KoSIT

Koordinierungsstelle für IT Standards
in Bremen

Freie Hansestadt Bremen

S.A.F.E.

Beate Schulte
Koordinierungsstelle für IT-Standards (KoSIT)

XÖV-Anwenderkonferenz 2011, Bremen

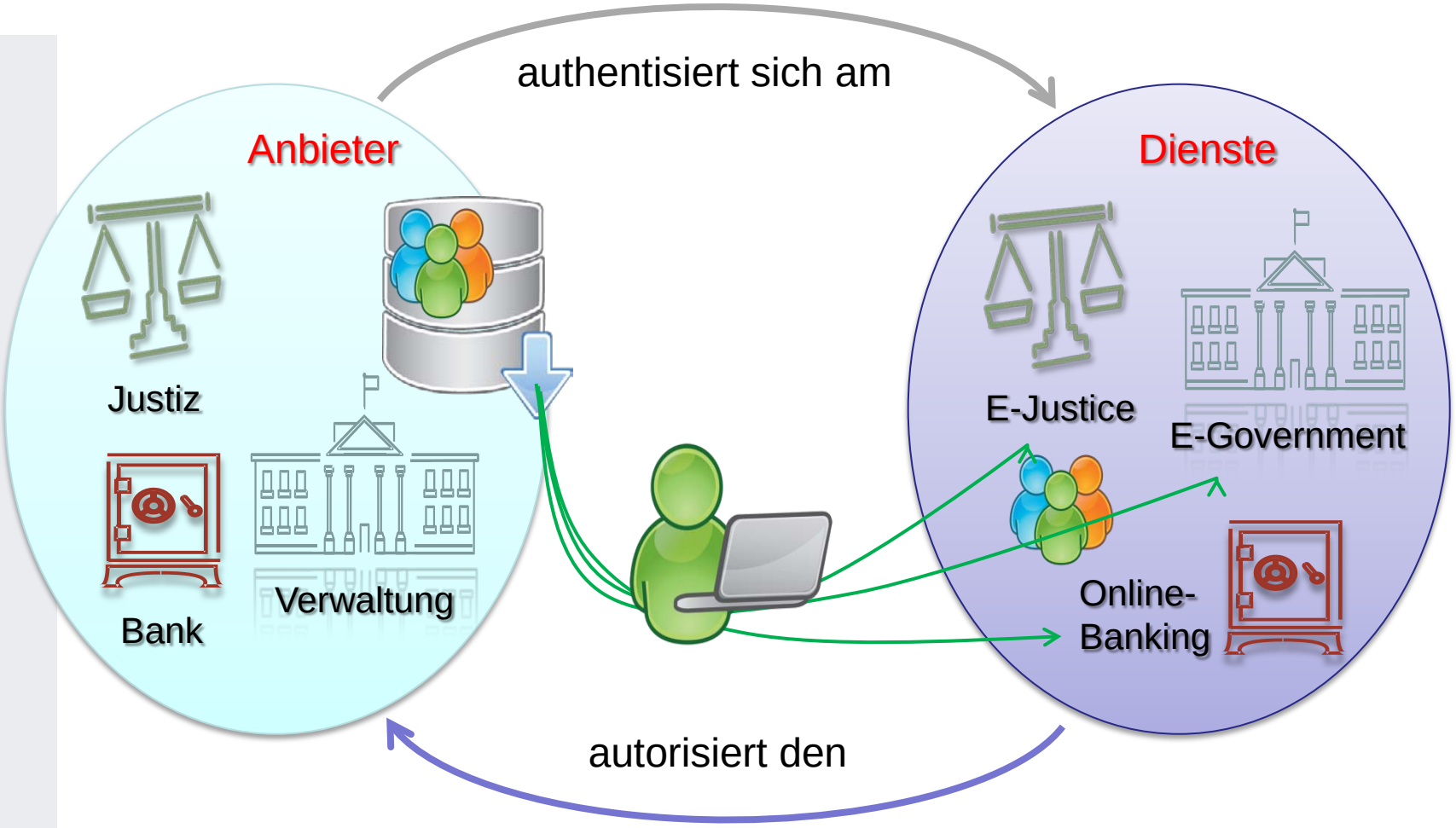
KoSIT

Herzlichen Dank!

Projektleitung S.A.F.E.: Meinhard Wöhrmann
(meinhard.woehrmann@olg-duesseldorf.nrw.de)

KoSIT

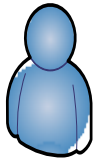
Was ist S.A.F.E. ?



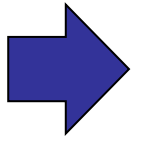
KoSIT

Identity-Management sprengt Applikationsgrenzen (I)

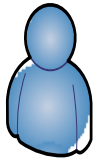
- Benutzerin möchte 3 verschiedene Anwendungen nutzen.
- Dazu muss sie sich 3x anmelden.



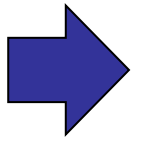
ID = govello-1212121
Name = Mustermann
Zertifikat = 2w3er45tz….



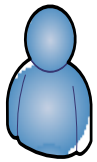
Anwendung A



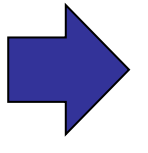
ID = MusterM
Name = Mustermann
E-Mail = max.m@wxc.de….



Anwendung B



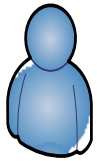
ID = mmogus
Kundennumer = 132234
Modemarke = Boss….



Anwendung C

Identity-Management sprengt Applikationsgrenzen (II)

- Identity Management verschmilzt die Benutzerprofile zu einer „Identität“.



ID-A = govello-1212121

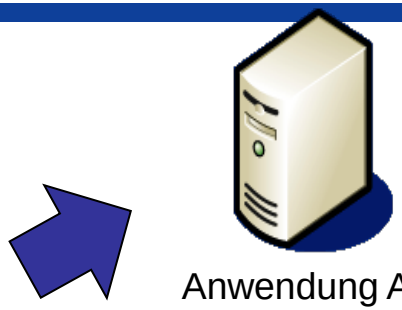
ID-B = mmogus

ID-C = MusterM

Kundennumer = 132234

E-Mail = max.m@wxc.de

Modemarke = Boss….



KoSIT

Identity-Management

„Identity-Management ist in der Informationstechnologie die Disziplin, die sich mit der **ganzheitlichen Verwaltung** Digitaler Identitäten befasst.“

- Erzeugen, registrieren, ändern und löschen
- Zuordnen von Rollen, Rechten und Eigenschaften
- Bereitstellen und verteilen
- Verwenden und überprüfen

KoSIT

Identity-Management

„Identity-Management ist in der Informationstechnologie die Disziplin, die sich mit der ganzheitlichen Verwaltung **Digitaler Identitäten** befasst.“

- Personendaten (Name, Kontaktdaten, etc.)
- Eigenschaften (Justizbedienstete, angemeldeter Nutzerin, etc.)
- Mittel der Authentisierung (Passwörter, Zertifikate, Smart-Cards, etc.)

Identifikation bzw. Authentisierung

- Kann **meine Anwendung** den Nutzer authentifizieren ?
  - Kennt meine Anwendung die identifizierte Nutzerin?
  - Reichen ihre Eigenschaften, ihre Rolle (Attribute) aus?

KoSIT

Was leistet S.A.F.E.?

- Datenbank für Identitäten (Benutzer) und Attribute (Benutzerdaten)
- Sichere Anmeldung zur Nutzung
  - von Kommunikationsdiensten
  - und anderen Services
- Abruf von Listen registrierter Benutzer und ihren Daten
- Flexibel und erweiterbar für beliebige Anwendungen und Anbieter
- Detaillierte Modellierung von Zugriffsrechten auf gespeicherte Daten
- Identity-Management-System / Single-Sign-On

⇒ **Secure Access to Federated E-Justice/E-Government**

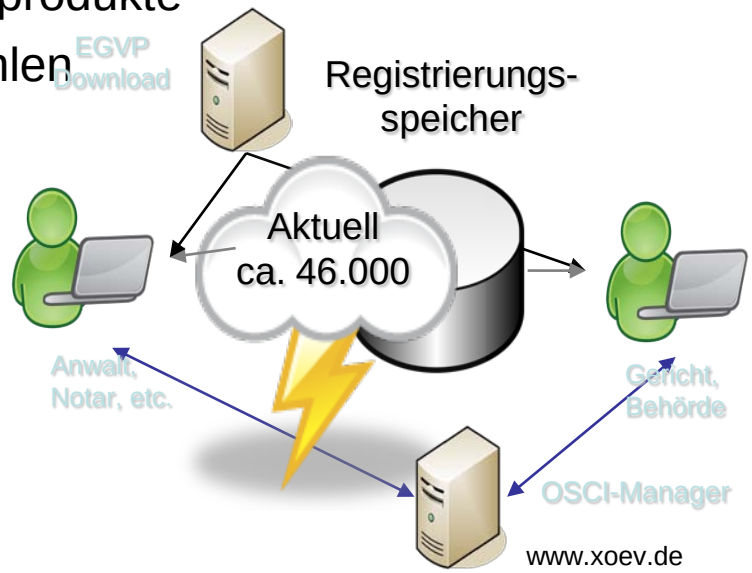
Wo wird S.A.F.E. eingesetzt? (I)

Seit 18.06.11 abgelöst: **EGVP-Registrierungsserver**

- Alle EGVP-Benutzer in einer Datenbank
- Proprietäre Schnittstellen zum EGVP-Client
- Benutzerattribute streng auf EGVP ausgerichtet
- Direkte Verzahnung zwischen EGVP und EGVP-DB

→ Keine Integrationsmöglichkeit für Fremdprodukte

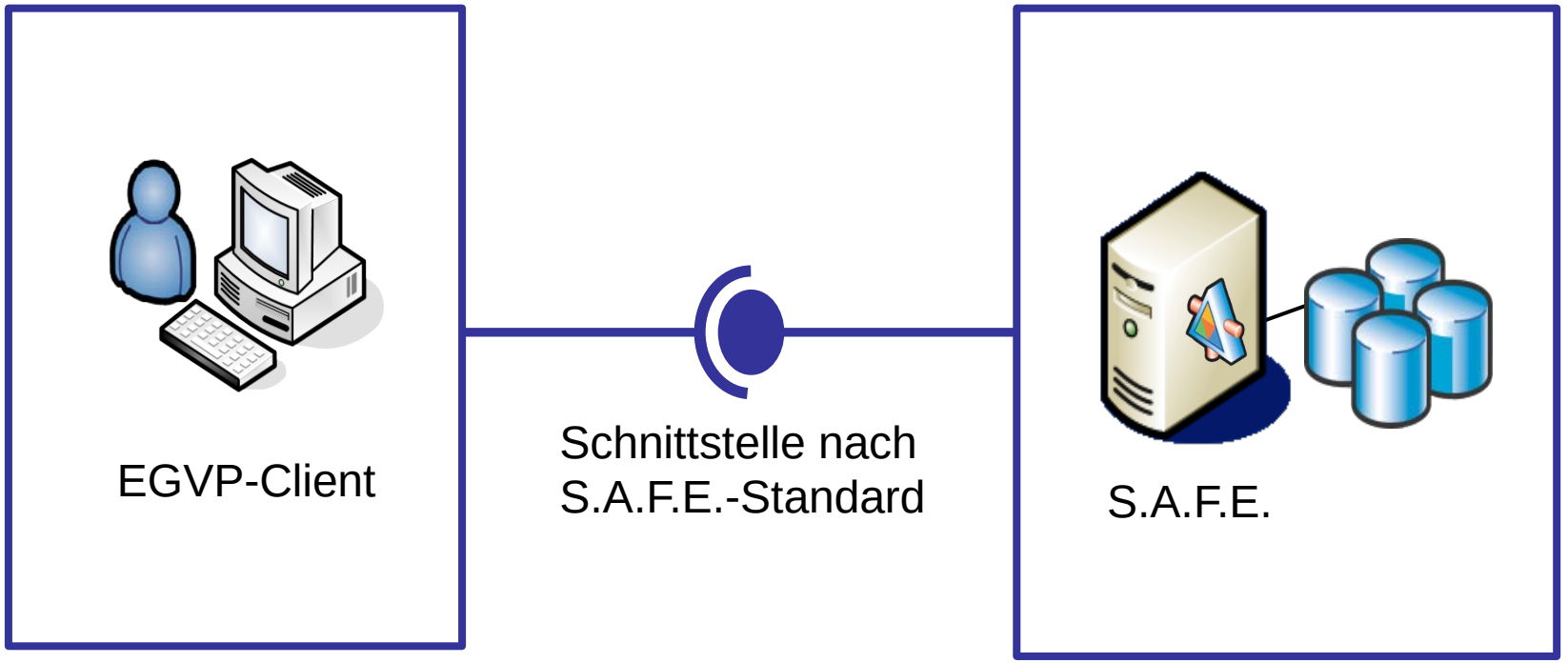
→ Starke Beschränkung bei den Nutzerzahlen



KoSIT

Wo wird S.A.F.E. eingesetzt? (II)

- S.A.F.E. entkoppelt den EGVP-Client von Benutzerdaten
- S.A.F.E. bietet eine universell nutzbare Schnittstelle



KoSIT

Wo wird S.A.F.E. eingesetzt? (III)

1. EGVP 2.6.0.2 seit dem 18. Juni **2011**
   - Adresssuche des Empfängers, Prüfung der Absenderadresse
2. Zentrales Testaments- und Vorsorgeregister – ab **2012**
   - bei der Bundesnotarkammer geführte Register ZTR/ZVR
   - Abfrageerfordernis durch Fachabteilungen der Justiz
3. Zentrales Vollstreckungsportal – ab **2013**
   - Einreichungen bei zentralen Vollstreckungsgerichten der Länder
     - Vermögensverzeichnisse durch Gerichtsvollzieher
     - Eingaben von Vollstreckungsbehörden (z. B. Finanzämter)
   - Auskünfte aus dem Vollstreckungsportal für Einsichtsberechtigte
4. Industrie- und Handelskammern, Bundesrechtsanwaltskammer („**künftig**“)
   - Registrierung
5. In EU-Projekten: D.I.M., e-Codex

KoSIT

Wie arbeitet S.A.F.E. ?

- S.A.F.E. nutzt behauptete Eigenschaften von Identitäten
- S.A.F.E. erzeugt aus den Eigenschaften elektronische Ausweise (Token)

Behauptung 1: **Name = Schulte**

Behauptung 2: **Vorname = Beate**

Behauptung 3: **E-Mail = beate.schulte@finanzen.bremen.de**

Behauptung 4: **Position = Referentin für Sicherheit**

Behauptung N: **... usw.**

- S.A.F.E. ist ein Identity Management System mit Standard-Services
  - für den Austausch von Token: **Secure Token Service**
  - für die Erzeugung und Änderung von Identitätsdaten: **Provisioningservice**
  - für die Suche nach Eigenschaften und Identitäten: **Attributservice**

KoSIT

S.A.F.E. basiert auf internationalen Standards

- S.A.F.E. nutzt den internationalen Webservice-Stack („WS-*“) Standard
- S.A.F.E. – Token sind nach dem SAML*-Standard beschrieben

  *(*Security Assertion Markup Language)*
- S.A.F.E. profiliert die Token aus der internationalen Beschreibung des Personal Profile der Liberty Alliance
- Token werden in SOAP*-Nachrichten übermittelt

  *(*Simple Object Access Protocol)*

KoSIT

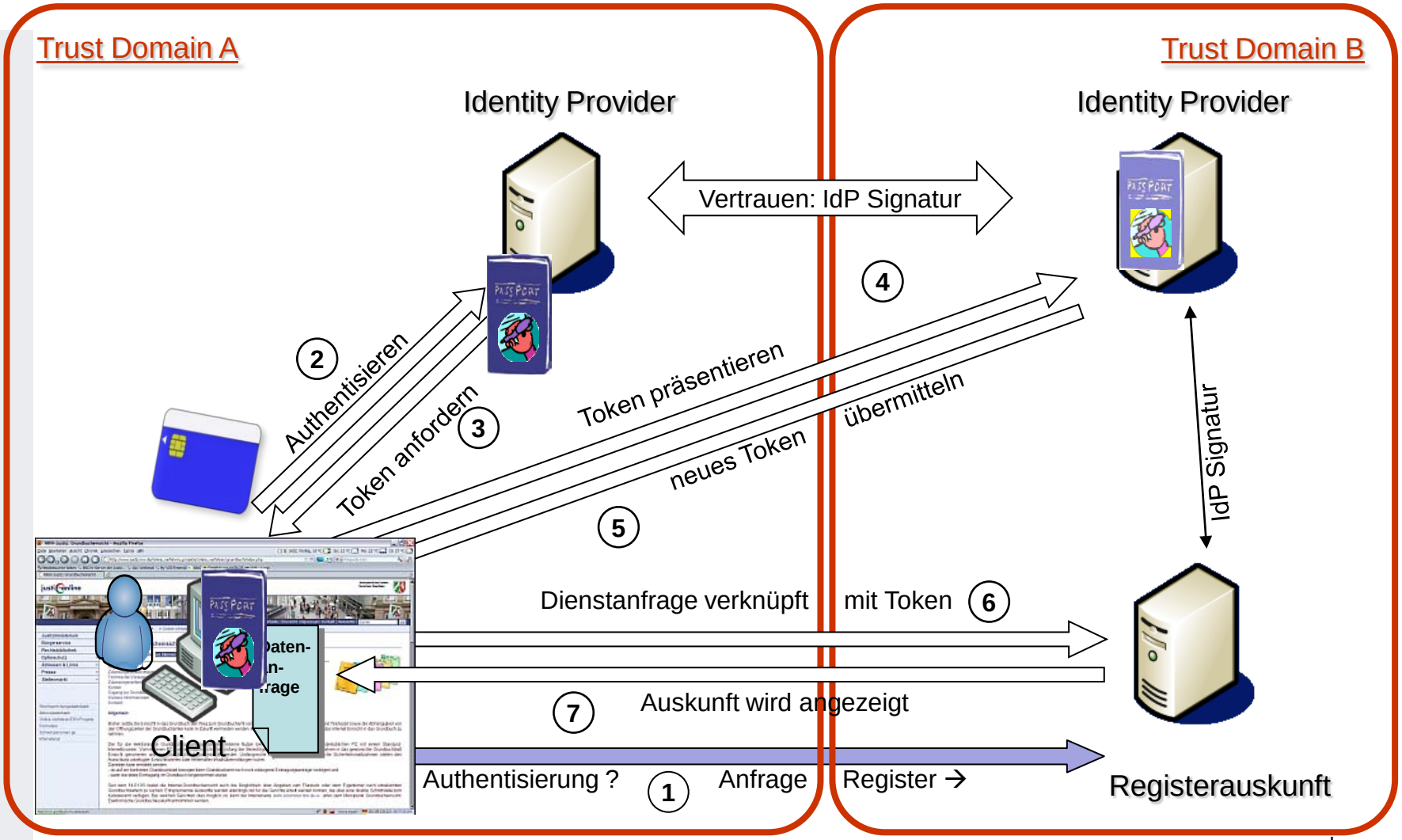
S.A.F.E.: Wie geht‘s weiter ?

- Anbindung unterschiedlicher Identity-Stores (LDAP etc.)
- Anmeldung mit dem nPA (Authentisierungsstufe hoch)
- **Föderation** mehrerer S.A.F.E. Instanzen
- **Föderation** mit anderen Identity Management Systemen

S.A.**F.**E.

KoSIT

Föderierter Service



KoSIT

S.A.F.E. in der Verwaltung

BLK für Datenverarbeitung und Rationalisierung in der Justiz:

- „Die Bund-Länder-Kommission hat (…) bekräftigt, künftig in allen elektronischen Kommunikationsbeziehungen S.A.F.E. einzusetzen; **die Nutzung durch andere öffentliche Verwaltungen ist kostenfrei möglich.“**

S.A.F.E. ist seit 2010 ein „Koordinierungsprojekt“ des IT-Planungsrates

Beschluss in 6.Sitzung des IT-Planungsrates (13.10.2011):

- „Der IT-Planungsrat sieht in S.A.F.E. **eine wesentliche** Komponente eines übergreifenden eID-Systems **für Verwaltung und Wirtschaft**.“

Errichtungskonzept der KoSIT:

- „Entwicklung eines Konzeptes zur Zusammenführung bestehender Verzeichnisdienste“

KoSIT

Koordinierungsstelle für IT Standards
in Bremen

Freie Hansestadt Bremen

Weitere Informationen zu S.A.F.E.
insbesondere auf www.justiz.de !

Herzlichen Dank für Ihre Aufmerksamkeit!