DESY–registry

HEPiX Spring 2005 — Karlsruhe, DE

Dirk Jahnke-Zumbusch
et.al.

IT-Systems Group · Hamburg

dirk.jahnke-zumbusch@desy.de

a central user registry…

- … is not exactly a brand new concept
- DESY had a UNIX-centric registry for many years
- but:
  - integration of other systems was only rudimental
  - technical implementation was based on scripts
  - subsystems essential for the registry were out-of-date and / or without support, like DCE/DFS
  - new requirements evolved

numerous backend systems

motivation for a central user registry

- every system has its own account registry
  - Windows / Active Directory
  - Kerberos / AFS
  - NIS
  - RADIUS, Oracle, SAP, Web, POTS, QIP
  - ... ~30 system in total
- and its own password
- and its own policies
- ...

user support
motivation for a central user registry

- this leads to many administrational tasks
  - creating accounts
  - synchronizing identical information across platforms
  - handling of different expiries
    (accounts, passwords for every platform, groups, mailing lists,…)
  - managing responsibilities
    (ownership of accounts and e-mail addresses)
  - getting rid of accounts
  - archiving tasks
  - …
- support by user consulting office split up into many consoles

new requirements
motivation for a central user registry

- **software usage regardless of user‘s client platform**
  - **groupware like calendaring, public folders, conferencing**
  - **special software like SAP-PS**
    (availability, costs UNIX vs. Windows)
  - **access controlled web content**
    (which password has to be entered on which web server)
- **possibility of delegation to non-IT administrators**
- **user requirements**
- **(mostly) identical policies on all platforms**

finding out the requirements

- what exactly should a central user registry do?
- at first there were lots of ideas
- work(flow) in all DESY groups would be affected
- workshops with experienced administrators
- involvement of DESY boards and committees
- collecting requirements during workshops

methodology
1

- in-depth analysis of actual state
  - user processes
  - policies
  - IT-internal processes
  - requirements of non-IT platforms
  - functional architecture
  - market survey
  - intermediate results ➔ decision
  - system architecture
  - detailed concepts / functional specification
  - review

methodology
2

- **implementation**
  (commercial product vs. own solution)
- **migration and consolidation(!)**
- **training of staff and administrators**
  (8h/4h)

- **continous maintenance necessary**
- **integration of non-primary/-legacy systems**

- **extension of functionality**

results of the workshops

- ~300 user requirements
- IT-internal requirements
- actual state of internal workflows

- written mandatory regulations

➔ **this is a relief !**

even if some users tend to forget about agreed policies

➔ **legal aspects**

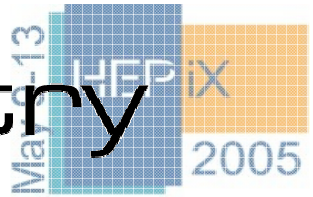
(privacy, passing on of accounts, ...)

results of market survey

- competing systems
  - CA eTrust
  - CriticalPath
  - Tivoli
  - ENTACT
  - Völcker
  - Ganymede
- none of the systems meets the most neccessary requirements (Tivoli came close)

➔ individual solution

highlights of the DESY – registry



- one leading account registry
- portal for user administration tasks
- delegation to non IT-administrators ➔ minute-maid accounts
- highly configurable
- event-oriented push mechanism
- single-sign-on ➔ a different approach
- dependencies of (abstract) ressources
- „cross-platformity“ of accounts and groups
- expiries ➔ also support for manging security incidents

roles and hierarchy

	name space	person	account	group	ressource access
user	✧	✧	✧	✧	✧
ObjAdm	✧	✧	✧	☆	✧
NSAdm	✧	☆	☆	✪	✧
NSSv	☆	☆	✪	✪	✪
UCO	★	★	✪	✪	✪
ITRA	✪	✪	✪	✪	✪

✧ view attributes

☆ change attributes

★ change entity

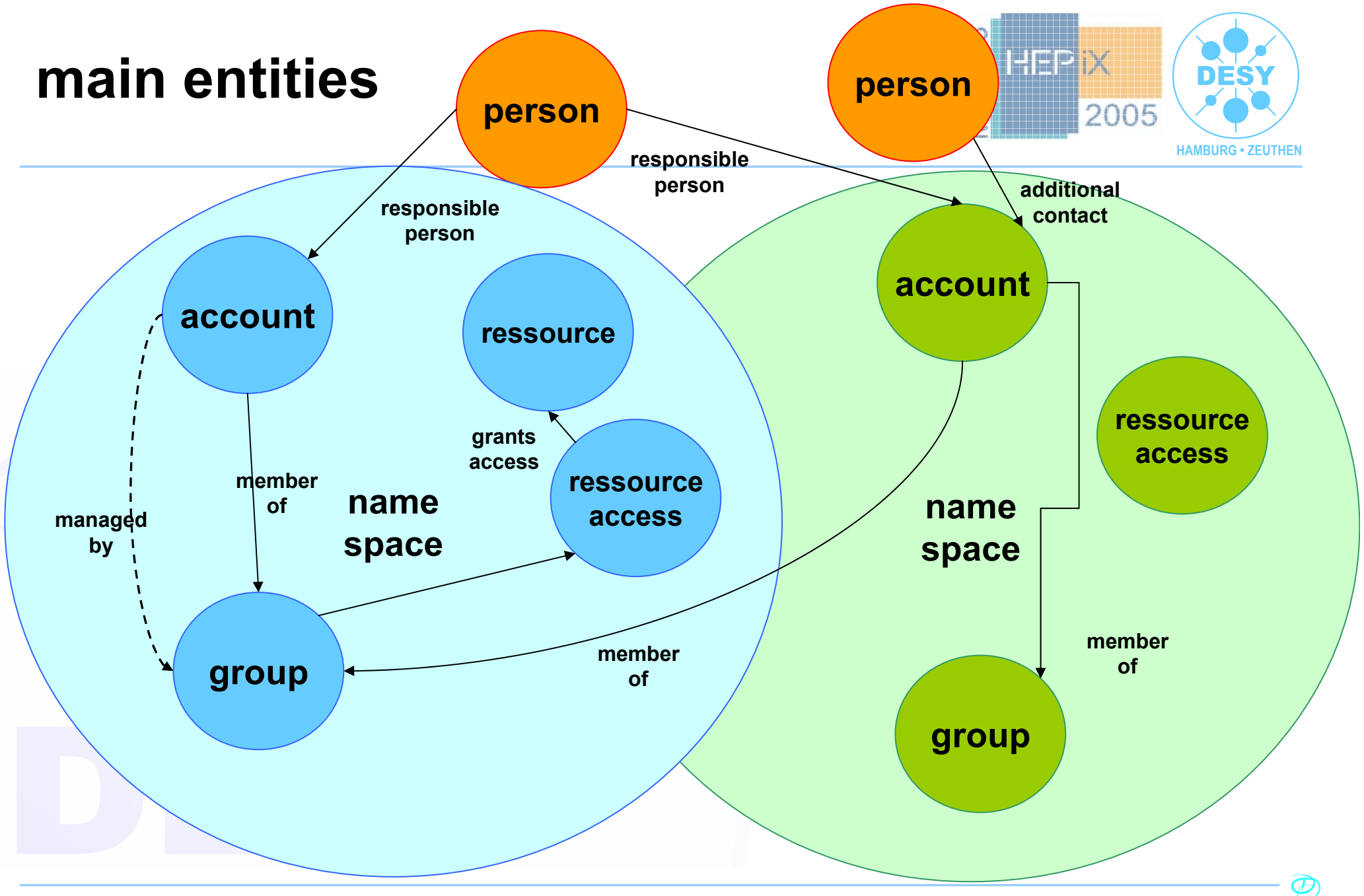
✪ modify everything

this is a simple overview

objects to manage

- accounts ➔ abstract, passwords
- groups ➔ memberships
  - organisational
  - access
  - mailing list like
- ressource access ➔ platforms
- partitionable ressources ➔ quota
- persons ➔ not only for registry purposes
- namespaces
- the registry itself (roles, paramters, queues, adapters)

main entities



namespace
main entities

- **unique name (Windows=OU, invisible in UNIX, may be e.g. a prefix)**
- **mean of delegation for business units or projects**
- **is managed**
  - **by NS-Supervisors → underwriter**
  - **by NS-Administrators → daily tasks**
- **is part of**
  - **group names**
  - **names of mailing lists**
  - **public folder names**
  - **URLs**
- **namespaces are managed by IT-RegAdmins**

persons
main entities

- the DESY-registry is not a leading system for person data
- nevertheless it has its own mechanism of synchronizing with other data sources
- persons own unique e-mail addresses (@desy.de, 5yrs.)
- persons may own accounts
- persons are created by namespace administrators
- a person itself may modfiy only very few attributes
- persons do not „expire“

accounts
main entities

- accounts are „abstract“, used cross-platform
- every account gets access to some default ressources (Windows, AFS, NIS, Kerberos)
- additional ressources may be assigned to an account (Oracle, RADIUS, CAD, ...)
- accounts expire by default, may be permanent
- different types of accounts
  - primary & personal
  - functional

passwords
main entities

- passwords of account belong to classes
  - e.g. Windows, Kerberos ➔ „secure“
  - e.g. Oracle, RADIUS ➔ „insecure“
- passwords are synchronized for each platform via the registry
- policy of pw. complexity is controlled by the registry
- passwords may be reset by NS-admins
- secret question & answer mechanism for remote identification

groups
main entities

- grouping of accounts
- ressource acces is granted via groups
- groups are managed by object administrators
  ➔ mean of delegation for NS-admin
- may be used as a mailinglist (to come)
- may have an alias
- maps to
  - managed group, Windows
  - AFS-group
  - NIS-group (not: netgroup)

ressource access
main entities

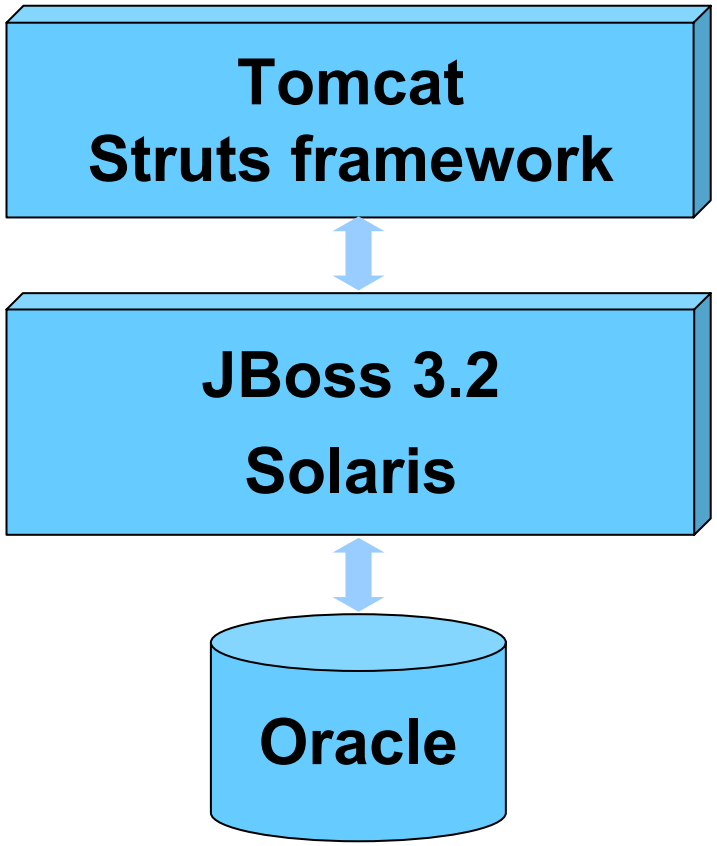
- mean of granting access to platforms
- may be „default“ for accounts
- may expire
- may have dependencies
- examples
  - Windows, AFS
  - NIS netgroups
  - VPN-access

data processing

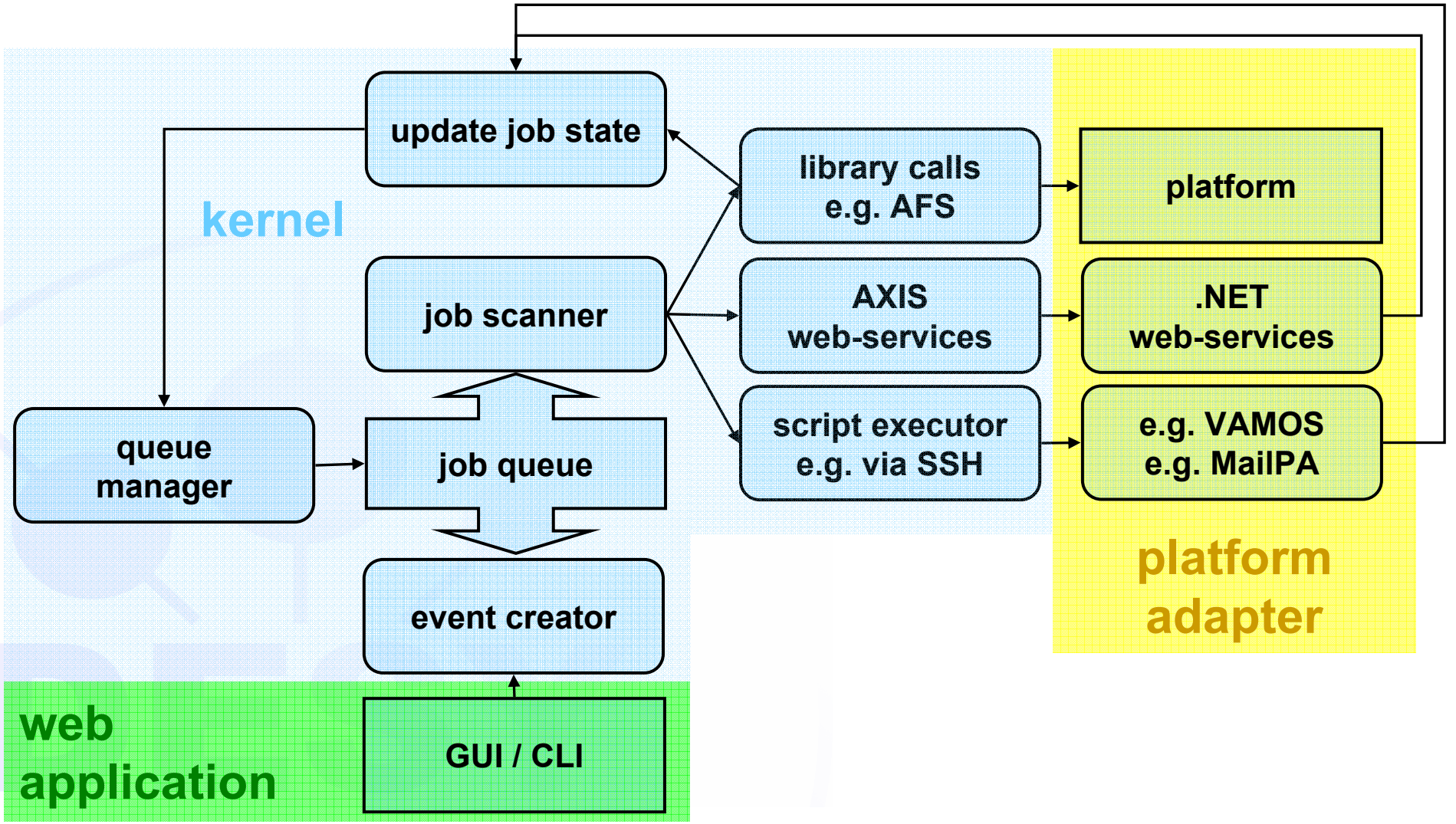
- event initiators
  - graphical user interface or command line interface
  - expiry scanner
- events
  - create jobs, resolve dependencies
  - take care of the processing order (configurable)
  - are of type „asynchronous“ or „synchronous“ (only pwd-set & lock)
- job queue
  - manage number of jobs for each event and platform
- platforms
  - are processing jobs and deliver status information
- reports
  - overview for administrators

architecture overview

- model – view – controller
- Web-Frontend / GUI & CLI based on JSP
- common Java design patterns
- J2EE application server
- database backend



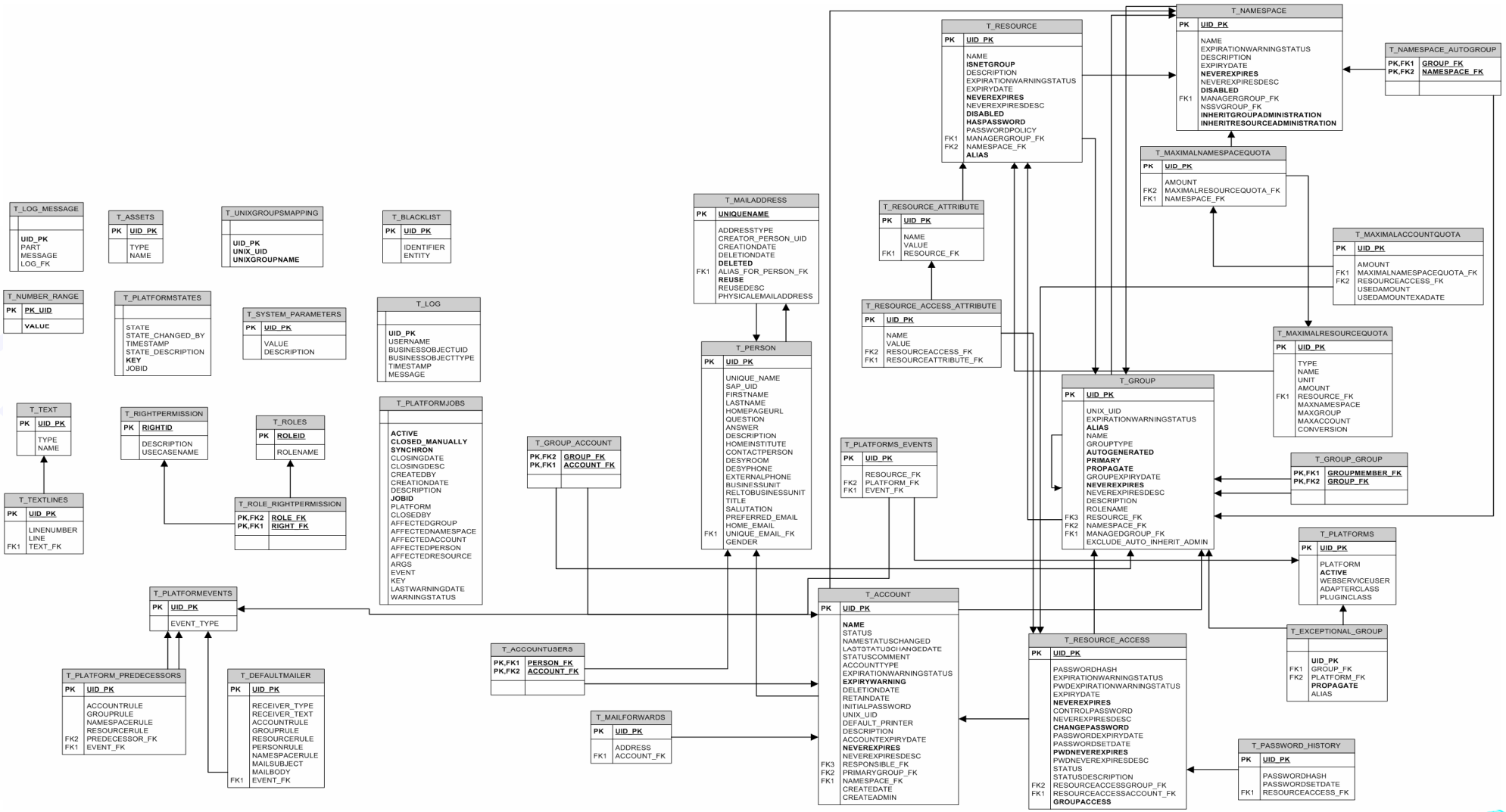
event processing



application metrics

type	classes	functions	lines	other
kernel	293	3,671	32,738	
web appl.	227	2,357	19,400	
Xdoclet (>2,000 tags)	358	3,513	10,271	← generated
JSP			> 9,500	80 pages
Oracle				38 tables
SQL/EJB-QL			> 200	statements
total	878	9,541	> 72,000	total

entity relationship



a bit of „history“

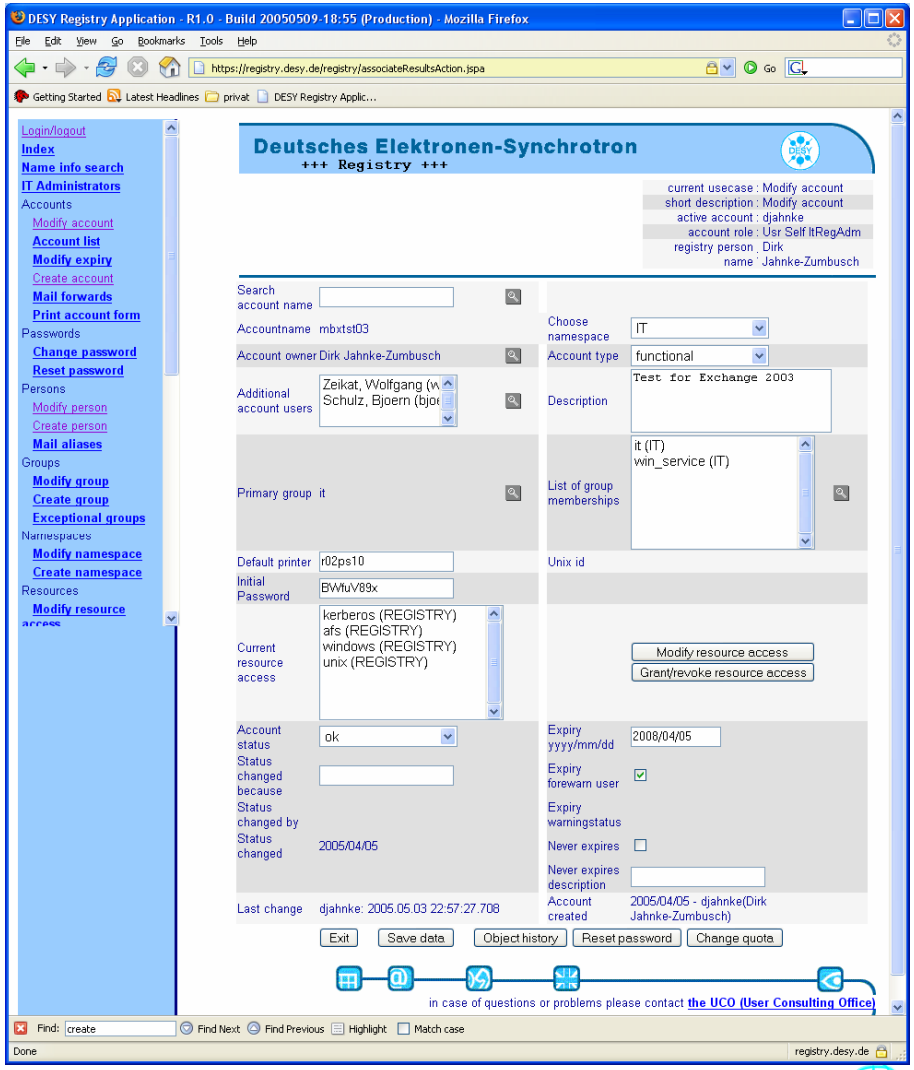
- **FEB/2002:** start of project
- **APR/2003:** start of implementation
- **AUG/2004:** support of Windows migration (NT➔AD) for ≤ 4,000 accounts + migration of 3,000 AFS-only accounts
- **SEP/2004:** UCO as user beside migration team
- **OCT/2004:** pilot phase with experienced administrators
- **FEB/2005:** production

user‘s & admin‘s reactions

- good acceptance by users and administrators
- ~10 „reset password“ events per day
- new accounts
- requests for
  - more overviews & reports
  - more intuitive forms (but what‘s intuitive?)
  - more functionality
- also: individual administrator tend to create „never expire“ accounts

planned functionality

- electronic workflow
- more quota handling
  - Exchange
  - Windows homes
  - CPU
- X.509 certificates for persons
- X.509 certificates for accounts
- coupling with grid-VOs
- interface to facility managment
  (people, rooms, buildings, phones)
- interface to SAP-HR



Thank you for your attention !

Any questions ?