Chip-TAN

Con la procedura Chip-TAN il cliente ha bisogno, oltre che dei dati d'accesso personali, di un lettore di schede e di una tessera bancaria, che rappresenta il secondo fattore di autenticazione.

A cosa bisogna fare attenzione quando si usa la procedura Chip-TAN:

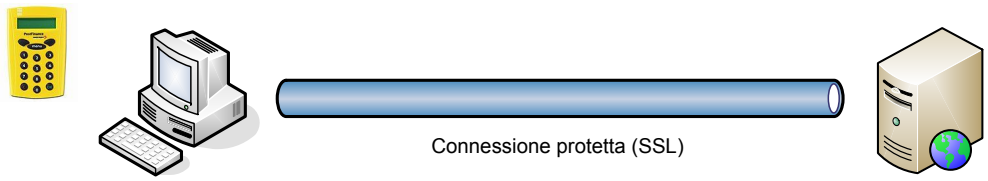
- Alla conferma delle transazioni verificate attentamente i dati da convalidare.
- Conservate i vostri dati d'accesso in un luogo separato dalla vostra tessera bancaria.
- Non annotate mai password e PIN su fogli di carta, a meno che non li custodiate sotto chiave.
- Immettete il vostro numero di identificazione, la password o il PIN e il chip-TAN esclusivamente nella maschera di login del vostro sistema di e-banking.

Funzionamento

Dopo aver inserito il numero di identificazione e la password o il PIN nel portale dell'e-banking, l'istituto finanziario comunica un codice una tantum da inserire nel lettore di schede (valore Challenge) e richiede il relativo codice di accesso del cliente (valore Response). Questo codice viene generato con il lettore di schede e la tessera bancaria dopo che viene inserito il codice visualizzato (valore Challenge). Per questo motivo la procedura Chip-TAN viene definita anche «Challenge-Response».

In alcuni casi anche le transazioni potenzialmente rischiose come i trasferimenti particolari devono essere confermate mediante procedura Chip-TAN.

La procedura è in grado di proteggere contro attacchi di manipolazione delle transazioni (p. es. gli attacchi del tipo man-in-the-browser) se i dati della transazione visualizzati sul display vengono controllati dal cliente prima della conferma.



Infrastruttura del cliente di e-banking
- Computer
- Lettore di schede
- Tessera bancaria

Infrastruttura dell'istituto finanziario
- Server web
- Piattaforma di autenticazione
- Sistema di e-banking

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