VON IDG COMPUTERWOCHE VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/t-systems-zertifiziert-aok-ausweise,1908301

Elektronische Gesundheitskarte

T-Systems zertifiziert AOK-Ausweise

Datum: 19.10.2009
Autor(en): Hartmut Wiehr

Langsam scheint die elektronische Gesundheitskarte zu kommen. Diesen Eindruck vermittelt zumindest der Deal zwischen T-Systems und 13 Landesverbänden der AOK: Der IT-Dienstleister hat den Zuschlag bekommen, für die kommenden digitalen Ausweise von 17 Millionen Versicherten die Sicherheitszertifikate zu erstellen und zu verwalten.

Der AOK-Bundesverband hat sich vorgewagt und stellvertretend für die meisten Landesorganisationen den Service-Anbieter T-Systems mit der Erstellung und Verwaltung der Sicherheitszertifikate für die elektronische Gesundheitskarte (eGK) beauftragt. Inhalt des Vertrages ist die Lieferung der Zertifikate für jede neu ausgegebene Karte an die Karten-Managementsysteme der AOK. T-Systems betreibt darüber hinaus im eigenen Trust Center einen Verzeichnis- und Sperrdienst, mit dem die Gültigkeit der Zertifikate überprüft werden kann.

Bei der Verwendung authentifizieren sich – so der gegenwärtige Stand der Planung – der Patient und das Mitglied eines Heilberufs gegenseitig. So ist laut AOK die eGK vor dem Zugriff unbefugter Dritter geschützt: "Wird eine Karte als verloren gemeldet oder wechselt der Versicherte die Krankenkasse, sperrt die AOK die elektronische Gesundheitskarte online. Das Trust Center erklärt die Sicherheitszertifikate dieser Karten sofort als ungültig und schützt so vor einer missbräuchlichen Verwendung der eGK."

Der Schutz der eGK soll mithilfe von fünf auf ihr gespeicherten Sicherheitszertifikaten vonstatten gehen. Das entspreche, so T-Systems, den Vorgaben der gematik, der Gesellschaft für Telematikanwendungen der Gesundheitskarte. Es gibt demnach je zwei Verschlüsselungs- und Autorisierungszertifikate für Daten und Datenzugriffe auf jeder eGK. Das fünfte digitale Identifizierungszeichen soll die Karte als echte Gesundheitskarte ausweisen.

T-Systems hat für solche Aufgaben bei seinem Trust Center spezielle Services eingerichtet und ist schon länger im Geschäft mit Zertifikaten. Bisher hat man hauptsächlich für Bundesbehörden und Kommunen sowie für die Automobilbranche und Verkehrsbetriebe gearbeitet. Wie Detlef Dienst, Leiter Trust Center Notary Services und als Leiter des akkreditierten Zertifizierungsdiensteanbieters gegenüber der Bundesnetzagentur verantwortlich, ausführt, habe man den Zuschlag für den Auftrag aufgrund fachlicher und preislicher Kriterien erhalten.

T-Systems liefert nur Schlüsselzertifikate

T-Systems liefert nicht die elektronischen Gesundheitskarten, berichtet Dienst, sondern lediglich die auf ihnen abgespeicherten Schlüsselzertifikate. Diese dienen als Beweis für die Identität der versicherten Personen, die durch einen unabhängigen Dritten, in diesem Fall dem Trust Center von T-Systems, bezeugt wird. Dienst erläutert im Gespräch mit CIO: "Wir liefern diese Zertifikate für die Gesamtzahl der Versicherten der 13 AOK-Landesverbände und betreiben dazu auch einen Sperrdienst, falls eine Karte vor Ablauf ihrer Gültigkeit gesperrt werden muss. Dafür werden wir ein Verzeichnis anlegen, vergleichbar etwa mit einem öffentlichen Telefonbuch, in dem alle Zertifikate hinterlegt sind."

Das Verzeichnis ist lediglich für eine geschlossene Benutzergruppe im Netz der Telematik-Infrastruktur des Gesundheitswesens erreichbar. Die Zertifikate können dann zum Beispiel von einem Arzt beim Praxis- oder Krankenhausbesuch zur Bestätigung abgerufen werden.

Ob jetzt nun alle oder nur ein Teil der Patienten- oder doch lediglich Rezeptdaten auf der eGK gespeichert werden, hat mit dem Aufgabenbereich des Trust Centers nichts zu tun. Hier geht es nur um die Identitätsprüfung der Versicherten.

Bei einer Zertifizierungsprüfung geht es nur um jene Daten, die als Schlüssel auf der Karte abgelegt und vom Trust Center beglaubigt worden sind. Das Trust Center tritt damit lediglich zu Beginn der Schlüsselerstellung auf der Karte in Erscheinung – in seiner Funktion eines unabhängigen Dritten, der die Identität einer Person beglaubigt – und später dann beim Abgleich mit dem Verzeichnis. Hier wird bestätigt, ob das Zertifikat gültig oder gesperrt ist. Insofern ist das Trust Center in den jeweils aktuellen Beglaubigungsprozess beziehungsweise in die Online-Gültigkeitsabfrage eingebunden.

Für Nicht-Techniker: Das entspricht der Überprüfung von Reisepässen an der Grenze oder auf dem Flughafen, wenn sie von den Grenz- oder Polizeibeamten "durchleuchtet", das heißt auf Gültigkeit oder spezielle Registereinträge abgeglichen werden.

AOK stellt hohe Hürden auf

Die erstellte Signatur ist selbst auch nachprüfbar, zum Beispiel ob sie von einem bestimmten Trust Center durchgeführt wurde. Die AOK hat deshalb bei ihrer Ausschreibung nur von der Bundesnetzagentur akkreditierte Trust Center oder solche, die sich ein gesondertes Sicherheitszeugnis ausstellen ließen, berücksichtigt. Diese hohen Bürden, wie sie die AOK aufstellte, werden von der gematik explizit gefordert. Für die spätere Identitätsüberprüfung wird im übrigen ein eigenes, abgesichertes Netzwerk, die Telematik-Infrastruktur des deutschen Gesundheitswesens, eingesetzt.

Der Kreis der akkreditierten Trust Center ist zwar momentan noch überschaubar, aber es zeichnet sich aufgrund der langsamen Ausbreitung von digitalen Signaturen doch ein wachsendes Geschäft ab.
