

Der zukunftssichere Transaktionsstandard für das Online-Banking

Dieter R. Bartl
Direktor, Mitglied der Geschäftsleitung

8. Trierer Symposium „Digitales Geld“, 20. - 21. Juni 2002

Das aktuelle HBCI beruht auf den in 1996 vorhandenen Technologien.

HBCI-Standard

Die 1. HBCI -Version wurde 1996 verabschiedet.

Basisfunktionalität

- Nachrichtenaufbau
- Dialogabfolge
- Bankparameterdatei
- Userparameterdatei
- Sicherheit (ausschl. Signaturverfahren)

Geschäftsvorfälle

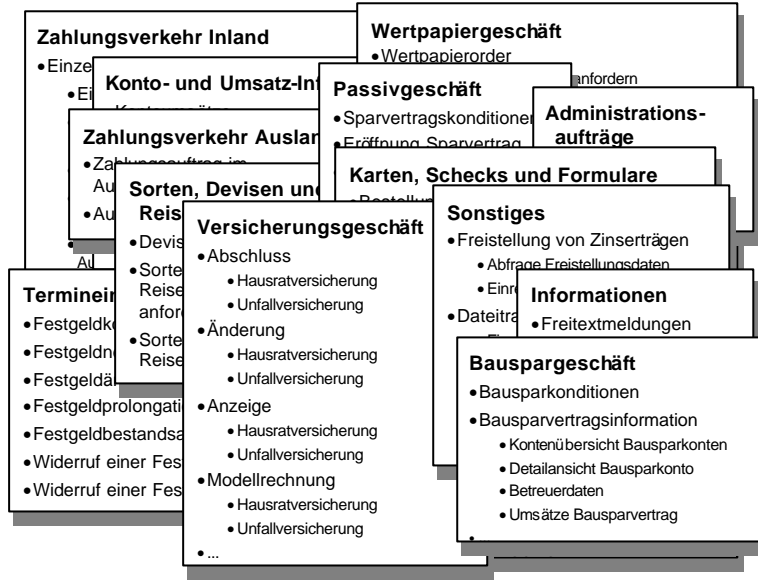
- ZKA-Standard
gültig für alle deutschen Kreditinstitute
- Individuelle Ergänzungen einzelner Verbände
z.B. Sparverkehr bei den Sparkassen

- **Eigene Verschlüsselungsverfahren / heute SSL-Standard**
- **Syntax analog UN/EDIFACT / heute XML als Internet-Standard**
- **Eingrenzung der zulässigen Sicherheitsverfahren (RDH und DDV-Chipkarte) / andere Sicherheitsverfahren weiterhin „im Markt“**
- **Ausschliesslich „Dialog-Verfahren“ / kein „E-Mail“ möglich**
- **Ausschliesslich für „Kunde-Bank-Dialog“ / kein Kunde-Intermediär-Bank-Dialog möglich**
- **Nur über eigenen Internet-Port (Port 3000) / Firewall-Problematik**

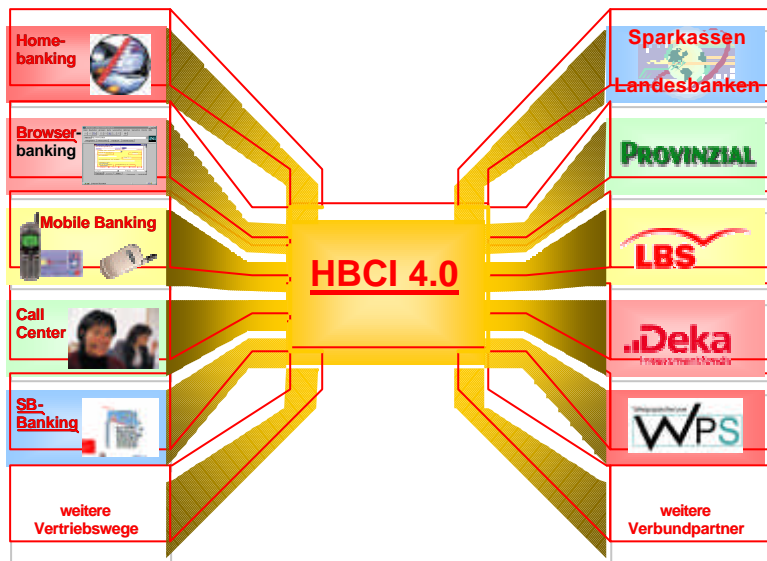
- HBCI und die Multikanal-Strategie
- HBCI 4.0 – die neue Generation
- Transaction-Services – sichere Transaktionen über alle Vertriebswege
 - Roadmap

SIZ 2001, S.2
Dieter Bartl

Derzeit sind bereits 100 Geschäftsvorfälle in der Sparkassenfinanzgruppe standardisiert.



Ziel: über jeden Vertriebsweg zu jedem Verbundpartner



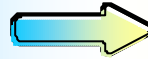
Mit Version V4.0 wird HBCI zum Multikanalstandard

Homebanking



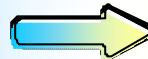
Multikanalfähigkeit

TCP/IP Port 3000



http, ftp, eMail, Webservices

Dialogbetrieb
synchron



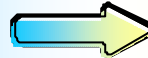
Dialog- / Datagrammbetrieb
synchron / asynchron

RSA mit Diskette
DES mit Chipkarte



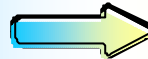
zusätzlich:
ZKA Signaturkarte
„UserDefinedSignature“

Kunde - Bank



Kunde - Intermediär - Bank
und Bank - Kunde

Privatkunde



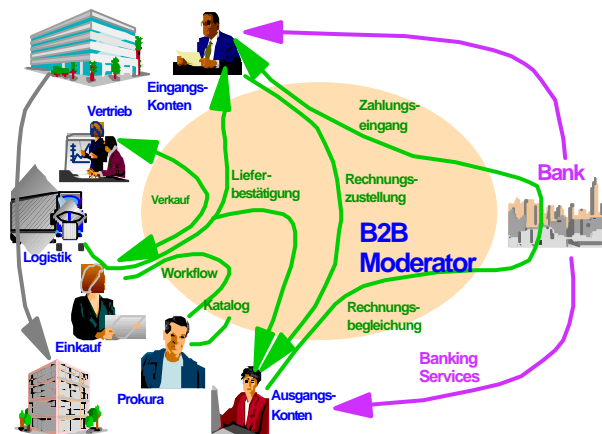
Privat- und Firmenkunde

national



Basis für internationale
Verwendung

Typische Geschäftsabwicklung im virtuellen Umfeld



- Vertraulichkeit:
 - „Konnte jemand meine Nachricht mitlesen?“
- Authentizität:
 - „Wer ist mein gegenüber? Ist der Absender wirklich derjenige, der er vorgibt zu sein?“
- Integrität:
 - „Können Manipulationen an den Daten erkannt werden?“
- Zurechenbarkeit:
 - „Kann das Absenden bzw. Empfangen einer Nachricht gegenüber Dritten nachgewiesen werden?“
- Kryptographie ist die Technik zur Erfüllung dieser Sicherheitsanforderungen

- Zwei Kommunikationspartner besitzen den gleichen Schlüssel zur Ver-/Entschlüsselung und Signaturerzeugung/-prüfung
- Aufwändiges Keymanagement
- Bekannte Algorithmen: „DES“ (Schlüssellänge nicht mehr zeitgemäß), „TripleDES“
- Neues Verfahren in Auswahl und Vorbereitung: „AES“
- Jeder Kommunikationspartner erzeugt ein Schlüsselpaar, stellt seinen „öffentlichen“ Schlüssel zur freien Verfügung und behält einen „privaten“ geheim.
- Keymanagement = Zertifizierungsinfrastrukturen
- Bekanntester Alg.: „RSA“, hohe Rechenintensität
- Neues Verfahren: „Elliptische Kurven“

Symmetrisch

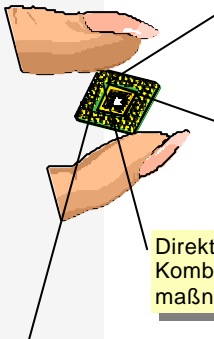
Asymmetrisch

Anwendungsszenarien digitaler Signaturen

- Asymmetrische Kryptographie - digitale Signaturen und Zertifikate - ist die Basistechnologie für sichere Internet-Anwendungen
 - Sicherer Webzugriff, z. B. SSL, X.509v3 Zertifikate
 - Sichere E-Mail, z. B. S/MIME
 - Sicherer Datenaustausch, z. B. Signed XML
 - Kryptographische Virtual Private Networks (VPN)
- Je nach Anwendungsszenario sind Zertifikate das funktionale Äquivalent zu:
 - Personalausweis,
 - **Bankkarte**,
 - Kundenkarte,
 - Visitenkarte, ...

Sicherheitsmodul zum Signieren

Ein Satz der Chipkarte



Überschaubares System als Grundlage einer Sicherheitsevaluierung (ITSEC E4 für Betriebssystem, E2 plus für Leser nach Maßnahmenkatalog)

Echte Zufallszahlen erlauben Schlüsselerzeugung auf der Karte (privater Schlüssel nie außerhalb der Karte)

Direktes Auslesen des Schlüssels wird durch eine Kombination von physikalischen + logischen Sicherheitsmaßnahmen verhindert

Ausführung der Algorithmen auf der Chipkarte (kein Schlüsseltransport in korruptierte Terminals, keine korruptierte Algorithmen)

Aufgabe einer Zertifizierungsstelle

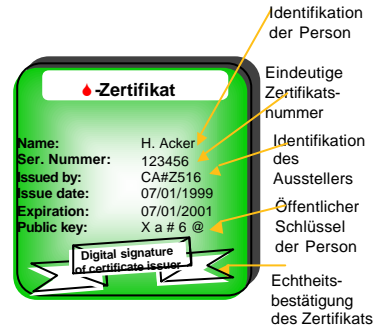
Schaffung einer

- authentischen und
- integeren

Verknüpfung von

- kryptographischen Schlüsseln mit
- natürlichen/juristischen Personen

in Form eines Zertifikates
(zeitlich begrenzt)
und dessen Veröffentlichung



Alternative Namen:
Trust Center, Trusted Third Party
(TTP)

Fazit

- Die Technik der digitalen Signatur ist ein Enabler für E-commerce.
- Verschiedene Anwendungen
 - haben unterschiedlich hohe Sicherheitsanforderungen
⇒ Verschiedene Arten von Signaturen und Zertifikaten
 - Stellen unterschiedliche funktionale Anforderungen an die Chipkarte
⇒ Hohe Komplexität einer „universell“ einsetzbaren Karte
- Kommunikation und Transaktion können mit den heute verfügbaren Techniken angemessen abgesichert werden.
- **Doch Vorsicht!** Sicherheit muss ganzheitlich betrachtet werden und betrifft alle Komponenten der IT-Infrastruktur. Insbesondere auch den PC des Endkunden. Dieser muss sensibilisiert werden bezüglich der Gefahren, wie z. B.: Virenbefall, Trojaner und Würmer, ...
- Benötigt wird eine ganzheitliche Sicherheitsstrategie, die innerhalb einer Organisation über alle Hierarchieebenen hinweg definiert, gelebt und ständig weiterentwickelt werden muss: Nur im Rahmen einer solchen, mittel- und langfristig angelegten Sicherheitsstrategie kann das Gefahrenpotential eines Unternehmens minimiert werden.