Identity Management

Nutzen – Konzepte –Standards

Dr. Oliver Stiemerling

ecambria systems GmbH
Hospeltstr. 35a
50825 Köln
Tel.: 0221 595527-0
Fax.: 0221 595527-5
os@ecambria-systems.com

http://www.ecambria-systems.com

- Was ist Identity Management?
- Beispiel Online-Banking
- Grundlegende Konzepte
  - Authentifizierung
  - Delegation
  - Single Sign On
  - Föderation
- Standards

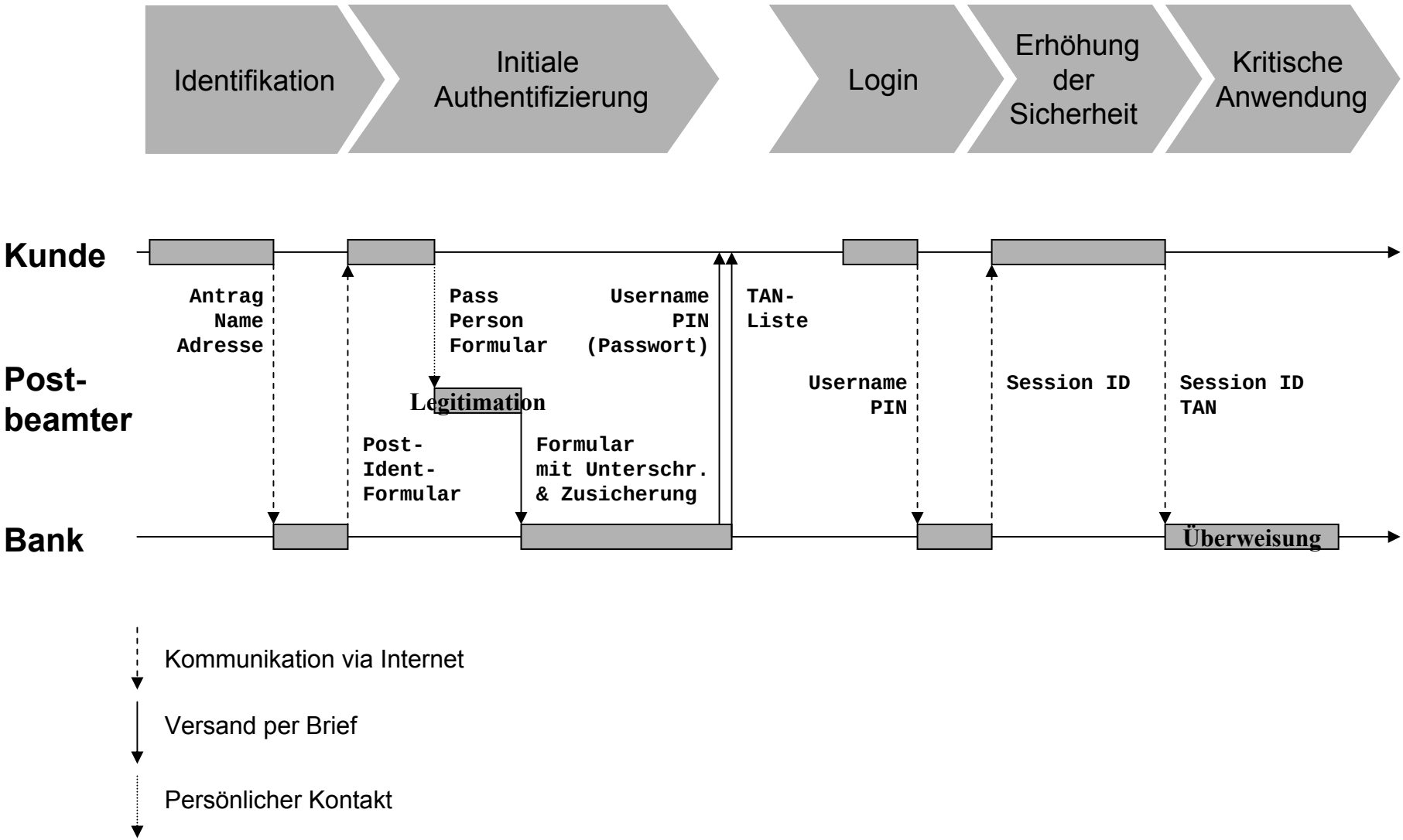
Was ist *Identity Management*?

- Motivation: Viele netzwerkbasierte Anwendungen benötigen zwingend die Identität der Benutzer:
  - eCommerce / Shopping / Auktionen
  - eCRM (Customer Relationship Management)
  - Electronic Banking
  - Mitarbeiterportale
  - Personalisierte Informationsdienste
  - Kommunikationsdienste (Email)
  - B2B-Gateways (Maschine-Maschine Schnittstellen zwischen Unternehmen)
  - ...

- Definition von Identitätsmanagement

„*Konzepte, Methoden und Technologien zur Authentifizierung, Autorisierung und Beschreibung (Attribute) von Identitäten*“

Identity-Management am Beispiel Online Banking



Verfahren zur Authentifizierung (kleiner Ausschnitt...)

- Verfahren zur initialen Authentifizierung einer Identität:
  - Persönliche Legitimation per Ausweis und Vergleich mit Person
  - Neutrale, dritte Instanz bürgt (Postbeamter, Notar, Personalabteilung...)
  - Einseitiges, operatives „Geheimnis“ (z.B. Kreditkartennummer und Name)
  - Gemeinsames „Geheimnis“ (z.B. Betrag der letzten Rechnung)
  - Alternativer Kommunikationsweg (Brief, „Überweisung“ des Passworts, SMS an Handy, ...)
- Verfahren zur laufenden Authentifizierung
  - Passwort, TAN (*Wissen*)
  - SmartCard, privater RSA-Schlüssel (*Besitz*)
  - Biometrische Verfahren – Gesicht, Fingerabdruck, Iris, DNA (*Sein*)
- Verfahren zur technischen Authentifizierung
  - Session ID (im Web z.B. in der URL oder in einem Cookie)
  - Kryptographischer Authentifizierungstoken (Cross-Domain)
- Einflussfaktoren bei der Wahl des Verfahrens
  - Bequemlichkeit für den Kunden (Usability)
  - Kosten des technischen und organisatorischen Verfahrens
  - Kosten des Missbrauchs (Kommerziell vs. Datenschutz)
  - Juristische Durchsetzbarkeit

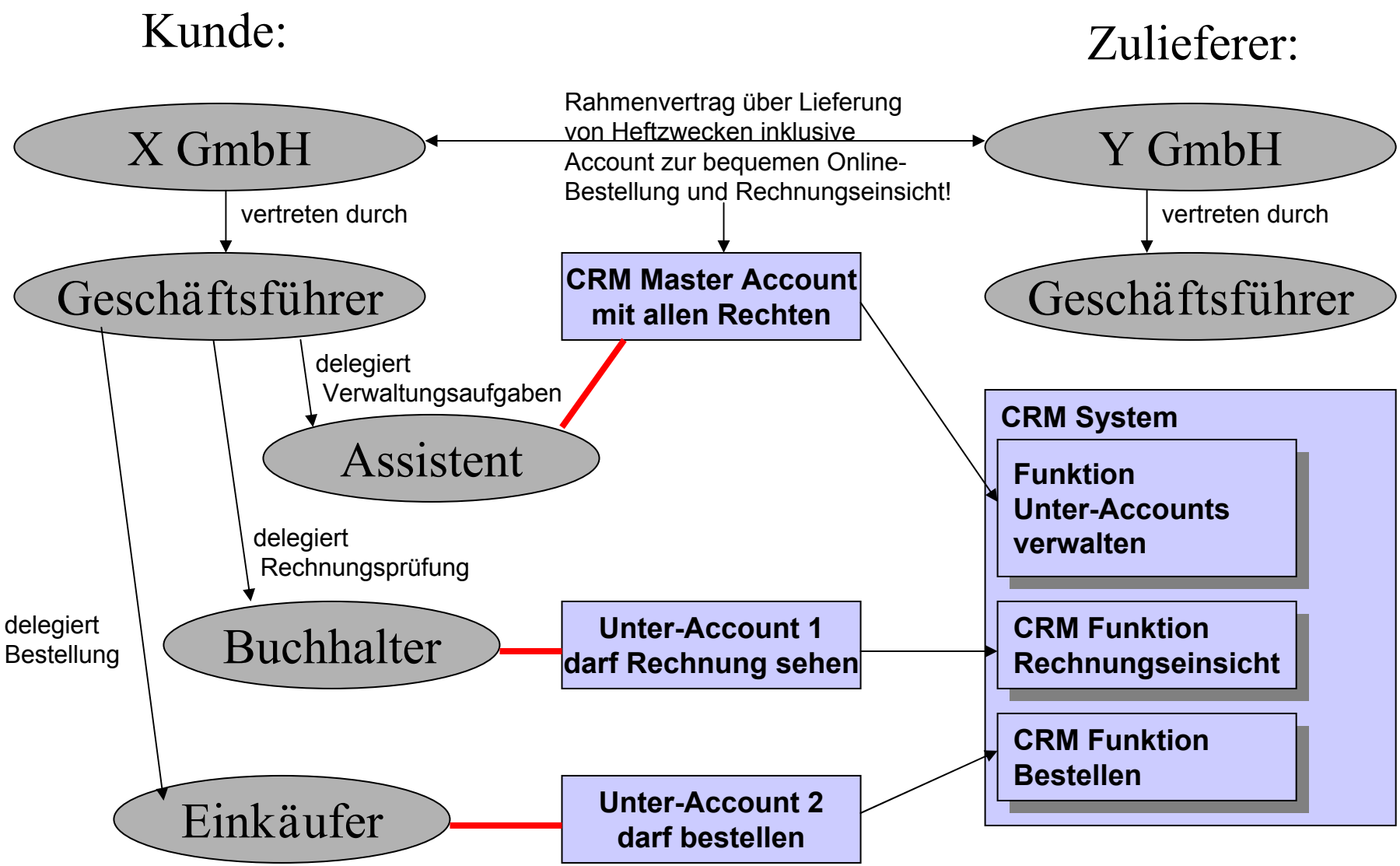
Problemfeld: Die Authentifizierung von juristischen Personen (GmbH, AG, e.V. etc.)

- Problem: Juristische Personen haben keine Personalausweise oder biometrischen Merkmale und führen selbst keine Handlungen aus.
- Lösung: Juristische Personen haben natürliche Personen, die als offiziell Bevollmächtigte für die juristische Person handeln dürfen (Geschäftsführer, Vorstände, Prokuristen...)
- „Authentifizierungspfad“ bei juristischen Personen:
  - Handelsregisterauszug / Vereinsregisterauszug (möglichst original)
  - enthält Name und Anschrift der Bevollmächtigten
  - Personalausweis des Bevollmächtigten

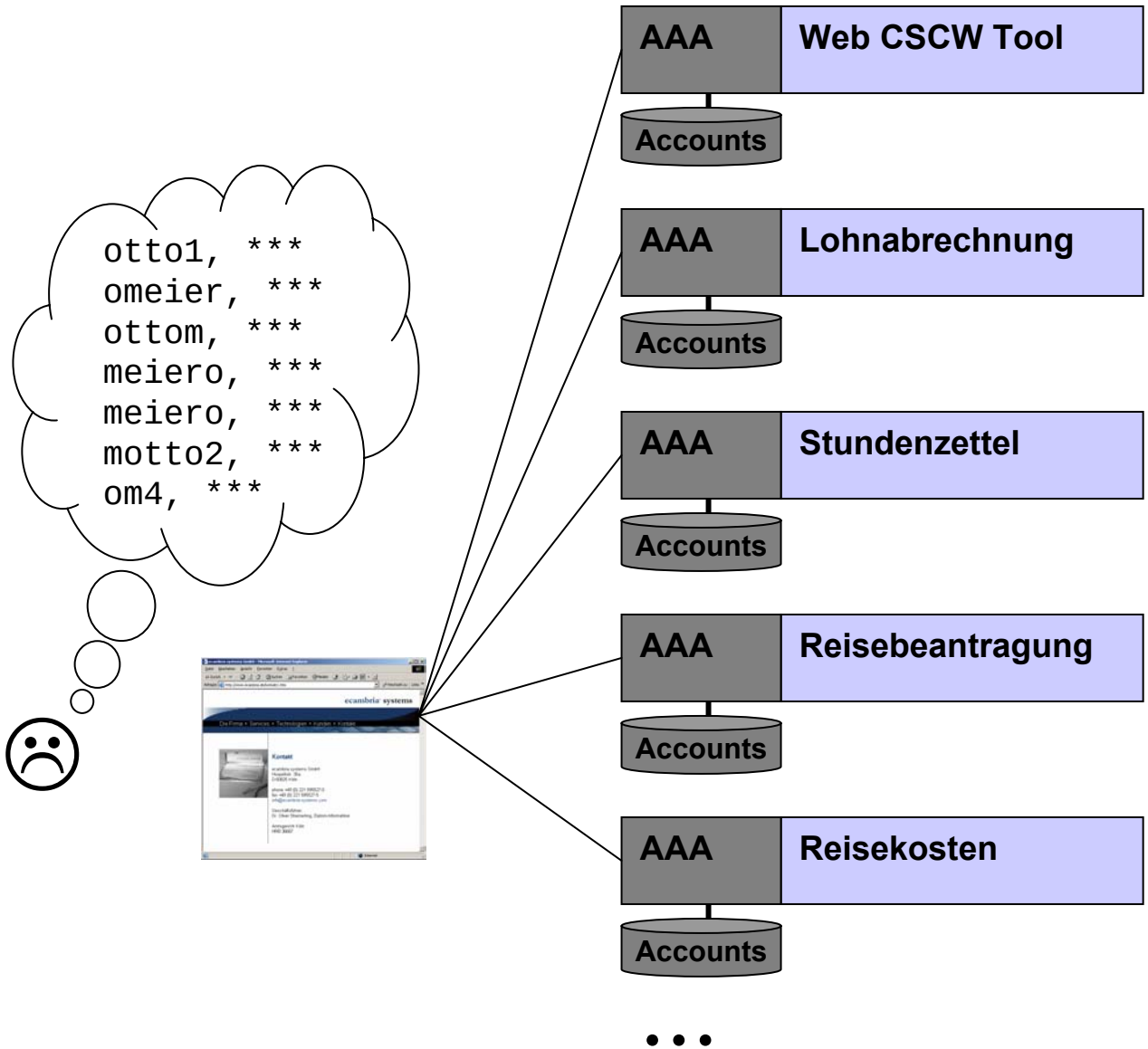
- Problem: Ein Geschäftsführer kann nicht alles selbst machen
- Lösung: Er delegiert einen Teil seiner Aufgaben

- Problem: Der Mitarbeiter, der die delegierte Aufgabe bearbeitet, soll nicht auf alles Zugriff haben.
- Lösung: Das Identitäts Management System erlaubt die Einrichtung von “Unter-Accounts” mit eingeschränkten Rechten.

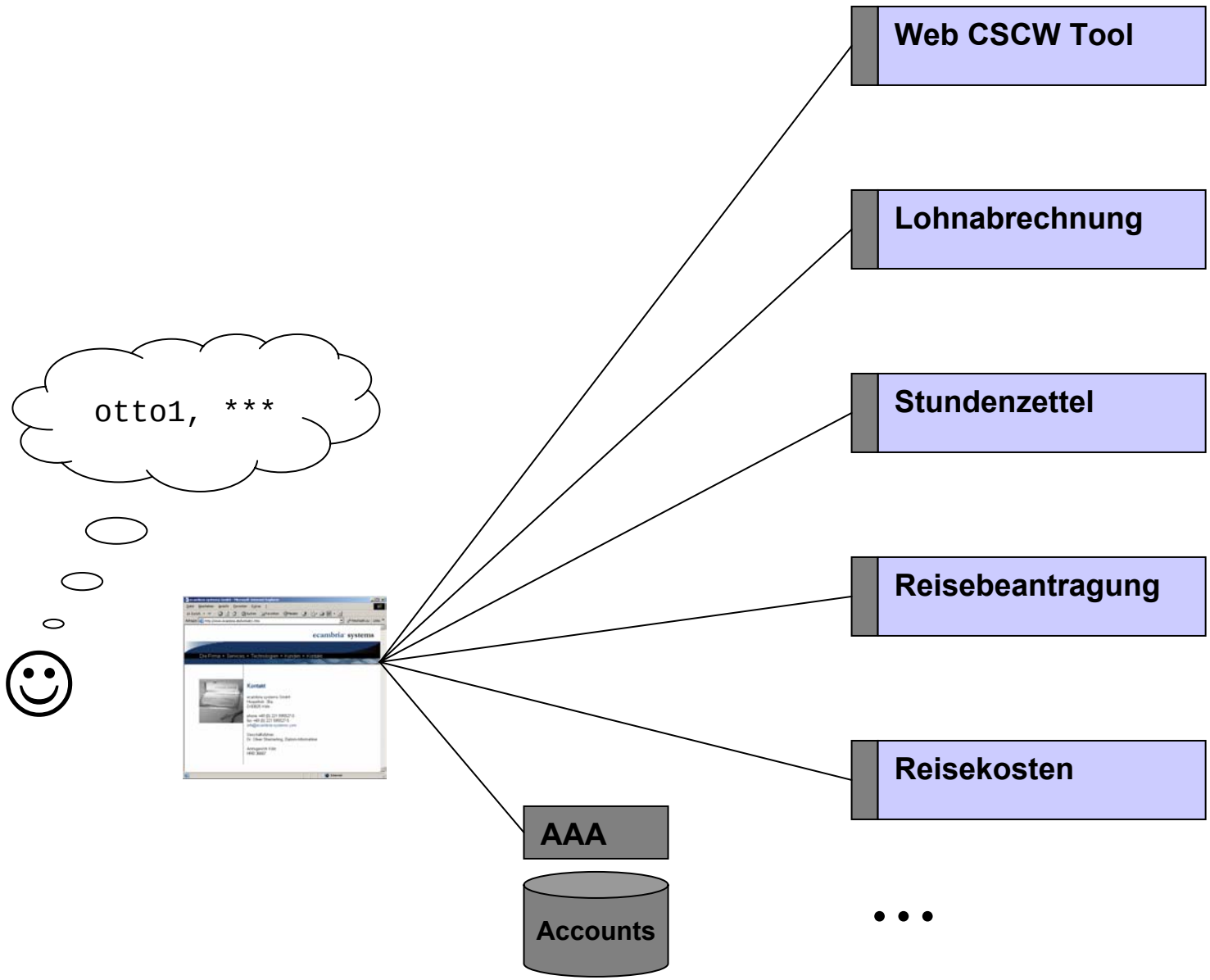
Delegation am Beispiel eines CRM Systems eines Büromaterialzulieferers



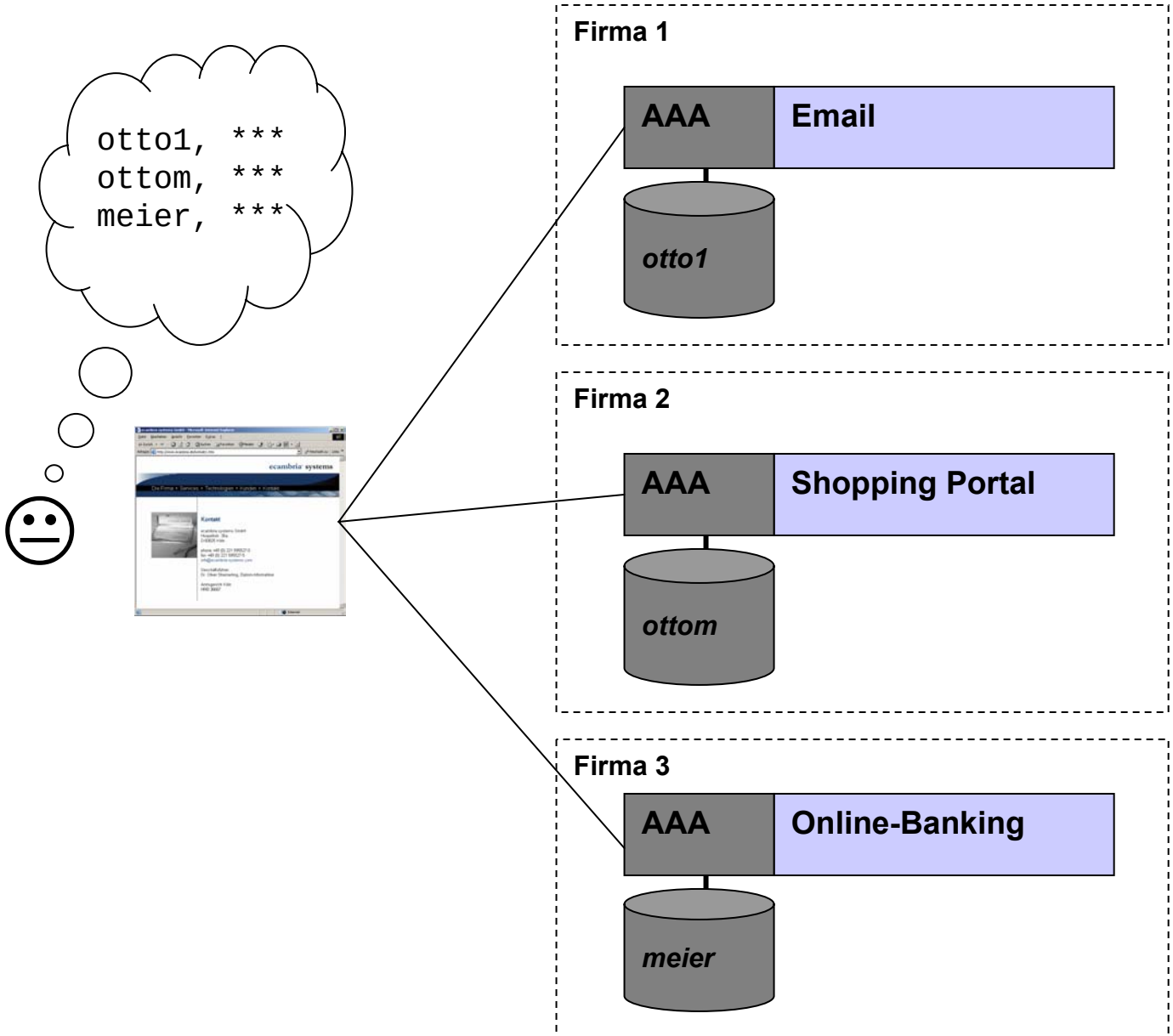
Single Sign On am Beispiel einer Intranetanwendung: Vorher



Nach Einführung von SSO: Nur noch einen Account für alle Anwendungen

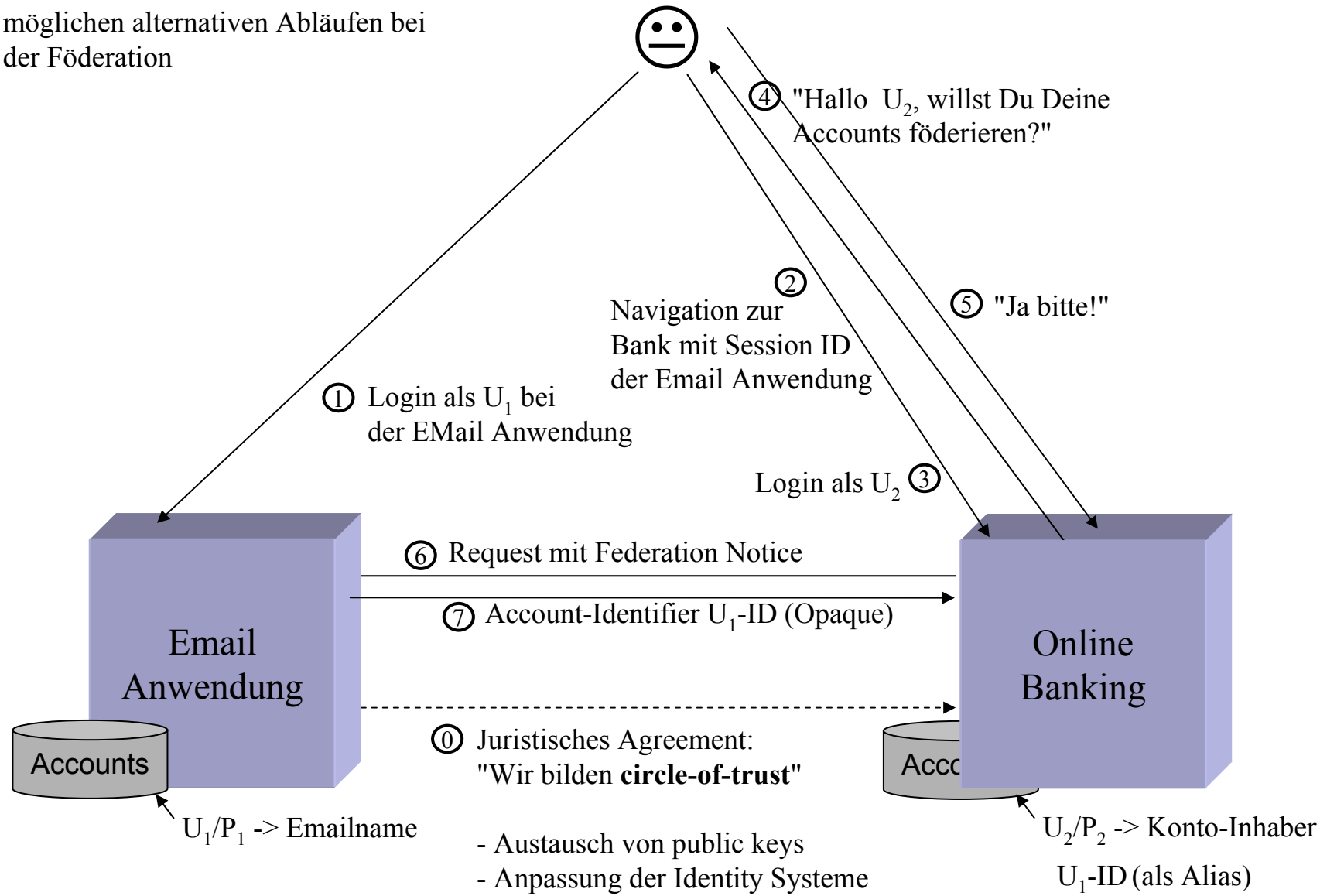


Föderation: Single Sign On über zwei oder mehr Account-Datenbestände

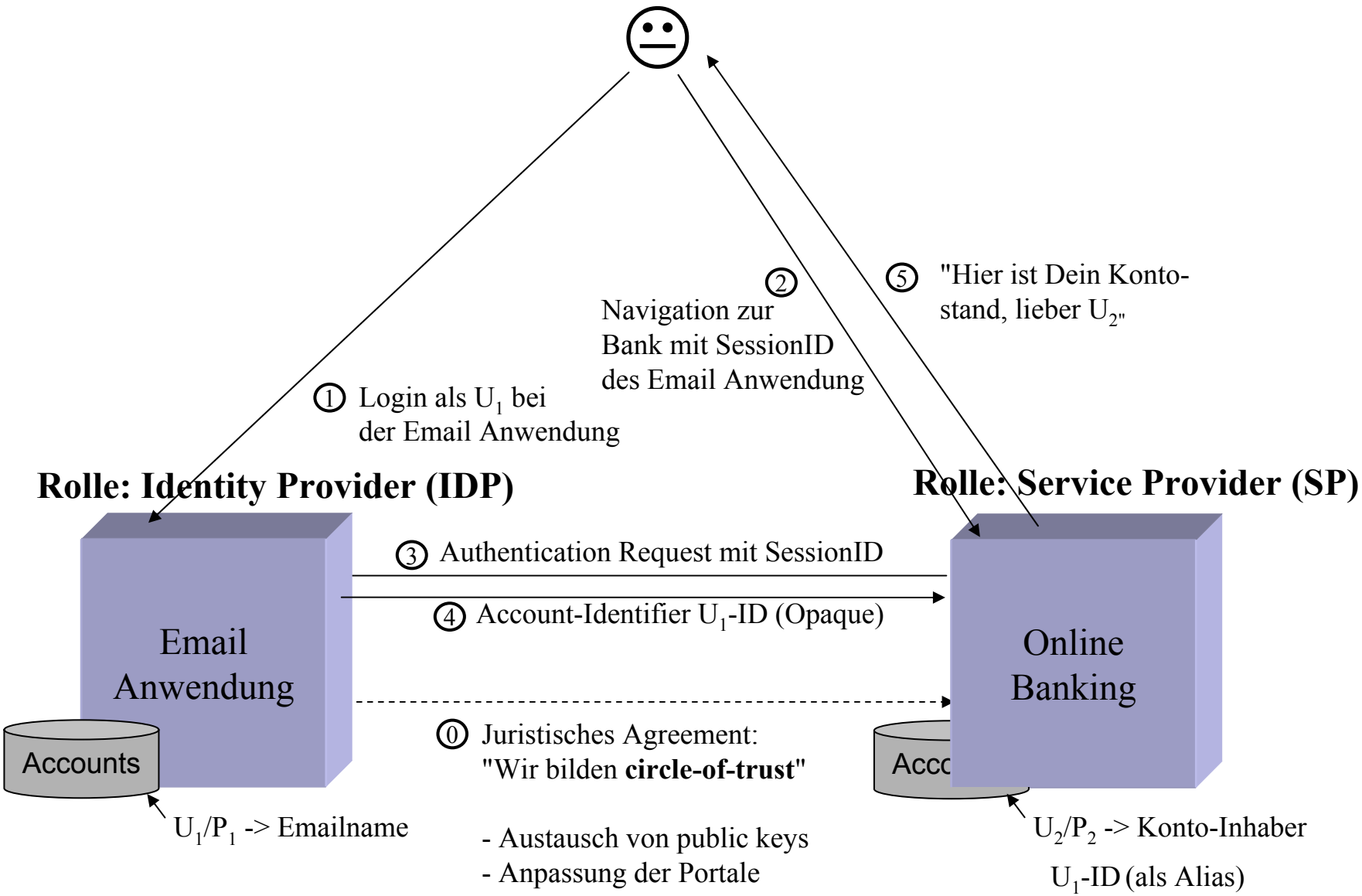


Ablauf einer Föderation

Hinweis: Dies ist nur einer von mehreren möglichen alternativen Abläufen bei der Föderation



Single Sign On nach einer Föderation



Standards im Kontext von Identity Management: SAML

- SAML = "Security Assertion Markup Language"
  - XML-Schemata zur Beschreibung sicherheitsrelevanter Information über Identitäten
    - Authentifizierung (Zusicherung der Identität)
    - Autorisierung (Rechte der Identität)
    - Attribute (Eigenschaften der Identität)
  - Interaktionsprotokolle und Transport-Bindings
    - Transport per SOAP über sicheren Server-Server-Kanal
    - Transport über Browser-POST
- Quelle: OASIS "*Organization for the Advancement of Structured Information Standards*" (non-profit Standardisierungsgremium)
- Ursprünglich intendierte Use Cases:
  - Singe-Sign-On
  - Verteilte Business Transaktionen
  - Autorisierungsservice

Standards im Kontext von Identity Management: Liberty Alliance Project

- Die Protokolle im Liberty Alliance Project basieren auf SAML
- Föderation
- Single Sign On
- Global Logout
  - Ein zentrales Logout kann beim IDP angestoßen werden
  - Es loggt den Benutzer aus allen SP-Sessions aus.
- Deföderation
  - Effekt: Opaque User-ID wird gelöscht
- Identity Provider Introduction Protocol
  - Common Domain Cookie (CDC) Ansatz
  - Ein IDP von vielen sagt "*Der User ist bei mir angemeldet*!"
  - Ein SP überprüft den CDC auf einem zentralen System und handelt entsprechend (Redirect des Nutzer zum relevanten IDP)

=> Komplexes Protokoll. Viele Konfigurationsmöglichkeiten und Topologien

Zusammenfassung

- Identity Management ist eine wichtige Basis für viele Netzwerkanwendungen
- Komplexes, interdisziplinäres Designproblem
- Grundlegende Konzepte in den Bereichen:
  - Authentifizierung
  - Delegation
  - Single Sign On
  - Föderation
- Standards
  - SAML: Security Assertion Markup Language
  - Liberty Alliance Project