Mobile ID

Special SIM cards enable secure processing of encrypted messages when logging into e-banking facilities.

Please note the following when using Mobile ID:

- Carefully check all data to be signed off before confirming any transaction.
- Store your access details separately from your mobile phone.
- Don’t use the same mobile phone for e-banking as the one you receive Mobile ID messages on.
- 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, your password or your PIN into the log-in template of your e-banking facility.
- Only ever enter your personal Mobile ID PIN on your mobile phone.

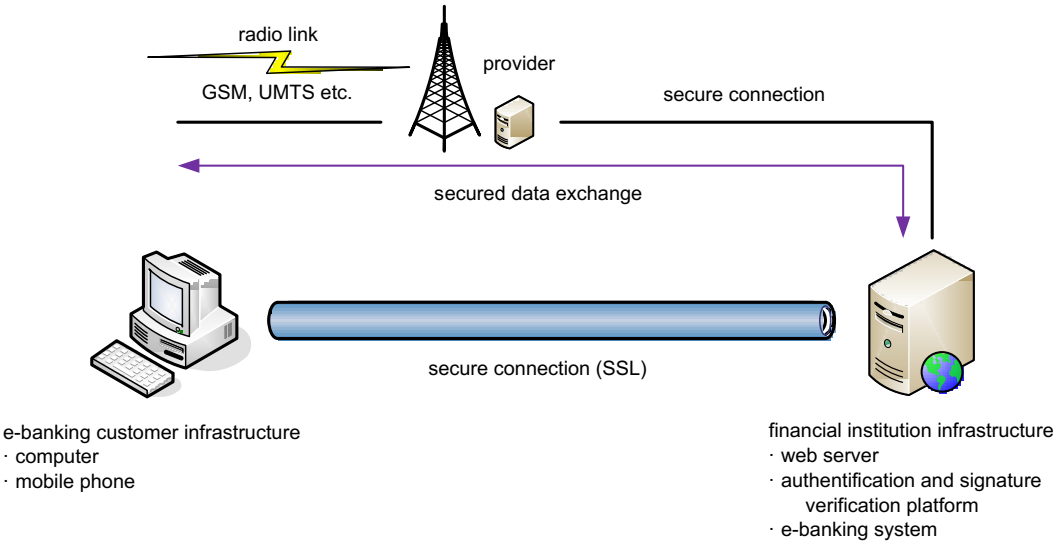
Operating principle

Similar to the mTAN log-in procedure, Mobile ID uses a smartphone, and data are transferred across an additional communication channel (mobile phone network).

The difference is the vital role played by the special SIM card holding the Mobile ID. This enables data to be transferred in an encrypted manner. The keys required to do so are generated when activating the Mobile ID and are then stored on the actual SIM card. This encrypted communication channel prevents attackers from capturing log-in or transaction requests.

When logging into the financial institution website, you will need to enter the ID number and potentially your password or PIN. Your mobile phone will then display a message which you have to confirm. You will then have to enter your personal Mobile ID PIN on your mobile phone. Only once you have done so will you obtain access to your account.

You will have to apply to your mobile phone network provider for a Mobile ID-enabled SIM card.



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