Position Paper

February 09

Privacy Features of European eID Card Specifications

enisa
European Network and Information Security Agency

www.enisa.europa.eu

Version: 1.0.1 | Date: 2009-01-27

ENISA Position Papers represent expert opinion on important NIS topics. They are produced by a group selected for their expertise in the area. The content of this paper was discussed between July 2008 and January 2009 via e-mails and personal communication. The table entries are based on the information given by the experts and on the references listed in the last section. The content of this paper was edited by ENISA and the final version has been reviewed by the people listed below.

Authors: **Ingo Naumann, Giles Hogben**
European Network and Information Security Agency (ENISA)
E-Mail: eid@enisa.europa.eu

Contributors:

Herbert Leitold	**Zentrum für sichere Informationstechnologie (A-SIT), *Austria***
Frank Leyman, Marc Stern	**Fedict, *Belgium***
Tarvi Martens	**AS Sertifitseerimiskeskus (SK), *Estonia***
Jens Bender, Dennis Kügler	**Bundesamt für Sicherheit in der Informationstechnik (BSI), *Germany***
Andrea de Maria	**Istituto Poligrafico e Zecca dello Stato (IPZS), *Italy***
André Vasconcelos	**Agency for the Public Services Reform (AMA), *Portugal***
Roberth Lundin	**CEN TC 224 WG 15 (European Citizen Card)**

Group members participate as individuals. This paper should therefore not be taken as representing the views of any company or other organisation, and does not in any way bind group members when dealing with the issues it covers in other contexts.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Contents

Abstract

As an authentication token and personal data source, a national eID card is a gateway to personal information. Any unwanted disclosure of personal information as a result of the issuance or use of the card constitutes a violation of the citizen's privacy rights. Apart from considerations of fundamental rights, this is also a serious obstacle to the adoption of eID card schemes and to their cross-border interoperability.

The aim of this paper is to allow easy comparison between privacy features offered by European eID card specifications and thereby to facilitate identification of best practice. The target audience is corporate and political decision-makers and the paper seeks to raise awareness of the legal and social implications of new developments in eID card technologies. In particular, the findings should have important implications for data protection and security policies. A clear statement of the status quo is an essential first step towards the important goals identifying best practice, improving the base-line of citizen privacy protection in eID cards throughout Europe and ultimately to improving interoperability and adoption by citizens.

We analyse the risks to personal privacy resulting from the use of national electronic identity card schemes and list all practicable techniques available to address these risks. The main part of the paper is then dedicated to a survey of how these available privacy enhancing technologies are implemented in existing and planned European eID card specifications, the European Citizen Card and ICAO electronic passport specifications. The information is based on the latest publicly available specifications with a complete set of references provided and is presented in a series of tables for easy comparison. The table entries show how diverse the European eID card landscape is. Although this paper only compares privacy features, other aspects of the cards are similarly diverse.

1. Introduction

As an authentication token and personal data source, an eID card is a gateway to personal information. This implies a set of risks to the privacy of the citizen, via the unwanted disclosure of personal information and its subsequent misuse. It is fundamentally important to address these risks, first and foremost because they represent a threat to the fundamental human rights of the citizen as enshrined in Article 8 of the European Convention on Human Rights [23], particularly in cases where card possession is compulsory or strongly encouraged by enabling compelling or even essential services. Another consideration for governments is that threats to privacy strongly demotivate citizens from using a scheme. This makes adequate privacy protection a *sine qua non* in countries where the ID card is optional, but even where its possession is compulsory, privacy risks will affect the card's degree of usage and decrease its popularity, making enforcement of any obligations more difficult.

For this reason, all existing and planned schemes already specify at least some *privacy features* to protect card holders against unwanted disclosure and abuse of personal information.

The aim of this paper is to allow easy comparison between privacy features offered by European eID card specifications and thereby to facilitate identification of best practice. A clear statement of the status quo is an essential first step towards the important goals identifying best practice, improving the base-line of citizen privacy protection in eID cards throughout Europe and ultimately to improving interoperability and adoption by citizens.

In this paper, a *privacy feature* is taken to mean:

any feature of an eID card which increases the control of the card owner over which data are disclosed about them and to whom

This includes control over disclosure of information to malicious attackers or people in unauthorised possession of the card, unintended identifiability of the card owner through linkability of authentication events, the leakage of data to casual observers and the legitimate disclosure of the owner's data *with unnecessarily high assurance* associated to it, due to the use of digital signature as an authentication token (see 4.3.2 Authentication vs. Digital Signature). There exists a great variety of privacy features: from simple PIN protection to sophisticated certificate-based access control mechanisms or domain-specific unique identifiers.

Ten European Union states have already rolled out electronic ID cards and thirteen states have committed to rolling out electronic ID cards and are in various stages of planning (see Table 1.). The increasing numbers of card schemes in place are creating opportunities for pan-European initiatives exploiting the new infrastructure. European policy initiatives such as the Services directive [25] already assume an interoperable infrastructure across borders and initiatives such as STORK [48] are exploring ambitious cross-border use-cases.

As with most other aspects of eID cards, privacy features have been developed, implemented and tested at a national level and there is no co-ordinated strategy at a European level as to which features should be implemented and how they should be implemented. The lack of co-ordination is an important obstacle to any possible cross-border interoperability of eID card schemes. This is important in order to be technically interoperable (features expected by one card specification may be lacking in another and therefore prevent interoperability). However it is most important in order to create the necessary trust in the users of such schemes – any cross-border scheme only offers as much protection as its weakest participating member: If just one participating country offers what is generally considered to be inadequate privacy protection, the citizens of the other countries are not likely to accept any cross-border interoperability scheme which puts their data at more risk than their national scheme.

This paper gives a brief overview of the range of privacy features available, but we refer to a previous article [44] for a more detailed description of available features. The main focus of this paper is to map the implementation of these features in the various national ID card schemes. This is an essential starting point in creating a uniform and interoperable implementation of best-practice for protecting citizens' private data, and an essential part of any wider interoperability initiative. The data presented also facilitates comparison of features between member states' schemes and it is hoped may also therefore provide an overall improvement in the level of privacy features.

Table 1 - ID Card Schemes in the European Economic Area (EEA) -- Overview

Country	ID Card?	Compulsory (i)/ primary ID	eID Card? (ii)	eID Card Planned?	References
Austria	yes	no	yes	--	[1][38][51]
Belgium	yes	yes	yes	--	[5][38] [50][51]
Bulgaria	yes	yes	(no)	(no)	[38][50][51]
Cyprus	yes	yes	no	no	[38][50] [51][40]
Czech Republic	yes	yes	no	no	[38][50][51]
Denmark	no	--	--	no	[38][50][51]
Estonia	yes	(yes)	yes	--	[6][38][50]
Finland	yes	no	yes	--	[7][38] [50][51]
France	yes	yes	no	yes	[38][50][51]
Germany	yes	(yes)	no	yes (specs.)	[10][38] [50][51]
Greece	yes	yes	no	no	[38][50][51]
Hungary	yes	no	no	yes	[38][50][51]
Ireland	no	--	--	no	[38][50][51]
Italy	yes	(yes)	yes (partial)	--	[11][38] [50][51]
Latvia	no	--	--	yes	[38]
Lithuania	yes	yes	no	no	[38][51]
Luxembourg	yes	yes	no	yes	[38][51]
Malta	yes	yes	no	yes	[38][51]
Netherlands	yes	(yes)	yes	--	[13][24] [38][51]
Poland	yes	yes	no	yes	[38][50] [51][14]
Portugal	yes	yes	yes	--	[15][38] [50][51]
Romania	yes	yes	no	yes	[38][50][51]
Slovakia	yes	yes	no	yes	[38][50][51]
Slovenia	yes	(yes)	no	yes	[38][40][33]
Spain	yes	yes	yes	--	[16][38] [50][51]
Sweden	yes	no	yes	--	[17][38] [50][51]
UK	yes (partial)	unknown	yes (partial)	--	[20][21][27] [38] [50][51]
Iceland	yes	yes	no	yes	[38][51]
Liechtenstein	yes	no	no	yes	[38]
Norway	no	--	--	no	[50][51]
Total	25	20	10	13	

Comments:

i. In some countries, the possession of an ID card or a passport is compulsory. However, the term "compulsory" has different meanings and implications in different countries. For example, requirement to carry an ID card may apply only after a certain age; in some cases, ID cards are compulsory for nationals and foreigners residing in that country; often, ID cards are only compulsory for nationals residing inside the country. A "yes" item in parenthesis in this column indicates that the ID card is the primary ID in a broader sense.

ii. The "yes"/"specs." entries in these columns are highlighted in red in order to indicate which implementations/specifications we have taken into account.

2. Privacy Threats

Before describing privacy features, we first give an overview of the categories of threat (exploitation of a vulnerability) they attempt to defend against. Note that, taking a definition of risk as the potential that a given threat will exploit a given system's vulnerabilities, we do not attempt to assess the overall risk level posed by these threats because information is not available on the probability of occurrence of the threats.

2.1. Assets

Assets are the target of protection in a risk analysis. The main assets at risk in eID card scenarios are usually the personal information and anonymity of the citizen. Loss of these assets can put at risk secondary assets such as physical property, financial assets, reputation (e.g. in the case where the card is used for identity theft) and the right to be left alone (via spam etc...).

2.2. Threats

The following are classes of threat (potential negative impact due to vulnerabilities in a system) to personal data assets in systems using eID cards. The focus of this paper is on the mapping of measures used to address these threats to existing or planned eID card specifications. We therefore give only a brief summary of these and refer to a more detailed description in related papers such as [32]. Note, following our definition of a privacy risk, any vulnerability which exposes data on the card creates a privacy risk:

1. *Falsification of Content:* The falsification of content due to unauthorised writing into the file system of the card is a threat. An altered UID could, for example, be accepted as authentic if there are no appropriate security measures in place.
2. *Eavesdropping:* an attacker intercepts the communication between the card and the reader and reads the data. This is especially important if contactless card interfaces are used but it also applies to contact interfaces with unshielded readers and cables (see [52]).
3. *Man-in-the-middle attacks:* similar to the privacy threat "eavesdropping" but the attacker is located between the card and the server/middleware and communicates with both sides.
4. *User signs a bogus document:* this can happen for example if what the user sees is not actually what they are signing. It can be a privacy threat because the user's data could be misrepresented as a result thereby compromising the privacy principle of the right to rectification.
5. *User authenticates to a bogus server* due to misplaced trust in a server. This constitutes a privacy threat because the bogus server can then access the user's information.
6. *Inappropriate delegation of card:* in certain cases, a card may be willingly delegated to another individual. In certain cases, where appropriate safeguards against abuse exist this may constitute a legitimate usage of the card. In other cases, however, card holders put themselves at risk by delegating their card.
7. *Loss or Theft of card:* if the card has inadequate proof-of-possession and/or access control mechanisms, personal data is put at risk.

8. *Physical Attacks:* invasive attacks involving, e.g. rewiring a circuit on the chip or using probing pins to monitor data flows. They usually aim at stealing private keys in order to access private data.
9. *Side-Channel Attacks:* these attacks use information leaked through so-called side-channels to gain access to private data. This additional information could be the timing of signals, power consumption, or radiation.
10. *Cryptanalytic attacks:* These attacks directly target the cryptographic algorithms in order to break the confidentiality of information transmitted (e.g. between the card and the reader).
11. *Skimming attacks:* an attacker opens a clandestine connection to the card and gains access to the data. This privacy threat does not apply to contact cards since in that case the card has to be plugged manually into the reader. The maximum distance from which an eID card can be read is usually relatively small (for ISO14443 compatible cards approx. 25cm, see [34][35]), but in theory there exists the possiblity of skimming. Even so, there is a considerable incentive to install a hidden reading device, close enough to eID cards carried around in back-pockets or handbags, that skims personal information from eID cards.
12. *Location Tracking:* an attacker generates person or card-specific movement profiles based on the location of readers. This is more likely and more powerful in combination with a skimming attack, although it could also be done as part of an otherwise legitimate application scenario (e.g. transport ticketing).
13. *Behavioural Profiling:* Similar to location tracking but instead of (just) the location, the profile contains information about the type of authentication, money spent, places visited, etc.
14. *Proving the trustworthiness of personal information to a third party:* Another interesting detail is whether the personal information is digitally signed by the document producer, e.g. because it is included in a public key certificate. This is the case with electronic passports. In the case where no signature is actually needed to perform the required operation, this constitutes a privacy threat because data is provided with an unnecessary level of assurance (see 4.3.2 Authentication vs. Digital Signature), thereby allowing the service provider who reads the data to prove its trustworthiness to a third party in any subsequent transaction. This aspect is often overlooked because it does not actually disclose more personal data, but only makes the data disclosed more open to abuse.

3. Addressing Privacy Threats

3.1. Available Privacy Features of eID cards

The following describes in general, the classes of features of eID cards designed to address the above risks:

1. *Encrypted data blocks:* The data on the card is encrypted with a secret key. Every reader can read the raw data block but the knowledge of this secret key is required to obtain the information in it. The only additional benefit offered by this feature where adequate access control is provided is that data may maintain its confidentiality when transmitted to third

parties after leaving the card (as long as secret keys are not also transmitted). NB encrypted data blocks are *not* used in any European eID card specification.

2. *Access control mechanisms:* The card carries the data as plain text but the service provider/card reader can only access it after a successful authentication of the service provider and/or the cardholder (proof-of-possession). A successful authentication usually consists of proving the knowledge of a PIN or secret/private key. An authentication is called "mutual" if, at the same time, the card authenticates to the service and the reader proves its trustworthiness to the card and to the holder.
3. *Privacy-respecting use of Unique Identifiers (UIDs):* unique identifiers are strings which allow applications to distinguish between individual citizens (citizen-specific UID) or their identity cards (card-specific UID). A card-specific UID changes when a new card is issued to the citizen. Identifiers have to be used very carefully in order to avoid privacy risks. A well-designed UID scheme might offers more privacy than for example using a social security number or the combination of name and date of birth as UID. In general, the more a UID is linkable to useage in other transactions (using the card, or otherwise), the less privacy it offers. It is important to note that individual static data on the card, like a public key or even an encrypted data block has all the attributes of a UID if it is unique.
4. *Domain-specific UID* (or sector-specific UID or sector-specific personal identifiers): The use of different identifiers in different application domains helps prevent merging databases. Domain-specific identifiers can be derived from (secret) identifiers held by a trusted central issuer.
5. *Selective Disclosure:* A commonly accepted privacy principle is that data disclosed should be the minimum required for the stated purpose. For example, this is an axiom of EU data protection law ([23], Article 7). In order to respect this principle, the card should not disclose more information than has been asked for by the requesting application. For example if the requesting application only requires the name of the card holder, the card should not give access to the user's address.
6. *Verify-only mode*: a simple case of selective disclosure is verify-only mode where instead of disclosing the actual value of a field, a yes-no answer is given for whether a query is satisfied – e.g. whether age is greater than a certain value or a biometric matches (with a given probability) a certain template. Or, for example if the requesting server asks the card to assert that the holder is between 18 and 30 (a boolean value), the card should not return the user's date of birth. A complete interpretation of this and the previous principle would require a query engine to be implemented on the card, which runs a query string against the data held. This requires too much processing and is largely unnecessary since the cases where a query cannot be matched exactly by existing fields are quite restricted for most eID card applications. Instead, the ability to return selected fields (rather than the whole data set) and to prove whether or not the user's date of birth is within a certain date range (usually to prove they are over 18) is sufficient for most use-cases. Another important related function is a match-on-card feature for fingerprint information. Several other useful cases exist, such as proving driving credentials or European Citizenship.
7. *Biometric templates:* A biometric template is a set of data derived from biometric information (e.g. a digital picture of a fingerprint) which allows comparison with live biometric data. The

use of biometric templates, instead of pictures, can be seen as a privacy-protecting measure because the biometric information itself is not stored on the card, thereby reducing the information stored about the holder.

8. *Secure communication between the card, the middleware and the server:* once data is released by the card, it is vulnerable to eavesdropping when in transit between the card and the middleware interfacing with the card and further on down the chain, in transit between the middleware and the destination service. In order to respect the privacy of the card holder, the data should therefore be encrypted between these three entities ideally in form of an end-to-end encryption between card and server, mitigating the risk of compromising the middleware/ computer of the card holder.

More detailed explanations of some of these mechanisms can be found in [44].

3.2. Examples in Existing Specifications

A number of existing PET (Privacy Enhancing Technology) implementations for eID cards (and electronic passports) can be found in the literature:

- Basic Access Control, as defined in the ICAO specifications for machine-readable travel documents [37] in order to prevent skimming and, to a lesser extent, eavesdropping
- (European) Extended Access Control (EAC) [8][9], as specified by the German Federal Office for Information Security and adopted by the European Union, addresses some minor weaknesses of BAC and prevents unauthorized devices to read the fingerprint information stored in EU passports. This mechanism is also proposed for inclusion, as "Modular EAC" , into the European Citizen Card standard [29][30].
- PACE [9] and similar protocols, some of them adopted by the ECC [29][30] standard, was originally developed for the German eID card. It replaces BAC and complements EAC in order to allow authentication to remote servers via the Internet.
- Random UIDs for the establishment of the contactless communication channels ([37] Doc 9303 part 3 volume II section III A1.16, or in older versions, Supplement to ICAO Doc 9303, E11)

Domain-specific identifiers (or UIDs), also called sector-specific identifiers [1][3] or Restricted Identity [9], as explained above (see item 4 in 3.1 Available Privacy Features of eID cards) are included in the specifications of the Austrian [3] and German [9] eID card specifications.

3.3. Privacy Enhanced PKI

So-called "privacy-enhanced PKI tokens" implemented in products such as the former U-Prove (recently acquired by Microsoft) [31] and Idemix (IBM) [36] provide cryptographic techniques which can:

○ Prevent linkability between identifiers presented to different services, even if those service-providers and the credential issuer later share data or otherwise collude. Using such technologies, the user can be known to each service provider under a different pseudonym. This allows them to make an assured assertion about themselves without revealing any unnecessary information (through linkage to other transactions). In particular, the verifier cannot discover the pseudonym by which the user is known to the credential issuer.

- Provide more extensive selective disclosure functionality.
- Enforce limited show protocols (e.g. for e-cash) whereby the user may prove an assertion only a limited number of times.
- Provide global revocation of a number of certificates held by a user while maintaining their unlinkability by the issuer and verifiers (see [28]). Note that this makes the reasonable assumption that neither the issuer nor the verifier can add arbitrary entries to the CRL. If they could, this would allow them to apply brute-force attacks by temporarily revoking combinations of certificates and then trying to verify others. This *is* a reasonable assumption however, since most CRLs are controlled by strict procedures which would make this attack impossible.

As such, privacy-enhanced PKI technologies have significant potential to enhance existing eID card privacy functions. Although these technologies have been available for a long time, there has not been much adoption[1] in mainstream applications and eID card implementations.

4. Overview of European eID Card Specifications

Electronic passports only contain an "ICAO application", as the functionalities according to the ICAO specifications [37] are usually called[2]. In addition to that, eID cards might be equipped with additional applications. Contact cards usually contain an electronic-signature application which can be used for electronically signing documents. In general, the user has to type a PIN in order to sign a document and cannot retrieve the private key from the card. A third application, nowadays usually referred to as an "eID application", allows the user to authenticate via the Internet to eBusiness or eGovernment services. In some cases, this application is not different from an electronic-signature application except for the designation of the certificates for authentication purposes (see also 4.3.2 Authentication vs. Digital Signature).

For comparison, we included data from the specifications of electronic passports, according to ICAO and the European Union (ICAO/EU[3]), in the tables.

[1] *Austria and Germany have taken some important steps towards unlinkability and selective dislosure (see chapter 3.2).*

[2] *The different sets of functionalities of smartcards are called "applications" [46].*

[3] *The EU ePassport specifications amend the ICAO specifications with a definition of and requirement for Extended Access Control (EAC). There exists at least one additional definition of Extended Access Control, from the Singapore goverment. In this paper we only refer to the European EAC specification.*

4.1. Interfaces and functionality

In the following table we give an overview of the already existing (or specified) European eID cards, their interfaces and their card applications.

Table 2 – Interfaces and functionality

Specification	Interface	(Optional) Electronic Signature (i)	eID Application	References
AT	**contact**	**yes**	**yes**	**[1]**
BE	**contact**	**yes**	**yes**	**[5]**
EE	**contact**	**yes**	**yes**	**[6]**
FI	**contact**	**yes**	**yes**	**[7]**
DE	**contactless**	**yes**	**yes**	**[9][10]**
IT	**contact**	**yes**	**yes**	**[11]**
NL	**contactless**	**no**	**no**	**[13]**
PT	**contact**	**yes**	**yes**	**[15]**
ES	**contact**	**yes**	**yes**	**[16]**
SE	**contact and contactless (two chips)**	**yes**	**yes**	**[17][38]**
UK	**contact and contactless**	**unknown**	**unknown**	**[27]**
ECC	**optional contact, contactless or both**	**yes**	**yes**	**[29][30]**
ICAO	**contactless**	**no**	**no**	**[37]**
ICAO/EU	**contactless**	**no**	**no**	**[37][22]**

Comments:

i. In all specifications the electronic signature application is optional, except for Estonia. In the case of Austria, it is mandatory to activate the card's electronic signature functionality but the card itself is not compulsory nor primarily a travel document.

4.2. Writing Data to a Card

The specification of whether or not data on the card can be written to after personalization is a crucial design factor with regard to security and privacy. On the other hand, of course, it enables many useful applications. In the following table we list which specifications allow writing to data on the card.

We distinguish three different categories of data which can be written to or updated on the card:

Primary data: Personal information or Citizen UIDs, also included in certificates, or the address.

Additional data: Application-specific data like letters, receipts, status of tax declaration or even personal files.

"Housekeeping" data: Minimal information needed by the card OS like remaining number of password/PIN trials, time stamps, updated CV certificates.

Table 3 - Write access

Specification	Primary data (e.g. address) on the card can be changed?	Additional data can be written	Only "house-keeping" data can be written	References
AT	**yes (i)**	**yes**	**yes**	**[1]**
BE	**yes**	**yes**	--	**[5]**
EE	**yes (ii)**	**no**	**--**	**[6]**
FI	**yes**	**yes**	**--**	**[7]**
DE	**yes**	**no**	**yes**	**[9][10]**
IT	**no**	**yes**	**--**	**[11]**
NL	**no**	**no**	**no**	**[37]**
PT	**yes**	**yes**	**--**	**[15]**
ES	**unknown**	**unknown**	**unknown**	
SE ct	**no**	**yes**	**yes**	**[18]**
SE cl	**no**	**no**	**no**	**[37]**
UK	**unknown**	**unknown**	**unknown**	**[27]**
ECC	**optional**	**optional**	**optional**	**[29][30]**
ICAO	**no**	**no**	**no**	**[37]**
ICAO/EU	**no**	**no**	**yes**	**[37][22]**

Comments:

i. Technically feasible but is not used because the change of primary data (e.g. the holder's name) would lead to certificate revocation and to card replacement.

ii. EE: a user cannot change data on the card. However, it is possible to renew private keys and certificates on the card (via a special procedure) from any computer connected to Internet.

4.3. Deployed Privacy Features

4.3.1. Access Control

There are different access control mechanisms deployed in European eID cards. The simplest way is to require the user to enter a secret PIN (stored on the card) before giving access to certain data groups. Using the private key(s) designated for (qualified) signature or authentication always requires the user to enter a secret PIN.

Secret keys can also be used as credentials to gain access to the card. Using symmetric algorithms, the secret key has to be known to the card and the reader/server and is very often derived from the serial number of the card. In this case, the key management for large systems is usually rather difficult because it requires the secure exchange of many secret keys between different entities.

Otherwise asymmetric algorithms may be used to authenticate the server via a private key held on the server. In the table we distinguish between symmetric-key based access control and certificate-based access control[4].

Table 4 - Privacy features: Access control and encryption

Specification	PIN-based access control	Symmetric-key based access control	Certificate-based access control	Encrypted data storage	Encrypted data transmission	Reference
AT	**yes**	**no**	**no**	**no**	**yes**	**[1]**
BE	**yes**	**no**	**yes (i)**	**no**	**yes**	**[5]**
EE	**yes**	**yes**	**no**	**no**	**yes**	**[6]**
FI	**yes**	**no**	**no**	**no**	**yes**	**[7]**
DE	**yes**	**no**	**yes**	**no**	**yes**	**[9][10]**
IT	**yes**	**no**	**no**	**no (iii)**	**yes**	**[11]**
NL	**no**	**no**	**no**	**no**	**yes**	**[13][24] [37]**
PT	**yes**	**no**	**yes**	**no**	**yes**	**[15][49]**
ES	**yes**	**yes**	**no**	**unknown**	**yes**	**[16][53]**
SE ct	**yes**	**no**	**no**	**no**	**yes**	**[18]**
SE cl	**no**	**no**	**no**	**no**	**yes**	**[37]**
UK	**unknown**	**unknown**	**unknown**		**unknown**	
ECC	**optional**	**optional**	**optional**	**optional**	**optional**	**[29][30]**
ICAO	**no**	**no**	**no**	**no**	**optional**	**[37]**
ICAO/EU	**no**	**no**	**yes**	**no**	**yes**	**[37][22]**

Comments:

i. Only for write access
ii. Depends on the implementation
iii. The Italian ID card has additional, encrypted data stored on the laser stripe.

4.3.2. Authentication vs. Digital Signature

For authentication and (qualified) digital signature, many European eID cards use the same mechanism but different certificates and public keys. The reason behind the use of

[4] *Even though Basic Access Control and similar mechanisms that prevent against skimming are in principle symmetric-key based access control mechanisms we do not list them here since the key is not secret but printed on the card. We do consider the BAC communication as encrypted, however, since the assumption is that an eavesdropper has no knowledge of the data printed on the card. See below.*

different certificates is usually the different legal implications of authentication and digital signature. However, the use of a digital signature for authentication-only events represents an infringement of privacy.

This is because a digital signature always leaves behind non-repudiable evidence of the signing event, and allows the relying party to show the same artefacts (either a simple response to a challenge or assertions about the signer), *with the same degree of assurance*, to another party. In the case of using a digital signature for authentication (e.g. using a signed challenge), this represents more of a privacy threat than an authentication-only event, which only provides proof that the party was authenticated. The difference can be compared in the physical world to *leaving* a witness-signed *copy* of a photograph as opposed to simply *showing* it to someone to identify oneself without that person recording any data from the photograph with signature.

This privacy threat is not addressed by using two different certificates because both certificates transmit signed data. Although digital signatures *do* authenticate the signer, as explained, they expose more information about the person with more assurance than required for a pure authentication event, thereby violating the minimal disclosure principle required in European data protection law (see [23], Article 7). Using the digital signature mechanism in a challenge-response protocol for authentication allows the service provider to prove the authenticity of the signed challenge to a third party [44] -- and therefore constitutes a bigger infringement of the citizen's privacy.

Table 5 - Authentication vs. electronic signature

Country	Authentication certificate different from signature	Signature application used for authentication?	Ref.
AT	**no (i)**	**yes**	**[1]**
BE	**yes**	**yes**	**[5]**
EE	**yes**	**yes**	**[6]**
FI	**yes**	**yes**	**[7]**
DE	**yes**	**no**	**[9][10]**
IT	**yes**	**yes**	**[11]**
PT	**yes**	**yes**	**[15]**
ES	**yes**	**yes**	**[16][53]**
SE	**yes**	**yes**	**[18]**
UK	**unknown**	**unknown**	
ECC	**optional**	**optional**	**[29][30]**

Comments:

i. For additional functionalities, there exists a second certificate/key pair on the card, but currently eID applications and qualified electronic signature use the same key pair.

ii. **First column:** yes = different certificates, public and private keys (and assigned PINs) are used for authentication and digital signature
Second column: yes = the *mechanisms* for the electronic signature (signing the text) and authentication (signing the challenge), including key lengths etc., are the same

4.3.3. Contactless eID Cards

Two countries in the European Union are currently issuing ID cards with a contactless chip and an ICAO application: the Netherlands and Sweden. Both adopted BAC in the specifications of their national ID cards where the MRZ is printed on the back of the card.

Table 6 - Contactless eID cards

Country	ICAO application	BAC	EAC	Random UID	Ref.
DE	**yes (i)**	**no (i)**	**yes**	**yes**	**[9][10]**
NL	**yes**	**yes**	**no**	**yes**	**[37]**
SE	**yes**	**yes**	**no**	**unknown**	**[37]**
ECC	**optional**	**optional**	**optional**	**optional**	**[29][30]**
ICAO	**yes**	**optional**	**optional**	**optional**	**[37]**
ICAO/EU	**yes**	**yes**	**yes**	**optional**	**[37][22]**

Comments:

i. In the German eID card specifications, BAC is replaced by PACE [9]and EAC applies to all data groups.

4.3.4. Personal Information and Linkable Identifiers

Personal data on eID cards can be stored and transmitted in simple pseudonym-attribute-value triples (e.g. Bob1 first-name "Bob") or equivalent. Such data is *only personal if* the pseudonym used is linkable to other instances of that pseudonym which are somehow uniquely associated with the physical person. For example, "xyz location: +51° 16' 26.76, +0° 21' 14.76" is *not* personal data for a service provider unless that service provider also knows the relationship of that data to some other personal information, e.g. "xyz social-security-number: 1231412423412". Note that the values themselves may also be pseudonyms – e.g. if the value is a public key string. For more information on the concept of linkability, see [45].

Obviously linkage between identifiers is necessary in any application which depends on a continuous identity, but in many cases, poor pseudonym management gives away more information to more parties than is necessary for the performance of the application. Improper management of pseudonyms therefore constitutes a privacy vulnerability because it allows unnecessary disclosure of personal data via linkage between different transactions.

This section describes first of all the data fields which are available on the card, and second what measures are taken to minimise linkability between the pseudonyms used in different transactions. Note that privacy-enhanced PKI (see chapter 3.3) might afford more sophisticated pseudonym management than is offered by any existing ID card scheme. In terms of existing eID card functionality, the following are existing possibilities:

1. Citizen-specific UIDs: are attached with every transaction and do not change even with the issuance of a new card.
2. Card-specific UIDs: change when a new card is issued to the citizen.
3. Domain-specific identifiers. Different pseudonyms are used for different service-providers. This may be implemented with different degrees of granularity – i.e. not necessarily a different pseudonym for each service provider but instead a limited set of pseudonyms are shared among groups of service providers.

Note also that the management of UIDs after they leave the card also has privacy implications. In some cases, regulations and security policies exist which prohibit the use of UIDs in certain scenarios. For example the use of a UID might be legally restricted to government-only use and it is prohibited for application-providers to store them.

The following two tables show how pseudonyms are managed in existing schemes and which data fields are available. The tables also show how such information may be accessed as this is important in determining how much of a privacy risk is posed by a particular scheme. The crucial question is how much effort an attacker needs to make in order to obtain how much personal information.

We distinguish the following cases:

UNUSED/NOT STORED Information is not stored on the card or does not exist

SKIM Everybody can skim this information up to a distance of several meters. An attacker would only need to be within this distance to the card in order to read the information. Please note that this case does not apply to any of the card specifications considered.

ANY Everybody can access this information when in possession of the card, e.g. if an attacker finds the card on the street

USER User can access this information after providing credentials (e.g. secret PIN)

GOV Government or authorized private companies can access this information after providing credentials (e.g. secret government key)

GOV+USER Government or authorized private companies can access this information after proving possession of credentials (e.g. secret government key) *and* user consent (e.g. secret PIN)

UNDEFINED Depends on the implementation; in some cases, the most probable case is given in curly brackets ({})

UNKNOWN unknown

TEMPLATE Fingerprints: use of template; can be combined with one of the above

Table 7 - Personal Information I -- Unique Identifiers

Country	Card UID (i)	Citizen UID (ii)	Domain-specific UID	Ref.
AT	UNDEFINED {ANY}	UNDEFINED {GOV+USER}	ANY **(iv)**	**[1][4]**
BE	ANY	ANY	UNUSED	**[5]**
EE	ANY	ANY	UNUSED	**[6]**
FI	ANY	ANY	UNUSED	**[7]**
DE	GOV **(iii)**	UNUSED	GOV+USER	**[9][10]**
IT	ANY	USER	UNUSED	**[11][12]**
NL	ANY	ANY	UNUSED	**[13][37]**
PT	ANY	ANY	UNUSED	**[15][49]**
ES	ANY	GOV+USER	UNUSED	**[16][53]**
SE ct (v)	ANY	ANY	UNUSED	**[38]**
SE cl	ANY	UNUSED	UNUSED	**[37]**
UK	UNKNOWN	UNKNOWN	UNKNOWN	
ECC	UNDEFINED {ANY}	UNDEFINED	UNDEFINED	**[29][30]**
ICAO	ANY	UNDEFINED {UNUSED}	UNUSED	**[37]**
ICAO/EU	ANY	UNDEFINED {UNUSED}	UNUSED	**[37][22]**

Comments:

i. A unique certificate, public key or encrypted data block can also act, to all intents and purposes, as a card UID.
ii. A subset of personal information (e.g. Name and Date of Birth) is not considered a citizen UID in this context.
iii. The public keys of the Chip Authentication will *not* be unique for every card.
iv. The calculation of the domain-specific identifier (bPK) takes place in a special middleware, outside of the card. The cards come in many different flavours (signature cards, student cards, etc.) and access control mechanisms can be different. Permission to perform the hash depends on being able to read the sourcePIN from the card, which again depends on the specific version of that card. NB the Austrian eGovernment law states that in industrial applications this hash calculation must not be performed on the server side but in the citizen's middleware.
v. After personalisation (Swedish eID cards are delivered without personalization of the contact chip to the citizen).

Table 8 - Personal Information II

Country	Personal Information (e.g. Name)	Facial image	Fingerprint information	Ref.
AT	UNDEFINED {ANY}	NOT STORED	NOT STORED	[1][2]
BE	ANY	ANY	NOT STORED	[5]
EE	ANY	NOT STORED	NOT STORED	[6]
FI	ANY	NOT STORED	NOT STORED	[7]
DE	GOV/ GOV+USER (ii)	GOV	GOV/NOT STORED (i)	[9][10]
IT	USER	UNKNOWN (iii)	UNKNOWN (iii)	[11][12]
NL	ANY	ANY	NOT STORED	[13][37]
PT	ANY	ANY	TEMPLATE	[15][49]
ES	GOV+USER	GOV+USER	NOT STORED	[16][53]
SE ct (iv)	ANY	NOT STORED	NOT STORED	[18]
SE cl	ANY	ANY	NOT STORED	[37]
UK	UNKNOWN	UNKNOWN	UNKNOWN	
ECC	UNDEFINED	UNDEFINED	UNDEFINED	[29][30]
ICAO	ANY	ANY	UNDEFINED	[37]
ICAO/EU	ANY	ANY	GOV	[37][22]

Comments:

i. According to [10] the citizen can decide whether their fingerprints will be stored on the card.

ii. Government authorities (police, border control) need physical possession (to perform PACE access control using CAN(Card Access Number) or MRZ both printed on the card) and must authenticate themselves using PKI-based authentication, eBusiness/eGovernment institutions need user consent (PACE using PIN) and must authenticate themselves using PKI-based authentication.

iii. Declared as "to be defined" in [12].

iv. After personalisation. See above.

5. Conclusions

A lot of very practical techniques exist to protect the citizen’s privacy and, from the survey of available techniques in this paper, it is possible to identify a set of best practice guidelines for the protection of personal data in national eID card schemes. European eID card specifications are very diverse in terms of their implementation of the privacy features we have identified: They are by no means universally implemented and where they are implemented, they are not always technically interoperable.

A lot of work is currently being done in the planning of new eID card specifications, in creating cross-border interoperability between specifications and in standardising eID card specifications. It is important that in creating these specifications and in working on the wider aspects of interoperability, the features identified in this paper should be carefully considered and built in “by-design”.

6. Terminology and Abbreviations

Abbreviation	
EAC	Extended Access Control
ECC	European Citizen Card
EEA	European Economic Area
eID	Electronic Identity
MRZ	Machine Readable Zone
PACE	Password Authentication Connection Establishment
PET	Privacy Enhancing Technology
UID	Unique Identifier

7. References and eID Card Specifications

Austria

[1] *Austria* The Austrian eID Card "Bürgerkarte", http://www.buergerkarte.at/ (includes the Bürgerkarte specifications)
[2] *Austria* Which data is saved on the citizen card?, http://www.buergerkarte.at/en/datenschutz-sicherheit/index.html
[3] *Austria* Bildung von Stammzahl und bereichsspezifischen Personenkennzeichen (bPK), Öffentlicher Entwurf vom 3.6.2004
[4] *Austria* Spezifikation MOA ID 2007-08-02

Belgium

[5] *Belgium* The Belgian eID Card, http://eid.belgium.be/ (includes the Belgian eID card specifications)

Estonia

[6] *Estonia* EstEID, the Estonian eID Card, http://www.id.ee/ (includes the EstEID specifications)

Finland

[7] *Finland* FINEID, the Finnish eID Card, http://www.fineid.fi/ (includes the FINEID specifications)

Germany

[8] *Germany* Federal Office for Information Security (BSI): Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11 (for electronic passports), http://www.bsi.bund.de/literat/tr/tr03110/TR-03110_v111.pdf
[9] *Germany* Federal Office for Information Security (BSI): Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC) and Password Authentication Connection Establishment (PACE), and Restricted Authentication, Version 2.0, (for national ID cards), http://www.bsi.bund.de/english/publications/techguidelines/tr03110/TR-03110_v200.pdf
[10] *Germany* Federal Ministry of the Interior (BMI): Einführung des elektronischen Personalausweises in Deutschland, Grobkonzept, Version 2.0, http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Themen/PaesseUndAusweise/Grobkonzept__Personalausweis,templateId=raw,property=publicationFile.pdf/Grobkonzept_Personalausweis.pdf

Italy

[11] *Italy* Carta di Identità Elettronica (C.I.E), the Italian eID Card, http://www.halnet.it/cie/ (includes the C.I.E specifications)
[12] *Italy* Carta di Identità Elettronica (C.I.E), File System, v.2.0.2

The Netherlands

[13]*The Netherlands,* Parliamentary documents, TK 2005-2006 25764 No. 30, http://www.overheid.nl/op/

Poland

[14]*Poland* Powszechny Elektroniczny System Ewidencji Ludności, http://pesel2.mswia.gov.pl/

Portugal

[15]*Portugal* The Portuguese eID Card, http://www.cartaodecidadao.pt/ (includes the Cartão de Cidadão specifications)

Spain

[16]*Spain* The Spanish eID Card, http://www.dnielectronico.es/

Sweden

[17]*Sweden* Fakta om nationellt id-kort, http://www.polisen.se/inter/nodeid=33378&pageversion=1.jsp

[18]*Sweden* Identification cards – Electronic ID Card, Swedish Profile, Svensk Standard SS-61 43 32, Utgåva 3

[19]*Sweden* Identification Cards – Electronic ID Certificate, Svensk Standard SS-61 43 31, Utgåva 2

United Kingdom

[20]*United Kingdom,* Home Office, National Identity Scheme, Delivery Plan 2008

[21]*United Kingdom,* Home Office, ID Cards, http://www.homeoffice.gov.uk/passports-and-immigration/id-cards/

European Union

[22]*European Union,* Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:EN:PDF

[23]*European Union*, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML*

[24]*European Union,* Commission Decision C(2006)2909 of 28 June 2006 establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States, http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc/c_2006_2909_fr.pdf (French version)

[25]*European Union,* Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, http://ec.europa.eu/internal_market/services/services-dir/proposal_en.htm

Other

[26] 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

[27] BBC News, Foreign national ID card unveiled, Sept. 25th, 2008, http://news.bbc.co.uk/2/hi/uk_news/politics/7634111.stm

[28] Brands, Stefan; Demuynck, Liesje; de Decker, Bart: A Practical System for Globally Revoking the Unlinkable Pseudonyms of Unknown Users, http://www.springerlink.com/content/e70m608878k11124/fulltext.pdf

[29] CEN: TC 224/WG 15 – European Citizen Card, Part 1-4, Technical Specification

[30] CEN: TC 224/WG 16 – Application Interface for Smart Cards Used as Secure Signature Creation Devices

[31] Credentica: U-Prove SDK, http://www.credentica.com/u-prove_sdk.html

[32] ENISA Position Paper: Security Issues in the Context of Authentication Using Mobile Devices (Mobile eID), November 2008, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_mobile_eid.pdf

[33] epractice.eu: eGovernment Factsheet - Slovenia - National Infrastructure, http://www.epractice.eu/document/3476

[34] Eurosmart: RFID technology security concerns: Understanding Secure Contactless device versus RFID tag, Oct. 2007

[35] German Federal Office for Information Security (BSI): Messung der Abstrahleigenschaften von RFID-Systemen (MARS), Projektdokument 1: Teilbericht zu den Möglichkeiten des passiven Mitlesens einer RFID-Kommunikation, http://www.bsi.de/fachthem/rfid/Mars_Teilbericht_1Therorie.pdf

[36] IBM Zürich: Idemix – Pseudonymity for E-Transactions, http://www.zurich.ibm.com/security/idemix/

[37] ICAO: Machine Readable Documents, Doc 9303 and Technial Reports, Machine Readable Travel Documents, http://mrtd.icao.int/

[38] IDABC: eID Interoperability for PEGS, Country Profiles, http://ec.europa.eu/idabc/en/document/6484/5644

[39] Microsoft, Credentica, http://www.credentica.com/

[40] Modinis IDM, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome

[41] Juels, Ari; Molnar, David; Wagner, David: Security and Privacy Issues in E-Passports

[42] 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

[43] Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A.: Handbook of Applied Cryptography, CRC Press, ISBN: 0-8493-8523-7

[44] Naumann, Ingo; Hogben, Giles: Privacy Features of European eID Card Specifications, Elsevier Network Security Newsletter, August 2008, ISSN 1353-48-58, pp. 9-13, http://www.enisa.europa.eu/doc/pdf/publications/privacy_features_of_eid_cards.pdf

[45] Pfitzmann, Andreas; Hansen, Marit: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, version v0.31, 2008, http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[46] 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

[47] Richter, Henning; Mostowski, Wojciech; Poll, Erik: Fingerprinting Passports, NLUUG 2008 Spring Conference on Security, pp. 21-30, 2008, http://www.cs.ru.nl/~erikpoll/papers/nluug.pdf

[48] STORK: Secure Identity Across Borders Linked, http://www.eid-stork.eu/

[49] Vasconcelos, André: Cartão de Cidadão, Apresentação Técnica, Presentation given at the Agora 2006 conference, October 25, 2006

[50] Wikipedia, ID Card, http://en.wikipedia.org/wiki/Id_card, captured Aug. 14th, 2008

[51] Wikipedia, List of Identity Card Policies by Country, http://en.wikipedia.org/wiki/List_of_identity_card_policies_by_country, captured Aug. 18th, 2008

[52] Wikipedia, Van-Eck phreaking, http://en.wikipedia.org/wiki/Van_Eck_Phreaking, captured Jan. 21st, 2009

[53] Communication via e-mail with the Spanish Police Authorities (Cuerpo Nacional de Policia), April 15th, 2008