



KARTENTERMINAL- SIMULATION (KT-SIM)

Kontakt

Dipl.-Inform. Andreas Hoffmann
Geschäftsbereich SQC
Tel. +49 30 3463-7392
andreas.hoffmann@fokus.fraunhofer.de

Dipl.-Inform. Nikolay Vassilev Tcholtchev
Geschäftsbereich SQC
Tel. +49 30 3463-7175
nikolay.tcholtchev@fokus.fraunhofer.de

M. Sc. Steven Ulrich
Geschäftsbereich SQC
Tel. +49 30 3463-7140
steven.ulrich@fokus.fraunhofer.de

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de

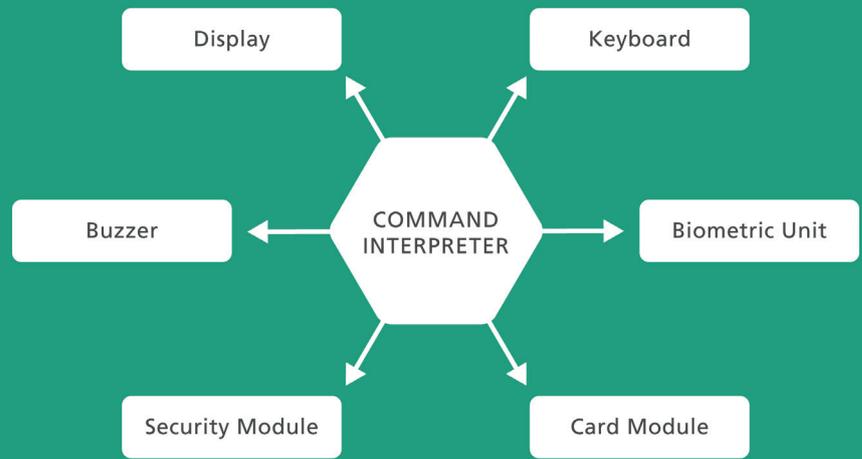
Auch in der Gesundheitsbranche nimmt die Digitalisierung immer weiter zu: Bis Ende 2018 sollen alle Arztpraxen und Krankenhäuser bundesweit an die Telematik-Infrastruktur (TI) angeschlossen werden. Für die Gesundheitsbranche in Deutschland spielt die TI eine wichtige und zentrale Rolle, da alle Akteure des Gesundheitswesens – bestehend aus Kostenträgern (z. B. Krankenkassen), Leistungserbringern und Patienten – vernetzt werden sollen.

Gemäß dem E-Health-Gesetz wird zunächst die Grundlage, nämlich ein modernes Versichertenstammdatenmanagement, aufgebaut. Anschließend werden schrittweise weitere Anwendungen wie medizinische Notfalldaten, Arzneimittelverordnungen oder Medikationspläne eingeführt. Dafür ist es notwendig, dass bei all diesen sensiblen und persönlichen Daten die verwendeten Komponenten der TI sicher und verschlüsselt miteinander kommunizieren. Bereits im Januar 2015 wurde die gesetzliche Krankenversicherungskarte (KVK) durch eine mit einem Prozessor versehene elektronische Gesundheitskarte (eGK+) abgelöst. Ziele der elektronischen Gesundheitskarte für Patienten sind eine höhere Effizienz und die sichere und verschlüsselte Kommunikation mit den Leistungserbringern und den Krankenkassen.

Software zur Simulation von Kartenterminals

Um die Komponenten der Telematik-Infrastruktur – insbesondere die dezentrale Komponente mit der Bezeichnung Konnektor, welche die Arztpraxen und Krankenhäuser mit der TI verbindet – zu testen, hat Fraunhofer FOKUS eine Java-basierte Kartenterminal-Simulation (KT-Sim) nach dem Mock-Up Prinzip entwickelt. Dadurch wird die Simulation möglichst einfach und robust gehalten. Die KT-Sim kann in allen Teststufen des Konnektors gleichermaßen für Positiv- als auch Negativ-Tests eingesetzt werden. Die Simulation

Abbildung: Systemarchitektur der Kartenterminals



ist hauptsächlich im Funktionalen Test, Konformitätstest, Last- und Performancetest, Sicherheitstest sowie Robustheitstest einsetzbar. Weitere Anwendungsbereiche wie beispielsweise Behavioural Fuzzing und Data Fuzzing werden aktuell erforscht und vorbereitet.

Simulation des Secure Interoperable Chip Card Terminals (SICCT)

Um ein Kartenterminal zu simulieren, erfolgt in erster Linie eine Simulation des SICCT-Protokolls. Die SICCT-Spezifikation beschreibt ein universell einsetzbares Chipkartenterminal, das gewisse Standards gemäß des Bundesverbands IT-Sicherheit e. V. erfüllen muss, sowie die Kommunikation mit einem geeigneten Kommunikationspartner. Ein Chipkartenterminal stellt eine dezentrale Komponente dar und kann sowohl mit der Komponente Konnektor als auch mit einem Primärsystem verbunden werden.

Für den Einsatz im Test von TI-relevanten Komponenten ist neben spezifikationskonformem Verhalten und Kommunikation auch die Manipulation der Kommunikation zwischen Konnektor und Kartenterminal möglich. Die Manipulation erlaubt zum einen die Verzögerung von Antwortnachrichten. Zum anderen bietet sie die Möglichkeit, alternative Antwortnachrichten zur Laufzeit zu verschicken.

Simulation von Karten

Mit der KT-Sim können neben dem Verhalten eines realen Kartenterminals die unterschiedlichen Arten und Generationen von Karten der Gesundheitsbranche simuliert werden. Dazu zählen neben der elektronischen Gesundheitskarte (EGK) und der Krankenversicherungskarte auch der elektronische Praxisausweis (SMC-B), der elektronische Heilberufsausweis (HBA), sowie die gerätespezifische Security Module Card (gSMC-KT).

- Verarbeitung von Kartenbefehlen gemäß des *Electronic Signals and Transmission Protocols* (ISO 7816 Part 3)
- Manipulation von Antworten der Kartenbefehle
- Logging / Protokollierung von Kartenbefehlen
- Aufbau / Initialisierung eines TrustedChannels
- Card2Card Authentication

Folgende UseCases der Gematik Konnektor Spezifikation werden adressiert:

- GetCards
- ReadVsd
- AutoUpdateVsd
- Verify Certificate
- Verify Pin
- Get Ressource
- Remote Update eines Kartenterminals
- TLS Verbindung
- Pairing
- Service Announcement
- Service Discovery