Identity Management

Prof. Dr. Norbert Pohlmann
Fachbereich Informatik
Verteilte Systeme und Informationssicherheit

Fachhochschule Gelsenkirchen

Inhalt

- Definitionen & Notwendigkeit
- Key Concepts
- Single Sign-On
- Circle of Trust
- Microsoft .Net Passport
- Liberty Alliance
- Zusammenfassung

Inhalt

- **Definitionen & Notwendigkeit**
  - Key Concepts
  - Single Sign-On
  - Circle of Trust
  - Microsoft .Net Passport
  - Liberty Alliance
  - Zusammenfassung

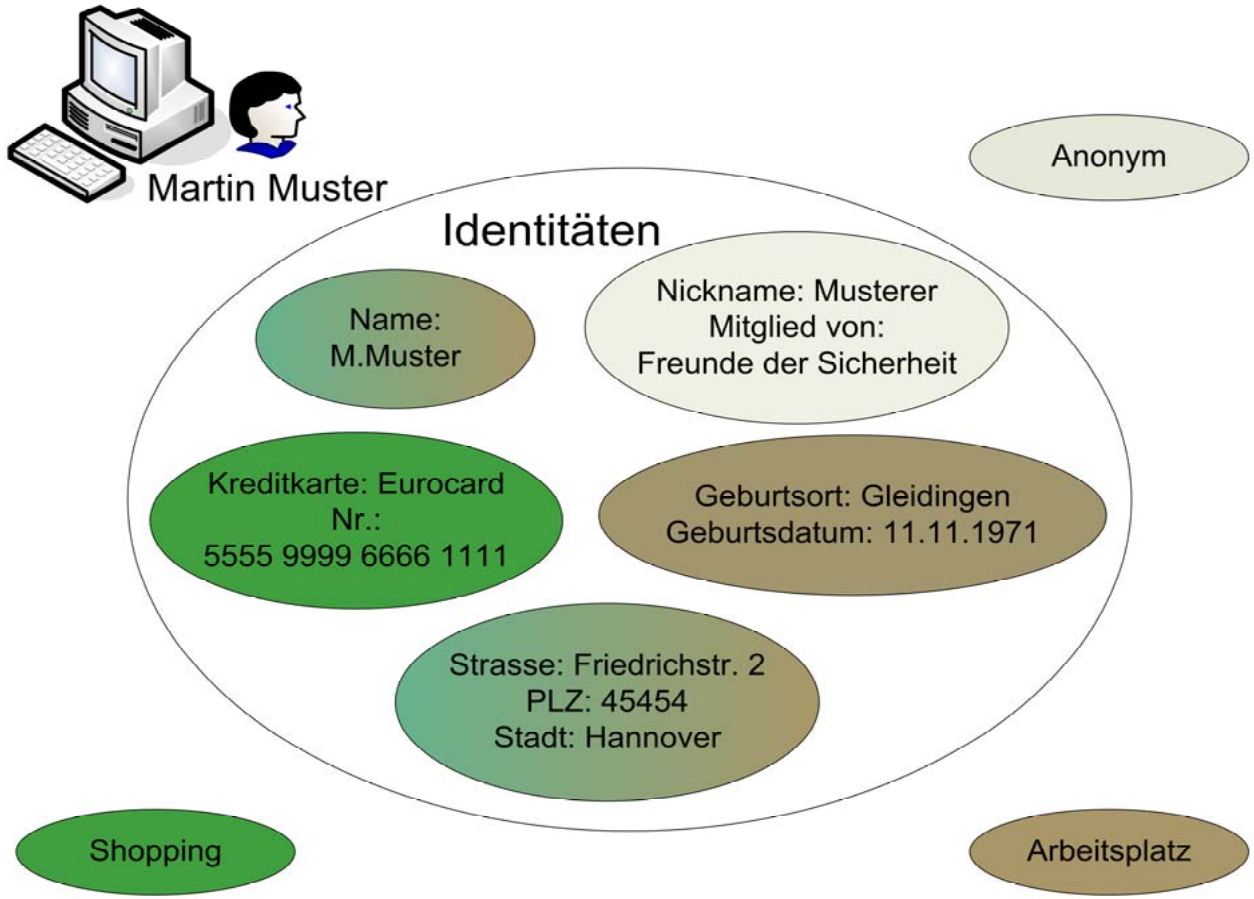
Definitionen

- **Identity Management**
  - In der Fachwelt hat sich bisher keine einheitliche Auffassung, was exakt unter Identity Management zu verstehen ist, durchgesetzt
  - *Der Begriff Identity Management beschreibt jeglichen Einsatz von digitalen Identitäten und deren Berechtigungen, sowie deren Pflege, Erzeugung, Nutzung und Löschung.*
  - *Das hierbei verfolgte Ziel ist es vertrauenswürdige, identitätsbezogene Prozesse plattformübergreifend und standardisiert, nutzbar zu machen [TeleTrusT-Verein].*

- **Digitale Identität**
  - Eindeutige Datensätze, bestehend aus global verfügbaren personen- oder objektbezogenen Attributen
  - Beispiele: Benutzername und Passwort, Zertifikat, Attribute, ...

Notwendigkeit (1/3)

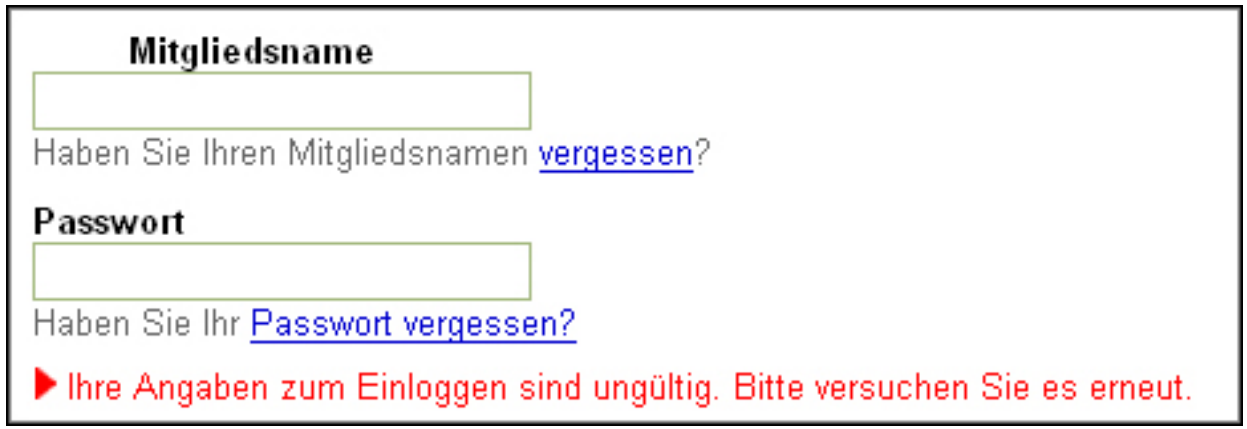
- Einfaches Szenario, warum Identity Management Systeme benötigt werden



Notwendigkeit (2/3)

- Unüberschaubare Mengen an Benutzerkonten
- Passwörter & Accounts werden vergessen
- Einfache & immer gleiche Passwörter

  → Identitätskollaps



Notwendigkeit (3/3)

- Folgen:
  - → Erhöhte Kosten
  - → Komfortverlust
  - → Steigender Administrationsaufwand
  - → Fehlende Kontrolle
  - → Informations- bzw. Datenverlust
  - → Sicherheitsrisiko

Inhalt

- Definitionen & Notwendigkeit
- **Key Concepts**
- Single Sign-On
- Circle of Trust
- Microsoft .Net Passport
- Liberty Alliance
- Zusammenfassung

Key Concepts
→ Anforderungen

- sichere Authentikation
- komfortable Authentikation
- strukturierte Identitäts-Datenspeicherung
- strukturierte Identitäts-Datenverwaltung
- Zusammenführung von Identitätsdaten

Key Concepts
→ Struktur und Technologie

- Struktur
  - Identitätsverwaltung
  - Berechtigungen
  - Provisioning
  - Access Management
  - Identifizierung und Authentifizierung
- Technologie
  - Single Sign-On
  - Circle of Trust
  - Global Logout
  - Föderation oder zentrale Datenhaltung
  - Einbindung von Webservices

Typische Struktur für die Anwendung in Firmennetzwerken

Key Concepts
→ Identitätsverwaltung

Basis:

- Eine übersichtliche Verzeichnisstruktur, bzw. ein exakt geordneter Verzeichnisdienst sind die Basis eines funktionierenden Identity Management Systems

Bedeutet:

- Identity Import aus maßgeblichen Instanzen (z.B. Personalverwaltungssysteme, Kundenbeziehungsmanagement-Systeme)
- Bereinigung, Vereinheitlichung und Zusammenführung der importierten Identities zu einer eindeutigen ID pro User
  - z.B. durch Metaverzeichnisse
  - Synchronisation
  - "Dateileichen" und veraltete Datensätze werden eliminiert

Mehrwert:

- Erreichen einer einzigen ID pro User

Key Concepts
→ Berechtigungen

Basis:

- Anwendungsübergreifende Berechtigungs- und Richtlinienverwaltung

Bedeutet:

- Berechtigungen: Rollen, Rechte, Gruppenzugehörigkeit
- Automatische Zuordnung der Berechtigungen, regel- und richtlinienbasiert

Mehrwert:

- Automatisierung der Vorgänge

Key Concepts
→ Provisioning

Basis:

- Das übergreifende Anlegen, Ändern und Löschen von Benutzerdaten und Berechtigungen auf unterschiedlichen System-Ressourcen

Bedeutet:

- Ressourcenübergreifende Bereitstellung von Passwörtern, E-Mail-Adressen, Accounts und Berechtigungen

Mehrwert:

- Bereitstellungszeit einer kompletten Identität wesentlich verkürzt
- Abstimmung der Vorgänge
- Automatisierung
- Vermeidung von Sicherheitslöchern durch fehlerhaftes Löschen von Identitäten
- Deutlich verminderter Arbeitsaufwand für Administratoren

Key Concepts
→ Access Management

Basis:

- Entscheidung über Zugriffsberechtigungen auf der Basis von Benutzeridentitäten oder -rollen und Zugriffsrechten (Policy Decision)
- Durchsetzen der Zugriffsentscheidungen (Policy Enforcement)

Mehrwert:

- Automatisierung der Vorgänge

Key Concepts
→ Identifizierung und Authentifizierung

Basis:

- Überprüfung von Identitäten
- Angebot von Authentifizierungsdiensten

Bedeutet:

- Das Identity Management ist gefordert Authentifizierungsdienste anzubieten, die den entsprechenden Sicherheitslevel vorgeben, der vorher mit den angeforderten Services abgeglichen wird

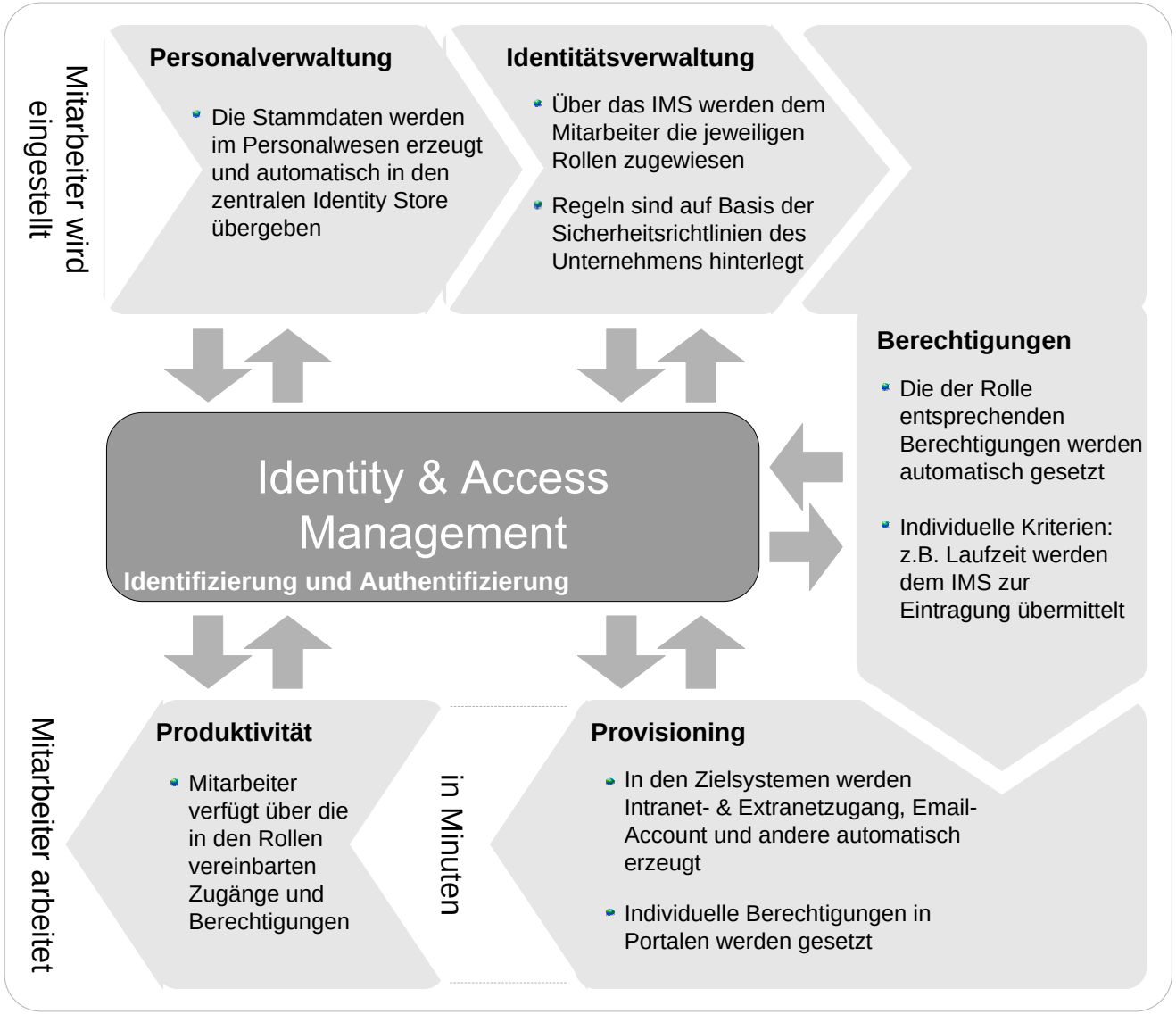
Mehrwert:

- Automatisierung
- Erreichen hoher Sicherheitslevel
- Konzeptionell bedingte höhere Sicherheit

→ Siehe Vorlesung "Authentikationsverfahren

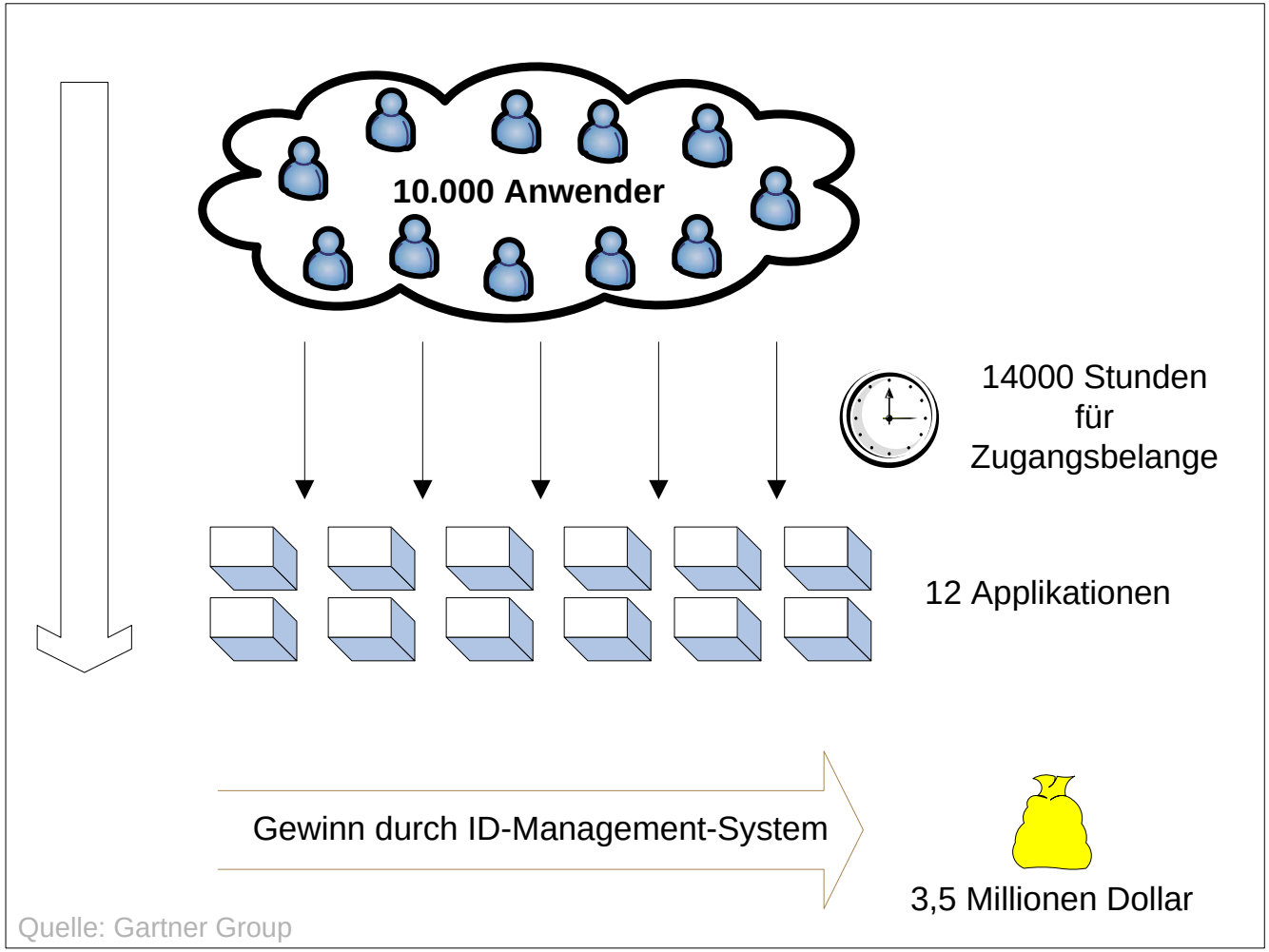
Key Concepts
→ Beispiel

- Typisches Identity Management Szenario innerhalb eines Unternehmens
- Der Zeitrahmen von der Einstellung bis zur vollständigen Integration des Mitarbeiters



Key Concepts
→ Kostenszenario

- Kostenersparnis durch Identity Management Systeme



Inhalt

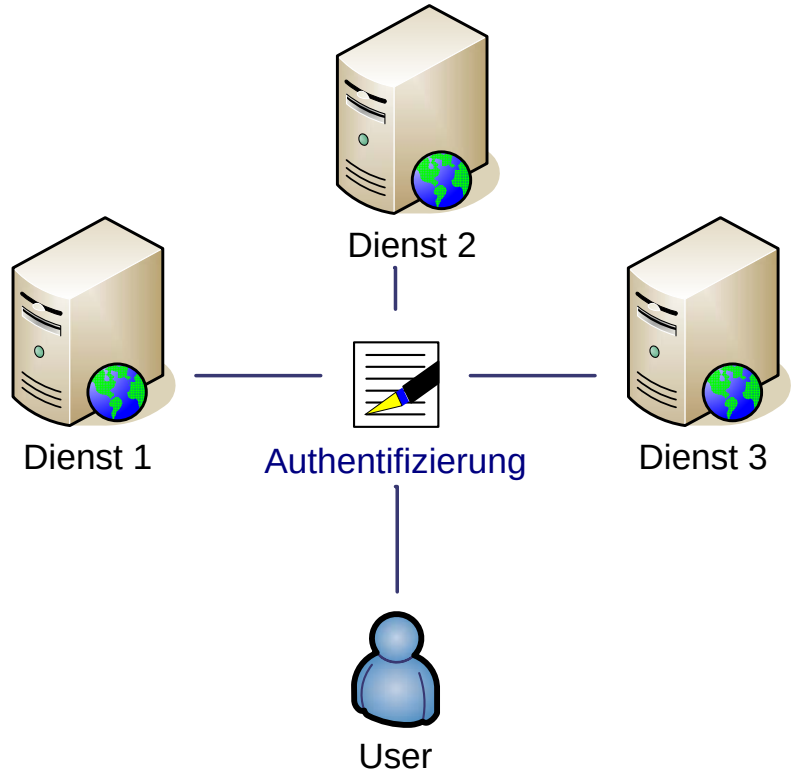
- Definitionen & Notwendigkeit
- Key Concepts
- **Single Sign-On**
- Circle of Trust
- Microsoft .Net Passport
- Liberty Alliance
- Zusammenfassung

Single Sign-On

- Einmalige Authentifizierung → Nutzung weiterer Dienste ohne erneute Authentifizierung
- Sicherheitsgewinn, da nur noch ein Passwort genutzt werden muss, dass komplexer gewählt werden kann
- Komfortgewinn für den Nutzer
- Unterschiedliche Interpretationen:
  - **Portallösung**
    - Nutzung mehrerer Dienste innerhalb eines Portals
    - Nutzung von Cookies
    - Verbreitung besonders in Intranet Systemen
  - **Ticketingsystem**
    - Nutzer erhält Daten (Ticket) welche bei den angeschlossenen Servern bekannt sind
    - Bsp.: Liberty Alliance, Microsoft .Net Passport
  - **Lokale Lösung**
    - Siehe "Unechtes SSO“

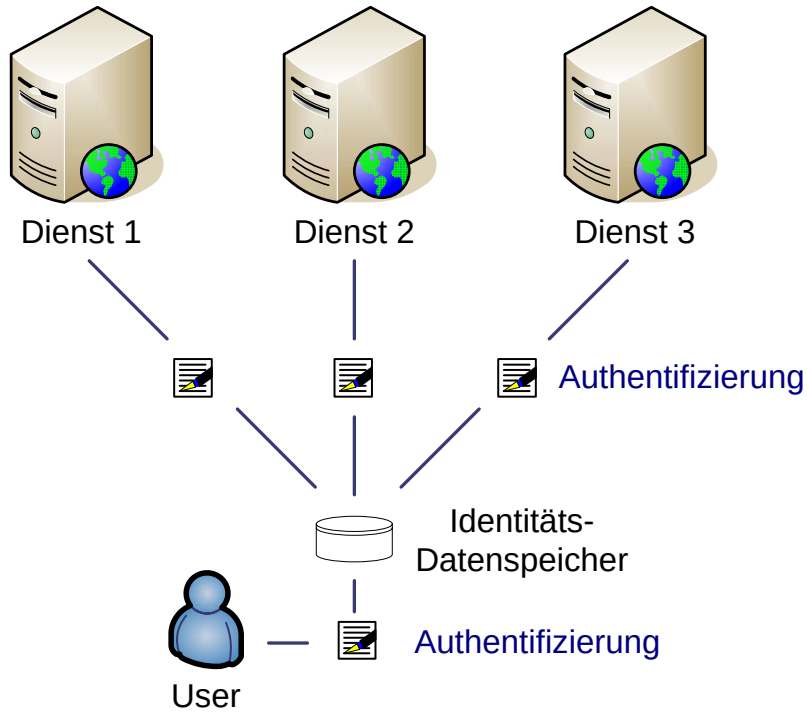
Single Sign-On
→ Echtes SSO

- Serverseitig implementiert
- Kommunikation der Server untereinander
- Vorausgehende vertragliche Vereinbarung zw. den Anbietern
- **Vorteile:**
  - Hoher Komfort
  - Hohe Sicherheit
  - Volle Mobilität
- **Nachteile:**
  - Aufwendige, komplexe Implementierung



Single Sign-On
→ Unechtes SSO

- Identitätsdaten-Eingabe-Automatismus
- Einmalige Authentifizierung an einem Identitätsdatenspeicher (Software, USB-Stick)
- Clientseitig implementiert
- Anbieterunabhängig
- **Vorteile:**
  - Sofort einsetzbar
  - Technischer Aufwand gering
- **Nachteile:**
  - Plattform- & betriebssystemabhängig
  - Eingeschränkt mobil



Inhalt

- Definitionen & Notwendigkeit
- Key Concepts
- Single Sign-On
- **Circle of Trust**
- Microsoft .Net Passport
- Liberty Alliance
- Zusammenfassung

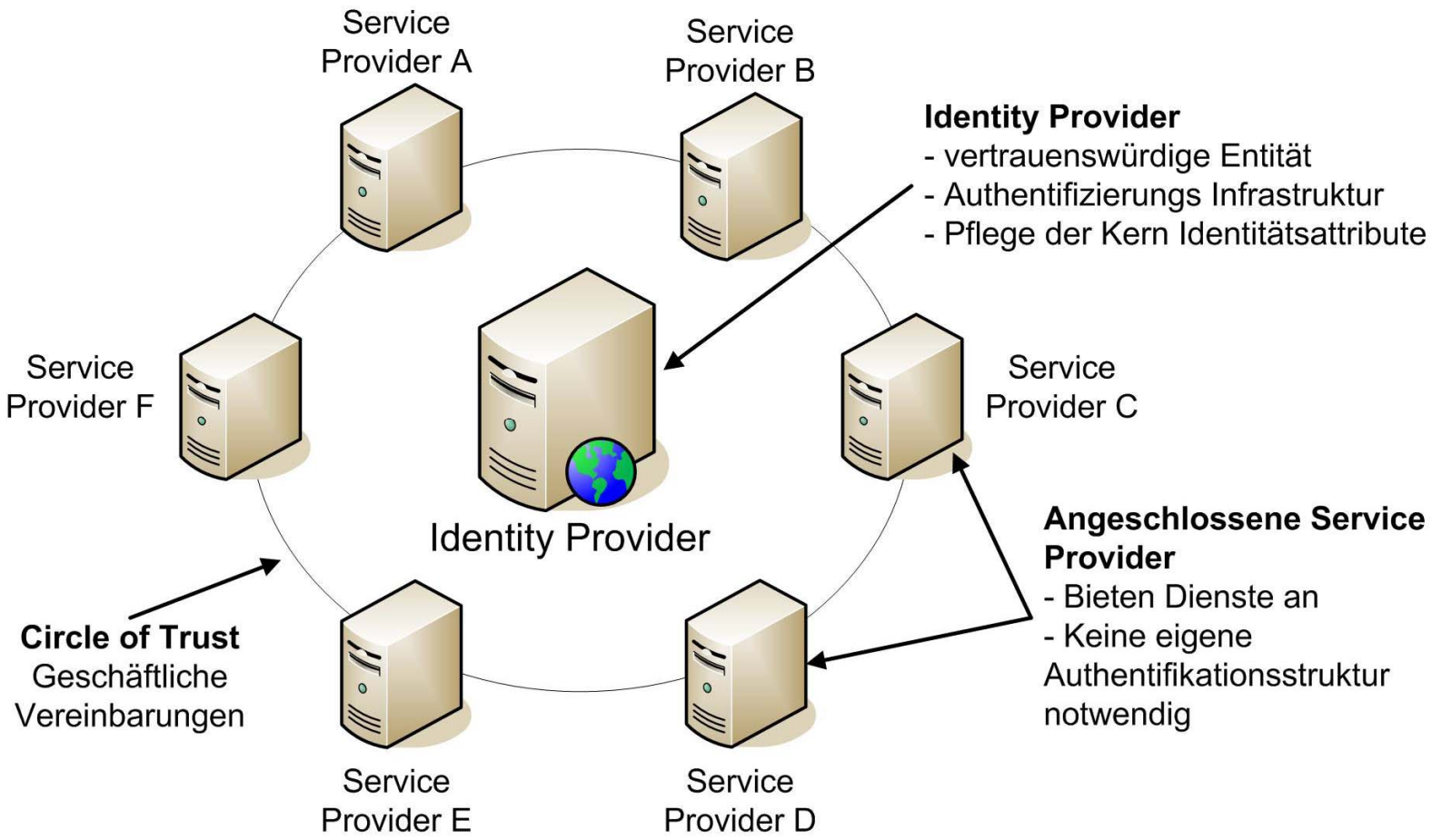
Circle of Trust (CoT)
→ Konzept

- Konzept um echtes Single Sign-On und weitere vernetzte Dienste anzubieten
- Basierend auf geschäftlichen Vereinbarungen zwischen Diensteanbietern (Einigung auf Technologie notwendig)

Bestehend aus:

- **Identity Providern**
  - Stellt Authentifizierungsinfrastruktur
  - Vertrauenswürdigste Instanz innerhalb des Circle of Trust (CoT) für den Nutzer, da vom Nutzer gewählt
  - Kennt alle angeschlossenen Service Provider
  - Verwaltet die Identitätsinformationen des Nutzers
- **Service Providern**
  - Diensteanbieter
  - Authentifizierungsinfrastruktur nicht notwendig
  - Kennt in der Grundform nur den Identity Provider

Circle of Trust (CoT)
→ Schema



Entstehung eines CoT → siehe Liberty Alliance

Inhalt

- Definitionen & Notwendigkeit
- Key Concepts
- Single Sign-On
- Circle of Trust
- **Microsoft .Net Passport**
- Liberty Alliance
- Zusammenfassung

Microsoft .Net Passport

- Identity Management System mit zentralem Ansatz
- .Net Passport ist ein Dienst
- Wichtigste Funktionalitäten: Authentifikation, bzw. Single Sign-On

Funktion:

- Identitätsdaten (Credentials) werden per verschlüsseltem Cookie weitergegeben
- Zwischen den Servern wird ein verschlüsselter Identifikator ausgetauscht → entschlüsselt die Credentials des Cookies
- Speicherung aller Profildaten zentral auf einem Passport-Server
- Alle an das Passport System angeschlossenen Server haben Zugriff auf jegliche User-Attribute.
- Nach Authentisierung am Passport-Server ist man für sämtliche angeschlossene Dienste authentifiziert.

Microsoft .Net Passport

Vorteile:

- Relativ einfacher Aufbau
- Single Sign-On

.Net Passport wird aufgrund von Sicherheitsproblemen nur noch MS intern verwendet

Nachteile:

- Besitz des Authentisierungstokens ist zur Anmeldung ausreichend
  → Im Bezug auf Sicherheit und Privatheit bedenklich
- Der User hat kein Entscheidungsrecht welches Passportmitglied seine Daten lesen kann
- Der User wird über neue Passportmitglieder nicht informiert (auch diese haben Einsicht in seine Daten)
- Vollständiger Global Logout ist nicht gewährleistet
  → Sicherheitsproblem
- Vertrauen gegenüber dem Microsoft Passport Server ist Voraussetzung.
- Zentrale Datenhaltung birgt Gefahren, Nutzerdaten sind passportweit verfügbar, Attacken auf Passportserver sind verheerend

Inhalt

- Definitionen & Notwendigkeit
- Key Concepts
- Single Sign-On
- Circle of Trust
- Microsoft .Net Passport
- **Liberty Alliance**
- Zusammenfassung

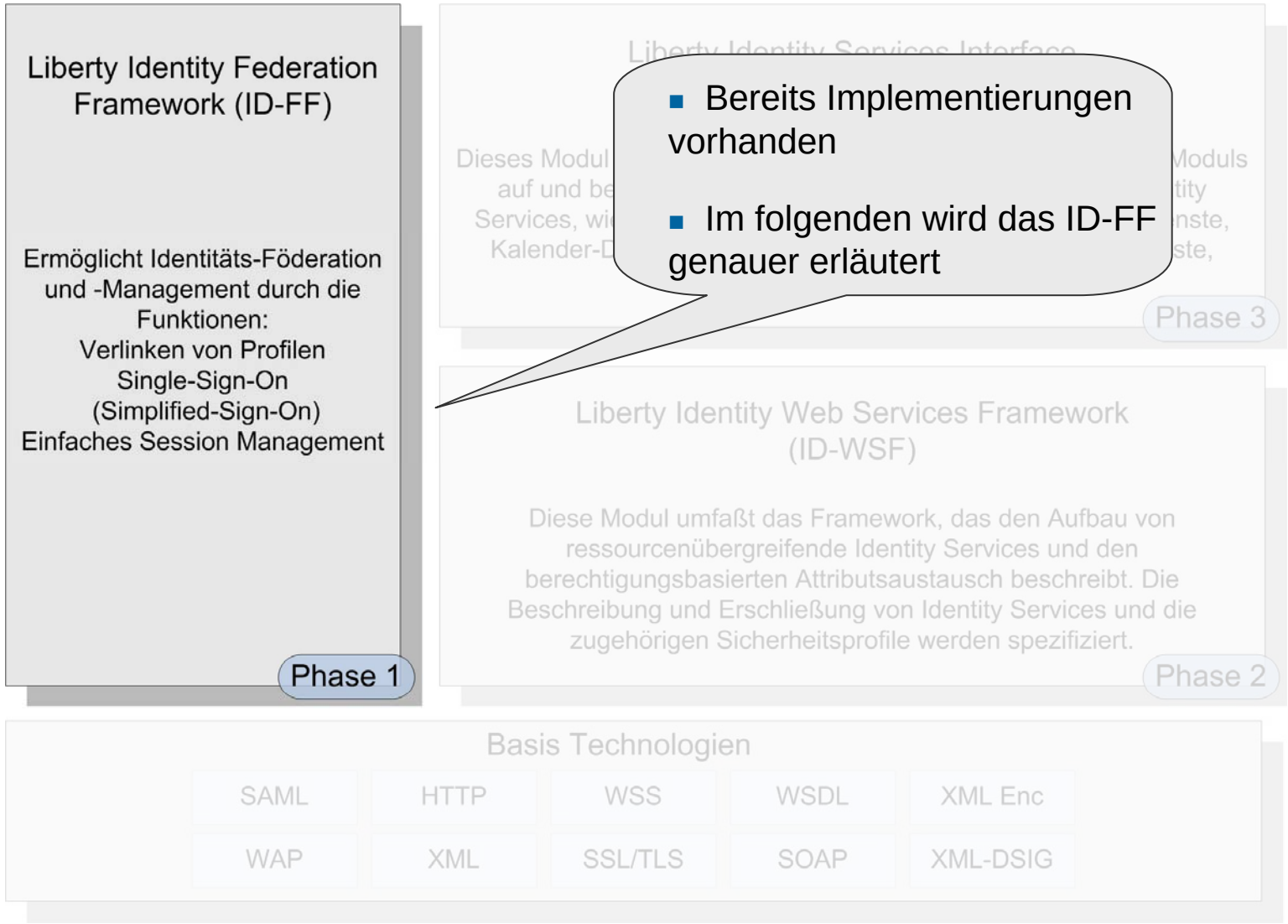
Liberty Alliance

- Identity Management Spezifikation mit dezentralem Ansatz
- Eine Vereinigung von mehr als 160 Firmen (Sun, RSA, AOL,…)
- Entwicklung eines Standards für föderierte Identitäten
  - Single Sign On Funktionalitäten
  - Austausch von Authentifizierungs-, Authorisierungs- und Benutzerprofilinformationen
  - Föderation vorhandener Profile → dezentraler Ansatz
  - Bildung von Vertrauenswürdigen Kreisen (Circles of Trust)
  - Sicherheitsaspekte werden diskutiert und vorgeschlagen, aber nicht festgelegt.

Liberty Alliance
→ Zielsetzung

- Schützen und Verwalten von privaten und sicherheitssensiblen Identitäts-Informationen
- Erhalten und Pflegen von Kundenbeziehungen ohne Dritthilfe
- Single Sign-On Standard mit dezentraler Authentifikation, Autorisierung und Datenhaltung für viele Provider
- Alle zukünftigen Zugangsstandards und Identitäts-Datenhaltungen sollen unterstützt werden
- Interoperabilität über Unternehmens- und Plattformgrenzen hinweg
- Grundlage für sichere identitätsbasierte Web-Services Nutzung in verteilten Netzen

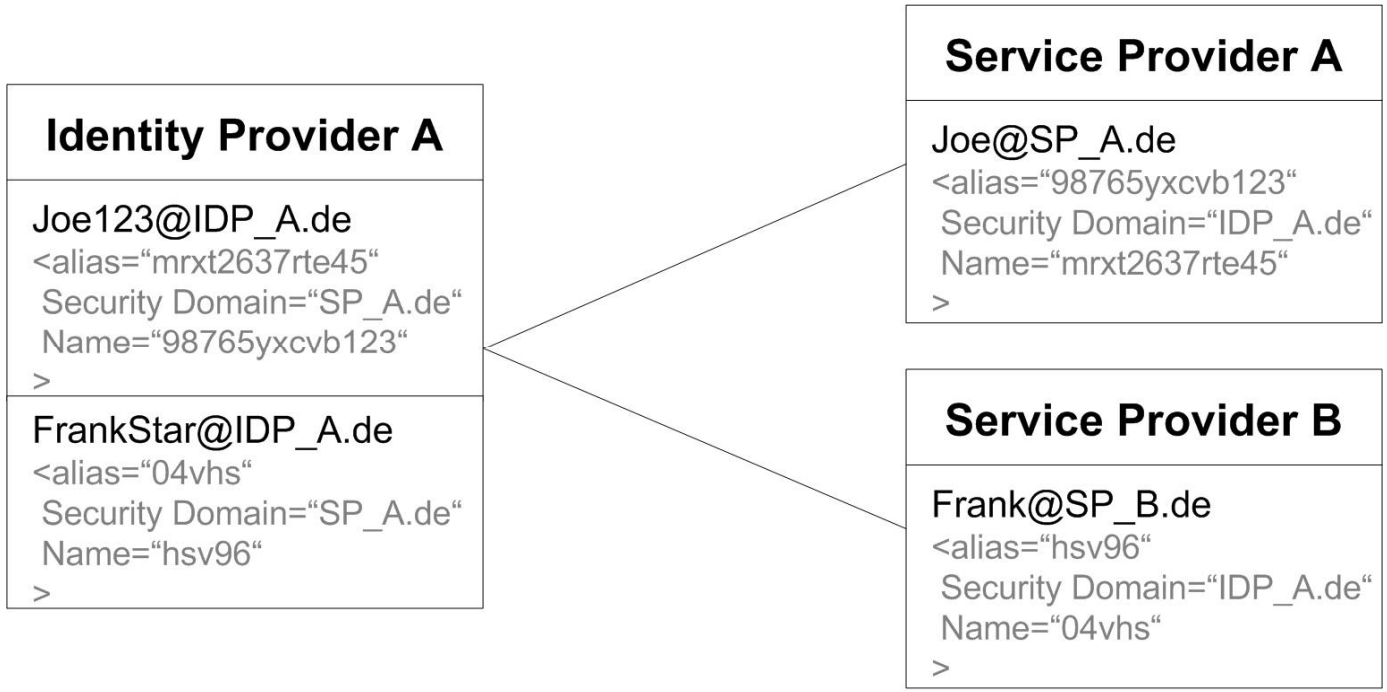
Liberty Alliance
→ Entwicklungsphasen der Liberty



- Bereits Implementierungen vorhanden
- Im folgenden wird das ID-FF genauer erläutert

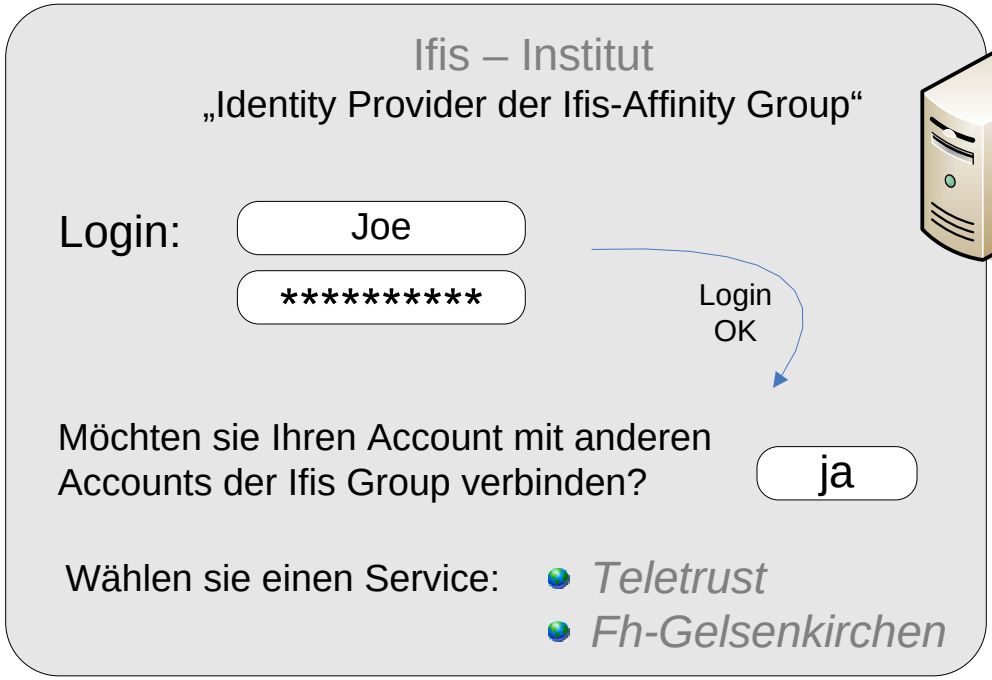
Liberty Alliance
→ Die Föderation

- Profile sind nur über so genannte Alias (Name Identifier) verknüpft
  - Lediglich ein Name, ein zugeordnetes Alias und die Domain sind dem jeweiligen gegenüber bekannt
  - Kein Austausch von personifizierten Profildaten



Liberty Alliance
→ Die Föderation (1/2)

- → Initiieren einer Föderation nach der Authentifikation beim IDP
  - → Ein Sprung zum SP wird initiiert



Ifis – Institut
Identity Provider

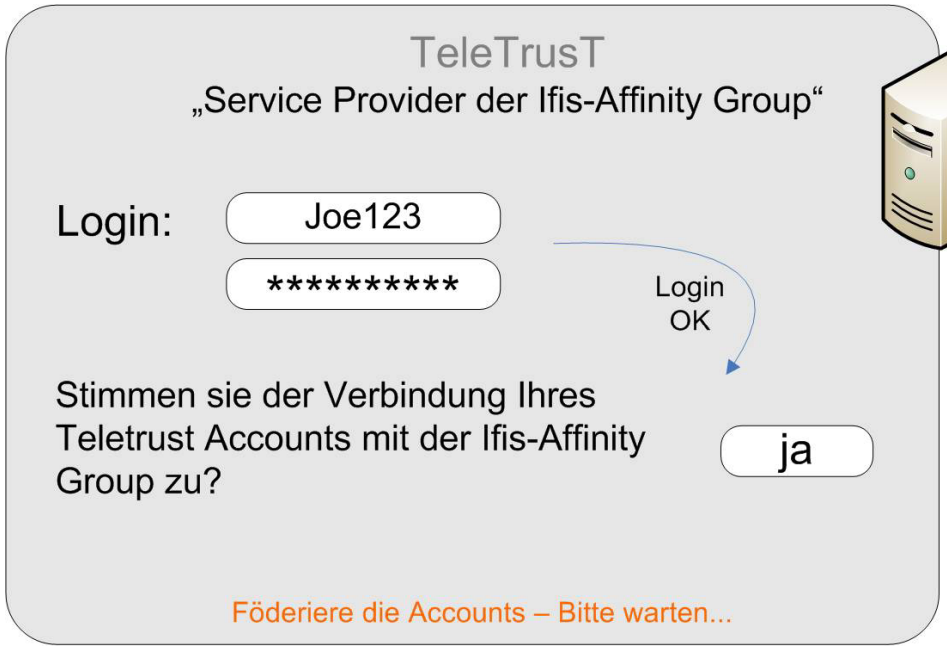
Joe: authentifiziert
Identitätsföderation: ja

TeleTrusT
Service Provider

Joe123: nicht authentifiziert
Identitätsföderation: nein

Liberty Alliance
→ Die Föderation (2/2)

- → Abschluss der Föderation durch die Authentifikation beim SP
  - → Anschließend findet Rücksprung zum IDP statt



TeleTrusT
Service Provider

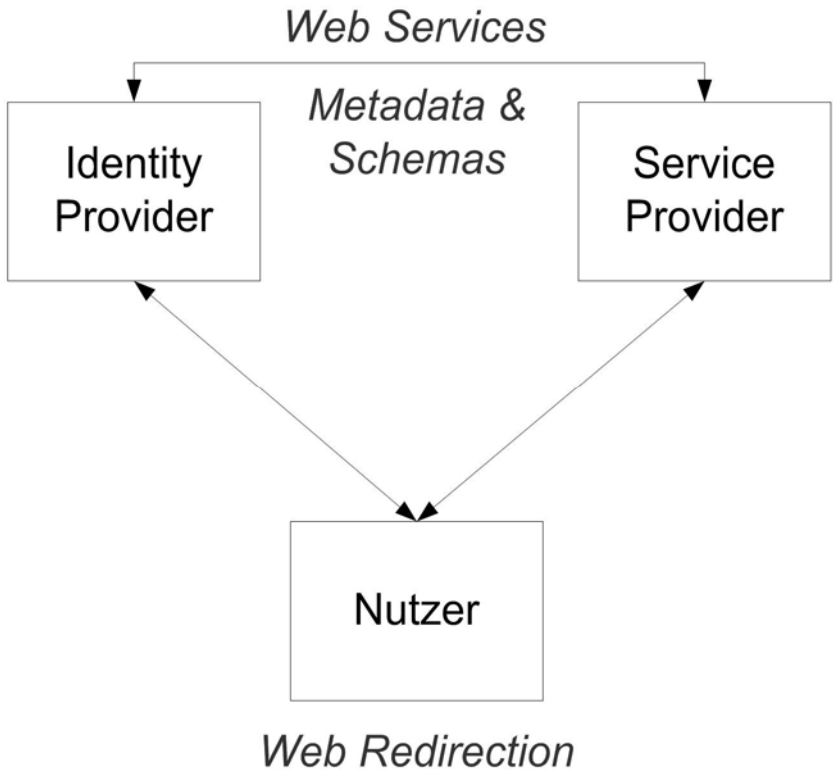
Joe123: authentifiziert
Identitätsföderation: ja
Ifis-Institut: Joe

Ifis – Institut
Identity Provider

Joe: authentifiziert
Identitätsföderation: ja
TeleTrusT: Joe123

Liberty Alliance
→ Architektur

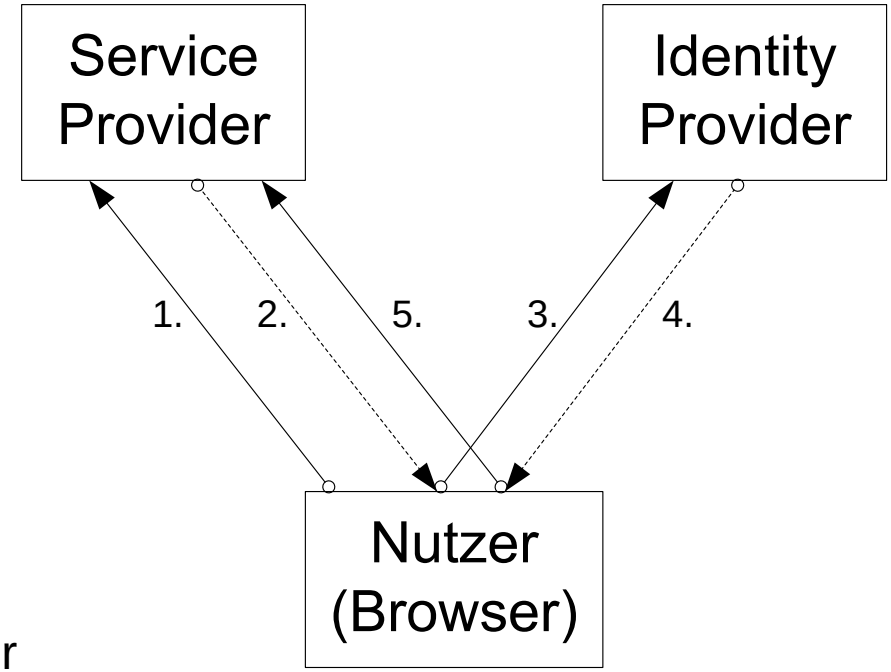
- Grundsätzliche Architektur der Liberty
  - Web redirection
    - Kommunikation über den Browser des Nutzers
  - Web Services
    - Direkte Kommunikation zwischen Liberty basierenden Entitäten
  - Metadata and Schemas
    - Satz von beschreibenden Daten und Formaten, die von Liberty fähigen Entitäten zur Kommunikation von Provider-spezifischen und anderen Informationen genutzt werden.



Liberty Alliance
→ Web Redirection (Bsp. SSO)

Web Redirection zwischen zwei Providern über einen Browser

1. HTTP Request
2. Service Provider initiiert „HTTP-Redirect“ zum entsprechenden IDP zur Authentifizierung
   a) LocationHeaderField: IDP-URI
   b) Zusätzlich: SP-URI
3. LocationHeaderField wird ausgelesen. Anfrage an IDP-URI
   a) SP-URI wird übernommen
4. Response (über Redirect) an die Adresse des SPs
   a) IDP-URI eingebettet & Auth-Infos
5. HTTP-Request an den Service Provider mit der Information, bzw. der Adresse des IDPs.



Liberty Alliance
→ Kommunikationstechniken

- Die Liberty nutzt verschiedene Arten der Kommunikation

  1. Reine Kommunikation über den Browser per Redirect und der Methode Get (Request & Response) → Austausch kleiner Informationsmengen
  2. Kommunikation über den Browser per Formular und der Methode POST → Austausch großer Datenmengen möglich
  3. Direkte Kommunikation zwischen den Providern per SOAP

- Die genannten Techniken kommen in unterschiedlicher Ausprägung in den verschiedenen Szenarien der Liberty Technologie zum Einsatz

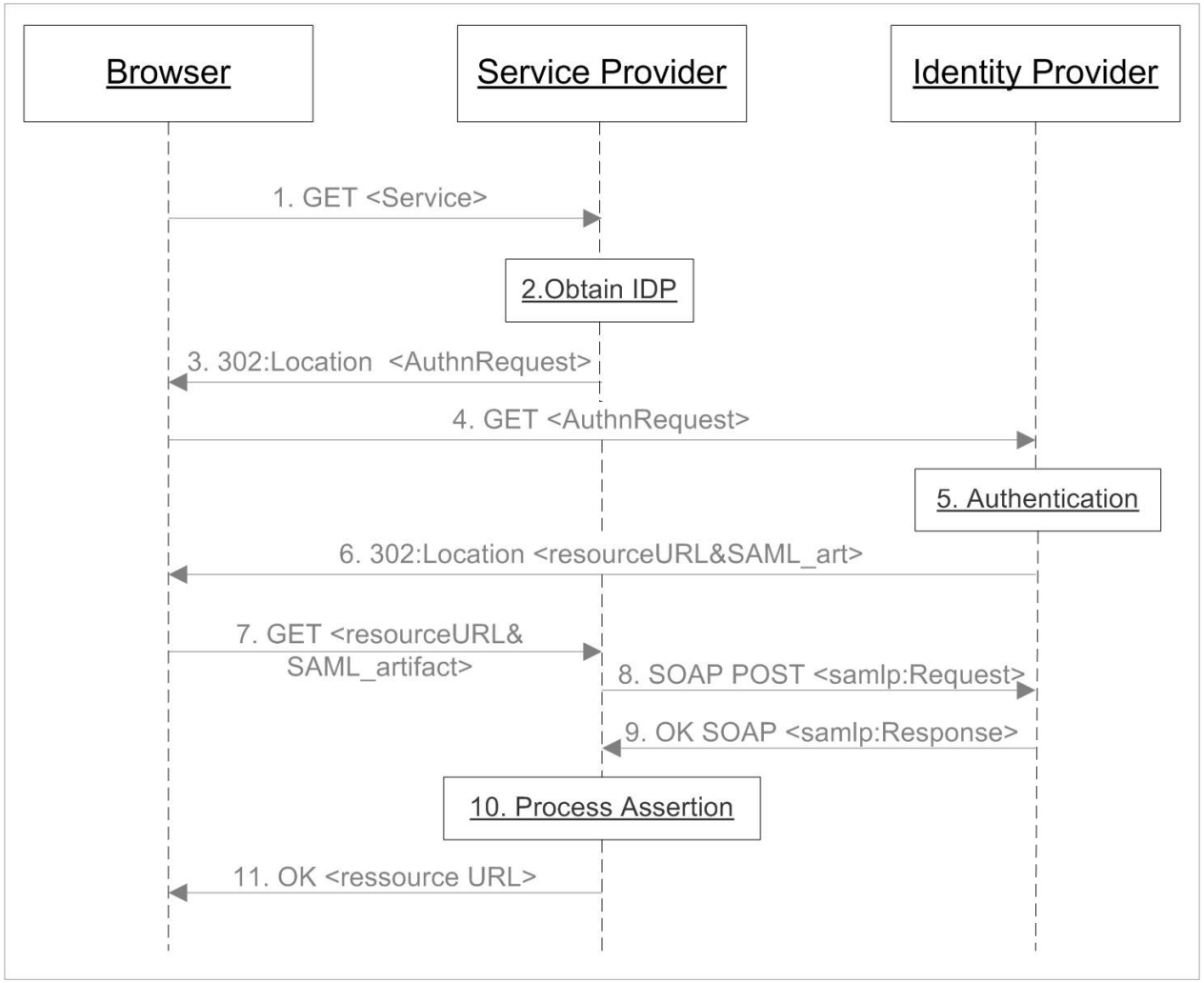
→ Drei grundsätzliche Profile für beispielsweise SSO folgen…

Liberty Alliance
→ Liberty Artifact Profile (Sequenzdiagramm)

- Kombination Redirect & SOAP
- Per Redirect wird ein Artifact übertragen
- Per SOAP nützt das Artifact als Erkennungsmerkmal

Artifact basierend auf SAML: unverständlicher, pseudo-zufälliger, kleiner Datensatz, eindeutig einem Nutzer zugeordnet

Motivation: Artifact klein genug für URL-codierte Übertragung mit GET-Methode

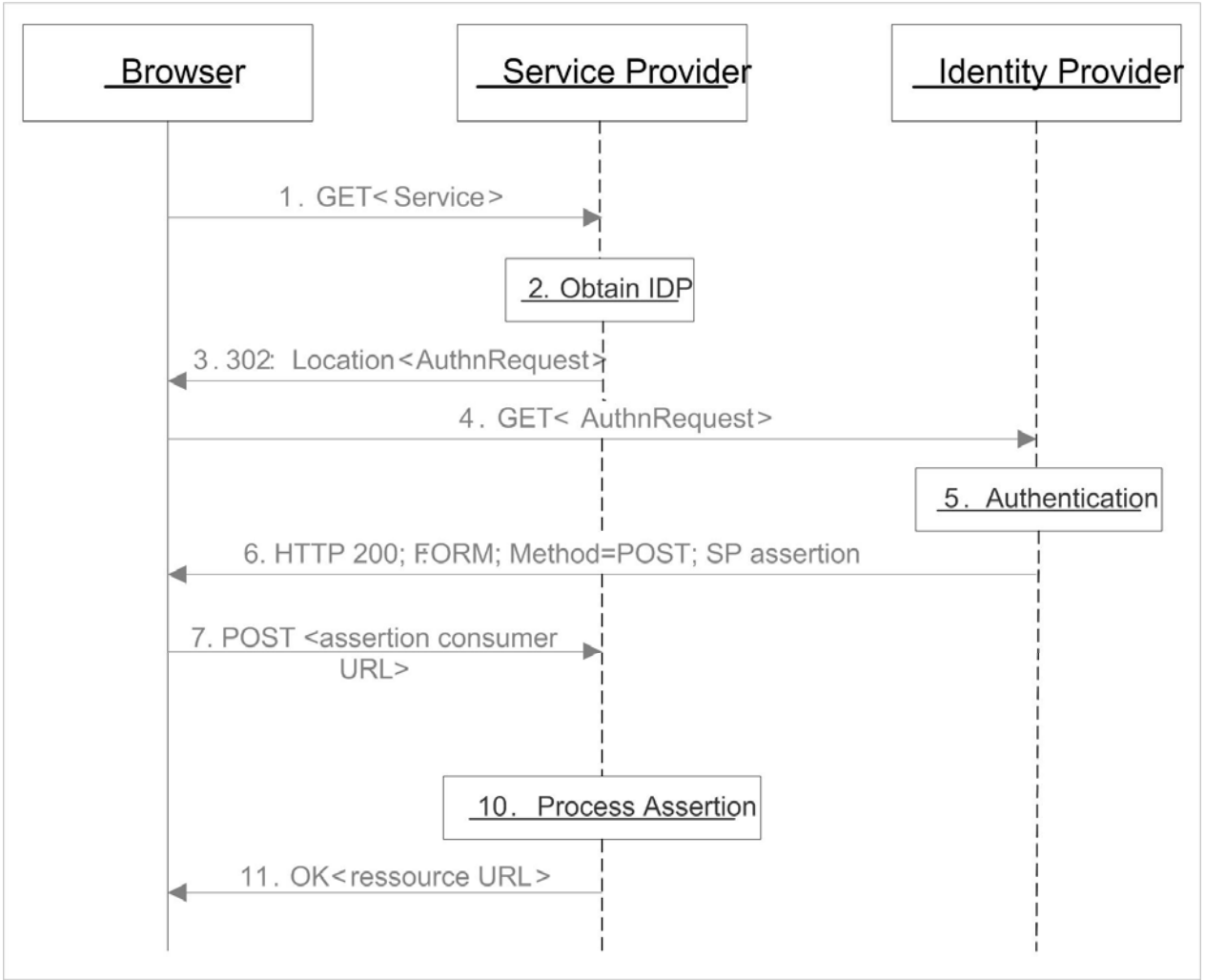


Liberty Alliance
→ Liberty Browser POST Profile (Sequenzdiagramm)

- Reiner Redirect
- Keine SOAP Nutzung

Speziell: Daten werden in ein Formular eingebettet. Das Formular wird per Javascript automatisiert auf Userseite abgeschickt

Motivation: keine Restriktionen im Bezug auf Datenmengen.



Liberty Alliance

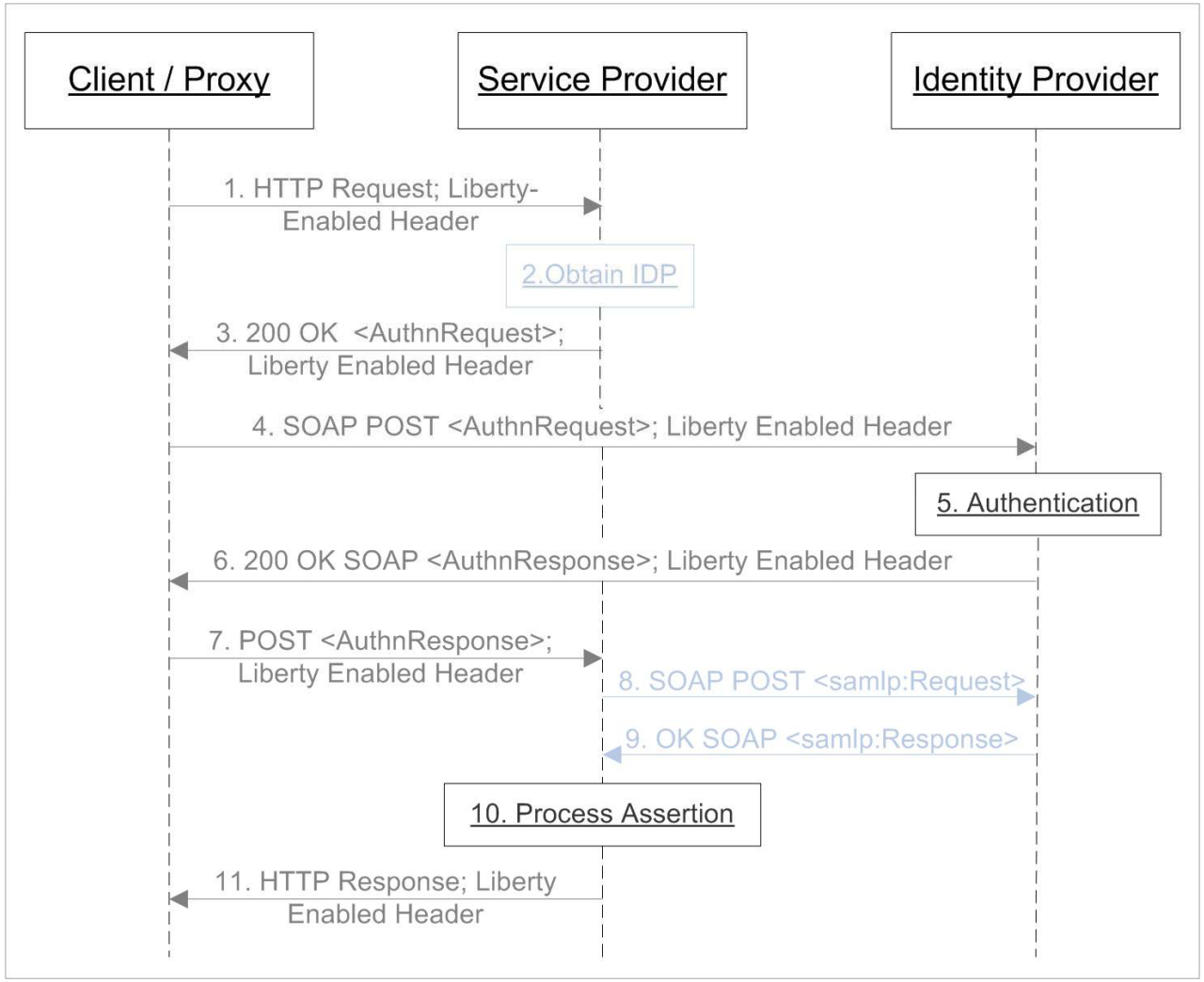
→ Liberty-Enabled Client and Proxy Profile (Sequenzdiagramm)

- spezifiziert die Interaktion zwischen libertyfähigen Clients bzw. Proxys und Service-, Identity Providern.
- Datenempfang innerhalb des Bodys der HTTP-Requests und Responses
- Basiert nicht auf Redirects, sondern auf SOAP mit libertyspezifischen HTTP-Headern

Anwendung:

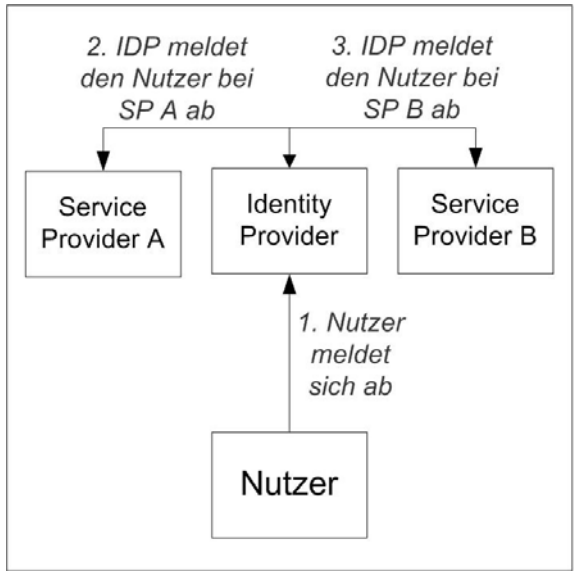
z.B. mobile Applikation (WAP-Gateway),

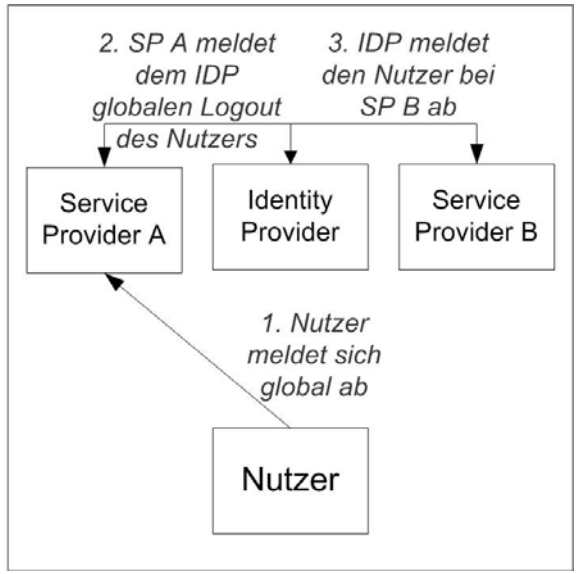
→ Nicht nur browserbasierte Clients



Liberty Alliance
→ Global Logout

- Zur Beendigung einer Session ist ein "Global Logout" über den gesamten CoT notwendig
- IDP kann alle Techniken nutzen, SP nur Profil 1 & 2





Techniken:

1. HTTP-Redirect-Based → Logout Info wird einzeln per Redirect an die SPs gesendet
2. HTTP-GET-Based → senden einer HTML Seite an den Browser, die img-Tags mit den Logoutpunkten aller SPs enthält
3. SOAP/HTTP-Based → 1zu1-Kommunikation zwischen IDP und allen SPs über SOAP

Liberty Alliance
→ Liberty Identity Web-Services Framework (ID-WSF)

Motivation:

- Identitätsbasierte Web-Services lokalisieren und ansprechen

Technik:

- SOAP
- SAML
- ID-FF

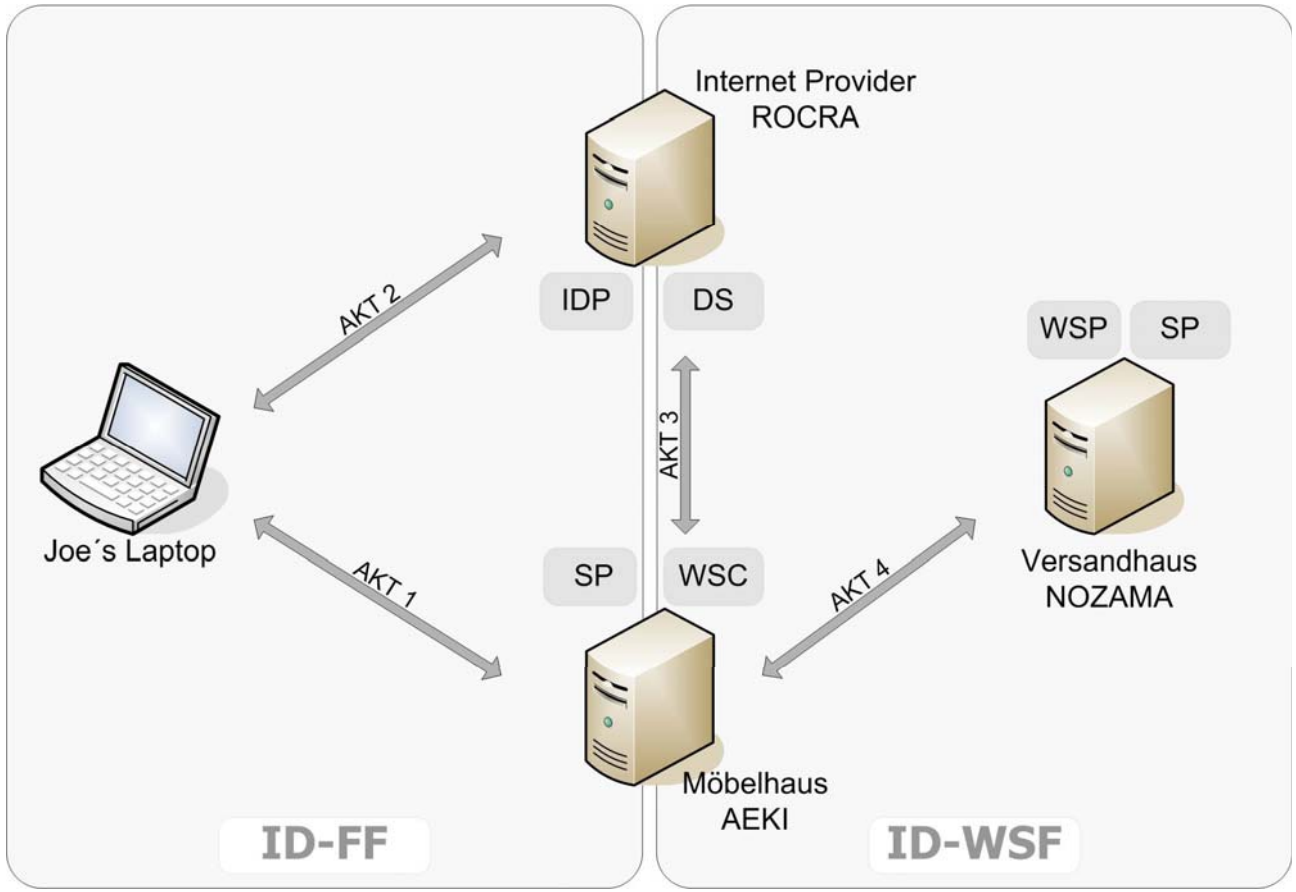
Elemente des ID-WSF:

- Web Services Client (WSC) → Principal, der einen identitätsbasierten Web Service aufruft
- Web Service Provider (WSP) → bietet identitätsbasierte Web Services an
- Discovery Service (DS) → Der DS vereinfacht die Registrierung an entdeckten Services, bildet die Registrierungsstelle und hilft somit die entsprechenden Services zu lokalisieren
- Credentials → beglaubigte Transfers von Eigenschaften eines Pseudonyms auf ein anderes, ohne dass es möglich wäre, Rückschlüsse auf das erste Pseudonym zu ziehen

Liberty Alliance
→ ID-WSF Anwendungsbeispiel

Beispiel:

1. Anfrage an AEKI von Joe (Tisch kaufen)
2. SSO über den IDP ROCRA
3. AEKI braucht Adressdaten von Joe. Sucht über den DS Service autorisiert von Joe. DS sendet Information und Zugang (Credentials) für NOZAMA
4. AEKI fordert Adressdaten von Joe bei NOZAMA mit den Credentials an und erhält die Daten



Liberty Alliance
→ Liberty Identity Services Interface Specification (ID-SIS)

Motivation:

- Identitätsabhängige Dienste bzw. Schnittstellen anbieten

Infos zum ID-SIS:

- Die ID-SIS Spezifikation ist noch nicht verabschiedet
- Folgende Dienste sind bisher angedacht:
  - Geo-location
  - Contact Book
  - Presence
  - Gaming
  - Content SMS/MMS Messaging

Liberty Alliance
→ Fazit

- **Vorteile:**
  - Circle of Trust wird durch den Nutzer per Opt-In zusammengestellt
  - Dezentraler Ansatz
  - Single Sign-On
  - Eigenverantwortung und Kontrolle über alle Profildaten und –attribute
  - In späteren Phasen Attributdaten Austausch möglich
- **Nachteile:**
  - Komplexe Struktur
  - Vertraglicher Zusammenschluss der Anbieter notwendig
  - Sicherheitsaspekte werden diskutiert, aber nicht vorgegeben

Inhalt

- Definitionen & Notwendigkeit
- Key Concepts
- Single Sign-On
- Circle of Trust
- Microsoft .Net Passport
- Liberty Alliance
- **Zusammenfassung**

Identity Management
→ Zusammenfassung

- Identity Management Systeme vereinfachen den Umgang mit Identitäten enorm
- ID ist ein sehr komplexes Thema
- *Zunehmend wird es wichtiger, Authentikationsverfahren zu verwenden, die in der globalen handelnden Gesellschaft über staatliche Grenzen und Verantwortungsbereiche hinaus verwendet werden können*.
  → Dieser Anspruch aus der Vorlesung Authentikation wird durch IMS unterstützt
- Die zukünftige Einführung von IMS oder einige Ihrer Konzepte, wie Single Sign-On, sind aufgrund der stetig steigenden Anzahl von Identitäten unausweichlich.

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Fachhochschule Gelsenkirchen