

Kurzbericht zum BMG-geförderten Forschungsvorhaben

Vorhabentitel	Konzeption und prototypische Realisierung einer mobilen Versichertenidentität (MOVI)
Schlüsselbegriffe	Virtuelle eGK, digitale Identität, Smartphone, Sicherheitsmechanismen mobiler Endgeräte, Attestation, TEE, HSM, Android, iOS, eIDAS
Vorhabendurchführung	<p>MitarbeiterInnen Fraunhofer FOKUS:</p> <p>Olaf Rode (Projektleitung, Konzeption, Entwicklung), Benny Häusler (Konzeption, Entwicklung), Aleksei Piatkin (Entwicklung), Emil Milanov (Entwicklung), Mike Brandtner (Entwicklung) Darya Martyniuk (Entwicklung)</p> <p>MitarbeiterInnen Fraunhofer SIT:</p> <p>Dominik Spychalski (Sicherheitsanalyse), Leon Würsching (Sicherheitsanalyse)</p> <p>MitarbeiterInnen OTH Regensburg:</p> <p>Georgios Raptis (Organisation/Konzeption, Durchführung Evaluation), Markus Ritthaler (Marktrecherche, Analyse)</p>
Vorhabenleitung	Olaf Rode
Autor(en)/Autorin(nen)	Olaf Rode (Fraunhofer FOKUS), Prof. Dr. Georgios Raptis (OTH Regensburg), Dominik Spychalski (Fraunhofer SIT)
Vorhabenbeginn	06/2019
Vorhabenende	12/2020

1. Vorhabenbeschreibung, Vorhabenziele

Das MOVI-Projekt hat sich das Ziel gesetzt, den Zugriff auf Anwendungen der elektronischen Gesundheitskarte für PatientInnen praktikabler zu gestalten. Hierbei wird eine Delegation der elektronischen Identität der eGK an eine „virtuelle eGK“ eines mobilen Geräts erforscht, um verschiedene Probleme zu adressieren, wie z.B. die fehlende NFC-Unterstützung bei „einfachen“ Android-Geräten oder die Einschränkungen bezüglich der Usability und Akzeptanz bei zu häufiger

PIN-Eingabe. Zur Untersuchung dieser Thematik wurde ein Projekt durch Fraunhofer FOKUS, Fraunhofer SIT und die OTH Regensburg aufgesetzt, welches folgende konkreten Ziele verfolgt:

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

2. Durchführung, Methodik

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 prototypisch umgesetzt. 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.

Es ist 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), konnte gezeigt werden, dass der Ansatz grundsätzlich realisierbar ist und anwendungsübergreifend Verwendung finden kann.

Das Projekt wurde dabei in 7 Arbeitsbereiche unterteilt: Dissemination und Vernetzung (AP1), Problem- und Umfeldanalyse (AP2), Konzeption und Spezifikation (AP3), Prototypische Umsetzung und Erprobung (AP4), Einführungsplanung (AP5), Sicherheitsanalyse (AP6) und Projektmanagement (AP7).

3. Gender Mainstreaming

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.

4. Ergebnisse, Schlussfolgerung, Fortführung

Das Projekt hat einen wichtigen Beitrag zur Diskussion im Umfeld der Realisierung einer „virtuellen eGK“ geleistet. Die Problem- und Umfeldanalyse führte zu einer detaillierten Analyse der durch Android und iOS unterstützten Sicherheitsfeatures. Dadurch konnte ein Nutzungsrahmen für den zukünftigen Einsatz einer virtuellen eGK abgesteckt werden. Ein Konzept wurde entwickelt, wie die virtuelle elektronische Gesundheitskarte entlang ihres Lebenszyklus umgesetzt werden kann. Prototypisch wurde eine App entwickelt, die in Kombination mit speziell angepassten Backend-Diensten die Aufgabe einer virtuellen eGK erfüllt. Diese Lösung kann grundsätzlich ein „substanzielles“ Vertrauensniveau gemäß eIDAS erreichen, allerdings nur, wenn bestimmte Sicherheitseigenschaften des Endgerätes gegeben sind. Leider konnte die entwickelte Lösung innerhalb der Projektlaufzeit nicht mit Projekt-externen Nutzern evaluiert werden. Dadurch ergeben sich Unsicherheiten in Bezug auf die Usability der Lösung. Der Standard FIDO 2 könnte perspektivisch eine Weiterentwicklung des Konzeptes erlauben. Entsprechende Lösungsansätze sollten in Folgeprojekten untersucht und wenn möglich weiterentwickelt werden.

5. Umsetzung der Ergebnisse durch das BMG

Die virtuelle eGK soll zukünftig die Identität des Versicherten in der virtuellen Welt repräsentieren und somit den Zugang zu den Online-Anwendungen des Versicherten steuern. Die entsprechenden Online-Anwendungen sollen dabei die Anwendungsszenarien der klassischen Welt ergänzen und zeitgemäße Versorgungsstrukturen ermöglichen, die auch den Einsatz von mobilen Geräten und auf diesen installierten Gesundheits-Apps berücksichtigen.

Das Projekt war ein Grundstein dafür, sichere digitale Identitäten als verpflichtend im Gesundheitswesen einzuführen (Vgl. § 291 (8) SGB V).

6. Verwendete Literatur

n.a.