Identity Management

Eine Einführung von
Katja Tebo & Christoph Spiller

Identity Management →Agenda

- Identität
- Identity Management
  - Motivation und Ziel
  - Beteiligte und ihre Interessen
  - Anforderungen
  - Federated Identity
  - Microsoft Passport
  - Liberty Alliance
  - Andere Ansätze
- Ausblick

Was ist Identität?

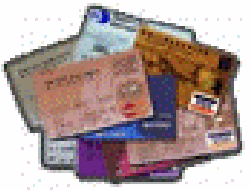
- Identität
  - Wer ist die Person?
- Authentisierung
  - Wie kann sie das nachweisen?
- Autorisierung
  - Welche Rechte / Pflichten hängen mit dem Nachweis zusammen?

Was ist Network Identity?

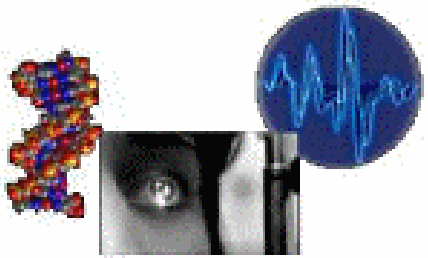
Ein Satz an Attributen, die ein oder mehrere Profile einer Person beschreibt.

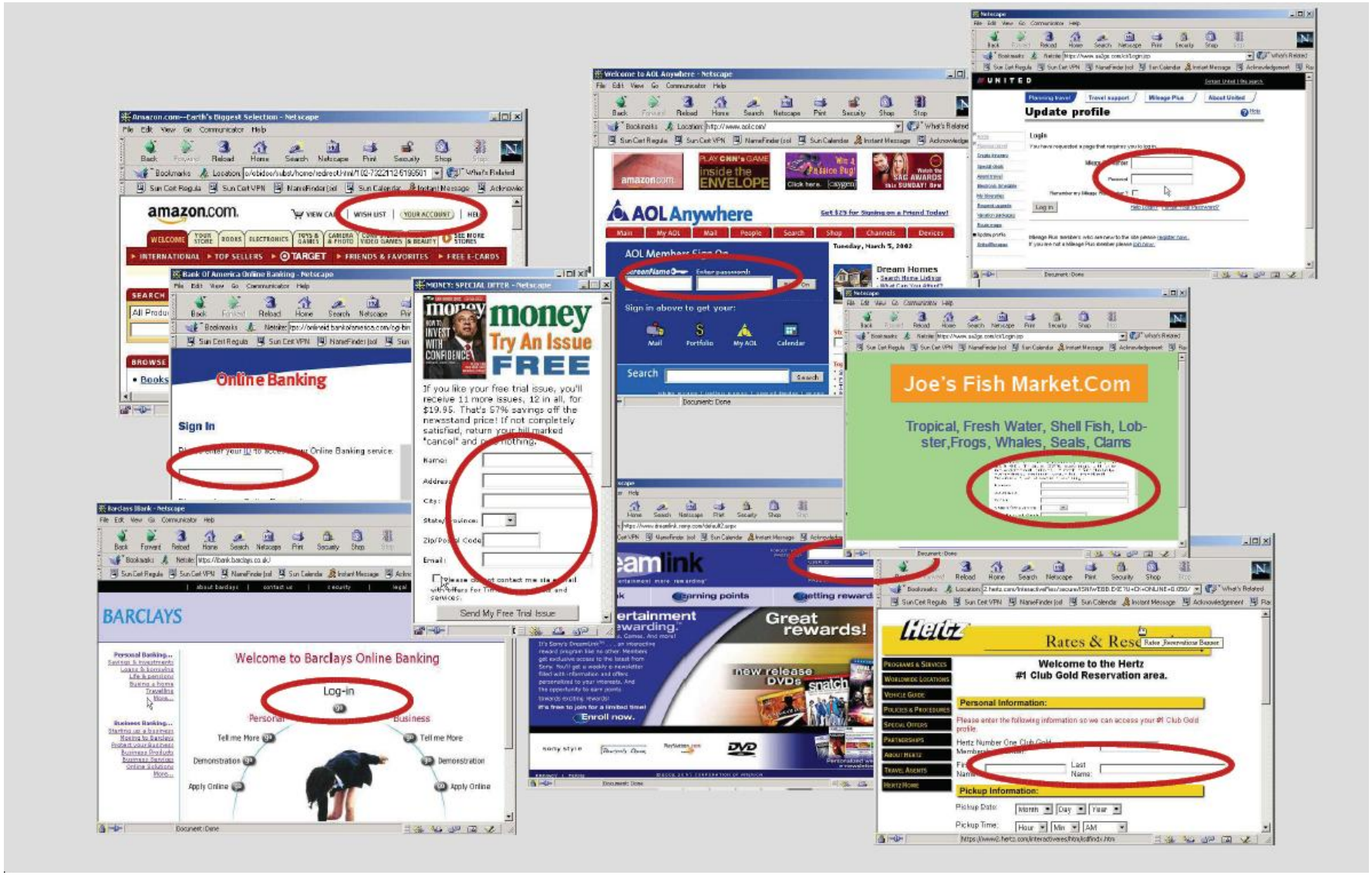
Kundenname	John Smith
Email -Alias	jsmith2@freemail.com
PIN	38721

Kreditkartennummer
Ausweisnummer
Führerschein
Reisepass
Retina-Scan
DNA



Unterhaltungsvorlieben
bevorzugteBenachrichtigung
Mitarbeiterautorisierung
Geschäftskalender
Restaurantpräferenzen
Zusatzprogramme
Freunde und Bekannte
Ausbildungshistorie
Krankenhistorie
finanzieller Hintergrund




amazon.com
Online Banking
Sign In
money
Try An Issue
FREE
Send My Free Trial Issue
AOL Anywhere
Sign in above to get your:
Update profile
Joe's Fish Market.Com
Tropical, Fresh Water, Shell Fish, Lobster,Frogs, Whales, Seals, Clams
BARCLAYS
Welcome to Barclays Online Banking
Log-in
Great rewards!
Enroll now.
Hertz
Welcome to the Hertz #1 Club Gold Reservation area.
Personal Information:
Pickup Information:

Identity Management
→ Motivation

- Zunehmende Kommerzialisierung
- Separate Anmeldung für jeden genutzten Dienst notwendig

  → Wahrscheinlichkeit für Fehler und Sicherheitsprobleme steigt
- Kosten für Administration und Help Desk steigen

Beispiel: Reisebuchung

- Flug buchen bei BILLIGFLUG AG
- Auto reservieren bei MIETWAGEN AG
- Hotelbuchung, Reiseführer bestellen …
- Jedesmal sind Login mit Benutzername und Passwort sowie Logout nötig

- Ziel: Eine Anmeldung für mehrere Dienste (Single Sign-On)

Identity Management
→ Beteiligte

- Nutzer
  - Kunden, Mitarbeiter, Geschäftspartner
- Dienstanbieter
  - Banken, Online-Shops, Internet Provider, öffentliche Einrichtungen, Behörden ...

Identity Management
→ Interessen der Nutzer

- Anonymität und Selbstbestimmung
- Personalisierte Dienste
- Protokollierung der Kommunikation
- Sicherheit
- Datenschutz

Identity Management
→ Interessen der Dienstanbieter

- Erhöhen der Sicherheit
- Schutz vor Betrug und unberechtigter Nutzung der Dienste
- Kosten für Administration senken
- Anfragen beim User Help Desk senken

Identity Management
→ Anforderungen

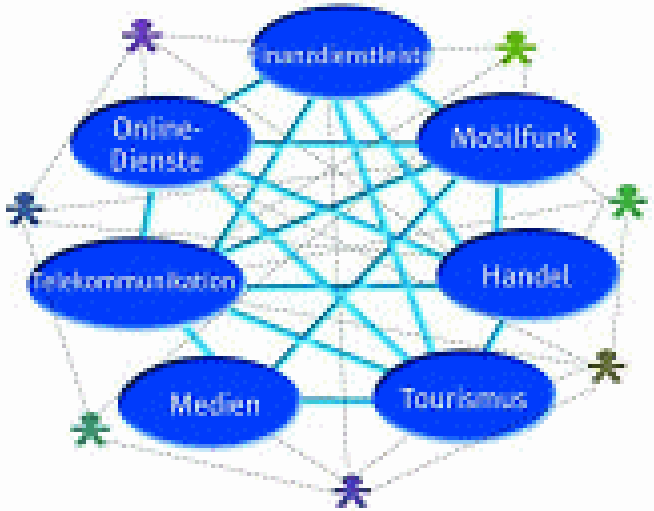
- Zusammenführen der Account-Daten von verschiedenen Diensten in einer föderierten Identität
- Datenschutz und Informationelle Selbstbestimmung wahren
- Zentrale Anmeldung und auch Abmeldung
- Unterschiedliche Sicherheitsansprüche
- Anwendungssicherheit

Federated Identity: Zwei Modelle

Zentralisiertes Modell

Ein einzelnes Unternehmen errichtet ein Monopol, sammelt Unternehmens-informationen und erhebt Gebühren für alle Internet Transaktionen.

Föderatives Modell



Viele Unternehmen, einigen sich auf offene, gemeinschaftliche Standards für die Identität im Netz.

Microsofts Passport

- Zentrale Verwaltung eines Benutzerprofils
- Partner: Hotmail, MSN, eBay, Monster, u.a.
- Einmaliger Login gewährt Zugriff auf alle Dienste
- Meta-Directory für Datenverteilung

Liberty Alliance

- Motto „Die freie Welt gegen Microsoft“
- Von Sun 2001 ins Leben gerufen
- Inzwischen rund 150 Partner, z.B. Nokia, AOL, General Motors, VeriSign, Cisco, IBM und American Express
- Liberty-Spezifikation 1.2 von Nov.2003

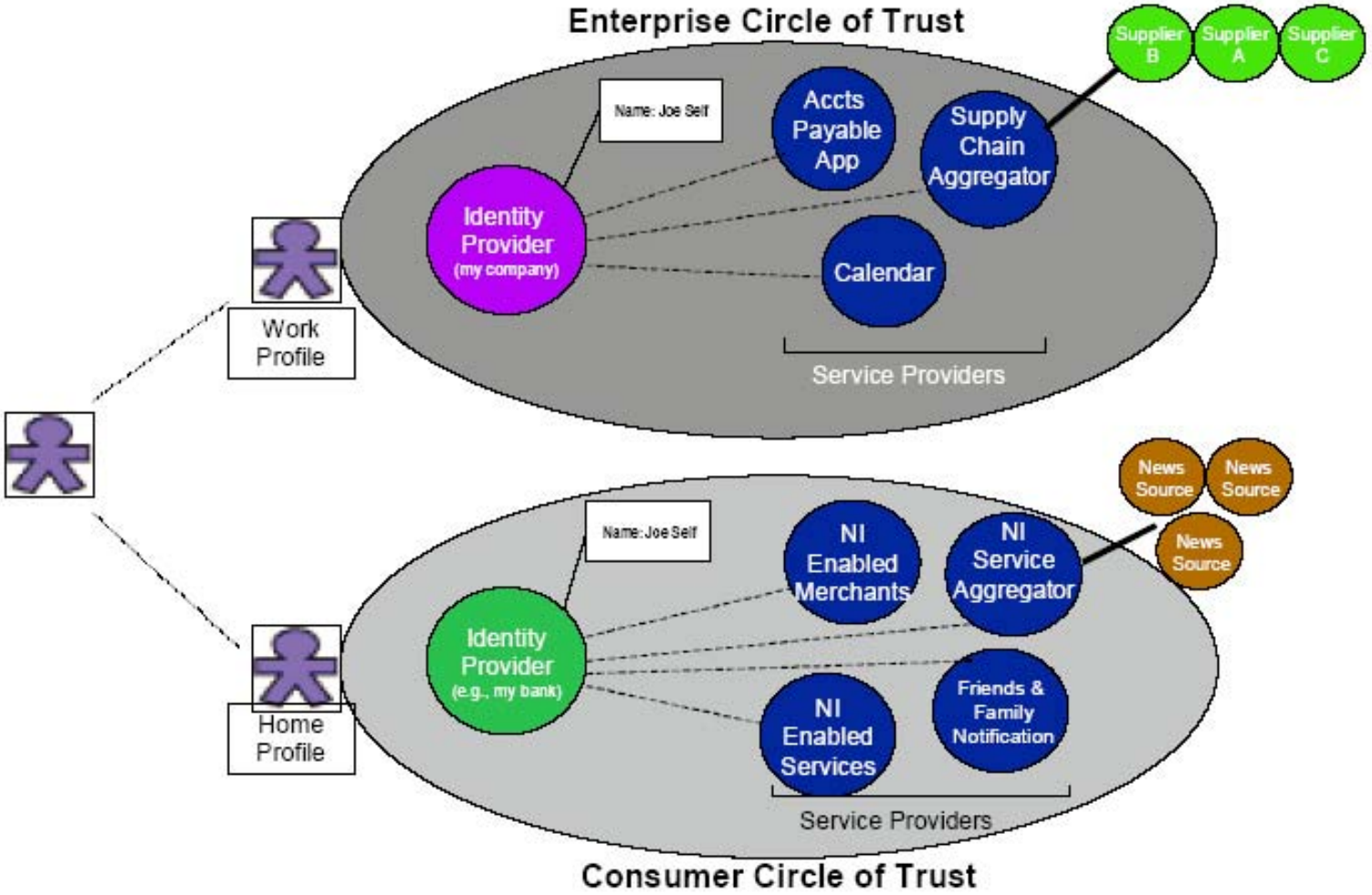
Liberty-Prinzip

- Liberty setzt auf das derzeit übliche System der verteilten Accounts auf
- Benutzer entscheidet über Aufbau einer föderierten Identität
- Pseudonyme sind möglich (Beruf / Privat)
- Identitätsverwaltung ist unabhängig vom Endgerät

Liberty-Prinzip

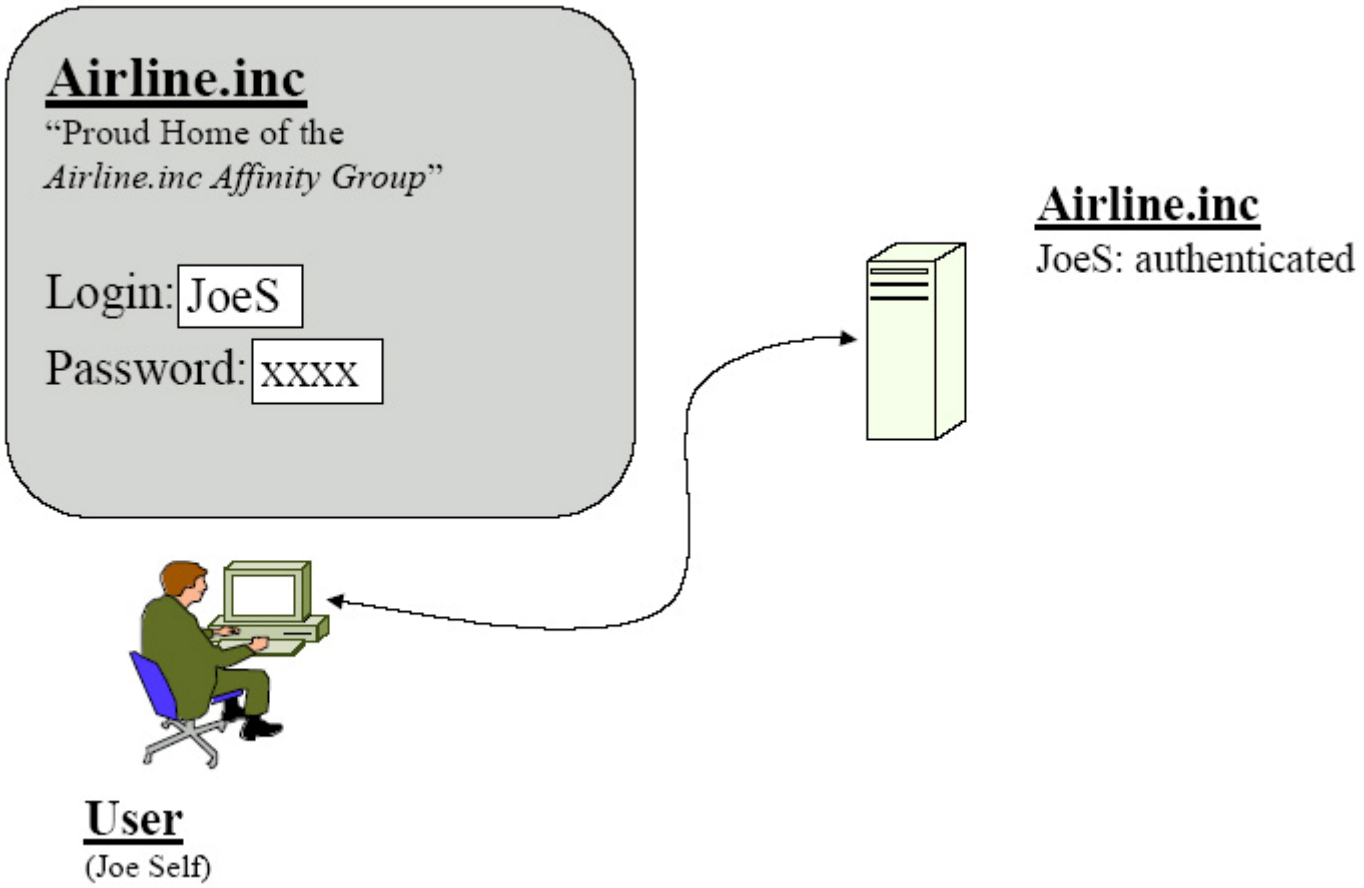
- Dienste können zwei Rollen einnehmen: Identity Provider oder Service Provider
- IP verwaltet die föderierte Identität
- Identity Provider und Service Provider müssen eine Vereinbarung getroffen haben, z.B. im Rahmen einer bestehenden Geschäftsbeziehung
  → Circle of Trust

Federated Network Identity

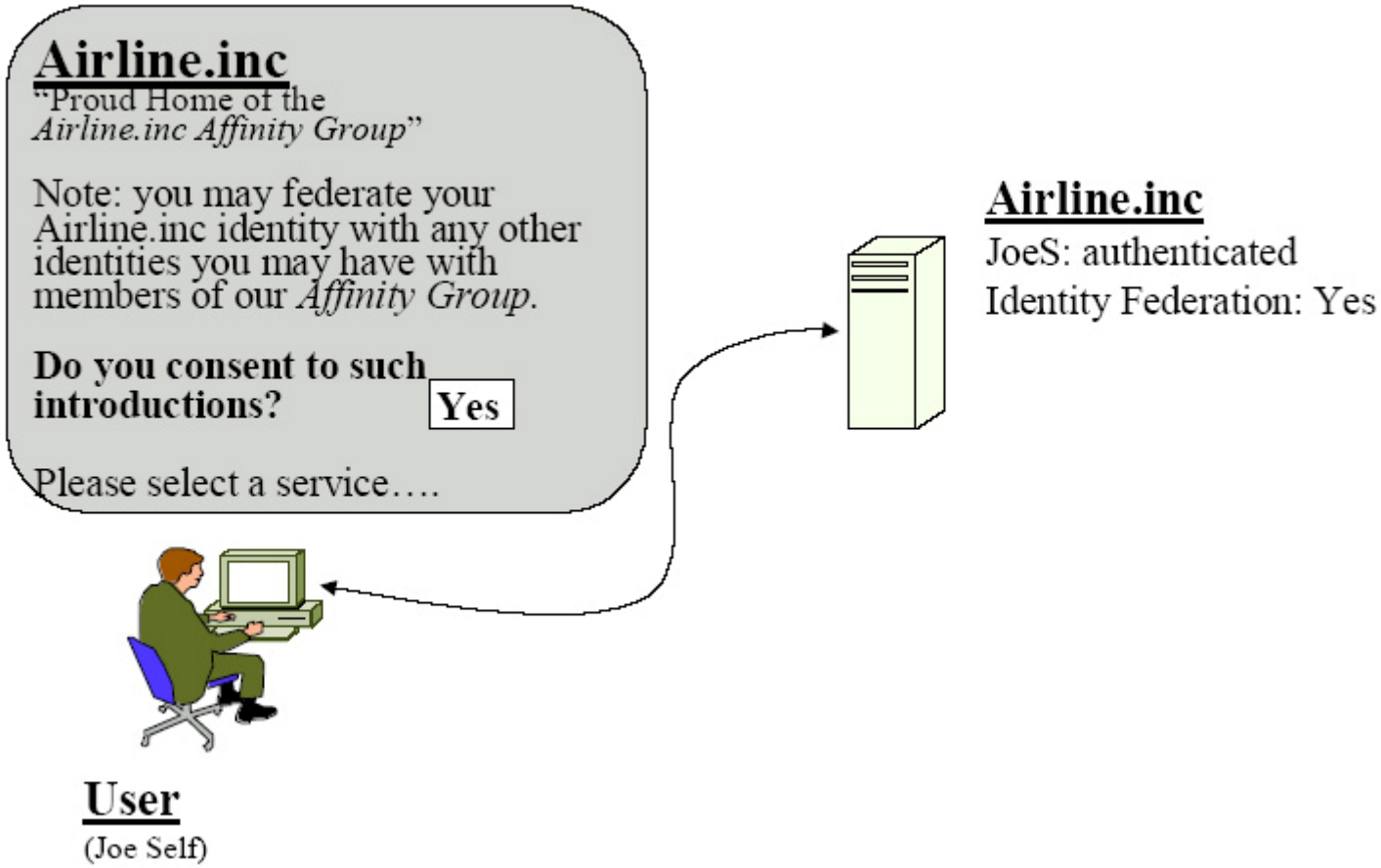


Liberty User Experience (1)

→ User logs in to Liberty-enabled website

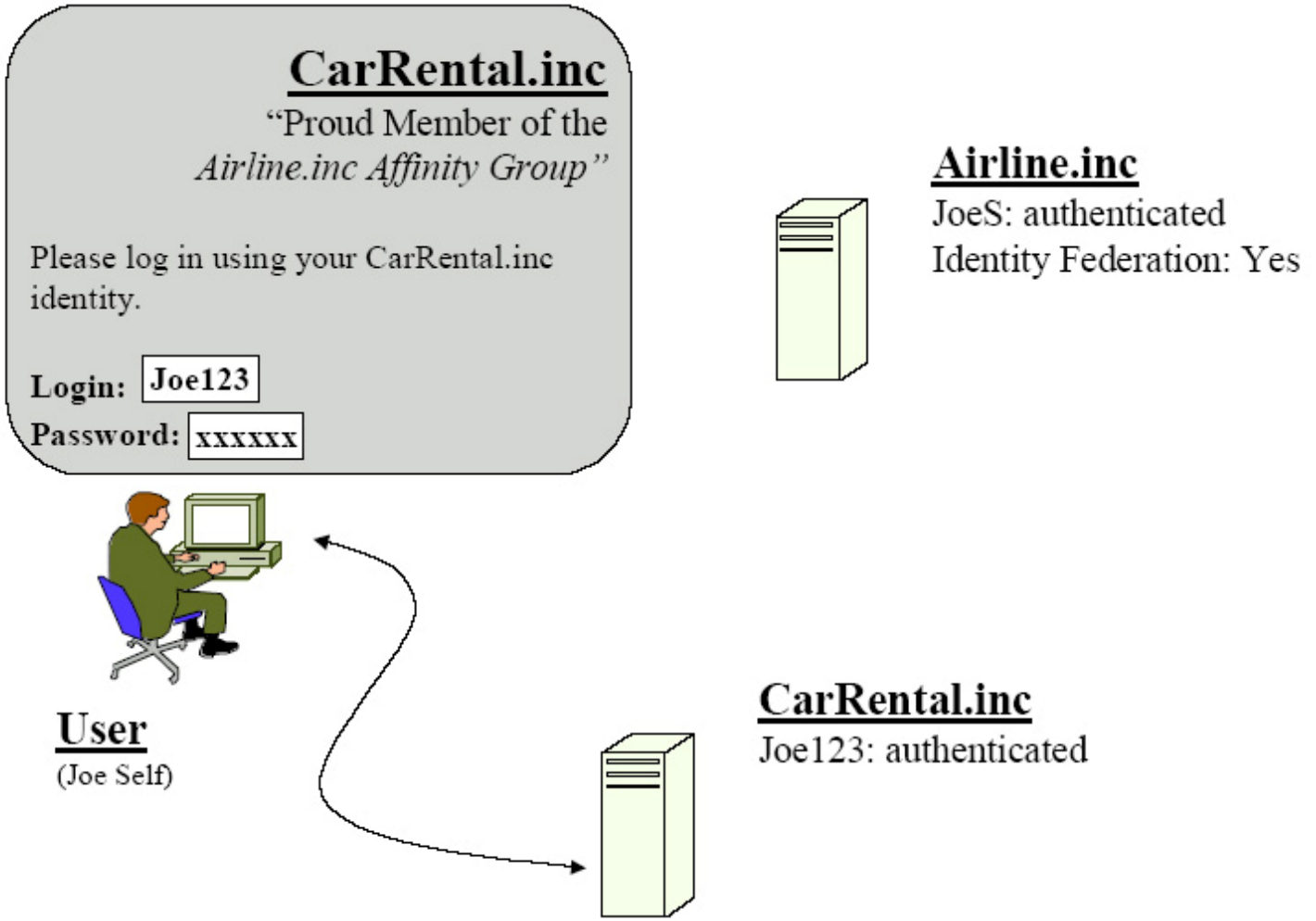


Liberty User Experience (2)
→ User elects to allow instructions



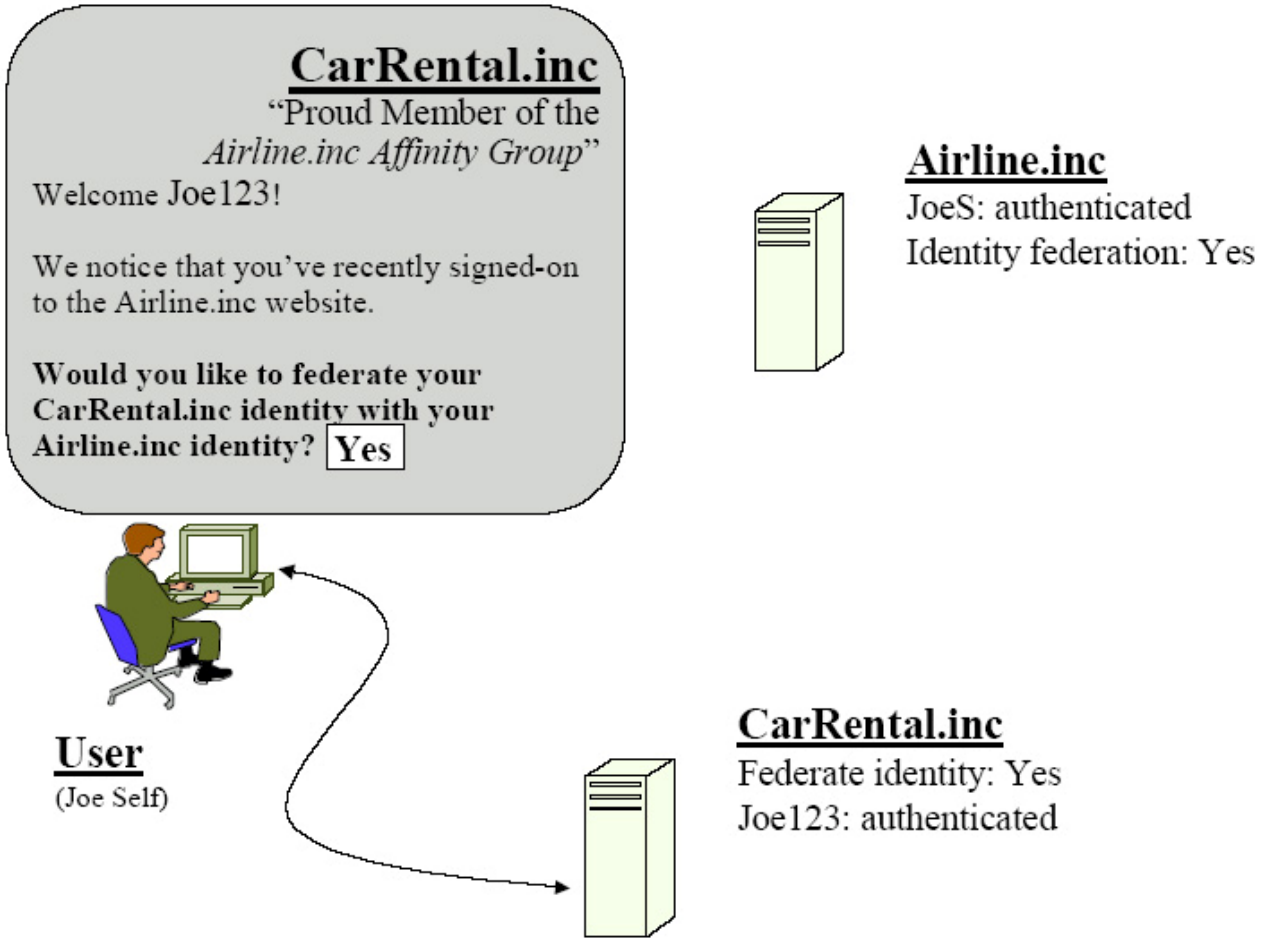
Liberty User Experience (3)

→ User signs-on using local SP identity



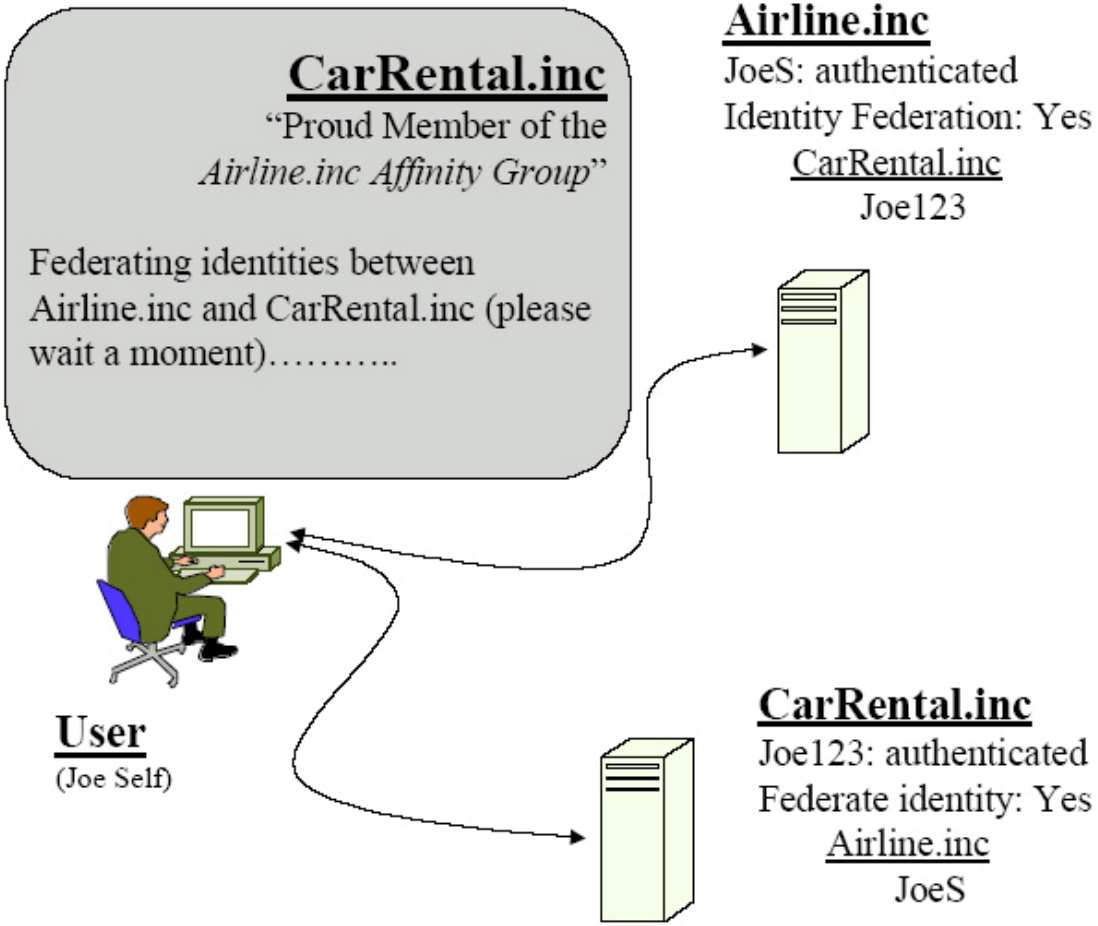
Liberty User Experience (4)

→ User allows to federate his local identities



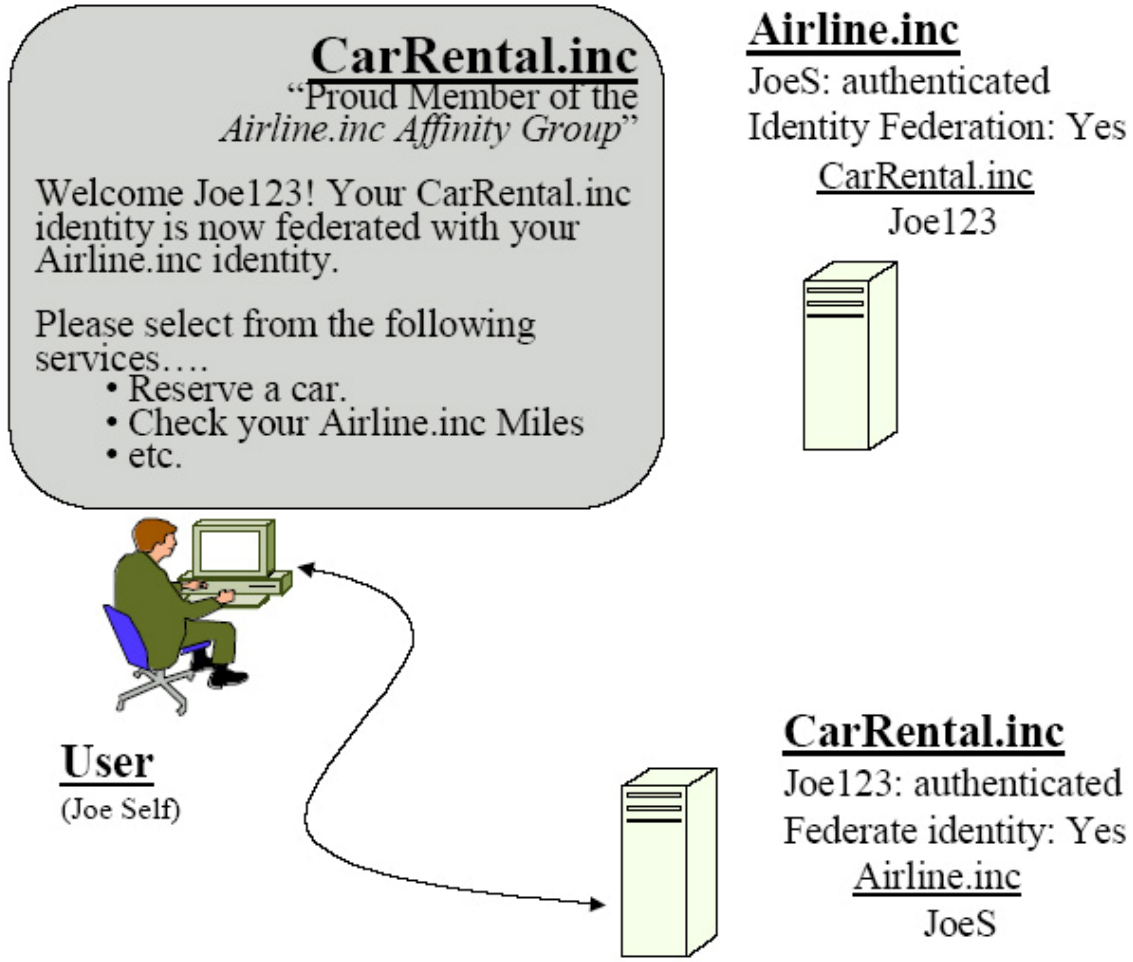
Liberty User Experience (5)

→ the websites federate the user‘s local id‘s



Liberty User Experience (6)

→ Service provider delivers services to user



Liberty User Experience (7)
→ Single Sign-On

- Startet der User seine Session beim Identity Provider, wird er automatisch bei allen verbundenen Service Providern angemeldet
- Startet er bei einem Service Provider, wird er zunächst zum Identity Provider geleitet.

Liberty Spezifikation

- Offene Standards
  - SAML (Secure Assertion Markup Language) als XML-basierendes Datenaustauschformat
  - Protokolle: HTTP und HTTPS
  - Implementierungsvorgaben eher vage
- Sicherheit
  - Nachrichten grundsätzlich digital signiert
  - Provider identifizieren sich durch Zertifikate

Identity Management
→ Weitere Ansätze

- Passport und Liberty stellen die Daten in die Verantwortung der Dienstleister
- Andere Blickrichtung stellt den Benutzer in den Mittelpunkt der Datenverwaltung
- Beispiele: DRIM (Dresden Identity Management) und ATUS (A Toolkit for Usable Security)

Ausblick

- Passport hat zukünftig nur noch Bedeutung für Microsoft-Services
- Microsoft wird vermutlich der Liberty Alliance beitreten
- Liberty-Ansatz ist vielseitig und kann z.B. auch im Firmenumfeld umgesetzt werden
- Erste Produkte wurden zertifiziert

Ausblick (2)

- Auch der benutzerorientierte Ansatz hat Berechtigung, z.B. Pseudonymverwaltung
- Er wird mit der Gesundheitskarte auch umgesetzt
- Erfolg von Identity Management hängt vom Vertrauen in das System ab → Anwender muss das Gefühl bekommen, volle Kontrolle über ihre Daten zu haben

Identity Management

Vielen Dank für die Aufmerksamkeit!

Gibt es noch Fragen?