2-Faktor-Authentifizierung: Nicht nur für das EPD wichtig!

Das EPDG verlangt eine 2-Faktor-Authentifizierung nicht nur von Patientinnen und Patienten, sondern auch von **Gesundheitsfachpersonen** und deren Hilfspersonen. Dieser Artikel zeigt auf, wie dies unter Nutzung der im Spital oder im Heim vorhandenen Mittel umgesetzt werden kann.

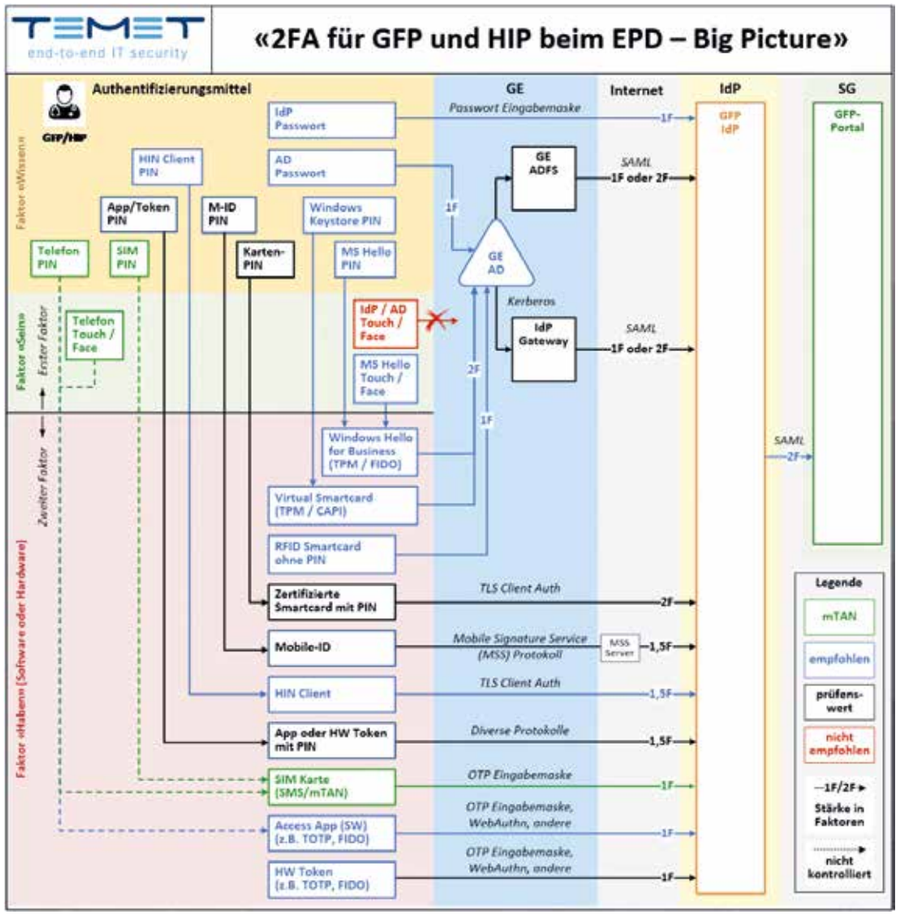
▶ THOMAS KESSLER

Der Identitätsdiebstahl ist eines der grossen Probleme der Informationssicherheit: Benutzerkonten bei Online-Diensten, die aus dem Internet erreichbar sind, sind ständigen Angriffen krimineller Individuen und Organisationen ausgesetzt. Seit Langem ist bekannt, dass diesen Angriffen mit einer starken Authentifizierung begegnet werden kann, wie sie zum Beispiel beim E-Banking gebräuchlich ist. Das Ausführungsrecht zum Bundesgesetz über das elektronische Patientendossier EPDG verlangt deshalb eine sogenannte 2-Faktor-Authentifizierung (2FA) aller Personen, die auf ein elektronisches Patientendossier zugreifen.

Die Situation beim Zugriff von Gesundheitsfachpersonen (GFP) und Hilfspersonen (HIP) unterscheidet sich allerdings von derjenigen bei Patientinnen und Patienten: Nicht alles, was einer Privatperson bei der sporadischen Nutzung eines Online-Dienstes zugemutet werden kann, taugt auch für den klinischen Alltag im Spital oder im Heim. Gleichzeitig stehen dort Mittel und Infrastrukturen zur Verfügung, die bei einer Privatperson nicht vorausgesetzt werden können. Im Folgenden zeigen wir auf, wie eine EPDG-konforme 2FA im Heim oder im Spital aussehen könnte.

2 Faktoren: Woher nehmen?

Als 2-Faktor-Authentifizierung bezeichnen wir Verfahren, die einen Faktor «Haben» mit einem Faktor «Wissen» oder einem Faktor «Sein» kombinieren. Der Faktor «Haben» wird in jedem Fall benötigt, wobei es sich hierbei um Hardware (eine Smartcard, eine SIM-Karte oder ein anderes Token) oder Software (zum Beispiel eine App) handeln kann. Der Faktor «Wissen» ist üblicherweise ein mehr oder weniger geheimes Passwort, das zentral auf einem Server oder dezentral auf einem persönlichen Gerät verwaltet und gegengeprüft wird; dieses wird auch als PIN oder Token-PIN bezeichnet. Der Faktor «Sein» schliesslich ist ein individuelles Körpermerkmal wie beispielsweise ein Fingerabdruck oder die Gesichtsform. Für alle drei Faktoren und deren Kombination gibt es verschiedene Implementierungsmöglichkeiten *(siehe Abbildung).*



Das Schaubild zeigt verschiedene Varianten für eine 2-Faktor-Authentifizierung. Ein Faktor «Haben» (roter Bereich) wird in jedem Fall benötigt und entweder mit einem Faktor «Wissen» (gelber Bereich) oder «Sein» (grüner Bereich) kombiniert. Die Authentifizierung gegenüber dem Identity Provider (IdP) erfolgt entweder direkt oder über das Active Directory der Gesundheitseinrichtung (GE AD).

Folgende Lösungsansätze sind besonders interessant:

› Heute noch sehr gebräuchlich ist das sogenannte **mTAN-Verfahren**, das ein Passwort (Faktor «Wissen») mit einer SIM-Karte (Faktor «Haben») kombiniert, wobei der Besitz der SIM-Karte durch die Zustellung eines Einmalpasswortes mittels SMS verifiziert wird. Das mTAN-Verfahren ist vor allem dann interessant, wenn die Anmeldung am Windows-Arbeitsplatz mit dem Active-Directory-Passwort als erstem Faktor genutzt wird. Aufgrund der zunehmenden Angriffe auf Mobiltelefone und GSM-Netzwerke hat das mTAN-Verfahren seinen Zenit allerdings überschritten.

› In der heutigen Zeit des «Mobile First» kämpfen unterschiedlichste **Authentifizierungs-Apps** um Marktanteile. Neben den Produkten der ganz Grossen wie «Google Authenticator» oder «Microsoft Authenticator» haben sich auch Nischenanbieter wie Kobil, Vasco oder Futurae mit interessanten Produkten etablieren können. Es ist an dieser Stelle nicht möglich, auf die verschiedenen Ausprägungen dieser Apps in Bezug auf die Kommunikationsprotokolle und Benutzerinteraktionen sowie die Nutzung der auf dem Smartphone zahlreich verfügbaren Sensoren einzugehen.

› Allen Authentifizierungs-Apps gemeinsam ist die Gefährdung durch Schadsoftware, die sich auf dem Trägergerät der App einnistet. Mit dem Argument der Malware-Resistenz setzen sich deshalb Anbieter von **Hardware-Token** in Szene. Einfach zu benutzende FIDO-Token wie Yubikey oder Google Titan sorgen auch in diesem Marktsegment für innovative Bewegung. Die von Swisscom, Sunrise und Salt angebotene Mobile-ID basiert auf der SIM-Karte und kann ebenfalls zur Kategorie der Hardware-Token gezählt werden.

› Der **FIDO-2-Standard** ist auch die Basis von Windows Hello for Business, mit dem Microsoft das Versprechen der passwortlosen Authentifizierung einlösen will. Dieses Verfahren kombiniert den Besitz einer sicheren Hardware-Komponente (Faktor «Haben»: ein im Endgerät verbautes Trusted Platform Module; TPM) wahlweise mit einem biometrischen Muster (Faktor «Sein»: Fingerabdruck oder Gesichtserkennung) oder mit einer PIN (Faktor «Wissen») und bietet eine 2-Faktor-Authentifizierung gegenüber dem firmeninternen Active Directory oder gegenüber dem Azure Active Directory in der Cloud. Hierzu sei angemerkt, dass biometrische Muster nur dezentral in einer persönlichen Hardware gespeichert und gegengeprüft werden sollten. Biometrische Verfahren ermöglichen für sich alleine keine 2FA, sind aber in Kombination mit einem «Haben-Faktor» durchaus interessant, zumal sich die Qualität moderner Sensoren durchaus mit der Qualität einer typischen PIN messen kann.

➡ Das mTAN Verfahren hat seinen Zenit überschritten.

Drei Stossrichtungen für die 2FA von GFP und HIP

Beim heutigen Stand der Technik empfehlen wir, für die folgenden drei Anwendungsfälle je eine unterschiedliche Lösung anzustreben:

› **Eine Lösung mit minimalem Investitionsaufwand** seitens der Gesundheitseinrichtungen, basierend auf der Kombination des Active-Directory-Passwortes mit einer Authentifizierungs-App oder einem Hardware-Token. Werden sowohl ein Token als auch eine App angeboten, dann können Benutzer mit und ohne Smartphone optimal bedient werden. Für beide Lösungselemente steht eine Vielzahl Produkte zur Auswahl, wobei die Benutzbarkeit im klinischen Alltag als wichtiges Evaluationskriterium berücksichtigt werden sollte.

› **Eine maximal benutzerfreundliche Lösung** mit Single SignOn im Heim oder Spital, basierend auf einer 2-Faktor-Authentifizierung gegenüber dem internen Active Directory, wobei die «Spielregeln» für die Anbindung eines nach EPDG zertifizierten Identity Providers (IdP) sowie dessen Anforderungen an die internen Komponenten und Prozesse vorgängig zu klären und mit dem Regulator abzustimmen sind. Auch hier gibt es verschiedene Lösungsansätze wie Windows Hello for Business, Microsoft Virtual Smartcard oder Lösungen mit RFID-Smartcard.

› **Eine Lösung speziell für niedergelassene Gesundheitsfachpersonen**, die möglichst geringe Anforderungen an die benutzerseitige Infrastruktur stellt und ohne ein lokales Authentifizierungssystem auskommt.

Die moderne Entwicklung der Informatik (Stichwort «Cloud») wird dazu führen, dass immer mehr Dienstleistungen aus dem Internet bezogen werden. Dies hat zur Folge, dass mittels 2FA abgesicherte Zugänge in der Art des EPD früher oder später zum Normalfall werden. Es ist deshalb wichtig, die Weichen heute richtig zu stellen und in eine ausbaufähige Lösung für die 2-Faktor-Authentifizierung beim EPD zu investieren.

Thomas Kessler ist Partner der TEMET AG in Zürich und IT-Sicherheitsarchitekt. Er studierte Physik an der ETH Zürich und ist seit über 25 Jahren in der Informationssicherheit tätig.