

REINERSCT<sup>®</sup>

# Online-Banking – aber sicher.



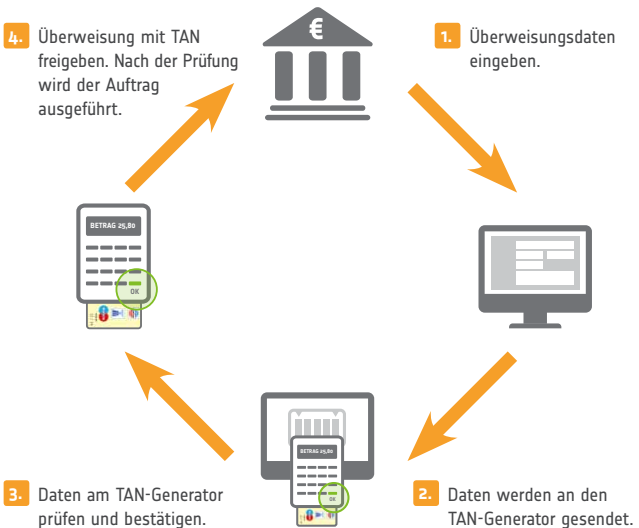
[www.reiner-sct.com](http://www.reiner-sct.com)

# Zwei Online-Banking-Verfahren in der Übersicht

## Das FinTS- bzw. HBCI-Verfahren



## Das optische Verfahren



### Ihr Weg zum Online-Banking

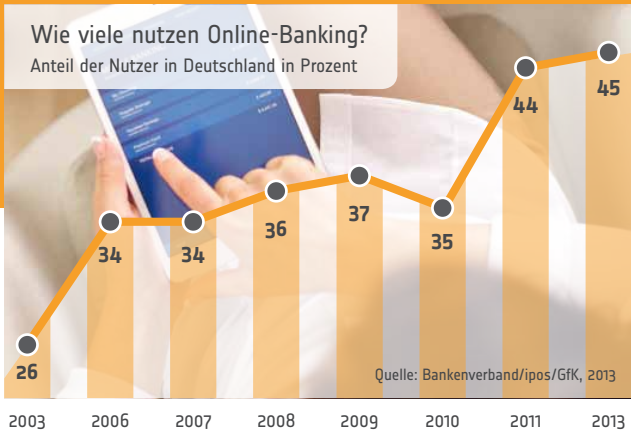
1. Kontaktieren Sie Ihr Kreditinstitut
2. Lassen Sie sich für eines der beiden Verfahren freischalten



# Online-Banking

## *Einfach und komfortabel*

Statt Überweisungen von der Filiale aus können Sie Ihre Finanzgeschäfte beim Online-Banking bequem über das Internet von zu Hause aus erledigen. 45% der Bürger in Deutschland nutzen mittlerweile Online-Banking.



## **In Deutschland haben sich folgende Verfahren im Online-Banking etabliert:**

- PIN/TAN (pushTAN, mobileTAN oder TAN-Generator).
- Financial Transaction Services (FinTS), bzw. Homebanking Computer Interface (HBCI), mit Absicherung durch PIN/TAN oder Chipkarte.

## **Sicherheit beim Online-Banking ist gefragt**

- Hackerangriffe auf persönliche Kontodaten nehmen rasant zu.
- Durch sogenannte Trojaner versuchen Angreifer PCs nach PINs und TANs auszuspionieren.
- Über Man-In-The-Middle Angriffe versuchen Hacker Online-Banking-Transaktionen zu manipulieren.

Mit TAN-Generatoren oder Chipkartenlesern können Sie sich vor solchen Gefahren schützen.



# Chipkartenleser

## *Garantiert sicher*

Experten, wie die IT-Behörde der EU (ENISA), die Europäische Zentralbank und das Landeskriminalamt Hessen raten beim Online-Banking zur einzig sicheren Methode: Den Einsatz von Chipkartenlesern.



VON BANKEN  
UND SPARKASSEN  
EMPFOHLEN



## **Online-Banking in Kombination mit Chipkartenleser erfolgt in fünf einfachen Schritten:**

- 1.** Zunächst wird eine Transaktion angelegt, wie z. B. eine Überweisung.
- 2.** Anschließend stecken Sie Ihre Chipkarte in den Leser.
- 3.** Nun geben Sie Ihre PIN in den Leser ein. Das Besondere dabei: Da Sie die PIN nicht an Ihrer Computertastatur eintippen, sondern am Chipkartenleser, können Dritte Ihre PIN nicht ausspähen. Der Vorgang ist also vollkommen abgesichert.
- 4.** Durch die Eingabe der PIN geben Sie die Transaktion frei. Sämtliche Daten werden verschlüsselt und anschließend an Ihre Bank übertragen.
- 5.** Nur bei vollständiger Übereinstimmung mit Ihren Auftragsdaten führt Ihr Kreditinstitut die Transaktion durch.



Info: Dieses Verfahren ist auch auf Tablets und Smartphones möglich.



# TAN-Generatoren

## *Der Standard in der Deutschen Kreditwirtschaft*

Bei den optischen TAN-Verfahren der Kreditinstitute benötigt man einen TAN-Generator, der als unabhängiges Gerät die gesamte Sicherheit der Transaktion gewährleistet.



VON BANKEN  
UND SPARKASSEN  
EMPFOHLEN



### **So einfach ist Online-Banking in Kombination mit TAN-Generatoren:**

- Zunächst wird eine Transaktion angelegt, wie z. B. eine Überweisung. Dann werden die Überweisungsdaten mittels eines optischen Signals („Flickergrafik“) oder via Bluetooth zurück auf den TAN-Generator übertragen.
- Im TAN-Generator werden die übertragenen Daten im Display angezeigt. Der Nutzer muss nun nachprüfen, ob die seinem Institut übertragenen Überweisungsdaten mit seinen übereinstimmen.
- Wenn dies der Fall ist, wird eine TAN erzeugt und in die Bankinganwendung eingegeben.
- Das Kreditinstitut führt nur die Überweisung mit den Daten aus, die vorher im TAN-Generator angezeigt wurden.



Info: Dieses Verfahren ist auch auf Tablets und Smartphones möglich.

# Unser Tipp:

[www.wikibanking.net](http://www.wikibanking.net)

*Das Portal rund ums Online-Banking*



Wikibanking.net erklärt u.a. verständlich die verschiedenen Online-Banking-Verfahren, klärt umfangreich über Risiken und Sicherheitsmaßnahmen auf und informiert Sie immer über aktuelle Themen rund um's Online-Banking.