

# Chip-TAN

Beim Chip-TAN-Verfahren benötigt der Kunde neben den persönlichen Zugangsdaten einen Kartenleser und eine Bankkarte, welche den zweiten Authentifizierungsfaktor darstellt.

## Das gilt es bei der Verwendung von Chip-TAN zu beachten:

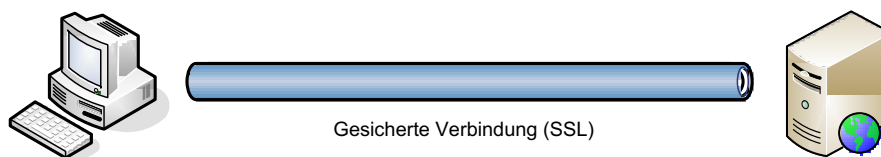
- Überprüfen Sie bei der Bestätigung von Transaktionen die zu signierenden Daten sorgfältig.
- Bewahren Sie Ihre Zugangsdaten getrennt von Ihrer Bankkarte auf.
- Schreiben Sie keine Passwörter und PINs auf, es sei denn, Sie halten die Notiz unter Verschluss.
- Geben Sie Ihre Identifikationsnummer, das Passwort oder Ihre PIN und die Chip-TAN ausschliesslich in der Login-Maske Ihres E-Bankings ein.

## Funktionsweise

Nach der Eingabe von Identifikationsnummer und Passwort oder PIN im E-Banking-Portal übermittelt das Finanzinstitut einen einmaligen Code zur Eingabe auf dem Kartenlesegerät (Challenge-Wert) und fragt nach dem zugehörigen Zutrittscode des Kunden (Response-Wert). Dieser wird mit Hilfe des Kartenlesers und der Bankkarte unter Angabe des angezeigten Codes (Challenge-Wert) generiert. Man spricht bei Chip-TAN deshalb von einem «Challenge-Response-Verfahren».

Teilweise müssen auch potenziell gefährliche Transaktionen wie z.B. auffällige Überweisungen mittels Chip-TAN-Verfahren bestätigt werden.

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
- Kartenleser
- Bankkarte

Infrastruktur des Finanzinstitutes

- Webserver
- Plattform zur Authentifikation
- E-Banking System

[https://www.ebas.ch/wp-content/uploads/2019/11/Chip-TAN\\_de.svg](https://www.ebas.ch/wp-content/uploads/2019/11/Chip-TAN_de.svg)