Chip TAN

With the Chip TAN process, customers will not only need their personal access data, but also a card reader and their bank card which make up the second authentification factor here.

Please note the following when using Chip TAN:

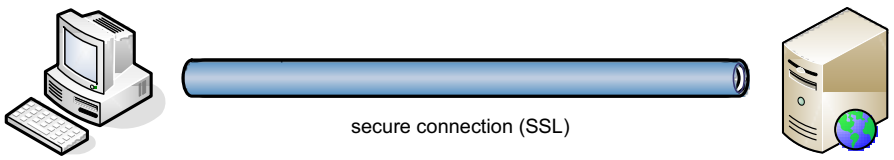
- Carefully check all data to be signed off before confirming any transaction.
- Store your access details separately from your bank card.
- Do not make any written notes of your passwords and PINs, unless you can keep such notes under lock and key.
- Only ever enter your ID number and your password or your PIN and your Chip TAN into the log-in template of your e-banking facility.

Operating principle

Once you enter your ID number and password or PIN into your e-banking portal, the financial institution will transmit a one-off access code (challenge code) for input to your card reader and will ask their customers for the respective access code (response code). This is generated with the help of the card reader and bank card while stating the displayed code (challenge code). Chip TAN is therefore called a “challenge response process”.

Sometimes, potentially risky transactions such as conspicuous remittances have to be confirmed via this Chip TAN procedure, too.

This process protects against attacks which manipulate transactions (e. g. man-in-the- browser attacks), for as long as bank customers check the transaction data shown on their display for their accuracy before confirming.



e-banking customer infrastructure
· computer
· card reader
· bank card

financial institution infrastructure
· web server
· authentification platform
· e-banking system

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

Copyright © 2020 – All rights reserved. Lucerne School of Information Technologies