

# ZKA-Signaturanwendung der deutschen Kreditwirtschaft

## Grundlagen - Anwendungen – Mehrwertdienste <sup>1</sup>

Dr. Detlef Hillen,  
SRC Security Research & Consulting GmbH, Bonn

### 1 Einleitung

Durch eine Richtlinie des Europäischen Parlaments wurden Rahmenbedingungen für die Einführung der elektronischen Signatur geschaffen. Diese wurden durch entsprechende Gesetze in das nationale Recht der einzelnen EU-Staaten übernommen (siehe [9] für das entsprechende deutsche Signaturgesetz).

Es stellt sich nun die Frage, wie die notwendige Infrastruktur für eine praktische Umsetzung der Nutzung der elektronischen Signatur geschaffen werden kann. In den letzten Jahren konzentrierten sich die Aktivitäten dabei im Wesentlichen auf die Realisierung von Trustcentern und übergeordneten (PKI-) Infrastrukturmaßnahmen. Die breite Ausstattung der potentiellen Benutzer mit Signaturkarten und geeigneten Kundenumgebungen und insbesondere auch die Integration der elektronischen Signatur in vorhandene bzw. neue Anwendungen wurde dabei nicht in gleichem Maße vorangetrieben. Die Angebote der Trustcenter bezüglich der Signaturkarten werden durch die Kunden aufgrund der hohen Preise und der fehlenden Einsatzmöglichkeiten nicht genutzt. Zusätzlich ist in Deutschland aufgrund der angespannten Situation bei den öffentlichen Haushalten nicht damit zu rechnen, dass öffentliche Stellen (z.B. Kommunen) Signaturkarten in großer Stückzahl ausgeben werden.

Deutsche Kreditinstitute geben bereits seit Jahren Kundenkarten als Chipkarten an ihre Kunden aus. Diese enthalten heute im Wesentlichen Zahlungsfunktionen. Für die Zukunft ist geplant, dass diese Kundenkarten auch eine Signaturfunktion enthalten können. Der ZKA<sup>2</sup> hat daher in [3] eine Signaturanwendung für die Chipkarten

---

<sup>1</sup> Siehe auch: Sicherheit in Informationssystemen, Proceedings der Fachtagung SIS 2002, Wien 3./4.10.2002, E. Erasim und Prof. Dr. D. Karagiannis (Hrsg.), vdf

<sup>2</sup> ZKA = Zentraler Kreditausschuss. In dem ZKA arbeiten die Spitzenverbände der deutschen Kreditwirtschaft (BdB, BVR, DSGV, VöB) zusammen.

der deutschen Kreditwirtschaft spezifiziert. Diese ermöglicht es den Kreditinstituten, in Zukunft Kundenkarten an ihre Kunden auszugeben, mit denen diese elektronische Unterschriften erzeugen können, und bei denen die gesetzlichen Anforderungen aus SigG [9] und SigV [10] erfüllt werden. Die Kundenkarten können dabei als reine Signaturkarten ausgestattet sein oder aber auch als multifunktionale Karten mit Signatur- und Zahlungsfunktionen (GeldKarte, EMV-Anwendungen).

Damit die ZKA-Signaturkarte ein Erfolg wird, müssen mindestens die folgenden Punkte erfüllt werden:

- Die Karte muss durch die Kunden (der Kreditinstitute) akzeptiert werden. Dazu ist es notwendig, dass ein breites Spektrum von Anwendungen auf verschiedenen Einsatzgebieten geschaffen wird.
- Für den Kartenherausgeber (Kreditinstitut) muss sich ein Mehrwert durch die Ausgabe der Karte ergeben. Dabei sind mögliche interne Rationalisierungseffekte, neue kostenpflichtige kreditwirtschaftliche Anwendungen, und neue Services, die den die Signaturkarte akzeptierenden Dienstleister angeboten werden können, zu betrachten.
- Dienstleister aus den Gebieten eGovernment, eBanking und eCommerce, die eine elektronische Signatur in ihren Anwendungen integrieren bzw. akzeptieren möchten, benötigen eine möglichst umfassende Ausstattung ihrer Kunden mit Signaturkarten.

Der ZKA hat daher nicht nur eine Signaturanwendung für die Chipkarten der Kreditwirtschaft spezifiziert, sondern auch Grundlagen für die Integration der Signaturkarte in Kundenumgebungen und Anwendungen erarbeitet. Zusätzlich wurden Mehrwertdienste spezifiziert, die aufbauend auf die ausgegebenen ZKA-Signaturkarten neue Services ermöglichen, die die kartenherausgebenden Institute Dienstleistern anbieten können, die eine elektronische Signatur in ihren Anwendungen akzeptieren. Insbesondere diese Mehrwertdienste bieten eine Möglichkeit, das Angebot eines Kreditinstitutes bei der Ausgabe einer ZKA-Signaturkarte deutlich gegenüber den Angeboten anderer Kartenherausgeber (Trustcenter) abzugrenzen und hervorzuheben.

In dem vorliegenden Dokument wird ein Überblick über die verschiedenen Aspekte der ZKA-Signaturanwendung, ihrer Einsatzmöglichkeiten und der Mehrwertdienste gegeben. Es werden dabei weniger die technischen Details behandelt als vielmehr die

Punkte beleuchtet, die für den praktischen Nutzen der ZKA-Signaturkarten von Bedeutung sind. Fragen der Kartenherstellung und der Trustcenterdienste werden nicht betrachtet.

## **2 Infrastruktur des Kunden**

Der ZKA hat durch seine Spezifikationen die Grundlagen für die notwendige Infrastruktur geschaffen, die ein Kunde benötigt, um eine elektronische Signatur nutzen zu können. Neben der eigentlichen ZKA-Signaturkarte wurden dabei auch Grundlagen für die Integration der ZKA-Signaturkarte in eine Kundenumgebung spezifiziert. In diesem Kapitel wird ein Überblick über die Ergebnisse zu diesen beiden Punkten gegeben.

### **2.1 Signaturkarte des ZKA**

Der ZKA hat in [3] eine Signaturanwendung für die Chipkarten der deutschen Kreditwirtschaft spezifiziert. Ziel dieser Spezifikation ist es, dass sich in Zukunft eine Signaturkarte an der Karte/Terminal-Schnittstelle einheitlich verhält, unabhängig davon, welches deutsche Kreditinstitut die Signaturkarte ausgegeben hat.

Die Spezifikation des ZKA hält sich eng an die Vorgaben der entsprechenden DIN-Dokumente [7,8]. Grundlage ist das neue Betriebssystem SECCOS [2], das ebenfalls durch den ZKA spezifiziert wurde. SECCOS wird das Standardbetriebssystem für Chipkarten der deutschen Kreditwirtschaft. Es ist unabhängig von dem konkreten Kartenhersteller. Verschiedene Hersteller wie G&D und GemPlus haben das Betriebssystem SECCOS realisiert.

Chipkarten mit dem Betriebssystem SECCOS und der Signaturanwendung des ZKA werden auch als ZKA-Signaturkarten bezeichnet. Im Folgenden werden weniger die technischen Details einer ZKA-Signaturkarte beschrieben. Es werden vielmehr die Punkte betrachtet, die für die Integration einer ZKA-Signaturkarte in zukünftige Sicherheitsanwendungen bzw. -infrastrukturen und für die Nutzung einer solchen Karte durch den Karteninhaber von Bedeutung sind.

#### *2.1.1 Sicherheitsdienste einer ZKA-Signaturkarte*

Eine ZKA-Signaturkarte bietet die folgenden drei verschiedenen Sicherheitsdienste an, die im Rahmen von Anwendungen genutzt werden können:

- Erzeugen einer (gesetzeskonformen) elektronischen Signatur.
- Unterstützung einer Client/Server-Authentikation.
- Entschlüsseln eines Kryptogramms.

Zusätzlich unterstützt eine ZKA-Signaturkarte eine Komponenten-authentikation zwischen Terminal und Chipkarte und eine Benutzerauthentikation.

Alle Sicherheitsdienste basieren auf dem Algorithmus RSA, wobei nach der Spezifikation Schlüssel eine Länge zwischen 1024 und 2048 Bit haben können<sup>3</sup>. Sie unterscheiden sich jedoch bezüglich des eingesetzten Schlüssels und der verwendeten Verfahren.

Bei dem Erzeugen einer (gesetzeskonformen) elektronischen Signatur setzt die Chipkarte einen Schlüssel ein, der grundsätzlich für keine weitere Funktion durch die Chipkarte verwendet werden kann. Als Signaturverfahren unterstützt eine ZKA-Signaturkarte

- PKCS#1 mit dem Hashalgorithmus SHA-1 und
- DIN-Signaturverfahren mit dem Hashalgorithmus RIPEMD-160.

Der Hashwert kann dabei innerhalb oder außerhalb der Chipkarte berechnet werden. Die Chipkarte kontrolliert aber die Einhaltung der Signaturverfahren (Länge des Hashwertes, Aufbau des Digest-Info und PKCS#1-Padding bzw. Padding mit einer durch die Chipkarte erzeugten Zufallszahl).

Eine ZKA-Signaturkarte erzeugt nur dann eine (gesetzeskonforme) elektronische Signatur, falls sich der Benutzer vorher durch das Verifizieren einer Signatur-PIN authentisiert hat. Diese Signatur-PIN ist immer numerisch und mindestens 6 Ziffern lang. Sie kann durch den Benutzer geändert werden. Durch die Personalisierung der Signaturkarte wird festgelegt, wie viele Signaturen nach dem einmaligen Verifizieren der Signatur-PIN erzeugt werden können. Zur Zeit soll dieser Wert bei ZKA-Signaturkarten standardmäßig auf eins gesetzt werden.

Die Unterstützung der Client/Server-Authentikation besteht ebenfalls aus dem Signieren von Daten durch die Chipkarte. Dabei werden jedoch keine besonderen Vorgaben bezüglich des Aufbaus der Daten bzw. bezüglich des Signaturverfahrens eingehalten. Durch die Chipkarte wird intern nur ein Padding der Eingabe gemäß PKCS#1

---

<sup>3</sup> Bezüglich der Schlüssellängen kann es zu Einschränkungen aufgrund der eingesetzten Hardware kommen.

durchgeführt.

Bei dem Entschlüsseln eines Kryptogramms überprüft die Chipkarte intern, ob bei der Verschlüsselung der Klartextdaten ein Padding gemäß PKCS#1 durchgeführt wurde. Nur in diesem Falle werden die Klartextdaten durch die Chipkarte ausgegeben.

Eine ZKA-Signaturkarte führt nur dann die beiden letzten Sicherheitsdienste aus, falls sich der Benutzer vorher durch das Verifizieren eines (Client/Server-) Passwortes authentisiert hat. Dieses Passwort ist alphanumerisch. Es muss nur einmal pro Aktivierung der Signaturkarte verifiziert werden. Der Benutzer kann das Passwort ebenfalls ändern.

Abhängig von der Personalisierung einer ZKA-Signaturkarte werden für die Unterstützung der Client/Server-Authentikation und das Entschlüsseln eines Kryptogramms zwei unterschiedliche Schlüssel oder ein gemeinsamer Schlüssel durch die Chipkarte eingesetzt. Da bei den beiden Sicherheitsdiensten durch die Chipkarte intern unterschiedliche Paddings gemäß PKCS#1 eingesetzt bzw. überprüft werden, führt auch der Einsatz eines gemeinsamen Schlüssels für die beiden Sicherheitsdienste zu keinen Sicherheitsproblemen. In jedem Falle ist jedoch der Schlüssel dieser Sicherheitsdienste getrennt von dem Schlüssel für das Erzeugen einer (gesetzeskonformen) elektronischen Signatur.

### 2.1.2 Gesetzeskonformität

ZKA-Signaturkarten erfüllen die Anforderungen, die SigG [9] und SigV [10] an "sichere Signaturerstellungseinheiten" stellen. Die dazu notwendigen Evaluierungen sind jedoch noch durchzuführen. Voraussetzung für die Erfüllung der gesetzlichen Anforderungen ist zusätzlich, dass bei der Personalisierung einer konkreten Signaturkarte die aktuellen Vorgaben bezüglich der Schlüssellängen berücksichtigt werden.

Es stellt sich dann die Frage, welche "Qualität" die mit einer ZKA-Signaturkarte erzeugten (gesetzeskonformen) elektronischen Signaturen haben. Diese hängt jedoch nicht von der Signaturkarte selber ab, sondern vielmehr von der "Qualität" der Zertifikate, die zu dem Schlüssel in einer ZKA-Signaturkarte gespeichert werden.

Kommen bei einer ZKA-Signaturkarte qualifizierte Zertifikate zum Einsatz, so erzeugt diese qualifizierte elektronische Signaturen. Handelt es sich nicht um qualifizierte Zertifikate sondern "nur" um fortgeschrittene, so erzeugt die ZKA-Signaturkarte entsprechend fortgeschrittene elektronische Signaturen.

Ein Kreditinstitut muss im Rahmen seiner Produktgestaltung entscheiden, ob es fortgeschrittene oder qualifizierte Zertifikate in die von ihm auszugebenen Signaturkarten einbringt. Es wird hierfür keine einheitlichen Regelungen des ZKA geben.

## **2.2 Privates Terminal des Kunden**

Der ZKA hat nicht nur die Signaturanwendung für die ZKA-Signaturkarten spezifiziert, sondern zusätzlich auch noch Grundlagen für die Nutzung der Karten in Kundenumgebungen erarbeitet. Ziel ist dabei nicht, ein vollständiges Signaturterminal (in SigG [9] auch "Signaturanwendungskomponente" genannt) zu spezifizieren. Es soll vielmehr eine Basis geschaffen werden, auf der entsprechende Anwendungen aufbauen können, und die dabei die Kompatibilität und die Zuverlässigkeit dieser Anwendungen bezüglich der Nutzung der ZKA-Signaturkarte erhöht. Im Folgenden soll die entstandene Architektur für Kundenumgebungen kurz beschrieben werden.

Grundlage für die Kundenumgebung ist ein PC, der über einen Chipkartenleser verfügt. Problem dabei ist jedoch, dass aufgrund von Sicherheitslücken bei einem PC mit einem Standardbetriebssystem Angriffe auf die Prozesse und Daten bei dem Erzeugen einer elektronischen Signatur denkbar sind. Dadurch ist es zum Beispiel möglich, dass ein Angreifer die Signatur-PIN des Benutzers ausforscht oder dass ohne Zustimmung des Benutzers eine elektronische Signatur mit der Signaturkarte erzeugt wird.

Um die Sicherheit insbesondere der Signatur-PIN und der Zustimmung des Benutzers zu dem Erzeugen einer elektronischen Signatur zu erhöhen, hat der ZKA ein Kundenterminal als Grundlage für die Kundenumgebung spezifiziert [4,5]. Ein Kundenterminal ist dabei im wesentlichen ein Klasse-3 Chipkartenleser, d.h. mit eigener Tastatur und Display, in dem einige besonders sicherheitsrelevante Abläufe (z.B. das Verifizieren der Signatur-PIN) implementiert sind. Kundenterminals sollen so konstruiert sein, dass (physische) Angriffe auf das Gerät durch den Benutzer erkannt werden (tamper evident). Die Software in dem Kundenterminal darf nur über kryptographisch abgesicherte Prozesse durch den Hersteller änderbar sein.

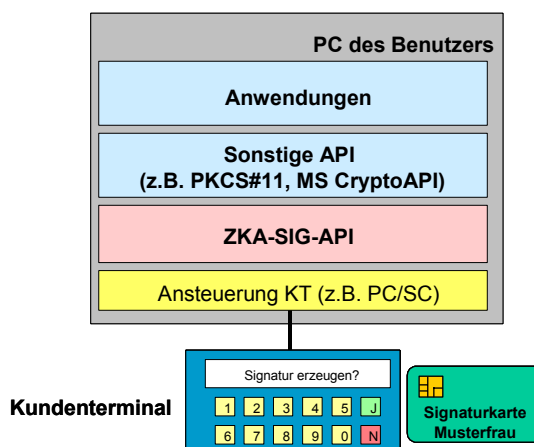
Die notwendige Hardware für entsprechende Kundenterminals ist heute bereits von verschiedenen Herstellern (z.B. G&D, Kobil, Reiner SCT) erhältlich. Die verfügbaren Kundenterminals sind aber (insbesondere in Bezug auf ihr Display) noch nicht leistungsfähig genug, um zum Beispiel eine Visualisierungskomponente für die Darstellung der zu signierenden Daten in einem Kundenterminal zu

realisieren. Die Abläufe, die im Rahmen der ZKA-Vorgaben innerhalb eines Kundenterminals realisiert werden sollen, beschränken sich daher auf die Folgenden:

- Information und explizite Bestätigung des Benutzers bei dem Erzeugen einer (gesetzeskonformen) elektronischen Signatur.
- Information und explizite Bestätigung des Benutzers bei dem Ändern von Kartendaten (z.B. Laden eines Zertifikats).
- Benutzerführung und Eingabe bei der Benutzerauthentikation mittels Signatur-PIN.
- Benutzerführung und Eingabe bei der Änderung der Signatur-PIN.
- Benutzerführung und Eingabe bei dem Rücksetzen des Fehlbedienungs Zählers mittels PUK.

Diese genannten Abläufe werden vollständig innerhalb eines Kundenterminals realisiert. Durch die Software des PC werden diese Abläufe nur "angestoßen". Die Information des Benutzers geschieht über das Display des Kundenterminals. Die genannten Eingaben bei der Bestätigung eines Vorgangs bzw. die Eingabe der Signatur-PIN geschieht über die Tastatur des Kundenterminals. Durch diese Architektur wird zum Beispiel verhindert, dass die Signatur-PIN durch Angriffe innerhalb des PC (z.B. Trojanische Pferde) ausgeforscht werden kann.

Die folgende Abbildung zeigt die Architektur im Überblick:



**Abbildung 1: Architektur der Kundenumgebung**

Die Spezifikation des ZKA umfasst dabei die Abläufe, die innerhalb eines Kundenterminals für einen Zugriff auf die ZKA-Signaturkarte realisiert werden müssen, und die ZKA-SIG-API. Diese dient dazu, Anwendungen die Funktionalität einer ZKA-Signaturkarte zur Verfügung zu stellen. Die ZKA-SIG-API soll dabei zum Lieferumfang des Kundenterminals gehören. Die Spezifikation ist offen zugänglich, so dass verschiedene Hersteller entsprechende Produkte anbieten können. Die ZKA-SIG-API stellt dabei sicher, dass Anwendungen unabhängig von dem konkreten Kundenterminal auf die ZKA-Signaturkarte zugreifen können.

Die ZKA-SIG-API soll dabei keine neue API für kryptographische Funktionen sein. Ihre Aufgabe ist nur die Abstraktion der Funktionalität einer ZKA-Signaturkarte. Sie bietet daher auch keine Funktionen für das Ver-/Entschlüsseln mit symmetrischen Verfahren und auch keine Funktionen für das Verifizieren von elektronischen Signaturen, da bei diesen Funktionen die Signatur-Anwendung einer ZKA-Chipkarte nicht (sinnvoll) eingesetzt werden kann. Die Spezifikation der ZKA-SIG-API hat ihre wesentliche Begründung in den folgenden Punkten:

- Die ZKA-SIG-API bietet eine klare Trennung zwischen den Aufgaben der Entwickler der Kundenterminals und den Aufgaben der Entwickler, die die ZKA-Signaturkarte in ihren Anwendungen integrieren möchten.
- Anwendungsentwickler, die auf die ZKA-SIG-API aufbauen, müssen keine Kenntnisse über technische Details der Realisierung der Signaturanwendung in einer ZKA-Chipkarte haben.
- Anwendungsentwickler benötigen keine speziellen Detail-Kenntnisse über die Spezifikationen des ZKA-Betriebssystems SECCOS bzw. der ZKA-Signaturanwendung.
- Die ZKA-SIG-API biete eine Grundlage für Schnittstellentests für Kundenterminals.

Die ZKA-SIG-API soll keine Alternative zu "Standard-Schnittstellen" für kryptographische Funktionen wie z.B. PKCS#11 und CryptoAPI sein. Die Entwicklung entsprechender Software für die Realisierung dieser Schnittstellen basierend auf einer ZKA-Signaturkarte wird jedoch durch die ZKA-SIG-API vereinfacht.

Durch die Arbeiten des ZKA wurde eine umfangreiche Grundlage geschaffen, auf der Anwendungen für eine Nutzung der ZKA-Signaturkarte entwickelt werden können, ohne dass dabei der Anwendungsentwickler die technischen Details der Realisierung der Signaturanwendung [3] und des Betriebssystems SECCOS [2] kennen muss. Die Spezifikation bzw. Realisierung entsprechender Anwendungen ist jedoch nicht Aufgabe des ZKA.

### **3 Anwendungen**

Um den Einsatz der elektronischen Signatur in weitem Umfang zu ermöglichen und voranzutreiben ist es nicht nur notwendig, die benötigte Infrastruktur (Signaturkarten, Kundenumgebungen, Trustcenter) zu schaffen. Es müssen vielmehr insbesondere auch Anwendungen geschaffen werden, in deren Rahmen eine Signaturkarte durch einen Benutzer eingesetzt werden kann. Um die Attraktivität der ZKA-Signaturkarte bei den Kunden der Kreditinstitute zu erhöhen ist es dabei notwendig, ein breites Spektrum an Anwendungen aus verschiedenen Einsatzbereichen zu realisieren.

#### **3.1 Unterstützung von Standard-Internet-Programmen**

Unter Standard-Internet-Programme werden in diesem Dokument die Browser und E-Mail-Programme von Netscape (Navigator und Communicator) bzw. Microsoft (Explorer und Outlook) verstanden. Durch die Bezeichnung „Standard-Internet-Programm“ sollen diese Programme nicht gegenüber anderen ausgezeichnet werden, es ist aber eine Tatsache, dass die überwiegende Mehrheit der PC-Nutzer der Kunden der Kreditwirtschaft mit diesen Programmen arbeitet.

Die genannten Programme bieten Sicherheitsfunktionen an, mit denen z.B. eine E-Mail elektronisch unterschrieben werden kann bzw. der Zugriff auf einen Internet-Server über das SSL-Protokoll mit Client-Authentikation geschützt werden kann. Im Allgemeinen sind diese Sicherheitsfunktionen heute jedoch nur durch Software realisiert, d.h. insbesondere werden auch die privaten Schlüssel des Benutzers in der Software des PC gespeichert und eingesetzt. Dieses Vorgehen hat nicht nur die bekannten Sicherheitsprobleme, es führt auch dazu, dass ein Benutzer an verschiedenen PCs unterschiedliche Schlüssel/Zertifikate für das Unterschreiben seiner E-Mails bzw. seiner Authentikation gegenüber Internet-Servern einsetzen muss oder einen umständlichen Import/Export seiner Schlüssel/Zertifikate durchführen muss. Durch den Einsatz einer Chipkarte werden diese Probleme behoben, da die privaten Schlüssel

des Benutzers sicher in der Chipkarte gespeichert bzw. eingesetzt werden und der Benutzer die gleiche Chipkarte bei seiner Arbeit an verschiedenen Rechnern einsetzen kann.

Für die Ausführung der Sicherheitsfunktionen nutzen die genannten Standard-Internet-Programme sogenannte kryptographische Token, die über Schnittstellen wie PKCS#11 (bei Netscape-Produkten) bzw. CryptoAPI (bei Microsoft-Produkten) angesprochen werden. Die Token sind dabei heute wie bereits erwähnt im Allgemeinen nur in Software realisiert.

Bei der Spezifikation und Realisierung der ZKA-Signaturanwendung war ein Ziel, dass der Karteninhaber seine ZKA-Signaturkarte auch für die Sicherheit im Rahmen der Standard-Internet-Anwendungen einsetzen kann. Hierzu ist es notwendig, Token für die oben genannten Schnittstellen PKCS#11 und CryptoAPI zu erstellen, die bezüglich der Speicherung der privaten Schlüssel und der Ausführung der eigentlichen kryptographischen Berechnungen die ZKA-Signaturkarte nutzen. Die Realisierung dieser Token soll dabei auf die im letzten Kapitel beschriebene ZKA-SIG-API aufbauen (siehe auch Abbildung 1).

Erste Prototypen wurden für die benötigten Token entwickelt und ihr praktischer Einsatz auf der letzten CeBIT2002 demonstriert. Der Benutzer kann aufgrund der Token seine ZKA-Signaturkarte einsetzen, um z.B. eine E-Mail zu signieren oder sich beim Aufbau einer SSL-Verbindung authentisieren. Die Bedienung und Abläufe bei den entsprechenden Programmen von Netscape bzw. Microsoft ändern sich durch den Einsatz der ZKA-Signaturkarte nicht.

### **3.2 Beispiel aus der Kreditwirtschaft: eScheck**

Im letzten Abschnitt wurde gezeigt, wie die ZKA-Signaturkarte in bereits bestehende Anwendungen integriert werden kann, um die Sicherheitsfunktionen dieser Anwendungen zu unterstützen. Es müssen jedoch weitere Anwendungen entwickelt werden, um die Attraktivität der ZKA-Signaturkarte für den Kunden zu steigern. Aus der Sicht der Kreditinstitute bieten sich hier insbesondere kreditwirtschaftliche Anwendungen im Umfeld des elektronischen Zahlungsverkehrs an, da hierbei einerseits eine klare Abgrenzung gegenüber den Möglichkeiten sonstiger Herausgeber von Signaturkarten besteht und andererseits die Nutzung der Anwendungen auch bepreist werden kann.

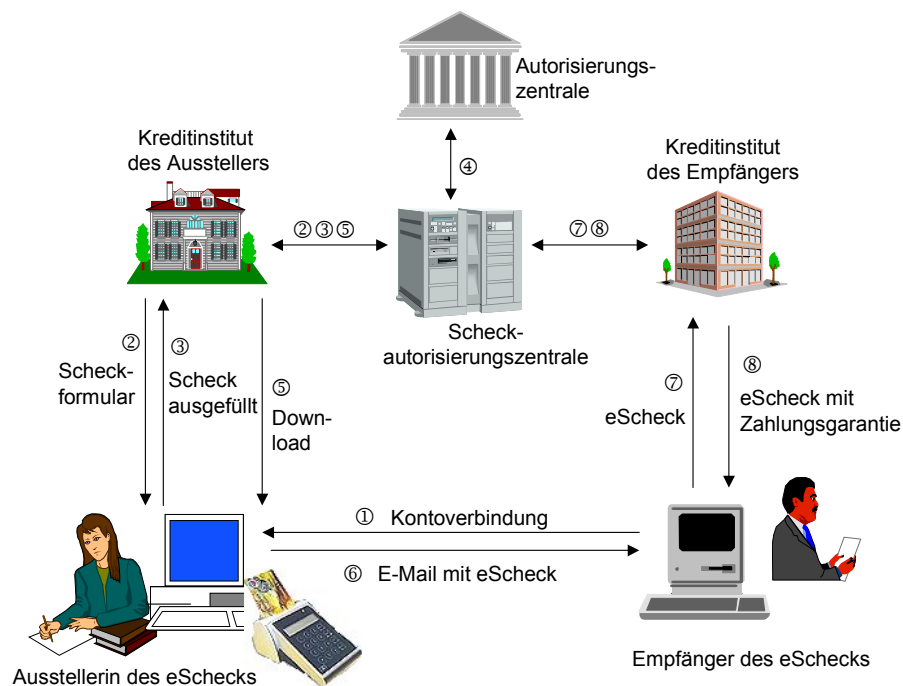
Als ein Beispiel einer möglichen kreditwirtschaftlichen Anwendung soll im Folgenden kurz das Prinzip des elektronischen Schecks (kurz

eScheck) [12] erläutert werden. Der eScheck wurde vom Bank-Verlag entwickelt. Der Einsatz der eSchecks wurde an einem Prototyp dieser Anwendung auf der CeBIT2002 demonstriert.

Der eScheck ist ein Zahlungsmittel im Internet mit Zahlungsgarantie. Er kann für Zahlungen von "Privat an Händler" eingesetzt werden, aber auch für Zahlungen von "Privat an Privat". Gerade die Möglichkeit von Zahlungen zwischen Privatpersonen unterscheidet den eScheck dabei von anderen bekannten Zahlungsmitteln, die heute im Internet eingesetzt werden können.

Die benötigte Infrastruktur auf Seiten des Ausstellers und des Empfängers eines eSchecks beschränkt sich auf einen Rechner mit Internetzugang. Nur der Aussteller eines eSchecks benötigt eine ZKA-Signaturkarte, mit der er seine eSchecks (elektronisch) unterschreibt. Zur Zeit sind nur eSchecks möglich, die (im Sinne eines Verrechnungsschecks) auf ein im eScheck anzugebendes Konto eingezahlt werden können. Der Aussteller eines eSchecks benötigt daher die Daten der Kontoverbindung des Empfängers.

Folgende Abbildung gibt einen Überblick über den Informationsfluss:



**Abbildung 2: Ausstellen eines eSchecks mit Zahlungsgarantie**

Die (technische) Abwicklung für das Ausstellen eines eSchecks und für die Überprüfung der Zahlungsgarantie wird durch eine Scheckautorisierungszentrale (SAZ) durchgeführt. Für die Autorisierung eines eScheck (Aussprechen der Zahlungsgarantie) greift diese auf die bereits vorhandene Autorisierungszentrale der Kreditwirtschaft zurück. Eingereicht wird ein eScheck über eine Scheckeinreichungszentrale (SEZ, in der Abbildung nicht dargestellt). Aussteller und Empfänger eines eSchecks greifen im Allgemeinen über Verbindungen zu ihren Kreditinstituten auf die Dienstleistungen von SAZ und SEZ zu, beide sind aber auch direkt über das Internet erreichbar.

Will ein Kunde einen eScheck ausstellen, wendet er sich (über sein Kreditinstitut) an die SAZ. Für die Verbindung zur SAZ wird eine SSL-Verbindung mit Client-Authentikation aufgebaut. Von der SAZ erhält der Aussteller ein eScheck-Formular ②, in dem bereits sein Name und seine Kontoverbindung (verschlüsselt) sowie eine Nummer des eSchecks enthalten sind. Der Aussteller füllt das Formular mit den Daten des Empfängers, dem Betrag und dem Verwendungszweck aus. Er signiert das Formular dann mit seiner ZKA-Signaturkarte, wobei eine (gesetzeskonforme) elektronische Unterschrift erzeugt wird. Ausgefülltes Formular und Signatur werden wieder an die SAZ gesendet ③, die die Daten des Ausstellers (soweit möglich) überprüft. Über eine Anfrage an die Autorisierungszentrale ④ wird der Möglichkeit zur Zahlung überprüft. Die SAZ unterschreibt den eScheck, wodurch eine Zahlungsgarantie bestätigt wird.

Der Aussteller erhält den eScheck von der SAZ zurück ⑤. Der eScheck wird dabei als XML-Datei an den Aussteller übermittelt, die durch geeignete Browser angezeigt werden kann. Diese Datei kann der Aussteller z.B. als Anhang für eine E-Mail an den Empfänger übermitteln ⑥.

Empfängt eine Person einen eScheck (XML-Datei) von einem Aussteller, so kann er diesen zur Überprüfung an die SAZ geben ⑦. Die SAZ überprüft die elektronischen Unterschriften des eScheck. Eine erneute Rückfrage bei der Autorisierungszentrale ist nicht notwendig. Durch eine weitere (elektronische) Unterschrift der SAZ bestätigt sie die Korrektheit des eSchecks und damit insbesondere auch die Zahlungsgarantie. Das Ergebnis (eScheck mit erneuter Unterschrift der SAZ) wird wieder als XML-Datei an den Empfänger übermittelt ⑧.

Der Empfänger kann den eScheck zu einem späteren Zeitpunkt (über sein Kreditinstitut) bei der SEZ einreichen. Ein eScheck (und damit auch die Zahlungsgarantie) hat eine festgelegte Gültigkeitsdauer. Der

Empfänger kann daher den eScheck auch einfach verfallen lassen, was zum Beispiel dann sinnvoll sein kann, falls der eScheck als Kautions für die Miete eines Objekts ausgestellt wurde.

Der eScheck kann auch als internationales Zahlungsmittel eingesetzt werden. Dafür werden nationale SAZ und SEZ benötigt. Bei einer internationalen Zahlung mittels eScheck müssen dann die SAZ, die einen ausgestellten eScheck autorisiert, und die SAZ, bei der der Empfänger einen eScheck überprüfen lässt, nicht mehr identisch sein.

Im Rahmen der Anwendung eScheck sind weitere Funktionalitäten realisiert. So kann ein Aussteller einen eScheck sperren lassen und ein Empfänger kann einen eScheck "elektronisch zerreißen". Die Abläufe bei der Ausstellung eines eSchecks von "Privat an Händler" sind ähnlich wie der beschriebene Fall. Hierauf soll jedoch nicht weiter eingegangen werden.

Durch den eScheck wurde ein elektronisches Zahlungsmittel geschaffen, das sowohl für den Aussteller als auch für den Empfänger einfach zu handhaben ist. Außer der ZKA-Signaturkarte des Ausstellers sind keine besonderen technischen Hilfsmittel notwendig. Insbesondere muss sich der Empfänger nicht für die Nutzung des Systems vorher registrieren lassen.

### **3.3 Ausblick, weitere Anwendungsgebiete**

Neben den in den letzten Abschnitten genannten Beispielen werden in unterschiedlichsten Einsatzgebieten Anwendungen entwickelt, bei denen eine ZKA-Signaturkarte für die Sicherheit der Anwendungen zum Einsatz kommen wird.

Es ist in Deutschland erklärtes Ziel der Regierung, die Dienstleistungen der Behörden in Zukunft über das Internet den Bürgern anzubieten (eGovernment). Die dabei entstehenden Anwendungen benötigen eine elektronische Signatur gemäß SigG. Eigene Signaturkarten sollen durch staatliche Stellen hierfür jedoch nicht ausgegeben werden. Gerade in diesem Umfeld wird stark auf eine Unterstützung durch die Kreditwirtschaft bei der Ausstattung großer Teile der Bevölkerung mit Signaturkarten und auch der benötigten Infrastruktur für die Kundenumgebungen gesetzt. Die technischen Ergebnisse der entsprechenden Arbeiten im ZKA müssen daher bei der Entwicklung der Anwendungen für den Bereich eGovernment berücksichtigt werden.

In der deutschen Kreditwirtschaft wurde für Anwendungen im Bereich

Homebanking der einheitliche Standard HBCI für die Kommunikation Kundenumgebung/Bankserver und für die entsprechenden Geschäftsvorfälle erarbeitet. HBCI unterstützt heute verschiedene Sicherheitsverfahren, wobei auf Seiten der Kunden verschiedene Sicherheitsmedien zum Einsatz kommen können. Mit der neuen Version 3.0 [11] sind auch die Sicherheitsdienste der ZKA-Signaturkarte als Sicherheitsverfahren und entsprechend die ZKA-Signaturkarte als Sicherheitsmedium des Kunden innerhalb von HBCI einsetzbar. Von Bedeutung ist dabei, dass diese ohne jede Erweiterung für HBCI einsetzbar ist. Hierin unterscheidet sich eine ZKA-Signaturkarte von heute im Rahmen von HBCI zum Einsatz kommenden Chipkarten.

Neben elektronischen Transaktionen, die im Rahmen von Homebanking über ein Netzwerk (Internet) ausgeführt werden, können auch Vorgänge durch den Einsatz der ZKA-Signaturkarte abgesichert werden, die der Karteninhaber direkt in einer Geschäftsstelle seines Kreditinstitutes durchführt. Heute werden z.B. bei der Änderung eines Dauerauftrages die neuen Daten am Schalter elektronisch aufgenommen und dann ausgedruckt und vom Kunden (handschriftlich) unterschrieben. Bei der institutsinternen Nachbereitung wird das unterschriebene Dokument später verfilmt und dann archiviert. Die bei der Bearbeitung eines solchen Vorgangs entstehenden Medienbrüche können verhindert werden, falls alle Dokumente elektronisch verarbeitet werden. Als Ersatz für die handschriftliche Unterschrift kann der Kunde das elektronische Dokument mit seiner ZKA-Signaturkarte elektronisch unterschreiben.

#### **4 Mehrwertdienste**

Basierend auf der Signaturanwendung des ZKA können Kreditinstitute in Zukunft Signaturkarten an ihre Kunden ausgeben. Dies kann als reine Signaturkarte oder auch als Multifunktionskarte mit Signaturanwendung und Zahlungsanwendungen (GeldKarte, EMV-Anwendungen, etc.) geschehen. Preislich liegt derzeit eine solche ZKA-Signaturkarte durch die hohen Anforderungen an die Hardware (Rechenleistung und Speicherbedarf) und die Sicherheit sowie den derzeit noch kleinen Stückzahlen noch weit über den Kosten für die heute weit verbreiteten Chipkarten der Kreditinstitute (GeldKarte). Zu den Kosten für die Chipkarte kommen zusätzlich noch die (ebenfalls nicht geringen) Kosten für die benötigten Zertifikate.

Die höheren Kosten für eine ZKA-Signaturkarte kann ein Kreditinstitut nicht ohne weiteres vollständig an seine Kunden weitergeben. Die

durch den Einsatz der ZKA-Signaturkarte bei der (elektronischen) Kommunikation zwischen dem Institut und seinem Kunden möglichen internen Rationalisierungseffekte werden ebenfalls nicht zu einem Ausgleich der Kosten für die Ausgabe der ZKA-Signaturkarte führen.

Wie bereits erwähnt erfüllen die ZKA-Signaturkarten die Anforderungen aus SigG und SigV an eine gesetzeskonforme elektronische Signatur. Der Karteninhaber kann daher seine ZKA-Signaturkarte auch im Rahmen von Anwendungen zum Erzeugen von elektronischen Signaturen einsetzen, die von anderen Dienstleistern (ohne Bezug zu seinem Kreditinstitut) angeboten werden. Solche Dienstleister können z.B. Behörden (e-Government), andere Kreditinstitute (e-Banking) oder Unternehmen (e-Commerce) sein, die Dienstleistungen oder Waren z.B. im Internet anbieten. Diese Dienstleister haben den Vorteil, dass einerseits die Sicherheit ihrer Anwendungen durch den Einsatz der elektronischen Signatur deutlich erhöht wird, und andererseits sie keine eigenen Signaturkarten an ihre potentiellen Kunden ausgeben müssen.

Zusammenfassend folgt, dass die höheren Kosten für die Ausgabe einer Signaturkarte durch den Kartenherausgeber (Kreditinstitut) zu tragen sind, während Dienstleister, die die elektronische Signatur in ihren Anwendungen integrieren, Einsparpotential ohne eigene Kosten für die Kartenausgabe erzielen. Es stellt sich daher die Frage, ob basierend auf den Signaturkarten neue sinnvolle Mehrwertdienste denkbar sind, die ein Kreditinstitut (als Kartenherausgeber) den Dienstleistern (als Akzeptanten der elektronischen Signatur) anbieten kann, und deren Nutzung für den Dienstleister kostenpflichtig ist.

Als eine Form von möglichen Mehrwertdiensten hat der ZKA die Grundlagen für eine elektronische Bankauskunft erarbeitet [1,6]. Dabei bietet ein Kreditinstitut (als Herausgeber einer ZKA-Signaturkarte) an, weitere Informationen zu einem Zertifikat auf Anfrage einem Dienstleister zur Verfügung zu stellen. Zur Zeit sind die folgenden Auskunftsdienste angedacht:

### **1. Identitätsdienst**

In einem Zertifikat sind Vorname und Name und evtl. sogar nur ein Pseudonym des Karteninhabers gespeichert. Dadurch wird der Karteninhaber nicht eindeutig identifiziert. Anfragen an den Identitätsdienst liefert weitere Daten wie Geburtsname, -datum und -ort. Zusätzlich können optional durch das Kreditinstitut auch Adressdaten ausgegeben werden.

## **2. Transaktionsbeschränkungen**

In einem Zertifikat können Angaben aufgenommen werden, dass der Einsatz der Signaturkarte nach Art und/oder Umfang beschränkt ist. Dieser Auskunftsdienst gibt Informationen zu den zu einem Zertifikat gehörenden genauen Beschränkungen.

## **3. Bonitätsauskunft**

Durch Anfragen an diesen Auskunftsdienst kann die Bonität des Karteninhabers überprüft werden.

## **4. Zahlungsgarantie**

Hierbei gibt das Kreditinstitut, das die Signaturkarte ausgegeben hat, dem Dienstleister eine Zahlungsgarantie (bzw. eine Ausfallversicherung) für den Fall, dass der beteiligte Kunde seinen Zahlungsverpflichtungen nicht nachkommt.

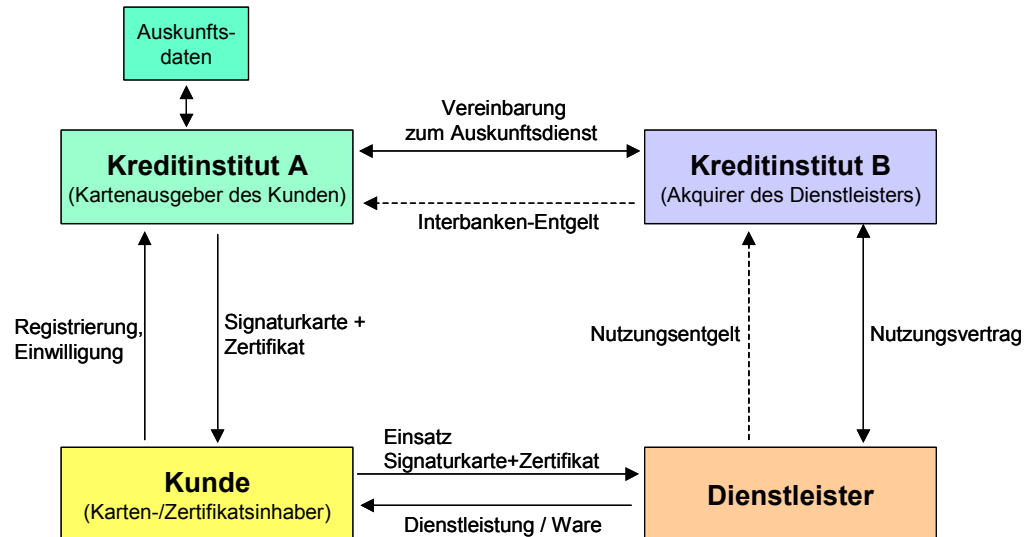
Die Unterstützung entsprechender Auskunftsdienste ist für ein Kreditinstitut selbstverständlich optional. Insbesondere bieten die Dienste "Bonitätsauskunft" und "Zahlungsgarantie" die Möglichkeit, die durch ein Kreditinstitut ausgegebenen Signaturkarten von denen anderer Kartenherausgeber außerhalb der Kreditwirtschaft zu unterscheiden.

Grundlage für die Auskunftsdienste sind die Daten, die ein Kreditinstitut über seine Kunden bereits heute hat, d.h. es müssen keine neuen Daten durch das Institut erhoben werden. Selbstverständlich muss der Karteninhaber gegenüber seinem Kreditinstitut seine Zustimmung erteilen, dass dieses über ihn im Rahmen der elektronischen Bankauskunft Auskünfte an Dritte gibt, wobei insbesondere auch die Anforderungen des Datenschutzes berücksichtigt werden müssen.

Für einen Dienstleister ist die Nutzung der genannten Auskunftsdienste kostenpflichtig. Er muss vor der ersten Anfrage einen entsprechenden Nutzungsvertrag mit seinem Kreditinstitut (Akquirer) schließen. Der Akquirer schließt den Nutzungsvertrag stellvertretend für die gesamte Kreditwirtschaft, d.h. der Dienstleister erhält dadurch Zugang zu den Auskunftsdiensten aller beteiligten Kreditinstitute. In diesem Nutzungsvertrag wird unter anderem auch das Nutzungsentgelt geregelt.

Ein Dienstleister rechnet seine Nutzung der Auskunftsdienste direkt mit seinem Akquirer ab. Dieser rechnet wiederum mit den Kartenherausgebern ab. Das dabei abzuführende Interbanken-Entgelt wird in Vereinbarungen zwischen den Instituten festgelegt.

Die folgende Abbildung zeigt die vertraglichen Beziehungen zwischen den beteiligten Instanzen:



### Abbildung 3: Vertragliche Beziehungen bei Mehrwertdiensten

Durch den ZKA ist geplant, einheitliche Schnittstellen zu spezifizieren, über die ein Dienstleister seine Anfragen an die Auskunftsdienste stellen kann bzw. über die er die entsprechenden Antworten erhält. Dazu werden in Zukunft ein oder mehrere kreditwirtschaftliche Kopfstellen eingerichtet, die im Auftrage der Kreditinstitute die technische Abwicklung der Auskunftsdienste übernehmen.

Ein Dienstleister erhält von seinem Akquirer Zertifikate (und die zugehörigen Schlüssel), mit denen er seine Berechtigung bei dem Stellen einer Anfrage gegenüber einer Kopfstelle nachweisen kann. Über diese Zertifikate (bzw. den Schlüsseln) wird auch die Sicherheit der Kommunikation zwischen den Kopfstellen und den Dienstleistern bzgl.

- der Identität des Absenders einer Anfrage bzw. Antwort,
- der Integrität einer Anfrage bzw. Antwort und
- der Vertraulichkeit von zu übermittelnden Auskunftsdaten

gewährleistet.

Die beschriebenen Auskunftsdienste bieten für das anbietende Kreditinstitut die Möglichkeit, basierend auf den von ihm

ausgegebenen Signaturkarten kostenpflichtige Mehrwertdienste anzubieten. Dadurch erhält es einen finanziellen Beitrag an dem Nutzen der Signaturkarte, den diese für den Kunden und die Dienstleister bei ihrem Einsatz hat. Für den nachfragenden Dienstleister bietet die Nutzung der genannten Auskunftsdienste den Vorteil, dass er bei der Abwicklung seiner Geschäftsvorfälle eine größere Zuverlässigkeit seiner Beziehung zu seinen Kunden erhält. So kann z.B. durch eine überprüfte Kundenidentität und -bonität die Anzahl der aufwendigen Rückabwicklungen von Warenlieferungen bei Bestellungen über das Internet wesentlich verringert werden. Behörden und Versicherungen erhalten erst durch die überprüfte Identität einer Person die Möglichkeit, über das Internet zum Beispiel Auskünfte über Versicherungsdaten zu erteilen. Die Angaben in einem Zertifikat zu der Identität des Zertifikatsinhabers dürfte hierfür nicht ausreichend sein.

## 5 Zusammenfassung, Stand der Arbeiten

Der ZKA hat durch seine Spezifikationen die technischen Grundlagen gelegt, um auf den kreditwirtschaftlichen Chipkarten eine einheitliche Signaturanwendung einführen zu können. Die Spezifikationen umfassen dabei

- die Signaturanwendung für die Chipkarten (Signaturkarten) und
- Grundlagen für eine einheitliche Kundenumgebung für die Nutzung der Signaturkarten.

Die Spezifikationen sind abgeschlossen (Signaturanwendung für die Chipkarten) bzw. befinden sich in der Abstimmung (Schnittstellen für eine einheitliche Kundenumgebung). Die Spezifikationen wurden an die relevanten Hersteller verteilt und zum Teil durch diese kommentiert. Erste Prototypen wurden auf der CeBIT2002 vorgeführt.

Neben den technischen Komponenten hat der ZKA Modelle für verschiedene Mehrwertdienste entwickelt. Diese Mehrwertdienste ermöglichen einem Kreditinstitut als Kartenherausgeber, basierend auf den von ihm ausgegebenen Signaturkarten (bzw. Zertifikaten) den Akzeptanten der elektronischen Signaturen neue (kostenpflichtige) Dienstleistungen anzubieten. Durch Nutzung der Mehrwertdienste wird ein Dienstleister, der in seinen Anwendungen eine elektronische Signatur akzeptiert und dadurch Vorteile (Sicherheit/Kosten) erhält, an den Kosten für die Ausgabe der Signaturkarten beteiligt, die sonst im Wesentlichen der Kartenausgeber trägt.

Die entsprechenden Konzepte für die Mehrwertdienste befinden sich zur Zeit in der Abstimmungsphase. Aus geschäftspolitischer Sicht ist dann zu entscheiden, ob entsprechende Infrastrukturen für die Realisierung der Mehrwertdienste aufgebaut werden.

Der ZKA setzt durch seine Spezifikationen einen einheitlichen Standard für eine mögliche Einführung der Signaturanwendung auf kreditwirtschaftlichen Chipkarten. Die Frage, ob tatsächlich entsprechende Signaturkarten ausgegeben werden, kann letztlich nur das einzelne Institut anhand seiner geschäftspolitischen Überlegungen entscheiden. Hierfür müssen die notwendigen tragfähigen Business Cases erarbeitet werden. Gelingt dies, wird die ZKA-Signaturkarte mittelfristig von ihrer Verbreitung bei den Endbenutzern her die bedeutendste Signaturkarte auf dem deutschen Markt sein und somit Standards auf dem Gebiet der Nutzung der elektronischen Signatur setzen bzw. wesentlich beeinflussen.

## 6 Literatur

- [1] Modell zum Einsatz einer kreditwirtschaftlichen Signaturkarte, Zentraler Kreditausschuss, Version 1.0, 2001
- [2] Schnittstellenspezifikation für die ZKA-Chipkarte, Secure Chip Card Operating System (SECCOS), Zentraler Kreditausschuss, Version 5.0, 2001
- [3] Schnittstellenspezifikation für die ZKA-Chipkarte, Signatur-Anwendung, Zentraler Kreditausschuss, Version 1.0, 2001
- [4] Schnittstellenspezifikation für die ZKA-Chipkarte, Konzept für die Unterstützung der Signatur-Anwendung der ZKA-Chipkarte durch das Internet-Kundenterminal, Zentraler Kreditausschuss, Version 1.0, 2002
- [5] Schnittstellenspezifikation für die ZKA-Chipkarte, Spezifikation für die Unterstützung der Signatur-Anwendung der ZKA-Chipkarte, Zentraler Kreditausschuss, Version 0.9, 2002
- [6] Signaturprozesse, Identitätsdienst, Zentraler Kreditausschuss, Version 0.9, 2002
- [7] Spezifikation der Schnittstelle zu Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV, DIN NI-17.4, Version 1.0, 1998
- [8] Chipcards with digital signature application/function according to SigG and SigV, Part 4: Basic Security Services, DIN V66291-4, Final Draft, 2000

- [9] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG), Mai 2001
- [10] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV), November 2001
- [11] HBCI Homebanking-Computer-Interface, Herausgegeben durch die BdB, BVR, DSGVO und VöB, Version 3.0 (Final Draft), 2002
- [12] eScheck - Proposal for a new international payment service, Bank-Verlag GmbH, Version , April 2002