Display-TAN: Die Bankkarte als TAN-Generator

Von Bernd Borchert

Die Idee, die Bankkarte zum TAN-Generator zu machen, ist nicht neu. Sicherheits- und/oder Probleme in Sachen Nutzerfreundlichkeit haben jedoch dazu geführt, dass sich entsprechende Ansätze bislang nicht durchsetzen konnten. Das könnte mit der Bluetooth-basierten Display-TAN, die ein Spin-off der Universität Tübingen entwickelt hat, möglicherweise anders sein, so Bernd Borchert. Der Erfolg des Konzepts, das fürs Online-Banking ebenso eingesetzt werden kann wie für Internet-Payments, könnte aber von der Entwicklung bei App-TANs abhängen, die ganz ohne zweites Medium neben dem Smartphone auskommen, räumt Borchert ein. Red.

Smartcards, die ein kleines Display haben und die dennoch so dünn und flexibel sind wie übliche Bankkarten, gibt es seit etwa 2006. Starre, dickere Vorgänger gab es schon vor dem Jahr 2000. Die Anwendung dieser Karten ist in den meisten Fällen die Anzeige eines One-Time-Passwords (OTP). So kann sich zum Beispiel ein Mitarbeiter auf seinem Mitarbeiter-Ausweis ein Einmalpasswort für den Zugang zum Firmen-Rechner generieren, ohne dass er ein weiteres Gerät dabei haben muss. Dass auf der Karte jedes Mal ein anderes, zufällig erscheinendes Einmalpasswort angezeigt wird, wird durch einen geheimen Seed auf der Karte garantiert, der zusammen mit einem internen Zähler („event-based") oder der Zeit einer Quarzuhr auf der Karte („time-based") als Input in eine Hash-Funktion eingeht, deren Output zum OTP verarbeitet wird.

Serverseitig wird ein OTP überprüft, indem dort die gleiche Hash-Funktions-Berechnung ausgeführt wird – der geheime Seed ist bekannt. Bei anlassbasierten OTPs muss der Server einkalkulieren, dass der Benutzer möglicherweise einige OTPs erzeugt hat, die nicht zum Server gelangt sind, und deshalb auch die OTPs mit etwas größeren Zählerwerten als nur dem aktuellen ausprobieren. Bei zeitbasierten OTPs muss er einkalkulieren, dass der Quarz auf der Karte nicht 100 Prozent genau ist, und dementsprechend kontinuierlich korrigieren.

Bankkarte als elektronische TAN-Liste

Die OTP-Displaykarten können auch als TAN-Generatoren für das Online-Banking eingesetzt werden. Die Bankkarte stellt also praktisch eine elektronische TAN-Liste dar. Der Vorteil ist, dass der Bankkunde nichts anderes braucht als seine Bankkarte, um eine TAN zu generieren. Das ist sicherer als eine i-TAN-Liste aus Papier, denn diese elektronische „Liste" kann nicht fotografiert werden. Auch Phishing-Angriffe sind schwieriger für Betrüger. Ein Beispiel für Time-Based-OTP-Displaykarten sind die aktuell in Umlauf kommenden 3-stelligen „dynamic CVV/CVC" Kreditkarten.

Für Online-Banking sind solche Displaykarten aber nicht sicher genug, denn es besteht die Gefahr von sogenannten Man-in-the-Middle-Angriffen. Ein solcher Angriff wird durchgeführt von einem Trojaner auf dem Endgerät, auf dem der Bankkunde das Online-Banking ausführt, sei es ein PC, Laptop, Tablet oder Smartphone: Der Bankkunde gibt eine Überweisung von X Euro an Empfänger Y ein. Der Trojaner gibt aber nicht diese Überweisung an den Bankserver weiter, sondern eine Betrugsüberweisung.

Die Bank empfängt die Betrugsüberweisung, kann sie aber nicht als solche erkennen und fragt nach der TAN für die Überweisung. Der Trojaner gibt die Anfrage auf dem Display des Endgeräts an den Bankkunden weiter, mit der gleichzeitigen Anzeige der Daten der vom Bankkunden eingegebenen Überweisung.

Der nichtsahnende Bankkunde erzeugt die TAN auf der Display-Karte, gibt sie in das

Zum Autor

Dr. Bernd Borchert, Wissenschaftlicher Mitarbeiter, Wilhelm-Schickard-Institut für Informatik, Universität Tübingen

Endgerät ein und der Trojaner gibt die TAN an den Bankserver weiter. Die Betrugsüberweisung wird vom Bankserver ausgeführt, denn für ihn sieht alles in Ordnung aus. Auch dem Kunden fällt vorerst nichts auf, denn der Trojaner hat ihm vorgespiegelt, dass seine und nicht die Betrugsüberweisung – ausgeführt wurde.

Für sicheres Online-Banking müssen also die Überweisungsdaten in die Erzeugung der TAN eingehen. In der neuen PSD2-Richtlinie wird das „dynamic linking" genannt (Par. 97(2).

Sicherheitsprobleme und/oder Mängel bei der Nutzerfreundlichkeit

Bei Display-Karten stellt sich damit die Frage: Wie kommen die Überweisungsdaten in die Karte?

Die erste Lösung etwa aus dem Jahr 2012 war es, durch 10 + 3 Tasten auf der Karte den Bankkunden die Ziffern der Überweisungsdaten in die Karte eintippen zu lassen. Diese „Mäuseklavier"-Lösung war ziemlich umständlich, sodass man schon wenig später dazu überging, diese 13-Tasten-Display-Karten mit einem zusätzlichen NFC-Funk-Zugang zu erweitern.

So konnten nicht nur die Überweisungsdaten per Funk übertragen werden, sondern die erzeugte TAN konnte auch per Funk zurück übertragen werden. Unterstützend kam dazu, dass zu der Zeit gerade viele neue Smartphones und Tablets mit der NFC-Technik ausgestattet wurden.

Praktisch gleichzeitig wurde auf der Cebit 2013 die Lösung „NFC-TAN" vorgestellt, die auf das Display und die Tasten verzichtet und nur per NFC die Überweisungsdaten auf die Karte überträgt, dort die TAN erzeugen lässt und sie per NFC sofort wieder zurückübertragen lässt. Die NFC-TAN-Lösung ist sehr benutzerfreundlich und extrem kostengünstig, vor allem für den Fall, dass die Bankkarten sowieso schon kontaktlos, das heißt, mit NFC ausgestattet, sind. Allerdings hat diese Lösung wegen des fehlenden Displays ein ähnliches Sicherheitsproblem mit Man-in-the-Middle-Trojanern auf dem Endgerät wie die OTP-Displaykarten-Lösung.

Beide NFC-Verfahren – mit und ohne Display – haben darüber hinaus noch das Problem, dass die Firma Apple die NFC-Schnittstelle auf ihren Tablets und Smartphones nicht für Apps freigibt, sodass i-Pads und i-Phones nicht als Endgeräte für die NFC-Verfahren zu nutzen sind. Alle bislang dargestellten Verfahren, die die Bankkarte zum TAN-Generator machen, haben also jeweils Sicherheits- und/oder Usability-Probleme, und/oder noch das Verbreitungs-Problem mit NFC. Tatsächlich gibt es auch nur wenige Banken, die eines dieser Verfahren implementiert haben.

Display-TAN soll die Probleme lösen

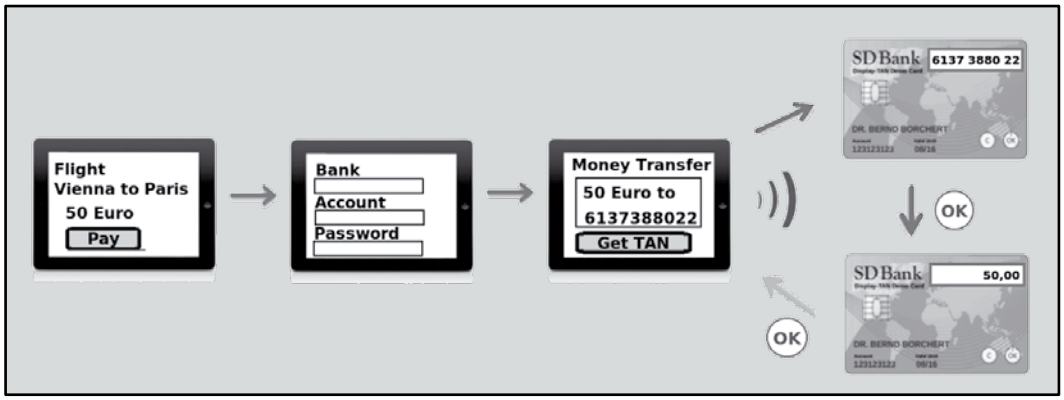
Das Verfahren „Display-TAN" hat den Anspruch, die dargestellten Probleme der beschriebenen Verfahren zu lösen. Die Display-TAN-Karte hat ein 10-Ziffern-Display und zwei Tasten sowie ein Modul für die Bluetooth Smart Funktechnik, auch Bluetooth Low Energy (BLE) genannt. Intern hat die Karte noch zusätzlich eine Flachbatterie, einen Prozessor, einen Speicher und einen Display-Controller. Mehr als die Hälfte der Kartenfläche im Karteninnern ist ausgefüllt mir der Display-TAN-Elektronik.

- Mit dem Display und der nochmaligen Anzeige der Überweisungsdaten erfüllt das Verfahren die Ansprüche für sicheres Online-Banking. Ein Man-in-the-Middle-Trojaner auf dem Endgerät wird an der Anzeige der tatsächlichen Überweisungsdaten auf der Karte scheitern – sofern der Bankkunde aufmerksam ist.

- Mit dem Verzicht auf die 10 + x Tasten für die Eingabe von Überweisungsdaten ist die notwendige Nutzerfreundlichkeit gegeben – die Überweisungsdaten werden grundsätzlich per Funk geschickt. Die zweite Taste C für „Cancel" ist vor allem aus rechtlichen Gründen auf der Karte: Mit ihr soll der Bankkunde eine Überweisung definiert abbrechen können, wenn etwas nicht in Ordnung ist.

- Bei der Wahl „NFC oder Bluetooth?" fiel die Auswahl auf Bluetooth. Ein wichtiger Grund sind die Apple-Geräte, die somit als Endgeräte infrage kommen. Außerdem ist Bluetooth etwas benutzerfreundlicher als NFC, denn die Karte muss nicht direkt an das Smartphone gehalten werden. Als dritter Vorteil gegenüber NFC kommt die Möglichkeit der Personalisierung der Karte beim ersten Gebrauch hinzu, was mit NFC nicht stabil durchführbar ist. Der Unsicherheitsaspekt, dass Bluetooth-Übertragungen leicht abgehört oder

Einsatz der Display-TAN-Karte beim Mobile Shopping



sogar manipuliert werden könnten, wird dadurch eliminiert, dass alle Bluetooth-Übertragungen verschlüsselt sind, und zwar mit dem individuellen Schlüssel nur dieser Karte. Es gibt also für Angreifer weder eine Chance, die Übertragungen abzuhören noch eine Chance, der Karte manipulierte Überweisungsdaten zu schicken, denn die Karte würde diese Daten wegen der inkorrekten Verschlüsselung sofort ablehnen.

Mobile-Banking- und Online-Banking-Workflow für Geräte ohne Bluetooth

Der Standard-Workflow für Display-TAN ist Mobile-Banking: Nach dem Einloggen auf Smartphone oder Tablet werden die Überweisungsdaten vom Bankkunden eingegeben und wie üblich mit einem „OK"-Knopf bestätigt und dann per Internet zum Bankserver geschickt. Der Bankserver registriert den Überweisungswunsch, versieht die Überweisungsdaten mit einem nur kurzzeitig gültigen Zufallsstring (Nonce) und verschlüsselt dieses Datenpaket mit dem geheimen Schlüssel der Display-Karte dieses Bankkunden. Die verschlüsselten Daten werden zum Smartphone geschickt und stehen dort zum Bluetooth-Versand an die Karte bereit.

Nach dem Einschalten der Karte und dem Aufbau der Bluetooth-Verbindung zwischen Karte und Smartphone werden die verschlüsselten Daten vom Smartphone an die Karte weitergeschickt – alles automatisch ohne Beteiligung des Bankkunden, von dem nur gefordert ist, dass er die Karte einschaltet. Die Karte empfängt die Daten und entschlüsselt sie mit dem geheimen Schlüssel der Karte. Wenn die Entschlüsselung ein nicht-lesbares Ergebnis liefert, wird der Vorgang abgebrochen und eine lapidare Fehlermeldung an das Smartphone zurückgeschickt. Stellt das entschlüsselte Datenpaket eine Überweisung dar, wird als erstes die Zielkontonummer auf der Karte angezeigt. Bestätigt der Bankkunde die Zielkontonummer auf der Karte mit der OK-Taste, wird als nächstes der Betrag angezeigt. Wird auch dieser Betrag bestätigt, wird vom Display-TAN-Prozessor durch die Berechnung einer Hash-Funktion die entsprechende, aus 8 Ziffern bestehende TAN erzeugt. Sie wird per Bluetooth an das Smartphone geschickt und von dort per Internet an den Bankserver weitergeschickt.

Der Bankserver überprüft die Richtigkeit der TAN, indem er mit den gleichen Inputs die gleiche Hash-Funktion Berechnung durchführt wie die Karte: Nur wenn die empfangene und die berechnete TAN übereinstimmen, wird die Überweisung ausgeführt. Abschließend wird der Bankkunde auf seinem Smartphone über die Ausführung der Überweisung beziehungsweise deren Ablehnung informiert.

Das Verfahren verläuft also im Prinzip wie andere TAN-Verfahren, zum Beispiel, das Flackercode-Verfahren. Der Unterschied besteht – neben technischen Details – im Formfaktor (Karte statt Flackercode-Gerät mit eingesteckter Karte) und im Übertragungsweg (Bluetooth statt Flackercode). Die aktuelle Display-TAN-Karte verwendet den Ocra-Standard, mit der SHA1 Hash-Funktion für die Erzeugung der TAN.

Display-TAN kann auch an Geräten eingesetzt werden, die kein Bluetooth haben. Bei diesem „Online Banking Workflow" werden die vom Bankserver verschlüsselten Überweisungsdaten in einem 2-D-Code am Bildschirm des Endgeräts dargestellt, und dieser 2-D-Code wird dann von einem Smartphone gelesen, das anschließend die Daten per Bluetooth an die Display-TAN-Karte weiterleitet, sodass dort die TAN-Generierung durch den Bankkunden angestoßen werden kann. Die erzeugte TAN wird von der Karte an das Smartphone und von dort per Internet an den Bankserver geschickt, eine manuelle Eingabe am Endgerät durch den Bankkunden ist aber auch möglich – so kennt er es ja schon vom SMS-TAN oder Flackercode-Verfahren.

Auch für Internet-Payments

Display-TAN kann auch für Internet Payments genutzt werden. Das ergibt sich ohne weiteres Zutun der Bank, wenn der Bankkunde über einen Zahlungsdienstleister wie zum Beispiel Giropay oder Sofortüberweisung zahlt: Der Bankkunde kann dann bei der Bestätigung der Überweisung das Display-TAN-Verfahren wählen. Besonders interessant ist das beim Mobile Internet Payment, also direkt auf dem Smartphone. Der Bankkunde muss ein paar Mal klicken (inklusive der Klicks auf der Karte) und Kontonummer, Bankleitzahl und Passwort eingeben. Die gesamte Bezahlung ist nur unwesentlich aufwendiger als zum Beispiel die bei Paypal, aber wegen des zweiten Faktors PSD2-konform.

Bei Online-Bezahlverfahren wie Giropay oder Sofortüberweisung ist die Möglichkeit zum Internet-Payment via Display-TAN automatisch gegeben, falls die Bank Display-TAN anbietet. Die Bank könnte aber auch zum Beispiel die Zahlungen der von ihr herausgegebenen Kreditkarten mit Display-TAN PSD2-konform absichern.

Das Endgerät muss nicht intialisiert werden

Das Bluetooth Endgerät (Smartphone, Tablet oder Laptop) und die Display-TAN-Karte sind nicht gekoppelt. Das würde nur stören, während es für die Sicherheit kei-

Daten und Fakten zur Display-TAN-Karte

- So dünn, flexibel und robust wie eine übliche Bankkarte.
- Haltbarkeit: 5 Jahre und 1800 Überweisungen.
- Display: e-Paper, 10 Zeichen: 4 davon 14-Segment, 6 davon 7-Segment und ein Punkt/Komma.

nen weiteren Vorteil bringt. Mit anderen Worten: Das Endgerät muss nicht initialisiert werden – das Verfahren funktioniert sofort. Und die gleiche Karte kann mit wechselnden Endgeräten arbeiten. Was auf dem Display der Karte angezeigt wird, ist flexibel gestaltbar, zum Beispiel können auch IBAN-Zielkontonummern dargestellt werden.

Die Personalisierung von TAN-Generatoren, das heißt die Speicherung des geheimen Schlüssels(Seeds), ist generell ein Problem, denn eine Bank kann das aus Sicherheitsgründen nicht vom Hersteller des TAN-Generators machen lassen. Mit der Bankkarte als TAN-Generator wird dieses Problem noch größer, denn die Bank ist dann auf ihren Karten-Hersteller/-Personalisierer angewiesen, der neben technischen Bedenken und Aufwandsbedenken gegebenenfalls auch noch ein dem entgegengesetztes wirtschaftliches Interesse hat.

Kartenpersonalisierung ohne Einbindung des Herstellers

Mit der Bluetooth-Übertragung gibt es eine Lösung, bei der der Bankkarten-Hersteller/-Personalisierer praktisch nicht involviert ist: Die Display-TAN-Karten werden bei der Herstellung mit vorläufigen Schlüsseln/Seeds versehen. Die mit der vollständigen Display-TAN-Elektronik und den vorläufigen Schlüsseln ausgestatteten Karten werden zum Bankkarten-Hersteller/-Personalisierer geschickt, der sie anstelle von Blanko-Plastik-Karten in seine Maschinen einfüttert und im weiteren Verlauf den Display-TAN-Teil der Karte ignoriert. Insbesondere gibt es keine elektrische Verbindung der Display-TAN-Elektronik mit dem Bankchip. Falls die Bankkarte eine NFC-Antenne für den Chip benötigt, werden die Display-TAN-Karten mit dieser zusätzlichen, elektrisch nicht verbundenen Antenne geliefert.

Die Bank bekommt eine Liste mit den vorläufigen Schlüsseln/Seeds je Karten-ID vom Display-TAN-Karten-Hersteller zugeschickt. Damit ist es möglich, dass die Karte beim ersten Gebrauch durch den Bankkunden personalisiert wird, und zwar im Hintergrund, ohne dass der Bankkunde etwas tun muss.

Wenn die Karte eingeschaltet wird, schickt der Bankserver an die Karte via Internet beziehungsweise das Smartphone die Anfrage nach der ID der Karte und bekommt über den gleichen Weg die Antwort zurück. Mit der Karten-ID kann der Bankserver den vorläufigen geheimen Schlüssel der Karte ablesen. Damit kann der Bankserver jetzt der Karte – wieder über den gleichen Weg den endgültigen geheimen Schlüssel/Seed schicken, und zwar verschlüsselt mit dem vorläufigen Schlüssel, sodass ein Abhörer der Nachricht nichts damit anfangen kann.

Die Karte empfängt die Nachricht, entschlüsselt sie und speichert endgültigen Schlüssel und Seed als solche ab. Das ist nach menschlichem Ermessen sicher genug gegen Abhörer, Manipulateure und Saboteure, die sich zum Beispiel im Internet oder als Trojaner auf dem Smartphone befinden. Und so kann die Karte personalisiert werden, ohne dass der Karten-Hersteller/-Personalisierer involviert ist.

Gegenargumente Haltbarkeit und Kosten

Bei den bisherigen Gesprächen mit Banken stellten sich die folgenden Bedenken gegenüber Display-TAN heraus:

- Bedenken bezüglich der Haltbarkeit/Robustheit von Display-Karten.

- Das Display von Display-TAN sei zu einfach. Besser wäre es, wenn auch kleine Buchstaben und Transaktionen mit längeren Texten dargestellt werden könnten.

- Der Preis der Display-TAN-Karten liegt in mittleren Bereich der Preise für herkömmliche TAN-Generatoren und damit ungefähr bei den akkumulierten durchschnittlichen laufenden Kosten für das SMS-TAN Verfahren.

Genau diese Kosten hoffen die Banken sich in Zukunft sparen zu können, indem sie die Smartphones der Bankkunden zu TAN-Generatoren machen, also durch eine von der Bank zur Verfügung gestellte App, die auf dem Smartphone die TAN erzeugt. Die Überweisungsdaten werden bei diesen „App-TAN"-Lösungen entweder per 2-D-Code vom Bildschirm abgelesen und per Internet-Push-Verfahren auf das Smartphone geschickt. Der geheime Schlüssel ist bei diesen Verfahren im Speicher des Smartphones abgelegt.

Ein technischer Rückschritt?

Display-TAN scheint in dieser Hinsicht zur Unzeit auf den Markt zu kommen, denn in dem Moment, in dem die Smartphones jetzt mit der passenden Funk-Technik Bluetooth Smart ausgestattet sind, wird das Smartphone selber von den Banken zum TAN-Generator gemacht. Die Kartenlösung wird nicht nur als zu teuer, sondern als technischer Rückschritt angesehen. Die Einschätzung als Rückschritt könnte aber revidiert werden:

- Erstens durch die Sicherheitsproblematik: Der bei App-TAN auf dem Smartphone gespeicherte geheime Schlüssel ist genau genommen eine Sicherheits-Katastrophe, denn ein Smartphone-Trojaner braucht nur den Speicher des Smartphones zu durchsuchen, um den geheimen Schlüssel auszuspionieren. Gerade beim Mobile Banking ist diese Gefahr besonders groß, denn der gesamte Überweisungsvorgang inklusive TAN-Erzeugung spielt sich nur auf dem einen Endgerät ab. Genau dieses Problem könnten auch die Regulierer von EZB oder EBA vor Augen gehabt haben, wenn sie in der PSD2 fordern, dass die durch den geheimen Schlüssel gegebene Sicherheit und die durch das Passwort gegebene Sicherheit unabhängig voneinander sein

sollen – was sie aber im App-TAN-Mobile-Banking nicht sind, da der gleiche Trojaner beides ausspionieren kann.

Zweitens könnte auch die Usability der App-TAN Lösung insgesamt schlechter sein als die von Display-TAN. Diese Einschätzung hört sich zunächst erstaunlich an, denn beim Mobile Banking mit App-TAN braucht der Bankkunde nichts anderes als sein Smartphone, während er für Display-TAN noch die Bankkarte hinzuziehen muss. Doch das auf die Dauer unangenehme Problem mit App-TAN ist die Bindung an das Smartphone: Jedes Gerät muss zuerst initialisiert, das heißt, mit dem geheimen Schlüssel ausgestattet werden, meistens via Papier-Brief von der Bank.

Der Bankkunde muss sich also merken, auf welchen Endgeräten er App-TAN initialisiert hat. Beim Smartphone-Wechsel muss nicht nur das neue Smartphone initialisiert werden, sondern der Bankkunde muss daran denken, dass auf dem alten noch ein wichtiger Schlüssel gespeichert ist. Reicht es, die App zu löschen? Bei Smartphone-Diebstahl entsteht ein ähnlicher Problemfall: Der Bankkunde könnte vergessen, der Bank den Verlust zum melden. Mit Display-TAN hat er alle diese Probleme nicht.

Wirtschaftliche Aussichten abhängig von Entwicklung der App-TAN

Die wirtschaftlichen Aussichten für Display-TAN hängen sehr davon ab, wie weit sich die App-TAN-Verfahren mittelfristig etablieren. Falls die tatsächlichen Angriffe darauf Überhand nehmen oder die Regulierer App-TAN zumindest für Mobile Banking verbieten (so wie SMS-TAN für Mobile Banking in Deutschland schon lange verboten ist), ist der Weg für eine Massen-Anwendung von Display-TAN frei, denn kein anderes TAN-Verfahren kann für das immer populärer werdende Mobile Banking die hohe, PSD2-konforme Sicherheit bieten, bei gleichzeitiger Mobilität in dem Sinne, dass der Bankkunde nichts Weiteres braucht als das, was er sowieso dabei hat.

Wenn sich die App-TAN-Verfahren doch etablieren und die Regulierer trotz der Vorgaben aus der PSD2 eine Laissez-Faire-Haltung einnehmen, dürften realistischerweise – wegen der Unsicherheit – App-TAN-Überweisungen von den meisten Banken mit einem Limit gedeckelt sein. Es bliebe dann für Display-TAN die Nische, ein mobiles Verfahren für diejenigen Bankkunden darzustellen, die potenziell ohne Limit überweisen wollen, generell auf die Sicherheit Wert legen und diejenigen, die den Usability-Vorteil von Display-TAN gegenüber App-TAN schätzen, etwa weil sie mehrere Endgeräte haben. Insgesamt könnten das 5 bis 10 Prozent der Kunden einer Bank darstellen, sogar wenn die Bankkunden die Kosten der Display-TAN-Karte selbst übernehmen müssen.

Smartcards mit HD-Displays sind in der Erprobung und teilweise auch schon im Umlauf, zum Beispiel als Bitcoin-Tresore. Für Online-Banking muss aber erst noch das Problem der Langzeit-Stromversorgung für die mehr als 20 000 Pixel gelöst und getestet werden, denn eine Haltbarkeit, die an die der Display-TAN- Karte mit 5 Jahren und 1 800 Überweisungen heranreicht, sollte gegeben sein. Das Display auf der Karte ließe sich auch für andere Anwendungen nutzen. Eine weitere Sicherheitsanwendung ist zum Beispiel eine PIN-Eingabe auf dem Endgerät, die für Trojaner unabhörbar ist, und zwar via eine vertauschte Anordnung der Ziffern, die jedes Mal eine andere ist. Der Benutzer tippt auf dem Endgerät die PIN ein, und zwar anhand der auf der Karte angezeigten Vertauschung der Ziffern.

Links

PSD2 Richtlinie: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L2366
EBA PSD2 Discussion Paper: https://www.eba.europa.eu/-/eba-seeks-input-on-strong-customer-authentication-and-secure-communication-under-psd2
CCC Kongress 2015, Vortrag über Push-TAN: https://media.ccc.de/v/32c3-7360-un_sicherheit_von_app-basierten_tan-verfahren_im_onlinebanking#video&t=1854
SMS-TAN ist nicht für Mobile Banking erlaubt: https://die-dk.de/zahlungsverkehr/electronic-banking/mobiletan/
13-Tasten Display-Karten:
http://www.nidsecurity.com/products/
http://www.smartdisplayer.com/page_01_a.html

Weitere Informationen: http://www.display-tan.com/?lang=de

GAA-Sicherheit

Deutlich mehr Transaction Reversal Fraud

Es sind vor allem die physischen Angriffe auf Geldautomaten, die im Jahr 2015 zugenommen haben. Das geht aus dem European ATM Creme Report 2015 des European ATM Security Teams (EAST), London, hervor. 2 657 Vorfälle dieser Art weist der Bericht für 2015 aus. Das entspricht einem Anstieg um 34 Prozent gegenüber dem Vorjahr. Die damit verbunden Verluste erhöhten sich sogar um 81 Prozent auf 49 Millionen Euro – obwohl in 40 Prozent der Fälle gar kein Bargeld erbeutet wurde. Weitaus schwerwiegender ist häufig der Sachschaden an Gebäude und Technik. Auch beim Betrug am Geldautomaten war im vergangenen Jahr wieder ein Anstieg zu verzeichnen, und zwar um 19 Prozent auf 18 738 Fälle, bei denen Verluste in Höhe von 327 Millionen Euro anfielen. Dabei spielt das Skimming eine immer geringere Rolle. 4 131 Skimming-Vorfälle weist der Bericht für 2015 aus, das sind 27 Prozent weniger als noch 2014. Kräftig zugenommen haben dagegen Manipulationen, bei denen der Angreifer das ausgezahlte Bargeld abgreift (sogenannter Transaction Reversal Fraud, kurz TRF). Solche TRF-Angriffe gab es im Jahr 2014 in 5 104 Fällen. Ein Jahr zuvor war diese Betrugsform erst 160-mal vorgekommen. **Red.**