Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

NEUER PERSONALAUSWEIS

INNOVATIVE INTERNETANWENDUNGEN KOSTENGÜNSTIGE UND SICHERE AUTHENTISIERUNG

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Ulrich Waldmann
Rheinstraße 75
64295 Darmstadt

Telefon: 0 61 51 8 69-222
Fax: 0 61 51 8 69-224
ulrich.waldmann@sit.fraunhofer.de
www.sit.fraunhofer.de

Der neue Personalausweis

Im November 2010 kommt der neue Personalausweis.
Von seinem Vorgänger unterscheidet er sich äußerlich durch die Verkleinerung auf das Scheckkartenformat (ID1). Revolutionärer sind die Neuerungen im Innern: Er wird über einen RFID-Chip gemäß ISO 14443 verfügen. Dieser stellt neben einer hoheitlichen Anwendung auch eine Authentisierungsmöglichkeit (eID-Funktion) und optional eine Anwendung für die digitale qualifizierte elektronische Signatur zur Verfügung. Die neue eID-Funktion eignet sich hervorragend für E-Government und E-Commerce. Sie überträgt das Vertrauen, das sich der Personalausweis als zuverlässiges Mittel der Identifizierung in der physischen Welt über Jahrzehnte erworben hat, in die virtuelle Welt des Internets. Dabei gewinnen Anbieter und Bürger an Sicherheit. Vorteile für den Bürger: Nur wenn der Inhaber durch PIN-Eingabe zustimmt, können Anbieter Daten aus dem Ausweis auslesen. Nur vertrauenswürdige Anbieter erhalten von einer staatlichen Vergabestelle digitale Berechtigungszertifikate, um über das Internet auf den Ausweis des Bürgers zugreifen zu können. Es handelt sich hierbei nicht um X.509-Zertifikate, sondern um CV-Zertifikate (card verifiable), die im Ausweis-Chip ausgewertet werden. Sie bieten einen maximalen Schutz des Bürgers, denn der Ausweis ist durch Schadsoftware nicht manipulierbar. Vorteil für Dienstanbieter: Der Anbieter seinerseits gewinnt an Sicherheit, weil er, geschützt durch kryptographische Protokolle, die Gewissheit erhält, dass die persönlichen Daten tatsächlich aus einem amtlichen Personalausweis stammen. Bislang war es z. B. kaum möglich, zuverlässig die Postanschrift eines Kunden zu ermitteln.

Die eID-Funktion ist von Anfang an datenschutzfreundlich gestaltet worden. So enthält jedes Berechtigungszertifikat einen Verweis auf eine Datenschutzerklärung, die dem Benutzer bei der Kontaktaufnahme mit dem Anbieter angezeigt wird. Anschließend sieht der Bürger, ob der Anbieter nur den Namen oder auch weitere Daten, wie etwa Geburtsdatum und Wohnort, auslesen will. Jedes Datum kann er interaktiv freischalten oder sperren.

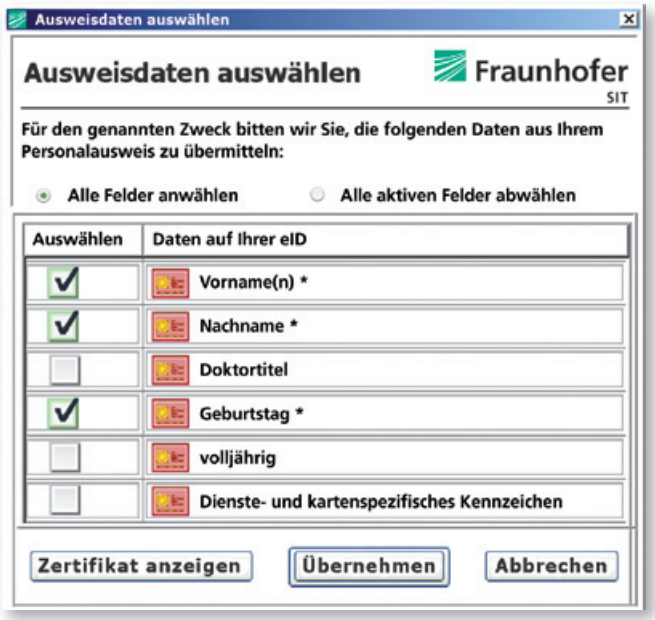
eID erfordert neues Denken

Die übliche Art, eine Verbindung zwischen Anbieter und Kunden abzusichern, führt über das TLS-Protokoll. Falls dabei überhaupt auf Kundenseite eine Smartcard vorhanden ist, wird sie in der Regel über die PKCS#11-Schnittstelle in das Protokoll eingebunden. Ein neuer Ausweis lässt sich auf keinen Fall als Schlüsselspeicher in das TLS-Protokoll integrieren. Das scheitert schon daran, dass die eID-Funktion überhaupt keine X.509- Zertifikate benutzt, weder auf Kunden- noch auf Serverseite. Stattdessen kommen mit dem neuen Ausweis neue Protokolle auf Basis etablierter mathematischer Algorithmen zum Einsatz.

Auch die Infrastruktur wird neu sein. Es wird natürlich die Möglichkeit geben, einen Ausweis auf Gültigkeit zu überprüfen. Die dabei verwendeten Sperrlisten unterscheiden sich aber wesentlich von den üblichen CRLs (certificate revocation lists), die vor zwanzig Jahren im X.509-Standard definiert wurden. Noch deutlicher sind die Unterschiede in Bezug auf die Überprüfung von

Anbieterzertifikaten. Da diese im Ausweis ausgewertet werden, der Ausweis-Chip aber keine Sperrlisten prüft, besitzen die Anbieterzertifikate nur sehr kurze Laufzeiten, etwa in der Größenordnung von zwei Tagen. Die Infrastruktur wird Dienste bereitstellen, um Anbietern automatisch neue Zertifikate zukommen zu lassen.

Für den interoperablen Zugriff auf den Ausweis hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) das eCard-API-Framework spezifiziert. Die Spezifikation erläutert, wie Anwendungen über eine XML-basierte Schnittstelle auf den Ausweis zugreifen können. Die Besonderheit der Technologie macht es erforderlich, dass sowohl Anbieter als auch Bürger über eine Implementierung der eCard-API verfügen müssen, auch wenn der Anbieter für seine Authentisierung natürlich keinen Ausweis einsetzt, sondern den Schlüssel seines Berechtigungszertifikats durch andere Mechanismen schützt.



Vorteile im E-Commerce

Anbieter können sich über den ePA einige Vorteile sichern:

- Sie erhalten die Daten des Kunden, die sie benötigen.
- Kartenausgabe, Kartenmanagement, und die gesamte Infrastruktur werden komplett von staatlich beauftragten Stellen betrieben.
- Jeder Bundesbürger über 16 Jahre erhält einen elektronischen Personalausweis.
- Berechtigungszertifikate vermitteln Vertrauen in den Anbieter.
- Identitätsdiebstahl etwa durch Erraten von Passwörtern wird in Zukunft sehr erschwert.

Es ist zu erwarten, dass durch die Existenz der eID-Funktion ein Druck auf Anbieter entstehen wird, unsichere Authentifizierungsmethoden durch sichere Alternativen zu ersetzen. Dabei ist eine frühzeitige Umstellung auf die Nutzung des ePA auch im Eigeninteresse des Anbieters.

Leistung des Fraunhofer SIT

Die Spezifikationen des elektronischen Personalausweises sind komplex. Allein die eCard-API umfasst mehr als 400 Seiten. Die Experten des SIT kennen die eCard-API, die kryptographischen Protokolle und den Aufbau der Karte in allen Details. SIT bietet dieses Wissen an, um den Ausweis kostengünstig, schnell, zuverlässig und individuell zugeschnitten in Anbietersysteme einzubinden. Die folgenden Leistungen können einzeln oder kombiniert gewählt werden:

1. Beratung zur Technik des elektronischen Personalausweises:

- Aufbau des elektronischen Personalausweises
  - hoheitliche Funktionen
  - eID-Funktion
  - Signaturfunktion
- PACE-Protokoll (Password Authenticated Connection Establishment)
- Terminal- und Chipauthentisierung

2. Beratung zur eCard-API des BSI:

- Aufbau und Einsatz der eCard-API
- Stellung der eCard-API zu herkömmlichen (SSL/TLS-basierten) Authentifizierungsmechanismen
- Nutzung der eCard-API unter verschiedenen Betriebssystemen

3. Beratung für Diensteanbieter (Server-Seite):

- Einsatz der eID-Funktion auf der Serverseite
- Erwerb und Bedeutung des Berechtigungszertifikats
- Umgang mit Datenschutzbestimmungen:
  - Datenschutzerklärung
  - Pseudonyme (»Dienste- und kartenspezifisches Kennzeichen«)
- Nutzung der Public-Key-Infrastruktur:
  - Erhalt neuer kurzfristig gültiger CV-Zertifikate
  - Gültigkeitsprüfung elektronischer Personalausweise
- Schnittstellen zu existierenden Server-Applikationen

4. Beratung für Dienstenutzer (Client-Seite):

- Übersicht über verfügbare Implementierungen des »Bürger Clients«
- Kartenterminals zur Nutzung des Ausweises
- Firewall und eCard-API
- Sicherheit des Gesamtsystems (Betriebssystem und neuer Personalausweis)

5. Weitere Leistungen nach Wunsch:

- Studien/Beratung zur Einbindung des Ausweises in Kundensysteme
- Unterstützung bei der Integration der eCard-API in Kundensysteme
- Unterstützung bei der Implementierung
- Unterstützung beim Einsatz der eID-Funktion auf Client-Seite

Informationen können in Form von Workshops oder Schulungen vermittelt werden, gerne auch im Hause des Kunden.