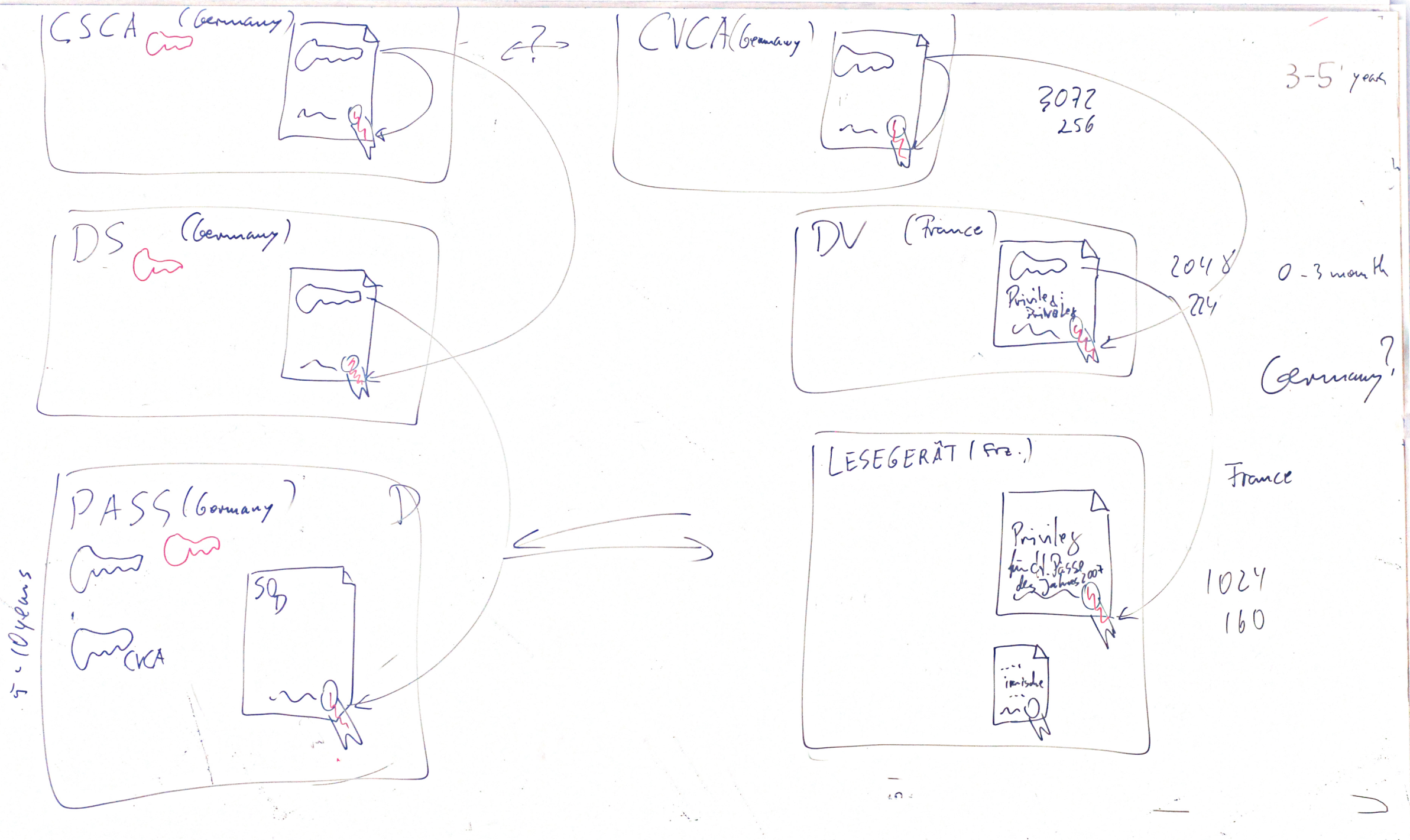
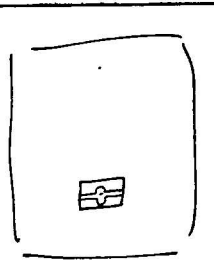
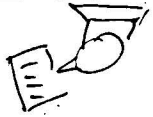
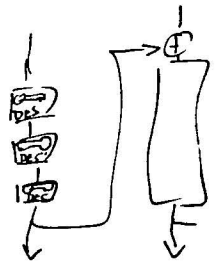

CSCA (Germany)
CVCA (Germany)
3072
256
3-5 years
DS (Germany)
DV (France)
Privileg
2048
224
0-3 month
Germany?
LESEGERÄT (Frz.)
France
PASS (Germany)
SOD
CVCA
5-10 years
Privileg
1024
160

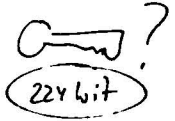


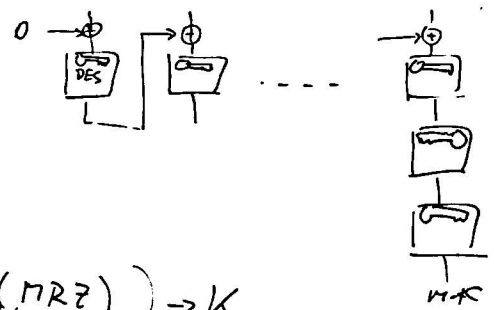


encryption: 2-TDES
(AES?)

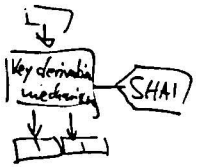


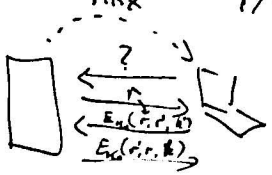
authentication: retail-CBC-MAC





BAC: key derivation(SHA1(MRZ)) → K_0





entropy: ~81 bits
(~56/40 bits)

key derivation($k \| k'$) → K_1

Chip Authentication (EAC)

= DH key exchange

key derivation(xyP) → $K_{2 \ldots}$

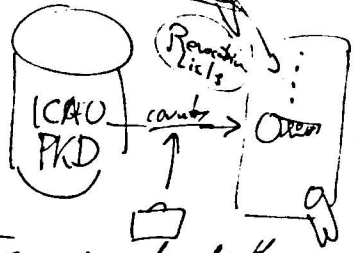
$(P, xP, yP) \xrightarrow{?} xyP$

Diffie-Hellman-Problem

Passive Authentication

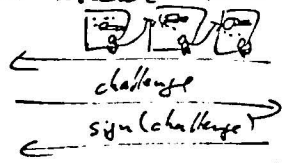
• Chip uses static key pair: (x, xP)

Terminal checks signature ECDSA & that the hash of xP is correct



Terminal Auth.

Check signatures based on a stored Root-CA



Verify.