Sichere Wege

Verschlüsselungsverfahren für das Onlinebanking

Kai-Oliver Detken

Die Verbreitung des vom Zentralen Kreditausschuß (ZKA) verabschiedeten Sicherheitsverfahrens HBCI für das Onlinebanking ist im Privatkundensegment schon relativ hoch und holt im Vergleich zum PIN/TAN-Verfahren immer mehr auf. Im Unternehmensbereich ist die Akzeptanz von HBCI – jetzt FinTS genannt – allerdings noch nicht gegeben; nur ein kleiner Teil der kleinen und mittelständischen Unternehmen benutzt schon den Standard.
Dies liegt zum einen an der fehlenden Integration von HBCI in bestehende Systeme der Unternehmen und zum anderen an der mangelnden Aufklärung durch die Kreditinstitute. Ihr Ziel ist es, FinTS V4.0 als Industriestandard zu etablieren. Die Einführung der Banken-Signaturkarte und neue Funktionalitäten werden dabei hilfreich sein.

Dr. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Das Homebanking Computer Interface (HBCI) wurde in praxistauglicher Form erstmals 1998 in der Version 2.01 veröffentlicht; Entwürfe reichen bis ins Jahr 1995 zurück. Es folgten die Versionen 2.1 (1999) und 2.2 (2000), die sich bis auf hinzugefügte Geschäftsvorfälle relativ wenig voneinander unterschieden.
Im Jahr 2002 wurde die Version 3.0 veröffentlicht und der Standard umbenannt in Financial Transaction Services (FinTS). Mit FinTS kamen das Sicherheitsverfahren PIN/TAN (Persönliche Identifikationsnummer/Transaktionsnummer) sowie der Einsatz von Signaturkarten hinzu. Abgesehen davon galten die Strukturen aus den Vorversionen in ähnlicher Form weiter.
In der Zwischenzeit hatte der Deutsche Sparkassenverband eine Version namens HBCI+ eingesetzt, bei der ein PIN/TAN-Sicherheitsverfahren genutzt wurde. In der Version FinTS V3.0 wurde dieses Verfahren dann als alternative Sicherheitslösung in den FinTS-Standard aufgenommen.
Schließlich wurde 2004 die Version FinTS V4.0 eingeführt. In ihr wurden alle internen Datenstrukturen komplett auf XML und XML-Schemata umgestellt, HTTPS als Kommunikationsprotokoll verwendet und weitere komplett neue Schnittstellen (z.B. WWW-Portale) eingeführt.
Nach einer zunächst zögerlichen Einführung wird HBCI seit 2002 von ca. 2.000 Banken, also etwa der Hälfte der deutschen Institute, angeboten. Obwohl ursprünglich auch eine internationale Verwendung des Standards angestrebt war, blieb HBCI rein auf den deutschen Bankenmarkt beschränkt.

PIN / TAN-Verfahren

Das älteste und technologisch am wenigsten komplexe Verfahren ist das PIN/TAN-Verfahren. Hier erfolgt die Authentifizierung eines Kunden durch eine Benutzerkennung (z.B. die Kunden- oder Kontonummer) in Verbindung mit einem nur dem Kunden bekannten Kennwort, der PIN. Die Benutzerkennung in Kombination mit der PIN muß einmalig pro Session eingegeben werden. Um eine einzelne Transaktion zu autorisieren, steht dem Kunden eine Liste zufällig generierter TANs zur Verfügung, von denen pro Transaktion eine verwendet werden muß und diese nur einmal verwendet werden kann. Die TANs werden dem Kunden in Form einer Liste per Briefpost zugestellt.
HBCI 2.2 wurde zunächst inoffiziell um das PIN/TAN-Verfahren erweitert. Man sprach hierbei von HBCI2.2 PIN/TAN oder auch HBCI+. Seit der Version FinTS 3.0 können HBCI-Aufträge auch offiziell mit dem PIN/TAN-Verfahren authentifiziert werden. Die in HBCI+ und FinTS 3.0 genutzten Varianten des PIN/TAN-Verfahrens unterscheiden sich jedoch voneinander.
Die Datenübertragung erfolgt über eine gesicherte HTTPS/SSL-Verbindung und funktioniert dadurch unverändert über HTTP-Firewalls. Dies steht im Gegensatz zum bisherigen HBCI, was die Freigabe des Port 3000 benötigt. Das

Das Thema in Kürze

Mit der Verabschiedung des HBCI-1.0-Standards durch den ZKA Ende 1996 wurde ein neues Zeitalter im Onlinebanking eingeläutet. HBCI definiert Übertragungsprotokolle, Nachrichtenformate und Sicherheitsverfahren. Mit HBCI 1.0 war es zum ersten Mal möglich, Transaktionen auch über das Internet abzuwickeln. Doch wie sicher sind solche Überweisungen? Der Beitrag gibt einen Überblick über Entwicklung und Sicherheitsmechanismen von HBCI.

Verfahren nutzt die Vorteile von HBCI zusammen mit der gewohnten Handhabung von TAN-Listen, was besonders aus Sicht der Banken eine Vereinfachung des HBCI-Zugangs bedeutet.
Allerdings verliert man einige Sicherheitsvorteile von HBCI; z.B. werden die Transaktionen bei PIN/TAN nicht mehr elektronisch signiert. Ein weiteres Problem ist das verstärkte Auftreten von Phishing nach PINs und TANs, also das Erschleichen von ihnen durch Trickbetrug. Trotzdem bieten immer mehr Kreditinstitute diesen Übertragungsweg an, besonders deshalb, da bisherige PIN/TAN-Zugänge den veralteten Zugang über T-Online Classic (Btx) verwendeten, dessen Betrieb nur noch für die Banking-Anwendung aufrechterhalten wurde.
Ein Vorteil des PIN/TAN-Verfahrens ist, daß auf seiten des Kunden keine zusätzlichen technischen Hilfsmittel eingesetzt werden müssen. Nachteilig sind Sicherheitsbedenken, die immer wieder – auch von Bankenvertretern – geäußert werden. Mit allen bekannten Angriffsverfahren (Man-in-the-Middle, Phishing, Trojaner, Social Hacking) auf Onlinebankingsysteme wird versucht, sich auch die Schwächen von PIN/TAN zunutze zu machen.
Wegen der Probleme des PIN/TAN-Verfahrens haben einige Anbieter eigene Erweiterungen vorgenommen, um die Sicherheit zu erhöhen. Eine Reihe von Banken setzt etwa das iTAN-Verfahren (indizierte TAN) ein, das bei der Abfrage einer TAN nicht eine beliebige, sondern ausschließlich eine festgelegte, indizierte TAN akzeptiert. Erste Evaluierungen ergaben, daß aber auch dieses Verfahren eine Reihe von Schwachpunkten besitzt.
Eine andere Erweiterung stellt die eTAN (elektronische TAN) dar. Hierbei bekommt der Kunde von seinem kontoführenden Institut ein Gerät zur Verfügung gestellt oder muß es käuflich erwerben, in das eine während der Transaktion erstellte Kontonummer eingegeben werden muß. Das Gerät erzeugt auf Basis der Eingabe eine gültige TAN, die vom Kunden dann im Onlinebanking-System der Bank eingegeben werden kann, um die Transaktion zu autorisieren.

Das besondere Merkmal von HBCI ist die Bankenunabhängigkeit, die Providerunabhängigkeit und die öffentliche Verfügbarkeit des Standards. Dadurch ist es prinzipiell jedem Programmierer oder Softwarehersteller möglich, eine Implementierung der Clientseite von HBCI zu erstellen und damit auf alle HBCI-fähigen Banken zuzugreifen. Der Standard sieht dazu mehrere Möglichkeiten der wirkungsvollen Authentifizierung vor, so daß die Hersteller- und Bankenunabhängigkeit in der Praxis tatsächlich für echte Geldgeschäfte in Anspruch genommen werden kann und eine Vielzahl von Anbietern die entsprechenden Softwarebausteine bereitstellt.

Verschlüsselungen

HBCI spezifiziert im wesentlichen zwei große Teilbereiche des Onlinebanking:

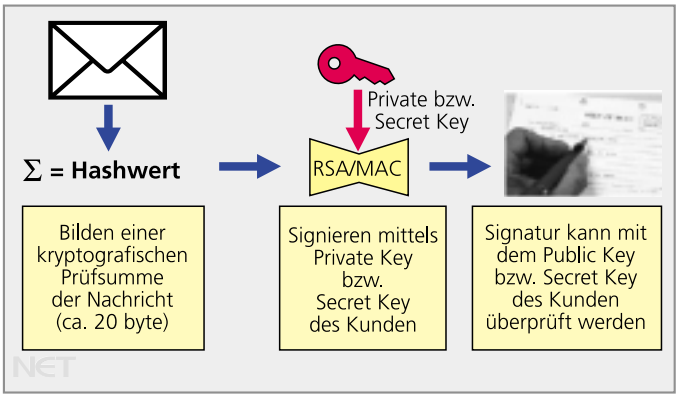
- Es werden mehrere Sicherheitsverfahren zur Authentifizierung und Verschlüsselung der Aufträge definiert, z.B. Chipkarten oder PIN/TAN.
- Es werden durch die Geschäftsvorfälle Datenformate und Abläufe für die Ausführung einzelner Bankgeschäfte festgelegt, z.B. Einzelüberweisung, Umsatzabruf eines Kontos, Änderung eines Dauerauftrags.

Eine Alternative zu den PIN/TAN-Verfahren ist der Einsatz von asymmetrischen Verschlüsselungsverfahren. Es werden damit nicht nur Verfahren zur Autorisierung und Authentifizierung angeboten, sondern auch Funktionen wie Transaktionskonzept und Mandantenfähigkeit. Das HBCI-Verfahren ist sowohl mit der Schlüsseldiskette als auch mit der Smartcard im Einsatz, wobei die höchste Sicherheit nur unter Verwendung der Smartcard mit entsprechendem Lesegerät erreicht wird. (Zum Zeitpunkt der ersten HBCI-Veröffentlichung war eine Diskette noch das vorherrschende beschreibbare Wechselmedium, so daß immer von der „Schlüsseldiskette“ die Rede ist, obwohl jedes andere Speichermedium – etwa ein USB-Stick – genausogut zu Anwendung kommen kann.) In jedem Fall muß der Kunde zur Autorisierung und Authentifizierung eine PIN eingeben, die dann den privaten Schlüssel des Kunden freischaltet, der sich auf Diskette oder Smartcard befindet. Der Schlüssel wird dann für das Erstellen einer digitalen Signatur der Transaktion verwendet. Der Bankserver auf der Gegenseite kennt den öffentlichen Schlüssel des Kunden und kann auf diese Weise die Signatur der Transaktion verifizieren. Die Verbindung mit der Bank wird ihrerseits unter Einsatz eines symmetrischen Verschlüsselungsverfahrens gesichert.
Konkret sieht dies so aus: Für die Authentifizierung wird in der Software des Kunden ein RSA-Schlüsselpaar (RSA – Rivest, Shamir und Adleman; Erfinder des Algorithmus) mit 768 bit Schlüssellänge erzeugt (HBCI V2.x; ab FinTS V3.0 auch 1.024 bis 2.048 bit, genannt Sicherheitsklasse RDH-2/3/4). Danach wird vom Benutzer ein elektronischer Fingerabdruck (Fingerprint) des öffentlichen Signaturschlüssels auf Papier ausgedruckt und unterschrieben an die Bank gesendet. Gleichzeitig wird der öffentliche RSA-Schlüssel elektronisch an den HBCI-Server der Bank gesendet. Die Bank kann anhand des unterschriebenen Fingerabdrucks sicherstellen, daß der elektronisch eingereichte Schlüssel auch tatsächlich und ausschließlich vom unterschreibenden Bankkunden stammt. Damit ist der selbst erzeugte Schlüssel auf sichere Weise authentifiziert und kann nun zur Signatur jedes Auftrags verwendet werden.
Zur Nachrichtenverschlüsselung wird das Triple-DES-Verfahren (Data Encryption Standard) genutzt. Für jede Nachricht wird ein neuer 112-bit-Einmalschlüssel generiert, der dann mit dem dauerhaften RSA- oder DES-Schlüssel verschlüsselt wird. Diese Vermischung des RSA- und DES-Verfahrens heißt im HBCI-Standard RSA-DES-Hybridverfahren (RDH).

Signaturen

Bei eingereichten Aufträgen ist es wichtig, daß die Herkunft eindeutig nachgewiesen werden kann. Dies wird durch die jeweilige elektronische Signatur gewährleistet. Beim DDV (DES-DES-Verfahren) besteht die theoretische Möglichkeit der Signatur eines Kundenauftrags durch ein Kreditinstitut. Dies wird allerdings durch das

Vertrauensverhältnis Kunde/Kreditinstitut aufgehoben. Ein echter Herkunftsbeweis ist nur bei asymmetrischen kryptografischen Verfahren wie dem RDH möglich.
Die elektronische Signatur soll beweisen, daß die FinTS-Nachricht auf dem Übertragungsweg nicht modifiziert wurde. Dazu wird ein sog. Hashwert über die gesamte Nachricht gebildet. Aus dem Ergebnis wird dann gemäß Message Authentication Code (MAC) bzw. RSA eine elektronische Signatur berechnet, die in das FinTS-V3.0-Segment „Signaturabschluß“ eingebettet wird (*Bild*). Bei FinTS V4.0 wird die Signatur unter dem entsprechenden Tagnamen in die Struktur nach XML-Signatur eingebettet. Der Empfänger bildet den Hashwert nach dem gleichen Algorithmus und überprüft die Signatur mittels Secret Key (bei DDV) bzw. Public Key (bei RDH).



Signaturbildung nach den Verfahren DDV und RDH

Sicherheitsgrade

Im Gegensatz zur elektronischen Signatur, bei der die Nachricht immer noch lesbar ist, wird bei der Verschlüsselung die gesamte Nachricht verschlüsselt und damit unleserlich gemacht. Dies hat vor allem Vorteile bei der Übertragung vertraulicher Informationen wie etwa Umsatzdaten.
Bei FinTS V3.0 wird zur HBCI-Verschlüsselung der Daten generell Triple-DES verwendet. Als Schlüssel wird aus Sicherheitsgründen nicht der eigentliche Chiffrierschlüssel benutzt, sondern ein nachrichtenspezifischer Schlüssel. Dieser wird für jede Nachricht neu aus einer Zufallszahl gebildet, die mit dem Chiffrierschlüssel gemäß DDV bzw. RDH verschlüsselt und der Nachricht vorangestellt wird. Bei FinTS V4.0 wird außer der HBCI-Verschlüsselung auch SSL angeboten. Da SSL bzw. HTTPS im Internet-Umfeld den Standard für Transportverschlüsselung darstellt, wird die HBCI-Variante nur bei folgenden Situationen angewendet: auf Verbindungen, die kein SSL (HTTPS) unterstützen (beispielsweise E-Mail mit SMTP) oder wenn eine Ende-zu-Ende-Verschlüsselung erforderlich ist.
Bei einem möglichen Angriff würde versucht werden, die Daten einer Verbindung abzuhören und die gespeicherten Informationen wiederholt einzuspielen. Diese sog. Replay-Attacke kann mehrfach durchgeführt werden, um so z.B. Überweisungen gegen den Willen des Kunden wiederholt zu tätigen. Oft wird daher als Kriterium für die Eindeutigkeit ein Zeitstempel herangezogen, was aber nicht von allen Endgeräten unterstützt wird und auch nicht immer zuverlässig funktioniert. In der FinTS-Spezifikation wurde deshalb ein Verfahren zur Doppeleinreichungskontrolle entwickelt, das unter Beibehaltung der Flexibilität den Mißbrauch ausschließt. Es besteht aus einer Kombination eines Sequenzzählers, der parallel auf dem Sicherheitsmedium und im Kreditinstitut geführt wird, und einer Liste von bereits eingereichten Sequenzen, in der die Lücken über einen bestimmten Zeitraum festgehalten werden. Dadurch können auch solche Angriffe ausgeschlossen werden.
Durch die HBCI-Sicherheitsverfahren RDH und DDV wird ein hohes Maß an Sicherheit erreicht:

- Beim Verfahren *RDH* werden jeweils Schlüsselpaare verwendet, die immer aus einem Private Key und einem Public Key bestehen. Der Kunde bekommt per Software oder auf einer Chipkarte ein persönliches Schlüsselpaar erzeugt und seine Aufträge mit seinem Private Key signiert. Das Kreditinstitut kann mittels zuvor übermitteltem Public Key die elektronische Unterschrift auf Korrektheit prüfen. Der Public Key beweist die Herkunft der Signatur eindeutig und muß nicht geheimgehalten werden, da mit ihm nur Signaturen überprüft werden. Nur mit Hilfe des geheimen Schlüssels – des Private Key – können die Daten wieder entschlüsselt werden.
  Bei HBCI werden in der Maximalausprägung bei der ZKA-Signaturkarte drei Schlüsselpaare verwendet (Signierschlüsselpaar, Authentisierungsschlüsselpaar, Chiffrierungsschlüsselpaar). In den meisten Fällen ist allerdings der Einsatz des Authentisierungsschlüsselpaars zur Signaturbildung ausreichend.
- Das Verfahren *DDV* ist ein symmetrisches Verfahren, weswegen die Schlüssel zum Signieren und Chiffrieren beiden Partnerinstanzen bekannt sein müssen. Daher müssen die Schlüssel vor der Kommunikation auf einem anderen Wege ausgetauscht werden. Die Sicherheit hängt davon ab, daß nur die beiden Partnerinstanzen den geheimen Schlüssel (Secret Key) kennen. Bei HBCI werden zwei Schlüsselarten verwendet: Signierschlüssel und Chiffrierschlüssel. Die hier zum Einsatz kommenden kryptografischen Funktionen werden auf der Basis des Triple-DES-Verfahrens durchgeführt.

Beide Verfahren und Mechanismen sind in der FinTS-V4.0-Spezifikation ausführlich beschrieben. Die Anwendung ist für Kunden- und Banksysteme meistens zwingend vorgeschrieben. Freiheitsgrade bestehen lediglich beim Signieren von Banknachrichten im RDH-Verfahren. Seit der Version HBCI V2.01 muß jede Nachricht verschlüsselt werden. Generelles Ziel aller Verbände ist ein asymmetrisches Sicherungsverfahren, basierend auf einer ZKA-weit standardisierten Banken-Signaturkarte. *(we)*