# Mobile TAN (mTAN / SMS-TAN)

**As the name already suggests, the mTAN process uses the public mobile telephone network in addition to the Internet as an additional communication channel, something which will hamper attempts at capturing TANs.**

**Please note the following when using Mobile TAN:**

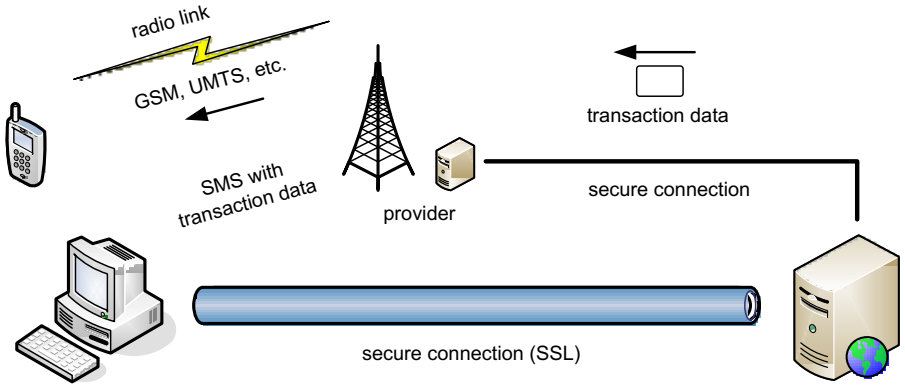
- Carefully check all data to be signed off before confirming any transaction.
- Store your access details separately from your mobile phone.
- Do not make any written notes of your passwords and PINs, unless you can keep such notes under lock and key.
- Only ever enter your ID number and your password or your PIN and your mTAN code into the log-in template of your e-banking facility.
- Notify your financial institution should you receive any mTAN codes without having requested them.

## 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 (mTAN) to your smartphone. Only once this additional access code has been entered, the log-in process is complete, and you are granted access to your account.

Sometimes, potentially risky transactions such as conspicuous remittances have to be confirmed via this mTAN procedure, too. Many systems are able to remember their customers' recurring payees, so that you don't have to confirm every single remittance in the future.

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
· mobile phone

financial institution infrastructure
· web server
· authentification and signature verification platform
· e-banking system
· SMS gateway

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