Automatische Authentifizierung mittels Bürgerkarte

Reinhard Posch/Udo Payer

Institut für angewandte Informationsverarbeitung und Kommunikationstechnologien (IAIK), Technische Universität Graz
A-8010 Graz, Inffeldgasse 16a
Reinhard.Posch@a-sit.at
Udo.Payer@iaik.at

Schlagworte: e-Government, Konzept Bürgerkarte, elektronische Signatur, Peer Entity Authentication, Security Layer,

Abstract: Das Konzept der österreichischen Bürgerkarte sieht neben der Erzeugung elektronischer Signaturen und der Herstellung vertraulicher Kommunikationskanälen auch Mechanismen vor, die zur Authentifizierung der in einem elektronischen Verfahren beteiligten Personen verwendet werden können. Dieser Text beschreibt den allgemeinen Ablauf einer solchen „Entity Authentication". Die Umsetzung geschieht in Verbindung mit einer weiteren vertrauenswürdigen Komponente, dem Security Layer. Dieser Layer bildet dabei die Schnittstelle zwischen den Anwendungen und der Chipkarte, verfügt aber zusätzlich über Mechanismen, die im Falle der automatischen Authentifizierung benötigt werden. Abhängig von den verwendeten Technologien können drei unterschiedliche Stufen (Qualitäten) der Authentifizierung realisiert und unterschieden werden. Dieses Dokument beschreibt einleitend das Konzept der österreichischen Bürgerkarte, die Rolle der Bürgerkarte in der elektronischen Verwaltung und gibt eine allgemeine Beschreibung der drei vorgeschlagenen Verfahren und der damit verbundenen Anforderungen[1] wieder.

1. Einleitung: Das Konzept Bürgerkarte

Das österreichische Konzept Bürgerkarte beinhaltet als Kernelement eine Chipkarte (oder andere, signaturgesetzkonforme Speichermedien für Signaturerstellungsdaten), die zur Erzeugung sicherer elektronischer Signaturen verwendet werden kann. Bislang sind Anträge an die Verwaltung an die Unterschrift der betroffenen Bürger gekoppelt. Daher müssen Ver-

---

[1] *S. Kraxberger*: „Technische Beschreibung – Automatische Authentifizierung mittels Bürgerkarte", April 2002.

fahren der elektronischen Verwaltung eine gleichwertige Möglichkeit auch im Falle eines elektronischen Anbringens bieten[2].

Signaturgesetz[3] und Signaturverordnung[4] schaffen die gesetzliche Basis, um zusammen mit der Bürgerkarte jene Signaturen erzeugen zu können, die bis auf wenige Ausnahmen den Zugang zur elektronischen Verwaltung auch ohne persönliches Einschreiten ermöglichen. Das Konzept Bürgerkarte sieht weiters vor, dass Verfahren der öffentlichen Verwaltung effizienter modelliert und damit dem Bürger kostengünstiger angeboten werden können. Dies setzt aber voraus, dass möglichst viele Anwendungen der elektronischen Verwaltung automatisierbar sind, und bedeutet aber auch, dass die Grundlagen derartiger Mechanismen bereits in der Infrastruktur gegeben sein müssen.

Von den verschiedensten Ausprägungen der Bürgerkarte, wird die Karte der Sozialversicherungsträger (e-Card) – *bedingt durch die Ausgabe an acht Millionen Sozialversicherte* – neben anderen Karten (Personalausweis, zukünftige Bankomatkarte etc) eine wesentliche Komponente sein.

Darüber hinaus basiert das Konzept Bürgerkarte und die eCard auf unterschiedlichen kryptographischen Mechanismen und können somit auf demselben Chip untergebracht werden. Eine Gefährdung durch Querverweise auf die jeweils anderen Bereiche ist somit ausgeschlossen.

Neben der Signaturerstellung sieht das „Konzept Bürgerkarte" auch die Möglichkeit vor, zusätzliche Datenelemente zu speichern. So die e-Card auch als Ausprägung einer Bürgerkarte zum Einsatz kommt, ist durch diese unterschiedlichen kryptographischen Mechanismen der Applikation SV-Karte und der Bürgerkartenfunktionalität gewährleistet, dass kein Austausch der am Chip gespeicherten Daten zwischen den beiden Anwendungen möglich ist. Die gespeicherten Daten müssen nicht notwendigerweise mit dem Inhaber der Sozialversicherungskarte verbunden sein, da diese von Anwendungen der Sozialversicherung ohnehin nicht gelesen werden können. Abgelegt in *Infoboxen* können zum Beispiel Zertifikate mitgeführt werden, um gegebenenfalls bei Inhaltsverschlüsselung der zu übertragenden Nachrichten nicht auf Onlinedienste zugreifen zu müssen. Diese Infoboxen können auch dazu verwendet werden, um elekt-

---

[2] *R. Posch*; Bürgerkarte-Infrastruktur für e-Government, in: *E. Schweighofer/T. Menzel/G. Kreuzbauer* (Hg) Auf dem Weg zur ePerson, Schriftenreihe Rechtsinformatik, Band 3. Verlag Österreich, Wien 2001, S 21-29.

[3] *C. Brenn*; Signaturgesetz, Erläuterte Ausgabe, Manz, Wien 1999.

[4] Signaturverordnung-SigV, BGBl II Nr 30/2000.

ronische Dokumente in geeigneter Form auf der Karte abzulegen. An Stelle von Dokumenten werden in der Regel Ort und Ordnungsbegriffe von Dokumenten in derartigen Infoboxen mitgeführt werden; damit können die Dokumente auch an beliebigen Stellen – *je nach Vertrauen des Bürgers* – abgelegt sein.

Inhalte und Umfang dieser Infoboxen werden aber letztlich durch den Karteninhaber selbst bestimmt.

Bedingt durch die Vielzahl der beteiligten Personen und deren Aufgaben, sieht das „Konzept Bürgerkarte" auch die Definition von *Rollen* und *Mandaten* vor. *Attributzertifikate* und andere Methoden der IT Sicherheit werden eingesetzt, um Rollen und Mandate technisch umsetzen zu können.

Öffentliche Zugänge zur Verwaltung haben einen besonderen Bedarf an Vertraulichkeit. Dieses Dokument beschreibt exemplarische Lösungen der Einbindung von kryptographischen Mechanismen, die sich zur Benutzerauthentifizierung in Anwendungen der elektronischen Verwaltung eignen. Entsprechend den unterschiedlichen Ansätzen können drei Stufen der sicheren Benutzerauthentifizierung unterschieden werden. Eine Beschreibung dieser Lösungen findet in Teil 4 dieses Beitrags statt.

Vor der detaillierten technischen Beschreibung und deren Umsetzung sollten einige grundsätzliche Mechanismen und Anforderungen an die Authentifizierung in der elektronischen Verwaltung diskutiert werden.

2. Rahmenbedingungen

Dieser Abschnitt beschreibt Rahmenbedingungen, die den in diesem Text beschriebenen Verfahren und Protokolle zugrunde liegen.

2.1. Einfachheit

Die Anzahl der verwendeten Technologien sollte begrenzt sein, damit eine rasche Umsetzung und Anpassung neuer Anwendungen schnell und einfach durchgeführt werden kann. Damit ist die Offenheit für alle System gegeben. Die Betroffenen (Entwickler von Anwendungen der elektronischen Verwaltung) treffen auf eine minimale Anzahl einfacher Strukturen, die ohne großen Aufwand erlernt und umgesetzt werden können.

2.2. Offene Schnittstellen

Die Schnittstellen an den Übergängen zwischen den Bereichen, die durch den Bürger verwaltet und administriert werden, müssen einfach ko-

ordinierbar und für alle berechtigten Interessenten ohne Behinderung verwendbar sein[5]. Die Schnittstelle der clientseitig installierten, vertrauenswürdigen Komponente (Security Layer) wird durch ein offenes Interface – *basierend auf TCP/IP oder HTTP* – hergestellt.

2.3. Berechtigungen/Attribute/Attributzertifikate

Die Authentifizierung sollte Ende-zu-Ende – *vom Benutzer zur Anwendung* – erfolgen. Portale sind nicht aktiv in die Authentifizierung eingebunden. Diese Ende-zu-Ende-Authentifizierung lässt sich mit Attributzertifikaten und elektronischen Signaturen herstellen.

Berechtigungen, die einer authentifizierten Person zufallen, sollten vornehmlich auf Funktionen (zB Leiter der Rechtsabteilung etc) basieren und sollten nicht Berechtigungen zur Benutzung einzelner Applikationen darstellen. Auch dann, wenn derartige Berechtigungen anlässlich neuer Anwendungen definiert werden, sind sie als Eigenschaft und nicht als Anwendungszugang zu definieren, damit diese Eigenschaften wiederverwendbar bleiben.

2.4. Benutzer-Identifikation

Die qualifizierte Identifikation der Bürger findet im Wege der Erbringung sicherer elektronischer Signaturen statt. Hierbei soll ein „qualifiziertes Zertifikat" verwendet werden. Für die Erbringung einer Signatur dieser Qualität ist aber eine eindeutige Willenserklärung des Benutzers (Bürgers) notwendig. Diese Willenserklärung kann durch Eingabe eines PINs erfolgen.

Für geringwertige Identifikationen sieht das Konzept Bürgerkarte Mechanismen vor, die keiner Eingabe des PINs bedürfen.

Es ist nicht wünschenswert, dass neben der Identifikation mit Hilfe der Karte weitere Verfahren auf Basis von Benutzerkennung und Passwort verwendet werden, da es dadurch zu einer Sicherheitslücke kommt und die Differenzierung von Rechten des Verwaltungszuganges besonders problematisch werden kann.

Die Identifikation des Bürgers ist immer eine Identifikation der Person. Sollte der Bürger weitere Eigenschaften vorweisen müssen, um ein entsprechendes Zugangsrecht zu Anwendungen der Verwaltung erwerben zu können, so werden Mechanismen eingesetzt, die auch in der konventi-

---

[5] *R. Posch/G. Karlinger/D. Konrad/A. Leiningen/T. Menzel*; Weissbuch Bürgerkarte, Mai 2002, abrufbar unter: http://www.buergerkarte.at.

onellen (nicht elektronischen) Verwaltung dafür geeignet wären. Zum Beweis der eindeutigen Identifikation (Namensgleichheit etc) wird die im § 13 Abs. 4a AVG vorgesehene Kennzeichnung verwendet. Zum Nachweis bestimmter Rollen könnten auch beigelegte Attributzertifikate dienen.

Um diesen Vorgang zu vereinfachen sieht das VerwaltungsreformG in der Novellierung des § 13 Abs. 4a AVG eine eindeutige Personenidentifikation anhand einer eindeutigen Nummer vor (zB ZMR-Nummer), die in abgeleiteter oder verschlüsselter Form zur Erzeugung einer verwaltungsbereichspezifischen Personenkennzeichnung (VPK) verwendet werden kann.

2.5. Identifikation der Personen der Verwaltung

Die Identifikation der in der Verwaltung tätigen Personen erfolgt in ähnlicher Weise wie die Identifizierung der Bürger. Dafür sind analog dem AVG die Möglichkeiten in BDG und VBG vorzusehen. Eigenschaften und Funktionen der in der Verwaltung Tätigen sind im Wege der Verzeichnisdienste zu ermöglichen. Die Inhalte dieser Verzeichnisdienste bilden die Basis für die Bildung von Rollen, für die Fähigkeit des Handelns dieser Personen, als auch für den kontrollierten Zugang zu Mechanismen der Verwaltung.

3. Zugriff auf die Bürgerkarte

Um Zugriff auf eine Bürgerkarte und all ihre Funktionen zu erlangen, sieht das Konzept Bürgerkarte eine einheitliche Schnittstelle vor. Diese Schnittstelle ist eine vertrauenswürdige Komponente, die clientseitig installiert werden muss, um Applikationen oder Web-Browsern den Zugriff auf die Karte zu ermöglichen. Diese Schnittstelle nennt sich – in Anlehnung an die Funktion dieser zusätzlichen Schicht – „Security Layer".

Browser als auch Applikationen können mit Hilfe des Security Layers auf einfache Art und Weise und ohne besondere Plug-Ins Signatur-Requests oder Signaturüberprüfungs-Requests an die Bürgerkarte senden. Erstellte Signaturen oder Ergebnisse einer Signaturüberprüfung werden an die Applikation oder den Browser weitergeleitet. Darüber hinaus sieht das Konzept Bürgerkarte auch weitere Features vor (wie zB Schreiben und Lesen der Infoboxen), die mittels Security Layers bedient werden können.

4. Automatische Authentifizierung

Online-Applikationen im Bereich der „Elektronischen Verwaltung" bedürfen unterschiedlicher Stufen der Sicherheit. Dies gilt auch für den Grad der Authentifizierung, da auch Anwendungen existieren, die keines qualifizierten Zertifikats und somit keiner Eingabe des PIN bedürfen.

In Abhängigkeit vom Grad der qualifizierten Authentifizierung können drei Stufen der Authentifizierung definiert und umgesetzt werden:

- (1) Sicher für den *Normalbetrieb*
- (2) Sicher bei einer *vertrauenswürdigen Infrastruktur*
- (3) Technische *Ende-zu-Ende*-Sicherung

Hierbei muss Punkt 2 noch hinsichtlich der Eigenschaften der zusätzlichen vertrauenswürdigen Strukturen und Punkt 3 hinsichtlich der Qualität der verwendeten Zertifikate unterschieden werden.

4.1. Sicher für den Normalbetrieb

Viele Anwendungen der „Elektronischen Verwaltung" stellen nur minimale Anforderungen an die „Qualität" der Authentifizierung. Diese Anforderungen können durch eine serverauthentifizierte SSL oder TLS Verbindung erreicht werden. Versucht ein Benutzer auf einen sicheren Bereich der Verwaltung zuzugreifen, so muss die Kommunikation zwischen Client und diesem Bereich durch einen sicheren Kanal (SSL/TLS) vor Zugriffen von außen gesichert werden.

Darüber hinaus müssen Normen eine minimale Schlüssellänge von mindestens 100 Bit vorschreiben. Es liegt in der Verantwortung des Clients, dass für den Vorgang der Authentifizierung ein vertrauenswürdiges Zertifikat verwendet wird.

Neben bekannten Problemen mit „serverauthentifizierten" SSL Verbindungen ist diese Annordnung potentiell anfällig für *Man-in-the-Middle* Attacken.

4.2. Sicher in vertrauenswürdiger Infrastruktur

Um clientseitig Steueraufgaben übernehmen zu können, bedarf es einer clientseitigen, vertrauenswürdigen, aktiven Komponente. Da Stufe 2 höhere Anforderungen an den Grad der Authentifizierung stellt, als Stufe 1, muss auch die Vertrauenswürdigkeit der aktiven Komponenten sichergestellt sein. Für vertrauenswürdige Infrastrukturen der Authentifizie-

rung kann die Authentifizierung der Benutzer durch den nachfolgenden Ablauf erfolgen.

4.2.1. Ablauf der automatischen Authentifizierung:

Der nun beschriebene *Challenge Response* Mechanismus beruht im Wesentlichen auf einer gegenseitiger Authentifizierung unter Verwendung digitaler Signaturen.[6]

Versucht ein Benutzer auf einen sicheren Bereich eines Verwaltungsservers zuzugreifen (1), so generiert der Server einen Zeitstempel t_S, der zusammen mit der Server-URL und der Session ID (SID) einen *Security Token* [t_S, URL_S, SID] bildet. Dieser Security Token wird mit Hilfe des geheimen Serverschlüssels signiert und dem Client zugesandt (2).

Der Client überprüft die Signatur des Servers und kann anhand der Signatur die Server-URL prüfen.

1.	C→S: Auth.Req.
2.	C←S: $cert_S$, $S_S(t_S, URL_S, SID)$
3.	C→S: $cert_C$, $S_C(t_S, URL_S, SID, ID_S)$
	$ID_C = S_{BH}(K_{PC1}, K_{PC2}, C, cert_{BH})$ ... Identity Link

K_{PC1} ... *öffentlicher Schlüssel eines normalen Zertifikats*
K_{PC2} ... *öffentlicher Schlüssel eines qualifizierten Zertifikats*
C ... *personenbezogene Information (Name, Geb.-Datum, ZMR, Matr.#)*
$cert_{BH}$ ... *von der Behörde ausgestelltes Zertifikat*
$S_{BH}()$... *von der Behörde signiert*
SID ... *Session ID*

War diese Überprüfung erfolgreich, generiert der Client einen *Authentication Block* [t_S, URL_S, SID, ID_S], der aus dem gerade empfangenen Timestamp, der gerade empfangenen Server-URL und dem personenbezogenen *Identity Link* ID_S besteht. Der Benutzer signiert nun diesen Authentication Block mit Hilfe der Bürgerkarte und schickt diesen signierten Block an den Server (3).

Mit diesem Vorgang unterzeichnet der Benutzer ein Dokument des Inhaltes *„Ich ... fordere heute, ... um ... den Zugang zu nachstehender*

---

[6] *A. Menezes/P. von Oorschot/S. Vanstone*: Handbook of Applied Cryptography; CRC Press, 1996.

Verwaltungsanwendung an: ....." Die Codierung dieser Anforderung ist aus Gründen der Verarbeitung formalisiert.

Eine aktive Serverkomponente (Servlet) kann nun anhand der Signatur die Authentizität des zu identifizierenden Bürgers prüfen und vergleicht Server-URL und Timestamp. Darüber hinaus wird noch geprüft, ob dieser Response noch innerhalb eines definierten Zeitfensters erfolgte.

Das Servlet kann nun mit Hilfe der gewonnen Information den Benutzer am Web-Server oder bei der entsprechenden Applikation anmelden.

4.3. Technische Ende-zu-Ende-Sicherung

Der Ablauf von Stufe III entspricht im Wesentlichen dem Ablauf aus 4.2. mit dem Unterschied, dass dieser Mechanismus auf einer technischen Ende-zu-Ende-Sicherung basiert. Diese Ende-zu-Ende-Sicherung wird dadurch sichergestellt, dass die für den Ablauf notwendigen Zertifikate direkt aus der sicheren SSL- oder TLS-Verbindung abgeleitet werden können. Hierzu ist es notwendig, dass clientseitig als auch serverseitig auf das Serverzertifikat der SSL-Verbindung zugegriffen werden kann. Die Qualität einer Stufe 3 Authentifizierung kann nun aufgrund der Qualität der verwendeten Zertifikate eingestuft werden.

5. Abschließende Bemerkung

Das Konzept Bürgerkarte[7] berücksichtigt Mechanismen zur Erbringung elektronischer Signaturen, beschreibt aber auch Interaktionen zwischen Bürgerkarte, der elektronischen Verwaltung und das mögliche Zusammenspiel mit Portalen und Marktplätzen. Ein wesentliches Merkmal dieser Mechanismen sind Verzeichnisdienste, Zertifikate und deren Attribute. Dieses Dokument beschreibt, dass die Bürgerkarte in Verbindung mit diesen Merkmalen in der elektronischen Verwaltung zur Identifikation beteiligter Personen eingesetzt werden kann. Hierbei ist aber darauf zu achten, dass sich Applikationen und Anwen-dungsstrukturen für diese Form der Identifikation eignen.

Weiters wird beschrieben, dass in Abhängigkeit von den verwendeten Technologien unterschiedliche Stufen der Authentifizierung zur Verfügung stehen. Aus all diesen Verfahren muss nun jenes ermittelt werden,

---

[7] Siehe dazu auch: *T. Menzel/P. Reichstädter,* Die Rolle der Bürgerkarten im eGovernment, *M. Wimmer,* (Hg), Impulse für e-Government: Internationale Entwicklungen, Organisation, Recht, Technik, Best Practices, books@ocg.at, Band 158, Österreichische Computergesellschaft, Wien, 2001, S 139 – 149.

das sich für eine bestimmte Anwendung am besten eignet oder ein Höchstmaß an Sicherheit bietet.