Der Verzeichnisdienst der Telematik-infrastruktur

Medizinische Daten gehören zu den sensibelsten personenbezogenen Daten, die über Patienten vorliegen und bei der Behandlung verwendet werden. Sie sind daher besonders schützenswert und durch geeignete technische Mittel vor einem unberechtigten Gebrauch abzusichern. Hierzu werden Techniken aus der Welt der Kryptographie verwendet, aus der sich in folgenden auch ein Bedarf für den sogenannten „Verzeichnisdienst der Telematikinfrastruktur" ableitet. Daher muss sichergestellt sein, dass nur Berechtigte auf die medizinischen Daten der Versicherten zugreifen können.

Aus diesem Grunde kommt es zu einem Aufbau eines Registers. Heilberufsausweisherausgeber, wie die Landesärztekammern, übermitteln an den TI-Verzeichnisdienst die Daten aller potenziellen Nutzer der Telematikinfrastruktur, also das Zertifikat (mit dem öffentlichen Schlüssel) des eHBA, den Namen des Ausweisinhabers sowie weitere adressierende Informationen, wie die Praxisanschrift und die Facharztbezeichnung, die sich gut als Suchkriterien eignen. Man muss sich den Verzeichnisdienst wie ein umfangreiches Adressbuch vorstellen.

Erst mit dem Eintrag im Verzeichnisdienst ist der Ausweisinhaber für Dritte in der Telematikinfrastruktur einfach adressierbar und es können für ihn Nachrichten verschlüsselt werden. Also sowohl für andere Leistungserbringer, die für ihn elektronische Arztbriefe verschlüsseln und mittels KIM übertragen wollen, als auch für Patienten, die dem Ausweisinhaber Zugriffsrechte auf Ihre elektronische Patientenakte erteilen wollen. Sowohl ein zugriffserteilender Patient als auch ein sendender Kollege müssen aus dem Verzeichnisdienst den öffentlichen Schlüssel des Empfängers herunterladen.

Das hört sich zunächst kompliziert an. In der praktischen Verwendung erfolgen diese Schritte, wie das Herunterladen und Ver- und Entschlüsseln, beim Sender und Empfänger im Hintergrund und ohne Zutun des Nutzers.

Eine Alternative wäre, dass jede Anwendung bzw. jeder Anwender ein „eigenes" Adressbuch aufbaut und pflegt. Da alle Ausweise (eHBA, SMC-B, eGK) aber eine begrenzte Laufzeit von max. 5 Jahren haben oder auch verloren gehen können und damit regelmäßig durchgetauscht werden und sich damit auch die Schlüsselpaare ändern, ist dies nicht praktikabel.

Der Gesetzgeber hat aus diesem Grund mit § 313 SGB V vorgegeben, dass die gematik den Verzeichnisdienst der Telematikinfrastruktur betreibt und gem. § 307 Abs. 5 i.V.m. §

311 Abs. 1 Nr. 3 i.V.m. § 313 SGB V datenschutzrechtlich Verantwortliche ist. Die Landesärztekammern
haben gem. § 313 Abs. 5 SGB V entsprechende personenbezogene Daten ihrer Kammermitglieder zu liefern.
Aktuell bauen die Landesärztekammern die entsprechenden IT-Strukturen auf, um bis zum gesetzlich geforderten Termin 01.12.2020 die erforderlichen Daten der eHBA-Inhaber an den TI-Verzeichnisdienst zu übermitteln und zu pflegen.

Technischer Hintergrund des Verzeichnisdienstes:

Für eine vertrauliche Übertragung einer Information an einen definierten Empfänger, erfolgt seitens des Senders (!) eine Verschlüsselung der Information mit dem öffentlichen Schlüssel des Empfängers (!). Der öffentliche Schlüssel heißt „öffentlich", weil aus seiner Kenntnis kein Sicherheitsproblem resultiert und für die „Öffentlichkeit" abrufbar ist. Er korrespondiert aber zum privaten Schlüssel, welcher im Heilberufsausweis sicher verwahrt ist und nur mit der korrekten PIN nutzbar wird. Das so genannten Zertifikat (gemäß dem Standard X.509v3) enthält den Namen und den öffentlichen Schlüssel und verbindet somit das Schlüsselpaar mit dem Ausweisinhaber. Der Name kommt aus der persönlichen Identifizierung bei Antragstellung des Heilberufsausweises. Manipulierbar ist das Zertifikat nicht, da es wiederum vom Ausweisherausgeber kryptographisch signiert wurde. Es bestätigt auch die Berufsgruppeneigenschaft „Ärztin/Arzt".
Die beiden Schlüssel (öffentlich/privat) korrespondieren insofern, dass alles was mit dem einen Schlüssel in die eine Richtung getan wurde, nur mit dem korrespondierenden anderen Schlüssel wieder rückgängig gemacht werden kann. Vergleichbar einem Türschloss, bei dem man mit dem einen Schlüssel nur „ZU" und mit dem anderen nur „AUF"-schließen kann. Der Fachausdruck dafür ist asymmetrische oder auch Public-Key-Kryptographie (PKI). Konkrete Beispiele für asymmetrische Kryptoalgorithmen sind „RSA" – nach den Mathematikern Rivest, Shamir, Adleman – oder auch das modernere „ECC", für Elliptic Curve Cryptography. Diese Verfahren basieren im Grunde auf mathematischen Problemen, die schwer lösbar sind, wie bspw. die Primfaktorzerlegung.
Wenn jetzt der Sender (!) den öffentlichen Schlüssel des Empfängers (!) zwingend für die Verschlüsselung benötigt, so dass nur der Empfänger die Informationen mit seinem privaten Schlüssel aufschließen kann, ergibt sich der Bedarf eines zentralen Adressbuches, in welchem der Sender den Empfänger suchen und dessen öffentlichen Schlüssel, resp. Zertifikat, finden und herunterladen kann.
Und genau diese Rolle und Funktion bietet der Verzeichnisdienst der Telematikinfrastruktur.

(Mitteilung der Bundesärztekammer)