

# Wie sicher ist Online-Banking?

Ein Überblick und aktuelle  
Handlungsempfehlungen

Stand: Mittwoch, 10.11.2010



- Aus der Abteilung „Los geht's!“ -

# Vorstellung und Überblick



## Dürfen wir uns vorstellen?

- Die Antago GmbH ist ein europaweit tätiges Unternehmen im Bereich der IT- und Informationssicherheit. Wir sorgen für die strukturierte, bedarfsorientierte Absicherung Ihrer Informationen.
- Unabhängig, kompetent und fair erhalten Sie von uns:
  - ✓ Security Scans von Systemen, Netzen und Applikationen  
Wenn Sie wissen wollen, wie ein Angreifer Ihre IT sieht.
  - ✓ Audits – Kompakt bis hin zu ISO 27001  
Wenn Sie sicher sein wollen, dass Ihre Informationen auch morgen sicher sind.
  - ✓ IT-Forensic  
Gerichtsfeste Beweissicherung und Untersuchungen von IT-Sicherheitsvorfällen.
  - ✓ Analyse und Erarbeiten von Sicherheitskonzepten  
Strukturierte Absicherung Ihrer IT – bedarfsgerechter Schutz für Informationen.
  - ✓ Livehackings, Schulungen und Mitarbeitersensibilisierungen  
Know-How aus erster Hand.





Wir sind KEIN...

### ...Systemhaus

- Wir haben kein Interesse daran, Ihnen Hard- oder Software zu verkaufen.

### ...Reseller/Integrator

- Wir sind unabhängig von Herstellern.

### ...fremdfinanziertes Unternehmen

- Wir sind unabhängig von Geldgebern.

### ...Tochterunternehmen

- Wir sind an keinen Konzern gebunden.



## Was erfahren Sie hier?

- Der Vortrag gliedert sich in folgende Teile:
  - ✓ Grundlagen
    - Die Ziele des Angreifers
    - Welche Angriffe gibt es heute?
    - Forderungen an sicheres Online-Banking
  - ✓ Gängige Verfahren fürs Online-Banking  
(Wie funktionieren sie und wie sicher sind sie?)
    - PIN und TAN
    - PIN und iTAN
    - HBCI mit Chipkarte
    - TAN via SMS (SMS-TAN)
- Es gibt natürlich weitere Verfahren, mit denen Online-Banking abgesichert werden kann. Diese werden hier jedoch (noch) nicht besprochen (es sind schon jetzt 47 Slides...).



EF61 A4D4 19C9 C9B0 E89B 7F8D CF85 7D99 117D 8595

- Aus der Abteilung „Grundsätzliches“ -  
**Die Ziele des Angreifers**

## Warum wird Online-Banking angegriffen?

- Beim Online-Banking geht es um viel, viel Geld: diese Infrastruktur wird von Millionen Benutzern verwendet und es werden in ihr Abermillionen kritischer Daten Tag für Tag ausgetauscht.
- Die Aussichten sind deshalb für Angreifer viel versprechend: Hier kann ein Krimineller schnell viel Geld verdienen.
- Betrüger nehmen hohe Aufwände bzw. Anlaufinvestitionen in Kauf, um Online-Banking anzugreifen, weil es sich einfach lohnt!
- Nicht zuletzt: die Masse macht's!  
Auch wenn ein Angriff in nur 0,05% aller Fälle erfolgreich ist, so kann er sich doch lohnen, wenn er nur oft genug durchgeführt wird.

## Wann hat ein Angreifer gewonnen?

- Heute gibt es eine Vielzahl von Angriffen gegen Online-Banking.
- Alle Angriffe lassen sich in zwei Kategorien unterteilen:

### **X** Informationsdiebstahl

Der Angreifer klaut Informationen, um anschließend im Namen des Benutzers betrügerische Bankgeschäfte durchzuführen.

### **X** Transaktionsmanipulation

Der Angreifer schiebt dem Benutzer betrügerische Transaktionen unter, die dieser (unwissentlich) legitimiert.

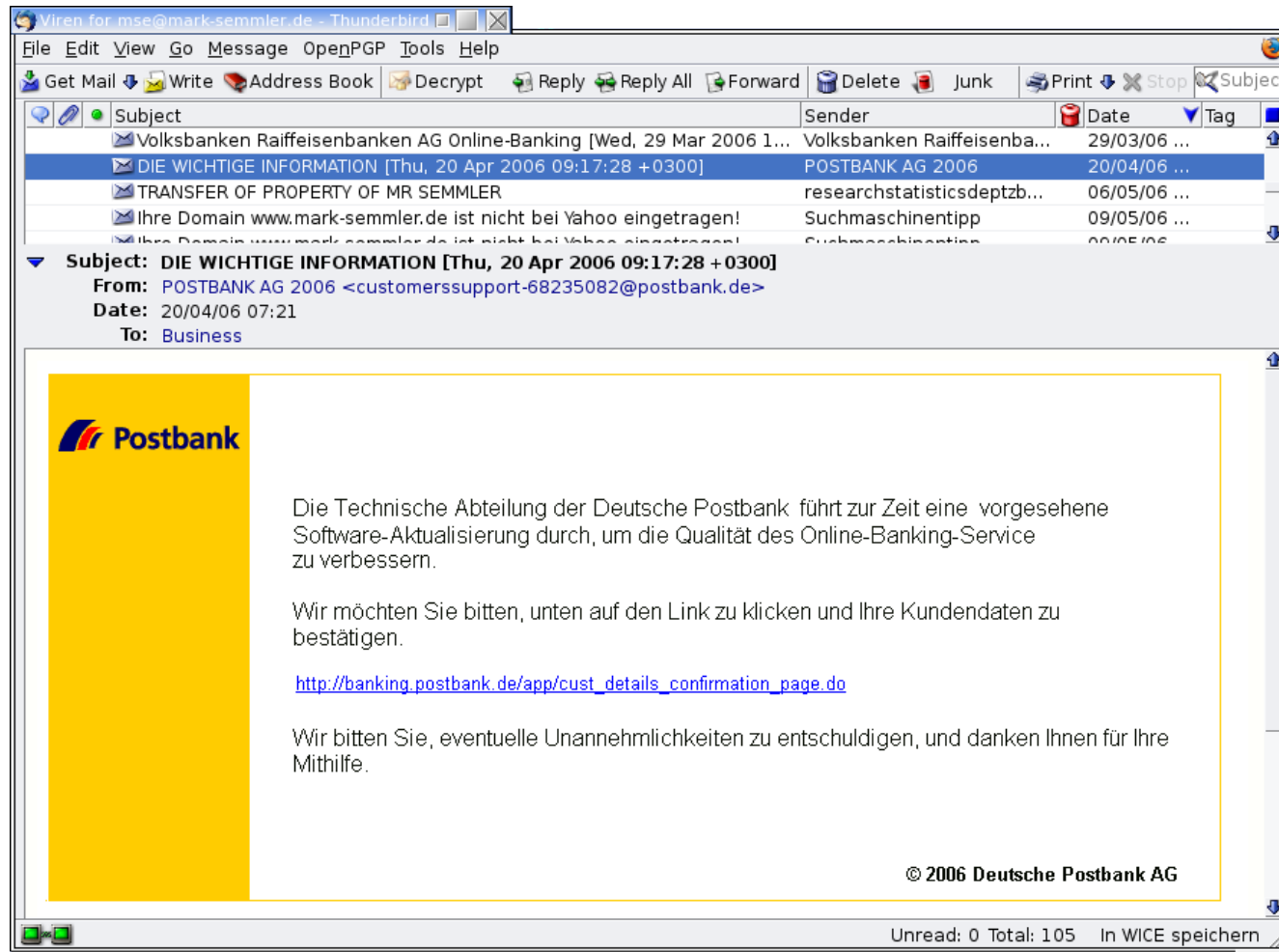


- Aus der Abteilung „Monster im Wald“ -  
**Welche Angriffe gibt es heute?**

## Phishing: Erschleichen von PIN und TAN

- Der Angreifer versendet Mails mit dem Layout einer Bank.
- Inhalt der Mail:  
“Rufen Sie diese Webseite auf und geben Sie dort Ihre Kontendaten ein!”  
sowie eine abenteuerliche Begründung, warum man das tun sollte.
- Die in der Mail angegebene Webseite ist eine nahezu identische Kopie des Internetauftritts der Bank. Hier soll das Opfer nun seine Kontonummer, seine PIN und eine bzw. mehrere TANs eingeben.
- Der Betrüger nutzt die erschlichenen Informationen, um per Online-Banking das Konto des Opfers zu plündern.
- Ähnliches funktioniert natürlich auch mit ebay, paypal oder anderen Zugängen (auch Mailkonten werden vermehrt so angegriffen!)

# Phishing: Hier eine Phishing-Mail...



EF81 4904 1909 C980 C898 7F80 CF85 7093 1170 8935

# Phishing: ...und die dazugehörige Webseite



The screenshot shows a browser window with a phishing website designed to look like the Postbank homepage. The browser's address bar shows 'Postbank - Leistung ohne Umwege - Mozilla Firefox'. The website layout includes a top navigation bar with 'Sitemap', 'Kontakt', 'FAQ', and 'Hilfe'. A search bar is present on the right. The main content area features a 'Sehr geehrter Kunde,' greeting and a warning about security updates. A login form is visible with fields for Name, Familienname, Telefon-Nr., Kontonummer, PIN, TAN, and Geheimfrage. The right sidebar contains a 'Vorsicht vor Betrügern!' warning, a 'Postbank Newsletter' subscription form, and a 'Postbank ist nationaler Förderer der FIFA WM 2006™' logo.

EFB1 AFD1 19C9 C8B0 28B8 7F8D CF85 1093 117D 8535

## Aktuelle Attacken: Schadsoftware

- Phishing ist relativ ineffizient – vor allem weil mehr und mehr Banken Verfahren nutzen, die mit Phishing nicht mehr (oder nur noch sehr schwer) anzugreifen sind.
- Die Angreifer haben deshalb – z.T. sehr komplexe! - Schadsoftware entwickelt, die verschiedene Arten von Online-Banking-Verfahren angreifen kann. Es ist mittlerweile eine ganze Familie dieser Schädlinge bekannt (z.B. die Win32.Banker-Familie).
- Die Schadsoftware arbeitet auf dem Rechner des Opfers und kann deshalb sehr effektiv Informationsdiebstahl und Transaktionsmanipulation durchführen!
- Sie kann z.B. Tastatureingaben belauschen (Keylogger), die Bildschirmausgaben protokollieren oder beliebig ändern, die Kommunikation zwischen Kunde und Bank umleiten, unterbrechen oder manipulieren und vieles, vieles mehr...

- Aus der Abteilung „Das. Will. Ich. Haben!!!“ -

# Forderungen an sicheres Online-Banking

## Unsere Forderungen an Online-Banking!

- Authentizität der Geschäftspartner:  
Der Kunde muss ganz sicher sein, dass er wirklich mit seiner Bank spricht - sonst landet er z.B. auf der Webseite des Angreifers!
- Transparenz der Transaktion:  
Der Kunde muss fälschungssicher sehen können, welche Transaktion er gerade legitimiert - sonst kann ihm der Angreifer eine falsche Transaktion unterschieben!
- Integrität der Transaktion:  
Die Transaktion muss so bei der Bank ankommen, wie der Kunde sie weggeschickt hat – sonst kann der Angreifer sie auf dem Weg zur Bank fälschen!
- All das muss selbst dann gewährleistet sein, wenn der Computer des Kunden komplett unter der Kontrolle des Angreifers steht.
- ...und alles muss bitte völlig narrensicher und einfach zu bedienen sein!



- Aus der Abteilung „Gute (?) alte (!) Zeit“ -

# Online-Banking mit PIN & TAN



## Wie funktioniert?

- Das Online-Banking via PIN und TAN wird über den Browser des Kunden abgewickelt.
- Die Bank übersendet dem Kunden dazu eine PIN und eine Liste von TANs.
- Der Kunde loggt sich mit seiner PIN (PIN = Persönliche Identifikationsnummer) auf der Webseite der Bank ein und legitimiert jede finanzielle Transaktion mit einer TAN (TAN = Transaktionsnummer), die danach ungültig ist (Einmal-Gebrauch).





## Wie sicher ist Online-Banking mit PIN und TAN?

- Das Online-Banking via PIN und TAN gilt heute als unsicher. Warum?
- Problem: Informationsdiebstahl  
Die Authentizität der Geschäftspartner hängt von der Geheimhaltung von PIN und TAN ab. Gibt der Kunde nicht acht, so kann er auf gefälschte Webseiten umgeleitet werden und dem Angreifer unwissentlich PIN und TAN übergeben (Phishing, Pharming). Wird die PIN und eine (beliebige) TAN vom Angreifer geklaut, kann dieser sich bei der Bank als legitimer Kunde ausgeben und das Konto plündern.
- Problem: Transaktionsmanipulation  
Die Integrität und Transparenz der Transaktionen ist bei PIN und TAN nicht sicher gestellt. Schadsoftware auf dem Computer des Kunden kann Transaktionsdaten auf dem Weg zur Bank fälschen. Der Benutzer legitimiert dann unwissentlich die gefälschte Transaktion durch die Eingabe einer TAN.



EF61 A4D4 19C9 C9B0 289B 7F8D CF85 7D93 117D 8535

- Aus der Abteilung „Stahlwollschaf“ -  
**Sicherheit für PIN & TAN**



## Grundsätzliches beim Einsatz von PIN & TAN (I)

- Gehen Sie verantwortungsvoll mit Ihrer PIN um!
- Geben Sie Ihre PIN ausschließlich beim Einloggen auf der Webseite des Online-Bankings ein. Geben Sie Ihre PIN niemals am Telefon, in Briefen, im persönlichen Gespräch oder im bei anderer Gelegenheit im Internet an Dritte weiter – egal wie gut das Argument Ihres Gegenübers ist oder mit wem auch immer Sie glauben, zu reden!
- Niemand, wirklich absolut niemand (außer die Webseite des Online-Bankings) hat ein berechtigtes Interesse an Ihrer PIN. Auch nicht der nette Bankangestellte, Polizist oder Kundenberater. Absolut niemand!
- Schreiben Sie Ihre PIN nicht auf und speichern Sie Ihre PIN nirgends ab (z.B. auch nicht in Ihrem Handy).



## Grundsätzliches beim Einsatz von PIN & TAN (II)

- Gehen Sie verantwortungsvoll mit Ihren TANs um!
- Geben Sie Ihre TANs ausschließlich auf der Webseite des Online-Banking ein. Geben Sie eine TAN niemals am Telefon, in Briefen, im persönlichen Gespräch oder im bei anderer Gelegenheit (z.B. im Internet) an Dritte weiter – egal wie gut das Argument Ihres Gegenübers ist oder mit wem auch immer Sie glauben, zu reden!
- Niemand, wirklich absolut niemand außer die Webseite des Online-Bankings hat ein berechtigtes Interesse an Ihrer TAN. Auch nicht der nette Bankangestellte, Polizist oder Kundenberater. Niemand!
- Speichern Sie Ihre TANs in keinem Computersystem ab - auch nicht in Ihrem Handy, Ihrem Laptop oder Ihrem PDA, MDA, iphone, Blackberry, ...!
- Wenn Sie Ihre PIN irgendwo aufgeschrieben haben (das sollten Sie nicht!): heben Sie PIN und TAN unbedingt getrennt voneinander auf.

## Grundsätzliches beim Einsatz von PIN & TAN (III)

- Sichern Sie Ihren Rechner ab – Implementieren Sie die wichtigsten Grundschutzmaßnahmen wie z.B.:
  - ✓ Regelmäßige Backups durchführen!
  - ✓ Automatischen Windows-Updates einschalten!
  - ✓ Regelmäßige Aktualisierung von sonstiger Software (z.B. des Adobe Acrobat Readers) durchführen!
  - ✓ Anti-Virus installieren, aktuell halten und permanent im Hintergrund mitlaufen lassen!
  - ✓ Lokale Firewall einschalten bzw. installieren!
  - ✓ Gute Passwörter wählen!
  - ✓ ...
- Wer hier mehr wissen möchte, schaut in den Vortrag „So viel Schutz muss sein!“ (kostenfrei auf unserer Webseite <https://www.antago.info> erhältlich).



## Grundsätzliches beim Einsatz von PIN & TAN (IV)

- Sichern Sie Ihren Webbrowser ausreichend ab!
- Die Browser-Sicherheit kann hier nicht erschöpfend behandelt werden. Deshalb hier nur einige kurze Hinweise.
  - ✓ Verwenden Sie einen aktuellen Browser, der über sämtliche Updates verfügt.
  - ✓ Wechseln Sie den Internet-Explorer gegen einen alternativen Browser (z.B. Firefox oder Opera). Wenn Sie den den Internet Explorer verwenden möchten oder müssen, dann bitte nur in der aktuellsten Version (Internet Explorer 8).
  - ✓ Installieren Sie zusätzliche Add-Ons für den Firefox-Browser, wie z.B. „NoScript“, um Ihre Sicherheit weiter zu erhöhen.
  - ✓ Löschen Sie nach dem Online-Banking den lokalen Cache des Browsers (geht bei Firefox z.B. beim Beenden auch automatisch).





## Grundsätzliches beim Einsatz von PIN & TAN (V)

- Vergewissern Sie sich, dass Sie tatsächlich auf der Webseite des Online-Bankings Ihrer Bank gelandet sind. Ihr Browser gibt Ihnen hier ganz eindeutig Auskunft:
  - ✓ Die Adresse muss mit dem Begriff „https://“ beginnen (wichtig ist das „s“).
  - ✓ Der Verbindungsaufbau muss fehlerfrei geschehen sein. Meldungen wie „Das Zertifikat ist nicht vertrauenswürdig!“ oder „Die Authentizität des Zertifikats kann nicht geprüft werden!“ bedeuten, dass Sie angegriffen werden.
  - ✓ Neben der Adresszeile muss ein geschlossenes Schloss zu sehen sein.
  - ✓ Die Adresszeile muss golden oder grün hinterlegt sein.
- Wenn auch nur eine der oben genannten Bedingungen nicht erfüllt ist: WEG HIER! Irgendetwas stimmt nicht!





## Abschließend ein sehr offenes Wort...

- Vergessen Sie PIN und TAN! Es existieren Angriffe, die dieses System überwinden. Wechseln Sie auf ein anderes Verfahren.
- Wenn dies nicht möglich ist:
  - ✓ Begrenzen Sie bei Ihrer Bank das Limit für Online-Überweisungen pro Tag und Woche.
  - ✓ Lassen Sie sich von Ihrer Bank eine Haftungsübernahme bestätigen: Die Bank soll für alle eventuellen Schäden haften.
  - ✓ Kontrollieren Sie Ihre Kontoauszüge zeitnah.
  - ✓ Besser: Verlassen Sie Ihre rückständige Bank und gehen Sie zu einem modernen Geldinstitut!



- Aus der Abteilung „Gammel bleibt Gammel“ -  
**Das iTAN-Verfahren**



## Wie funktioniert?

- Online-Banking mit PIN und iTAN funktioniert genau so wie Online-Banking mit PIN und TAN.
- Im Vergleich mit PIN und TAN hat sich nur eines geändert: Die TANs sind nun nummeriert (iTAN = Indiziertes TAN) und die Bank fordert bei jeder Transaktion die Eingabe einer spezifischen TAN.





## Welche Vorteile bringt's?

- Das iTAN-Verfahren ist als Maßnahme gegen Phishing entwickelt worden.
- Ein Angreifer muss sowohl die PIN als auch die gesamten (noch gültigen) TANs eines Opfers kennen, um mit Sicherheit eine Transaktion durchführen zu können.
- Über normales Phishing kann man nur sehr wenige Opfer dazu bringen, eine gesamte iTAN-Liste einzugeben.
- Besitzt ein Angreifer nur eine iTAN des Opfers, so reduziert sich die Wahrscheinlichkeit eines erfolgreichen Angriffs sehr deutlich.





## Welche Nachteile hat's?

- Der Benutzer muss die gesamte iTAN-Liste mit sich führen, wenn er (z.B. von unterwegs oder im Urlaub) Bankgeschäfte durchführen möchte.
- iTAN-Listen werden deshalb häufig in elektronische Medien (Handy, PDA, Blackberry, Laptop, ...) übertragen. Wenn auf diesen Geräten auch noch die PIN gespeichert ist, ist nach dem Diebstahl des Gerätes das Konto leer...





## Wie sicher ist Online-Banking mit PIN und iTAN?

- Das Online-Banking via PIN und iTAN ist heute unangemessen unsicher. Das iTAN-Verfahren schützt zwar recht gut gegen Phishing. Gegen Schadsoftware hat es keine Chance.
- Problem: Informationsdiebstahl  
Informationsdiebstahl wird bei iTAN nur wesentlich erschwert, nicht aber wirkungsvoll verhindert.
- Problem: Transaktionsmanipulation  
Die Integrität und Transparenz der Transaktionen ist bei PIN und iTAN nicht sicher gestellt. Schadsoftware auf dem Computer des Kunden kann Transaktionsdaten auf dem Weg zur Bank fälschen. Der Benutzer legitimiert dann unwissentlich die gefälschte Transaktion durch die Eingabe der geforderten iTAN.





EF81 A4D4 19C9 C9B0 E89B 7F8D CF85 7D99 117D 8595

- Aus der Abteilung „Stahlwollschaf+“ -  
**Sicherheit mit PIN & iTAN**



## Schutz für das iTAN-Verfahren

- Prinzipiell gelten alle Sicherheitsmaßnahmen wie beim Gebrauch von PIN und TAN.
- Zusätzlich gilt:  
Übertragen Sie iTAN-Listen niemals in mobile Endgeräte (Handy, PDA, iPhone, ...).





## Auch hier ein offenes Wort

- Das iTAN-Verfahren stellt für Kriminelle kein Problem mehr dar, erklärte Mirko Manske, Kriminalhauptkommissar im Bundeskriminalamt (BKA) auf dem 11. IT-Sicherheitskongress des Bundesamts für Sicherheit in der Informationstechnik in Bonn. Zwar seien Phishing-Angriffe mit iTAN schwieriger geworden, so Manske "aber nicht unmöglich".
- Bereits Ende 2005 hatte eine Arbeitsgruppe der Ruhr-Universität Bochum einen Angriff auf das Online-Banking Verfahren mit indizierten TANs erfolgreich demonstriert.
- Anfang 2007 tauchten dann erste Phishing-Kits auf, die in der Lage waren, per Man-in-the-Middle-Attacke abgephischte iTANs in Echtzeit für eigene Transaktionen zu benutzen.
- Quelle: heise online vom 18.05.2009



EF81 A4D4 19C9 C9B0 E89B 7F8D CF85 7D99 117D 8595

- Aus der Abteilung „Elektronisches Fort?“ -  
**HBCI mit Chipkarte**

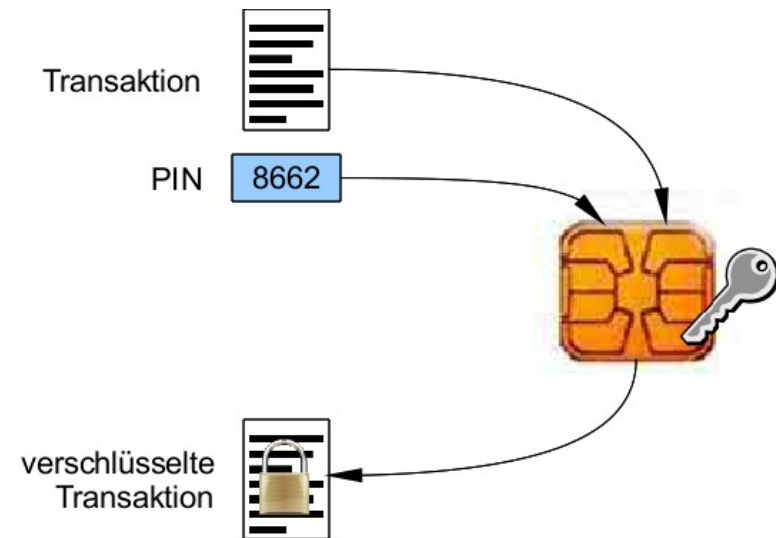


## HBCI: Was ist's?

- HBCI steht für Home Banking Computer Interface. Es ist ein offener Standard für Homebanking, der verschiedene Arten von Online-Banking Verfahren unterstützt (unter anderem auch PIN und TAN!).
- HBCI mit PIN und TAN lassen wir hier außen vor. Hier gelten genau die gleichen Einschränkungen wie bei PIN und TAN ohne HBCI.  
**Nicht verwenden!**
- Ebenfalls außen vor: HBCI mit Schlüssel auf Diskette.  
**Nicht verwenden!.**
- Aktuelles HBCI arbeitet mit Kartenleser und Chipkarte.

## HBCL mit Chipkarte: Wie funktioniert?

- HBCL arbeitet mit einem Kartenleser und eine Chipkarte.
- Auf der Chipkarte ist ein Schlüssel sicher gespeichert - der Schlüssel kann die Chipkarte nicht verlassen.
- Wenn eine Überweisung Der Kunde übergibt die Transaktion der Chipkarte und muss sich bei ihr mit einer PIN-Nummer ausweisen.
- Bei Eingabe der richtigen PIN wird die Transaktion von der Chipkarte so verschlüsselt, dass nur noch die Bank sie entschlüsseln kann.
- Die verschlüsselte Transaktion wird an die Bank gesandt.
- Liebe Experten: Ich weiß - diese Darstellung ist stark vereinfacht. Nicht böse sein!





## Welche Vorteile bringt HBCI mit Chipkarte?

- Absicherung gegen Informationsdiebstahl:  
Es werden keine TANs mehr verwendet - die Transaktion wird von der Chipkarte verschlüsselt. Es muss aber sicher gestellt sein, dass die PIN der Karte geheim bleibt (die richtige PIN bringt die Karte ja dazu, Überweisungen zu legitimieren).
- Absicherung gegen Transaktionsmanipulation:  
Die Überweisung kann nicht unbemerkt manipuliert werden, wenn sie einmal verschlüsselt wurde. Es muss aber sicher gestellt sein, dass die Chipkarte die richtige Transaktion erhält.
- Ein Angreifer muss die PIN kennen und zugleich Zugriff auf den die Chipkarte besitzen, um illegale Transaktionen durchführen zu können – oder er muss in der Lage sein, eine gefälschte Transaktion zur Chipkarte zu senden und den Benutzer dazu bringen, seine PIN einzugeben.



## HBCI mit Klasse-1-Kartenleser: Igitt!

- Wie sicher HBCI mit Chipkarte ist, hängt stark vom Kartenleser ab, der eingesetzt wird
- Absolut unsicher: „Dummer Chipkartenleser“ (Klasse-1-Kartenleser)!
- Eine Schadsoftware kann die PIN des Benutzers ausspähen (die Eingabe der PIN erfolgt ja über die Tastatur des Rechners!) und dann der Chipkarte beliebige Transaktionen zur Legitimierung vorlegen.



## HBCL mit Klasse-2-Kartenleser: gut, nicht optimal

- Klasse-2-Kartenleser besitzen eine eigene Tastatur. Eingaben auf dieser Tastatur werden nur vom Kartenleser verarbeitet - es besteht keine Möglichkeit, die Tastatureingaben vom angeschlossenen Computer aus mitzulesen: Schadsoftware auf dem Computer des Kunden kann die PIN der Chipkarte nicht ausspähen.
- Ein letztes (kleines) Schlupfloch bleibt aber: Eine Schadsoftware kann die originale Transaktion abfangen, bevor die das Lesegerät erreicht und gegen eine illegale Transaktion ersetzen.
- Das Problem bei Klasse-2-Kartenlesern: Der Benutzer sieht bei diesem Kartenleser nicht, welche Transaktion er legitimiert...



## HBCL mit Klasse-3-Kartenleser: Super sicher!

- Kartenleser der Klasse 3 zeichnen sich dadurch aus, dass sie eine autonome Tastatur und ein autonomes Display besitzen.
- Das Display kann unabhängig vom PC betrieben werden und zeigt z.B. genau an, welche Transaktion der Benutzer durch die Eingabe seiner PIN legitimiert.
- Wichtig:  
Die Online-Banking-Software muss Klasse-3-Geräte voll unterstützen und die Features des Geräts auch nutzen!





## Welche Nachteile hat HBCI mit Kartenleser?

- Der Kartenleser kostet Geld (die Banken sind plötzlich taub, wenn man als Kunde den Kartenleser umsonst bekommen möchte...).
- Der Benutzer muss den Chipkartenleser und ggf. spezielle Software mit sich führen, um Online-Banking nutzen zu können (versuchen Sie mal im Urlaub einen Kartenleser im Internetcafe vor Ort zum Laufen zu bekommen...).





- Aus der Abteilung „Sichere Pfade“ -

# TAN via SMS

(auch mobileTAN, SMS-TAN oder mTAN genannt)



## Was ist's und wie funktioniert's?

- Der Kunde benutzt Online-Banking mit seinem Browser. Nachdem er die Transaktion abgeschickt hat, übermittelt ihm die Bank innerhalb weniger Sekunden eine TAN per SMS auf sein Handy (daher auch der Name)
- Die TAN ist ausschließlich für diese spezielle Transaktion gültig. Sie verfällt nach wenigen Minuten.
- In der SMS wird nicht nur die TAN übertragen, sondern auch die Transaktion noch einmal zusammengefasst („Ihre TAN für die Überweisung von EUR 35,95 an das Konto 54545408 lautet: CF44GB)“.





## Welche Vorteile bringt's?

- Absicherung gegen Informationsdiebstahl:  
Die TAN wird für jede Transaktion individuell erstellt und auf einem sicheren Kanal übertragen (GSM-Netz) – Schadsoftware kann die TAN nicht manipulieren oder missbrauchen.
- Absicherung gegen Transaktionsmanipulation:  
Die Transaktion kann nicht unbemerkt manipuliert werden, da die wichtigsten Daten noch einmal in der (sicher übertragenen) SMS enthalten sind.
- Um Geld zu stehlen muss also ein Angreifer die PIN für das Online-Banking kennen und darüber hinaus im Besitz des (betriebsbereiten) Handy's des Kunden sein. Beides in Kombination ist sehr unwahrscheinlich (der Verlust des Handy's wird meistens schneller als den Verlust der Geldbörse bemerkt...).
- Last but not least: Der Benutzer bleibt mobil. Es wird keine zusätzliche Hardware, keine spezielle Software oder gar TAN-Listen benötigt.



## Wie sicher ist SMS-TAN nun wirklich?

- Aktuell zählt SMS-TAN zu den sehr, sehr sicheren Verfahrenen.
- Das Verfahren ist dann gebrochen, wenn es dem Angreifer gelingt...
  - x ...das Handy des Benutzers unter seine Kontrolle zu bringen
  - x ...die Übertragung von SMS im Mobilfunknetz zu stören und/oder zu manipulieren
  - x ...in die Infrastruktur der Betreiber des Mobilfunks einzubrechen oder
  - x ...den Benutzer zu täuschen
- Die dunkle Seite beginnt gerade damit, sich dem Thema zu widmen. Da es viele Angriffspunkte gibt (Handy's werden immer intelligenter und damit auch anfälliger gegen Schadsoftware; die im GSM-Netz verwendeten Techniken und Protokolle sind sehr alt; die IT-Infrastruktur der Netzbetreiber ist komplex; ...) und es um viel Geld geht, werden wir in Zukunft wohl mit verfeinerten Angriffen konfrontiert werden.



## Leichteste Beute beim SMS-TAN: der Benutzer!

- Aktuell sind die ersten Exemplare einer Schadsoftware aufgetaucht, die den Benutzer von SMS-TAN dazu auffordert, mit seinem Handy eine bestimmte Webseite anzufurten, um von dort eine „zusätzliche Sicherheitssoftware“ zu installieren. Dabei handelt es sich natürlich um weitere Schadsoftware, die die SMS-TANs auf dem Handy manipuliert.
- Denkbar sind auch Angriffe sehen, bei denen der Benutzer nach einer Transaktion nicht nur die SMS-TAN von seiner Bank, sondern kurz danach eine weitere SMS der Angreifer erhält:
  - SMS-TAN der Bank: „Ihre TAN für die Überweisung von EUR 2500,00 an das Konto 14532761 lautet: D5F12M“
  - Kurz darauf die SMS der Angreifer: „Die Überweisungsdaten wurden in der letzten SMS leider falsch eingetragen. Wir bitten dies zu entschuldigen. Die richtigen Daten der Überweisung lauten: EUR 35,50 an das Konto 54545408. Bitte verwenden Sie die soeben von uns erhaltene TAN – Ihre Bank.“
- Wie viele Kunden werden wohl drauf reinfallen...? Au weia!



EF61 A4D4 19C9 C9B0 E89B 7F8D CF85 7D99 117D 8595

- Aus der Abteilung „Fazit“ -  
**Kommen wir zum Ende**



## Welche Verfahren sind also empfehlenswert?

- Von den hier vorgestellten Verfahren ist HBCI mit einem voll unterstützten Klasse-3-Kartenleser oder SMS-TAN empfehlenswert.  
Beide Verfahren gelten aktuell als sehr sicher.
- Bei PIN und TAN, PIN und iTAN sowie HBCI mit gammeligen Kartenlesern ist Vorsicht angebracht...
- ...oder die Haftungsübernahme der Bank angesagt!
- Und bitte niemals das gesunde Misstrauen an der Garderobe abgeben!!!



# Vielen Dank für Ihre Aufmerksamkeit.

Bei Fragen stehen wir gerne zur Verfügung.  
Bis demnächst auf Ihrem Server.



