2FA für die Authentifizierung von GFP: Am EPD und in der Cloud

Swiss eHealth Forum 2020

Solution Präsentation Fr 15:15 – 15:45

Thomas Kessler, IT-Security Architekt, TEMET AG

06.03.2020

Agenda

- Einführung in das Thema 2-Faktor Authentifizierung (2FA)
  - Grundmodell für die 2FA Implementierung
  - Anforderungen
- 2FA im Spital: Architekturvarianten
  - Variante 1: „Interne Lösung“
  - Variante 2: „Hybridlösung“
  - Variante 3: „Gateway-Lösung“
  - Variante 4: „IdP-Lösung“
- Zielarchitektur und Umsetzung in Etappen

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

Über die TEMET AG

Die TEMET AG positioniert sich im Markt als unabhängige und auf Security fokussierte Firma, deren Berater fachliche Expertise mit Management und Projektkompetenz verbinden.

2FA Referenzprojekte (seit 1993)

- 2019, Spital: 2FA Grobkonzept für EPD und Cloud
- 2018, Krankenversicherer: 2FA für Privileged Access (PAM)
- 2018, Bank: IAM Federation Services Zielarchitektur und RFI
- 2014, Bank: Studie ID-Verfahren für eBanking Kunden
- 2012, Bundesamt: 2FA am Arbeitsplatz (Smartcard)
- 2011, Bundesamt: 2FA ohne Vorinstallation (mTAN)
- 2008-2011, Versicherer: Architekt und Projektleiter „BrokerGate IdP“ (mTAN, OTP-Token und SuisseID)
- 1997, Bank: Teilprojektleiter 2FA-Lösung für erstes E-Banking
- 1993-1995, Bank: PL Bank-interne Einführung von OTP-Token

EPD Referenzprojekte (seit 2015)

- Seit 2018 unterstützt die Temet vier grosse Häuser in allen DSDS-Aspekten der EPD-Anbindung (inkl. IAM-Integration)
- 2019/2020, Stammgemeinschaft: Projektleiter für die Zertifizierung
- 2019, eHS: Umsetzungshilfe „Funktionsabnahmen“
- *2019, Spital: Grobkonzept für die 2-Faktor Authentifizierung von GFP
- *2018, myEPD: DSDS-Verantwortlicher für den myEPD Pilotbetrieb
- *2017, USB: Sicherheitsreview myEPD-Anbindungskonzept
- *2016, eHealth NWCH: AKV für die Informationssicherheit im EPD
- *2015, BAG: Bedrohungs- und Risikoanalyse für das EPD

*: Öffentlich vorgestellte Projekte anlässlich der eHealth Foren 2016/2017/2018/2019/2020

Glossar vorab

Abkürzung	Bedeutung
2FA	2-Faktor Authentifizierung; Faktoren «Wissen» oder «Sein» + «Haben»
AD	Microsoft Active Directory; Regelt den Login am Windows Arbeitsplatz
ADFS	AD Federation Service; ins AD integrierter IdP
EPD	Elektronisches Patientendossier nach EPD-Gesetz
GE	Gesundheitseinrichtung, z.B. ein Spital, ein Heim oder eine Arztpraxis
GFP	Gesundheitsfachperson, z.B. ein Arzt oder ein Apotheker
IAM	Identity and Access Management; Benutzer- und Berechtigungsverwaltung
IdP	Identity Provider; Herausgeber von Identifikationsmitteln
OTP	One-Time Passwort; Einmalpasswort, generiert von einem HW- oder SW-Token
SAML	Security Assertion Markup Language; Protokoll für die Identitätsweitergabe

Identity and Access Management (IAM)

Einführung 2FA (1/4)

Die Hauptaufgaben des IAM sind:

- Die Verwaltung der Benutzer mit ihren Berechtigungen
- Die Authentifizierung und Zugriffskontrolle zur Laufzeit

Das IAM ist eine tragende Säule der Informationssicherheit und muss *Effizienz*, *Sicherheit* und *Benutzerfreundlichkeit* unter einen Hut bringen.

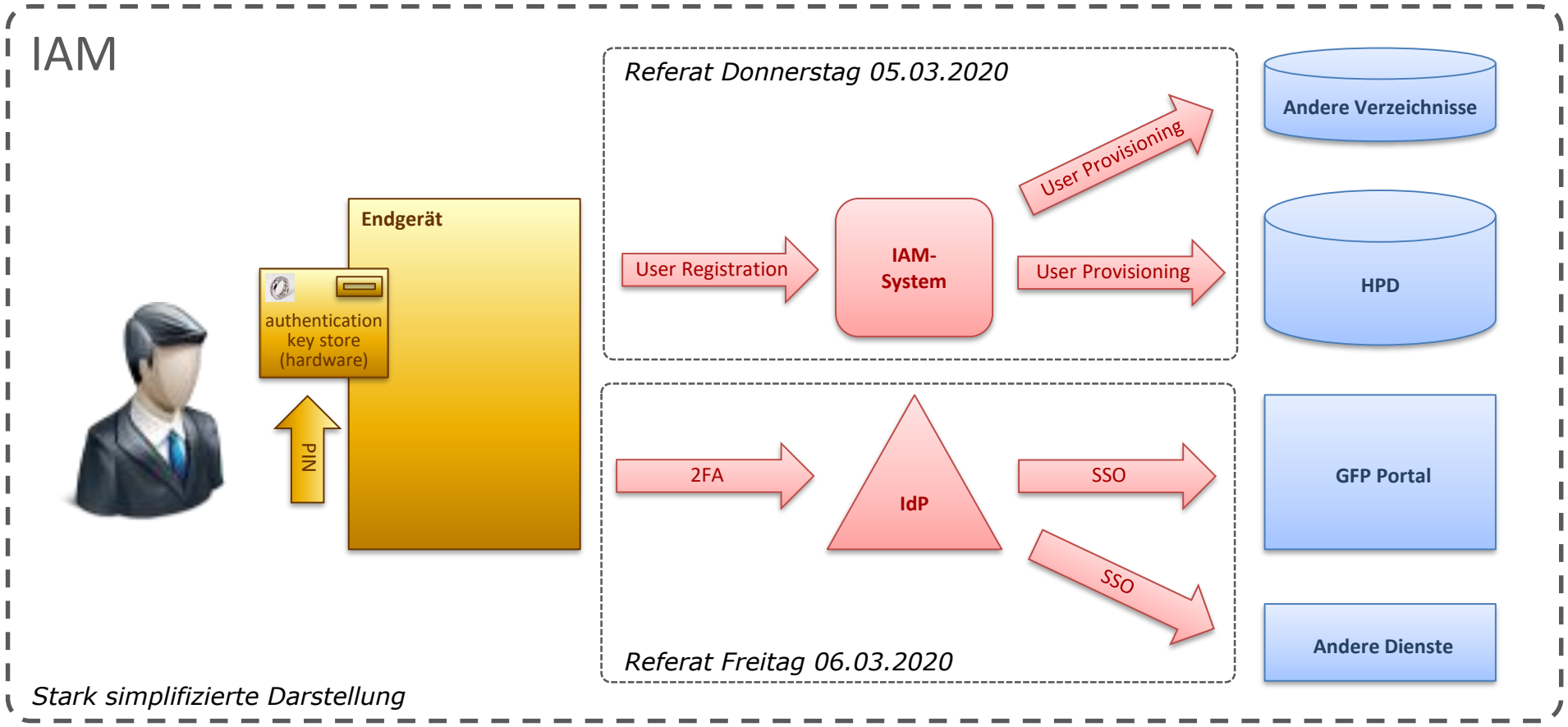
Das IAM muss die Entwicklung der IT-Landschaft unterstützen; aktuell insb. firmenübergreifende Geschäftsprozesse und Cloud-Services.

⇨ Das *EPD als Vorbild* für die sichere Nutzung externer Dienste (*!?!*)

Zwei Themen – zwei Referate

Einführung 2FA (2/4)

Die *IAM-Infrastruktur* ermöglicht sichere und effiziente Prozesse:



2-Faktor Authentifizierung (2FA)

Einführung 2FA (3/4)

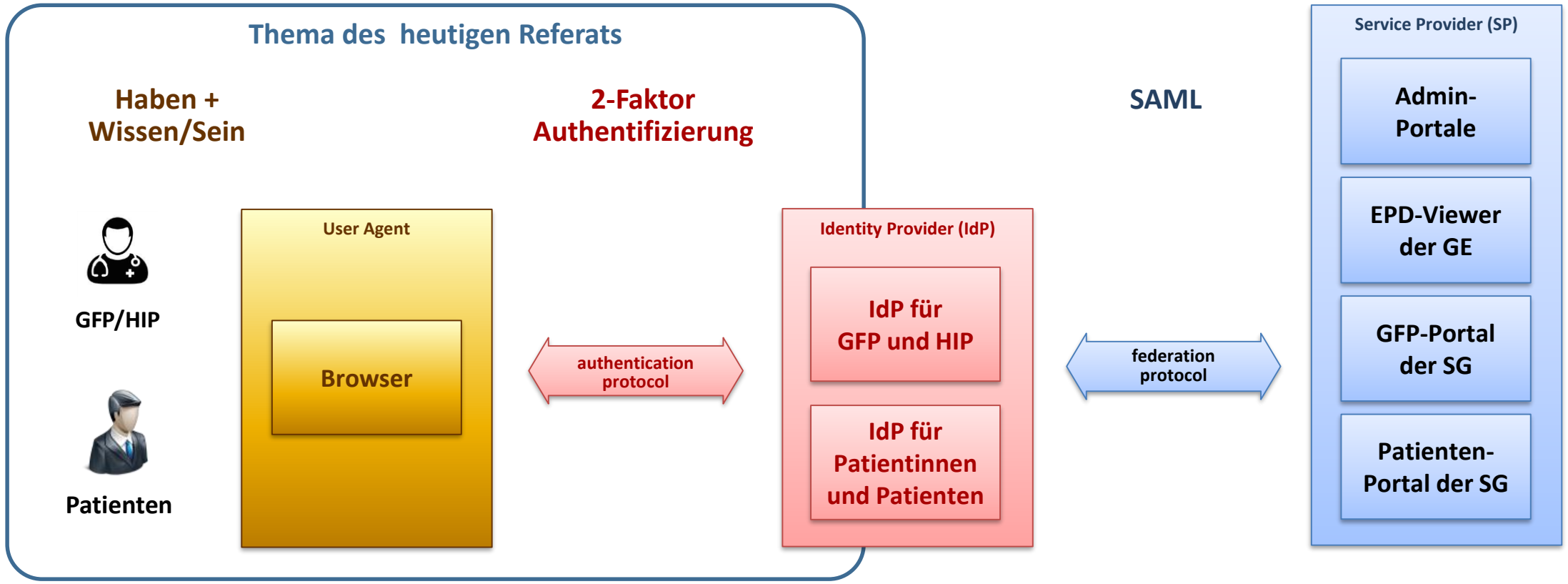
- Die Benutzerauthentifizierung gewährleistet eine sichere Identifikation der Benutzer zur Laufzeit.
  - Andere Sicherheitsservices wie Zugriffskontrolle und Audit Trail vertrauen darauf.

- 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 oft als PIN oder Token-PIN bezeichnet.

Anforderungen des EPD

Einführung 2FA (4/4)

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

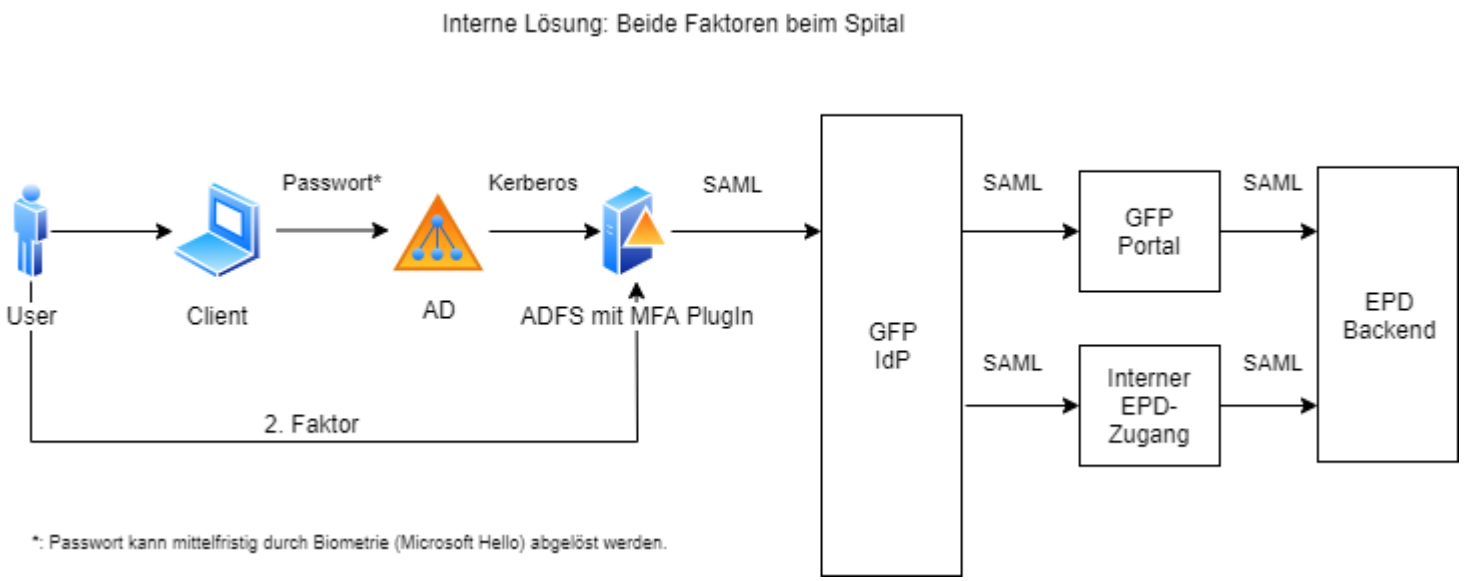


Anforderungen des Spitals

- Das Spital muss eine 2-Faktor Authentifizierung von GFP und HIP für den Zugriff auf das EPD implementieren.
  - Initial zwei Service Provider (GFP-Portal + Interner EPD-Zugang), wenige Benutzer
  - Die Lösung muss nach EPDG zertifizierbar sein
- Das Spital beabsichtigt, diese Lösung nicht nur für das EPD einzuführen sondern zukünftig generell im Spital zu nutzen.
  - Langfristig viele Service Provider und mehrere tausend Benutzer
- Zukünftige weitere Anwendungsfälle sind insbesondere extern betriebene Anwendungen (Cloud Lösungen) aller Art:
  - Infrastrukturanwendungen (z.B. Signing Service)
  - Fachanwendungen einzelner Kliniken

Architekturvariante 1: Interne Lösung

Interne Lösung



- 1. Faktor ist der bestehende AD-Login
- 2. Faktor wird durch ADFS mit MFA-PlugIn geprüft
- Das Resultat wird von ADFS an den GFP-IdP übertragen

Beurteilung der Variante 1

Pro

- Basiert auf Standardkomponente ADFS (AD Federation Services)
- Einfache Nutzung von 2FA auch für Anwendungen ausserhalb EPD
- Breites Angebot 2FA-Verfahren
- Alleinige Kontrolle durch Spital, minimale Abhängigkeit vom IdP

Contra

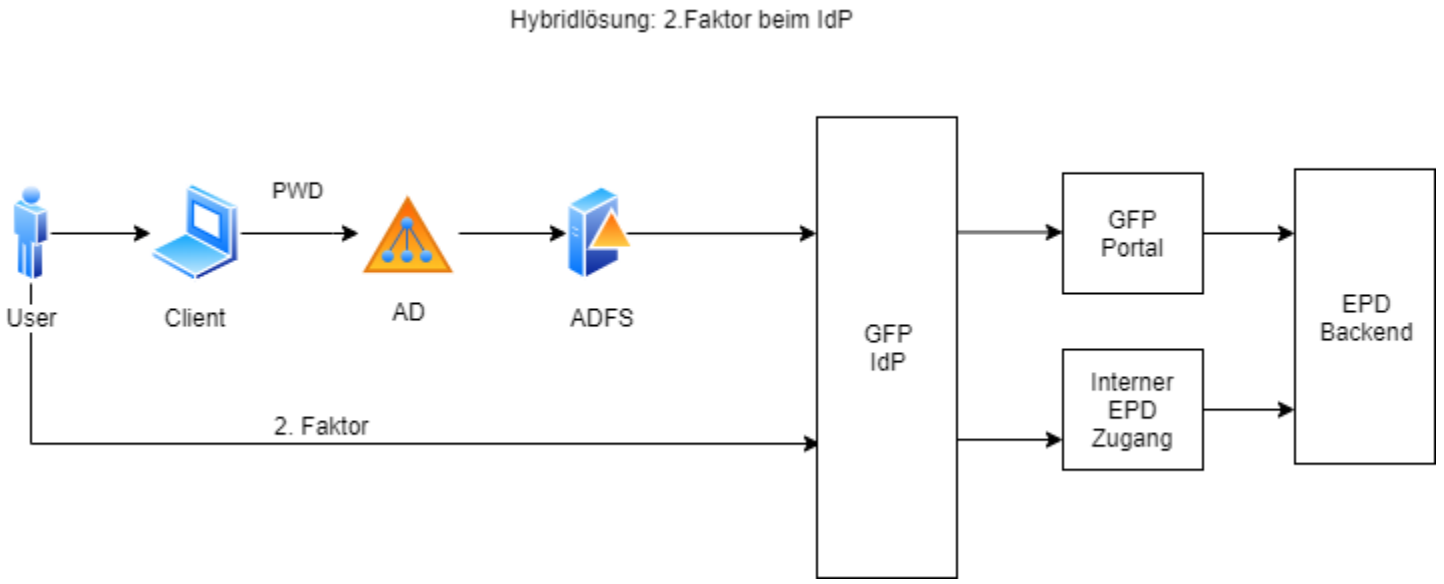
- Grosses EPD-Zertifizierungsrisiko (grosse Delta-Zertifizierung) und deshalb grosses Projektrisiko
- Höchste Kosten auf Grund des internen 2FA-Zusatzaufwandes bei geleichbleibenden IdP-Kosten («Bundle-Angebot»)

Allgemeines

- Betriebsrisiko, Stabilität und Sicherheit liegen vor allem in eigener Verantwortung; kann sowohl positiv als auch negativ beurteilt werden.

Architekturvariante 2: Hybridlösung

Hybridlösung



- 1. Faktor ist der bestehende AD-Login, der über ADFS an den GFP-IdP übertragen wird
- 2. Faktor wird durch den GFP-IdP geprüft

Beurteilung der Variante 2

Pro

- Nutzt Standardkomponente ADFS (AD Federation Services)
- Mittlere Erweiterbarkeit (ADFS kann auch ausserhalb des EPD als 1. Faktor genutzt werden)
- Minimaler interner Aufwand (ADFS ist so bereits in Betrieb)

Contra

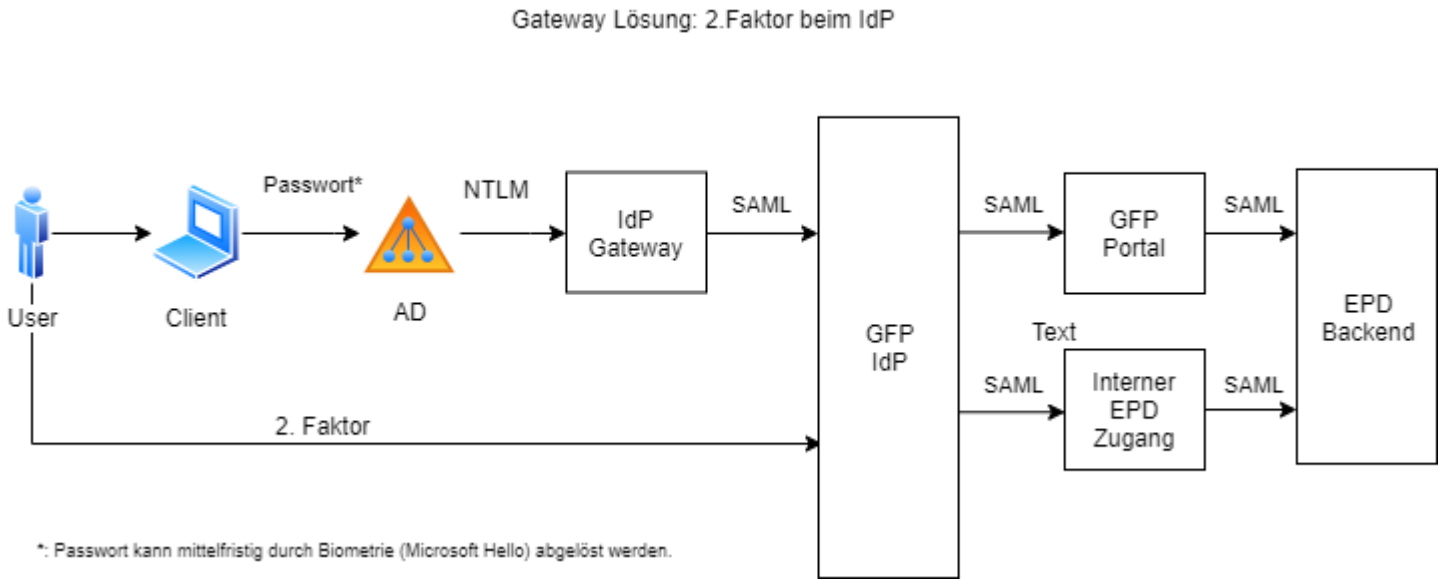
- Kleines EPD-Zertifizierungsrisiko (kleine Delta-Zertifizierung) und deshalb kleines Projektrisiko
- Abhängigkeit vom GFP-IdP bezüglich dem 2. Faktor und der Anbindung weiterer Service Provider ausserhalb EPD.

Allgemeines

- Höhere Komplexität durch geteilte Verantwortung für Betriebsrisiko, Stabilität und Sicherheit (1.Faktor: Intern; 2.Faktor GFP-IdP).

Architekturvariante 3: Gateway-Lösung

Gateway-Lösung



- 1. Faktor ist der bestehende AD-Login, der via den IdP-Gateway an den GFP-IdP übertragen wird
- 2. Faktor wird durch den GFP-IdP geprüft

Beurteilung der Variante 3

Pro

- Aktuell weit verbreitete Lösung
- Prozesse sind bereits weitgehend definiert und bei anderen erprobt, Prozessrisiko und Entwicklungs-aufwand entsprechend gering

Contra

Analog Variante 2 aber zusätzlich:

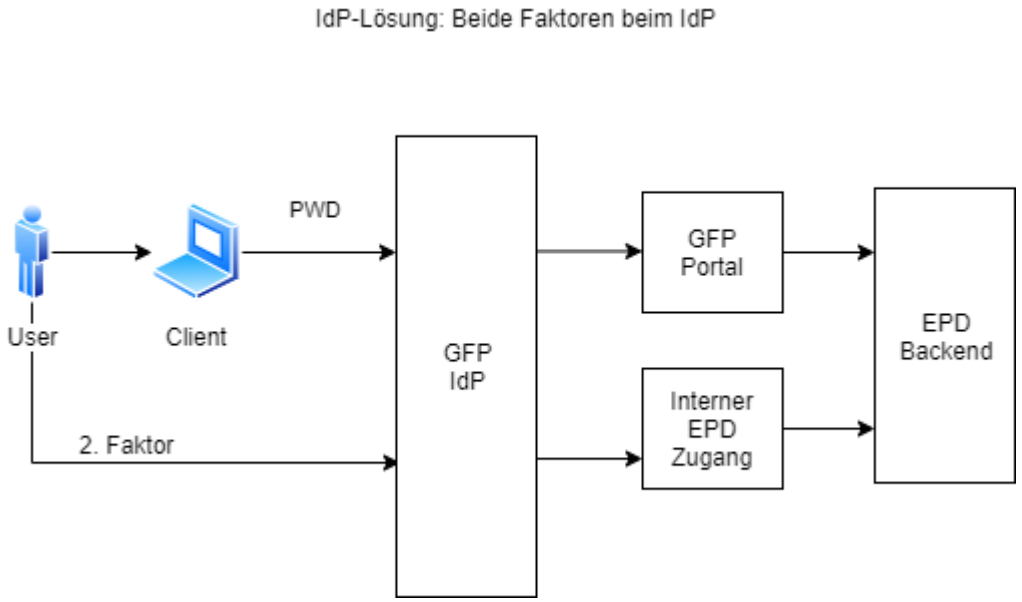
- Proprietäre Zusatzkomponente IdP-Gateway mit zusätzlichem Betriebsaufwand intern
- Eingeschränkte Erweiterbarkeit (Lösung kann nicht unabhängig vom IdP genutzt werden)

Allgemeines

- Betriebsrisiko, Stabilität und Sicherheit liegen hauptsächlich beim IdP (IdP-Gateway wird als Appliance zur Verfügung gestellt)

Architekturvariante 4: IdP-Lösung

IdP-Lösung



- GFP meldet sich mit einem extra Passwort und einem 2. Faktor beim GFP-IdP an

Beurteilung der Variante 4

Pro

- Kein EPD-Zertifizierungsrisiko (keine Delta-Zertifizierung) und deshalb kleines Projektrisiko

Contra

- Nicht benutzerfreundlich (zusätzliches Passwort)
- Hohe Abhängigkeit vom IdP
- Kaum wiederverwendbar für andere Services

Allgemeines

- Betriebsrisiko, Stabilität und Sicherheit liegen komplett beim IdP

Varianten 2FA-Verfahren*

TEMET
end-to-end IT security

Angebot ADFS

- TOTP (freeOTP, Google und MS Authenticator)
- Futurae App (inkl. SoundProof)
- Mobile-ID
- HW OTP-Token
- diverse weitere (siehe Link**)

Angebot ELCA/trustID

- mTAN (SMS)
- trustID App (mit PIN)
- TOTP-App (freeOTP, Google und Microsoft Authenticator)
- Matrixkarte

Angebot HIN

- mTAN (SMS)
- Futurae App (inkl. SoundProof)
- Hardware OTP-Token in Evaluation

*: Aktueller Kenntnisstand des Referenten

**: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-additional-authentication-methods-for-ad-fs

Beurteilungskriterien 2FA-Verfahren

TEMET
end-to-end IT security

Benutzbarkeit

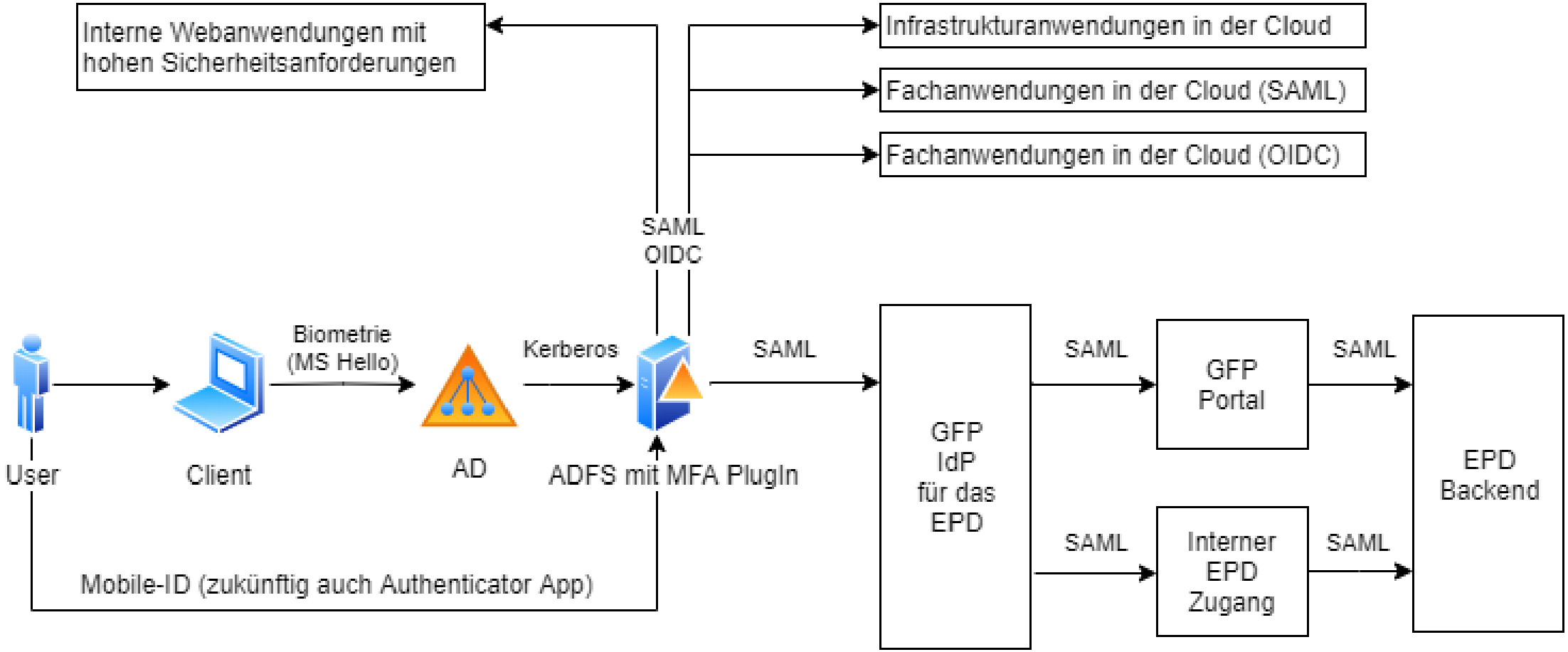
- Ist einfach in Betrieb zu nehmen
- Ist einfach zu benutzen
- Funktioniert überall zuverlässig
- Ist portabel bzw. „immer dabei“
- Funktioniert für mobilen Kanal
- Ist geräte- und kanalunabhängig
- Ist zukunftsorientiert und modern

Sicherheit

- Kann nicht kopiert werden
- Ist immun gegen Malware
- Resistent gegen klassisches Phishing
- Resistent gegen paralleles Phishing
- Resistent gegen man-in-the-network
- Resistent gegen man-in-the-client
- Von NIST nicht RESTRICTED

Zielarchitektur

Zielarchitektur 2FA für GFP im Spital



Umsetzung in Etappen

- Etappe 1: Implementieren IdP-Lösung (Variante 4)
  - Minimieren des EPD-Projektrisikos
  - Ist zumutbar, so lange die Anzahl von GFP und HIP mit EPD-Zugang klein ist
- Etappe 2: Migrieren auf Interne Lösung (Variante 1)
  - Ist strategisch am vorteilhaftesten, weil für die Anbindung interner und externer Fachanwendungen keine Abhängigkeit von einem externen GFP-IdP besteht;
  - Ist langfristig am kostengünstigsten, weil ADFS von vielen Cloud-Services out-of-the-box unterstützt wird;
  - Ist betrieblich am effizientesten, weil vorhandene Standardkomponenten genutzt werden;
  - Ist am benutzerfreundlichsten, weil zwischen einer grossen und ständig wachsenden Zahl von 2FA-Verfahren ausgewählt werden kann.
- Der Migrationszeitpunkt ist abhängig vom Erfolg des EPD und der Einführung anderer Cloud-Services.

Schlusswort / Aufruf

- Die für die EPD-Anbindung aufgebaute 2FA-Lösung soll generell im Spital nutzbar sein, auch für andere Cloud-Services!
- Eine GFP IdP-Lösung ist in der Anfangsphase OK, skaliert aber nicht und bietet zu wenig Flexibilität.

⇨ Damit das EPD nicht zum Verhinderer von 2FA-Lösungen im Spital wird, braucht es einen praktikablen Ansatz für die Zertifizierung einer Spital-internen 2FA-Lösung (Architekturvariante 1).

… zum Erfolg

Besten Dank
für Ihre Aufmerksamkeit!

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