

Clemens Engelke *

Ernst Stahl **

Electronic Banking: Spagat zwischen Sicherheit und Mobilität

Bankkunden wollen bei der Abwicklung ihrer Online-Geschäfte möglichst mobil sein. Wie die Studie „Bankpräferenzen“ der PPI AG zeigt, will jeder zweite Kontoinhaber uneingeschränkt über verschiedene PCs auf seine Bankdaten zugreifen

können – ohne Abstriche bei der Sicherheit in Kauf nehmen zu müssen [PPI 2008]. Dieser Wunsch nach Mobilität und Sicherheit bietet den deutschen Kreditinstituten Anknüpfungspunkte zur Kundengewinnung und -bindung. Den Manipulationsschutz beim mobilen Einsatz des E-Bankings zählen deshalb drei Viertel der E-Banking-Verantwortlichen bei Kreditinstituten zu den größten zukünftigen Herausforderungen. Als Folge sind neue Verfahren zur sicheren Authentifizierung gefragt. Das ergab die Expertenbefragung „Electronic Banking“ von PPI und ibi research [PPI/ibi 2008].

Rein wissensbasierte Authentifizierungsmethoden wie PIN und TAN geraten angesichts der Phishing- und Pharming-Problematik, die laut aktueller Kriminalstatistik im letzten Jahr erneut zugenommen hat, immer stärker in die Kritik. Die Banken sind daher gefordert, neue, sichere Authentifizierungsmethoden einzusetzen. Wie die E-Banking-Verantwortlichen bei deutschen Banken und Sparkassen die zukünftige Bedeutung unterschiedlicher Authentifizierungsmethoden einschätzen, zeigt die Expertenbefragung „Electronic Banking“ [PPI/ibi 2008].

Dem ZKA-TAN-Generator wird eine wichtige Rolle zukommen

Im Privatkunden-Segment stehen derzeit neue Authentifizierungsinstrumente in der Diskussion. 85 Prozent der befragten Experten prognostizieren beispielsweise dem TAN-Generator des Zentralen Kreditausschusses (ZKA) zukünftig eine wichtige Rolle [PPI / ibi 2008]. Er ist mobil und kann sowohl im Online Banking über den Browser

als auch im lokal installierten Kundenprodukt genutzt werden. Dabei werden die TANs über eine Verschlüsselungsanwendung, die sich auf dem Chip der EC-Karte befindet, erzeugt und im Banksystem nachgerechnet. Die generierten TANs erhalten einen individuellen Auftragsbezug und können nur einmalig verwendet werden. Es ist also nicht mehr möglich, einen Auftrag durch einen Virus oder Trojaner auf dem Kunden-PC so zu manipulieren, dass Zahlungen auf das Konto des Angreifers übertragen werden.

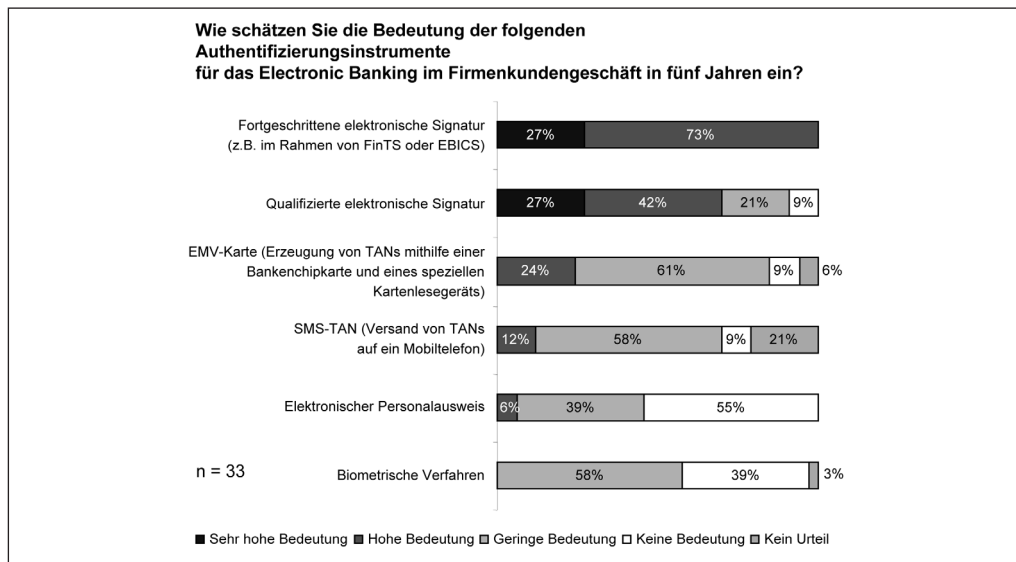
Eine besonders komfortable Variante des ZKA-TAN-Generators hat zusätzlich eine optische Schnittstelle. Der Kunde muss das Gerät nur vor eine flackernde Grafik auf dem Bildschirm halten und das Gerät scannt die Informationen zum Auftrag. Anschließend bestätigt der Kunde die Werte und schon wird die TAN berechnet.

* PPI AG

[clemens.engelke@ppi.de]

** ibi research an der Universität Regensburg GmbH
[ernst.stahl@ibi.de]

Abbildung 1:
Bedeutung der
Authentifizierungs-
instrumente für das
Electronic
Banking im
Firmenkunden
geschäft in
fünf Jahren
[Quelle: PPI /
ibi 2008]



Von Banken bevorzugt: fortgeschrittene elektronische Signatur

In den kommenden fünf Jahren kommt der fortgeschrittenen elektronischen Signatur unter den Authentifizierungsinstrumenten die größte Bedeutung zu (siehe Abbildung 1). Sie erfüllt die Kosten-Nutzen-Anforderungen, da keine Zertifikate erforderlich sind. Kunden ersetzen mit der fortgeschrittenen elektronischen Signatur auf digitalem Wege ihre eigenhändige Unterschrift.

Die fortgeschrittene elektronische Signatur wird beim Online Banking und bei lokal installierten Kundenprodukten neben dem TAN-Generator-Verfahren angeboten. Im Firmenkunden-Zahlungsverkehr über EBICS, bei dem besonders hohe Datenvolumina zur Bank eingereicht werden, wird in ganz Deutschland ausschließlich die fortgeschrittene Signatur eingesetzt.

Qualifizierte Signatur: Vom Kostenzwang ausgebremst?

Neben der fortgeschrittenen elektronischen Signatur rückt auch ihr „Upgrade“ – die qualifizierte Signatur – zunehmend in den Fokus der Top-Entscheider (siehe Abbildung). Sie beruht auf einem qualifizierten Zertifikat und wird zusätzlich mit einer sicheren Signaturerstellungseinheit (SSEE) erzeugt. Zwei von drei Experten schätzen

die Bedeutung für die Zukunft des Electronic Bankings hoch bis sehr hoch ein. Schließlich hätte sie für Firmenkunden viele attraktive Vorteile: Qualifizierte Signaturen könnten für Vertragsabschlüsse, die elektronische Rechnungsstellung und die Kommunikation mit den Bundesbehörden genutzt werden.

Für eine flächendeckende Verbreitung gilt es jedoch noch einige infrastrukturelle Hürden zu überwinden und eine dem Kundenwunsch angemessene Kostenpolitik zu etablieren. Die Zertifikate, die bei der qualifizierten Signatur erforderlich sind, sind kostenpflichtig und können nur von zugelassenen Trust Centern ausgegeben werden.

Bei der Verbreitung von fortgeschrittenen Zertifikaten kann EBICS immerhin zukünftig eine Schlüsselrolle einnehmen: Ende des Jahres wird Frankreich ein erweitertes EBICS-Protokoll im Zahlungsverkehr mit Firmenkunden einführen und für die Übermittlung der Schlüssel Zertifikate benutzen. Verläuft die Einführung erfolgreich, wäre auch eine Adaptierung für Deutschland denkbar – vorausgesetzt, dass der Kostenzwang nicht die Verbreitung hemmt.

Secoder – Chipkartenleser mit Potenzial

Spricht man über sichere Verfahren für das Online Banking, darf man den Secoder nicht unerwähnt lassen. Dabei handelt es sich um einen Chipkartenleser, der über betriebssystemspezifische Erweiterungen verfügt. Er zeigt auf seinem Display die Daten, die von einem Banksystem gesendet werden. Per Tastendruck kann der Kunde diese Textnachrichten bestätigen. Unter Verwendung der eingelegten Chipkarte erzeugt der Secoder intern eine kundenindividuelle Signatur passend zu den Textnachrichten des Banksystems.

Das Banksystem kann dann prüfen, ob der gesendete Text korrekt vom Kunden signiert wurde. Nach derzeitiger Einschätzung ist der Secoder das sicherste Verfahren. Da er aber nur im abgeschlossenen Modus am PC betrieben werden kann, sind der Mobilität heute noch Grenzen gesetzt. Mobile Lösungen des Secoders befinden sich jedoch bereits in Vorbereitung.

Mobile Kundenprodukte bieten hohe E-Banking-Sicherheit

Lokal installierte Kundenprodukte, die auf dem HBCI/FinTS-Protokoll basieren, haben in Deutschland mittlerweile eine mehr als zehnjähri-

ge Tradition als sicherer Bankzugang. Erstaunlicherweise ist das Vertrauen in die HBCI/FinTS-basierten Kundenprodukte niedriger als in das browserbasierte Online Banking: Der Studie „Bankpräferenzen“ zufolge halten 73 Prozent der Kunden Online Banking über die Bankinternetseite für sicherer als Finanzgeschäfte über lokal installierte Kundenprodukte [PPI 2008]. Dabei sind Angriffe auf HBCI-Kundenprodukte kaum bekannt, was zeigt, dass Aufklärung in diesem Bereich dringend notwendig ist.

HBCI-Kundenprodukte, die ein wesentlich sicheres Online Banking ermöglichen und wie der ZKA-TAN-Generator auch mobil einsetzbar sind, können aus heutiger Sicht den Königsweg zur gleichzeitigen Erfüllung der Mobilitäts- und Sicherheitsanforderungen darstellen.

Literatur

PPI (2008). Bankpräferenzen 2008. Studie von PPI in Kooperation mit dem IMWF Institut für Management- und Wirtschaftsforschung und Handelsblatt.com.

PPI / ibi (2008). Electronic Banking 2008 – Delphi-Expertenbefragung zu Trends und zukünftigen Anforderungen im Firmenkundengeschäft. Regensburg.

Informationen zur Studie Electronic Banking 2008:

Delphi-Expertenbefragung zu Trends und zukünftigen Anforderungen im Firmenkundengeschäft

Oktober 2008

99 Seiten, 37 Abbildungen, 11 Tabellen

ISBN: 978-3-940416-03-2

Weitere Informationen unter www.ibi.de/ebanking

