

10.07.2009 19:21

## E-Gesundheitskarte: Datenverlust mit Folgen

Die Testläufe der elektronischen Gesundheitskarte (eGK) und den ärztlichen Heilberufsausweis der Generation 1 haben einen gravierenden Rückschlag erlitten. Nach dem Ausfall eines **Hardware Sicherheitsmoduls** [<http://de.wikipedia.org/wiki/Hardware-Sicherheitsmodul>] (HSM), auf dem das private Schlüsselmaterial der Root Certificate Authority (Root-CA) für Karten der Generation 1 gespeichert war, stellte sich heraus, dass es kein Backup dieser Daten gab. Die Konsequenz: Werden neue Karten für die Feldtest benötigt, müssten alle bisher für die Testreihen produzierten Karten ausgetauscht werden, da eine neue Root-CA erzeugt werden müsste.

Die elektronische Gesundheitskarte ist in vieler Hinsicht ein ambitioniertes Großprojekt. Unter anderem wird hier die weltweit größte Public-Key-Infrastruktur (PKI) aufgebaut. Sie soll einmal 80 Millionen Gesundheitskarten und Heilberufsausweise in die Lage versetzen, sich gegenseitig auf Echtheit zu überprüfen. Für diese Authentifizierung gibt es auf den Karten ein Card-Verifiable-Zertifikat (CV-Zertifikat), das in letzter Instanz von einer Root Certificate Authority (Root-CA) abhängt. Alle Kartenhersteller beziehen sich auf die Root-CA, wenn sie CV-Zertifikate auf den Karten anbringen.

Neben der Authentifizierung ist die Root-CA auch für den Einzug von Karten (Revocation Service) wichtig. Öffentliche und private Schlüssel werden von einem Hochsicherheitsmodul (HSM), einer besonders leistungsfähigen Smartcard mit eigenem Prozessor und Zufallszahlengenerator, erzeugt und gespeichert. Mit einer speziellen Backup-Prozedur werden alsdann die Daten gespeichert, denn das HSM verfügt über eine eigene Schutzsoftware, die Angriffe erkennen soll und bei Anomalitäten (fehlerhaften PIN-Eingaben, Spannungsabfälle etc.) das HSM herunter fährt.

Für den Betrieb der PKI der Gesundheitskarte hat sich die Projektgesellschaft **Gematik** [<http://www.gematik.de>] entschieden, die Root-CA als Dienstleistung an die zur Bundesdruckerei gehörende Firma **D-Trust** [<https://www.d-trust.net/internet/files/pm-20060509.pdf>] zu vergeben. In deren Trustcenter passierte offenbar nach einem Spannungsabfall das, was D-Trust Geschäftsführer Matthias Merx gegenüber heise online als etwas beschrieb, was schonmal vorkommt: "Das HSM hat eigenständig die Daten gelöscht, weil es einen Angriff vermutete."

Doch die übliche Trustcenter-Routine, die Daten zu restaurieren, konnte nicht greifen, weil es kein Backup gibt. "Die Gematik hat entschieden, 'Wir verzichten auf das Backup'. Das haben wir als Dienstleister zu akzeptieren," erklärte Merx, nicht ohne darauf hinzuweisen, dass es zum Start der richtigen Gesundheitskarte Backups der Root-CA-Daten geben werde. So aber müsse eine neue Root-CA angelegt werden. Das sei kein Problem. "Das Testsystem kann weiterlaufen, solange keine neuen Karten ausgegeben werden müssen."

Die Erklärung, dass man beim Dienstleister auf einen Test ohne Backup der privaten Schlüssel der Root-CA bestanden habe, verweist Gematik-Sprecher Daniel Poeschkens gegenüber heise online in das Reich der Legende: "Wir haben uns nicht gegen einen Backup-Dienst entschieden. Vielmehr ist es so, dass der Dienstleister den Betrieb des Testsystems übernommen und auch den fortlaufenden Betrieb zu gewährleisten hat. Wie er dieser Verpflichtung nachkommt, obliegt seiner Verantwortung."

In einem heise online vorliegenden Rundschreiben an die Testpartner erklärt die Gematik, was der Störfall bedeutet: "In der Konsequenz heißt dies, dass zu den derzeit im Umlauf befindlichen korrekten eGK-Musterkarten der Generation 1 insbesondere keine Muster-HBA der Generation 1 mehr produziert werden können, die mit den bereits existierenden eGKs eine erfolgreiche Card-to-Card-Authentifizierung durchführen können. Bitte beachten Sie daher, dass die für den nordrheinischen Interoperabilitätstest verteilten korrekten Muster-eGKs ausschließlich für Tests im Basis-Rollout-Szenario verwendet werden können und nach den Basis-Rollout-Tests zu vernichten sind. Obwohl die Muster-eGKs korrekt sind, müssen sie für Tests in künftigen Stufen der Telematik-Infrastruktur noch einmal ersetzt werden."

Das Hickhack um die Datensicherheit einer Root-CA, die eine relativ kleine Menge von Testkarten stützt, mag trivial erscheinen. Indessen überrascht, dass ein zentraler Dienst, der auf alle Testkarten einer Generation ausstrahlt, so vernachlässigt wurde. Die Versicherung, dass beim echten System alles richtig gesichert wird, muss man erst einmal glauben – oder auch nicht. Ein System verteilter Root-CAs, wie sie vom Karlsruher Gesundheitskarten-Kritiker Thomas Maus vorgeschlagen wurde, könnte hier Abhilfe bringen.

Andreas Bogk vom Chaos Computer Club, der vor wenigen Wochen dem Bundestag in einer Anhörung zur Gesundheitskarte Rede und Antwort stand, macht auf einen seiner Ansicht nach vergleichbaren Aspekt aufmerksam: "Das ist dasselbe Problem, das auch bei den Daten der elektronischen Gesundheitsakte auftreten wird. Das Backup-Problem lässt sich ja auch da nur mit Hilfe eines Backups des Private Keys lösen. Damit wird aber das gesamte Sicherheitsversprechen ("zentrale Speicherung ist kein Problem, denn der Schlüssel ist nur auf der Karte und damit in der Verfügungsgewalt des Patienten") hinfällig. (*Detlef Borchers*) / (**vbr** [<mailto:vbr@ct.heise.de>] /c/t)

English version: **Loss of data has serious consequences for German electronic health card** [<http://www.h-online.com/security/Loss-of-data-has-serious-consequences-for-German-electronic-health-card-/news/113740>]