Chapter 12
The German Electronic Identity Card: Lessons Learned

Christoph Sorge
CISPA and Institute of Legal Informatics, Saarland University, Germany

ABSTRACT
Authentication is an important aspect of e-government applications, as in many cases the identity of a citizen has to be established before provision of a service. Germany is among the countries that have established an electronic identification and authentication infrastructure, based on an electronic identity card. The card enables both local and remote authentication to service providers and authorities. While privacy-enhancing technologies have been used to a large extent in its design and there are no known attacks on its security protocols, the eID card has been harshly criticized. Less than a third of the citizens requesting an identity card choose to activate the eID function. Using the example of Germany, this chapter discusses whether the establishment of an electronic authentication infrastructure makes sense and presents possible reasons for the German eID card’s lack of success. In addition, the author considers electronic signatures and their integration in an electronic authentication infrastructure.

INTRODUCTION
In many countries, the provision of identity cards, enabling citizens to prove their identities to authorities or private companies (like banks), is considered as a task of the state. Smartcard technology allows integrating additional features, like storage of biometric data, in such identity cards. Given the growing importance of e-business and e-government transactions, some countries have also decided to support remote authentication to the respective service providers. Both developments can be combined (i.e., remote authentication can be performed by a chip on an identity card), but this is not strictly a necessity. For example, Malaysia’s MyKad (Loo, Yeow, & Chong, 2009) uses a multi-application smartcard that can, in principle, be used locally and remotely. The Austrian Bürgerkarte for remote authentication, on the other hand, is not bound to a national iden-
The German Electronic Identity Card

In this chapter, we focus on Germany, where a new identity card was introduced in November, 2010. Besides changing the dimensions of the identity card and improving the protection against forgery, the main innovation lies in the addition of a contactless smartcard. Like existing electronic passports, the smartcard can be used at border controls and during other inspections of the identity card by authorities; this way, the authenticity of the data contained on the card can be confirmed, and (optionally) stored fingerprints can be used for biometric verification of the card holder’s identity. Like in case of the (older) electronic passport, data stored on the smartcard can be digitally signed, thus making it very difficult (if not impossible) to forge any information.

In addition, the smartcard can also be used for (remote) authentication to service providers, e.g. online retailers, banks or e-government services (so-called eID function). This feature requires the user to purchase a smartcard reader; the service provider needs a certificate confirming his authorization to use specific information from the identity card, and server software implementing the protocols used by the card. For each service provider, a different identifier is used; the creation of user profiles across service providers is therefore not possible based on those identifiers.

Finally, the electronic identity card is a secure signature creation device, as specified by the European Signature Directive; thus, it can potentially be used to sign documents in a legally binding manner. However, the certificates used in the signature creation process are issued by private companies.

The remainder of this chapter is structured as follows: First, we give a short overview on smartcards, and describe the technology and the infrastructure used for the German eID card. We then comment on the current adoption of the electronic authentication infrastructure based on the eID card. Next, based on the example of Germany, we discuss whether the introduction of such an infrastructure makes sense, and describe related benefits. The chapter concludes with an outlook on possible future research directions.

BACKGROUND

In this section, we first provide some general background about smartcards, before looking at the German eID card in more detail.

Smartcards

Though the idea of smartcards has been around since 1968, the first major successful rollout was not until the 1990s (Shelfer & Procaccino, 2002). Among the earliest applications was the replacement of banking cards with magnetic stripes: smartcards have the advantage of a greater memory capacity. In this chapter, we focus on smartcards that come with a processor, instead of pure storage cards; in fact, some authors consider only such processor cards as smartcards.

Such a processor can enforce access control restrictions, and in addition, it can perform (cryptographic) computations. For example, cryptographic keys can be stored on the card, and the processor makes sure that these keys are only used after the card holder has been authenticated using a secret PIN. The keys never have to leave the card. As a consequence, some operations that have to be performed by a trustworthy component (e.g. the computation of an electronic wallet’s current balance) can be performed on the card, while previously (using magnetic stripes), a trusted server had to be contacted.

Among the most common smartcards are bank cards and subscriber identity modules (SIM cards) used for the authentication of mobile phones.
Related Content

E-Government Research: Capabilities, Interaction, Orientation, and Values
www.igi-global.com/chapter/government-research-capabilities-interaction-orientation/7325?camid=4v1a

Conquering the Invasion of Technology: E-Government and Property Tax Collections in the Stonewall County Tax Commissioner's Office
www.igi-global.com/chapter/conquering-invasion-technology/6193?camid=4v1a

Towards Digital Governance in UK Local Public Services?
www.igi-global.com/chapter/towards-digital-governance-local-public/21458?camid=4v1a

Harnessing Interagency Collaboration in Inter-Organizational Systems Development: Lessons Learned from an E-government Project for Trade and Transport Facilitation
www.igi-global.com/article/harnessing-interagency-collaboration-inter-organizational/45740?camid=4v1a