Fraunhofer FOKUS
Competence Center E-HEALTH

Abschlussbericht

Abschlussbericht zum Projekt „MOVI“

Konzeption und prototypische Realisierung einer mobilen Versichertenidentität (MOVI)

Fraunhofer-Institut für Offene Kommunikationssysteme
Kaiserin-Augusta-Allee 31
10589 Berlin

olaf.rode@fokus.fraunhofer.de
Fraunhofer-Institut FOKUS

Inhalt

1 Titel und Verantwortliche

Titel des Vorhabens	Konzeption und prototypische Realisierung einer mobilen Versichertenidentität (MOVI)
Förderkennzeichen	ZMVI 1 2519 FSB 010
Projektleitung	Olaf Rode
Projektmitarbeitende	**MitarbeiterInnen Fraunhofer FOKUS:** Olaf Rode (Projektleitung, Konzeption, Entwicklung), Benny Häusler (Konzeption, Entwicklung), Aleksei Piatkin (Entwicklung), Emil Milanov (Entwicklung), Mike Brandtner (Entwicklung) Darya Martyniuk (Entwicklung) **MitarbeiterInnen Fraunhofer SIT:** Dominik Spychalski (Sicherheitsanalyse), Leon Würsching (Sicherheitsanalyse) **MitarbeiterInnen OTH Regensburg:** Georgios Raptis (Organisation/Konzeption, Durchführung Evaluation), Markus Ritthaler (Marktrecherche, Analyse)
Kontaktdaten Projektleiter	Olaf Rode Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS Kaiserin-Augusta-Allee 31 10589 Berlin e-Mail: olaf.rode@fokus.fraunhofer.de Telefon: 030 34637626
Laufzeit	06/2019 – 12/2020
Fördersumme	220.373,90 €

2 Inhaltsverzeichnis

3 Zusammenfassung

Im Rahmen des Projektes wurden die Sicherheitsmechanismen der führenden Mobilplattformen Android und iOS dahingehend analysiert, ob sich mit ihnen eine „virtuelle elektronische Gesundheitskarte“ (d.h. eine Smartphone-basierte Digitale Identität) sicher realisieren lässt.

Basierend auf den Ergebnissen dieser Analysen und einer Marktanalyse wurden Prämissen für die Ausgestaltung der virtuellen eGK definiert und mit dem BMG abgestimmt. Diese Prämissen bildeten die Grundlage für die Konzeption und prototypischen Umsetzung einer Lösung für die Android-Plattform; die grundsätzliche Machbarkeit für iOS wurde theoretisch konzipiert und aufgezeigt.

Die Nutzbarkeit der umgesetzten Lösung wurde anhand von zwei Anwendungsszenarien untersucht: Video-Conferencing und Secure Messaging. Es konnte gezeigt werden, dass die virtuelle eGK in beiden Szenarien als Sicherheitsmechanismus im Kontext der Authentisierung genutzt werden kann. Im Rahmen einer Sicherheitsanalyse konnte ebenfalls gezeigt werden, dass die entwickelte Lösung prinzipiell ein „substanzielles“ Sicherheitsniveau gemäß eIDAS aufweist. Die Erprobung der Lösung mit projektexternen Dritten musste aufgrund der Corona-Pandemie leider entfallen.

Prinzipiell wäre die entwickelte Lösung im Zusammenspiel mit den vorgesehenen Sicherheitsdiensten der Telematikinfrastruktur geeignet, um im beschriebenen Anwendungsbereich perspektivisch eine wichtige Rolle als mobile Authentisierungslösung zu spielen. Notwendige Anpassungen von TI-Diensten im Kontext einer Einführungsplanung wurden identifiziert und konzipiert.

Die im Rahmen des Projektes erarbeiteten Ergebnisse und entwickelten Apps und Dienste stehen unter http://movi.fokus.fraunhofer.de zur freien Nutzung zur Verfügung.

4 Einleitung

Während mobile Gesundheitsanwendungen mit Stichworten wie „Convenience“ und „User Experience“ punkten, hat die Telematikinfrastruktur bislang vorrangig auf das Thema „Datenschutz“ gesetzt. Bisherige Konzepte (z. B. für die elektronische Patientenakte) sehen keine praktikable Schnittstelle der Anwendungen der elektronischen Gesundheitskarte für die Versicherten vor.

Das vom BMG aufgesetzte AsK-Projekt griff diese Problematik erstmalig konsequent auf und zeigte, wie eine NFC-fähige eGK mit mobilen Endgeräten (Smartphones und Tablets mit NFC-Schnittstelle) zusammenarbeiten kann. Der Ansatz ging jedoch davon aus, dass für jeden Anwendungsfall die physische eGK (inkl. PIN-Eingabe) genutzt werden muss. Außerdem war eine direkte Integration zu Apps für TI-Anwendungen, wie die ePA, nicht möglich.

Im MOVI-Projekt sollte untersucht werden, ob bzw. wie eine Delegation der elektronischen Identität der eGK an eine „virtuelle eGK“ eines mobilen Geräts – also eine „Digitale Identität“ – erfolgen kann, um weiterhin bestehende Probleme (z.B. fehlende NFC-Unterstützung bei „einfachen“ Android-Geräten + Einschränkungen bezüglich der Usability und Akzeptanz bei zu häufiger PIN-Eingabe) zu adressieren. Von besonderem Interesse sind hierbei die folgenden Themen:

- Analyse grundlegender Sicherheitskonzepte und -aspekte für die Android-Plattform
- Vergleich von Mechanismen zur Gewährleistung der Geräteintegrität für Android und iOS
- Analyse der Entsperrmechanismen von Mobilgeräten auf der Basis von Wissen, Biometrie und Besitz
- Vergleich der Mechanismen zur Absicherung des Zugriffs auf kryptografische Schlüssel zwischen Android und iOS
- Möglichkeiten einer iOS-Umsetzung (ohne diese prototypisch zu realisieren)

Das Projekt wurde durch Fraunhofer FOKUS, Fraunhofer SIT und die OTH Regensburg durchgeführt und gliederte sich in die folgenden Arbeitsbereiche:

- AP1 - Dissemination und Vernetzung (Lead: OTH Regensburg)
- AP2 – Problem- und Umfeldanalyse (Lead: Fraunhofer FOKUS)
- AP3 – Konzeption und Spezifikation (Lead: Fraunhofer FOKUS)
- AP4 – Prototypische Umsetzung und Erprobung (Lead: Fraunhofer FOKUS)
- AP5 – Einführungsplanung (Lead: OTH Regensburg)
- AP6 – Sicherheitsanalyse (Lead: Fraunhofer SIT)
- AP7 – Projektmanagement (Lead: Fraunhofer FOKUS)

5 Methodik

Die folgenden Ziele wurden im Projektantrag formuliert:

1. Definition von Struktur und Inhalt einer virtuellen eGK auf Grundlage zu erwartender Anwendungsfälle
2. Definition von relevanten Mindestanforderungen an mobile Endgeräte mit Blick auf die genutzte Soft- und Hardware
3. Darstellen der grundsätzlichen Abbildbarkeit einer „virtuellen eGK“ auf aktuellen mobilen Endgeräten mit Android und iOS als Betriebssystem
4. Nachweis der Umsetzbarkeit einer „virtuellen eGK“ anhand einer prototypischen Implementierung für die Android-Plattform
5. Bewertung der Nutzbarkeit, Praktikabilität und Sicherheit einer „virtuellen eGK“ im Kontext zweier Anwendungsszenarien

Die folgenden Abschnitte beschreiben für jedes dieser Ziele, ob und wie es erreicht werden konnte sowie welche Indikatoren bzw. Methoden zur Bestimmung der Zielerreichung herangezogen wurden.

Definition von Struktur und Inhalt einer virtuellen eGK auf Grundlage zu erwartender Anwendungsfälle

Basierend auf den definierten und mit dem BMG abgestimmten Prämissen wurde die virtuelle eGK vornehmlich als Authentifizierungslösung konzipiert, die das verwendete Schlüsselmaterial über die vom Betriebssystem und dem jeweiligen Endgerät angebotenen Sicherheitsmechanismen schützt. Entsprechende Konzepte mit detaillierten technischen Festlegungen wurden erarbeitet und im Rahmen der prototypischen Realisierung umgesetzt.

Definition von relevanten Mindestanforderungen an mobile Endgeräte mit Blick auf die genutzte Soft- und Hardware

Relevante Mindestanforderungen wurden im Rahmen des Projektes identifiziert und innerhalb der entwickelten Konzepte berücksichtigt.

Darstellen der grundsätzlichen Abbildbarkeit einer „virtuellen eGK“ auf aktuellen mobilen Endgeräten mit Android und iOS als Betriebssystem

Im Rahmen einer Sicherheitsanalyse wurde die konzipierte Lösung detailliert analysiert und bewertet. Betrachtete Anforderungen betrafen u.a. folgende Aspekte: kryptografische Algorithmen, Erzeugung und Speicherung von Schlüsselmaterial und weiteren kryptografischen Artefakten sowie mögliche Registrierungsprozesse. Die entwickelte Lösung wurde darüber hinaus bzgl. der eIDAS-Vorgaben bewertet. Grundlage der Diskussion und Einschätzung war die Durchführungsverordnung der Europäischen Kommission (EU) 2015/1502 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel.

Nachweis der Umsetzbarkeit einer „virtuellen eGK“ anhand einer prototypischen Implementierung für die Android-Plattform

Im Rahmen des Projektes ist es gelungen, die für die Android-Plattform entwickelten Konzepte prototypisch umzusetzen. Basis der Umsetzung war hierbei die Android Account API im Zusammenspiel mit diversen Backend-Diensten. Anhand von zwei exemplarischen Anwendungen (Video Conferencing + Secure Messaging), die auf diese Lösung zurückgriffen, konnte gezeigt werden, dass der Ansatz grundsätzlich realisierbar ist und anwendungsübergreifend Verwendung finden kann.

Bewertung der Nutzbarkeit, Praktikabilität und Sicherheit einer „virtuellen eGK“ im Kontext zweier Anwendungsszenarien

Aufgrund der zu Beginn 2020 einsetzenden Corona-Pandemie konnte – anders als von der Projektplanung vorgesehen – keine Erprobung und Bewertung der Lösung durch Projekt-externe Akteure durchgeführt werden.

6 Durchführung, Arbeits- und Zeitplan

Die im Projekt geleistete Arbeit orientierte sich zu Beginn der Laufzeit noch sehr dicht am Projektplan. Durch die einsetzende Corona-Pandemie ergaben sich 2020 jedoch größere Abweichungen von der ursprünglichen Planung, da die geplante Evaluation trotz einer Projektverlängerung nicht wie vorgesehen durchgeführt werden konnte.

Die folgenden Abschnitte geben einen Überblick über die in den einzelnen inhaltlich orientierten Arbeitspaketen geleisteten Arbeiten, die erreichten Zielen und etwaige Abweichungen zur Planung.

6.1 Problem- und Umfeldanalyse (AP2)

Der Fokus der Arbeiten im entsprechenden Arbeitspaket lag – entsprechend der Arbeitsplanung – sehr stark auf der Beantwortung und Adressierung der im folgenden dargestellten Fragestellungen bzw. Aspekte:

Lebenszyklusmanagement für Schlüsselmaterial, Unterstützte kryptografische Verfahren + Sichere Speicherung von privatem Schlüsselmaterial, Marktanalyse, Übersicht über übliche Key-Enrollment und Registration-Verfahren

Im Rahmen der Arbeiten wurde eine detaillierte Analyse der Sicherheitsfeatures der Android-Plattform durchgeführt (https://movi.fokus.fraunhofer.de/androidSecurityFeatures/) und geprüft mit welchen Attestation-Mechanismen die perspektivische Umsetzung einer virtuellen eGK (vgl. https://movi.fokus.fraunhofer.de/MobileDeviceAttestationSecurity/) unterstützt werden könnte.

Im Rahmen des Projektes wurde ferner eine App entwickelt, mit welcher es möglich ist, die in einem Android-Smartphone realisierten Hard- und Software-Sicherheits-Features zu erfassen. Dies bildete die Grundlage für die Bewertung praktikabler Lösungsansätze, die sich auf einer Vielzahl von Android-Geräten umsetzen ließen.

Lebenszyklusmanagement der „virtuellen eGK“

Relevante Prozesse im Lifecycle einer virtuellen Gesundheitskarte (vgl. https://movi.fokus.fraunhofer.de/anwendungsfaelle/) wurden identifiziert und bildeten die Grundlage der Arbeiten in AP3.

Die Ergebnisse der Problem- und Umfeldanalyse mündeten in einer Reihe von gemeinsam mit dem BMG abgestimmten Prämissen, die die Grundlage für die weitere Projektarbeit bilden sollten:

1. Die virtuelle eGK soll mit bereits heute verfügbaren Mobiltechnologien realisiert werden können
2. Die virtuelle eGK soll die physische eGK in einem ersten Schritt nicht vollständig ersetzen
3. Bestimmte Anwendungen der physischen eGK (z.B. VSDM) sollten nicht auf die mobilen Endgeräte der Versicherten migriert werden
4. Die virtuelle eGK repräsentiert die Identität der Versicherten in der virtuellen Welt.

Die Ergebnisse wurden – wie vom Arbeitsplan vorgesehen – auf der Projektwebseite detailliert dargestellt (https://movi.fokus.fraunhofer.de/ergebnisse/ → Bereich: Grundlagen und Analysen).

6.2 Konzeption und Spezifikation (AP3)

Im Rahmen der Konzeption und Spezifikation sollten entsprechend des Arbeitsplans primär Festlegungen zu folgenden inhaltlichen Aspekten getroffen werden: logischer Aufbau einer virtuellen eGK, übergreifende Systemarchitektur, Standards und Protokolle, virtuelle eGK für die Android Plattform, virtuelle eGK für die iOS Plattform, Lebenszyklusmanagement und Anwendungen auf Grundlage der virtuellen eGK.

Wesentliche Ergebnisse des Arbeitsbereiches umfassten:

- eine Übersicht und detaillierte Ausarbeitung der relevanten Anwendungsfälle, Konzepte und Abläufe entlang des Lebenszyklus einer virtuellen Gesundheitskarte, welche die Basis für die Realisierung bilden (https://movi.fokus.fraunhofer.de/ergebnisse/ - Bereich: Anwendungsfälle, Konzepte und Abläufe),
- eine technische Lösungsarchitektur, die die Grundlage für die Umsetzung und Verwendung der virtuellen eGK bildet (https://movi.fokus.fraunhofer.de/architektur/),
- sowie eine technische Lösungsarchitektur für die Anwendungsfälle Videoconferencing und Secure Messaging (https://movi.fokus.fraunhofer.de/signal/)

Die erarbeiteten Ergebnisse decken sich weitgehend mit der ursprünglichen Planung des Antrags. Lediglich die Konzeption einer virtuellen eGK für die iOS-Plattform konnte nicht – wie ursprünglich geplant – vollständig ausgearbeitet werden. Die Arbeiten in diesem Umfeld konzentrierten sich primär auf Analysen und Sicherheitsbewertungen der von der Plattform angebotenen Sicherheitsfeatures (vgl. AP2 + AP5). Die technischen Möglichkeiten der Implementierung wurden analysiert und Lösungswege theoretisch ausgezeigt, jedoch – im Einklang zu den abgestimmten Projektzielen, s. Kap. 6.4, Einführungsplanung – diese nicht in der Praxis nachgewiesen.

6.3 Prototypische Umsetzung und Erprobung (AP4)

Aufbauend auf den Ergebnissen des AsK-Projektes (https://ask.fokus.fraunhofer.de/) war es möglich, eine generisch nutzbare Android-App zu entwickeln, die im Zusammenspiel mit für das Projekt entwickelten und angepassten Backend-Diensten die Aufgabe einer virtuellen Gesundheitskarte übernimmt. Innerhalb der App (und im Zusammenspiel mit den relevanten Backend-Diensten) wurden die als relevant identifizierten Lifecycle-Management-Prozesse der virtuellen eGK umgesetzt. Im Detail wurden die folgenden Ergebnisse erarbeitet:

- detaillierte Beschreibung der prototypisch umgesetzten Architektur zur Abbildung der Anwendungsfälle (https://movi.fokus.fraunhofer.de/architektur/)
- Bereitstellung des Quelltextes in mehreren git-Repositories (Bereitstellung auf Anfrage)

Um die Anwendbarkeit der virtuellen eGK zu demonstrieren, wurden die fachlichen Anwendungsfälle Video-Conferencing und Secure-Messaging umgesetzt. Hierzu wurde auf Vorarbeiten aus anderen Projekten (z.B. AsK) sowie existierende Open Source Lösungen (Signal) zurückgegriffen und diese jeweils dahingehend angepasst, dass sie die virtuelle eGK als Authentifizierungsmechanismus integrieren.

Einen Eindruck der umgesetzten Funktionalität bieten die auf der Webseite bereitgestellten Demovideos (https://movi.fokus.fraunhofer.de/demo/). Auch hier kann der Quelltext auf Anfrage bereitgestellt werden.

Wichtig: Eine Erprobung/Evaluation mit projektexternen Dritten war aufgrund der Anfang 2020 einsetzenden Corona-Pandemie leider NICHT mehr möglich. In Abstimmung mit dem BMG wurden die im Projekt freiwerdenden Ressourcen für weitergehende Analysen im Bereich der Einführungsplanung (insb. iOS) verwendet.

6.4 Einführungsplanung (AP5)

Als Grundlage der Einführungsplanung wurde zunächst eine Marktanalyse (vgl. AP2) durchgeführt, um die Verbreitung geeigneter Endgeräte zu ermitteln. Da die Implementierung der Digitalen Identität nur für Android-Geräten als Projektziel ausgewiesen war und auch durchgeführt wurde, wurden zusätzlich technische Möglichkeiten auf theoretischer Ebene für eine Einführung auch für iOS-basierten Geräten eruiert; ein Weg einer Einführung konnte aufgezeigt werden.

Backend-seitig erfolgte eine Analyse von Diensten der Telematik-Infrastruktur, welche für einen Betrieb mit den Digitalen Identitäten angepasst werden mussten. Der Signaturdienst wurde als anzupassender Dienst identifiziert; die erforderlichen konzeptionellen Anpassungen wurden analysiert und in einem Dokument festgehalten, welches auch Aussagen zur Sicherheit des Verfahrens beinhaltet. Dazu wurde noch eine technische Konzeption für die Kommunikation des Frontends des Versicherten (unter der Prämisse von Digitalen Identitäten), dem Authenticator (als Ergebnis des Projektes) und des Identity Providers der Gematik erstellt.

Alle entsprechenden Erfordernisse bzgl. Anpassungen von Diensten der Telematik-Infrastruktur wurden mit der Gematik diskutiert. Letztendlich wurde die Integrationsfähigkeit der Digitalen Identität in der Telematik-Infrastruktur für alle relevanten mobilen Plattformen nachgewiesen.

6.5 Sicherheitsanalyse (AP6)

Die Arbeiten in diesem Bereich orientierten sich eng an der ursprünglichen Planung. Folgende Ergebnisse wurden erarbeitet:

- Durchführen von Analyse zu den Sicherheitsmerkmalen der beiden Mobilplattformen Android und iOS sowie sich aktuell etablierender Standards
- Definition von Sicherheitsanforderungen
- Detaillierte Sicherheitsanalyse der erarbeiteten Konzepte
- Diskussion des Sicherheitsniveau der erarbeiten Lösung nach eIDAS

Die Arbeiten am Sicherheitskonzept wurden eng mit der Konzeption und Umsetzung verzahnt. Für die Sicherheit relevante Feststellungen wurden unverzüglich in die entsprechenden Arbeitspakete zurückgespielt und dort berücksichtigt.

6.6 Zusammenfassung: Umsetzung des Arbeitsplans

Ein Großteil der im Projektplan des Antrags definierten Arbeiten wurden umgesetzt, wobei der Fokus in einzelnen Arbeitspaketen sehr stark auf technischen Fragestellungen lag:

- Arbeitspaket 1 - Dissemination und Vernetzung: Die im Rahmen des Projektes erarbeiteten Ergebnisse wurde in einer Reihe von Workshops und Vorträgen vorgestellt und mit allen relevanten Stakeholdern diskutiert (vgl. Abschnitt 11). Für die wissenschaftliche Fachöffentlichkeit wurden die Ergebnisse des Projektes in einer wissenschaftlichen Konferenz veröffentlicht.

- Arbeitspaket 2 – Problem- und Umfeldanalyse: Die Ergebnisse dieses Arbeitspaketes lieferten einen guten Überblick über den Status Quo und mündeten in der Formulierung von Umsetzungsprämissen, welche die Basis der Konzeption bildeten.
- Arbeitspaket 3 – Konzeption und Spezifikation: Die in der ursprünglichen Planung vorgesehenen Ergebnisse wurden erzielt. Es ist gelungen die für die Umsetzung einer virtuellen Gesundheitskarte erforderlichen Komponenten und Abläufe detailliert zu beschreiben.
- Arbeitspaket 4 – Prototypische Umsetzung und Erprobung: Die prototypische Umsetzung konnte nachweisen, dass eine virtuelle Gesundheitskarte gemäß der entwickelten Konzepte grundsätzlich realisierbar ist. Anhand der Integration in die Anwendungsszenarien Video-Conferencing und Secure-Messaging konnte dies auch praktisch belegt werden.
- Arbeitspaket 5 – Einführungsplanung: Im Rahmen der Einführungsplanung konnte gezeigt werden, dass ein Zusammenspiel der Lösung mit den Diensten der Telematikinfrastrukt grundsätzlich möglich ist; auch eine grundsätzliche technische Machbarkeit auf iOS-Basis (als zusätzliches Projektziel aufgrund der Pandemie bedingten ausgefallenen externen Evaluation) wurde aufgezeigt.
- Arbeitspaket 6 – Sicherheitsanalyse: Die Arbeiten zur Sicherheitsanalyse folgten weitgehend der ursprünglichen Planung. Durch leichte Verschiebungen in der Schwerpunktsetzung konnten zum Teil detailliertere Analysen der beiden Plattformen durchgeführt werden, als zunächst angenommen. Es konnte gezeigt werden, dass die konzipierte Lösung grundsätzlich ein „substanzielles“ Sicherheitsniveau gemäß eIDAS realisieren kann.

Eine größere Abweichung vom ursprünglichen Projektplan ergab sich in Bezug auf die nicht erfolgte Erprobung der Lösung (vgl. AP4) aufgrund der Corona-Pandemie, welche in Abstimmung mit dem BMG durch eine Analyse der Machbarkeit unter iOS (s. AP5) ausgeglichen wurde.

7 Ergebnisse

Im Projekt wurden die folgenden Ergebnisse erzielt:

- Beschreibung grundlegender Sicherheitskonzepte und -aspekte für die Android-Plattform
- Vergleich von Mechanismen zur Gewährleistung der Geräteintegrität für Android und iOS
- Analyse der Entsperrmechanismen von Mobilgeräten auf der Basis von Wissen, Biometrie und Besitz
- Vergleich der Mechanismen zur Absicherung des Zugriffs auf kryptografische Schlüssel zwischen Android und iOS
- Authentifizierung durch Besitz mit FIDO2
- Diskussion des MOVI-Konzeptes anhand des Sicherheitsniveaus nach eIDAS
- Übersicht, Bewertung und Analyse der im Projekt eingesetzten sowie entwickelten Mechanismen und Komponenten mit Verweisen auf die o.g. Konzepte.
- Untersuchen verschiedener Endgeräte auf Kompatibilität (Marktanalyse)
- Detaillierte Beschreibung der logischen und technischen Gesamtarchitektur der Lösung
- Beschreibung der für die prototypische Realisierung genutzten Client- und Serverkomponenten
- Anpassung einer Anwendung für die Videosprechstunde (Integration mit virtueller eGK)
- Anpassung einer Anwendung für sicheres Messaging (Integration mit virtueller eGK)
- Erstellung einer Webseite mit Informationsmaterial zu den Projektinhalten- und Ergebnissen
- Veröffentlichen des Quelltexts der entwickelten Komponenten unter einer Open Source Lizenz (inkl. umfassende Dokumentation)

8 Diskussion der Ergebnisse, Gesamtbeurteilung

Die wesentlichen Projektziele konnten innerhalb der einzelnen Arbeitspakete erreicht werden. Im Rahmen der Problem- und Umfeldanalyse wurde eine detaillierte Analyse der durch die aktuellen Versionen der Mobilplattformen Android und iOS unterstützten Sicherheitsfeatures durchgeführt. Dabei konnte gezeigt werden, dass insbesondere die Attestierungsfunktionen im Bereich der Schlüsselgenerierung und -verwendungen einen wesentlichen Baustein für die Realisierung einer virtuellen eGK (Smartphone-basierte Digitale Identität) bilden können. Aber auch die Grenzen des Systems sind deutlich geworden, so dass im Ergebnis über die Formulierung von Prämissen ein Nutzungsrahmen für den zukünftigen Einsatz einer virtuellen eGK abgesteckt werden konnte.

Basierend auf diesen Prämissen wurde ein Konzept entwickelt, wie eine virtuelle elektronische Gesundheitskarte entlang ihres Lebenszyklus, d.h. von der Registrierung über ihre Nutzung bis hin zur De-Registrierung auf der Android-Plattform umgesetzt werden kann. Im Mittelpunkt der Lösung stehen dabei sogenannte Key Attestation Zertifikate, die eine verlässliche Bindung des über eine TEE oder ein HSM gesicherten Schlüsselmaterials an ein bestimmtes Endgerät ermöglichen.

Im Zuge einer prototypischen Umsetzung, welche sich entsprechender Attestation-Ansätze bediente, konnte unter Verwendung der Android Account API eine App entwickelt werden, welche im Zusammenspiel mit speziell angepassten Backend-Diensten, die Aufgabe einer virtuellen eGK erfüllt. Anhand von zwei ebenfalls prototypisch realisierten Anwendungsszenarien (Videokonsultation und Secure Messaging) konnte exemplarisch gezeigt werden, wie sich die virtuelle eGK als transparentes Authentifizierungsverfahren in andere Anwendungen einbetten lässt.

Im Rahmen der Sicherheitsanalyse konnte herausgearbeitet werden, dass die konzipierte Lösung grundsätzlich ein „substanzielles“ Vertrauensniveau gemäß eIDAS erreichen kann. Voraussetzung hierfür sind jedoch bestimmte Sicherheitseigenschaften des mobilen Endgerätes, welches mindestens über eine Trusted Execution Environment (TEE) verfügen muss. Die Marktanalyse hat gezeigt, dass dies für die meisten Geräte (Stand 2021, Tendenz steigend) flächendeckend zutrifft.

Im Zusammenhang mit der Sicherheitsanalyse wurde auch der Standard FIDO 2 untersucht, der perspektivisch eine Weiterentwicklung des erarbeiteten Konzeptes erlauben könnte. Die entsprechende Fragestellung sollte ggf. in einem Folgeprojekte nochmals gesondert untersucht werden.

Unglücklicherweise konnte aufgrund der beginnenden Corona-Pandemie die entwickelte Lösung innerhalb der Projektlaufzeit nicht mehr mit Projekt-externen Nutzern evaluiert werden. Hierdurch ergeben sich insbesondere Unsicherheiten in Bezug auf die Bewertung der tatsächlichen und wahrgenommen Usability der Lösung.

Zusammenfassend kann dennoch gesagt werden, dass das Projekt einen wichtigen Beitrag zur Diskussion im Umfeld der Realisierung einer „virtuellen eGK“ geleistet hat. Wir hoffen, dass die entwickelten Konzepte in die aktuellen und perspektivischen Arbeiten der gematik in diesem Bereich einfließen werden. Konkrete Anknüpfungspunkte hierfür wurden im Rahmen des Arbeitspakets „Einführungsplanung“ ebenfalls erarbeitet und entsprechend kommuniziert.

9 Gender Mainstreaming Aspekte

Ursprünglich war geplant, die verschiedenen Fragestellungen der Evaluation (vgl. AP4) auch dahingehend auszuwerten, ob sich größere Unterschiede in der Bewertung in Abhängigkeit des Geschlechtes der befragten Person ergeben. Durch die Corona-Pandemie war es jedoch leider nicht möglich eine Erprobung der Lösung durch projektexterne Dritte durchzuführen. Entsprechend liegen keine Erkenntnisse in diesem Umfeld vor.

10 Verbreitung und Öffentlichkeitsarbeit der Projektergebnisse

10.1 Workshops / Vorträge

05. Juli 2019 - Berlin: Kick-Off-Veranstaltung mit BMG

16. September 2019 - Darmstadt: Workshop zur Sicherheitsanalyse (Diskussion verschiedener Lösungsansätze und Abstimmung des weiteren Vorgehens)

30. September 2019 – Wien: Workshop mit RISE (Vorstellen des Projektes, Diskussion der Lösungsansätze, Ausloten von Kooperationsmöglichkeiten)

01. Oktober 2019 - Berlin: Workshop mit gematik (Vorstellen des Projektes, Diskussion der Lösungsansätze, Ausloten von Kooperationsmöglichkeiten)

25. Februar 2020 - Berlin: Workshop mit dem Vega-Projekt (Vorstellen des Projektes, Diskussion der Lösungsansätze, Ausloten von Kooperationsmöglichkeiten)

26. März 2021 - Berlin: Abschlusspräsentation (Vorstellen der Projektergebnisse)

10.2 Messen

Hinweis: Ursprünglich war die Präsentation der Ergebnisse auf der DMEA 2020 am Stand des Fraunhofer FOKUS geplant. Aufgrund der Pandemie ist diese Messe entfallen.

10.3 Abschlussarbeiten

Im Rahmen der Projektes sind mehrere Abschlussarbeiten entstanden:

- Piatkin (HTW Berlin) - Konzeption und prototypische Realisierung eines Secure Messaging Systems unter Nutzung von eGK und HBA
- M. Deglmann (OTH Regensburg) - Prototypische Implementierung einer mobilen Anwendung für das „Deutsche Elektronische Melde- und Informationssystem für den Infektionsschutz (DEMIS)“ auf Basis von Android und FHIR
- M. Ritthaler (OTH Regensburg) - Authentifizierungsprotokolle für die elektronische Patientenakte und die elektronische Verordnung in der Telematik-Infrastruktur: Analyse und Empfehlungen.
- M. Fathi (OTH Regensburg & TalTech/EST) - An authenticator App (iOS) for a virtual electronic health card implementing the openID connect protocol.

10.4 Wissenschaftskommunikation - Konferenzbeitrag

Spychalski D., Rode O., Ritthaler M., Raptis G. (2021), Conceptual Design and Analysis of a Mobile Digital Identity for eHealth Applications, 2021 IEEE EMBS International Conference on Biomedical and Health Informatics (BHI), doi: 10.1109/BHI50953.2021.9508554

10.5 Weitere Öffentlichkeitsarbeit und Vernetzung

Das Projekt wurde von Prof. Raptis und Herrn Rode bei mehreren Anlässen präsentiert, z. B.:

- gesonderte Gespräche mit GKV-Vertretern
- gesonderte Gespräche mit VZBV - Vertreter der Patienten
- gesonderte Gespräche mit BÄK – Vertreter der Ärzte
- gesonderte Gespräche mit Standing Committee of European Doctors (CPME) – Vertreter der Ärzte auf europäischer Ebene

11 Verwertung der Projektergebnisse (Nachhaltigkeit / Transferpotential)

Die MOVI-Ergebnisse wurden auf einer Webseite (http://movi.fokus.fraunhofer.de) veröffentlicht und stehen für die Nachnutzung im Rahmen beliebiger Projekte zur Verfügung. Die Webseite wird nach Projektabschluss für mindestens 2 Jahre weiterbetrieben.

Der Quellcode der entwickelten Software wurde unter einer Open Source Lizenz veröffentlicht und kann im Rahmen beliebiger Projekte, die den Einsatz einer virtuellen eGK im Zusammenspiel mit NFC-fähigen Android Endgeräten planen, genutzt werden. Die Herausgabe des Quelltextes erfolgt auf Anfrage beim Fraunhofer FOKUS.

Die Ergebnisse wurden in einer wissenschaftlichen Konferenz präsentiert; das zugehörige Paper ist in den einschlägigen Wissenschafts-Datenbanken (IEEE-Explore, Web of Science, google scholar) indiziert und zugänglich.

12 Publikationsverzeichnis

Sämtliche Projektergebnisse sind über folgende Website abrufbar: http://movi.fokus.fraunhofer.de.