Chapter 76
Extending the Scope of eID Technology:
Threats and Opportunities in a Commercial Setting

Vincent Naessens
Katholieke Hogeschool Sint-Lieven, Belgium

Bart De Decker
Katholieke Universiteit Leuven, Belgium

ABSTRACT

In 2002, Belgium has adopted an electronic identity card as one of the first countries in Europe. By the end of 2009, the roll-out of the eID card will be completed. This means that each Belgian citizen will possess an eID card. The card enables her to digitally prove her identity and to legally sign electronic documents. The Belgian eID card opens up new opportunities for the government, its citizens, service providers and application developers. The Belgian eID technology originally aimed at facilitating transactions between Belgian citizens and the government. Although many eID applications have been developed, the success of the Belgian eID technology has not been what was expected. Therefore, the Belgian government encourages developers to build commercial applications that use the eID card (for authentication or e-signatures). However, extending the scope of the Belgian eID technology from e-government to the commercial sector is no sinecure and not without risks.

INTRODUCTION

Every Belgian citizen (older than 12) has an electronic identity card since 2009. The Belgian Electronic identity card (BeID) allows citizens to identify themselves, to authenticate and to sign electronic documents. The BeID technology originally aimed at facilitating transactions with the Belgian government. Using the BeID *authentication* and/or *e-signature* functionality, citizens can get access to personal information stored in governmental databases[1] (such as personal records at the National Registration Office), retrieve official documents[2] (such as proof of birth/life/residence/nationality), declare their taxes[3], report criminal offences, etc. The card also supports *identification* of the card holder to police forces and to

DOI: 10.4018/978-1-60960-042-6.ch076

authorized border control officials. Identification with the BeID avoids inconsistencies and results in more reliable governmental databases (e.g. no double entries for the same individual due to manual input errors). Moreover, the card technology impedes counterfeiting and hence, identity fraud. Orthogonal to the basic functionality of the card, user-friendliness and restriction of integration/deployment costs were crucial concerns. As mainly governmental applications[4] were targeted, privacy was less important[5]. These concerns had an impact on the design of the BeID card. For instance, the user's address is stored in the chip and is not printed on the card. Hence, there is no need for issuing a new BeID when a user moves to another address (i.e. the address file can be updated). Furthermore, the card implements no access control mechanism to read out the stored picture, identity and address files. Hence, the police can easily retrieve the data while keeping the infrastructural costs minimal (a simple card reader suffices; no keys/certificates need to be installed or regularly updated). Another concern was the "simplicity to integrate the BeID in existing or new applications". Application developers should not be security experts, and hence, it should be easy to use the BeID as a means to authenticate to web services. Since TLS (SSL) is one of the paradigms for mutual authentication in web applications, it seemed appropriate to make the card TLS-compatible. The threat model and design decisions (driven by low cost, high usability and easy deployment) were reasonable in the initial setting (i.e. the e-government domain). However, these design decisions result in serious privacy and security risks when extending the BeID technology to other domains (e.g. the commercial sector) (Verhaeghe et al., 2008). Currently, many countries and regions are planning to introduce eID technology. Each of them will be confronted with similar design decisions. Testing and evaluating the technology within one domain and later extending it gradually to other domains seems a good strategy. This strategy is indeed reasonable to evaluate certain parameters (such as usability, performance and cost). Yet, changing the setting may also change the privacy and security risks.

This paper elaborates on those risks and presents (partial) solutions. The rest of this chapter is structured as follows. First, an overview of the BeID technology (the card, the middleware and existing BeID applications) is presented (see section 2). Second, the crucial barriers that delay and hinder the development of commercial eID applications are classified (see section 3) and some (ad hoc) solutions are presented. Next, more structural approaches are discussed to accelerate commercial eID applications with the current card. The requirements and solutions resulted from discussions with many SMEs and large companies in Flanders within the scope of a technology transfer project funded by the government. Reusable software extensions as well as a framework that integrates the crucial components for privacy-friendly eID applications are presented. It will be shown that those solutions may tackle some major weaknesses and will lead to *second generation BeID applications*. However, some security threats still remain and can only be solved by a different eID design. The current BeID is therefore compared with other approaches, namely a domain-specific approach and a service-specific approach (e.g. the German eID card). The alternatives are compared and evaluated on multiple parameters (infrastructural cost, performance, usability, security and privacy). This chapter ends with a general conclusion.

OVERVIEW OF THE BELGIAN EID TECHNOLOGY

The Belgian eID card (Stern, 2003) is a smart card that allows Belgian citizens to both visually and digitally prove their identity and to sign electronic documents. The eID card contains three files: (1) a digital picture of the card holder, (2) an identity file, which contains the basic identity information