Datenschutz und Usability bei Smartcards:

Card-to-Card-Authentication

Dr. S. Buschner

Competence Center Health 3 - Telematik
adesso AG
Rotherstr. 19
10245 Berlin
stefan.buschner@adesso.de

Abstract: Der Vortrag ist ein Bericht über die Sicherheitstechnologien bei der elektronischen Gesundheitskarte (eGK), die bei der gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH spezifiziert wird. Die gematik ist ein langjähriger Kunde der adesso AG und zahlreiche Mitarbeiter der adesso AG haben in diesem Projekt mitgearbeitet, sei es in der Spezifikation, beim Bau von Referenzsystemen als auch bei Test und Zulassung der Komponenten für den Regelbetrieb. Das besondere an den Sicherheitstechnologien der Gesundheitskarte ist, dass es gelungen ist, die Sicherheit gegenüber Standardverfahren zu steigern und gleichzeitig die Usability des Systems zu verbessern.

1. Ausgangssituation

Smartcards sind das Mittel der Wahl, wenn es darum geht, Daten „mitnehmbar“ zu haben und gleichzeitig die Daten maximalen Schutz bedürfen. Die Karten in der Größe einer Visitenkarte sind in der Lage jeden illegalen Zugriff auf die Daten zu verhindern. Deswegen werden Smartcards auch als Träger des Schlüsselmaterials für die qualifizierte elektronische Signatur eingesetzt, die höchsten gesetzlichen Ansprüchen genügen muss. Selbst ein direkter Angriff auf die Microstruktur des Chips lässt keinen Zugriff auf die Daten, in diesem Fall das Schlüsselmaterial, zu. Die Authentifikation des Users gegenüber der Smartcard erfolgt dabei i.d.R. per PIN.

2. Card-to-Card-Authentication

Die Daten auf der eGK haben, da es sich um medizinische Daten der Versicherten handelt, besonderen Schutzbedarf. Den verschiedenen Akteuren im Gesundheitswesen soll dabei ein fachgerechter Zugriff auf diese Daten gegeben werden, so dass eine pauschale Freischaltung der eGK per PIN nicht in Frage kommt. Außerdem soll der Versicherte die PIN so selten wie möglich eingeben müssen, um maximale Usability zu gewährleisten. Die Lösung ist die Card-to-Card-Authentication. Dafür bekommen die Leistungserbringer im Gesundheitswesen ebenfalls Smartcards (so genannte HPCs), die

sich gegenüber der eGK des Versicherten per Zertifikat authentifizieren und so die eGK gemäß den Rechten des Leistungserbringers freischaltet.

Literaturverzeichnis

Spezifikationen zur elektronischen Gesundheitskarte (s. www.gematik.de)