

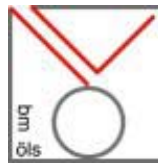
# Weißbuch Bürgerkarte



Prof. Reinhard Posch

Gregor Karlinger · Daniel Konrad  
Alexander Leiningen-Westerburg · Thomas Menzel

[www.buergerkarte.at](http://www.buergerkarte.at)



Bundesministerium für öffentliche Leistungen und Sport



Zentrum für sichere Informationstechnologie - Austria (A-SIT)

© Mai 2002

## Executive Summary

Das österreichische Konzept Bürgerkarte versteht sich als Instrument, das die Migration zu bürgernahen, modernen Verwaltungsabläufen über Informationstechnologie (IT) unterstützt. Dabei wird einerseits mit konkreten Ausprägungen des „Konzepts Bürgerkarte“ den Bürgerinnen und Bürgern jene Schlüsseltechnologie in die Hand gegeben, die es über die elektronische Signatur ermöglicht, der öffentlichen Verwaltung unter Nachweis der Identität durchgängig elektronisch gegenüberzutreten, andererseits vice versa kann die öffentliche Verwaltung durch e-Government Prozesse effizienter modellierten und damit verbesserten Service kosteneffektiver anbieten.

Das Weißbuch Bürgerkarte ist als ein in diesem Kontext projektbegleitendes Orientierungspapier anzusehen, das in weiterer Folge die Aspekte der Umsetzung definiert und spezifiziert. Es soll als Diskussionsgrundlage für alle Beteiligten dienen und dabei die breite Diskussion der Beteiligten ermöglichen, also der öffentlichen Hand, des privaten Sektors und der Bürgerinnen und Bürger. Es handelt sich daher um ein öffentlich zugängliches Dokument. Die Inhalte des Weißbuches umfassen, nach seiner Struktur gegliedert:

### **Konzept Bürgerkarte**

Erläutert werden Mindestanforderungen im Konzept Bürgerkarte, wie zum Beispiel die sichere elektronische Signatur, die Personenbindung, der Security Layer sowie optionale Elemente. Ebenso werden die technischen Grundlagen des Konzeptes Bürgerkarte und die grundlegenden Umsetzungsziele skizziert.

### **Ausprägungen der Bürgerkarte**

Es werden die Attribute der Kernelemente Token und Oberfläche den verschiedenen möglichen Ausprägungen gegenübergestellt.

### **Lebenszyklus**

Die Lebenszyklusabschnitte einer Chipkarte werden beschrieben. Der Schwerpunkt liegt dabei auf dem Bereich Registrierung und den Leistungen der Zertifizierungsdiensteanbieter.

### **Anwendungen im e-Government**

Verschiedene Anwendungsszenarien werden dargestellt. Diese umfassen sowohl konventionelle und elektronische Anbringen seitens der Bürgerin und des Bürgers, als auch die verwaltungsseitige Verarbeitung. Verfahren mit hohem Umsetzungspotential im Bereich der Verwaltung werden identifiziert.

### **Rechtliche Aspekte**

Bei der Verwendung der Bürgerkarte ist die Einhaltung der gesetzlichen Rahmenbedingungen zu beachten. Wichtige gesetzliche Grundlagen unter Einbeziehung des Datenschutzaspekts werden vorgestellt.

## Inhalt

Executive Summary.....	2
Inhalt.....	3
1 Einleitung .....	4
1.1 Das Ziel .....	5
1.2 Grad der Öffentlichkeit .....	5
2 Konzept Bürgerkarte .....	6
2.1 Anforderungen und optionale Komponenten .....	6
2.1.1 Sichere elektronische Signatur .....	6
2.1.2 Personenbindung/Authentifikation .....	7
2.1.3 Inhaltsverschlüsselung .....	7
2.1.4 Infoboxen .....	8
2.1.5 Verfügbarkeit des Security Layers .....	8
2.2 Security-Layer .....	8
2.2.1 Begriffsdefinitionen .....	8
2.2.2 Anforderungen .....	8
2.2.3 Weiterführende Literatur .....	9
2.3 Technische Aspekte.....	9
2.3.1 Algorithmen .....	9
2.3.2 Formate.....	10
2.3.3 Ausstattung beim Bürger .....	11
3 Ausprägungen der Bürgerkarte .....	11
3.1 e-card.....	12
3.2 Personalausweis .....	12
3.3 OCG Karte .....	12
3.4 Studentenkarten .....	12
3.5 Bankkarten .....	13
3.6 Signaturkarten der Zertifizierungsdiensteanbieter .....	13
4 Lebenszyklus .....	14
4.1 Personalisierung.....	14
4.1.1 Oberfläche .....	14
4.2 Registrierung.....	14
4.2.1 Freie Wahl des Zertifizierungsdiensteanbieters (ZDA) .....	14
4.2.2 Behörden als Registrierungsstellen .....	14
4.3 Verzeichnis- und Widerrufsdienste .....	15
4.4 Zertifikatsverlängerung .....	16
5 Anwendungen im e-Government .....	16
5.1 Signatur .....	16
5.1.1 Identifikation .....	17
5.1.2 Echtheit.....	17
5.1.3 Abschluß und Warnung .....	17
5.1.4 Unleugbarkeit.....	17
5.2 Infoboxen.....	17
5.2.1 Dokumente .....	17
5.2.2 Vollmachten.....	18
5.3 Skizze e-Government-Session .....	19
6 Rechtliche Aspekte .....	21
6.1 SigG, SigV.....	21
6.2 AVG und ZustellG .....	21
6.3 MeldeG, MeldeV .....	22
6.4 Datenschutz.....	22
Glossar .....	23
7 Referenzen.....	30

# 1 Einleitung

## Vorbemerkung

Zur besseren Lesbarkeit wurde in diesem Dokument auf eine geschlechtsneutrale Formulierung verzichtet. Die verwendeten Formulierungen (z.B. Bürger, Karteninhaber, Zertifikatsinhaber, ...) richten sich an beide Geschlechter.

## Ziele des Weißbuchs

Das Weißbuch Bürgerkarte versteht sich als kohärenter Rahmen der Definition und Koordination des Projektes Bürgerkarte. Es bildet damit Leitfaden und Orientierungspapier der Planung bürgernahe elektronischer Verwaltung, dessen sukzessiver Umsetzung in den Ressorts, wie auch der abgestimmten Vorgehensweise der technischen Durchführung mit den Betreibern und der Wirtschaft.

## Begriff Konzept Bürgerkarte

Konzept Bürgerkarte ist der Arbeitstitel der österreichischen Verwaltung für jenes Werkzeug, das es dem Bürger und der Verwaltung ermöglicht an e-Government sicher und authentisch teilzunehmen. Es stellt dies eine Schlüsseltechnologie bei der Nutzung von e-Government dar. In einem möglichst offenen und daher für die weiteren Entwicklungen des hoch dynamischen Bereiches der e-Technologien geeigneten System ermöglicht ein dem Konzept Bürgerkarte entsprechender Token die notwendige Identifikation der Betroffenen. Transaktionen, die bislang nur durch persönliches Erscheinen oder mit konventionellen Mitteln (unterfertigte Formulare) möglich waren, können damit online durchgeführt werden.

## Grundstruktur e-Government

Bürgerinnen und Bürger sollen über festgelegte Schnittstellen an die verschiedenen Anwendungen der Verwaltung herantreten können. Der Hoheitsbereich der Verwaltung erstreckt sich primär auf den hinter den Schnittstellen gelegenen Bereich. Dadurch entsteht hinreichend Raum, um auch privatwirtschaftliche Umsetzungen und Lösungen zur Heranführung des Bürgers an e-Government Anwendungen zu ermöglichen. Diese generelle Struktur wird in weiterer Folge ausgeführt.

## Sicherheit ist ein Anliegen der Betroffenen und des Gesetzgebers

Für Bürgerinnen und Bürger aber auch für die Verwaltung sind die Identität und die Berechtigung, in einer gewissen Rolle zu agieren, von großer Bedeutung. In gleichem Maße kann die Vertraulichkeit ein Anliegen sein, und es wird diese teilweise durch das Datenschutzgesetz 2000 explizit erforderlich. In einem derartigen System, welches Struktur sowie offene und definierte Schnittstellen voraussetzt, schafft ein dem Konzept Bürgerkarte entsprechender Token die bei der Heranführung an die Verwaltungsanwendungen notwendige Sicherheit. Damit ist er der Grundstein für ein modulares, offenes Verwaltungssystem und auch die Voraussetzung, die ein sich Konzentrieren der Verwaltung auf die Kernbereiche ermöglicht.

Der Heranführungsbereich kann automatisiert oder auch von Angesicht zu Angesicht erfolgen. Damit ist durch konkurrierenden Methoden Effizienz gesichert und auch für den Betroffenen ein auf seine Bedürfnisse zugeschnittenes Interface vorhanden. Für Menschen mit besonderen Bedürfnissen und für jene Gruppen, die nicht an der elektronischen Verwaltung teilnehmen wollen oder können, entsteht dabei ebenfalls ein Markt. Die Teilnahme seitens der Bürger muss dabei durch Komfort und Nutzen für den Bürger motiviert werden.

Das in Österreich im Laufe des Jahres 2002 umzusetzende Konzept Bürgerkarte wird im Wesentlichen drei Funktionen zur Verfügung stellen:

### a) Die sichere elektronische Signatur:

Primär sollte diese Signatur für die Bereiche des e-Government eine Basis und Infrastruktur bieten, die allen Bürgerinnen und Bürgern zugänglich ist. Die Entscheidung, sich tatsächlich registrieren zu lassen und die Signatur anzuwenden, basiert auf Freiwilligkeit. Der Vorgang ermöglicht, dass ein Bürger ein vorliegendes Dokument entsprechend den

gesetzlichen Regelungen so unterfertigt, dass er damit die Gleichwertigkeit zur Schriftform und damit die Möglichkeit zum Einsatz in Anbringen an die Verwaltung erreicht.

#### **b) Identifikation und Authentifikation durch die Personenbindung**

Die Personenbindung ermöglicht die eindeutige Feststellung der Identität eines Bürgers im elektronischen Verkehr mit der Behörde. Sie bindet zu diesem Zweck die vom Bürger verwendeten Zertifikate an einen eindeutigen Ordnungsbegriff, die sog. ZMR-Zahl. Erstellt wird die Personenbindung durch das Zentrale Melderegister im Rahmen der Registrierung zur Signatur.

#### **c) Datenspeicher (Infoboxen)**

Das Konzept Bürgerkarte macht weitere Bereiche, die auf dem Token verfügbar sind, nutzbar. Infoboxen sind fest vorgegebene Datenblöcke auf dem Token, die nicht mit der elektronischen Signatur in Interaktion treten und die als Datenblöcke gelesen und geschrieben werden können, aber keine weiteren Funktionen auf der Karte auslösen. Damit können oft benötigte Informationen, wie etwa Vollmachten, im Sinne der Mobilität und Bequemlichkeit auf der Karte gespeichert werden. Die Infoboxen sind allerdings nicht grundsätzlich an den Token gebunden, sondern können auch an einem anderen Ort, z.B. dem eigenem PC oder einem Server des Vertrauens des Bürgers eingerichtet werden.

Im Sinne einer möglichst großen Verbreitung des Konzeptes wurde mit dem Security Layer eine genormte Schnittstelle geschaffen, die es Applikationen auf einfache Weise ermöglicht, mit unterschiedlichen Bürgerkarten zu kommunizieren. Anwendungen können damit losgelöst von aktuellen Technologien umgesetzt werden. Das Konzept ist somit in hohem Masse offen gegenüber zukünftigen Entwicklungen.

## **1.1 Das Ziel**

### **Wer sollte das Dokument verwenden?**

Dieses Dokument richtet sich an die Enabler, Planer und Umsetzer von Aktivitäten im Bereich des Konzeptes Bürgerkarte. Es soll die allgemeine Strategie und die Rahmenbedingungen abstecken, damit möglichst interoperable Anwendungssysteme entstehen können. Aktivitäten der elektronischen Verwaltung entstehen nebeneinander und oft ohne enge Koordination. Das Konzept Bürgerkarte als ein zentrales Element des e-Government hat besonderen Bedarf, mit anderen Aktivitäten abgestimmt zu werden.

Die elektronische Signatur erlaubt die wirksame Trennung der Bereiche Anwendung, Portal, Heranführung und Bürger, die ihrerseits eine wichtige Basis für weitere Veränderungen aufgrund von Technologieentwicklung ermöglicht.

Aus diesem Grund stellt dieser Text ein Orientierungspapier dar, welches die zentralen Elemente des Konzeptes Bürgerkarte zusammenfasst und damit einen Beitrag zur Koordination leistet. Die Referenzen umfassen die Schnittstellen und die Normen sowie die allgemeinen Verwendungsrichtlinien. Damit wird dieses Dokument eine Basis der e-Koordination im Bereich des Konzeptes Bürgerkarte.

## **1.2 Grad der Öffentlichkeit**

Dieses Dokument ist öffentlich verfügbar, damit die Informationen alle Betroffenen erreichen. Damit sollen die folgenden Effekte erzielt werden:

- a) Koordination in allen Stadien, um Parallelitäten und damit Organisations-Overhead vermeiden zu helfen. Aus dieser Koordination entsteht Diskussion.
- b) Diese entstehende Diskussion bzw. die Ergebnisse daraus sind im Sinne einer Weiterentwicklung laufend einzubinden.

## 2 Konzept Bürgerkarte

Das Konzept Bürgerkarte beschreibt keine physische Karte, sondern definiert nur jene Rahmenbedingungen, die notwendig sind, um einen Signatur Token im e-Government einsetzen zu können. Damit ist die Teilnahme am „Konzept Bürgerkarte“ allen offen. Bereits jetzt ist absehbar, dass der Bürger unter mehreren Angeboten an Chipkarten wählen können wird. Interessensvertretungen, Kammern und privatwirtschaftliche Unternehmen planen bereits die Ausgabe von Chipkarten, die dem Konzept Bürgerkarte entsprechen.

Eine Bürgerkarte oder ein anderer Token zur Speicherung und Anwendung der Signaturerstellungsdaten stellt den Kern des Konzepts Bürgerkarte dar. Diesen Kern umschließt die in untenstehender Grafik dargestellte Bürgerkarten-Umgebung. Sie kapselt in Ergänzung zum Bürgerkarten-Token jene Komponenten, die notwendig sind, um die über die Schnittstelle des Security Layers festgeschriebene Funktionalität einer Applikation zur Verfügung zu stellen.



In dieser Umgebung sind alle sicherheitsrelevanten Komponenten integriert, sodass sich einerseits der Applikationsersteller nicht um eventuell gesetzlich geforderte Sicherheitsbescheinigungen dieser sensitiven Komponenten (Sichere Anzeige, Hashberechnung und PIN-Eingabe) kümmern muss, weil sie vom Zertifizierungsdiensteanbieter bereitgestellt werden. Andererseits können sich in der Bürgerkarten-Umgebung lokale Speicher sowie Zugriffsmechanismen zu Webservices befinden, um der Applikation im Zusammenspiel mit dem verfügbaren Speicher auf dem Bürgerkarten-Token einen nach außen hin transparenten, verteilten Datenspeicher zur Verfügung stellen zu können.

### 2.1 Anforderungen und optionale Komponenten

#### 2.1.1 Sichere elektronische Signatur

Der Einsatz sicherer elektronischer Signaturen in der Kommunikation mit der Verwaltung ist das Schlüsselement für die Gewährleistung der Sicherheit im e-Government. Ein wesentliches Sicherheitsmerkmal stellt hier die geeignete Wahl des Speicherplatzes für die Signaturerstellungsdaten dar. Der exklusive Zugriff nur des Berechtigten auf seine Signaturerstellungsdaten wird nach dem derzeitigen Stand der Technik am besten durch die Speicherung dieser Daten auf einer Chipkarte mit Krypto-Prozessor gewährleistet sodass die Signaturerstellungsdaten die Karte nie verlassen können. Die Entwicklung anderer Speichermedien, wie etwa USB-Tokens oder Chips, die in Form eines Handy-SIMs ausgeführt sind, wird ebenfalls durch das Konzept Bürgerkarte berücksichtigt.

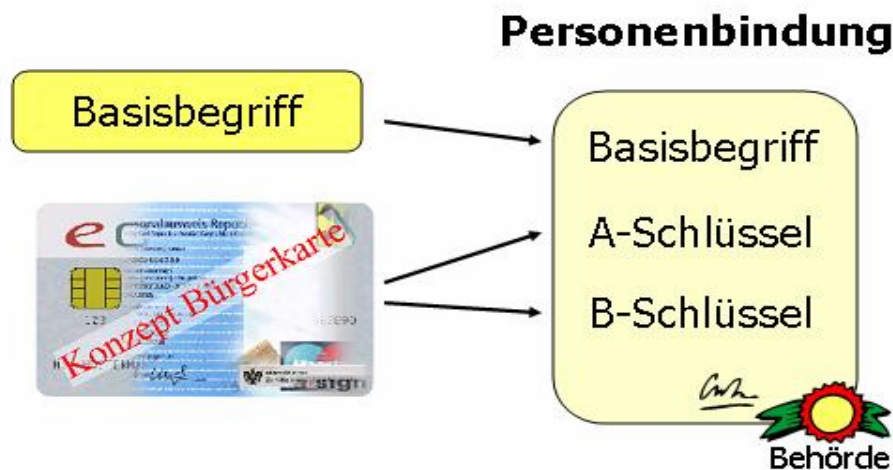
Das österreichische Signaturgesetz definiert die Anforderungen an die sichere elektronische Signatur für den Einsatz im e-Commerce und e-Government gleich, sodass auch Karten, die für e-Commerce-Lösungen konzipiert werden als Bürgerkarte eingesetzt werden können. Dabei werden folgende Elemente notwendig:

- Public-Key-Kryptographie, auch als asymmetrische Kryptographie bezeichnet, stellt die mathematische Grundlage dar
- Hash-Verfahren gewährleisten Integrität der Daten und erlauben einen effizienten Signaturerstellungsprozess
- Zertifikate binden die technischen Elemente wie kryptographische Schlüssel an die Identität des Signators

Insbesondere ist zu erwähnen, dass das Signaturgesetz sowohl den Einsatz von RSA als auch Verfahren mittels elliptischer Kurven zur Signaturerstellung zulässt. Der Einsatz von speziellen Verfahren ist im Konzept Bürgerkarte daher nicht vorgeschrieben.

### 2.1.2 Personenbindung/Authentifikation

Zur eindeutigen Identifikation des Bürgers sind die im Konzept Bürgerkarte verwendeten Zertifikate alleine nicht geeignet, da die Angaben zur Person des Bürgers im Zertifikat (meist lediglich Vor- und Nachname) unter Umständen nicht zur eindeutigen Zuordnung in Verwaltungsverfahren führen. Dazu findet eine Datenstruktur Anwendung, genannt Personenbindung, welche die öffentlichen Schlüssel aus den Zertifikaten des Bürgers kryptographisch an einen eindeutigen Ordnungsbegriff, die sog. ZMR-Zahl durch elektronische Signatur bindet. Die folgende Grafik veranschaulicht den Aufbau der Personenbindung:



In die einzelnen Verfahren fließt der Ordnungsbegriff der Personenbindung aber nicht selbst ein, sondern eine davon abgeleitete, verfahrensspezifische verschlüsselte Personenkennung. Dadurch ist garantiert, dass nicht von einer derartigen Kennung auf eine andere Kennung in einem anderen Verfahren desselben Bürgers geschlossen werden kann. Die rechtliche Grundlage zur Speicherung der Personenbindung im Bereich des Karteninhabers bildet die vom Verwaltungsreformgesetz 2001 durchgeführte AVG-Novelle.

### 2.1.3 Inhaltsverschlüsselung

Die Kommunikation zwischen Bürger und Verwaltung soll aber nicht nur authentischen Inhalt der Dokumente und Authentifikation der Teilnehmer ermöglichen. Ein ebenfalls grundlegendes Element ist die Vertraulichkeit der Kommunikation, die durch Inhaltsverschlüsselung der Dokumente am Übertragungsweg erreicht wird. Schlüssel, welche zur Erstellung sicherer elektronischer Signaturen verwendet werden, dürfen gemäß den Bestimmungen des Signaturgesetzes allerdings nicht im Rahmen anderer kryptographischer Prozesse eingesetzt werden, daher ist auf der Karte noch zumindest ein weiterer privater Schlüssel gespeichert, der zur inhaltlichen Verschlüsselung und zur Authentifizierung des

Karteninhabers verwendet wird. Dadurch wird eine Trennung des sicheren Signaturprozesses von allen anderen Prozessen, die ebenfalls auf asymmetrischer Kryptographie beruhen, verwirklicht. Um eine eindeutige Schlüsselzuordnung zu gewährleisten, ist auch der öffentliche Schlüssel dieses Schlüsselpaars in die Personenbindung aufzunehmen.

### 2.1.4 Infoboxen

Es ist sinnvoll, der Applikation weiteren Datenspeicher, logisch strukturiert in Infoboxen, zur Verfügung zu stellen.

Beispielsweise könnten Vollmachten oder Beilagen, die immer wieder bestimmten Anbringen beigelegt werden müssen, über diesen Datenspeicher abrufbar gemacht werden. Praktischer Weise sollten die Daten physikalisch so abgelegt werden, dass der Bürger unabhängig vom Verwendungsort der Bürgerkarte Zugriff auf die Daten hat.

Die Entscheidung, welche Daten der Applikation zur Verfügung gestellt werden sollen, wird vom Bürger getroffen.

### 2.1.5 Verfügbarkeit des Security Layers

Die Offenheit des Konzepts Bürgerkarte bedingt die Definition einer Schnittstelle, über die Applikationen unabhängig von der aktuellen Technologie auf die Funktionalität der verschiedenen Bürgerkarten-Ausprägungen zugreifen können.

Die Schnittstellendefinition des Security Layers ermöglicht nicht nur eine langfristige Offenheit gegenüber zukünftigen Entwicklungen wie z.B. PDAs, Handys, etc., sondern auch die Integration von ‚Fremdtechnologien‘ (z.B. Bürgerkarten aus anderen Staaten). Dabei liegt es im Verantwortungsbereich des Anbieters einer Bürgerkarten-Umgebung, etwa eines Zertifizierungsdiensteanbieters, einerseits die Struktur-Anforderungen der Applikationen zufrieden zustellen, andererseits die Karte oder ein anderes sicheres Signaturerstellungsgesetz in den e-Government Prozess zu integrieren.

Eine prototypische Implementierung des Security Layers wird von der IKT-Stabsstelle interessierten Parteien frei zur Verfügung gestellt.

## 2.2 Security-Layer

e-Government Anwendungen beschränken sich bei der Verwendung von Bürgerkartenfunktionen auf die Funktionen des Security Layers.

### 2.2.1 Begriffsdefinitionen

#### 2.2.1.1 Security-Layer und Security-Kapsel

Als Security-Layer wird die Schnittstelle bezeichnet, über die eine Applikation die Funktionalität des Konzepts Bürgerkarte nutzt. Der Begriff Security-Kapsel bezeichnet ein System, das die Schnittstelle des Security-Layers implementiert.

#### 2.2.1.2 Infoboxen

Über die Schnittstelle des Security-Layers kann die Applikation auf den Datenspeicher der Bürgerkarten-Umgebung zugreifen. Dieser Datenspeicher ist in logische Einheiten gegliedert, die so genannten Infoboxen. Von der logischen Sicht der Applikation auf den Datenspeicher in Form von Infoboxen ist die tatsächliche physikalische Gliederung des Datenspeichers innerhalb der Bürgerkarten-Umgebung zu unterscheiden.

### 2.2.2 Anforderungen

Die Schnittstelle des Security-Layers umfasst eine Vielzahl von Befehlen, welche die Applikation benutzen kann, um auf Funktionalitäten aus dem Konzept Bürgerkarte zuzugreifen. Aus der Sicht eines Anbieters einer Schnittstellenimplementierung stellt sich die Frage, welche dieser Befehle jedenfalls implementiert sein müssen, damit ein Produkt als Bürgerkarten tauglich bezeichnet werden kann.

### 2.2.2.1 Erstellung einer elektronischen Signatur

Die Schnittstelle stellt Befehle zur Verfügung, welche die Erstellung einer elektronischen Signatur nach zwei gängigen standardisierten Formaten erlaubt: CMS [Hous99] und XMLDSIG [EaRS02].

### 2.2.2.2 Überprüfung einer elektronischen Signatur

Als Gegenstück zu den Befehlen zur Erstellung einer elektronischen Signatur existieren entsprechende Befehle zur Überprüfung von elektronischen Signaturen in den beiden erwähnten Formaten. Überprüft werden können nicht nur solche elektronische Signaturen, die nach dem Profil des Security-Layers erstellt wurden, sondern auch beliebige andere, solange sie der grundlegenden Spezifikation von CMS und XMLDSIG entsprechen.

### 2.2.2.3 Benützung des Datenspeichers (Infoboxen)

Der Applikation stehen eine Reihe von Befehlen zur Verwendung des Datenspeichers des Konzepts Bürgerkarte zur Verfügung, der logisch in sog. Infoboxen gegliedert ist. Neben der Abfrage einer Liste verfügbarer Infoboxen stehen Befehle zum gezielten Lesen und Schreiben einer Infobox oder von Teilbereichen davon zur Verfügung.

### 2.2.2.4 Abfrage von Eigenschaften

Schließlich kann eine Applikation eine Reihe von Eigenschaften sowohl des Bürgerkarten-Tokens selbst als auch der eingesetzten Bürgerkarten-Umgebung abfragen. Beispielsweise kann abgefragt werden, ob der Bürgerkarten-Token von der Umgebung angesprochen werden kann, um gegebenenfalls dem Bürger zu signalisieren, den Token einzustecken.

### 2.2.2.5 Erstellung eines Sitzungszertifikates

Zur Unterstützung des Aufbaus einer vertraulichen und authentifizierten Kommunikation kann die Security-Kapsel die Möglichkeit, ein Session-Schlüsselpaar zusammen mit einem zugehörigen Session-Zertifikat zu generieren, bieten.

## 2.2.3 Weiterführende Literatur

Eine Definition der Schnittstelle des Security-Layers sowie die Minimalanforderungen an eine Implementierung dieser Schnittstelle finden sich in [HoKa02].

## 2.3 Technische Aspekte

### 2.3.1 Algorithmen

#### 2.3.1.1 Signatur

Ein Schema zur sicheren elektronischen Signatur im Sinne des Gesetzes umfasst die folgenden Kryptoalgorithmen:

- Einen Algorithmus zum Hashen von Daten (eine Hashfunktion), der die zu signierenden Daten auf einen Hashwert, d.h. eine Bitfolge fester kurzer Länge, reduziert. Signiert werden dann nicht die Daten selbst, sondern stattdessen jeweils ihr Hashwert.
- Gegebenenfalls Anwendung einer Kodierungsoperation auf den Hashwert (Padding bei RSA)
- Ein asymmetrisches Signaturverfahren, das aus einem Signier- und einem Verifizieralgorithmus besteht. Das Signaturverfahren hängt von einem Schlüsselpaar ab, bestehend aus einem privaten (d.h. geheimen) Schlüssel zum Signieren (Erzeugen einer Signatur) und dem da zugehörigen öffentlichen Schlüssel zum Verifizieren (Prüfen) der Signatur.

Die technischen Verfahren und Formate und ihre Parameter sind in der Signaturverordnung (Anhang 2, bzw. Anhang 1) geregelt.

Die zulässigen Signaturverfahren unterscheiden sich durch die verwendete Signatur- und Verifikationsfunktion (RSA, DSA oder ECDSA), den verwendeten Hashalgorithmus zur Bestimmung des Hashwertes (SHA-1 oder RIPEMD-160) und das verwendete Paddingverfahren (bei RSA). Welche Algorithmen Anwendung finden, bestimmt der Zertifizierungsdiensteanbieter.

Die Algorithmen und ihre Parameter werden gemäß der weiteren Entwicklung der kryptologischen Forschung und den Erfahrungen mit praktischen Realisierungen von Signaturverfahren aktualisiert und gegebenenfalls ergänzt werden. Im Rahmen der European Electronic Signature Standardisation Initiative (EESSI) arbeitet die Algorithmen Gruppe (ALGO) an der laufenden Überprüfung und Ergänzung der kryptographischen Verfahren und definiert geeignete Algorithmen und Parameter für sichere elektronische Signaturen [Algo01].

Im Rahmen des Konzeptes Bürgerkarte sind von der Verwaltung alle Signaturverfahren zu akzeptieren, die der Signaturverordnung entsprechen. Für die Signaturen der Verwaltung ist es sinnvoll, sich auf ein einzelnes Verfahren zu beschränken.

Seitens der Verwaltung werden Signaturverfahren, die auf elliptischen Kurven basieren empfohlen (ECDSA). Dies verspricht eine längere Lebensdauer der Token, da die Schlüssel nach heutigem Wissenstand deutlich später als nicht mehr gültig einzustufen sein werden.

Dies ist nachfolgend an einem Beispiel dargestellt. Erheblich kürzere Signaturen (~ 1/3 der Länge von RSA 1024) haben folgenden Vorteil beim Ausdruck:



XML-basierte signierte Dokumente können aus dem Papierausdruck inklusive der Signatur rekonstruiert werden, und Papier und elektronische Form haben gleiche Beweiskraft.

## 2.3.2 Formate

### 2.3.2.1 Signatur

Die Schnittstelle des Security-Layer unterstützt die Erstellung sowie die Überprüfung von elektronischen Signaturen nach zwei gängigen international standardisierten Formaten: Cryptographic Message Syntax (CMS) und XML-Signature Syntax and Processing (XMLDSIG).

CMS wurde von der Internet Engineering Task Force (IETF) standardisiert, basiert auf ASN.1 und findet heute hauptsächlich Anwendung bei der Signierung von Email. XMLDSIG ist ein neueres Signaturformat, das gemeinsam von der IETF sowie dem W3C (World Wide Web Consortium) spezifiziert wurde. Es basiert auf XML und eignet sich daher besonders für die Signierung von strukturiert in XML vorliegenden Daten oder Protokollelementen.

Eine minimale Implementation des Security-Layers muss Erstellung und Überprüfung von elektronischen Signaturen im Format XMLDSIG erlauben. Der Umgang mit CMS-Signaturen ist hingegen optional.

### 2.3.2.2 Zertifikat

Um digitale Signaturen Personen zuzuordnen, bedarf es einer Bindung des Namens einer Person an den entsprechenden öffentlichen Schlüssel. Diese Bindung erfolgt in der Form eines speziellen digitalen Dokumentes, welches von einer vertrauenswürdigen dritten Instanz ausgestellt wird. Diese Dokumente, üblicherweise als Zertifikate bezeichnet, können als "digitale Ausweise" angesehen werden. Technisch gesehen sind Zertifikate Datenstrukturen, die Informationen enthalten, mit denen eine Bindung von öffentlichen Schlüsseln an Schlüsselhaber gewährleistet wird. Die konkrete Bindung eines öffentlichen Schlüssels an

einen bestimmten Schlüsselinhaber wird durch eine vertrauenswürdige und neutrale Zertifizierungsstelle (CA, certification authority, ZDA) bewerkstelligt, die das zugehörige vollständige Zertifikat mit ihrer digitalen Signatur beglaubigt. Zertifikate haben nur eine begrenzte Gültigkeitsdauer, die ebenfalls als Bestandteil des Zertifikates von der Zertifizierungsstelle mitsigniert ist. Die Zertifizierungsstelle übernimmt die Prüfung des Namens und bindet durch eine digitale Signatur (mit ihrem privaten Schlüssel) den Namen der Person an den öffentlichen Schlüssel dieser Person. Das Resultat der Zertifizierung eines öffentlichen Schlüssels ist ein Zertifikat.

### 2.3.3 Ausstattung beim Bürger

Das Konzept Bürgerkarte schränkt durch die Wahl offener Schnittstellen (z.B. im Security Layer) die verwendbaren Technologien nicht ein. Es ist auch denkbar, dass zukünftig der Bürgerkarten-Token, die Bürgerkarten-Umgebung und die Bürgerkarten-Applikationen auf einem einzelnen Gerät realisiert sind.

Nach dem derzeitigen Stand der Technik wird folgende Ausstattung benötigt:

- Eine bürgerkartenfähige Chipkarte (siehe Kapitel 3)
- Ein geeignetes Chipkartenterminal
- Ein Arbeitsplatz

Für die Erstellung sicherer Signaturen nach SigG bestehen gesetzliche Anforderungen an technische Komponenten. Die Zertifizierungsdiensteanbieter sind verpflichtet, ihren Kunden geeignete Geräte und Applikationen für die Erstellung sicherer Signaturen zu nennen.

## 3 Ausprägungen der Bürgerkarte

Das von A-SIT und der CIO-Unit erarbeitete Konzept zur Bürgerkarte sieht ausdrücklich keine bestimmte Karte oder Kartentyp vor.

Die Entscheidung ein offenes Modell zu wählen, in dem verschiedenste Kartenarten unterschiedlicher ausgebender Stellen als Bürgerkarte eingesetzt werden können, beruht auf folgenden Überlegungen:

Die Festlegung auf ein Konzept und nicht auf eine bestimmte Karte soll zu einer raschen und weiten Verbreitung der Bürgerkarte führen, die alle im Bereich e-Government eingesetzt werden können.

Im Sinne einer Public-Private-Partnership, sollen die Karten nicht nur von Behörden ausgegeben werden, wie es derzeit bei amtlichen Lichtbildausweisen der Fall ist. Auch Karten, die von der Privatwirtschaft, wie etwa Banken, oder Kammern ausgegeben werden, sollen als Bürgerkarte zur Kommunikation mit der Verwaltung einsetzbar sein. Generell ist in den nächsten Jahren eine deutliche Erhöhung des Anteils an Chipkarten, der auch sichere elektronische Signaturen erzeugen kann, zu erwarten.

Ebenso, wie die Karten auch von privaten Stellen ausgegeben werden, ist der Einsatz der Karten, die als Bürgerkarte eingesetzt werden können, nicht nur auf die Verwendung zur Kommunikation mit der Verwaltung beschränkt, der Karteninhaber kann sie ebenso im Rahmen seiner privaten Geschäftstätigkeit einsetzen, was auch für den Bereich des e-Commerce eine deutliche Erhöhung des Sicherheitsniveaus bedeutet.

Das Konzept Bürgerkarte baut auf Technologieneutralität auf. Bewusst wird für das Speichermedium der Signaturerstellungsdaten nicht das Wort Chipkarte sondern der Überbegriff Token verwendet, sodass neue Speichermedien wie etwa USB-Tokens oder Handy-SIMs ebenfalls bürgerkartenfähig sein können. Eine homogene Infrastruktur mit nur einer Kartenausprägung ist schwerer auf neue Technologien umzustellen, als langsame Penetration neuer Technologien durch mehrere ausgebende Organisationen. Folgende Ausprägungen des Konzeptes Bürgerkarte werden in den nächsten Monaten verfügbar sein:

### 3.1 e-card



Die österreichischen Sozialversicherungen werden bis Ende 2003 an etwa 8.000.000 Versicherte und deren Angehörige die sogenannte e-card ausliefern. Diese Chipkarte wird den Krankenschein ersetzen. Entsprechend dem gesetzlichen Auftrag (56. ASVG Novelle) ist die Karte zur Kombination mit Bürgerkartenfunktionen besonders geeignet.

Auf der Vorderseite der Karte sind Familien- und Vorname, Versicherungsnummer, Titel und Folgenummer der e-card angedruckt. Die

Rückseite trägt die Internet-Adresse sowie die Telefonnummer des Call Centers, welches bei Verlust oder Diebstahl zu verständigen ist.

Die Grundeinteilung des Chips besteht aus zwei Bereichen:

- dem Bereich der Sozialversicherung.
- dem Bereich der Bürgerkarte, der die bereits beschriebenen Elemente, die das Konzept Bürgerkarte vorsieht, enthält.

Der Bereich der Sozialversicherung basiert auf symmetrischen Schlüsseln und kann nur mit einer Gegenkarte, der Ordinationskarte des Arztes, ausgelesen werden. Er ist für andere Anwendungen nicht sichtbar. Damit ist die sichere Trennung der Sozialversicherungsanwendung von jenen des „Konzepts Bürgerkarte“ gewährleistet.

### 3.2 Personalausweis

Seit 08.01.2002 wird der Personalausweis neu als Plastikkarte im Chipkartenformat ausgegeben. Im 3. Quartal 2002 soll auf Wunsch des Bürgers auch ein Chip in den Personalausweis implementiert werden. Prinzipiell ist jeder beliebige Signaturchip einsetzbar, solange die Anforderungen aus dem Konzept Bürgerkarte erfüllt sind.



### 3.3 OCG Karte

Die Österreichische Computergesellschaft wird als erste Institution Mitgliedskarten mit Bürgerkartenfunktionalität ausgeben. Die Mitglieder der OCG sind naturgemäß IT-erfahrene Anwender. Ihr Knowhow und ihr Verständnis für Problemstellungen bei neuen Soft- und Hardwareprodukten machen sie zur idealen Gruppe eines erweiterten Feldtestes des Konzeptes Bürgerkarte. [OCG2002]

### 3.4 Studentenkarten

In Österreich haben bereits zwei Universitäten Erfahrungen mit Studentenausweisen in Chipkartenform gesammelt. Es sind dies die Kepler Universität Linz, die schon 1996 den Studentenausweis auf eine digitale Chip-Karte umgestellt hat, sowie die Wirtschaftsuniversität Wien, die im Wintersemester 2000/2001 eine Chip-Karte eingeführt hat. Im Sommersemester 2002 werden auch die Universitäten Innsbruck und Salzburg erstmals Studienausweise in Form von Chipkarten ausgeben. Allerdings erfüllen diese Karten derzeit noch nicht die Grundanforderungen des Konzepts Bürgerkarte. Einzig die Karte der WU-Wien soll ab Herbst 2002 alle Anforderungen erfüllen.

Studentenkarten müssen, was die Oberfläche betrifft, Ausweisfunktion erfüllen. Darüberhinaus können Chipkarten viele verschiedene Funktionen abdecken. Signaturwürdige

Vorgänge, im Sinne des „Konzeptes Bürgerkarte“ ergeben sich sowohl für Studierende als auch für Universitätsangestellte. Für Studierende sind dies:

- Datenkorrekturen (Adress-, Namensänderung)
- Wechsel der Studienrichtung
- Beurlaubungen
- Anmeldungen zu Lehrveranstaltungen mit Beifügung der notwendigen Dokumente
- Prüfungsan- bzw. -abmeldung
- Evaluierung von Lehrveranstaltungen
- Externe Anträge (Studien- u. Familienbeihilfen, Befreiungen etc.)
- Identifikation bei Wahlen

Auf Seiten der Universitätsbediensteten ergeben sich mehr und vor allem häufigere signaturwürdige Transaktionen:

- Prüfungsverwaltung (Ankündigung von Terminen, Beurteilungen, Anrechenbarkeiten)
- Lehrverwaltung (Erstellung Institutsvorschlag, Ankündigungen der Dozenten im Rahmen ihrer Lehrbefugnis, Zuordnung durch Studienkommission, Überarbeitung bzw. Beauftragung durch Studiendekan, Erstellung der Beauftragungsdekrete, Gegenzeichnung durch die Vortragenden, Beginnmeldung der Vorlesung)
- Bestellungen
- Budgetmittel (Antrag, Zuweisung, Abruf, Zeichnungsberechtigungen)
- Personalwesen (SV-Anmeldung, Urlaub, Krankenstand)
- Ausschreibungen
- Zeugnisausstellung

Darüber hinaus sind für beide Gruppen Zugangskontrollen, Zeiterfassungssysteme und Single Sign On, Anwendungen, die mit Hilfe einer „Konzept Bürgerkarte“ konformen Struktur ideal gelöst werden können.

### 3.5 Bankkarten

Laut Austrian Internet Monitor (4.Qu.2001) nutzt bereits jeder vierte Internetuser die Möglichkeiten des Online Bankings. Die derzeit dafür verwendeten PIN/TAN Verfahren bieten bei zunehmender Useranzahl immer weniger Sicherheit.

Die sichere elektronische Signatur eröffnet die Möglichkeit Bankgeschäfte einfach, rechtssicher und nachvollziehbar über das Internet abzuwickeln. Neben dem qualitativen Sicherheitsgewinn im Online Banking können mittels sicherer elektronischer Signatur auch andere Transaktionen wie Kontoeröffnung, Vertragsabschlüsse oder Ähnliches rechtsverbindlich aber beleglos ohne weitere Legitimationsverfahren abgewickelt werden.

Die österreichischen Banken planen ab 2004 bürgerkartenfähige Bankomatkarten auszugeben.

### 3.6 Signaturkarten der Zertifizierungsdiensteanbieter

Die Zertifizierungsdiensteanbieter bieten ihren Kunden eigene Chipkarten für die Erstellung sicherer Signaturen an. Sofern diese Karten die unter 2.2.2 genannten Anforderungen erfüllen, können sie als Bürgerkarte eingesetzt werden.

## 4 Lebenszyklus

Der klassische Lebenszyklus einer Chipkarte besteht nach ISO 10 202-1[www.iso.ch] aus 5 Phasen:

- **Herstellung von Chip und Chipkarte.** In diese Phase fallen das Chipdesign, die Betriebssystemerstellung, die Produktion des Chips und der Module, die Herstellung des Kartenkörpers und das Einbetten der Module in den Kartenkörper.
- **Kartenvorbereitung.** Hier wird das Chipkarten-Betriebssystem komplettiert. Sowohl diese Phase, als auch die vorangegangene sind nicht Teil des Weißbuchs, da sie individuell vom Hersteller, je nach Verwendungszweck der Karte gestaltet werden.
- **Anwendungsvorbereitung.** Dieser Teil deckt die optische und elektronische Personalisierung der Chipkarte ab.
- **Kartenbenutzung.** Der e-Government spezifische Teil wird in Kapitel 5 abgehandelt. Ansonsten differiert die Nutzung je nach Karte und wird daher hier nicht näher behandelt.
- **Ende der Kartenbenutzung.** Hier werden nach ISO 10 202-1 alle Maßnahmen bei Ende der Kartennutzung festgelegt. Dies sind vor allem die Deaktivierung der Anwendungen und die Deaktivierung der Chipkarte selbst.

### 4.1 Personalisierung

In dieser Phase des Lebenszyklus werden alle Daten, die einer einzelnen Person oder Karte zugeordnet sind, in die Chipkarte ein- bzw. aufgebracht.

#### 4.1.1 Oberfläche

Das Konzept Bürgerkarte schreibt keine bestimmte Oberflächengestaltung einer Karte vor. Es sollte lediglich gewährleistet sein, dass jeder Karteninhaber seine ihm zugeordnete Karte eindeutig identifizieren kann.

### 4.2 Registrierung

#### 4.2.1 Freie Wahl des Zertifizierungsdiensteanbieters (ZDA)

Das qualifizierte Zertifikat stellt ein wesentliches Element der sicheren elektronischen Signatur dar, indem es Angaben zum Signator und dessen öffentlichen Schlüssel miteinander verknüpft, um so dessen Identität den Empfängern der signierten Dokumente nachzuweisen. Da Dienste zu gewerblichen Zwecken in Österreich ausschließlich der Wirtschaft vorbehalten sind, werden Zertifizierungsdienstleistungen im engeren Sinn (die Generierung und Veröffentlichung des Zertifikats in den Verzeichnissen und die Durchführung eines Widerrufs) von den am Markt tätigen Zertifizierungsdiensteanbietern, die qualifizierte Zertifikate anbieten, erbracht.

#### 4.2.2 Behörden als Registrierungsstellen (RS)

Die Durchführung der Registrierung in einer Dienststelle der Verwaltung ist als Serviceleistung für die Bürger sinnvoll, da viele Bürger gelegentlich eine Behörde aufsuchen müssen. Besitzt der Bürger bereits eine schon bürgerkartentaugliche Chipkarte mit Personenbindung, Zertifikate und sichere elektronische Signatur ist eine nochmalige Registrierung durch die Behörde nicht notwendig.

Alle ZDAs sind, soweit sie die technischen Anforderungen erfüllen, im Rahmen der Registrierung gleich zu behandeln. Insbesondere sind Empfehlungen durch die registrierende Dienststelle zugunsten eines ZDA verboten.

Bei der Dienststelle sollte ein Wechseln nach der Registrierung für einen ZDA zur Registrierung für einen anderen ZDA möglichst schnell erfolgen. Vorzugsweise wird eine

Applikation zur Datenerfassung im Rahmen der Registrierung für alle ZDAs verwendet, die die im Rahmen der Registrierung erfassten Daten an alle ZDAs in standardisierter Form (XML-Protokoll) übermitteln kann.

Im Rahmen der Registrierung ist der Karteninhaber entsprechend § 20 SigG zu belehren. Die Belehrungsmaterialien werden seitens der ZDAs beigestellt. Die Belehrung muss nicht unmittelbar bei der Registrierung bzw. während des Registrierungsprozesses erbracht werden. So kann der Nachweis zumindest für den ZDA-unabhängigen Bereich einer gleichartigen Schulung über den Umgang mit elektronischen Signaturen etwa auch durch die Absolvierung eines Kurses wie dem Europäischen Computerführerschein (ECDL) erbracht werden.

#### 4.2.2.1 Schnittstelle zwischen RS und ZDA

Die Registrierung soll unabhängig vom ZDA mit einer einheitlichen Software vorgenommen werden. Voraussetzung für eine solche gemeinsame Software ist eine wohl definierte Schnittstelle für die notwendigen Abfragen der RS beim ZDA. Folgende Abfragen könnten abhängig vom jeweiligen Registrierungsszenario von der RS an den ZDA gestellt werden:

- Abfrage der vom ZDA vorerfassten Registrierungsdaten: Zur Verringerung der bei der Registrierung durchzuführenden Tätigkeiten ist es sinnvoll, einen Großteil der vom Bürger anzugebenden Daten bereits vorab - beispielsweise über ein Webformular beim ZDA - zu erfassen. Diese Daten werden dann zu Beginn des Registrierungsvorgangs beim ZDA abgerufen.
- Übermittlung sämtlicher bei der Registrierung erfassten Daten zur weiteren Bearbeitung an den ZDA. Diese Daten umfassen die persönlichen Angaben des Bürgers, Angaben zum gewählten Produkt des ZDA, Zertifikatsantrag, Identitätsnachweis sowie ggf. den Nachweis der erfolgten Belehrung des Bürgers. Als Antwort auf diese Übermittlung sendet der ZDA - abhängig davon, ob der Bürgerkarten-Token in der RS vorhanden ist oder nicht - entweder die dort auf den Bürgerkarten-Token zu schreibenden Daten (Zertifikat und Personenbindung) oder lediglich die Bestätigung des Erhalts der übermittelten Daten.

Die Schnittstelle für diese Abfragen ist in [Karl02b] spezifiziert.

### 4.3 Verzeichnis- und Widerrufsdienste

Das grundlegende Prinzip der Vertrauensbildung in öffentlichen Sicherheitsinfrastrukturen beruht auf dem Vertrauen in die von Zertifizierungsdiensteanbietern ausgestellten und von ihnen signierten Zertifikate, durch die letztlich eine Bindung der zugehörigen öffentlichen Schlüssel an die jeweiligen Schlüsselinhaber erreicht wird.

Bei der Erstellung eines Zertifikates wird u.a. eine Gültigkeitsdauer für dieses Zertifikat festgelegt und als Bestandteil in das Zertifikat integriert. Der Zeitpunkt der Zertifikatserstellung muss dabei nicht mit dem Beginn der Gültigkeitsdauer übereinstimmen. Er kann durch optionale Zertifikatserweiterungen als Bestandteil des Zertifikates angegeben werden. Prinzipiell kann davon ausgegangen werden, dass ein Zertifikat während seiner gesamten Gültigkeitsdauer benutzt wird. Es gibt jedoch bestimmte Situationen, die eine vorzeitige Beendigung der Gültigkeitsdauer eines Zertifikates veranlassen und erzwingen, dass das betreffende Zertifikat vom zuständigen Zertifizierungsdiensteanbieter zu sperren ist. Sobald eine missbräuchliche Nutzung eines Signaturschlüssels nicht mehr ausgeschlossen werden kann (z.B. aufgrund des Verlusts oder Diebstahls der Signaturkomponente), muss mit möglichen Angriffen und damit mit einer Verletzung und Gefährdung der Sicherheit während der restlich verbliebenen Gültigkeitsdauer eines Zertifikates gerechnet werden. Für diese kritischen Situationen müssen entsprechende Vorkehrungen und Sicherheitsmaßnahmen vorgesehen werden, mit dem Ziel das Restrisiko für Angriffe und dadurch die verursachte Gefährdung der Sicherheitsinfrastruktur zu minimieren. In diesem Zusammenhang spielen die Verzeichnis- und Widerrufsdienste des Zertifizierungsdiensteanbieters eine entscheidende Rolle.

Der Verzeichnisdienst im Sinne des Signaturgesetzes ist von jenen Diensten zu unterscheiden, die üblicherweise als Verzeichnisdienst (X.500 oder LDAP Directory Service)

bezeichnet werden. In diesem Dokument wird mit Verzeichnisdienst der Verzeichnisdienst im Sinne des Signaturgesetzes bezeichnet. Ein Verzeichnisdienst führt alle ausgestellten Zertifikate (gültig oder ungültig) eines Zertifizierungsdiensteanbieters.

Widerrufsdienste stellen Sperrlisten (CRLs - Certificate Revocation Lists) zur Verfügung, die alle gesperrten und widerrufenen Zertifikate eines Zertifizierungsdiensteanbieters beinhalten.

Als unmittelbare Folge der Forderung nach einer Minimierung des Restrisikos für Angriffe lassen sich für Zertifikatsinhaber und Zertifizierungsdiensteanbieter folgende Konsequenzen ziehen:

Zertifizierungsdiensteanbieter sollten möglichst frühzeitig

- Sperrsituationen erkennen,
- Meldungen von Zertifikatsinhabern erhalten,
- die Aktualisierung von Sperrlisten durchführen,
- Updates an ihren Verzeichnisdienst zur Verfügung stellen und
- nur Online-Dienste mit bestimmten Sicherheitsrichtlinien zulassen.

Zertifikatsinhaber sollten möglichst frühzeitig

- Sperrsituationen erkennen,
- Meldung an den zugehörigen Zertifizierungsdiensteanbieter machen,
- sich aktuelle Sperrlisten beschaffen und
- bei der Prüfung von Zertifikaten in geeigneter Weise Online-Dienste zur Statusabfrage von Zertifikaten nutzen.

Zertifizierungsdiensteanbieter müssen Widerrufs- bzw. Sperrlisten online zur Verfügung stellen und diese in regelmäßigen Abständen aktualisieren.

## 4.4 Zertifikatsverlängerung

Zertifikate werden vom Zertifizierungsdiensteanbieter grundsätzlich mit einer begrenzten Gültigkeitsdauer ausgestattet.

Dem Zertifikatsinhaber sollen vom Zertifizierungsdiensteanbieter geeignete Möglichkeiten bereitgestellt werden, vor Ablauf der Gültigkeitsdauer eine Zertifikatsverlängerung auch auf elektronischem Wege vornehmen zu können, ohne dass dazu erneut eine Registrierungsstelle aufgesucht werden muss.

## 5 Anwendungen im e-Government

Dieses Kapitel beschreibt die möglichen Anwendungen eines dem Konzept Bürgerkarte entsprechenden Tokens im Bereich des e-Governments. e-Commerce Anwendungen bleiben davon unberührt.

### 5.1 Signatur

Ohne kryptographische Methoden bei der Kommunikation über das Internet besteht die Unsicherheit über die wahre Identität des Kommunikationspartners und Zweifel, ob abgesandte Informationen auch authentisch sind und nicht am Übertragungsweg verändert wurden, störende Faktoren, die den durch die schnelle und kostengünstige Informationsübertragung erzielten Nutzen deutlich schmälern. Diese Sicherheitsrisiken machten bisher den Einsatz des Internets für die Kommunikation mit der Verwaltung in allen Fällen, in denen an Anbringen und Erledigungen Rechtsfolgen geknüpft waren, im großen Umfang unmöglich. Im Folgenden sollen die Funktionen einer eigenhändigen Unterschrift kurz beschrieben werden, um daran die Anforderungen an die sichere elektronische Signatur, wie sie mit einer Bürgerkarte erzeugt werden kann, aufzuzeigen.

### 5.1.1 Identifikation

Eigenhändige Unterschriften und sichere elektronische Signaturen sind dadurch gekennzeichnet, dass die Identität des Ausstellers durch sie nachgewiesen ist. Die Gewährleistung dieser zentralen Funktion durch sichere elektronische Signaturen ist eine der Hauptfunktionen des Konzepts Bürgerkarte. Das qualifizierte Zertifikat muss den Namen des Signators enthalten. Die technischen Komponenten und Verfahren sind so zu gestalten, dass ein Umgehen der Identitätsfunktion mittels einer Verwendung der sicheren Signaturerstellungseinheit zur Abgabe einer elektronischen Signatur mit fremden Namen durch Dritte verhindert wird.

### 5.1.2 Echtheit

In engem Zusammenhang zur Identitätsfunktion steht die Echtheitsfunktion der Unterschriften und Signaturen. Sie bietet die Gewähr, dass das Dokument vom signierenden Aussteller stammt. Nachträgliche Änderungen des Inhaltes, unter Umständen ohne Wissen der Unterzeichner, werden durch den Einsatz von signierten Hashwerten zuverlässig erkannt.

### 5.1.3 Abschluß und Warnung

Weiters dient die Signatur auch dazu, den Abschluss eines Dokumentes anzuzeigen. Dadurch wird zum Ausdruck gebracht, dass das Dokument fertig gestellt ist und sich nicht mehr in der Entwurfsphase befindet. Die Signatur schließt ein Dokument räumlich und zeitlich ab.

Auch kommt der Signatur eine Warnfunktion zu. Die PIN-Eingabe, die den Signaturvorgang auslöst, macht dem Signator die Rechtsverbindlichkeit seiner abgegebenen Erklärung deutlich.

### 5.1.4 Unleugbarkeit

Eine rechtserhebliche Willenserklärung verlangt, dass der Prozess der Übermittlung der Willenserklärung rückwirkend von den Beteiligten nicht mehr abzustreiten ist. In engem Zusammenhang mit der Beweisfunktion sicher elektronisch signierter Dokumente soll keiner der Kommunikationsteilnehmer im Nachhinein abstreiten können, eine Nachricht abgesendet oder erhalten zu haben. Für die Nachweisbarkeit von Zeitpunkten ist im Rahmen des Signaturgesetzes auch die Integration von gesicherten Zeitstempeln integriert, die der Nachweisbarkeit, dass ein Dokument zu einem gewissen Zeitpunkt jemandem zugestellt wurde, dienen kann.

## 5.2 Infoboxen

Wie bereits unter 2.1. erwähnt, umfasst die Funktionalität des Konzepts Bürgerkarte den Zugriff auf den Datenspeicher der Bürgerkarten-Umgebung über die Schnittstelle des Security-Layers. Dieser Datenspeicher ist logisch in so genannte Infoboxen unterteilt, die jeweils zusammengehörige und in sich abgeschlossene Daten kapseln. Beispielsweise können so Dokumente oder Vollmachten auf dem Token selbst abgelegt bzw. Verweise auf den tatsächlichen Speicherort dieser Beilagen auf dem Token gespeichert werden.

### 5.2.1 Dokumente

Für Applikationen im e-Government soll es möglich sein, verfahrensspezifische Daten in der Bürgerkarten-Umgebung zu speichern. Beispielsweise könnten in einem Verfahren, das zeitlich gesehen in mehreren Teilen abgewickelt wird, die Resultate aus früheren Teilen zwischengespeichert werden, um die spätere Fortsetzung des Verfahrens für den Bürger möglichst komfortabel zu gestalten.

Eine solche Speicherung ist jedoch vom Konzept Bürgerkarte her nur durch aktive Mitwirkung des Bürgers möglich, da ein Neuanlegen von Infoboxen über die Schnittstelle des Security-Layers nicht vorgesehen ist. Vielmehr muss dieses Neuanlegen der Bürger selbst über eine nicht näher definierte Konfigurationsschnittstelle seiner Bürgerkarten-Umgebung

vornehmen. Damit hat der Bürger jedenfalls die Kontrolle, welcher Applikation er die Verwendung von Infoboxen über die standardisierten Fälle hinaus erlaubt.

Eine neu angelegte Infobox steht dann der Applikation für Lese- und Schreibzugriffe über die Schnittstelle des Security-Layers zur Verfügung, wobei die Selektion über einen vom Bürger beim Anlegen vergebenen Bezeichner erfolgt.

### 5.2.2 Vollmachten

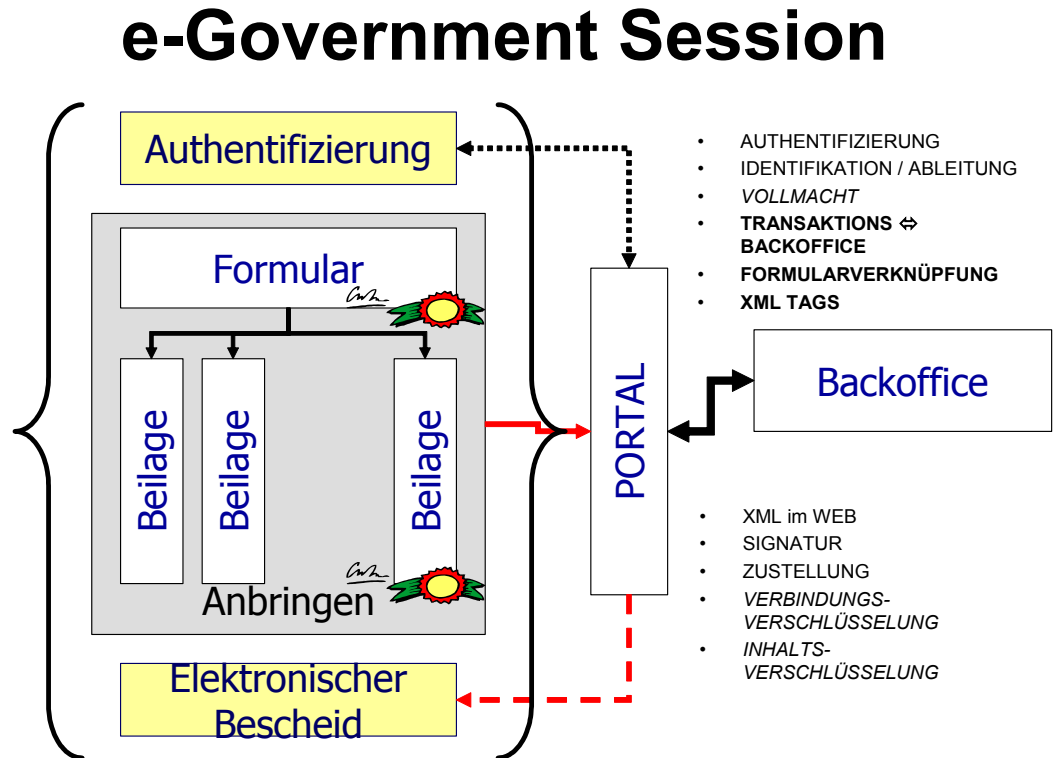
Vollmachten sind ein oft verwendetes Instrument im rechtlichen Handeln. Jemand anderer - der Vollmachtnehmer - handelt im Namen des Vollmachtgebers, aber zeichnet unter Berufung auf die (und eventuell unter Vorlage der) Vollmacht mit seiner eigenen eigenhändigen Unterschrift.

Dieser Vorgang ist auch im e-Government nötig und kann mit elektronischen Signaturen abgebildet werden. Der Vollmachtgeber signiert eben ein Formular, das einerseits die Art der Vollmacht in standardisierter Form enthält (welche Art von Geschäften, bis in welche Höhe, für wie lange), andererseits die Personenbindung des Vollmachtgebers und den öffentlichen Schlüssel des Vollmachtnehmers. Dieses signierte Dokument, die eigentliche Vollmacht, wird dem Vollmachtnehmer übermittelt, der nun mit seiner eigenen elektronischen Signatur unter Berufung auf die Vollmacht im Namen des Vollmachtgebers handeln kann.

Vollmachten, die oft verwendet werden, sollen sinnvollerweise direkt in der Infobox auf der Karte des Vollmachtnehmers gespeichert werden, sodass sie jederzeit zur Verfügung stehen. Verfügt jemand über sehr viele Vollmachten, zum Beispiel ein Wirtschaftstreuhand, wird die Karte nicht genug Platz bieten, um alle Vollmachten selbst dort zu speichern. Auf der Karte wird dann nur ein Zeiger auf den Ort, etwa auf den Datensafe des Wirtschaftstreuhanders, liegen, wo die Vollmachten gelesen werden können. Vollmachten können ohne weiters auch von Dritten gelesen und gespeichert werden, da sie nur in Verbindung mit dem privaten Schlüssel des Vollmachtnehmers verwendet werden können, und dieser nur vom Vollmachtnehmer verwendet werden kann.

### 5.3 Skizze e-Government-Session

Welche Phasen bei einer typischen e-Government Sitzung durchlaufen werden und welche Ausprägungen der e-Government-Session im speziellen berücksichtigt werden müssen, ist verfahrensabhängig. Trotzdem ist eine Grundstruktur bei den meisten Verfahren erkennbar:



Nach positiver Authentifizierung mittels Bürgerkarte sowie Ermittlung der Berechtigungen unter Einbeziehung des Security Layers wird die eigentliche e-Government Session etabliert. Dass man bei der Etablierung der e-Government Session auf Verbindungsverschlüsselung und andere sicherheitstechnische Grundstrukturen zurückgreift, ist als selbstverständlich vorauszusetzen. Im Browser wird z.B. ein HTML-Formular angezeigt, in dessen Formularfelder der Benutzer bereits Daten eingegeben hat. Die Formulardaten werden an den Web-Server übertragen, der daraus ein anwendungsspezifisches XML-Format erstellt, das an den Web-Browser zurückgegeben wird. Dieser Schritt ist erforderlich, da die Security-Kapsel nur XML-Daten in einem definierten Format (Security Layer) verarbeiten kann und diese zuvor aus den Formulardaten erstellt werden müssen. Die so erzeugten XML-Daten werden dann über die Schnittstelle des Security-Layers an die Security-Kapsel geschickt, um beispielsweise eine elektronische Signatur zu erstellen. Diese Aufgabe wird an den Web-Server delegiert, der wiederum eine HTML-Seite retourniert, die unsichtbare Felder (hidden-fields) enthält, in denen das definierte XML-Format enthalten ist. XML-Daten und Signatur werden an den Web-Server übertragen, der eine Weiterverarbeitung der Daten vornimmt und eine Statusmeldung zurückliefert.

Die XML-Formulardaten werden verfahrensbedingt durch Vollmachten bzw. andere (signierte) Beilagen erweitert und in einen XML-Container verpackt, über den dann ebenfalls signiert wird. Bei den Beilagen kann es sich auch um bereits zuvor zugestellte, signierte Bescheide (z.B. Strafregisterbescheinigung etc. ...), welche als Input für das Verfahren notwendig sind oder um elektronischen Zahlungsbestätigungen, in Form eines XML-Records handeln. Derartige Zahlungsbestätigungen werden von der Bankenwelt bzw. STUZZA ab dem Q3/2002 für alle elektronischen Banking-Verfahren angeboten werden. Es gilt zudem

sicherzustellen, dass diese Beilagen verwaltungsübergreifend (Bund, Ministerien, Länder, Gemeinden, ...) genutzt werden können, um Medienbrüche im Aktenlauf zu vermeiden.

Die signierten Formulare und Beilagen werden am Portal der Behörde auf einer virtuellen ‚Einlaufstelle‘ deponiert und dann dem jeweils zuständigen Kernbereich der Verwaltung (Backoffice) zur weiteren Verarbeitung zugeführt.

Für den Bürger muss bezüglich der Forderung nach Transparenz der Verwaltungsverfahren die Möglichkeit bestehen, Statusabfragen hinsichtlich der durchgeführten e-Government Verfahren zu initiieren. Auch für eventuell unvollständige Verwaltungsverfahren besteht auf Grund des strukturierten Aufbaus der Verfahren die Möglichkeit, an Schlüsselstellen die Kommunikation mit der Einlaufstelle bzw. Behörde fortzusetzen.

Als Ergebnis der Behördenaktivitäten erhält der Antragsteller in den meisten Fällen einen (signierten) Bescheid in Form eines XML-Datencontainers zugestellt. Dazu wird die Etablierung eines ‚elektronischen Amtskalenders‘ in LDAP-Format notwendig sein, der die Berechtigungen in punkto ‚Wer darf einen elektronischen Bescheid ausstellen‘ beinhaltet. Zudem müssen die verwendeten XML-Strukturen, welche dem Bescheid der Behörde zu Grunde liegen, hinsichtlich der verwendeten XML-Tags normiert sein, um eine automatische Weiterverarbeitung zu ermöglichen.

Effizientes e-Government setzt Automatisierung bei den Anbringen, aber auch bei den Antworten der Behörde (Zustellungen) voraus. Dafür wurde zwar in § 17 Zustellgesetz die generelle Grundlage geschaffen, doch sind dazu erst geeignete Randbedingungen zu finden, die auch ein annehmbares Verfahren ermöglichen. Folgende Bausteine werden für ein sicheres elektronisches Zustellungsverfahren benötigt:

- Ein Zustellserver, der von der Verwaltungsapplikation die zuzustellende Sendung abnimmt und dies gegenüber der Applikation und dem Empfänger verbindlich protokolliert. Mit dem Zustellserver wird in der Praxis oft auch ein Dokumentensafe verbunden sein.
- Ein System der Verständigung, sofern die Zustellung nicht interaktiv im Rahmen des Anbringens geschieht. Diese Verständigung kann auf unterschiedlichste Weise erfolgen. (e-Mail, SMS, Voicemail etc.)
- Die Zustellung bestehend aus der Abholung in elektronischer Form mit der Möglichkeit, die Authentizität zu prüfen (Signatur des Bescheides).
- Ein Nachweis der erfolgten Zustellung für die spätere Nachforschung.
- Für die Fälle, wo eine Zustellung in elektronischer Form nicht erfolgen kann, eine Überleitung in ein konventionelles Zustellverfahren.

Dazu kommen folgende weitere Anforderungen aus der Sicht der Sicherheitstechnik:

- Die zuzustellenden Schriftstücke müssen seitens der ausgebenden Applikation (Behörde) signiert sein. Da die automatische Signatur keinen nennenswerten Aufwand erfordert, wird dies unabhängig vom „Wert“ der Zustellung sinnvoll sein, um ein einheitliches Bild bei den Adressaten zu erzeugen.
- Die Dokumente und Signaturen müssen ein Format besitzen, welches nach Ausdruck ein Rückführen zum elektronischen Dokument einschließlich der Signatur erlaubt. Wenn es dabei Teile gibt, die dieser Anforderung nicht genügen können (z.B. Pläne, Bilder etc.), dann sind diese getrennt zu signieren und entsprechend eindeutig zu referenzieren.
- Die Übertragung hat generell verschlüsselt stattzufinden. Damit die Dienste der Zustellung nicht auf eine Behörde oder behördenähnliche Situation beschränkt sind, sind die Dokumente an den Zustellserver bereits verschlüsselt anzuliefern.
- Die Verschlüsselung hat sich auf den Empfänger zu beziehen.
- Bei der Verwendung als Dokumentensafe sind Maßnahmen, die dem rechtmäßigen Benutzer der Dokumente bei Verlust der Schlüssel einen angemessenen Zugang liefern,

sinnvoll. Diese Technologien sollten idealerweise unabhängig vom Dokumentensafe umgesetzt sein.

Die einzelnen Schritte sind verfahrensabhängig und werden unterschiedlich oft durchlaufen. Im Sinne eines verwaltungsübergreifenden Ansatzes sind allerdings noch einige Schritte in Richtung normierter Verfahrensdefinitionen, bereitgestellter Dokumentation der Strukturen und Elementgruppen sowie die Definition von ‚Formularen‘ und ‚Beilagen‘ und Offenlegung bzw. freie Verfügbarkeit dieser Strukturen (z.B. die Personenbindung, ... ) auf einem (öffentlichen) Server als unbedingt notwendig vorauszusetzen. Gemeinsam mit der Arbeitsgruppe der Länder wurden im Rahmen der eAustria Initiative bereits erste Fortschritte erzielt. Blickt man über die Landesgrenzen hinaus, würde es Sinn machen, Strukturen auch im internationalen Kontext zu sehen und so auch in Richtung e-Government innerhalb von eEurope für behördenübergreifende Verfahren bereit zu sein.

## 6 Rechtliche Aspekte

Im folgenden Abschnitt sollen die für die Bürgerkarte und ihre Anwendung im e-Government nötigen gesetzlichen Bestimmungen kurz vorgestellt werden. Eine nähere Diskussion des Rechtsrahmens anhand des Ablaufs einer typischen e-Government-Session ist bei [Menz02] zu finden.

### 6.1 SigG, SigV

Mit der Einführung und Anerkennung elektronischer Signaturen sollen die **rechtlichen Grundlagen** für den Einsatz **sicherer Technologien und Verfahren** im Internet und anderen elektronischen Netzwerken geschaffen werden. Dabei sollen unter anderem die Tätigkeit und die Verantwortung von Zertifizierungseinrichtungen, die in einem Zertifikat die Identität einer Person bescheinigen, geregelt werden. Weiters sollen die Rechtswirkungen elektronisch signierter Erklärungen klargestellt werden. Auf Grund des grenzüberschreitenden Charakters der neuen elektronischen Medien soll auch der Anerkennung ausländischer Regelungen über die elektronische Signatur besonderes Augenmerk gewidmet werden. Der Geltungsbereich des Signaturgesetzes erstreckt sich nicht nur auf die privatwirtschaftliche Tätigkeit, sondern es wurden bewusst für den Einsatz elektronischer Signaturen im Verwaltungsbereich keine zusätzlichen Anforderungen normiert, sodass hier dieselben durch Signaturgesetz und Verordnung vorgegebenen Rahmenbedingungen gelten.

#### Inhalt des Signaturgesetzes

Vorgabe von Mindestkriterien bezüglich der Sicherheit der eingesetzten technischen Verfahren und Komponenten;

- Zulassung und **Nichtdiskriminierung elektronischer Signaturen** im Geschäfts- und Rechtsverkehr inklusive der Kommunikation mit der Verwaltung;
- weitgehende Gleichstellung der **Rechtswirkungen einer sicheren elektronischen Signatur** mit den Rechtswirkungen einer eigenhändigen Unterschrift;
- Einführung eines **Aufsichtssystems über Zertifizierungseinrichtungen** einschließlich der Schaffung eines Systems zur freiwilligen Akkreditierung;
- Einführung von **Haftungsregelungen** für Zertifizierungseinrichtungen;
- Regelung der Voraussetzungen einer **Anerkennung ausländischer elektronischer Signaturen**.

### 6.2 AVG und ZustellG

Durch die Novellierung des Allgemeinen Verwaltungsverfahrensgesetzes 1991 und des Zustellgesetzes durch die Verwaltungsverfahrensnovelle 2001 und das Verwaltungsreformgesetz 2001 konnten die wesentlichen notwendigen Änderungen zur Einführung des e-Government im Bereich der österreichischen Behörden durchgeführt werden.

Im Wesentlichen bilden folgende Änderungen die Grundlage für das Konzept Bürgerkarte:

- Die ZMR-Zahl darf als Ausgangsbasis für eine verwaltungsbereichsspezifisch unterschiedliche, abgeleitete und verschlüsselte Personenkennzeichnung verwendet werden und auf Bürgerkarten als Ausgangszahl für die eindeutige Identifikation des Karteninhabers bei der Anwendung der elektronischen Signatur gespeichert werden. Die ZMR-Zahl darf von der Behörde anlässlich der elektronischen Identifikation nicht aufgezeichnet werden.
- Die Freiwilligkeit des e-Government: Im Wege automationsunterstützter Datenübertragung oder in jeder anderen technisch möglichen Weise können schriftliche Erledigungen dann übermittelt werden, wenn die Partei dieser Übermittlungsart ausdrücklich zugestimmt hat oder wenn sie Anbringen in derselben Weise eingebracht und dieser Übermittlungsart nicht gegenüber der Behörde ausdrücklich widersprochen hat.

### 6.3 MeldeG, MeldeV

Die ZMR-Zahl, die als grundlegender Identifikator im Rahmen der Verwendung einer Bürgerkarte gilt, wird vom Zentralen Melderegister erstellt und verwaltet und ist über dessen Datenbankschnittstelle abfragbar.. Die Bestimmungen stellen sicher, dass auch Behörden als Registrierungsstellen und die ZDAs, so sie Zertifikate für Bürgerkarten ausstellen, auf die ZMR-Datenbank zugreifen können und die für die Bürgerkarte notwendige Personenbindung vom ZMR als Resultat jeder gültigen Abfrage übermittelt bekommen.

### 6.4 Datenschutz

Grundrechte im liberalen Sinn sind Abwehrrechte des Einzelnen gegenüber überschießender Staatsgewalt. Im Sinne des besonders durch den deutschen BGH ausgearbeiteten Prinzips der informationellen Selbstbestimmung und der internationalen Akzeptanz dieses Prinzips, dem auch das DSG 2000 folgt, wird das Grundrecht auf Datenschutz insbesondere in Richtung der Freiwilligkeit der Weitergabe von Daten durch den Einzelnen ausgelegt. Dem folgend ist die österreichische E-Government-Lösung im allgemeinen und der Einsatz einer Bürgerkarte im besonderen nur auf Wunsch und mit Zustimmung des Bürgers möglich. Er entscheidet selbst, ob und wann er die Verwaltung auf elektronischem Wege kontaktiert. Konventionelle Wege zur hoheitlichen Verwaltung auf allen Ebenen stehen jedem weiterhin offen. Der Datenschutzrat und die Datenschutzkommission als gesetzlich eingesetzte Hüter dieses Grundrechtes überwachen jede generell-abstrakte und individuell-konkrete Einsatzmöglichkeit im Rahmen von E-Government auf die Übereinstimmung mit den Grundrechten und anderen Bestimmungen des Datenschutzrechtes. Das Konzept Bürgerkarte entspricht allen Vorschriften des DSG 2000.

## Glossar

### AES

Advanced Encryption Standard, vom NIST als DES Nachfolger bestimmt. Basiert auf dem Rijndael-Algorithmus. Als Schlüssellängen sind 128, 192 und 256 bit spezifiziert.

### ASN.1

Die Abkürzung ASN.1 (abstract syntax notation one) bezeichnet eine genormte abstrakte Notation zur Beschreibung von Datentypen und Datenwerten.

### Asymmetrische Schlüssel

Ein Schlüsselssystem, welches sicherstellt, dass man aus dem Verschlüsselungsschlüssel den Entschlüsselungsschlüssel nicht ermitteln kann. Durch die Eigenschaften des Schlüsselpaars gewährleistet es verschlüsselte Kommunikation, ohne dass von den Kommunikationspartnern vorher über einen gesicherten Kanal ein gemeinsamer (symmetrischer) Schlüssel vereinbart werden muss.

### Attributzertifikat

Ein international genormtes Format (X.509 oder ISO/IEC 9594-8:1998) dient im elektronischen Datenverkehr dazu, den Besitz von Rollen wie die Vertretungsmacht gegenüber Dritten nachzuweisen. Im Gegensatz zu einem Signaturschlüsselzertifikat enthält ein Attributzertifikat keinen öffentlichen Schlüssel.

### Authentifizierung

Eine Sicherheitsdienstleistung, die der Feststellung der Identität dient. Starke Authentifizierung wird mit kryptographischen Mechanismen realisiert.

### Bürgerkarten-Umgebung

Eine System, das die Bürgerkarte sowie die zum Einsatz der Bürgerkarte notwendigen Komponenten wie PIN-Eingabe, Hash-Berechnung, sichere Anzeige und Speicher kapselt und die daraus resultierende Funktionalität nach außen über die Schnittstelle des Security-Layer den Applikationen zur Verfügung stellt.

### Bürgerkarten-Token

Jener Hardware-Token, der zur Erstellung einer sicheren elektronischen Signatur nach SigG zur Kapselung der Signaturerstellungsdaten benötigt wird. Nach heutigem Stand der Technik wird das in den meisten Fällen eine Chipkarte mit kryptographischem Befehlssatz sein, vorstellbar sind aber etwa ein USB-Token oder das SIM-Modul eines Mobiltelefons.

### Brute-Force-Angriff

Angriff auf ein kryptographisches Verfahren bei dem alle möglichen Schlüssel durchprobiert werden, bis der Passende gefunden wird.

### Chipkarte

Eine Karte mit einem eingebetteten Mikroprozessor und ggf. kryptographischem Koprozessor (auch Prozessorkarte, Smartcard genannt).

### CMS Signaturen

Cryptographic message syntax. Signaturformat festgelegt in RFC 2630: Cryptographic Message Syntax (CMS). IETF Request For Comment, Juni 1999.

**CRL**

Certificate Revocation List. Widerrufsliste in der widerrufenen Zertifikate gelistet werden.

**DER**

DER (distinguished encoding rules) ist eine spezielle Kodierungsvariante von ASN.1, die eine Einschränkung von deren Transfersyntax ermöglicht, die man zu einer eindeutigen Dekodierung empfangener Daten benötigt.

**DES**

Data Encryption Standard ist ein von IBM entwickeltes symmetrisches Verschlüsselungsverfahren, das 1977 vom NIST als Standard veröffentlicht wurde. DES verwendet einen 56 bit Schlüssel, der 1999 in 22 Stunden gebrochen werden konnte. Heute wird vor allem Triple-DES (3DES) mit 2 oder 3 Schlüsseln eingesetzt (effektive Schlüssellänge 112 bit bzw. 168 bit). DES wird von AES als Standard-Verschlüsselungsalgorithmus abgelöst werden.

**DSA**

DSA steht für Digital Signature Algorithm und ist seit 1994 als Standard für elektronische Signaturen akzeptiert. DSA ist eine Variante der Unterschriftsalgorithmen von Schnorr und ElGamal.

**ECDSA**

Elliptic Curve Digital Signature Algorithm. Der auf elliptischen Kurven basierende Signaturalgorithmus ECDSA wurde 1998 als ISO (International Standards Organization) Standard (ISO 14888-3), 1999 als ANSI (American National Standards Institute) Standard (ANSI X9.62), und 2000 als IEEE (Institute of Electrical and Electronics Engineers) Standard (IEEE P1363) und FIPS (Federal Information Processing Standards ) Standard (FIPS 186-2) akzeptiert.

**e-Commerce**

Elektronische Dienstleistungen im elektronischen Handel.

**e-Government**

Elektronische Dienstleistungen in der öffentlichen Verwaltung.

**Elliptische Kurven**

Ein kryptographisches Verfahren mit asymmetrischen Schlüsseln, mit dem unter anderem auch elektronische Signaturen erstellt werden können.

**ELSY**

Elektronisches System zur Verwaltung im Sozialbereich; in der ersten Stufe wird der elektronische Krankenschein umgesetzt.

**Elektronische Signatur**

Elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung (d.h. der Feststellung der Identität des Signators) dienen.

**Hash-Funktion**

Eine Hash Funktion ist ein Verfahren zur Komprimierung von Daten mittels Einwegfunktion, so dass die ursprünglichen Daten nicht rückrechenbar sind. Das Ergebnis einer Hash Funktion ist der Hashwert.

## Infobox

Logische Einheit des Datenspeichers, die Applikationen durch die Bürgerkarten-Umgebung über die Schnittstelle des Security-Layer zur Verfügung gestellt wird. Eine Infobox kapselt logisch zusammengehörige Daten, unabhängig vom tatsächlichen physischen Speicherort der Einzeldaten innerhalb der Bürgerkarten-Umgebung.

## Integrität

Eine Sicherheitsdienstleistung, die sicherstellt, dass zu schützende Daten nicht auf unerlaubte Weise modifiziert wurden.

## Kryptographie

Wissenschaft von den Methoden der Ver- und Entschlüsselung von Daten.

## Kryptographische Schlüssel

Sicherheitstechnisch relevante elektronische Daten, die als Parameter in kryptographischen Verfahren verwendet werden. Bei jedem Verfahren gelten spezielle Regeln für die Erzeugung geeigneter Schlüssel.

## Kryptoprozessor

Meist auf Chipkarten implementierter Prozessor, der kryptographische Berechnungen ausführt.

## LDAP

Lightweight Directory Access Protocol. Protokoll für den Zugang zu Verzeichnisdiensten, das in den RFCs 2251 bis 2256 beschrieben wird.

## Nachsignieren

Erneutes elektronisches Signieren eines Dokumentes mit aktuell sicheren Verfahren wegen drohender Verringerung des Sicherheitswerts.

## NULLPIN

Ein Zugangscode, mit dem die Chipkarte an den Karteninhaber geliefert wird, und der vor der ersten Verwendung von dem Karteninhaber auf einen nur ihm bekannten Wert geändert werden muss.

## Öffentliche Schlüssel

Wenn ein Verschlüsselungsverfahren unterschiedliche aber zusammenhängende kryptographische Schlüssel für Verschlüsselung und Entschlüsselung verwendet, wird einer dieser Schlüssel der öffentliche Schlüssel und der andere der private Schlüssel genannt.

## Padding

Erweiterung eines Datenstrings mit Fülldaten, um einen Datenstring auf eine bestimmte Länge zu bringen

## PEM

Privacy Enhanced Mail. Sichere elektronische Post.

## Personalisierung der Chipkarte

Das sichere Aufbringen der personenbezogenen Daten auf eine Chipkarte (Rohling).

## **Personalisierung des Zugangs**

Eine Identifikation der Arbeitsumgebung bei dem Online-Zugang zu einem Portal, die mit der Person gleichgeschaltet sein kann.

## **Personenbindung**

Die Identität des Bürgers beim Herantreten an die Behörde muss eindeutig festgestellt werden können. Dieser Feststellung dient die Personenbindung genannte Datenstruktur, die auf der Karte abgelegt wird.

## **PIN**

Personal Identification Number: Kurzer Berechtigungscode (oft in Form einer 4 - 6 stelligen Nummer), der vor dem Zugriff auf eine Resource (etwa die Signaturerstellungsdaten) eingegeben werden muß. Damit ist der Schutz der Resource gemäß dem Prinzip von Besitz und Wissen sichergestellt.

## **PKCS#11**

Cryptographic Token Interface Standard, entwickelt von den RSA Laboratories.

## **PKI**

Eine Public Key Infrastruktur (PKI) ist eine Kombination von Software, Verschlüsselungstechnologien und Diensten, die sichere Geschäftskommunikationen und Datentransaktionen ermöglicht. PKIs helfen bei der Bereitstellung und Verwaltung von Zertifikaten und kryptographischen Schlüsseln, die Grundlagen für diverse Sicherheitsdienste sind.

## **Portal**

Ein Zugangspunkt im öffentlichen Datenübertragungsnetz (z.B. Internet) zu Informationen und Diensten (z.B. zum Verzeichnisdienst, Datenbanken etc).

## **Public Private Partnership**

Partnerschaft zwischen öffentlichem Bereich und Privatwirtschaft.

## **Qualifiziertes Zertifikat**

Ein Zertifikat, das die Angaben des § 5 SigG enthält und von einem den Anforderungen des § 7 SigG entsprechenden Zertifizierungsdiensteanbieter ausgestellt wird.

## **Registrar**

Der in einer Registrierungsstelle mit der Zertifikatsausstellung Beauftragte. Seine Hauptaufgabe ist die gesamte Durchführung der Erstregistrierung eines qualifizierten Zertifikats.

## **Registrierung**

Anmeldevorgang bei der elektronischen Signatur. Er dient der einmaligen Überprüfung der Identität des Signators durch persönliches Erscheinen bei einer Registrierungsstelle und Vorzeigen eines amtlichen Lichtbildausweises

## **Registrierungsstelle (RS)**

Für den Zertifizierungsdiensteanbieter tätige Stelle, bei der die persönliche Kontrolle der Identität eines Zertifikatswerbers durchgeführt wird.

## Rohling

Eine noch zu personalisierende Chipkarte, wie diese aus der Herstellung kommt.

## RSA

Von Rivest, Shamir und Adleman 1978 in den USA veröffentlichtes asymmetrisches Kryptosystem. RSA kann sowohl zur Verschlüsselung als auch für elektronische Signaturen eingesetzt werden.

## Security-Layer

Applikationsschnittstelle zur Funktionalität der Bürgerkarten-Umgebung. Über Befehle dieser Schnittstelle kann eine Anwendung beispielsweise eine elektronische Signatur erzeugen oder eine Infobox aus dem Datenspeicher der Bürgerkarten-Umgebung lesen.

## Sichere elektronische Signatur

Eine sichere elektronische Signatur ist eine elektronische Signatur, die ausschließlich dem Signator zugeordnet ist; die Identifizierung des Signators ermöglicht; mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann; mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass jede nachträgliche Änderung der Daten festgestellt werden kann; sowie auf einem qualifizierten Zertifikat beruht und unter Verwendung von technischen Komponenten und Verfahren, die den Sicherheitsanforderungen des Signaturgesetzes und der auf seiner Grundlage ergangenen Verordnungen entsprechen, erstellt wird.

## SigG

Siehe Signaturgesetz.

## Signaturerstellungsgesetz

Ein Gerät, das zur Erstellung elektronischer Signaturen dient (z.B. Chipkarte; auch Signaturerstellungseinheit genannt).

## Signaturgesetz

Bundesgesetz, das den rechtlichen Rahmen für die Erstellung und Verwendung elektronischer Signaturen sowie für die Erbringung von Signatur- und Zertifizierungsdiensten regelt (seit 1.1.2000 in Kraft).

## Signaturschlüssel

Ein privater Schlüssel zur Erstellung elektronischer Signaturen (siehe auch öffentlicher Schlüssel).

## SIM

Subscriber Identity Modul. GSM-spezifische Chipkarte, Träger der geheimen Authentisierungsinformationen für den GSM Betreiber und benutzerspezifischer Daten, wie beispielsweise Telefonnummern.

## SMS

Short Message Service. Kurze Nachrichten, die in der Regel von einem Handy zum anderen versandt werden. Die maximale Zeichenlänge beträgt 160 Zeichen.

## STUZZA

Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr GmbH, ein gemeinsames Unternehmen österreichischer Banken. In der STUZZA werden technische und organisatorische Normen ausgearbeitet, sowie gemeinsam getragene Regeln für deren Umsetzung durch die Geldinstitute, unabhängig ihrer unterschiedlichen geschäftlichen Ziele.

## Symmetrische Schlüssel

Wenn ein Verschlüsselungsverfahren den gleichen kryptographischen Schlüssel für Verschlüsselung und Entschlüsselung verwendet, wird dieser Schlüssel symmetrisch genannt.

## TAN

Transaction Number: Eine nur für eine einzelne Transaktion verwendbare Nummer, die erhöhten Schutz bei der Transaktion dient. Listen mit einem Set von TANs werden vorher über einen gesicherten Kanal übermittelt. Üblicherweise werden TANs bei den jetzigen Internet-Banking-Lösungen eingesetzt, um einzelne Überweisungen zu schützen.

## TCP/IP

Transmission Code Protocoll/Internet Protocoll: Standardisiertes Netzwerkprotokoll, das zum Datenaustausch unterschiedlichster Computer über das Internet normiert wurde.

## Transportschlüssel

Bezeichnet kryptographische Schlüssel (siehe auch Zugangsschlüssel), die den Zugang auf Bereiche einschränken und damit diese gegen unzulässige Modifikationen in ungesicherter Umgebung während des Transportes schützen, z.B. während des Transportes vom Hersteller zur Betreibergesellschaft.

## USB Token

Token der am Universal Serial Bus eines Computers angesteckt werden kann.

## Vereinzelung

Vereinzelung der Karten bezeichnet einen Vorgang, bei dem im Herstellungsprozess vorerst in Chargen idente Karten eindeutig und somit „einzelne“ Karten paarweise unterscheidbar werden. Dies wird bevorzugt über kryptographische Methoden abgesichert.

## Vereinzelungskennung

Eine im Zuge der Vereinzelung aufgebrachte, eindeutige Kennung der Karte. Diese kann im Zuge der Personalisierung, oder bereits zuvor im Zuge der Herstellung erfolgen.

## Verschlüsselung

Ein kryptographisches Verfahren, mit dem die Daten mit einem kryptographischen Schlüssel verarbeitet werden, sodass man das Ergebnis ohne diesen Schlüssel nicht lesen oder verstehen kann (d.h. entschlüsseln).

## Verzeichnisdienst

Ein Dienst des Zertifizierungsdienstanbieters, durch den ein elektronisch jederzeit allgemein zugängliches Verzeichnis mit Zertifikaten, Attributzertifikaten und anderen relevanten Daten (z.B. Widerruflisten) zur Verfügung gestellt wird.

## Widerrufsdienst

Ein Dienst des Zertifizierungsdienstanbieters, durch den ein Zertifikat widerrufen werden kann (z.B. wenn der Signaturschlüssel kompromittiert wird).

## XML

Extensible Markup Language, eine genormte Meta-Markup Sprache, mit der die Syntax anderer Markup-Sprachen definiert werden kann.

## XMLDSIG

Ein auf XML basierendes Format für digital signierte Daten.

### **Zeitstempel**

Elektronisch signierte Bescheinigung eines Zertifizierungsdiensteanbieters, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen sind.

### **Zertifikat**

Eine elektronische Bescheinigung, mit der ein öffentlicher Signaturschlüssel einer bestimmten Person zugeordnet wird und deren Identität bestätigt wird.

### **Zertifizierungsdienst**

Die Bereitstellung von Signaturprodukten und -verfahren, die Ausstellung, Erneuerung und Verwaltung von Zertifikaten, Verzeichnis-, Widerrufs-, Registrierungs- und Zeitstempeldienste sowie Rechner- und Beratungsdienste im Zusammenhang mit elektronischen Signaturen.

### **ZMR**

Zentrales Melderegister. Zentrale Datenbank, mit der Möglichkeit der österreichweiten Gesamtsicht über alle Meldungen einer Person. Das ZMR ist eine Evidenz in der alle gemeldeten Menschen einmal erfasst sind.

### **ZMR-Zahl**

Melderegisternummer, die dem Gesamtdatensatz einer Person beigegeben wird, ohne Informationen über den Betroffenen zu enthalten.

## 7 Referenzen

### [Hous99]

Hously, R.: RFC 2630: Cryptographic Message Syntax (CMS). IETF Request For Comment, Juni 1999. Abgerufen aus dem World Wide Web am 15. Mai 2002 unter <http://www.ietf.org/rfc/rfc2630.txt>

### [EaRS02]

Donald Eastlake, Joseph Reagle und David Solo: XML-Signature Syntax and Processing. W3C Recommendation, Februar 2002. Abgerufen aus dem World Wide Web am 15. Mai 2002 unter <http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/>

### [Karl02a]

Karlinger, Gregor: Anforderungen an die Bürgerkarten-Umgebung nach dem Konzept Bürgerkarte. Konvention zum e-Government Austria erarbeitet vom CIO des Bundes, Operative Unit. Öffentlicher Entwurf, Version 1.0.0, 12. April 2002. Abgerufen aus dem World Wide Web am 15. Mai 2002 unter <http://www.buergerkarte.at/konzept/spezifikation/20020412/>

### [Karl02b]

Karlinger, Gregor: Protokoll für Abfragen der Behörde als RS beim ZDA. Konvention zum e-Government Austria erarbeitet vom CIO des Bundes, Operative Unit. Interner Entwurf, 30. Jänner 2002.

### [HoKa02]

Hollosi, Arno und Karlinger, Gregor: Security-Layer für das Konzept Bürgerkarte. Konvention zum e-Government Austria erarbeitet vom CIO des Bundes, Operative Unit. Öffentlicher Entwurf, Version 1.0.0, 25. Februar 2002. Abgerufen aus dem World Wide Web am 15. Mai 2002 unter <http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20020225/>

### [Algo01]

EESSI Algorithm Group: Algorithms and Parameters for Secure Electronic Signatures, v2.1 Oktober 2001.

[http://www.ict.etsi.org/eessi/Documents/20011019\\_Algorithm\\_Proposal\\_V2.11.doc](http://www.ict.etsi.org/eessi/Documents/20011019_Algorithm_Proposal_V2.11.doc)

### [ITUT97]

Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). ITU-T Rec. X.690 (1997).

[http://www.itu.int/ITU-T/studygroups/com17/languages/X.690\\_1297.pdf](http://www.itu.int/ITU-T/studygroups/com17/languages/X.690_1297.pdf)

### [Menz02]

Menzel, Thomas: Rechtsrahmen des E-Government. In: Juristische Ausbildung und Praxis (JAP) Heft 4, Manz, 2001/2002, S. 251.

### [Oswa01]

Oswald, Elisabeth: Einsatz und Bedeutung Elliptischer Kurven für die elektronische Signatur, Studie, Juni 2001

### [SigG00]

Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), BGBl. I Nr. 190/1999 idF: BGBl. I Nr. 152/2001.

**[SigV00]**

Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung - SigV),  
BGBl. II Nr. 30/2000.