

Identitätsmanagement, personalisierte Services und Verzeichnisse



Dr. Uwe Hübner
huebner@his.de

- Motivation
- Was ist "Identitätsmanagement"?
- Welches Spektrum an Verzeichnissen existiert schon?
- Wie werden "personalisierte Services" organisiert?
- Welche Schnittstellen bieten die HIS-Moduln heute und zukünftig?
- Wie steht es um den Datenschutz?

Zielgruppe: Entscheider, Admins

Motivationen

Wozu soll "Identitätsmanagement" gut sein?

Effizienz der IT-Nutzung verbessern:

- kurzfristige IT-Nutzung durch neue Mitarbeiter/Studenten
- komfortable Passwortänderungen
- Reduzierung manueller Fehler bei der Provisionierung

IT-Administrationskosten senken:

- Selbstbedienfunktionen für Ändern von Passwörtern
und persönlichen Informationen
- konsistente Nutzungsrichtlinien
bei Kombination aus zentraler Steuerung und lokaler Autonomie

Einhaltung gesetzlicher Vorgaben:

- Richtliniensetzung und Auditierung
-

Begriffe

Identität (*identity*)

- lat.: identitas - Wesenseinheit
- Summe der Merkmale, anhand derer sich ein Mensch (oder eine Sache) von anderen unterscheidet
- erlaubt eindeutige Identifizierung

Identitätsmanagement (*identity management*)

- Regelung von Identitäten und Berechtigungen in Unternehmen
- nicht nur "eigene Mitarbeiter" - auch Partner, Kunden ...
- Infrastruktur für "digitale Identitäten" ist erforderlich

Authentifizierung (*authentication*)

- Nachweis (Verifikation) einer Identität oder Rolle
- Authentifizierung kann zur Identifikation dienen
- Authentifizierung muß nicht immer mit Identifikation verbunden sein
mechanischer Schlüssel "authentifiziert" Besitzer gegenüber Schloß, gibt aber nicht unbedingt die Identität des Besitzers preis

Autorisierung (*authorization*)

- Zuweisung und Überprüfung von Rechten
 - zur Benutzung von Diensten
 - zum Zugriff auf Daten
- Autorisierung schließt Authentifizierung ein

Abrechnung (*accounting*)




Authentifizierung

Mit welchen Merkmalen kann eine Authentifizierung erfolgen?

1. **Wissen**
Passwort, PIN
2. **Besitz**
Chipkarte, RFID-Token, Passwortgenerator ...
3. **Eigenheiten**
Fingerabdruck, Gesicht ...
4. **Fähigkeiten**
Unterschrifts-Dynamik, Stimme ...

Mehrfaktor-...

Verzeichnisse an einer Hochschule

-  Mitarbeiter [HIS](#)
-  Studierende [HIS](#)
-  Studienbewerber [HIS](#)
-  Studieninteressenten [HIS](#)
-  Alumni [HIS](#) *
-  Bibliotheksnutzer
-  Chipkarteninhaber
-  Zertifikats-Inhaber
-  Zutrittskontrolle/Arbeitszeitregistrierung
-  Schlüsselinhaber, Parkberechtigungen
-  Lernmanagement-Systeme [HIS](#) *
-  Telefonverzeichnis
-  Softwarelizenz-Inhaber
-  Lieferanten [HIS](#)
-  Kunden (Kurse ...)
-  Gäste, Freunde und Förderer [HIS](#) *
-  Email-Adressen [HIS](#)
-  IT-Nutzungsrechte ... [HIS](#) *

* - Schnittstelle in Vorbereitung

Domänen für Verzeichnissysteme

 Personeninformationen

 Strukturinformationen

mehrere unabhängige Bestände

 mit jeweils eigener "Provisionierung"

 Inkonsistenzen

● Summe der Änderungsaufwendungen

● sichere Ersteinträge?

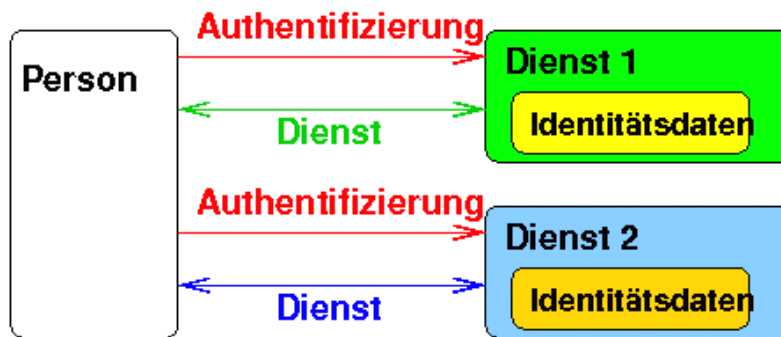


Bild 6-1

Personalisierte Services

und mögliche Quellen für Nutzerinformationen

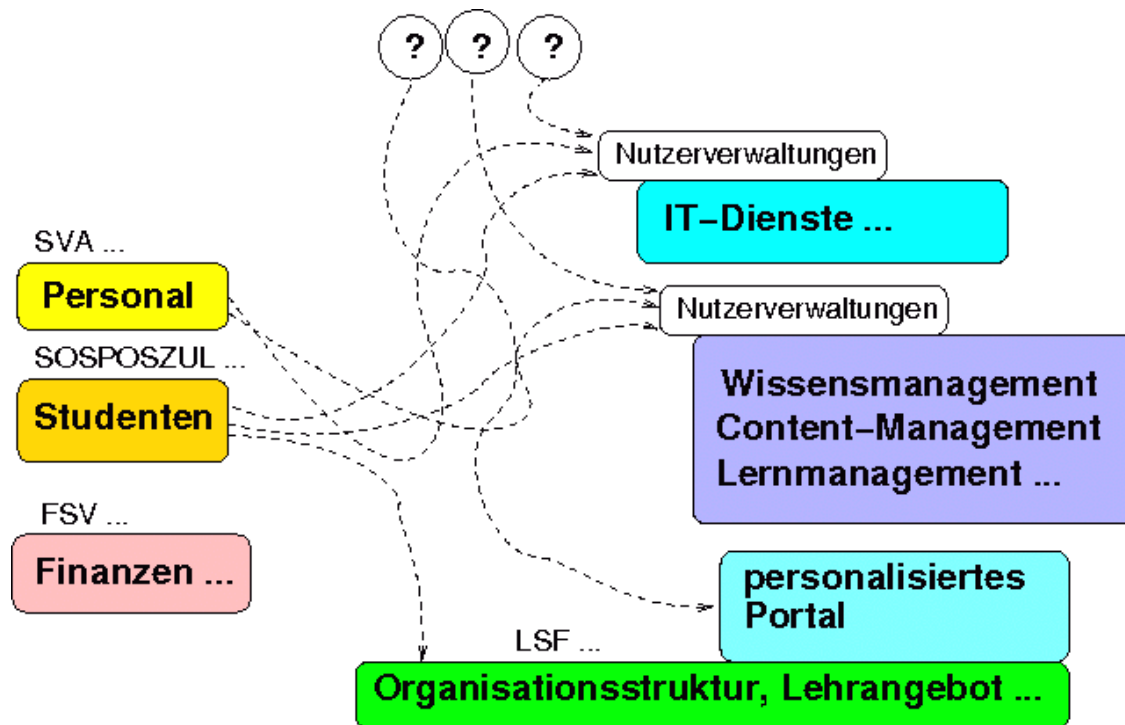


Bild 7-2

Provisionierung ... Deprovisionierung

● Konfigurieren eines Dienstes für einen bestimmten Nutzer

● Authentifizierungsmerkmale, Berechtigungen ... Abrechnungsdaten

Zentrale Identitätsverwaltung

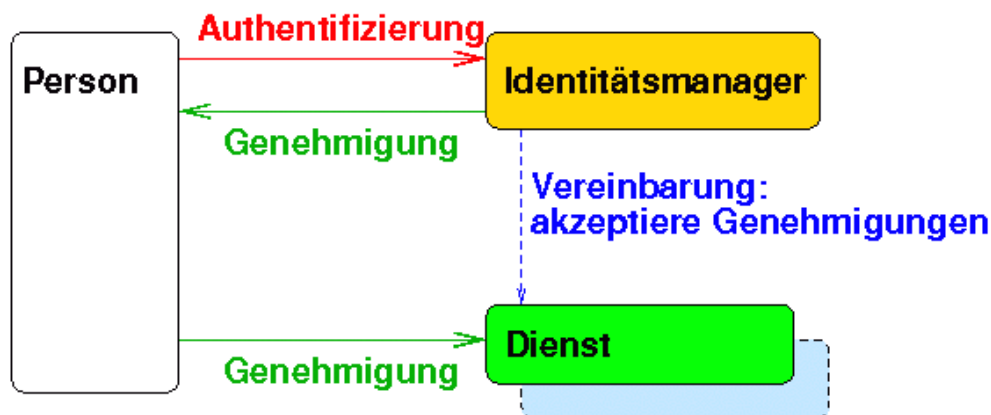


Bild 8-3

Relation zu **Single Sign On (SSO)** und **Unified Login**

Unterstützung personalisierter Dienste und Verzeichnisse

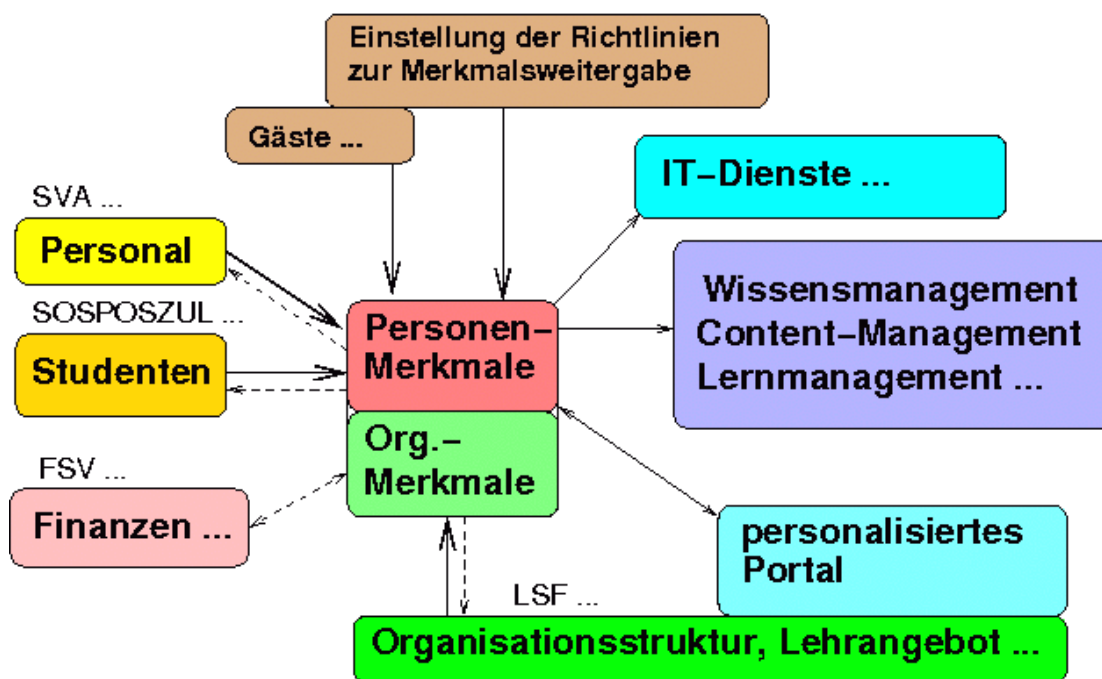


Bild 9-4

Funktionalitäten

- Vermittlung des Zugriffs auf ausgewählte Merkmale
- Replikation der Merkmale (*wenn nötig*)
- Behandlung von Spezialfällen (*gleichzeitig Student/Mitarbeiter ...*)

- Einstellung der Richtlinien zur Weitergabe (*welche Merkmale wohin?, Replikation ...*)
- Aufnahmemöglichkeit zusätzlicher Personen

Kopplung mit anderen Identitätsmanagement-Systemen

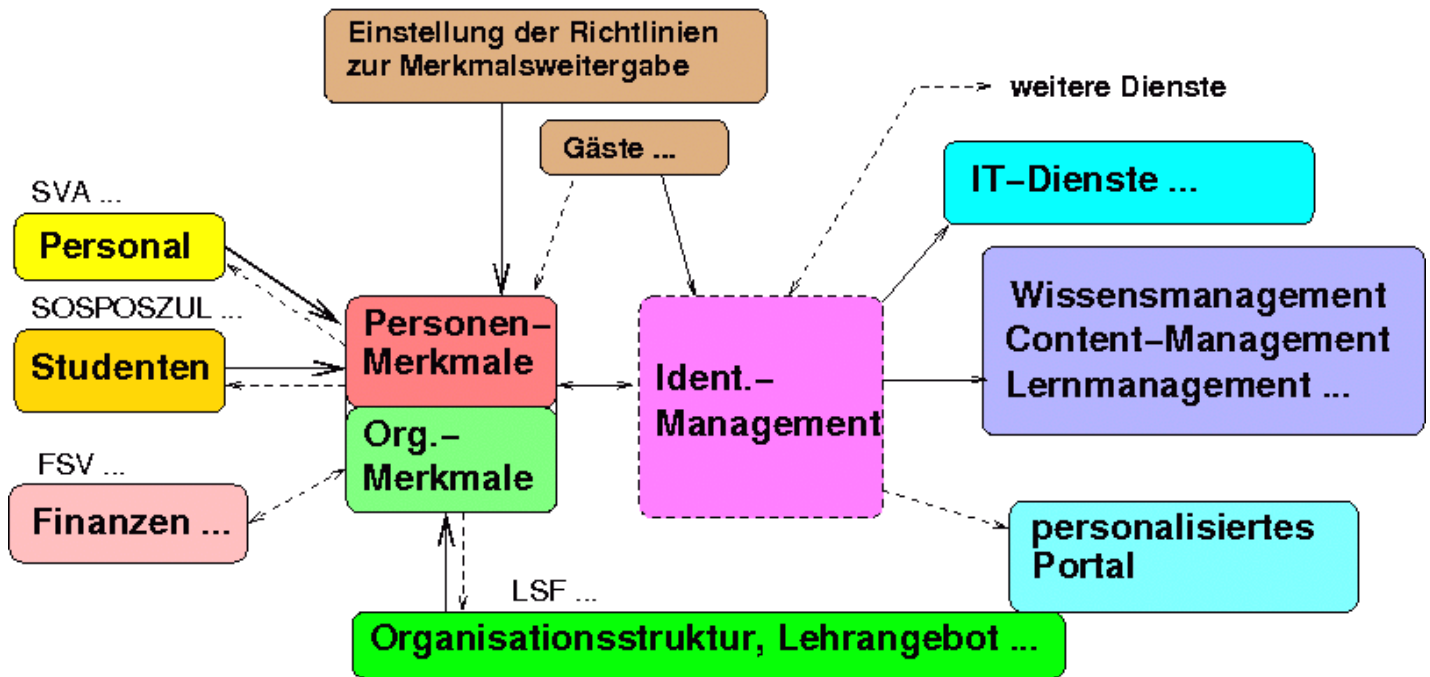


Bild 11-5

Datenschutz-Aspekte

- nur die für die Benutzung eines konkreten personalisierten Dienstes **notwendigen** Daten werden weitergegeben
- jede Person kann **einsehen**, welche Daten an welche Systeme/Anwendungen weitergegeben werden
- jede Person kann Daten ggf. **korrigieren** oder korrigieren lassen
Richtlinien geben Aktualisierungsrichtung vor!
- jede Person kann **einstellen**, welche Daten an welche Systeme/Anwendungen weitergegeben werden
 - Richtlinien geben Grundeinstellung vor
z.B. Name und Fach an eigenes Lernmanagement, nichts an andere Einrichtungen
 - Unterschied zu "Selbstanmeldung" bei den personalisierten Diensten
Daten von der Verwaltung verifiziert

- Grundeinstellung "nichts weitergeben"?
es funktioniert kein Dienst, Rechner/E-Mail nicht benutzbar ...

Identitätsmanagement aus Sicht von Privatpersonen

- zielgerichteter und verantwortungsvoller Umgang mit Identität, Anonymität und Pseudonymität
EU-Projekt PRIME (Privacy and Identity Management for Europe)
- in verschiedenen Situationen unter verschiedenen Identitäten agieren?
erschwert Anlegen umfangreicher Profile über Nutzer (ohne deren Einverständnis)
- Problemfall **Identitätsdiebstahl (identity theft)**

Ausblick: Föderationen

*was gern übersehen wird:
Partnerschaften, Fusionen, Organisations-Änderungen ...*

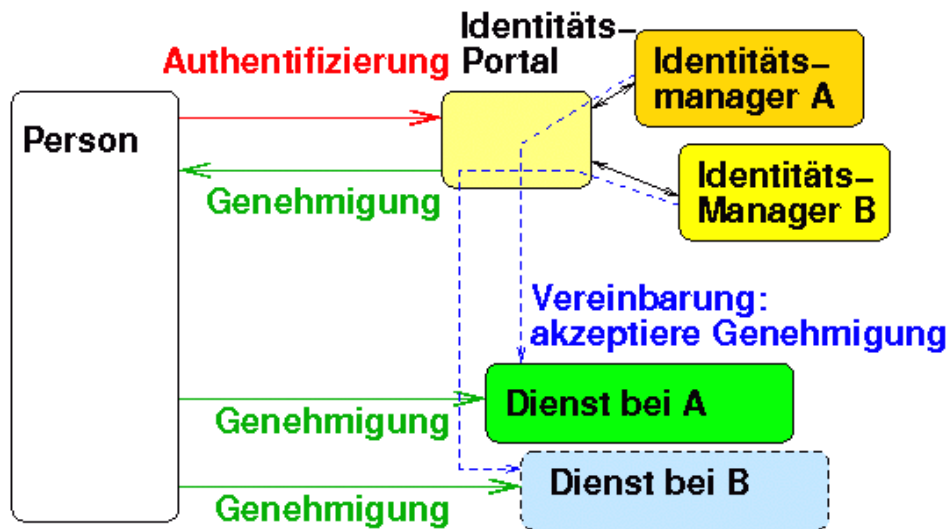


Bild 14-6