Identitätsverwaltung und Nachweis mit der KommDB an der Universität Tübingen

Dietmar Kaletta
Zentrum für Datenverarbeitung
Universität Tübingen

Dietmar.Kaletta@uni.tuebingen.de

ZKI-Arbeitskreis Verzeichnisdienste, Tübingen 28.06.2005

KommDB

Zielsetzung

Entwicklung und Einführung einer zentralen Kommunikations-Datenbank (KommDB) an der Universität Tübingen als Grundlage für zentrale Elektronische Dienste der Universität

Dietmar Kaletta, Tü 28.06.05

Probleme

- **Verschiedene Datenquellen mit unterschiedlichen, z.T. unvollständigen Personenverzeichnissen und -attributen in unterschiedlichen Einrichtungen der Universität**
- **Fehlende gesicherte Identitätsfeststellung der Personen**
- **Fehlende Identitätsverwaltung (fehlende join engine)**
- **Starke Vermischung von Identitätsmerkmalen mit Rollen und Rechten (applikationsspezifische Benutzerverwaltung)**
- **Datensicherheit im Internet der Universität**
- **Datenschutzproblematik personenbezogener Daten**
- **Organisatorische Vielfalt, kaum DV-orientierte Geschäftsprozesse**

Fragen

- **Gibt es einen gemeinsamen Satz von Personenattributen für die wichtigsten Anwendungen wie Maildienst, HIS-LSF, Mitarbieterverzeichnisse, Ausleihdienste, Portaldienste etc? (minimal vs. maximal)**
- **Wer ist für die Pflege der Attribute zuständig und verant-wortlich und mit welchem Aufwand? (dezentral vs. zentral)**
- **In welcher technischen Form werden die Personendaten vorgehalten und mit welchen Schnittstellen wird auf das Daten-Repositorium zugegriffen? (Datenbank vs. Verzeichnis, ODBC- vs. LDAP-Schnittstelle)**

Tübinger Lösungsansatz

- **Beschränkung auf einen Minimalsatz von Personen-attributen, im wesentl. sind es Kommunikationsattribute, die von allen elektronischen Diensten gleichermaßen benötigt werden**
- **Verzicht auf die Aufnahme von Rollen. Dieses soll von der Applikation geregelt werden. Ausgenommen sind die vier generischen Rollen, denen die Personen zugeordnet werden: Mitarbeiter, Student, Gast, Alumni**
- **Definition einer verteilten Zuständigkeit auf Attributsbasis**
- **Identitätsverwaltung erfolgt in einer DB, der Zugriff auf die Daten für den Identitätsnachweis nach (gefiltertem) Daten-export in einen LDAP-Server über seine LDAP-Schnittstelle**

Zusammensetzung des KommDB-AK

- **ZDV (Moderation, technische Realisierung und Betrieb, ZDV-Applikationen)**
- **ZV, Personalabteilung**
- **ZV, Studentenabteilung**
- **ZV, Datenschutzbeauftragter**
- **ZV, Rechenzentrum (HIS-Applikationen)**
- **UB, Rechenzentrum (UB-Applikationen)**
- **regelmäßige Berichterstattung der Aktivitäten in einem Kontrollausschuss aus Kanzler, Prorektor, DM und ZDV**

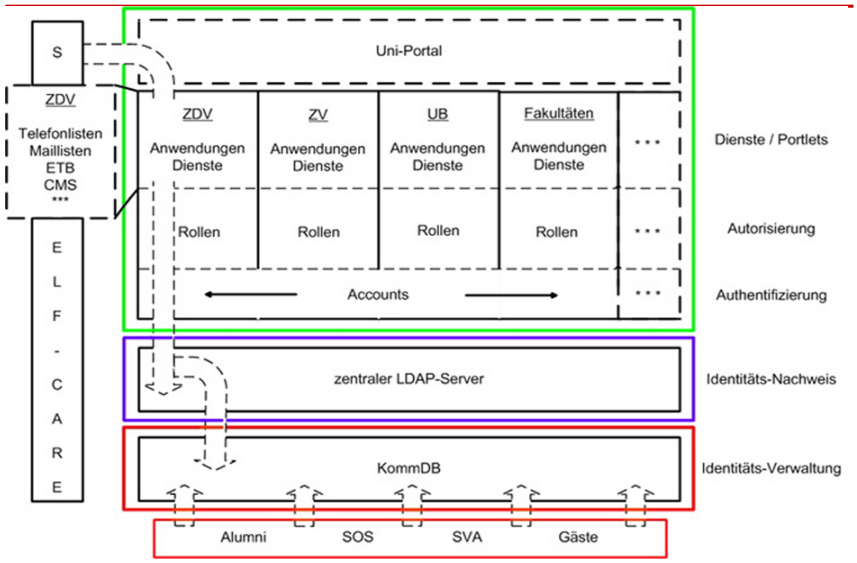
ZENDAS

Eine KommDB an sich, d.h. ohne Applikation, in der gesagt wird, was mit den Personendaten passieren soll, ist datenschutzrechtlich nicht begründbar.
Ergo:
Die Nutzung einer KommDB lässt sich nur durch entsprechende Applikationen recht-fertigen. Damit muss die KommDB in ein Gesamtbild gesetzt werden.

Die Tübinger Sicht

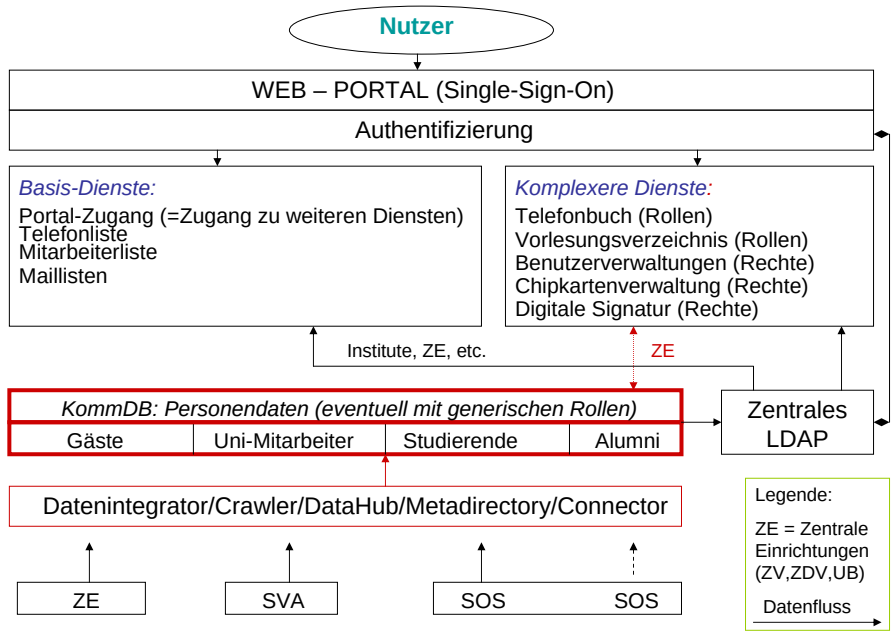
• geht von dem Nutzer aus, der die elektronischen Dienste über ein Universitäts-Portal angeboten bekommen soll
• verlangt für den Zutritt zum Portal eine Authentifizierung
• strebt in der Authentisierung eine Single-Sign-On Lösung für die im Portal angebotenen Dienste an
• und führt daher auf eine Schichtenlösung der folgenden Struktur

KommDB



Dietmar Kaletta, Tü 28.06.05

Nutzersicht auf die ihm angebotenen Dienste



KommDB

Ausarbeitung "Attribute" der Arbeitsgruppe "Kommunikations-Datenbank (KommDB)"
(Bearbeitet von der KommDB-AG am 19. Mai 2005: Attribute in den Abschnitten 0 und 1)

KommDB-Attribut	sichtbar (intern)	Gruppe[1]	Datenzuständigkeit[2] (Neueintrag, Änderung, Löschung)												
			Dez.I (RA)	Dez. I (SOS)	Dez. II (SVA)	Dez. VI (DM)	Controlling	ZDV	Berechtigte	Alumnat	ZIT	Selbst	PKI	TMV (einmalig)	System/ autom. Quellen
0. Technische Attribute															
PIN		Alle													autom. generiert, ext. DB-Schlüssel
Fremdschlüssel		Alle													
Kostenstellenschlüssel[3]		M, G					X (M)		X (G)						
Welt-Sichtbarkeit (gen.)[5]		M	X (M)												
Welt-Sichtbarkeit (spez.)		Alle										X			
1. Allgemeine Personenattribute															
Name, Vorname (n)	x	Alle		X (S)	X (M)				X (G)	X (A)	X (K)				
Geschlecht	x	Alle		X (S)	X (M)				X (G)	X (A)	X (K)				
Namenszusatz[6] (n)	x	Alle			X (M)				X (G)	X (A)	X (K)				
akad. Titel (n)	x	Alle		X (S)	X (M)				X (G)	X (A)	X (K)			X	
Geburtsdatum		Alle		X (S)	X (M)				X (G)	X (A)	X (K)				
Nationalität (n)		M, S, A		X (S)	X (M)					X (A)					
Kontaktanschrift		S, G, A, K		X (S)					X (G)	X (A)	X (K)				
2. Kommunikationsattribute															
E-Mail-Adresse[4] (offiz.)	x	Alle			[X (M)]			X			X (K)				
Portal-LoginID		Alle						X							
Zertifikat (offiz.)	x	M, S											X		

2005-05-19, ZDV 1 / 3

Dietmar Kaletta, Tü 28.06.05