SICHERE APP-ENTWICKLUNG

AUTHENTISIERUNG MITTELS ELEKTRONISCHER GESUNDHEITSKARTE

Gerald Bartz

gematik GmbH | iOS Development E-Rezept

Holger Ahl

gematik GmbH | Development E-Rezept

gematik

DIE ELEKTRONISCHE GESUNDHEITSKARTE

gematik

DIE ELEKTRONISCHE GESUNDHEITSKARTE

Versicherungsnachweis als gesetzlich Versicherte:r

gematik

DIE ELEKTRONISCHE GESUNDHEITSKARTE

Enthält Daten zur gesetzlichen Versicherung (Versichertenstammdaten)

gematik

DIE ELEKTRONISCHE GESUNDHEITSKARTE

Identitätsnachweis der (gesetzlich) Krankenversicherten in Deutschland

gematik

DIE ELEKTRONISCHE GESUNDHEITSKARTE

gematik

AUTHENTISIERUNG MITTELS ELEKTRONISCHER GESUNDHEITSKARTE

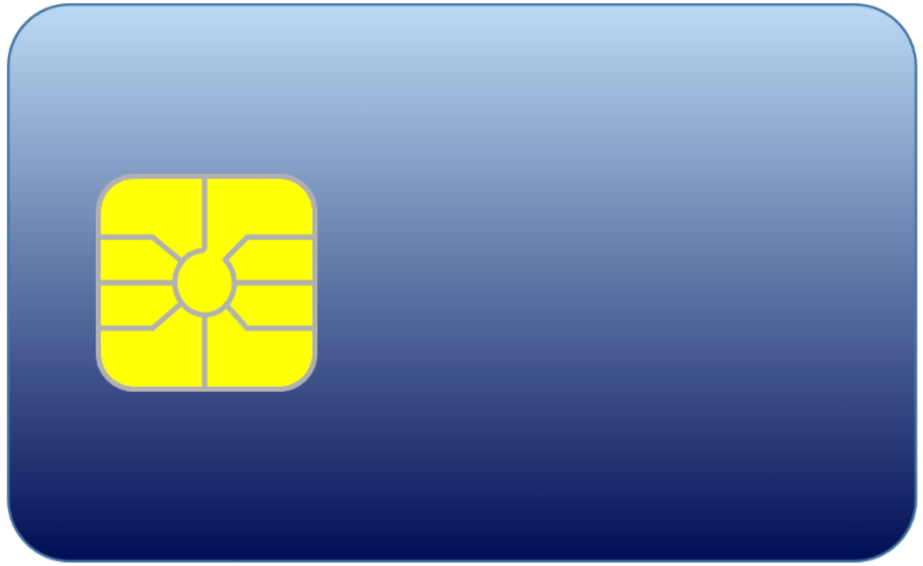
Wie sieht so etwas aus?

AUTHENTISIERUNG MITTELS ELEKTRONISCHER GESUNDHEITSKARTE

Wie sieht so etwas aus?

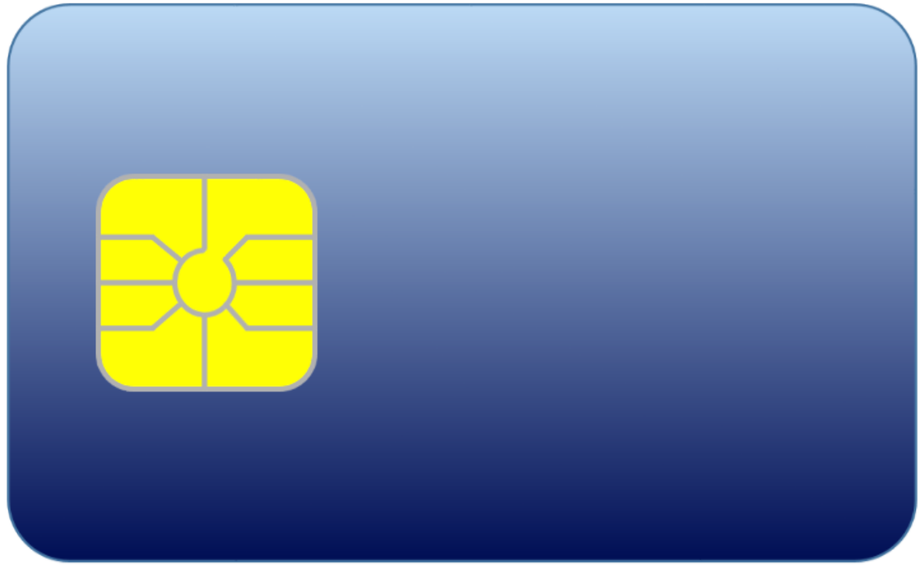
DEMO

GESUNDHEITSKARTE ALS SMARTCARD



gematik

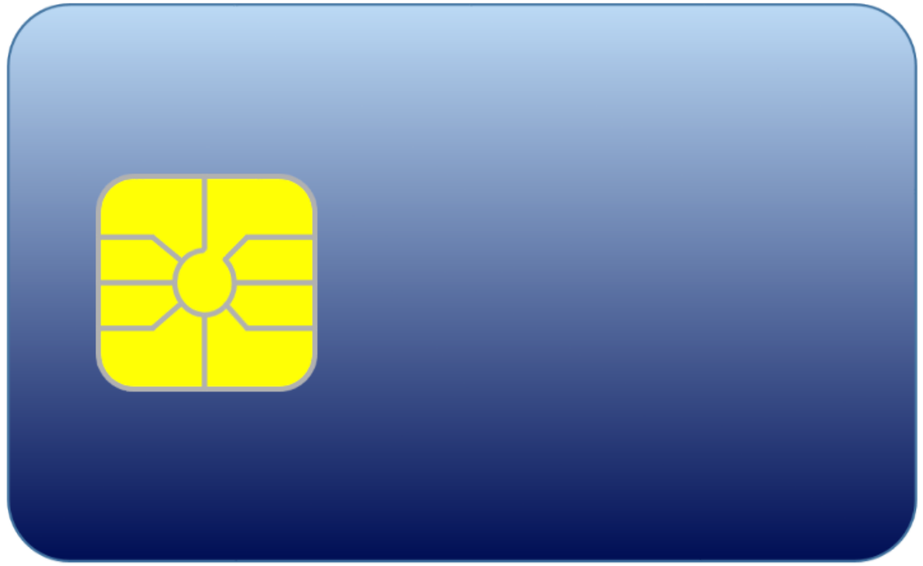
GESUNDHEITSKARTE ALS SMARTCARD



- Prozessorkarte

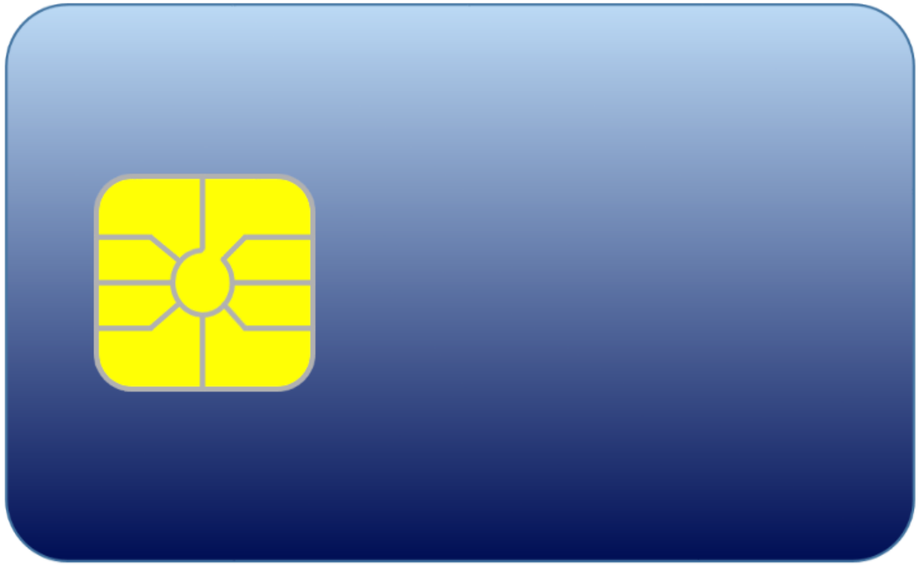
gematik

GESUNDHEITSKARTE ALS SMARTCARD



- Prozessorkarte
- sicherer Speicher

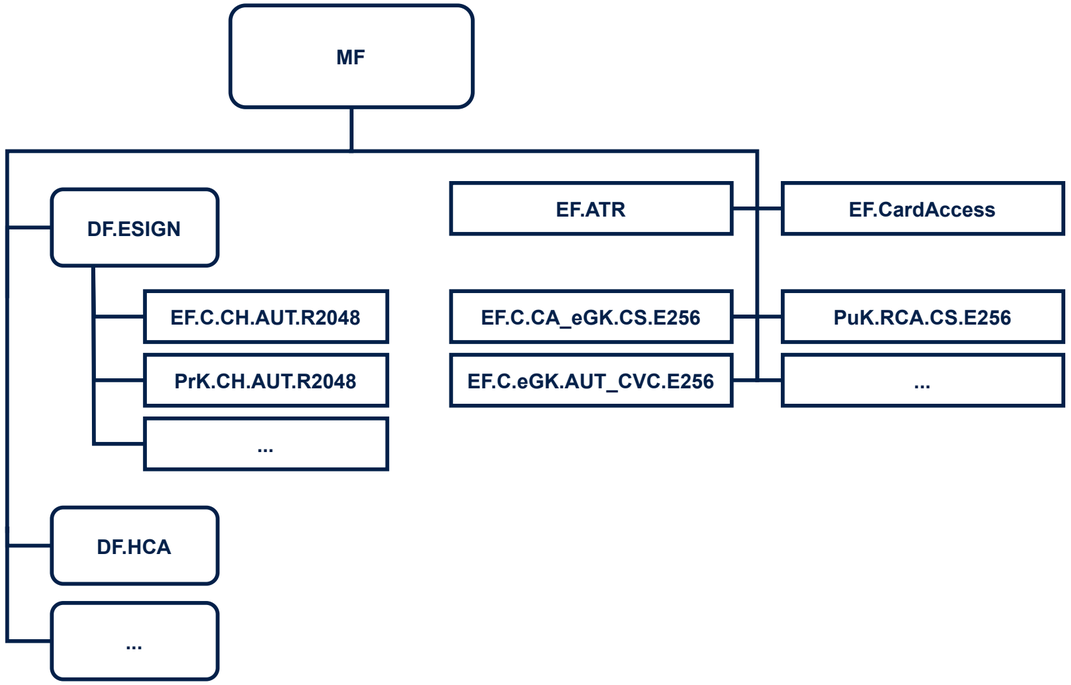
GESUNDHEITSKARTE ALS SMARTCARD



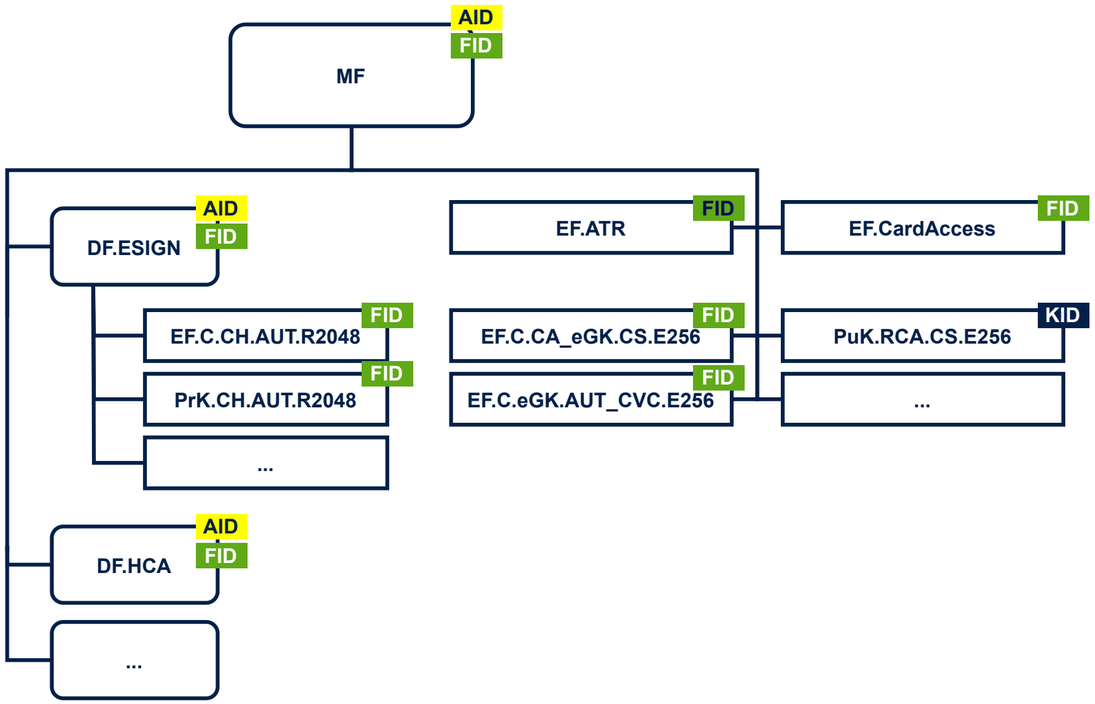
- Prozessorkarte
- sicherer Speicher
- kryptografische Operationen

gematik

OBJEKTSYSTEM

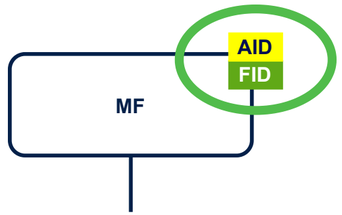


OBJEKTSYSTEM



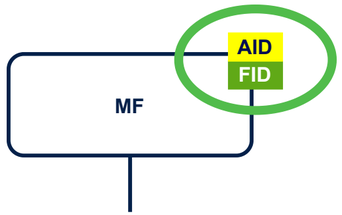
gematik

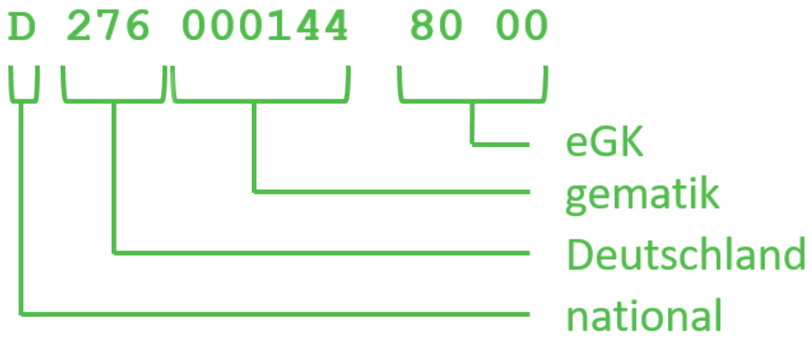
KARTENTYP



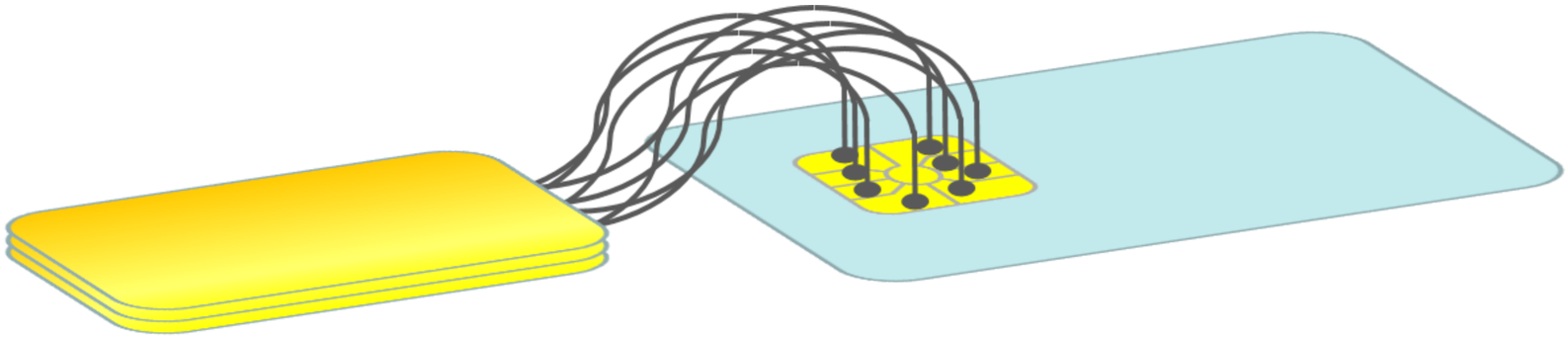
AID bestimmt den Kartentyp

KARTENTYP


AID
FID
MF


D 276 000144 80 00
eGK
gematik
Deutschland
national

KARTENTYP ERKENNEN



gematik

AID BEKANNT GEBEN

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
  "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  ...
  <key>
    com.apple.developer.nfc.readersession.iso7816.select-identifiers
  </key>
  <array>
    <string>
      D2760001448000
    </string>
  </array>
```

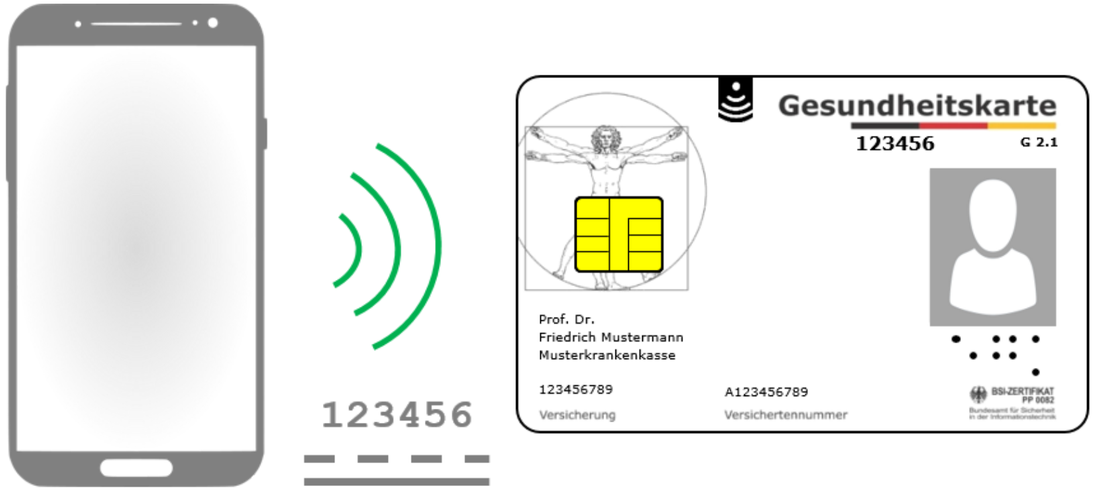
https://developer.apple.com/documentation/corenfc/nfciso7816tag

gematik

NEAR FIELD COMMUNICATION (NFC)

gematik

NEAR FIELD COMMUNICATION (NFC)

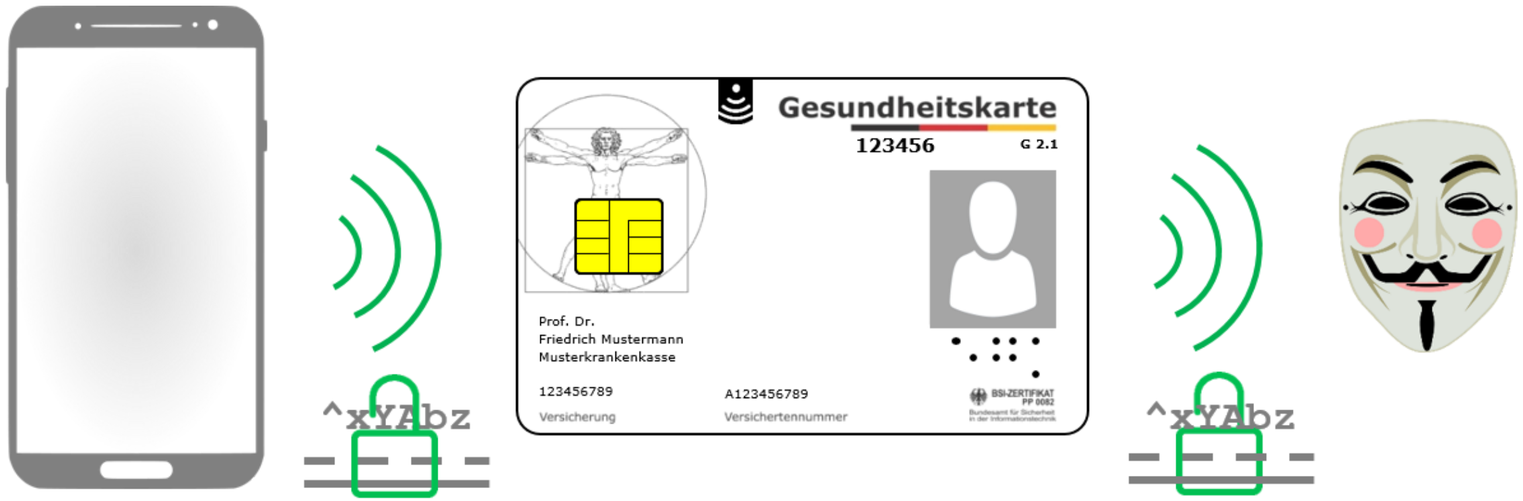


gematik

NEAR FIELD COMMUNICATION (NFC)

gematik

NEAR FIELD COMMUNICATION (NFC)



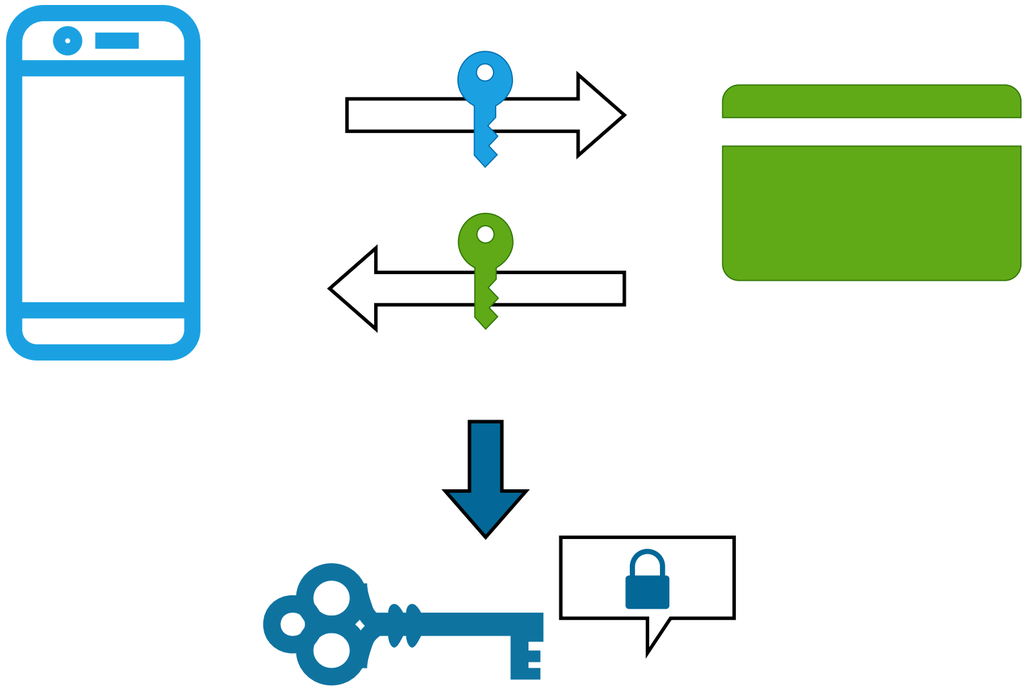
gematik

ANFORDERUNGEN AUSTAUSCH VIA NFC

1. Daten verschlüsselt übertragen
2. nur durch direkten Zugriff initiiert

gematik

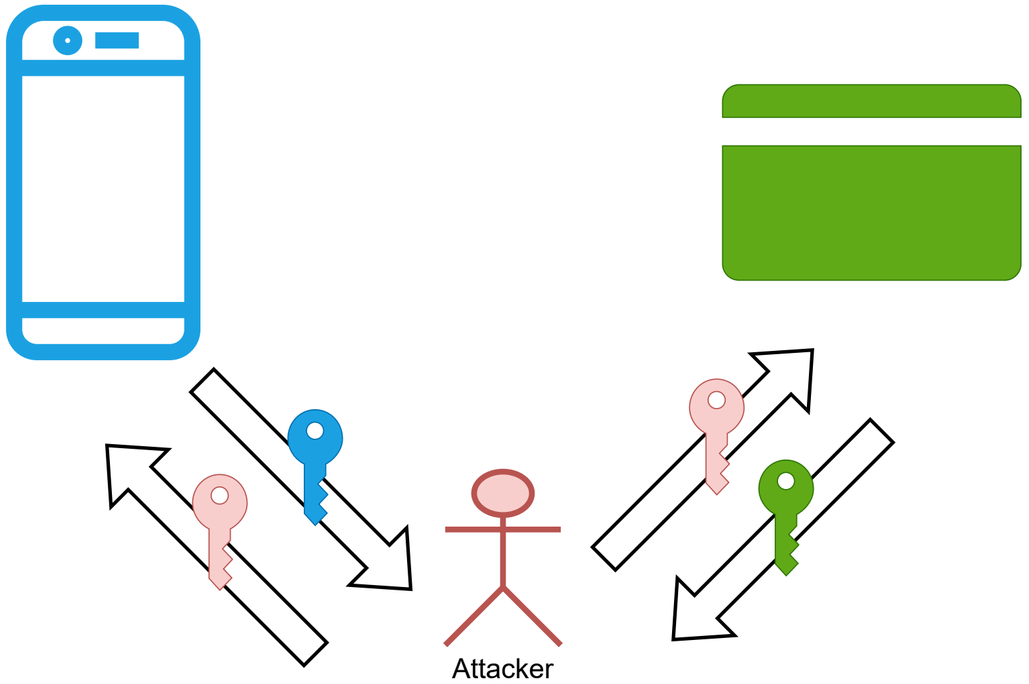
KEY AGREEMENT



Gemeinsames Geheimnis zur Nachrichtenverschlüsselung

KEY AGREEMENT

- "Man in the middle"-Problematik
- auch indirekt initiierbar



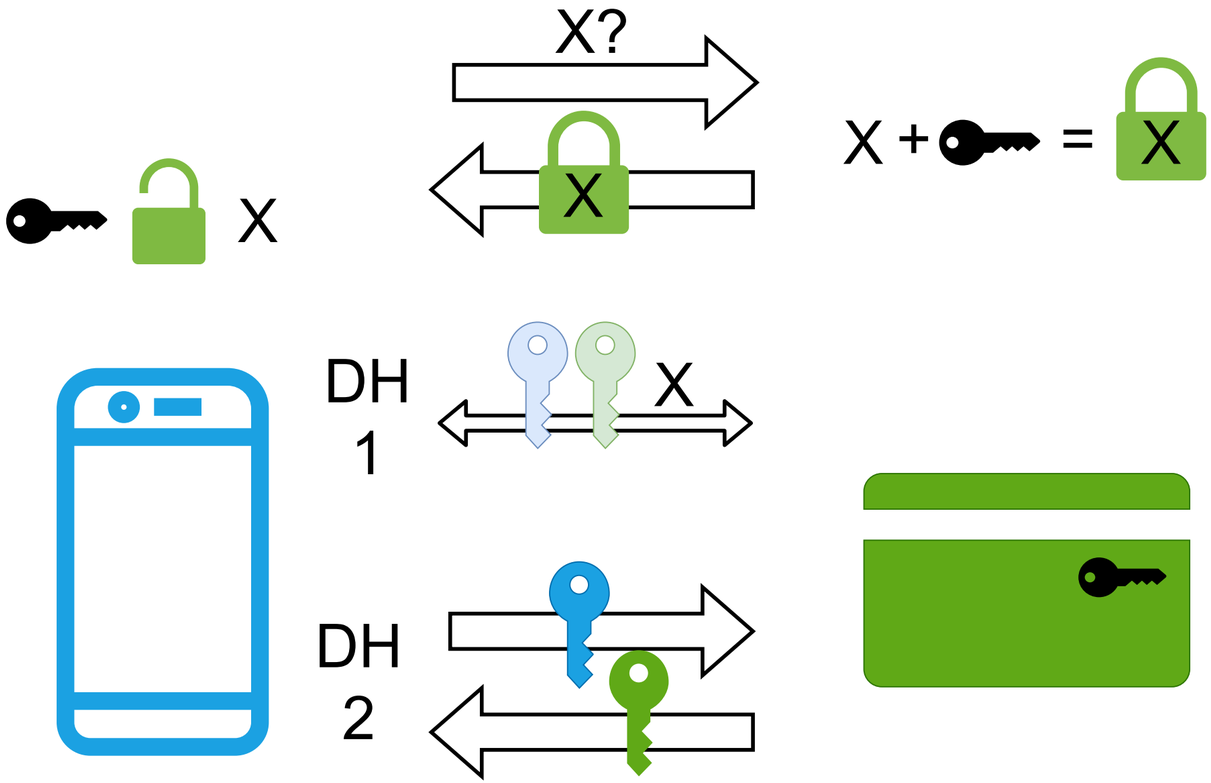
gematik

PACE PROTOKOLL

Password Authenticated Communication Establishment

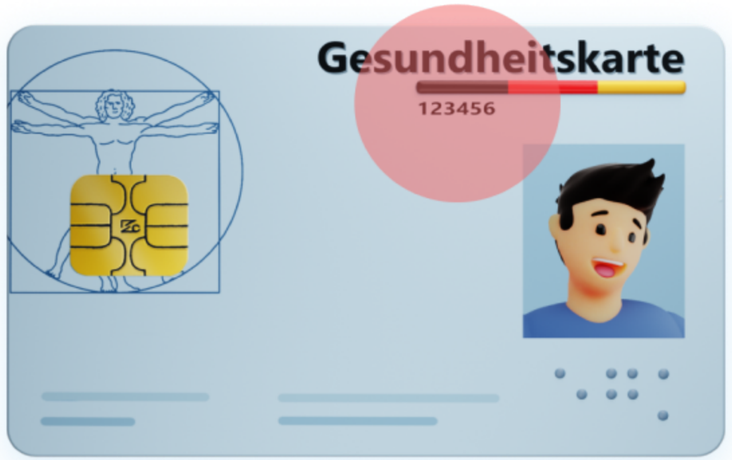
PACE PROTOKOLL

Password Authenticated Communication Establishment



gematik

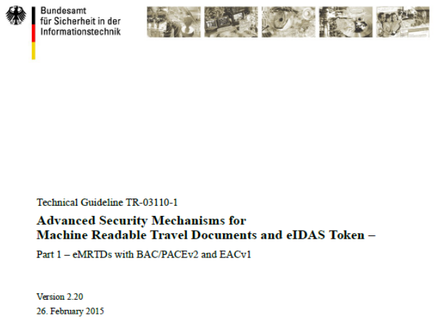
CARD ACCESS NUMBER (CAN)



gematik

PACE - PROTOKOLL

BSI TR 03110



1. Nonce encryption via Password
2. Nonce mapping on Elliptic Curve
3. Key Agreement (EC DH + Derivation)
4. Authentication token exchange

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03110/TR-03110_node.html

PACE - PROTOKOLL

BSI TR 03110

1. Nonce encryption via Password
2. Nonce mapping on Elliptic Curve
3. Key Agreement (EC DH + Derivation)
4. Authentication token exchange

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03110/TR-03110_node.html

SECURE MESSAGING

erst jetzt: Kommunikation via Secure Channel

Command Header				Command Body		
CLA	INS	P1	P2	LC	DATA	LE

b8	b7	b6	b5	b4	b3	b2	b1	Bedeutung
X	0	0	–	–	–	–	–	command class
–	0	0	x	–	–	–	–	command chaining indicator
–	**0**	**0**	**–**	**x**	**x**	**–**	**–**	**secure messaging indicator**
–	**0**	**0**	**–**	**1**	**1**	**–**	**–**	**secure messaging**
–	**0**	**0**	**–**	**0**	**0**	**–**	**–**	**no secure messaging**
–	0	0	–	–	–	x	x	channel number

PACE - PROTOKOLL

DEMO

DANKE

OpenHealthCard connect App-Store

https://apps.apple.com/de/app/openhealthcard-connect/id1450490405

OpenHealthCard connect GitHub

https://github.com/gematik/ref-OpenHealthCardKit

gerald.bartz@gematik.de

holger.ahl@gematik.de

BILDQUELLEN

https://www.pixabay.com