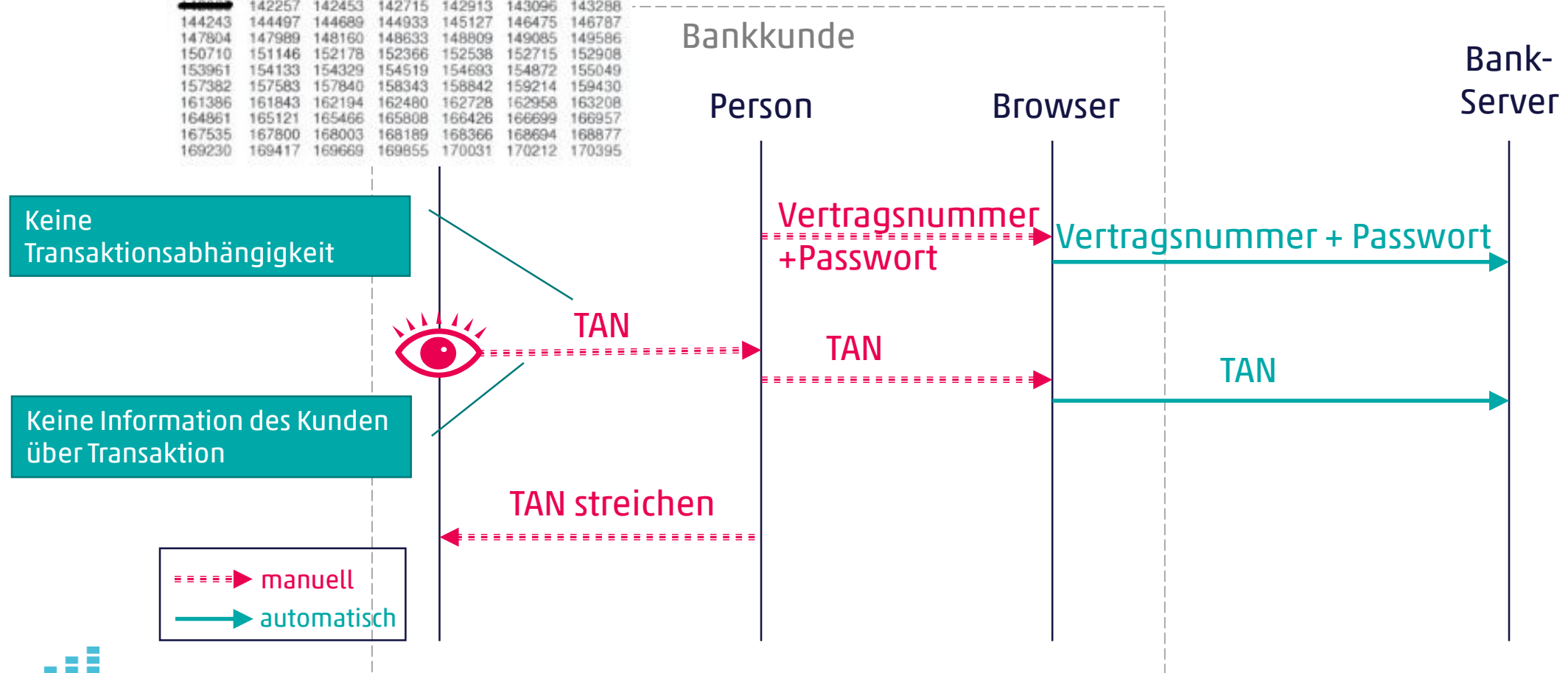


# E-Banking-Authentisierung

cnlab security AG, Martina Minges  
14.02.2019

# Streichliste

<del>121601</del>	119105	119561	119739	119914	120099	120290
<del>121602</del>	121409	121590	121770	121956	122139	122317
<del>121603</del>	123596	123794	123988	124179	124354	124531
<del>121604</del>	125768	125947	126132	126306	126535	126723
<del>121605</del>	128051	128225	128394	128564	128766	128959
<del>121606</del>	130216	130408	130594	130789	131007	131198
<del>121607</del>	132529	132795	132977	133154	133324	133491
<del>121608</del>	134927	135230	135450	135899	136286	136509
<del>121609</del>	140006	140178	140351	140525	140694	140972
<del>121610</del>	142257	142453	142715	142913	143096	143288
<del>121611</del>	144243	144497	144689	144933	145127	146475
<del>121612</del>	147804	147989	148160	148633	148809	149085
<del>121613</del>	150710	151146	152178	152366	152538	152715
<del>121614</del>	153961	154133	154329	154519	154693	154872
<del>121615</del>	157382	157583	157840	158343	158842	159214
<del>121616</del>	161386	161843	162194	162480	162728	162958
<del>121617</del>	164861	165121	165466	165808	166426	166699
<del>121618</del>	167535	167800	168003	168189	168366	168694
<del>121619</del>	169230	169417	169669	169855	170031	170212
<del>121620</del>						170395



# Matrixkarte (iTAN)

Banken z.B.:

- Bank Cler
- SZKB

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

Keine Information des Kunden  
über Transaktion

====> manuell  
————> automatisch

Bankkunde

Person

Browser

Bank-  
Server

Vertragsnummer  
+Passwort

Vertragsnummer + Passwort

Position

Position

TAN

TAN

TAN

# mTAN (Code per SMS)

Banken z.B.:

- Schwyzer Kantonalbank
- Zürcher Kantonalbank
- St.Galler Kantonalbank
- Raiffeisen

Bankkunde

Mobil-  
Telefon

Person

Browser

Bank-  
Server

Transaktionsabhängigkeit und  
Information des Kunden über  
Transaktion möglich.

Vertragsnummer  
+Passwort

Vertragsnummer + Passwort

SMS-Code: RU7X für Login  
Letztes Login: 11.07.2018 16:06

====> manuell  
—> automatisch



TAN

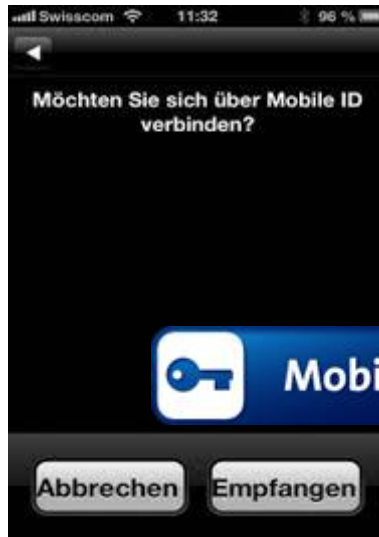
TAN

TAN



# Mobile ID

Banken z.B.:  
- PostFinance



Bankkunde

Person

Browser

Swisscom  
Server

Bank-  
Server

PIN-Schutz der Mobile ID-  
Funktion möglich

Kein Abtippen

Transaktionsabhängigkeit  
und Information des Kunden  
über Transaktion möglich.

Vertragsnummer  
+ Passwort

Vertragsnummer + Passwort

«Login»?

Login!

ok

ok, Signatur

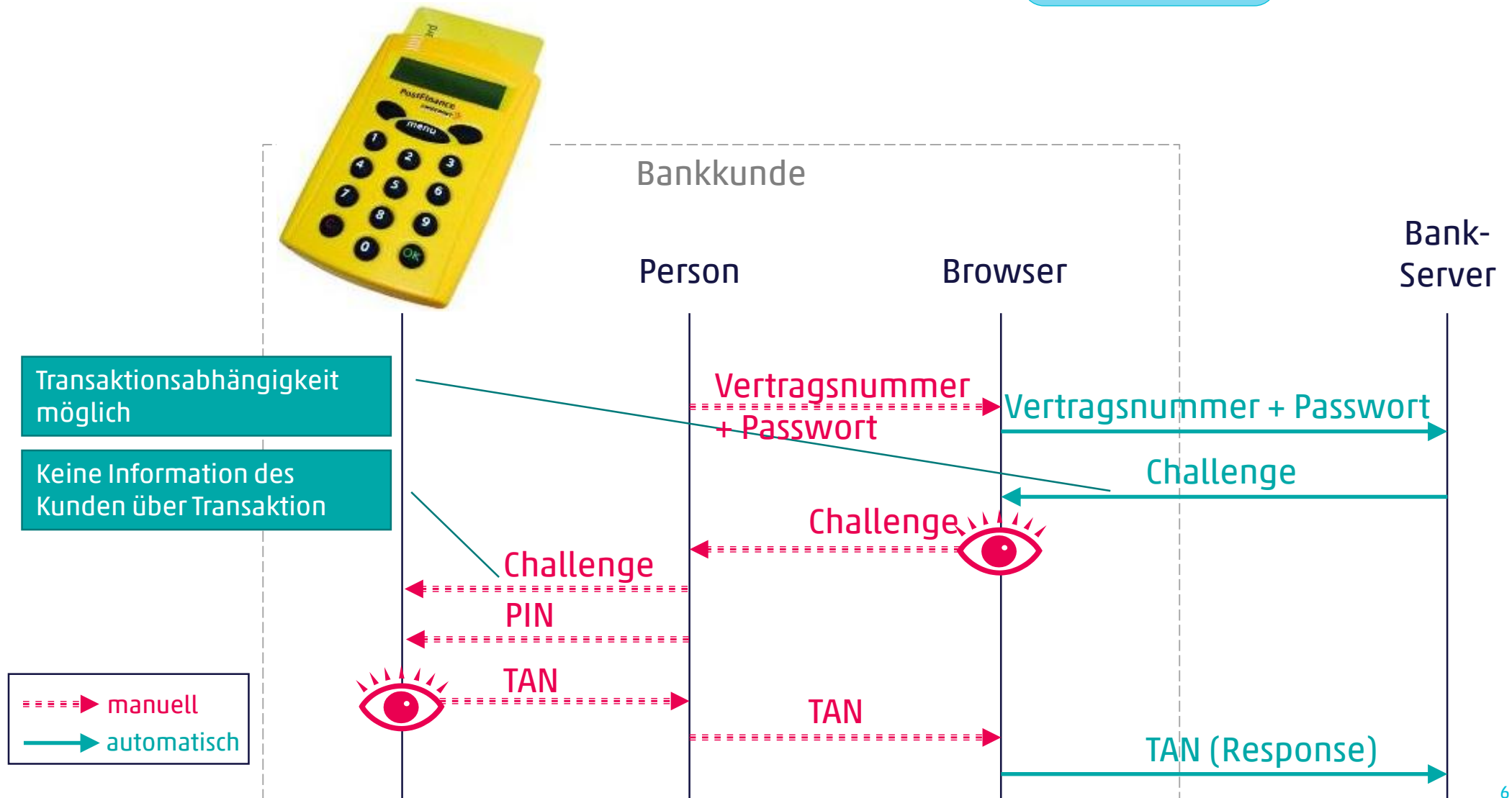
ok

=====► manuell  
—————► automatisch

# Challenge/Response-Tools (Smart-Card mit PIN)

Banken z.B.:

- UBS
- PostFinance



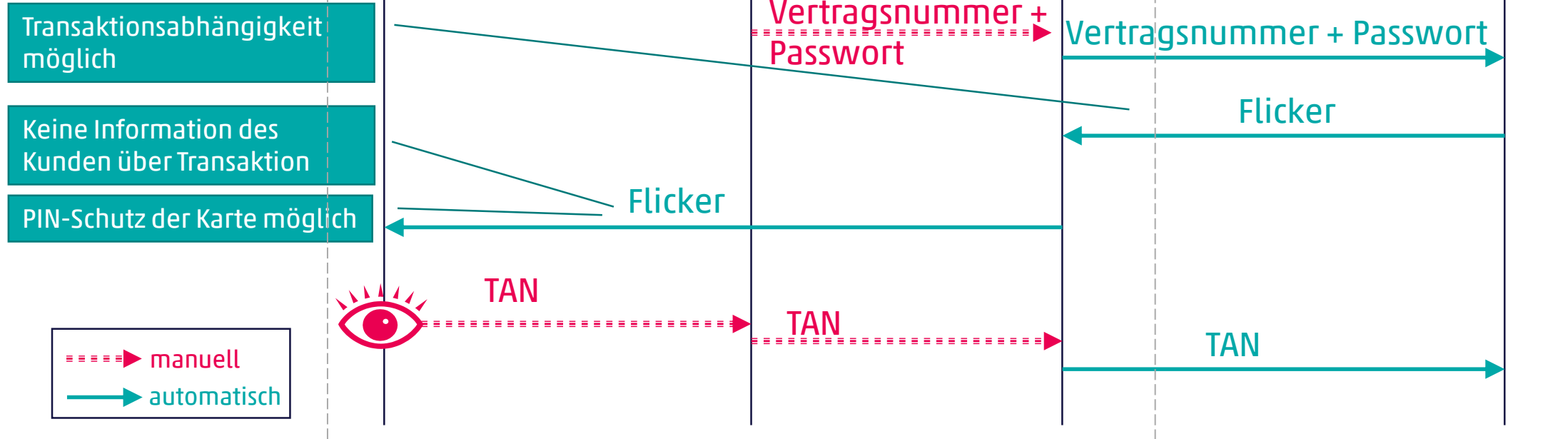


# Flicker



Banken z.B.:

- VPBank (FL)
- Sparkasse (D)

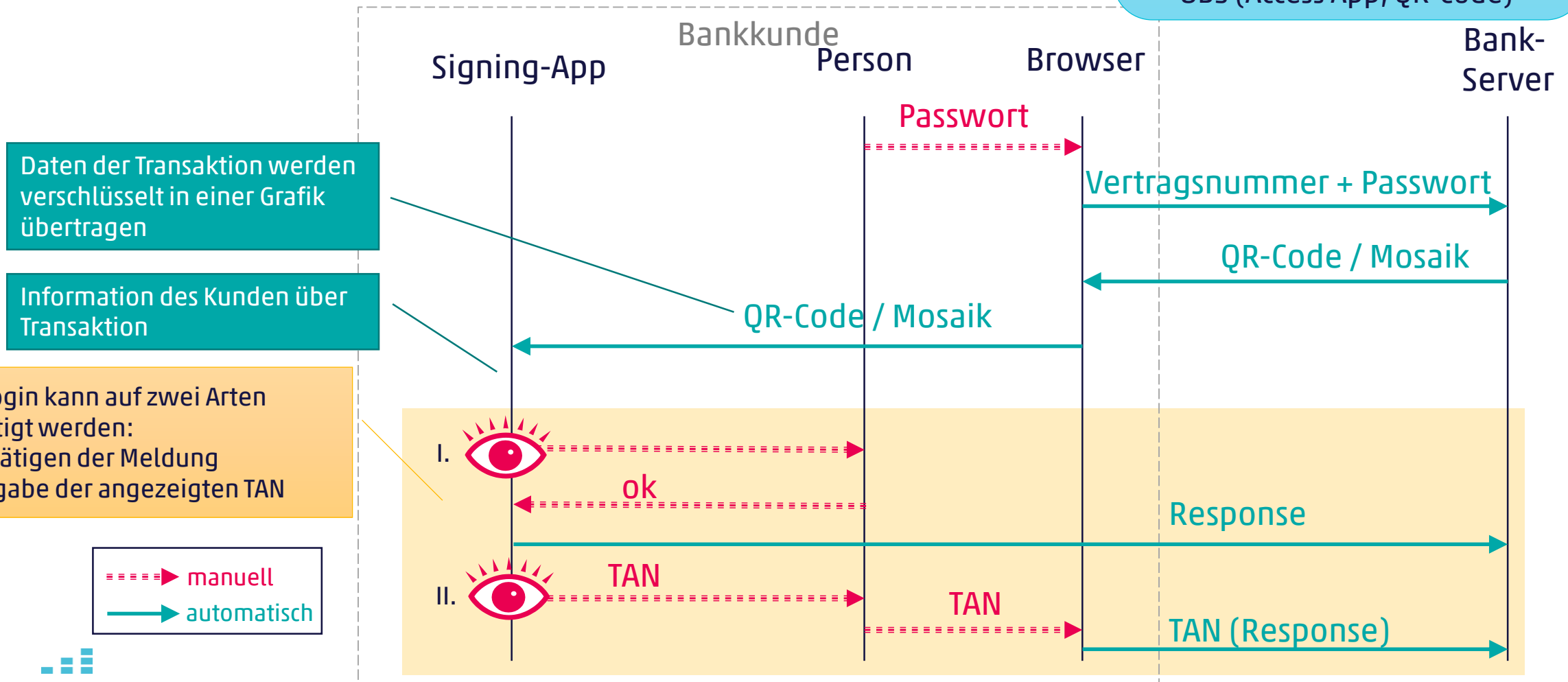


# Signing-Apps: 2 Geräte (graphisch)

Bei Betrieb auf einem Gerät ist der Ablauf wie bei der Push-Authentication.

Banken z.B.:

- Raiffeisen (PhotoTAN)
- ZKB (PhotoTAN)
- Valiant (Cronto Sign Swiss)
- CS (SecureSign)
- UBS (Access App, QR-Code)





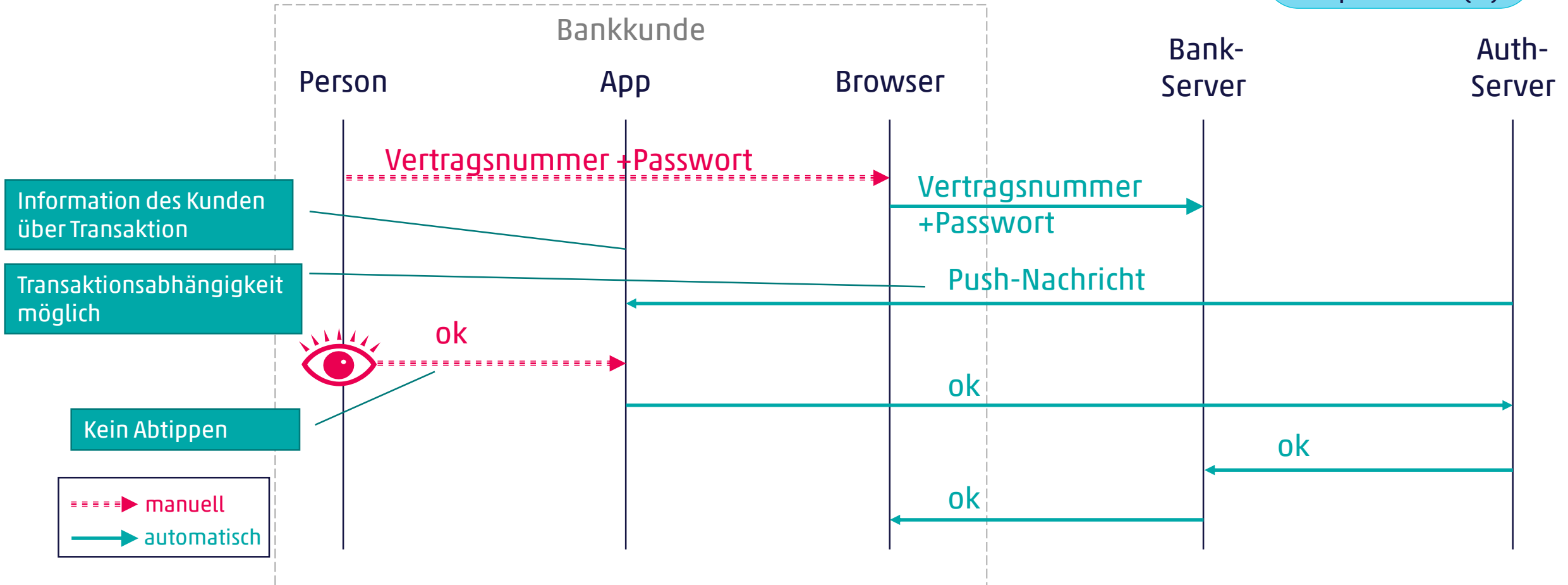
# Push-Authentication: 2 Geräte

Beispiele:

- CLX PushTAN
- Entersekt Transakt
- Gemalto SafeNet MobilePASS+
- Vasco Digipass App
- UBS Access App

Banken z.B.:

- SGKB
- Julius Bär
- AKB
- UBS
- Sparkassen (D)



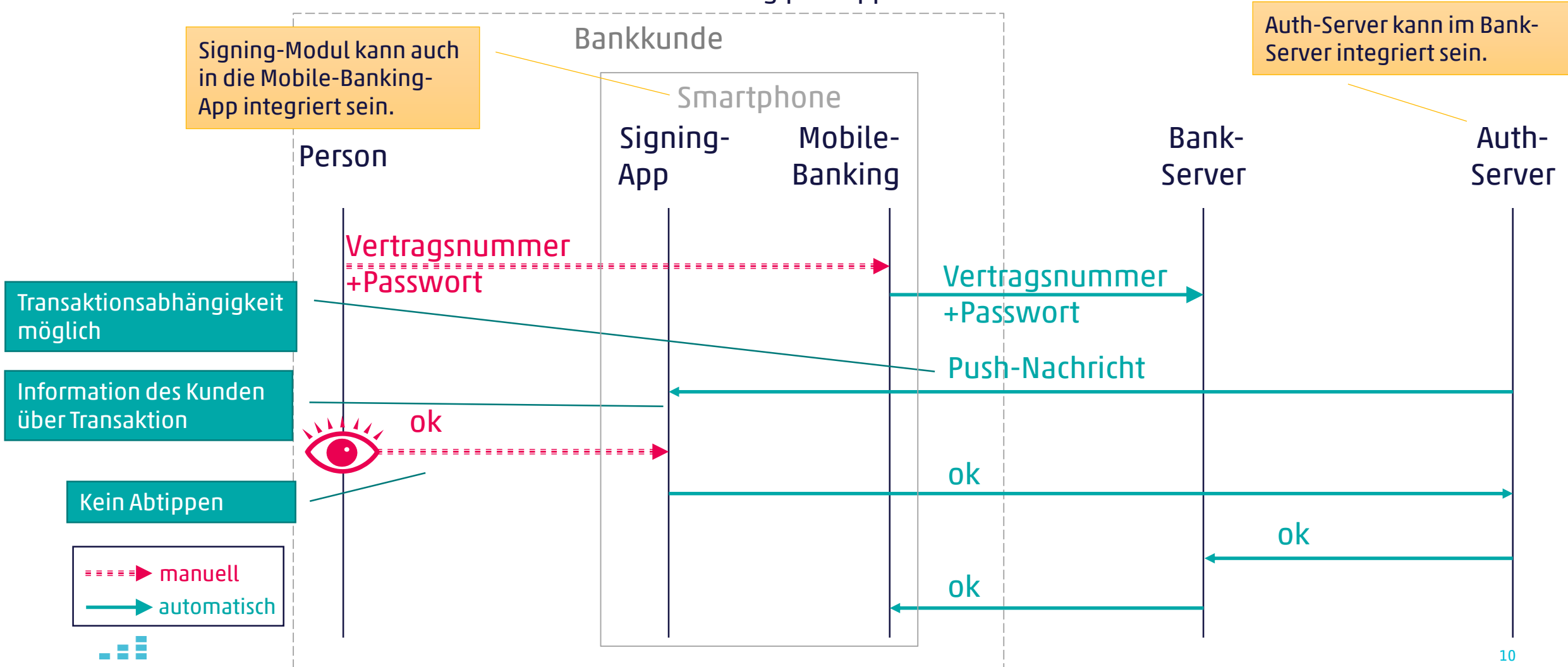
# Push-Authentication: 1 Gerät

Beispiele:

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

Banken z.B.:

- UBS (Access App)
- Sparkasse (D)



# Dynamisches Passwort

Beispiel:

- RSAsecurID
- Vasco DIGIPASS

Banken z.B.:

- Coutts
- Sarasin
- Vontobel



Keine Information des Kunden  
über Transaktion



Code

Code

Code

Vertragsnummer  
+ Passwort

Vertragsnummer + Passwort

====> manuell  
————> automatisch

Bankkunde

Person

Browser

Bank-  
Server

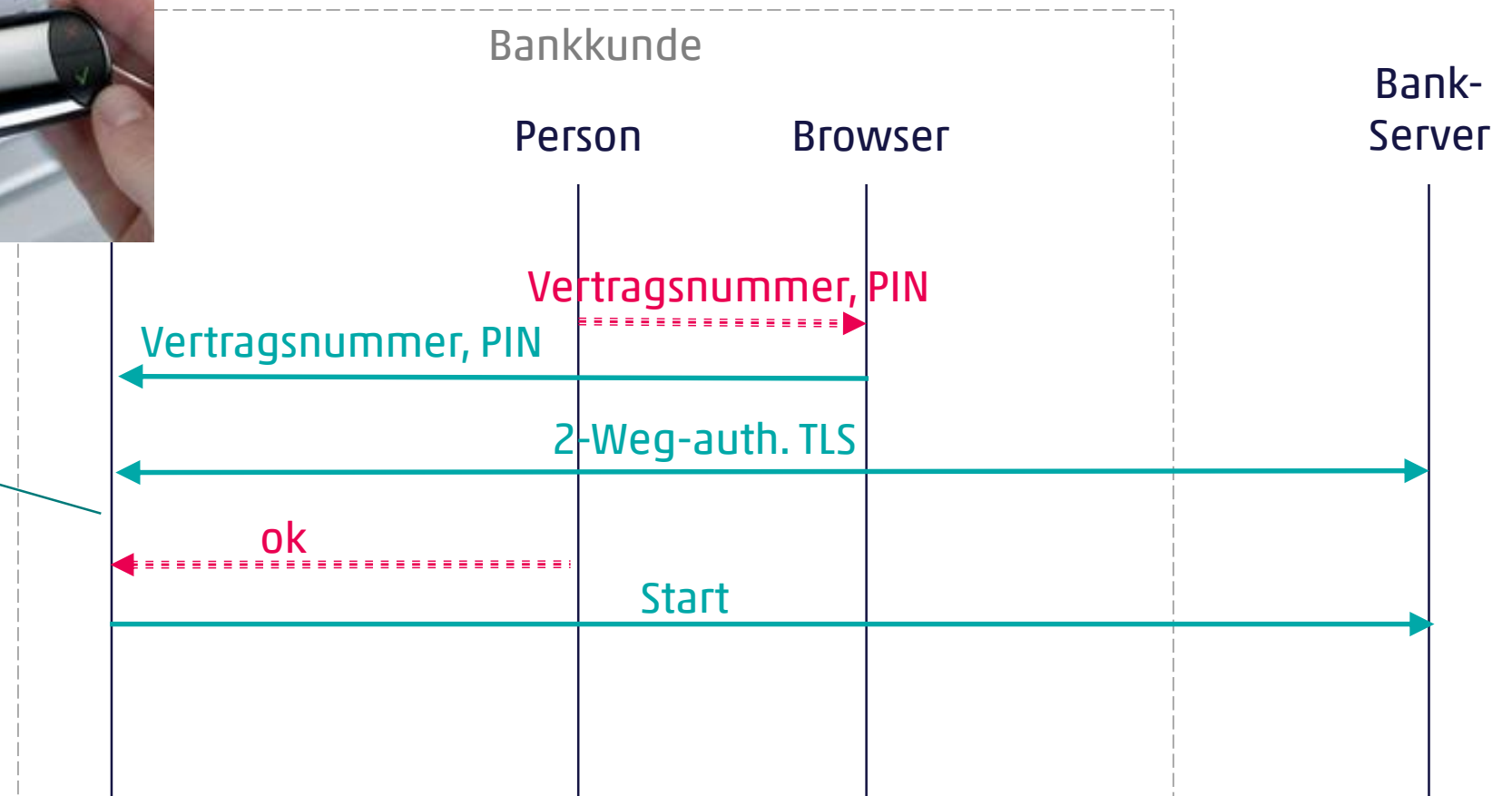
# Verbundenes C/R-Token mit Zertifikat (Proxy)

Banken z.B.:  
- UBS



Beispiel:  
- IBM ZTIC

Information des Kunden über Login



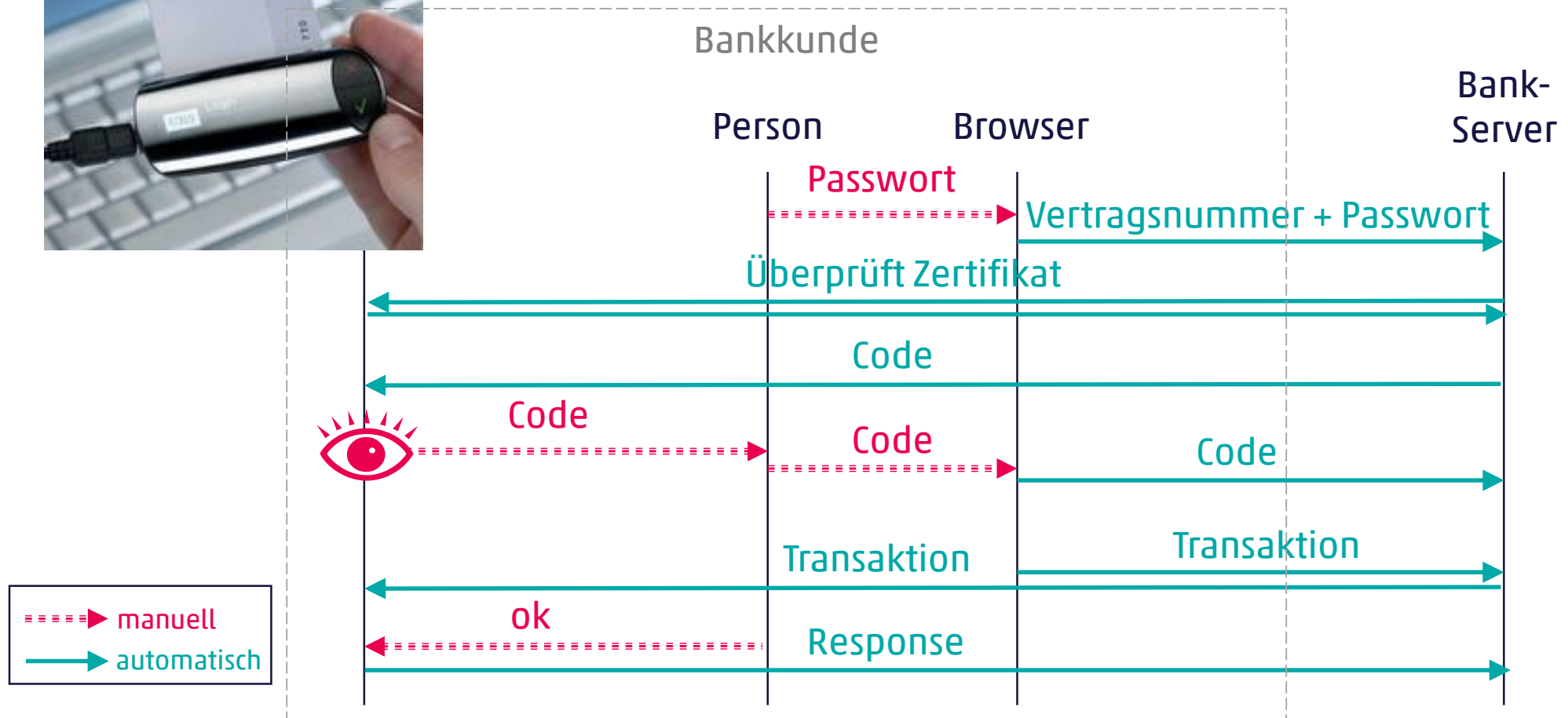
# Verbundenes C/R-Token mit Zertifikat (2 Verbindungen)

Banken z.B.:

- Zürcher Kantonalbank



Beispiel:  
- IBM ZTIC



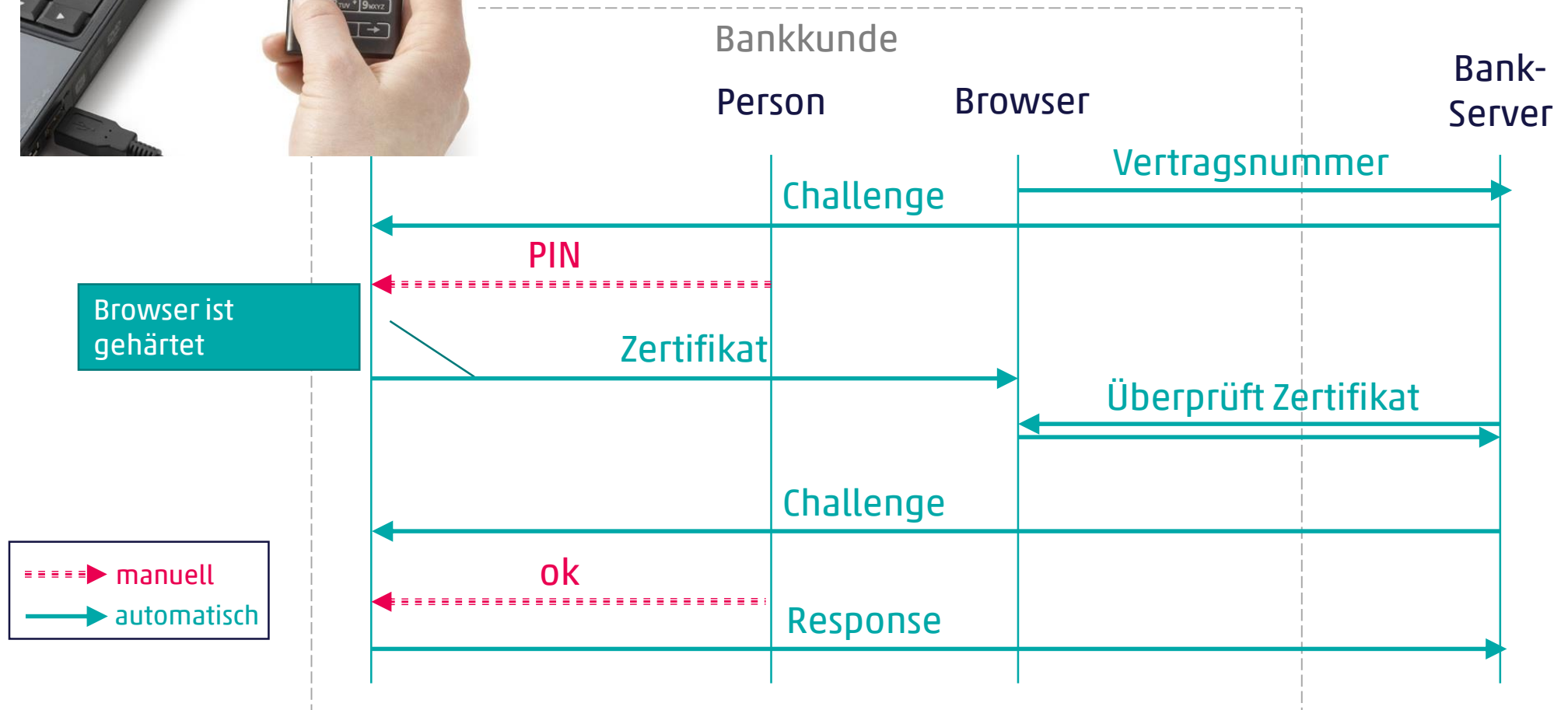
# Verbundenes C/R-Token mit Zertifikat + gehärteter Browser

Banken z.B.:  
- Keine bekannt



Beispiele:

- CLX.SentinelDisplay
- Kobil miDentity visual



# Kobil AST mit 2 Geräten



Mögliche Gerätekombinationen:

- Computer – Computer
- Computer – Smartphone
- Smartphone – Smartphone
- etc.

Banken z.B.:

- Migros Bank
- Vontobel

Bankkunde

Person

Browser

Bank-  
Server

Login auf beiden  
Geräten

Information des  
Kunden über  
Transaktion

Kein Abtippen

Passwort 1

Vertragsnummer

Überprüft Zertifikat

Passwort 2

Vertragsnummer

Überprüft Zertifikat

Challenge

ok

Response

=====> manuell

—————> automatisch

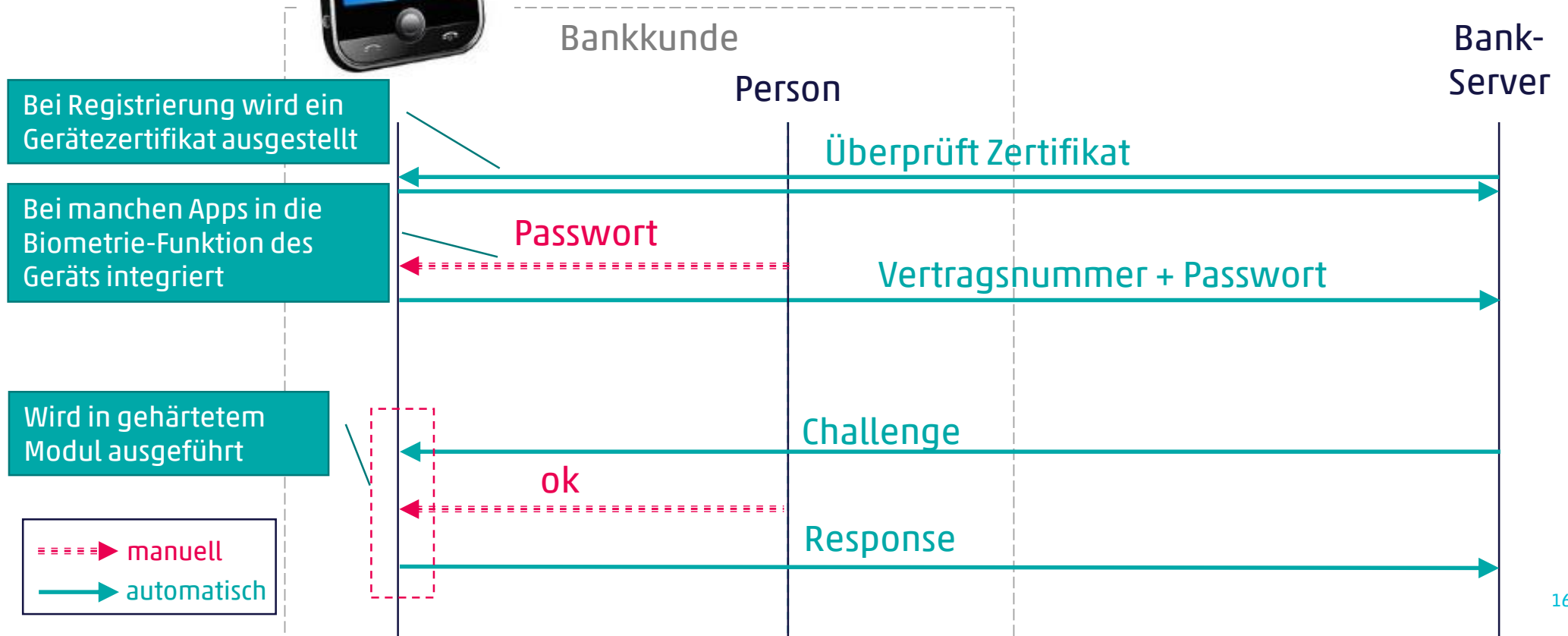


# Kobil AST-Verfahren mit nur 1 Gerät

Banken z.B.:  
- Keine bekannt

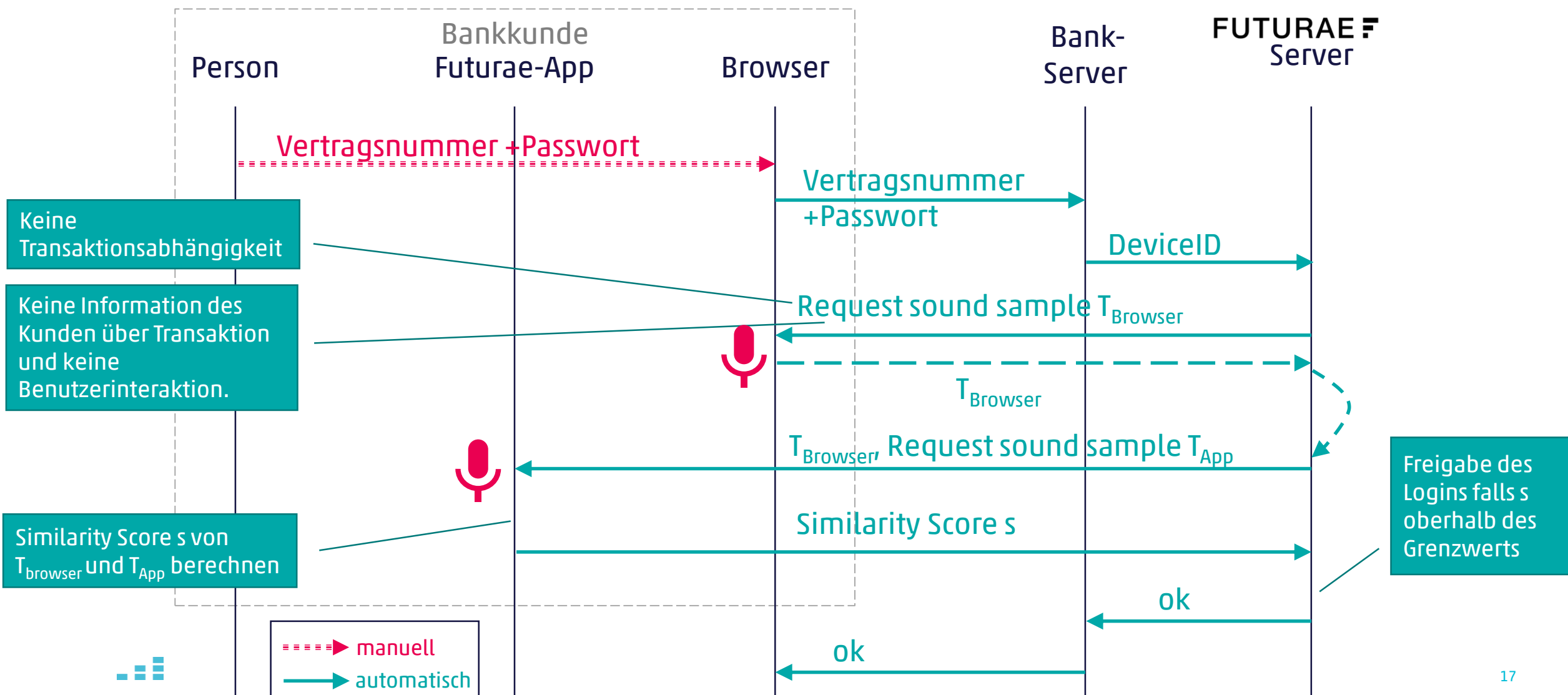


Typischerweise Smartphone-App mit gehärtetem Software-Modul, das Ausspionieren der Zertifikatsschlüssel durch Schadsoftware erschweren soll



# Futuræ SoundProof

Banken z.B.:  
- Keine bekannt



# Vergleich des Potenzials

Login + Lesezugang

Diebstahl Credentials  
Phishing passiv  
Man-in-the-Middle  
Malware

Streichliste / Matrixkarte	mTAN (SMS)	Mobile ID	Challenge-Response Token	Signing-App (PhotoTAN, Flicker, QR-Code) + Browser	Signing App 1 Gerät	Dynamisches Passwort	Zertifikat (Smartcard) + gehärteter Browser	Zertifikat (Smartcard) + C/R Token	Zertifikat (Smartcard) + C/R Token + gehärteter Browser	Kobil AST 2 Geräte	Kobil AST 1 Gerät	Futarae Soundproof + Browser
Diebstahl Credentials	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
Phishing passiv	Red	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow
Man-in-the-Middle	Red	Red	Red	Red	Green	Red	Green	Green	Green	Green	Green	Red
Malware	Red	Red	Red	Red	Yellow	Red	Yellow	Red	Yellow	Yellow	Yellow	Red

Transaktion

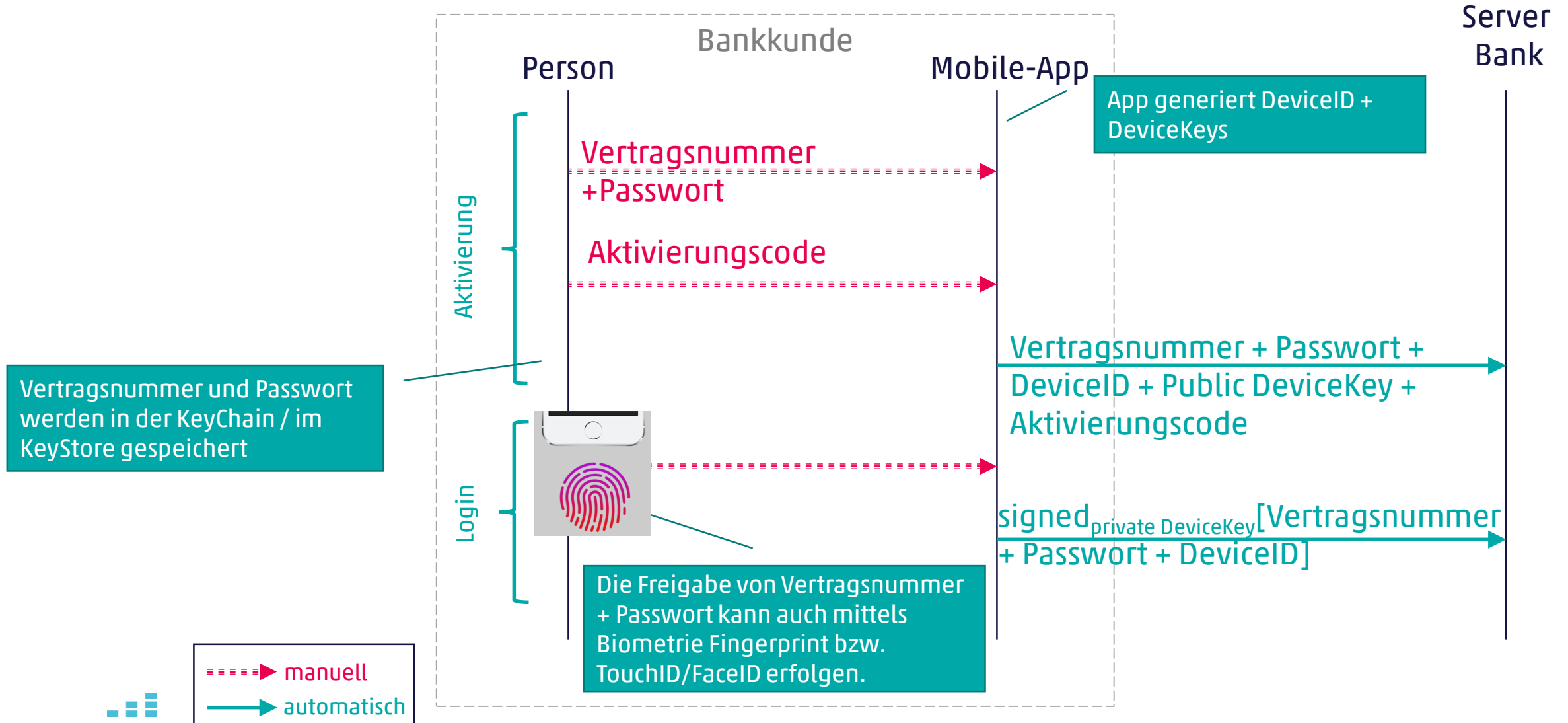
Session hijack  
Session riding  
Man-in-the-Middle  
Malware

Streichliste / Matrixkarte	mTAN (SMS)	Mobile ID	Challenge-Response Token	Signing-App (PhotoTAN, Flicker, QR-Code) + Browser	Signing App 1 Gerät	Dynamisches Passwort	Zertifikat (Smartcard) + gehärteter Browser	Zertifikat (Smartcard) + C/R Token	Zertifikat (Smartcard) + C/R Token + gehärteter Browser	Kobil AST 2 Geräte	Kobil AST 1 Gerät	Futarae Soundproof + Browser
Session hijack	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Red
Session riding	Yellow	Yellow	Green	Green	Green	Green	Yellow	Green	Green	Green	Green	Red
Man-in-the-Middle	Red	Yellow	Green	Yellow	Green	Red	Green	Green	Green	Green	Green	Red
Malware	Red	Yellow	Green	Yellow	Yellow	Red	Yellow	Green	Green	Green	Yellow	Red

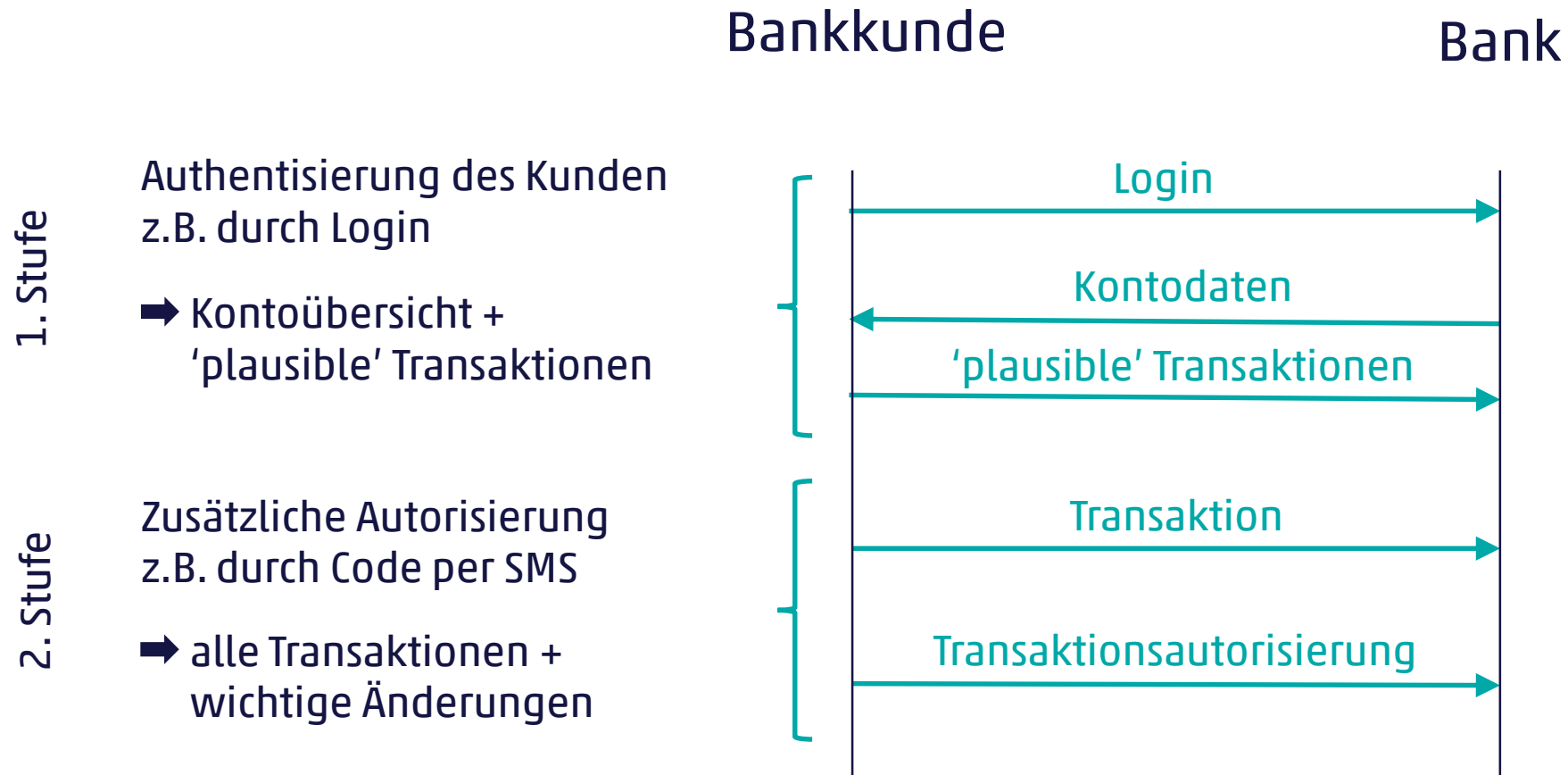
# Vereinfachtes Login mittels Biometrie (Fingerprint und TouchID/FaceID)

Banken z.B.:

- Raiffeisen
- Postfinance



# Vereinfachung mit einfachem Login und Transaktionsbestätigung



# Vielen Dank für Ihre Aufmerksamkeit\_

**Christian Birchler**

christian.birchler@cnlab.ch

+41 55 214 33 40

**Thomas Lüthi**

thomas.luethi@cnlab.ch

+41 55 214 33 41

info@cnlab-security.ch

+41 55 214 33 33

**Paul Schöbi**

paul.schoebi@cnlab.ch

+41 55 214 33 33

**René Vogt**

rene.vogt@cnlab.ch

+41 55 214 33 41

cnlab security AG

Obere Bahnhofstrasse 32b

CH-8640 Rapperswil-Jona

Switzerland

**Stephan Verbücheln**

stephan.verbuecheln@cnlab.ch

+41 55 214 33 36

**Martina Minges**

martina.minges@cnlab.ch

+41 55 214 33 42