# Authentisierung und Autorisierung im Digital Banking

cnlab security AG, Zuzana Trubini
Januar 2021

cnlab

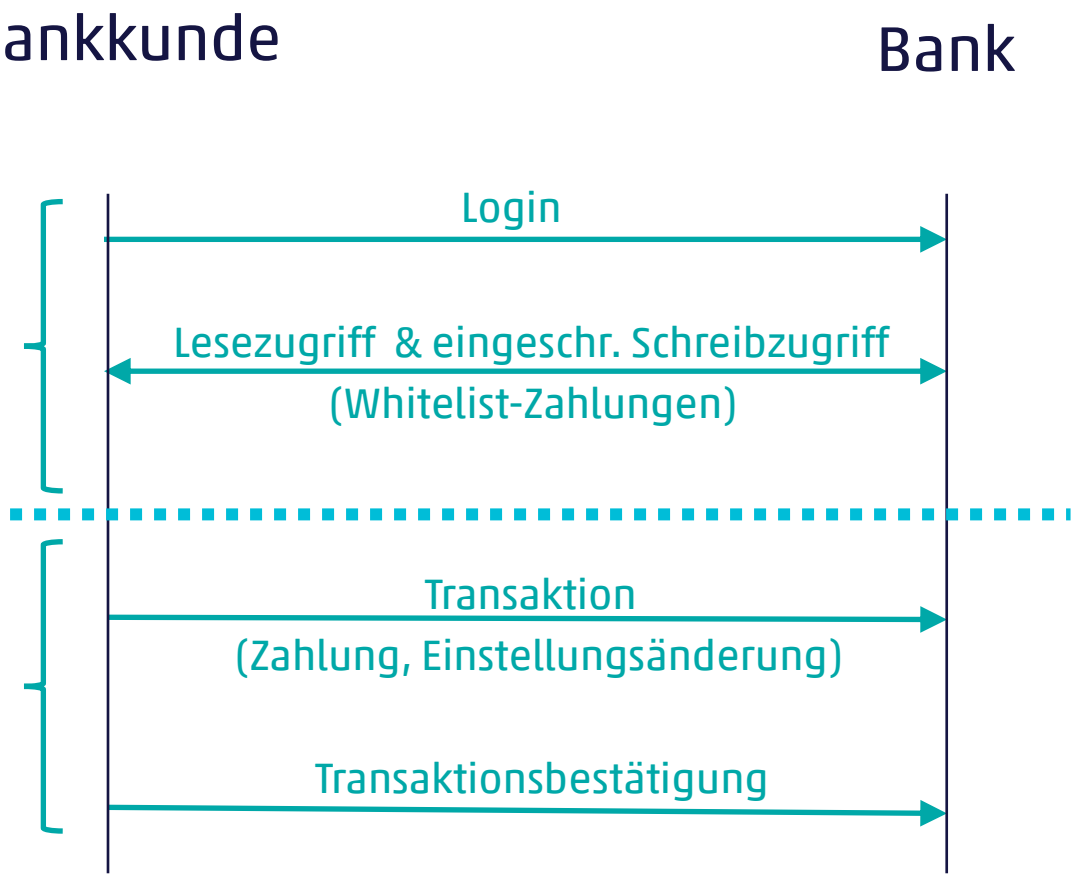
# Authentisierung und Autorisierung

**Login** (bei den meisten Banken 2FA)
(Authentisierung des Kunden)

➡ Kontoübersicht +
Zahlungen an Whitelist-Empfänger

**Transaktionsbestätigung**
(Autorisierung der Transaktion)

➡ Restliche Zahlungen +
Sicherheitsrelevante Änderungen



# eBanking vs. Mobile-Banking

eBanking

- im Browser (typischerweise auf einem Computer)
- Vorteile:
  - Falls auf dem Computer – Smartphone kann als Zweit-Gerät eingesetzt werden

    -> typischerweise 2-Geräte-Lösung

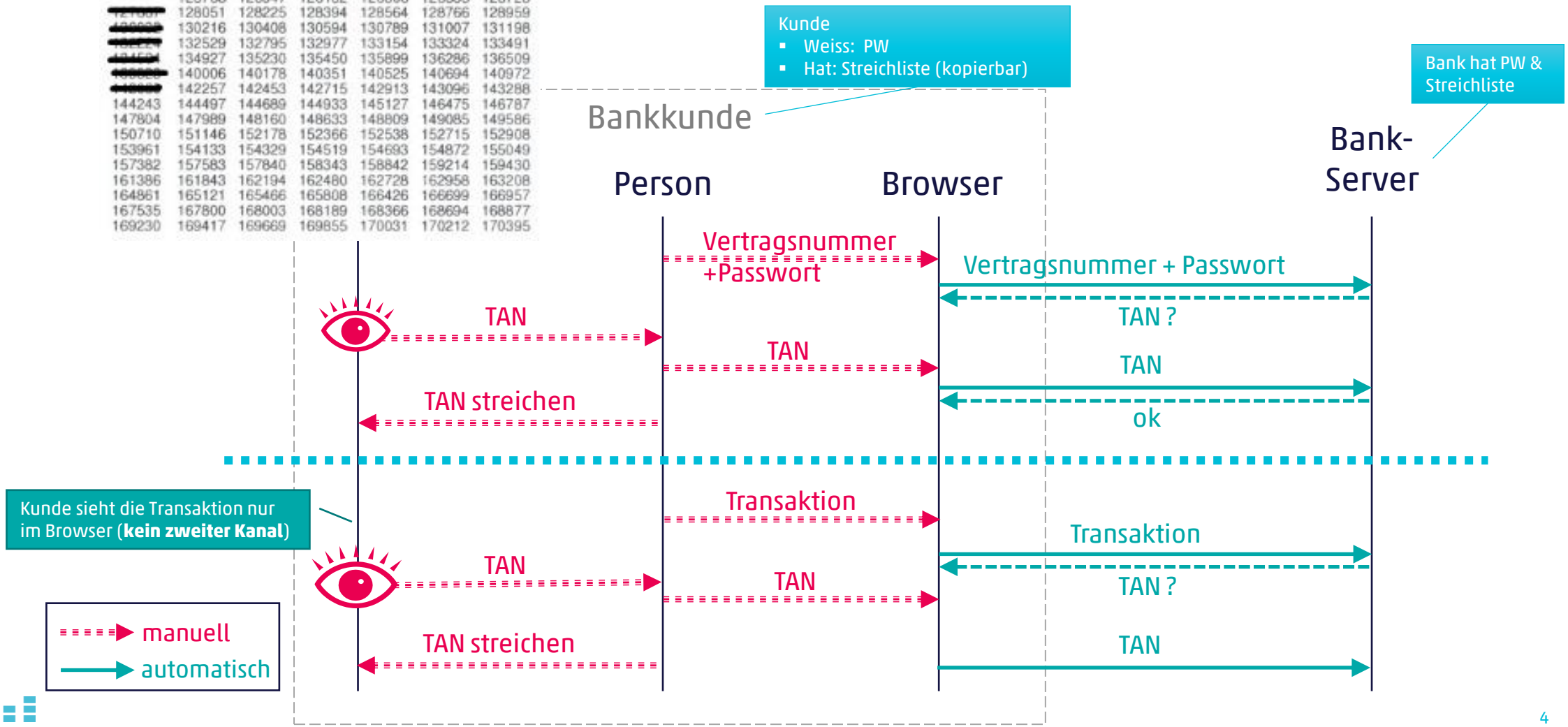
Mobile-Banking

- In einer App (typischerweise auf Smartphone)
- Vorteile:
  - Resistenter gegen
    - Session-Angriffe
    - Man-in-the-Middle
    - Malware

# PW und Streichliste

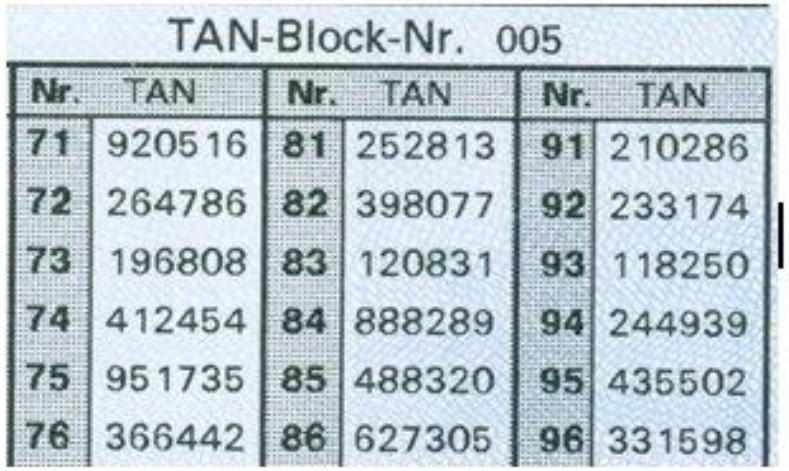
Banken z.B.:
- keine bekannt

| | | | | | |
|---|---|---|---|---|---|
| 119105 | 119561 | 119739 | 119914 | 120099 | 120290 |
| 121409 | 121590 | 121770 | 121956 | 122139 | 122317 |
| 123596 | 123794 | 123988 | 124179 | 124354 | 124531 |
| 125768 | 125947 | 126132 | 126306 | 126535 | 126723 |
| [redacted] | 128051 | 128225 | 128394 | 128564 | 128766 | 128959 |
| [redacted] | 130216 | 130408 | 130594 | 130789 | 131007 | 131198 |
| [redacted] | 132529 | 132795 | 132977 | 133154 | 133324 | 133491 |
| [redacted] | 134927 | 135230 | 135450 | 135899 | 136286 | 136509 |
| [redacted] | 140006 | 140178 | 140351 | 140525 | 140694 | 140972 |
| [redacted] | 142257 | 142453 | 142715 | 142913 | 143096 | 143288 |
| 144243 | 144497 | 144689 | 144933 | 145127 | 146475 | 146787 |
| 147804 | 147989 | 148160 | 148633 | 148809 | 149085 | 149586 |
| 150710 | 151146 | 152178 | 152366 | 152538 | 152715 | 152908 |
| 153961 | 154133 | 154329 | 154519 | 154693 | 154872 | 155049 |
| 157382 | 157583 | 157840 | 158343 | 158842 | 159214 | 159430 |
| 161386 | 161843 | 162194 | 162480 | 162728 | 162958 | 163208 |
| 164861 | 165121 | 165466 | 165808 | 166426 | 166699 | 166957 |
| 167535 | 167800 | 168003 | 168189 | 168366 | 168694 | 168877 |
| 169230 | 169417 | 169669 | 169855 | 170031 | 170212 | 170395 |



# PW und Matrixkarte (iTAN)

Banken z.B.:
- Bank Cler
- SZKB



# PW und dynamisches Passwort (TOTP)

Banken z.B.:
- Vontobel

Beispiel:
- RSAsecurID
- Vasco DIGIPASS


Kunde
- Weiss: PW
- Hat: RSA SecureID (nicht kopierbar)

Bank hat PW & TOTP

Bankkunde

Person | Browser | Bank-Server

Vertragsnummer + Passwort

Vertragsnummer + Passwort

Code ?

Code

Code

Code

ok

Transaktion

Transaktion

Code ?

Code

Code

Code

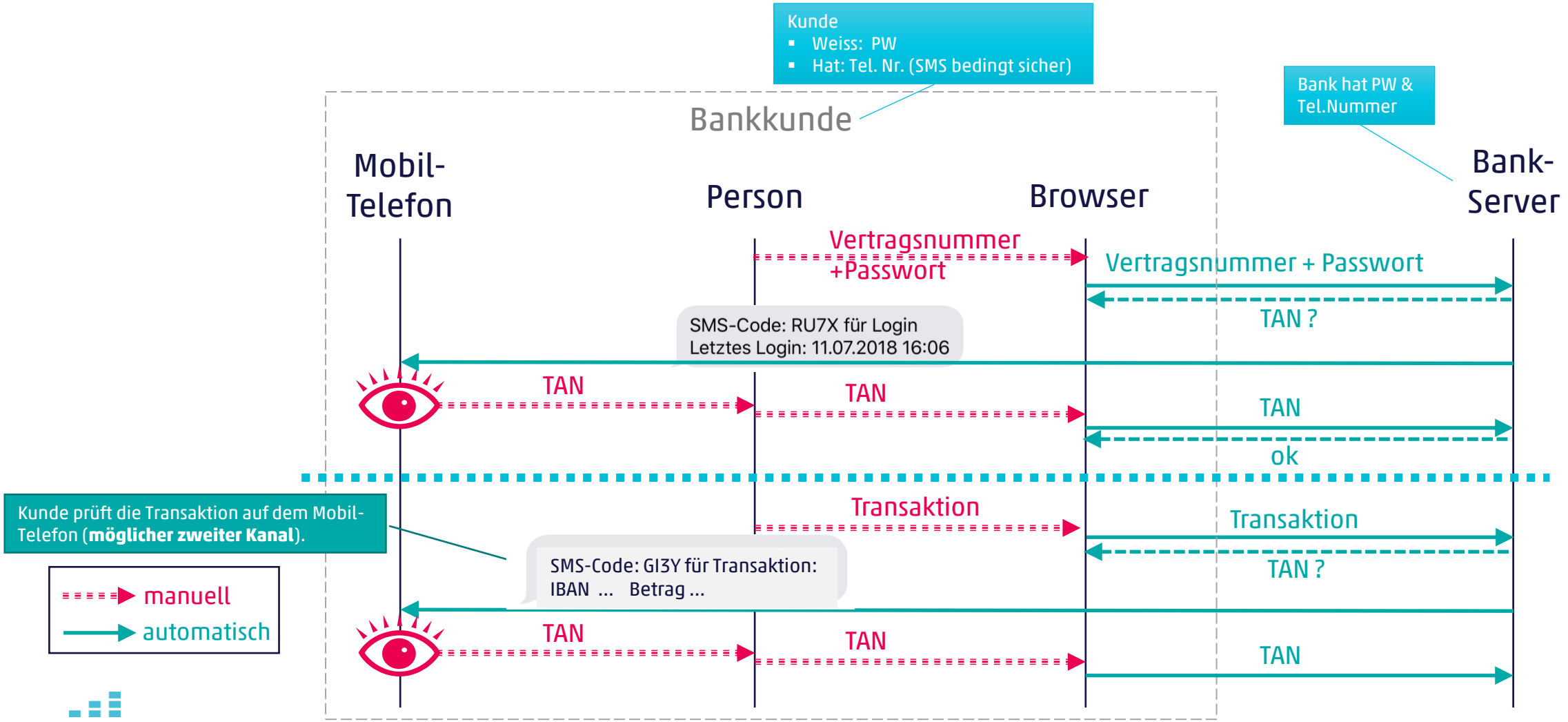
Kunde sieht die Transaktion nur im Browser (**kein zweiter Kanal**)

manuell

automatisch

# PW und mTAN (Code per SMS)

Banken z.B.:
- Schwyzer Kantonalbank
- Raiffeisen



# PW und Mobile ID

Banken z.B.:
- PostFinance


Kunde
- Weiss: PW
- Hat: SIM-Karte mit Zertifikat & SecretKey

Bank hat PW & Tel.Nummer

Bankkunde

Person | Browser | Swisscom Server | Bank-Server

Vertragsnummer +Passwort

Vertragsnummer + Passwort

Login!

«Login»?

PIN-Schutz der Mobile ID-Funktion möglich

ok

Sig(ok)

ok

ok

Keine Bindung zwischen Login-Bestätigung und Browser-Session. Anfällig auf Same-Time-Attacken.

Kunden prüft die Transaktion auf dem Mobil-Telefon (**möglicher zweiter Kanal**).

Transaktion

Transaktion

Trans.

Transaktion

ok

Sig(Trans.)

ok

manuell

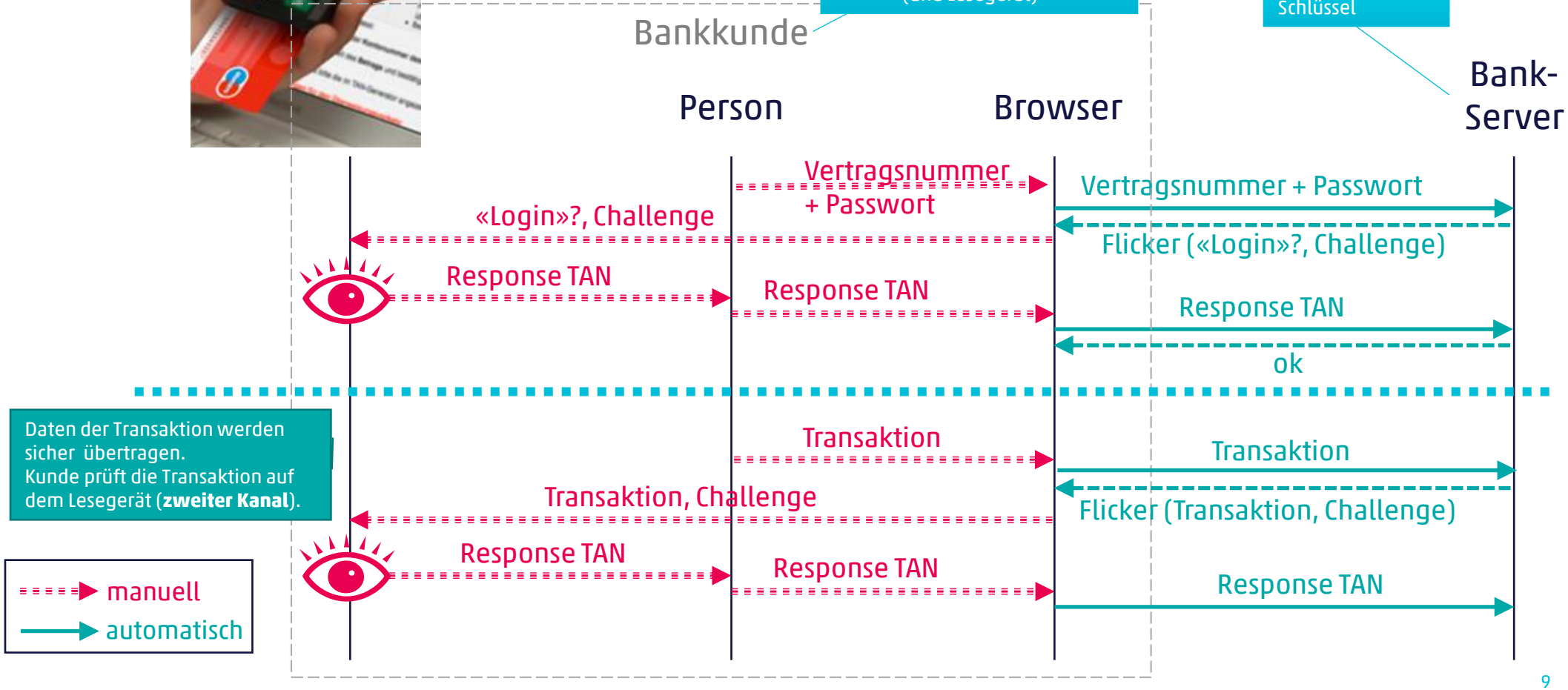
automatisch

# PW und Flicker

Banken z.B.:
- VPBank (FL)
- Sparkasse (D)

Kunde
- Weiss: PW
- Hat: Karte mit Schlüssel (und Lesegerät)

Bank hat PW & Schlüssel



# PW und/oder Karte mit Challenge/Response-Tool (Smart-Card mit PIN)

Banken z.B.:
- UBS (ohne PW, nur Access Card mit PIN)

Kunde
- Hat: Karte mit PIN-geschütztem Schlüssel (und Lesegerät)
- Weiss: PW und/oder PIN

Bank hat PW & Schlüssel

# Karte und verbundenes C/R-Token mit Zertifikat (Proxy)

Banken z.B.:
- UBS

Beispiel:
- IBM ZTIC

Kunde
- Hat: Karte mit PIN-geschütztem SK und Client-Zertifikat
  Token mit Server-Zertifikat (Pinning)
- Weiss: PIN

CA-Schlüssel

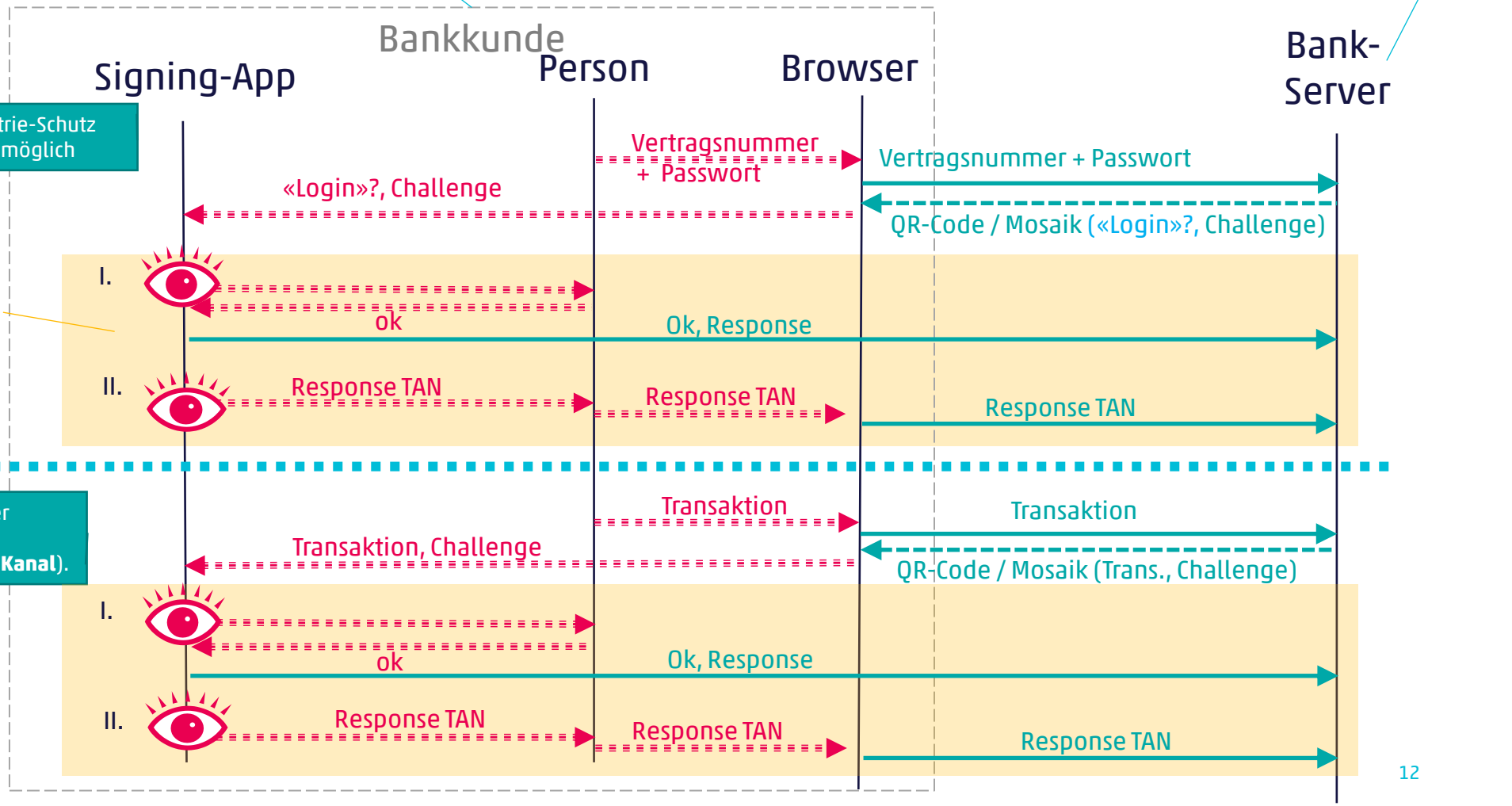
# PW und Signing-App
## optische Übertragung via Browser

Hier: Bank → Signing-App via Browser (optisch)
Signing-App → Bank direkt oder via Browser

Kunde
- Hat: App mit Schlüssel
- Weiss: PW und/oder PIN

Banken z.B.:
- Raiffeisen (PhotoTAN) – mit PW, ohne PIN
- ZKB (PhotoTAN) - mit PW, ohne PIN
- Valiant (Cronto Sign Swiss)
- CS (SecureSign) - mit PW, ohne PIN
- UBS - ohne PW, mit PIN, nur AuthN
- LGT

Bank hat PW & Schlüssel



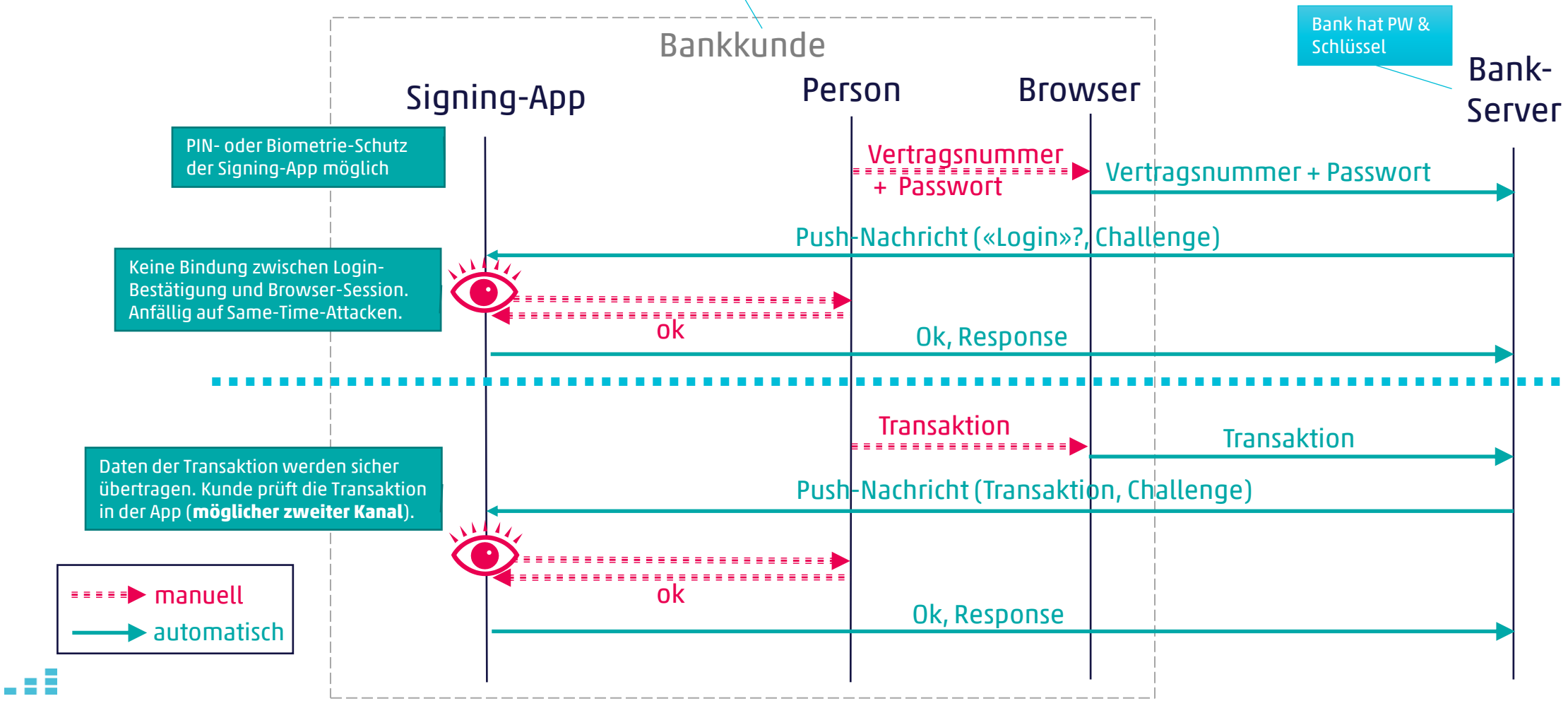
# PW und Signing-App
## Übertragungen Bank <-> App direkt

Hier: Bank → Signing-App direkt (PushTAN)
Signing-App → Bank direkt

Kunde
- Hat: App mit Schlüssel
- Weiss: PW und/oder PIN und/oder
- «Ist»: Fingerprint/FaceID

Beispiele:
- CLX PushTAN
- Entersekt Transakt
- Gemalto SafeNet MobilePASS+
- Vasco Digipass App

Banken z.B.:
- SGKB
- Julius Bär
- AKB
- Postfinance (PW & FaceID)
- Sparkassen (D)
- LGT



# Kobil AST mit 2 Geräten

Mögliche Gerätekombinationen:
- Computer – Computer
- Computer – Smartphone
- Smartphone – Smartphone
- Computer – Dediziertes Gerät

Banken z.B.:
- Migros Bank
- Vontobel

Kunde hat zwei aktivierte Geräte mit Client-Zertifikaten und PW geschütztem Secret-Key gehärtetem Browser (App) mit Server-Zertifikat Pinning

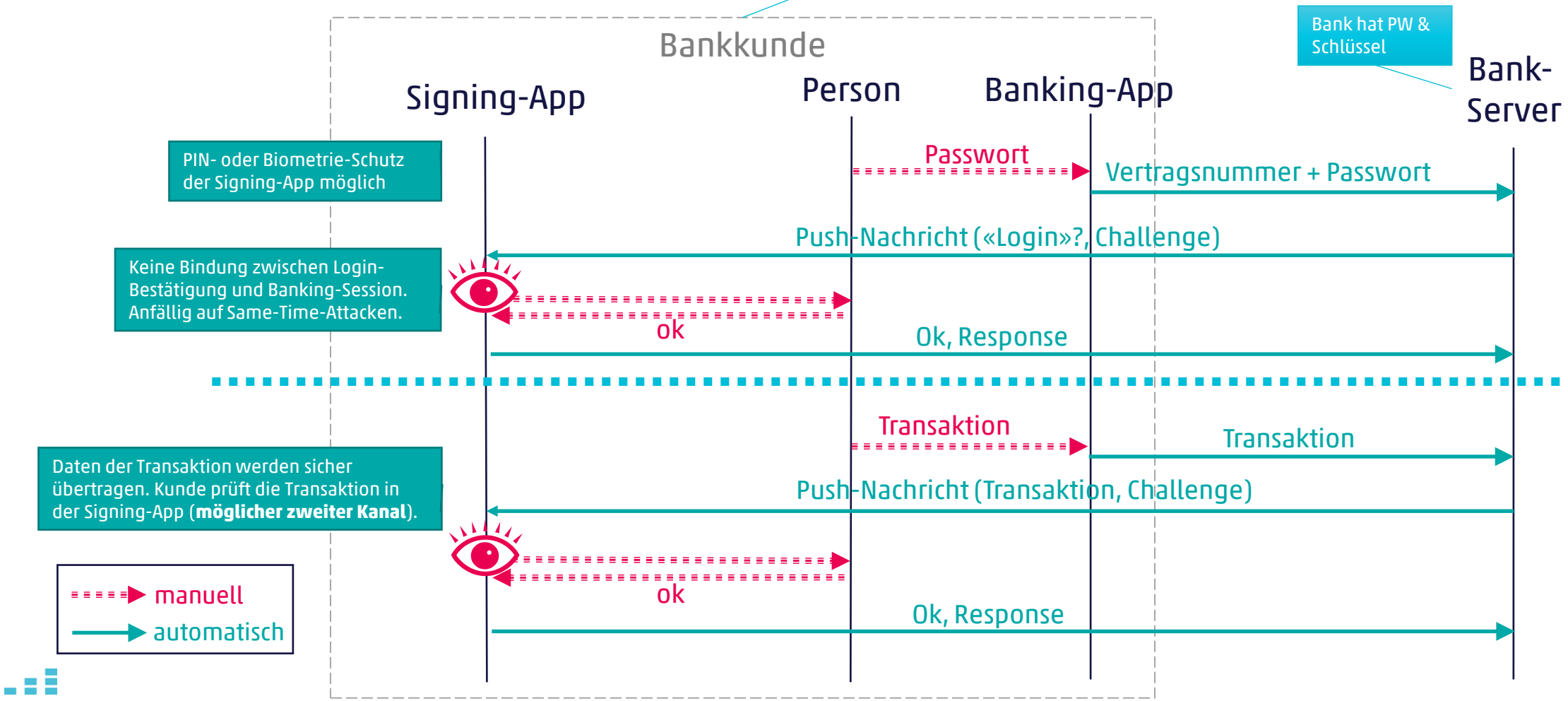
Bank hat PW & Schlüssel

# Banking-App und Signing-App
## Ein oder zwei Geräte

Hier: Bank → Signing-App direkt (PushTAN)
Signing-App → Bank direkt

Kunde
- Hat: App mit Schlüssel
- Weiss: PW und/oder PIN
und/oder
- «Ist»: Fingerprint/FaceID

Banken z.B.:
- Keine bekannt



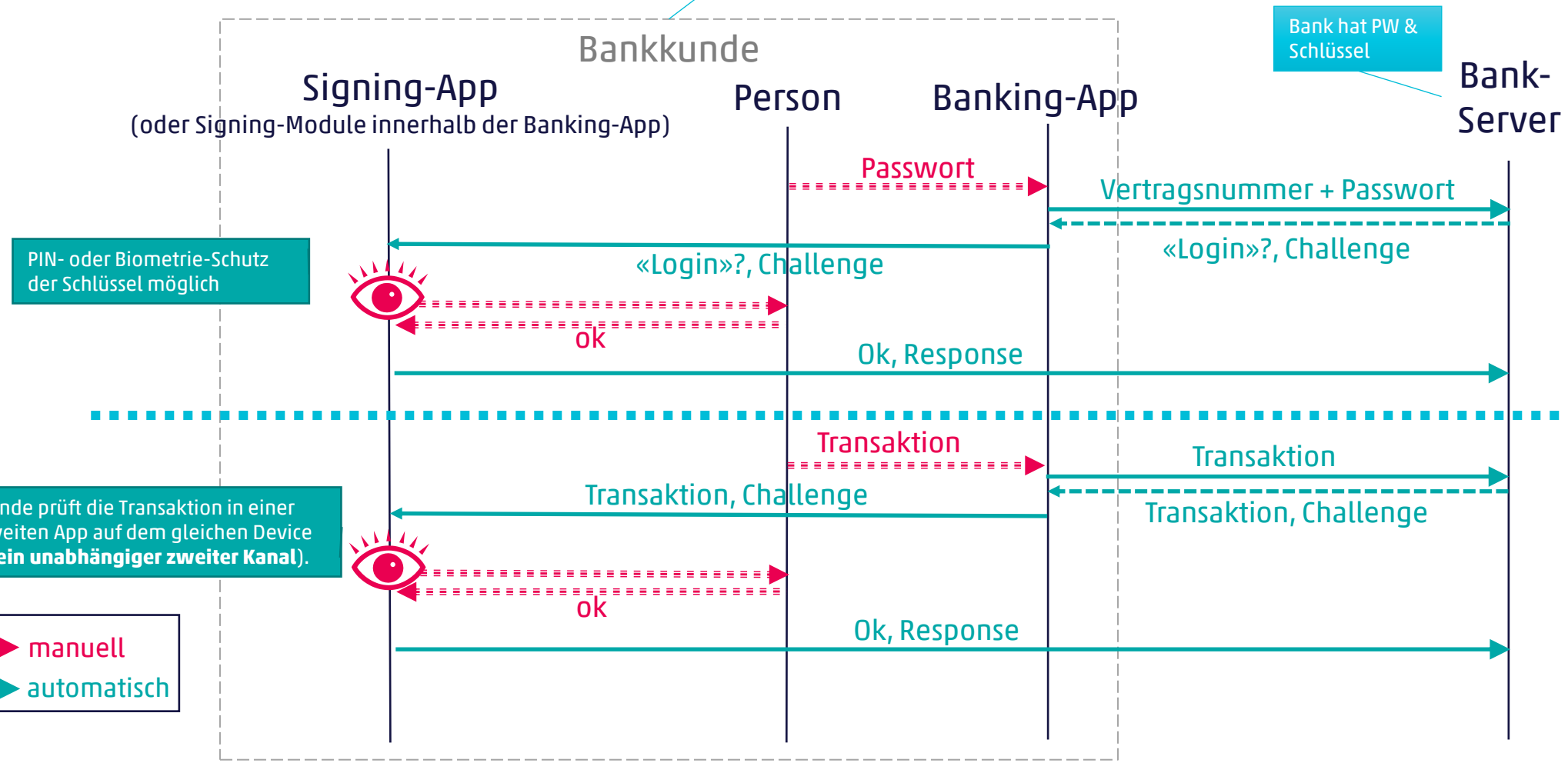
# Banking-App und Signing-App
## Ein Gerät, App2App-Kommunikation

Hier: Bank → Signing-App via Banking-App (App2App)
Signing-App → Bank direkt

Kunde
- Hat: App mit Schlüssel
- Weiss: PW und/oder PIN
und/oder
- «Ist»: Fingerprint/FaceID

Beispiele:
- OneSpan Cronto
- Vasco

Banken z.B.:
- Raiffeisenbank
- LGT (PW oder Biom.)



# Banking-App (mit 2FA)

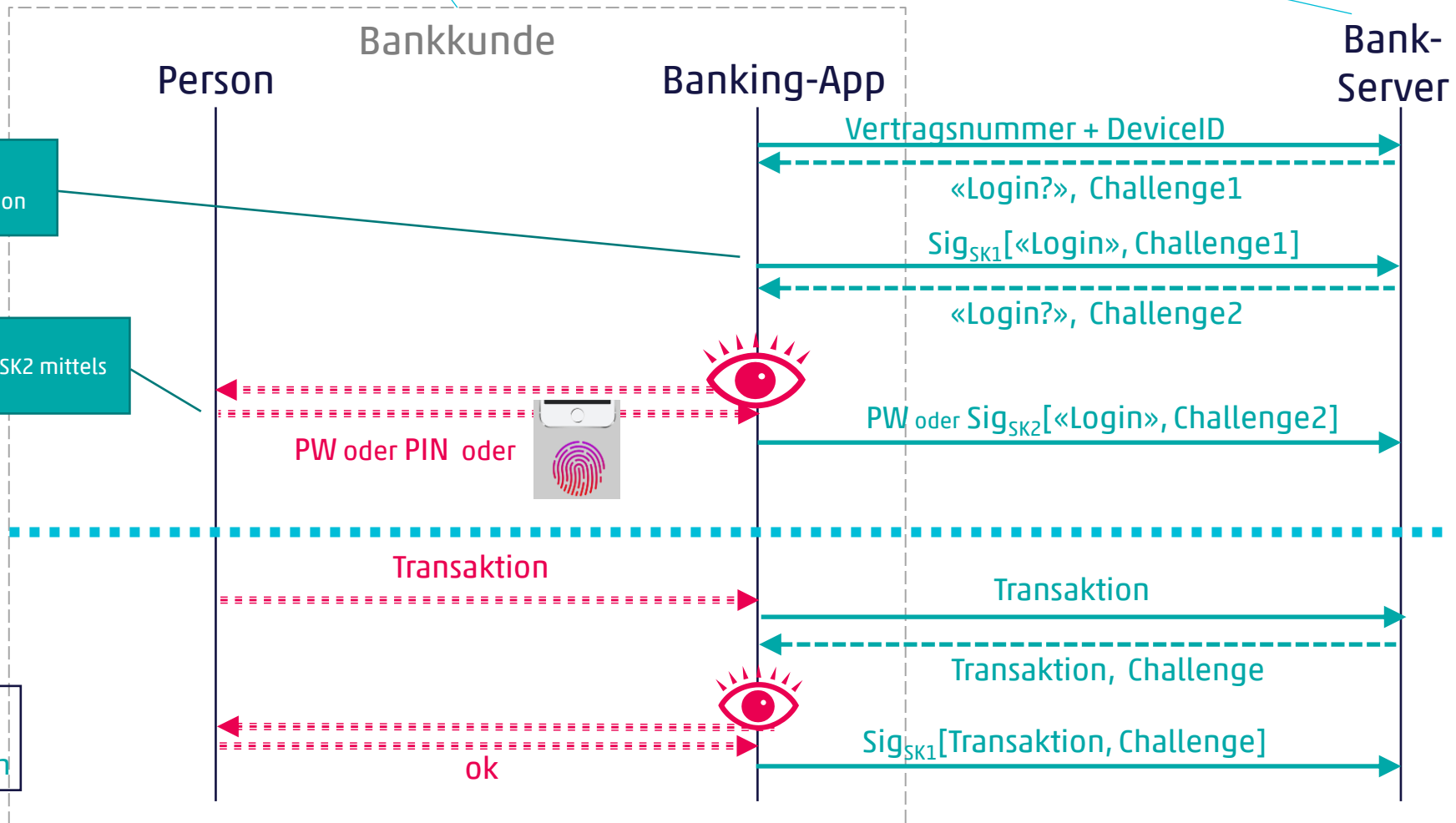
Beispiele:
- CLX

Banken z.B.:
- BJB
- SGKB

Kunde
- Hat: App mit Schlüssel (SK1 und ev. SK2)
- Weiss: PW oder PIN

oder
- «Ist»: Fingerprint/FaceID

Bank hat PW
und Schlüssel (PK1,PK2)

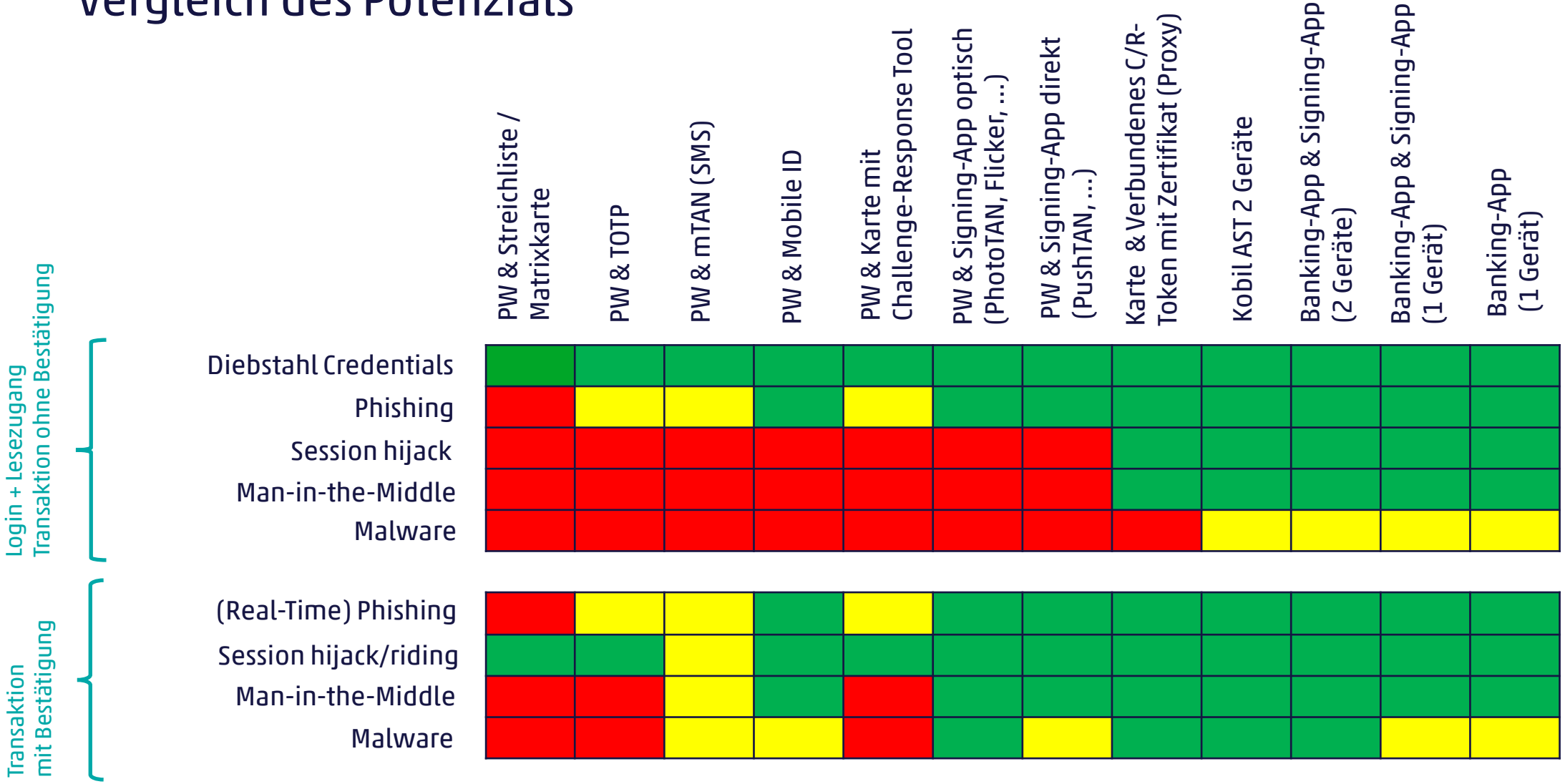



**Device Authentisierung:**
Automatisch, ohne Userinteraktion

**User Authentisierung:**
PW-Eingabe oder Freigabe vom SK2 mittels Biometrie oder PIN

manuell
automatisch

# Vergleich des Potenzials



# Was noch gesagt werden muss

- Kunden-Onboarding und -Reboarding, Geräte-Aktivierung und -Reaktivierung, PIN- und PW-Rücksetzung , Adressenänderung, Whitelist-Bildung usw. sind sicherheitsrelevante Operationen und müssen sicher gestaltet werden. Unsichere Prozesse in diesen Bereichen untergraben sonst die Sicherheit des gesamten digitalen Bankings.
- Bietet eine Bank mehrere Verfahren gleichzeitig an (ohne, dass der Kunde diese wirksam einschränken kann) ist das gesamte digitale Banking nur so sicher wie das schwächste dieser Verfahren. D.h. solange der Angreifer wählen kann, ist die zusätzliche Sicherheit, die das sicherere Verfahren bietet nutzlos – oft unabhängig davon welches Verfahren der Kunde faktisch verwendet.
- Authentisierung (inkl. 2FA) bietet keinen Schutz gegen Malware auf einem Device. Dagegen helfen nur Transaktionsbestätigungen auf einem zweiten Device, das über einen unabhängigen, sicheren zweiten Kanal mit der Bank kommuniziert und über ein eigenes Display verfügt, auf dem die Transaktion überprüft werden kann.

# Vielen Dank für Ihre Aufmerksamkeit_

Zuzana Trubini
zuzana.trubini@cnlab.ch
+41 55 214 33 34

info@cnlab-security.ch
+41 55 214 33 40

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland

cnlab