Authentisierung und Autorisierung im Digital Banking

cnlab security AG, Zuzana Trubini, Deniz Simsek
Januar 2026

cnlab

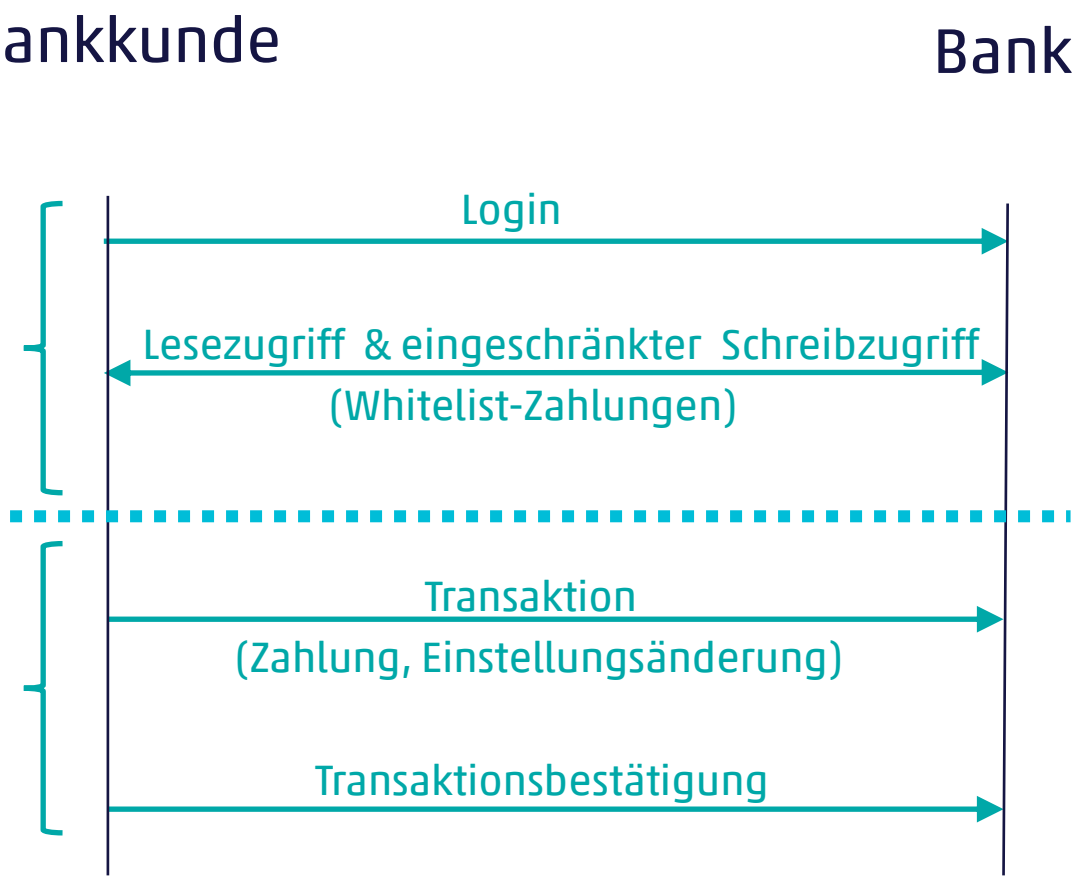
Authentisierung und Autorisierung

Login mit 2FA
(Authentisierung des Kunden)

➡ Kontoübersicht +
Zahlungen an Whitelist-Empfänger

Transaktionsbestätigung
(Autorisierung der Transaktion)

➡ spezielle Zahlungen +
sicherheitsrelevante Änderungen



E-Banking vs. Mobile-Banking

E-Banking

- im Browser (meist auf PCs)
- Falls auf dem PC: Smartphone kann als unabhängiges Zweit-Gerät eingesetzt werden: **2-Geräte-Lösungen**
  - ⇒ hohe Sicherheit gegen Malware
    - trotz hoher Verbreitung von Malware auf PCs
    - dank dem unabhängigen zweiten Faktor
  - ⇒ Sicherheit gegen Malware hängt stark vom zweiten Faktor ab

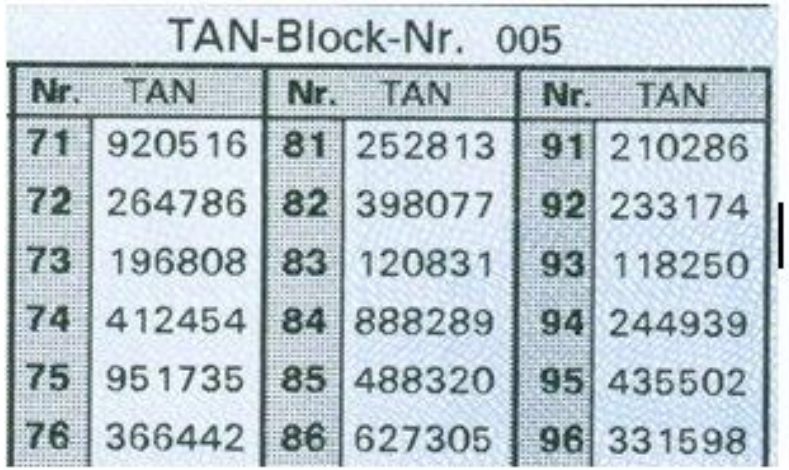
Mobile-Banking

- In einer Banking-App (meist auf Smartphones)
- Beim Arbeiten mit Smartphone ist meist kein Zweit-Gerät vorhanden: **Single-Device-Lösungen**
  - ⇒ mittelmässige Sicherheit gegen Malware, da
    - zwar wenig Malware auf Smartphones,
    - aber kein unabhängiger zweiter Faktor
  - ⇒ Härtung der App schützt gegen
    - Session-Angriffe
    - MitM (Phishing und Server Impersonation)

PW und Streichliste

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)



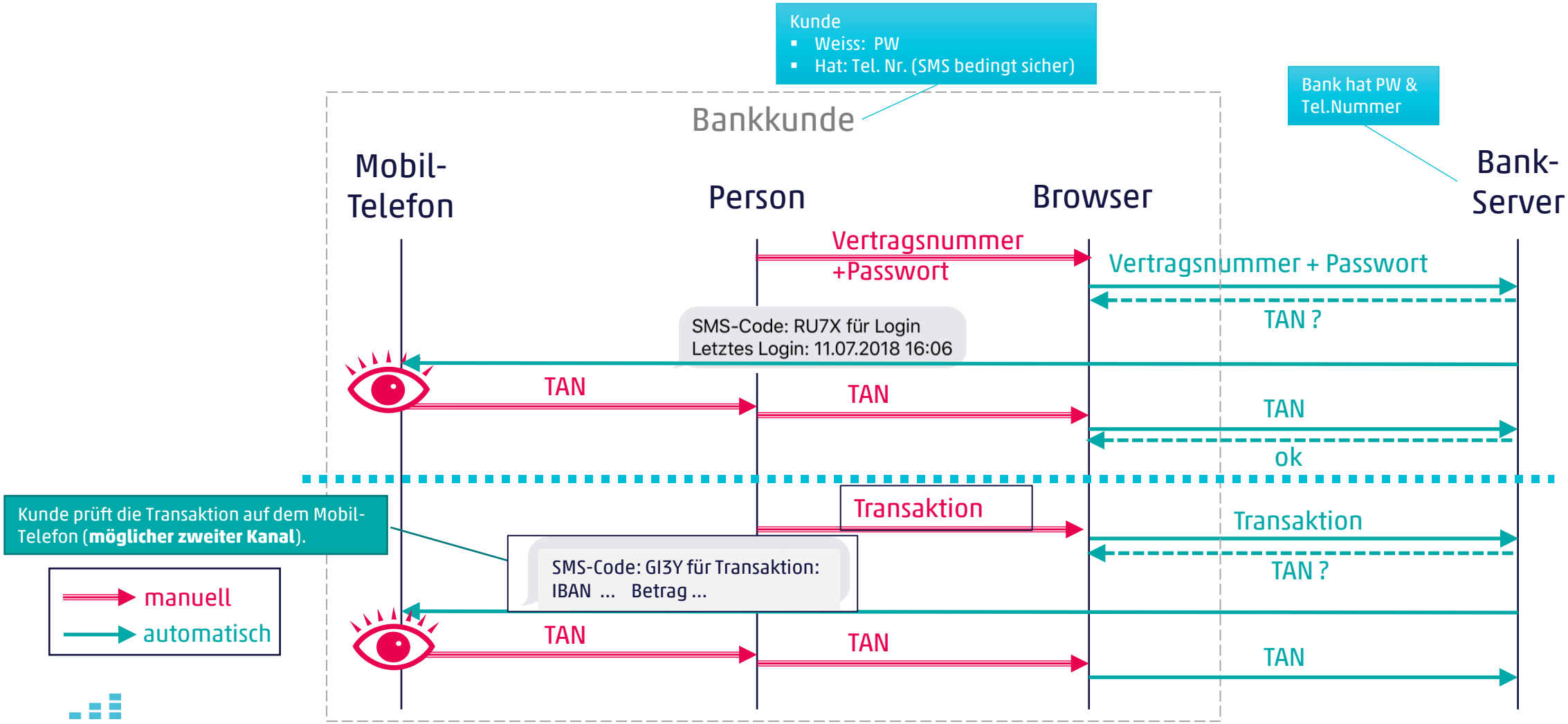
TAN-Block-Nr. 005

Nr.	TAN	Nr.	TAN	Nr.	TAN
71	920516	81	252813	91	210286
72	264786	82	398077	92	233174
73	196808	83	120831	93	118250
74	412454	84	888289	94	244939
75	951735	85	488320	95	435502
76	366442	86	627305	96	331598

PW und dynamisches Passwort (TOTP)

Beispiel:
- RSAsecurID
- Vasco DIGIPASS

PW und mTAN (Code per SMS)



PW und Mobile ID

Kunde
- Weiss: PW
- Hat: SIM-Karte mit Zertifikat & Secret Key (SK)

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 MFA-Fatigue und Same-Time-Attacken.

Transaktion

Transaktion

Trans.

Transaktion

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

ok

Sig(Transaktion)

ok

manuell

automatisch

PW und Flicker

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

Bank hat PW & Schlüssel

Bankkunde

Person | Browser | Bank-Server

Vertragsnummer + Passwort

«Login»?, Challenge

Vertragsnummer + Passwort

Flicker («Login»?, Challenge)

Response TAN

Response TAN

Response TAN

ok

Daten der Transaktion werden sicher übertragen.
Kunde prüft die Transaktion auf dem Lesegerät (**zweiter Kanal**).

Transaktion

Transaktion

Transaktion, Challenge

Flicker (Transaktion, Challenge)

Response TAN

Response TAN

Response TAN

manuell

automatisch

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

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

Bank hat PW & Schlüssel

Bankkunde

Person | Browser | Bank-Server

Übertragung auch via NFC möglich

Vertragsnummer + Passwort

Vertragsnummer + Passwort

Challenge

Challenge + PIN

Challenge

Response TAN

Response TAN

Response TAN

ok

Transaktion

Transaktion

Kunde gibt **die vom Browser verlangten** Positionen des IBANs ein (**kein unabhängiger zweiter Kanal**)

Positionen

Positionen (für IBAN)

IBAN an Positionen

PIN

TAN

TAN

TAN

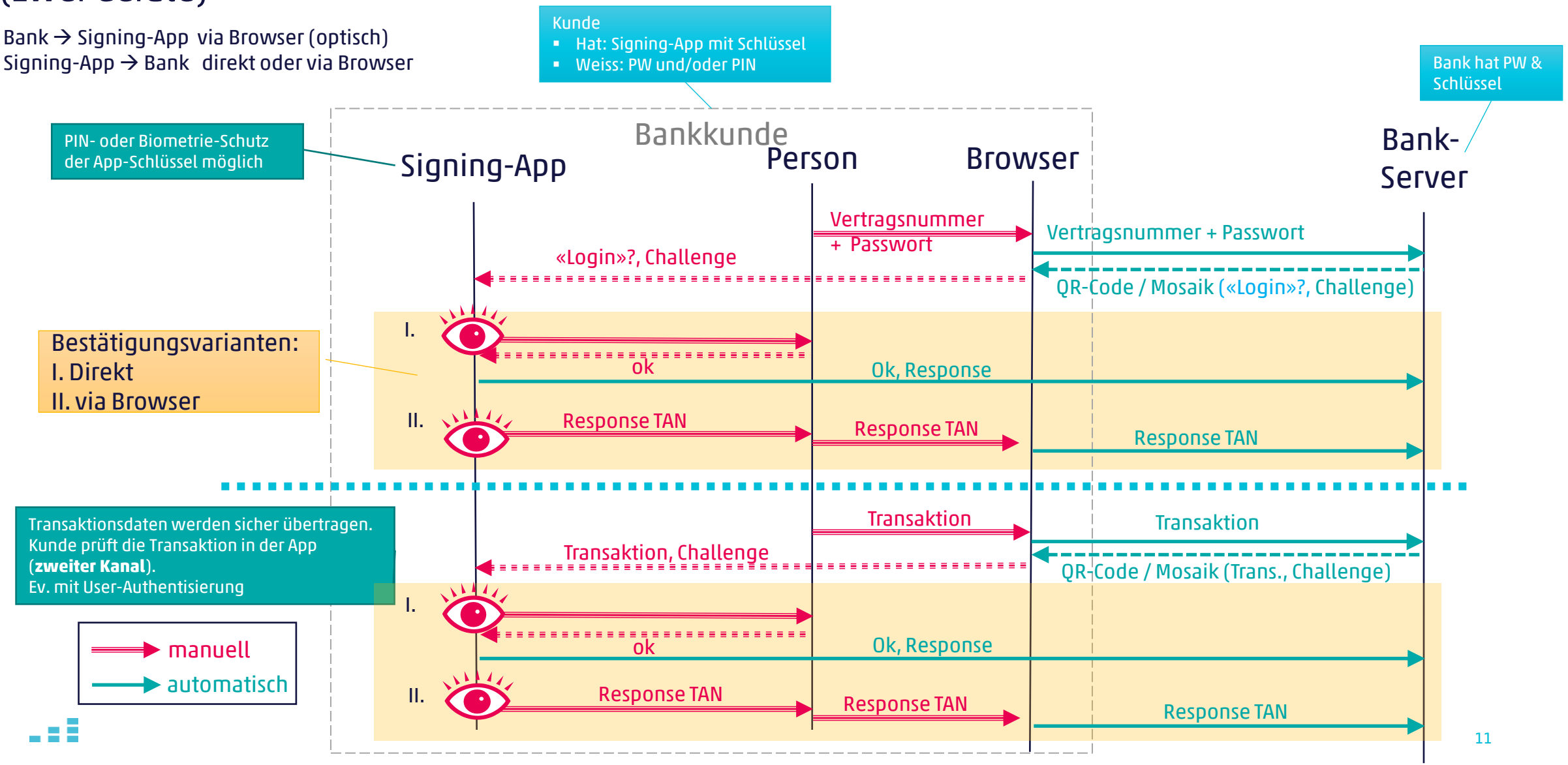
manuell

automatisch

PW und PhotoTAN-Signing-App mit optischer Übertragung via Browser

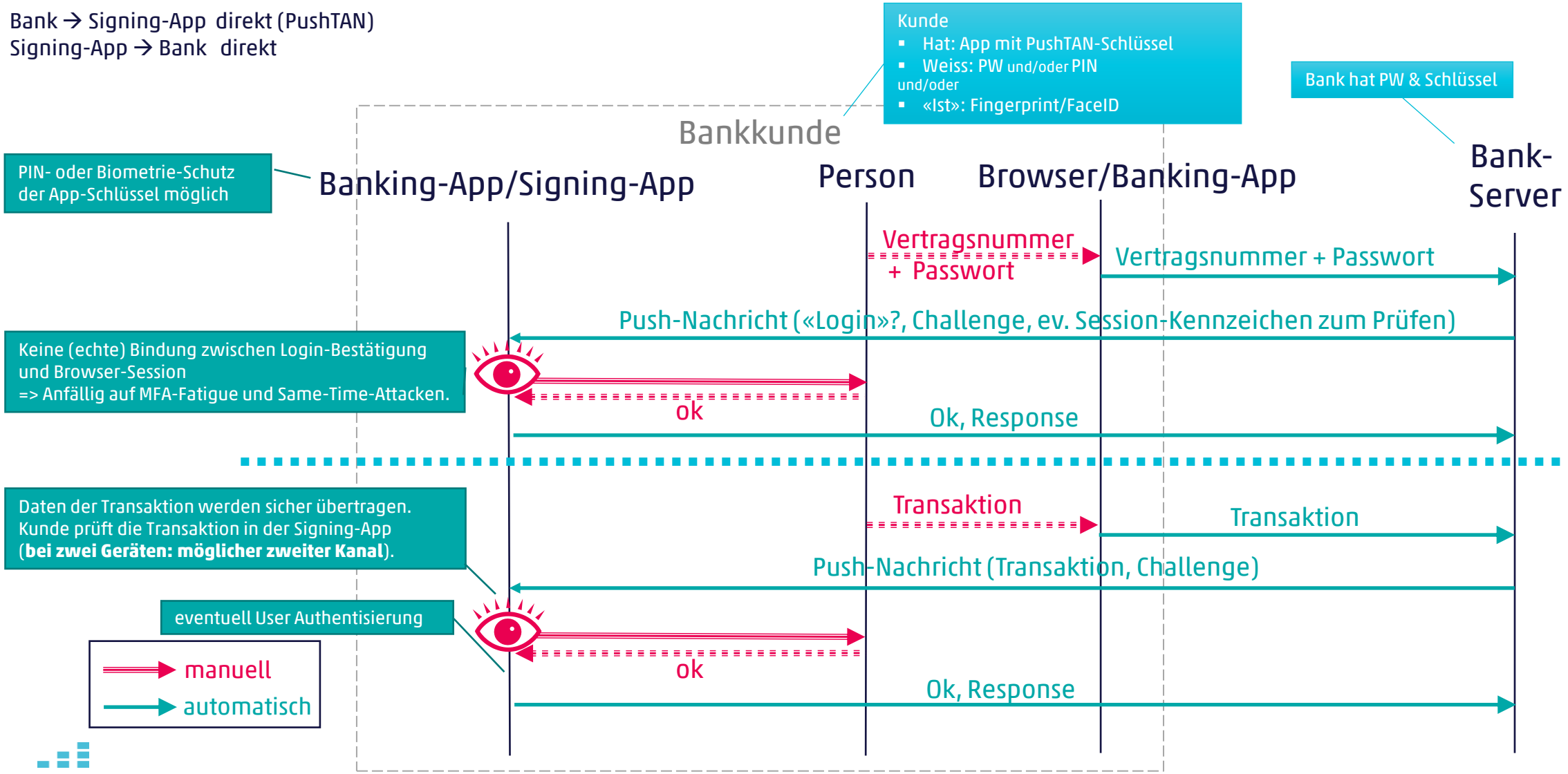
(zwei Geräte)

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

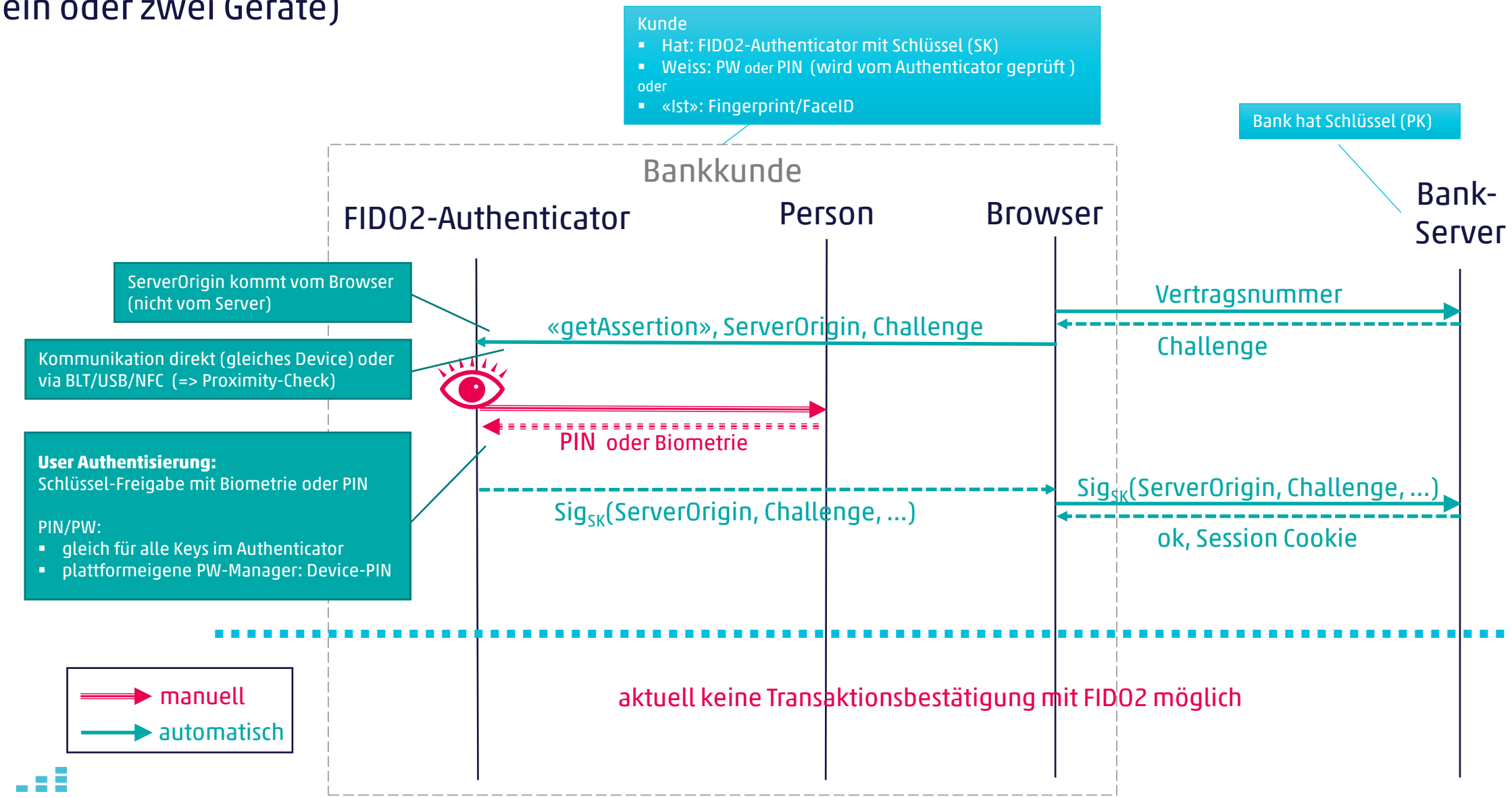


PW und PushTAN mit «ok»-Knopf
(ein oder zwei Geräte, Browser und/oder eine oder zwei Apps)

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

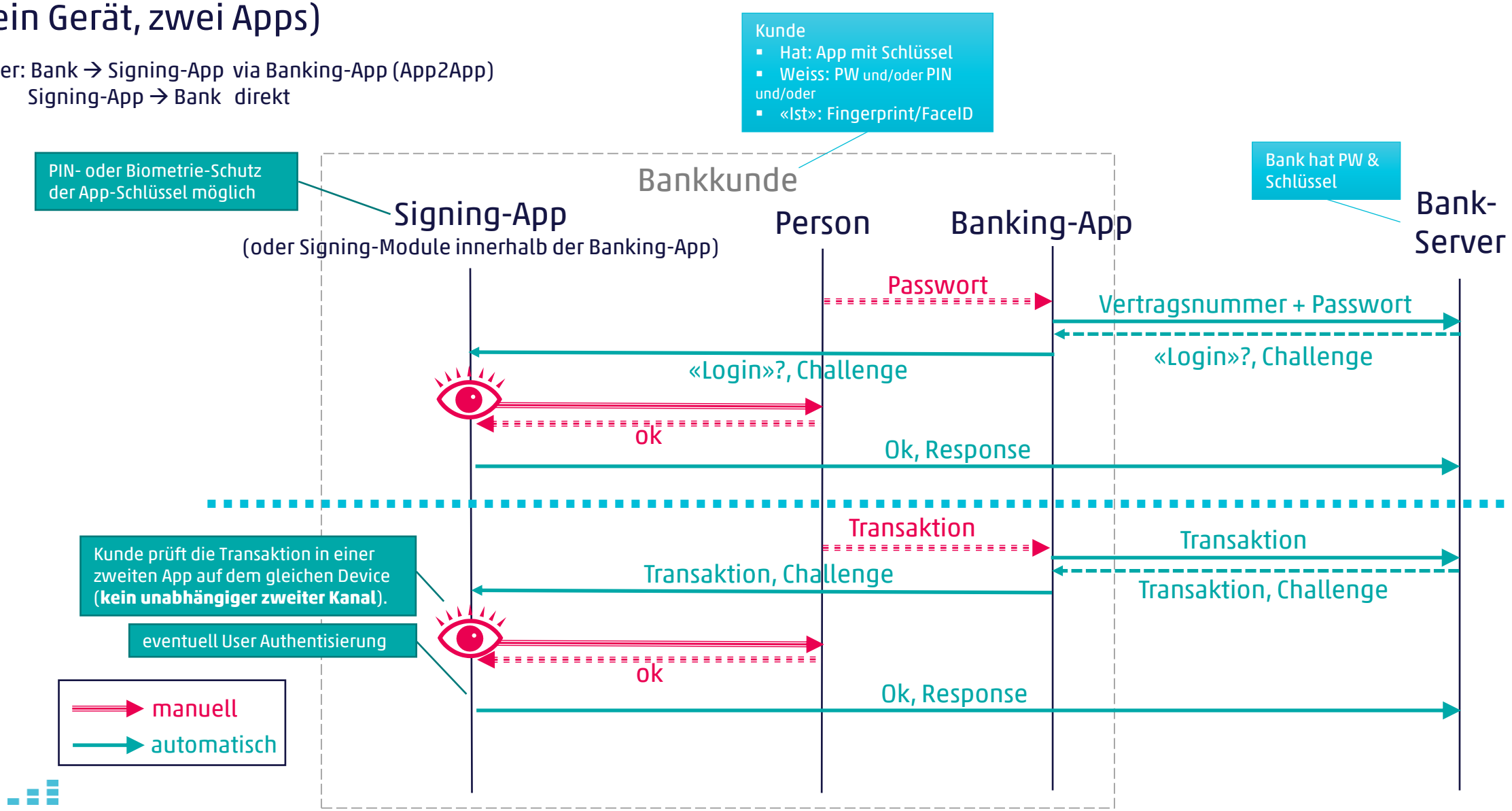


Browser und FIDO2
(ein oder zwei Geräte)

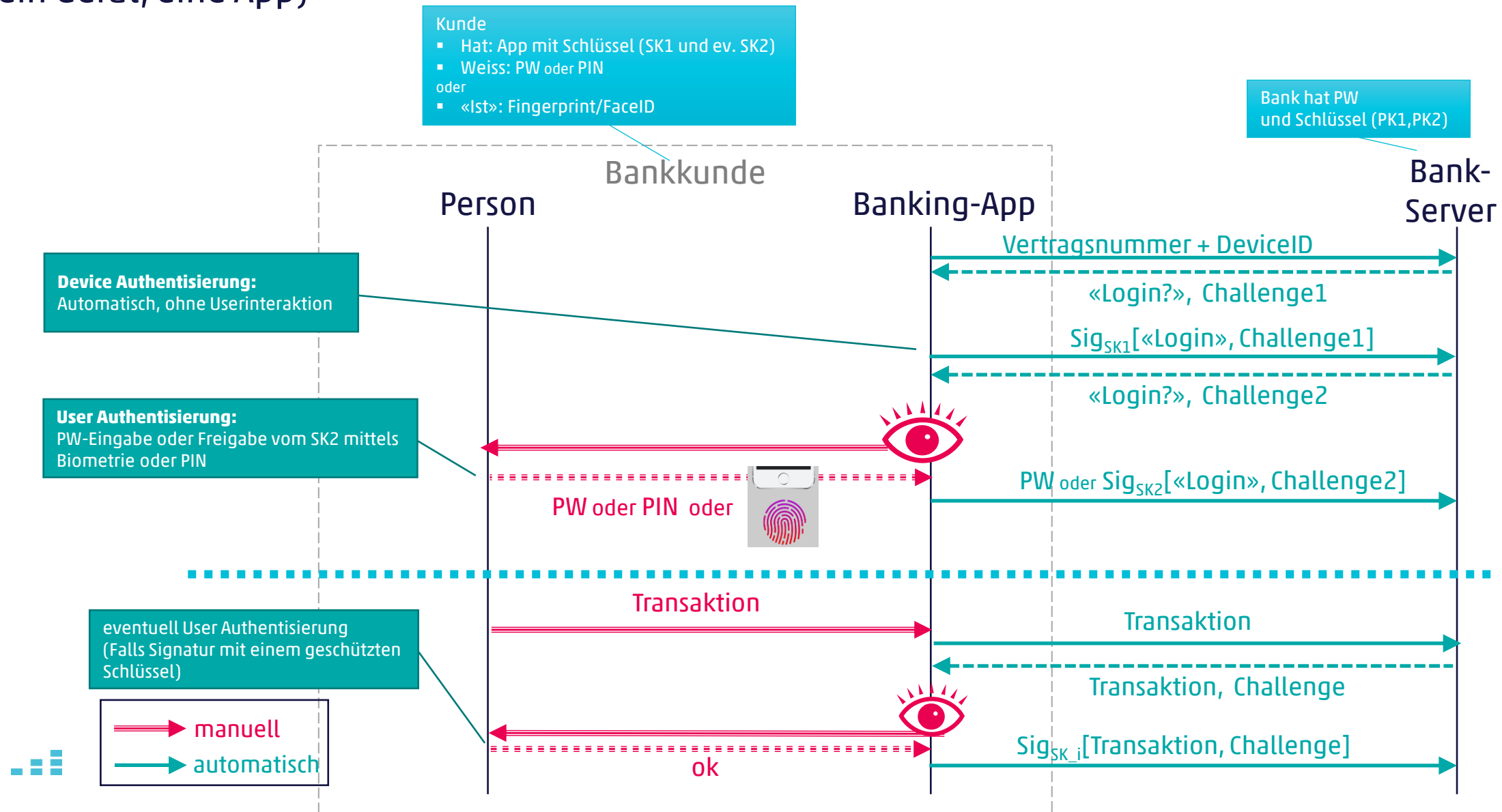


Banking-App und Signing-App mit App2App-Kommunikation
(ein Gerät, zwei Apps)

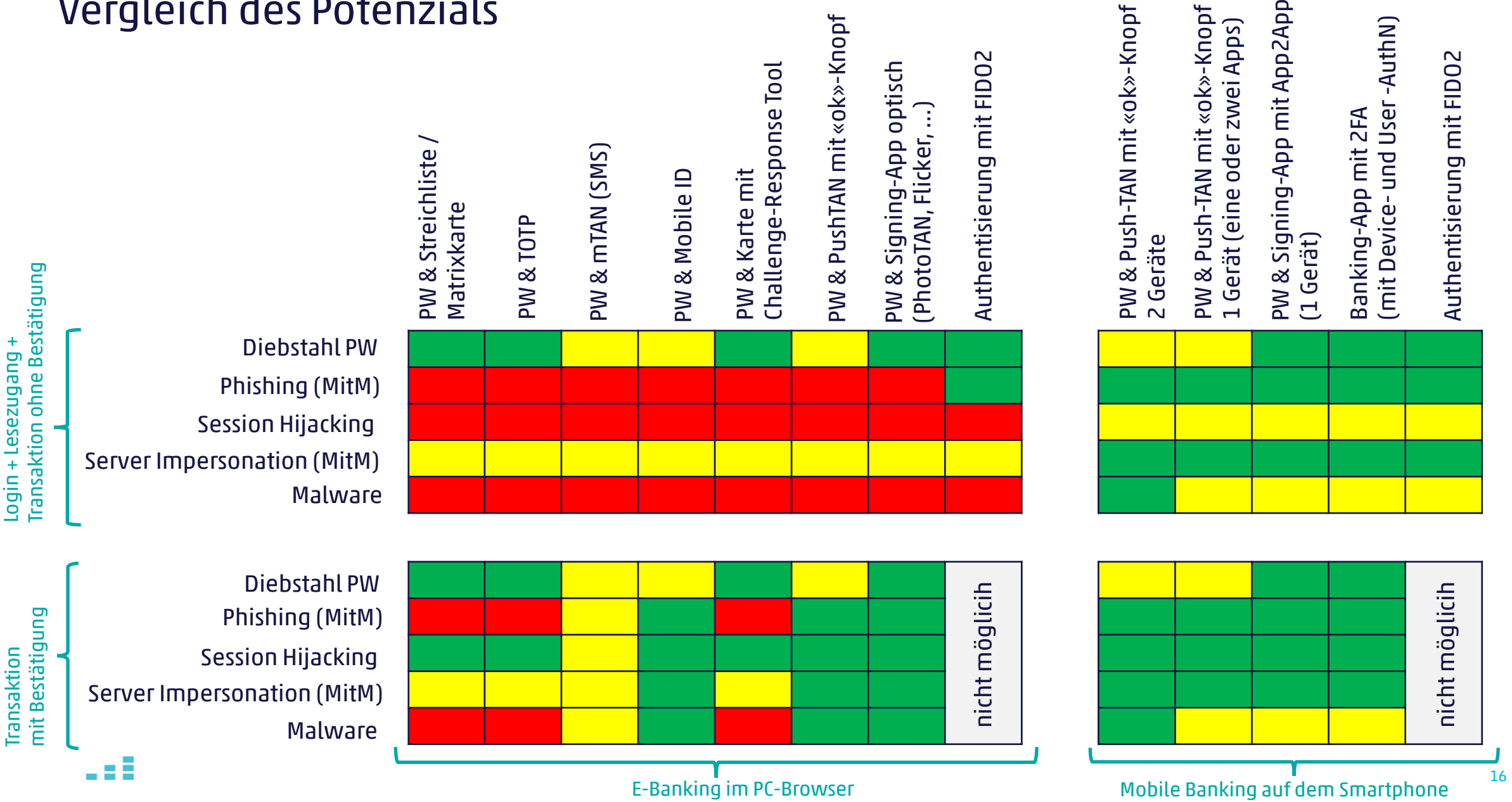
Hier: Bank → Signing-App via Banking-App (App2App)
Signing-App → Bank direkt



Banking-App mit 2FA (mit Device- und User-Authentisierung)
(ein Gerät, eine App)



Vergleich des Potenzials



Erklärung zur Tabelle

- Die Farbe reflektiert zwei Aspekte:
  1. Wie schwer ist es den Angriff durchzuführen?
  2. Wie hoch ist die Sicherheit im Falle eines solchen Angriffes?

- Annahmen
  - Schutz-Massnahmen:
    1. SMS ist nur mittelmässig sicher (SS7-Angriffe, SIM-Swapping, bösartige Apps können SMS lesen, ...)
    2. Login-Bestätigung über Push-TAN und Mobile-ID ist nur mittelmässig sicher («ok»-Knopf –> MFA-Fatigue, Same-Time Angriffe)
    3. FIDO2 bietet aktuell keine Möglichkeit für Transaktions-Bestätigungen
  - Angriffe:
    1. Phishing (MitM): erfolgt immer via Browser (Phishing-Apps aktuell nicht verbreitet)
    2. Session Hijacking: ist bei PC einfach, bei Smartphone schwieriger
    3. Server Impersonation (MitM): ist bei PC schwierig, Apps sind (dank Zertifikats-Pinning) sicher
    4. Malware: ist bei PC verbreitet, bei Smartphone nicht

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. Der Angreifer wird das schwächste wählen Verfahren wählen.
- Authentisierung (inkl. 2FA) bietet keinen Schutz gegen Malware auf einem Device. Dagegen helfen nur Transaktionsbestätigungen auf einem zweiten Device, auf dem die Transaktion überprüft werden kann.
- Transaktions-Bestätigungen auf dem gleichen Device ohne User-Authentisierung bieten praktisch keinen Schutz. Jeder der Zugriff zu einem Gerät mit einer eingeloggten App hat, kann eine Transaktion eingeben und bestätigen.
  => Single-Device-Lösungen sollten für Transaktions-Bestätigungen User-Authentisierung verlangen.

Vielen Dank für Ihre Aufmerksamkeit_

Zuzana Trubini, Deniz Simsek
zuzana.trubini@cnlab.ch
deniz.simsek@cnlab.ch

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

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

cnlab