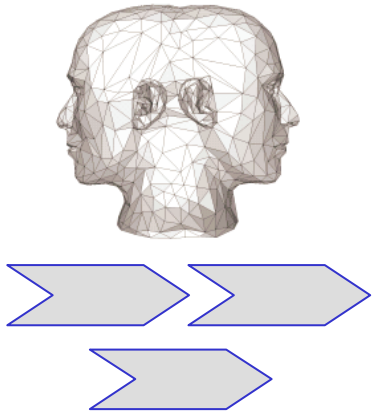
GenericIAM

generic processes for the
Identity- & Access Management



7th Meeting, 2007-06-29

Munich, CSC IT Management & Security,
Sandstr. 7-9 • 80335 München

Version 1.0

Agenda

- 09:00 welcome - housekeeping – new members introduction
- 09:15 meeting minutes from 2007-03-02 and 2007-05-07
- 09:45 assignments from last 2 meetings
- 10:15 activities report WG Organisation (Horst Walther)
- 10:45 activities report WG Presentation (Horst Walther)
- 11:15 activities report WG Modelling (Andreas Netzer)
- 12:30 --- lunch break ---
- 13:00 activities report WG Validation (Angelika Steinacker)
- 13:30 activities report TF Compliance (Norbert Boß)
- 14:00 Next steps, planning of Workgroup meetings, next regular meeting, assignments, Please feel free to propose additional topics to the agenda if necessary.
- 17:00 End

confirmend participants

- CSC Deutschland Solutions GmbH (Goswin Eisen)
- CSC Deutschland Solutions GmbH (Dr. Angelika Steinacker)
- CSC Deutschland Solutions GmbH (Wolfgang Zwerch)
- ConSecur GmbH (Arslan Brömme)
- ConSecur GmbH (Norbert Book)
- Covisint a subsidiary of Compuware Corporation (Dr. Friedel Vogel)
- IBSolution GmbH (Markus Kunkel)
- iC Compas GmbH & Co KG (Andreas Netzer)
- Johann Wolfgang Goethe University Frankfurt Main (Denis Royer)
- KPMG (Marko Vogel)
- Siemens Enterprise Communications GmbH & Co. KG (Hanns Nolan)
- SiG Software Integration GmbH (Horst Walther)
- Völcker Informatik AG (Peter Weierich)

no participation

- accenture (Stefan Sulistyo)
- Beta Systems AG (Roland Awischus)
- Berliner Volksbank (Holger Nahrgang)
- DEKRA e.V. (Martina Hendricks)
- doubleSlash Net-Business GmbH (Oliver Belikan)
- doubleSlash Net-Business GmbH (Matthias Neher)
- First@ttribute GmbH (Jens Petersen)
- IDS Scheer AG(Britta Hilt)
- it-advisory.com (sabine.burba)
- firstAttribute (Joerg van gen Hassend)
- Kuppinger, Cole + Partner (Martin Kuppinger
- NIFIS (Peter Knapp)
- NIFIS (Volker Ludwig)
- Novell Austria (Matthias Schabl)
- Novell GmbH (Michael Lang)
- Siemens Enterprise Communications GmbH & Co. KG (Bernd Hohgräfe)
- SUN Microsystems GmbH (Norbert Boss)
- Syntlogo GmbH (Dr. Giovanni Barruzi)
- Thoranet GmbH (Octavio Brito)
- Unternehmensberatung Nicole Kleff (Nicole Kleff)

no response

- BMW Group (Doerte Neundorf)
- iSM-Institut für System-Management GmbH (Holger Görz)
- iSM-Institut für System-Management GmbH (Prof. Dr. Dr. Gerd Rossa)
- ORACLE Deutschland GmbH (Heike Jürgensen)
- Peak Solution GmbH, Dr. Hans-Jörg Kremer
- Trivadis (Juergen Kuehn)
- UMIT, Institut für Informationssysteme des Gesundheitswesens (Roland Blomer)
- WestLB AG (Manfred Hübner)

housekeeping

- agenda
- breaks,
- smoking,
- Mobiles,
- minutes,
- Presented contributions, results,
- Workshop nature,
- ...

The (new) members introduce themselves
3 – 5 Minutes per Person

- Who I am?
- Where I come from?
- What exposure I have to IAM?
- Why I came here?
- What I may contribute?

Report from the WG Organisation / next steps
(Horst Walther)

- “sponsorship” & booth on the EIC 2007 + short meeting (but no contribution!)
- blog (http://blog.genericiam.org/)
- Web-Site (www.genericIAM.org) translated into English language
- New members since 2007-05-07: Denis Royer, Markus Kunkel (?)
- Public relations
  - On June 12th and 13th I had the chance to present our initiative GenericIAM on the joint conference of the enisa and the eema.
  - My comments have been quoted in the Publication "securely manage identities" in „IT im Unternehmen“, 6-2007 → hints GenericIAM
  - With number 23, June 8th, we started a series of articles about digital identity in the IT-Newspaper "Computerwoche". The first part was published on page 28/29 with the headline "No integration without digital identities". Three more articles will follow. → hints GenericIAM
  - Presentation on the 1st NIFIS-forum on applied information security
- Conclave Workshop on June 27th-28th (see slides)

Additional topics

- Using the ARIS-Licences?
- Modelling progress
- Legal framework under GPLv3 ?
- Holger Nahrgang (Berliner Volksbank) has submitted his Master thesis (100 pages) „A pattern based reference model for the IdM“
- Speakers of the working groups.
  - Modelling - Andreas Netzer
  - Validation – Angelika Steinacker
  - Presentation – Octavio Brito (new representative needed)
  - Organisation – Horst Walther
- Next meeting

Members of the working groups
each group determines a speaker (s) and his deputy (d)

Modelling
- Roland Awischus
- Giovanni Baruzzi
- Oliver Belikan
- Norbert Boss
- Holger Görz
- Nicole Kleff
- Matthias Neher
- Andreas Netzer (S)
- Gerd Rossa
- Peter Weierich

Validation
- Jürgen Kühn
- Martin Kuppinger (D)
- Angelika Steinacker (S)
- Marko Vogel

Presentation
- Arslan Brömme (S)
- Octavio Brito
- Martin Kuppinger
- Horst Walther (D)

Organisation
- Horst Walther (S)
- Friedel Vogel (D)

ToDo‘s

„Who will do what & until when?“

- Validation of the actual **A**pprove-**R**equest-**P**rocess
- Extend the ARP to include missing components
  - Provisioning
  - Role Constraints
  - Additional Detail Levels
- General Definition of underlying role model
- Checking which processes are able to map to the ARP
- Define Process Models for non-mapable processes
- Verbal Description of the ARP
- Additional levels of description
  - Additional presentation formats for „selling“ the results.
  - More detailed level for the formal standardization process (DIN, etc)

Decisions

- Agree to the principal idea of modelling (usage of a Petri-Net)
- Going Public with the first model (after validation) via NIFIS
- Presentation at the next congress

Closing

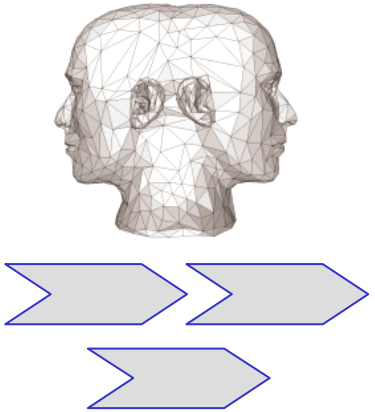
- Feedback
  - How did you the Meeting?
    - contents - schedule – Location – Moderation - Participation
  - Are we still on the right way?
  - Are there modifications necessary to our direction?
  - Do you believe, that we will be successful in the end?
  - Which changes should we apply to our approach?

Questions - comments – suggestions?

NIFIS

GenericIAM

generic processes for the
Identity- & Access Management



Conclave workshop

2007-06-27 – 28

Arslan Brömme • Andreas Netzer • Horst Walther

Benediktinerabtei zum Hl. Kreuz
Schyrenplatz • 1 85298 Scheyern

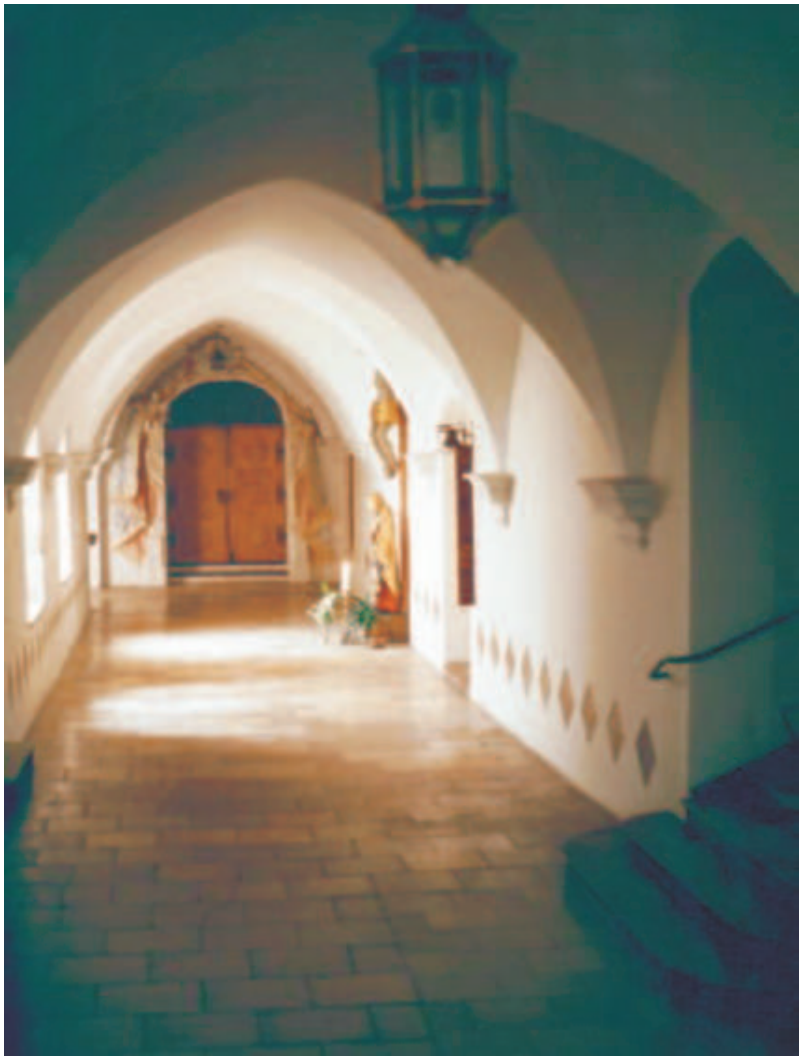
Version 1.0

- Start: Wednesday, 2007-06-27, 09:00
- End: Thursday, 2007-06-28, 17:00

- Despite the fact, that the location offers some leisure time facilities, the major focus will be intensive modelling work. ;-)
- Each participant should be prepared to contribute appropriately. Personal tasks will be assigned in bilateral talks with registered attendees.

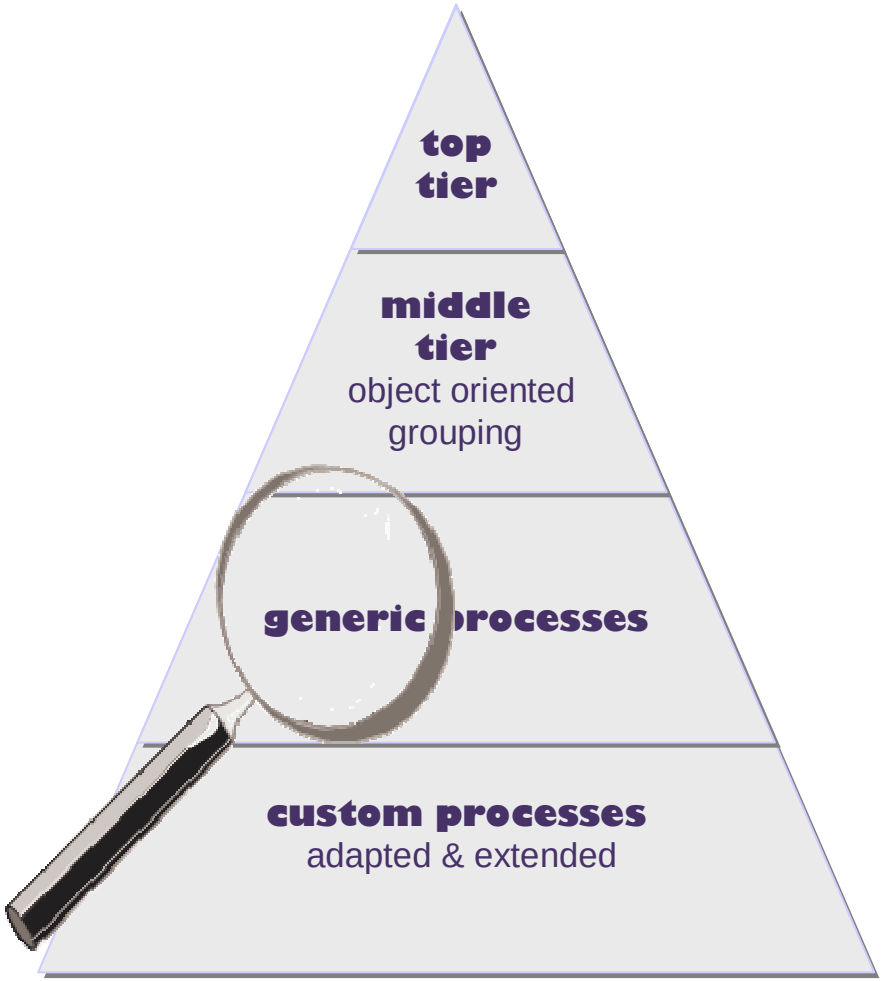
The location
Kloster Scheyern

- Location
  - Benediktinerabtei zum Hl. Kreuz
  - Schyrenplatz 1
  - 85298 Scheyern
- Telefon:
  - 08441/ 752 - 0 (Klosterpforte)
  - 08441/ 752 - 230 (Klosterverwaltung)
  - 08441/ 752 - 181 (Kath. Pfarramt)
- Async contacts
  - Telefax: 08441/ 752 - 210
  - e-mail: info@kloster-scheyern.de
  - http://www.kloster-scheyern.de/
- Room prices are ~ 30 € per night.
- Additional costs (e.g. conference room) where sponsored by iC Compas.



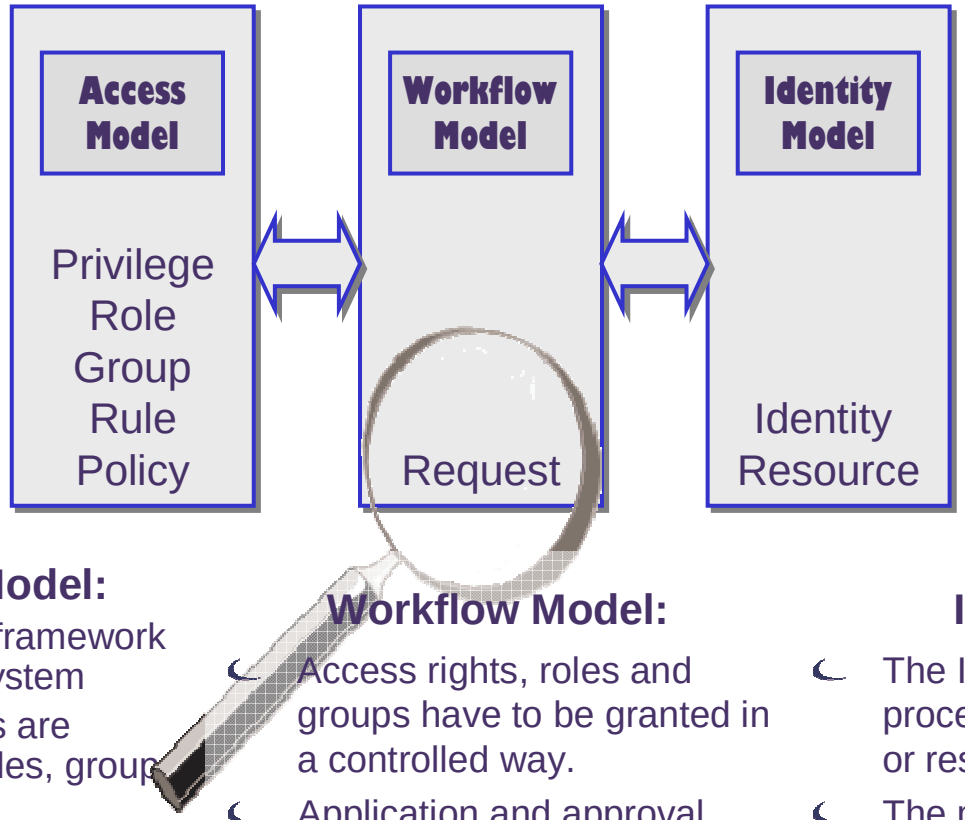
Layers of processes

how to include generic processes into a process model.



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:

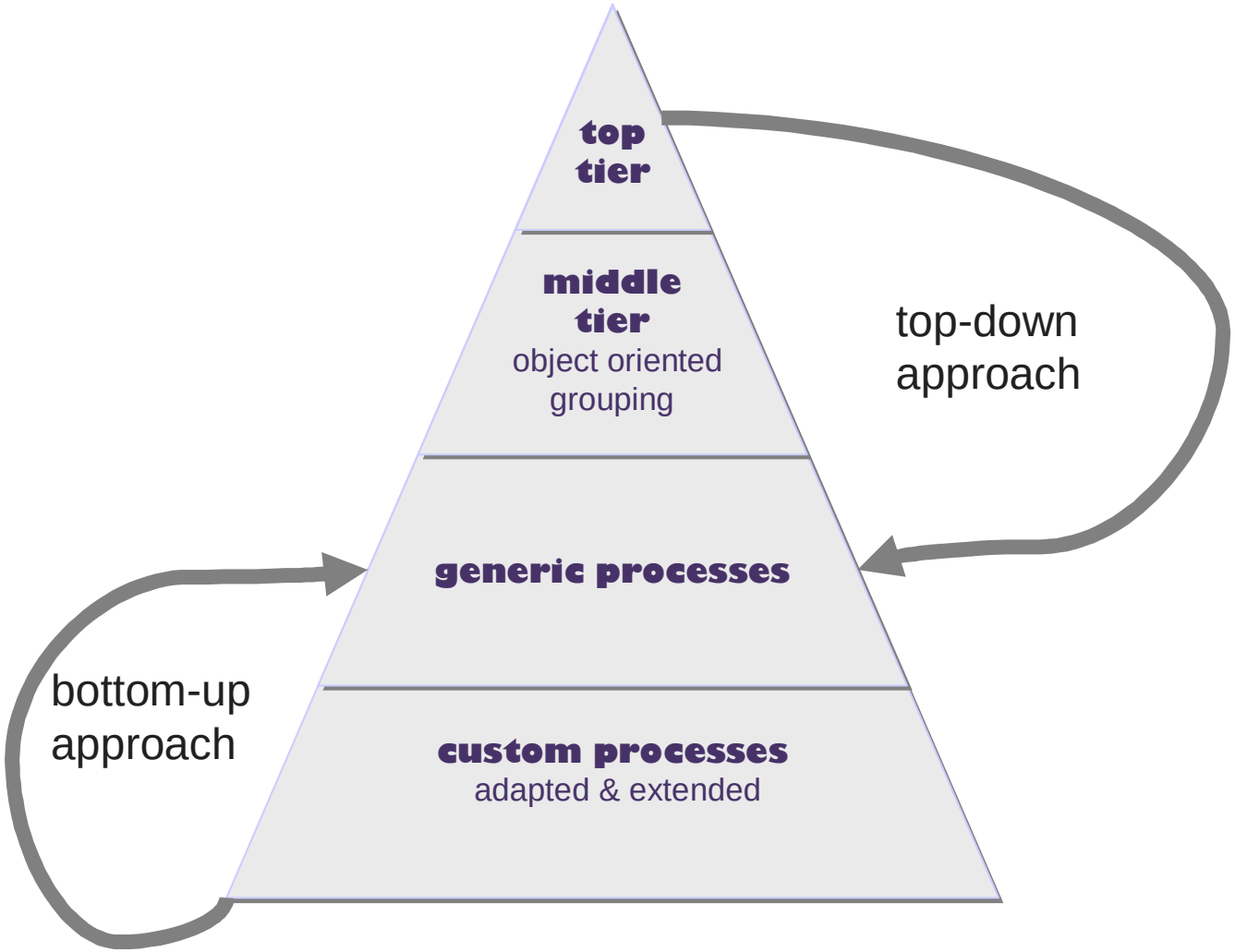
- Access rights, roles and groups have to be granted in a controlled way.
- Application and approval processes are located here.
- The main object is the request.

Identity Model:

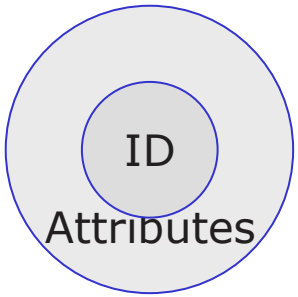
- The Identity Model contains all processes for specific identities or resources.
- The main objects are the identities and resources.
- IAM products implement many of the processes of this model.

Modelling approach

bottom-up- and top-down-approach lead to one generic model



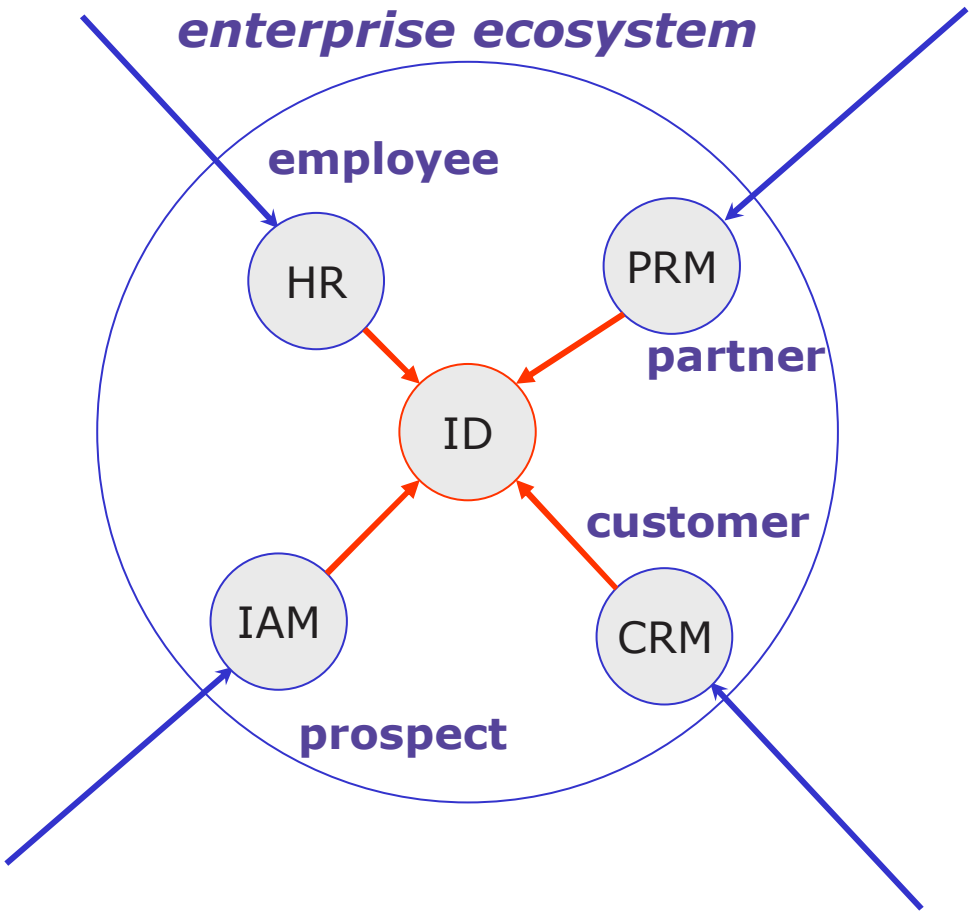
The Identity
and its “less rich” sibling the digital identity



- Identity is the fundamental concept of identity management
- In philosophy Identity is the sameness of two things.
- In object-oriented programming Identity is a property of objects that allows the objects to be distinguished from each other.
- But in Identity Management …
  - “*We usually speak of identity in the singular, but in fact subjects have multiple identities*.”
  - “*These multiple identities or personas, as they are sometimes called, …*”.
- The sum of all these Personas makes up the identity.
- In turn personas are to be understood as its projection to the space of information demand in a specific context.
- Biometrics ties the digital identity to the real world physical identity.

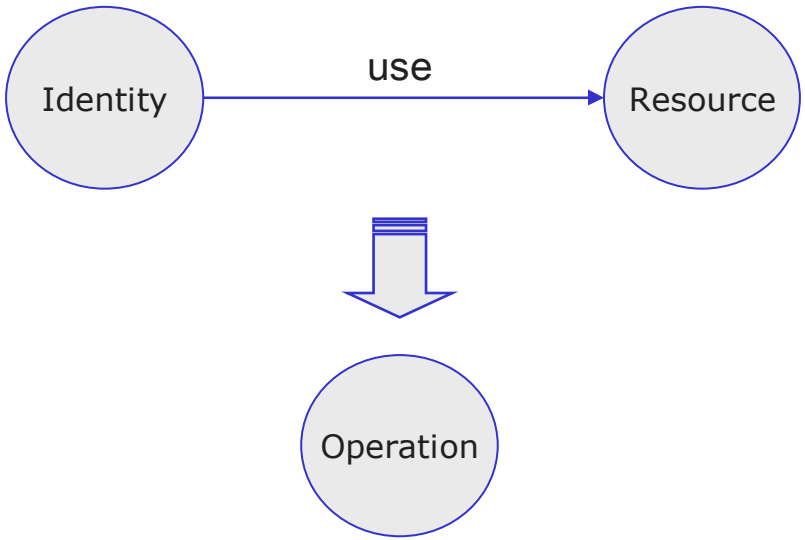
The central digital identity

whenever an individual enters the enterprise ecosystem first time …



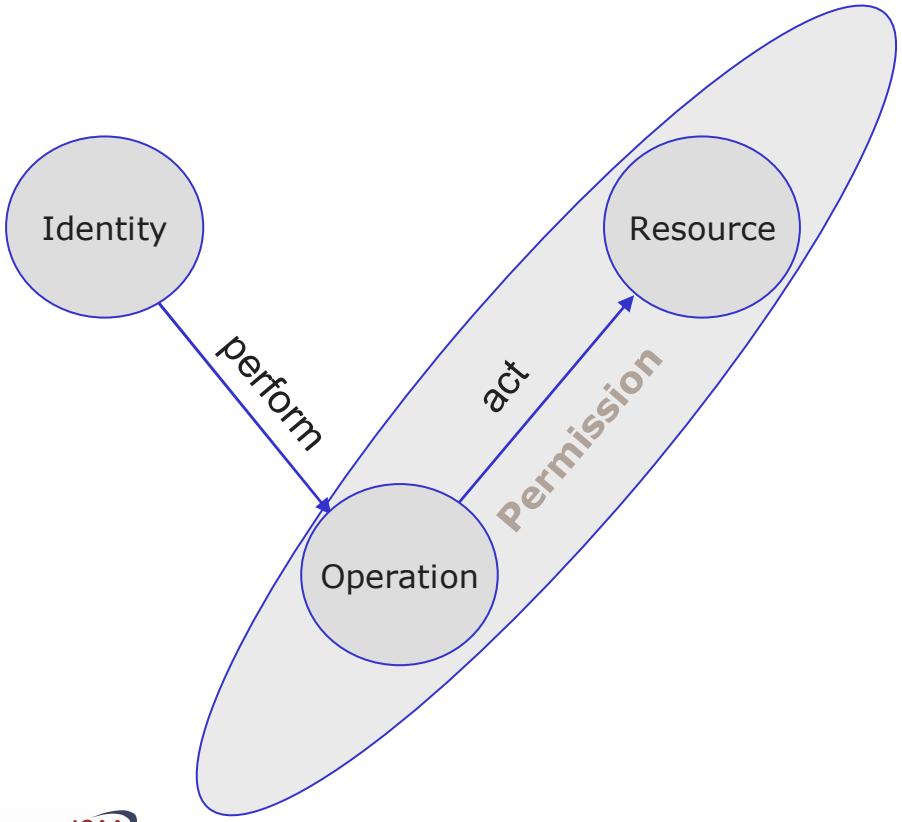
- Its digital identity is created whenever an individual enters the enterprise ecosystem 1st time.
- Regardless if it is a user or not
- Being a *user* represents a class of roles already
- The digital identity is the individuals digital sibling.
- Its lifetime is determined by the lifetime of the enterprises interest.
- The digital identity is global and unique
- It carries the minimal identifying attributes.

The Identity uses a Resource



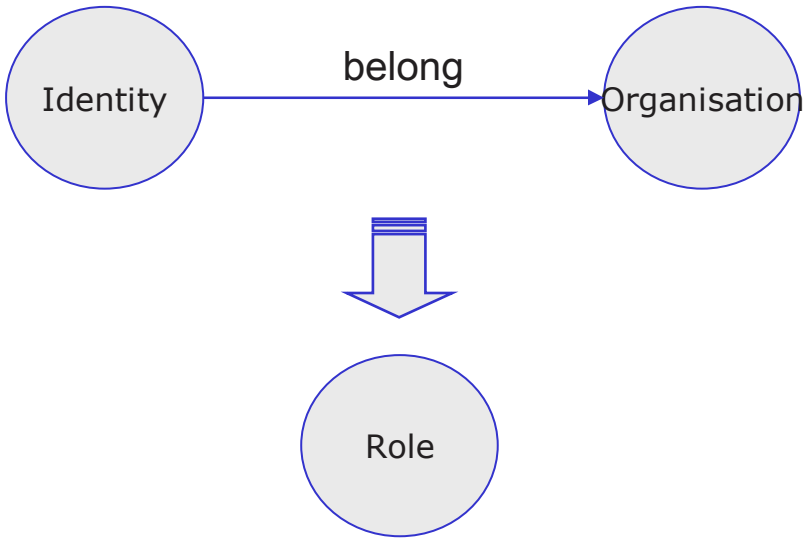
- Identities are often tied to resources
- They „use“ resources
- They do so by performing operations
- This relations may carry attributes
- It turns to a derived object: the user.

Permission = Operations on Resources



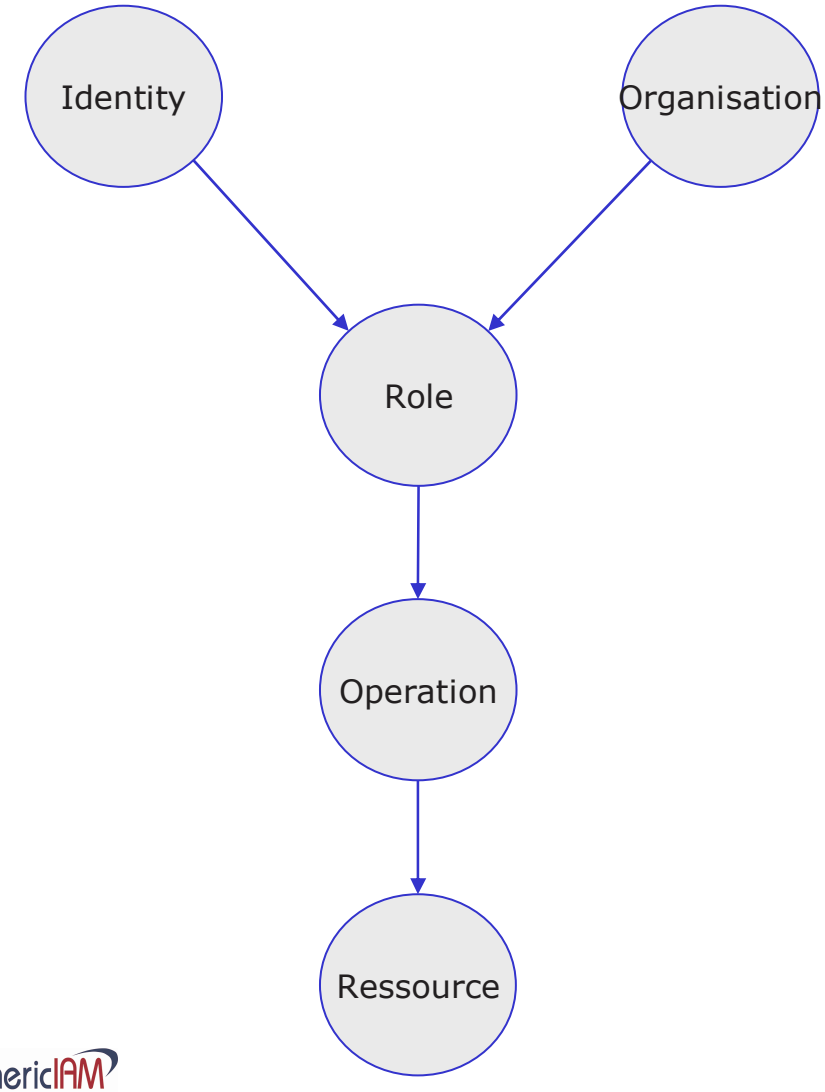
- The Identity performs an operation
- The operation acts on the resource
- Operations on resources (objects) may be labelled with “permissions”.
- Permissions are elementary
  - They are simple by definition
  - There may be a large number
  - There is a limited set of permissions

The Identity belongs to an organisation



- The Identity has a relationship to an organisation
- There are many specialisations to this relationship
- There might be more than on relationship
- This relationship may carry attributes
- It turns to a derived object: the role.

The Identity belongs to an organisation



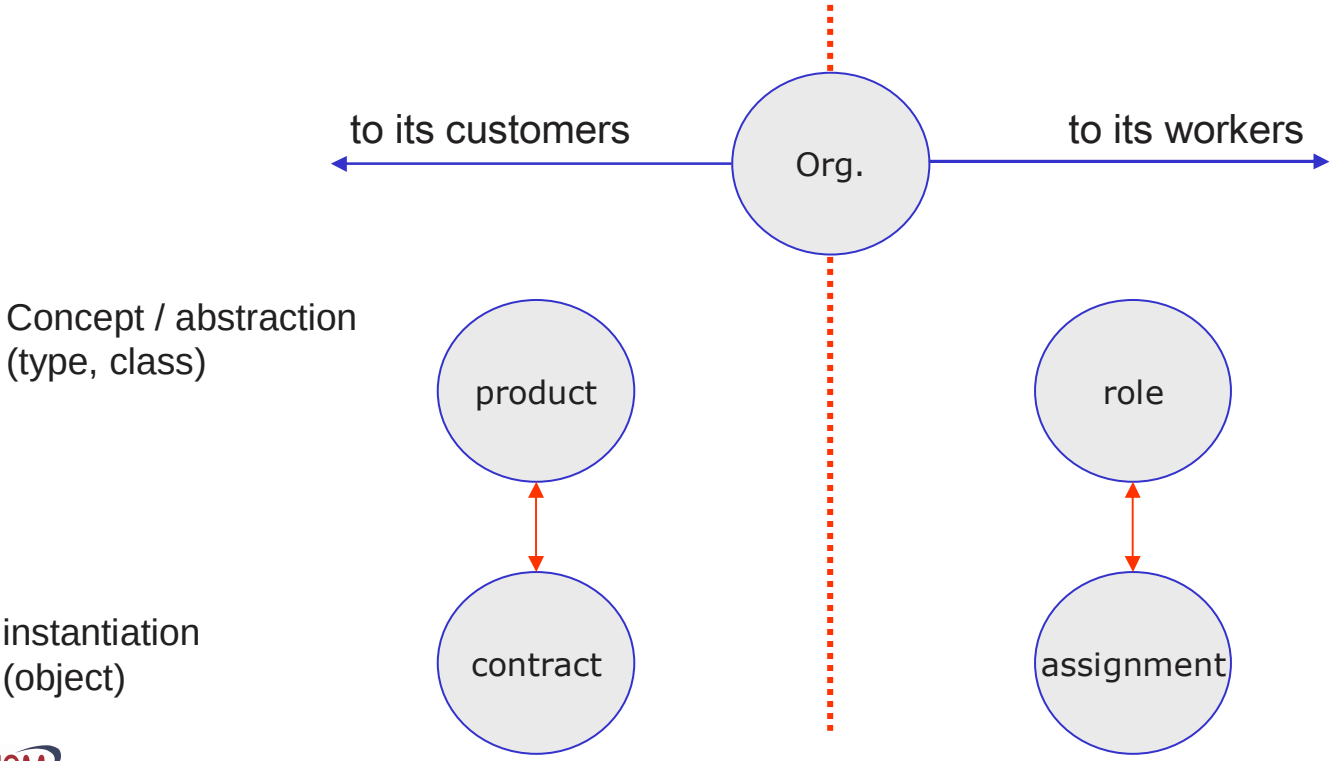
- The Identities role in an organisation …
- Performs operations on resources
- The role has a fine structure.
  - A contract defines the relationship
  - The roles define incarnation details

The role

- The role is an abstraction
- Like the „product“ abstracts the „contract“
- Hence the role relates to assignments like products to contracts.
- The privilege assignment looks similar to an employee contract.
- Both may in fact may be one “agreement”.
- They may as well be left separate.
- A customer may draw a privilege assignment as well.
- The (privilege) assignment and the contract may well be one agreement (collapse to one).

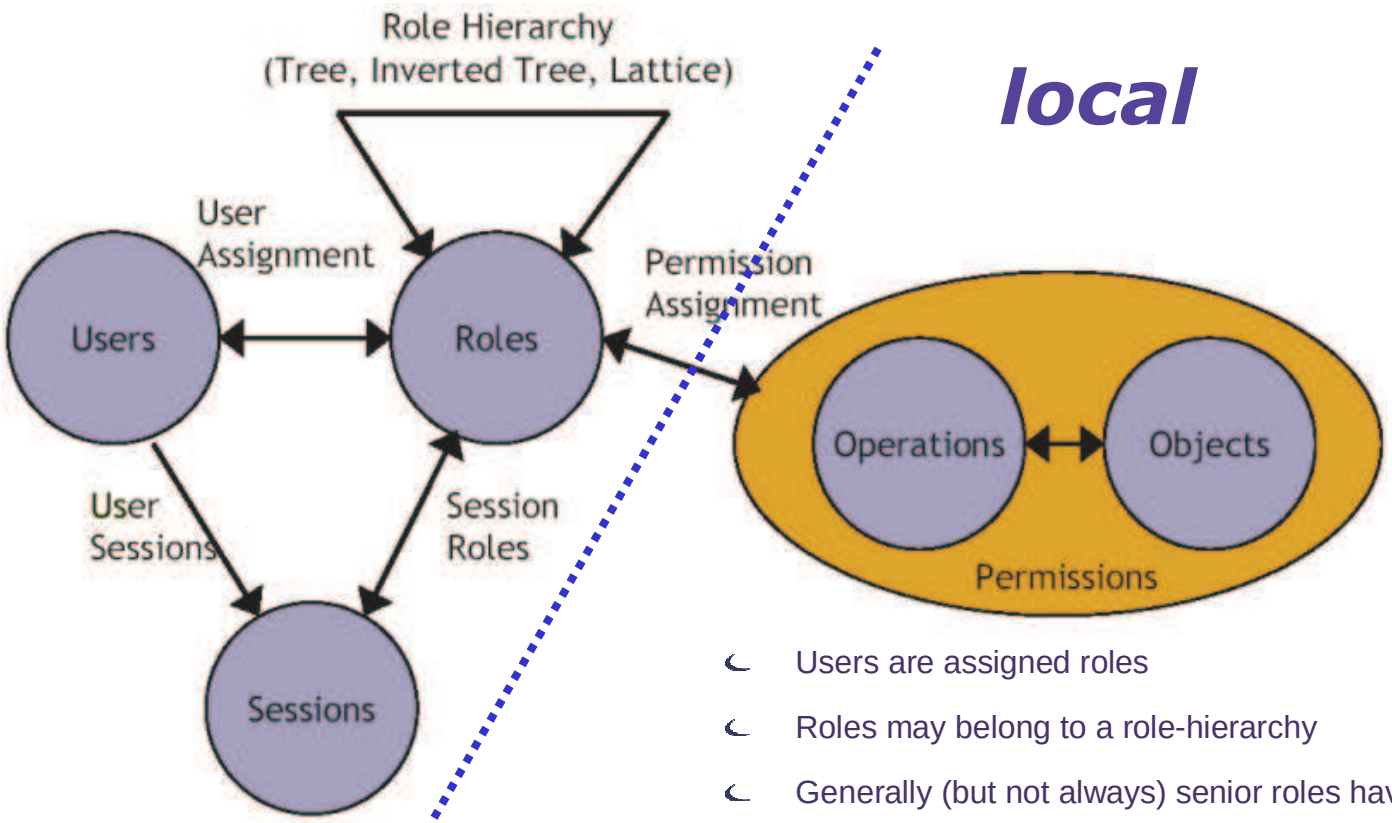
The concept of a role is an abstraction
like the product to the contract.

- The product generalises the contract
- The contract instantiates the concept of a product.
- The role generalises the (privilege) assignment.
- The (privilege) assignment instantiates the concept of a role.



Central vs. Local

IDs & roles are central by nature, while permissions are local



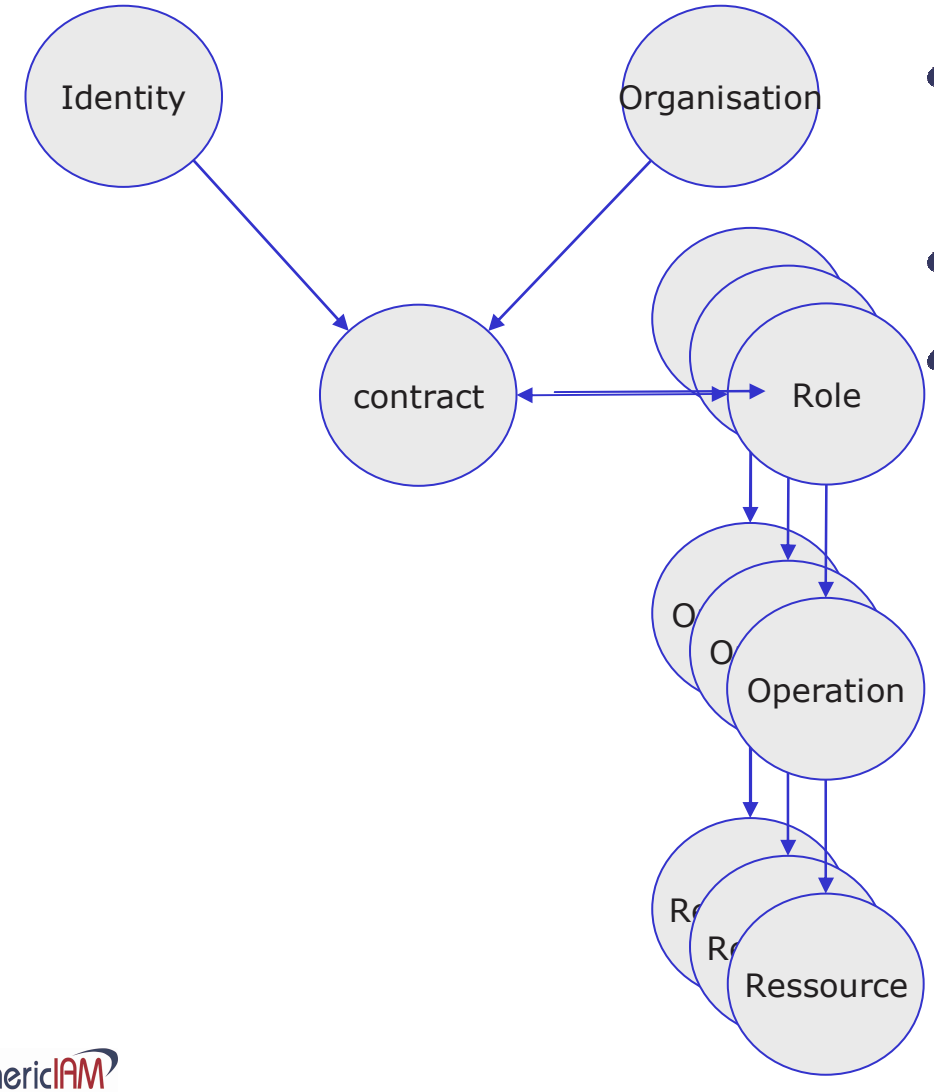
local

central

- Users are assigned roles
- Roles may belong to a role-hierarchy
- Generally (but not always) senior roles have all permissions assigned to junior roles
- Permissions are operations on objects.
- Permissions can be assigned + (additional) or - (subtractive)
- Roles Standard for Role Based Access Control

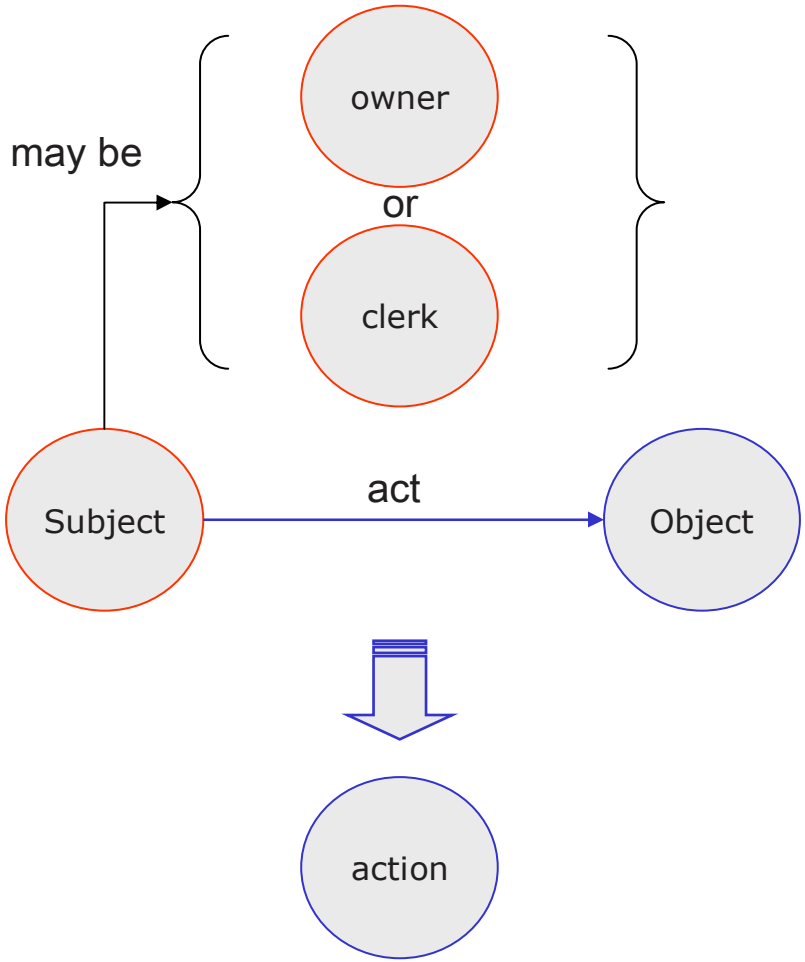
Source: Ferraiolo, Sandhu, Gavrila: A Proposed Standard for Role-Based Access Control, 2000.

Relationships are fixed in contracts



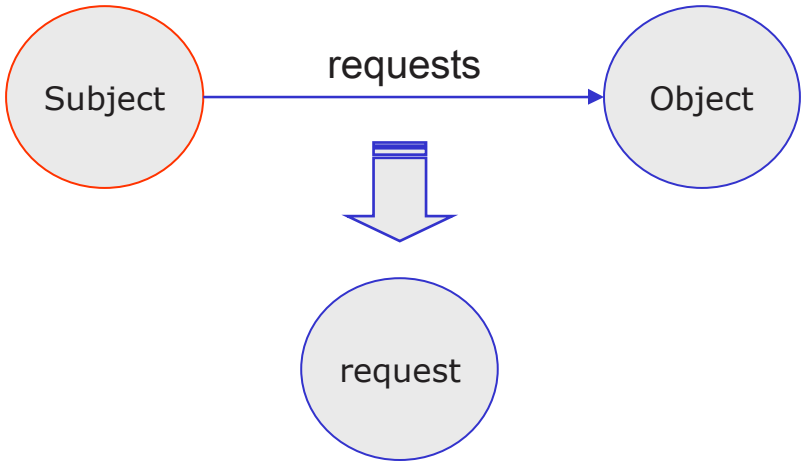
- The Identities role in an organisation …
- Performs operations on resources
- The role has a fine structure.
  - A contract defines the relationship
  - The roles define incarnation details
  - “the contract is expressed by several roles”

Subjects are acting on objects

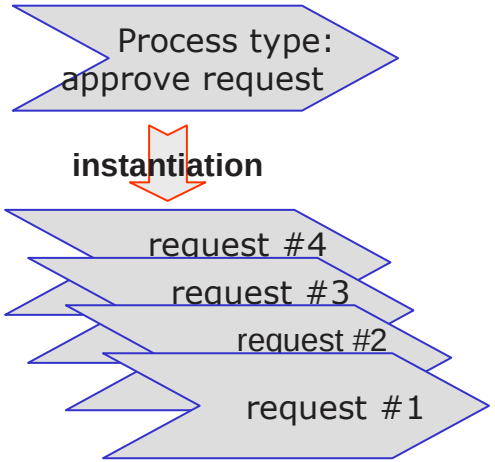


- In workflows subjects (actors) act on objects
- Subject may be owners or a clerk
- Owners are responsible
- Clerks act on behalf of owners
- Owners delegate to clerks
- Subject act or react
- Their action triggers an event
- Reactions often are approvals

Request & approval

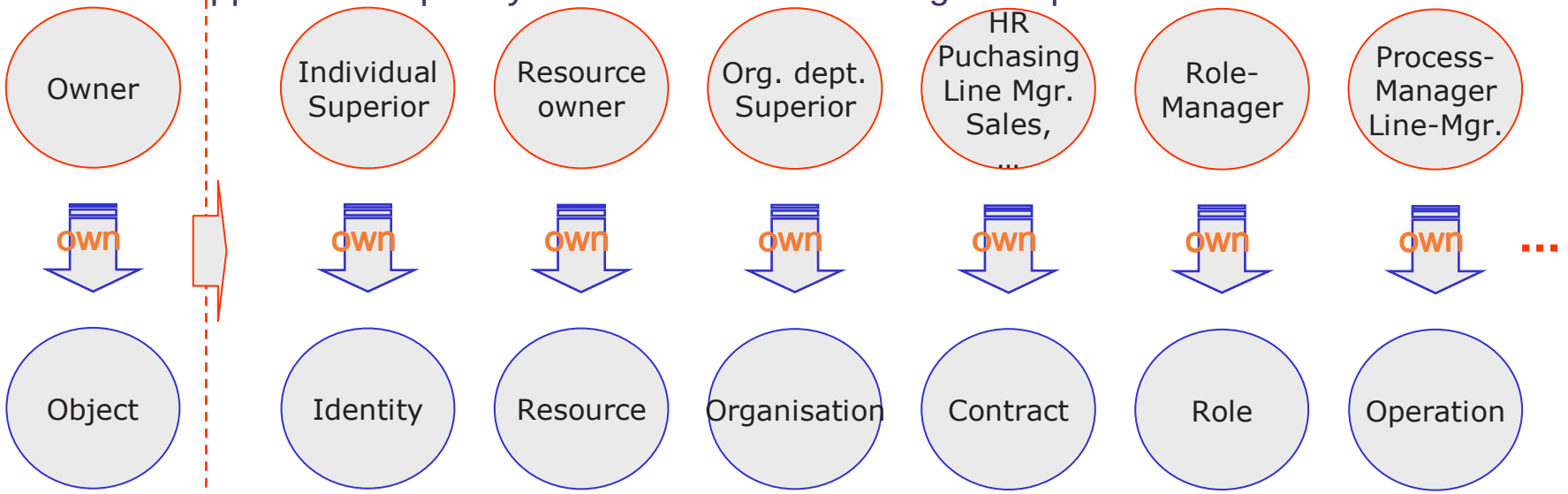


- The request is a transient object.
- It can be understood as the instantiation of a process type.
- The request is created by an event.
  - E.g. when a subject requests access to an object.
  - Or when time has come to re-validate a role / privilege.

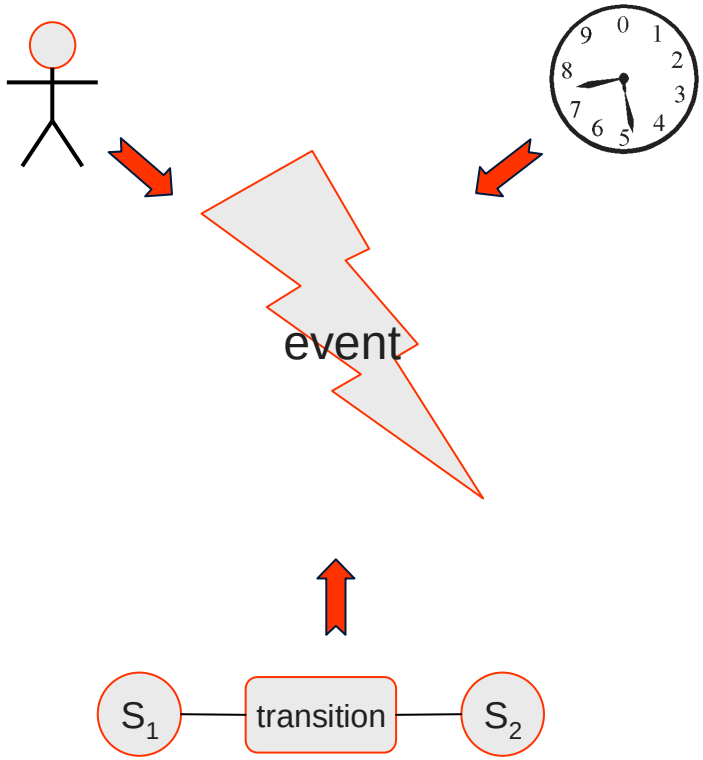


Every object has an owner

- Each object as one owner
- The owner is responsible for the object
- The owner may delegate object management to a custodian.
- The owner may temporarily transfer ownership (full responsibility) to delegate.
- Owners differ considerably from one organisation to another
- This apparent complexity is a result of customising a simple model



events



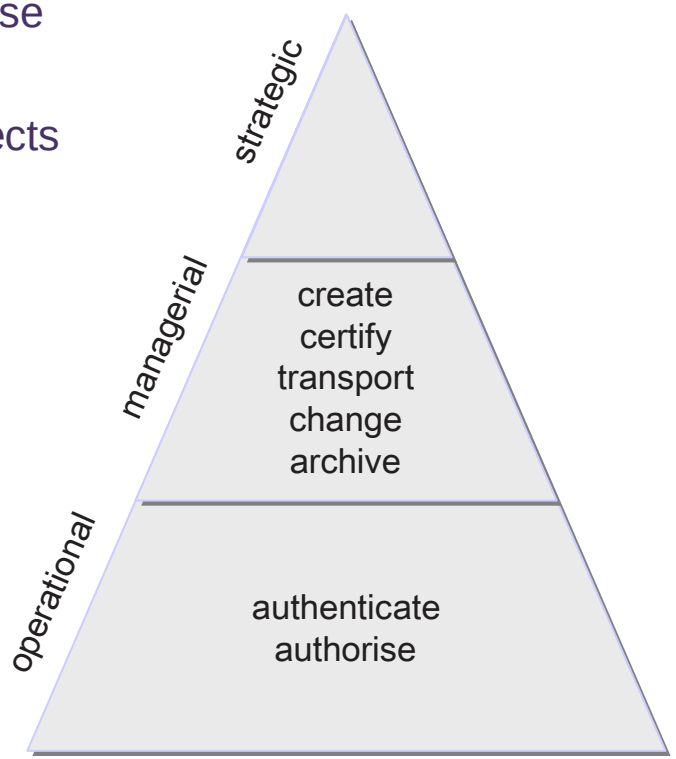
- There are events …
  - Created by an subject
  - Time triggered events
- State transitions fire events

Processes of the Identity Management

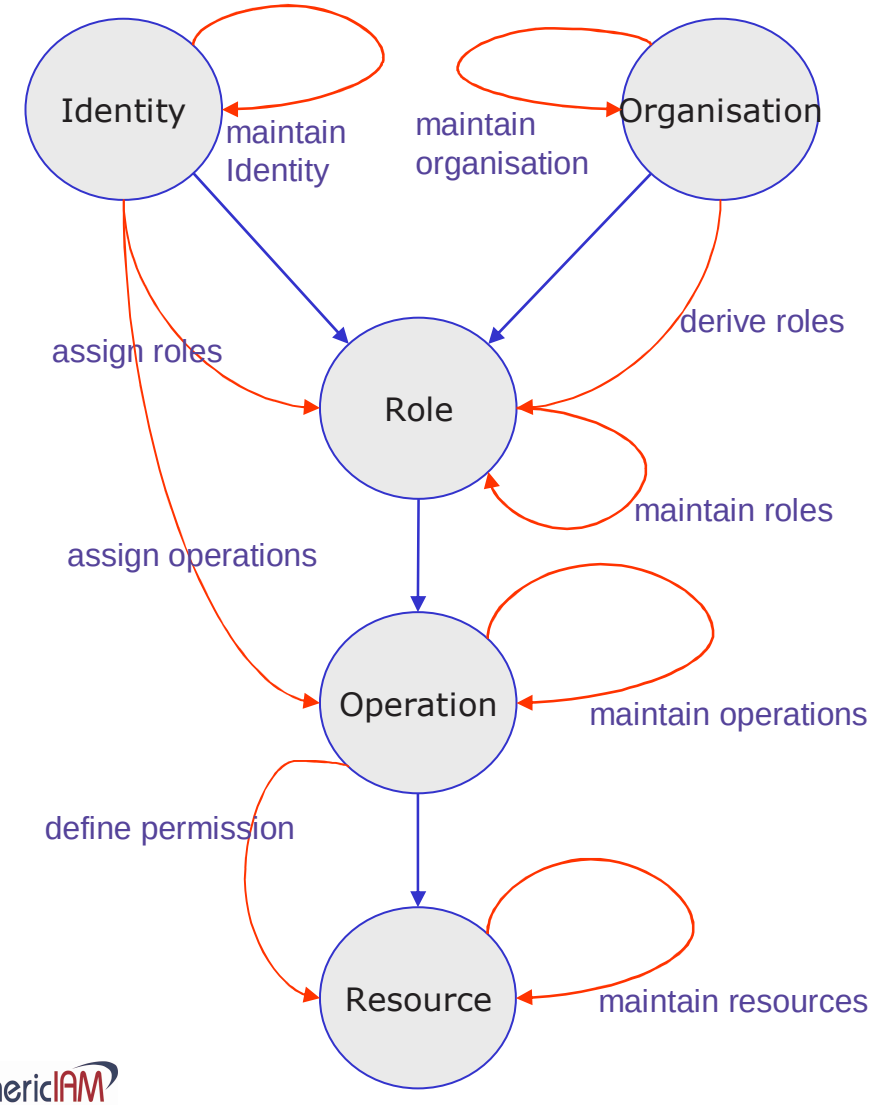
The Processes of the Identity Management may be grouped ...

- into operational, managerial and change
  - operational: identify, authenticate and authorise
  - managerial: administer digital Identities
  - Change: changing the implementation of objects
- into essential and physical
  - essential: administer and use
  - physical: integrate, transport, transform and “provision”
- into existence, certificate and context
  - create, read, change, delete
  - certify, revoke
  - assign, change, remove roles and privileges

➔ each classification has its specific value.



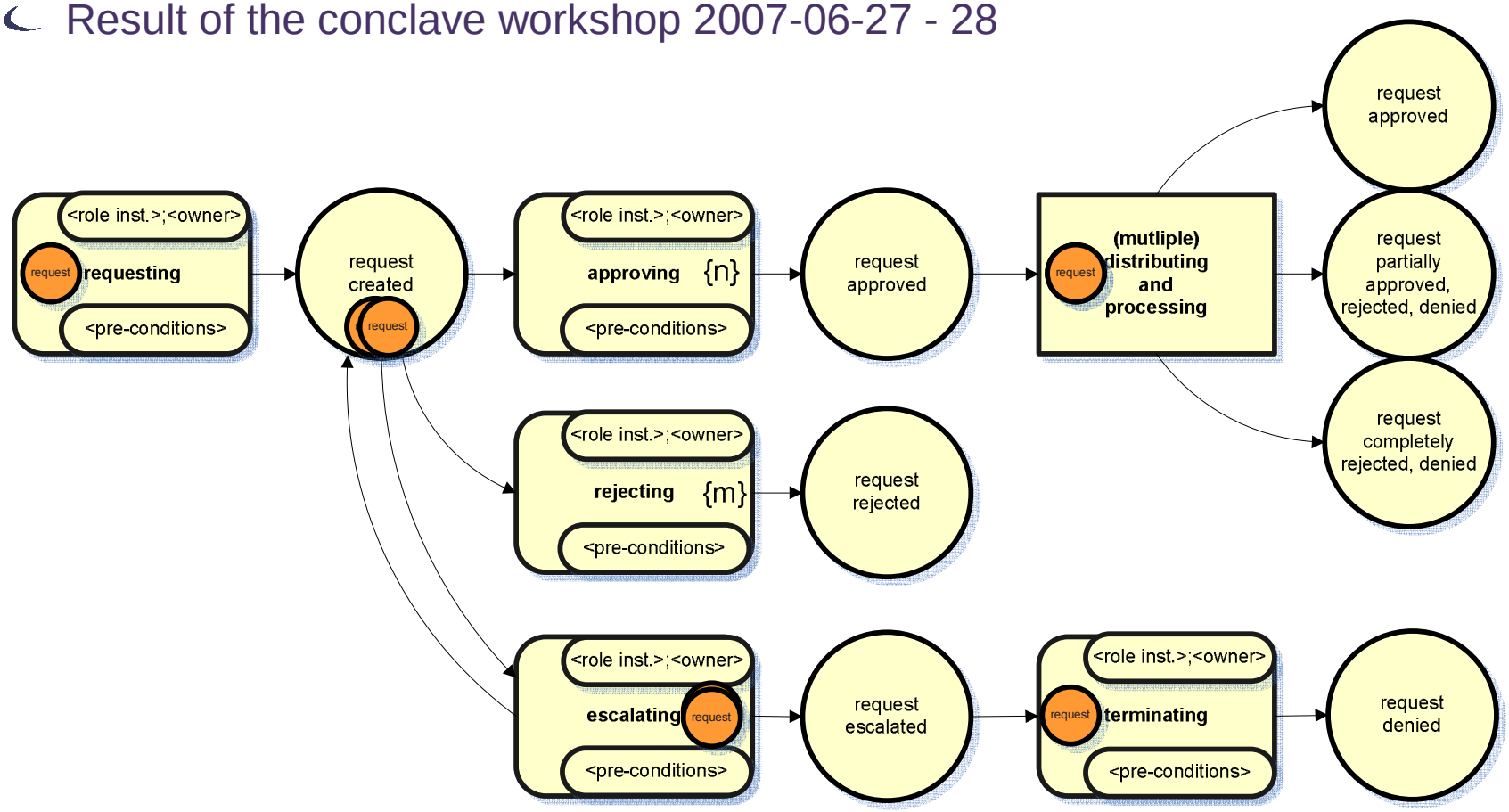
Elementary actions – changes on objects



- Processes consist of >= 1activities.
- They are triggered by an event.
- They lead to a meaningful result to a subject.
- Process types (the class or definition) and process instantiations (incarnation, actual).
- Operational processes and managerial processes.
- Operational processes: *identification*, *authentication* and *authorisation*.
- The managerial:
  - *administrative processes*,
  - *audit processes* and
  - *change processes*.
- The administrative processes represent the "lions share" of all IAM processes.
- Its most prominent representative is the "*request & approval process*".

Approve request
generic process example using petri nets

- Result of the conclave workshop 2007-06-27 - 28



Questions - comments – suggestions?

Caution Appendix

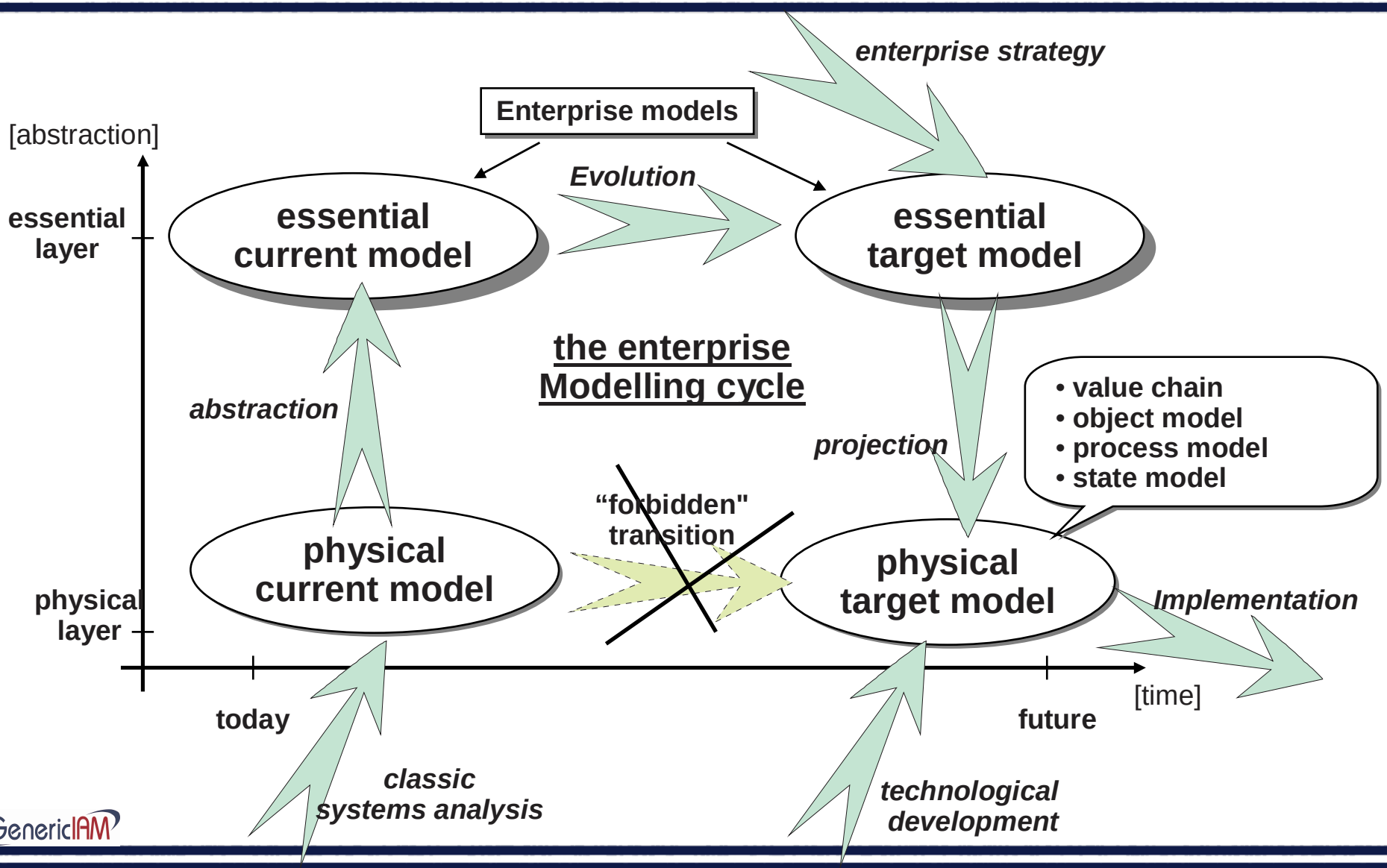
Here the notorious back-up-slides follow ...

Modelling process

In a four step Process to the target implementation model

- McMenamin and Palmer 1984 recommend to start a **four-step** Specification process with the analysis of the source model :
  - Analysis of the current systems; creating a model of the current implementation of the system.
  - Analysis of the fundamental concepts of this Implementation: creating a model of the essence of the current system. It will be abstracted from all implementation specific properties des (perfect technology).
  - Deriving the requirements to the new system: creating a model of the essence of the target system. This model describes the requirements and is not affected by any implementation considerations.
  - Designing the target system: creating a model of the implementation model of the target system.
- The requirements specification is limited to the 3rd step.

The modelling cycle
finding the essence removes implementation artefacts

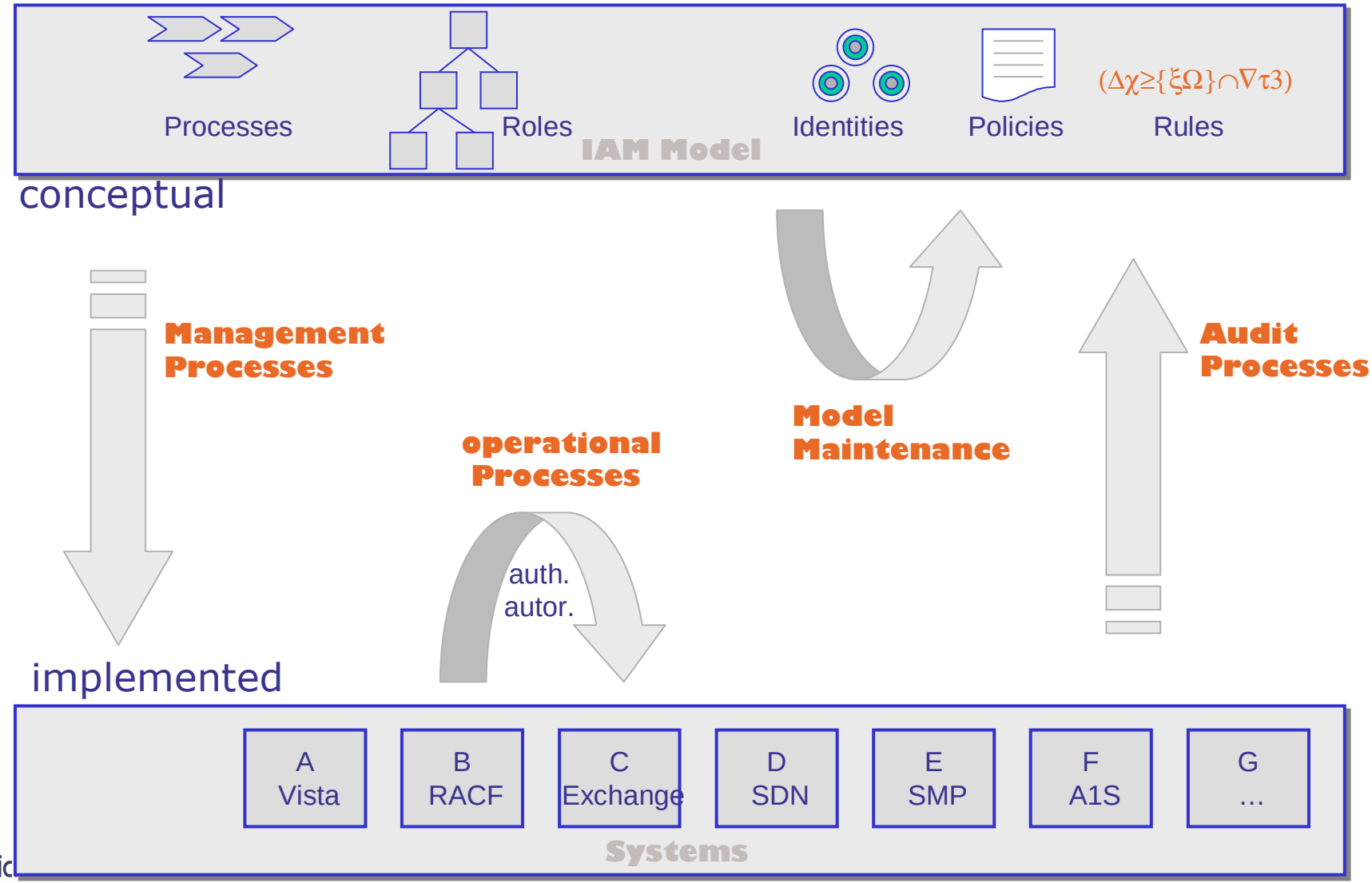


essential modelling
avoiding technical „folklore“ through perfect technology

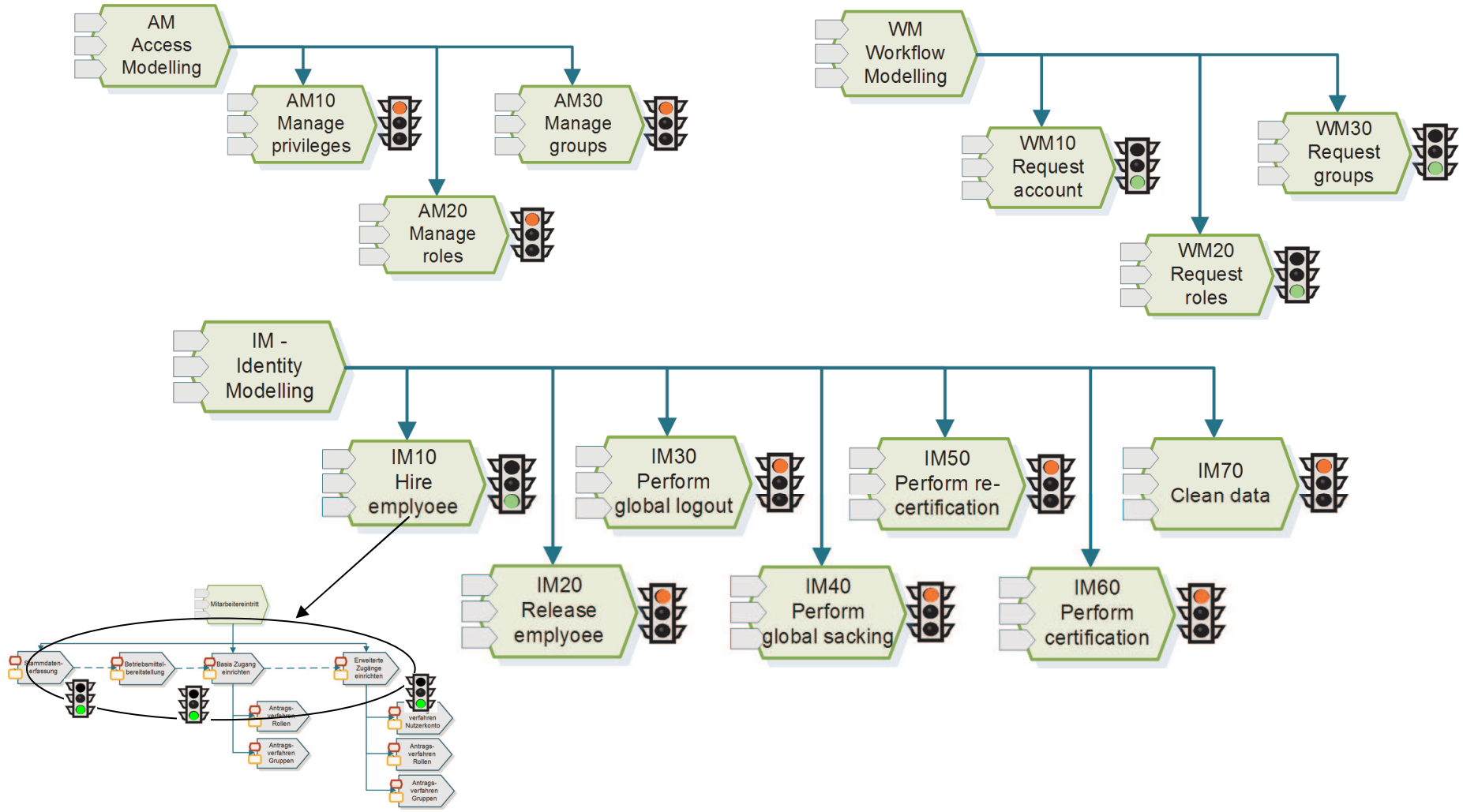
- McMenamin and Palmer require the existence of perfect technology for the System to be modelled.
  - in the **internal** neither errors nor processing- or waiting times occur.
  - check, translation und transport processes are absent there.
  - the **system context** is considered as imperfect.
  - at the **System border** there is a physical ring of these check, translation und transport processes .
- Essential Processes are triggered by external of by time events.
- Fundamental essential processes deliver an external result.
- Administrative essential processes store a result internally for a fundamental essential process.
- Essential Processes communicate asynchronously via essential stores – they are time decoupled.

Common IAM-Ownership

A central responsibility ensures a seamless architecture



generic process candidates
Identified the bottom-up way



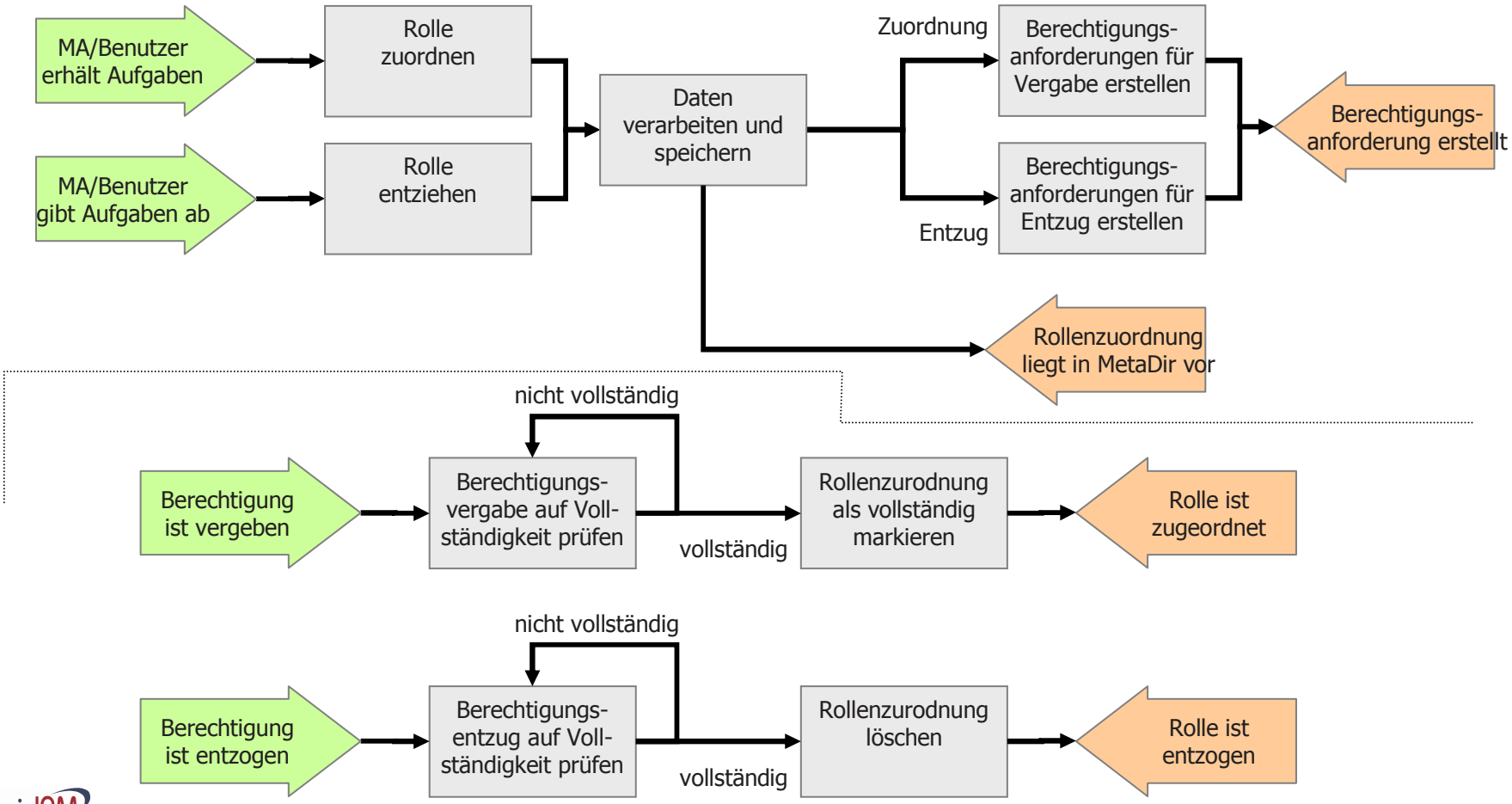
Validation of input against model

Bottom-up & top-down should meet somewhere …

- Example processes from input source have to be mapped against the proposed model:
  - Dekra
  - BMW
  - WestLB
  - DoubeSlash
  - ism
  - Others …

Detail of the Dekra Processes

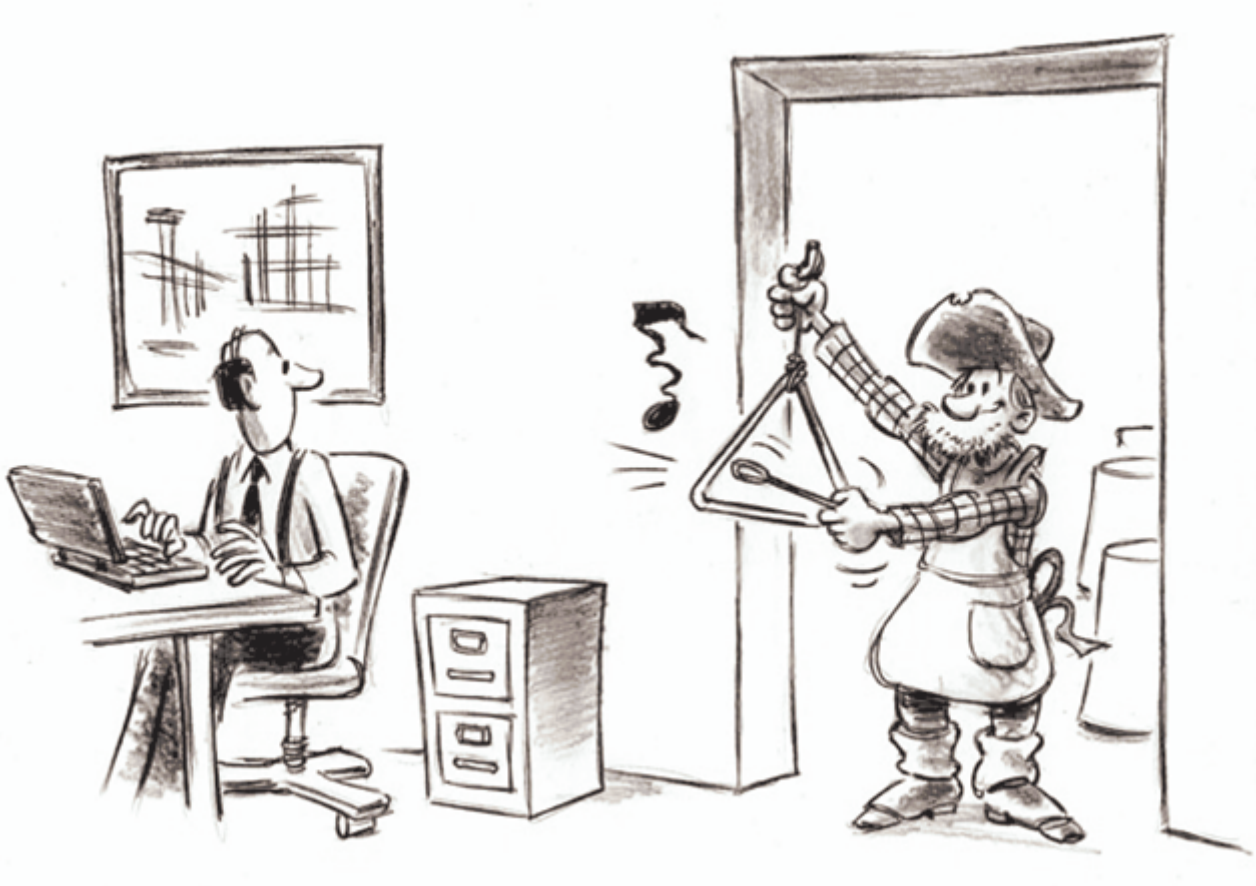
Role assign / remove



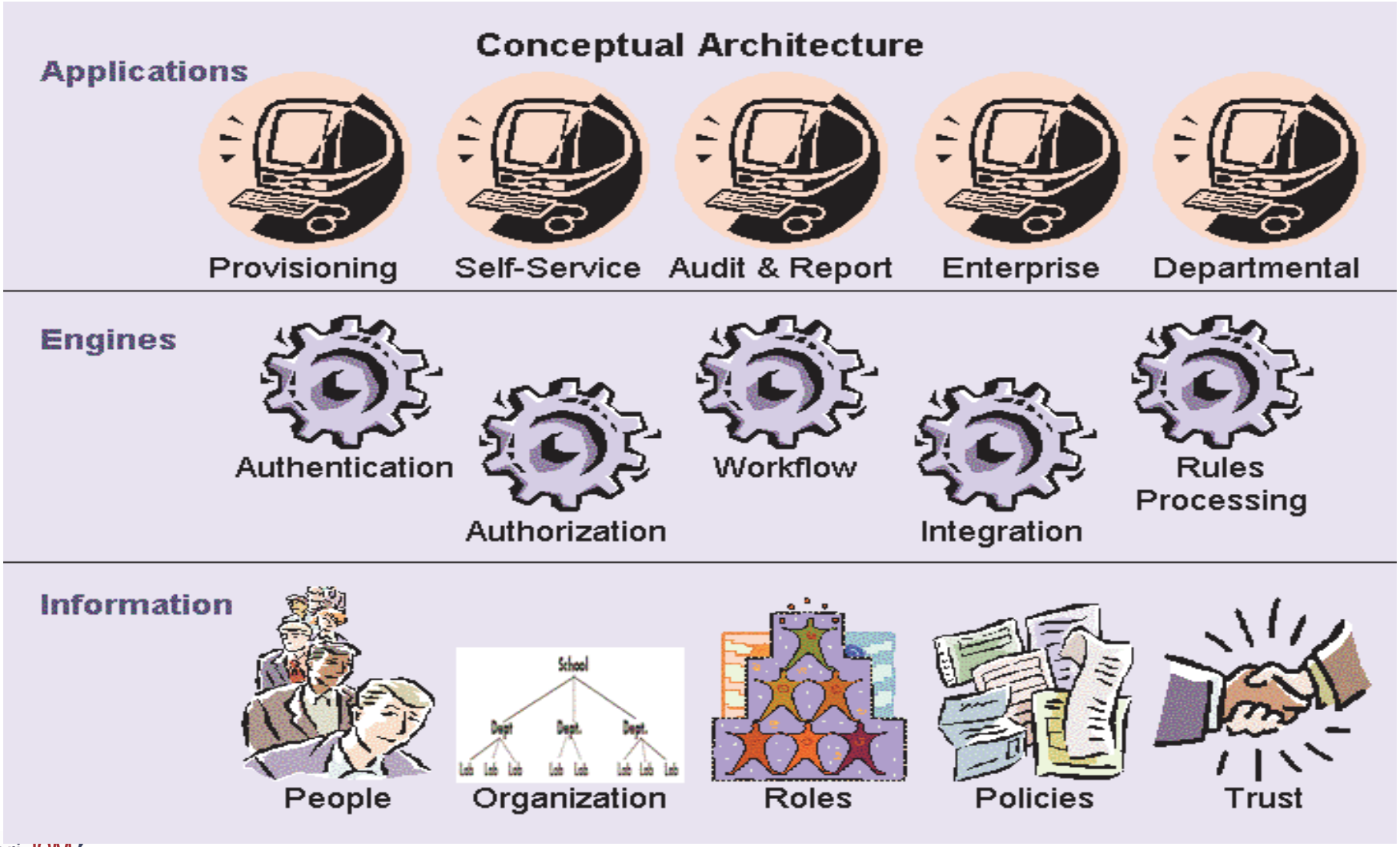
Reference Model - examples

- Supply Chain Operations Reference Model (SCOR-Modell)
- IDS Scheer führt Value Reference Model (VRM) für unternehmensweiten Support über die 'ARIS Platform' ein

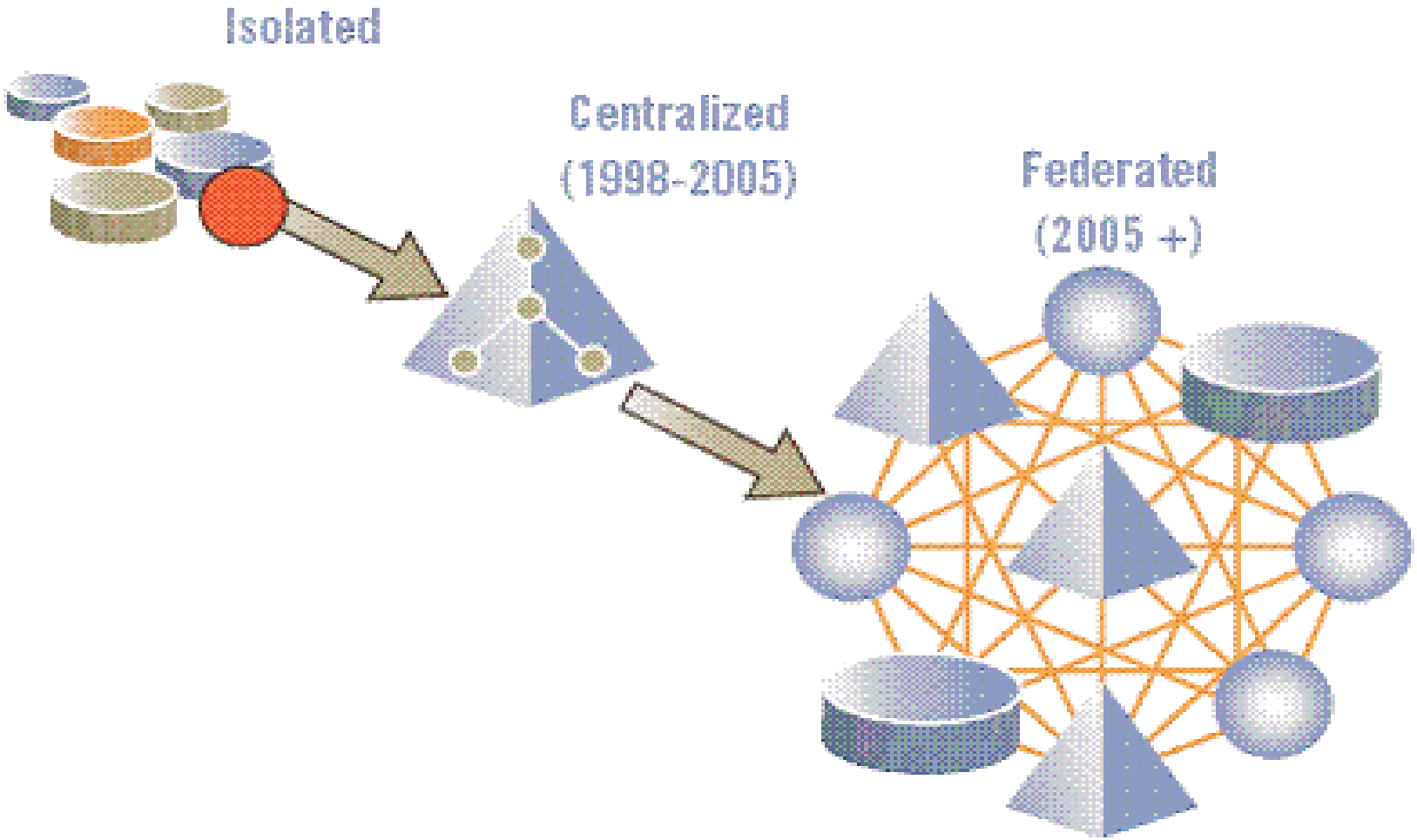
Lunch break



SOA – The Identity layer



Evolution of identity centralisation



Identity- & related Managements

- Identity Management
  - Access Management
  - Personalisation
  - Compliance Management
- Identity: to find out who you are
- Trust is being built by time
- IdM generations
  - Identity 1.0 = Silo
  - Identity 1.5 = Federation
  - Identity 2.0 = user centric