TEMET
end-to-end IT security

EPD-Anbindung des USB Implementierung wichtiger Use Cases

Swiss eHealth Forum 2018

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

08.03.2018

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

Agenda

- Einleitung
  - Ziele
  - Termine und Vorgehen
  - Systemübersicht
- Implementierung ausgewählter Use Cases
  - Use Cases Übersicht
  - Patientendossier eröffnen
  - EPD schreiben
  - Gesundheitsfachpersonen und Hilfspersonen registrieren
  - EPD lesen
- (Noch) offene Punkte

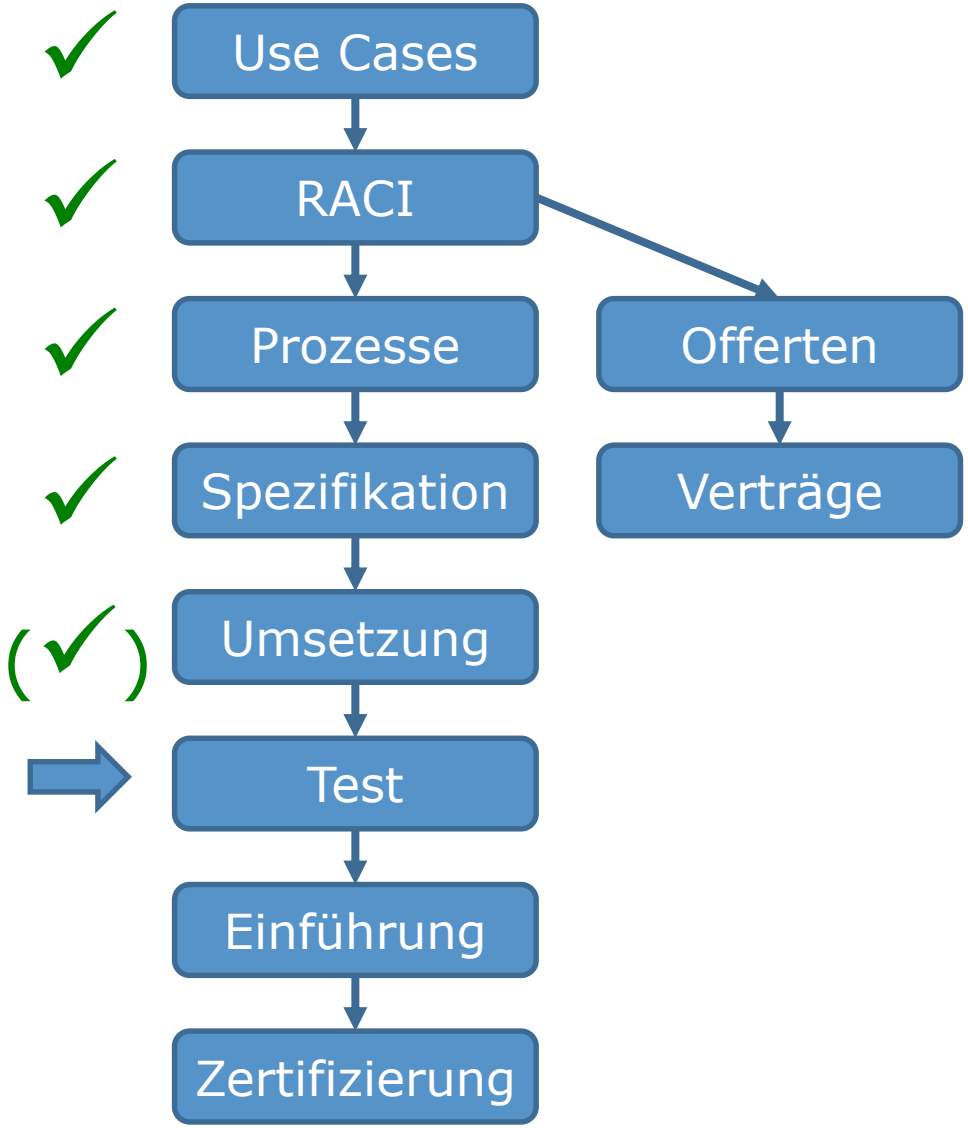
Ziele der EPD-Anbindung

TEMET
end-to-end IT security

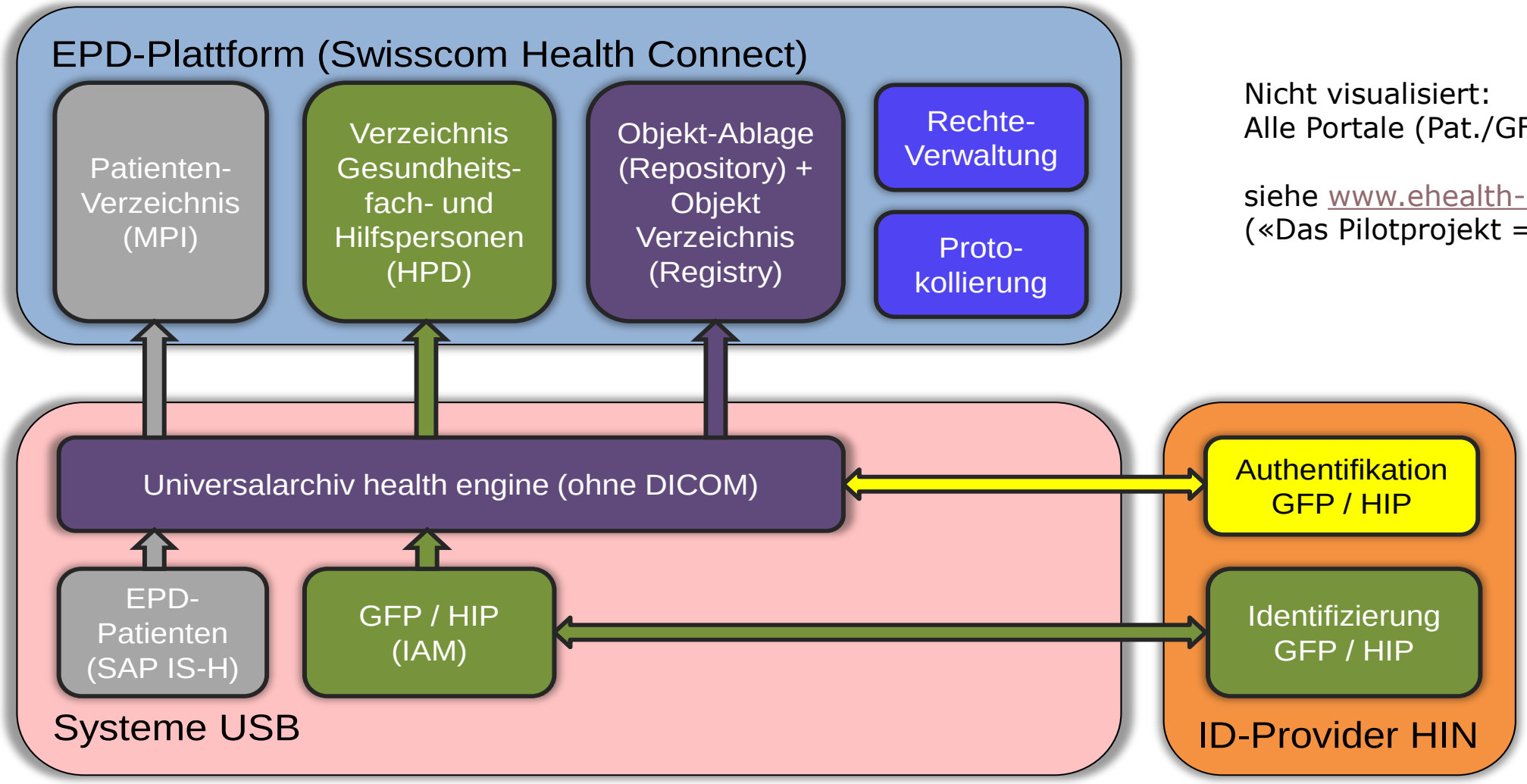
- «structure follows process»: Einbettung der EPD-Anwendungsfälle in den klinischen Alltag
- Entlastung der GFP / Hilfspersonen (HIP) => möglichst tiefe Integration
- EPD als eHealth-Basis-Infrastruktur; zertifizierungsfähige Lösungen
- Hohe Gewichtung Datenschutz / Datensicherheit: Einbindung TEMET

Termine und Vorgehen

- Einbettung in den Gesamtzeitplan eHealth-Pilot NW (myEPD.ch)
- Go-Live an den USB-Kliniken HNO, plast./Hand-Chirurgie und Mund-/Kiefer-/Gesichts-Chirurgie am 19. Juno 2018.
- Alle gesetzlichen EPD-Features ausser EPD-Stv. (folgt ca. Herbst 2018)



Systemübersicht



Nicht visualisiert:
Alle Portale (Pat./GFP/Admin)

siehe www.ehealth-nw.ch
(«Das Pilotprojekt => Konzepte»)

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

Use Cases Übersicht

TEMET end-to-end IT security

n Auswahl für das Referat

- Abfrage Patientenstammdaten im EPD-MPI
- Aktualisierung EPD-MPI
- Patientenaufklärung und –einwilligung
- 1 – EPD-Eröffnung
- EPD-Widerruf
- EPD-Patientensupport
- 3 – EPD-Zugang für Gesundheitsfachpersonen (GFP) und Hilfspersonen (HIP)
- EPD-Austritt GFP und Hilfspersonen (HIP)
- 4 – Dokumente aus dem EPD beziehen («EPD lesen»)
- Ermächtigung zur Delegation der Zugriffsrechte an andere GFP oder Gruppen von GFP
- Ausschluss Behandlungsdokumente
- 2 – Dokumente im EPD speichern («EPD schreiben»)

Patientendossier eröffnen (1/2)

Beteiligte Organisationen und Systeme

	Leistungserbringer (USB)	**EPD-Plattform** (SG / Swisscom)	**Identity Provider** (Swisscom)
Benutzer	Patientenadministration des USB	-	-
Systeme	• SAP IS-H • Health Engine EPD-Konnektor	• Evita Patienten-Portal • Evita Admin-Portal • EPD-MPI	• Evita Identity Provider • Evita Webservice

Patientendossier eröffnen (2/2)

TEMET end-to-end IT security

Prozess (High Level)

- Die USB-Patientenadministration identifiziert den Patienten oder die Patientin und überprüft den EPD-Consent
- Die USB-Patientenadministration kennzeichnet die Patientin oder den Patienten im SAP IS-H («EPD Flag»)
- Die Daten (Attribute) zur Patientin oder zum Patienten werden via den Health Engine EPD-Konnektor übertragen:
  - a) an den EPD-MPI z.Hd. des Evita Patienten-Portals (EPD)
  - b) an den Evita Identity Provider (IdP für Patienten)
- Die USB-Patientenadministration eröffnet das EPD-Dossier im Evita Admin-Portal und bestätigt die erfolgreiche Identifizierung
- Die Patientin oder der Patient aktiviert ihr oder sein Patientendossier

EPD schreiben (1/2)

Beteiligte Organisationen und Systeme

	Leistungserbringer (USB)	**EPD-Plattform** (SG / Swisscom)	**Identity Provider** (Swisscom)
Benutzer	Automatisierter Upload durch «Maschine»	-	-
Systeme	• Health Engine Universalarchiv • Health Engine EPD-Konnektor	• EPD-MPI • EPD-Repository • EPD-Registry	-

EPD schreiben (2/2)

TEMET end-to-end IT security

Prozess (High Level)

- Der Health Engine EPD-Konnektor authentifiziert sich gegenüber der EPD-Plattform (Mutual TLS authentication für M2M-Kommunikation)
- Es wird im EPD-MPI abgefragt, ob der Patient oder die Patientin über ein aktives Patientendossier verfügt
- Die Dokumente der für das EPD relevanten Belegarten werden ins EPD-Repository hochgeladen, sofern das EPD-Flag für den Fall gesetzt ist
  - Die nötigen EPD-Metadaten werden von der Health Engine erzeugt
- Die Metadaten der hochgeladenen EPD-Dokumente werden in die EPD-Registry geschrieben

Hinweis: Im Ausnahmefall ist ein manueller Upload über das GFP-Portal möglich; die Metadaten müssen dann von Hand erfasst werden.

EPD-Zugang für GFP und Hilfspersonen

TEMET end-to-end IT security

Beteiligte Organisationen und Systeme

	Leistungserbringer (USB)	**EPD-Plattform** (SG / Swisscom)	**Identity Provider** (HIN)
Benutzer	Team Stammdaten des USB	-	-
Systeme	• (SAP HCM)* • IAM (almanid) • Health Engine EPD-Konnektor	• EPD-HPD	• Identity Provider (IdP)

*: Quelle für das IAM

EPD-Zugang für GFP und HIP (2/2)

Implementierung - Datenflüsse

Attribut	SAP HCM	IAM almanid	Health engine (USB)	IdP (HIN)	HPD (SG)
Personalien GFP/HIP (Vorname, Name, Geschlecht)	Q →	↔ Abgleich mit HIN vor Übergabe an he	→	→	
Geburtsdatum GFP / HIP (Prüf-Faktor bei HPD-Mutationen)	Q →				
GLN GFP/HIP	Q →	→	Umwandlung in OID →	→	
KST Anstellung GFP/HIP (Grundlage Gruppen-Zuteilung)	Q →				
Nummer Ausweis / ID GFP/HIP*				Q, nur bei HIN	
Profession / Spezialisierung GFP		←	→	Q →	
EPD-Rolle/-Attribute GFP oder HIP (Trigger Export in HPD SG)		←	Q →	Q →	
Gruppen-Zugehörigkeit der GFP, basierend auf KST (inkl. zu GE)		Q →	→	→	
Zugehörigkeit HIP zu GFP		Q →	→	→	

Q = Quellsystem **Wird via Video-Identifikation durch HIN erhoben*

Ebenfalls in den HPD der Stammgemeinschaft (SG) zu melden:

- Gesundheitseinrichtung GE (mit Bezeichnung, OID, Adresse, BUR-Nummer)
- Gruppen (mit Bezeichnung, OID, basierend auf OID der GE)

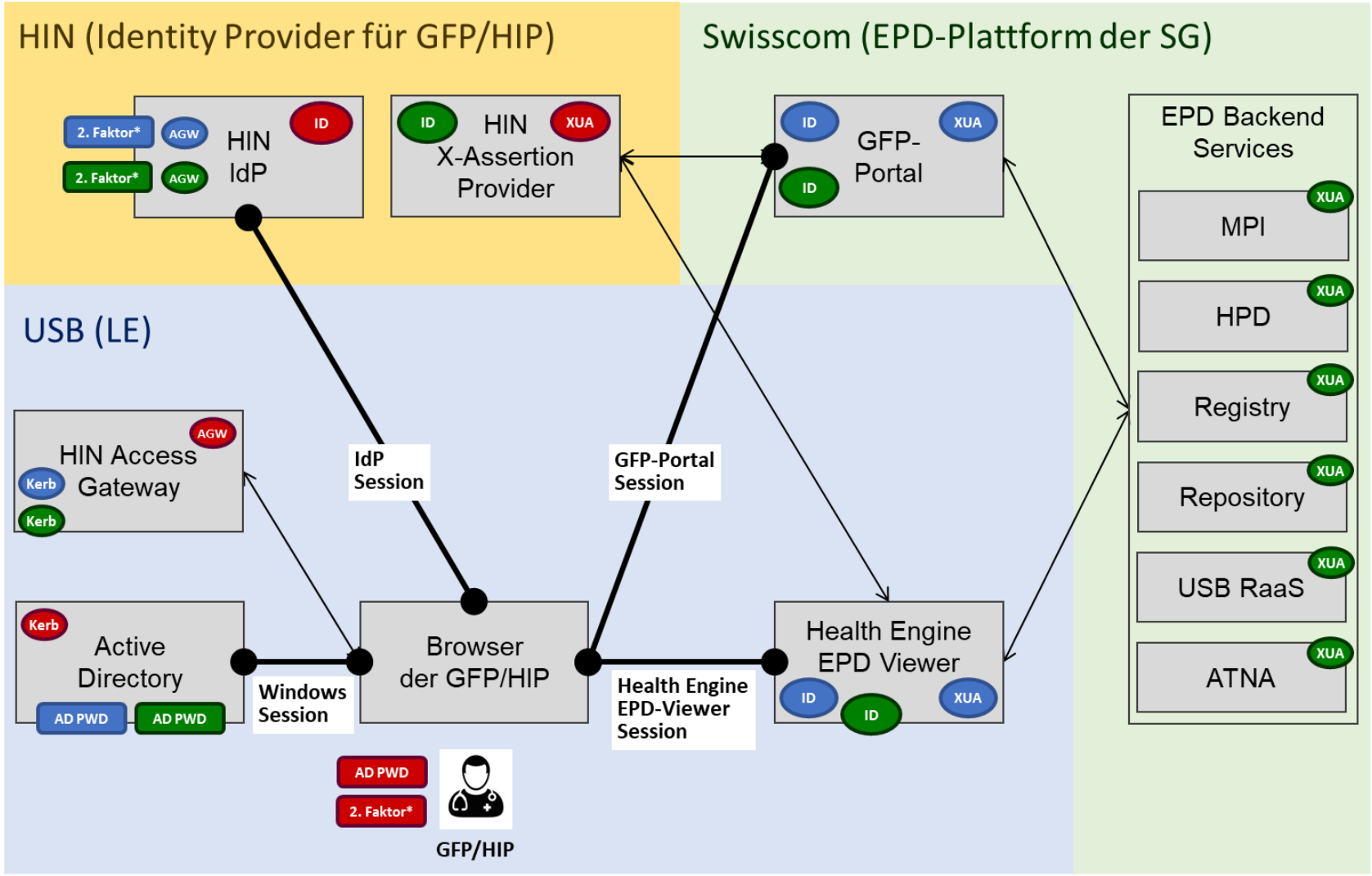
EPD lesen (1/3)

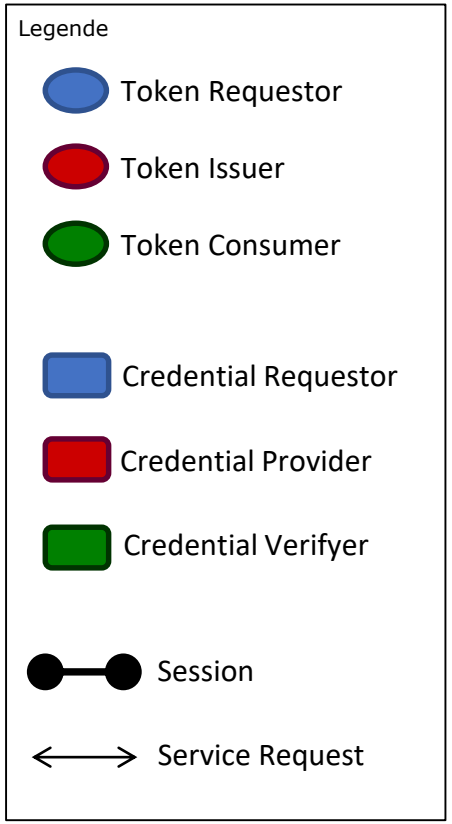
Beteiligte Organisationen und Systeme

	Leistungserbringer (USB)	**EPD-Plattform** (SG / Swisscom)	**Identity Provider** (HIN)
Benutzer	• GFP und Hilfspersonen beim USB (ca. 800 Personen)	-	-
Systeme	• Health Engine EPD-Viewer • Active Directory (AD) • HIN Access Gateway	• GFP-Portal (EPD)	• Identity Provider (IdP) • X-Assertion Provider

EPD lesen (2/3)

Implementierung – Sessions und Token





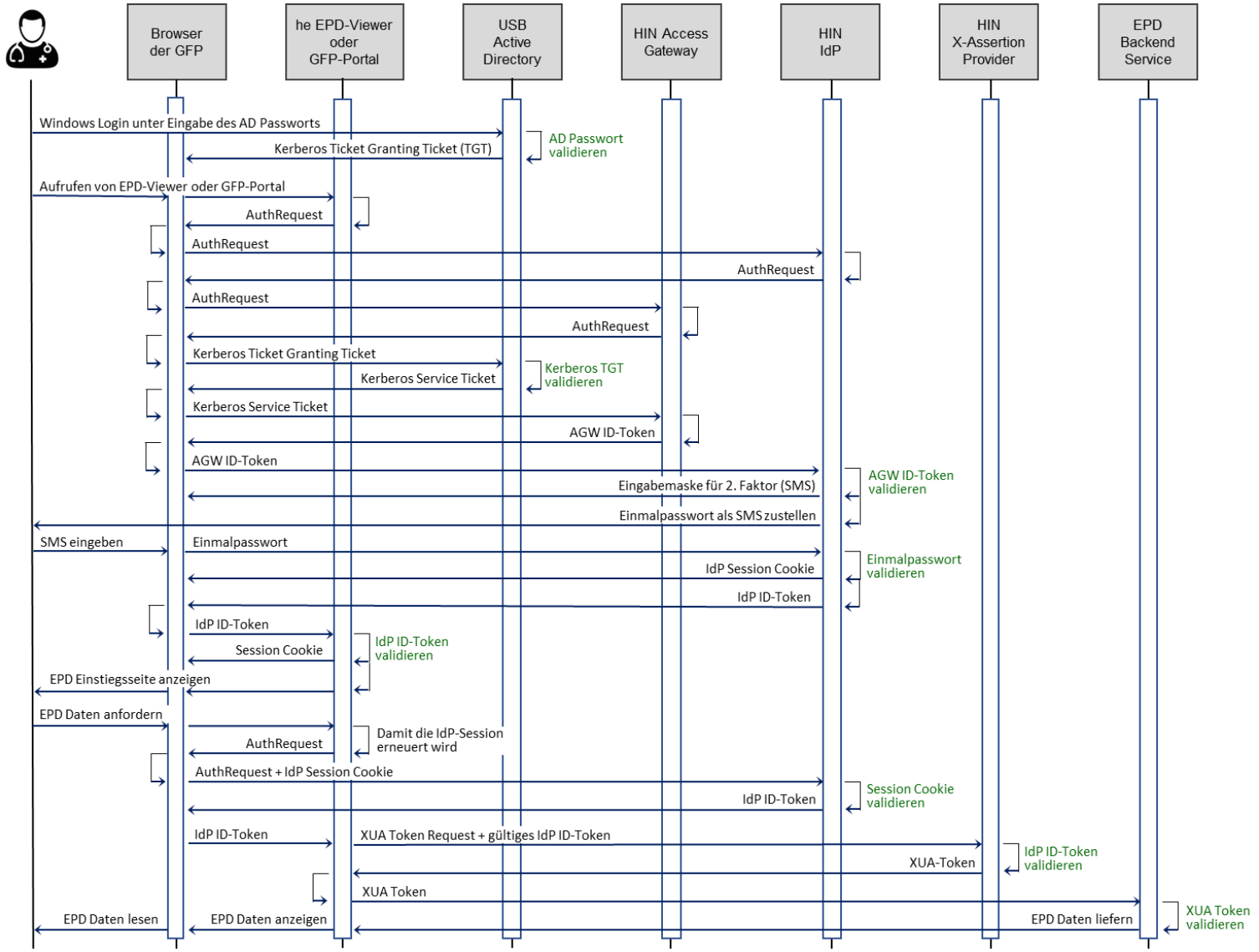
EPD lesen (3/3)

Implementierung – Sequenzdiagramm

Der Benutzer authentisiert sich mit zwei Faktoren:

- Windows-Passwort gegenüber dem AD
- Einmalpasswort (SMS) gegenüber dem IdP

Im Hintergrund werden diverse Token automatisch ausgetauscht und geprüft



(Noch) offene Punkte (1/4)

TEMET end-to-end IT security

Die **Lebensdauern** von

- IdP-Session
- Portal-Sessions
- ID-Token
- XUA-Token

sind (noch) nicht verbindlich definiert.

Diese haben erheblichen Einfluss sowohl auf die Benutzbarkeit als auch auf die Sicherheit.

Aktuelle Arbeitshypothese:

Artefakt	Lebensdauer	Bemerkung
IdP-Session	*Bei Patienten:* Session Idle Timeout: 10 Minuten	In Anlehnung an typische E-Banking Regelungen
	Bei GFP und HIP: Session Idle Timeout: 30 Minuten	In Anlehnung an typische Firmen Security-Policies
Zugangsportal-Session	*Bei Patienten:* Session Idle Timeout: 10 Minuten	Falls neben dem EPD noch weitere Services genutzt werden.
	Bei GFP und HIP: Session Lifetime: 1 Minute (fix). Session wird bei jedem Bezug eines XUA-Token neu aufgebaut (AuthRequest zu Handen des IdP).	Doppelt so lange wie die Lebensdauer des XUA-Token
ID-Token	Token Lebensdauer: 30 Sekunden	Kann länger gewählt werden, falls sich diese Werte als unpraktikabel erweisen.
XUA-Token	Token Lebensdauer: 30 Sekunden	

(Noch) offene Punkte (2/4)

TEMET
end-to-end IT security

Remote Access durch GFP und Hilfspersonen

- Die Gesundheitseinrichtungen sind dazu verpflichtet, eine sichere Konfiguration der Endgeräte sicherzustellen, die von den GFP für den Zugriff auf das EPD genutzt werden [TOZ, Absatz 4.7.1 c)]
- Die Spital-internen Endgeräte genügen den TOZ-Anforderungen vollauf
- Es gibt zudem einen sicheren VDI-Zugang («virtueller Desktop»), über den die GFP auch von ausser Haus via die sichere USB-Infrastruktur auf das EPD zugreifen können

- Es kann aktuell nur organisatorisch (mittels Verbot / Instruktion via easylearn EPD4GFP) verhindert werden, dass eine am USB angestellte GFP mit einem unkontrollierten (privaten) Endgerät über das GFP-Portal auf das EPD zugreift

(Noch) offene Punkte (3/4)

TEMET
end-to-end IT security

M2M-Kommunikation zwischen USB-Systemen und EPD-Services

- Der automatisierte Upload von Dokumenten ins EPD wird durch eine Maschine (das Universalarchiv resp. die Health Engine) und nicht eine Gesundheitsfachperson durchgeführt. Dasselbe gilt bei der Kommunikation IS-H → MPI / IdP sowie IAM → HPD
- Die starke Authentisierung kann über TLS mutual authentication sichergestellt werden. Dabei ist festzulegen:
  - Wie der Inhaber des Maschinen-Zertifikats identifiziert wird (Arbeitshypothese: Als Organisation «USB», evt. mittels OID)
  - Wie der private Schlüssel der Maschine sicher gespeichert wird (Arbeitshypothese: Als lokales verschlüsseltes File)
- Dies wurde im EPD Ausführungsrecht bisher nicht adressiert

(Noch) offene Punkte (4/4)

TEMET
end-to-end IT security

Kontext-abhängige Zugriffskontrolle ist im EPDG nicht vorgesehen

- Aus der möglichen Mehrfachanstellung von GFP in Kombination mit Gruppen-Zugriffsrechten ergibt sich folgende «AKV-Problematik»:
  - Der Patient erteilt ein Gruppen-Zugriffsrecht an Klinik «A» im Vertrauen darauf, dass seine Daten im Verantwortungsbereich dieser Klinik bleiben
  - Es ist möglich, dass eine GFP gleichzeitig bei den Kliniken «A» und «B» in einem Anstellungsverhältnis steht (Mehrfachanstellung)
  - Klinik «A» kann die Ausübung des Gruppen-Zugriffsrechts nicht kontrollieren, während diese GFP bei der Klinik «B» tätig ist
- Diese Problematik könnte gelöst werden, indem der Zugriffs-Kontext bei der Evaluation von Gruppen-Zugriffsrechten überprüft wird
  - Das aktuelle EPD Ausführungsrecht sieht eine solche Kontext-abhängige Zugriffskontrolle allerdings nicht vor

Schlusswort / lessons learned (so far)

TEMET
end-to-end IT security

- (Externer) Security-Review hochgradig relevant
- Konfiguration (Systeme / SST) / Nachbesserungen nur aufgrund geklärter Zuständigkeiten möglich (RACI-Tabellen TEMET)
- Use-Case-Einbettung (Prozesse; Betriebskonzepte; Schulungen; Dokumentation zuhanden Stammgemeinschaft): nicht zu unterschätzen.

… zum Erfolg

Besten Dank
für Ihre Aufmerksamkeit!

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