

Verzeichnisdienste
LDAP
Rollenmodelle

Gliederung

- Was ist ein Verzeichnisdienst?
- Schema des HIS-LDAP-Servers
- Verwaltung von Rollen

Gliederung

- Was ist ein Verzeichnisdienst?
- Schema des HIS-LDAP-Servers
- Verwaltung von Rollen

Was ist ein Verzeichnisdienst?

Ein Verzeichnisdienst ist ein elektronischer Dienst, in welchem Daten in einer hierarchischen Struktur zur Verfügung gestellt werden

Einige typische Eigenschaften eines Verzeichnisdienstes

- Häufig lesender Zugriff
- Selten schreibender Zugriff
- In einer hierarchischen Struktur aufgebaut
- Möglichkeit verteilter Datenhaltung in dem Teilbäume auf verschiedene Hosts verteilt werden

Sinnvolle Anwendungen von Verzeichnisdiensten

- Domain Name System (DNS)
- Abbildung von Organisationen

Warum verwendet man keine relationalen Datenbanken?

Relationale Datenbanken haben gegenüber Verzeichnissen zwar Vorteile (Transaktionsfähigkeit, referenzielle Integrität), verzeichnisgestützte Systeme können aber die eben aufgeführten Eigenschaften besser ausnutzen.

Warum verwendet man keine relationalen Datenbanken? (Wiederholung der Eigenschaften)

- Häufig lesender Zugriff
- Selten schreibender Zugriff
- In einer baumartigen Hierarchie aufgebaut
- Möglichkeit verteilter Datenhaltung indem Teilbäume auf verschiedene Hosts verteilt werden

Geschichte

- In den 80er Jahren existierten viele unterschiedliche Systemarchitekturen nebeneinander
- Es entstand der Wunsch des Datenaustausches zwischen den Systemen

Geschichte

- Um nicht zu viele unterschiedliche Schnittstellen zwischen den Systemen entwickeln zu müssen, wird ein zentrales Kommunikationsprotokoll entworfen
- In diesem Rahmen entstehen eine Reihe von X-Standards (die X.500-Serie)

Geschichte

- Die X.500-Standards definieren, wie Verzeichnisdaten zur Verfügung gestellt und abgerufen werden:
 - *Verschlüsselung*
 - *Authentifizierung*
 - *Replikation*
 - *Verwaltung*

Geschichte

- X.500 hat das Problem, dass es auf dem komplizierten 7-schichtigen OSI-Modell basiert.
- In der Praxis setzt sich TCP/IP durch.
- Als Ausweg aus diesem Dilemma wurde im Juli 1993 das **L**ightweight **D**irectory **A**ccess **P**rotocol spezifiziert.

Geschichte

- LDAP sollte eine wesentliche Teilmenge des Protokolls von X.500 implementieren und auf der TCP-Schicht basieren.
- Seit August 1998 wird das OpenLDAP-Projekt von der OpenLDAP Foundation (<http://www.openldap.org>) koordiniert.

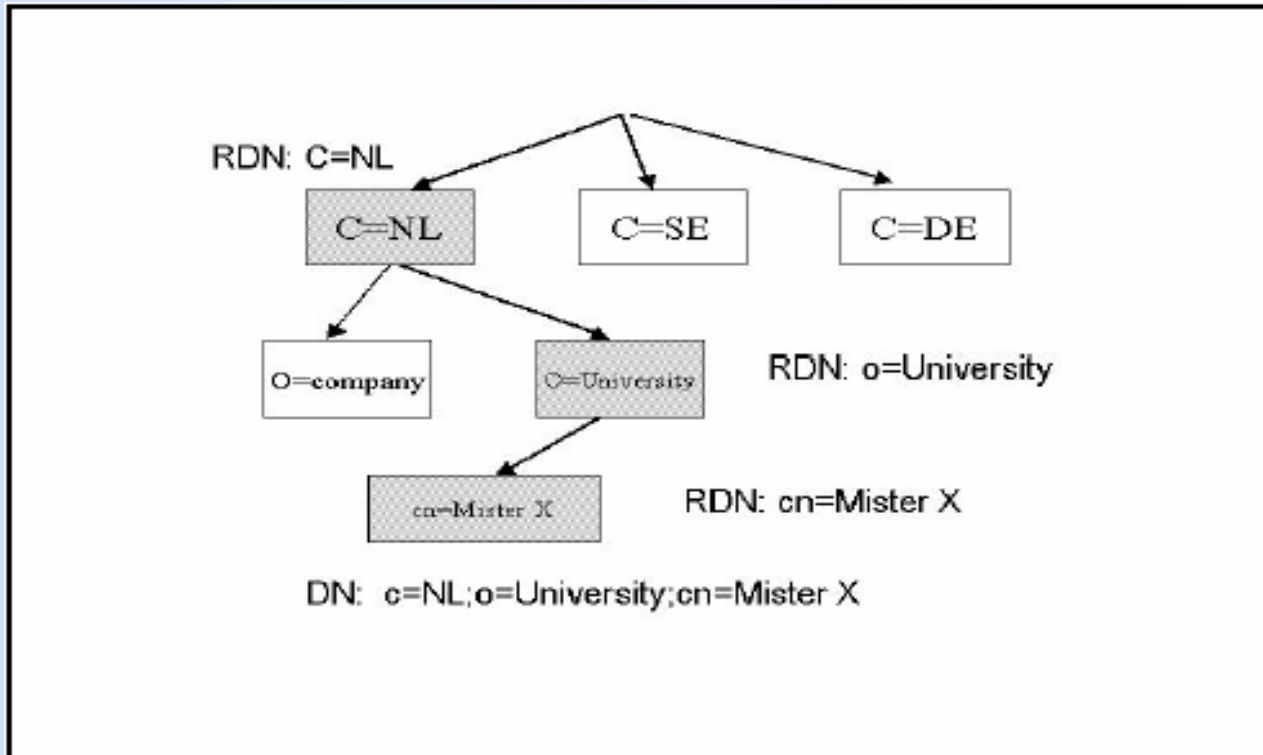
Geschichte

- Mittlerweile steht eine vollständig kompatible LDAP-Implementierung im Source Code zur Verfügung

Datenmodell

- Die Welt der LDAP-Protokolle besteht aus Objekten.
- Wesentliche OO-Konzepte wie Objekte, Klassen, Vererbung, Polymorphie finden Verwendung in der LDAP-Welt.

Datenmodell



Datenmodell

- Es können beliebige Daten gespeichert werden
- Insbesondere ist es möglich, Zeiger zu verwenden, die auf Bereiche innerhalb des Verzeichnisbaumes verweisen

Datenmodell

- Eine Ansammlung von Objektklassen, Attributen, Attributsyntaxen und Vergleichsregeln wird Schema genannt

Datenmodell

- Es existieren Standards für Personen, Organisationen,
- Darüber hinaus können eigene Schemata definiert werden.

Anwendungsmöglichkeiten von LDAP

- Kontaktdateninformationsdienste
- Authentifikationsdienste
- Metadirectory
- Zertifikatserver für PKI

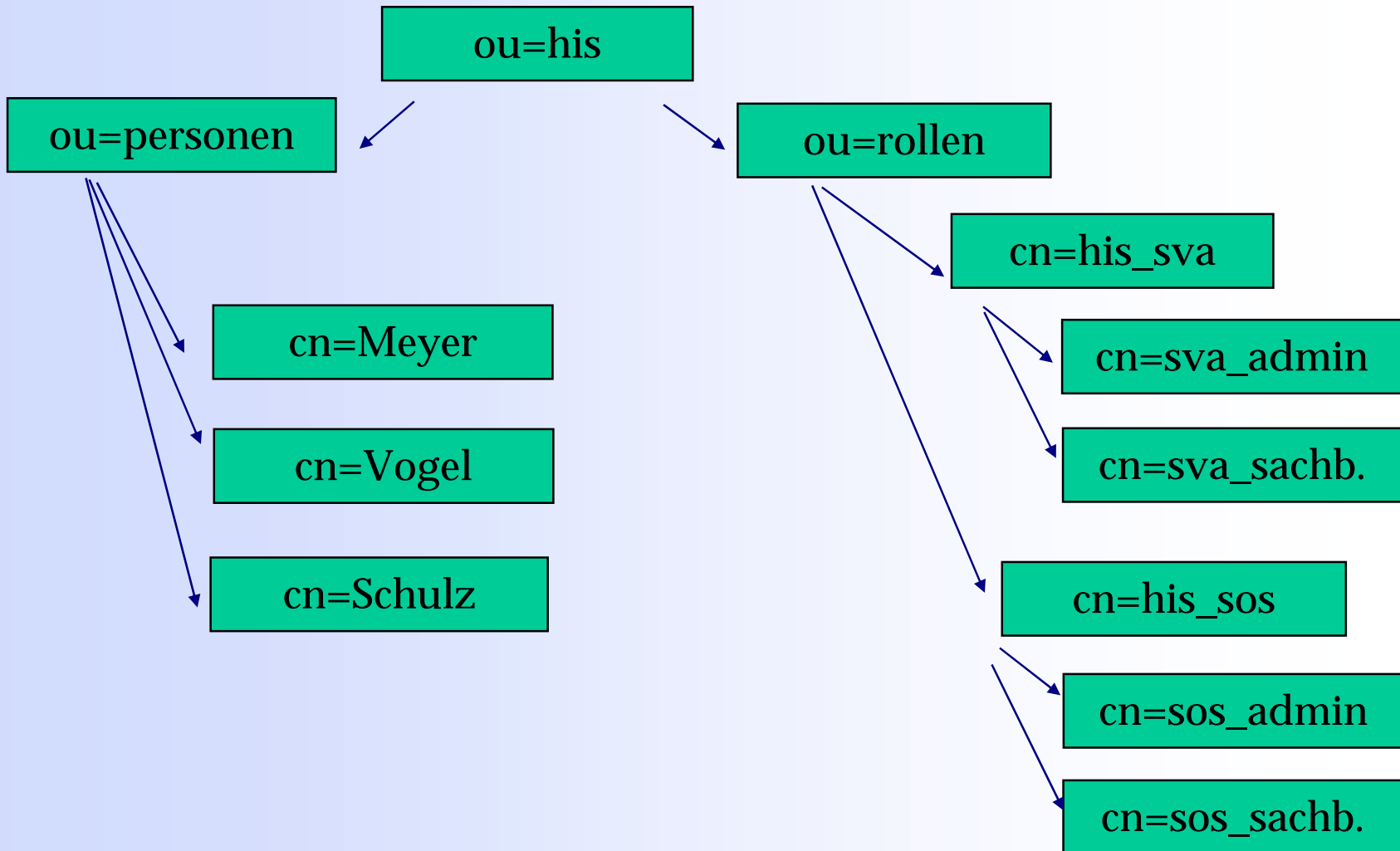
Gliederung

- Was ist ein Verzeichnisdienst?
- Schema des HIS-LDAP-Servers
- Verwaltung von Rollen

- Der HIS-Verzeichnisdienst stellt Daten aus zwei Teilbäumen zur Verfügung

- Im Teilbaum **ou=personen** werden Daten von Hochschulangehörigen, also Mitarbeitern, Studierenden, Gästen und Alumni sowie Emeritis abgelegt.

Im Teilbaum **ou=rollen** werden die Rollen abgelegt. In diesem Teilbaum können weitere Unterteilungen vorgenommen werden. So ist es zum Beispiel möglich, Rollen für Bedienstete und Rollen für Mitarbeiter zu pflegen.



Zum Abbilden der Personenobjekte wurden die folgenden Standard-Schemaklassen verwendet:

person

inetOrgPerson

organizationalPerson

eduPerson

naturalPerson

Die folgenden Merkmale wurden nicht von den Standard-Schemata abgedeckt:

Geburtsdatum *Akademischer Titel*

Geburtsort *Anrede*

Staatsangehörigkeit *Wohnsitz*

Geschlecht *Gebäude*

Land in Adressenangaben

Adelstitel und sonstige Namenszusätze

Adressenzusatz

Kostenstelle

Einstellungsdatum

Matrikelnummer

Immatrikulationsdatum

Exmatrikulationsdatum

Studiengang

Studienfach/

Fachsemester

*Datum der Beendigung des Mitarbeiter-
verhältnisses*

Jede Person soll über eine ID als Identität gekennzeichnet werden. Zu diesem Zweck enthält das HIS-Schema das Merkmal

HIS-UUID

Zum Abbilden der Rollenobjekte wurde die Standard-Schemaklasse *organizationalRole* verwendet.

Gliederung

- Was ist ein Verzeichnisdienst?
- Schema des HIS-LDAP-Servers
- **Verwaltung von Rollen**

Beispiele für Rollennamen

- SVA_Sachbearbeiter
- SVA_Personen_A_M
- SOS_Sachbearbeiter

Beispiele für Rollennamen

- SOS_Admin
- SVA_Admin

- HIS_Studierender

- Die Namen der Rollen werden unter Verwendung eines Administrationswerkzeugs in das Verzeichnis eingetragen.
- Es gibt Rollen, die zukünftig von den HIS-Modulen direkt eingetragen werden.

1. Die „Interpretation“ der Rolle wird von dem jeweiligen HIS-Modul vorgenommen.
2. Im Rahmen der „Interpretation“ wird der Rollenbegriff in Datenbankrechte, Tabellenrechte, Berechtigungen, Menüeinträge usw. „übersetzt“
3. Die Namen der Rollen, die SVA auswertet, müssen mit „sva_“ beginnen!

1. Das HIS-Modul interpretiert die Rolle direkt beim Anmelden.
2. Bei jeder Anmeldung mit SVA wird geprüft, ob die Daten zwischen LDAP und Datenbank synchron sind. Wenn nicht, kann keine Anmeldung erfolgen.
3. Alle Änderungen an den Personen werden künftig nur im LDAP gepflegt und müssen anschließend mit der sva-Datenbank synchronisiert werden. Davon ausgenommen sind die konkreten Rechte der Rollen oder Personen.

Eine Authentifizierung gegen das LDAP wird nicht von SVA durchgeführt.

- PostgreSQL und INFORMIX (ab 9.40) Datenbanken können aber so eingestellt werden, dass sie zur Authentifizierung LDAP benutzen.

Voraussetzungen

- SVA 8.0
- Unterstützung für PostgreSQL und Informix ab 9.x.
- Vorhandenes Verzeichnis muss um das HIS-PERSON Schema erweitert werden.
- Angepasster LDAP-Browser zur Pflege der Attribute wird benötigt.

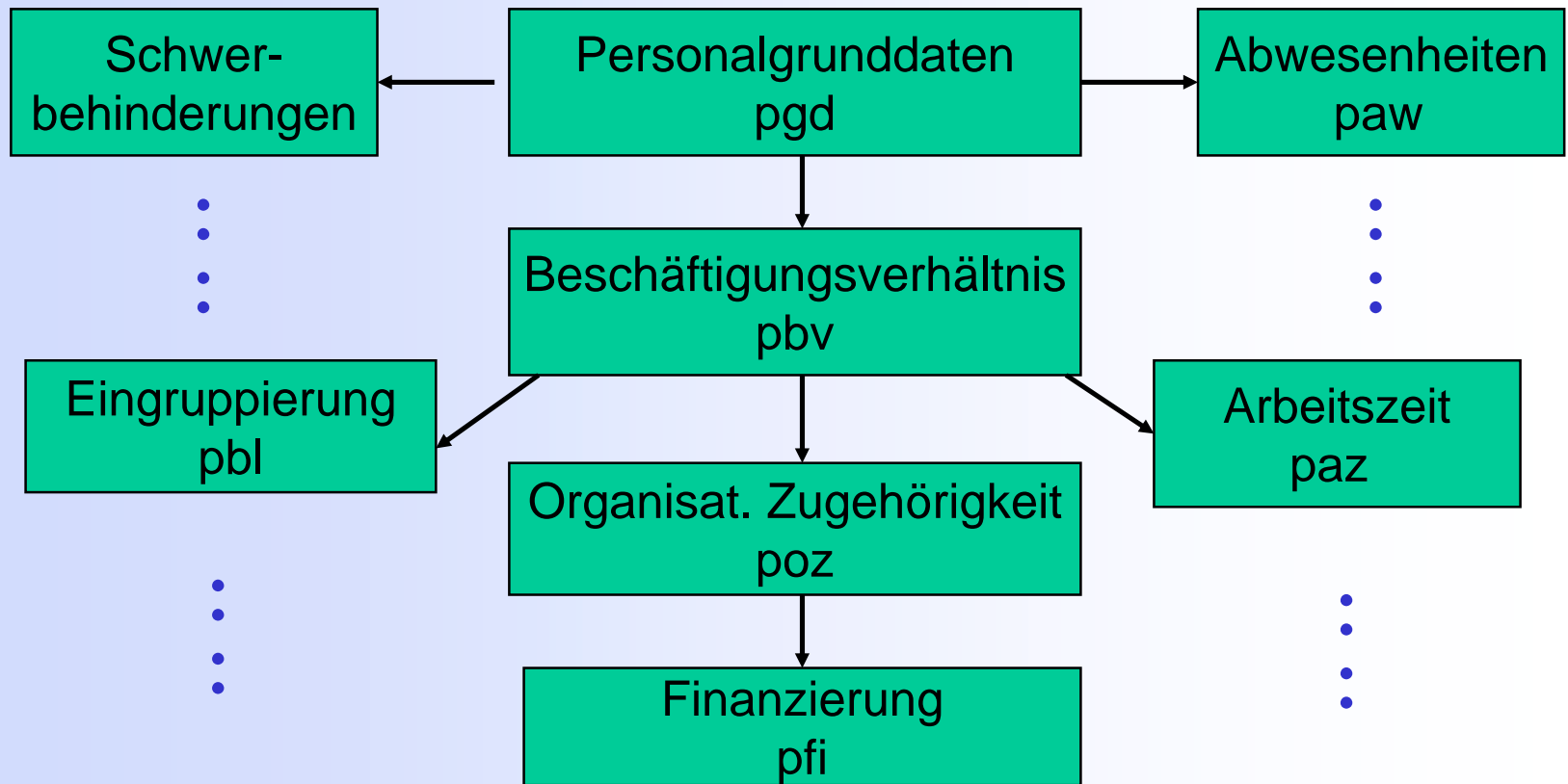
Gliederung

- Was ist ein Verzeichnisdienst?
- Schema des HIS-LDAP-Servers
- Verwaltung von Rollen
- Stagingtabellen

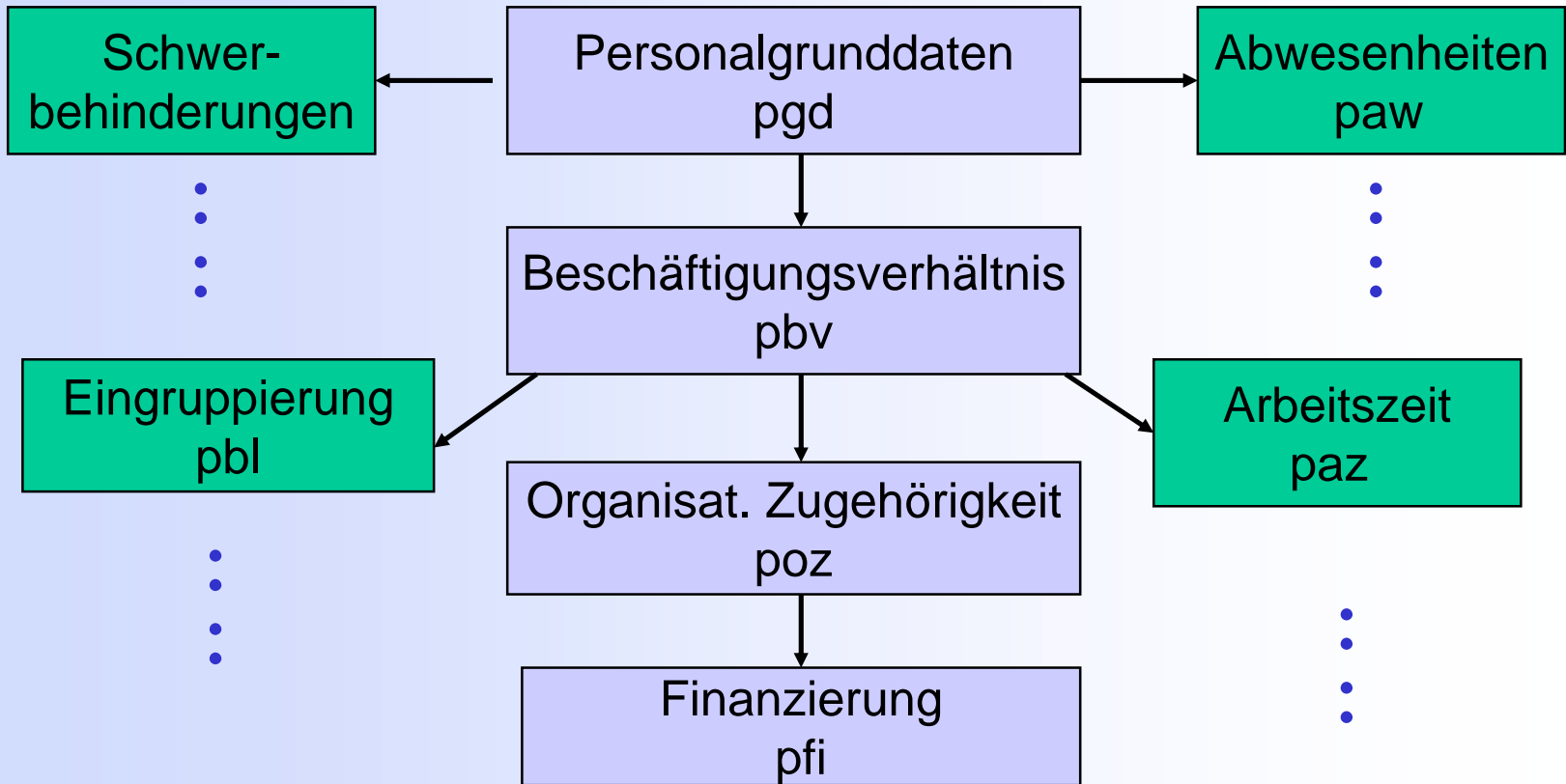
Übersicht

- Welche Daten liefern SVA und SOS?
- Wie sind die Staging-Tabellen aufgebaut?
- Wie werden die Staging-Tabellen beliefert?
- Wie wird der Datenschutz sichergestellt?
- Ausblick

Auszug aus dem SVA-Datenmodell



Auszug aus dem SVA-Datenmodell



Welche Daten liefern SOS und SVA?

Daten zur Person

Nachname

Vornamen

Namenbestandteile

Personalnummer (SVA)

Matrikelnummer (SOS)

Geburtsname

Geburtsname

Geburtsort

Akademischer Grad

Staatsangehörigkeit

Geschlecht

Immatrikulationsdatum (SOS)

Welche Daten liefern SOS und SVA?

Daten zum Studiengang (SOS)

Matrikelnummer
Studiengangnummer
Studiengang
Fachsemester

Beginn des
Studienganges
Ende des
Studienganges

Welche Daten liefern SOS und SVA?

Daten zum Beschäftigungsverhältnis (SVA)

Personalnummer
Beschäftigungs-
verhältnisnummer
Beschäftigungsstelle

Beschäftigungs-
verhältnisbeginn
Beschäftigungs-
verhältnisende
Kostenstellencode
Kostenstellen-
beschreibung

Aufbau der Staging-Tabellen (meta_person)

Spaltenname	Typ	Beschreibung	Beispiel	aus SOS	aus SVA
ID	Sequence	PK	1	X	X
Surname	char(64)	Nachname	Bach	X	X
GivenName	char(32)	Vorname	Otto	X	X
NameExtension	char(32)	Namenszusätze	Freiherr von dem	X	X
StudentNumber	char(10)	Matrikelnummer	543210	X	
employeeNumber	char(10)	Interne Personalnummer	98765		X
DateOfBirth	Date	Geburtsdatum	05.05.1955	X	X
MaidenName	char(128)	Geburtsname		X	X

Aufbau der Staging-Tabellen (meta_person)

Spaltenname	Typ	Beschreibung	Beispiel	aus SOS	aus SVA
BirthPlace	char(128)	Geburtsort	Stieglitz	X	X
AcademicTitle	char(128)	Akademischer Titel	Prof. Dr. Dr.	X	X
Citizenship	char(128)	Staatsangehörigkeit	Frankreich	X	X
Sex	char(1)	Geschlecht	M	X	X
DateOfMatriculation	Date	Einschreibedatum	01.10.2003	X	
Address	Char(64)	Strasse und Hausnummer	Hauptstr. 27b	X	X
AddressExtension	Char(64)	Adresszusatz	Bei Fr. Müller	X	

Aufbau der Staging-Tabellen (meta_person)

Spaltenname	Typ	Beschreibung	Beispiel	aus SOS	aus SVA
PostalCode	Char(15)	Postleitzahl	99958	X	X
City	Char(64)	Stadt	Obertönna	X	X
Country	Char(64)	Land	Deutschland	X	X
OperationType	char(3)	Art der Operation	MOD	X	X
Flag	char(1)	Bearbeitungskennzeichen	1	X	X
CreatedTimestamp	Timestamp	Datensatzerstellung	2003-11-11 15:23	X	X
ProcessedTimestamp	Timestamp	Datensatzverarbeitung	2003-11-11 15:30		

Aufbau der Staging-Tabellen (meta_rolle)

Spaltenname	Typ	Beschreibung	Beispiel	aus SOS	aus SVA
ID	Sequence	PK, wird nicht im Rollenobjekt gespeichert	1	X	X
StudentNumber	char(10)	Matrikelnummer, Relation zu Person, wird nicht im Rollenobjekt gespeichert	543210	X	
employeeNumber	char(10)	Personalnummer, Relation zu Person, wird nicht im Rollenobjekt gespeichert	98765		X
CourseNumber	char(2)	Lfd. Studiengangnummer, wird für die Bildung der Assoziation verwendet	02	X	
JobNumber	char(8)	Beschäftigungsstellen-ID (ID der Beschäftigungsstellenzuordnung) , wird für die Bildung der Assoziation verwendet	87623542		X

Aufbau der Staging-Tabellen (meta_rolle)

Spaltenname	Typ	Beschreibung	Beispiel	aus SOS	aus SVA
CourseOfStudy	char(128)	Studiengang	Informatik	X	
Position	char(128)	Beschäftigungsstelle	Baustatik		X
JobType	char(64)	Beschäftigungs- verhältnisart lt. HIS- System-Schlüssel	Studentische Hilfskraft		X
SemesterOfCourseStudy	char(4)	Fachsemester	7	X	
StartDate	Date	Gültig ab	01.10.2003	X	X
ExpiryDate	Date	Gültig bis	30.03.2004	X	X
CostAllocation	char(128)	Kostenstellencode	02034711		X

Aufbau der Staging-Tabellen (meta_rolle)

Spaltenname	Typ	Beschreibung	Beispiel	aus SOS	aus SVA
CostAllocationText	Char(256)	Kostenstellenbeschreibung	DFG-Sachb. 313		X
OperationType	char(3)	Art der Operation	MOD	X	X
Flag	char(1)	Bearbeitungskennzeichen	1	X	X
CreatedTimestamp	Times- tamp	Datensatzerstellung	2003-11-11 15:23	X	X
ProcessedTimestamp	Times- tamp	Datensatzverarbeitung	2003-11-11 15:30		

Aufbau der Staging-Tabellen

- Für jedes Merkmal befindet sich ein Flag in den Staging-Tabellen.

- Flag = 0 => keine Änderung
- Flag = 1 => Änderung

Aufbau der Staging-Tabellen

- Für jeden Datensatz in den Staging-Tabellen wird die Art der Operation hinterlegt
 - add
 - mod
 - del

Belieferung der Staging-Tabellen

Ereignisse in SOS bzw. SVA

- Anlegen eines Datensatzes
- Ändern eines Datensatzes
- Löschen eines Datensatzes

Belieferung der Staging-Tabellen

Anlegen eines Datensatzes

Unterschiedliche Tabellen in SVA bzw. SOS erfordern ein unterschiedliches Vorgehen beim Beliefern der Staging-Tabellen.

Belieferung der Staging-Tabellen

Anlegen eines Datensatzes

1. Fall:

Anlegen einer Person bzw. Anlegen eines Beschäftigungsverhältnisses erzeugt immer einen Datensatz in Staging-Tabelle „meta_person“ bzw. „meta_rolle“ mit FLAG = „add“.

Belieferung der Staging-Tabellen

Anlegen eines Datensatzes

2. Fall:

Anlegen von Datensätzen in den SVA-Tabellen „Organisatorische Zugehörigkeit“ bzw. „Finanzierung“ erzeugt gegebenenfalls einen Datensatz in der Staging-Tabelle „meta_rolle“ mit FLAG = „mod“.

Belieferung der Staging-Tabellen

Ändern eines Datensatzes

Das Ändern eines Datensatzes erfordert gegebenenfalls das Anlegen eines Datensatzes in den Staging-Tabellen mit Flag =„mod“.

Belieferung der Staging-Tabellen

Löschen eines Datensatzes

Unterschiedliche Tabellen in SVA bzw. SOS erfordern ein unterschiedliches Vorgehen beim Beliefern der Staging-Tabellen.

Belieferung der Staging-Tabellen

Löschen eines Datensatzes

1. Fall:

Das Löschen einer Person bzw. eines Beschäftigungsverhältnisses erzeugt immer einen Datensatz in der Staging-Tabelle „meta_person“ bzw. „meta_rolle“ mit FLAG = „del“.

Belieferung der Stagingtabellen

Löschen eines Datensatzes

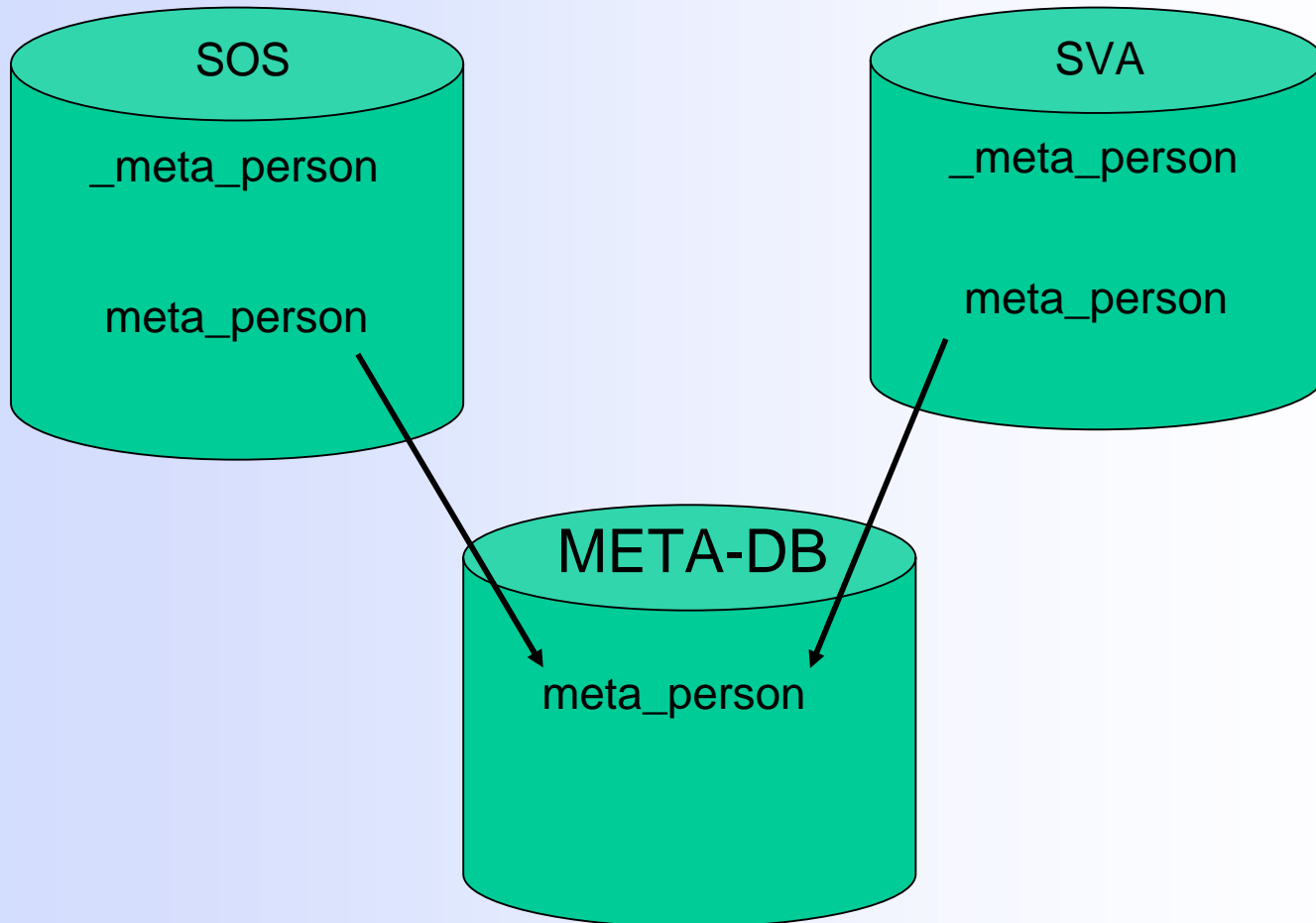
2. Fall:

Das Löschen von Datensätzen in den SVA-Tabellen „Organisatorische Zugehörigkeit“ bzw. „Finanzierung“ erzeugt gegebenenfalls neuen Datensatz in der Staging-Tabelle „meta_rolle“ mit FLAG = „mod“

Datenschutz

- Die Staging-Tabellen werden umbenannt.
- Es werden Synonyme mit gleichen Namen wie die Staging-Tabellen erzeugt.
- Die Synonyme sind Verweise auf gleichnamige Tabellen in einer anderen Datenbank („META-DB“).

Datenschutz



Datenschutz

- Zum Lesen der Staging-Tabellen sind keine Rechte an der SOS bzw. der SVA-Datenbank notwendig.
- Zum Lesen der Staging-Tabellen werden ausschließlich Rechte auf der Datenbank „META-DB“ und Tabellen dieser Datenbank benötigt.