Mobile TAN (mTAN / SMS-TAN)

Wie der Name vermuten lässt, nutzt das mTAN-Verfahren neben dem Internet das Mobilfunknetz als zusätzlichen Kommunikationskanal, was das Abfischen von TANs erschwert.

Das gilt es bei der Verwendung von Mobile TAN zu beachten:

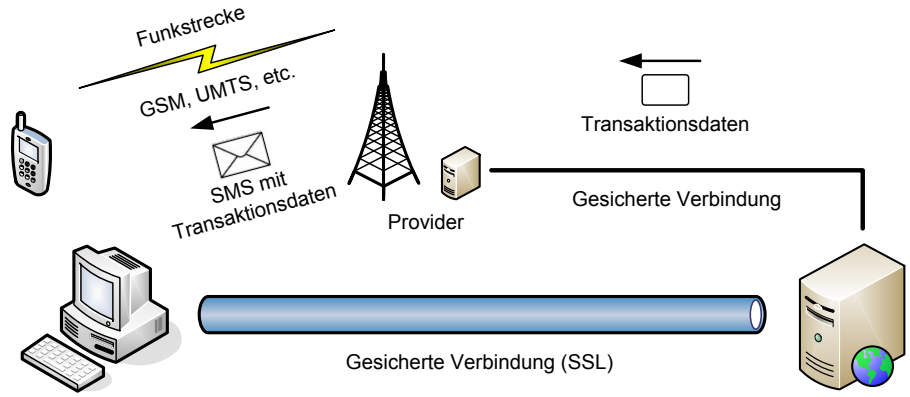
- Überprüfen Sie bei der Bestätigung von Transaktionen die zu signierenden Daten sorgfältig.
- Bewahren Sie Ihre Zugangsdaten getrennt von Ihrem Mobiltelefon auf.
- Schreiben Sie keine Passwörter und PINs auf, es sei denn, Sie halten die Notiz unter Verschluss.
- Geben Sie Ihre Identifikationsnummer, das Passwort oder Ihre PIN und die mTAN ausschliesslich in der Login-Maske Ihres E-Bankings ein.
- Melden Sie dem Finanzinstitut, wenn Sie unaufgefordert mTAN-Codes zugestellt erhalten.

Funktionsweise

Nach der Eingabe von Identifikationsnummer und Passwort oder PIN im E-Banking-Portal übermittelt das Finanzinstitut einen einmaligen Zugangscode (mTAN) mittels SMS. Erst nach Eingabe dieses zusätzlichen Zugangscodes ist der Login-Vorgang abgeschlossen und der Zugriff auf das Konto wird gewährt.

Teilweise müssen auch potenziell gefährliche Transaktionen wie z.B. auffällige Überweisungen mittels mTAN-Verfahren bestätigt werden. Viele Systeme merken sich wiederkehrende Zahlungsempfänger eines Kunden, so dass nicht mehr jede Überweisung bestätigt werden muss.

Das Verfahren schützt vor Angriffen, welche Transaktionen manipulieren (z.B. Man-in-the-Browser-Angriffen), sofern der Bankkunde die auf dem Display angezeigten Transaktionsdaten vor dem Bestätigen auf ihre Richtigkeit hin überprüft.



Infrastruktur des E-Banking Kunden
- Computer
- Mobiltelefon

Infrastruktur des Finanzinstitutes
- Webserver
- Plattform zur Authentifikation und Signaturverifikation
- E-Banking System
- SMS-Gateway

(https://www.ebas.ch/wp-content/uploads/2019/09/mTAN_de.svg)