device optically scans the document and authenticates to the chip using keys derived from the MRZ printed on the data page. Some European countries, like the Netherlands and Sweden [15], adopted BAC in the specifications of their national ID cards where the MRZ is printed on the back of the card.

[5] Usually, the number of operations necessary for this action would not exceed the computational capacities of the attacker's system, in particular because the method can easily be parallelised.

The BAC mechanism only weakly addresses the issue of eavesdropping and it does not prevent reading (or copying) the data of a lost passport [12][16][17]. However, in the second generation of European passports, this problem is addressed by the Extended Access Control (EAC) protocol which, besides the mutual authentication of card and reader, establishes a strongly encrypted communication channel [5]. Similar techniques, some of them adapted to internet-authentication use-cases, can be found in the specifications for the German eID card [6] and inclusion into the European Cititzen Card standard is currently under discussion [9][10].

Location tracking is an important privacy issue in contactless eID systems. An electronic passport with an RFID chip, if equipped with Basic Access Control, does not reveal any personal information of the passport holder as long as it is safely stored in a pocket and its MRZ is unknown to the attacker. However, the initialisation of wireless communication according to ISO 14443 requires the chip to send a unique identifier to the card reader. An attacker with several distributed reading devices (e.g. in door frames) could therefore distinguish the passport holder without actually having access to the files on the chip. Combined with other data sources, the attacker might be able to generate person or card-specific profiles. This particular attack is relatively easy to avoid – most electronic passports generate random UIDs for every session (see Supplement 9303, E11, [12]) but as a general rule, privacy-protecting RFID systems should be designed very carefully.

10 Conclusion

This article presents privacy features of electronic ID cards from a theoretical perspective.

A forthcoming ENISA Position Paper will include an overview of privacy features currently deployed in European eID projects. We will look at combinations of these features and give recommendations for future developments. Furthermore, we will explore possible uses of anonymous credential systems (like Idemix [11] and Credentica [14]) in eID cards. The Position Paper will be published in Q4 of 2008.

11 References

[1] *Austria* The Austrian eID Card "Bürgerkarte", http://www.buergerkarte.at/
[2] *Austria* Bildung von Stammzahl und bereichsspezifischen Personenkennzeichen (bPK), Öffentlicher Entwurf vom 3.6.2004
[3] *Finland* FINEID, the Finnish eID Card, http://www.fineid.fi/
[4] *Finland* Preliminary Study on Mutual Recognition of eSignatures for eGovernment Applications, National Profile Finland, April 2007, http://ec.europa.eu/idabc/servlets/Doc?id=29082
[5] *Germany* BSI : Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.1 (for electronic passports)
[6] *Germany* BSI : Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 2.0 Public Beta 2 (for national ID cards)
[7] *Spain* The Spanish eID Card, http://www.dnielectronico.es/
[8] Article 29 Data Protection Working Party: Opinion 4/2007 on the Concept of Personal Data, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf
[9] CEN: TC 224/WG 15 – European Citizen Card
[10] CEN: TC 224/WG 16 – Application Interface for Smart Cards Used as Secure Signature Creation Devices
[11] IBM Zürich: Idemix – Pseudonymity for E-Transactions, http://www.zurich.ibm.com/security/idemix/
[12] ICAO: Machine Readable Documents, Doc 9303, Machine Readable Travel Documents, http://mrtd.icao.int/
[13] Eurosmart: White Paper – Common Platform for Electronic Health Cards in Europe, http://www.eurosmart.com/
[14] Microsoft, Credentica, http://www.credentica.com/
[15] Bouzbib, Ari: Electronic Identity Cards in Europe, Presentation at the 11th Porvoo Group Meeting, May 24-25, 2007 http://www.ama.pt/porvoo/apresentacoes/24_tarde/porvoo11_aribouzbib.pdf

[16] Juels, Ari; Molnar, David; Wagner, David: Security and Privacy Issues in E-Passports
[17] Mayáš, Václav; Ríha, Zdenek, Švénda, Petr: Security of Electronic Passports, UPENET, UPGRADE European NETwork, Upgrade Vol. VIII, No. 6, Dec. 2007, http://www.upgrade-cepis.com/issues/2007/6/upg8-6Upenet.pdf
[18] Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A.: Handbook of Applied Cryptography, CRC Press, ISBN: 0-8493-8523-7
[19] Rankl, Wolfgang; Effing, Wolfgang : Handbuch der Chipkarten, Carl Hanser Verlag , ISBN: 3-446-22036-4; English translation: Smard Card Handbook, John Wiley & Sons, ISBN: 0-470-85668-8