

# Photo TAN (Optical TAN process)

In addition to your password, the Photo TAN process also uses a smartphone app or a specific reader. These are employed to record and encrypt optical information displayed on your log-in page.

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

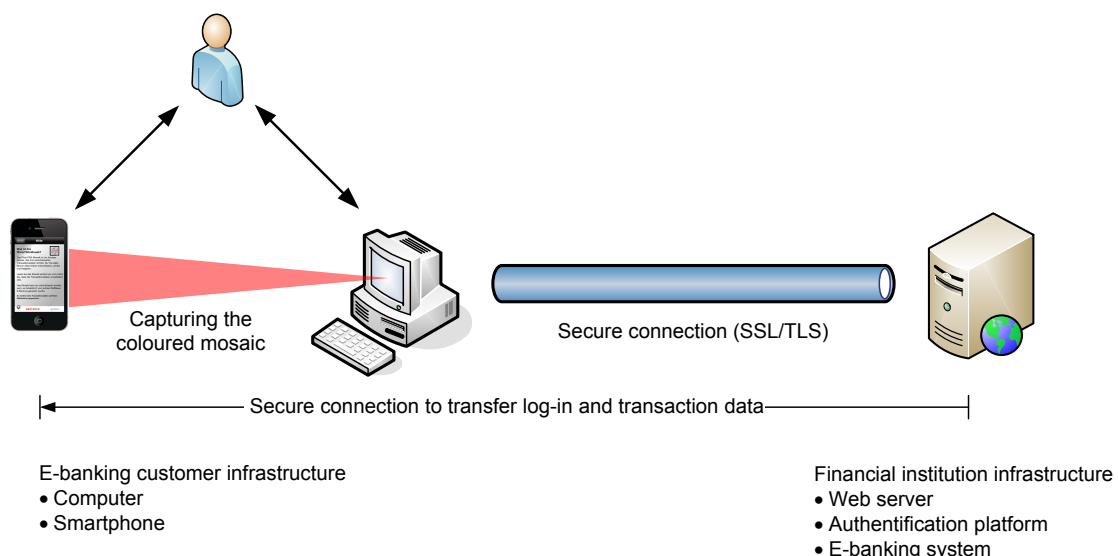
- Carefully check all data to be signed off before confirming any transaction.
- Store your access details separately from your Photo TAN reader.
- Follow all [security recommendations applicable to smartphones \(https://www.ebas.ch/en/mobile-banking-app/\)](https://www.ebas.ch/en/mobile-banking-app/).
- 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 Photo TAN code 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 TAN in the shape of a static, coloured mosaic (hence the name “Photo TAN”) to your screen. This is recorded using your smartphone camera or a dedicated reader, and then decoded. The access code it contains is then displayed on your screen.

Sometimes, potentially risky transactions such as conspicuous remittances have to be confirmed via this Photo TAN procedure, too. In addition to a verification code, this process can also be used to transfer detailed transaction data.

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.



([https://www.ebas.ch/wp-content/uploads/2019/09/Photo-TAN\\_en.svg](https://www.ebas.ch/wp-content/uploads/2019/09/Photo-TAN_en.svg))