

Die Funktionen der Health Professional Cards als elektronischer Heilberufsausweis

Die Spezifikation für die Health Professional Card - Version 2.0 wurde von der Ärzte- und Apothekerschaft unter Federführung des „Zentralinstituts für die kasernenärztliche Versorgung in der Bundesrepublik Deutschland“ in Auftrag gegeben und von FhG-SIT erstellt. Die HPCs werden eine maßgebliche Rolle bei der Realisierung der Informatik-Plattform für das Gesundheitswesen spielen. Als Heilberufler, die die HPC erhalten sollen, sind zunächst Ärzte und Apotheker vorgesehen. Sie soll - mit entsprechenden berufsspezifischen Zugriffsautorisierungen – auch für andere Heilberufler nutzbar sein.

Die HPC beinhaltet zunächst einmal die Kenndaten des betreffenden Health Professionals in ähnlicher Form, wie sie im heutigen Sichtausweis enthalten sind. Will ein Arzt z.B. Medikamente in der Apotheke holen, dann ist die HPC dort vorzulegen und kann elektronisch geprüft werden.

Als Sicherheitsfunktionen aus der Sicht des Heilberufslers bietet die HPC die elektronische Unterschrift, Verschlüsselung und Client-Server-Authentisierung. Der Signaturschlüssel für qualifizierte Signaturen ist mit einer eigenen PIN geschützt. Das zugehörige Schlüssel-Zertifikat sowie ggf. Attribut-Zertifikate können auf der HPC abgelegt werden. Als Signatur-Verfahren ist der RSA-Algorithmus vorgesehen.

Die Verschlüsselungs-Funktion kommt nur beim Empfang verschlüsselter Daten zum Einsatz, da die HPC nur für das Schlüsselmanagement, nicht aber für die eigentliche Datenver- und -entschlüsselung verwendet wird.

Die Client-Server-Authentisierung-Funktion gestattet dem Heilberufler den Zugriff auf Server-Systeme, die z.B. für elektronische Patienten-Akten genutzt werden sollen. Die Nutzung der Verschlüsselungs- und Client-Server-Authentisierungsfunktion erfordert die Eingabe einer für diese Funktionen vorgesehenen separaten PIN.

Besonders wichtig ist jedoch die Card-to-Card Authentisierung-Funktion, da mit ihrer Hilfe der Heilberufler seine Zugriffsrechte gegenüber einer elektronischen Gesundheitskarte – wie vom GMG gefordert – nachweisen kann. Auch diese Funktion ist PIN geschützt, damit bei Diebstahl oder Verlust einer HPC kein Unbefugter auf eine elektronische Gesundheitskarte zugreifen kann. Da bisher die elektronische Gesundheitskarte noch nicht spezifiziert ist, wurde für die HPC sowohl ein symmetrisches als auch ein asymmetrisches Authentisierungsverfahren spezifiziert. Die Card-To-Card-Authentisierung ist zugleich auch eine Echtheitsprüfung von HPC und elektronischer Gesundheitskarte.

Abstract

Die HPC-Spezifikation beinhaltet auch die Spezifikation einer sog. Security Module Card SMC, die ähnliche Funktionen wie eine HPC bietet. Hauptzweck einer SMC ist die Card-to-Card Authentisierungs-Funktion sowie eine institutionsbezogene Verschlüsselungsfunktion, so daß verschlüsselte Dokumente entweder an eine bestimmte Person oder aber, etwas generalisierter, z.B. an eine Arztpraxis oder eine Krankenhausabteilung gesandt werden können. Außerdem kann mit der SMC auch eine ablauforganisationsgerechte Nutzungsart von HPCs (Zugriff auf die HPC von verschiedenen Stationen) erreicht werden.