TEMET
end-to-end IT security

Thomas Kessler

Identity Provider – kurze strategische Betrachtung

Fachvortrag an der security-zone 2013

Thomas Kessler / thomas.kessler@temet.ch / 079 508 25 43 / www.temet.ch

Inhalt

- Angaben zum Referenten / zur TEMET AG
- Ausgangslage / Situation «2013»
- Identity Provider - Begriffsbestimmung
- «Business Case» aus Sicht der Anwender

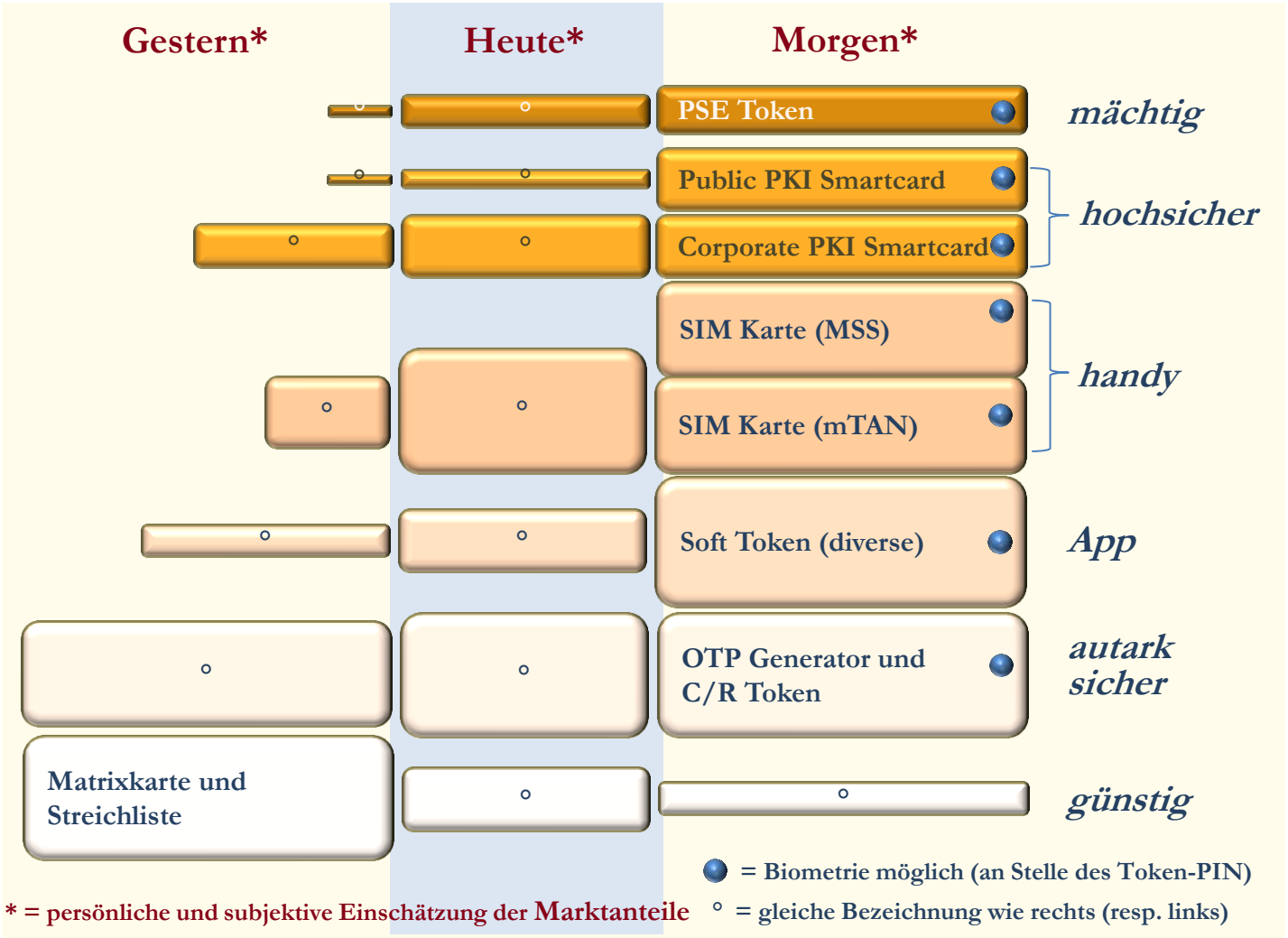
Angaben zum Referenten:
Thomas Kessler

- Dipl. Physiker ETH, MAS ZFH in BA
- 22 Jahre Tätigkeit in der IT-Security
  - 6 Jahre Fachstelle IT-Security bei einer Grossbank
  - 3 Jahre Leiter Security Engineering bei einem Finanzdienstleister
  - 13 Jahre IT-Security Consulting
- Geschäftsführer TEMET AG
  - Angebot: IT-Security Konzepte und Projekte
  - Kunden: Banken, Versicherer und Verwaltungen
- Persönliche Schwerpunkte
  - IT-Sicherheitsarchitektur
  - 2-Faktor Authentisierung 2-FA
  - Identity and Access Management IAM

Informationen zur TEMET AG

- Die Temet mit Sitz in Zürich wurde 2010 von erfahrenen IT-Security Experten gegründet
- Die Temet bietet ausschliesslich hochwertige IT-Security Beratung an und vereint technische Expertise mit Management- und PL-Kompetenz
- Die Temet ist als unabhängige und herstellerneutrale Beratungsfirma nur ihren Kunden verpflichtet
- Bereits 28 renommierte Unternehmen, vorab aus dem Finanzsektor und der öffentlichen Verwaltung, vertrauen auf die Kompetenz der TEMET AG

Authentisierungsverfahren



Ausgangslage «2013»

TEMET
end-to-end IT security

Authentisierung von Benutzern

- Authentisierungsverfahren kommen – und bleiben!
- Zunehmend unübersichtlicher «Zoo» von Verfahren
- One size does not fit all
  (Diversität der Anforderungen bzgl. Kosten, Convenience, Assurance, Functionality)
- Assurance Level schaffen Ordnung im Chaos
- Durch Entkopplung können Komplexität und Aufwand im Griff gehalten werden
  (Economies of Scale, Wieder-verwendbarkeit, Kernkompetenz)

Registrierung von Benutzern

- Die Zeit der zentralen Verwaltung aller Benutzer ist vorbei!
- Die Benutzer (= digitalen Identitäten) werden möglichst nahe an ihrem Vertrag verwaltet
- Mitarbeiter: HR System
- B2B Partner: Beim Partner!
  (sofern der Partnerschaftsvertrag auf Ebene «juristische Person» liegt)
  - Branchenverbände wie IG B2B oder FMH als Vermittler
- Privatkunden: ??
  - Einwohnerregister?
  - Communities?

Identity Provider

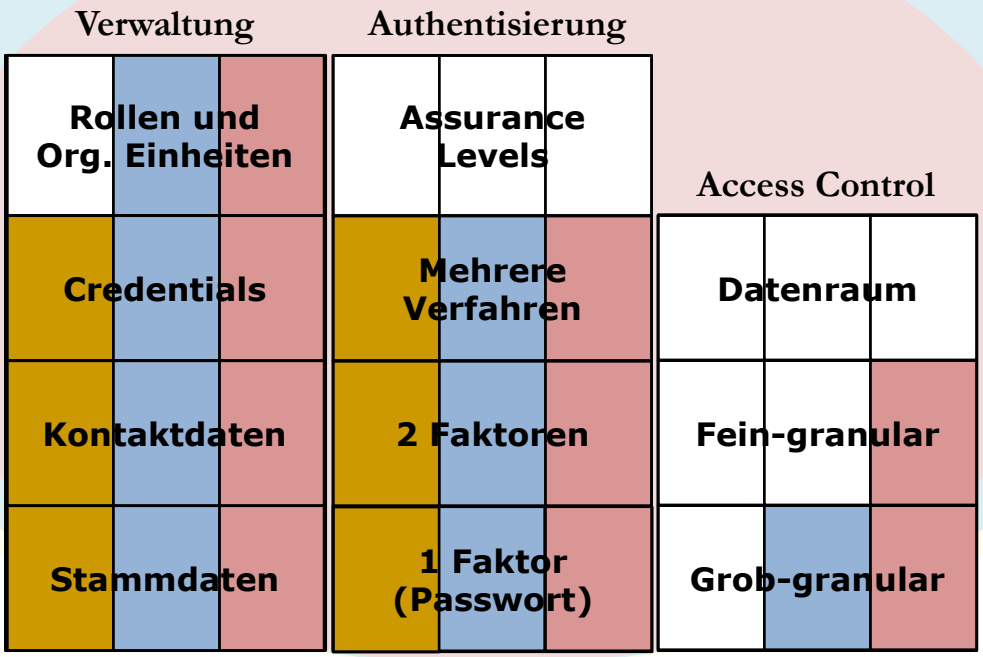
- *Identity Provider* unterstützen (sehr) *viele* Verfahren für die Benutzerauthentisierung
  - Achtung: Dies muss auch flexible und sichere Prozesse für die *Verwaltung* der unterschiedlichen Token umfassen!
- *Übergreifender* Single SignOn im Fokus
  - Identity Propagation über Bereiche/Domänen/Firmen… hinweg
  - Klammer über verschiedene (viele) Cloud-Anwendungen hinweg
- (Indirekte) Kontrolle über *Assurance Levels* nötig:
  - Assurance der *Verfahren* bzw. Token und der *Prozesse*
- Anwendungsbereiche:
  - *Corporate IdP:* Konsolidierung nach innen *und aussen*
  - *Closed user group IdP:* Vereinfachung von B2B Geschäftsprozessen
  - *Public IdP:* Social networking, eCommerce, eGov,…

Enter the Scene: Identity Provider

Public IdP, z.B. SuisseID

Closed User Group IdP, z.B. BrokerGate

Corporate IdP, z.B. SSO Portal



Business Case für Anwender
Business Aspekte

Einmalige Aufwände (Integrationsprojekt)

- Abbilden auf bestehenden Benutzer- und Partnerstamm
- Anpassen interner Prozesse, z.B. für Vertragsverwaltung
- Im Falle von BrokerGate: Abbildung auf interne Rechte

Wiederkehrende Einsparungen

- Benutzerverwaltung
- Tokenverwaltung und Login-Support (z.B. Passwort reset)
- Im Falle von BrokerGate: Berechtigungsverwaltung

Strategische / Qualitative Vorteile

- Konzentration auf Kerngeschäft und Fachanwendungen
- Verbesserte Datenaktualität und Datenqualität
- Branchenkonforme IT-Sicherheit
- Kundenbasis des IdP als Benutzerpotential

Business Case für Anwender
IT Aspekte

Einmalige Aufwände (Integrationsprojekt)

- **SSO-Anbindung, z.B. SAML Service Provider und dessen Integration in die bestehende Authentisierungs-Infrastruktur**
- **IMI-Anbindung, z.B. User Provisioning Webservice und dessen Integration in die bestehende IAM-Infrastruktur**

Wiederkehrende Einsparungen

- **Betrieb und Weiterentwicklung «starke Authentisierung»**
- **Betrieb und Wartung «delegierte Benutzerverwaltung»**

Strategische / Qualitative Vorteile

- **Verzicht auf Eigenbau für starke Authentisierung**
- **Verzicht auf Eigenbau für (delegierbare) Benutzerverwaltung**

Erfahrungen aus 12 BrokerGate Anbindungsprojekten

Durchschnittliche Projektdauer: ~9 Monate

- Grosse Spannbreite (3 bis 18 Monate)
- Konzept -> Realisierung -> Test -> Pilot -> Einführung

Recht unproblematische technische Anbindung

- SAML als gut standardisierte Technologie
- User Provisioning Webservice ist vergleichsweise simpel
- Geringer Betreuungsaufwand dank guter Dokumentation

Integration in interne IAM-Umgebung als Stolperstein

- Historisch gewachsene Autorisierungssysteme
- Technische Limitierungen, z.B. Länge der möglichen UserID
- Fehlende interne Automatisierung der Benutzerverwaltung erschwert die Bewältigung der erhöhten Mutationsrate

Thomas Kessler
Mobile +41 79 508 25 43
thomas.kessler@temet.ch

Besten Dank für Ihre Aufmerksamkeit!

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