Alternative Versichertenidentität (al.vi)

Die ePA unterstützt neben der eGK als Authentifizierungsmittel auch eine sog. alternative Versichertenidentität (al.vi) gem. § 336 Abs. 2 SGB V, die der Versicherte bspw. auf Wunsch zusätzlich zu seiner eGK bei der Krankenkasse beantragen kann, damit er auf seine ePA mittels mobilen Endgeräts (zB Smartphones, Tablets als Frontend des Versicherten)[1] zugreifen kann. Die Anschaffung eines Kartenterminals (auch sog. Kartenlesegerät) oder eines Smartphones mit NFC-Unterstützung ist damit zur ePA-Nutzung nicht zwingend notwendig. Der private Schlüssel zur Authentisierung wird bei diesem Verfahren in einem sicheren Schlüsselspeicher[2] des **Signaturdienstes** der TI Plattform gespeichert. Der Signaturdienst ist als Dienst der TI Plattform potenziell auch von anderen Anwendungen als der ePA nutzbar. Die Authentifizierung des Versicherten erfolgt dann durch Auslösung einer Signatur mit diesem Schlüssel (Fernsignatur). Für die Authentifizierung des Versicherten am Signaturdienst wird das eIDAS Level „substanziell“ gem. Art. 8 eIDAS VO gefordert.[3] Das Verfahren selbst ist nicht näher spezifiziert, muss aber geeignet sein, das Vertrauensniveau „substanziell“ gem. BSI TR 03107-1 zu erfüllen.[4] Auch vom Hersteller und Anbieter wird für die Implementierung des Dienstes das substanzielle Sicherheitsniveau verlangt, was auch im Rahmen des Sicherheitsgutachtens bei der Zulassung überprüft wird.[5] Das Sicherheitsniveau der Authentifizierung mittels Smartcard ist demgegenüber als „hoch“ iSv Art. 8 eIDAS VO einzustufen. Der Identitätsnachweis und die Überprüfung des Versicherten bei der Registrierung der Fernsignatur als elektronisches Identifizierungsmittel erfolgt – wie bereits die Ausgabe der eGK – nach den Vorgaben der Richtlinie des GKV-Spitzenverbands nach § 217f Abs. 4b SGB V.

Die Unabhängigkeit von der eGK bei der Nutzung der ePA wird nicht allein durch die al.vi, sondern erst im Verbund mit dem Schlüsselgenerierungsdienstes (SGD) erreicht. Durch die Nutzung der al.vi wird die Authentifizierungsidentität der eGK nicht benötigt und durch die Nutzung des SGD entfällt die Notwendigkeit des Einsatzes der Verschlüsselungsidentität des Versicherten auf der eGK. Dadurch wird allerdings das Authentifizierungsverfahren zum neuralgischen Punkt für die Gesamtsicherheit der ePA. Überwindet ein Angreifer die Authentifizierung, hat er Zugriff auf das kryptographische Verschlüsselungsmaterial des Versicherten und damit auf die Inhalte von dessen ePA. Somit besteht bzgl. der Authentifizierung ein höheres Schadensrisiko bei gleichzeitig abgesenktem Sicherheitsniveau für das Authentifizierungsverfahren. Das BSI attestiert der aktuellen Lösung zwar den Status einer Übergangslösung nach dem Stand der heutigen Technik, fordert aber nach Ende einer Übergangsfrist ein stärkeres Authentifizierungsverfahren.[6] Es ist daher zu erwarten, dass die al.vi in absehbarer Zeit von den karteunabhängigen Identitäten im Zusammenspiel mit einem Identity Provider der TI abgelöst wird.

1)
§ 312 Abs. 1 Nr. 11 SGB V.

2)
Dazu muss ein nach einschlägigen Standards sicherheitsevaluiertes Hardware Security Modul (HSM) zum Einsatz kommen (vgl. gemSpec_SigD, S. 12, Anforderung A_17339).

3)
gemKPT_Arch_TIP, S. 94, Anforderung A_17640 und gemSpec_SigD, S. 15 f., Anforderung A_17384.

4)
gemSpec_SigD, S. 16, Anforderung A_18172.

5)
gemSpec_SigD, S. 11, Anforderung A_17373 und A_17336.

6)
S. aerzteblatt.de v. 2.5.2019, www.aerzteblatt.de/nachrichten/102771/Behoerde-sieht-Sicherheitsluecken-bei-mobilem-Authentifizie

rungsverfahren-fuer-elektronische-Patientenakte (25.7.2022).