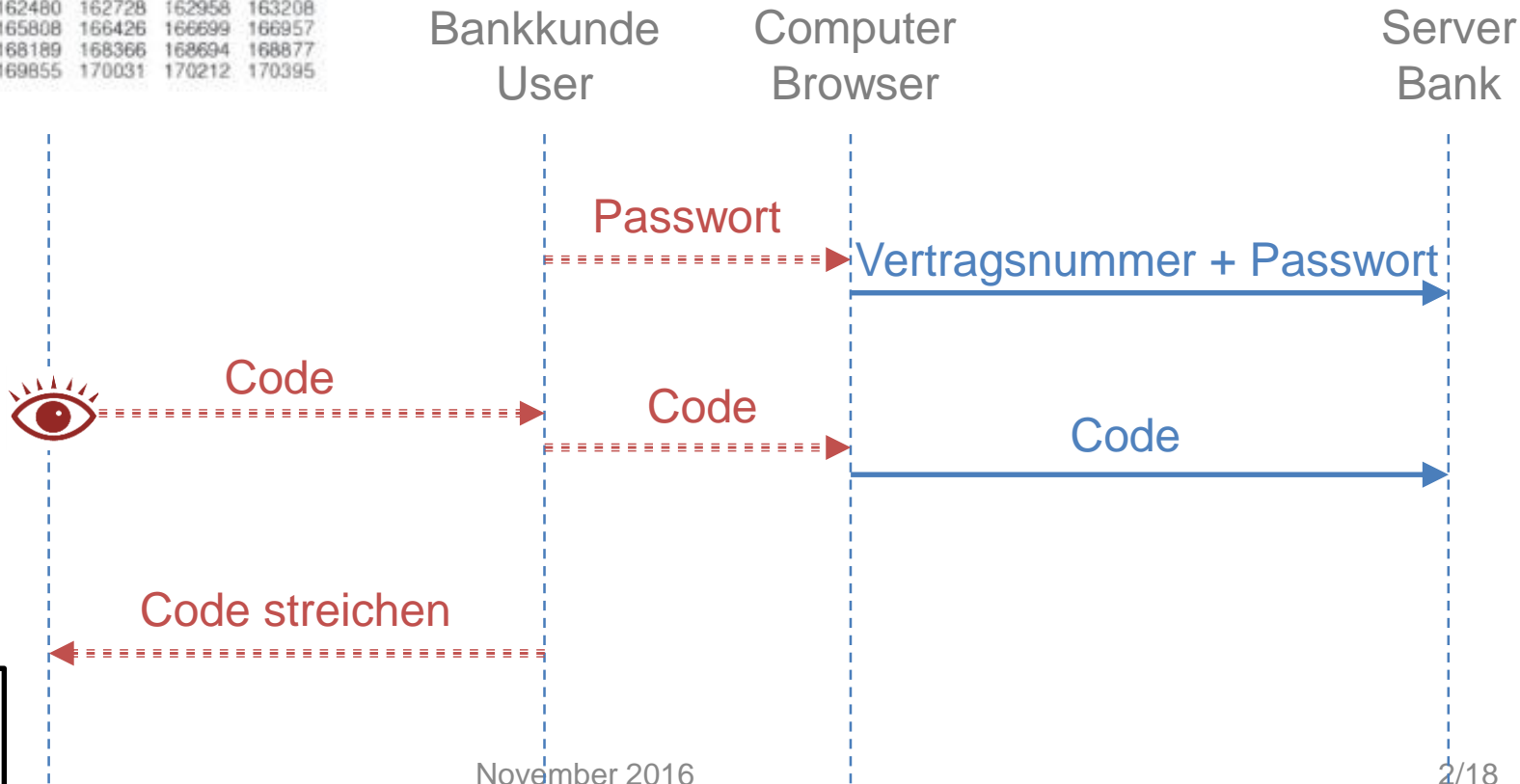


E-Banking-Authentisierung

cnlab security ag, obere bahnhofstr. 32b, CH-8640 rapperswil-jona

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
127007	128051	128225	128394	128564	128766	128959
130008	130216	130408	130594	130789	131007	131198
132025	132529	132795	132977	133154	133324	133491
134155	134927	135230	135450	135899	136286	136509
138008	140006	140178	140351	140525	140694	140972
	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

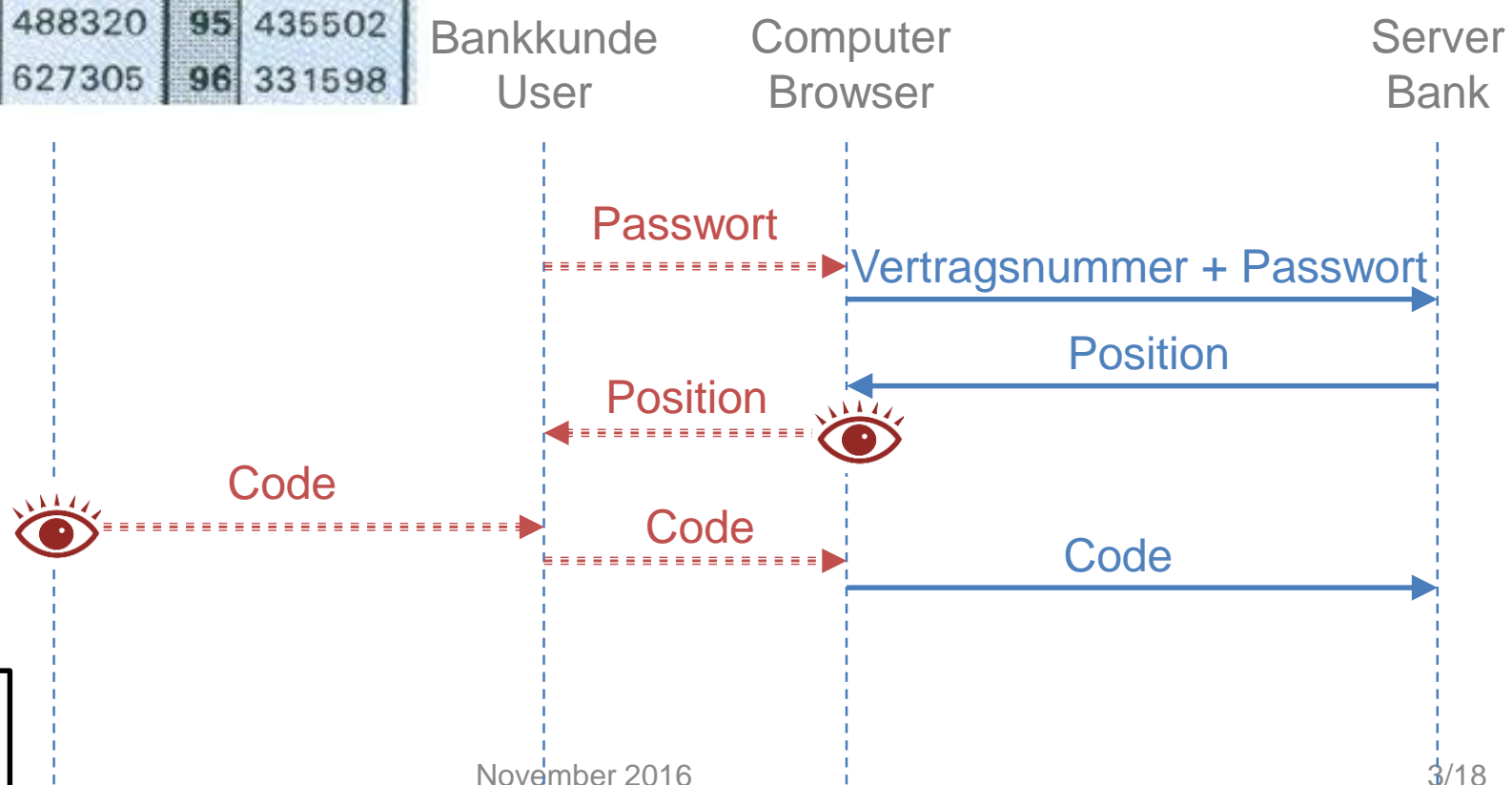


Matrixkarte (iTAN)

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

- Banken:
- Coopbank
 - Raiffeisen
 - etc.

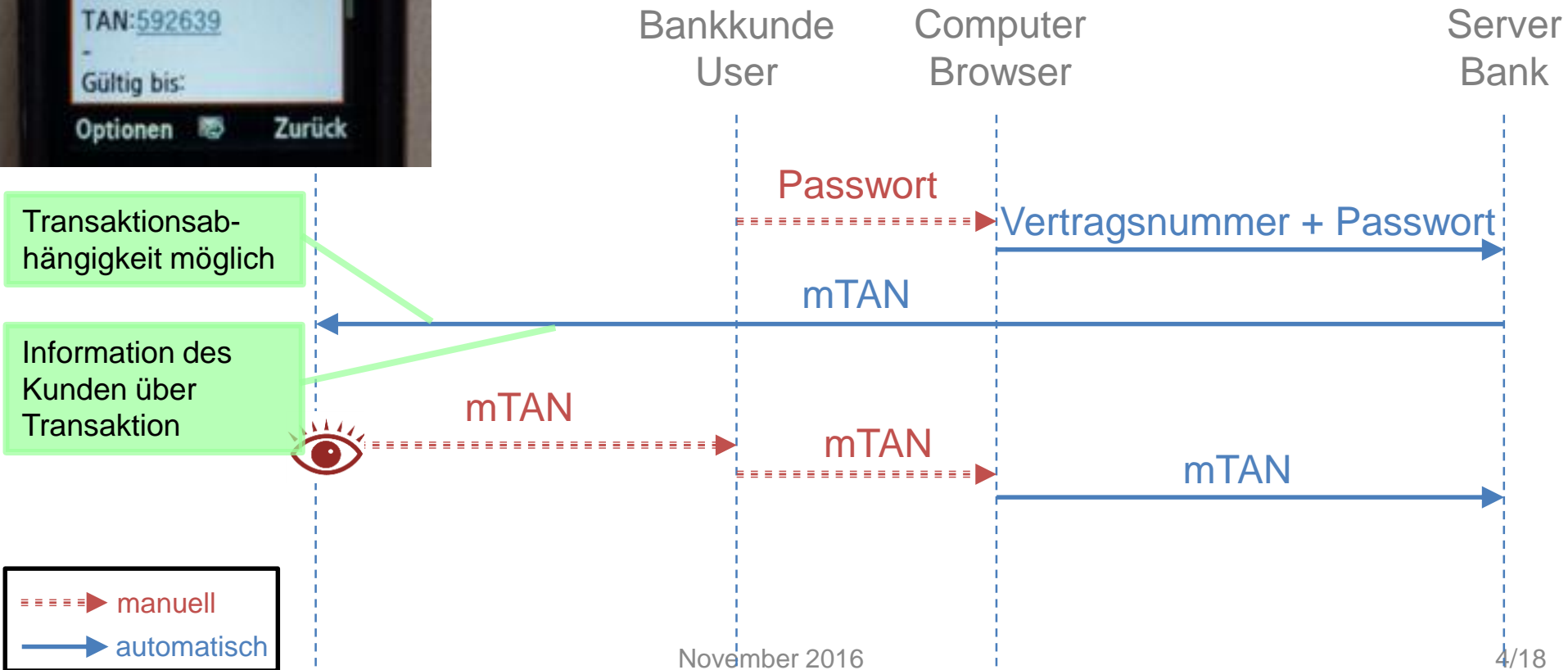


mTAN (Code per SMS)



Banken:

- Schwyzer Kantonalbank
- Zürcher Kantonalbank
- St.Galler Kantonalbank
- Credit Suisse
- etc.

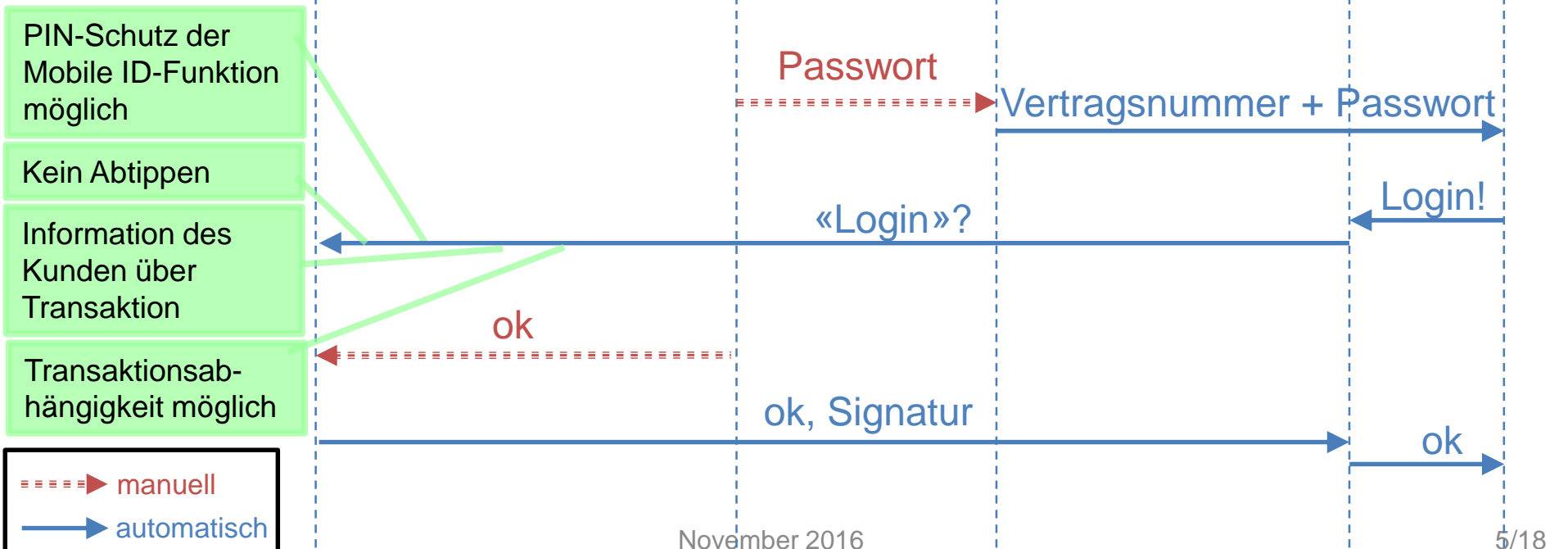


Mobile ID

Banken:
- PostFinance



Bankkunde User Computer Browser Server Swisscom Bank Server Bank



PIN-Schutz der Mobile ID-Funktion möglich

Kein Abtippen

Information des Kunden über Transaktion

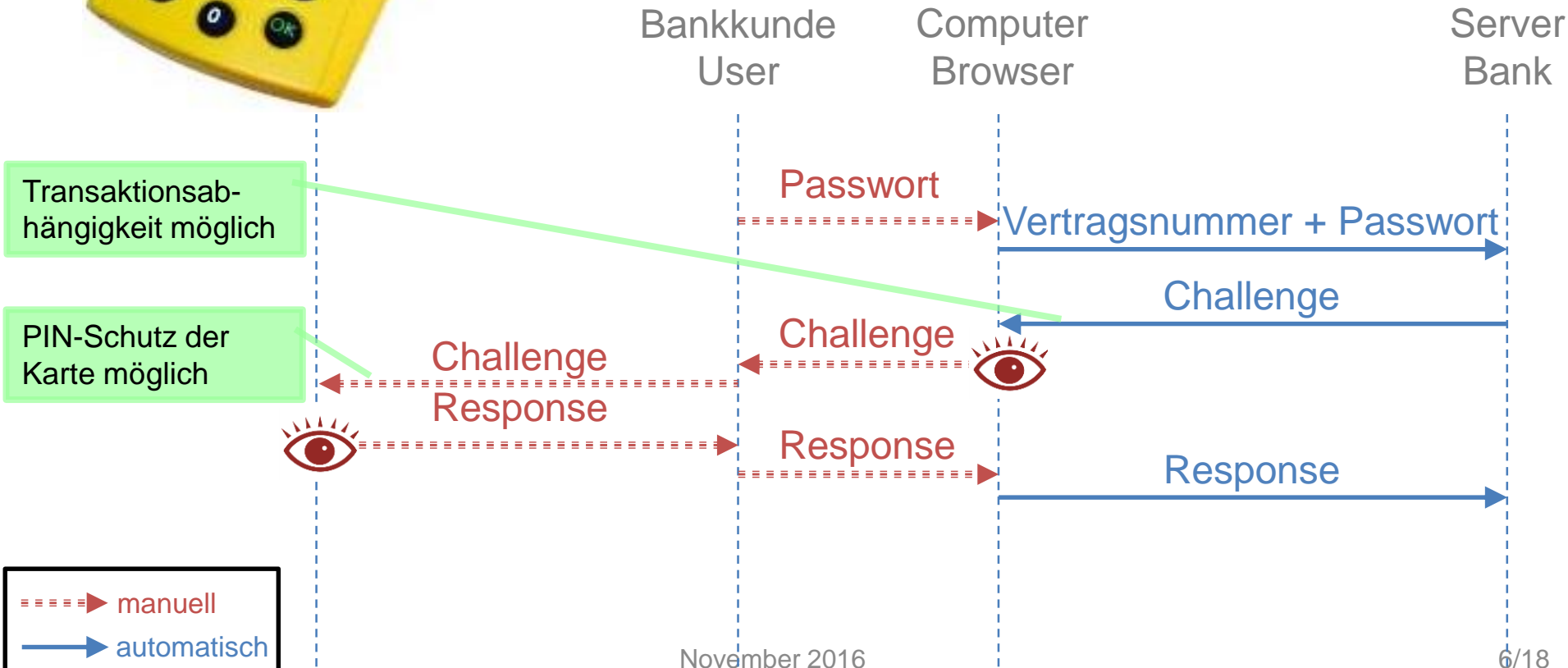
Transaktionsabhängigkeit möglich

====> manuell
——> automatisch

Challenge/Response-Tools



- Banken:
- UBS
 - PostFinance

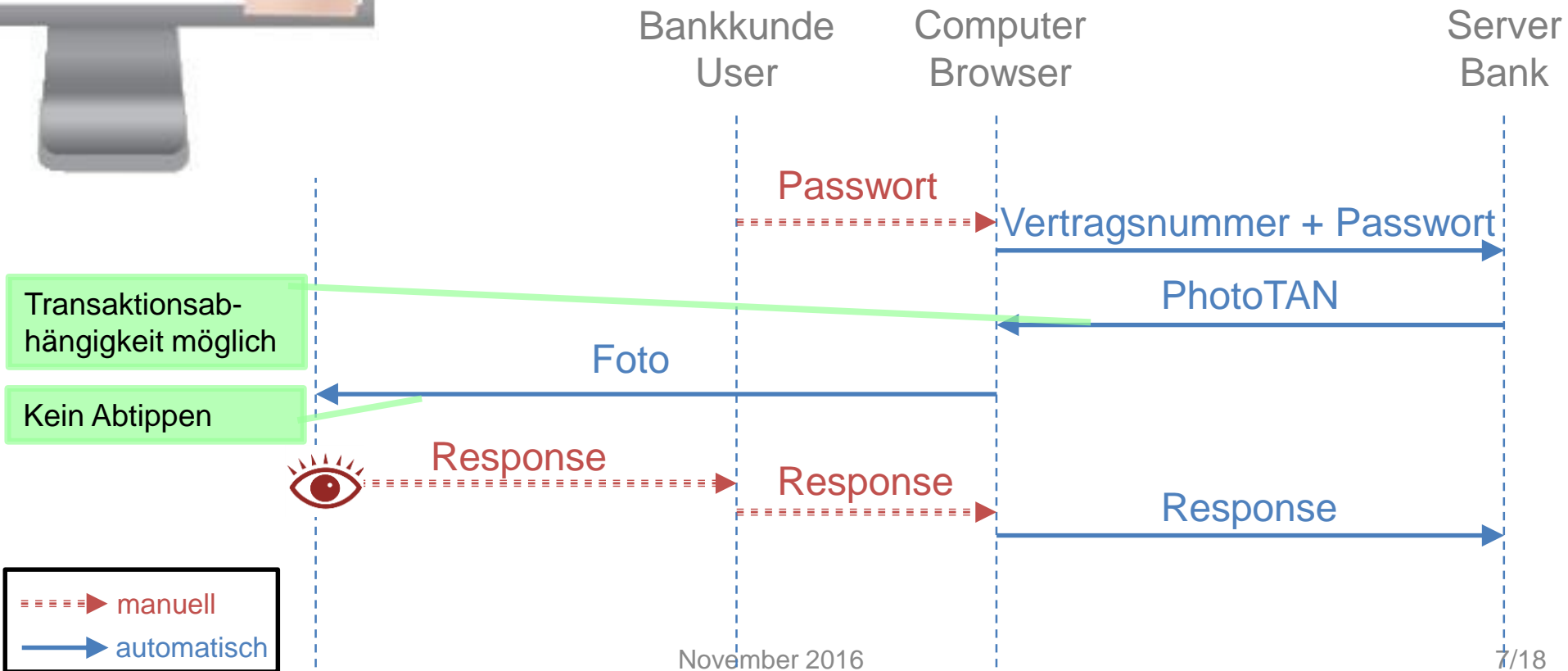


PhotoTAN



Banken:

- Raiffeisen
- Commerzbank (D)

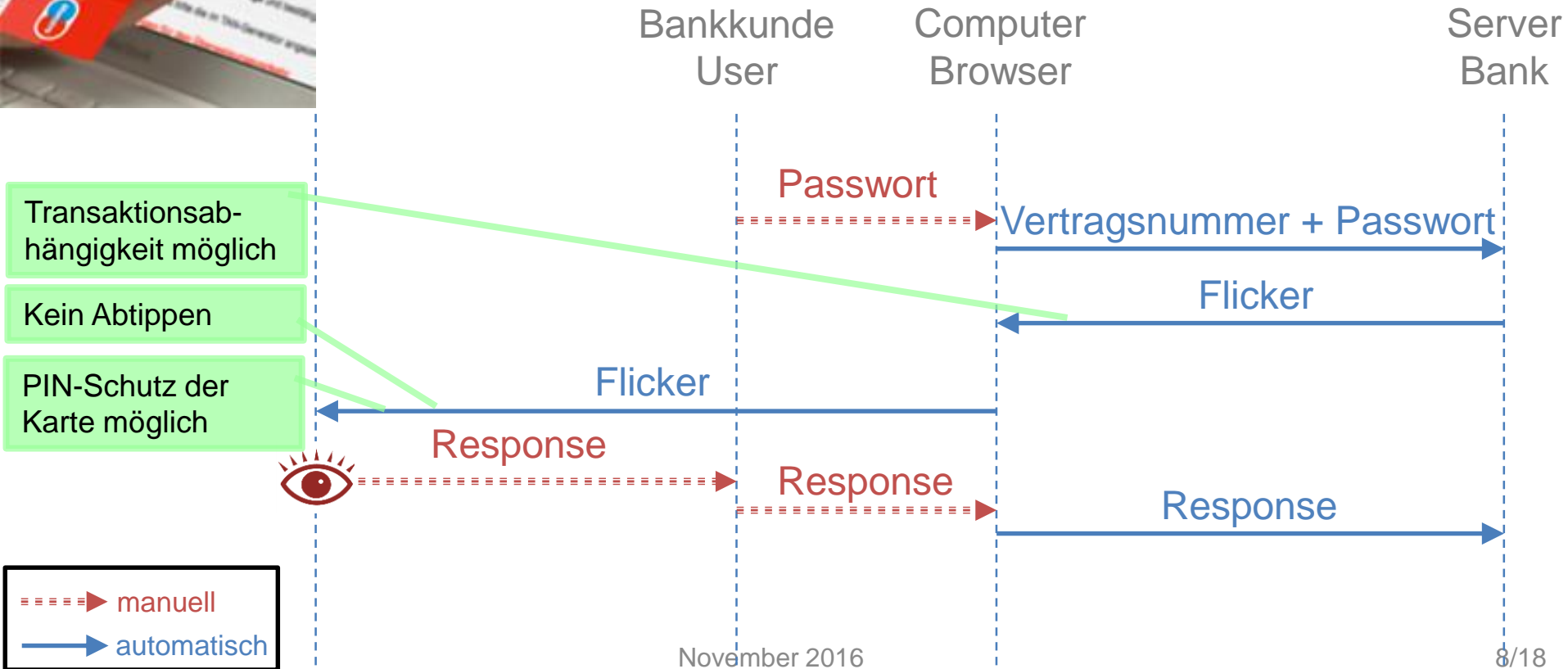


Flicker



Banken:

- VPBank (FL)
- Sparkasse (D)

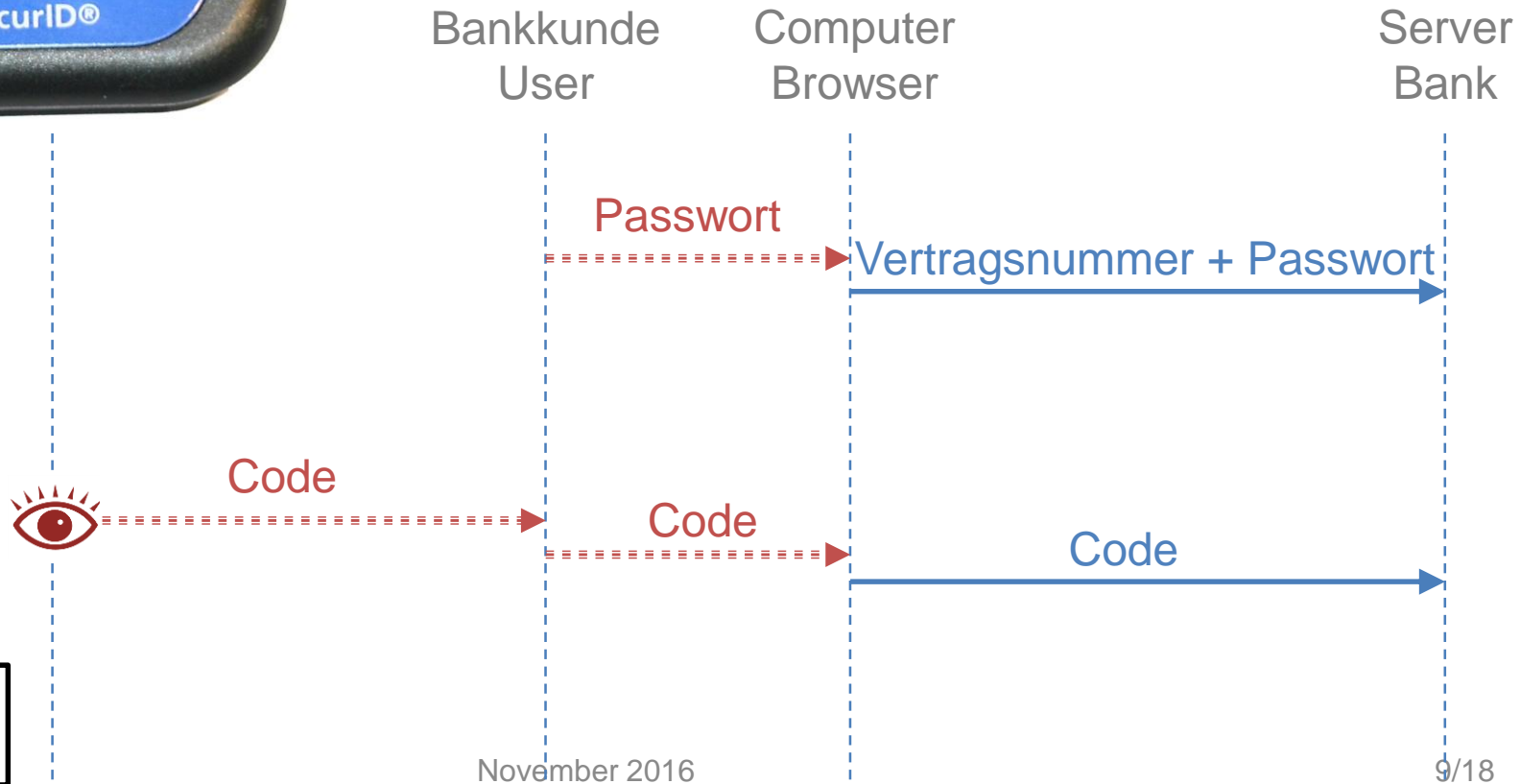


Dynamisches Passwort



- Beispiel:
- RSAsecurID
 - Vasco DIGIPASS

- Banken:
- Coutts
 - Sarasin
 - Vontobel



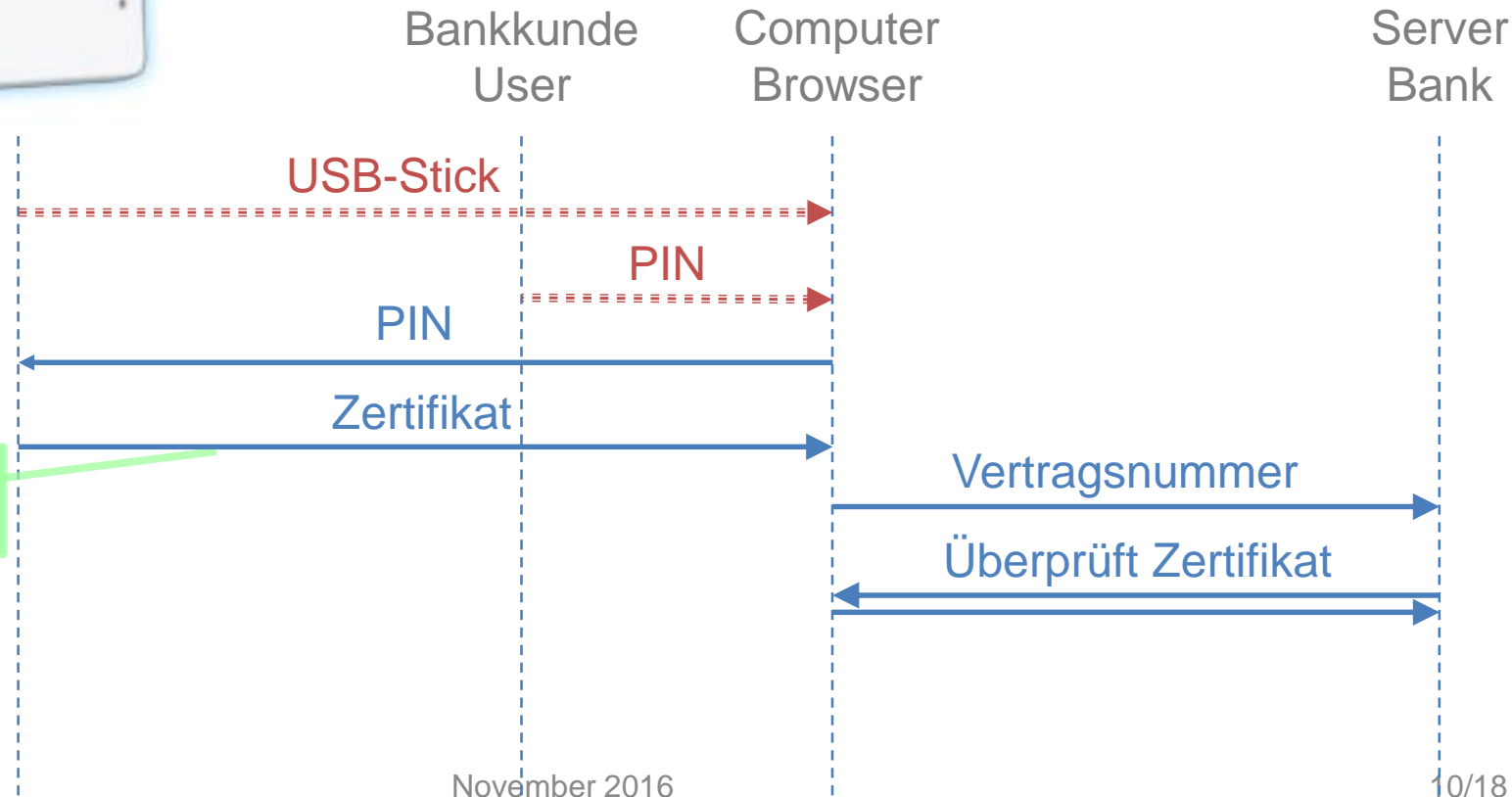
Zertifikat + gehärteter Browser

Banken:

- St. Galler Kantonalbank
- Luzerner Kantonalbank

Beispiele:

- CLX.Sentinel
- Kobil mIDentity



Browser ist gehärtet

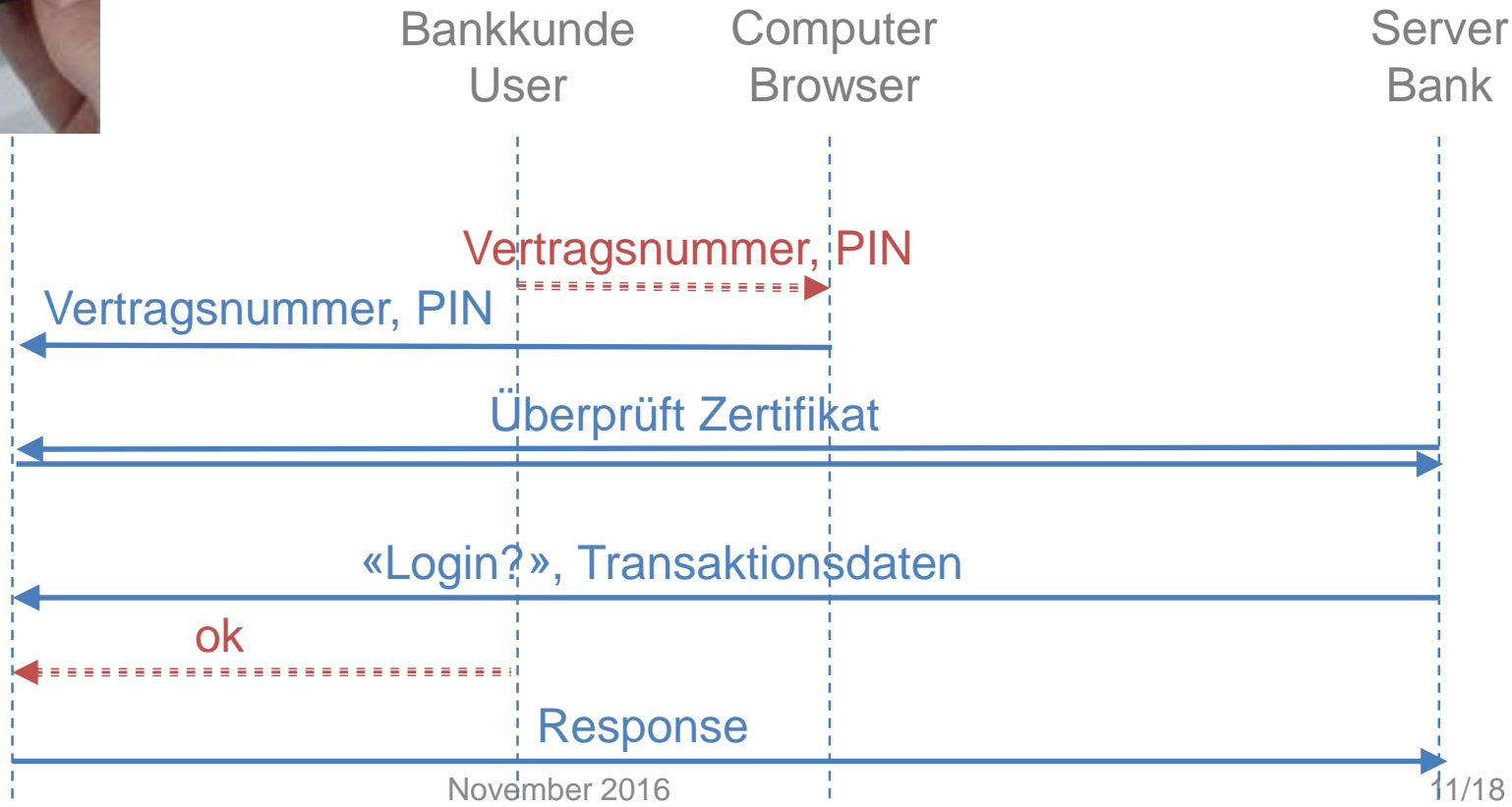


Verbundenes C/R-Token mit Zertifikat (Proxy)

Banken:
- UBS



Beispiel:
- IBM ZTIC



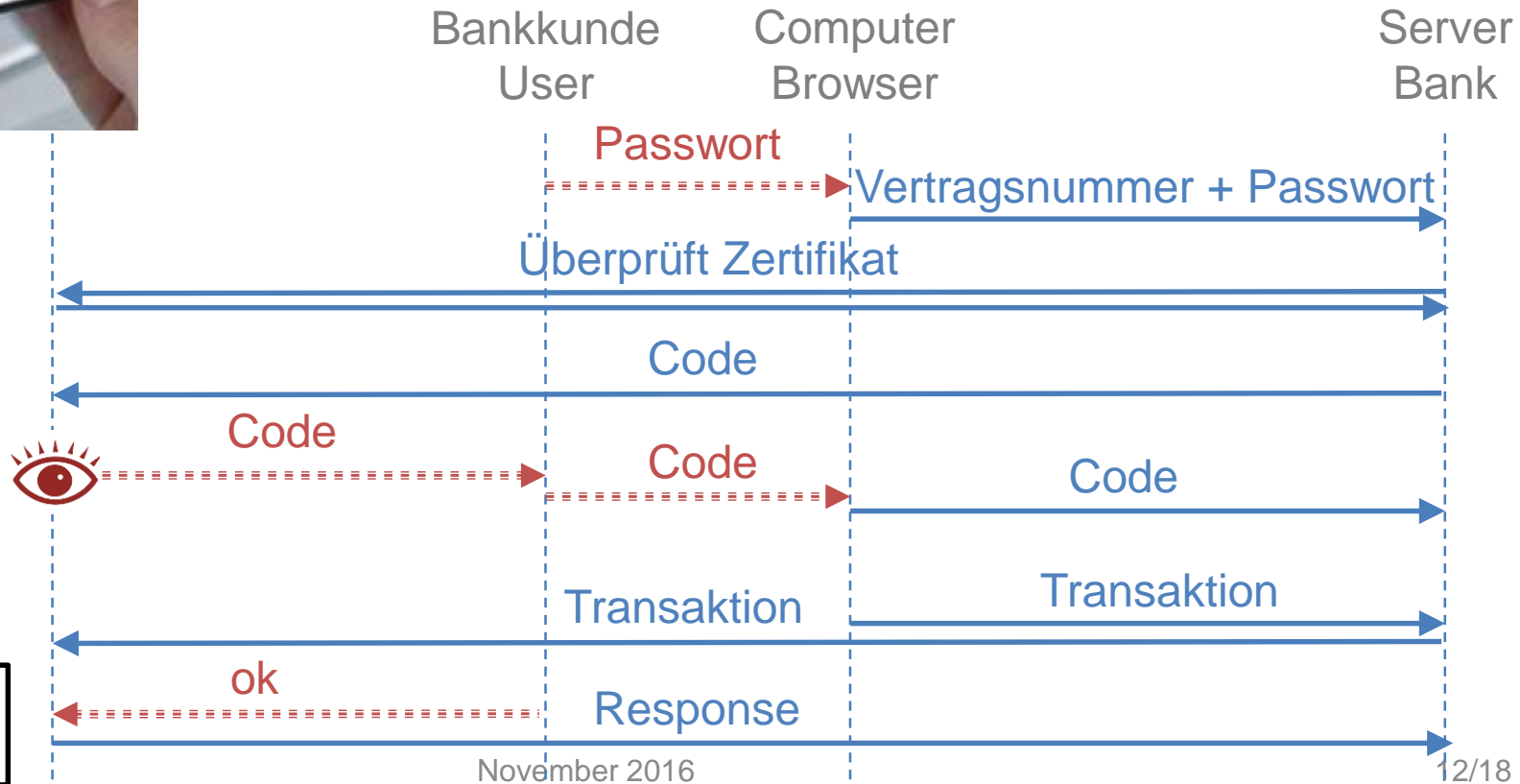
Verbundenes C/R-Token mit Zertifikat (2 Verbindungen)

Banken:

- Zürcher Kantonalbank



Beispiel:
- IBM ZTIC



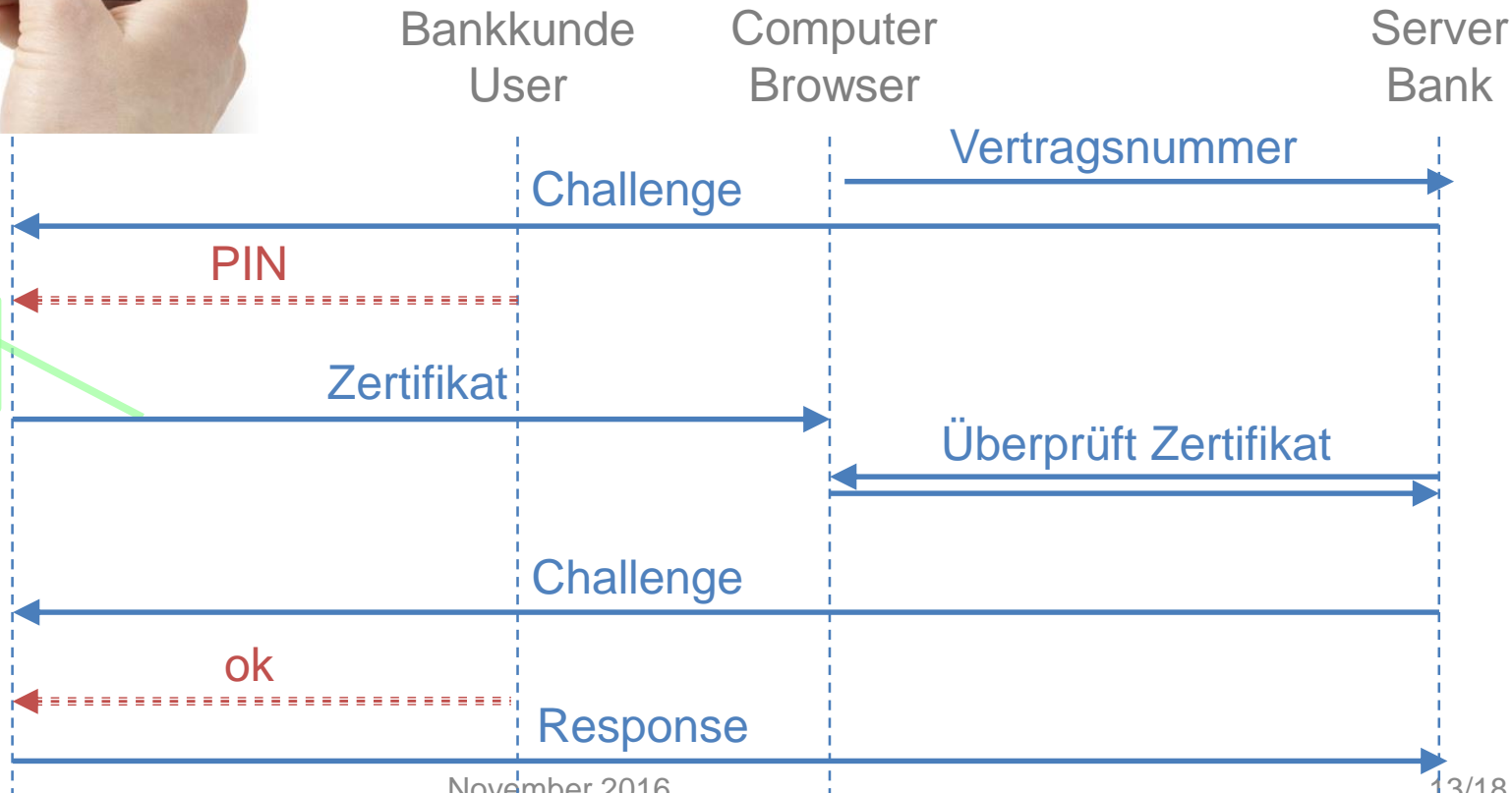
Verbundenes C/R-Token mit Zertifikat + gehärteter Browser

Banken:
- Julius Bär



Beispiele:

- CLX.SentinelDisplay
- Kobil mIdentity visual



Browser ist gehärtet

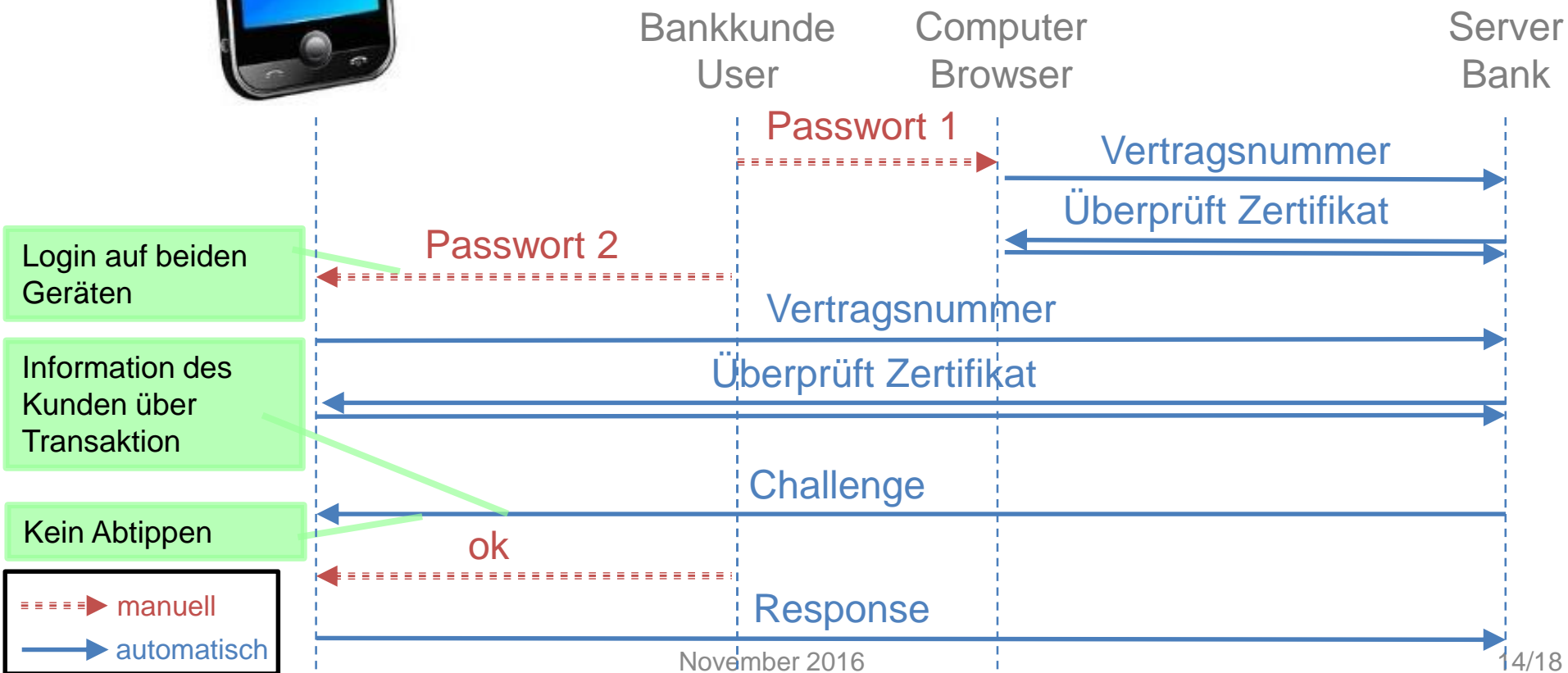
====> manuell
—> automatisch

Kobil AST mit 2 Geräten



- Mögliche Gerätekombinationen:
- Computer – Computer
 - Computer – Smartphone
 - Smartphone – Smartphone
 - etc.

Banken:
 - Migros Bank (im Aufbau)

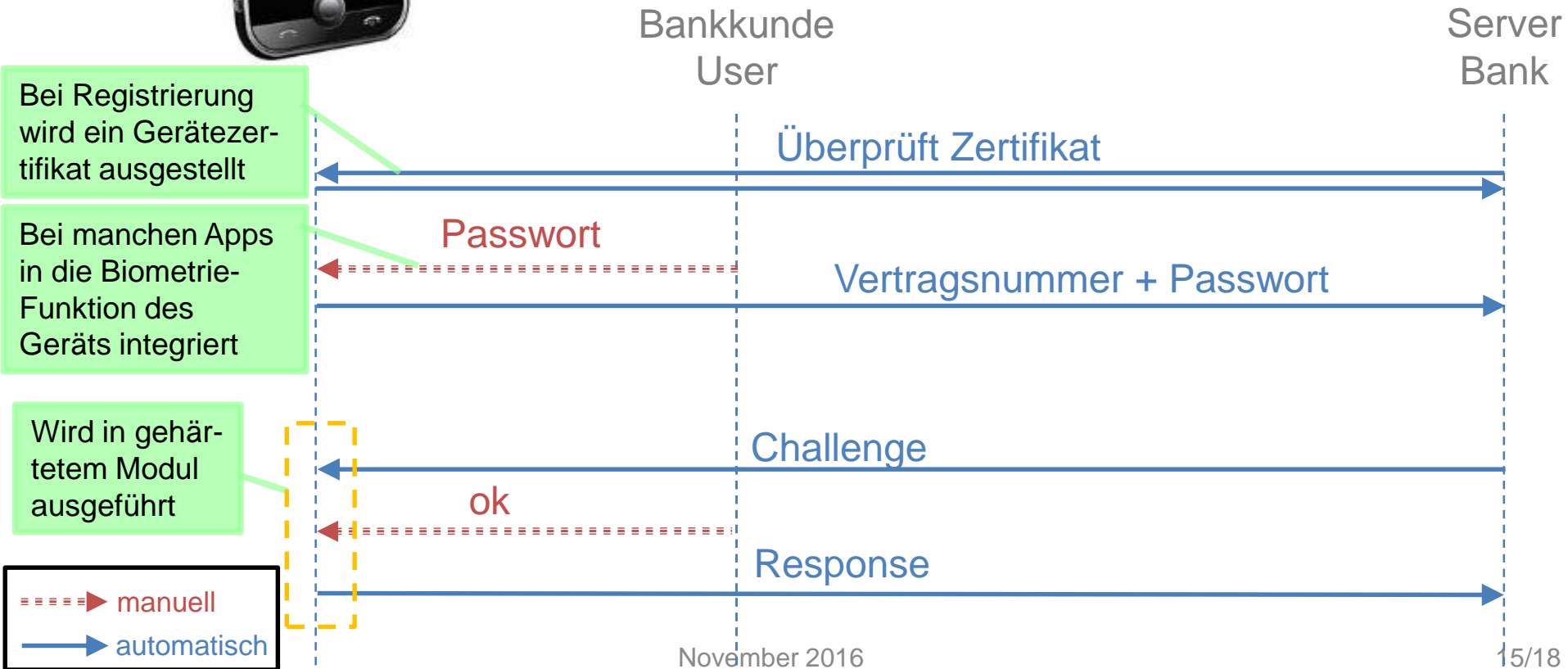


Verfahren mit nur 1 Gerät



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

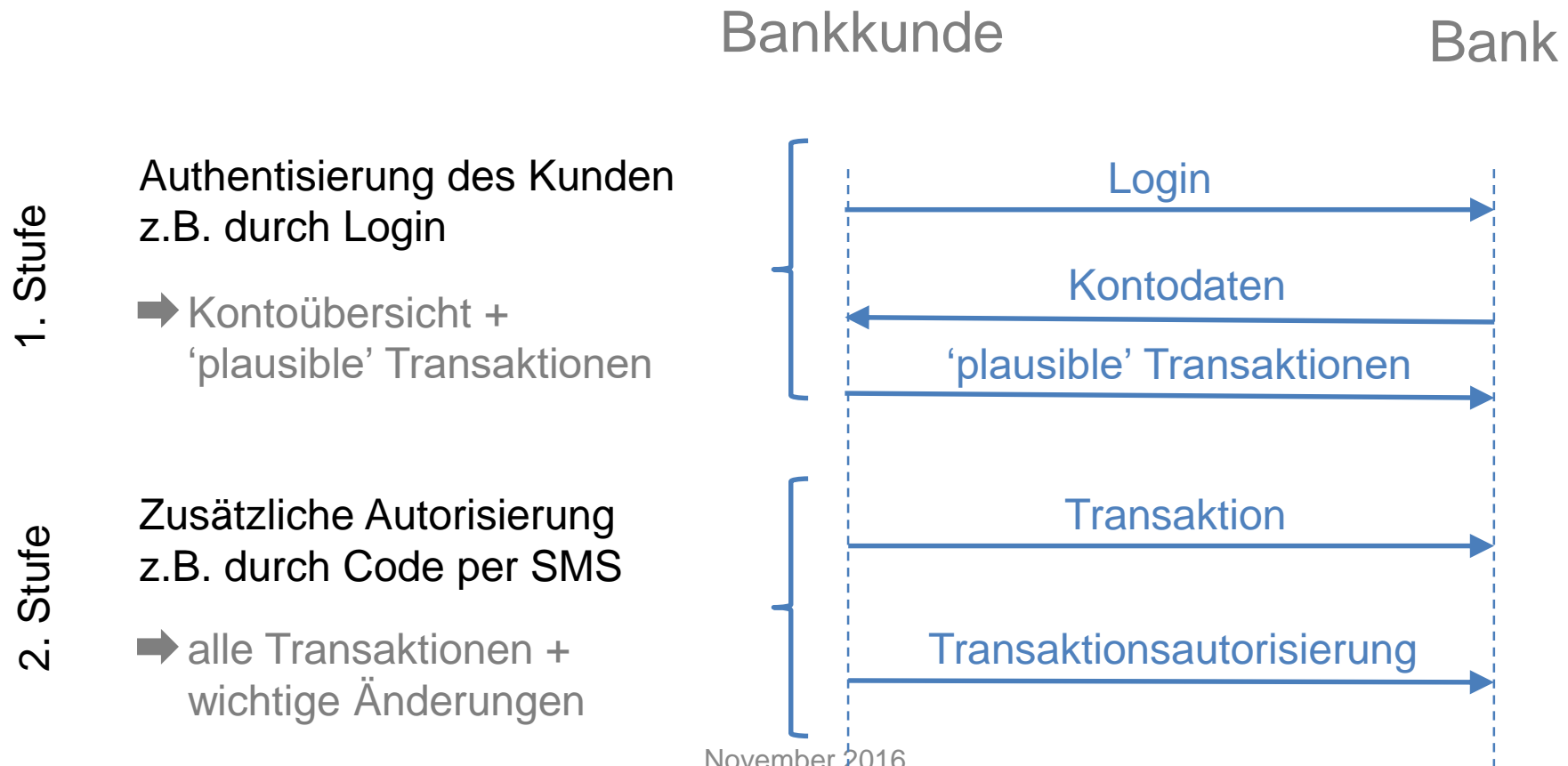
Banken:
- Bisher keine im Betrieb



Vergleich des Potenzials

		Streichliste / Matrixkarte	mTAN (SMS)	Mobile ID	Challenge-Response Token	PhotoTAN / Flicker	Dynamisches Passwort	Zertifikat (auf Smartcard) + gehärteter Browser	Zertifikat (auf Smartcard) + C/R Token	Zertifikat (auf Smartcard) + C/R Token + gehärteter Browser	Kobil AST 2 Geräte	Systeme mit nur 1 Gerät
Login + Lesezugang	Diebstahl Credentials	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
	Phishing passiv	Red	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
	Man-in-the-Middle	Red	Red	Red	Red	Red	Red	Green	Green	Green	Green	Green
	Trojaner	Red	Red	Red	Red	Red	Red	Yellow	Red	Yellow	Yellow	Yellow
Transaktion	Session hijack	Red	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
	Session riding	Red	Green	Green	Green	Green	Green	Yellow	Green	Green	Green	Green
	Man-in-the-Middle	Red	Green	Green	Yellow	Green	Red	Green	Green	Green	Green	Green
	Trojaner	Red	Green	Green	Yellow	Green	Red	Yellow	Green	Green	Green	Yellow

Sicherheit mit einfachem Login und Transaktionsbestätigung



Vergleich der Verfahren mit einfachem Login und Transaktionsbestätigung

		Passwort	Passwort + Gerätebindung mit Bindungscookie	Passwort + Gerätebindung mit SSL-Zertifikat	Transaktionsunabhängige Signatur	Transaktionsabhängige Signatur
Login + Lesezugang	Diebstahl Credentials	Red	Green	Green	White	White
	Phishing	Red	Green	Green	White	White
	Man-in-the-Middle	Red	Red	Green	White	White
	Trojaner	Red	Red	Red	White	White
Transaktion	Session hijack	White	White	White	Green	Green
	Session riding	White	White	White	Green	Green
	Man-in-the-Middle	White	White	White	Red	Green
	Trojaner	White	White	White	Red	Green

Danke

Christian Birchler

christian.birchler@cnlab.ch
+41 55 214 33 40

Thomas Lüthi

thomas.luethi@cnlab.ch
+41 55 214 33 41

Paul Schöbi

paul.schoebi@cnlab.ch
+41 55 214 33 33

René Vogt

rene.vogt@cnlab.ch
+41 55 214 33 31

Stephan Verbücheln

Stephan.verbuecheln@cnlab.ch
+41 55 214 33 36