

ZKA-KOMPENDIUM

ONLINE-BANKING-SICHERHEIT

ZKA-Zentraler Kreditausschuss

www.zka.de

info@zka.de

09. November 2009

Warum Sicherheit im Online-Banking?

Die Kommunikation zwischen dem Kunden und seiner Bank fand von jeher in einer speziell geschützten Umgebung statt. Noch heute verbergen sich hinter der freundlichen Atmosphäre der Bankfiliale zahlreiche Maßnahmen, um die Sicherheit bei der Abwicklung von Finanzgeschäften zu ermöglichen und sich gegen Bankräuber zu schützen. So war es auch bei der Einführung des Online-Banking vor 25 Jahren unverzichtbare Voraussetzung, für die Kommunikation zwischen Kunde und Bank ein vertrauenswürdiges Umfeld zu schaffen – das damalige PIN/TAN-Verfahren.

Seitdem hat eine rasante Entwicklung stattgefunden und es ist heute möglich über das Internet fast jede Art von Transaktion in einer virtuellen Filiale von zuhause aus abzuwickeln. Dies stellt naturgemäß einen großen Anreiz für Angreifer dar, die fließenden Geldströme auf das eigene Konto umzuleiten. Das PIN/TAN-Verfahren

INHALT

Warum Online-Banking-Sicherheit?	1
Grundlagen zur Online-Banking-Sicherheit	1
Die HBCI -Karte	3
Der Secoder	3
chipTAN-Verfahren	4
mobileTAN-Verfahren	5

bietet seit einigen Jahren keinen passenden Schutz mehr gegen die immer besser werdenden Angriffe. Daher kümmert sich der Zentrale Kreditausschuss seit Jahren um die Weiterentwicklung solcher Sicherheitsmaßnahmen und hat sich auch auf einige grundlegende Verfahren geeinigt, die bei vielen Banken und Sparkassen zum Einsatz kommen und das Sicherheitsniveau im Vergleich zum klassischen PIN/TAN-Verfahren anheben können.

Grundlagen zur Online-Banking-Sicherheit

Für die Abwicklung von Geldgeschäften müssen Sicherheitsniveaus erreicht werden, die über eine normal abgesicherte SSL-Internetkommunikation weit hinaus gehen. Im Wesentlichen sind zwei Faktoren

ausschlaggebend für das geforderte Sicherheitsniveau:

1. Spricht der „echte“ Kunde mit seiner Bank und umgekehrt (Authentizität)?

2. Die Absichtserklärung des Kunden zum Tätigen eines Bankgeschäfts

Das erste Sicherheitskriterium ist noch relativ leicht zu erfüllen – über vereinbarte Zugangsdaten wie eine Kundennummer und die Online-Banking-PIN in Verbindung mit der SSL-Übertragungssicherheit – können Kunde und Bank an jedem Ende der Kommunikationsstrecke leicht identifiziert werden. Aus diesem Grund darf die Online-Banking-PIN nie fremden Personen mitgeteilt und auf bankfremden Internetseiten eingegeben werden. Auch die Verschlüsselung der Datenübertragung ist hinreichend gewährleistet.

Schwerer abzusichern ist die Absichtserklärung des Kunden mit den damit verbundenen Parametern wie z. B. Betrag und Empfänger der Zahlung, weil dies sehr viel attraktiver für Angreifer ist. Gelingt es hier, die Daten zu manipulieren, können Geldströme ohne Wissen des Kunden umgeleitet werden. Genau hier setzen die neuen ZKA-Sicherheitsmaßnahmen an:

Die im Folgenden vorgestellten Verfahren lassen sich nach Art des Einsatzszenarios in stationäre und mobile Verfahren unterscheiden. Stationäre Verfahren gehen davon aus, dass der Kunde seine Bankgeschäfte an einem fest installierten Arbeitsplatz erledigt, an dessen USB-Schnittstelle ein Chipkartenleser angeschlossen ist. Will der Kunde von unterwegs auf seine Konten zugreifen, so eignen sich mobile Verfahren besser, bei denen ein Standard-PC oder ein Smartphone ausreicht. Beide Varianten funktionieren unabhängig davon, ob eine Finanzsoftware zum Einsatz kommt, oder ein Internet-Browser verwendet wird.

Da das eigentliche Endgerät z. B. mit seinem PC-Betriebssystem die Hauptangriffsfläche bietet, gilt es diese Umgebung für den kritischen Prozess zu umgehen. Dies bedeutet jedoch nicht, dass der Kunde nicht mehr auf die Absicherung seines Arbeitsplatzes achten muss. Die Installation eines Virenschanners bei aktuell gehaltenen Virendefinitionen ist die Voraussetzung für jegliche Geschäftstätigkeit im Internet.

Das entscheidende „Ich will diesen und genau diesen Auftrag jetzt ausführen“ wird bei den neuen Verfahren über mehrere Wege speziell abgesichert:

1. Die HBCI-Karte spielt bei den meisten der angebotenen Verfahren eine zentrale Rolle. Der Kunde muss im Besitz der Karte sein und diese meist mit einer Karten-PIN separat freischalten. Die entscheidenden Verschlüsselungsprozesse finden allerdings innerhalb der Chipkarte statt und können von außen nicht manipuliert werden.
2. Speziell im mobilen Bereich stellt sich die Frage, wie gerade die sensiblen Daten eines Auftrags wie beispielsweise Betrag und Empfänger in die Karte gelangen können, ohne dass ein Angreifer sie manipulieren kann. Hierfür gibt es zwei Möglichkeiten, nämlich (1) die Verwendung eines TAN-Generators mit separater Anzeige und Tastatur und (2) die Übertragung über einen separaten Kommunikationskanal.

Wie diese Maßnahmen zusammenwirken zeigt die Vorstellung der ZKA-Verfahren in den nächsten Abschnitten.

Stationäre Verfahren:

Die HBCI-Karte

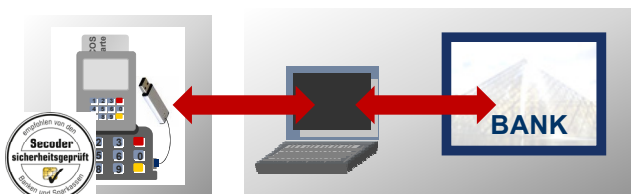


Die HBCI-Karte stellt bereits seit Einführung des HBCI-Standards (heute: FinTS-Standard) den zentralen Bestandteil für die stationäre Verwendung dar. War damals die Konfiguration eines Chipkartenlesers am PC teilweise noch schwierig, so stellt dies heute mit USB-Anschlüssen keine Hürde mehr dar. Die HBCI-Karte ist mit aktuellen Sicherheitsverfahren ausgerüstet und sorgt für eine sichere Abwicklung der Verschlüsselungsfunktionen, die mit einer Karten-PIN vor Zugriffen durch Fremde geschützt sind. Beim Klasse-2-Leser mit eigener Tastatur wird die PIN direkt am Kartenleser eingegeben und von der Karte geprüft, ohne, dass die Daten jemals mit dem PC in Verbindung kommen können. Nach Freischaltung der HBCI-Anwendung auf der Karte ist diese bereit, Verschlüsselungsfunktionen durchzuführen. Hierfür wird der Bankauftrag im PC über ein so genanntes Hashverfahren stark

komprimiert und in der Chipkarte mit einer Signatur versehen. Da diese Signatur zusammen mit dem Kundenauftrag über Internet an die Bank geschickt wird, kann der Auftrag ab diesem Zeitpunkt nicht mehr verändert werden.

Trotz der Verwendung der HBCI-Karte bleibt ein theoretisches Restrisiko: Der Kunde kann die Auftragsdaten im Chipkartenleser nicht mehr kontrollieren, d. h. er hat keine Transparenz, welche Daten zum Chipkartenleser zur Signaturbildung geschickt wurden. Dieses Restrisiko hat jedoch in der Vergangenheit noch nie zu einem Missbrauch geführt. Diese vermeintliche Schwachstelle kann z. B. durch die Verwendung von sicheren Signaturanwendungskomponenten, wie sie bei Qualifizierten Elektronischen Signaturen vom Gesetzgeber vorgeschrieben sind, behoben werden. Diese Lücke wird aber auch durch den Secoder, den neuen Chipkartenleser der Kreditwirtschaft geschlossen, wie im nächsten Abschnitt erläutert wird.

Der Secoder



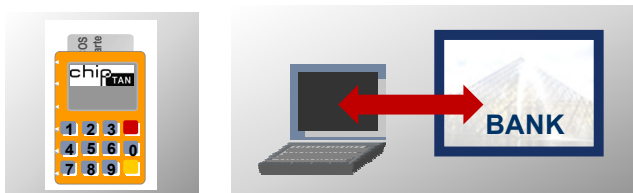
Nachdem die Verwendung von Chipkarten für Bankanwendungen sich in den letzten Jahren in verschiedenen Einsatzszenarien bewährt hat und weiter ausgebaut werden

soll, haben sich Banken und Sparkassen entschieden, einen eigenen, sicheren Chipkartenleser zu standardisieren, der anwendungsunabhängig zum Einsatz kommen und zu einem attraktiven Preis angeboten werden soll. Der Secoder bietet eine sichere Umgebung für die Anzeige und Eingabe bzw. Bestätigung von Daten und bietet dem Kunden somit die Möglichkeit,

die kritischen Daten eines Auftrags im Leser kontrollieren und freigeben zu können. Hierbei fließt der gesamte Bestätigungsprozess – was wurde angezeigt und wie hat der Kunde reagiert? – in die Signaturbildung mit ein und kann auf der Bankseite nachvollzogen werden. Dabei ist es für den Secoder unerheblich, ob es sich um Online-Banking, einen Logon-Prozess mit PIN oder eine Geldkarten-Ladetransaktion handelt. Damit der Secoder aber auch für nicht-kreditwirtschaftliche Anwendungen wie z. B. das Lesen einer SIM-Karte wie ein normaler Chipkartenleser fungieren kann, verfügt er über einen Default-Modus, aus dem jedoch kein Zugriff auf das Display des Lesers erlaubt ist. Die Anzeige von Daten funktioniert nur im

sicheren Anwendungsmodus und ist über spezielle Firewallregeln im Secoder abgesichert. Da diese Betriebsart anhand von Signaturen vom Banksystem überprüft werden kann, ist somit ein sehr hoher Sicherheitsstandard gegeben, der technisch keine signifikanten Angriffsflächen mehr bietet. Unter dem Motto „what you see is what you get“ („was du siehst ist was du bekommst“) kann der Kunde am Secoder alle relevanten Auftragsdaten auf sichere Weise kontrollieren und bestätigen. Organisatorisch wird die Sicherheit von Secoder-Produkten durch ein spezielles Freigabe- und Zertifizierungsverfahren gewährleistet. Nur Produkte, welche diese Tests bestehen, dürfen das Secoder-Logo tragen und frei am Markt vertrieben werden.

stationäre / mobile Verfahren: chipTAN-Verfahren



Das neue chipTAN-Verfahren verbindet den Einsatz eines üblichen TAN-Verfahrens am PC mit einem TAN-Leser, der ebenfalls das Visualisierungskonzept des Secoders nutzt. Auch hier stellt die HBCI-Karte das Herzstück dar, da sie aus den eingegebenen Daten ein Kryptogramm errechnet, das vom TAN-Leser zu einer 6-stelligen numerischen TAN umgeformt wird, die der Kunde als Mini-Signatur zur Freigabe des Auftrags am PC eingibt. Doch zuvor müssen die relevanten Auftragsdaten auf sichere Art und Weise in den TAN-Leser gelangen. Da das manuelle Abtippen von Auftragsdetails wie Betrag oder

Empfängerdaten unbequem und fehleranfällig ist, wurde vom ZKA ein optisches Übertragungsverfahren mit Hilfe einer animierten Grafik entwickelt. Die blinkenden schwarzen und weißen Rechtecke stellen die zu visualisierenden Auftragsdaten dar. Hält der Kunde nun seinen TAN-Leser mit der gekennzeichneten Kante vor den Bildschirm so werden über integrierte optische Elemente die Daten in den TAN-Leser übernommen. Dies dauert nur wenige Sekunden und ist an allen gängigen Displays wie Flach- oder Röhrenbildschirmen, bei einigen kleinen Produkten auch mit SmartPhones, möglich. Die Verarbeitung der Daten im TAN-Leser geschieht nun ähnlich wie beim Secoder: die Auftragsdaten werden einzeln im Leser-Display angezeigt und können so mit den

Originaldaten am Beleg verglichen werden. Der Kunde hat nun wie beim Secoder die Möglichkeit, die Korrektheit der Daten außerhalb der PC-Sphäre zu kontrollieren und damit deren Richtigkeit zu bestätigen. Da die einzelnen Visualisierungsschritte

auch hier in die TAN-Berechnung mit eingehen, kann der Vorgang auf der Bank-Seite nachvollzogen und geprüft werden. Damit wird eine ähnlich hohe technische Sicherheit wie beim angeschlossenen Secoder erreicht.

mobile Verfahren:

mobileTAN-Verfahren



Alle bisher vorgestellten ZKA-Verfahren verwenden die HBCI-Karte als Basis. Dies erfordert jedoch in jedem Fall den Einsatz von Kartenlesern, was für manchen Kunden unbequem ist und für Wenignutzer die Anschaffung eines TAN-Lesers nicht rechtfertigt. Diese Lücke wird nun durch das mobileTAN-Verfahren geschlossen. Hier bedient man sich der Technik der Übertragung über zwei unterschiedliche Kanäle, zum einen das Festnetz für die Internet-Verbindung zum PC zum anderen das GSM-Netzwerk für die Kontrolle und Bestätigung der Daten. Dies impliziert bereits, dass die Verwendung des mobileTAN-Verfahrens z. B. über nur ein mobiles Smartphone für beide

Kommunikationsstrecken nicht zulässig ist und daher in den aktuellen Kundenbedingungen explizit ausgeschlossen wird.

Die Auftragsabwicklung geschieht bei mobileTAN wie bei den anderen PC-basierten TAN-Verfahren. Zusätzlich zur Spiegelung der Auftragsdaten am PC-Bildschirm des Kunden wird eine SMS an die mit dem Kunden vereinbarte Handynummer gesendet, die außer den kritischen Auftragsdaten wie z. B. Betrag und Empfängerdaten auch die zentral ermittelte TAN für diesen Auftrag enthält. Der Kunde kann diese nach sorgfältiger Prüfung gegen die Originaldaten am Beleg am PC eingeben und damit den Auftrag freigeben.

Auch die Restrisiken des mobileTAN-Verfahrens sind aus technischer Sicht vernachlässigbar, wenn die Rahmenbedingungen für die Kanaltrennung eingehalten werden. Somit steht auch für diese Kundengruppe ein geeignetes und sicheres Online-Banking-Sicherheitsverfahren zur Verfügung.