TeleTrusT EBCA
European Bridge Certificate Authority

TeleTrusT-EBCA "PKI-Workshop"

Berlin, 26.06.2018

Authentifizierung mit und ohne PKI

Falk Goossens,

SecCommerce Informationssysteme GmbH,
SecSign Technologies AG

SecCommerce

SECSIGN

Die populärsten Authentifizierungsformen

- One-Time-Passwords (OTP): Per SMS, Hardware-Token, Apps
- Mobile Push-Authentifizierung - auch OTP- oder PKI-basiert
- Yubico Keys - FIDO - UAF und U2F

Häufige Einwände gegen PKI-basierte Authentifizierung

- Für Benutzer zu komplex (Was genau ist ein Zertifikat? Wie wird es installiert?)
- Zertifikate müssen zentral erstellt und dann auf die Clients übertragen werden
- Nur als Hardwarelösung wirklich sicher (Wie sichere ich den privaten Key bei einer Softwarelösung?)

Häufige Einwände gegen PKI-basierte Authentifizierung

- Hohe administrative Kosten (Verknüpfung der 2FA für Benutzer / Verknüpfung mit dem IDM)
- Extrem aufwändige Integration seitens des Services und des Clients

Wie kann eine PKI-basierte Authentifizierung aussehen?

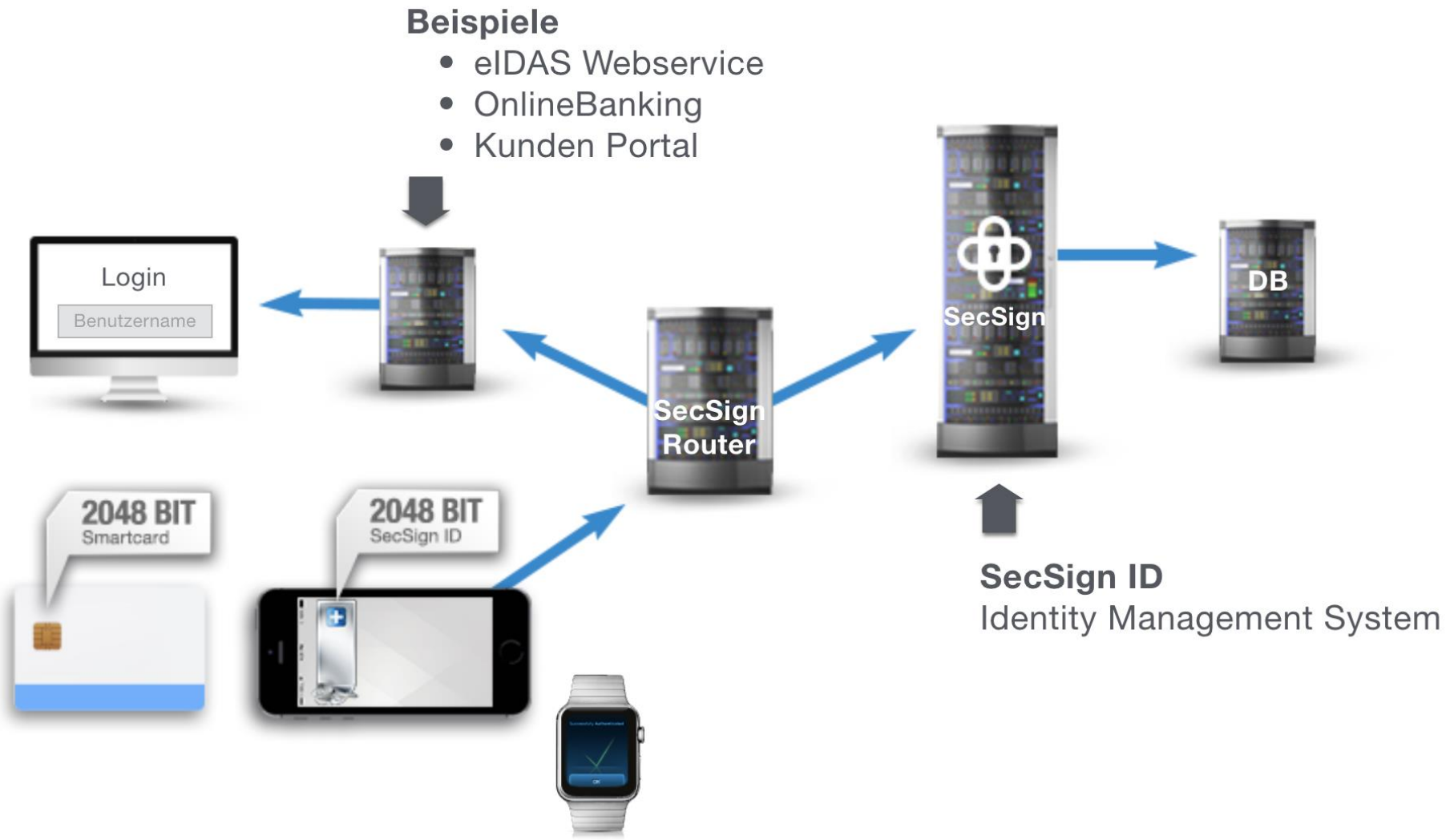
- Hardwarebasiert (z.B. als Smartcard = extrem hohes Sicherheitsniveau)
- Softwarebasiert (z.B. als Smartphone App / Desktop App)

Wie kann eine PKI-basierte Authentifizierung aussehen ?

- Live-Vorführung der smartphonebasierten 2FA-PKI anhand eines abgesicherten Jira-Logins und des SecSign Portals

- URL’s:
- secsign.com
- portal.secsign.com

Wie kann eine PKI-basierte Authentifizierung aussehen ?



Was sind bei einer PKI-basierten 2FA die beiden Faktoren?

- Privater Key und App-Zugriffsschutz (z.B. PIN oder Fingerabdruck)
- OTP: Der Zugriff auf das Handy und das Passwort für die Website

Vorteile der Authentifizierung ohne PKI

- Bei OTP via SMS kaum Anforderungen an Endgerät
- OTP Hardware-Token günstiger als Smartphone
- Hardware-Token leichter und günstiger zu verwalten als Diensttelefone

Vorteile der PKI-basierten Authentifizierung:

- Zertifikat und Schlüsselmaterial für Authentifizierung, Signatur und Verschlüsselung (Was mache ich bei OTP?)
- Trotz Erhöhung des Sicherheits-niveaus kann das Login für den Benutzer sogar noch komfortabler werden
- Komfortable Verknüpfung mit digitalen Identitäten und bestehendem IDM