

Extended Access Control (EAC) und der elektronische Personalausweis (ePA)

Ein starkes Team für eine sichere Zukunft im Netz?

Im Sinne von „Never change a running team“ wird sich manch einer fragen, warum der weitreichend etablierte und akzeptierte „konventionelle“ Personalausweis ausgetauscht wird. Tatsächlich wird der Personalausweis eher vervollständigt, indem der neue ePA auf die Anforderungen einer sicheren Zukunft im Netz eingeht. Unter anderem werden Möglichkeiten geschaffen, sich anhand eines Ausweisdokuments sicher über das Internet zu identifizieren und zu authentisieren. Diese Authentisierungsfunktion wird durch den Schutzmechanismus Extended Access Control implementiert. Das vom BSI entwickelte Protokoll bildet somit die Grundlage, um unter anderem der stetig steigenden Bedeutung und den Bedürfnissen von E-Government und E-Business gerecht zu werden.

Einleitung und Notwendigkeit des ePA

Den „konventionellen“ Personalausweis kennt jeder Bürger Deutschlands. Das vom Staat ausgegebene Dokument ist langjährig etabliert und in breiter Masse akzeptiert. Das hoheitliche Identifizierungs- und Reisedokument wird sowohl in der Verwaltung als auch im privatwirtschaftlichen Umfeld für verschiedene Ziele eingesetzt. Neben vielfältigen Identifizierungszwecken wird der „Perso“ auch als Altersnachweis eingesetzt. Bereits Mitte 2008 hat die deutsche Bundesregierung die Einführung eines neuen, elektronischen Personalausweis – des ePA – beschlossen (siehe Abbildung 1). Eine flächendeckende Einführung soll im November 2010 stattfinden.

Aber was stellt die Notwendigkeit eines solchen Vorhabens dar? Eine mangelnde Fälschungssicherheit des bisherigen Personalausweises kann es nicht sein – er gehört zu den am schwersten fälschbaren Ausweisen der Welt. Vielmehr wird auf die fehlenden Möglichkeiten eingegangen, sich anhand von Ausweisdokumenten über das Internet zu identifizieren und zu authentisieren. PIN-Codes, Passwörter und Co können auf Dauer den hohen Ansprüchen nicht gerecht werden. Diese Lücke soll der ePA

schließen und eine sichere Authentisierung über das Internet ermöglichen. Das neue Dokument soll die bewährten Funktionen des konventionellen Personalausweises um elektronische Funktionen ergänzen und sich somit an die Herausforderungen und Möglichkeiten des 21. Jahrhunderts anpassen. Die Möglichkeit eines Personalausweises zur sicheren Authentisierung auf die virtuelle Welt zu erweitern, ist in Anbetracht der digitalen Gefahren lange überfällig. Der Ausweis allein erschlägt keinesfalls alle aktuellen Probleme, ist jedoch ein großer Schritt in Richtung einer sicheren Zukunft im Netz.

Der ePA als Instrument für sicheres E-Government und E-Business

Wir sind im Informationszeitalter angekommen. Nicht nur in der Privatwirtschaft, auch in der Verwaltung werden Geschäftsprozesse vermehrt auf elektronische Verfahren umgestellt – oder sind es bereits. Allerdings entstehen mit der Umstellung auf IT-Prozesse nicht nur Möglichkeiten und Chancen, sondern auch viele neue Gefahren. Es werden sichere Identifizierungslösungen benötigt, die auch für den Einsatz in der elektronischen Welt des E-Government und E-Business eingesetzt werden können. Als allgemeine Anforderungen an den ePA können Vertraulichkeit, Authentizität und Verfügbarkeit angegeben werden. Zudem muss der Ausweis einheitlich und von den Bürgerinnen und Bürgern einfach zu handhaben sein. Konkret sollen die auf dem Personalausweis aufgedruckten Daten auch in elektronischer Form vorgehalten werden. Bei der Abwicklung einer Online-Transaktion müssen die erforderlichen Informationen dem Geschäftspartner auf sichere Art und Weise elektronisch über-

mittelt werden. Dies geschieht nach einer Berechtigungsprüfung des Gegenübers sowie nach persönlicher Freigabe durch den Ausweisinhaber mittels PIN. Dieser „elektronische Identitätsnachweis“, auch Authentisierungsfunktion genannt, wird durch das Protokoll Extended Access Control realisiert.

Neben der Authentisierungsfunktion können biometrische Informationen des Inhabers in den Ausweis integriert werden. Diese können aus einem Gesichtsbild sowie Fingerabdrücken des Ausweisinhabers bestehen. Eine weitere optionale Anwendung stellt die qualifizierte elektronische Signatur dar. Diese wiederum repräsentiert das Äquivalent zur eigenhändigen Unterschrift in der realen Welt.

Die Authentisierungsfunktion des elektronischen Personalausweises

Den Begriff Authentisierungsfunktion kann man definieren als sichere Übertragung von Daten des elektronischen Personalausweises an einen berechtigten Dritten. Hierbei ist zu beachten, dass die Vertraulichkeit der Informationen, also die Authentizität und Integrität, nicht nur während der Übertragung gewährleistet sein soll, sondern auch bei der Speicherung der Daten. Die Authentisierungsfunktion soll dabei auch dem E-Government und E-Business zur Verfügung stehen, während die Identifikation mit Hilfe von biometrischen Merkmalen lediglich für den hoheitlichen Anwendungsbereich vorgesehen ist. Spezielle Anwendungen der Authentisierungsfunktion sind beispielsweise die Anmeldung eines KFZ über das Internet, die Registrierung in einem Online-Shop oder eine Altersverifikation als Jugendschutzfunktion.



Abb. 1: Ein Entwurf des elektronischen Personalausweises – BMI

EAC – Die Implementierung der Authentisierungsfunktion

Der Zugriffsmechanismus Extended Access Control (EAC) soll die eben beschriebenen Anforderungen realisieren, die Authentizität und Integrität der Daten sowohl in gespeicherter Form als auch während der Übertragung zu garantieren. Der Mechanismus EAC wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) beschrieben und umfasst in der Spezifikation der Kernfunktionalitäten rund 90 Seiten. Das Verfahren ähnelt dem Verschlüsselungsprotokoll TLS oder SSL und besteht aus den drei Protokollen „Password Authenticated Connection Establishment“, „Terminal Authentication“ sowie „Chip Authentication“ (siehe Abbildung 2). Diese werden im Folgenden näher beschrieben.

Schritt 1 – Password Authenticated Connection Establishment (PACE)

Der erste Schritt im Verfahren EAC betrifft die Sicherheit des Funkkanals zwischen Chip und Lesegerät. Das Protokoll „Password Authenticated Connection Establishment“ (PACE) schaltet den ePA frei und gibt dem Lesegerät Zugriff auf den Funkkanal zum Chip. Eine PIN, welche nur dem Inhaber des elektronischen Personalausweises bekannt ist, fungiert hierbei als Passwort. Aus kryptographischer Perspektive stellt dies eine verschlüsselte Diffie-Hellman-Schlüsseleinigung dar.

Schritt 2 – Terminal Authentication (TA)

Nachdem im ersten Schritt eine sichere Verbindung zwischen Lesegerät und ePA aufgebaut wurde, wird im zweiten Schritt des Mechanismus auf die Authentifikation des Terminals gegenüber dem Chip eingegangen. Die Zugriffsberechtigungen des Terminals werden mittels Challenge-Response-Verfahren und eines sogenannten „Terminal Certificate“ überprüft. Die Root-Zertifikate basieren auf einer internationalen Public-Key-Infrastruktur (PKI), in der das BSI die Wurzelinstanz für Deutschland übernimmt.

Das Terminal Certificate (oder auch Berechtigungszertifikat) enthält eine Liste von Attributen, auf die zugegriffen werden soll (siehe Abbildung 3). Diese Attribute können sowohl explizite personenbezogene Daten wie Vorname oder Geburtsort ent-

halten, aber auch aus impliziten Aussagen wie „Person ist volljährig“ bestehen. Letzteres kann als Jugendschutzfunktion eingesetzt werden und beachtet dennoch das Minimalprinzip in Bezug auf die Menge der preisgegebenen Daten.

Neben den Zugriffsberechtigungen für die Attribute eines ePA beinhaltet das Berechtigungszertifikat den öffentlichen Schlüssel der Endkomponente auf Serverseite. Außerdem werden Informationen mitgeliefert, wie der Name des Zertifikatinhabers oder die Signatur der ausstellenden Behörde. Das Berechtigungszertifikat muss durch einen gültigen Document Verifier signiert worden sein, um sicherzustellen, dass nur Inhalte der Datenfelder an den Server gesendet werden, für die er auch tatsächlich authentifiziert ist.

Schritt 3 – Chip Authentication (CA)

Nachdem in Schritt 1 eine sichere Funkverbindung hergestellt und in Schritt 2 das Terminal authentifiziert wurde, wird im letzten Protokollschritt des EAC der elektronische Personalausweis gegenüber dem Terminal authentifiziert. Durch die Überprüfung der Authentizität des Chips wer-

den implizit auch die Daten, die der Chip liefert, authentisiert. Dies erfolgt aus kryptographischer Sicht über eine Diffie-Hellman-Schlüsseleinigung mit statischem Chip-Schlüssel.

Erst jetzt, nachdem alle drei Verfahren (PACE, TA und CA) des Schutzmechanismus EAC abgeschlossen sind, ist ein sicherer und verschlüsselter Ende-zu-Ende-Kanal etabliert. Dieser startet beim Chip des elektronischen Personalausweises, geht über das Lesegerät und endet im Terminal, der Endkomponente auf Serverseite.

Schwachstellen und Angriffe

Der vom BSI entwickelte Schutzmechanismus EAC bietet grundsätzlich ein hohes Maß an Sicherheit. Bedingt durch die Konzeption wird den Angreifern nur eine begrenzte Angriffsfläche geboten. Beispielsweise scheitert der Austausch von Kernkomponenten in der Regel, da eine beidseitige Authentifikation in den Endpunkten stattfindet. Auch erfolgt ein Angriff auf die Transportverschlüsselung und -integrität üblicherweise erfolglos, da eine stabile Kryptographie zum Einsatz kommt.

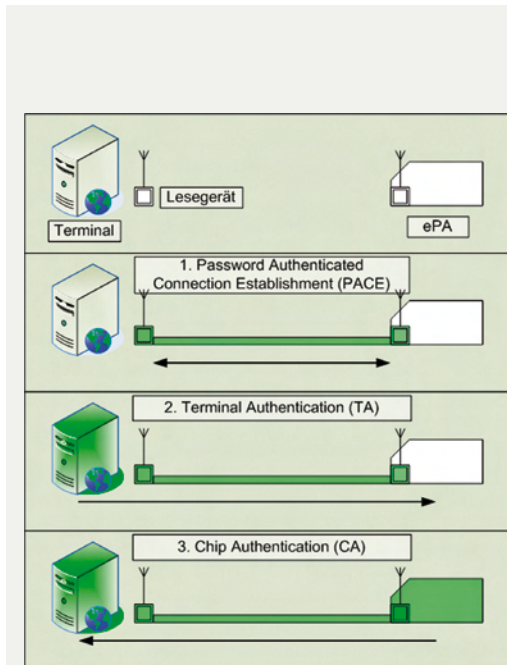


Abbildung 2: Der Ablauf des dreistufigen Zugriffsmechanismus EAC

Möchten Sie dem u.g. Zertifikatsinhaber Zugriff auf den elektronischen Personalausweis (ePA) erlauben?

Zertifikatsinhaber: DE_T_ifis_01

Attribut	Zugriff erlaubt?
Nachnamen	<input checked="" type="checkbox"/>
Vornamen	<input checked="" type="checkbox"/>
Geschlecht	<input checked="" type="checkbox"/>
Geburtsort	<input checked="" type="checkbox"/>

Das Zertifikat ist gültig.

Verwendungszweck:
Anmeldung eines KFZ

zuständige Datenschutzaufsichtsbehörde:
LDI - Landesbeauftragte für Datenschutz und Informationsfreiheit NRW

<https://www.ldi.nrw.de>

Zugriff auf ePA zulassen Zugriff auf ePA verweigern

Abbildung 3: Ein beispielhaftes Terminal Certificate. Zu erkennen sind die an- und abwählbaren Attribute Nachnamen, Vornamen, Geschlecht und Geburtsort

Die strengen Vorgaben bezüglich der Kryptographie wurden vom BSI fest in der Spezifikation verankert.

Ein möglicher verbleibender Ansatzpunkt für einen Angriff gegen den elektronischen Personalausweis kann die Verifikation des Terminal Certificate bieten. Ein ePA kann den Zugriff durch ein Terminal eventuell fälschlicherweise zulassen, falls drei Bedingungen erfüllt sind. Der Angreifer einerseits muss in den Besitz des Schlüsselmaterialeines vormals legitimen Terminals gelangen. Außerdem benötigt er ein in Bezug auf die Realzeit abgelaufenes Terminal Certificate. Der elektronische Personalausweis andererseits muss ebenfalls (negative) Voraussetzungen für diesen Angriff erfüllen. Die logische Uhr des ePA wird anhand von erfolgreichen Verifikationen in der Vergangenheit synchronisiert. Ist der Personalausweis nur sehr selten im Einsatz, so ist die Abweichung der logischen Uhr größer als bei einem regelmäßig genutzten Ausweis. Weicht nun die logische Uhr des ePA stark von der Realzeit ab, so kann dem Terminal irrtümlich der Zugriff gewährt werden.

Ein weiteres mögliches Angriffsszenario ist bei der Wahl der abzufragenden Attribute gegeben. Das Terminal Certificate enthält eine Liste von Attributen, die es vom Chip des ePA auslesen möchte. Der Ausweisinhaber hat die Möglichkeit, den Zugriff auf bestimmte Attribute zu verweigern. Kryptographisch kann allerdings nicht festgestellt

werden, ob tatsächlich nur die freigegebenen Informationen übermittelt werden oder nicht doch eine größere Anzahl an Daten.

Fazit

Die Spezifikation des Extended Access Control ist ein bedeutender Meilenstein. Neben der Konzeption muss aber auch die Implementierung von hoher Qualität sein. Zusammen mit der Tatsache, dass der elektronische Personalausweis jeder Bundesbürgerin und jedem Bundesbürger zur Verfügung stehen wird, kann den Herausforderungen und Möglichkeiten des 21. Jahrhunderts entgegengegangen werden.

Neben der Technik spielt aber auch stets der Faktor Mensch eine Rolle. Der Kartenleser kann unter Umständen eine neue Herausforderung darstellen, wenn alte Menschen oder technisch unversierte Anwender die vollen Möglichkeiten des ePA ausschöpfen möchten. Außerdem muss das IT-Sicherheitsbewusstsein der Benutzer auf dasselbe hohe Niveau gehoben werden, auf dem sich das Sicherheitsbewusstsein in der realen Welt befindet. Ein Zugriff auf den elektronischen Personalausweis und seine Daten kann unter Umständen schadhaft sein, wenn zwar der Zugang legitim, aber der Kommunikationspartner zwielichtig oder nicht vertrauenswürdig ist.

Der etablierte „konventionelle“ Personalausweis wird mit der Integration von bio-

metrischen Informationen, dem elektronischen Identitätsnachweis sowie einer qualifizierten elektronischen Signaturfunktion einen sicheren Umgang in der virtuellen Welt bieten können. Der ePA stellt nicht nur einen zuverlässigen realen und elektronischen Identitätsnachweis dar, sondern auch ein wichtiges Instrument für E-Government und E-Business. Der Ausweis allein erschlägt nicht alle aktuellen Probleme, ist aber absolut notwendig für sichere Online-Anwendungen und stellt einen großen Schritt in Richtung einer sicheren Zukunft im Netz dar.

Autor



B.Sc. Sebastian Feld ist wissenschaftlicher Mitarbeiter des Instituts für Internet-Sicherheit im Forschungsschwerpunkt Identity Management.

Anzeige

Herzlich willkommen zum Identitätsmanagement mit Governikus



Wir implementieren den **Governikus eID-Server** auf Basis des eCard-API-Frameworks.

Damit sind Sie bereit für den elektronischen Personalausweis.

Governikus. Passt immer.

bremen
online services



Am Fallturm 9, 28359 Bremen, Germany
www.bos-bremen.de