Business-Process-Management and Identity-and-Access-Management

Selecting a Business-Process-Management-System in conjunction with an Identity-and-Access-Management-System

Dirk Jahnke-Zumbusch
HEPiX fall 2012
IHEP, Chinese Academy of Sciences
Beijing, China
2012-10-16

Optimizing business processes using electronic workflows

- business processes are integral parts of every day (mostly non-technical) administrative tasks – lots still on paper forms
- business process management goals are the identification of business processes, their (re-)design and documentation, implementation, controlling and (continuous) improvement
- a joint project of DESY's administration division and the High-Energy-Physics department was started to provide the organizational and technical prerequisites for establishing electronic workflows
- the more prominent objectives
  - processes will be handled faster, important for high volume processes
  - better traceability and views on process bound data during execution
  - uniform execution

Business Process Management aspects

> o.k., you all know them: business processes …

- … are established on paper forms
- … already exist as electronic workflows (e.g. SAP HCM)
- … sometimes appear to be handed down by oral traditions more than having being written down
- … are nothing to be afraid of (?)
- … a source of lots of thinking about organizational stuff

> business processes are used to describe what is happening

➔ Zachman framework as a mean to structure the description of what is going on at your site (company, enterprise,…)

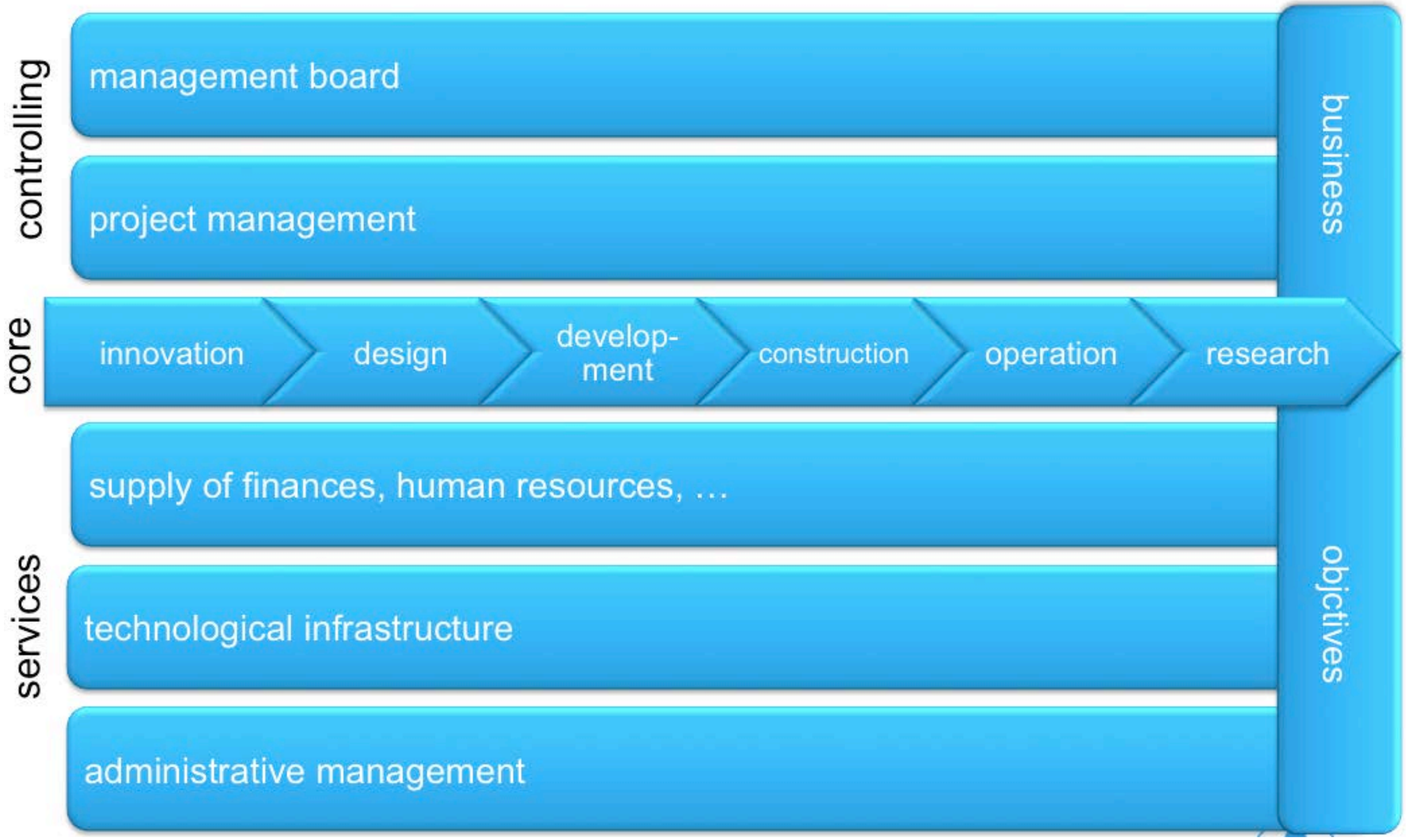
Zachman framework – a structured description

classifications ➔ audience ↓ perspectives	what data	how function	where location	who people	when time	why motivation
scope (contextual) planner	list of things important to business	list of processes that the business performs	list of locations in which the business operates	list of organizations important to the business	list of events or cycles important to the business	list of business objectives/strategies
business model (conceptual) designer	e.g. semantic model	e.g. business process model	e.g. business logistics system	e.g. workflow model	e.g. master schedule	e.g. business plan
system model (logical) designer	e.g. logical data model	e.g. application architecture	e.g. distributed system architecture	e.g. human interface architecture	e.g. process structure	e.g. business rule model
technology model (physical) builder	e.g. physical data model	e.g. system design	e.g. technology architecture	e.g. presentation architecture	e.g. control structure	e.g. rule design
detailed representations (out-of-context) subcontractor	e.g. data definition	e.g. program	e.g. network architecture	e.g. security architecture	e.g. timing definition	e.g. rule definition
functioning enterprise	e.g. data	e.g. function	e.g. network	e.g. organization	e.g. schedule	e.g. strategy

after John A. Zachman [http://www.zachman.com/]

results of an analysis – a possible process map

> one results is a business process map
  - in theory: all (known) processes
  - in reality: an overview of candidates for an implementation



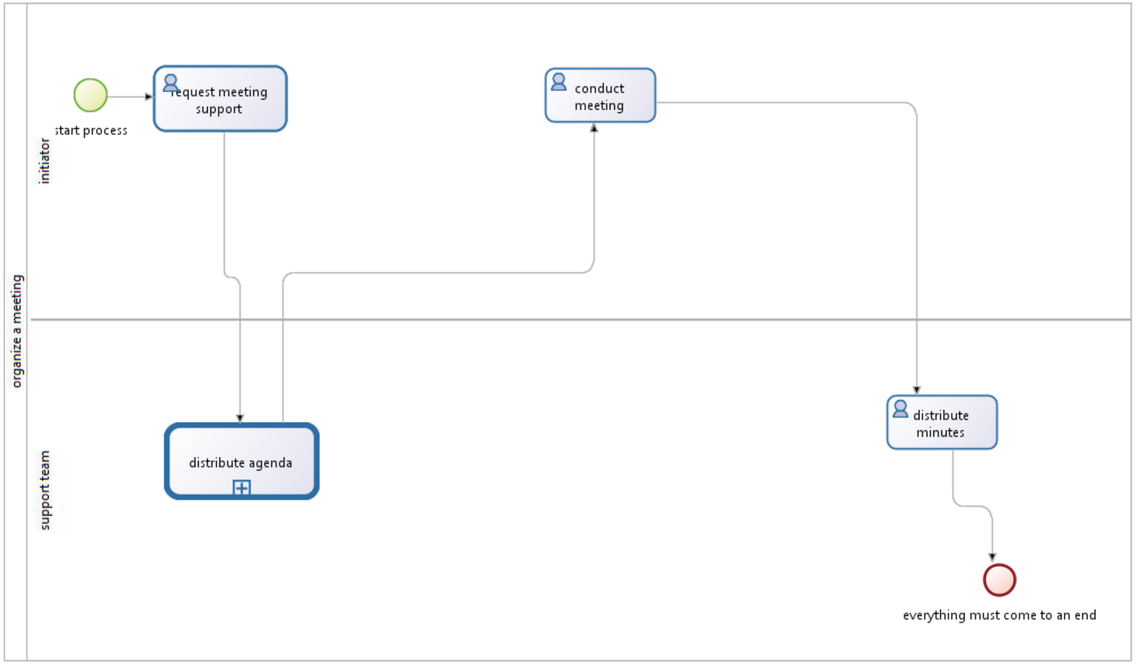
business process – an example

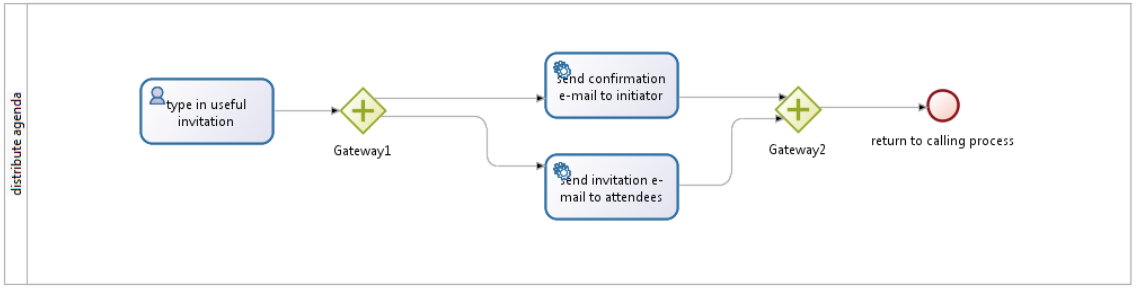
> what you see in the topmost picture: humans are carrying out activities

➔ we need to know them

➔ this is, where identity management is necessary

> what you see in the lower picture is, that also non-interactive activities are executed and other systems than the BPMS are involved




distribute agenda
type in useful invitation
Gateway1
send confirmation e-mail to initiator
send invitation e-mail to attendees
Gateway2
return to calling process

different views of processes

- when you document and analyze processes with process owners, you normally need a view free of “technical plumbing” to keep diagrams understandable
- when you would like to implement a process, you need some plumbing to put the pieces of the puzzle to work, e.g. define web forms, send and receive data to and from other systems
- round trip engineering
  - alterations in one or the other view of the process model have to be also made in the remaining model respectively – preferably automatically or at least assisted
  - e.g. instead of (electronically) signing serially you now want to sign in parallel

components needed for an implementation

- two main technical elements for an implementation
  - business process management system (BPMS)
  - identity and access management (IAM) system
- there are standards – for BPM
  - BPMN 2.0 business process model and notation (by IBM ➔ Obj. Mgmt. Group OMG)
  - BPEL, XPDL and others with decreasing importance
- identity management is about persons
  - persons are carrying out activities

    ➔ mostly on behalf of their business roles, e.g. supervisor, HR staff

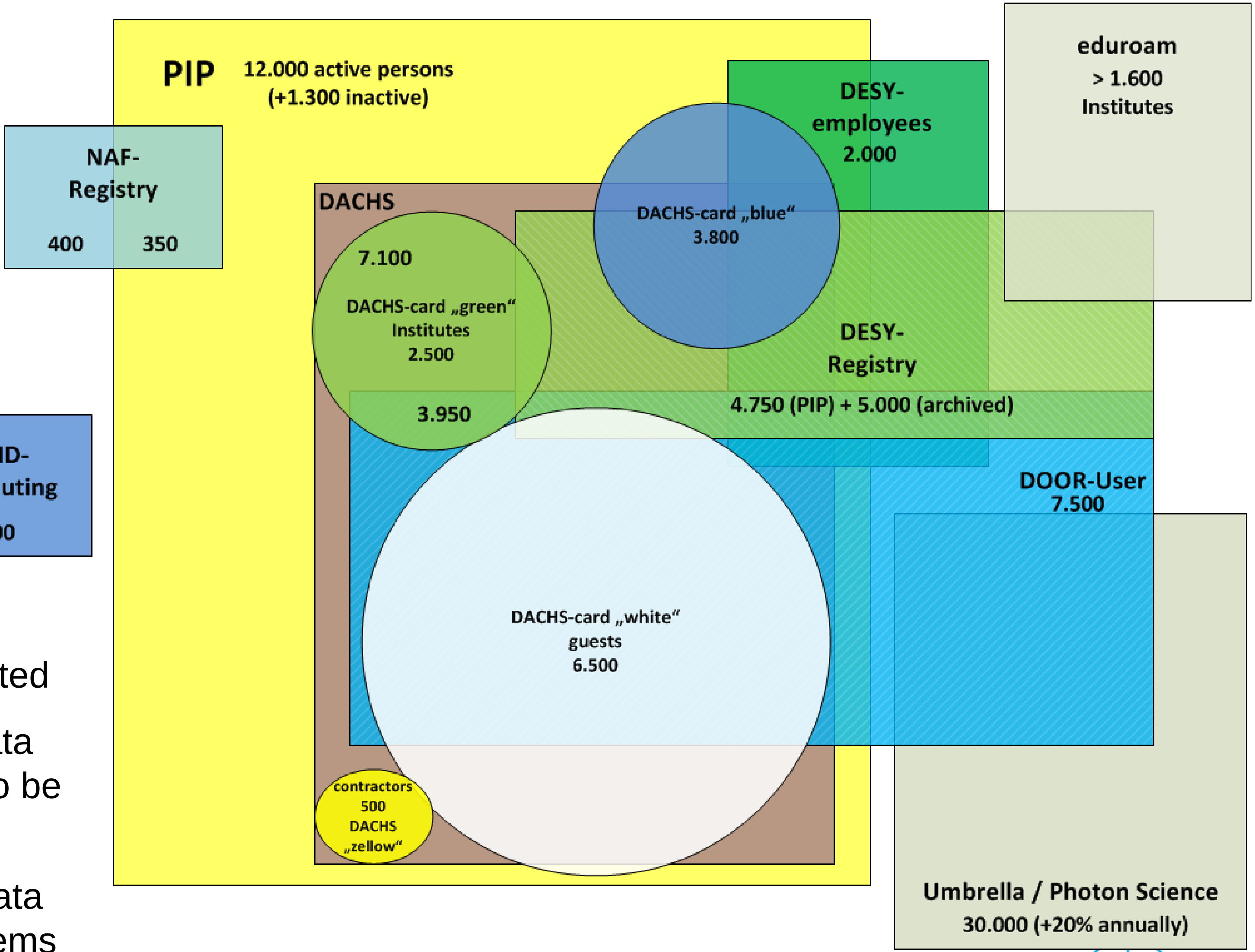
    ➔ sometimes with an individual role, e.g. taking holiday

    ➔ sometimes also IT systems are involved ;-)

    ➔ sometimes not; this is why identity management is not account handling

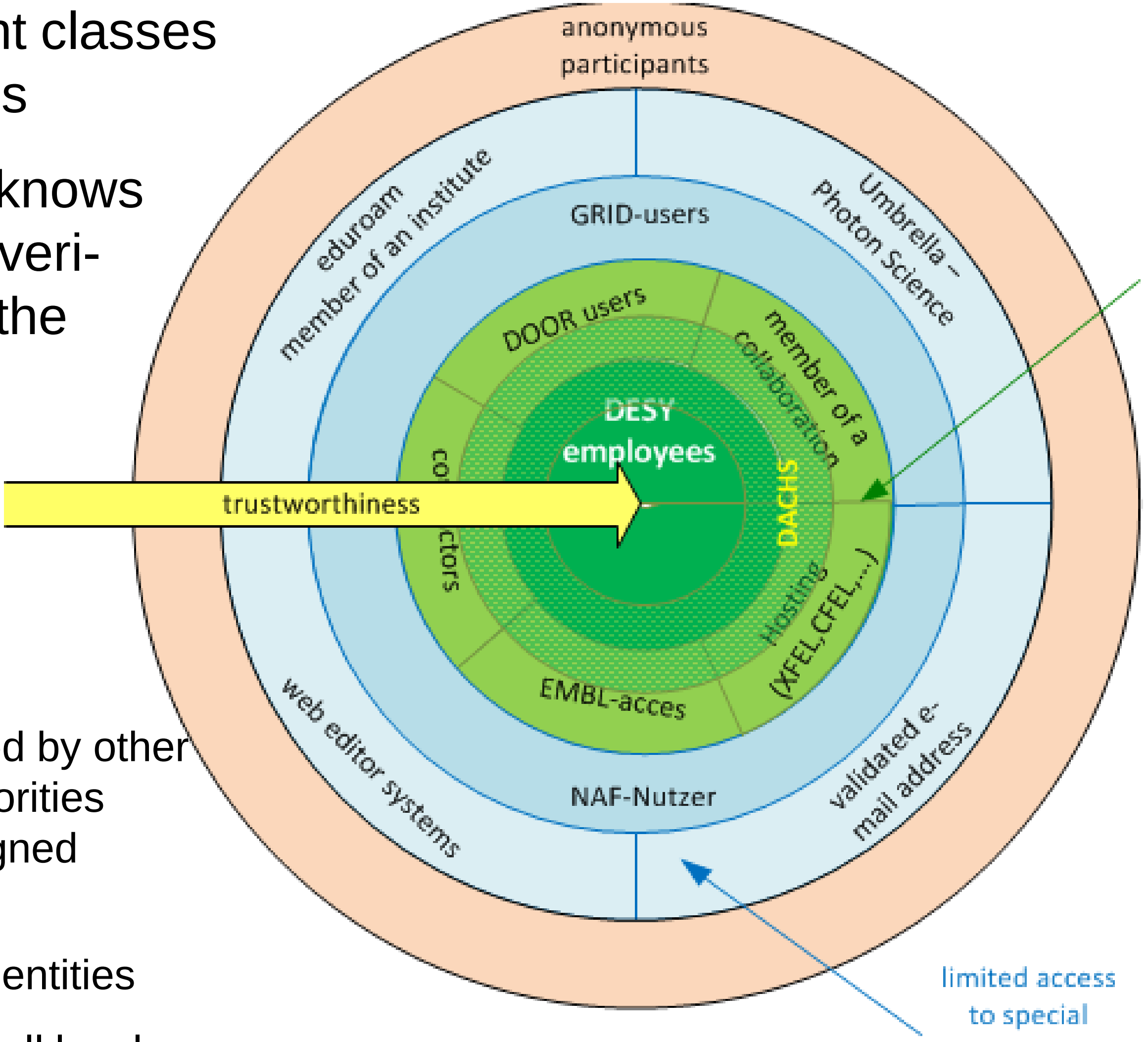
Person classes involved with DESY

- lots of different sources
- what about
  - trustworthiness of information
  - duplicates
  - nearly duplicates
  - the different ways data of persons is collected
  - the amount of data which is or has to be collected
  - propagation of data to technical systems



levels of trust – of person related data

- establish different classes of trustworthiness
- the more DESY knows about a person (verified), the higher the level of trust
  - employee or other person where the ID or passport was checked
  - certificates issued by other registration authorities DESY has an signed agreement with
  - self-registered identities
  - anonymous and all levels in between



fullz qualified DESY-accounts
➔ at least entry in PIP

limited access to special szstems (w/o PIP-entry)

BPM comes in handy – ILM identity lifecycle management

- support of the different ways people are registered with DESY
- documented and comprehensible registration process(es)

➔ BPM as a mean to design the manifold alternatives of on-boarding

- and think about
  - off-boarding
  - re-boarding
  - job hopping
  - and:
- roles which persons are assigned
  - automatically or
  - with manual approval
- and everything would be reproducible :-)

personal data – requirements and challenges

> how much data should be stored (and how): only as much as is needed
  - ➔ enrich personal data sets where necessary
  - ➔ store only data centrally which has to be centrally accessible

  - ➔ DESY has an open campus: no need to store anything in the first place
  - ➔ people have to adhere to special rules, e.g. using IT resources, and have to be (re-)identified; handling of duplicates?

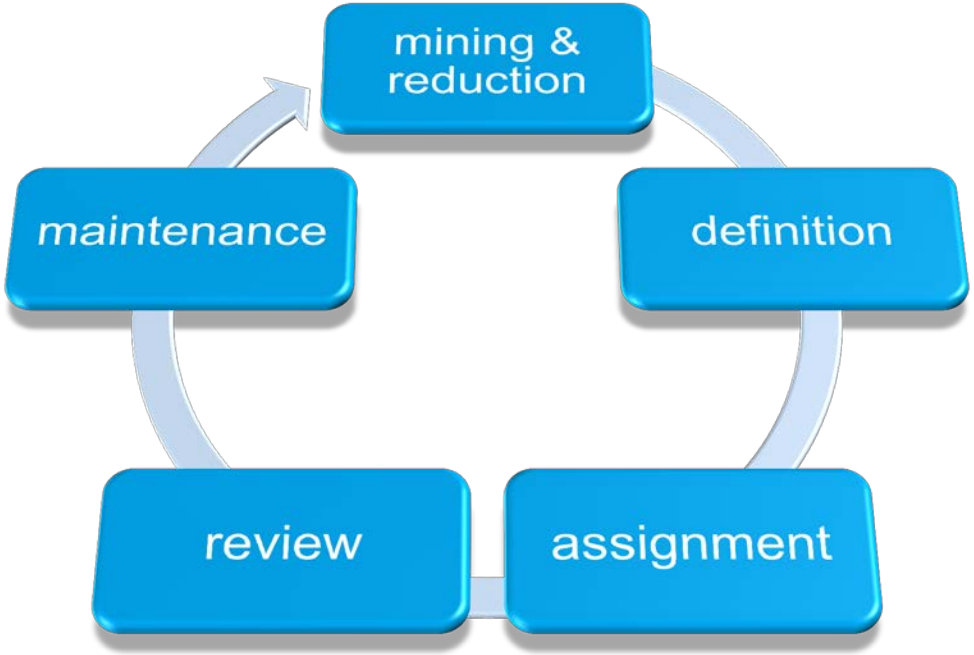
  - ➔ legal requirements: people equipped with a dosimeter have to be uniquely identified for at least 30 years; think “birthday” and “place of birth”
  - ➔ who is allowed to see which kind of personal data? Legal requirements are very strict, esp. when people have no direct working contract with DESY; e.g. pre-registration of personal data from people of other institutes before it is known that they will get a dosimeter. What data may be checked looking for duplicates during registration? Can one deduce restricted data?

roles and their management

- roles are bound to
  - job function – e.g. “team lead”
  - processes – e.g. “initiator of a meeting”
  - technical systems – e.g. within SAP HCM / ERP with a plethora of intrinsic roles
- it is planned to
  - provide roles which are used on more than one technical system
  - have individual roles; this is more like an attribute to a person
  - derive roles within processes by using business roles (e.g. “supervisor of this group”)
  - assign roles within dedicated systems to (a) business or process role(s)
    ➔ no duplication of the intrinsic role management of existing systems, like SAP
  - where there are no roles in technical systems, role assignment boils down to group assignments; e.g. NTFS knows about rights of groups per file system object. The owner of the data has to take care, which roles should have which kind of access but should be assisted in knowing which group corresponds to which role(s)

roles and their management – role lifecycle management

- again BPM comes in handy
- manage role assignment
- mange role lifecycle
- helps keeping an overview what is (or was) active in connected systems



Procurement procedure

- Preparation started 18 months ago
- collecting the more abstract requirements and some technical ones
- chained procedure
  - call for tenders started at the end of 2012
  - invitation of tenderers for a presentation
  - preparation of benchmarks for the remaining (best) tenderers
  - benchmark execution: two days for each tenderer
    NB: benchmarking in this cases delivers scores for a comparison between candidates
- cross-sectional selection of DESY participants over user groups
- questionnaire for all DESY participants were handed out for each “visit” of a tenderer ➔ only the “best” managed it to get into the next round
- there is no singular value to find out, what is “best”, as you could optimize for UI, functions, integration, operation, …
  ➔ pursue a consensus between all DESY participants

BPM & IAM – COTS ?

- BPM
  - commercial off the shelf is available ☺
- IAM
  - most systems are more an account provisioning system than an identity management system
  - esp. identity lifecycle management aspects (ILM) are not comprehensively covered

    ➔ there will implementation work done by ourselves

    ➔ the IAM framework should provide “enough” functionality
- IAM is a prerequisite for the BPMS
- the BPMS is a prerequisite for the IAM

questions & answers

thank you for your attention