

Sichere Authentisierung im e-Banking

paul.schoebi@cnlab.ch

Schweizer Verfahren

1. Streichliste
2. Matrix-Karte
3. Dynamisches Token (SecurID)
4. Mobiltelefon (MTAN)
5. Challenge/Response-Tools
6. EMV/CAP
7. Axionics
8. SSL Client-Zertifikat

9. USB-Stick mit Smart-Card und Browser (Kobil)

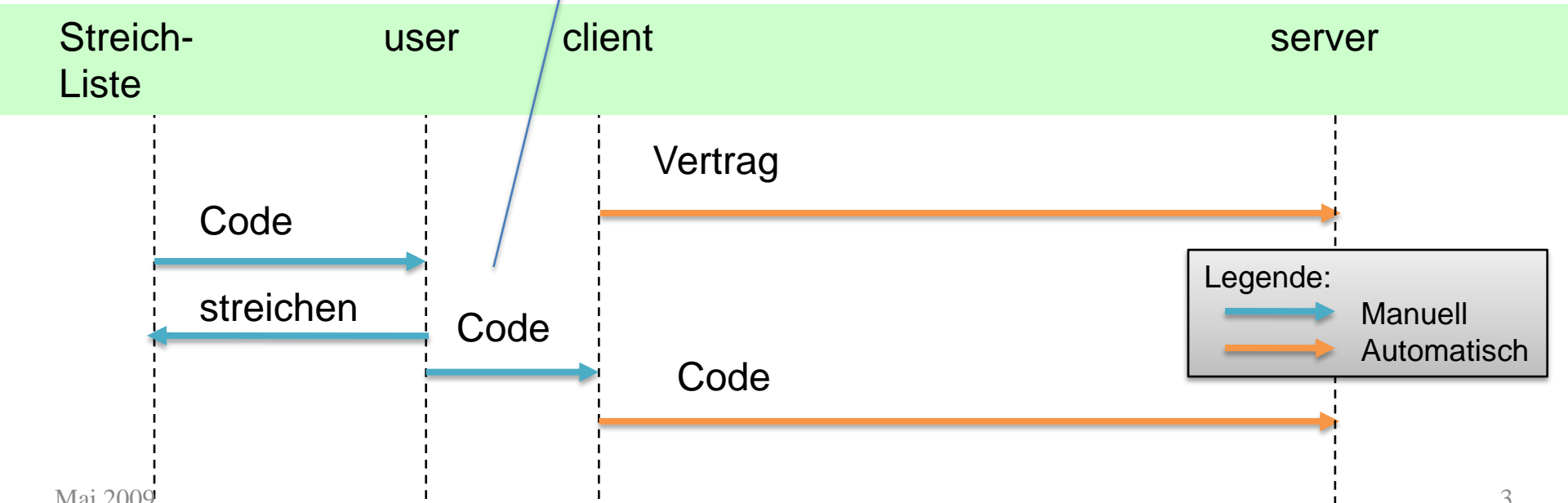
1. Streichliste

Streichliste

7563	1329	2009
1223	1569	0909
7443	1432	2333
2673	1667	1414
7823	3489

Transaktions-
Bestätigung möglich
durch mehrfache
Codes

- Eingesetzt:
- SGK
 - TGKB
 - LUKB



Legende:
 Manuell
 Automatisch

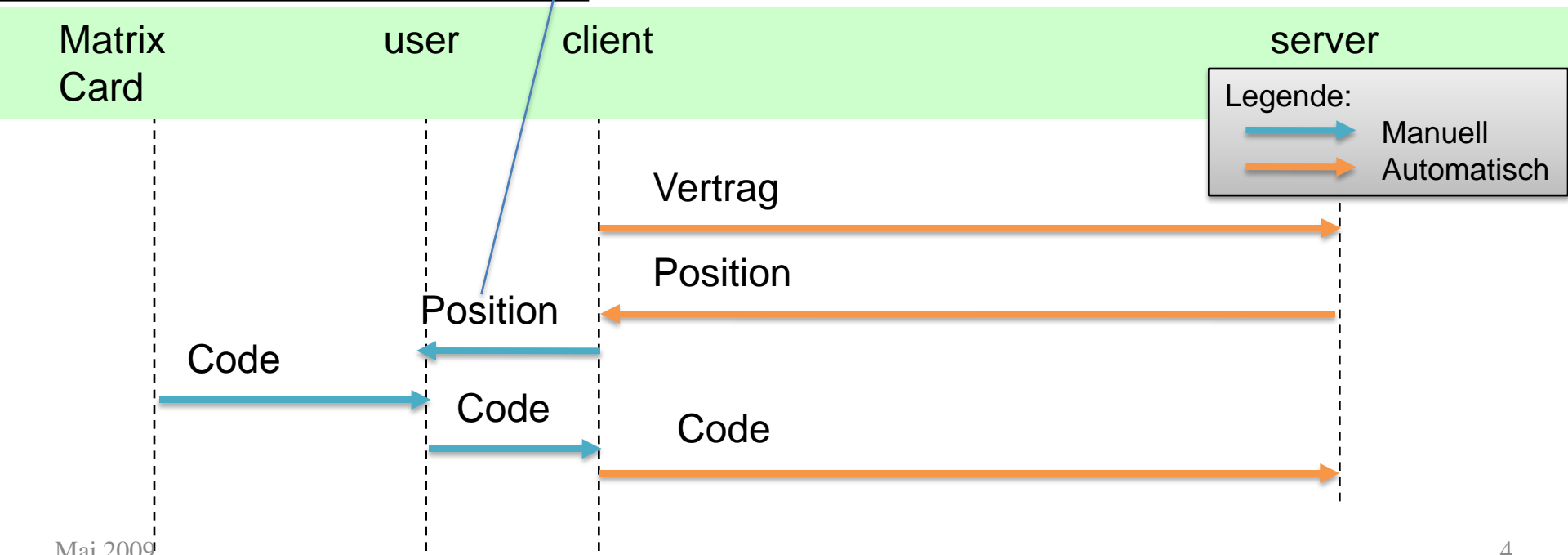
2. Matrix-Karte

Grid card

01 751163	11 132329	21 205609
02 122433	12 154669	22 093109
03 744293	13 149832	23 112333
04 267213	14 166657	24 122414
....

Transaktions-
Bestätigung möglich
durch mehrfache
Codes

Eingesetzt:
- Raiffeisen



3. Dynamisches Token



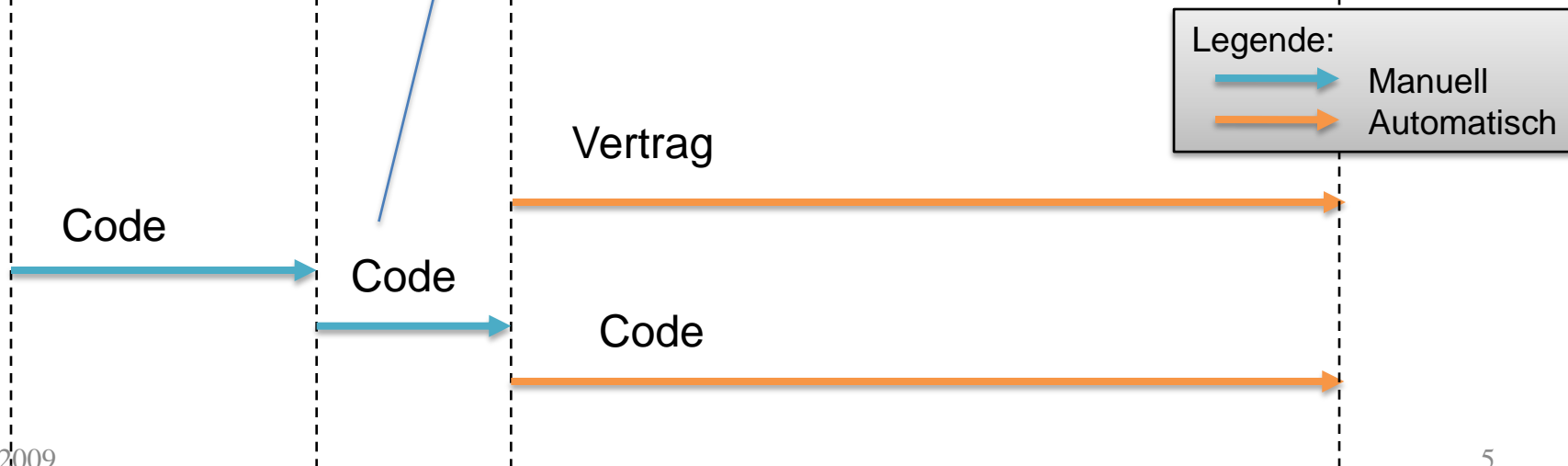
Code wechselt automatisch (z.B. alle 30 Sekunden)

Transaktions-
Bestätigung möglich
durch mehrfache
Codes

Eingesetzt

- Credit Suisse DirectNet

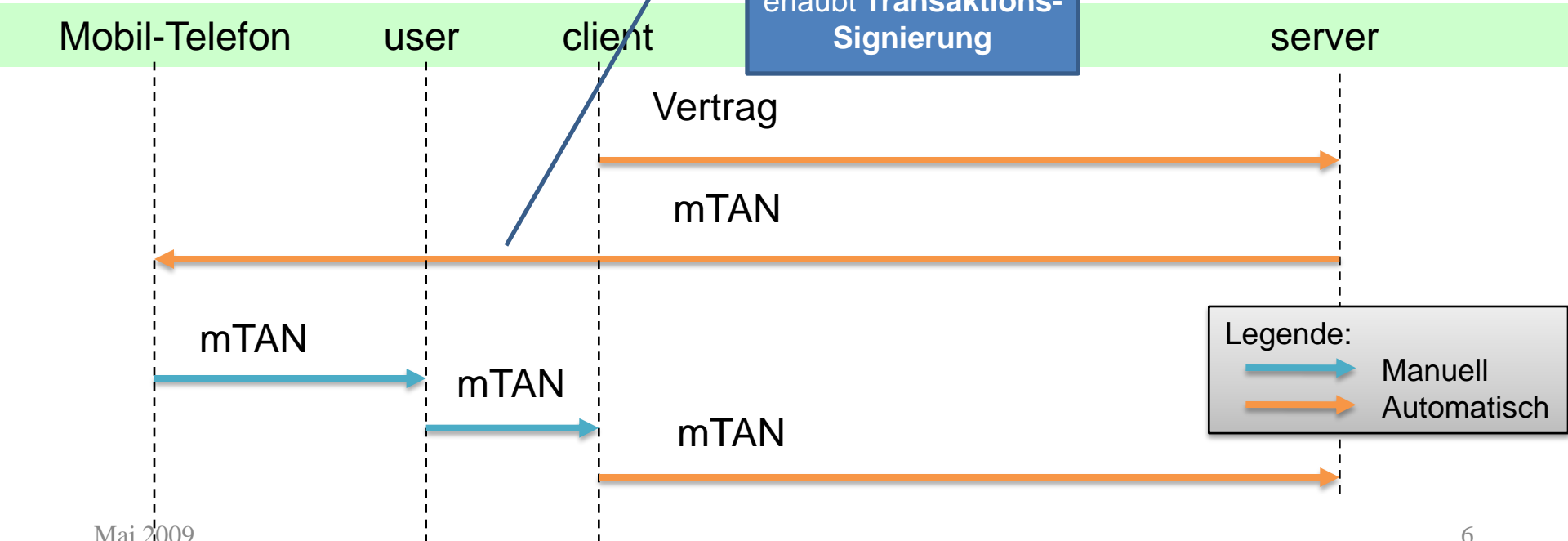
Token user client server



4. Mobiltelefon (MTAN)



- Eingesetzt:
- ZKB
 - Raiffeisen
 - <http://www.postbank.de>

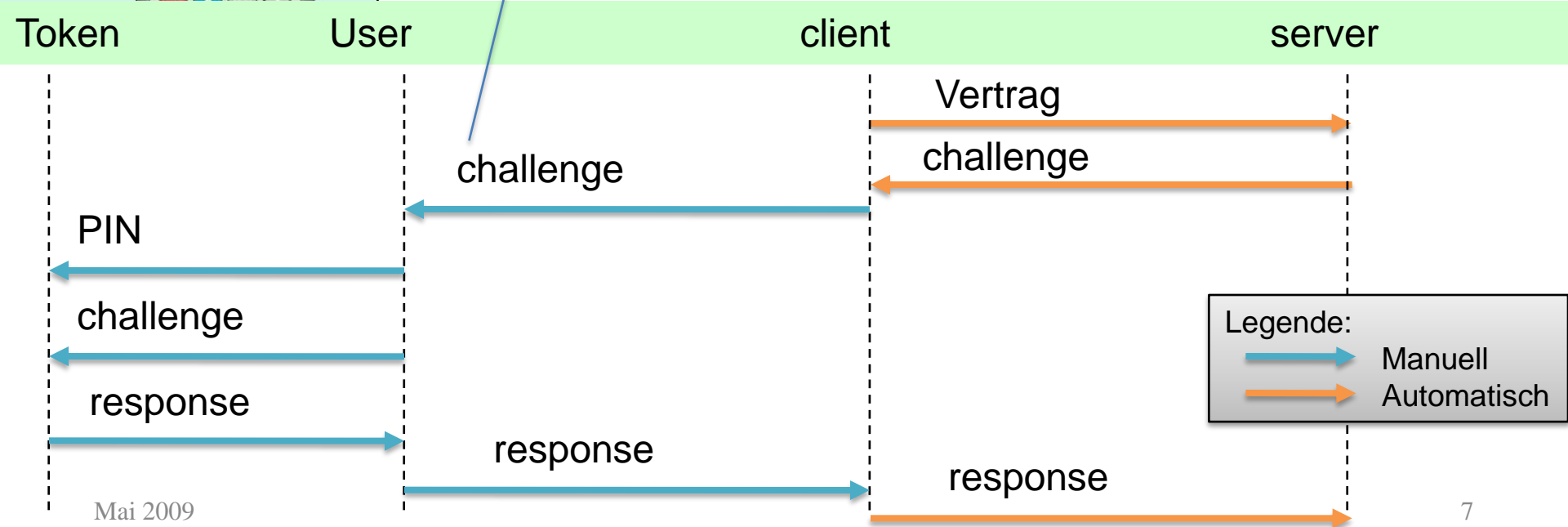


5. Challenge/Response-Tools



Transaktions-
Bestätigung möglich
durch mehrfache
Codes

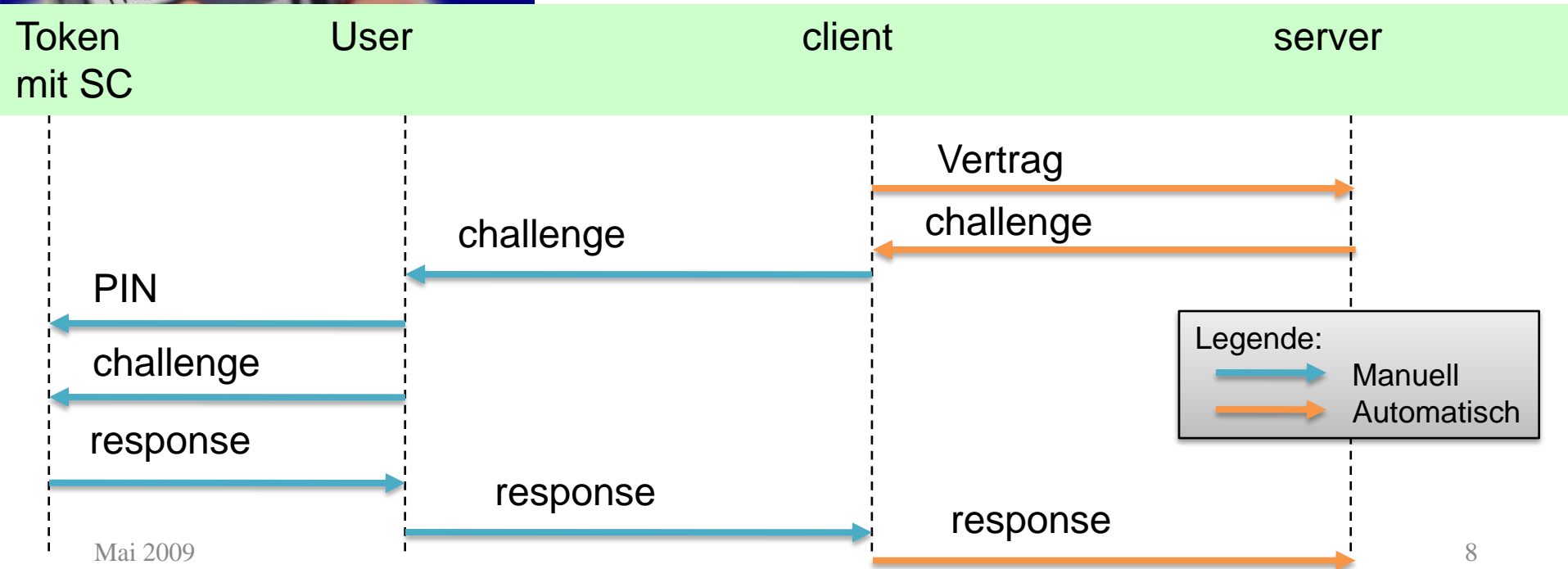
Eingesetzt:
- UBS Telebanking
- Postfinance



6. EMV CAP (Card Authentication Protocol)



Bisher keine breite Anwendung.



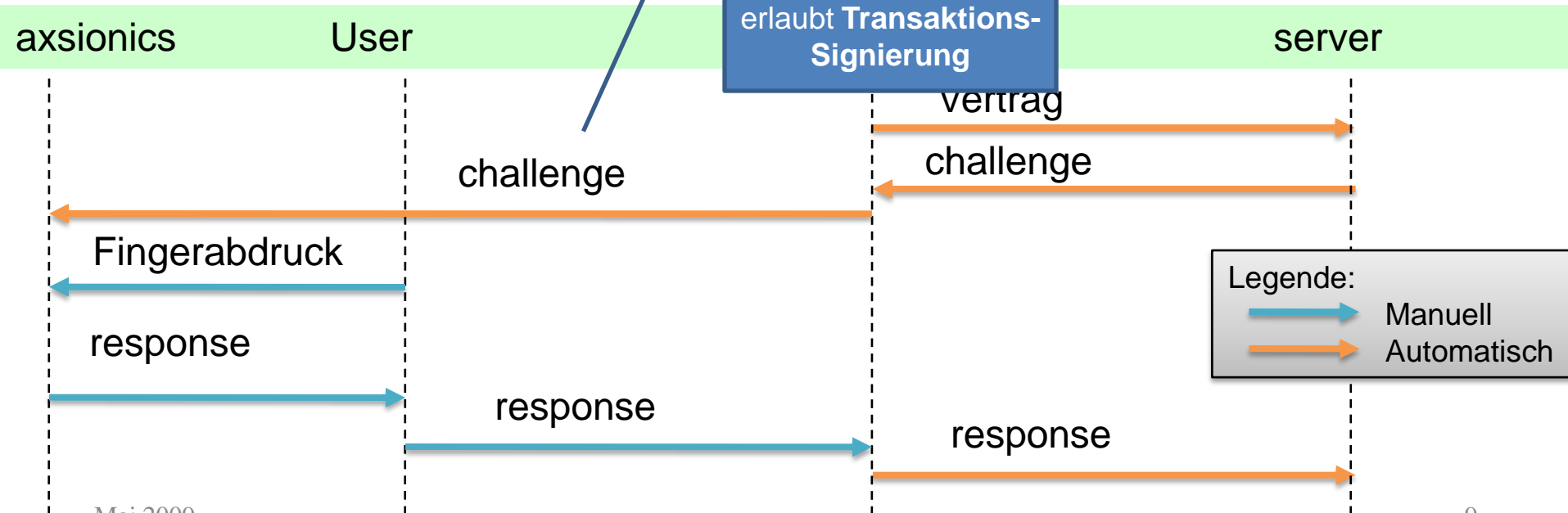
7. Axsionics

- Fingerprint-Leser
- „Flickering“-Interface
- Grosser Display



Bisher keine breite Anwendung.

Transaktions-
abhängiger Challenge
erlaubt **Transaktions-
Signierung**

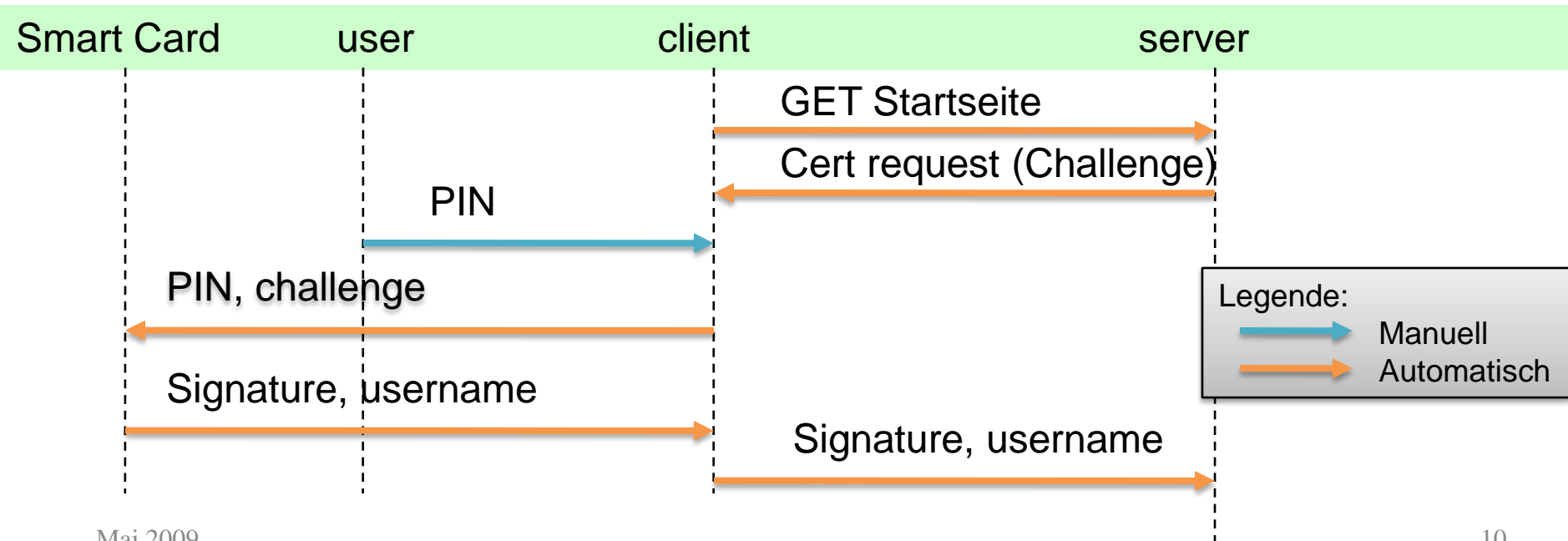


8. SSL Client-Certificate



Zertifikat ist auf einer Smart-Card installiert

Eingesetzt:
– Vereinzelt für B2B-Anwendungen



9. USB-Stick (Smart-Card und Browser)



Browser ist gegen Angriffe geschützt

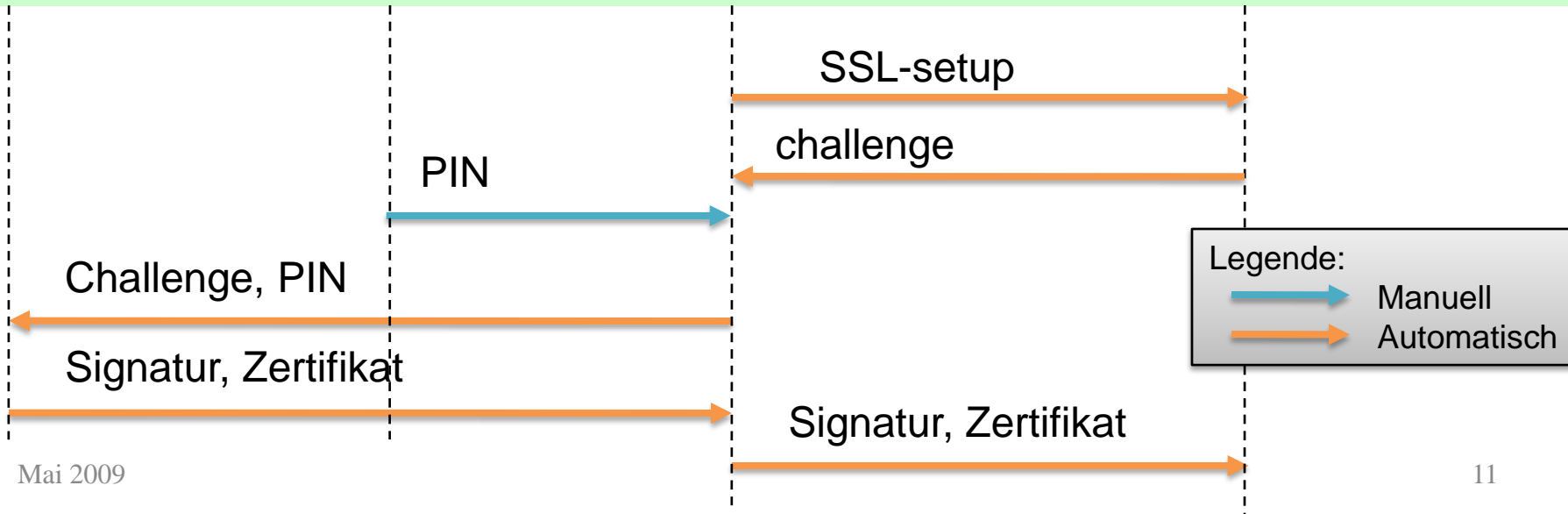
Eingesetzt:
- Migros Bank

USB-Stick
mit SC

user

client

server



Vergleich

Legende
kein Schutz
teilweise geschützt
gut geschützt

		Streichliste / Matrix Ca	dynamisches Token	Mobiltelefon (mTAN)	C/R token	Axonics	SSL-Zertifikat (hard)	SSL-Zertifikat (soft)	Kobil
		1,2	3	4	5,6	7	8	8	9
login, read data									
	Diebstahl Credentials	teilweise geschützt	gut geschützt	gut geschützt	gut geschützt	gut geschützt	gut geschützt	teilweise geschützt	gut geschützt
	Phishing passiv	teilweise geschützt	gut geschützt	gut geschützt	gut geschützt	gut geschützt	gut geschützt	gut geschützt	gut geschützt
	Man-in-the-Middle	kein Schutz	kein Schutz	kein Schutz	kein Schutz	kein Schutz	gut geschützt	gut geschützt	gut geschützt
	Trojaner	teilweise geschützt	teilweise geschützt	teilweise geschützt	teilweise geschützt	teilweise geschützt	gut geschützt	kein Schutz	gut geschützt
Transactions									
	session hijack	kein Schutz	gut geschützt	gut geschützt	gut geschützt	gut geschützt	gut geschützt	gut geschützt	gut geschützt
	session riding (html)	kein Schutz	gut geschützt	gut geschützt	gut geschützt	gut geschützt	kein Schutz	kein Schutz	teilweise geschützt
	Man-in-the-Middle	kein Schutz	kein Schutz	gut geschützt	kein Schutz	gut geschützt	gut geschützt	gut geschützt	gut geschützt
	Trojaner	kein Schutz	kein Schutz	gut geschützt	kein Schutz	gut geschützt	kein Schutz	kein Schutz	teilweise geschützt