**From Student Smartcard Applications to the German Electronic Identity Card**

Lucie Langer, Axel Schmidt, Alex Wiesmaier
Technische Universität Darmstadt, Department of Computer Science, Darmstadt, Germany
langer@cdc.informatik.tu-darmstadt.de
axel@cdc.informatik.tu-darmstadt.de
wiesmaier@cased.de

**Abstract:**
This paper deals with the German electronic identity (ID) card, which is to be introduced in November 2010. Apart from enhancing the possibilities for identity checks by providing biometric identifiers, the new ID card will enable citizens to prove their identity to service providers and administrative authorities over the Internet. This is going to open up a variety of applications in e-Government and e-Business.

While the national ID card is yet to come in Germany, similar concepts have already been realized at a smaller scale: At Technische Universität Darmstadt (TUD), a student smartcard was introduced in the 2005/2006 winter term. It offers the students a digital proof of identity, which can be used to access electronic resources and services provided by the university. Thus this "TUD card" works as an electronic ID card for the university campus, which makes it a good starting point for extrapolating this scenario to a nationwide ID card.

The goal of our work is to compile and analyze the potential applications of the upcoming German electronic ID card. We approach the issue by categorizing the applications according to their purpose of use. For each category, we start with examples of matching TUD card applications. Then we generalize from campus-bound use to the scenario of a nationwide ID card and describe application possibilities in e-Government as well as e-Business.

As we specify potential applications for the ID card, this work is relevant to private and public service providers and may encourage them to prepare for the upcoming introduction of the ID card. Our work also aims to increase the acceptance of the ID card among the German citizens. We show how the ID card increases the usability of existing online services and how it allows for new services which have not been feasible so far.

**Keywords:** German electronic ID card, e-Government and e-Business applications, identity management

## 1. Introduction

In July 2008 the German Federal Government approved a new law governing the German electronic ID card. Besides providing all functions of its non-electronic predecessor, the new ID card is supposed to facilitate online identity management and also improve its security. The electronic ID card will enhance online authentication and it will open up a variety of possibilities regarding e-Government as well as e-Business. Besides facilitating the citizens' everyday life and securing activities on the Internet, the new ID card will provide improved fraud resistance (Federal Ministry of the Interior 2008).

The electronic passport (Federal Office for Information Security 12 Jan 2009) was introduced in 2005 and made Germany one of the first countries in the world to issue biometric passports. The electronic ID card is a relevant and up-to-date reaction to the ongoing transformation of service delivery and thus will be another important step towards security in an online society.

At Technische Universität Darmstadt (TUD), a student smartcard was introduced already in the 2005/2006 winter term. It offers the students a digital proof of identity and thus can be referred to as a campus-bound ID card. We take this TUD card as a basis for our investigation of possible ID card applications. The focus of the paper is not on providing technical details of the respective cards, but rather on highlighting possible application scenarios for the upcoming electronic ID card and thus emphasizing its relevance.

The paper is structured as follows. In Section 2 we introduce the TUD card as well as the new electronic ID card and describe their functionality in a generally understandable way. In Section 3 we investigate potential applications of the upcoming electronic ID card by extrapolating the campus-bound TUD card applications. Section 4 summarizes the paper.

## 2. TUD card and electronic ID card

### 2.1 The TUD card

In the 2005/2006 winter term, an electronic ID card for students and staff members was issued at TUD. This smartcard provides two independent functions. It holds the student's digital identity and thus enables its holder to access electronic resources and services provided by the university. Additionally, it can be used as an anonymous electronic purse for various utility services such as cafeteria, refectory, vending machines and also for copiers and printers on the campus. As this functionality is not relevant for identity management, we restrict the scope of Section 3 to the function of the TUD card as an electronic ID for the university campus.

The following personal data is stored on the TUD card: Full name, abbreviation of the owner's organizational unit (which is "STUD" for students), university e-mail address and an university member ID or the user name provided by the campus data center respectively. From the outside the card shows only the university logo and a serial number and is otherwise anonymous. Thus, the TUD card surface does not reveal the identity of the owner but merely shows the university affiliation.

The TUD card holds two different chips: A contact chip and a contactless RFID chip. The contact chip uses the TeleSec Chipcard Operating System (TCOS) (Deutsche Telekom 1999). It holds the owner's private signature key as well as the respective public certificate and provides a cryptographic processor. The signature key enables the students both to sign electronic documents and to gain logical or physical access to applications, computers or university buildings respectively via certificate-based authentication. For these actions a card reader is necessary and the student has to enter the correct PIN. The PIN is set when the card is activated. At this point also the user's certificate is uploaded to the card. The RFID chip provides the payment function and is also used for accessing lockers in the university libraries.

### 2.2 The German electronic ID card

According to §1 of the German Identity Card Act (Gesetz über Personalausweise, PersAuswG), every German citizen aged over 16 years is obliged to hold an ID card to be able to prove his or her identity (PersAuswG 1986). The data on the ID card includes the signature and biometric photograph of the holder as well as his or her full name, day and place of birth, height, eye color, address and citizenship.

In July 2008 the German Federal Government approved the law governing the electronic ID card. The ID card is supposed to be issued to German citizens starting November 2010. The credit card sized identification document will provide an ISO 14443 (ISO 2009) compliant contactless RFID chip. In the following we explain the three different functions of the ID card.

1. Identification (electronic passport function)
The electronic ID card may be used for identity checks within the country and also as a travel document for specific countries in substitution for a valid passport. As to the current non-electronic ID cards, personal information such as name and address will be visibly applied to the new card to allow for identity checks by visual inspection. In addition, the electronic ID card will provide biometric information about the owner. While the digitalized photograph is mandatory, each citizen may decide whether his or her fingerprints are to be stored digitally on the ID card. Biometric data is exclusively accessible to sovereign authorities.

2. Electronic identification for e-Government and e-Business applications (electronic ID function)
In addition to the human readable information on the ID card, the holder's personal data is stored securely on the RFID chip in the card. This enables citizens to authenticate against third parties such

as online service providers in e-Government and e-Business. Upon the holder's request, the electronic ID function of the ID card can be activated or deactivated at any time by the competent authority, i.e. the identity cards office. Making use of the electronic ID function requires a computer and a certified card reader. The ID card holder proves his or her identity to the service provider. The service provider proves its authorization to read personal data from the card. The latter is accomplished by providing a certificate of authorization which the service provider receives from a public agency upon justified application.

3. Qualified electronic signature
The ID card allows for an optional chargeable certificate which supports qualified electronic signatures according to the German Signature Act (Signaturgesetz, SigG 2001). Citizens who decide to include such a certificate in their ID card can thereafter use it for issuing legally binding electronic signatures as an equivalent to handwritten signatures. This facilitates many e-Government and e-Business applications.

## 3. Transferring TUD card applications to the electronic ID card

As explained in Section 2.1 the TUD card works as an electronic ID card for the university campus. This makes it a good starting point for extrapolating the campus-bound application scenario to a nationwide ID card. In the following we describe examples of TUD card applications. We subsequently use them to generalize from campus-bound use to the scenario of a nationwide ID card, providing application possibilities for the ID card in e-Government as well as e-Business. The applications are categorized according to their purpose of use. Each of the following Sections 3.1 to 3.6 deals with one category. The applications described in Sections 3.1 to 3.5 are related to the authentication function of the electronic ID card. The applications described in Section 3.6 are related to the ID card's signature function.

### 3.1 Authenticated data interchange

The TUD card enables the students to interchange authenticated electronic data with the university. This includes both upload to and download from secured university servers.

An example of an authenticated upload is the submission of completed exercises. It is usual that students have to complete a couple of exercises at home during a semester. There are fixed closing dates at which the students must have submitted their completed exercises to the university. The university provides the students with the possibility to upload their exercises using the TUD card. For doing this, the students open a dedicated website and authenticate using their TUD card. Upon successful authentication the students can submit their exercises. If the closing date has not yet expired, the website presents a respective upload dialog. By knowing the students' ID from the TUD card, the university server is able to link the uploaded exercise to the respective student. By using the TUD card it is assured that each student is able to upload exercises in his or her own name only. The students have to assure that the exercises have been completed without inappropriate help by others.

An example of an authenticated download is the retrieval of lecture notes or similar documents from the university. Students who are registered for certain lectures are entitled to receive the respective lecture notes or other related documents. Students not registered to these lectures are not entitled to receive these documents. The university provides the students with a means to download such documents using the TUD card. For doing so, the students open a dedicated website and authenticate using their TUD card. Upon successful authentication the students can select the documents they want to download. By knowing the students' ID from the TUD card, the university server is able to determine whether a student is allowed to download the desired documents or not. By using the TUD card it is assured that each student is able to download documents in his or her own name only. The students have to assure that they do not give the downloaded documents to others.

These scenarios can be transferred to applications for the German electronic ID card. There are possible scenarios for both, authenticated upload and authenticated download of electronic data.

An example of a possible authenticated upload using the electronic ID card is the submission of the income tax return request to the responsible authorities. The authenticity of the income tax return forms is established by the citizen's legally binding signature. But other associated documents, such as bills or receipts, are signed by third parties and lack an intrinsic authentication by the submitting citizen. Thus, the whole request (forms and associated documents) has to be submitted to the authorities in an authenticated manner. The submission of the request may be realized via data upload using the electronic ID card in analogy to the upload of exercises using the TUD card as presented above.

An example of a possible authenticated download using the electronic ID card is the retrieval of registration cards from registration offices. For data privacy reasons it has to be assured that registration cards are protected against unauthorized disclosure. The download of registration cards may be realized via data download using the electronic ID card in analogy to the download of lecture notes using the TUD card as presented above.

### 3.2 Authenticated orders and bookings

The TUD card enables the students and staff members to access shared resources in a centralized and controlled manner. This includes both reservation and cancelation of resources.

An example of this is the scheduling of seminar rooms. All staff members and certain students may freely book certain seminar rooms. As long as a room is not booked by another person, each authorized person is able to book this room for his or her own purposes. Each staff member and authorized student is able to see which rooms are booked at which time, by whom and for what purpose. A booking can be cancelled by the person who booked the room or by the administrators only.

The university provides the staff members and selected students with a means to book these rooms using the TUD card. In order to do so, the staff members or the authorized students open a dedicated website and authenticate using their TUD card. After a successful authentication the staff members or the selected students respectively can view a calendar containing the reservations of all seminar rooms in the system. By selecting existing reservations detailed data regarding these reservations can be viewed. If the viewed reservation is booked by the person himself or herself, the reservation can be changed or cancelled. By selecting free slots, seminar rooms can be booked. By knowing the ID of the booking person from the TUD card, the university server is able to link a reservation to the respective person. Having this information, the server is also able to determine which existing reservations may be changed by this person. By using the TUD card it is assured that each staff member or selected student can book seminar rooms in his or her own name only.

This scenario can be transferred to the electronic ID card. The possible applications include reservation and cancelation. An example of a possible authenticated booking using the ID card is car rental. A customer willing to rent a car is interested in seeing which cars are available at which dates. For privacy reasons a customer is not allowed to see who booked a certain car at a certain time or who booked any cars at all. Depending on the company's policy the customer may have the possibility to change or cancel reservations already made by this customer. The booking of rental cars may be realized using the electronic ID card in analogy to the seminar room booking using the TUD card as shown above.

### 3.3 Authenticated queries

The TUD card can be used for special queries in the campus environment. The students can, for example, use their TUD card to query their grades or results of exams. Therefore the TUD provides a secure database server hosting all information about test results and general grades. The information can only be accessed after a successful authentication of the student using his or her TUD card.

Generally speaking, this kind of activity is an authenticated query for personal information provided by an official institution. Outside the campus there are many similar scenarios where the national ID card could be used in the same way. Citizens could, for example, access a database holding information on their pension insurance. Currently, such a query has to be issued via postal service and has to include a handwritten signature for authentication purposes. Of course this takes more time and effort than issuing an electronic query.

Another example is the driver's license points system which is used in Germany. Starting at a given level of severity, each person holding a driver's license receives points for transportation offenses. At 18 points the license is confiscated. Using the ID card each driver can access the database containing the driver's license points to see the current points he or she has accumulated. Other possible applications are gaining access to personal data at the health insurance company or data concerning entries in the driver's offenses records at the automobile insurance.

### 3.4 Authenticated registration and application

Students can use their TUD card for registration purposes at the campus. For example, they can register electronically for courses they want to take. The same way they can apply for exams they need to pass. In order to do this, the students authenticate against the corresponding service in the university's network using their TUD card. The network can be accessed from computer pools located at the campus or remotely using the Internet. In order to accomplish registration processes the students authenticate against and submit data to a web service where the data is processed further.

This idea can be transferred to the more general scenario of the national ID card. Here, similar applications can be found in e-Government and e-Business scenarios. For example, in the field of e-Government applications the ID card enables the user to register his or her vehicle at the responsible authority. Similarly, citizens can register at the registration office after moving to a new location. Moreover, citizens can apply online for the qualified electronic signature feature of the new ID card. Finally, registration for online civil service portals or for Internet services like secure e-mail can be realized using the ID card.

In the field of e-Business, the ID card could be used to support the citizens in online business process execution. In this context a proof of identity is usually necessary. For example, users could use the ID card to apply online for bank accounts. Using the ID card avoids the need for additional proof of identity using classical offline methods because the electronic ID card can do the same completely online. Hence, processes requiring proof of identity may be transferred to the Internet. This holds for many different processes in business and public administration areas.

### 3.5 Authenticated access

The TUD card can be used to provide logical as well as physical access control. The contactless RFID chip in the card allows for authenticated access to university buildings and rooms such as student computer laboratories and hence enables physical access control. Inside the laboratories, the students can again use their TUD card to log on to the workstations. The card can also be used to establish a Virtual Private Network (VPN) in order to access internal web sites of the university network from outside the campus. Both these scenarios of logical access control (i.e. computer log on and VPN access) are accomplished via certificate-based authentication.

Regarding the scenario of authenticated access via national ID card, a variety of applications is possible. As an example, the ID card can be used to provide access control in companies or institutions. This way the badges which are used for staff authentication will no longer be necessary. At the same time, access control for external visitors is facilitated as manual control can be automatized.

In the world of employment the notion of the mobile office is becoming increasingly important. Besides on-site authentication, access control and computer login at work, the ID card can as well be used for remote work purposes. Employees working at home have to access the internal network of the company and can for example be required to authenticate via ID card in order to gain access.

Furthermore, the ID card can be used as an electronic car key: The electronic ID function of the ID card provides additional authentication in order to drive a car. Thus access to the car is restricted to the owner or to a specific group of people. This could be a strong measure to prevent car theft.

Another scenario of authenticated access via ID card is age verification. By means of the electronic ID card a user is able to prove that he or she has reached a certain age without having to reveal his or her actual date of birth (Eckert 2008). This gives an efficient method to prevent misuse of age-restricted online services such as online games or videos.

### 3.6 Qualified electronic signatures

As explained in Section 2.1, the TUD card provides a signature function. The contact chip on the card contains a cryptographic processor and holds the private signing key as well as the public certificate of the user. The TUD card can hence be used to support e-mail security by signing e-mails. It may as well be used for signing files in PDF format, and thus enhancing authenticity of electronic documents.

E-Business and e-Government applications often require qualified electronic signatures as an equivalent replacement for handwritten signatures for completing legally binding contracts or administrative procedures. Therefore, the electronic ID card will be prepared to hold a qualified certificate in accordance with the German Signature Act (SigG 2001).

The qualified electronic signature provided by the electronic ID card (upon the holder’s request) will make substantial contributions to facilitating legal transactions over the Internet. With respect to the German Signature Act (SigG 2001), only qualified signatures are equivalent to handwritten signatures. We consider two examples of possible applications in the following.

At present, employers in Germany issue about 60 million income statements for their employees per year (Federal Ministry of the Interior 2008). This practice consumes a lot of paper. An innovation referred to as ELENA (which is the abbreviation for the German expression “elektronischer Entgeltnachweis”, i.e. electronic remuneration statement) is supposed to improve this situation (Federal Parliament 2008). Instead of issuing certificates on paper, employers transmit the income data electronically to a central repository. To ensure confidentiality the income data is encrypted before it is stored in the repository. Queries to the database by authorized officials can only be performed provided that the employee involved has approved. The employee may give his or her consent by registering for the ELENA procedure and providing his or her qualified electronic signature. ELENA is supposed to start in January 2012. Citizens will be able to retrieve their electronic income statements from the repository, for example in order to apply for social security benefits such as unemployment compensation, child-raising allowance or housing allowance.

Another application scenario regarding the use of the qualified electronic signature functionality provided by the ID card is signing electronic bills. This is an important issue in e-Business. According to the German Value Added Tax Act (Umsatzsteuergesetz, UStG), electronic bills only entitle to input tax deduction if they show a qualified electronic signature (UstG 2005, §14). Although qualified electronic signatures are already possible at present; the electronic ID card will facilitate this proceeding since issuing additional signature cards will no longer be necessary.

## 4. Summary

The paper compiles and analyzes the potential applications of the upcoming German electronic ID card. By extrapolating campus-bound uses of the TUD card to the scenario of a nationwide ID card, many application possibilities in e-Government as well as e-Business are identified. The goal is to increase the acceptance for this new technology among the citizens and to encourage private and public service providers to prepare for the upcoming introduction of the ID card.

This work was funded by the Institute for Interdisciplinary Study of Politics, Law, Administration and Technology (ISPRAT) in the framework of the project Applications of the Electronic Identity Card. The responsibility for this article lies with the authors. This work was also supported by the Center for Advanced Security Research Darmstadt (CASED), a new interdisciplinary research center funded by the German State of Hesse through its Initiative for the Development of Scientific and Economic Excellence (LOEWE).

**References**

Deutsche Telekom (1999) “TCOS Betriebssystem für Smart Cards”, [online], http://www.cryptin.de/PDF/tcos20.pdf [26 January 2009].

Eckert, Claudia (2008) “Elektronische Reise- und Ausweisdokumente”, [online], http://www.oldenbourg-wissenschaftsverlag.de/fm/694/Eckert_epass.pdf [12 January 2009].

Federal Ministry of the Interior (2008) “Einführung des elektronischen Personalausweises in Deutschland“, [online], http://www.cio.bund.de/cae/servlet/contentblob/84336/publicationFile/6992/grobkonzept_02_07_2008_download.pdf [25 January 2009].

Federal Office for Information Security (accessed 12 January 2009) “ePass – Der Reisepass mit biometrischen Merkmalen“, [online], http://www.bsi.de/fachthem/elekausweise/epass.htm

Federal Parliament (2008) “Entwurf eines Gesetzes über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz)”, [online], http://dip21.bundestag.de/dip21/btd/16/104/1610492.pdf [12 January 2009].

ISO – International Organization for Standardization (2009) “Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics“, [online], http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39693 [19 January 2009]

*PersAuswG – Gesetz über Personalausweise* (1986), Version as promulgated on 21 April 1986, Federal Law Gazette I, pp. 548, Bonn, Germany.

*SigG – Signaturgesetz* (2001), Version as promulgated on 16 May 2001, Federal Law Gazette I, pp. 876–884, Bonn, Germany.

*UStG – Umsatzsteuergesetz* (2005), Version as promulgated on 21 February 2005, Federal Law Gazette I, pp. 386–433, Bonn, Germany.