Privacy-friendly revocation management without unique chip identifiers for the German national ID card

Jens Bender, Dennis Kügler, Marian Margraf, Ingo Naumann

On 1 November 2010, Germany will start issuing new identity cards. One of the main differences compared with the previous version, besides the different physical format, is the integration of an ISO14443-compliant chip that contains a government-only application for identification purposes and two commercial applications, one of which is an optional electronic signature application.

IT security and privacy considerations played a crucial role during the design phase of the electronic functionalities. Reliable protection for personal information required a co-ordinated approach to legal provisions, organisational measures and technical implementation.

The legislative framework for the current national ID card (*Personalausweisgesetz*) already contains various provisions about the use of the card, including restrictions. Thus, only in exceptional cases is making a paper copy of the ID document permitted; the serial number of the ID card must not be used for data mining purposes; and the Machine-Readable Zone (MRZ) and the data in it must only be used for government purposes.

Additional security

These provisions were transferred into the legal framework for the new, electronic national ID card. However, because of the new electronic functionalities, additional security mechanisms have to be specified and implemented. Therefore, the following requirements were taken into account during the design phase of the chip functionalities:

- All data transmissions must be encrypted.
- All transmissions of data have to be approved by the cardholder.
- An illicit use of the ID card by a third party must be impossible.
- The cardholder must know to whom their personal data will be transmitted.
- Only personal data that are necessary may be requested.
- The use of the card cannot be monitored by government institutions or other parties.
- The ID card must enable pseudonymous authentication.
- Lost or stolen ID cards must be revocable.
- Unique citizen identifiers must not be used.

The last three requirements, in particular, require a careful design of the revocation management for lost ID cards, which is our main focus here. First, we will describe the electronic authentication mechanism used by the ID card; second, we will give an overview of the implementation of revocation management. For an overview of the security mechanisms of the German ID card, see reference 2. In reference 6 there is an overview of the privacy features and data protection mechanisms of European eID cards.

Commercial applications

Besides their use in identity verification at police and border controls, national ID cards are frequently used for commercial applications. In all these scenarios, cardholders identify themselves using their ID cards (and the biometric information on them) to a business or government officer in order to prove their identity.

In general, a cardholder knows the person to whom he or she proves identity because this takes place either on the premises of the commercial organisation or the government office, or both persons involved show each other their ID cards. This is usually the basis of the trust between the two persons regardless of whether they are acting on behalf of the institution(s) they represent.

In a technical sense, a *mutual* authentication takes place. However, both parties receive just a 'snapshot' of the authentication, and they cannot prove the other person's identity to a third party. In contrast, a signature – which can, if necessary, be presented to a court or in administrative proceedings – constitutes such a proof.

Moving ID documents into the digital world

The objective of the introduction of the new national ID card on 1 November 2010 is to extend the conventional use of ID documents to the digital world. In order to meet this objective, the new ID card offers two electronic functions for e-business and e-government service providers:

- **Electronic authentication:** which enables mutual authentication of two parties via the Internet in such a way that each party knows the person with whom he or she is communicating.
- **Qualified electronic signature *(Qualifizierte Elektronische Signatur* – QES):** which is a digital equivalent to a legally binding, handwritten signature according to the German Electronic Signature Act (*Signaturgesetz*).

The cardholder has full control over the use of both functions: the ability of the card to perform an electronic authentication will be enabled or disabled when the citizen receives the card (and it can be changed later), and an electronic signature requires the prior loading of a (qualified) certificate onto the card.

Electronic authentication

According to the definitions in the *Grundschutzkatalog* of the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – BSI) the term 'electronic authentication' refers to a procedure or an operation for the verification of an identity.

The current procedure for service providers is normally to check the security features of an ID card and compare the photo to the customer; an equivalent online procedure requires different sorts of mechanisms.

Smartcard-based cryptographic protocols can replace the verification of security features – ie, the verification of the trustworthiness of the ID card. A secret PIN, only known to the cardholder, acts as a substitute for the verification of biometric features (comparing the photo). By demonstrating knowledge of the PIN, the claimant proves to be the legitimate owner of the ID card.

Another objective, in addition to the authentication of the cardholder to the service provider, is the authentication of the service provider to the cardholder. The means for doing this are Card-Verifiable (CV) certificates that can be verified by the chip on the ID card. Besides the expiry date and the name of the institution that owns the certificate, they contain fine-grained information about which data categories the service provider is allowed to access.

"A service provider applying for a CV certificate has to submit evidence as to why access to personal data on their customers' electronic ID cards is necessary for the service"

A new government institution, the Issuing Unit for Terminal Certificates (*Vergabestelle für Berechtigungszertifikate* – VfB) which is part of the Federal Office of Administration (*Bundesverwaltungsamt – BVA*), issues CV certificates to service providers. A service provider applying for a CV certificate has to submit evidence as to why access to personal data on their customers' electronic ID cards is necessary for the service; the Issuing Office verifies, in a formal procedure, that this evidence meets the requirements.

One of the main aspects of this procedure is the selection of the data fields (of the eID card) to which the access will be granted. The data protection principle of minimal disclosure applies; for example, service providers who only need to verify whether a customer is above a certain age, will only obtain access rights to a binary inquiry function for exactly this purpose (age verification). Other services such as online shops might be granted access to additional personal information such as name or address.

Service providers will receive their CV certificates from one of the trust centres that act as certification authorities (eID CA). A trust centre that wants to provide CV certificates for the German electronic ID card must fulfil the requirements for issuing qualified electronic signature certificates according to the German Electronic Signature Act and be registered at the Federal Network Agency (*Bundesnetzagentur* – BNetzA).

Pseudonyms

A special option offered by the German eID card is a card-specific and service-specific identifier that enables pseudonymous authentication. If requested, the chip generates a cryptographic token from the sector ID, which is part of the CV certificate, and a secret key is stored in the chip. Thus, this token is unique for each combination of card and service provider but different for different service providers (even using the same card) or different cards.

This token or pseudonym, therefore, enables a service provider to recognise an eID card without the possibility of cross-referencing with another service provider's authentication data.

Requirements for revocation management

In order to impede the illegitimate use of lost or stolen ID cards, the cardholder has to be able to revoke them.

A very common mechanism for chip cards – eg, qualified electronic signature cards – is the creation of a global revocation list that includes the (unique) public keys or the serial numbers of all revoked cards and/or certificates.

The disadvantage of this mechanism is that a unique public key or serial number constitutes a card-specific identifier, which acts as a direct link to the

cardholder's identity. Such a mechanism therefore contradicts the design principle of minimal disclosure.

For example, if one service provider has only access rights for age verification (see above) whereas another one also has access to other personal information, such as the name, even those who are granted full access to the service provider's databases must not be given a link to the client's authentication data. This notably applies in the case when pseudonyms are used.

A solution to this problem is the use of service provider-specific revocation lists – that is, each card provides a service provider-specific and card-specific revocation token to the service provider, who verifies it against its individual service provider-specific revocation list. The technical and organisational implementation of this concept will be described in the following section.

Technical and organisational implementation of revocation management

Every service provider who gets permission to connect to its users' eID cards using electronic authentication receives a service provider-specific revocation list which is derived from a global revocation list. The service provider-specific and card-specific revocation token which is sent to the service provider during authentication can then be compared with the entries in that list in order to identify revoked ID cards.

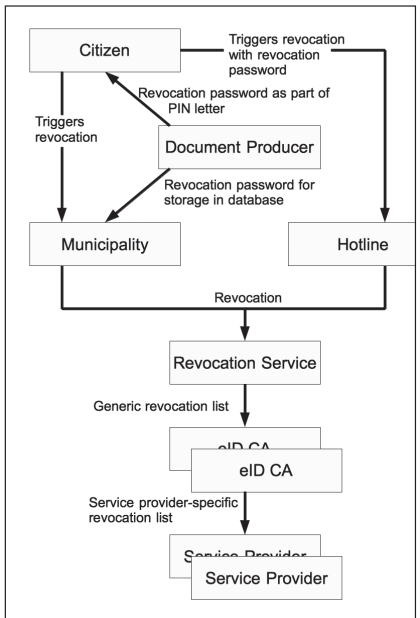

Figure 1: Overview of the revocation process for a lost or stolen ID card.

Initialisation

As revocation of a lost or stolen ID card involves several entities, an overview is shown in Figure 1. The most notable participants are the following:
The document producer
The revocation service
The eID certification authority
The citizen or cardholder
The service provider

- **Initialisation of the revocation service:** the revocation service generates a key pair and publishes the public key – referred to as the 'revocation sector public key' (*sperrsektor*).
- **Initialisation of the service provider:** each eID certification authority generates for its clients – ie, registered service providers – an individual key pair. The public key for this key pair – referred to as the 'sector public key' (*sektorkennung*) – is calculated from the chosen private key and the service provider's public key (ie, the revocation sector public key). The service provider then receives a certificate containing its sector public key; the eID certificate authority retains the private key.
- **Production of the ID card:** the document producer generates three items for each document and sends them to the revocation service: a revocation key, a revocation password and a revocation code. They may be described as follows:
- **Revocation key:** the revocation key is the public key of the key pair generated during the production of the ID card. The corresponding private key is securely stored in the chip of the ID card and is used for the generation of the revocation token during authentication.
- **Revocation password:** the revocation password is a conventional password, randomly chosen from a list of words during the production of the document. It is: a) sent to the municipality (*Personalausweisbehörde*) where it is stored in the database (*Personalausweisregister*); and b) printed in the letter to the citizen which also contains the PIN code for the eID card. The revocation password cannot be changed.
- **Revocation code:** the revocation code (or revocation hash value) is a cryptographic hash value of a concatenation of the cardholder's date of birth, surname, first name and revocation password. The revocation code is generated during the production and sent with the revocation key to the revocation service and to the municipality where it is stored. It is used by the municipality or the revocation hotline in the case of revocation and sent to the revocation service (for authentication), and also used by the municipality in the case of withdrawal of revocation and sent to the revocation service. In principle, the municipality could also re-generate the revocation code instead of storing it.

Revocation

The cardholder can initiate the revocation at the municipality, with the police or via the revocation hotline. The revocation consists of transferring the revocation code to the revocation service.

Where the revocation is initiated via the revocation hotline, the cardholder needs to provide all data required for the generation of the revocation code – ie, the revocation password and relevant personal information.

When the revocation is initiated in the municipality, all necessary data can be taken from the municipality's database; thus, revocation is also possible if the citizen has forgotten the revocation password.

The revocation service looks up the respective revocation key and projects it 'into' the revocation sector, a mathematical operation that requires the revocation service's private key. This so-called 'activated revocation key' is then distributed to all eID certification authorities.

Calculation of service provider-specific revocation lists

The eID certification authorities carry the main workload in the execution of a revocation. It is their task to generate individual revocation lists for all their registered clients – ie, service providers. This requires the transformation of every activated revocation key into a service provider-specific revocation token by making use of the service provider-specific private key.

When authenticating to a service provider, the eID card calculates the same revocation token, which is therefore contained in the service provider-specific revocation list; this enables the service provider to recognise that the eID card has been revoked.

A detailed technical description of the implementation of the revocation management, including all cryptographic algorithms (which are based on Diffie-Hellman techniques), can be found in reference 4.

In reference 5 you will find organisational details and details concerning the calculation of the revocation code.

Privacy-friendly implementation of revocation management

The use of service provider-specific and card-specific revocation tokens makes it impossible for a service provider to recognise an ID card that has already authenticated to another service provider. Something similar applies to the revocation service: even this central institution cannot derive the service provider-specific and card-specific revocation tokens from the revocation keys (without help from the service provider and the eID certification authority). Thus, it is impossible to track an eID card by making use of the revocation mechanism.

"This privacy-friendly implementation of revocation management allows an effective revoking of ID cards without the need of a central register that contains citizens' personal information"

As mentioned previously, the generation of the service provider-specific revocation lists requires the revocation key. For security considerations, this key has a length of 256 bits and therefore cannot be memorised by the cardholder.

On the other hand, the revocation of lost or stolen ID cards has to be possible seven days a week, 24 hours a day, even when the cardholder is away from home. A possible solution to this problem would have been to store, in addition to the revocation keys, all the personal information necessary for the identification of all cardholders in the revocation service's database. This would have generated a *de facto* central database of all citizens – but this is prohibited by German law.

The implementation described here shows a viable alternative. The revocation service's database stores only the revocation keys and their respective revocation code – ie, the cryptographic hash value over the concatenation of the cardholder's date of birth, surname, first name and revocation password.

This privacy-friendly implementation of revocation management creates an effective method of revoking ID cards without the need for a central register that contains citizens' personal information.

About the authors

Jens Bender and Dennis Kügler are with the Official Electronic ID Documents section of the German Federal Office for Information Security (BSI) in Bonn, Germany. Marian Margraf is with the Biometrics, Travel and ID Documents division of the German Federal Ministry of the Interior in Berlin. Ingo Naumann was seconded from BSI to the European Network and Information Security Agency (ENISA) in Heraklion, Greece, until June 2010. All four authors have been involved in the design and implementation of the technical specifications for the new German national ID card.

References

1. Bender, Jens; Kügler, Dennis; Margraf, Marian, Naumann, Ingo. 'Das sperrmanagement im neuen deutschen personalausweis – sperrmanagement ohne globale chipindividuelle merkmale', datensicherheit und datenschutz (DuD), May 2010 (in German).
2. Bender, Jens; Kügler, Dennis; Margraf, Marian, Naumann, Ingo. 'Sicherheitsmechanismen für kontaktlose chips im deutschen elektronischen personalausweis', datensicherheit und datenschutz (DuD), March 2008 (in German).
3. Gesetz über personalausweise und den elektronischen identitätsnachweis vom 24. Juni 2009 (Germany's ID card law, in German).
4. 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.
5. Federal Office for Information Security (BSI): Technical Guideline TR-03127, Technical Architecture of the New German ID Card (in German)
6. ENISA Position Paper, 'Privacy Features of European eID Card Specifications', January 2009.