Security and Privacy Threats of the Belgian Electronic Identity Card and Middleware

Pieter Verhaeghe[1], Jorn Lapon[2], Vincent Naessens[2],
Bart De Decker[1], Kristof Verslype[1] and Girma Nigusse[1]

[1] Katholieke Universiteit Leuven, Department of Computer Science,
Celestijnenlaan 200A, 3001 Heverlee, Belgium
[2] Katholieke Hogeschool Sint-Lieven, Department of Industrial Engineering
Gebroeders Desmetstraat 1, 9000 Gent, Belgium

Abstract. The Belgian Electronic Identity Card was introduced in 2002. The card enables Belgian citizens to prove their identity digitally and to sign electronic documents. Today, many application developers foresee e-ID plugins in their applications. Users may even be forced to use their e-ID card to access certain services. However, inappropriate use of the card may cause harm to individuals.
This paper gives a detailed overview of privacy and security dangers related to the Belgian e-ID card and the current middleware. Existing threats are classified according to multiple categories. Finally, we point to possible solutions to tackle the weaknesses.

1 Introduction

Belgium is one of the first countries in Europe that introduced an electronic identity card [1, 2] in 2002. Today, nearly 80% of the Belgian population has an e-ID card. The card enables the Belgian citizens to prove their identity digitally and to sign electronic documents. The Belgian e-ID card opens up new perspectives for the government, their citizens, service providers and application developers. The government aims at increasing the quality of services that are offered to its citizens by implementing e-government applications. For instance, using the e-ID card, individuals can consult personal information stored in governmental databases [3, 4]. They can also request official documents [5] or submit and consult tax declarations [6]. Players in both the public sector and the profit sector also benefit from the penetration of the e-ID card. New applications are developed and existing applications are extended with plugins that support e-ID authentication and e-ID signing [7, 8]. Some examples are e-Access applications [9, 10], e-Banking[11], e-Commerce [12], e-Health [13], ... The Flemish government also funds research projects that focus on e-ID integration [14–16]. It is clear that many application developers benefit from this evolution. Today, integrating e-ID technology for authentication purposes is a real hot topic in Belgium. However, strong authentication is not necessary in many applications. Moreover, the electronic e-ID card brings along a number of security and privacy risks. Irresponsible use may lead to economic and/or psychosocial damage. However, many citizens are unaware of these pitfalls. On the contrary, unexperienced users are encouraged (or even obliged) to use the e-ID card for many purposes.

This paper mainly outlines security and privacy flaws using the Belgian electronic identity card and middleware. Hence, a set of measures are presented that

can be adopted by government departments, citizens, application developers, e-ID developers and service providers to reduce the risks.

2 Belgian Electronic Identity Card technology

The Belgian e-ID card is a smart card that allows Belgian citizens to prove their identity visually and digitally and to sign electronic documents [17, 18]. Of special interest for this paper are the digital components embedded in the card.

Private information such as the owner's name, his address, a digital picture of the owner and his National Registry Number is stored in three seperate files, an identity file, an address file and a picture file, all signed by the government. The National Registry Number (*RijksRegisterNummer* or RRN) is a unique nation-wide identification number for each natural person. Two PIN-protected key pairs allow digital authentication and signing. The public keys are embedded in a certificate containing the RRN and the name of the card holder, signed by a government department that is part of the Belgian PKI infrastructure. The private keys are stored in a tamper-proof part of the chip and can only be activated (not *read*) with a PIN code. The cryptographic functionalities of the Belgian e-ID card are available through middleware [19]. It acts as an intermediary for all accesses to the e-ID card by other applications. Applications typically interact with the card via a simple API [20] offered by this middleware. If a document has to be signed, the middleware passes a hash of the document to the card. Similarly, a hash of the challenge is passed to the card for authentication purposes. When an application wants to authenticate or sign a document with the e-ID card, the middleware invites the user to enter the appropriate PIN code. The middleware can also verify the validity of the certificates (using CRL or OCSP). The *privacy service*, part of the middleware tools, prevents other applications to have direct access to the card. It therefore requests the user's consent when an application attempts to read the identity or address information. However, when the privacy service is disabled, applications can access the e-ID card directly.

3 Current shortcomings of the Belgian e-ID card

Careless use of the e-ID card and middleware may cause economic and psychosocial damage. This section focuses on security and privacy risks related to the use of the Belgian Electronic Identity card [21, 22]. First, we discuss the security and privacy threats assuming that both the middleware and the application are uncompromised. Next, we discuss attacks that can be performed by malicious applications. Thereafter, the assumption of trusted middleware is omitted: we show how the middleware can easily be disabled or modified. Finally, we discuss how implementation flaws can lead to privacy/security incidents.

3.1 Uncompromised middleware and uncompromised application

When both middleware and application software are trustworthy, security and privacy risks still exist. Note that these threats apply to all users.

		Privacy threats	Security threats
Uncompromised middleware	**Uncompromised application**	– Sensitive certificate attributes – Unaware authentication – Automatic certificate storage	– Signatures with incorrect key – PIN code capturing
	Compromised application	– Distributing picture, identity and address – Collecting personal records	– Surreptitious authentication – Surreptitious signatures
Compromised middleware		– Identity theft	– Denial-of-service
Implementation flaws		– Insecure communication channels – Inappropriate privacy policies	– Insecure communication channels – Incomplete validity checks – Problematic certificate chains

Fig. 1: Overview of security and privacy threats

Privacy risks. When authenticating to a service provider using the e-ID card, the authentication certificate is automatically sent to the service provider. Since the certificate contains the RRN, all actions performed by the same citizen can be linked. The date of birth and gender of the individual can also be derived from the RRN. Similarly, all signatures created with the same e-ID card can easily be linked.

Moreover, once the citizen entered his PIN code to authenticate to a certain website, the private authentication key remains activated. Hence, the PIN code is no longer required to authenticate to other sites as long as the card is not removed from the reader. When the user then browses to multiple sites that require e-ID authentication, authentication is performed transparently. This implies that users are unaware that identity information (i.e. the authentication certificate) is transferred to these sites. Another threat is related to the default settings of the middleware. When inserting the e-ID card in the card reader, the authentication and signing certificates are stored in persistent memory by default. Disabling this option prevents that these certificates are stored automatically. However, it also prevents users to authenticate with the e-ID card in certain applications (e.g. Internet Explorer).

Security risks. Documents that are signed with the signature key K_{Sig} on the Belgian e-ID card are legally binding. Multiple applications offer support to sign digital documents with the e-ID card. When a user wants to sign a document in Open Office or Adobe Reader, he can choose to sign the document with K_{Aut} or K_{Sig}. An unaware user may use his *authentication key* K_{Aut} to sign a document. Hence, verifiers must check that a valid *signing key* was used.

3.2 Uncompromised middleware and compromised application

Compromised applications can circumvent the security and privacy measures in the middleware. To prevent malicious software to access the e-ID card directly, a privacy

service was developed. However, when this service is stopped, malicious programs are no longer prohibited to access the card directly. Sometimes, the user has to disable the service [23] to allow applications to read other (non-Belgian e-ID) smart cards.

Privacy risks. The picture, personal and address information on the e-ID card is not PIN-protected. In normal circumstances, the middleware will request the user's consent to access this information. However, if the name of a program that makes use of the middleware API is the same as the name of a trusted application (such as beidgui.exe or beidsystemtray.exe), the user's consent is no longer required. Moreover, a program connecting directly to the card can collect identity information and distribute it over the Internet. This is especially problematic when children use their e-ID card to login at a "secure" chat box. Or if the card is used to get access to a building (e.g. sauna complex) then the identity and address data can be misused. Not only personal information that is stored on the e-ID card can be collected. After a user has entered his PIN code once, a compromised application can authenticate to multiple websites (such as tax-on-web [6], RRN dossier [5], medical records [13]) transparently and collect even more identifying data. The application can then forward this information for later misuse (e.g. identity theft).

Security risks. A malicious application can deceive the user and let the e-ID card sign another document than the one intended. Assume that a user wants to sign a document. The application can send another document to the middleware and forward the signature to a malicious host transparently. Moreover, as the PIN code for authentication only has to be entered once, an application can connect to other e-ID protected sites and order goods in the name of the cardholder. The PIN code, captured with for instance a keylogger can be exploited for clandestine authentication or signing, in case the privacy service is stopped.

3.3 Compromised middleware

A malicious program running with administrative privileges can also compromise the middleware. The modified middleware will probably have a similar GUI, so that the user will not notice any difference. Compromised middleware can have full control to identity information on the card and the PIN code can be intercepted and stored unless a card reader with separate keypad is used. Thereafter, it can be used for fetching more information from protected websites during a longer period. Malicious middleware can have full control over the authentication and signing functions and can even change the PIN code transparently. Hence, the card can no longer be used by the owner.

The same attacks are possible if an individual uses his card on an untrusted platform. Assume that a malicious insurance company asks an individual to insert his e-ID card and enter his PIN code on a workstation to sign the insurance contract. Meanwhile, if no keypad is used, the PIN code can be intercepted and personal records can be retrieved by that workstation, by transparently authenticating to trusted web services that keep records of that user. The insurance company can then stipulate other conditions in the contract based on the collected info.

3.4 Implementation flaws

Many application developers include e-ID plugins in their software. However, not all developers are security specialists. This may lead to implementation flaws that

can result in privacy and security problems. For instance, web servers may enforce users to authenticate over an insecure connection. If so, all identity information that is transferred can be eavesdropped. Moreover, web servers do not always check the validity and revocation status of the authentication/signing certificate. Many web servers also have credential management problems (even servers that are administered by the government such as [5]). When a client connects to a secure site, the server should return a chain of certificates required to verify the server certificate. Many servers are not configured appropriately. Hence, the user receives a warning that the server certificate could not be verified. Many users ignore that warning and proceed. However, connecting to a malicious web server will often result in the same warning.

4 Improvements

This section proposes solutions to offer better security and privacy protection to the information on the e-ID card and to give more control to the user if personal information needs to be released.

Some simple techniques can be applied to realise a more privacy friendly e-ID card. A first solution is to divide the information stored in the identity file into multiple files. The release of these files should only be possible with consent of the user. Moreover, some information (especially the RRN) may only be revealed after successful authentication of the requesting parties (e.g. the police, government, ...) to the card. A second solution is that every attribute in the identity file can be encrypted. Hence, the user can select a set of decryption keys (and thus the part of identity information) that is released to the application. A similar technique is to hash each personal attribute instead of encrypting it and to reveal a subset of corresponding attribute values instead of decryption keys. An application can easily verify the correctness of the disclosed personal data by comparing the hash of each value with the corresponding hashes in the identity file. A more flexible technique is to use anonymous credentials[24]. With such a credential, it is for instance possible to prove that you are older than 18 years without revealing your birth date. Moreover different proofs are not linkable. Since this protocol requires a lot more computational resources, this cannot be implemented yet on a smart card. However, in the long term this should be possible since the computational capabilities of smart cards are steadily improving.

In order to give more control to the user of which action is performed on the e-ID card, there should be a different PIN code for authentication, signing and reading out identity information. Moreover, certified card readers can have a keypad and a small screen. This way, users can enter their PIN code securely and do not longer need to trust the middleware on the PC. The screen on the card reader can display the hash value of the document that is to be signed or the personal data that will be released. This hash prevents malicious programs to sign another document than the one intended. To enforce that only certified card readers are used, the card readers should authenticate to the e-ID card.

To make the authentication and signature certificate more privacy friendly, the names and RRN should be replaced by the hash of the identity file. Hence, when the user authenticates to a server, the RRN is no longer revealed. This way the user has control of which attributes he wants to give to the other party.

5 Conclusion

The main part of this paper discusses privacy and security risks using the Belgian e-ID card technology. These threats are classified according to multiple categories to make a clear overview of the current dangers with the e-ID card. As the number of e-ID applications still increases and as citizens will be obliged to use their e-ID card to benefit from certain services, these threats can cause harm on a very large scale. To tackle those risks, a set of improvements was presented in the last part of this paper.

References

1. D. De Cock, C. Wolf, and B. Preneel, "The Belgian Electronic Identity Card (Overview)," in *Sicherheit 2005: Sicherheit - Schutz und Zuverlässigkeit, Beiträge der 3rd Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.v. (GI)* (J. Dittmann, ed.), vol. LNI P-77 of *Lecture Notes in Informatics (LNI)*, (Magdeburg,DE), pp. 298–301, Bonner Köllen Verlag, 2006.
2. D. De Cock, K. Wouters, and B. Preneel, "Introduction to the Belgian EID Card: BELPIC," in *European PKI Workshop: Research and Applications* (S. Gritzalis, S. K. Katsikas, and J. Lopez, eds.), vol. 3093 of *Lecture Notes in Computer Science*, (Samos Island,GR), pp. 1–13, Springer-Verlag, 2004.
3. "The Belgian Rijksregister website." `http://www.ibz.rrn.fgov.be/`.
4. "Kruispuntbank van de sociale zekerheid." `http://www.ksz-bcss.fgov.be/`.
5. "Mijn dossier." `https://www.mijndossier.rrn.fgov.be/`.
6. "Tax-on-web." `http://www.taxonweb.be/`.
7. "Open Office." `http://www.openoffice.org/`.
8. "Microsoft Office." `http://office.microsoft.com/`.
9. "SafeBoot." `http://www.safeboot.com/`.
10. S. Gamby, L. Schumacher, and J. Ramaekers, "Securisation of SIP Presence notifications thanks to the Belgian electronic identity card," *ngmast*, pp. 125–129, 2007.
11. "KeyTrade." `http://www.keytrade.be/`.
12. "Tele Ticket Service." `http://www.teleticketservice.com/`.
13. "Be-Health." `http://www.behealth.be/`.
14. "The e-IDea project website." `http://ingenieur.kahosl.be/projecten/e-idea/`.
15. "The ADAPID project website." `https://www.cosic.esat.kuleuven.be/adapid/`.
16. M. Ide, T. Deryckere, and L. Martens, "Exploiting the Benefits of an Electronic Identity Card in an Interactive Television Environment," *ccnc*, vol. 0, pp. 809–810, 2008.
17. H. G. Jos Dumortier, *Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications*, 2007.
18. M. Stern, *Belgian Electronic Identity Card content.* Zetes, CSC, 2.2 ed., 2003.
19. P. Andries, *eID Middleware Architecture Document.* Zetes, 1.0 ed., 2003.
20. J. Rommelaere, *Belgian Electronic Identity Card Middleware Programmers Guide.* Zetes, 1.40 ed., 2003.
21. L-Sec, "Secure use of the eID," 2006.
22. E. Giles Hogben, "ENISA Position Paper No.1: Security Issues and Recommendations for Online Social Networks," 2007.
23. "KBC: Pin-verification error - stop the disturbing active processes of the e-id card." `http://www.kbc.be/welkom`.
24. J. Camenisch and A. Lysyanskaya, "An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation," in *EUROCRYPT '01: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques*, (London, UK), pp. 93–118, Springer-Verlag, 2001.