URL: http://www.fr-online.de/in_und_ausland/wissen_und_bildung/aktuell/?em_cnt=1292801

**Diagnose**

# Schlüssel

**Von Dr. med. Bernd Hontschik**

Braucht ein Patient für die Benutzung seiner elektronischen Gesundheitskarte (eGK) in Zukunft eine Grundausbildung in Informatik? 120.000 niedergelassene Ärzte, 65.000 Zahnärzte, 2000 Apotheken, 2200 Krankenhäuser und 270 Krankenkassen werden bald mit Hunderttausenden von Terminals ausgestattet sein, in die 80 Millionen Krankenversicherte ihre PIN-geschützte eGK in den einen Schlitz und der Inhaber eines elektronischen Heilberufsausweises (eHA) denselben in den anderen Schlitz stecken, damit mehr als elf Milliarden sensible medizinische Datentransaktionen pro Jahr über das Internet versandt, auf zentralen Servern abgespeichert und ständig online abgeglichen werden können. Natürlich alles sicher und verschlüsselt.

Die eGK hat Pflichtinhalte (Name, Geburtsdatum, Versichertenstatus, Foto, Sozialversicherungsnummer), und "freiwillige" Inhalte, wie etwa die elektronische Patientenakte (ePA) mit allen Rezepten und Verordnungen. Freiwillig heißt, dass der Patient entscheidet, welche Informationen gespeichert werden und welche nicht, welche lesbar sein dürfen und welche nicht. Ihr orthopädischer Schumacher muss ja nicht unbedingt wissen, ob Sie eine psychotherapeutische Behandlung hinter sich haben, HIV-positiv sind oder Viagra verschrieben bekommen. Und im Internet möchten Sie das alles schon gar nicht veröffentlichen.

Es brauchen alle Beteiligten also einen Berechtigungs-Schlüssel. Entweder benutzen Sender und Empfänger zum Verschlüsseln und Entschlüsseln den gleichen Schlüssel, was bei den sensiblen Gesundheitsdaten im Internet aber keine sichere Verschlüsselung garantiert. Deswegen muss asymmetrisch verschlüsselt werden, wobei zwei halbe Schlüssel entstehen: einer zum Verschlüsseln, einer zum Entschlüsseln.

Den einen halben Schlüssel zum Entschlüsseln stellt der Empfänger dem Sender bereit (public key). Mit diesem öffentlichen Schlüssel verschlüsselte Nachrichten kann dann nur der Empfänger mit der anderen, der zweiten Schlüsselhälfte (private key) entschlüsseln. Das ist der Entschlüsselungs-Schlüssel, mit dem die verschlüsselten Daten gelesen werden können.

Man müsste die eine entscheidende Schlüsselhälfte kennen, um Zugang zu finden zu den Plänen und Gedanken der Politiker und Verschlüsselungsexperten, die sich das alles ausgedacht haben (politician key). Dann könnte man ihnen mit der zweiten Schlüsselhälfte (physician key) zusenden, worum es in der Humanmedizin eigentlich geht - oder wenigstens gehen sollte. Jedenfalls bestimmt nicht um die Rendite der beteiligten Schlüsselindustrien.

**Kontakt: www.medizinHuman.de**


Dokument erstellt am 22.02.2008 um 17:08:02 Uhr
Letzte Änderung am 22.02.2008 um 20:06:54 Uhr
Erscheinungsdatum 23.02.2008