2-Faktor Authentifizierung beim EPD: Eine Orientierungshilfe

Swiss eHealth Forum 2019

Solution Präsentation Do 15:15 – 15:45

Martin Bruderer, Strategischer Projektleiter eHealth / EPD, USB
Thomas Kessler, IT-Security Architekt, TEMET AG

07.03.2019

Agenda

- 2-Faktor Authentifizierung am USB
  - Heutige Lösung
  - Vorgehensplan
- Gesetzliche Anforderungen
- Auslegeordnung der Lösungsvarianten
  - 2FA Kombinationsvarianten
  - Das Big Picture
- Vorgehensempfehlung

Über den Referenten

Martin Bruderer

Eidg. dipl. Experte in Organisationsmanagement

Strategischer Projektleiter EPD/eHealth
am Universitätsspital Basel

Teilprojektleiter Prozesse & Services
für die Stammgemeinschaft NW

Kontakt
Tel: +41 79 659 71 22 / +41 61 328 53 65
E-Mail: martin.bruderer@usb.ch

2-Faktor Authentifizierung am USB

Hybride Authentifizierungslösung für den EPD-Zugang

Bei der aktuellen Lösung im USB wird der erste Faktor intern vom USB und der zweite Faktor extern vom HIN IdP geprüft:

- Als erster Faktor dient der Login am Arbeitsplatz (Active Directory) mittels AD-Passwort bzw. RFID-Smartcard.
- Als zweiter Faktor wird vom HIN Identity Provider ein Einmalpasswort überprüft, das dem Benutzer vorgängig als SMS Textnachricht zugestellt wurde (sog. mTAN Verfahren).
- Für die Weitergabe des AD Login an den Identity Provider wird der innerhalb des USB Netzwerk betriebene HIN Access Gateway (AGW) verwendet.

2-Faktor Authentifizierung am USB

Beurteilung «Benutzbarkeit»

Stärken von mTAN

+ Das mTAN-Verfahren ist heute weit verbreitet und die Handhabung bei den meisten Benutzern entsprechend gut «eintrainiert».
+ Es wird weder ein zusätzliches Token noch eine zusätzliche Software (App) spezifisch für das EPD benötigt.
+ Einfaches Credentials Management (= Telefonnummernverwaltung)
+ Portierung der SIM-Karte bei Gerätewechsel ist ein gut etablierter Prozess

Schwächen von mTAN

- Nicht alle GFP / HIP wollen dieses für berufliche Zwecke nutzen, vor allem, was die HIN-APP der Video-Identifikation betrifft
- GSM-Funkverbindung ist nicht überall sichergestellt
- Zustellung des Einmalpasswortes als SMS kann (vor allem im Grenzgebiet) lange dauern oder fehlschlagen
- Langfristig fallen erhebliche Kosten für den SMS-Versand an

Weiteres Vorgehen am USB

- Einstieg bei zertifizierter Axsana/HIN voraussichtlich mit mTAN.
  - Wechsel auf langfristig sicheres und user-freundliches Verfahren braucht mind. 2 Jahre
- Aus Gründen der Benutzbarkeit und Sicherheit soll mittelfristig ein alternatives Authentifizierungsverfahren für GFP / HIP implementiert werden.
- Neben der Sicherheit und den Kosten muss bei der Lösungssuche insbesondere die Benutzbarkeit im klinischen Alltag betrachtet werden.
- Für GFP und HIP am USB ist eine Lösung unter Einbezug der lokalen Komponenten (insb. Active Directory) vorteilhaft.
- Als langfristige Investition in die Sicherheit soll die Lösung nebst dem EPD auch andere absehbare Anwendungsfälle berücksichtigen.

Weiteres Vorgehen am USB

- Es soll mittelfristig ein nachhaltig sicheres und spitaltaugliches Authentifizierungsverfahren für GFP und HIP implementiert werden.

- Hinweis: auch Admin-Personal (EPD-Admin-Portale) unterliegen den EPD-Anforderungen einer 2F-Authentifizierung. Die Smartphone-Akzeptanz ist hier sehr gering.

- Es gibt hierfür (zu) viele Möglichkeiten

⇨ Orientierung tut Not!

Über den Referenten

Thomas Kessler

Dipl. Physiker ETH
MAS ZFH in Business Administration

IT-Security Architekt, Partner
In der IT-Security tätig seit 1991

Spezialgebiete
Security Architecture and Strategy
Strong Authentiction
Identity Provider (IdP)

Kontakt
Tel: +41 79 508 25 43
E-Mail: thomas.kessler@temet.ch

Agenda

- 2-Faktor Authentifizierung am USB
  - Heutige Lösung
  - Vorgehensplan
- Gesetzliche Anforderungen
- Auslegeordnung der Lösungsvarianten
  - 2FA Kombinationsvarianten
  - Das Big Picture
- Vorgehensempfehlung

2-Faktor Authentifizierung (2FA)

Eine Definition

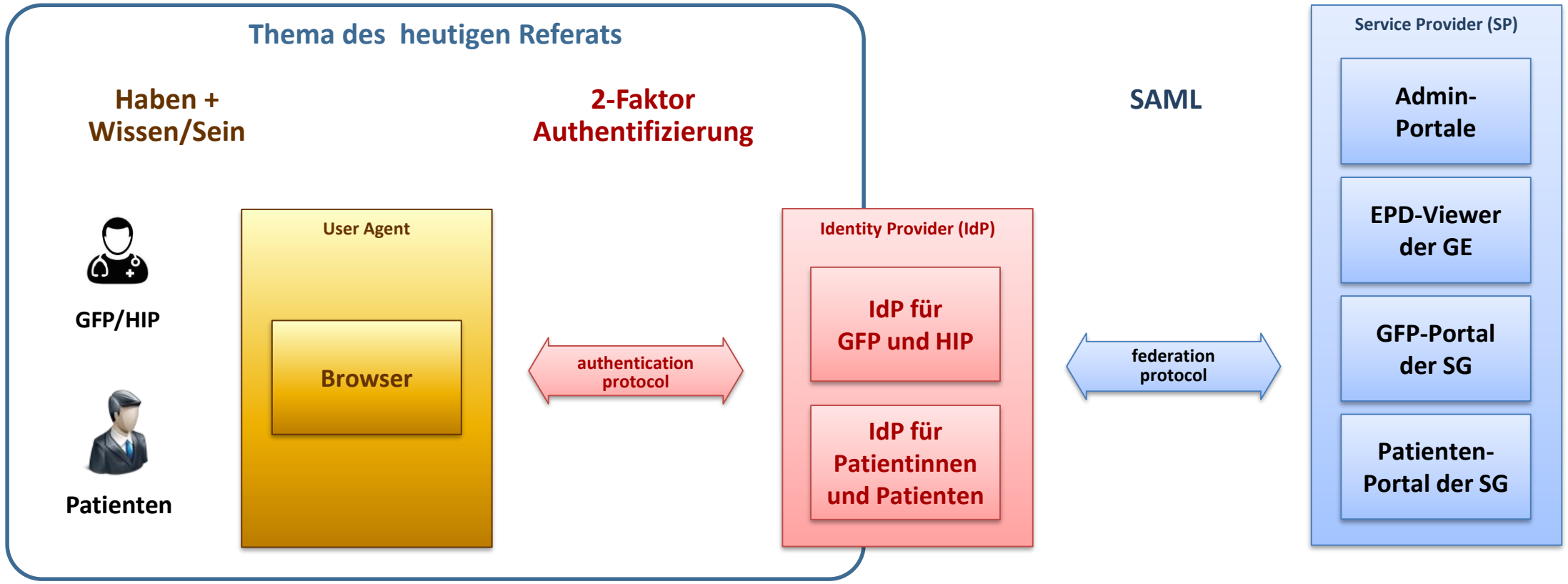
- Die Benutzerauthentifizierung gewährleistet eine sichere Identifikation der Systembenutzer zur Laufzeit.
  - Andere Sicherheitsservices wie Zugriffskontrolle und Audit Trail vertrauen darauf.

- 2-Faktor Authentifizierung (2FA) bezeichnet Verfahren, die einen Faktor „Haben“ mit einem Faktor „Wissen“ (Passwort oder PIN) oder einem Faktor „Sein“ (Biometrie) kombinieren.
  - Der Faktor „Haben“ wird in jedem Fall benötigt, wobei es sich hierbei um Hardware oder Software 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; Letzteres wird im Folgenden als PIN oder Token-PIN bezeichnet.

2FA im EPD

High Level Architektur

Das EPD Ausführungsrecht sieht einen zertifizierten Herausgeber der Identifikationsmittel (IdP) sowie eine 2-Faktor Authentifizierung vor



Gesetzliche Grundlagen (1/3)

Die TOZ verweisen bezüglich der Authentifizierung von Gesundheitsfachpersonen und Patienten auf die Verordnung:

1.4 Identifizierung und Authentifizierung (Art. 9 Abs. 2 Bst. e EPDV)

1.4.1 Gesundheitsfachpersonen müssen sich für den Zugriff auf das elektronische Patientendossier mit gültigen Identifikationsmitteln authentifizieren, die von einem nach Artikel 31 EPDV zertifizierten Herausgeber herausgegeben wurden.

8.3 Identifikation und Authentifizierung beim Zugriff (Art. 17 Abs. 1 Bst. c EPDV)

8.3.1 Patientinnen und Patienten müssen sich für den Zugriff auf das elektronische Patientendossier mit gültigen Identifikationsmitteln authentifizieren, die von einem nach Artikel 31 EPDV zertifizierten Herausgeber herausgegeben wurden.

Gesetzliche Grundlagen (2/3)

Die Verordnung verlangt explizit eine 2-Faktor Authentifizierung und verweist wiederum auf den internationalen Standard ISO/IEC 29115

4. Kapitel: Identifikationsmittel

Art. 23 Anforderungen

Das Identifikationsmittel muss:

a. der Vertrauensstufe 3 der Norm ISO/IEC 29115:2013(E)[3] entsprechen;

b. so aufgebaut sein, dass es nur von der berechtigten Person verwendet werden kann;

c. ein Authentifizierungsverfahren nach dem aktuellen Stand der Technik mit mindestens zwei Authentifizierungsfaktoren verwenden; und

d. eine Gültigkeitsdauer von höchstens fünf Jahren aufweisen.

Gesetzliche Grundlagen (3/3)

ISO/IEC 29115:2013(E) stellt keine spezifischen Anforderungen an die technische Ausprägung des Haben-Faktors:

6.3 Level of assurance 3 (LoA3)

At LoA3, there is high confidence in the claimed or asserted identity of the entity. This LoA is used where substantial risk is associated with erroneous authentication. This LoA shall employ multifactor authentication. Any secret information exchanged in authentication protocols shall be cryptographically protected in transit

---

1 LoA is a function of the processes, management activities, and technical controls that have been implemented by a CSP for each of the EAAF phases based on the criteria set forth in Clause 10.

and at rest (although LoA3 does not require the use of a cryptographic-based challenge-response protocol). There are no requirements concerning the generation or storage of credentials; they may be stored or generated in general purpose computers or in special purpose hardware.

Hinweis:

ISO/IEC 29115:2013(E) sieht auch einen noch höherwertigen LoA4 vor, der einen sicheren Hardware-Schlüsselspeicher verlangt.

Agenda

- 2-Faktor Authentifizierung am USB
  - Heutige Lösung
  - Vorgehensplan
- Gesetzliche Anforderungen
- Auslegeordnung der Lösungsvarianten
  - 2FA Kombinationsvarianten
  - Das Big Picture
- Vorgehensempfehlung

Pro Memoria

Eine Definition

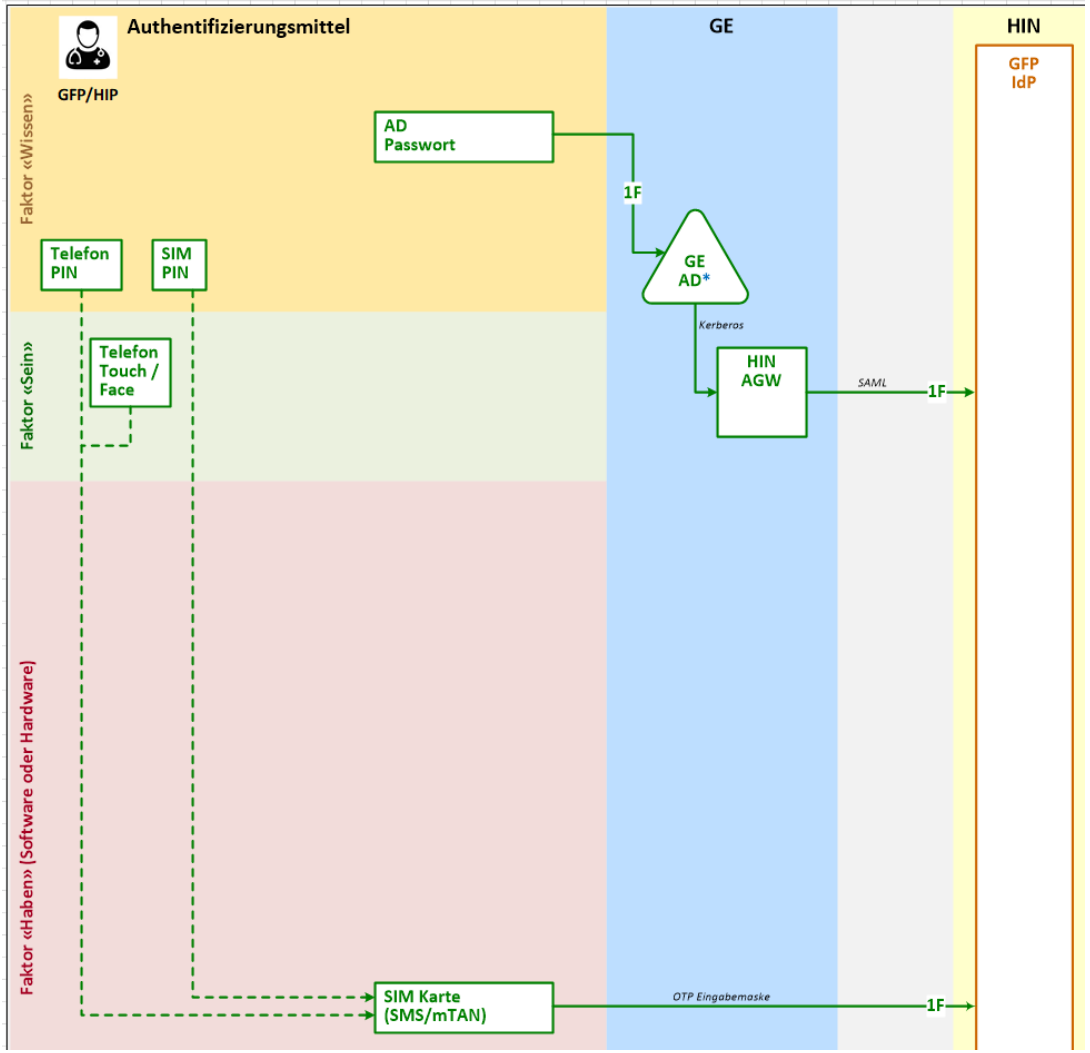
- 2-Faktor Authentifizierung (2FA) bezeichnet Verfahren, die einen Faktor „Haben“ mit einem Faktor „Wissen“ (Passwort oder PIN) oder einem Faktor „Sein“ (Biometrie) kombinieren.

- Es gibt verschiedenste Kombinationsmöglichkeiten!
- Nicht alle (aber viele) sind heute auf dem Markt relevant

mTAN hat den Zenit überschritten

Marktentwicklung (1/6)

- Angriffe auf Telefongeräte und GSM-Netzwerke werden laufend einfacher und häufiger.
- Banken ersetzen oder ergänzen mTAN zunehmend mit anderen Verfahren (insb. Apps aller Art).
- NIST SP 800-63-3b (Digital Identity Guidelines) setzte mTAN im Juni 2017 auf die „Watch List“:
  - Status RESTRICTED verlangt eine Alternative sowie einen Migrationsplan

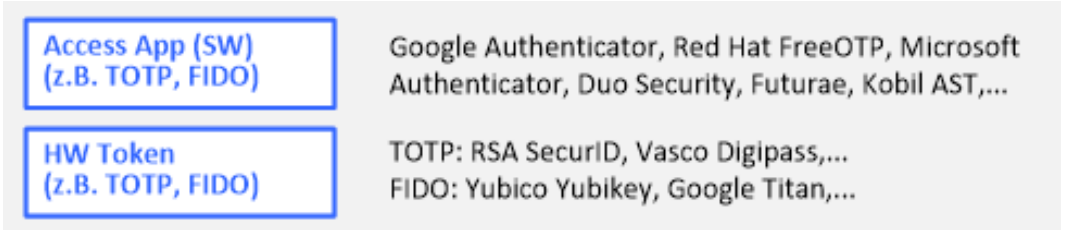


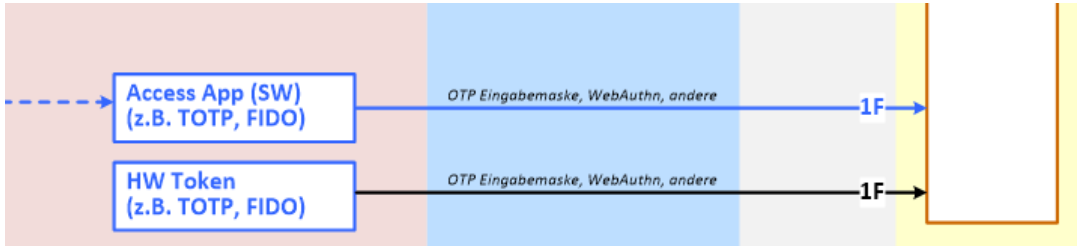
Access Apps spriessen, FIDO Token keimen

Marktentwicklung (2/6)

- Apps aller Art kämpfen um Marktanteile
  - OTP oder challenge-and-response
  - Offline oder Online
  - 2nd Channel oder in-Channel
  - Separat oder über SDK integriert
  - Nutzen diverse Sensoren
- Auch der Markt für HW-Token ist wieder in Bewegung
  - Proprietäre OTP-Generatoren haben Mühe
  - FIDO Token drängen auf den Markt und trumpfen mit Malware-Resistenz

- Apps und HW-Token gelten in der Regel als ein Faktor (1F)

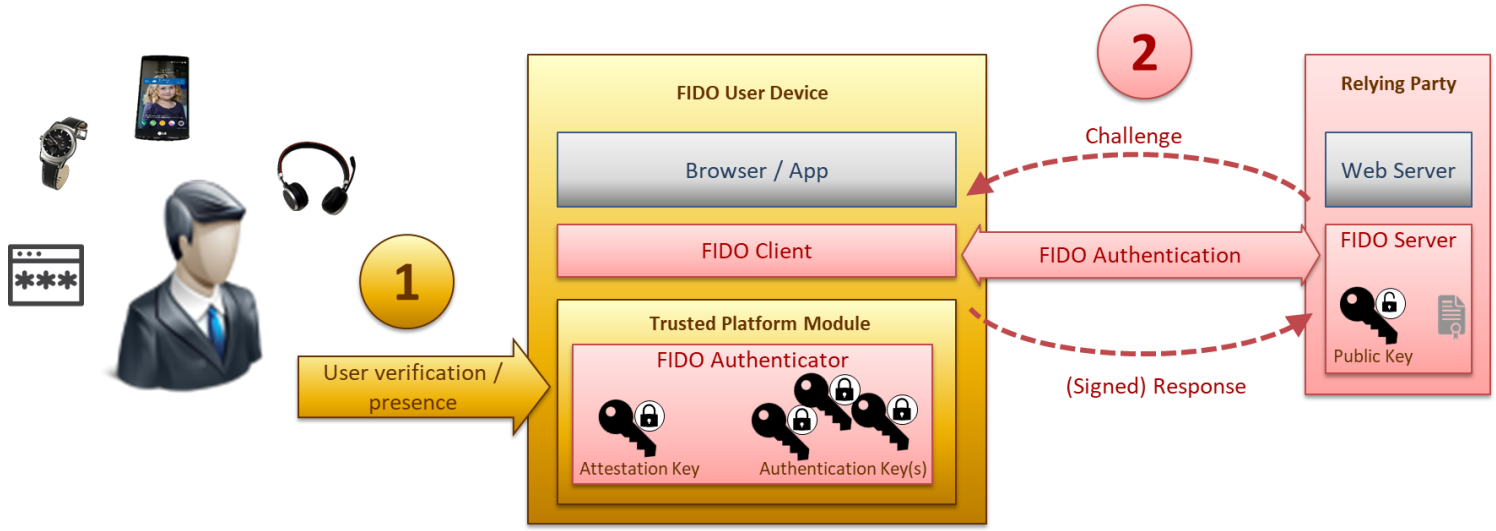




FIDO als Game Changer im Hintergrund

Marktentwicklung (3/6)

- Mit FIDO 2 (Fast Identity Online) ist seit 2018 ein breit abgestützter Industriestandard für die Authentifizierung verfügbar.
- FIDO 2 basiert auf Public Key Kryptographie, kommt aber ohne eine zentrale Certification Authority (CA) aus.



FIDO UAF:

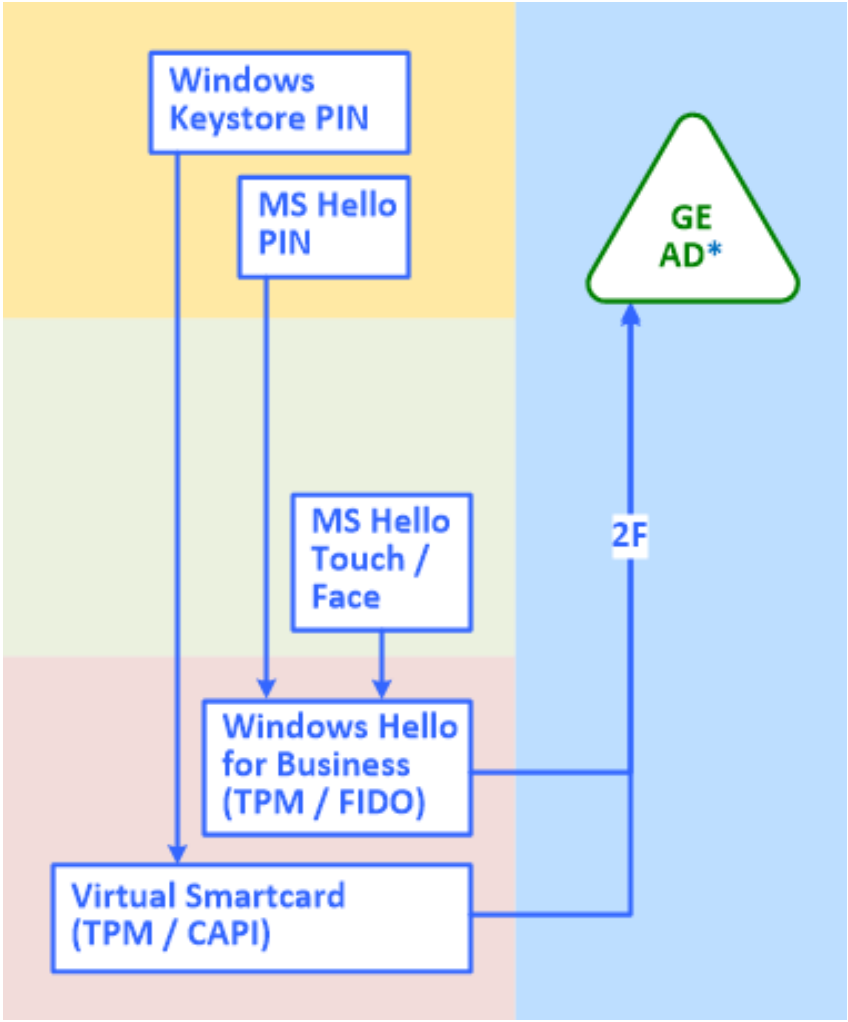
Der Benutzer wird mittels PIN, Biometrie, Wearables oder Sensorik authentifiziert

Der aktivierte private Schlüssel wird für die Authentifizierung gegenüber dem FIDO Server genutzt.

«Windows Hello for Business»

Marktentwicklung (4/6)

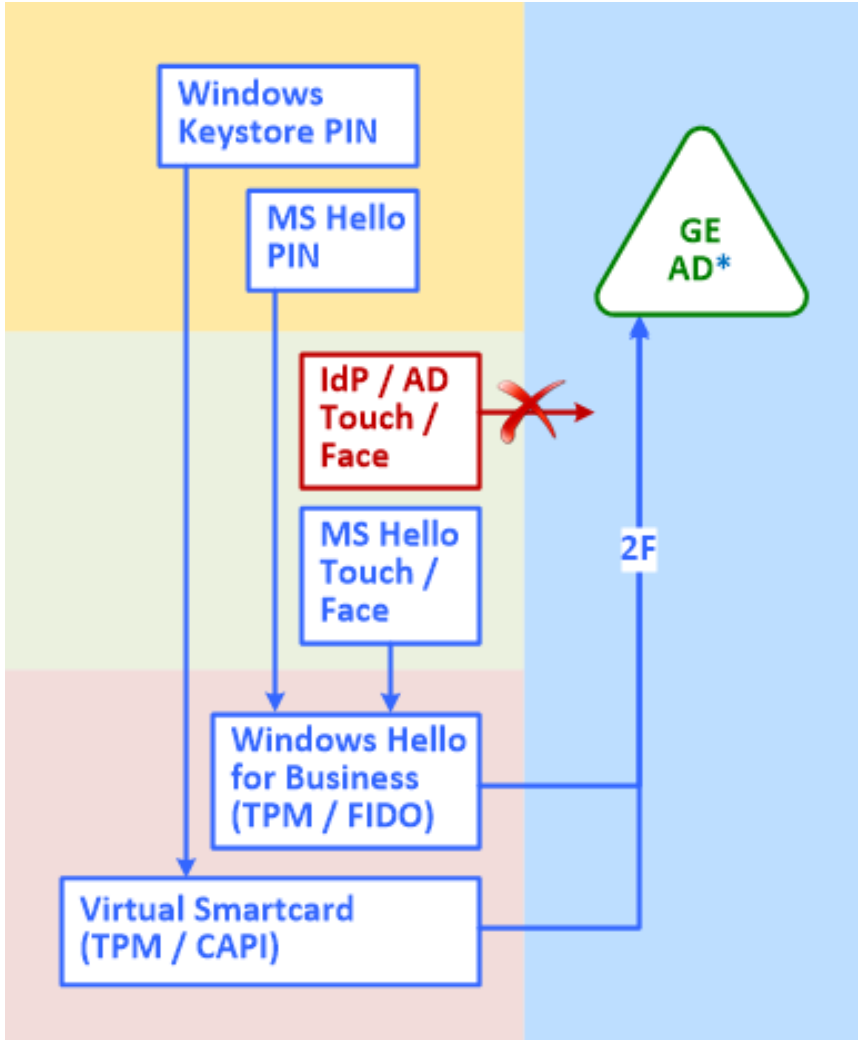
- Windows Hello for Business ist die Microsoft Implementierung von FIDO 2
  - Windows 10 Arbeitsplatz als FIDO Client, AD Domänenkontroller als FIDO Server
  - Weiterentwicklung der Virtual Smartcard mit klassischer PKI
- Der private Schlüssel ist im Trusted Platform Module (TPM) auf dem Gerät gespeichert
- Die Aktivierung basiert auf Biometrie und/oder einem PIN (als Fallback immer vorhanden)



«Passwordless Authentication»

Marktentwicklung (5/6)

- Passwordless Authentication meint Ersatz des PIN durch Biometrie.
- Biometrische Muster sollten nur dezentral im persönlichen Authenticator gespeichert werden
- Qualität moderner Sensoren kann sich mit der Qualität typischer PIN messen
  - Ist nicht Schwarz/Weiss
- Interessantes Projekt in diesem Zusammenhang: NIST SOFA-B
  - https://pages.nist.gov/SOFA/



«Outbound Federation»

Marktentwicklung (6/6)

- Die zunehmende Nutzung von extern betriebenen Services (Cloud) verlangt nach Outbound Federation Services
  - Ein „Mitarbeiter-IdP" ermöglicht sicheren Single SignOn für Cloud-Dienste
  - SAML und OpenID Connect (OIDC) als Standardprotokolle
  - AD Federation Services (ADFS) oder spezialisierte Produkte wie Ping Identity
- Der Mitarbeiter-IdP kann selber ebenfalls als Cloud Service bezogen werden (Identity as a Service, IDaaS)
- Konsequenz: Mittels 2-Faktor Authentifizierung abgesicherte Zugänge in der Art des EPD sind der zukünftige Normalfall!
  - Es ist deshalb wichtig, die Weichen heute richtig zu stellen.

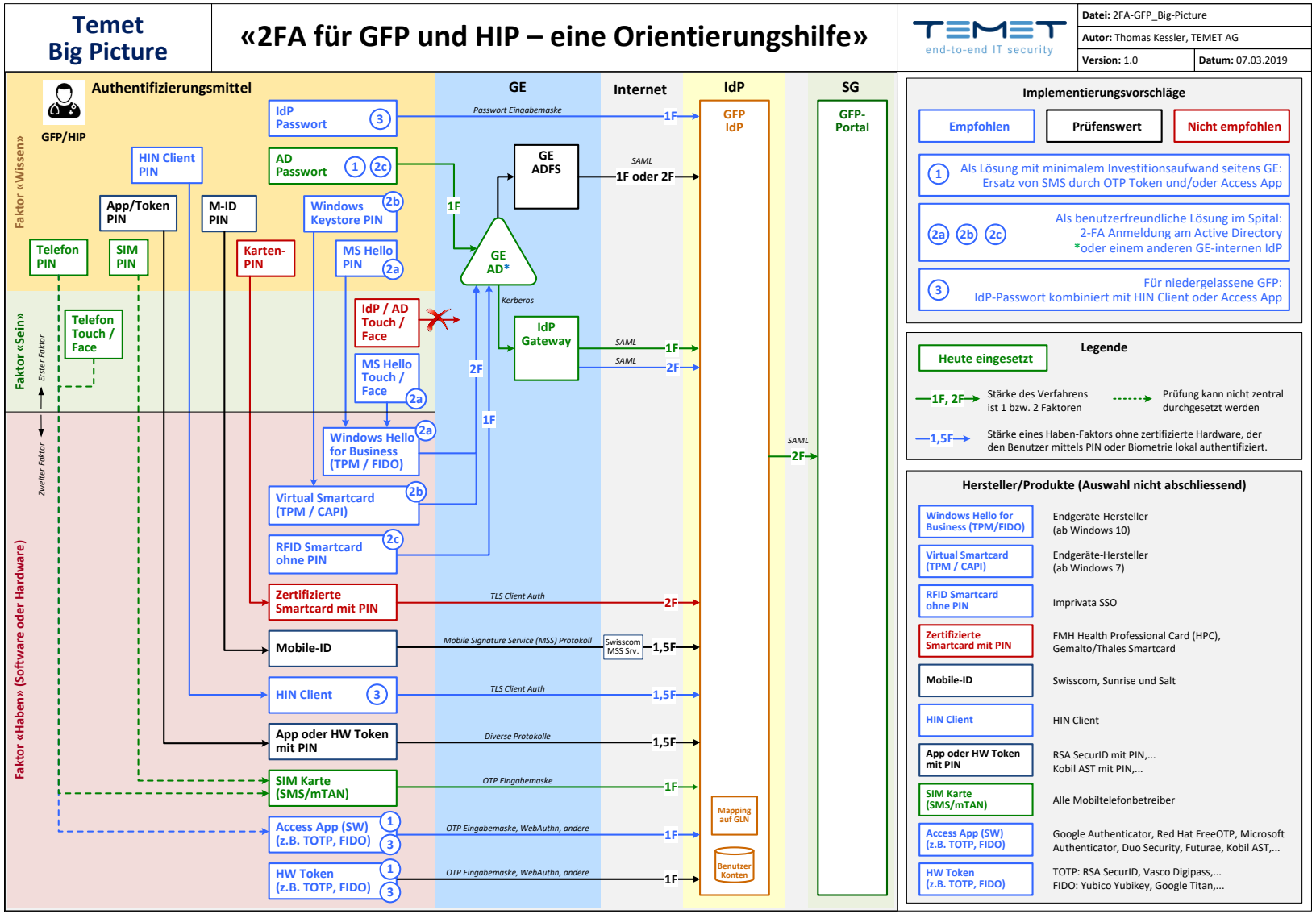
Was sonst noch so läuft

Marktentwicklung (7/6)

- Die klassische Smartcard hat (nur) für firmeninterne Nutzung nach wie vor ihren Platz
  - Kombinierbar mit dem Zutrittsbadge und gut geeignet für Shared Desktops
- Bei diversen Spitälern sind Smartcards mit RFID-Schnittstelle ohne PIN im Einsatz. Banken und Behörden verwenden typischerweise Smartcards mit Kontaktschnittstelle und PIN.

- Swisscom, Sunrise und Salt haben für die Nachfolge von mTAN mit der Mobile-ID ebenfalls ein Pferd im Stall.
  - Mobile-ID basiert auf dem internationalen Mobile Signature Service (MSS) Standard
  - Mobile-ID basiert auf der SIM-Karte und kann als Hardware-Token betrachtet werden
  - Mobile-ID verwendet die Mobiltelefonnummer, was die Migration von mTAN vereinfacht

Das Big Picture



Hinweise:

- Haben-Faktoren ohne zertifizierte Hardware, die den Benutzer mittels PIN oder Biometrie lokal authentifizieren, sind mit dem Faktor 1,5 bewertet.
- Eine gestrichelte Linie bedeutet, dass die lokale Authentifizierung nicht technisch durchsetzbar ist.
- Die Weitergabe der Identität vom AD an den HIN IdP hat, je nach verwendetem Verfahren, die Stärke von einem oder zwei Faktoren (1F oder 2F).

Agenda

- 2-Faktor Authentifizierung am USB
  - Heutige Lösung
  - Vorgehensplan
- Gesetzliche Anforderungen
- Auslegeordnung der Lösungsvarianten
  - 2FA Kombinationsvarianten
  - Das Big Picture
- Vorgehensempfehlung

Strategische Empfehlung

- Das mTAN Verfahren wird durch mehrere Verfahren ersetzt.
  - Die Identity Provider (IdP) bieten gesetzeskonforme Alternativen zu mTAN an
  - Jede Gesundheitseinrichtung kann das für sie passende Angebot auswählen
- Es werden unterschiedliche Lösungen für die folgenden drei Anwendungsfälle angeboten:
  - Eine Lösung mit minimalem Investitionsaufwand seitens der GE
  - Eine maximal benutzerfreundliche Lösung mit Single SignOn im Spital
  - Eine Lösung speziell für niedergelassene Gesundheitsfachpersonen
- Die Zertifizierbarkeit aller drei Lösungen wird in Abstimmung mit BAG (Schema-Owner), den IdP-Zertifizierern und den IdP sichergestellt.
  - Formulieren der technischen und organisatorischen Anforderungen an die GE-seitigen Komponenten (insb. Active Directory) und Prozesse (insb. Token-Verwaltung und initiale Verknüpfung von GE-Identifikator und IdP-Identität).

Stossrichtung 1

Lösung mit minimalem Investitionsaufwand seitens der GE

- 1:1 Ersatz von SMS durch ein OTP-Token und/oder eine Access-App.
  - Werden sowohl ein OTP-Token als auch eine Access-App unterstützt, dann können Benutzer mit und ohne Smartphone optimal bedient werden.
  - Es steht eine Vielzahl von Produkten zur Auswahl. Bekannte Beispiele sind das Vasco Digipass OTP-Token oder die Google Authenticator Access-App.
  - Die Benutzbarkeit im klinischen Alltag ist ein wichtiges Evaluationskriterium.
- Evaluation und Realisierung der Lösung erfolgt in einem gemeinsamen Vorhaben mit den IdP unter Führung der Stammgemeinschaften.
- Die Verwaltungsprozesse für OTP-Token und Access-App werden von den IdP vorgegeben, passend auf den klinischen Alltag bei Spitälern.

Stossrichtung 2

Maximal benutzerfreundliche Lösung mit Single SignOn im Spital:

- 2-Faktor Authentifizierung gegenüber dem Active Directory des Spitals
  - Jedes Spital kann die passende 2FA-Lösung selber evaluieren. Diese kann neben dem EPD-Zugang auch für GE-interne Zwecke genutzt werden.
  - Es gibt hierfür verschiedene Lösungsansätze wie beispielsweise Windows Hello for Business, Microsoft Virtual Smartcard oder Imprivata SSO mit RFID-Smartcard.
- Es werden Spielregeln für die Anbindung an die IdP definiert.
  - Festlegen der Verantwortlichkeiten von IdP und Gesundheitseinrichtung
  - Protokoll für die Föderierung der authentifizierten AD-Identität an den IdP (z.B. SAML)
  - Technische und organisatorische Anforderungen an das 2FA-Verfahren im Spital, damit die Bedingungen der IdP-Zertifizierung nach EPDG jederzeit erfüllt sind.
- Die Verwaltungsprozesse für die 2FA-Anmeldung am AD werden von jedem Spital selber definiert und umgesetzt.

Stossrichtung 3

Lösung für niedergelassene Gesundheitsfachpersonen:

- 2-Faktor Authentifizierung gegenüber dem IdP beispielsweise mittels einem weit verbreiteten IdP-Client mit zusätzlichem IdP-Passwort
- Die Verwaltungsprozesse für den IdP-Client und das IdP-Passwort werden vom IdP definiert

Schlusswort

- Die vom EPDG Ausführungsrecht verlangte 2-Faktor Authentifizierung ist für Zugriffe auf sensible extern betriebene Services angemessen.
- Der Markt bietet heute eine verwirrend grosse und zukünftig weiter wachsende Auswahl von Möglichkeiten.
- Es ist wichtig, pro Anwendungsfall die richtige Lösung zu wählen!

- Für Spitäler und andere grössere Gesundheitseinrichtungen ist die interne 2-Faktor Authentifizierung mit Föderierung zu Handen eines EPDG-zertifizierten IdP eine sichere, benutzerfreundliche und langfristig nachhaltige Option.

… zum Erfolg

Besten Dank
für Ihre Aufmerksamkeit!

TEMET AG
Basteiplatz 5
8001 Zürich
044 302 24 42
info@temet.ch
www.temet.ch