

## **DIE ROLLE DER BÜRGERKARTEN IM e-GOVERNMENT**

### **Begriff Bürgerkarte**

Unter dem Begriff "Bürgerkarte" versteht man ein Konzept für verschiedene Ausprägungen von Bürgerkarten. Es handelt sich dabei um Token, die die sichere elektronische Kommunikation zwischen Verwaltung und BürgerInnen – d.h. die sichere Teilnahme der BürgerInnen am e-Government – ermöglichen sollen. Unter Token versteht man einen Datenträger, auf dem der Schlüssel zur Signatur und Chiffrierung von Daten, die dazugehörigen Zertifikate sowie weitere vertrauliche Informationen gespeichert sind.

Bei der Bürgerkarte handelt es sich also nicht um einen bestimmten Kartentyp, sondern es wurden Mindestanforderungen definiert, welche der Token erfüllen muss. Diese Mindestanforderungen garantieren unter anderem die sichere Identifikation und Authentifikation des/der BürgerIn.

Die BürgerInnen können unter verschiedenen Angeboten an Karten bzw. anderen Token wählen.

### **Grundanforderungen des Konzepts Bürgerkarte**

Eine Karte mit Bürgerkartenfunktionalität muss folgende Grundanforderungen erfüllen:

- **Einsatz der sicheren elektronischen Signatur**

Ein wesentliches Sicherheitsmerkmal stellt die geeignete Wahl des Speicherplatzes für die Signaturerstellungsdaten (privater Schlüssel) dar, die am besten auf einer Chipkarte mit Krypto-Prozessor (dient der Verschlüsselung und der digitalen Signatur von Dateien) gespeichert werden. Aber auch andere Speichermedien wie z.B. Chipkarten in Form eines Handy-SIMs, USB Token, PDAs, etc. sind möglich. Die elektronischen Signaturen müssen strengen Anforderungen genügen, um die Datenintegrität (Unverfälschtheit der Daten) sicherzustellen.

- **Authentifikation des/der SignatorIn**

Da die Angaben zur Person im Zertifikat nicht zur eindeutigen Identifikation des/der SignatorIn genügen, wird zusätzlich das Verfahren der "Personenbindung" angewandt. Bei der Personenbindung werden die öffentlichen Schlüssel (dienen zur Prüfung der digitalen Signatur) des/der BürgerIn an die sogenannte ZMR-Zahl (wird vom Zentralen Melderegister abgefragt) gebunden. Diese Datenstruktur der Personenbindung fließt jedoch nicht in die Verfahren ein, sondern es wird - von dieser ausgehend – eine verschlüsselte Personenkennung abgeleitet, die eine Rasterabfrage über die ZMR-Zahl verhindern soll.

- **Schnittstelle "Security Layer"**

- unterstützt die Erstellung und Überprüfung von elektronischen Signaturen in den Formaten CMS (Cryptographic message syntax) und XMLDSIG (ein auf XML basierendes Format für digital signierte Daten),
- ermöglicht einer Applikation, technologieunabhängig auf die Bürgerkarte zuzugreifen,
- trennt gemäß Signaturgesetz die Aufgaben und Verantwortungen des Zertifizierungsdiensteanbieters vom Applikationsanbieter
- gewährleistet die Offenheit gegenüber zukünftigen Entwicklungen (Bürgerkarte für PDAs, Handys etc.).



- **Inhaltsverschlüsselung**

Um die Vertraulichkeit von Nachrichten zu gewährleisten, ist auf der Karte ein weiterer privater Schlüssel – der nicht der elektronischen Signatur, sondern der Inhaltsverschlüsselung dient – gespeichert.

- **optionale Infoboxen**

Dabei handelt es sich um zusätzliche Datenspeicher, die in Infoboxen strukturiert und nicht näher definiert sind. Sie dienen dazu, oft gebrauchte Datensätze, die immer wieder bestimmten Anträgen beigelegt werden müssen (z.B. die elektronische Erteilung von Vollmachten), abrufbar zu machen. Der/Die BürgerIn entscheidet, welche Daten in den Datenspeichern zur Verfügung gestellt werden.

### **Zertifizierungsdiensteanbieter**

Die für die Erstellung von digitalen Signaturen wichtigen qualifizierten Zertifikate sollen die sichere Identifizierung des/der SignatorIn ermöglichen. Dies erfolgt mittels eindeutiger Zuordnung des öffentlichen Schlüssels zu dem/der SignatorIn. Vereinfacht ausgedrückt handelt es sich beim qualifizierten Zertifikat um einen digitalen Ausweis im Internet.

Qualifizierte Zertifikate werden von Zertifizierungsstellen angeboten, welche neben der Generierung auch für die Veröffentlichung des Zertifikats und die Durchführung eines Widerrufs zuständig sind. Für den/die BürgerIn besteht die freie Wahl des Zertifizierungsdiensteanbieters.

### **Möglicher Einsatz von Bürgerkarten**

Da das "Konzept Bürgerkarte" nur Mindestkriterien festlegt, die von einem Token erfüllt werden müssen, sind zahlreiche Kartentypen für die Kommunikation mit der Verwaltung möglich, so etwa:

- elektronischer Personalausweis
- StudentInnen-Service-Card
- e-Card
- Bankkarten
- Karten für Kammermitglieder
- Dienstkarten für Bedienstete der öffentlichen Verwaltung
- diverse privatwirtschaftliche Karten (z.B. OCG-Karte)

### **Ablauf**

Am Anfang jeder e-Government-Session ist die Authentifizierung mittels Bürgerkarte notwendig. Browser-Daten (z.B. ausgefülltes Formular) werden an den Web-Server übertragen, der daraus ein für die Verarbeitung notwendiges XML-Format erstellt.

Werden XML-Daten und Signatur an den Web-Server übertragen, liefert dieser eine Statusmeldung. Die XML-Daten können durch Vollmachten bzw. andere (signierte) Beilagen (z.B. Strafregisterbescheinigung, elektronische Zahlungsbestätigung etc. ) erweitert werden. Diese werden in einen XML-Container verpackt, der ebenfalls signiert wird.

Die signierten Formulardaten und Beilagen werden am Portal der Behörde auf einer virtuellen "Einlaufstelle" deponiert und dann dem jeweils zuständigen Bereich der Verwaltung zur weiteren Verarbeitung zugeführt. Das Anbringen wird auf formale Richtigkeit überprüft. Ist diese Überprüfung positiv, wird der Antrag bearbeitet und der/die AntragstellerIn kann einen (signierten) Bescheid in Form eines XML-Datencontainers zugestellt bekommen. Nicht elektronisch zustellbare Bescheide werden konventionell zugesandt. Während des Verfahrens hat der/die BürgerIn die Möglichkeit, Statusabfragen an die Behörde zu richten.