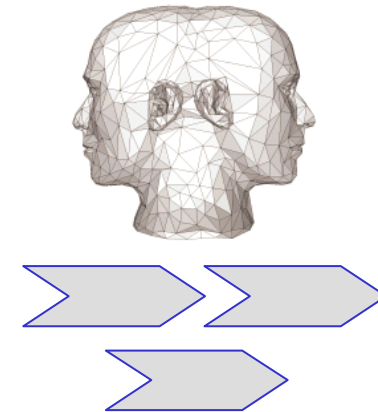


# GenericIAM

generic processes for Identity- & Access  
Management

An introduction to be presented at the  
joint conference of enisa with EEMA on eldentity,  
12-13 June 2007  
at the Radisson SAS, Paris CDG Airport



Version 0.2

# By this presentation we explain ...



- ↳ **Why** we started the initiative GenericIAM – our Motivation,
- ↳ **Where** it will lead us **to** – The objectives of the initiative,
- ↳ **Who** are the Members of GenericIAM and their experiences,
- ↳ **How** we work,
- ↳ **What** the input we receives and the results will deliver and
- ↳ **When** will we come up with substantial results

↳ **Why?** – Motivation for GenericIAM

↳ **Where to?** – The objective of the initiative

↳ **Who?** – Members of GenericIAM and their experiences

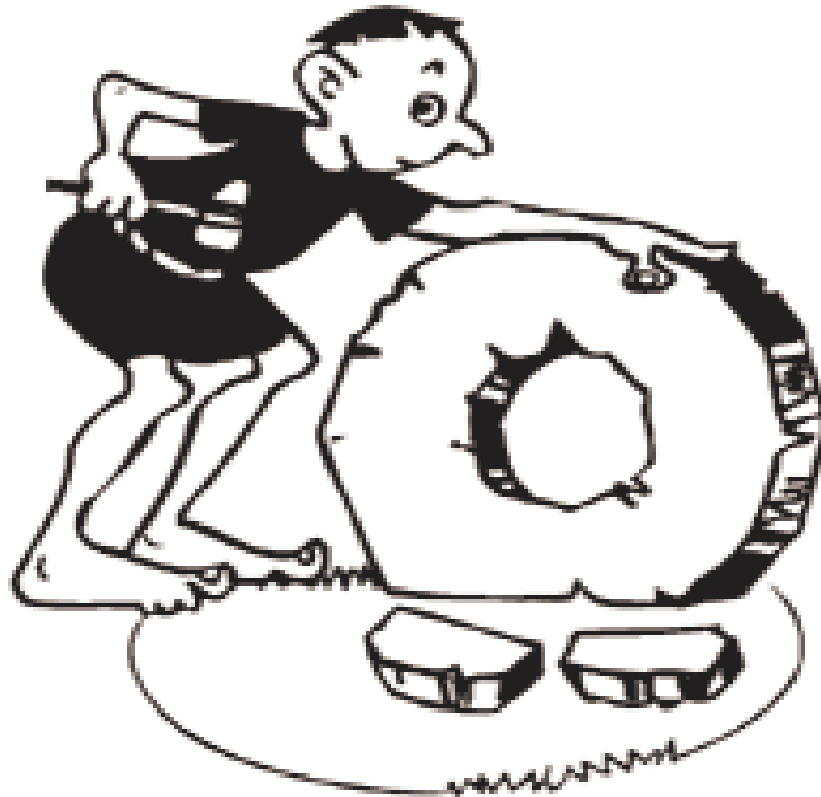
↳ **How?** – How we work

↳ **What?** – input & results

↳ **When?** – Yesterday, today and tomorrow

## Our motivation

**Wanted:** a construction kit for standard processes within IAM



The idea behind GenericIAM

- ⤵ The definition of IAM-processes cause major effort.
  - According to experience they account for up to 2/3 of the overall effort.
  - Nevertheless a core set of standard processes remains remarkable stable.
- ⤵ Aren't there considerable similarities?
- ⤵ Why start with a blank sheet of paper?
- ⤵ Why reinvent the wheel again and again?
- ⤵ Shouldn't we concentrate our efforts on the differences?
  - ... and use the common set of standard processes "of the shelf"?
  - ... from "GenericIAM"?

- ↳ *Why?* – Motivation for GenericIAM
- ↳ *Where to?* – The objective of the initiative
- ↳ *Who?* – Members of GenericIAM and their experiences
- ↳ *How?* – How we work
- ↳ *What?* – input & results
- ↳ *When?* – Yesterday, today and tomorrow

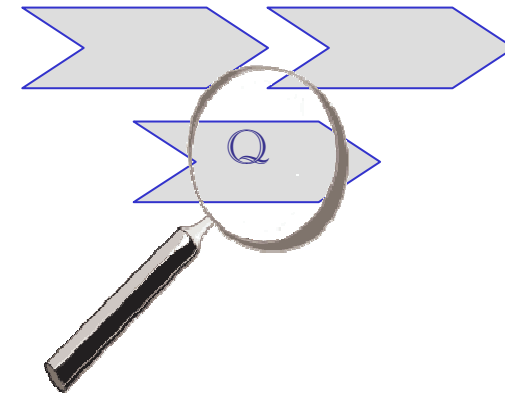
- ↳ Mission  
which goals are we aiming at?
- ↳ Target Group  
Who should be interested in GenericIAM?
- ↳ Benefits ...  
stakeholders will gain benefits from generic IAM processes
- ↳ Context  
the industrialisation of the service sector

# Mission

which goals are we aiming at?



- ☞ It is our **objective** to define a multi-purpose generic **process model** for the Identity- & Access Management (IAM)
- ☞ The process model may **serve as a template** for enterprise specific processes.
- ☞ Occasionally, it will be implemented unmodified.
- ☞ The processes shall be of an appropriate **high level of quality**.
- ☞ They shall be to in line with regulatory **compliance requirements**.



# Target Group

Who should be interested in GenericIAM?



- ↳ GenericIAM may be useful for every enterprise and every individual dealing with Identity- & Access Management.
- ↳ Our core target group comprises of enterprises with IAM processes and systems in place and / or under construction.
- ↳ Together with **vendors, consultants, analysts** and **system integrators** the represent the entire market.
- ↳ This desirable combination promises to deliver high quality and widely accepted results.
- ↳ Representatives of this target group are invited to become members of our initiative GenericIAM.
- ↳ They are expected to make a contribution in **content-, infrastructure-, PR-** and/or **financial** terms to support our objectives.

# Benefits ...

stakeholders will gain benefits from generic IAM processes



## ↳ Implementing enterprises ...

- ↳ will benefit most by receiving a stable set of validated standard IAM processes.
- ↳ They may complement and unify their implemented processes.

## ↳ System integrators and vendors ...

- ↳ Are enabled to deliver pre-built proven and realistic sample process.
- ↳ In turn their clients may reduce modeling costs and project schedules.

## ↳ Project Managers and Consultants ...

- ↳ May start from a foundation of generic standard processes.
- ↳ They can focus on the true enterprise specifics.

## ↳ The entire discipline ...

- ↳ We contribute to the professionalism of the **Identity- & Access Management** in total through an approved and widely used process reference model.
- ↳ We hence **ease the implementation** of policies, processes and IAM systems.

## ↳ GenericIAM members ...

- ↳ Demonstrate their professional IAM process expertise and experience to a broader audience by participating in leading edge standardization activities.

# Context

## the industrialisation of the service sector



- ↳ We believe – we are part of surging wave
- ↳ ITIL, SOA, compliance frameworks are details of a broader picture.
  - ↳ Regulatory compliance enforces the use of infrastructure standards
  - ↳ ITIL is just the beginning – more standardisation is to come.
  - ↳ SOA provides a technical framework for its implementation.
- ↳ Market forces will drive to concentration on core competencies.
  - ↳ non-competitive activities will become standard commodities.
  - ↳ They will be low priced and sourced globally
  - ↳ ... or outsourced / used as a 3<sup>rd</sup> party provided service.
- ↳ Organisational reference models take the development to the next level.
- ↳ GenericIAM as “Open org” may gain an open source like influence.

- ↳ **Why?** – Motivation for GenericIAM
- ↳ **Where to?** – The objective of the initiative
- ↳ **Who?** – Members of GenericIAM and their experiences
- ↳ **How?** – How we work
- ↳ **What?** – input & results
- ↳ **When?** – Yesterday, today and tomorrow

- ↳ Who we are ...  
within the GenericIAM Initiative
- ↳ Current members  
Users, analysts, consultants, vendors and system integrators
- ↳ GenericIAM and the NIFIS  
Competence center „Identity Management“ within NIFIS

# Who we are ...

within the GenericIAM Initiative



## ↳ We are ...

- ↳ a group of volunteers.
- ↳ We are driven by the vision to develop a comprehensive generic process model for Identity- & Access Management.

## ↳ We are from ...

- ↳ various enterprises,
- ↳ consulting companies,
- ↳ analyst corporations,
- ↳ system vendors,
- ↳ system integrators and
- ↳ universities and other academic institutions.

## ↳ Our objective is ...

- ↳ to develop and professionalize the Identity- & Access Management
- ↳ to derive benefit from the participation for our daily work.

# Current members

Users, analysts, consultants, vendors and system integrators



as of 2007-05-13:



- ↳ **Identity- & Access Management** is the essential foundation of an corporate-wide **security architecture**.
- ↳ Identity- & Access Management links technical to organizational tasks.
- ↳ The “National Initiative for Internet Security” (**NIFIS** e.V.) represents a group of enterprises to jointly fight the threats to the internet security.
- ↳ NIFIS acts as a point of contact for questions and issues to solve for all internet security related topics.
- ↳ **GenericIAM** fits perfectly in NIFIS’ objectives and approach.
- ↳ GenericIAM therefore joined NIFIS as **competence center** on December 1, 2006.
- ↳ Despite its national orientation the NIFIS will support GenericIAMs international move.

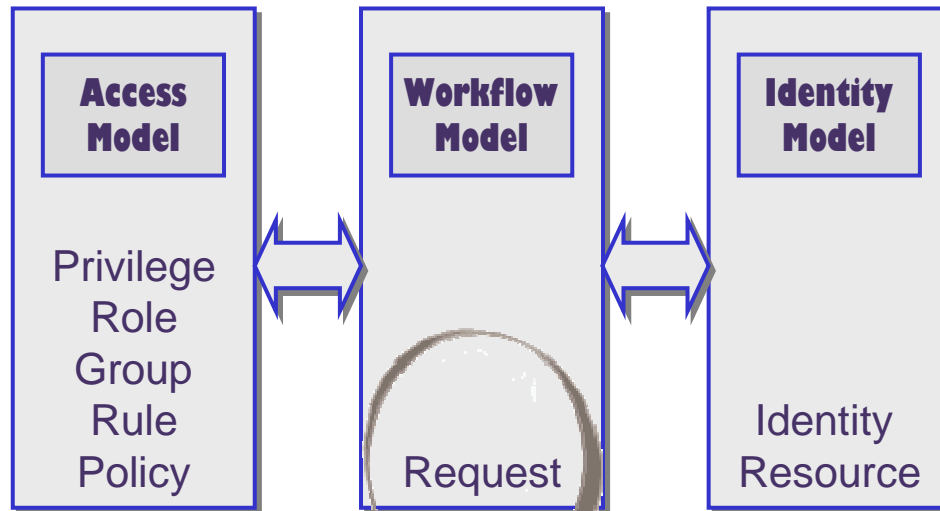
**NIFIS Contact:**  
NIFIS e.V.  
Competence Center  
Identity Management  
Weismüllerstraße 21  
60314 Frankfurt  
Phone: +49 69 40809370  
Fax: +49 69 40147159

- ↳ **Why?** – Motivation for GenericIAM
- ↳ **Where to?** – The objective of the initiative
- ↳ **Who?** – Members of GenericIAM and their experiences
- ↳ **How?** – How we work
- ↳ **What?** – input & results
- ↳ **When?** – Yesterday, today and tomorrow

- ☞ IAM Processes  
Gartner Group defines three groups of IAM processes ....
- ☞ Layers of processes  
how to include generic processes into a process model.
- ☞ Our approach  
From a specific solution to a standardized model
- ☞ Quality Assurance ...  
is an essential part to achieve our objectives.
- ☞ Meetings  
we meet quarterly in person.

# IAM Processes

Gartner Group defines three groups of IAM processes ....



## Access Model:

- Describes a framework for an IAM system
- Major objects are privileges, roles, groups, and policies.

## Workflow Model:

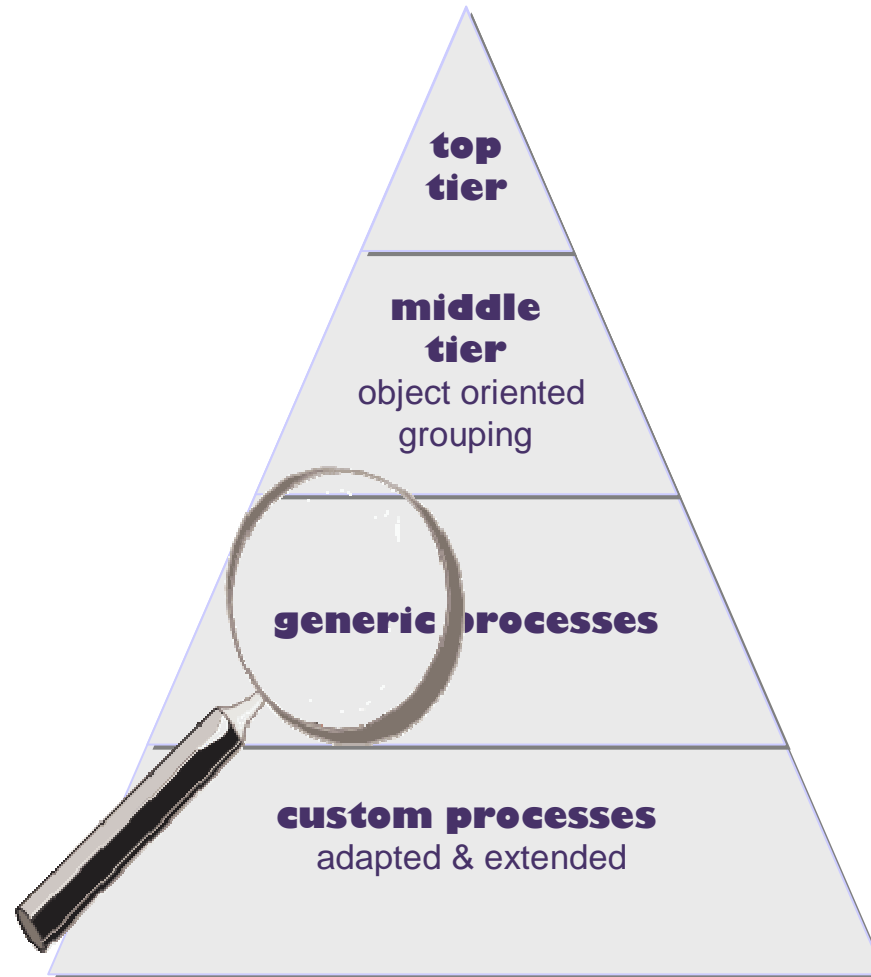
- Access rights, roles and groups have to be granted in a controlled way.
- Application and approval processes are located here.
- The main object is the request.

## Identity Model:

- The Identity Model contains all processes for specific identities or resources.
- The main objects are the identities and resources.
- IAM products implement many of the processes of this model.

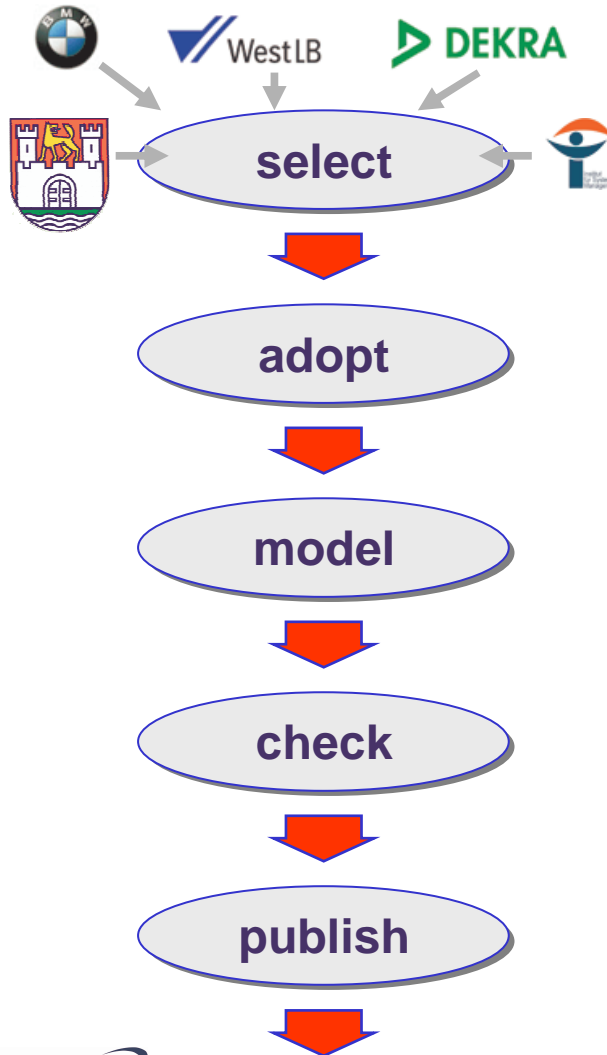
# Layers of processes

how to include generic processes into a process model.



# Our approach

## From a specific solution to a standardized model



- Enterprises contribute their IAM processes
- These processes are processed to the generic process model.
- They usually don't add to their competitive advantage.

- Enterprises may hand over their models in various formats.
- NDA's will be signed on request.
- The modeling team selects the generic process candidates.

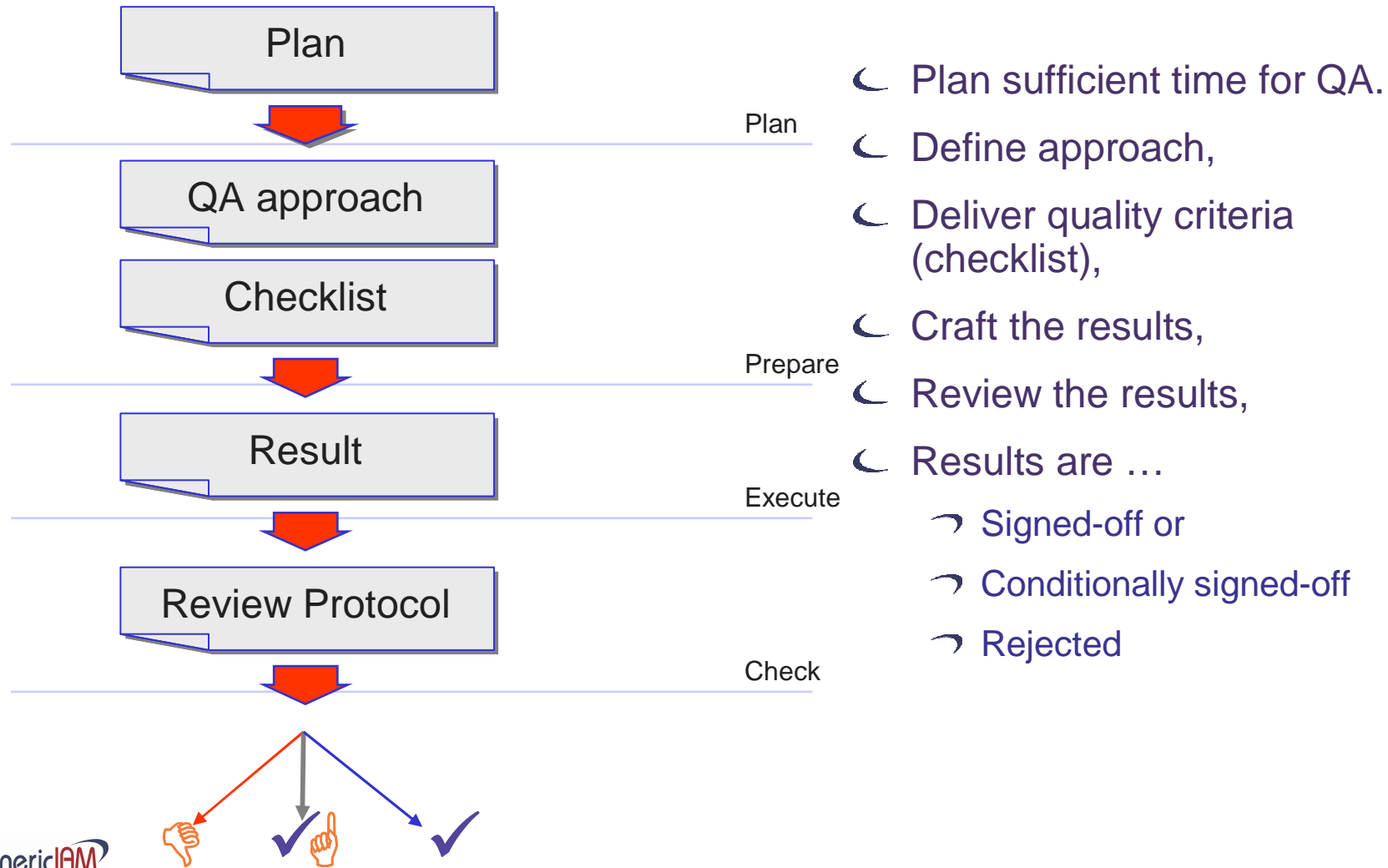
- The processes are anonymized to remove enterprise specific terms.
- They are standardized through naming and modeling conventions.
- They are generalized to take advantage of standard roles.

- The results will be checked by our review team.
- The generic processes will be formally signed off for publication
- Reviewers are GenericIAM- and occasionally external experts.
  - They release only defect-free processes.
  - The modeling team will remedy deficiencies

- The process model will be published annually.
- Members of GenericIAM will get them free of charge.
- Interested parties can purchase the process model.



# Quality Assurance ... is an essential part to achieve our objectives.

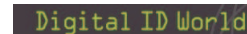


# Meetings

we physically meet once per quarter.



- ↳ We hold quarterly one day meetings at a member's location.
- ↳ We discuss and sign-off results during these meeting.
- ↳ We defined and assign new tasks and decide next steps.
- ↳ Meeting minutes document the meeting decisions.
- ↳ Previous meetings were...
  - ↳ 2006-04-25, Frankfurt, host: Kuppinger, Cole + Partner
  - ↳ 2006-06-20, München, host: Kuppinger, Cole + Partner
  - ↳ 2006-09-27, Wiesbaden, host: Digital ID-World
  - ↳ 2006-12-01, München, host: ORACLE
  - ↳ 2007-03-02, Düsseldorf, host: WestLB AG
  - ↳ 2007-05-07, München, host: EIC 2007



- ↳ **Why?** – Motivation for GenericIAM
- ↳ **Where to?** – The objective of the initiative
- ↳ **Who?** – Members of GenericIAM and their experiences
- ↳ **How?** – How we work
- ↳ **What?** – input & results
- ↳ **When?** – Yesterday, today and tomorrow

- ☞ Process model  
basic processes
- ☞ Terms and sorting  
process identification and classification
- ☞ Process list  
the first 10 processes of our model
- ☞ An Example  
generic process “Hire employee”

# Naming and order

process identification and classification



- ↳ Processes are identified by an **unique identifier (ID)**
- ↳ Processes are assigned to one of the following categories ...
  - ↳ Access Model (**AM**)
  - ↳ Workflow Model (**WM**)
  - ↳ Identity Model (**IM**)
- ↳ Processes are numbered with two numbers within the categories.
- ↳ Category and numbers form the four-digit unique **process ID**.
  - ↳ Example: IM47

# Process list

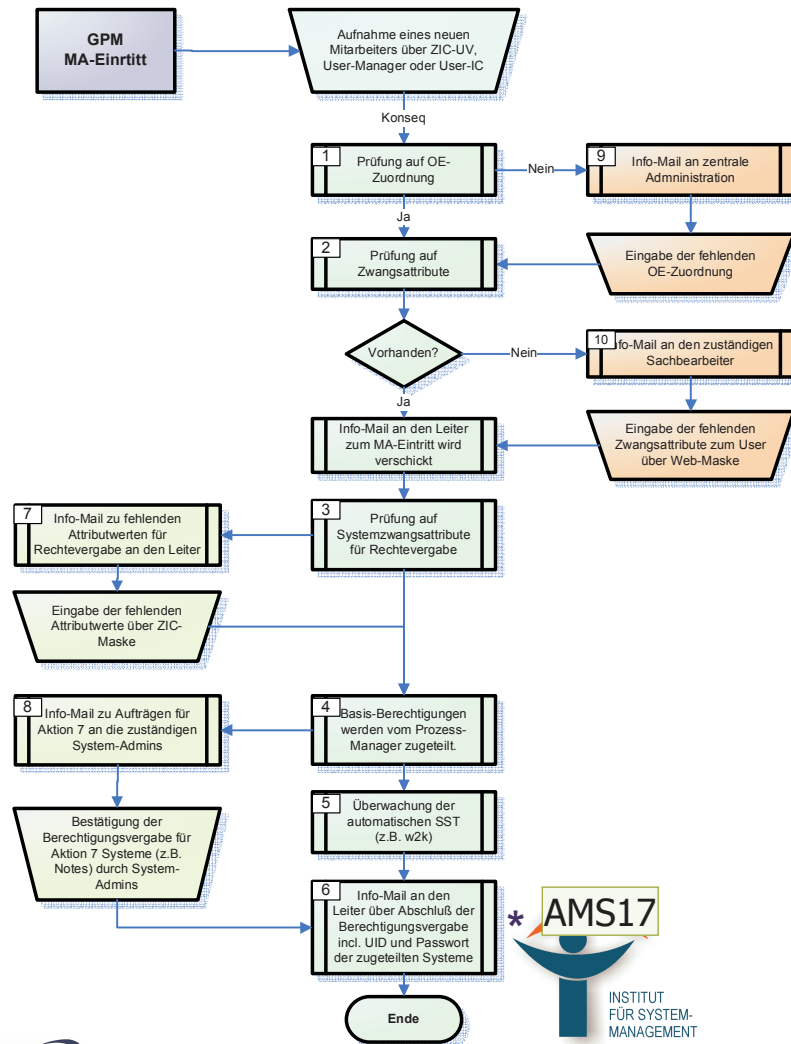
1<sup>st</sup> processes - anonymized, standardized but not generalized



- ↳ **hire employee**  
describes the entry of an employee in an organization.
- ↳ **release employee**  
describes the scheduled or unscheduled leaving of an employee.
- ↳ **logout globally**  
terminates immediately all started and current application sessions.
- ↳ **sack globally**  
describes the immediately locking of the employee's access rights to enterprise resources (as an exception).
- ↳ **re-certify**  
describes a periodic process during which someone has to confirm the current access rights of a subject to a resource.
- ↳ **certify**  
with this process the compliance of products and services to standards is confirmed.
- ↳ **clean data**  
describes the process of finding and cleansing inconsistent, fragmentary and redundant IAM data.
- ↳ **request account**  
describes how to request and approve access to an IT system.
- ↳ **request roles**  
describes how to request and approve a role.
- ↳ **request groups**  
describes how to request and approve a group.

# Input-Example

## non-generic process “Hire employee”



- ☾ If an employee is not assigned to a business unit:
  - ☞ Inform the central administration.
- ☾ If the necessary user attributes are not known:
  - ☞ Identify and inform the corresponding official.
  - ☞ Insert missing user attributes.
- ☾ If necessary system attributes are not known:
  - ☞ Inform recipient, e.g. manager
  - ☞ Insert missing system attributes.
- ☾ Assign basic access right automatically via basic roles.
- ☾ Assign logon name for systems automatically according to name generating rule.
- ☾ Create privileges within systems automatically (user provisioning) or via mail to system administrator. AM
- ☾ Technical monitoring of the connectors
- ☾ Inform manager about employee’s privileges.

## Folie 27

---

**AMS17** Hier gibt es sicherlich von iSM schon eine englische version, die man einfügen kann. Wenn nicht, kann ich die Texte noch verallgemeinern (da produktbezogen und nicht "generisch") und übersetzen.

Dr. Angelika Steinacker, 05/05/2007

**AMS18** Hier habe ich nicht verstanden, welche "Output-Connectoren" gemeint sind und warum diese (von wem?) überwacht werden sollen. Deshalb habe ich den Satz nicht übersetzt.

Dr. Angelika Steinacker, 05/05/2007

- ↳ **Why?** – Motivation for GenericIAM
- ↳ **Where to?** – The objective of the initiative
- ↳ **Who?** – Members of GenericIAM and their experiences
- ↳ **How?** – How we work
- ↳ **What?** – input & results
- ↳ **When?** – Yesterday, today and tomorrow

# History & Orientation

Starting small & national, acting globally.



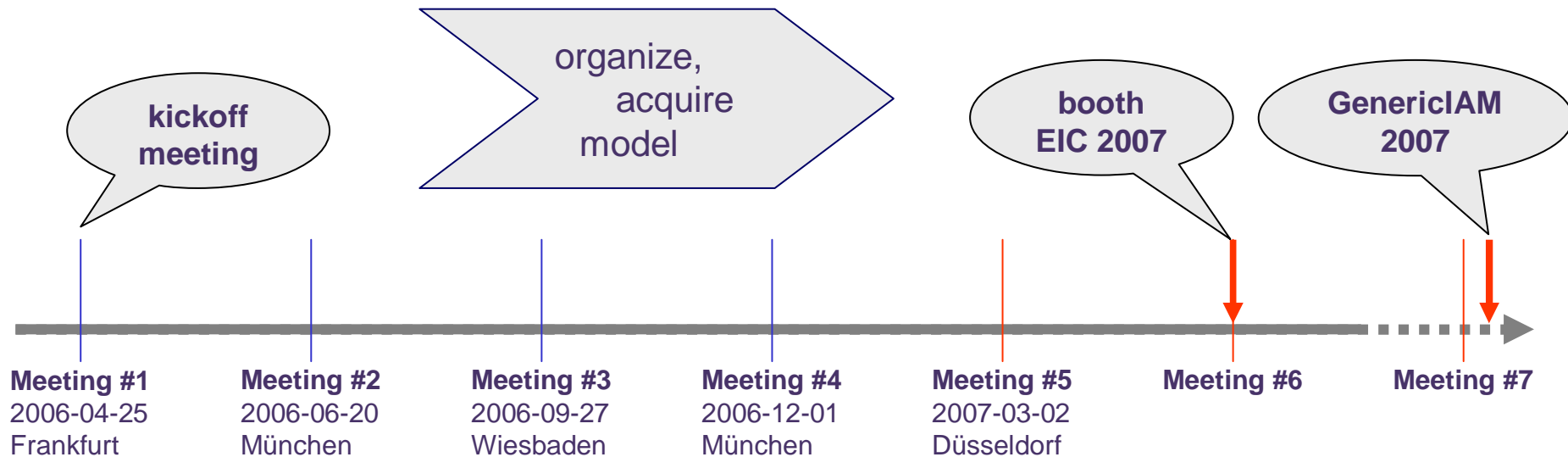
- ↳ GenericIAM started in Germany in May 2006.
- ↳ GenericIAM is set up as a competence center within **NIFIS** e.V..
- ↳ After one year (~ May 2007) we decided to internationalize our work.
- ↳ We synchronized our activities with **The OpenGroup** so far.
- ↳ We are in talks with several other standardization bodies and focus groups: ITU-T, enisa, more ...
- ↳ Our first results will be delivered in autumn 2007.
- ↳ From then on we will publish them yearly.
- ↳ An appropriate success provided, we will feed our results to an established international standardization body.

# When?

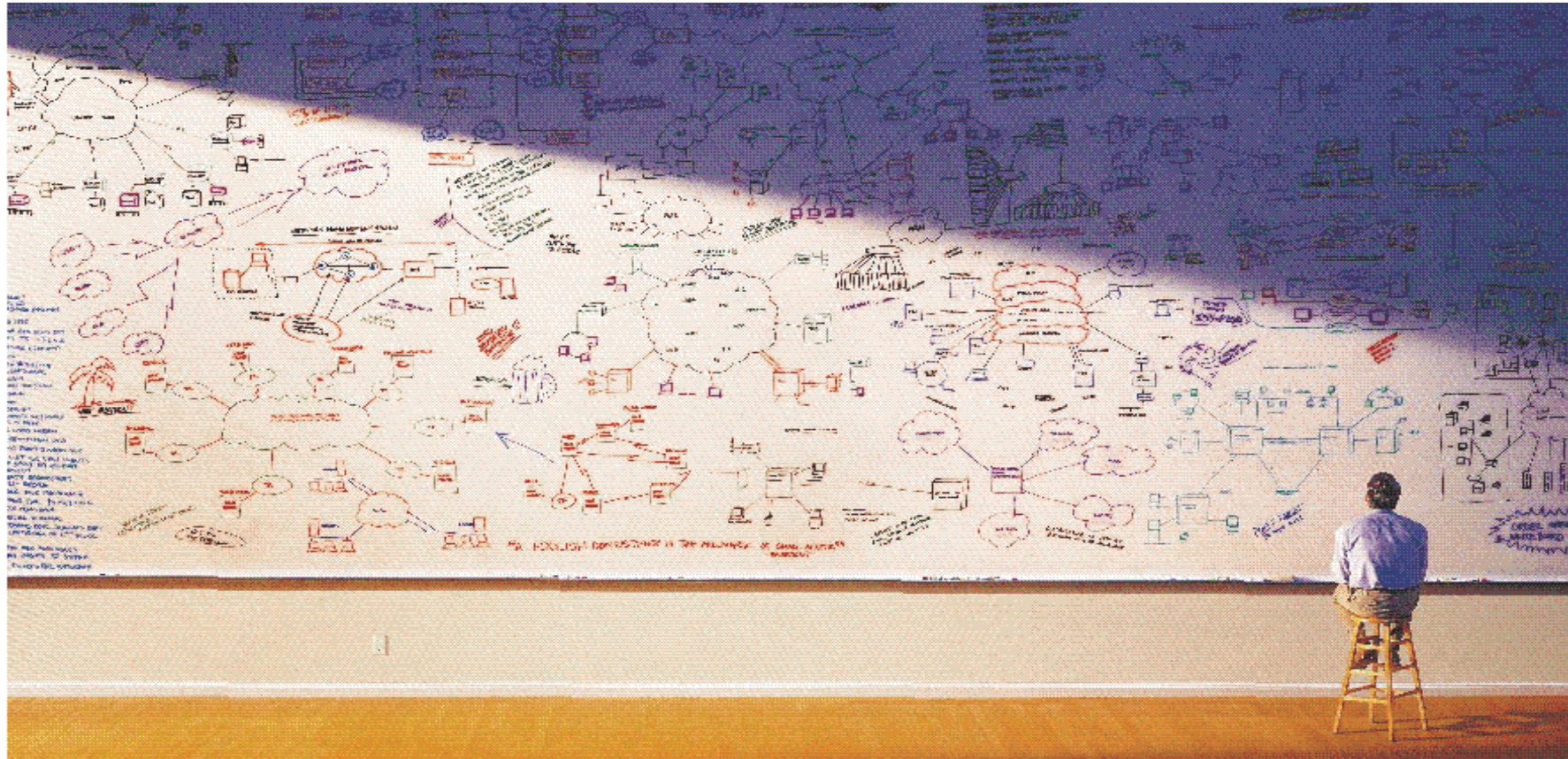
Yesterday, today and tomorrow



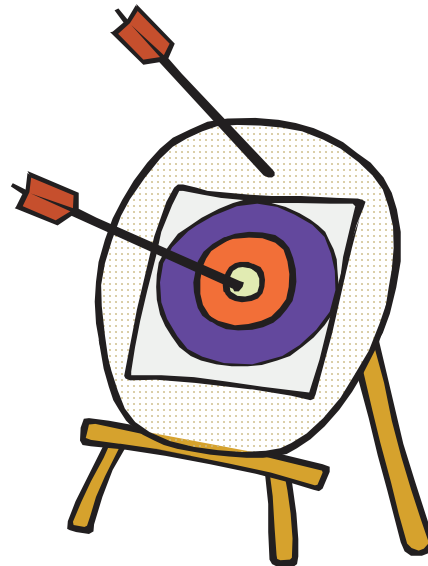
- ⤵ We met for the first time in Q1/2006 triggered by a call for meeting published in a Kuppinger, Cole + Partner newsletter.
- ⤵ Since then we meet quarterly.
- ⤵ We will deliver the first results in Q3/2007.



# Questions – Comments – Suggestions?



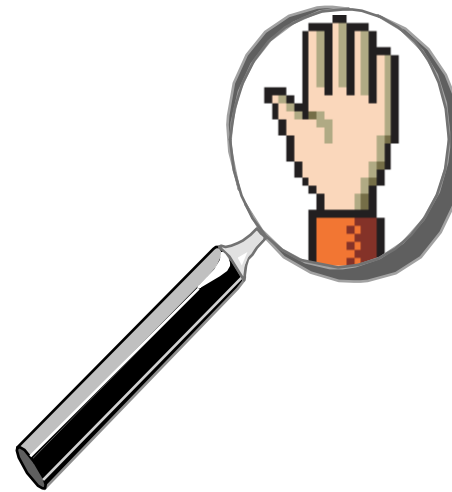
The end ...



Thank you very  
much for your  
attention!

In case of any questions:  
[horst.walther@nifis.org](mailto:horst.walther@nifis.org),  
skype: HoWa01

VoIP: +40 40 414314453



**A**ttention

**B**ackup slides