

*There shall in that time be rumors of things going astray, erm, and there shall be a great confusion as to where things really are, and nobody will really know where lieth those little things with the sort of raffia-work base, that has an attachment. At that time, a friend shall lose his friend's hammer, and the young shall not know where lieth the things possessed by their fathers that their fathers put there only just the night before, about eight O'clock.*

*Life of Brian, Monty Python, 1979*

# Identity and Access Management

Elmar Geese

Jens Neumaier

# Agenda

Was ist Identity und Accessmanagement (IAM)?

IAM Leitbegriffe und Komponenten

Anwendungsfälle und Kontext

Produkte und Lösungen

Implementierung

Ausblick

# Identität ist ein weites Feld

↳ tarent

Definition: Die Identität einer Person ist die eindeutige Unterscheidbarkeit von einer anderen Person

Soziale Identität: Bevorzugung der eigenen Gruppe gegenüber anderen (Minimal Group Experiment)

Psychologisch: das Gefühl, »mit sich einig zu sein«, oder auch, vollkommen in einer Rolle aufzugehen, die man in der Gemeinschaft zu spielen hat.

# Identität ist ein weites Feld

## Philosophischer Kontext

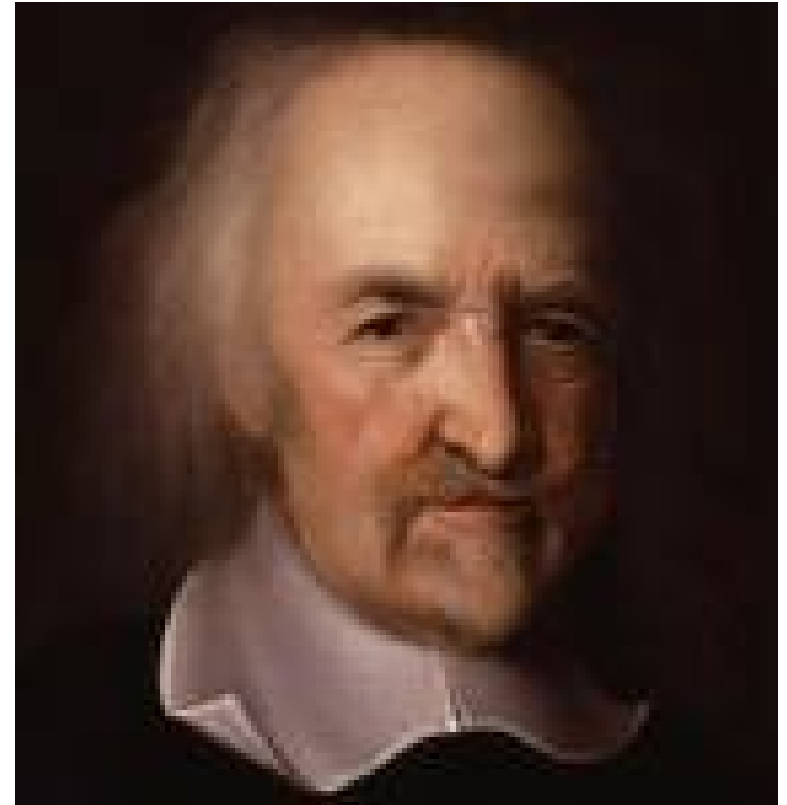
Wir nehmen eine Planke vom Schiff des Theseus.

Das ändert nicht die Identität des Schiffes.

Wir nehmen noch eine und noch eine, bis wir aus den Planken wieder ein Schiff bauen können.

Dieses ist offensichtlich nicht identisch mit dem ersten Schiff.

Wie viele Identitäten haben wir in der digitalen Welt ?



Thomas Hobbes (1588 - 1679)

# Identität ist ein weites Feld

## Sozialer Kontext

Wir können unsere Identität als „sozial geformt“ betrachten: Der soziale Kontext bestimmt die Identität mit der wir wahrgenommen werden (wollen).

## Rechtlicher Kontext

Zwei Seiten: Identifizierbarkeit zur Wahrung unserer Rechte und Pflichten – Recht auf Pseudonyme, Namensänderung, Geschlechtsänderung, Privatsphäre

## Technischer Kontext

Sicherheit vs. Machbarkeit vs. kommunikativer Selbstbestimmung in der digitalen Welt.

# Motivation

- Eine große Zahl von Menschen wird mit einer großen Zahl von IT Systemen konfrontiert.
- Das Internet sorgt dafür, dass es täglich mehr werden
- Auch innerhalb von Unternehmen und Behörden trifft man viele unterschiedliche Systeme an, die komfortabel und vertrauensvoll nutzbar sein müssen.
- Physische Identität - Logische Identitäten

# Motivation

- Ohne Digitale Identitäten gibt es keine wirklich vertrauenswürdigen digitalisierten Geschäftsprozesse
- Ohne für den Nutzer transparente digitale Identitäten gibt es keine Sicherheit und keine Privatsphäre
- Identität und Anonymität

# Access Management

Access Management leistet die Verwaltung von Nutzern und deren Zugriffsrechte:

*Access Management ist „The Process responsible for allowing Users to make use of IT Services, data or other Assets. Access Management helps to protect the Confidentiality, Integrity and Availability of Assets by ensuring that only authorized Users are able to access or modify the Assets.“*

(ITIL v3)

Identity Management leistet die Verwaltung von Accounts und deren Mapping auf Identitäten:

*Der Zweck des Identity and Access Management (IAM) ist die Vielzahl der Kennungen und personenbezogenen Informationen welche die Anwender für den Zugriff auf Applikationen, Ressourcen und IT-Systeme benötigen, zu reduzieren und nach Möglichkeit in einer einzigen digitalen Identität zusammenzufassen.*

[http://www.iam-wiki.org/Identity\\_and\\_Access\\_Management\\_\(IAM\)](http://www.iam-wiki.org/Identity_and_Access_Management_(IAM))

# Aber ...

↳ tarent

*... Access Management is sometimes referred to as Rights Management or Identity Management.*

(ITIL v3)

# Szenarien

- Ein Bürger, der eGovernment Dienstleistungen nutzen möchte, soll einerseits nicht mit einer Vielzahl von Accounts abgeschreckt werden, und will Kontrolle über seine Daten.
- Ein Sicherheitsbeauftragter in Unternehmen oder Verwaltung muss die Rechte eines Mitarbeiter kennen und verändern können.
- Der Datenschutz fordert, dass Benutzerdaten und deren Freigaben durch Selbstverwaltung gepflegt werden können.

- Digitale Identitäten schaffen
- Sicherheit und Komfort bei der Nutzung
- Systemgrenzen durch Standards und Interoperabilität überwinden
- Komponentenbasiertes IAM
- Wiederverwertung vorhandener Werkzeuge

# IAM Komponenten

- Authentifizierung
- Zugriffskontrolle
- Single Sign On
- Identity Federation
- Provisioning

# Authentifizierung

- Authentisierung
  - Nachweis der eigenen Identität
    - Benutzer ist Subjekt
  - Authentisierungsmethoden
    - Haben (Schlüssel)
    - Wissen (Passwort)
    - Sein (Biometrisches Merkmal)
- Authentifizierung
  - Verifizierung der behaupteten Identität
    - *Identity Provider* ist Subjekt

# Zugriffskontrolle

- Autorisierung
  - Einräumung von Rechten / Berechtigungen
- In verteilten System bietet sich eine rollenbasierte Zugriffskontrolle (RBAC) an
- Dreistufige Gliederung
  - Benutzer
  - Gruppen (Menge von Benutzer)
  - Rollen (Menge von Gruppen/Benutzern)
- Benutzer kann mehrere Rollen besitzen

- Einzelne Anwendungen verwalten Berechtigungen für einzelne Aktivitäten
- Die Gewährung einer Berechtigung hängt von der Rolle des Subjekts ab
- Rollen werden im Identity Management System verwaltet und zugewiesen
- Berechtigungen kennen nur Anwendungen

# Single Sign On

↳ tarent

- „Einmalanmeldung“
  - Einmalige Authentifizierung ist für mehrere Komponenten eines Gesamtsystems gültig
- Besonders im Kontext von Portalen häufig vorausgesetzt
- Eine *physische* Identität im gesamten System
  - Verschiedene Benutzernamen (*logische* Identitäten) möglich

# Single Sign On - Lösungsansätze

↳ tarent

- Speicherung sämtlicher Authentifizierungsdaten  
(Einfaches Beispiel: Passwort-Manager im Firefox)
- Erhalt eines Sitzungsgeheimnisses bei Anmeldung  
(Ticket, Token o.ä.)
  - Anwendungen teilen Geheimnis  
(z.B. über Cookies)
  - Verifikation und Abfrage der Identität über  
zentrales SSO-System

# Identity Federation

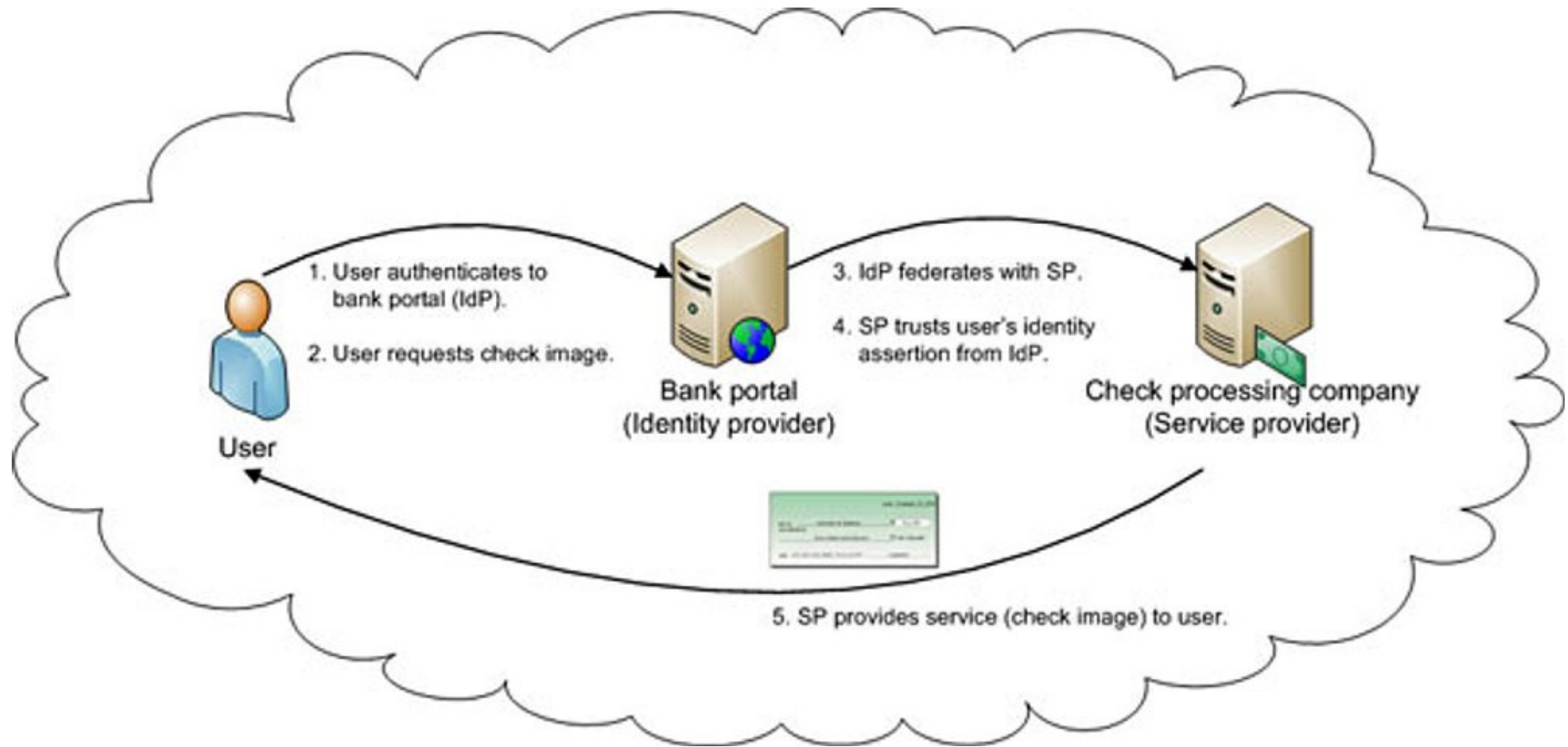
- Federation  $\hat{=}$  Vereinigung
- Verknüpfung *logischer* Identitäten unterschiedlicher autonomer Sicherheitssysteme mit einer *physischen* Identität
- *Identity Provider* kennt logische Identität „A“ des Benutzers
- *Service Provider* kennt eine andere logische Identität „B“ des Benutzer
- Benutzer „A“ möchte einen Dienst beim *Service Provider* nutzen
- Kein Mehrfachlogin erwünscht

# Identity Federation

- Aufbau einer *Federation* zweier *logischer* Identitäten
  - Benutzer meldet sich in beiden System an und macht Vereinigung bekannt
  - Systeme können Vereinigung selbst eindeutig vornehmen
- In Zukunft weiß *Identity Provider*, dass Benutzer „A“ von *Identity Provider* Benutzer „B“ des *Service Provider* entspricht
- *Service Provider* vertraut *Identity Provider* und erfragt zukünftig die zugehörige Identität
- Unterstützung durch SAML 2.0

# Identity Federation

↳ tarent



Quelle: <http://opensso.dev.java.net>

# Provisioning

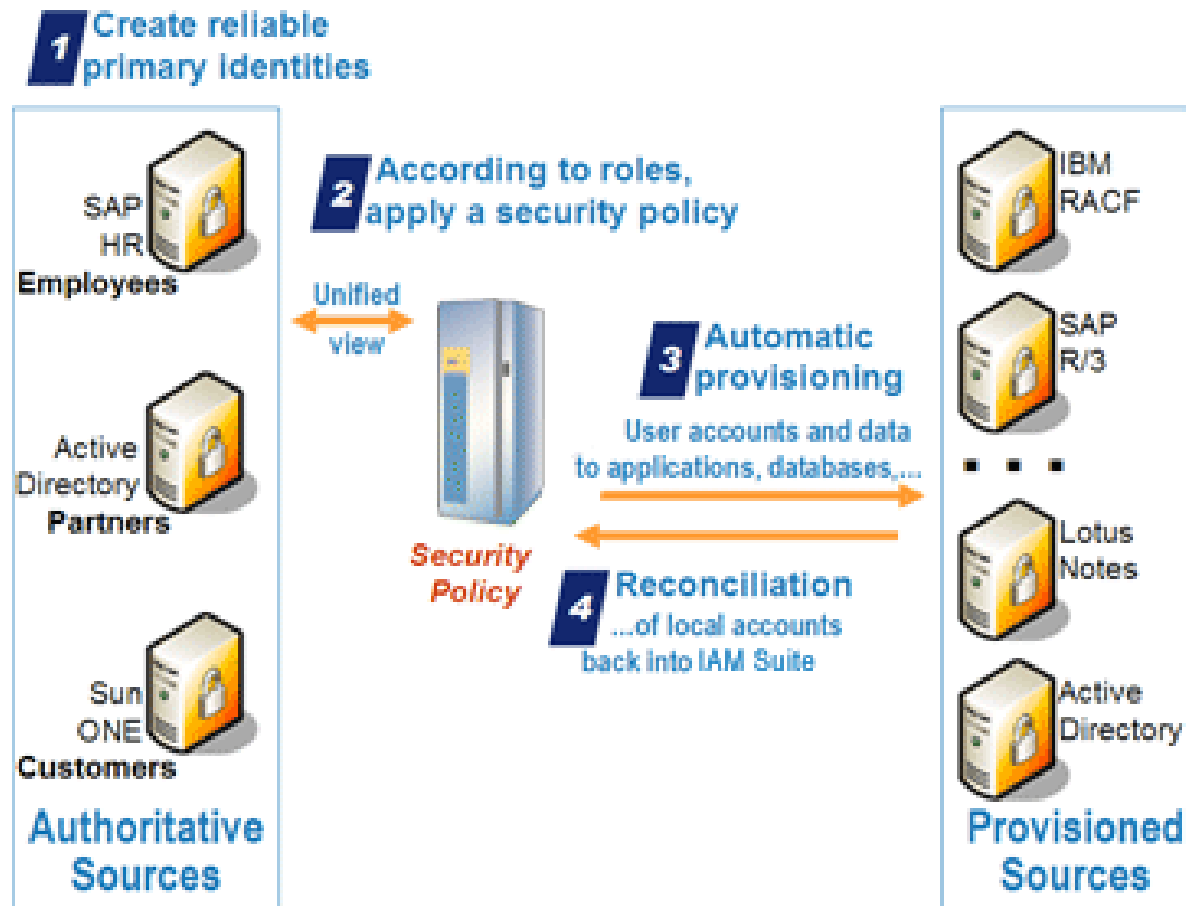
- Prozess um Anwendern automatisiert Zugang zu Systemen zu verschaffen
- Benutzer erhalten auf Basis von Regeln und Rollen Benutzerzugänge und Berechtigungen zu diversen Systemen
  - Zugang zu Gebäuden
  - Zugang zu Systemen  
(Desktop-System, DMS etc.)
  - Zugang zu Anwendungssoftware  
(Buchhaltungssoftware, Projektplanung etc.)
  - E-Mail Zugang u.v.m

# Provisioning

- Problem:
  - Uneinheitliche Systemlandschaft
  - Viele Accounts in verschiedenen Systemen und Anwendungen benötigt
- Lösungsansätze:
  - Provisioning System legt Accounts in externen Systemen an
  - Authentifizierungs-Komponenten der Systeme sind an Provisioning System gekoppelt und erstellen benötigte Accounts automatisch

# Provisioning

↳ tarent



Quelle: <http://www.evidian.com>

# IAM Werkzeuge

↳ tarent

- Zertifikate
- Verzeichnisdienste
- Datenbanken

- Zertifikatsbasierte Authentifizierung
- Basiert auf eine **Public-Key-Infrastructure**:
  - Asymmetrisches Kryptografieverfahren
  - Schlüsselpaare aus **privaten** und **öffentlichen** Schlüsseln
  - Öffentliche Schlüssel werden von Zertifizierungsstelle vergeben und von Registrierungsstelle geprüft
  - Nur Benutzer besitzt privaten Schlüssel um seine digitale Identität zu beweisen

# Verzeichnisdienste

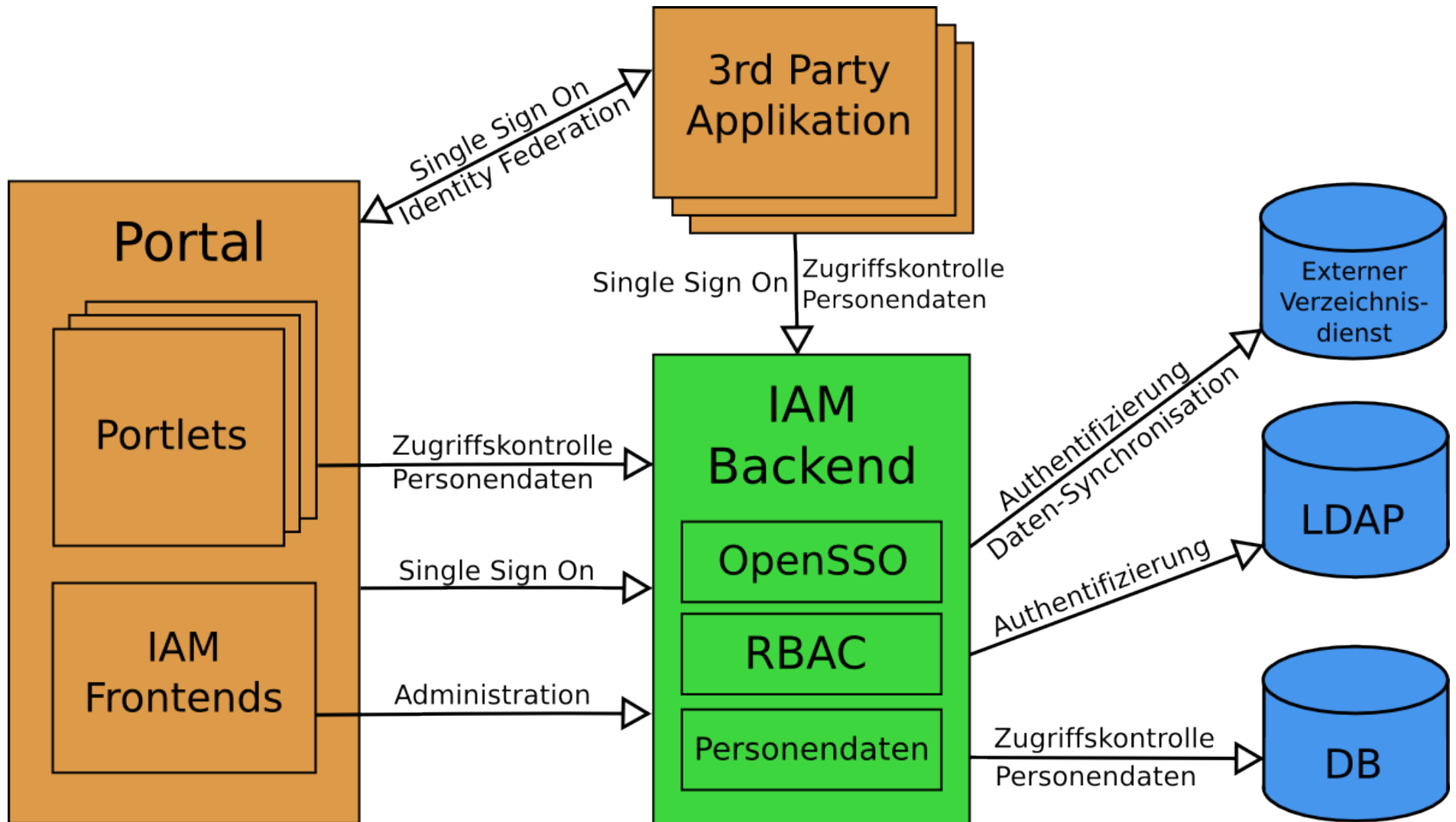
- Spezielle hierarchische Datenbanken zur Sammlung von Daten bestimmter Art
- Lightweight Directory Access Protocol (LDAP)
- Verbreitete Verzeichnisdienste:
  - OpenLDAP (OpenSource, Sun)
  - Microsoft ActiveDirectory
  - Novell eDirectory
  - u.v.m

# Verzeichnisdienste

- Benutzerdaten liegen häufig in Verzeichnisdiensten vor
- Häufig unterschiedliche Verzeichnisdienste für Abteilungen oder Unternehmensbereiche
- Enthalten häufig auch Personendaten und Gruppenzugehörigkeiten
- Identity Management System muss diverse Verzeichnisdienste einbinden
  - Wer hat die Hoheit über Benutzerdaten?
  - Synchronisationsprobleme

# Architekturbeispiel eines OSS IAM

↳ tarent



# OSS Tools und Bausteine

↳ tarent

- OpenSSO
- OpenLDAP
- PostgreSQL, MySQL
- JEE
- JAX-WS
- WS-Security & SSL

# OpenSSO

- Kurz: Open Web Single Sign-On Project
- OpenSource: CDDL (anerkannte FSF OS-Lizenz)
- Basiert auf kommerziellem Produkt:  
Sun Java System Access Manager
- Benötigt LDAP Verzeichnisdienst
- SSO und Identity Federation über:
  - Webservice und REST-Schnittstellen
  - SAML 2.0
- <http://opensso.dev.java.net/>

# OpenLDAP

- LDAP-Verzeichnisdienst
- Lauffähig unter Unix, Linux, Mac OS X und Microsoft Windows
- OpenSource: OpenLDAP Public License
- Sehr aktives und stabiles Projekt
- Sehr gute Reaktionszeiten
- <http://www.openldap.org/>

# PostgreSQL, MySQL o.ä.

↳ tarent

- Relationale Datenbank zur Speicherung personenbezogener Daten
- PostgreSQL und MySQL verfügen über Funktionalitäten zur Verschlüsselung von Spalten, Tabellen oder ganzer Datenbanken
- Notfalls Dateisystemverschlüsselung verwenden
- Schlüssel nicht dauerhaft auf System halten (USB-Stick oder ähnliches beim Hochfahren der Datenbank)

- Identity Management System ist ein zentraler Knoten der gesamten IT-Infrastruktur
  - Reaktionszeiten
  - Hochverfügbarkeit
  - Skalierbarkeit
- Java Enterprise Lösungen bieten Konzepte und Plattformen um dies einfacher zu gewährleisten
  - Beispiel: EJBs im JBoss Application Server

- Java API for XML - Web Services
- JSR 224: JAX-WS 2.0
- Annotationsbasierte Auszeichnung von WebServices
- WebServices über SOAP oder REST
  - SOAP lässt sich leicht mit WS-Security erweitern
- Wechsel des WS-Providers möglich:
  - Sun Metro WS-Stack, Apache CXF-Stack, JBoss Native Stack o.a.

- WS-Security
  - WS-Nachrichten können verschlüsselt und signiert werden
  - Über Signatur kann geprüft werden, ob der Client zu bestimmten Anfragen berechtigt ist
- SSL
  - Einfach einstellbare Verschlüsselung
  - Anfragen an relationale Datenbanken und LDAP-Verzeichnisdienste verschlüsseln

# IAM Standards

↳ tarent

- Kerberos
- SAML 2.0
- OpenID

# Status IAM Produkte

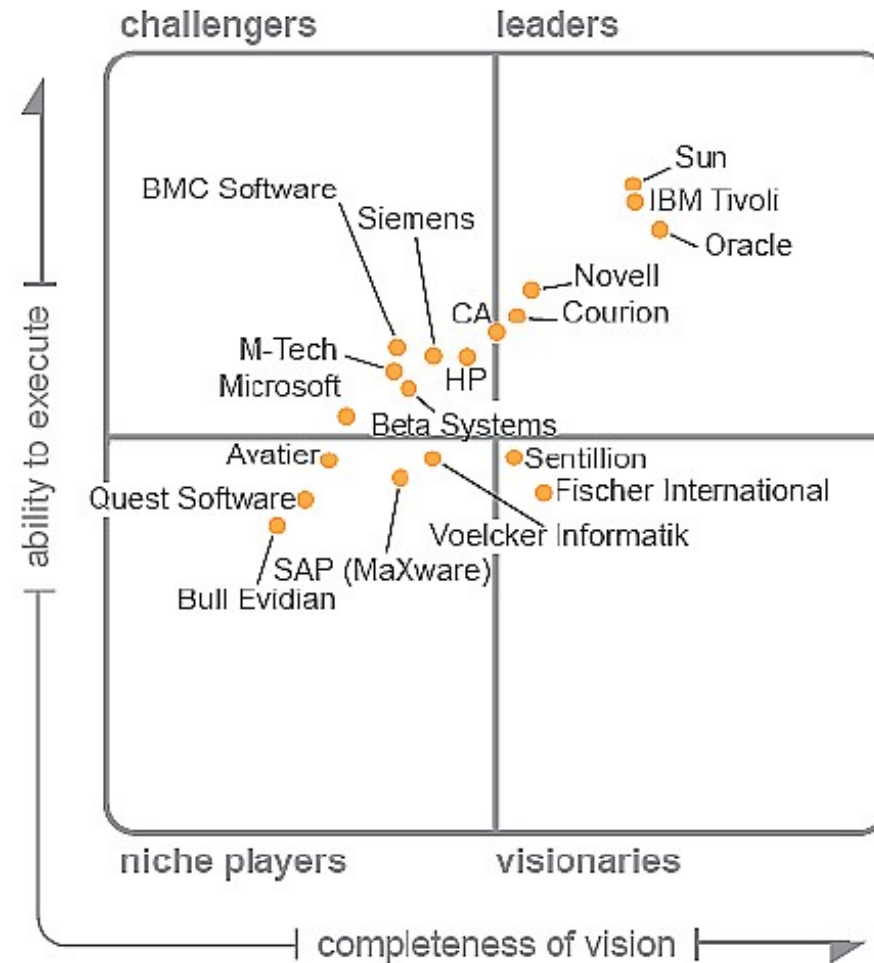
- Erste Lösungen bestehen, meist abgeleitet aus Access Management und Verzeichnisdiensten
- Nur Teilbereiche werden adressiert, ganzheitliche Ansätze fehlen meist
- Fragmentierter, wachsender Markt
- Zähe Entwicklung

# Historie

- Access Management
- Verzeichnisdienste (Novell, LDAP, Microsoft ADS, ...)
- Single Sign On
  - Kerberos (RFC4120) 1978
  - Microsoft Passport 1999-2007
  - OpenID 2005

# Marktsicht

↳ tarent



As of August 2007

Source: Gartner (August 2007)

# Liberty Alliance

- Von Sun als Gegenmaßnahme zu MS Passport gegründet
- Ziel: geregelter Datenaustausch zwischen prinzipiell gleichberechtigten Benutzeraccounts auf verschiedenen Rechnern.
- Mitglieder: Novell, Oracle, Sun, Intel
- GPL Implementierung Lasso:  
<http://lasso.entrouvert.org/>

# Microsoft Passport

- Architektur: zentralisierter Server
- Einführung durch Marktdruck
- Zwangsintegration via Hotmail
- Verbreitung via MS-eigenen Diensten (Expedia, MSN)
- Keine Akzeptanz als SSO System
- Inzwischen durch Microsoft CardSpace aus dem .Net-Framework 3.0 abgelöst.

- Offener Standard zur Identifikation & Authentifizierung
- Gemeinsame Nutzung von Daten möglich
- Jeder kann einen *Identity Provider* für das OpenID-Verfahren bereitstellen
- Viele Unternehmen unterstützen OpenID-Authentifizierung:
  - AOL, BBC, Google, IBM, Microsoft, MySpace, Orange, PayPal, VeriSign, Yandex, Ustream and Yahoo! u.v.m

1) Anmeldung am *Service Provider* durch OpenID



2) *Service Provider* leitet zum OpenID *Identity Provider* weiter

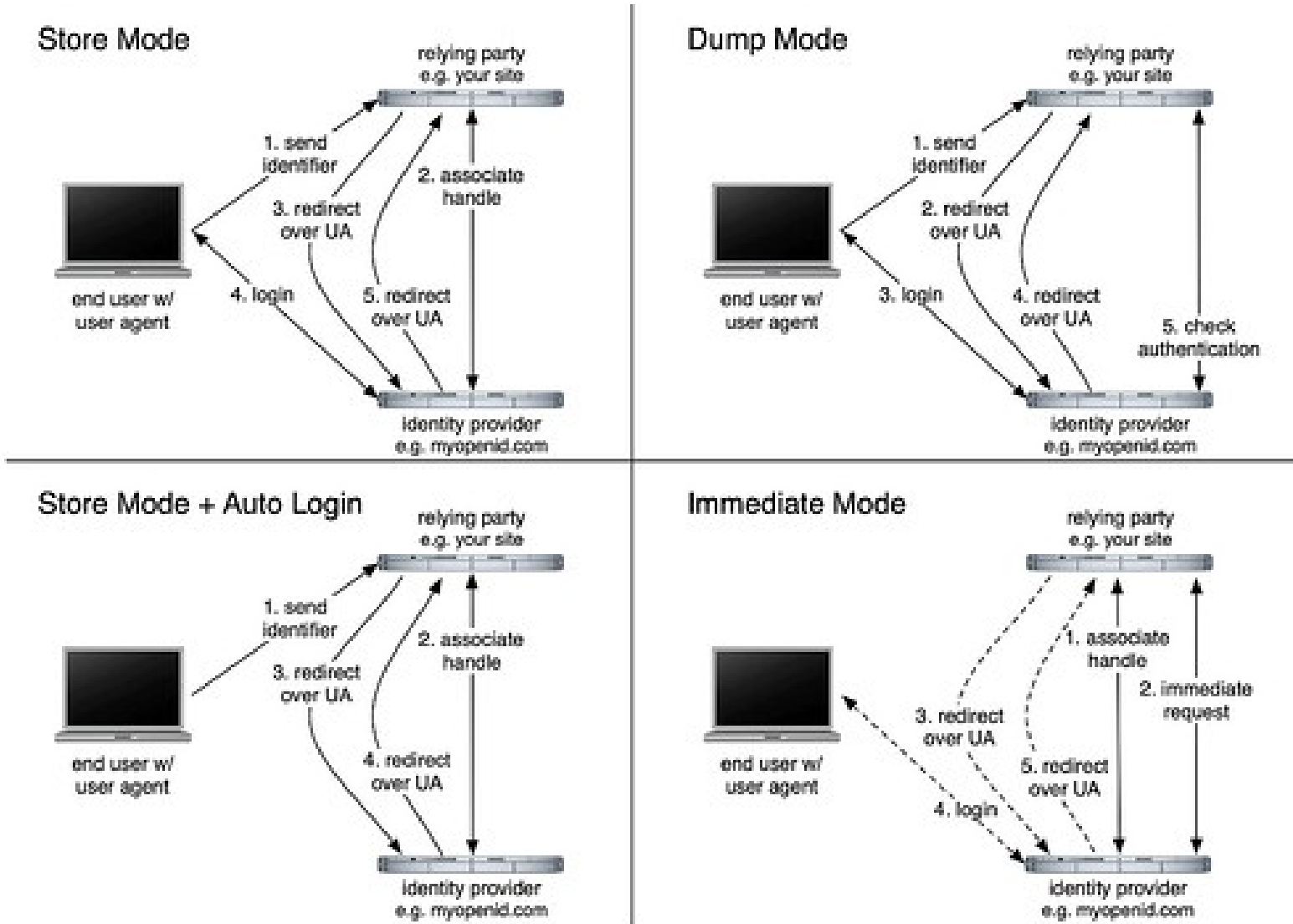
3) Benutzer authentifiziert sich am *Identity Provider*

4) *Identity Provider* verifiziert Identität und leitet Benutzer zum *Service Provider* zurück

5) Benutzer nutzt *Service Provider*

# OpenID

↳ tarent



Quelle: <http://www.flickr.com/photos/keepthebyte>

- Alle Bausteine zum Aufbau eines IAM sind frei vorhanden
- Grundanforderungen können gewährleistet werden
  - Reaktionszeiten & Hochverfügbarkeit
  - Sicherheit bei Speicherung & Übertragung
- Probleme
  - Übernahme/Einbindung von Verzeichnisdiensten
    - Benutzer, Personendaten, Gruppen
  - Einbindung bestehender Berechtigungssysteme
    - Anwendungen müssen sich integrieren

# IAM aus Benutzersicht

↳ tarent

- Komfort und Risiken
- Identität vs Anonymität/Pseudonymität
- Informationelle Selbstbestimmung

# Umgang mit Personendaten

- Gemeinsame Nutzung personenbezogener Daten
  - Grundschatz: Name, Adresse, Geburtsdatum
  - Besonderer Schutz:  
rassische und ethnische Herkunft, politische Meinungen,  
religiöse oder philosophische Überzeugungen,  
Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben
  - Unterschiedlicher Schutzbedarf nach BSI-  
Grundschatzhandbuch
- Hauptprinzipien
  - Datensparsamkeit und Vermeidung
  - Erforderlichkeit und Zweckbindung

- Gemeinsame Nutzung von Personendaten in einem Identity Management System
  - Benutzer möchte persönliche Daten wie Namen, Adressen und andere Kontaktdaten nicht mehrfach pflegen
- Daten nur dort speichern wo sie gebraucht werden?
  - Vorteil: kein Freigabeproblem
  - Nachteil: Anwendungen speichern Daten mit Schutzbedarf und müssen dementsprechend abgesichert werden

- Gemeinsame Nutzung von Personendaten in einem Identity Management System
  - Benutzer möchte keinen Freischein für die Verteilung der Daten herausgeben
  - Anwendungen der Personalabteilung dürfen meine Kontodaten einsehen
  - Anwendungen zur Antragsbearbeitung dürfen nur meine Meldeadresse einsehen
  - Firmen-interne Dienste dürfen meine private Telefonnummer einsehen

- Datenschutzrechtliche Maßnahmen
  - Übertragung - Verschlüsselung von Verbindungen
    - SSL, WS-Security o.ä. PKI-basierte Kryptografieverfahren verschlüsseln
  - Speicherung - Verschlüsselung von Daten
    - Im Zweifel höheren Schutzbedarf erwarten
    - Datenbanken verschlüsseln
    - Daher zusätzliche relationale Datenbanken statt LDAP-Verzeichnisse

# Zusammenfassung

- IAM ist ein sich entwickelnder Bereich
- Viel Nachfrage, wenig Lösungen
- Noch viel zu tun
- Standards fehlen
- Viel Raum für OpenSource IAM Systeme

**Man:**

I think it was, "Blessed are the cheesemakers"!

**Gregory's wife:**

What's so special about the cheesemakers?

**Gregory:**

Well, obviously it's not meant to be taken literally.

It refers to any manufacturers of dairy products.

Aus „Life of Brian, Monty Python 1979“