



# Therefore IAM

Identity and Access Management  
@  
Freie Universität Berlin

1637

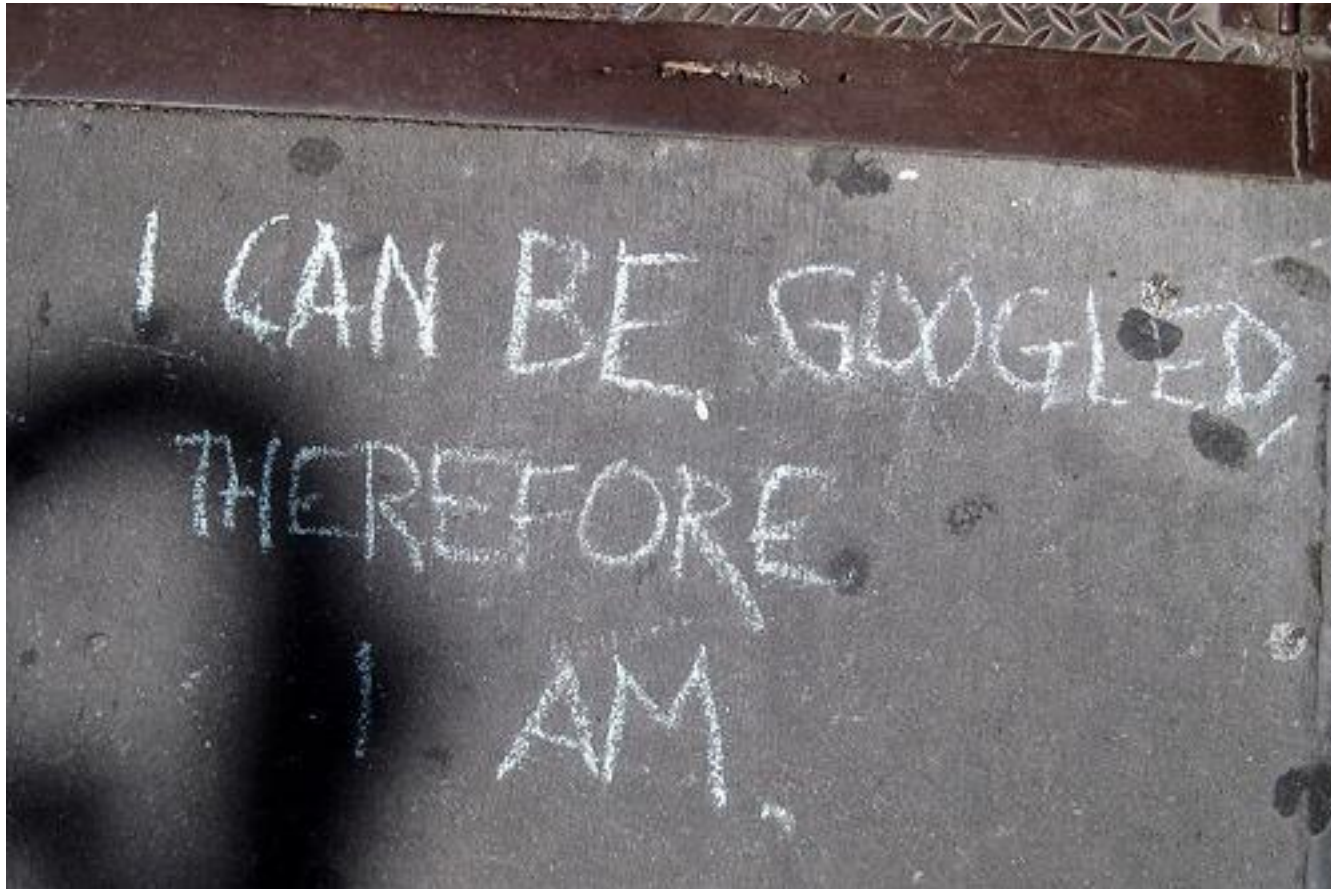


I think, therefore I am.

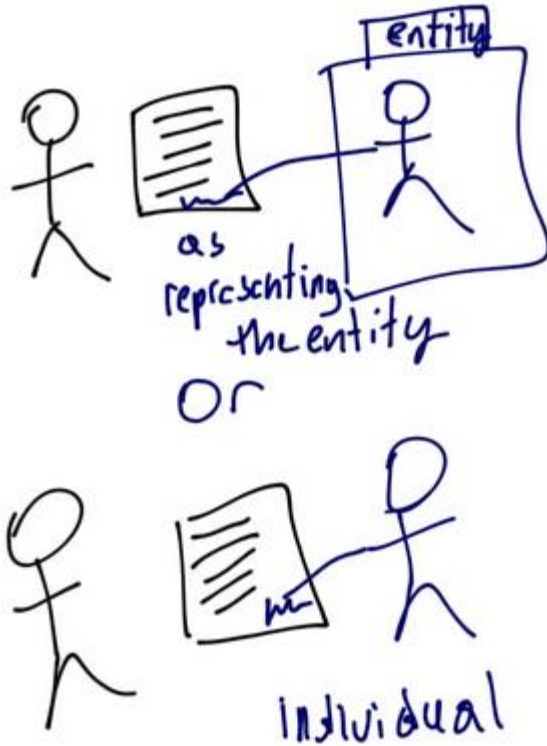
(Rene Descartes)

[izquotes.com](http://izquotes.com)

2014



## More typical in administrative environments:



I have a contract,  
therefore I am



# Proof of Identity

Now after I made sure that I am ...

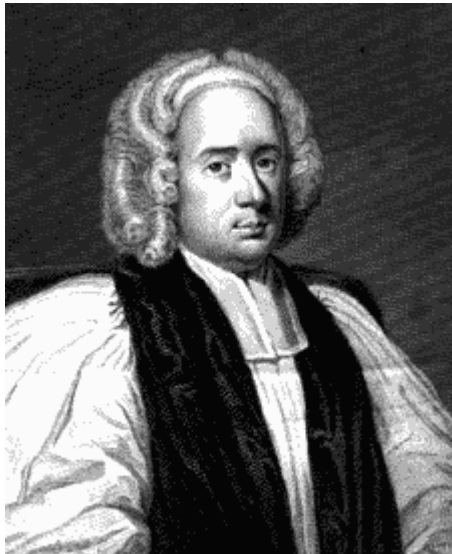


...I need to determine who or what I am.

# Characteristics of Identity

# Theoretical Groundwork

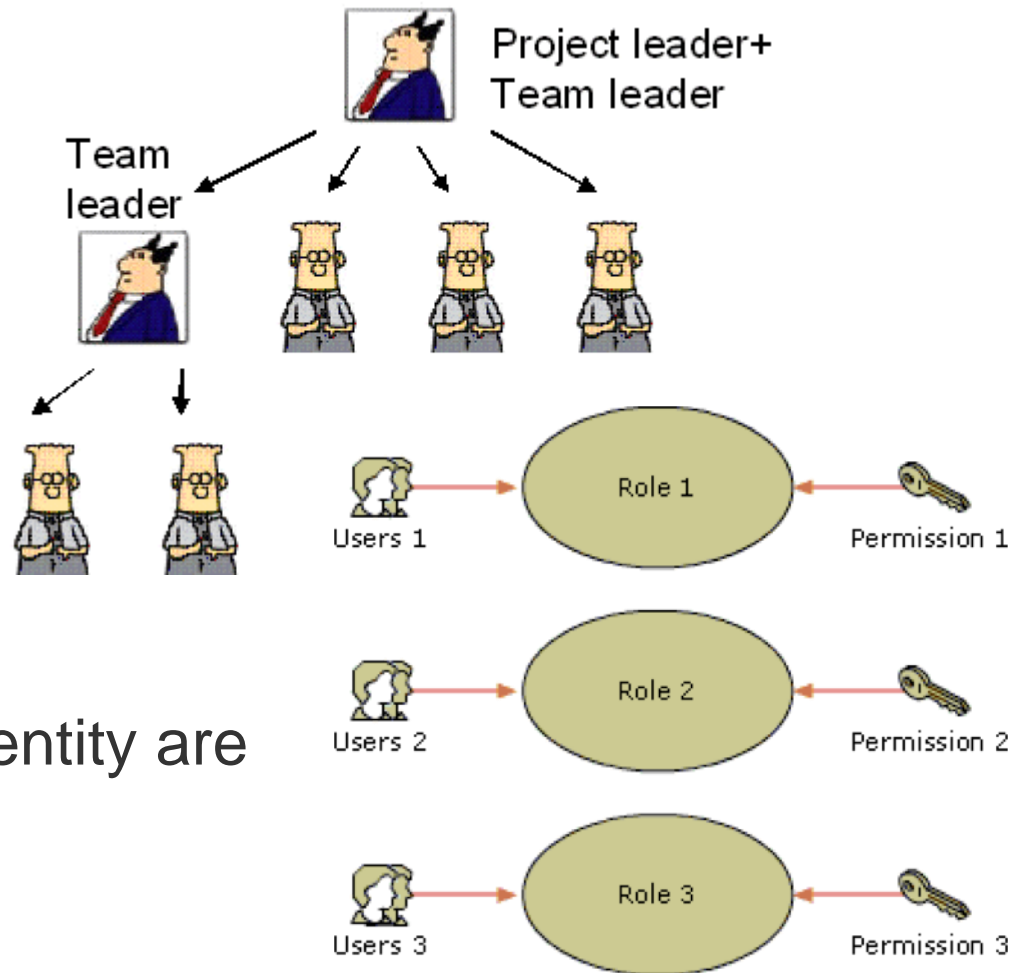
"Every thing is what it is, and not another thing."  
*Fifteen Sermons Preached at the Rolls Chapel (1726)*



**Joseph Butler** (1692–1752)  
English Bishop and Philosopher

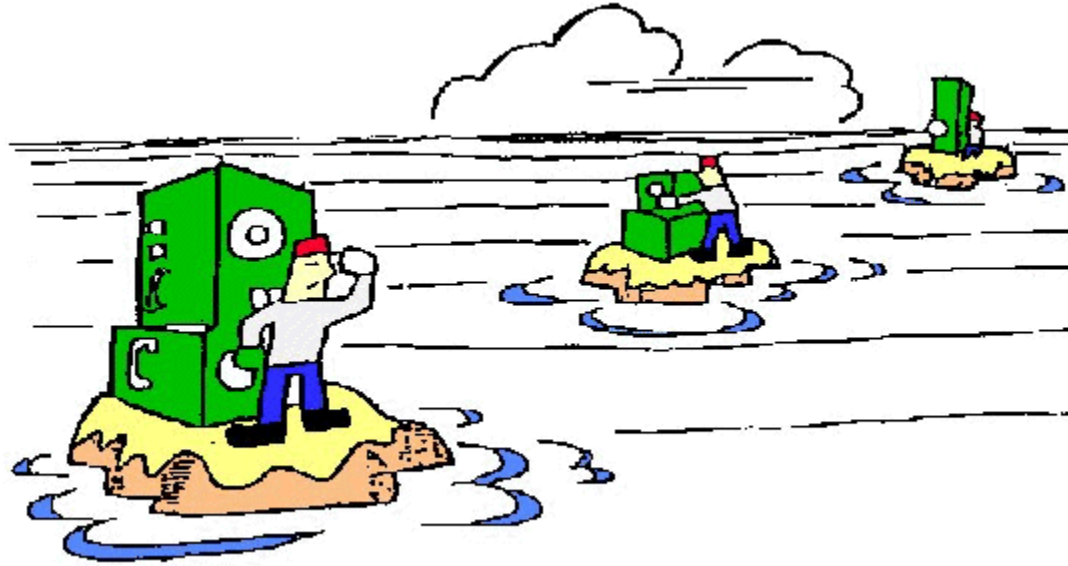


## More typical in administrative environments:

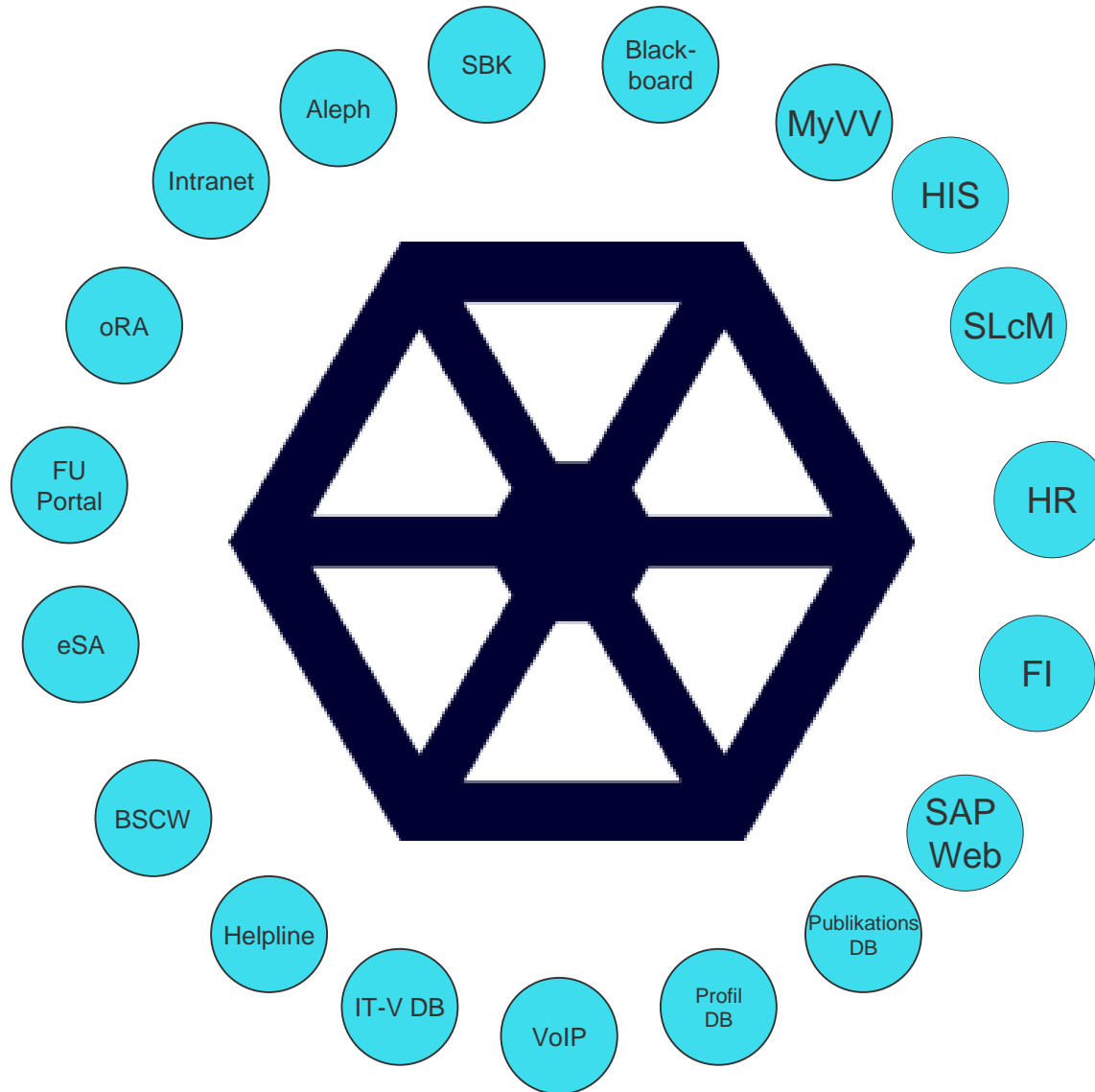


Characteristics of identity are determined by roles

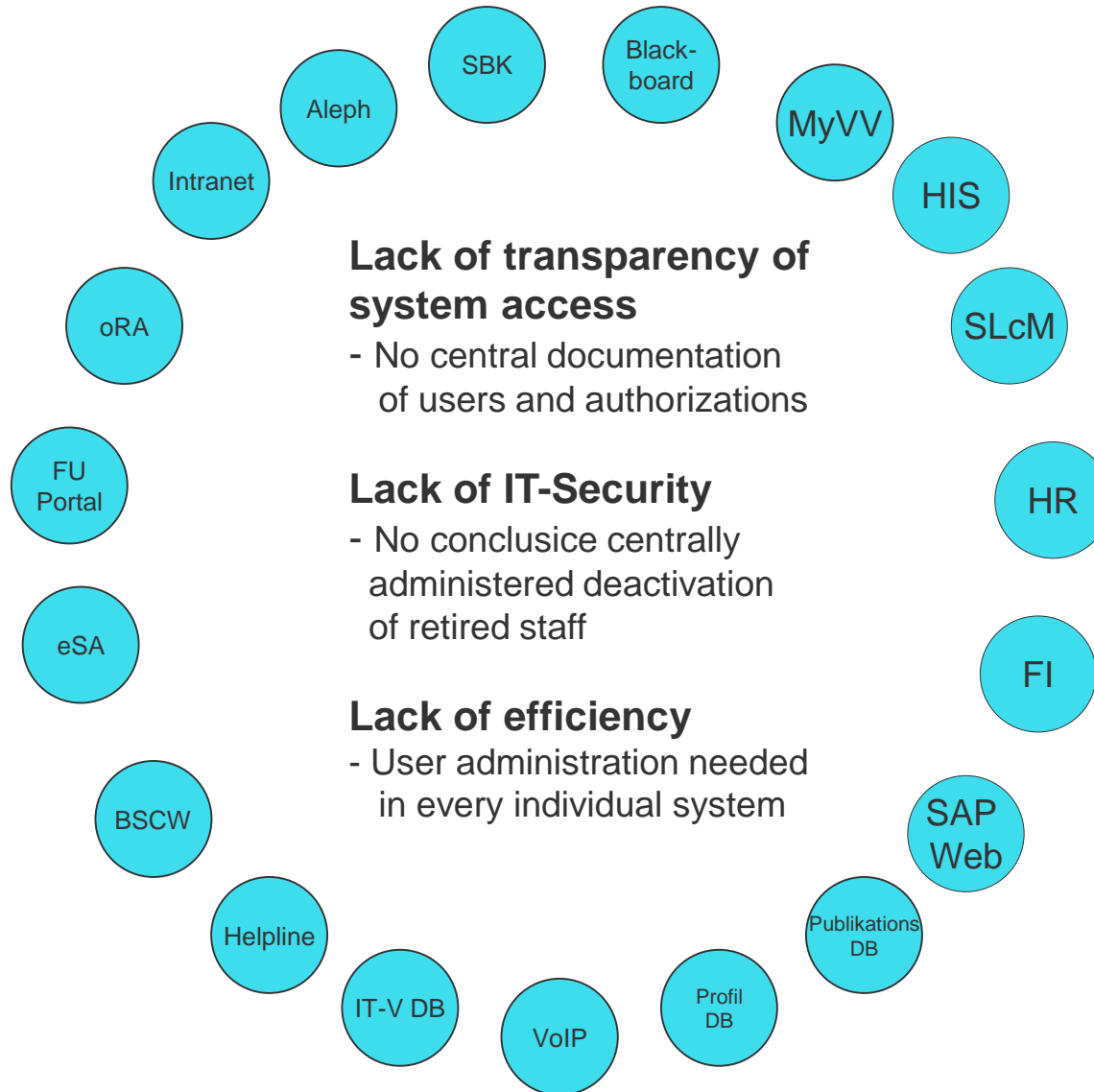
Why would  
anybody in IT  
care?



# The Confederation of independent Systems @ FU Berlin



# Independent Systems @ FUB



# Integration as central task of IT in HER

„For a long time increase of efficiency was attained by casting processes hitherto unsupported by IT into hard- and software based systems without much change to the process in question. Today the focus lies on cross-linking and integration. Thus integrated information management has become the central task for planning and deployment of modern information technology at Universities.“

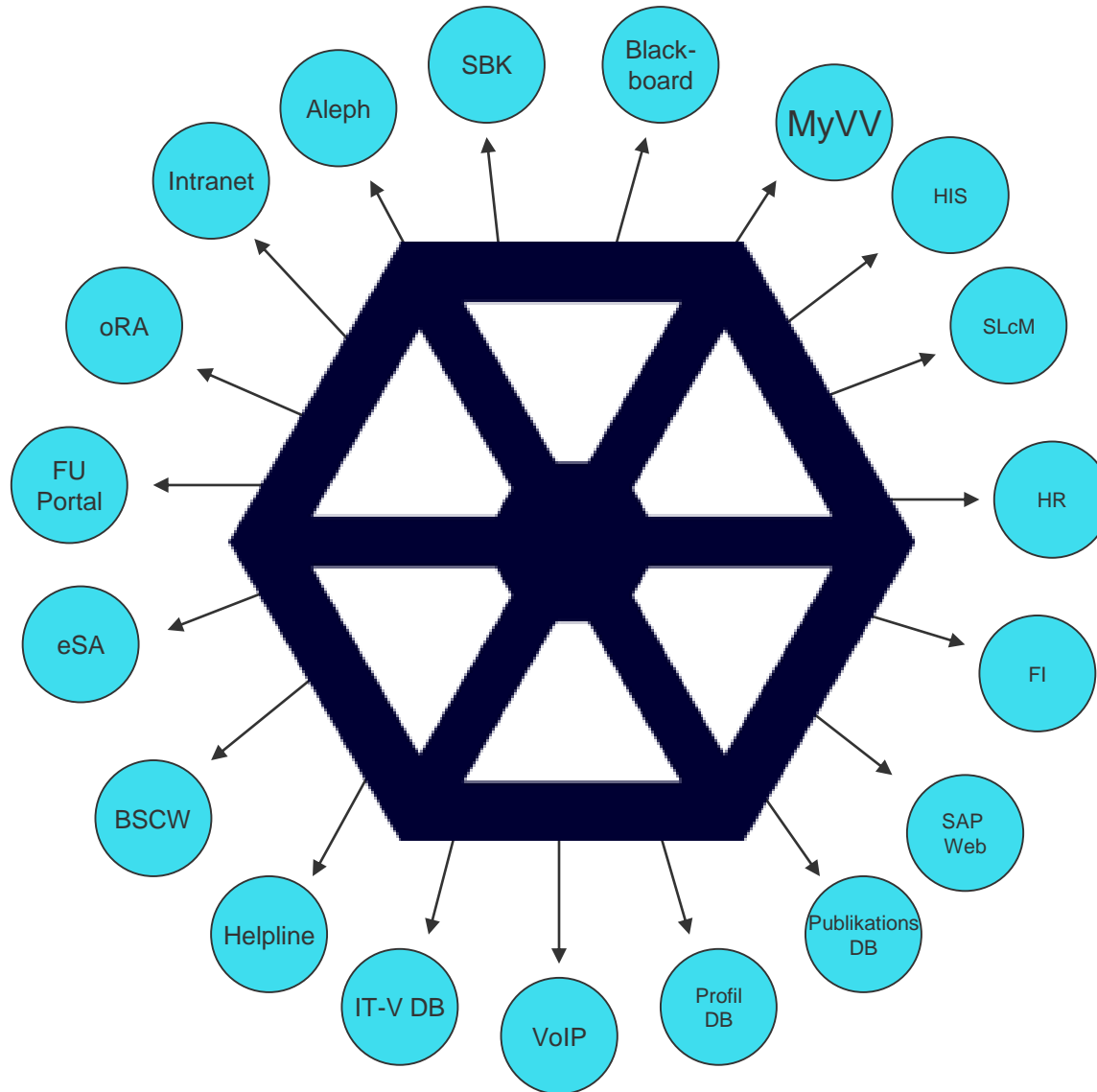
## „Informationsverarbeitung an Hochschulen“

Empfehlungen der Kommission für IT-Infrastruktur für 2011 – 2015

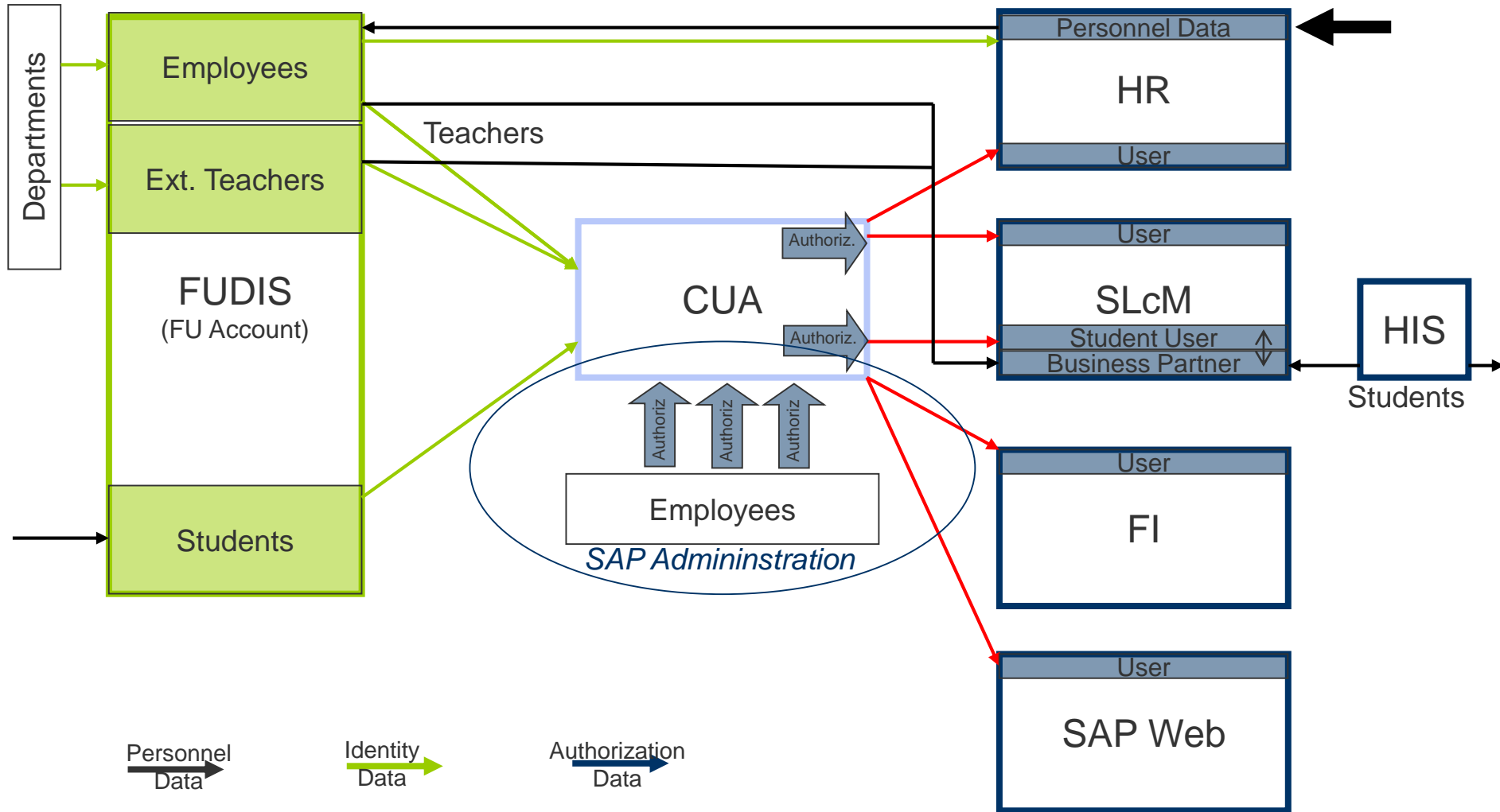
Deutsche Forschungsgemeinschaft DFG

*(my translation, chw)*

# 1st step of Integration: Identity Management

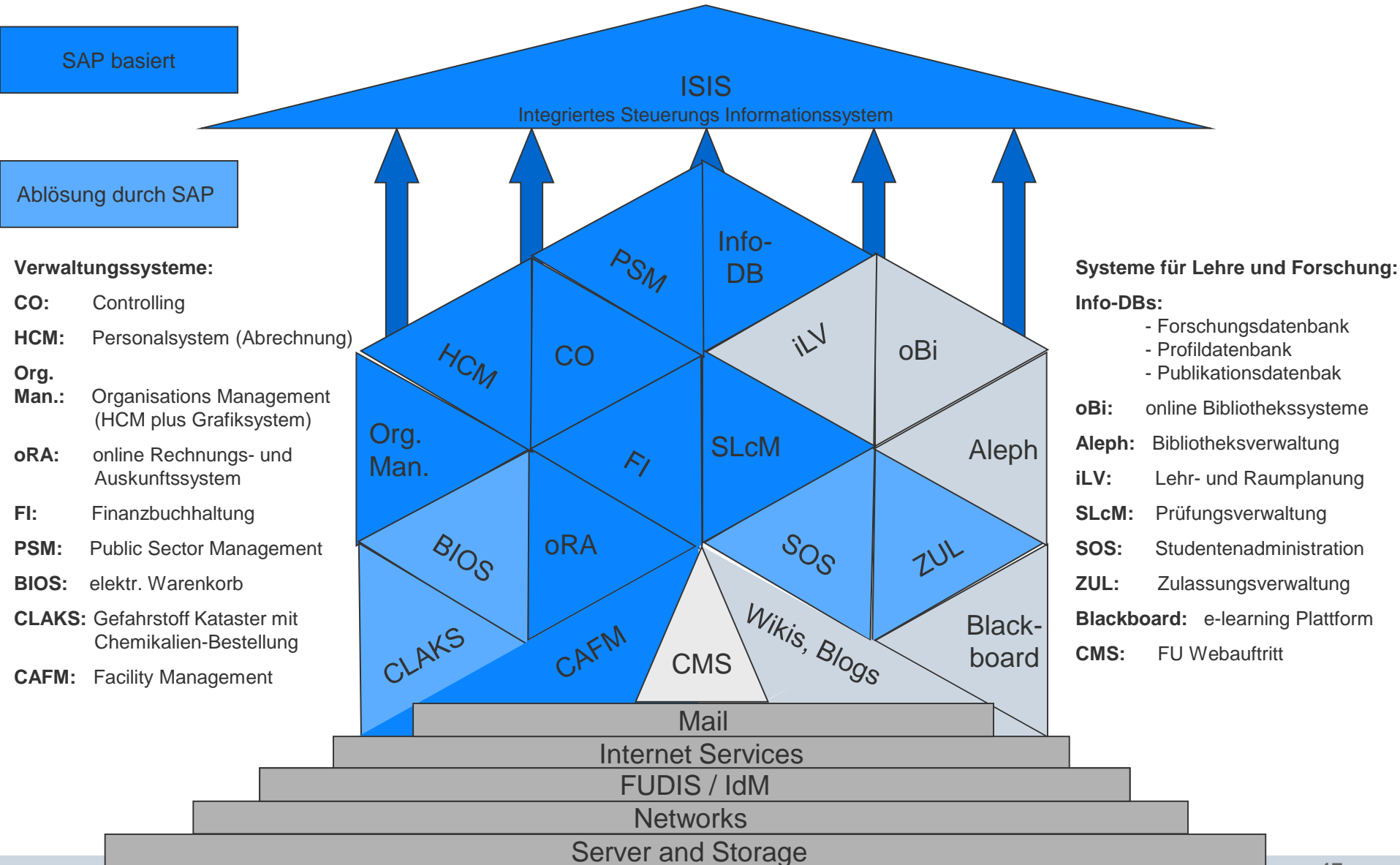


# Onboarding & Authorization (legacy architecture)

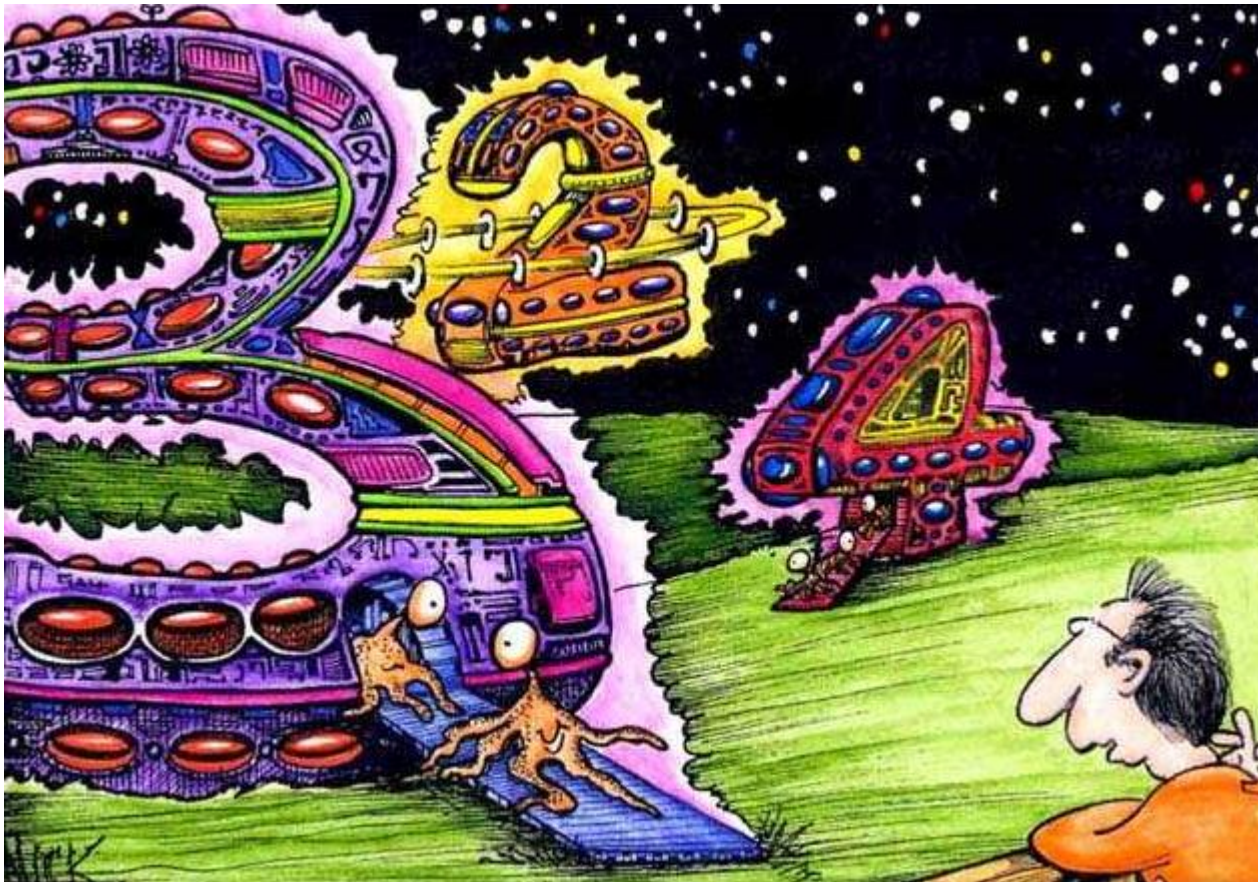




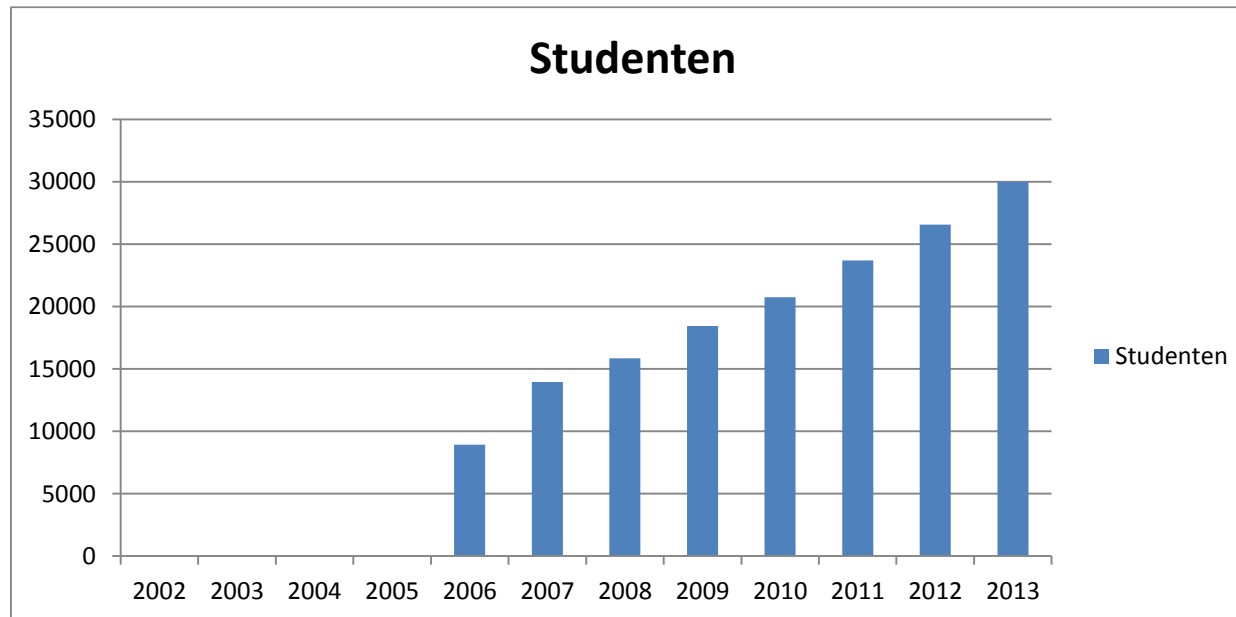
# Extension of SAP Footprint



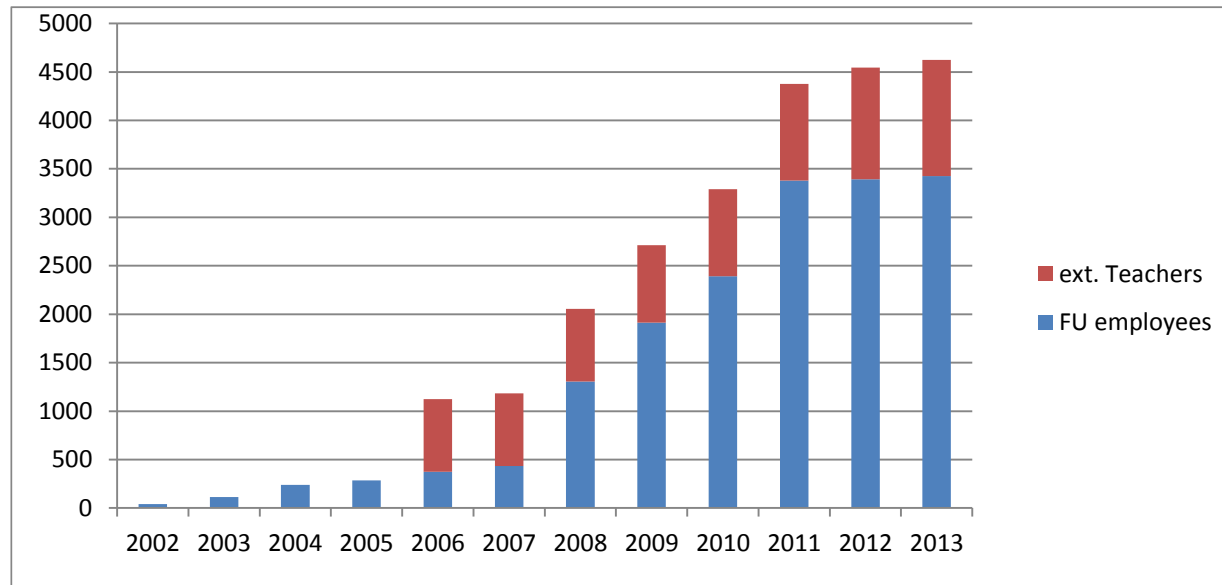
# Consequences of pervasive SAP Use: We never saw users in such numbers



# Increase of Student Users with SLcM Roll Out

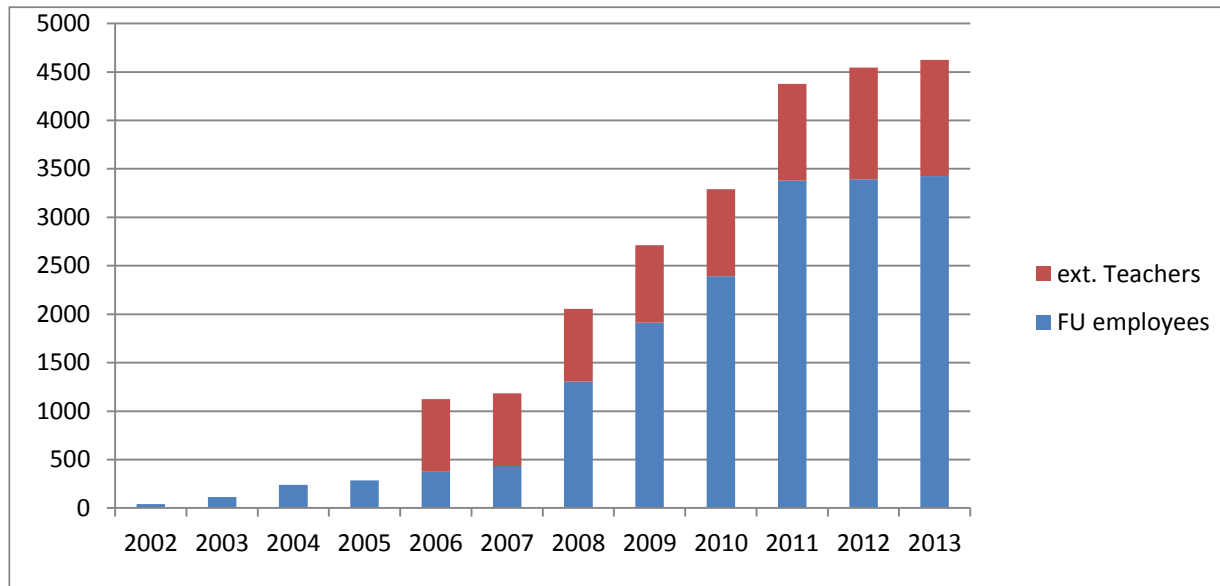


# Increase of staff and teachers as SAP users



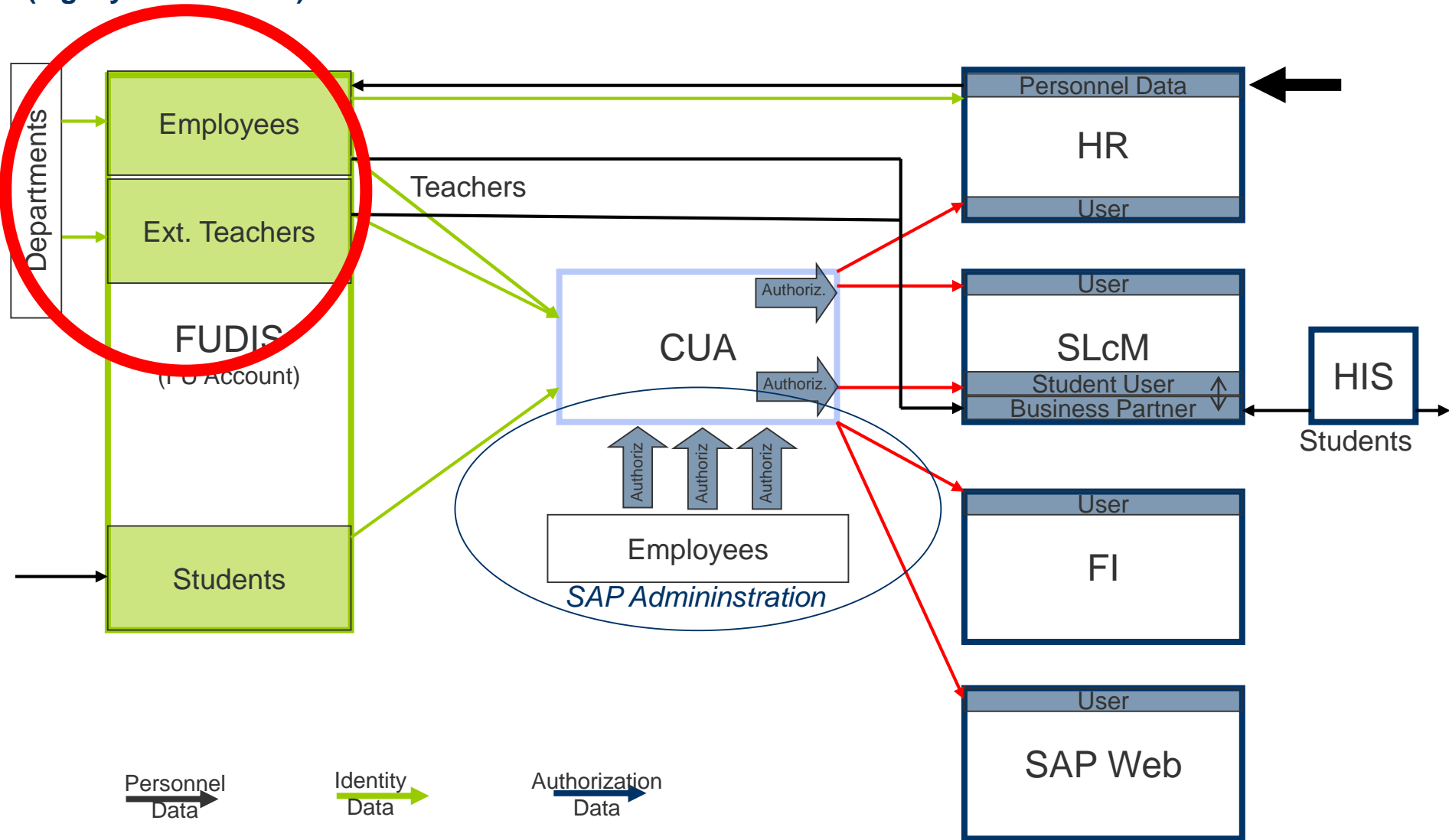
	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
FU employees	40	114	239	287	374	435	1306	1912	2391	3378	3394	3425
ext. Teachers					750	750	750	800	900	1000	1150	1200
Studenten					8936	13966	15848	18443	20747	23707	26568	30000
<b>Total Users</b>	<b>40</b>	<b>114</b>	<b>239</b>	<b>287</b>	<b>10060</b>	<b>15151</b>	<b>17904</b>	<b>21155</b>	<b>24038</b>	<b>28085</b>	<b>31112</b>	<b>34625</b>

# Challenge: External Teachers not documented in HR



	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
FU employees	40	114	239	287	374	435	1306	1912	2391	3378	3394	3425
ext. Teachers					750	750	750	800	900	1000	1150	1200
Studenten					8936	13966	15848	18443	20747	23707	26568	30000
<b>Total Users</b>	<b>40</b>	<b>114</b>	<b>239</b>	<b>287</b>	<b>10060</b>	<b>15151</b>	<b>17904</b>	<b>21155</b>	<b>24038</b>	<b>28085</b>	<b>31112</b>	<b>34625</b>

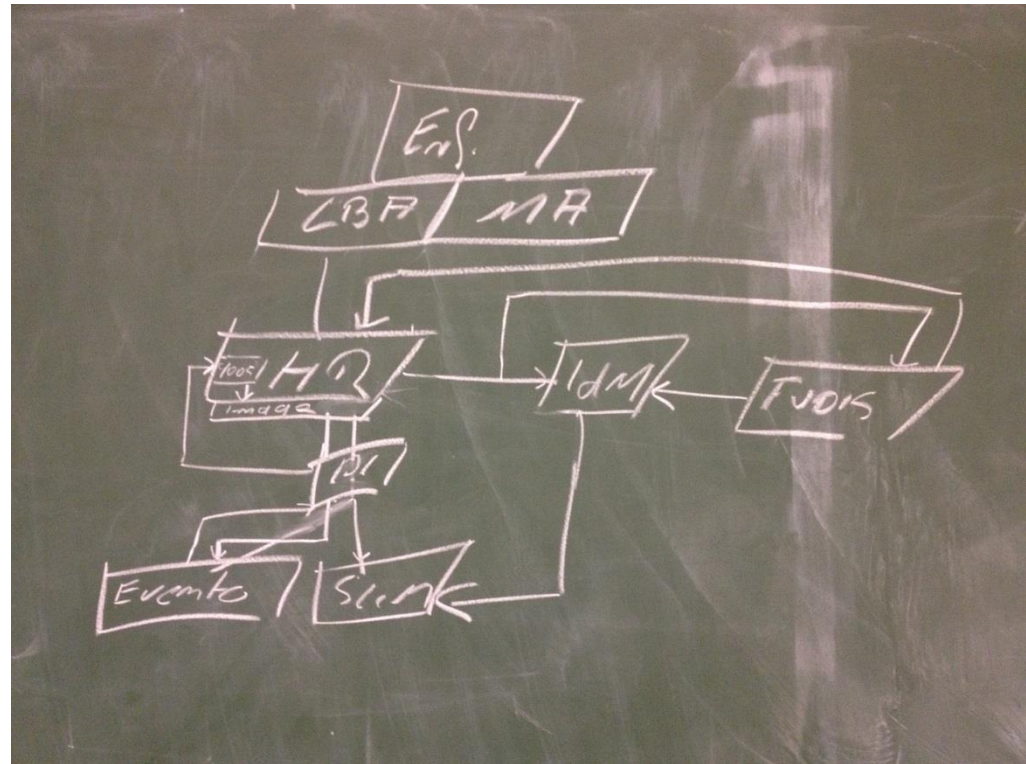
# Onboarding & Authorization (legacy architecture)



IT:

„Something has to  
be done!“

# Implementation of new Identity and Access Management



Top 1:  
 New Onboarding Architecture  
 (Proof of Identity)



# Proof of Identity at Universities



# The of External Teachers



# The of External Teachers

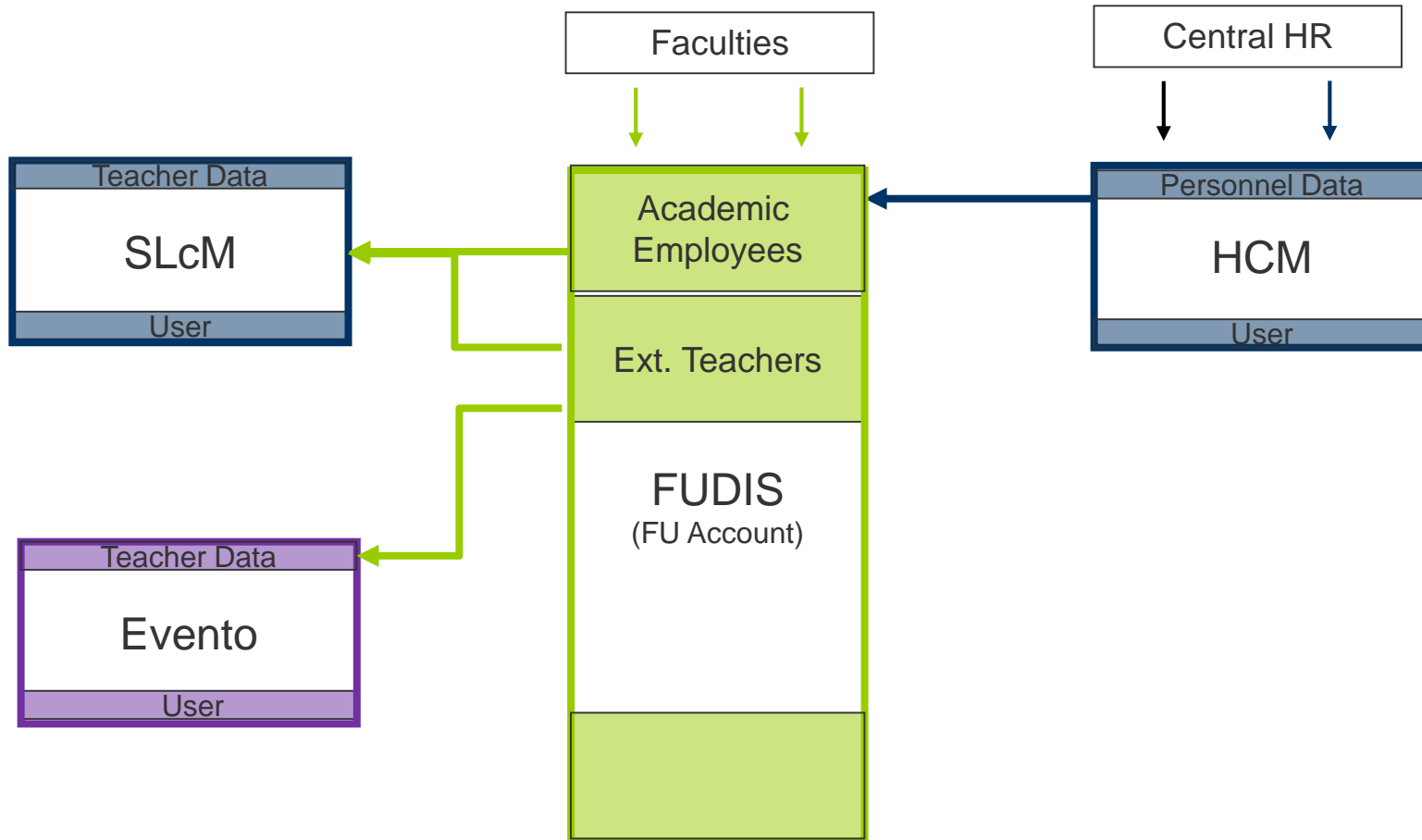


## 2011 – 2013 Reimplementation of Academics Dataflow



- ❖ **Improvement of data quality**
- ❖ **Avoiding of duplicates**
- ❖ **Reduction of user accounts to the needed number**

# Distributed Master Data Management (legacy architecture)



**EVERYTHING HAPPENS  
FOR A REASON.  
BUT SOMETIMES THE  
REASON IS THAT  
YOU'RE STUPID AND  
YOU MAKE BAD DECISIONS.**

# Masterdata where?

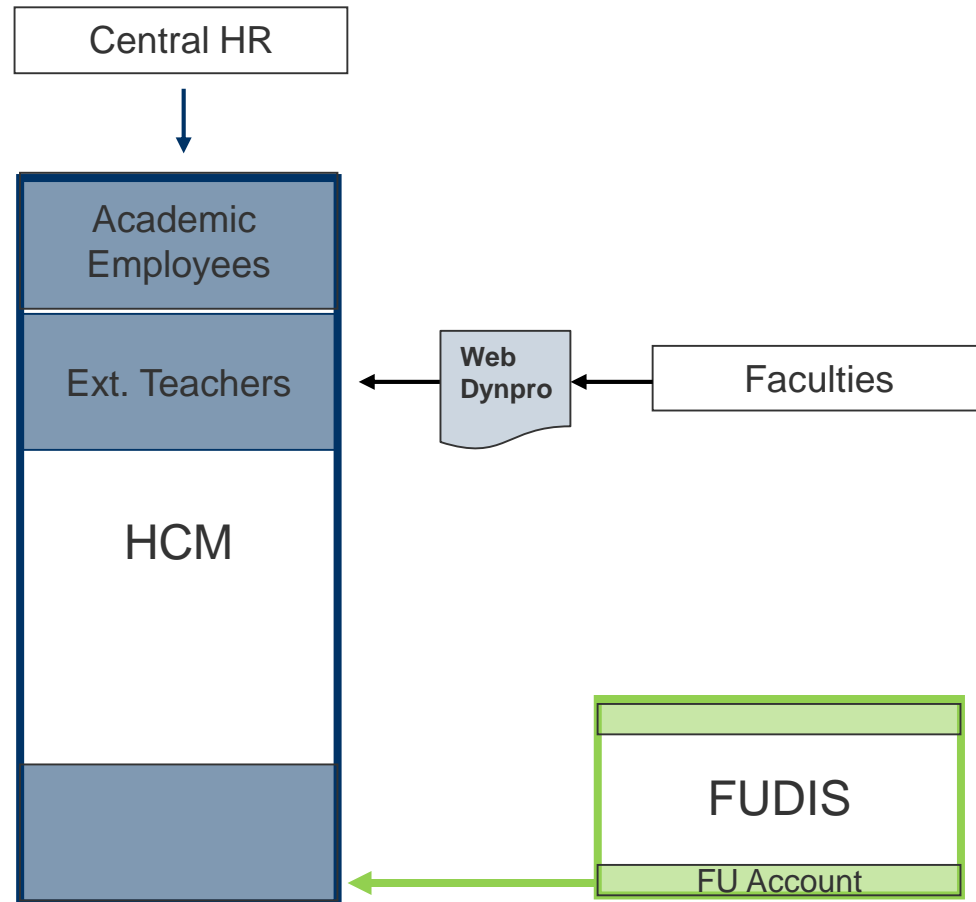


# Masterdata who?





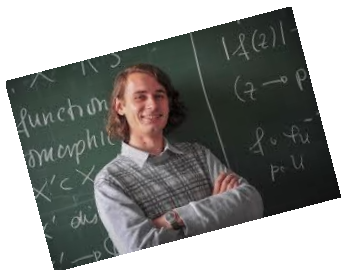
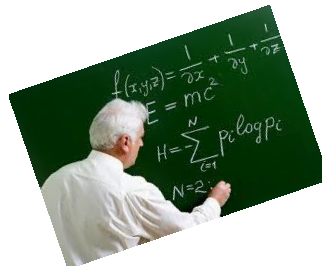
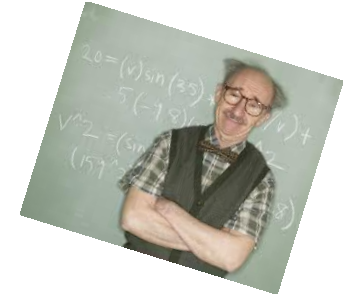
# Improvement of data quality



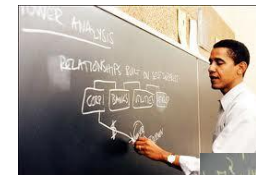
# JERUSALEM SYNDROME



# Teaching SYNDROME



# Teaching SYNDROME

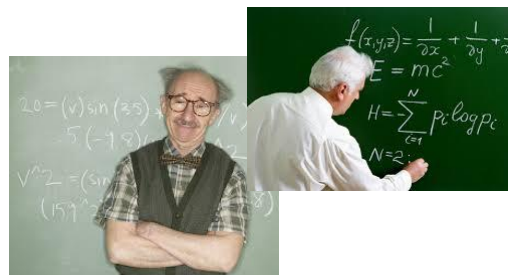


Employed Academics

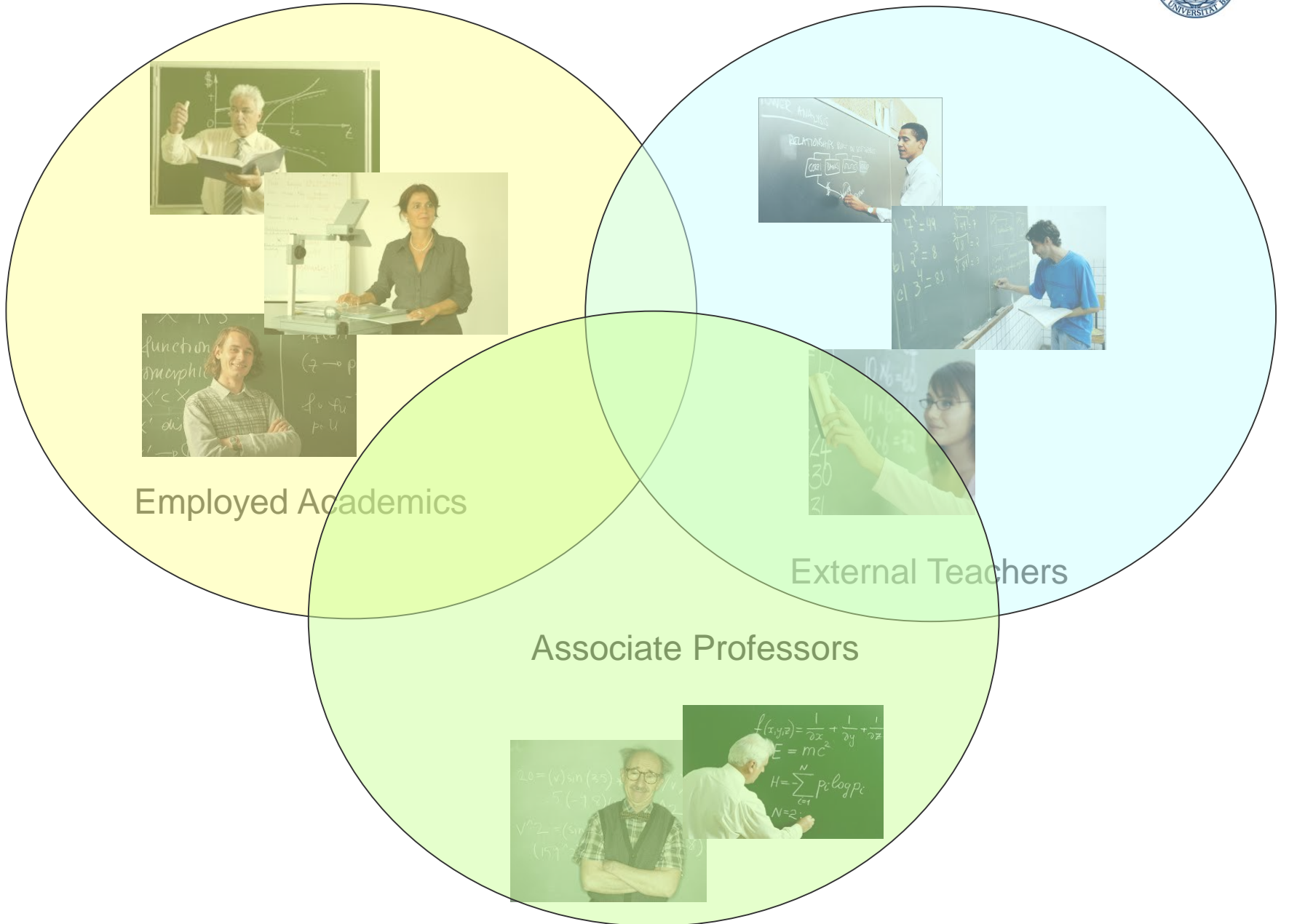
External Teachers



Employed Non Academics



Associate Professors



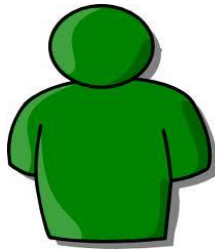
Employed Academics

External Teachers

Associate Professors

# The Introduction of the Central Person

**Marcus Miller**  
External Teacher



HCM Person # 1

**Marcus Miller**  
Employed Academic

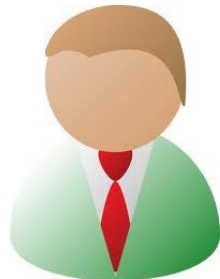
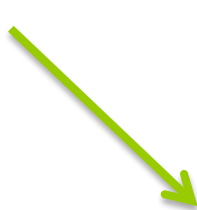


HCM Person # 2

**Marcus Miller**  
Associate Professor

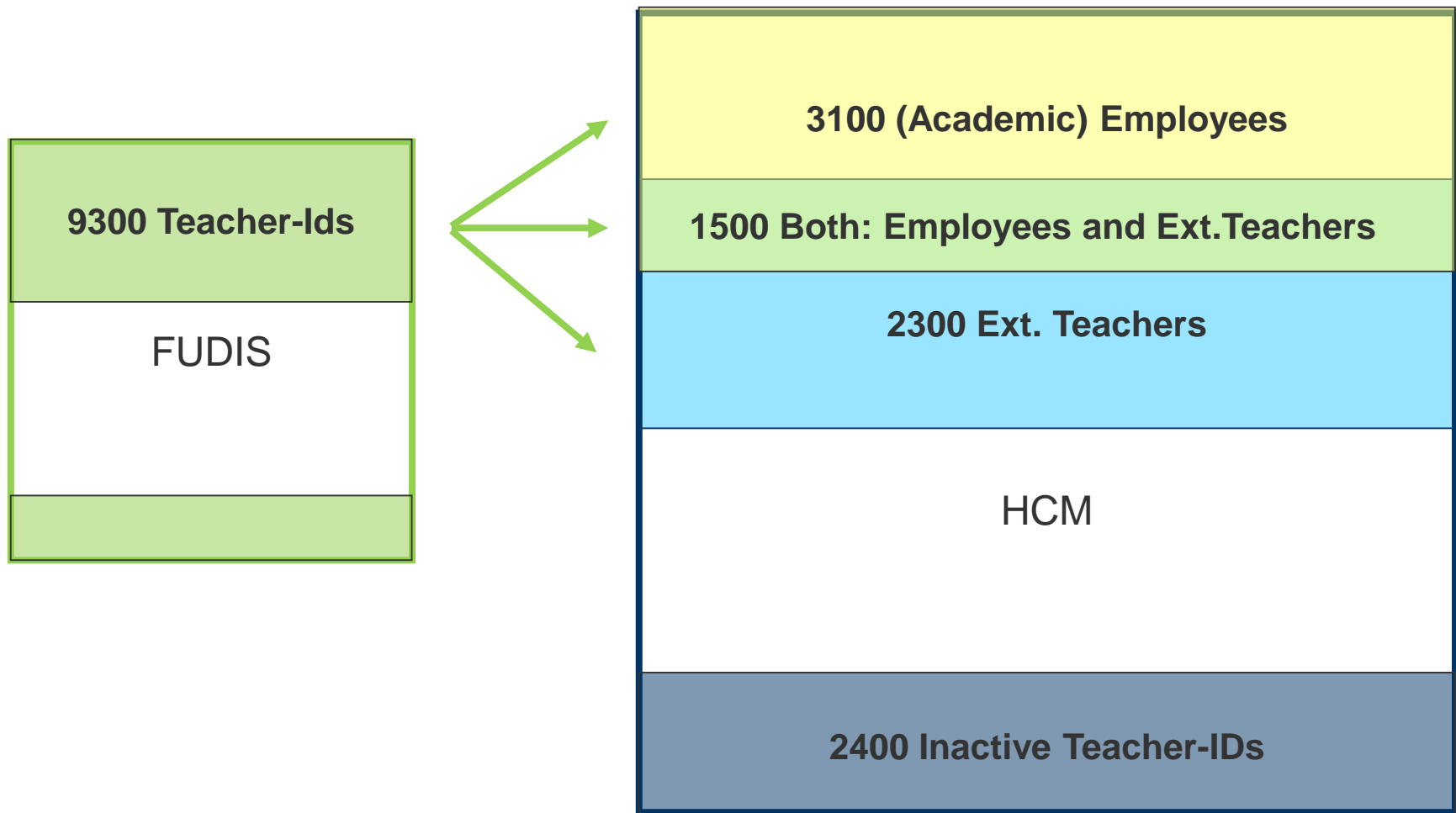


HCM Person # 3



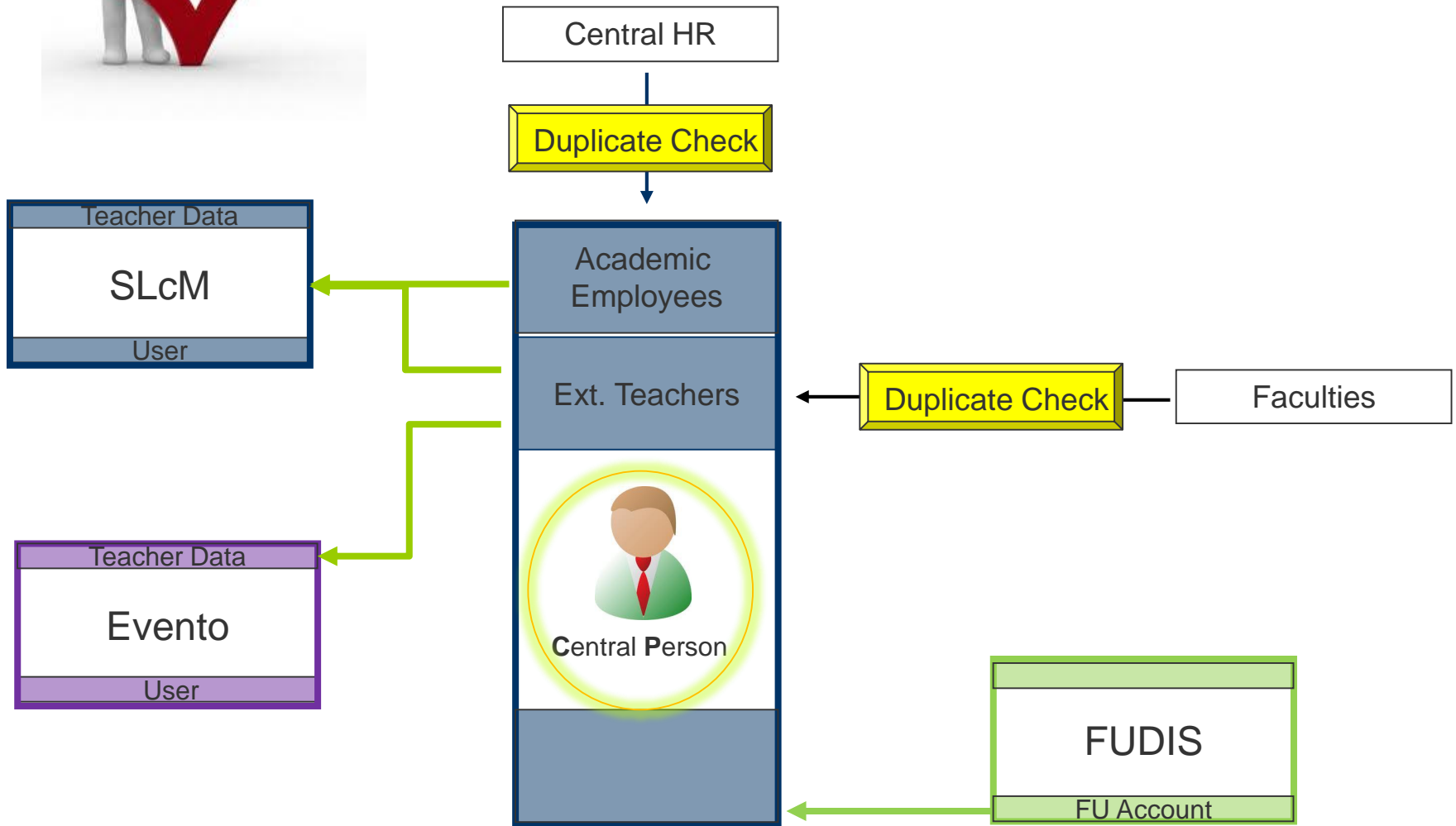
**Central Person # 1**

# Initial Master Data Migration FUDIS => HCM





# Avoiding of Duplicates





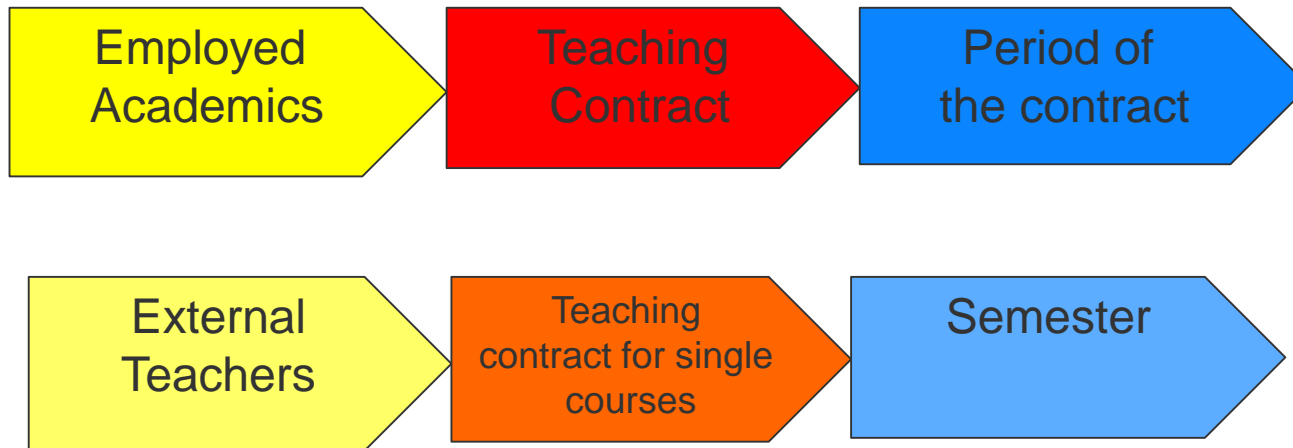
# Active Teachers?

*Who?*

*Why?*

*When?*

*How?*

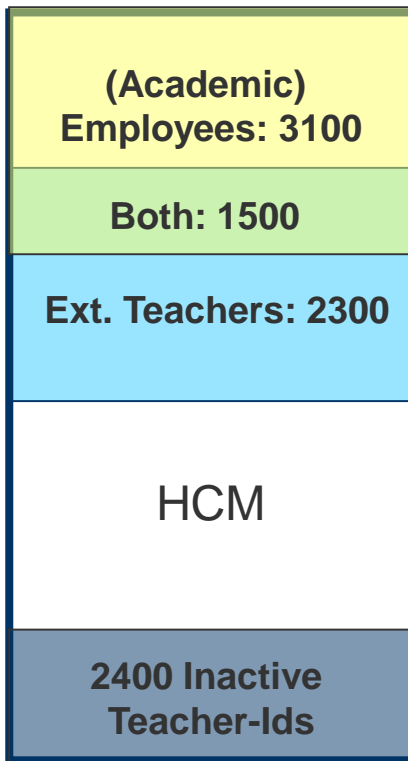


Academic Employees
Hire Fire Dates
Ext. Teachers
List of courses per semester
HCM

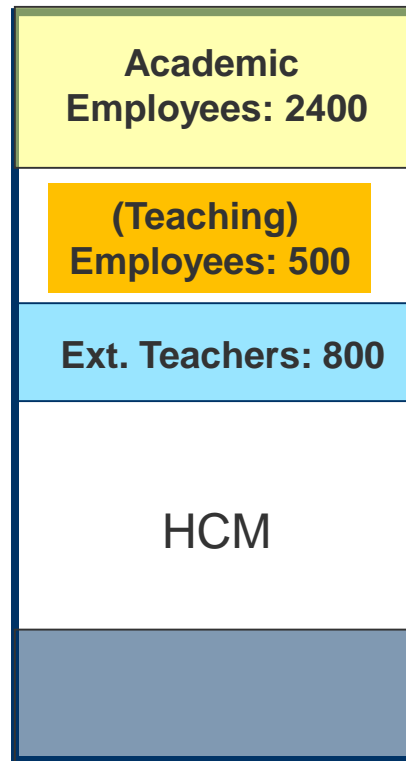


# Reduction of user accounts to the needed number

*April 2013: 6900*



*April 2014:*



*3700*

*Activity Control*



# A Matter of Perspective



## Masterdata where?



Was the decision  
for HCM a good one?

# Activity Matrix

Interface to	Group	Before Course	After Course	After hired in HCM	After fired in HCM
SLcM	Employed (Academics)	3 month			7 month
	Associate Professors				7 month
	External Teachers	6 month	7 month	7 month	
	Academic Supervisors			12 month	
Evento	Employed (Academics)	3 month			
	External Teachers	6 month	7 month	7 month	
IDM	Employed (Academics)				7 month
	Associate Professors				7 month
	External Teachers	6 month	7 month	7 month	
	Academic Supervisors			12 month	

**HCM has to define and provide the activity period of the teachers for other systems. It offers no standard functionality for this.**

**The function that computes the activity of a teacher has to be implemented in all the reporting, the web dynpros for teachers, the interfaces and the query tools.**



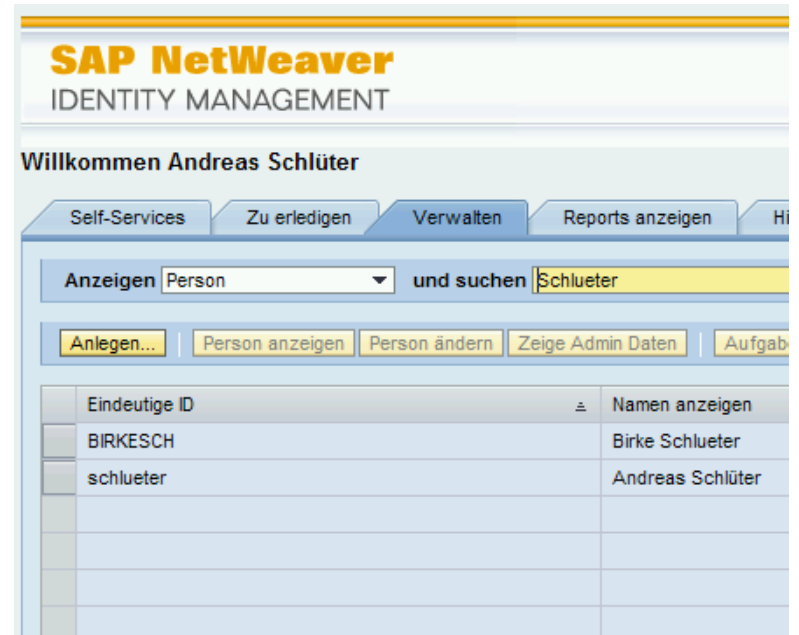
# Structured Information about Teachers for IDM



Past Members for...Month	Active Members of FU	Future Members for... Month
7	Employed Academics	-
7	Employed Non Academics teaching	-
7	Associate Professors	-
7	External Teachers	6
-	Academic Supervisors	-

# Implementation of new Identity and Access Management

## Top 2: Introduction of Roles (Characteristics of Identity)



**SAP NetWeaver**  
IDENTITY MANAGEMENT

Willkommen Andreas Schlüter

Self-Services | Zu erledigen | **Verwalten** | Reports anzeigen | Hi

Anzeigen  und suchen

Anlegen... | Person anzeigen | Person ändern | Zeige Admin Daten | Aufgab

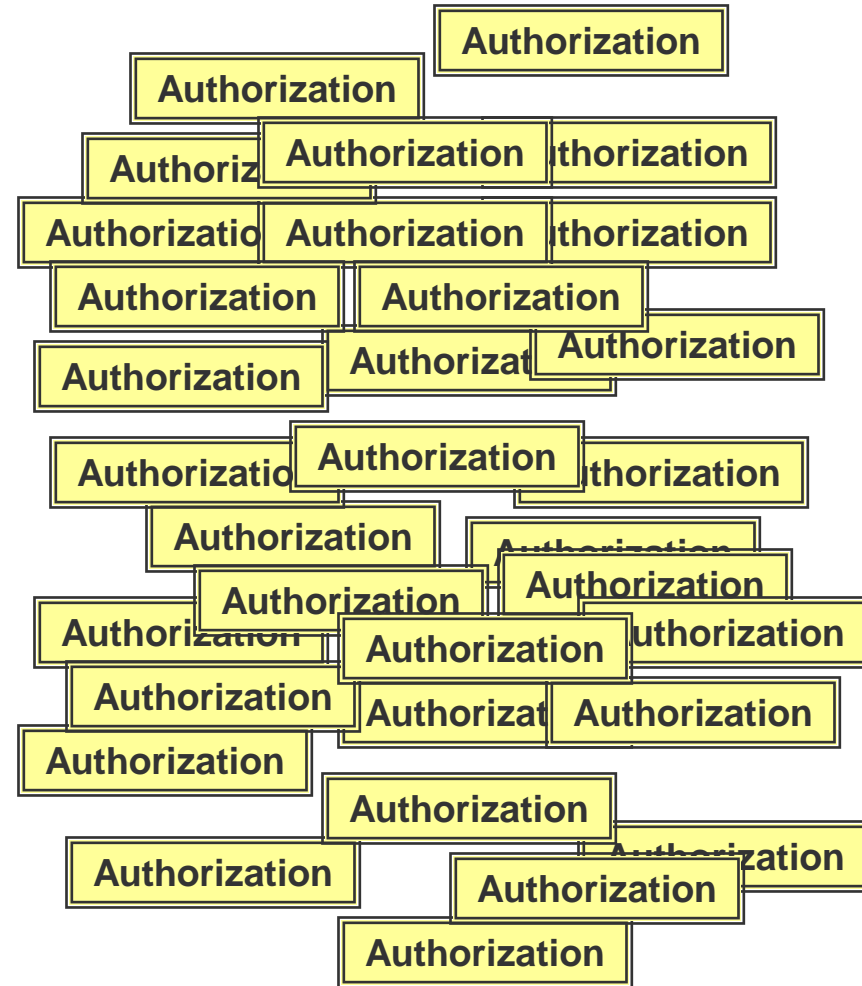
Eindeutige ID	Namen anzeigen
BIRKESCH	Birke Schlueter
schlueter	Andreas Schlüter

# Authorization before ...

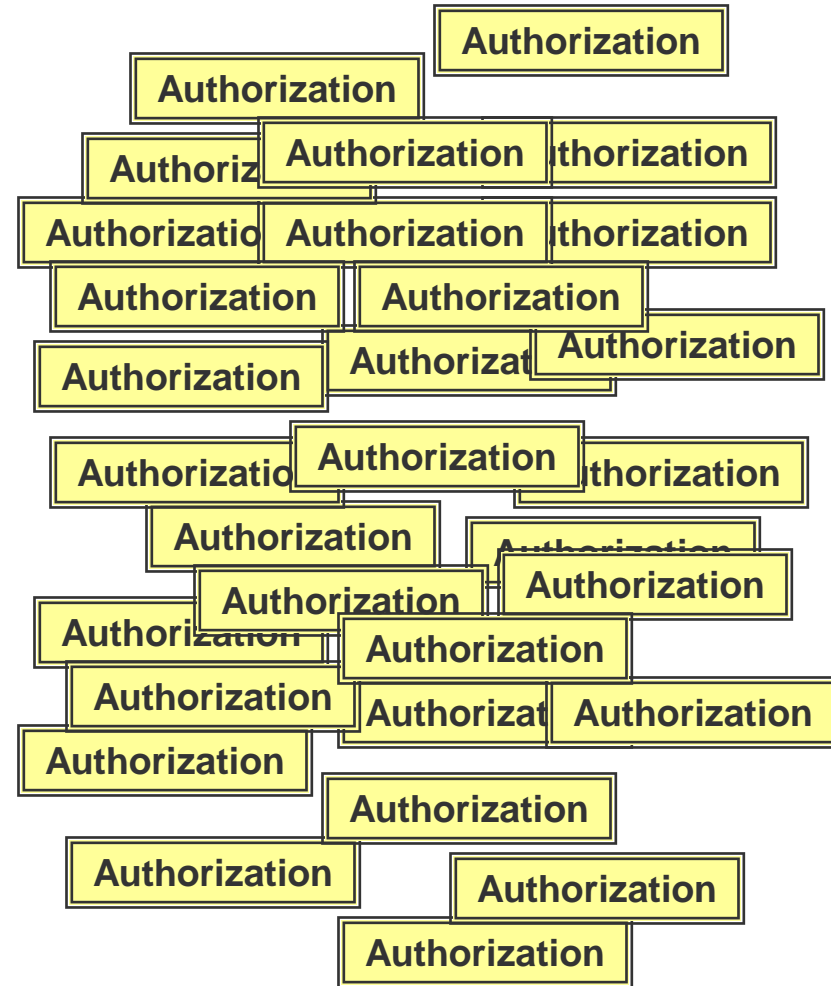




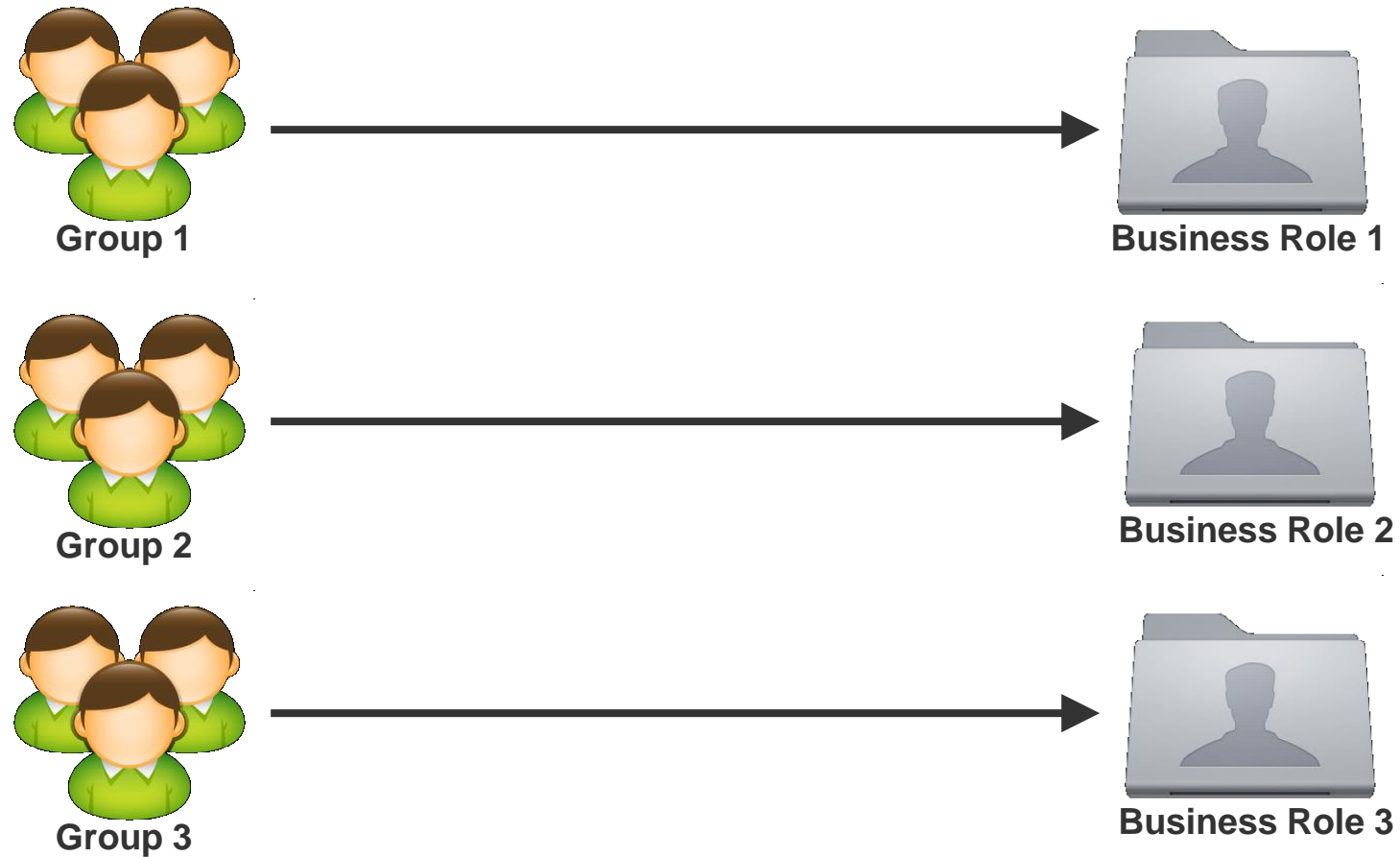
# Introduction of Roles



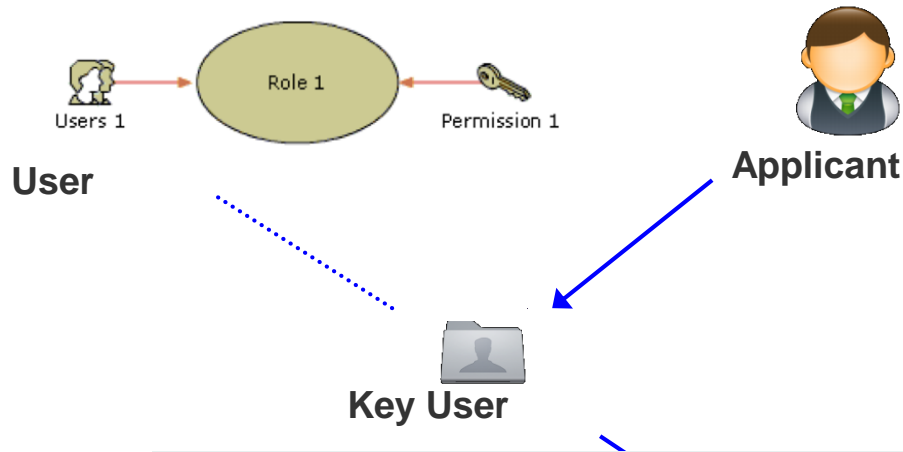
# Introduction of Roles



# Introduction of Roles



# Role Approval Workflow



**Authoriz:**

### Application

Eindeutige ID Miguel Namen anzeigen Miguel Nachname Unamuno Vorname Miguel

Alle neuen Rollen werden entweder sofort oder nach Genehmigung des Verantwortlichen zugeteilt. Eventuelle Genehmiger werden umg

Nach Zuordnung der Rolle, werden die zugehörigen Berechtigungen innerhalb weniger Minuten im SAP System erteilt.

Falls dies Ihre erste Berechtigung innerhalb eines SAP Systems ist, wird dort ein neues Benutzerkonto unter Ihrer IdM Identifizierung ang

Löschen von Rollen:  
Sie können jede Ihnen zugeordnete Rolle löschen. Alle an die Rolle gebundenen Berechtigungen werden Ihnen daraufhin in den SAP Sys

**Zugeordnete Rollen**

**Verfügbar**

Anzeigen  **und suchen**

Namen anzeigen	Eindeutige ID	Bezeichnung
HR-Sachbearbeiter	ROLE:HR-SB	Sachbearbeiter im HR

### Approval

Gültig ab:

Gültig bis:

Anforderungsgrund:

Attributname:

Attributwert: Wolfram Fassbender

Ziel Eintrag: Administrator

---

**Grund**

# Did it help ?

# Identity Management at work:



"Now! ... That should clear up a few things around here!"

# Strategic Goals reached with the new IAM

## Comprehensive offer of information

→ Information online available about who has which rights in what system since when and awarded by whom

## Mobile Information

→ Web based role request and provisioning

## Smarte Processes

→ Trans-departmental process of onboarding with single point of entry for information

## Secure data

→ Automated process of user deactivation upon end of employee status

## Sustainable use of resources

→ No more fees for licenses for inactive users



## elektronische Administration und Services

Dr. Christoph Wall  
Director administrative IT-Services

Boltzmannstraße 18  
14195 Berlin  
Germany  
Tel: +49 30 838 58000  
Web: [www.fu-berlin.de/eas](http://www.fu-berlin.de/eas)

Gudrun Buchholz  
Team Lead HCM-Services

Boltzmannstraße 18  
14195 Berlin  
Germany  
Tel: +49 30 838 54764  
Web: [www.fu-berlin.de/eas](http://www.fu-berlin.de/eas)