Jens Bender, Dennis Kügler, Marian Margraf, Ingo Naumann

Das Sperrmanagement im neuen deutschen Personalausweis

Sperrmanagement ohne globale chipindividuelle Merkmale

Dieser Artikel beschreibt im Detail die datenschutzfreundliche Ausgestaltung des Sperrmanagements, wie es im neuen deutschen Personalausweis zum Einsatz kommt.

Dr. Jens Bender

Referent im Bundesamt für Sicherheit in der Informationstechnik (BSI)
E-Mail: Jens.Bender@bsi.bund.de

Dr. Dennis Kügler

Referent im Bundesamt für Sicherheit in der Informationstechnik (BSI)
E-Mail: Dennis.Kuegler@bsi.bund.de

Dr. Marian Margraf

Referent im Bundesministerium des Innern (BMI)
E-Mail: Marian.Margraf@bmi.bund.de

Dr. Ingo Naumann

Referent im Bundesamt für Sicherheit in der Informationstechnik (BSI), derzeit nationaler Experte bei der European Network and Information Security Agency (ENISA)
E-Mail: Ingo.Naumann@enisa.europa.eu

1 Einleitung

Ab 01.11.2010 wird der neue Personalausweis in Deutschland ausgegeben. Wesentliche Neuerungen dieses Dokumentes sind, neben der zukünftigen Form im Scheckkartenformat, die Integration eines kontaktlosen Chips mit ISO 14443-Schnittstelle, der sowohl eine Anwendung für den hoheitlichen Bereich enthält, z.B. im Rahmen einer Grenzkontrolle, als auch zwei Anwendungen für die Nutzung im privatwirtschaftlichen Umfeld.

- **Bei der Gestaltung der elektronischen Funktionen wurden in besonderer Weise die Anforderungen an Datenschutz und Datensicherheit beachtet und umgesetzt.**

Ein zuverlässiger Schutz personenbezogener Daten kann nur durch ein Zusammenspiel rechtlicher Bestimmungen, organisatorischer Maßnahmen und technischer Umsetzungen gewährleistet werden. Auch für die bisherige Nutzung des Ausweises in der Papierwelt hat das bis heute gültige Personalausweisgesetz verschiedene Bestimmungen zum Umgang mit dem Dokument vorgesehen. So ist z.B. eine Kopie des Ausweises nur in Ausnahmefällen gestattet, die Seriennummer eines Ausweises darf nicht für einen automatisierten Abgleich in Datenbanken genutzt werden und der maschinenlesbare Bereich steht außerhalb hoheitlicher Anwendungen nicht zur Verfügung.

Diese Regelungen wurden in das neue Personalausweisgesetz übernommen. Darüber hinaus müssen aber, gerade für die Absicherungen der neuen elektronischen Funktionen, zusätzliche Sicherheitsmechanismen realisiert werden. Daher wurden bei dem Design der Funktionen des Chips insbesondere die folgenden Anforderungen umgesetzt:

- Eine Datenübermittlung erfolgt stets verschlüsselt.
- Datenübermittlungen erfolgen nur im Einvernehmen mit dem Inhaber.
- Eine unberechtigte Nutzung des Personalausweises durch Dritte ist nicht möglich.
- Der Inhaber weiß, wem gegenüber er seine Daten übermittelt.
- Es werden nur die Daten übermittelt, die auch benötigt und vom Inhaber freigegeben werden.
- Die Nutzung kann weder von einer staatlichen noch von anderen Stellen überwacht werden.
- Mit dem Personalausweis ist auch eine pseudonyme Anmeldung möglich.
- Verloren gegangene Personalausweise können jederzeit gesperrt werden.
- Ein globales eindeutiges, den Personalausweis oder den Inhaber zuzuordnendes Merkmal, existiert nicht.

Gerade die letzten drei Punkte erfordern ein besonderes Vorgehen bei der Umsetzung des Sperrmanagements für verloren gegangene Ausweise, das in diesem Artikel im Detail beschrieben wird.

Wir erläutern zunächst im zweiten Abschnitt den für E-Business und E-Government nutzbaren elektronischen Identitätsnachweis des neuen Personalausweises, bevor wir die Umsetzung des Sperrmanagements beschreiben. Für einen Überblick über die weiteren Sicherheitsfunktionen siehe [1]. In [5] findet sich weiter eine Zusammenfassung der Ausgestaltung

des Datenschutzes in verschiedenen europäischen ID-Systemen.

2 Anwendungen im privatwirtschaftlichen Umfeld

Neben der Feststellung der Identität bei der Grenz- oder Personenkontrolle, z.B durch Polizei oder Zoll, werden Personalausweise auch regelmäßig im privatrechtlichen Umfeld genutzt. Der Grundgedanke ist dabei immer derselbe. Der Ausweisinhaber weist sich gegenüber einer anderen Person, hier z.B. gegenüber einem Geschäftspartner oder einem Behördenvertreter, mit dem für seine Person ausgestellten Dokument aus und zeigt damit, dass er tatsächlich derjenige ist, der er vorgibt zu sein.

Üblicherweise ist dem Ausweisinhaber bekannt, wem gegenüber er seine Identität nachweist. Im geschäftlichen oder behördlichen Umfeld betritt man die Räumlichkeiten einer Institution oder lässt sich von der Person gegenüber ebenfalls einen Ausweis zeigen. Auf dieser Grundlage nehmen Ausweisinhaber an, dass die Personen gegenüber im Auftrag der so verkörperten Institutionen handeln.

Es findet also eine **gegenseitige** Authentisierung statt. Bei dieser Art des Identitätsnachweises handelt es sich allerdings lediglich um eine Momentaufnahme, bei der keine der beiden Parteien ohne weiteres im dauerhaften Besitz eines von Dritten anerkannten Beweises über die Identität und den Willen des anderen bleibt. Ein solcher Beweis wird durch eine eigenhändige Unterschrift geschaffen, welche bei Bedarf in Verwaltungs- oder Gerichtsverfahren herangezogen werden kann.

Ziel des neuen Personalausweises, der am 01.11.2010 in Deutschland eingeführt wird, ist es, diese herkömmliche Nutzung von Ausweisen in der „Papierwelt" auf die elektronische Welt auszuweiten. Dazu stehen zwei Funktionen für Diensteanbieter im E-Government- und E-Businessbereich zur Verfügung:

- Der *elektronische Identitätsnachweis (kurz eID-Funktion)* realisiert eine gegenseitige Authentisierung zweier Kommunikationspartner über das Internet, so dass beide Parteien wissen, mit wem sie kommunizieren.
- Die *qualifizierte elektronische Signatur (kurz QES)* nach deutschem Signaturgesetz stellt das Äquivalent zur eigenhändigen Unterschrift im elektronischen Rechts- und Geschäftsprozess dar.

Über die Nutzung beider Funktionen bestimmt der Ausweisinhaber selbst: die eID-Funktion wird entsprechend der Entscheidung des Inhabers bei der Ausgabe (oder auch später) aus- oder eingeschaltet, die QES-Funktion wird erst durch das Nachladen eines Zertifikates durch den Ausweisinhaber aktiviert.

2.1 Der elektronische Identitätsnachweis

Nach Definition aus den Grundschutz-Katalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist Authentisierung ein Vorgang oder Verfahren zur Überprüfung und Bestätigung einer Identität.

Geschieht dies auf Seiten des Diensteanbieters beim bisherigen Personalausweis durch Sichtprüfung der Sicherheitsmerkmale und Abgleich des Gesichtsbildes, müssen in der elektronischen Welt andere Mechanismen gefunden werden. Die Prüfung von Sicherheitsmerkmalen, d.h. das Überprüfen, ob ein echter Personalausweis vorliegt, kann durch geeignete kryptographische Echtheitsnachweise geschehen.

An Stelle der Überprüfung der Übereinstimmung körperlicher Merkmale (Abgleich des Gesichtsbildes) tritt in der elektronischen Welt die Eingabe einer geheimen, nur dem Ausweisinhaber bekannten PIN. Durch diesen Prozess beweist der Besitzer des Personalausweises auch rechtmäßiger Inhaber des Personalausweises zu sein.

Ein weiteres Ziel ist, dass sich nicht nur der Personalausweisinhaber gegenüber einem Diensteanbieter authentisiert, sondern auch der Diensteanbieter gegenüber dem Personalausweisinhaber. Dies geschieht über so genannte Berechtigungszertifikate, die Diensteanbieter erhalten. In diesem ist neben Angaben zur Gültigkeit und zum Inhaber des Zertifikates auch die Kategorien der Daten, die der Diensteanbieter vom Chip des Personalausweises lesen darf, enthalten.

Die Berechtigung für den Erhalt dieser Zertifikate erhalten Diensteanbieter von einer staatlichen Stelle, der Vergabestelle für Berechtigungszertifikate (VfB), die beim Bundesverwaltungsamt (BVA) betrieben wird. Dabei muss der Diensteanbieter ein berechtigtes Interesse nachweisen, personenbezogene Daten aus dem elektronischen Personalausweis auszulesen. Das berechtigte Interesse wird innerhalb einer Erforderlichkeitsprüfung festgestellt und stellt die Voraussetzung für die Vergabe von Berechtigungszertifikaten dar. Wesentliches Ziel dieses Verwaltungsaktes durch die VfB ist auch zu prüfen, welche der auf dem Chip des Ausweises gespeicherten Daten der Diensteanbieter auslesen darf. Beispielsweise erhalten Dienste, die eine Altersverifikation durchführen müssen, lediglich Zugriff auf eine Abfragefunktion, ob der Inhaber ein gewisses Alter über- oder unterschritten hat. Andere Dienste, wie zum Beispiel Online-Versandhäuser, können darüber hinaus auch Zugriff auf Daten wie Name, Vorname und Wohnadresse erhalten.

Die eigentlichen Berechtigungszertifikate werden dann den Diensteanbietern von Trustcentern zur Verfügung gestellt, den sogenannten *Berechtigungs-CAs* (die Abkürzung CA steht für Certificate Authority). Es werden nur Trustcenter für die Ausgabe von Berechtigungszertifikaten zugelassen, die den Betrieb zur Ausstellung qualifizierter elektronischer Signaturzertifikate nach Signaturgesetz bei der Bundesnetzagentur angezeigt haben.

2.2 Pseudonym

Eine besondere Funktion des elektronischen Identitätsnachweises ist das karten- und dienstespezifische Kennzeichen oder Pseudonym. Diese Funktion erzeugt aus der im Berechtigungszertifikat enthaltenen Sektorkennung des Diensteanbieters und einem auf dem Ausweischip gespeicherten Geheimnis ein kryptographisches Merkmal.

Dieses Merkmal ist für eine Karte und einen Diensteanbieter fest, aber für verschiedene Diensteanbieter bzw. verschiedene Karten unterschiedlich.

- **Das Pseudonym erlaubt es also einem Diensteanbieter, einen Ausweis eindeutig wiederzuerkennen, ohne dass jedoch ein Vergleich mit dem Pseudonym, das von einem anderen Diensteanbieter ausgelesen wurde, möglich ist.**

Das Pseudonym ermöglicht es dem Ausweisinhaber, sich pseudonym gegenüber Diensteanbietern zu authentisieren, ohne dass ein diensteübergreifendes Nachverfolgen (tracking) des Ausweises bzw. dessen Inhabers möglich ist.

2.3 Anforderungen an das Sperrmanagements

Um die missbräuchliche Nutzung gestohlener oder verloren gegangener Personalausweise zu verhindern, müssen diese vom Ausweisinhaber gesperrt werden können.

Üblicherweise werden heutige Chipkarten, wie z.B. Karten für die qualifizierte elektronische Signatur, über einen chipindividuellen öffentlichen Schlüssel gesperrt, der über eine Sperrliste abgeglichen werden kann, also über ein globales chipindividuelles Merkmal. Ein chipindividuelles Merkmal ist aber immer personenbezogen, da es den Chip und damit auch den Inhaber eindeutig identifiziert.

Solch ein Mechanismus stünde damit im Widerspruch zu der datenschutzfreundlichen Ausgestaltung der eID-Funktion, bei der nur diejenigen Daten aus dem Chip übermittelt werden, die für den Dienst benötigt werden. Beispielsweise darf ein Online-Dienst, der lediglich eine Altersverifikation für altersbeschränkte Dienstleistungen benötigt, seine aus dem Ausweis ausgelesenen Daten nicht über ein eindeutiges Sperrmerkmal mit einem Dienst abgleichen können, der Name, Adresse u.ä. Daten aus dem Ausweis erhält (dies gilt im besonderen Maße auch für das Pseudonym).

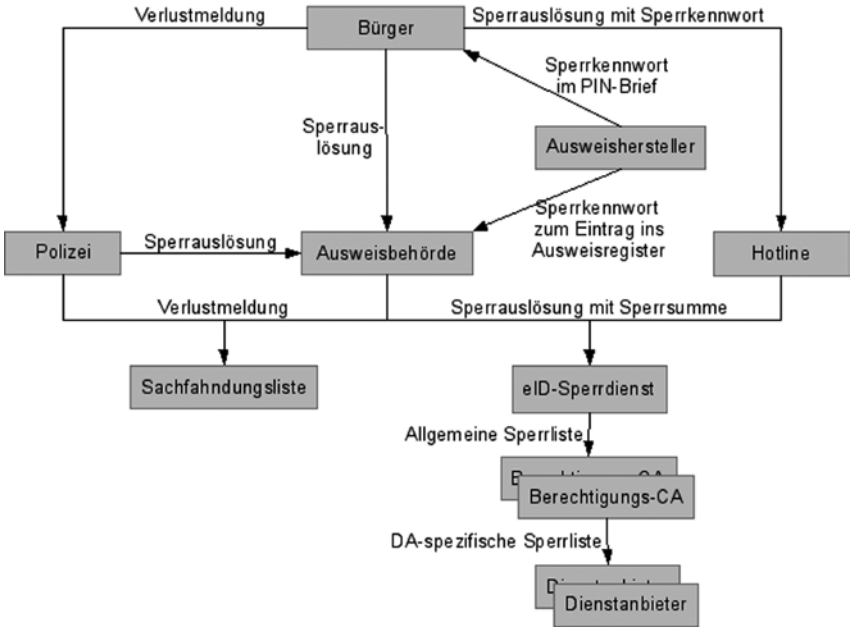
Eine Lösung dieses „Widerspruchs" ist die Verwendung von dienstespezifischen Sperrlisten, d.h. jeder Ausweis übersendet während des elektronischen Identitätsnachweises ein dienste- und kartenspezifisches Sperrmerkmal an den Diensteanbieter, den dieser gegen seine individuelle, d.h. dienstespezifische Sperrliste abgleicht.

Die technische und organisatorische Umsetzung dieses Sperrmanagements ist imfolgenden bAbschnitt beschrieben.

3 Technische und organisatorische Umsetzung des Sperrmanagements

Für jeden Dienst, der die eID-Funktion des neuen Personalausweises nutzt, wird aus einer globalen Sperrliste eine dienstespezifische Sperrliste erzeugt. Ein dienste- und kartenspezifisches Merkmal, das während der Nutzung der eID-Funktion vom Chip des Ausweises an den Diensteanbieter gesendet wird, kann dann mit den Merkmalen aus dieser spezifischen Sperrliste abgeglichen werden, um gesperrte Ausweise als solche erkennen zu können.

Abbildung 1 | Sperrauslösung



3.1 Vorbereitung

An der Sperrung verloren gegangener oder gestohlener Ausweise sind mehrere Stellen beteiligt, eine vollständige Übersicht gibt Abbildung 1. Für die Beschreibung einer Sperrung werden die folgenden Stellen näher betrachtet:

- Der Ausweishersteller,
- der Sperrdienst,
- die Berechtigungs-CAs,
- der Ausweisinhaber und
- die Diensteanbieter

Initialisierung des Sperrdienstes: Der Sperrdienst wählt ein Schlüsselpaar und publiziert den öffentlichen Schlüssel (den sogenannten *Sperrsektor*).

Initialisierung der Diensteanbieter: Jede Berechtigungs-CA erzeugt für die bei ihr registrierten Diensteanbieter ein eigenes Schlüsselpaar, wobei der öffentliche Schlüssel (die sogenannte *Sektorkennung*) aus dem gewählten privaten Schlüssel und dem öffentlichen Schlüssel des Sperrdienstes, also dem Sperrsektor, berechnet wird. Der Diensteanbieter erhält nun ein Zertifikat, das seine Sektorkennung enthält, der private Schlüssel verbleibt bei der Berechtigungs-CA.

Produktion eines Personalausweises: Der Hersteller erzeugt für jeden Personalausweis einen *Sperrschlüssel*, ein *Sperrkennwort* und eine *Sperrsumme*:

Sperrschlüssel: Der Sperrschlüssel ist der öffentliche Teil eines Schlüsselpaares, das während des Herstellungsprozesses erzeugt wird. Er wird zusammen mit der Sperrsumme an den Sperrdienst übertragen und dort zur Verwendung für eine eventuelle Sperre gespeichert. Der zugehörige private Schlüssel ist im Ausweis sicher gespeichert und wird bei der Nutzung der eID-Funktion zur Erzeugung der dienstespezifischen Sperrmerkmale genutzt.

Sperrkennwort: Das Sperrkennwort ist ein während der Ausweisherstellung vom Hersteller zufällig aus einer Wörterliste gewähltes Klartextpasswort. Das Sperrkennwort wird

- zur Personalausweisbehörde übertragen und dort im Personalausweisregister gespeichert und
- im PIN-Brief abgedruckt und so dem Ausweisinhaber mitgeteilt.

Ein Wechsel des Sperrkennwortes ist nicht möglich.

Sperrsumme: Die Sperrsumme (oder Sperrhash) besteht aus dem Hash über die Verkettung von Geburtsdatum, Vorname, Nachname und Sperrkennwort. Die Sperrsumme

- wird im Produktionsprozess vom Hersteller erzeugt, zusammen mit dem Sperrschlüssel zum Sperrdienst übertragen und dort gespeichert;

- im Sperrfalle von der Ausweisbehörde bzw. der Sperrhotline gebildet und zum Sperrdienst übertragen und
- im Falle einer Entsperrung oder einer Abfrage des Sperrstatus von der Ausweisbehörde gebildet und zum Sperrdienst übertragen.

3.2 Auslösung der Sperrung

Der Ausweisinhaber kann die Sperrung seines Ausweises bei der zuständigen Ausweisbehörde, der Polizei oder der Sperrhotline auslösen. Die Sperrung erfolgt durch Übermittlung der Sperrsumme an den Sperrdienst.

Wird die Sperrung über die Sperrhotline ausgelöst, so muss der Ausweisinhaber alle zur Berechnung der Sperrsumme notwendigen Daten (d.h. Sperrkennwort und die relevanten personenbezogenen Daten) übermitteln.

- **Bei einer Sperrung über die Ausweisbehörde können die zur Berechnung der Sperrsumme notwendigen Daten auch dem Personalausweisregister entnommen werden, so dass hier auch eine Sperrung bei vergessenem Sperrkennwort möglich ist.**

Der Sperrdienst transformiert den empfangenen Sperrschlüssel, indem er diesen unter Verwendung seines privaten Schlüssels in den Sperrsektor abbildet. Der so aktivierte Sperrschlüssel wird anschließend an alle Berechtigungs-CAs verteilt.

3.3 Berechnung der dienstespezifischen Sperrlisten

Die Hauptlast bei der Durchführung einer Sperrung liegt bei den Berechtigungs-CAs. Diese müssen für jeden der bei ihnen registrierten Diensteanbieter individuelle Sperrlisten erstellen. Dazu transformiert jede Berechtigungs-CA den aktivierten Sperrschlüssel für jeden Diensteanbieter in ein Sperrmerkmal durch Anwendung des dienstespezifischen privaten Sektorschlüssels.

Authentisiert sich ein gesperrter Personalausweis gegenüber dem Diensteanbieter, so berechnet dieser das gleiche Sperrmerkmal, das in der dienstespezifischen Sperrliste enthalten ist und der Diensteanbieter wird die Sperrung erkennen.

Eine detaillierte technische Beschreibung des Sperrverfahrens, inkl. der verwendeten kryptographischen Algorithmen (basierend auf dem bekannten Diffie-Hellman-Verfahren), finden sich in [3]. In [4] wird auf die organisatorische Umsetzung und insbesondere auf die Berechnung der Sperrsumme genauer eingegangen.

3.4 Datenschutzfreundliche Ausgestaltung des Sperrmanagements

Durch der Benutzung von dienste- und kartenspezifischen Sperrmerkmalen ist es Diensteanbietern nicht möglich, aus den von Personalausweisen übermittelten Sperrmerkmalen diensteübergreifend Personalausweise wiederzuerkennen. Ähnliches gilt für den Sperrdienst, auch diese zentrale Stelle kann ohne Mithilfe der Diensteanbieter und Berechtigungs-CAs nicht vom Sperrschlüssel auf die dienste- und kartenspezifischen Sperrmerkmale eines Personalausweises schließen, ein Nachverfolgen von Personalausweisen über den Sperrmechanismus ist somit nicht möglich.

Ebenfalls positiv im Sinne des Datenschutzes ist die Verwendung von Sperrkennwort und Sperrsumme.

Wie bereits erläutert, wird für die Erzeugung der dienstespezifischen Sperrlisten der Sperrschlüssel benötigt. Um die oben beschriebene Sicherheit des Verfahrens gewährleisten zu können, hat dieser Schlüssel eine Länge von 256 Bit und kann damit sicherlich vom Personalausweisinhaber nicht auswendig behalten werden.

- **Eine Sperrung von abhanden gekommenen Personalausweisen muss jederzeit, d.h. sieben Tage die Woche, 24 Stunden täglich und vor allem auch unterwegs möglich sein.**

Eine Lösung wäre, beim Sperrdienst neben dem Sperrschlüssel auch die für die Identifizierung notwendigen personengebundenen Daten des Inhabers zu speichern, was de facto einem zentralen Bundesmelderegister entspräche.

Das im Personalausweis zum Einsatz kommende Verfahren geht einen anderen Weg, es wird lediglich der Hashwert (die Sperrsumme) über Name, Vorname, Geburtsdatum und dem Sperrkennwort zusammen mit dem Sperrschlüssel gespeichert.

Diese Umsetzung erlaubt eine effektive Sperrung von Personalausweisen ohne ein zentrales Register, in dem personengebundene Daten gespeichert werden müssen.

4 Fazit

Das für den neuen Personalausweis zum Einsatz kommende Sperrmanagement führt die datenschutzfreundliche Ausgestaltung des elektronischen Identitätsnachweises fort. Weder zwei Diensteanbietern noch einer zentralen Stelle allein ist es möglich, Daten, die aus dem Chip des Ausweises ausgelesen wurden, mittels eines globalen Sperrmerkmals miteinander abzugleichen.

Literatur

[1] Bender, J., Kügler, D., Margraf, M., Naumann, J.: Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. DuD – Datenschutz und Datensicherheit, 32(3), 2008

[2] Gesetz über Personalausweise und den elektronischen Identitätsnachweis vom 24. Juni 2009

[3] BSI: Technische Richtlinie TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)

[4] BSI: Technische Richtlinie TR-03127, Architektur Elektronischer Personalausweis

[5] ENISA: Position Paper, Privacy Features of European eID Card Specifications. 2009