gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Data protection vs. access convenience – card-to-card-authentication: the approach of choice

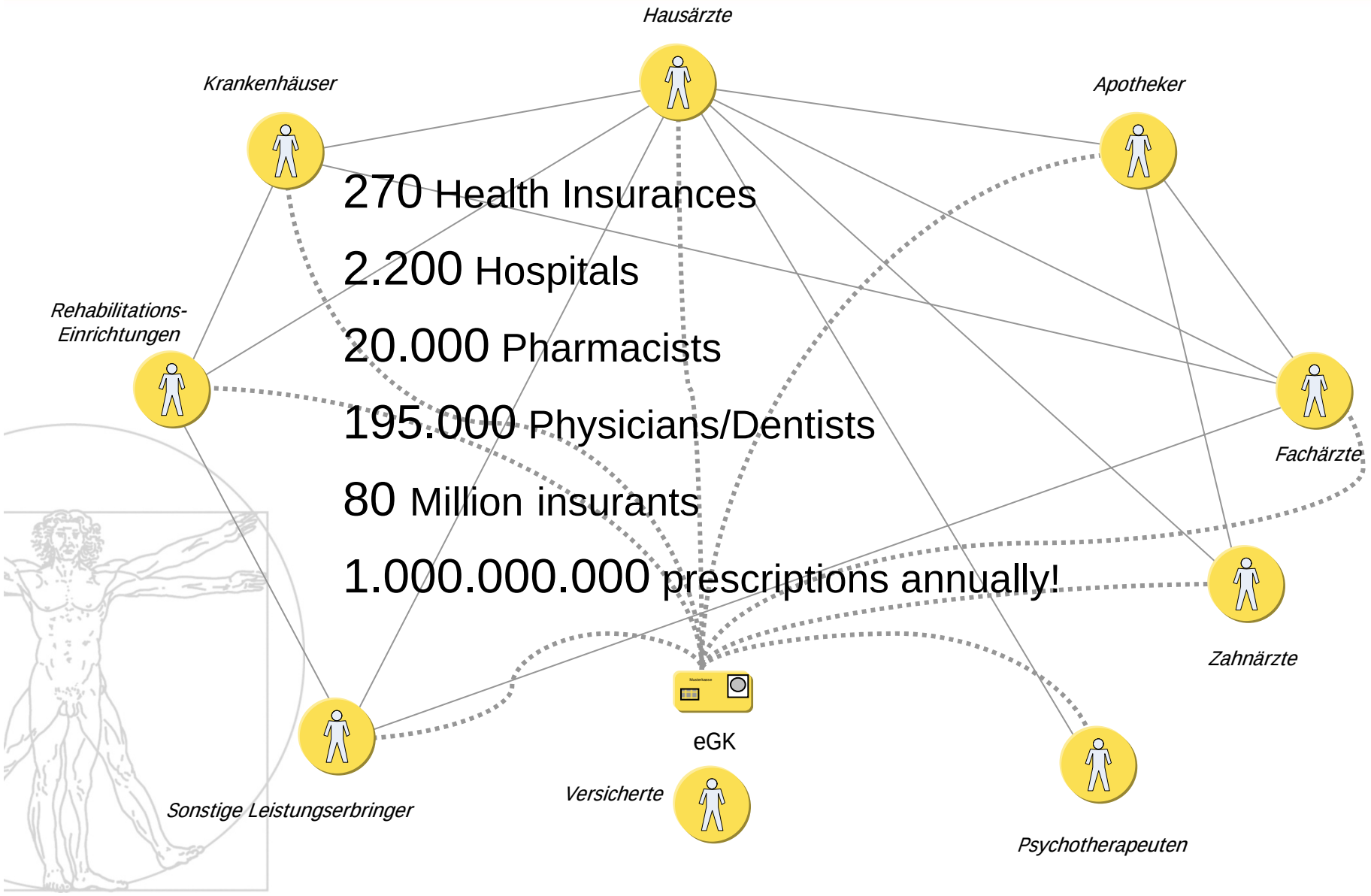
Dr. Stefan Buschner

gematik - Gesellschaft für Telematikanwendungen
der Gesundheitskarte mbH
Friedrichstraße 136
10117 Berlin

11.09.2008

Aim: Interconnection of all participants

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH



270 Health Insurances

2.200 Hospitals

20.000 Pharmacists

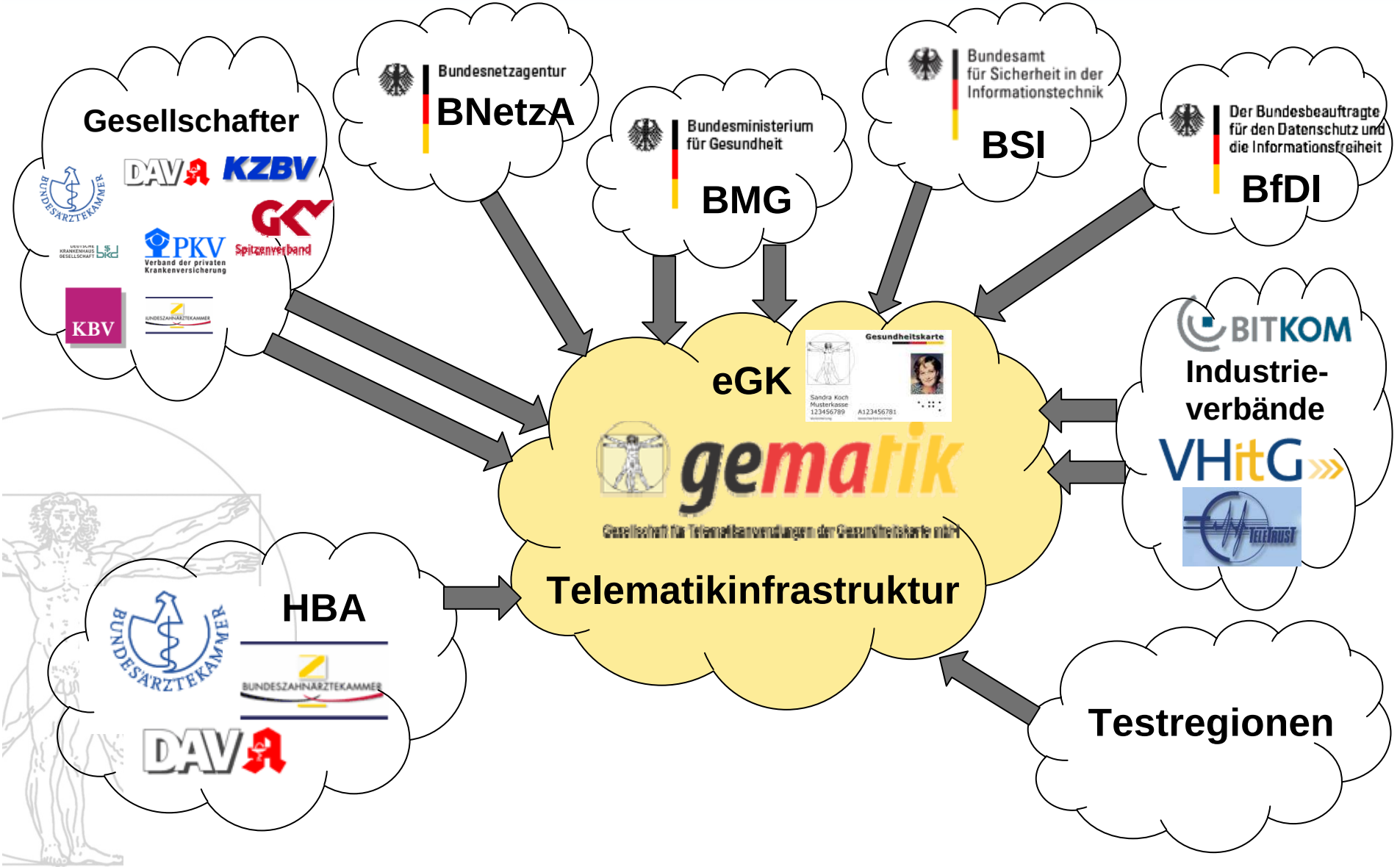
195.000 Physicians/Dentists

80 Million insurants

1.000.000.000 prescriptions annually!

eGK context

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH



Step-by-step introduction

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

- Functionality **(offline)**
  - insurant data (VSD)
  - e-prescription
  - emergency data

RELEASE 1

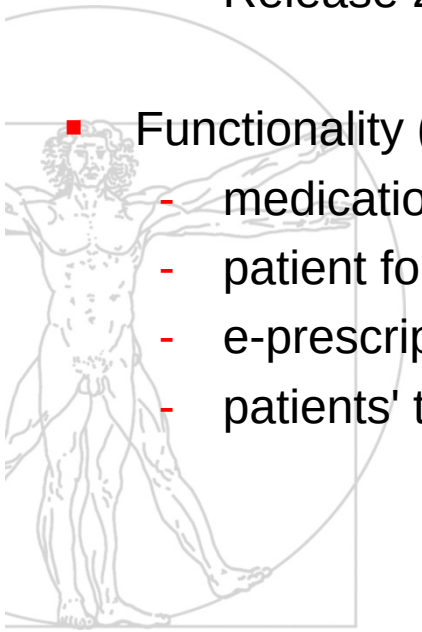
- Functionality **(online)**
  - insurant data, physician's letter and e-prescription
  - Release 2.K comfort-signature

RELEASE 2

RELEASE 2K

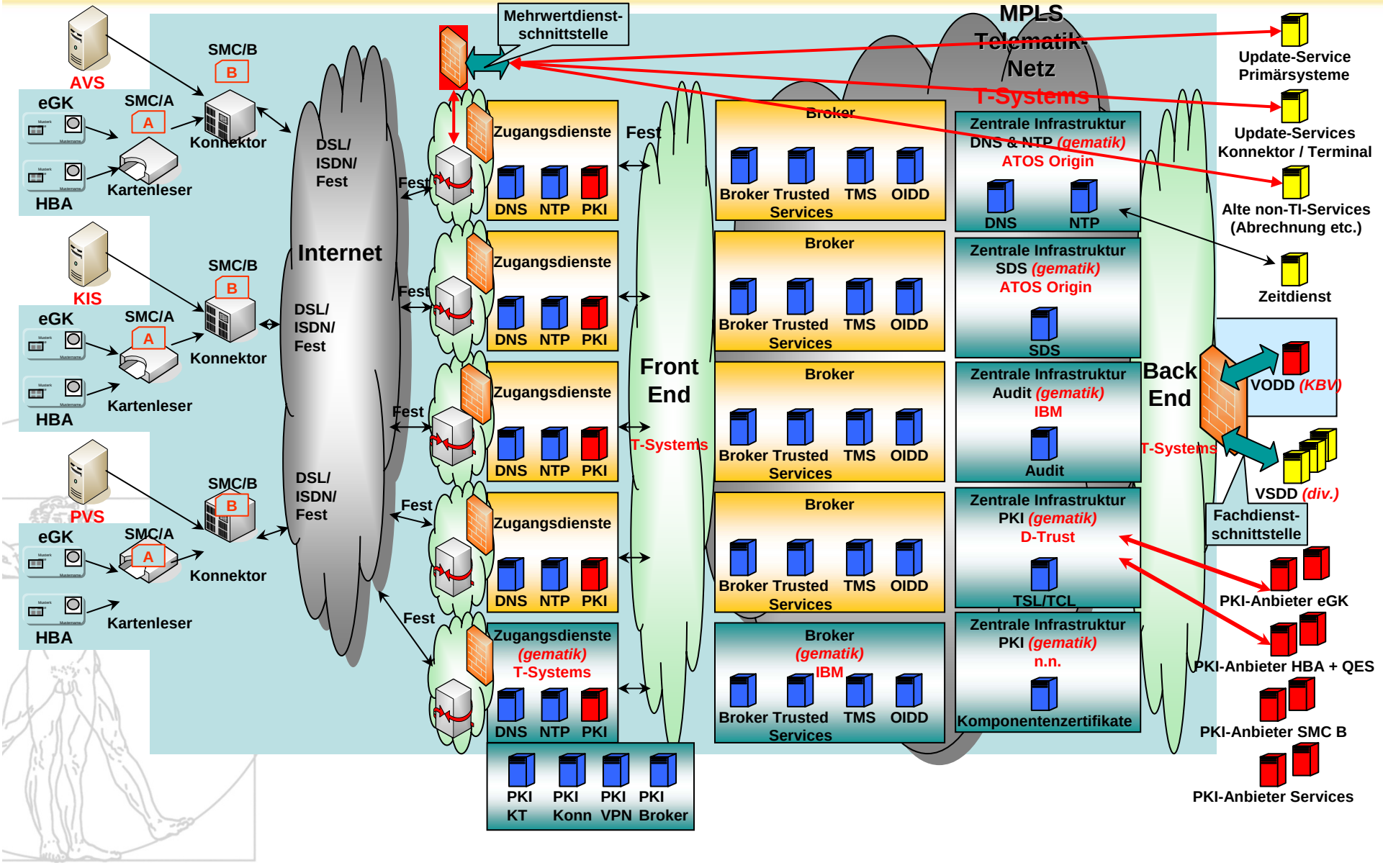
- Functionality **(online)**
  - medication-interaction-testing (AMTS)
  - patient folder
  - e-prescription: hospitalization, BTM, modality
  - patients' terminal (eKiosk)

RELEASE 3



Telematic infrastructure

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

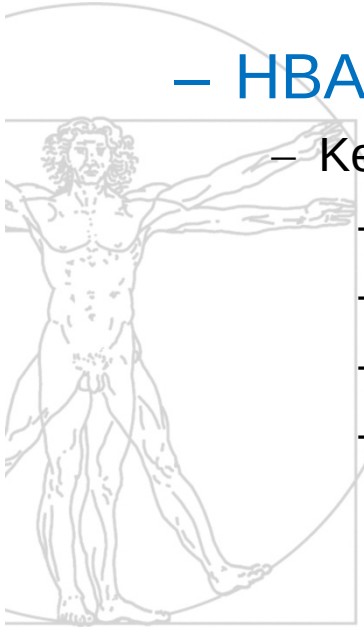


Cards

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Cards of the telematic infrastructure:

- eGK: electronic health card
  - Insurant data
  - medical data
  - Keys and certificates (X.509 und CVC)
- HBA: electronic health professional card
  - Keys and certificates (X.509 und CVC)
    - qualified electronic signatures
    - Personal identity
    - Authentication
    - C2C-Authentication to SMC and eGK for setting the security level

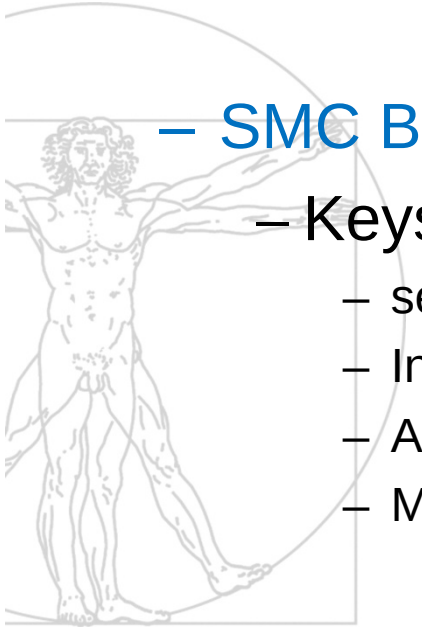


Cards II

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Cards of the telematic infrastructure:

- SMC A: Secure Module Card A
  - Keys and Certificate (CVC)
    - C2C-Authentication to eGK for setting the security level
    - Installing Trusted Channel to HBA

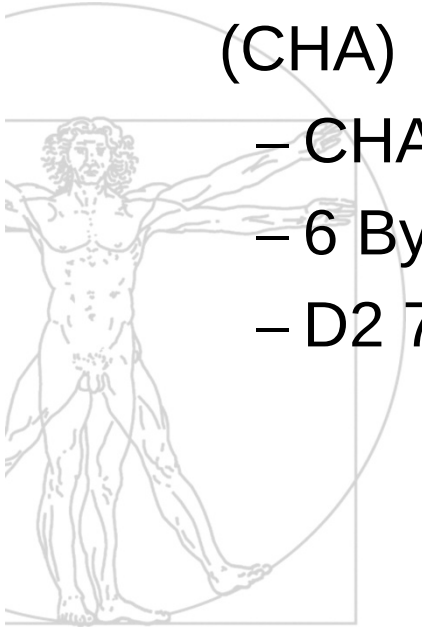


- SMC B: Secure Module Card B
  - Keys and Certificate (X.509 und CVC)
    - see SMC A
    - Institution identity (surgery, hospital, pharmacy)
    - Authentication (SSL-tunnel to Broker)
    - Message signature, decryption

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

CVC: Card-Verifiable-Certificate

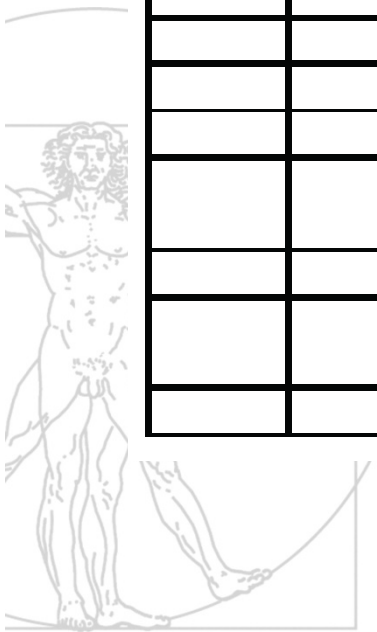
- ASN.1-coded certificate (ISO 7816-8)
- Is verifiable by a card with the help of a public CA-key
- Certificate without expiring date
- Certificate contains “Certificate Holder Authorisation” (CHA)
  - CHA hallmarks the role of the user/institution
  - 6 Byte prefix, 1 Byte profile-ID
  - D2 76 00 00 40 00 || 0x



Example CVC

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

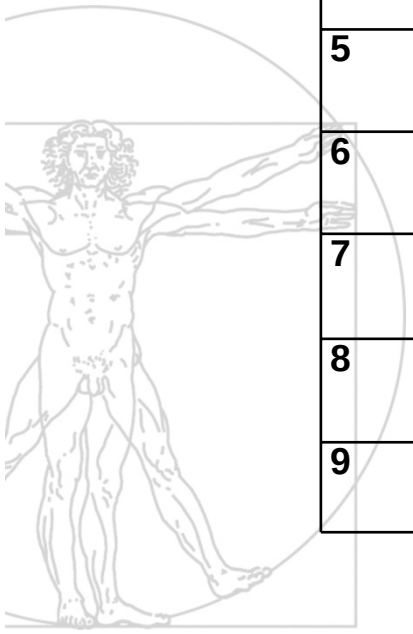
Tag	L	Wert		
'7F21'	'81CD'	CV-Zertifikat (205 Byte)		
		Tag	L	Wert
		'5F37'	'8180'	SIG.CA (128 Byte)
				Digital Signature Input für SIG.CA ('6A' ..'BC'):
				'6A' = Padding entsprechend [ISO9796-2]
				'04' = CPI
				'xx..xx' = CAR (8 Byte)
				'xx..xx' = CHR (12 Byte)
				'xx..xx' = CHA (7 Byte)
				'xx..xx' = OID (6 Byte)
				'xx..xx' = PK part 1 (erster Teil des Modulus, 72 Byte)
				'xx..xx' = Hash (20 Byte, Hash Input: DEs CPI ... PK, siehe Tabelle B.10)
				'BC' = Trailer
		'5F38'	'3C'	'xx..xx' = PK-Rest (Rest des Modulus, gefolgt vom Exponenten '00010001', 60 Byte)
		'42'	'08'	'xx..xx' = CAR (8 Byte)



Profile-IDs of CHA

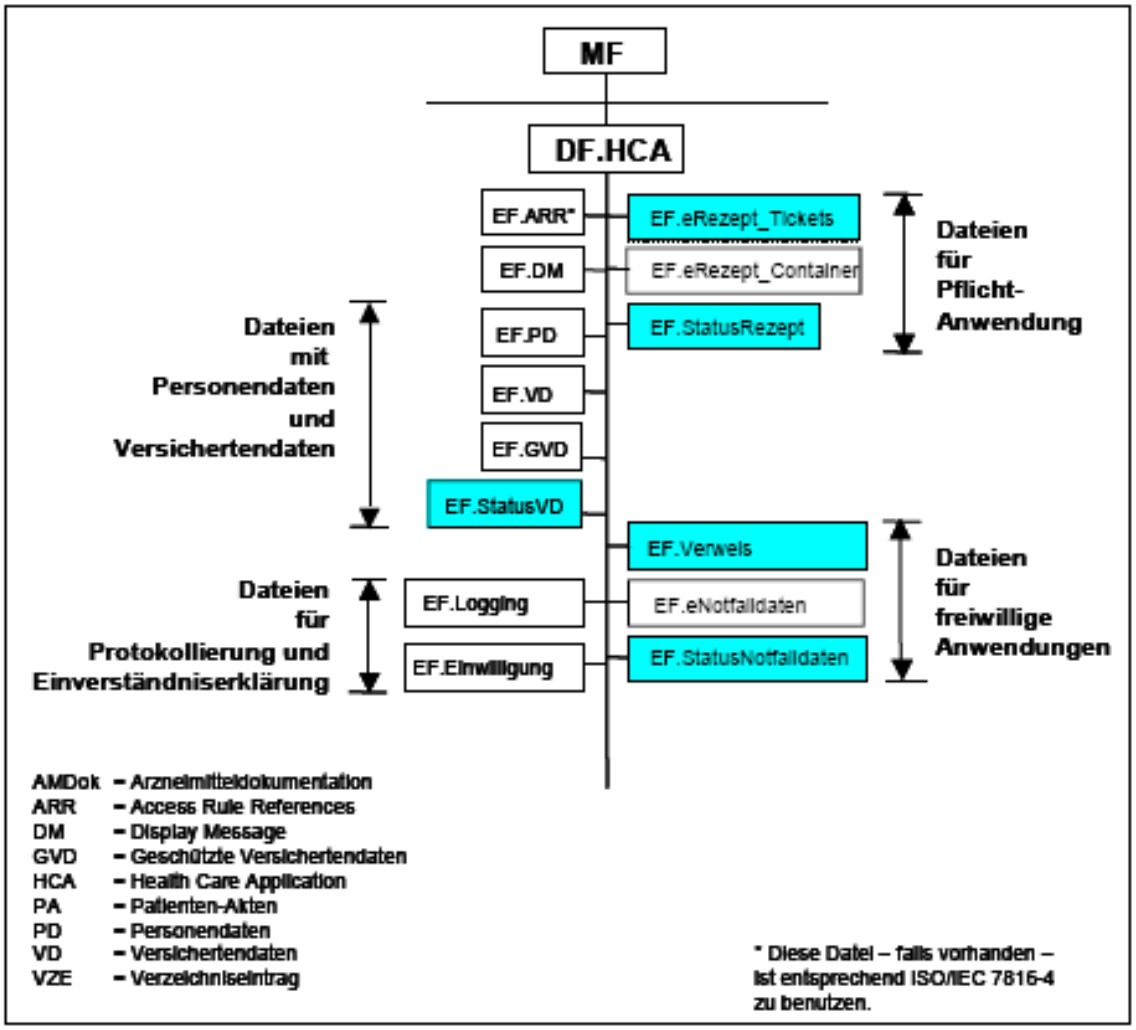
gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Profile	Role
1	eKiosk
2	Physician, medical secretary, SMC-B surgery/hospital
3	Pharmacist, pharmaceutical assistant, SMC-B pharmacy
4	Psychotherapist (HBA + SMC B)
5	HBA healthcare therapist
6	-
7	Ambulance officer
8	SMC B health insurance
9	SMC B other medical personal



eGK applications

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH



eGK access rules

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Profile	Personal data, insurance data	Protected personal data	Aggree-ment	link	Prescrip-tion	Prescripti on tickets	Emer-gency data	logging
PIN-home	R	R	RAD	RUAD	R	READ	AD	R
1+*	R	R	RAD	RUAD	R	READ	AD	R
2	R	R	(RUAD)*	(RUA D)*	RU	RUE	R(UE)*	
3	R	R	(RUAD)*	(RUA D)*	RU	RUE	R(E)*	
4	R	R	(RUAD)*	(RUA D)*			R(E)*	
5	R	R			RU	RUE		
7	R	R*					R	
8	R	R						
9	R	R		(RU)*	(R)*	(RE)*		

R=read, U=update, A=activate, D=deactivate, E=erase, *=+PIN.CH

eGK access rules for keys and certificates

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Profile	Cert Auth	PrK Auth	Cert Enc	PrK Enc	Cert AuthN	PrK AuthN	Cert EncV	PrK EncV
PIN-home	R	IS	R	V	R	IS	R	V
1	R	(IS)*	R	V*	R*	(IS)*	R*	V*
2	R	(IS)*	R	V*	R	IS	R	V
3	R	(IS)*	R	V*	R	IS	R	V
4	R	(IS)*	R	V*	R	IS		
5	R	(IS)*	R	V*	R	IS	R	V
7	R		R					
8	R		R		R	IS		
9	R	(IS)*	R		R	IS	R*	V*

R=read, I=internal authentication, S=electronic signature, V=decipher, *=+PIN.CH

Thank you for your attention!

gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

info@gematik.de ▪ www.gematik.de