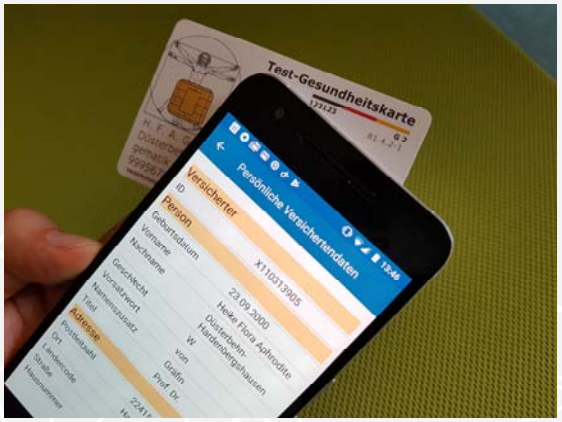
NUTZUNG DER EGK ÜBER DIE NFC-SCHNITTSTELLE MOBILER ENDGERÄTE



conhit 2018

Fraunhofer FOKUS

Fraunhofer SIT

OTH Ostbayerische Technische Hochschule Regensburg

Gefördert durch:
Bundesministerium für Gesundheit
aufgrund eines Beschlusses des Deutschen Bundestages

PROJEKTBESCHREIBUNG UND -ZIELE

Ziele / Gegenstand der Förderung

„… Im Vorfeld und begleitend zu den Maßnahmen der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) zum Ausbau der TI sollen Maßnahmen gefördert werden, die auf Basis von Konzepten und Komponenten der TI technische Lösungen für eine **sichere Nutzung von elektronischen Anwendungen aus dem privaten Bereich** erarbeiten und anhand beispielhafter konkreter Anwendungen erproben. Es gilt in erster Linie, eine **Machbarkeitsstudie** durchzuführen und die Ergebnisse aus dieser Studie in Form eines **„Proof of Concept“ (PoC)** darzulegen.

Dabei soll speziell die Nutzung verbreiteter **mobiler Endgeräte der Versicherten** — insbesondere Smartphones — untersucht werden.

…

Dabei muss für mobile Endgeräte eine **2-Faktoren-Authentifizierung mittels eGK und PIN direkt über die NFC-Schnittstelle** implementiert und erprobt werden.

….“

Fraunhofer FOKUS Fraunhofer SIT OTH Ostbayerische Technische Hochschule Regensburg

INFORMIERTE EINWILLIGUNG

Zielsetzung / Funktionsumfang der App im Zusammenspiel mit Backend-Diensten

- **Übersichtliche Darstellung von Information** zu einer medizinischen Anwendung und ggf. Behandlung
- Funktion zur automatisierten **Übernahme von Versichertenstammdaten** der eGK in die zu erstellende Einwilligungserklärung
- **Erklärung einer Einwilligung** auf elektronischem Weg unter Zuhilfenahme der Authentifizierungsfunktion der eGK
- **Dauerhafte Speicherung von erteilten Einwilligungen** und zugehörigen Informationen für eine spätere Einsicht und Veränderung
- **Veränderung/Widerruf bestehender Einwilligungserklärungen** auf elektronischem Weg unter Zuhilfenahme der Authentifizierungsfunktion der eGK

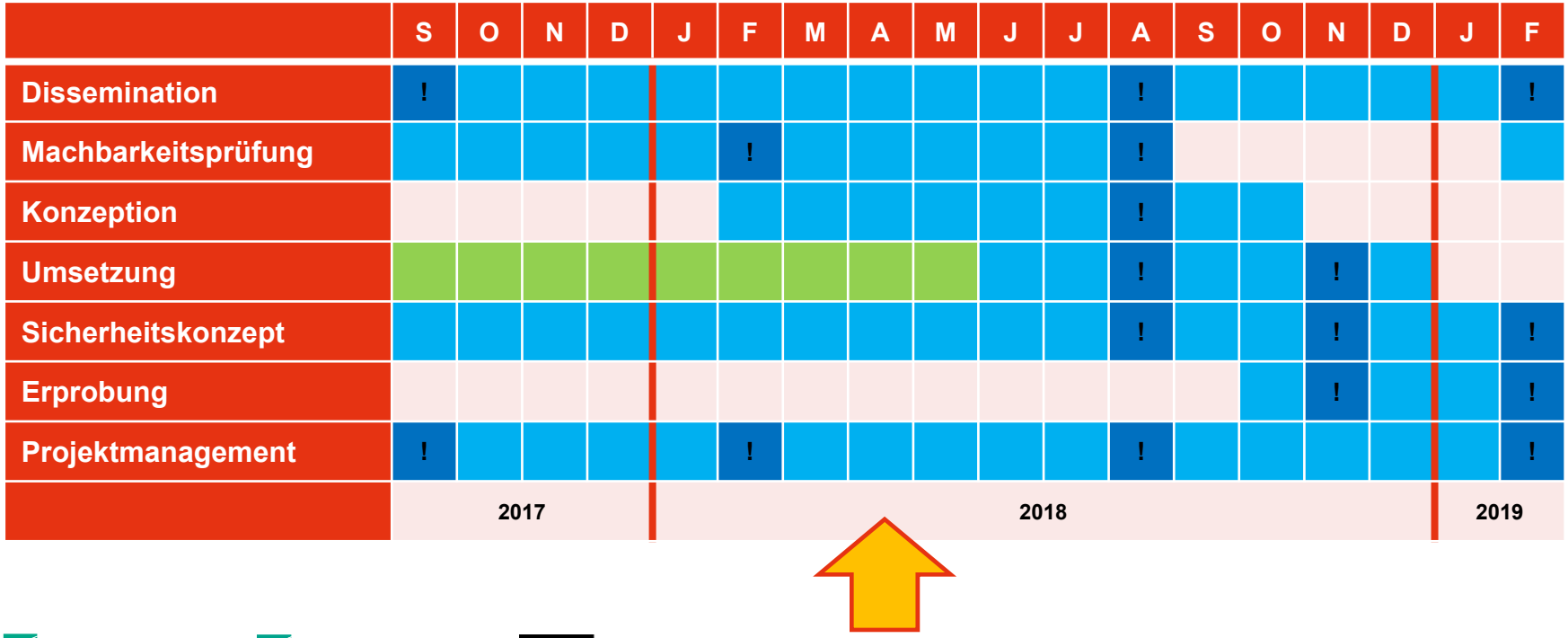
VIDEOSPRECHSTUNDE

Zielsetzung / Funktionsumfang der App im Zusammenspiel mit Backend-Diensten

- **Kryptografisch abgesicherter Aufbau einer Punkt-zu-Punkt Kommunikation** zum Austausch von Video- und Audiodaten
- **Identifizierung und Authentisierung des Patienten** gegenüber dem Arzt unter Nutzung von auf der eGK gespeicherten Schlüsseln und Zertifikaten

GESAMTPROJEKTPLANUNG

Planung



Fraunhofer FOKUS Fraunhofer SIT OTH Ostbayerische Technische Hochschule Regensburg

GRUNDLAGEN

Fraunhofer FOKUS

Fraunhofer SIT

OTH Ostbayerische Technische Hochschule Regensburg

GRUNDLAGEN

Status NFC eGK

- Die aktuellen Spezifikationen der gematik sehen die NFC-Schnittstelle der eGK als eine mögliche Option (Option_kontaktlose_Schnittstelle) vor
- Entsprechende Karten sind bei den Herstellern bereits verfügbar, wurden bisher jedoch durch keine der Kassen herausgegeben
- Die Nutzung der eGK über die NFC-Schnittstelle ist nur über den Aufbau eines sicheren Kanals zur Karte möglich
- Bestimmte Operationen der Karte (z.B. Signaturoperationen) erfordern die Eingabe einer PIN
- eGK PINs wurden bisher nicht herausgegeben

KARTENKOMMUNIKATION ÜBER DIE NFC-SCHNITTSTELLE

Aufbau eines sicheren Kanals

- Ziele:
  - Nicht jedes Endgerät soll auf die Karte zugreifen können.
  - Die Kommunikation zur Karte soll verschlüsselt erfolgen.

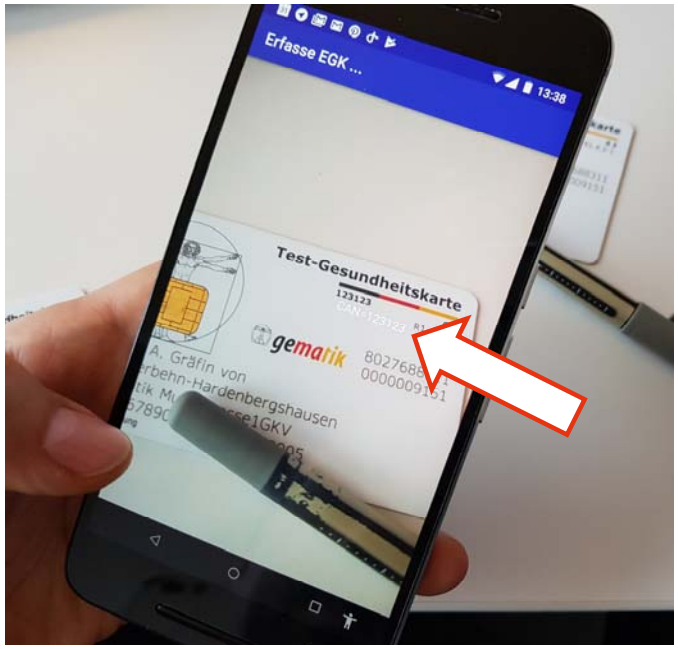
- Nutzung von PACE (Password Authenticated Key Exchange) zur Etablierung eines sicheren Kanals
- Die auf der eGK aufgedruckte Card Access Number (CAN) dient als Password für das Protokoll

KARTENKOMMUNIKATION ÜBER DIE NFC-SCHNITTSTELLE

HERAUSFORDERUNGEN

Accessibility / Barrierefreiheit

– Die Card Access Number (CAN) ist insbesondere für Personen mit Sehbehinderungen schwer zu identifizieren, bildet jedoch die zwingende Voraussetzung für die Nutzung der eGK → ***automatische Erkennung durch das Smartphone (OCR)***



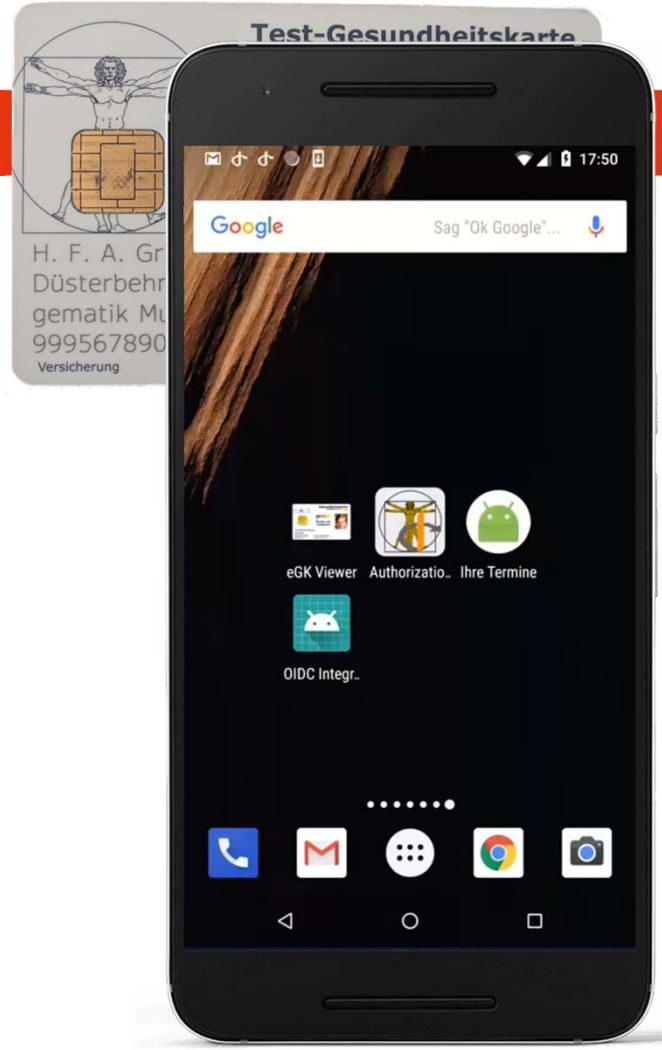
CAN-ERKENNUNG PER OCR

Fraunhofer FOKUS

Fraunhofer SIT

OTH OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

EGK VIEWER



Fraunhofer FOKUS

Fraunhofer SIT

OTH OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

GRUNDÜBERLEGUNGEN

PIN und CAN (Sicherheit vs. Usability)

Herausforderung:

- Die Card Access Number (CAN) wird benötigt, um einen verschlüsselten Kanal zwischen Karte und mobilem Endgerät aufzubauen
- Die PIN wird benötigt, um bestimmte Funktionen der Karte freizuschalten
- Der Umgang mit diesen Sicherheitsmerkmalen stellt aus Usability-Sicht ein Problem dar

Grundüberlegung:

- Einmalige Eingabe und Speicherung der CAN im Zuge einer „Kartenregistrierung“ → persönliches Endgerät des Versicherten
- Reduzieren der Anzahl der notwendigen PIN-Eingaben (ggf. über die Ableitung von zusätzlichen Sicherheitsmerkmalen)

Fraunhofer FOKUS Fraunhofer SIT OTH Ostbayerische Technische Hochschule Regensburg

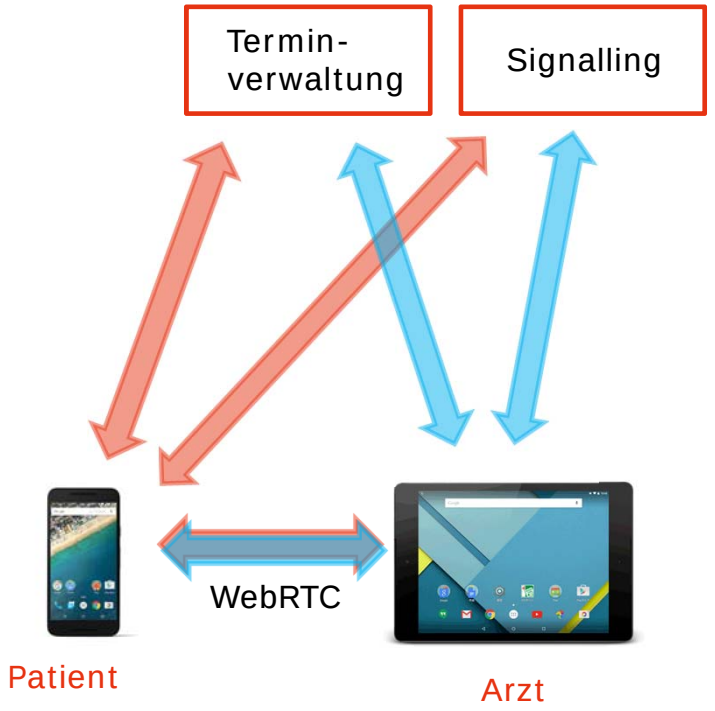
KOMMUNIKATIONSBEZIEHUNGEN VIDEOKONFERENZ

Konzeption Videosprechstunde

Terminverwaltung – *Zuordnung Termin + Teilnehmer*

Signalling – *Gesprächsvermittlung: Austausch von WebRTC-Verbindungsparametern*

WebRTC – *Peer-2-Peer-Audio-/Videoverbindung*



Fraunhofer FOKUS
Fraunhofer SIT
OTH Ostbayerische Technische Hochschule Regensburg

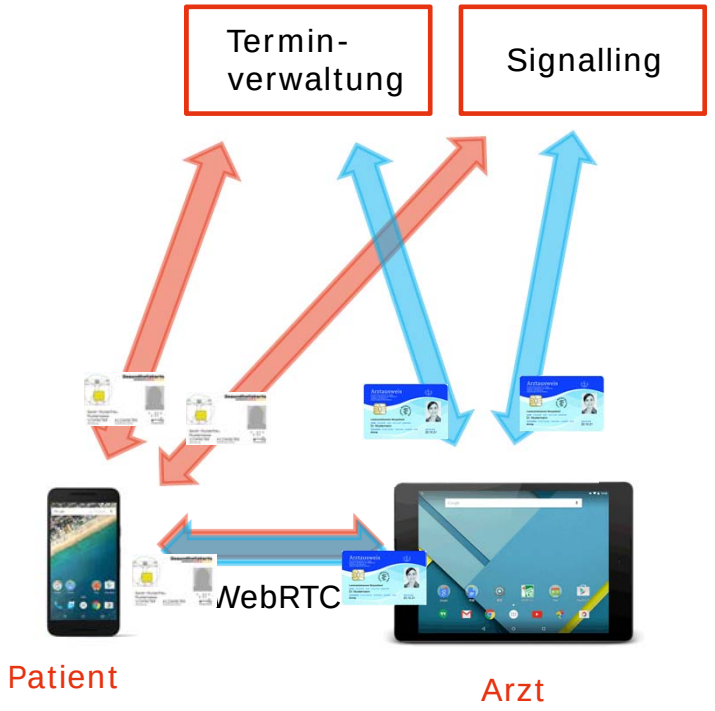
KOMMUNIKATIONSBEZIEHUNGEN VIDEOKONFERENZ

Konzeption Videosprechstunde

Terminverwaltung – *Zuordnung Termin + Teilnehmer*

Signalling – *Gesprächsvermittlung: Austausch von WebRTC-Verbindungsparametern*

WebRTC – *Peer-2-Peer-Audio-/Videoverbindung*



Fraunhofer FOKUS Fraunhofer SIT OTH Ostbayerische Technische Hochschule Regensburg

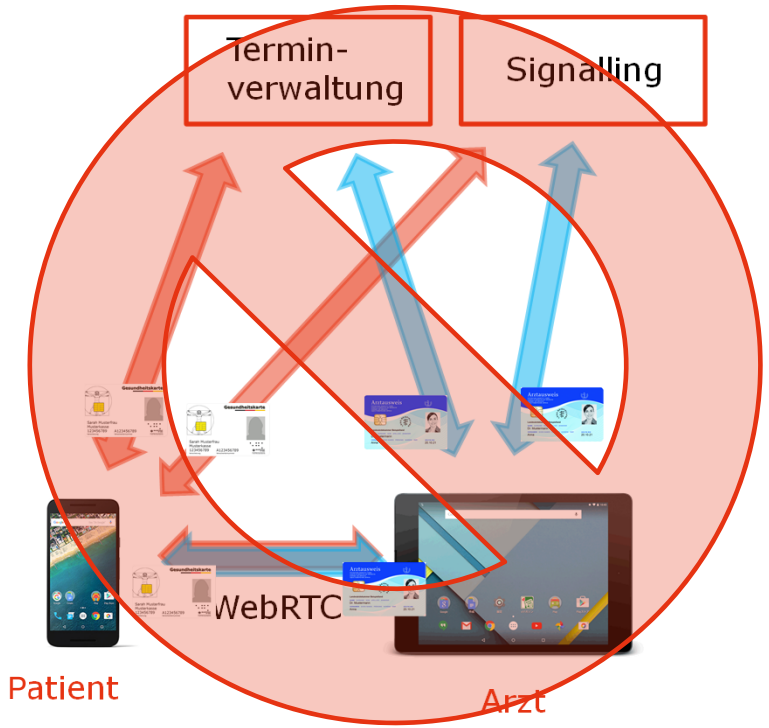
KOMMUNIKATIONSBEZIEHUNGEN VIDEOKONFERENZ

Konzeption Videosprechstunde

Terminverwaltung – *Zuordnung Termin + Teilnehmer*

Signalling – *Gesprächsvermittlung: Austausch von WebRTC-Verbindungsparametern*

WebRTC – *Peer-2-Peer-Audio-/Videoverbindung*



Fraunhofer FOKUS
Fraunhofer SIT
OTH Ostbayerische Technische Hochschule Regensburg

KOMMUNIKATIONSBEZIEHUNGEN VIDEOKONFERENZ

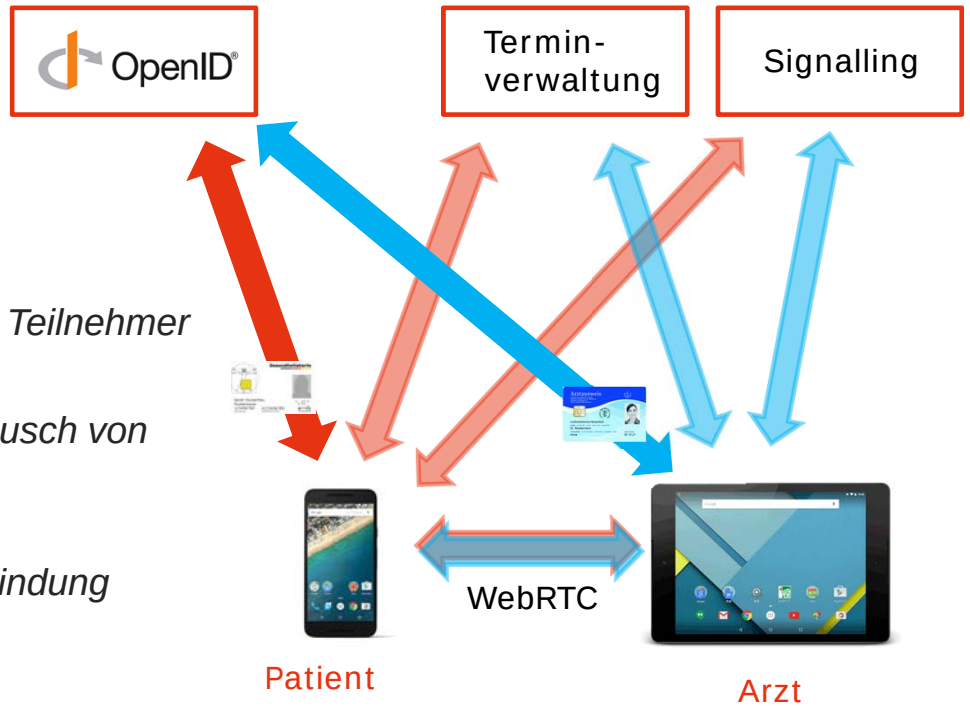
Konzeption Videosprechstunde

OpenID – *Authentifizierungsdienst: Ausstellen von Token*

Terminverwaltung – *Zuordnung Termin + Teilnehmer*

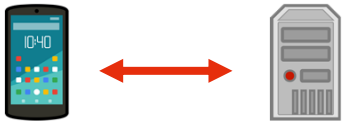
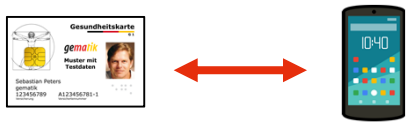
Signalling – *Gesprächsvermittlung: Austausch von WebRTC-Verbindungsparametern*

WebRTC – *Peer-2-Peer-Audio-/Videoverbindung*



GRUNDÜBERLEGUNGEN

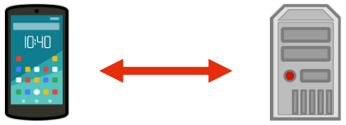
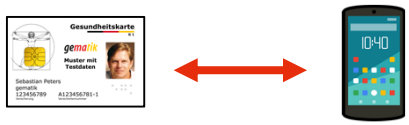
Direkte Kartennutzung vs. Ableiten von Sicherheitsmerkmalen

Vertrauensbasis	Token von Identity-Provider 	Signatur durch Karte 
Vorteil	**Komfort:** eGK wird nur zu Beginn einer Sitzung benötigt	**Sicherheit:** Signaturerstellung erfolgt immer direkt auf eGK
Nachteil	**Sicherheit:** App-Sitzung hat Sicherheitsbedarf (z. B. durch Sperrbildschirm)	**Komfort:** Karte muss während jeder Signaturoperation an das Smartphone gehalten werden (inkl. PIN-Eingabe)

Fraunhofer FOKUS Fraunhofer SIT OTH Ostbayerische Technische Hochschule Regensburg

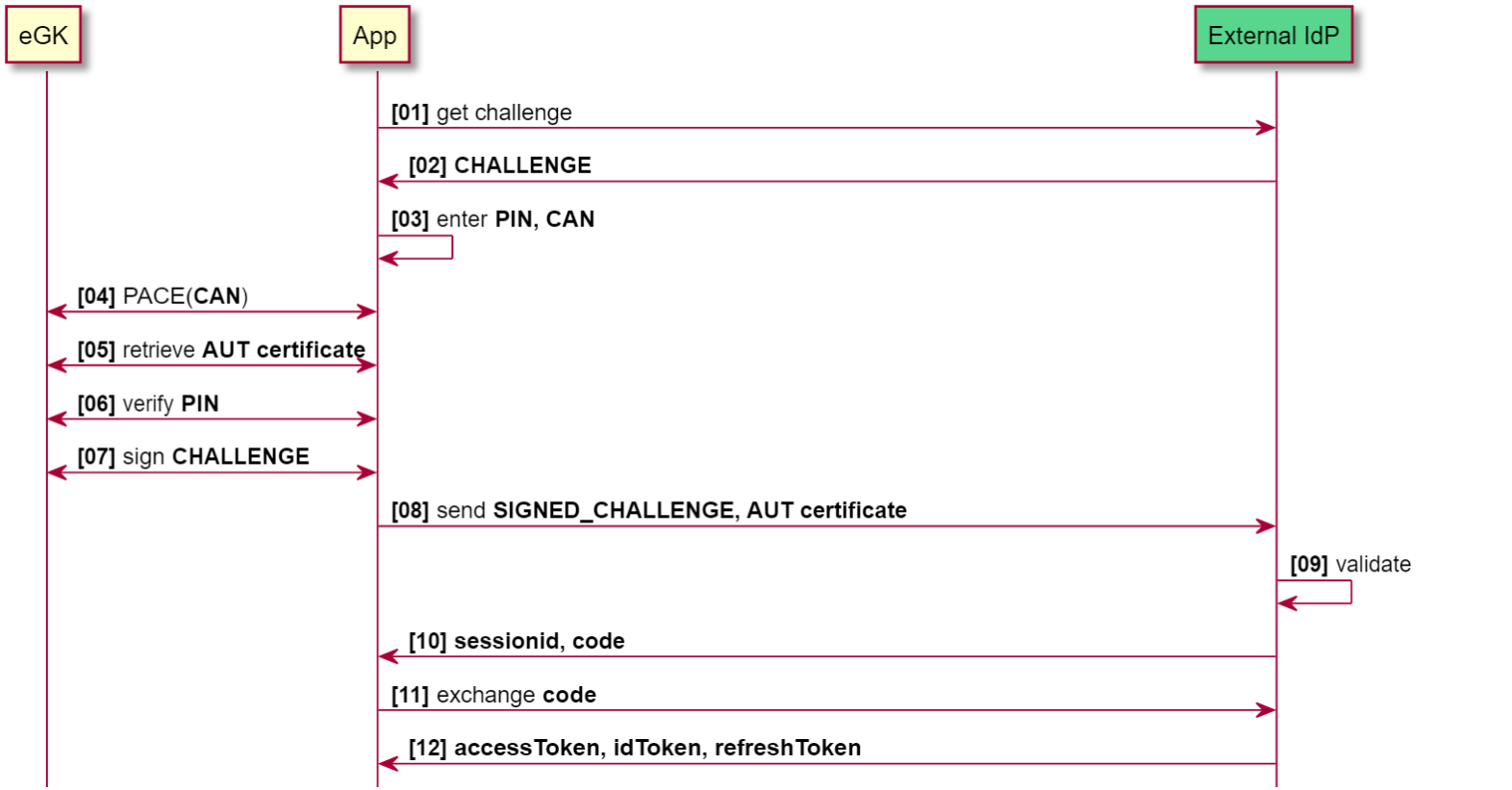
GRUNDÜBERLEGUNGEN

Direkte Kartennutzung vs. Ableiten von Sicherheitsmerkmalen

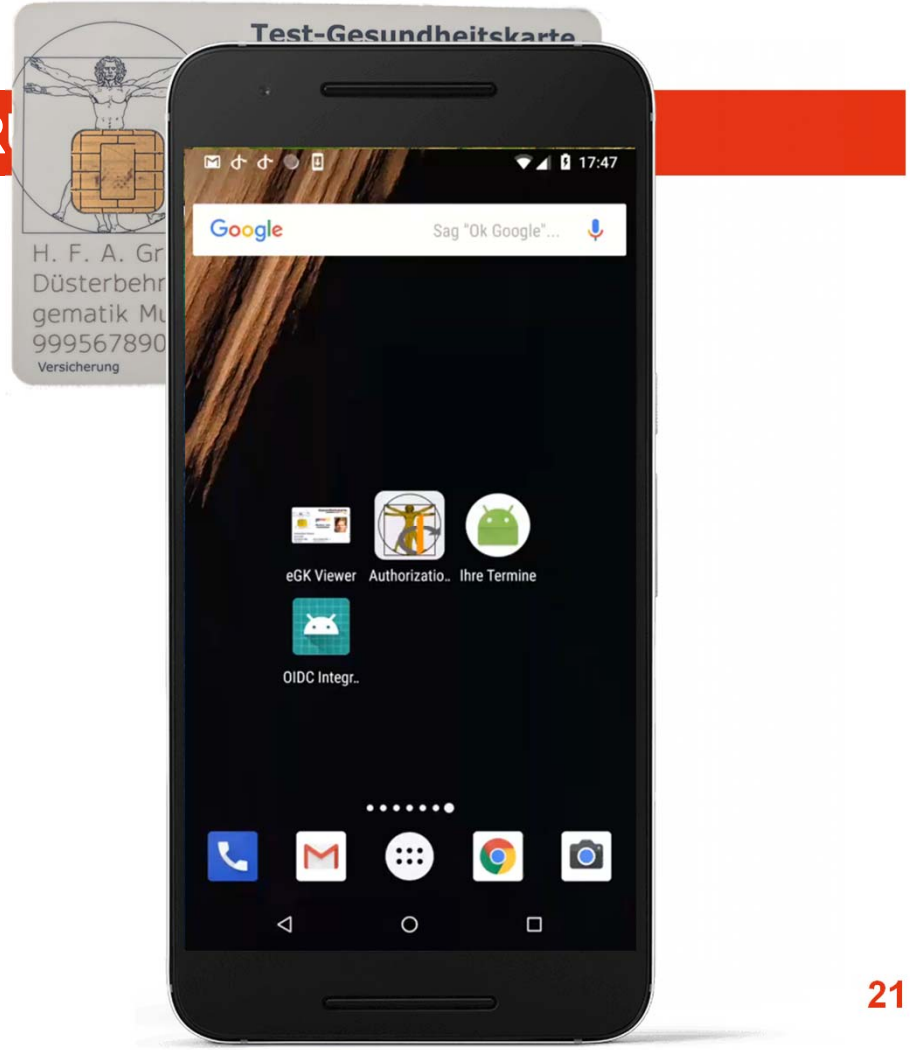
Vertrauensbasis	Token von Identity-Provider 	Signatur durch Karte 
Vorteil	**Komfort:** eGK wird nur zu Beginn einer Sitzung benötigt	**Sicherheit:** Signaturerstellung erfolgt immer direkt auf eGK
Nachteil	**Sicherheit:** App-Sitzung hat Sicherheitsbedarf (z. B. durch Sperrbildschirm)	**Komfort:** Karte muss während jeder Signaturoperation an das Smartphone gehalten werden (inkl. PIN-Eingabe)

Fraunhofer FOKUS Fraunhofer SIT OTH Ostbayerische Technische Hochschule Regensburg

VEREINFACHTER AUTHENTICATION FLOW



EGK BASIERTE AUTHENTISIERU

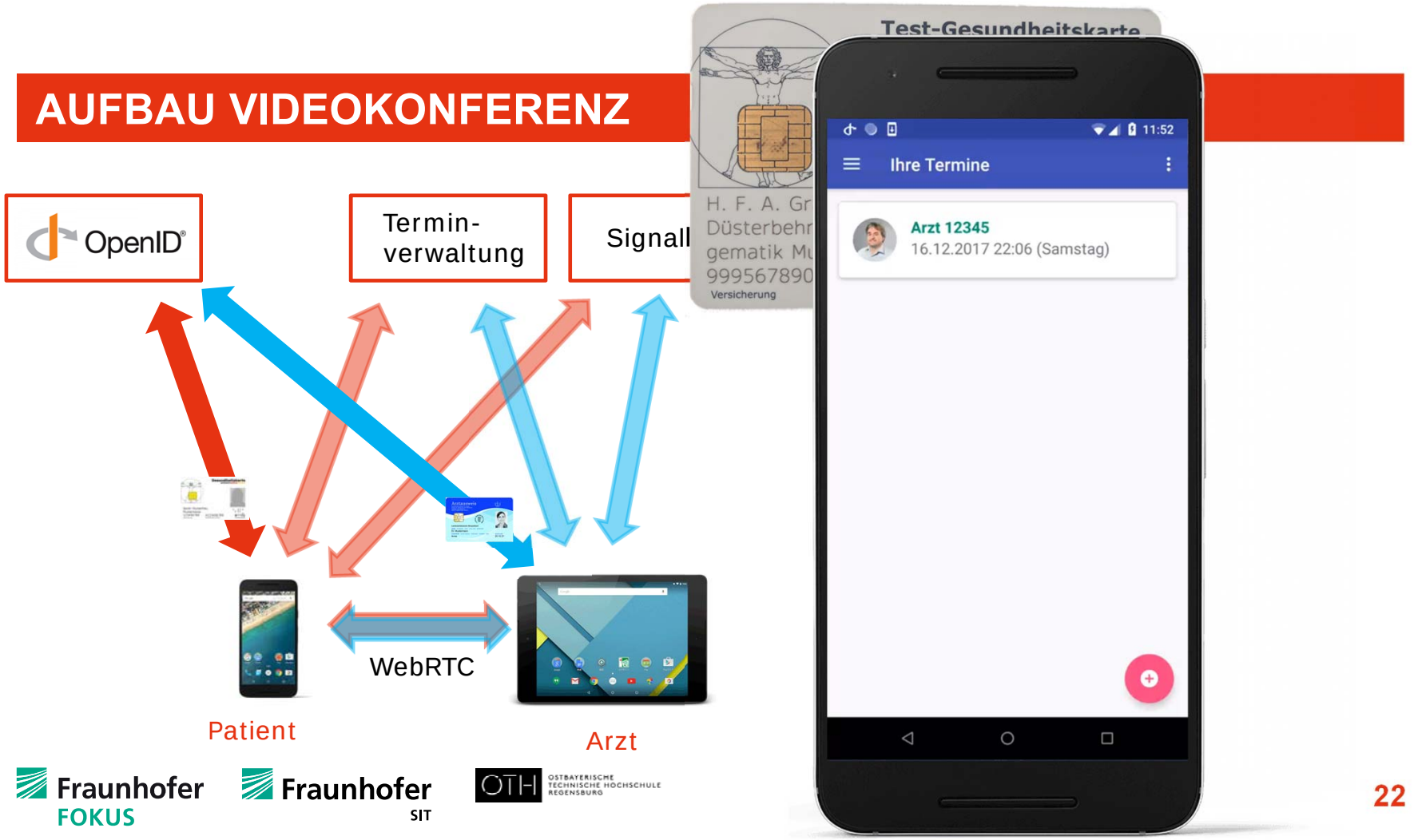


Fraunhofer FOKUS

Fraunhofer SIT

OTH Ostbayerische Technische Hochschule Regensburg

AUFBAU VIDEOKONFERENZ



Fraunhofer FOKUS

Fraunhofer SIT

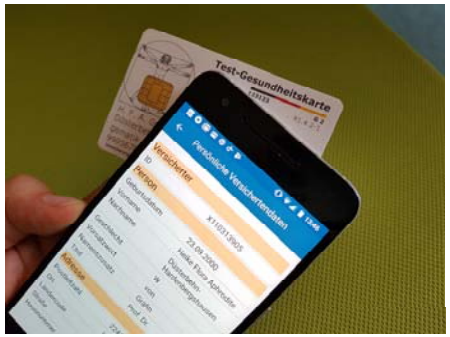
OTH Ostbayerische Technische Hochschule Regensburg

AKTUELLER STAND DER ARBEITEN

Vorarbeiten der gematik

- Sehr gute **Tools und Bibliotheken** für die Nutzung der eGK auf der Android Plattform **wurden durch die gematik bereitgestellt**:
  - Kartenzugriffsschicht
  - Authentifizierungsfunktionen auf Basis von OpenID Connect

- Die **Nutzung und Weiterentwicklung** ist im Rahmen des Projektes vorgesehen
  - Unterstützung weiterer Endgeräte
  - Unterstützung von Karten anderer Hersteller
  - Unterstützung EC-basierter Crypto-Verfahren
  - Sicherheitsbetrachtung



Fraunhofer FOKUS Fraunhofer SIT OTH Ostbayerische Technische Hochschule Regensburg

HERAUSFORDERUNGEN

Organisatorische Rahmenbedingungen

Verfügbarkeit / Herausgabe von NFC-fähigen Smartcards

- Schnittstellen sind spezifiziert und durch die Kartenhersteller weitestgehend umgesetzt
- Die Kassen geben entsprechende Karten derzeit nicht heraus

Herausgabe von PINs

- Keine der Kassen verteilt bisher PINs an ihre Versicherten

Verfügbarkeit von Sicherheitsdiensten

- OCSP-Responder zur Prüfung der Authentifizierungszertifikate sind nur bei einzelnen Kassen über das Internet erreichbar

Fraunhofer FOKUS Fraunhofer SIT OTH Ostbayerische Technische Hochschule Regensburg

HERAUSFORDERUNGEN

Technische Rahmenbedingungen

Unterstützung verschiedener Betriebssysteme

- Zwei vorherrschende Plattformen (Android + iOS)
- iOS Unterstützung bisher nicht durch native APIs des Betriebssystems realisierbar

Verfügbarkeit NFC-fähiger Endgeräte

- Nicht alle Endgeräte sind mit einem NFC-Chip ausgestattet

FRAGEN UND DISKUSSION

Fraunhofer FOKUS

Fraunhofer SIT

OTH Ostbayerische Technische Hochschule Regensburg

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Name	Organisation	Kontaktdaten
Olaf Rode	Fraunhofer FOKUS	030 34637626 030 34637626 olaf.rode@fokus.fraunhofer.de
Georgios Raptis	Ostbayerische Technische Hochschule Regensburg	0177 6910807 0941 9439699 georgios.raptis@oth-regensburg.de
Dominik Spychalski	Fraunhofer SIT	06151 869249 06151 869224 dominik.spychalski@sit.fraunhofer.de

Fraunhofer FOKUS Fraunhofer SIT OTH Ostbayerische Technische Hochschule Regensburg

BACKUP

PACE

Password Authenticated Key Exchange

1. The chip randomly chooses a random number, encrypts it with a password-derived key and sends the encrypted random number to the terminal, where it is recovered.
2. Both the chip and the terminal use a mapping function to map the random number to parameters for asymmetric cryptography.
3. The chip and the terminal perform a DiffieHellman protocol based on the parameters generated during step 2.
4. The chip and terminal derive session keys, which are confirmed by exchanging and checking the authentication tokens.