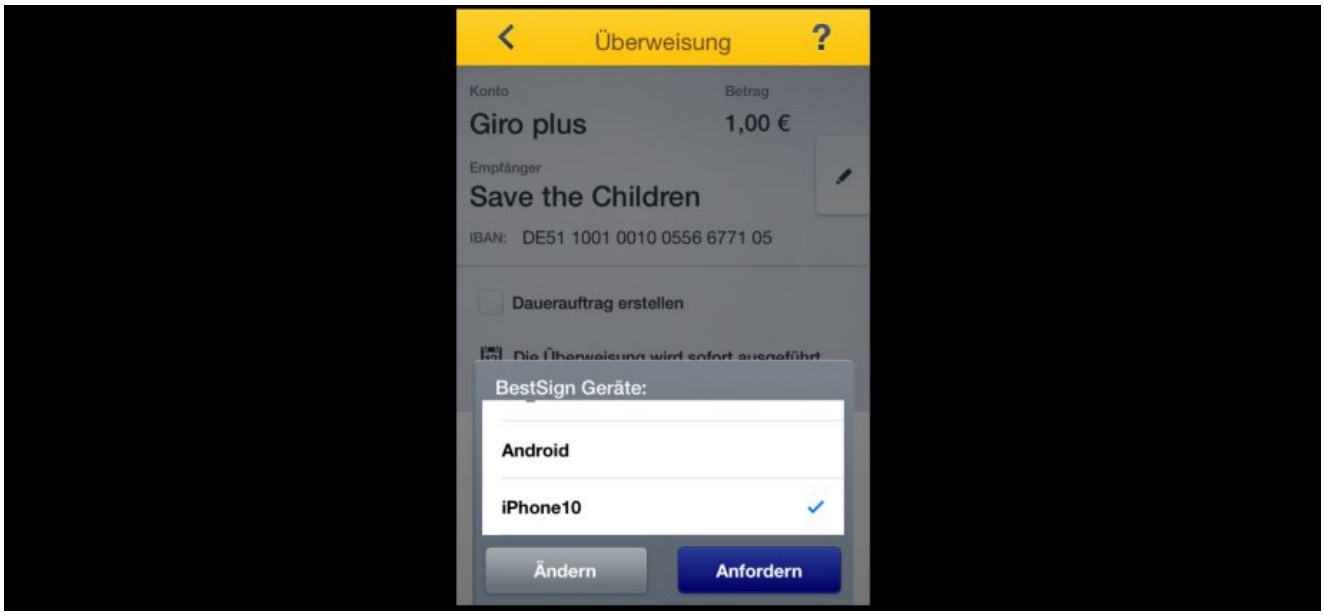


Endlich: Mobile Banking ohne TAN-Gerät

Das SMS-TAN-Verfahren ist bei Bankkunden beliebt, aber für mobile Banking leider keine Lösung. Seine einzige Sicherheitsfunktion besteht in der Kanaltrennung zwischen Online und Mobile. Und die ist ja nun nicht wirklich gegeben, wenn beides auf dem Smartphone zusammenläuft.

Die Alternative bestand bisher in zusätzlicher Hardware zur Erzeugung von TANs – „eTAN", „Smart-TAN" und wie sich die Geräte alle nennen. Das ist die sicherste Lösung, aber natürlich hat man den Generator nicht immer dabei. Das hat die mobilen Transaktionen bisher stark limitiert. Nicht umsonst berichten Banken gern die Anzahl der Logins in ihr mobile Banking, aber kaum je die Anzahl der Transaktionen.

Die Postbank hat jetzt ein mobile TAN-Verfahren eingeführt, das ganz ohne Zusatzgerät auskommt. Es basiert auf dem bereits im Postbank Online Banking eingesetzten BestSign-Verfahren.

Bisher basierte auch das Bestsign-Verfahren auf einer Hardware, einem „SealOne"-Gerät. Es wurde per USB an den Computer angeschlossen und baute von sich aus eine verschlüsselte Verbindung zur Bank auf. Quasi ein sicherer Tunnel, bei dem der Computer nur der Datenweiterleitung dient. Er kann weder Daten lesen noch verändern. Die online erfasste Transaktion wird dann von der Bank

zusätzlich durch den Tunnel an das SealOne-Gerät gesendet, auf dessen Display angezeigt und vom Kunden per Knopfdruck am Gerät freigegeben. Das Gerät erzeugt eine digitale Signatur der Daten und sendet sie an die Bank. Damit ist die Transaktion freigegeben.

Die Neuerung ist, dass im Mobile Banking anstelle der Hardware eine App eingesetzt wird. Die App hat dieselbe Funktion wie vorher das Hardware-Device: Sie baut einen kryptographisch gesicherten Tunnel zur Bank auf, um die Transaktion über diesen zweiten Kanal neben dem Mobile Banking zu bestätigen.

Die BestSign-App wird dabei von der Banking-App gestartet, so dass der Benutzer sich nicht selbst mit dem Wechsel der App vom Mobile Banking zur Freigabe-App und zurück zu Recht finden muss. Im Unterschied zum Hardware-Gerät muss bei der BestSign-App eine PIN eingegeben werden, um sie zu aktivieren. Bei der Hardware hat man noch unterstellt, dass der Besitz allein ausreicht, um den Benutzer zu identifizieren. Nach dem Motto: bewahren Sie das Gerät so auf, dass nur Sie selber Zugriff haben. Bei einem Smartphone, das man immer dabei hat, ist diese sichere Aufbewahrung utopisch. Deshalb macht die PIN absolut Sinn.

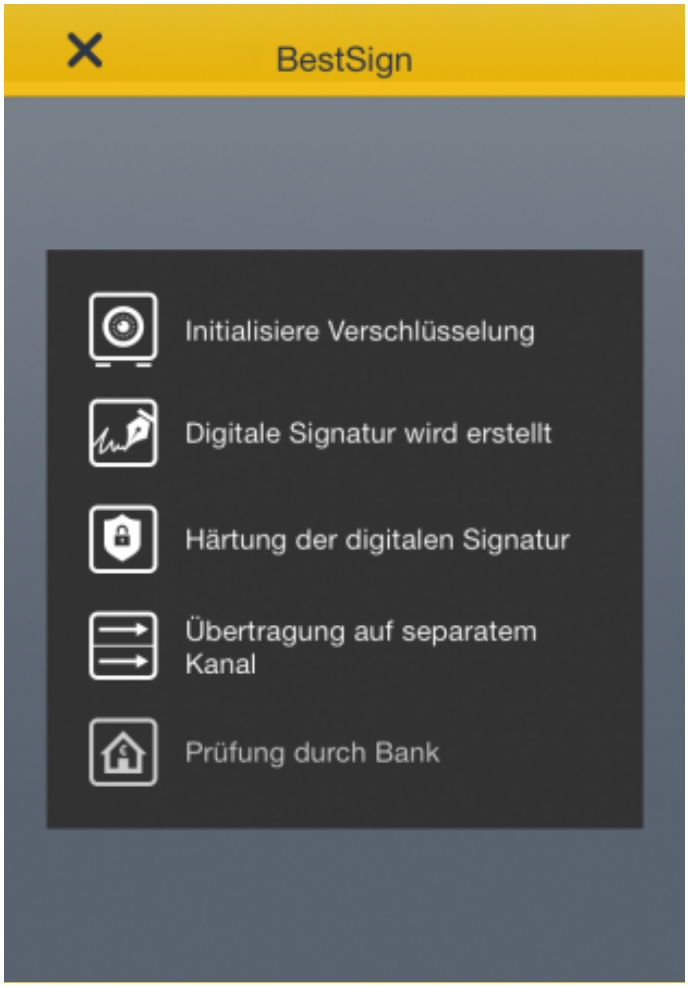
Das Verfahren ist meines Erachtens ein riesiger Durchbruch in Sachen mobile Transaktionen. Eigentlich ist es das erste Verfahren mit guter Usability überhaupt, alles andere ist eine Zumutung.

Wie ist es um die Sicherheit bestellt? Das hängt vom Schutz der App und der Qualität der PIN ab. Software auf Smartphones ist nur dann so sicher wie eine separate Hardware, wenn sie auf einem „Secure Device" läuft, also als Chip-Anwendung auf der SIM-Karte oder einem separaten Chip, wie er beispielsweise in den Samsung Galaxy Geräten schon seit einiger Zeit verbaut ist. Jede normale App, auch die hier verwendete BestSign-App, läuft in einer Umgebung, die letztlich zu komplex ist, um dasselbe Sicherheitsniveau herstellen zu können. Aber das ist ja auch gar nicht die Frage, es geht nur darum: Ist es sicher genug?

Ich habe keine Informationen, wie BestSign die App absichert. Man kann da jedenfalls einiges absichern. Dadurch, dass es eine separate App mit sehr überschaubarer Funktionalität ist, bietet sie von vornherein wenig Angriffsfläche. Wenn man das noch kombiniert mit aktiven Schutzfunktionen wie dem Erkennen von Jail Breaks und dem Abfangen von Einsprüngen anderer Apps an nicht vorgesehenen Stellen, dann lässt sich eine wirklich wehrhafte App programmieren. Metaforic bietet entsprechende Schutzsoftware als Produkt an. Sie nennen das ein "Immunsystem" für Apps.

Das größere Risiko sehe ich in der PIN. Die darf der Benutzer nämlich selbst vergeben. Und wir kennen die Studien zu selbst vergebenen 4-stelligen-PINs: Mehr als 18% der Nutzer wählen 1234, 0000 und 1111. Ok, hier geht es um Geld, da werden sich die Kunden schon etwas vorsichtiger verhalten. Trotzdem dürfte Social Engineering auf absehbare Zeit das relevanteste Angriffsszenario sein.

Um es kurz zu machen: Werde ich das Verfahren einsetzen? Auf jeden Fall. Genau darauf warten wir doch alle schon lange.



Elmar Borgmeier

Gestaltet Online Finance seit 1997. Glaubt an die Symbiose von Finance und IT. Ist Mitgründer und Chief Innovation Officer der syngenio AG. Moderator des JAX Finance Day. Berater für Next Generation Finance. Philosophiert gern über IT und realisiert noch lieber konkrete Lösungen.

26. MÄRZ 2014 · **KOMMENTARE 8**

Veröffentlicht in: ***Multichannel / Omnichannel***, ***Online Banking / Online Finance***, ***Sicherheit / Security***

Schlagwörter: ***Mobile Banking***, ***TAN***