IAM-Architektur für die Ära der Cloud

ICMF Wintertagung 2019

21. November 2019, 13:40 – 14:25 Uhr

Thomas Kessler, IT-Security Architekt, TEMET AG

21.11.2019

Agenda

- Kurzvorstellung des Referenten
- IAM Evolutionsschritte von 1993 bis heute
- Federated IAM: Standards und Technologien
- IdP-Landschaft Schweiz
- IAM-Architektur für «Outbound Federation»
- IAM-Architektur für «Inbound Federation»

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

IAM Erfahrungen (kleine Auswahl)

- 1993: Projektleiter Bank-interne Einführung SecurID OTP-Token
- 1997: Teilprojektleiter 2FA-Lösung für erstes E-Banking
- 2010: Architekt und Projektleiter „BrokerGate Identity Provider“
- Seit 2015: Elektronisches Patientendossier (EPD) (diverse Mandate)
- 2017: Co-Autor eCH-0107 (Gestaltungsprinzipien für das IAM)
- 2018: IAM Federation Zielarchitektur für eine Universalbank
- 2019: 2FA-Zielarchitektur für ein Spital
- 2019: Portal-Architektur für Justitia 4.0

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.

Identity and Access Management (IAM)

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 kombinieren.

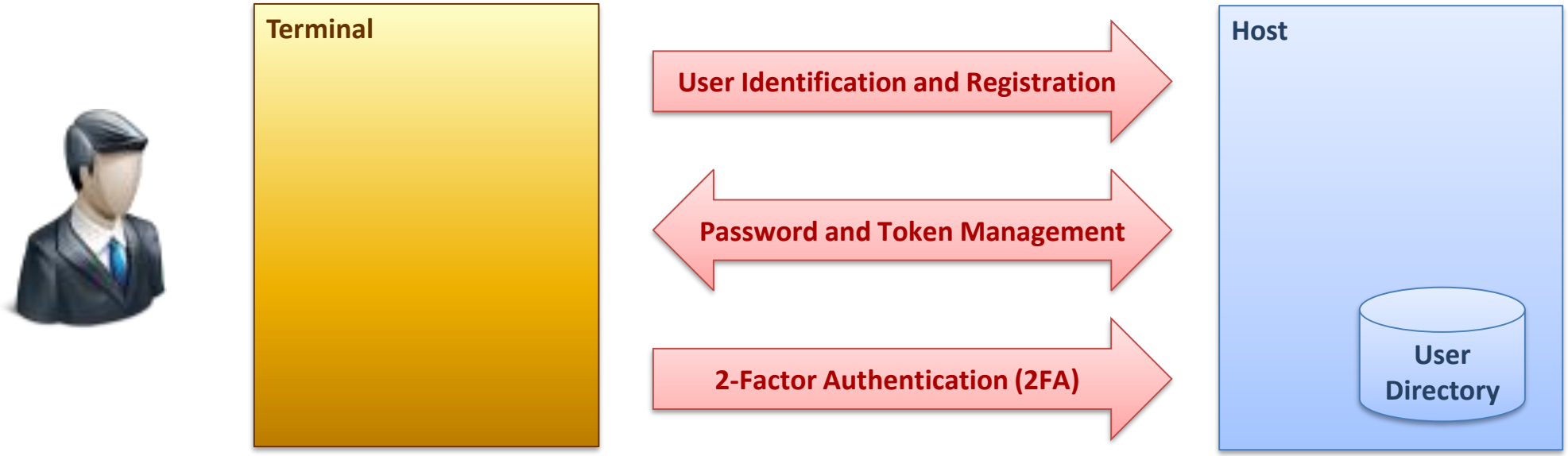
Das IAM muss die Entwicklung der IT-Landschaft unterstützen; aktuell insb. firmenübergreifende Geschäftsprozesse und Cloud-Services.

⇨ Dies ist auch der Fokus des heutigen Referates

IAM-Kernfunktionen seit 1993

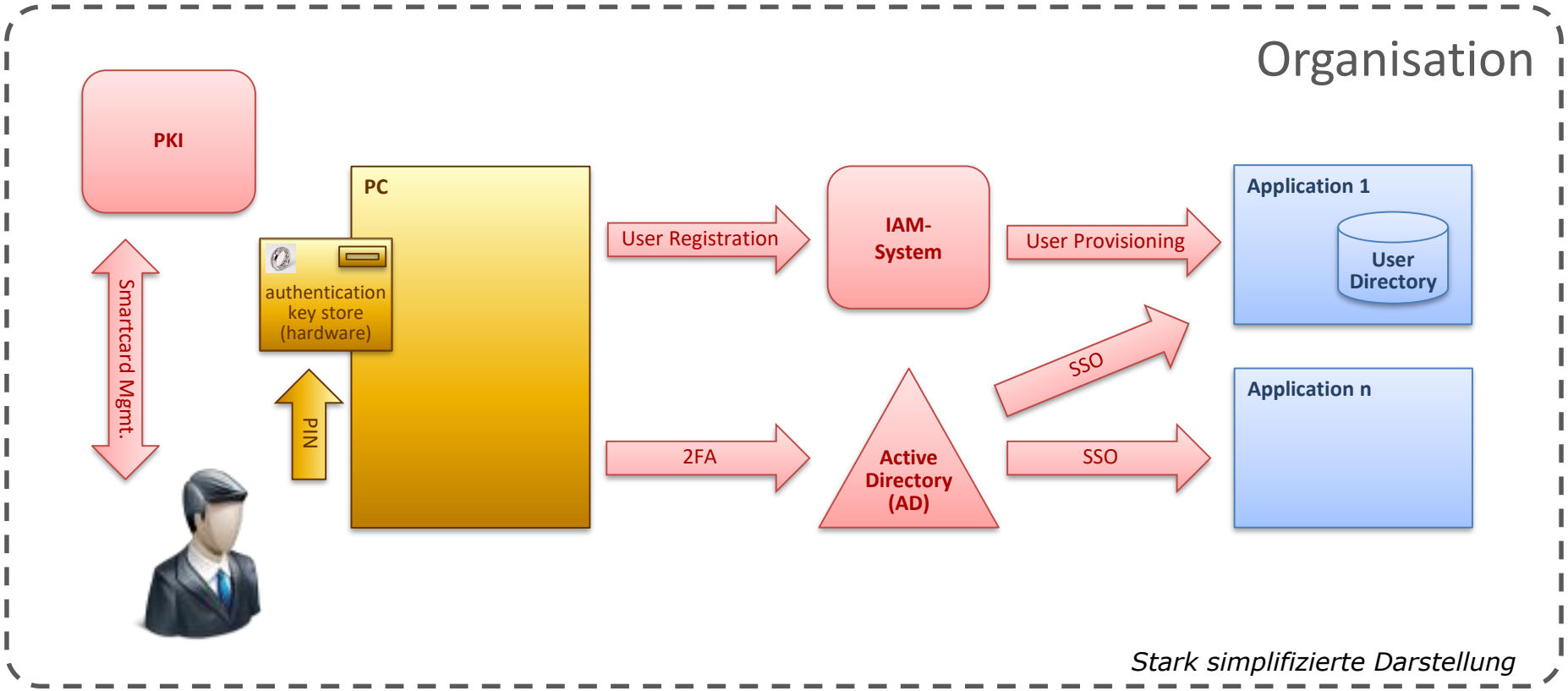
TEMET
end-to-end IT security

Die IAM-Kernfunktionen waren schon 1993 ein Thema



Das IAM der 2000er Jahre

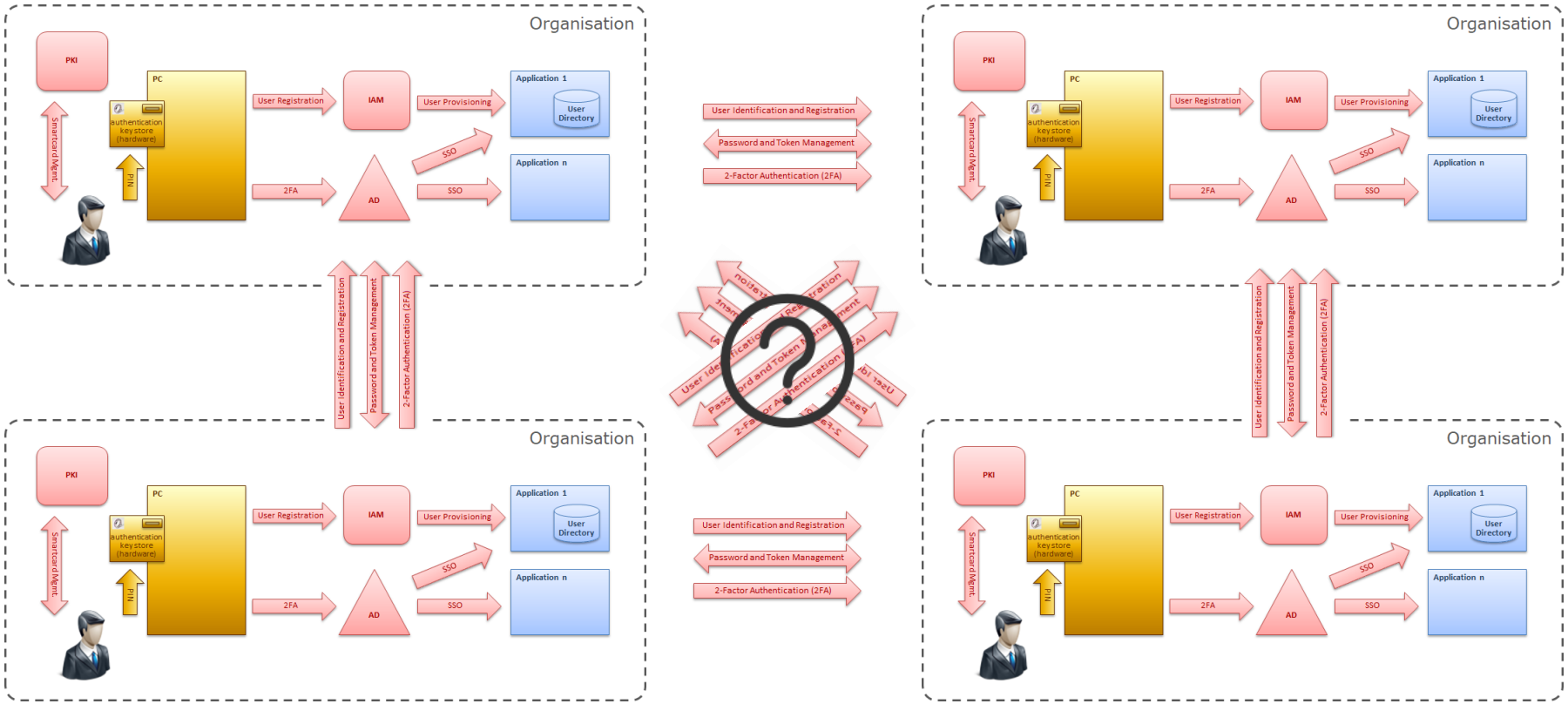
IAM-Infrastrukturen bewältigen die organisationsinterne Komplexität



Federated IAM in der Ära der Cloud

Die Herausforderung

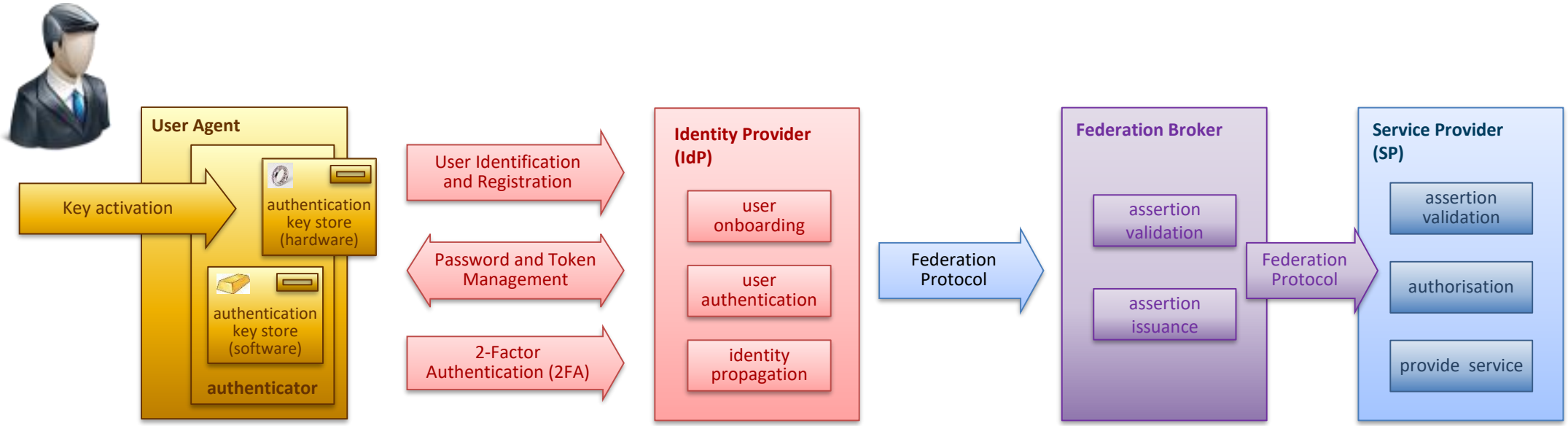
Wie werden die IAM-Systeme vieler Organisationen interoperabel?



Federated IAM - Basiselemente

Die Bausteine der Lösung

- Neue Komponenten Identity Provider (IdP) und Federation Broker
- Neue Protokolle für Authentifizierung und Identitätsweitergabe



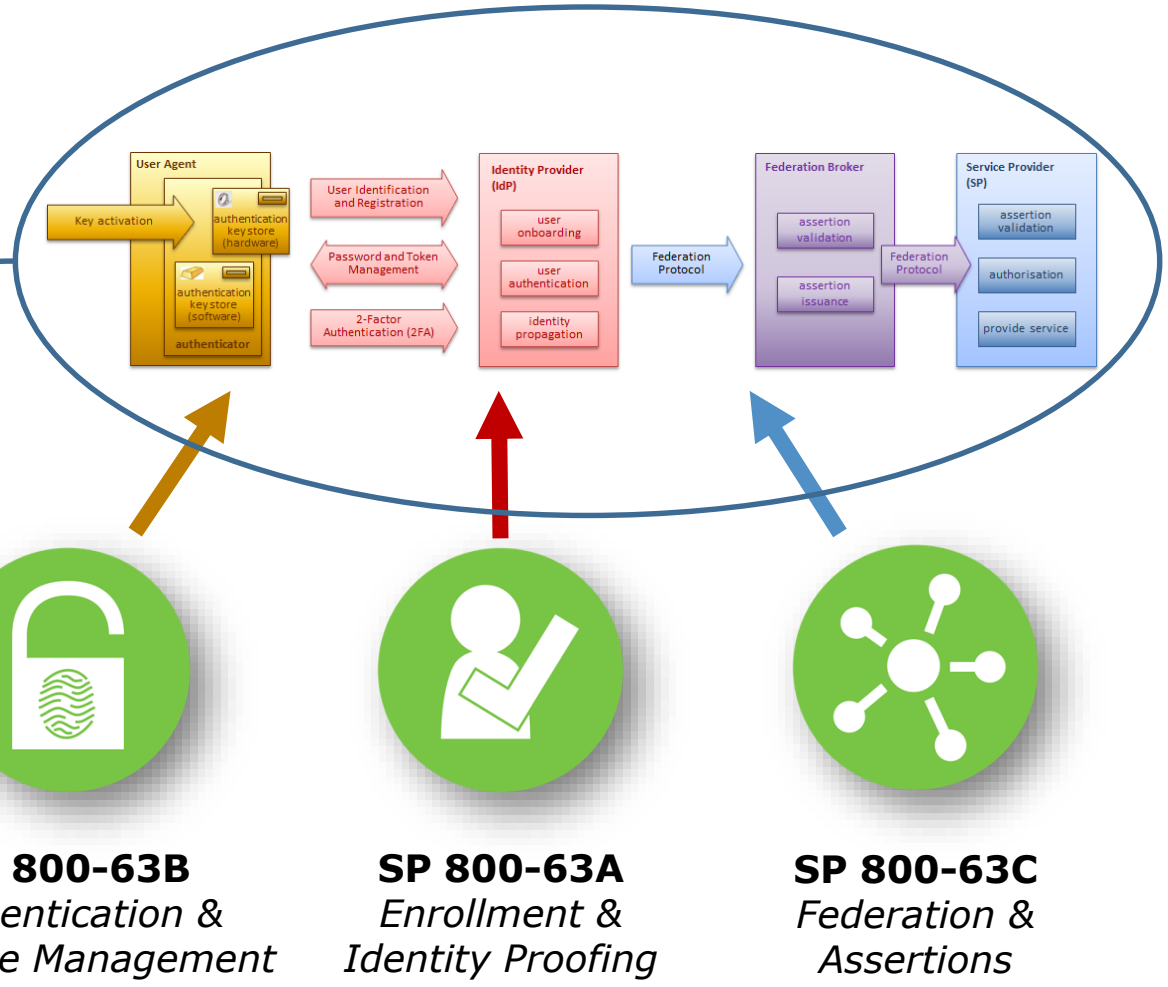
There is a Standard!

NIST Special Publication SP 800-63-3
"Digital Identity Guidelines"

- Publiziert im Juni 2017
- Besteht aus vier Dokumenten
- Insgesamt 213 Seiten

Und spezifisch
für die Schweiz:

- E-ID-Gesetz
- eCH-0107



SP 800-63-3
Digital Identity Guidelines

SP 800-63B
Authentication & Lifecycle Management

SP 800-63A
Enrollment & Identity Proofing

SP 800-63C
Federation & Assertions

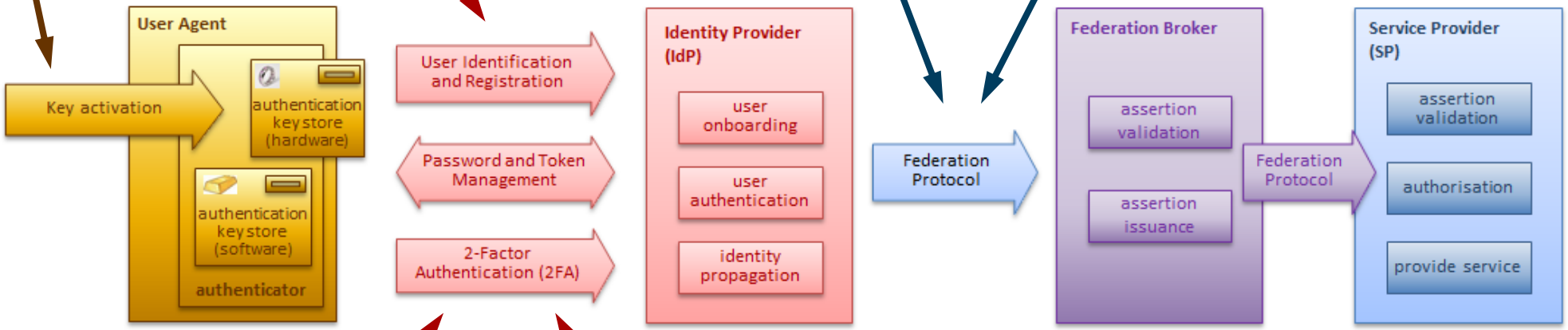
Einige interessante Technologien

SOFA-B
Strength of Function for Authenticators – Biometrics
- NIST Discussion Draft -

WebAuthn
Authentifizierungsprotokoll als Kernkomponente von FIDO 2
- W3C Standard -

OIDC
OpenID Connect basierend auf OAuth 2.0
- OpenID Foundation -

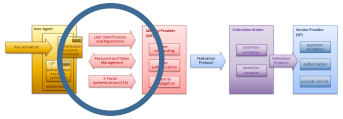
SAML
Security Assertion Markup Language basierend auf XML
- OASIS -



TOTP / HOTP
Time-based / HMAC-based one-time-password von OATH
- IETF RFC 6238 / 4226 -

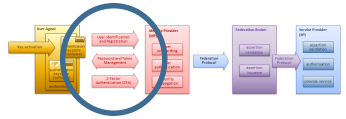
MSS
Mobile Signature Service
z.B. Swisscom MobileID
- ETSI 102 203 -

Authentication Protocol Trends (1/2)

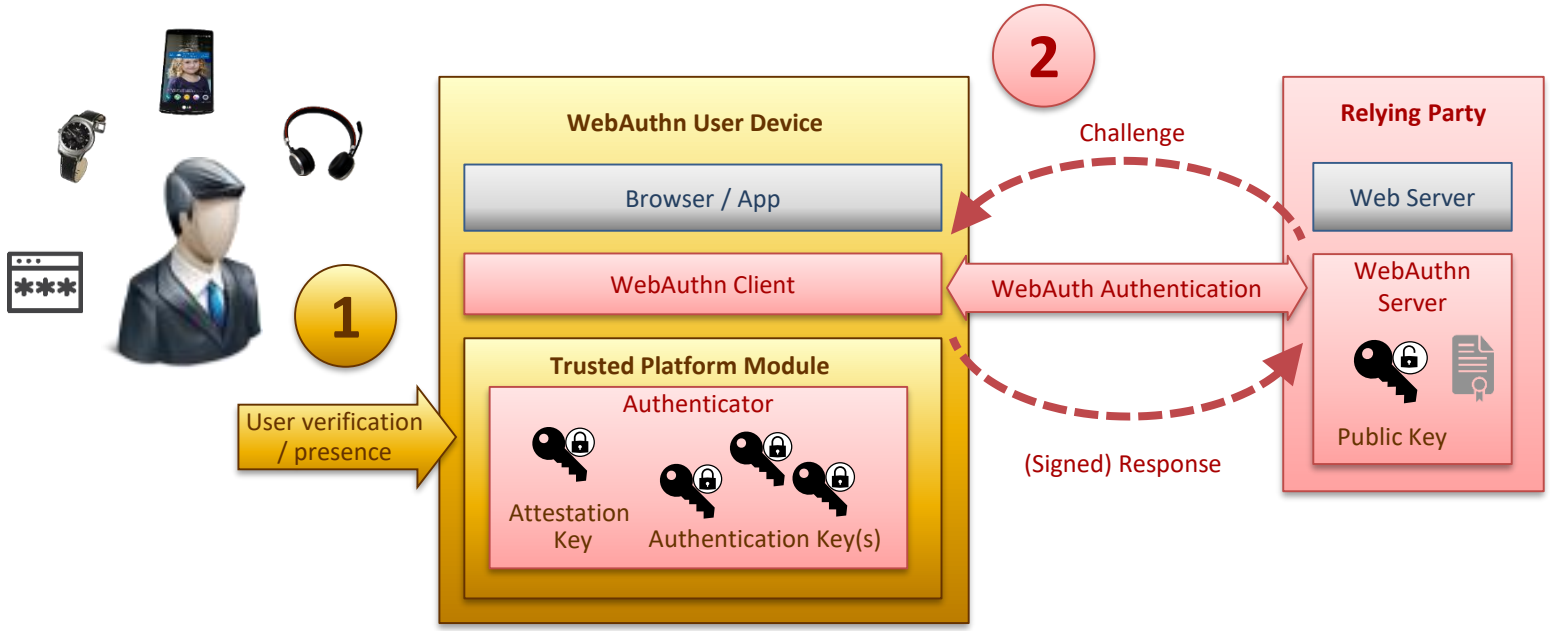


- mTAN (Passwort + OTP über SMS) hat den Zenit überschritten.
- MSS (Mobile Signature Service), in der Schweiz als MobileID bekannt, hat sich als Nachfolger erst punktuell etablieren können.
- Authenticator Apps aller Art beherrschen aktuell den Markt
  - TOTP / HOTP oder challenge-and-response
  - Offline oder Online
  - 2nd Channel oder In-Channel
  - Separat oder über SDK integriert
  - Die Apps nutzen diverse Sensoren (Kamera, Fingerabdruckleser, Mikrofon, GPS, …)
- Auch der Markt für HW-Token ist wieder in Bewegung
  - Proprietäre OTP-Generatoren haben Mühe
  - Diverse FIDO-Token drängen auf den Markt und trumpfen mit Malware-Resistenz

Authentication Protocol Trends (2/2)



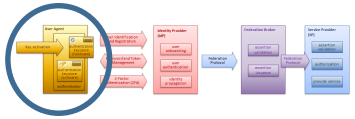
- Mit WebAuthn (entstanden aus FIDO 2) ist seit 2018 ein breit abgestützter Industriestandard für die Authentifizierung verfügbar.
- WebAuthn basiert auf Public Key Kryptographie, kommt aber ohne eine zentrale Certification Authority (CA) aus.



1. Der Benutzer authentifiziert sich mittels PIN, Biometrie, Wearables oder Sensorik.

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

Key Activation Trends (1/2)

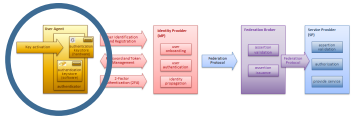


- Der Ersatz der PIN durch Biometrie wird unter dem Begriff „Passwordless Authentication“ zunehmend relevant.
- Biometrische Muster sollten nur dezentral im persönlichen Authenticator gespeichert werden (nie auf einem Server)
- Die Qualität moderner Sensoren kann sich mit der Qualität einer typischen PIN (4-6 Zahlen) durchaus messen
  - Ist nicht Schwarz/Weiss
- Interessantes Projekt in diesem Zusammenhang: NIST SOFA-B
  - https://pages.nist.gov/SOFA/

Key Activation Trends (2/2)

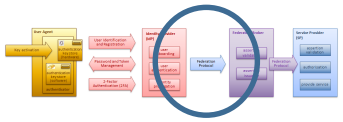
		Fingerprint	Face	Iris	Voice
Level A	**Time**: short **Expertise:** anyone **Equipment:** readily available	paper printout, direct use of latent print on the scanner	paper printout of face image, mobile phone display of face photo	paper printout of iris image, mobile phone display of iris photo	replay of audio recording
	Source of biometric characteristic: easy to obtain	lift of fingerprint	photo from social media	photo from social media	recording of voice
Level B	**Time**: >3 days **Expertise:** moderate skill and practice needed **Equipment:** available but requires planning	fingerprints made from artificial materials such as gelatin, silicon.	paper masks, video display of face (with movement and blinking)	video display of an iris (with movement and blinking)	replay of audio recording of specific passphrase, voice mimicry
	Source of biometric characteristic: more difficult to obtain	latent print, stolen fingerprint image	video of subject, high quality photo	video of subject, high quality photo	recording of voice of specific phrase
Level C	**Time**: >10 days **Expertise:** extensive skill and practice needed **Equipment:** specialized and not readily available	3D printed spoofs	silicon masks, theatrical masks,	contacts lens with a specific pattern	voice synthesizer
	Source of biometric characteristic: more difficult to obtain	3D fingerprint information from subject	3D face information from subject	high quality photo in Near IR	multiple recordings of voice to train synthesizer

Quelle: NIST Strength of Function for Authenticators - Biometrics (SOFA-B) Discussion Draft

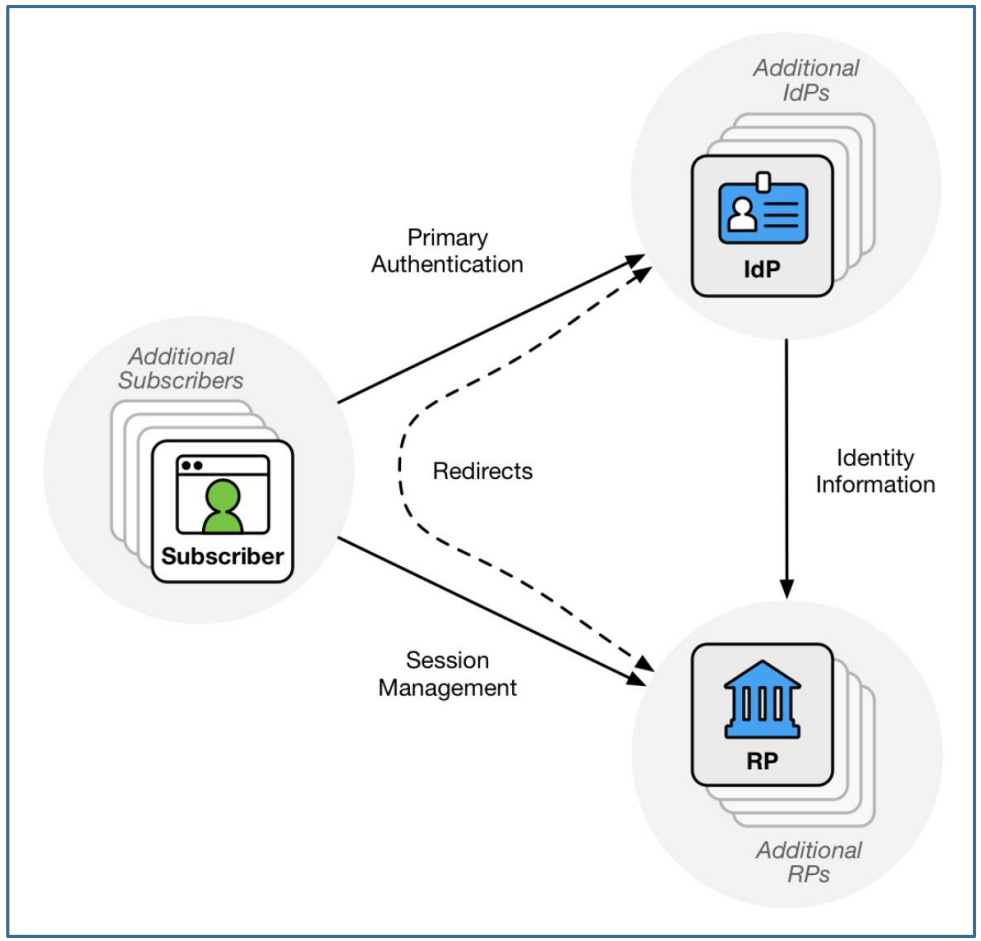


Das NIST SOFA-B Projekt als interessanter Versuch, die Qualität biometrischer Sensoren zu quantifizieren

Federation Protocol Trends (1/2)

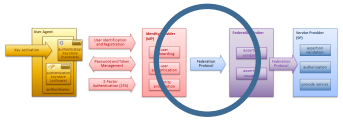


- SAML (Security Assertion Markup Language) ist lange verfügbar und im B2B-Umfeld weit verbreitet.
- OIDC (OpenID Connect) ist neuer, hat sich im eCommerce etabliert und wird SAML verdrängen.
- Bei beiden Protokollen wird die Identität des authentifizierten Benutzers vom Identity Provider (IdP) an Relying Parties propagiert.



Quelle: NIST SP 800-63C "Federation and Assertions"

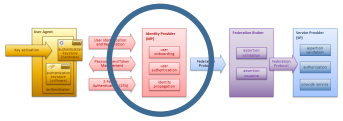
Federation Protocol Trends (2/2)



Sowohl SAML als auch OIDC kennen diverse Protokollvarianten, z.B.:

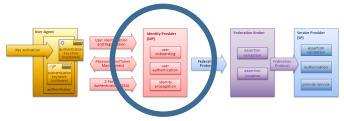
- Werden Assertions nur signiert oder auch verschlüsselt?
  - Die Stufe drei (FAL3) „holder-of-key“ ist in der Praxis noch kaum je anzutreffen
- Werden Assertions via den User Agent transportiert („Front-Channel Presentation“) oder von der Relying Party beim Identity Provider abgeholt („Back-Channel Presentation“)?
- Interagiert der Benutzer zuerst mit der Relying Party („Destination-site first“) oder ruft er diese über ein Portal auf („IdP-first“)?
  - Im ersten Fall stellt sich das Problem, pro Benutzer den richtigen IdP zu involvieren

IdP-Landschaft Schweiz - Organisationen



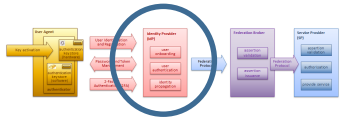
- Bei Organisationen mit hohen Sicherheitsanforderungen (insb. Banken) sind IdP mit 2FA (z.B. Smartcards) für Mitarbeitende weit verbreitet.
  - Die Identifizierung und Registrierung sind Bestandteil der HR-Prozesse;
  - Die benötigte Infrastruktur (z.B. Smartcard-Lesegerät) gehört zum Arbeitsplatz;
  - Die Verwaltung der Authentifizierungsmittel (PIN, Smartcard) erfolgt durch etablierte Administrationsstellen und Supportprozesse;
  - Ausnahmeprozesse (z.B. vergessene/defekte Smartcards) sind hoch effizient.
- Ein Single SignOn bindet viele (hunderte) Anwendungen ein.
  - Dieselbe Smartcard wird auch für physischen Zutritt genutzt.
- Aktuell etablieren auch Firmen mit mittleren Sicherheitsanforderungen IdP mit 2FA insbesondere für die Nutzung von Cloud-Services.

IdP-Landschaft Schweiz - Privatpersonen



- Soziale Medien haben sich als öffentliche IdP für Anwendungen mit tiefen Sicherheitsanforderungen etabliert
  - Google-ID, Apple-ID, Facebook-ID,…
- Es gibt aktuell keinen öffentlichen IdP mit substanziellem Sicherheitsniveau und nennenswerter Verbreitung
  - Die von Banken getriebene SwissKey ist 2000 gescheitert
  - Die vom Bund mitfinanzierte SuisseID ist den Erfolg schuldig geblieben
  - Die SwissID ist noch nicht mit Sicherheitsniveau substanziell verfügbar
- Das E-ID-Gesetz verspricht langfristig Besserung
  - Wir werden sehen, ob das Versprechen gehalten werden kann

IdP-Landschaft Schweiz - Branchen



- Digitale firmenübergreifende Geschäftsprozesse haben dazu geführt, dass verschiedene Branchen eigene IdP etabliert haben
  - HIN IdP für niedergelassene Ärzte und Ärztinnen
  - Ofac IdP für Apothekerinnen und Apotheker
  - BrokerGate für Versicherungsbroker
  - SWITCH edu-ID für Studentinnen und Studenten
  - EJPD SSO-Portal für Polizeien
- Für den Zugriff auf das elektronische Patientendossier (EPD) verlangt der Gesetzgeber eine 2-Faktor Authentifizierung durch zertifizierte IdP
  - GFP-IdP für Gesundheitsfachpersonen, Patienten-IdP für Patienten
  - EPDG-zertifizierte IdP werden sich voraussichtlich auch nach E-ID-Gesetz anerkennen lassen, sofern sie nicht auf eine spezifische Berufsgruppe (z.B. Ärzte) fokussiert sind.

«Outbound Federation»

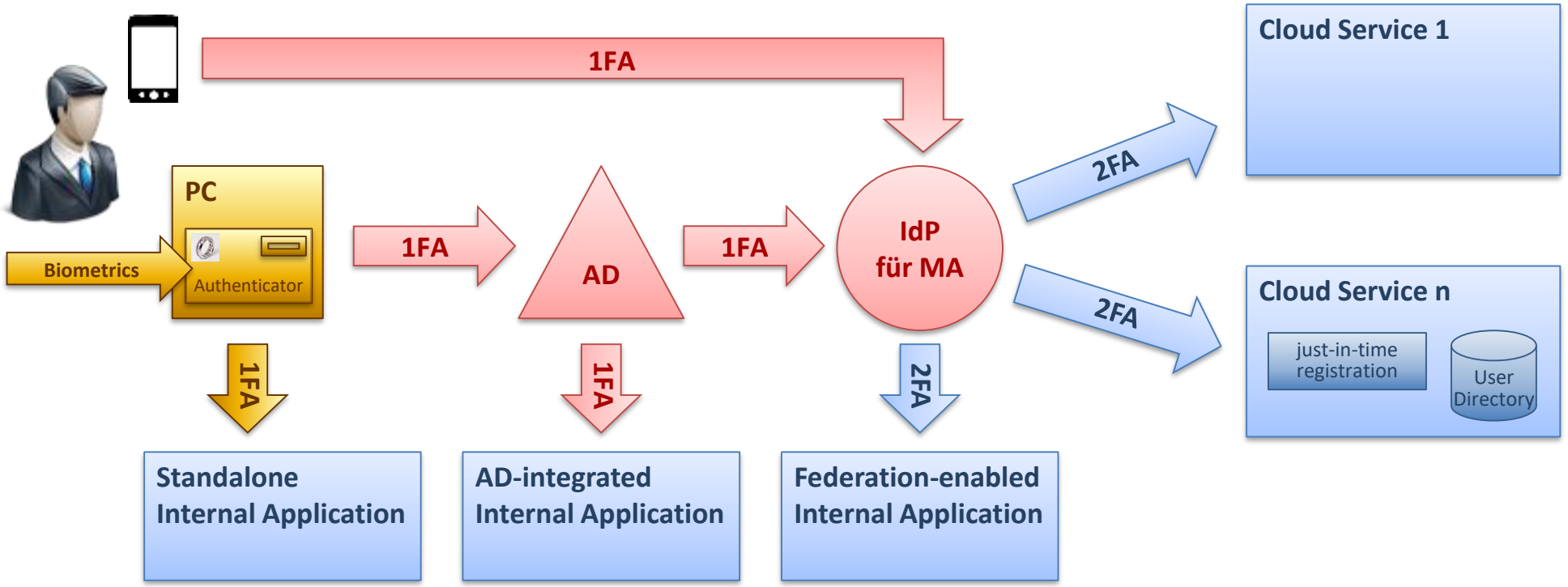
Worum es geht

- Wie authentifizieren sich die eigenen Mitarbeitenden mit 2 Faktoren gegenüber extern betriebenen Services?
  - Applikationen von Partnern im Rahmen von firmenübergreifenden Geschäftsprozessen
  - Cloud-Services aller Art (IaaS, PaaS und SaaS)
- Wie registrieren sich die eigenen Mitarbeitenden bei extern betriebenen Services?
  - Moderne Services haben kein Benutzerverzeichnis. Die Zugriffskontrolle erfolgt zur Laufzeit anhand der Attribute in der Assertion (Attribute Based Access Control, ABAC).
  - Andere Services registrieren den Benutzer beim ersten Zugriff, indem sid die benötigten Benutzerattribute aus der Assertion entnehmen und im lokalen Verzeichnis ablegen.
  - Eine De-Provisionierung ist auf diesem Weg allerdings nicht möglich, weshalb zusätzlich ein periodischer Bereinigungsprozess erforderlich ist.

IAM-Architektur für Outbound Federation

TEMET
end-to-end IT security

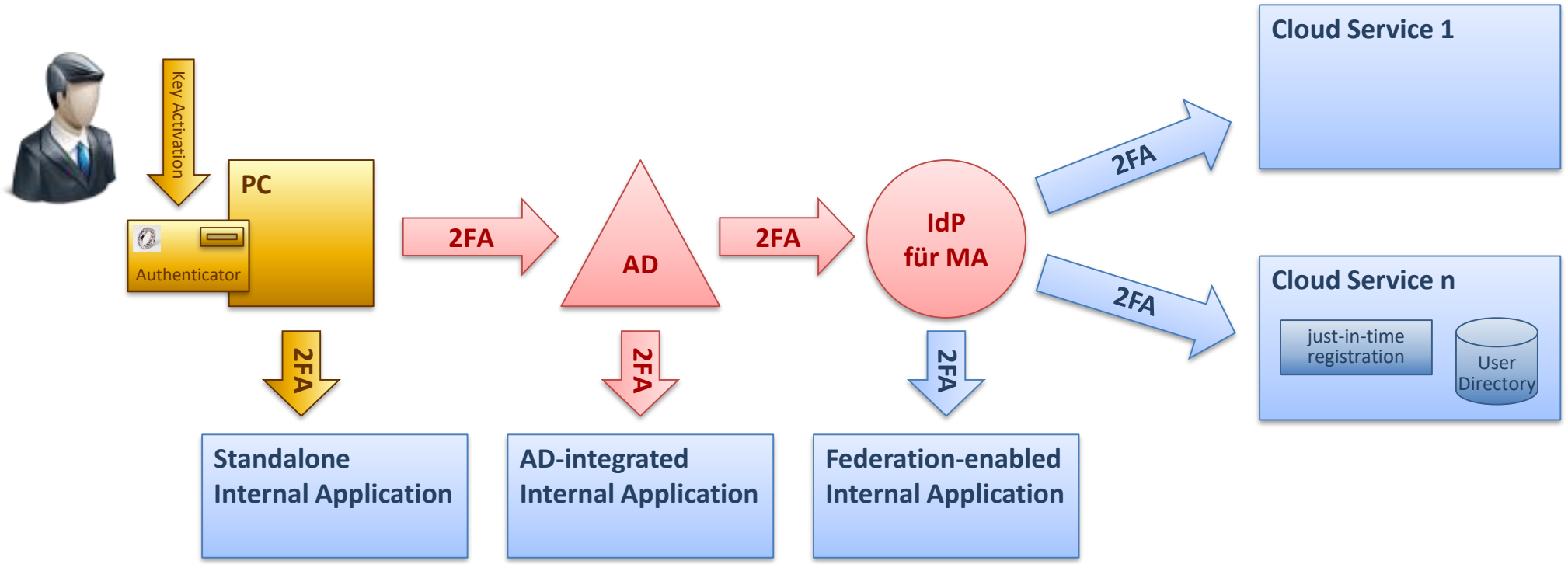
Anbindung von Cloud Services über einen „IdP für Mitarbeitende“



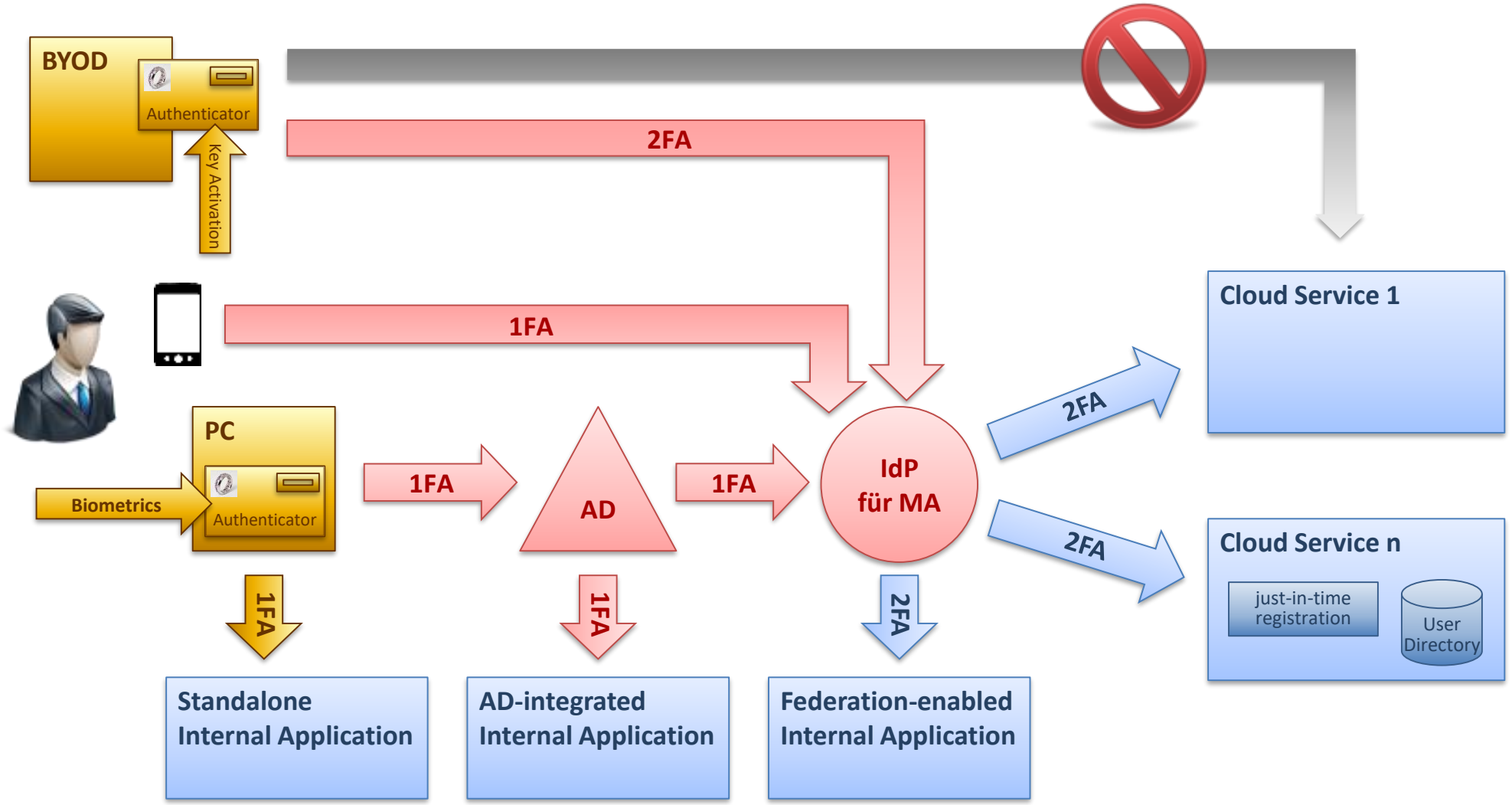
Variante mit 2FA am Arbeitsplatz

Anbindung von Cloud Services über einen „IdP für Mitarbeitende“

- Variante mit 2FA (Hardware Authenticator) am Arbeitsplatz



Outbound Federation und BYOD



Outbound Federation - Optionen

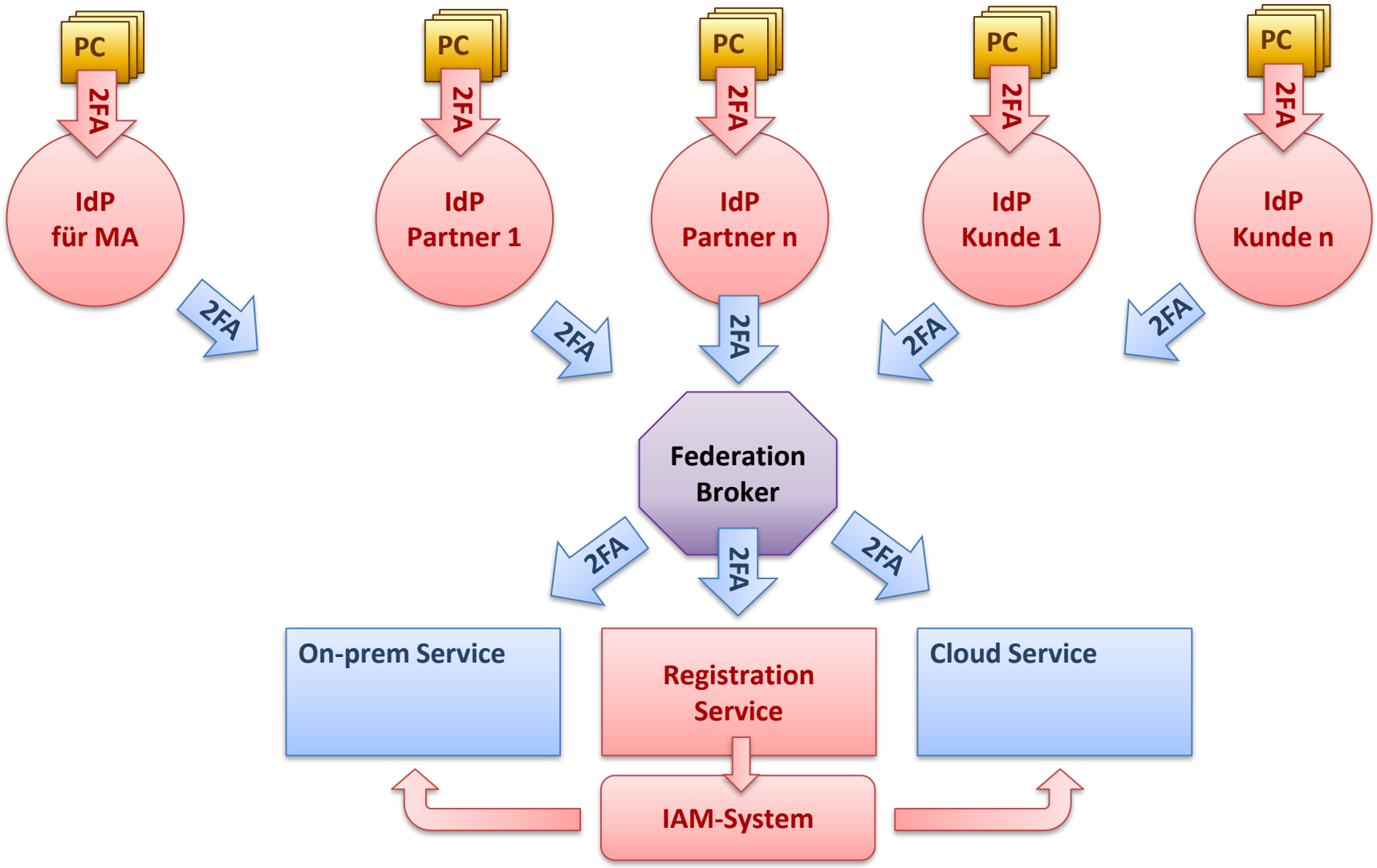
- Der Mitarbeiter-IdP kann selber ebenfalls als Cloud Service bezogen werden (Identity as a Service, IDaaS)
- Nutzung von ADFS (Active Directory Federation Services) oder Evaluation eines spezialisierten Zusatzprodukts
- Es steht eine kaum überschaubare Menge von Authenticator Apps und Authenticator Token zur Auswahl

«Inbound Federation»

Worum es geht

- Wie authentifizieren sich die diversen Benutzergruppen gegenüber den eigenen Services, die über das Internet angeboten werden?
  - MA von Partnerfirmen im Rahmen von firmenübergreifenden Geschäftsprozessen
  - Privatkunden und Firmenkunden
  - Die eigenen Mitarbeitenden
- Wie registrieren sich diese Benutzer bei den eigenen Services?
  - Wie kann eine „Registrierung pro Service" verhindert werden?
  - Welche Rolle spielt das intern etablierte IAM-System?

IAM-Architektur für Inbound Federation



Inbound Federation - Optionen

- Der Federation Broker kann on-prem betrieben oder als Cloud Service bezogen werden
- Der Federation Broker kann mit Zusatzfunktionen erweitert werden
  - Verschlüsselung und Entschlüsselung der transportierten Nutzdaten
  - Inhaltsvalidierung und/oder Konvertierung
  - Data Leakage Prevention (DLP)

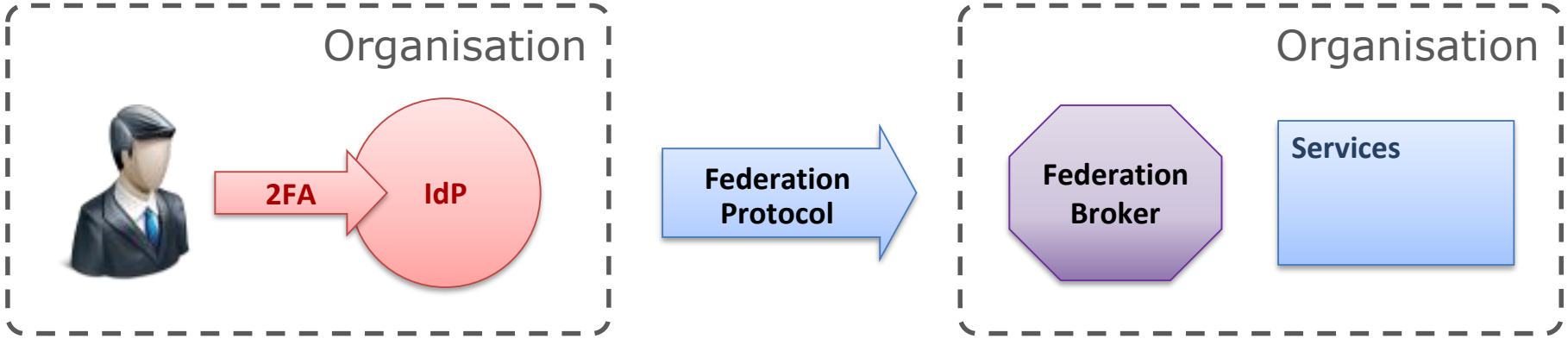
⇨ Cloud Access Security Broker (CASB)

Fazit / Schlusswort

Die Ära der Cloud erfordert - und bietet - neue Konzepte auch im IAM:

- Identity Provider (IdP) bündeln die Benutzer
- Federation Broker bündeln die Applikationen
- Federation Protokolle verbinden die Organisationen

Diese neuen Bausteine können evolutiv in die IAM-Infrastruktur integriert werden; eine Revolution kann vermieden werden.



… zum Erfolg

Besten Dank
für Ihre Aufmerksamkeit!

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