

Identity and Access Management for Today's Businesses



April 2007

Ir. Christophe Sténuît, CISM, CISSP

Ogeris

Organization & Security
in Information Management
www.ogerris.be

About OGERIS

- OGERIS: IT management consulting since 2003
- IT Risk and Security Management: Governance, Policies, Risk Control, Identity and Access Management, Security Architectures, Data Center design & guidelines (Physical Security)
- IT Organization: Process Engineering, ERP, e@Business, Optimal Service Management, RFQ, Project Management
- Education
- References: DHL London, DHL Prague, Delhaize, FEDICT, TDS Logistics, AJMAT



Organisation & Security
in Information Management
www.ogeris.be

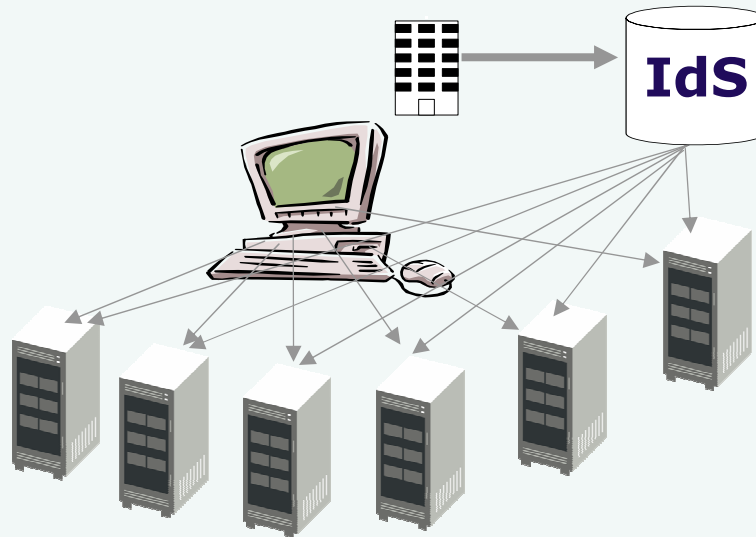
Today objectives

- To provide management views rather than technical details
- To provide background view on Identity Management
- To provide overview on current studies and standards
- To provide background view on Access Management
- To provide few technical architecture trends and models
- To provide process views
- To share experiences

Agenda

- Part one: Identity Management Framework
 - Identity, concepts, models, framework
 - Identity Management
 - Identity Management and Information Technology
- Part two: Identity and Access Management (IAM)
 - IAM issues, ideas and concepts
 - IAM model, Security Shared Services
 - IAM components
 - Process understanding

Why do we need IdM?



User info maintenance scattered amongst different groups of people

■ IdM original goals

- guarantees the validity of identities
- guarantees accuracy of user's info
- save huge effort and costs in users' information updates

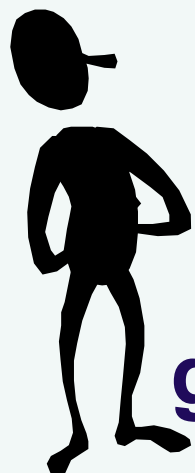
Ogeris

Organisation & Security
in Information Management
www.ogerris.be

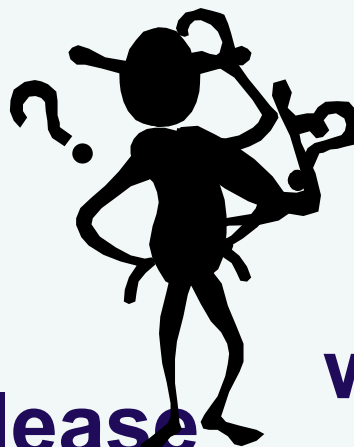
What is IdM in IT?

- IdM must ensure that accurate information is provided on the initiator of any access to information systems
- IdM is not a purveyor of accounts, privileges, credentials, auditing tool, etc. but all these subsequent needs are closely related
- Different
 - Views
 - Scopes
 - Objectives
 - Definitions
 - **Understandings**

Identity ontology



give me privilege please



what do I need to know

- How do we know who do we talk to?
- Identity should provide uniqueness of an entity in the context and facilitate this process
- Identity must also be authenticated. We need a bootstrapping process

Ogeris

Organisation & Security
in Information Management
www.ogeri.be

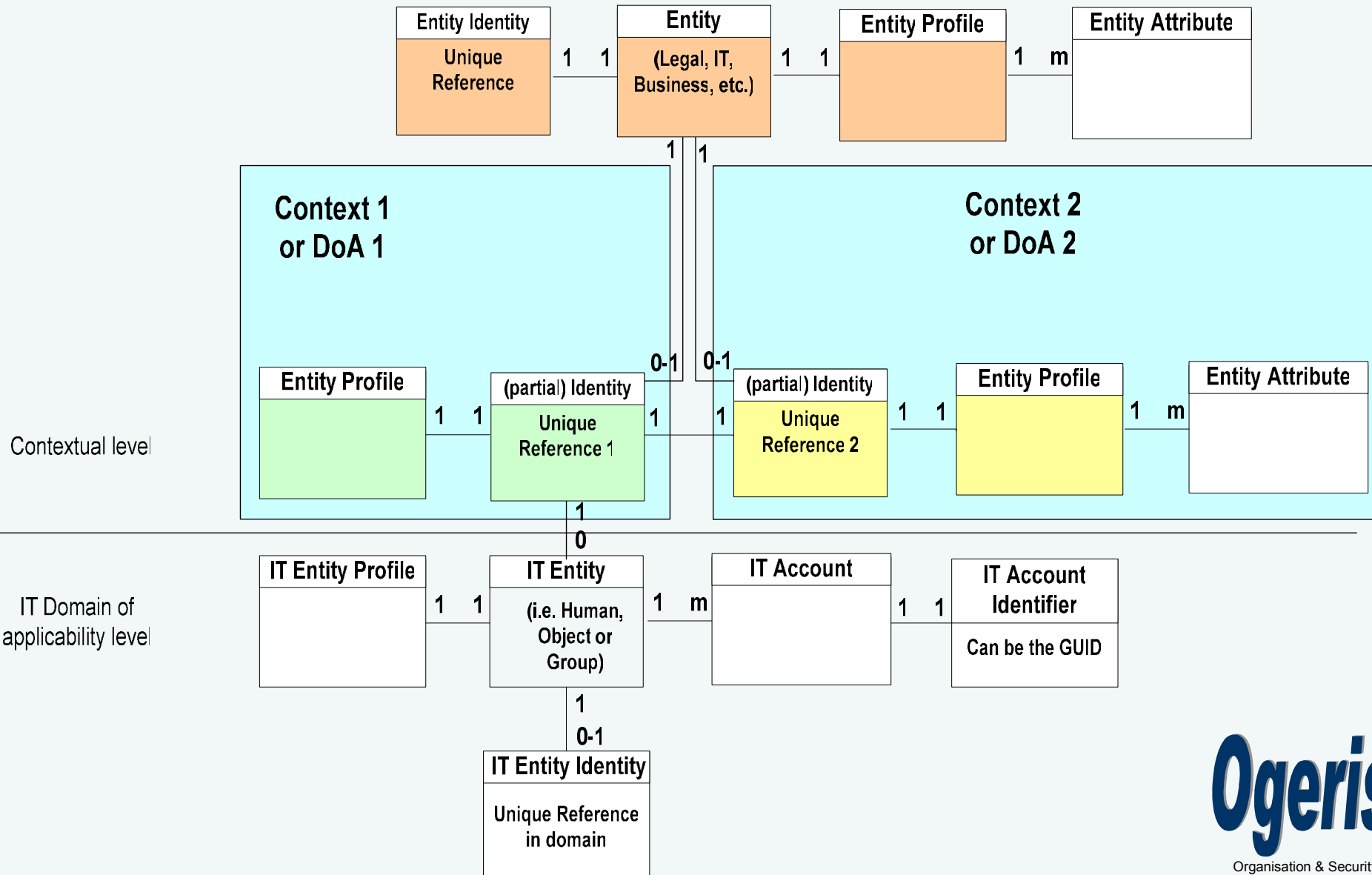
Entity, Identity, Identification

- Entity: physical person, organization (institution or company), object, a group of these individuals
- Entity
 - may have different identities in different contexts
 - may have different identity references in one context
 - may use different identifiers in one context
- The identification process identify the entity's identity, its references, its attributes, a profile of characteristics periodically modified during the entity life cycle

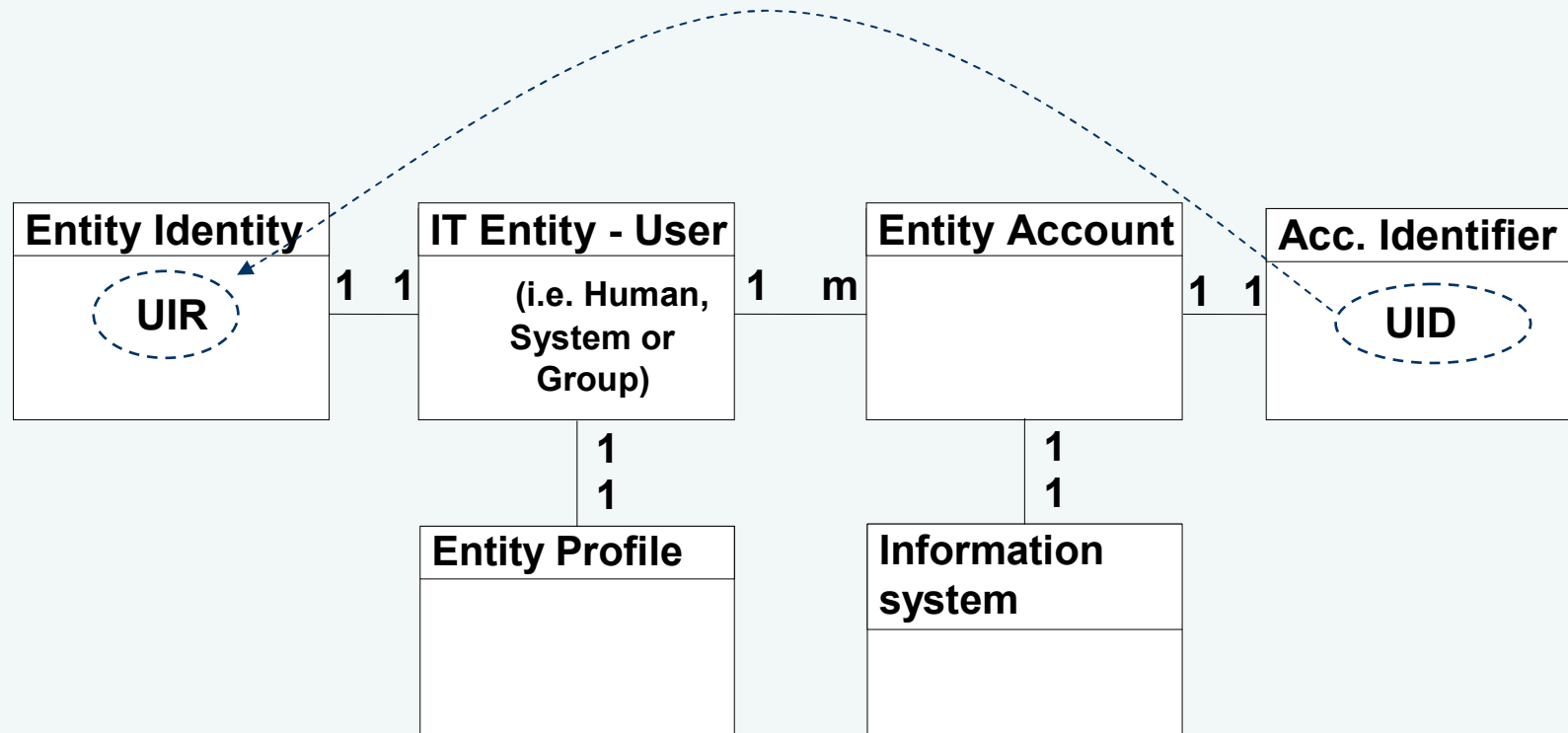
Contexts, Authentic Sources, Domains of applicability, Federated Identity

- Identity is unique within a context
- Entity recognized across different domains of applicability of the context with different prerogatives
- Different partial identities and a federated identity.
- Cross domains and cross context identification with controls of attributes transfers: Privacy
- Recognition of sources of Authentic Information

Identity Model



Identity and Identifier

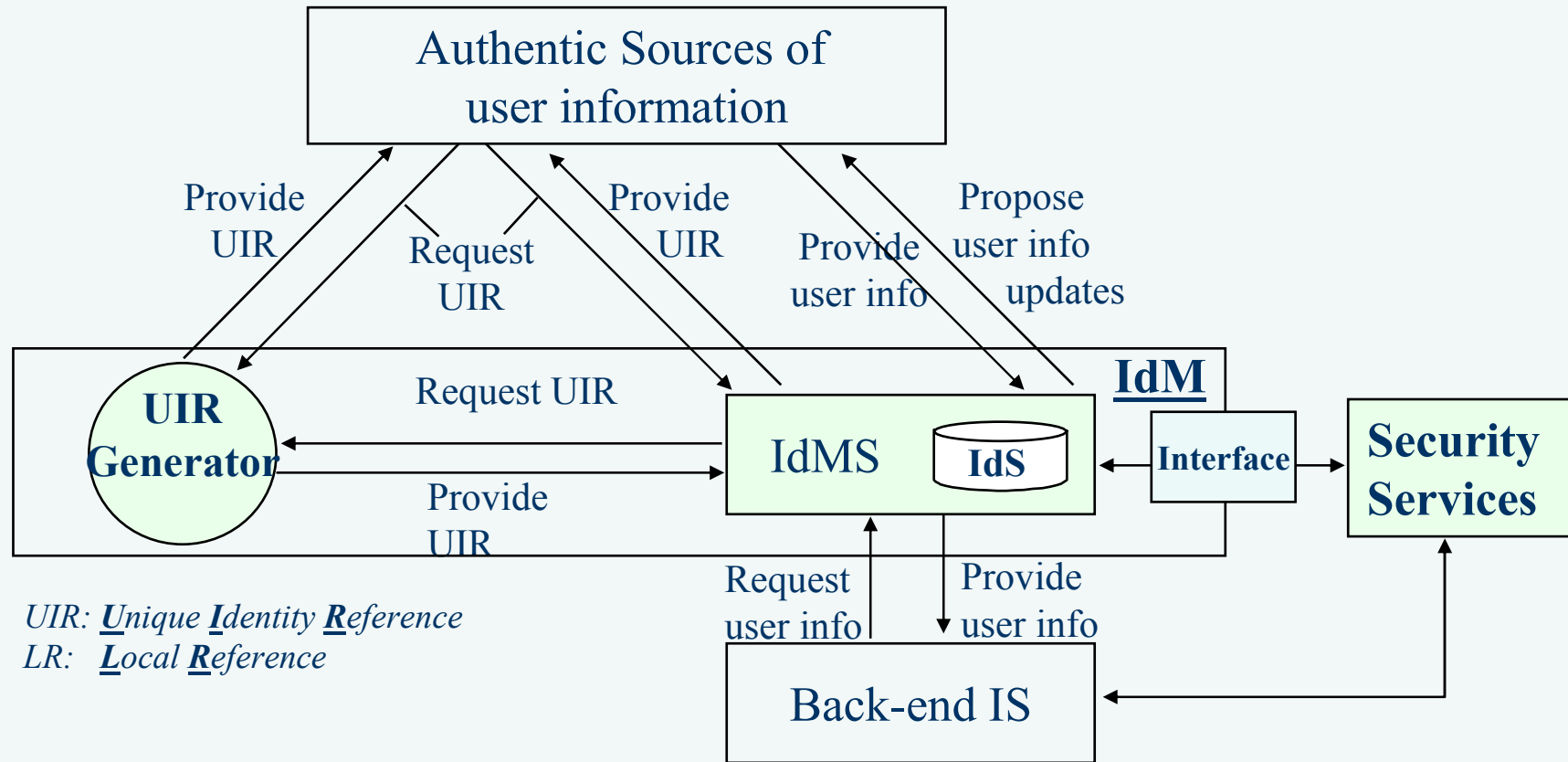


- Identity reference may be used as identifier
- Does not work in all circumstances
- Is managed by different groups of actors

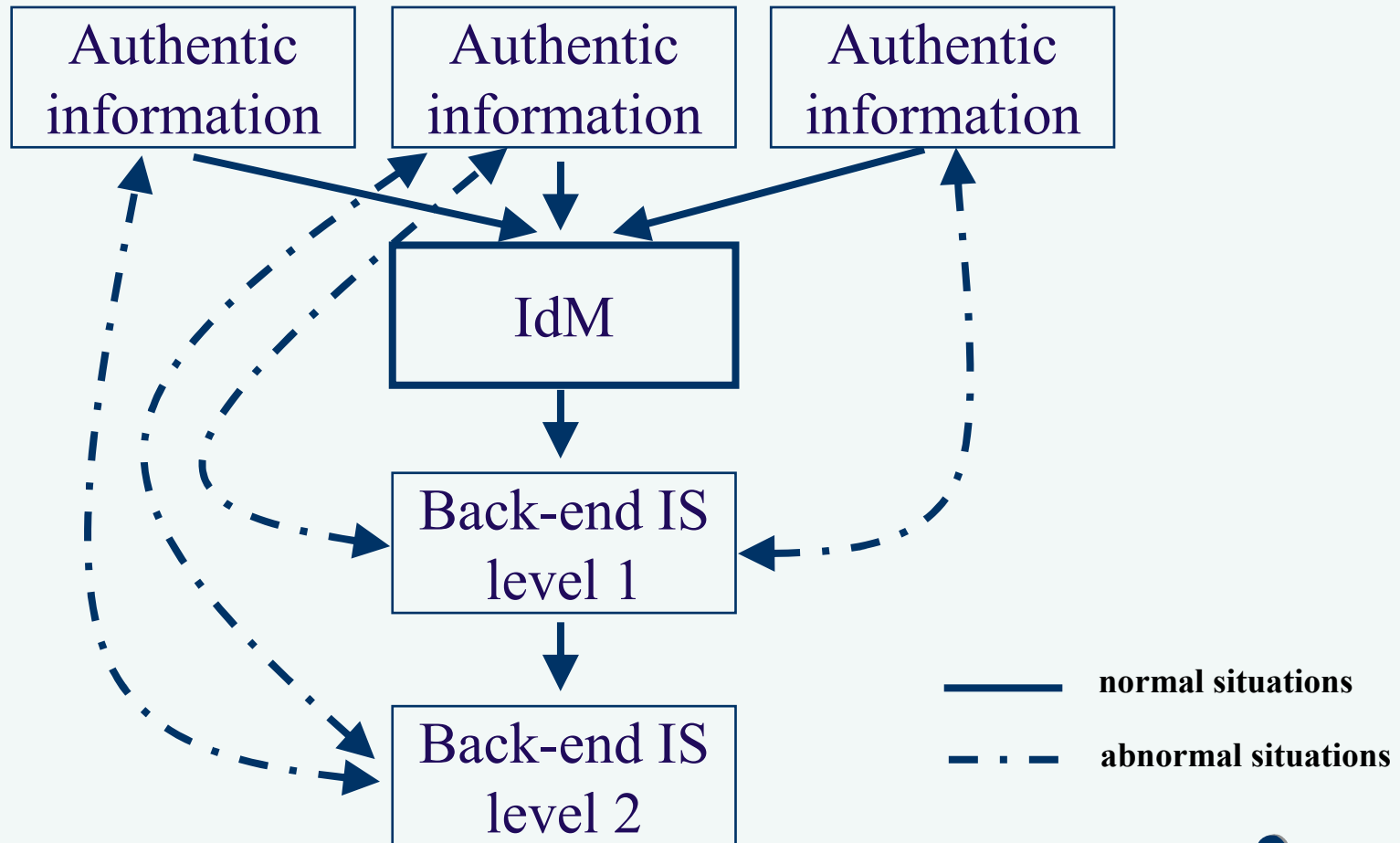
Identity Management

- Integrated management processes, policies and technologies that control the use of identity information
- Manages identity life cycle, creation, changes, revocation
- Manages and publishes changes of identities
- Manages identity conflicts, ambiguity, alteration, repudiations
- Maintain trust relationships between stakeholders

IdM Architecture



Network of trust



IdM and Information Society

- Legal and regulation constrains
- Governance and ISMS
- Control objectives: reliable processes, privacy protection

Ogeris

Organisation & Security
in Information Management
www.ogeris.be

Essential definitions

- Entity, Context, Domains Of Applicability
- Identity, Identification, Identity Reference, Identifier
- Identity Management
- Identity authentication, Identity verification
- Mutual authentication, federated identity
- Authentic repository, authentic information

Refer to the ISO 24760 working draft for details

Major work items

- ISO/IEC 24760, A framework for Identity Management (& Access)
- Open Group Identity Management Forum
(<http://www.opengroup.org/onlinepubs/>)
- Fidis, Future of Identity in the Information Society (www.fidis.net)
- ISO TC68/SC2, IdM for financial industry needs
- ITU-T SG17, Framework for identity controls: was considered as an add-in to be attached to 24760 as the later has a broader scope
- Open Mobile Alliance (OMA): Identity Management Framework Requirements

Conclusions

- A progressive maturity
- A shared concern
- No support from the community (on its way)
- A work in progress

Identity Management

Questions before the break

Ogeris

Organisation & Security
in Information Management
www.ogerus.be

Agenda

- Part one: Identity Management Framework
 - Identity, concepts, models, framework
 - Identity Management
 - Identity Management and Information Technology
- Part two: Identity and Access Management (IAM)
 - IAM issues, ideas and concepts
 - IAM model, Security Shared Services
 - IAM components
 - Process understanding

Observations

- Security access controls are constantly reinvented
- No minimal access is guaranteed
- Security maintenance is scattered amongst different groups of people: poor understanding and awareness of security concepts
- Authorization process is not controlled
- Authentication is not proportional to the risk
- Review of accesses is poorly done
- Lack of homogeneity in solutions, major cause of security breaches, Equivalent security is difficult

Access Management

- Integrated management processes, policies and technologies
- Manages users and users' prerogatives life cycle, manages and publishes changes
- Manages conflicts, changes, transfers of information
- Maintain trust relationships between stakeholders

Approach

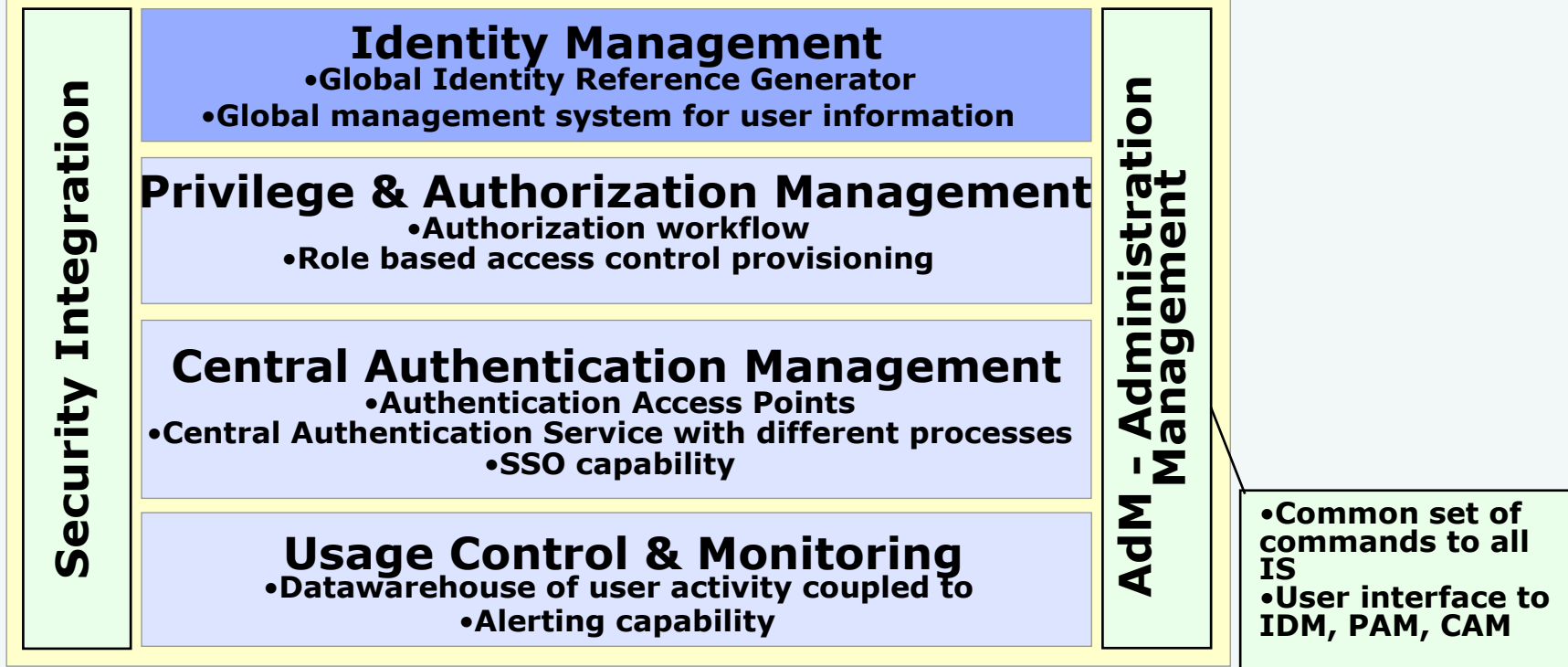
- A different approach is needed
 - Harmonized processes, model supported by policies
 - Model independent of the infrastructure, supporting different needs, with central co-ordination and distributed means
 - Equivalent security controls
- Shared security services provisioning
- Security controls are pushed aside of the infrastructure

Ideas

Facts	Ideas	Benefits	Impacts
Duplic. of user data	Central IDM system	User data quality	Recognized access
Who access what?	Central privilege mgt	View on user access	User administration
Min. author. f(pos.)	Integr. procedures	Time to access	Hiring process
How to ask access	Workflow processes	Awareness	Access process
Signing structures	Uniform (and single) signing	Adequate controls	All systems must comply
Review of activities	Central logging	Prevention	Development

IAM Services & Components

User Access Management Security Services

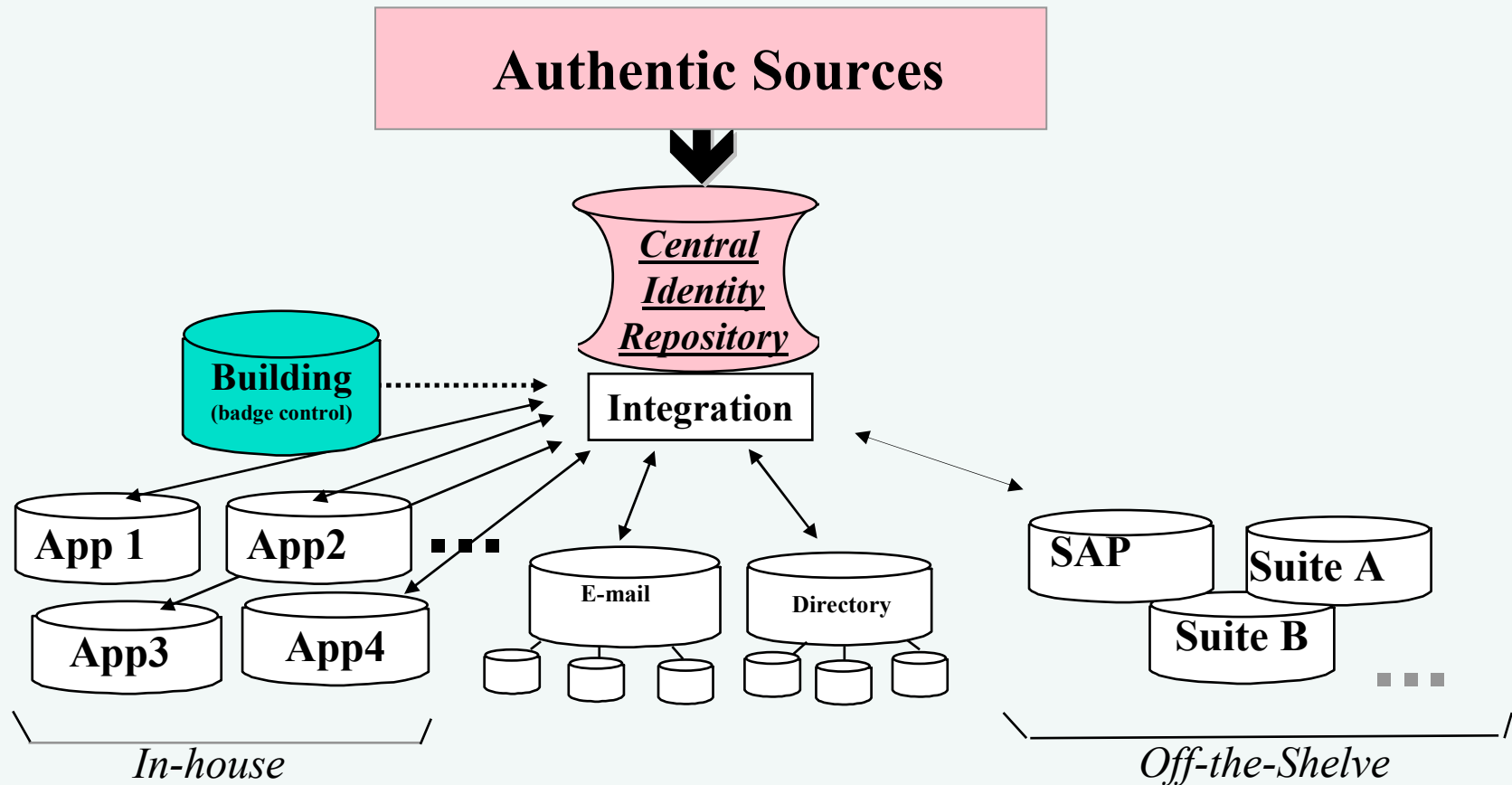


A structured process driven model, centrally managed with distributed means

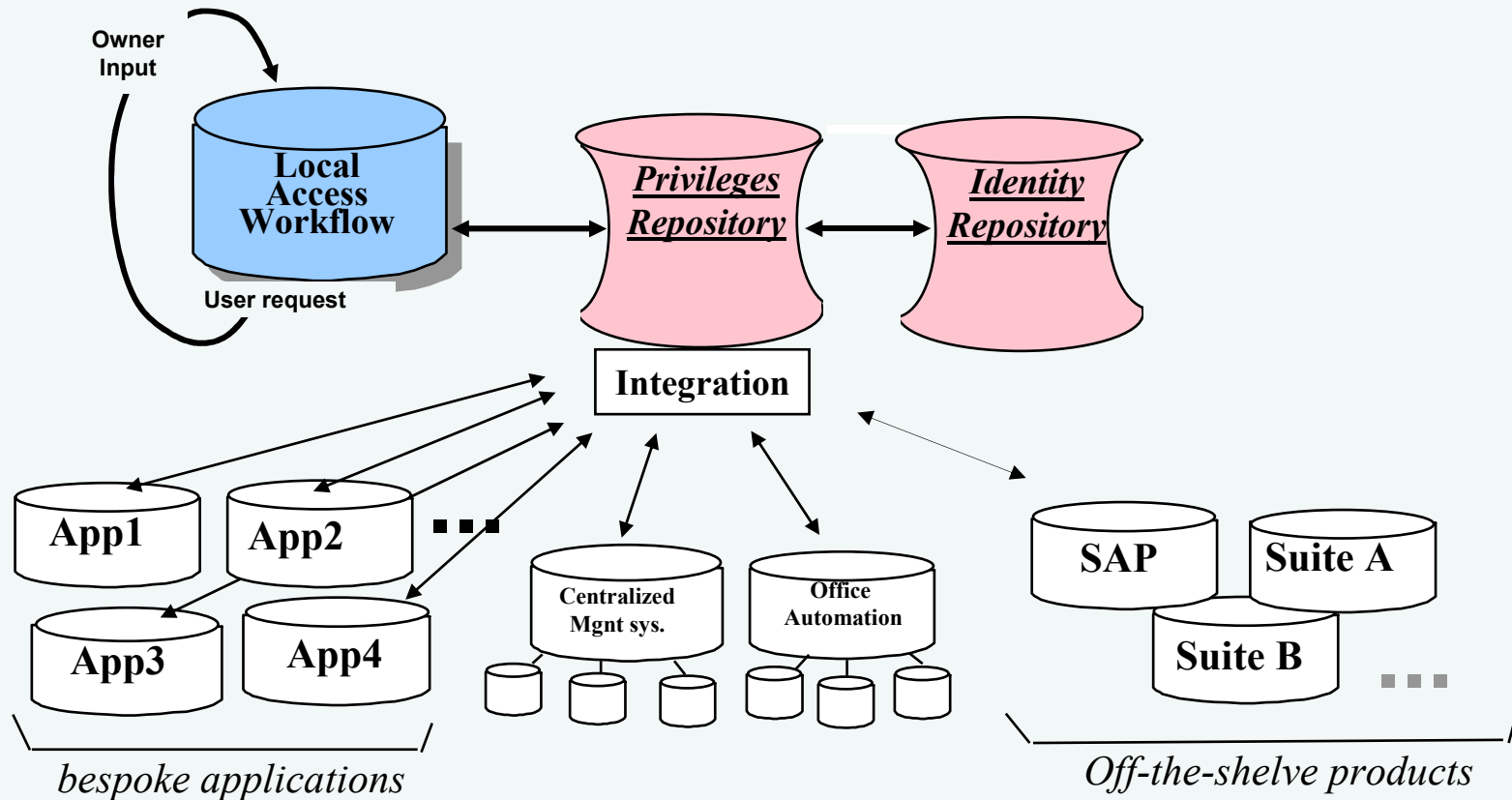
Ogeris

Organisation & Security
in Information Management
www.ogerus.be

Identity Management (IdM), user information control & distribution



Privilege and Authorization Management (PAM)

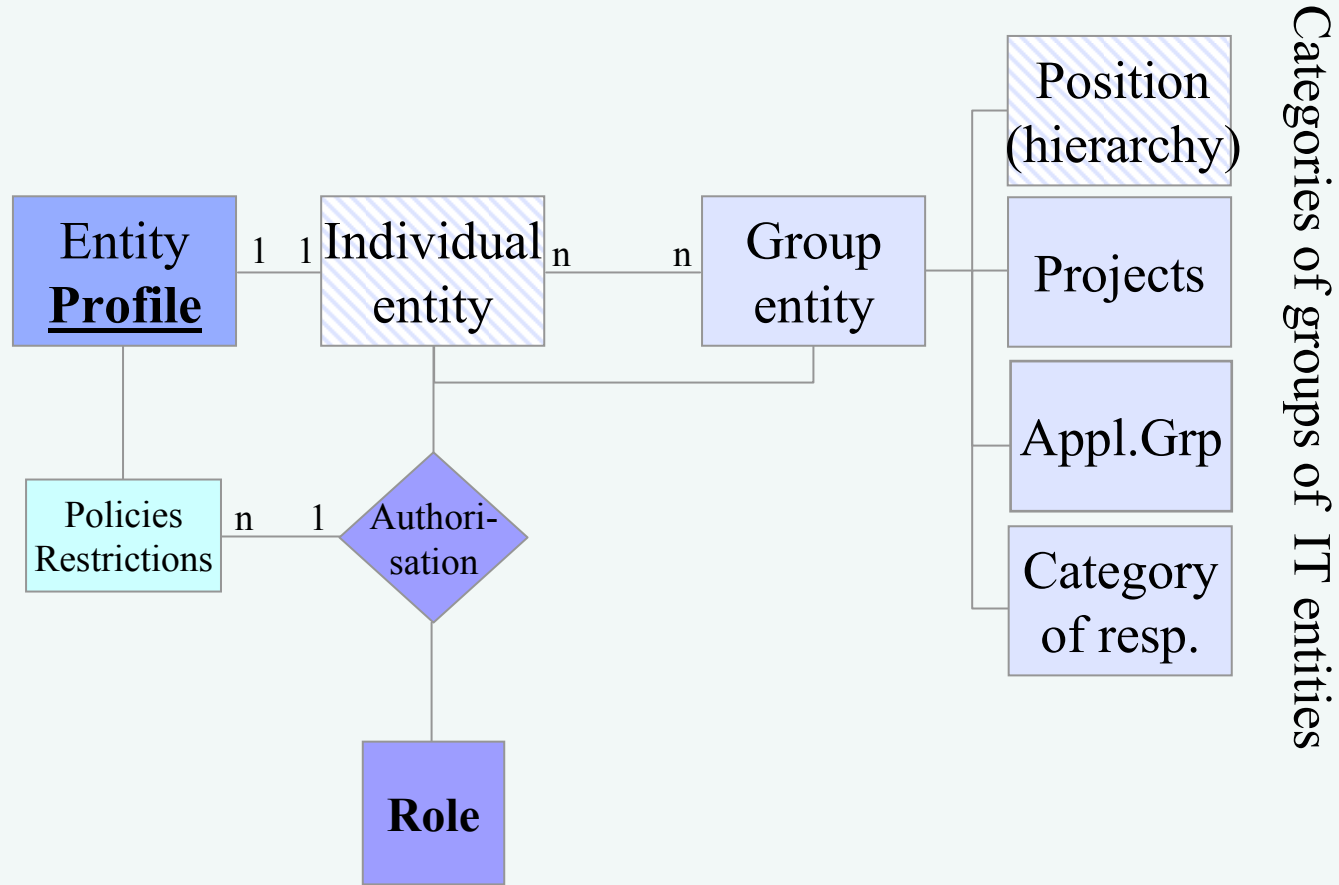


The same structure that for IdM with different means for different needs

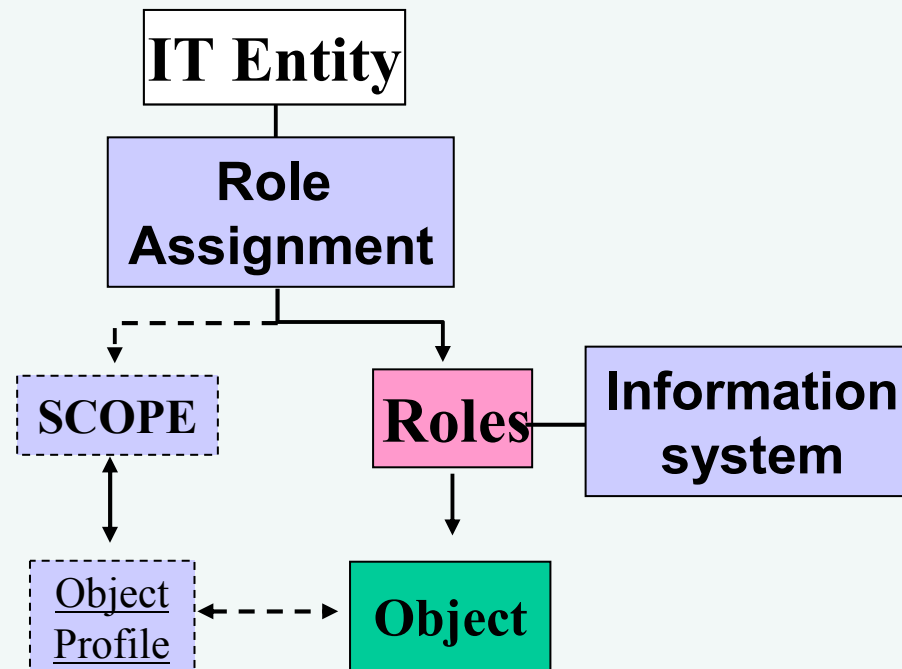
Ogeris

Organisation & Security
in Information Management
www.ogerris.be

RBAC: Use of Group entities to reduce the number of roles

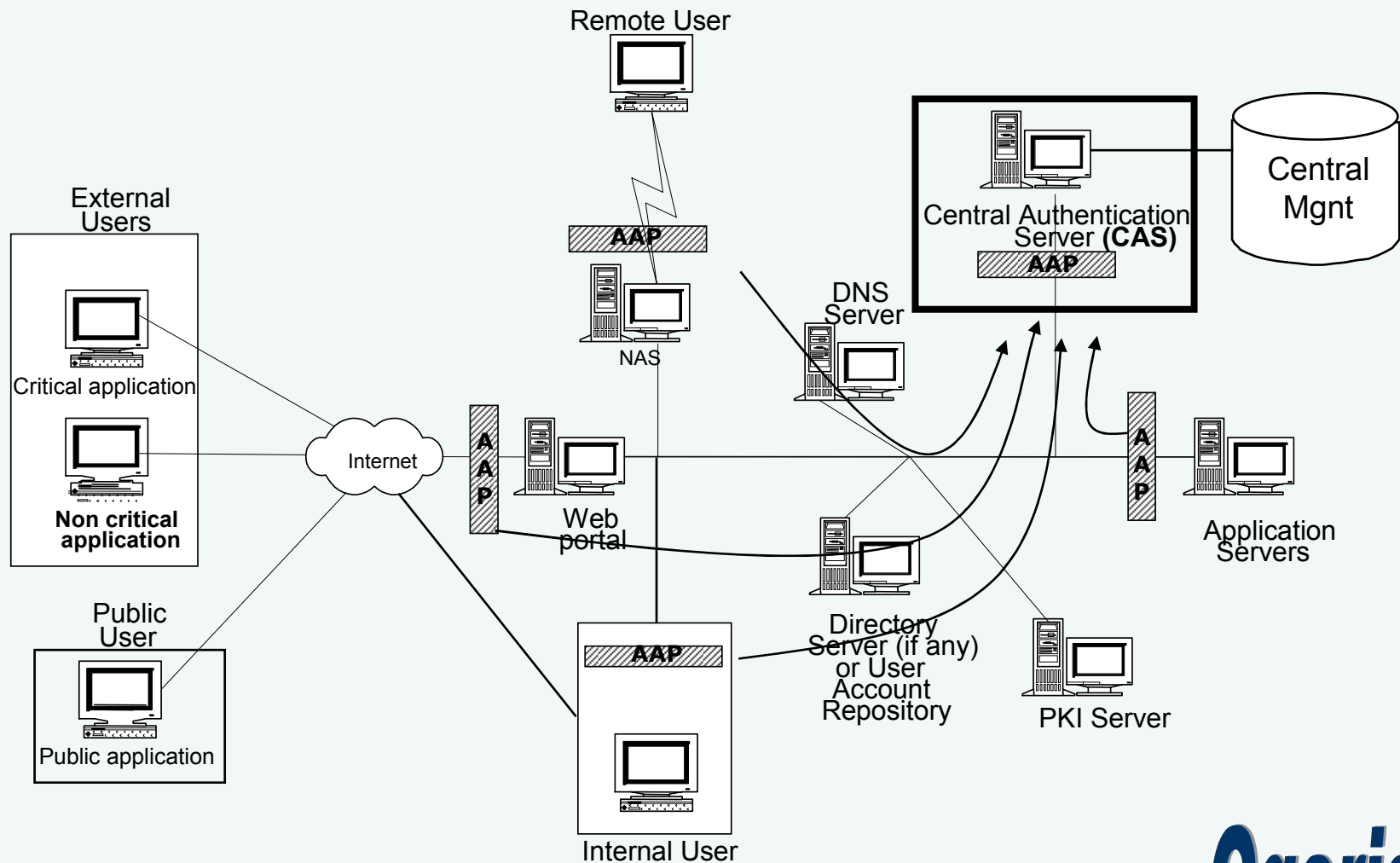


RBAC: Use of data views to reduce the number of roles



A role engineering data model is required, independent of IAM, but on which the IAM processes must be organized

Central Authentication Management (CAM), Authentication Access Points



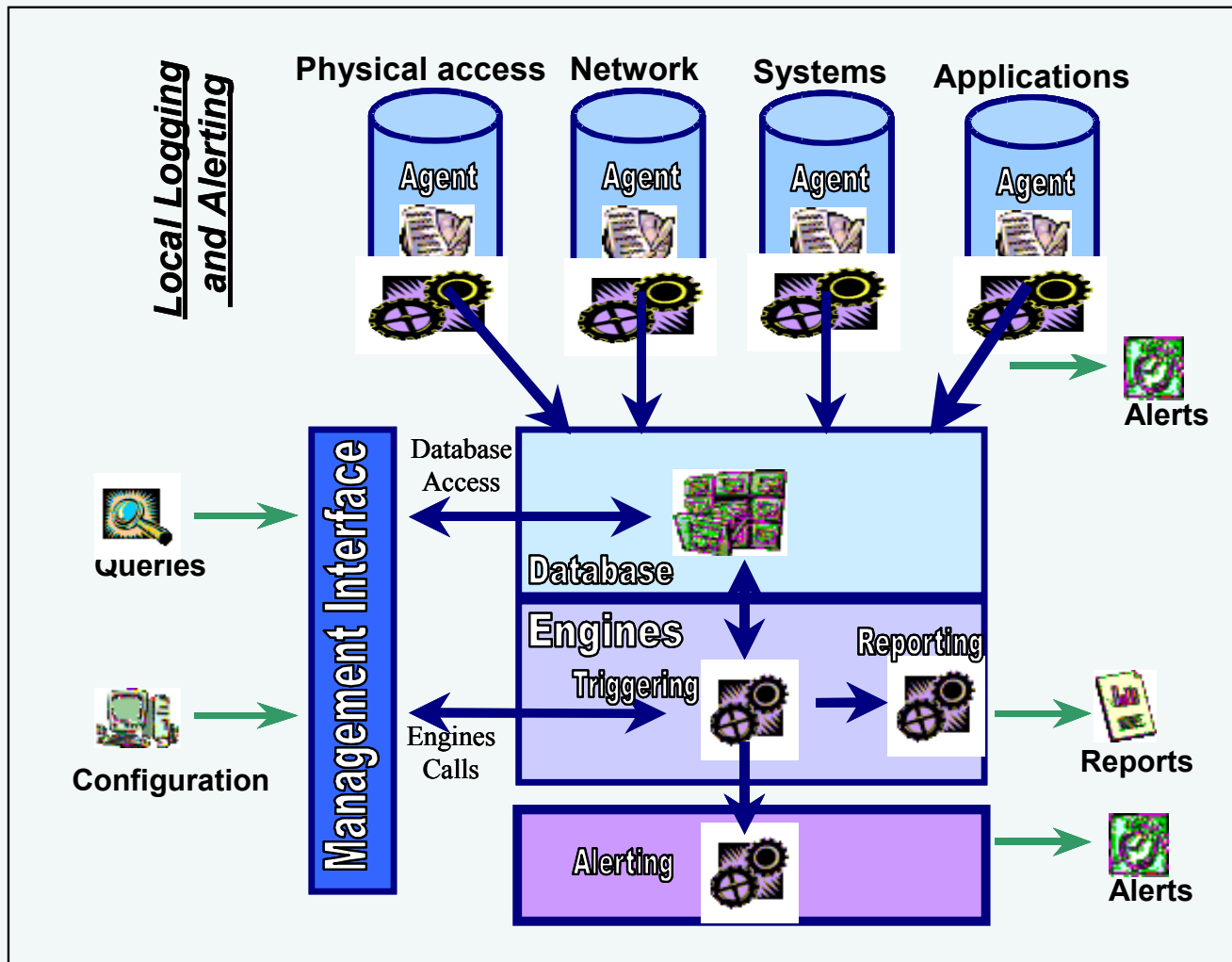
Ogeris

Organisation & Security
in Information Management
www.ogerris.be

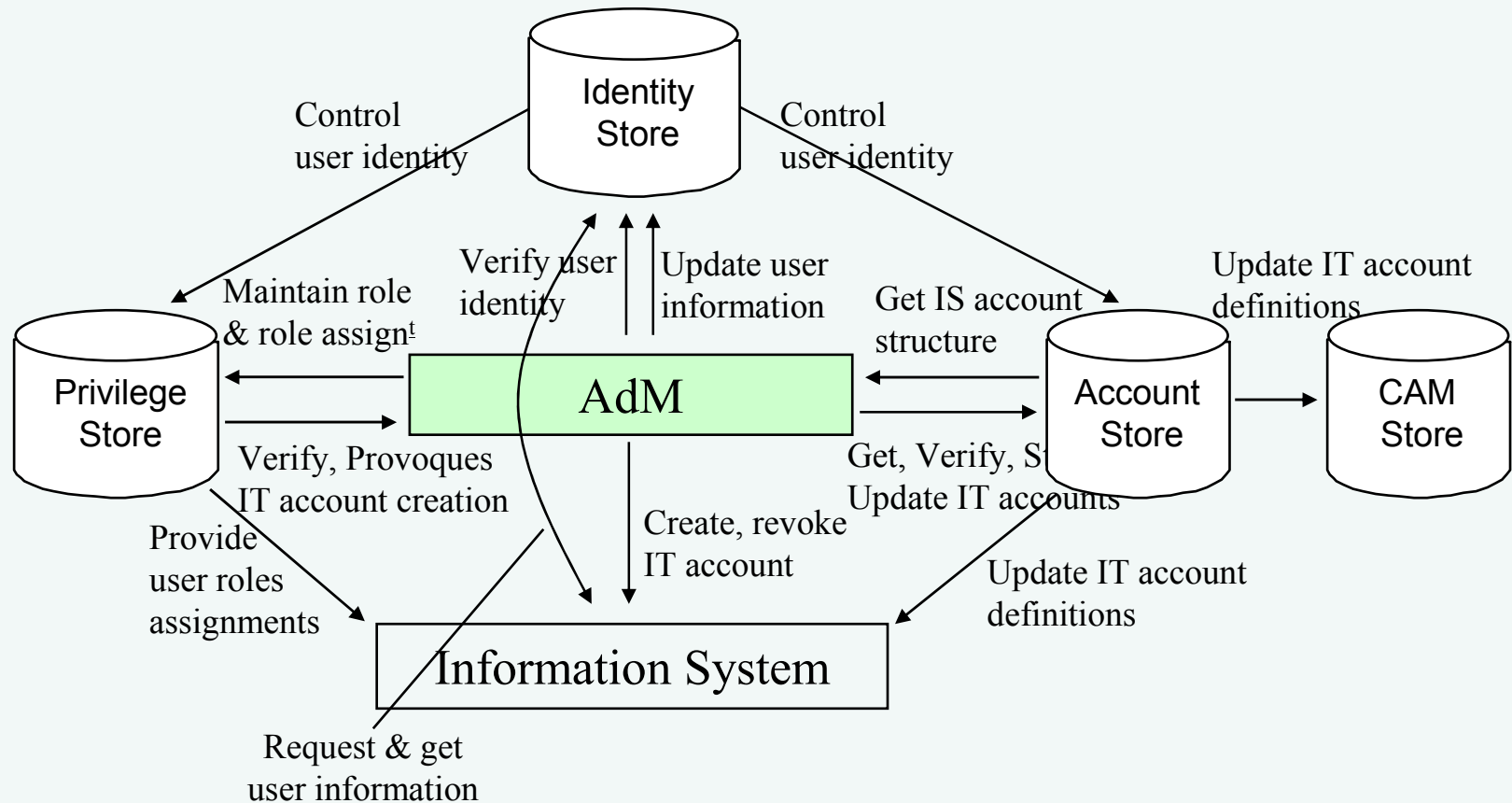
CAM, a three tiers approach

- API on gatekeepers to reroute the authentication process
- AAP's that face the users' requests
- Central Authentication Service
 - Mutual control with IdM
 - AAP support and control
 - Multiple authentication process and policies
 - Secure communication between peers
 - Enabler of SSO

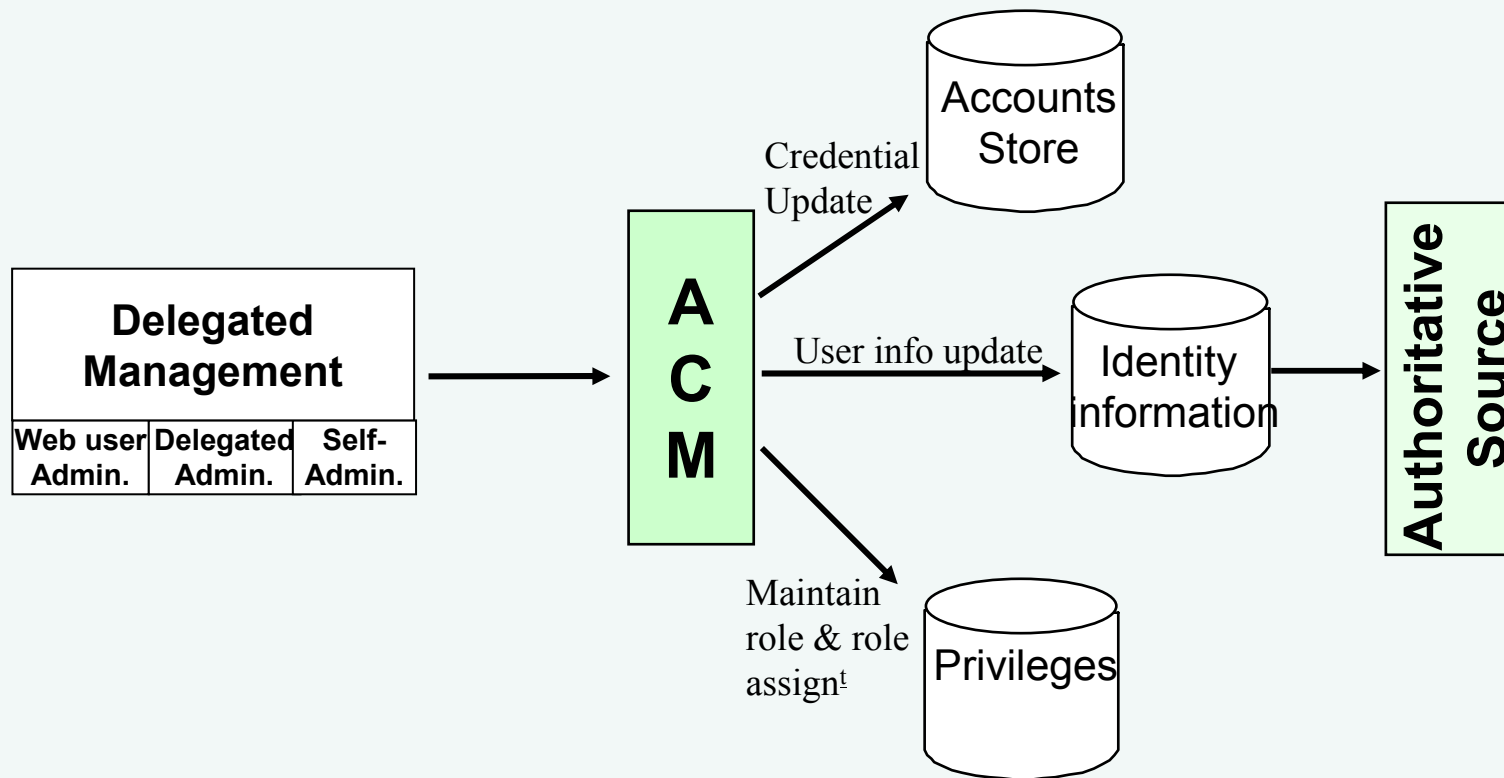
Usage Control and Monitoring Management (UCM)



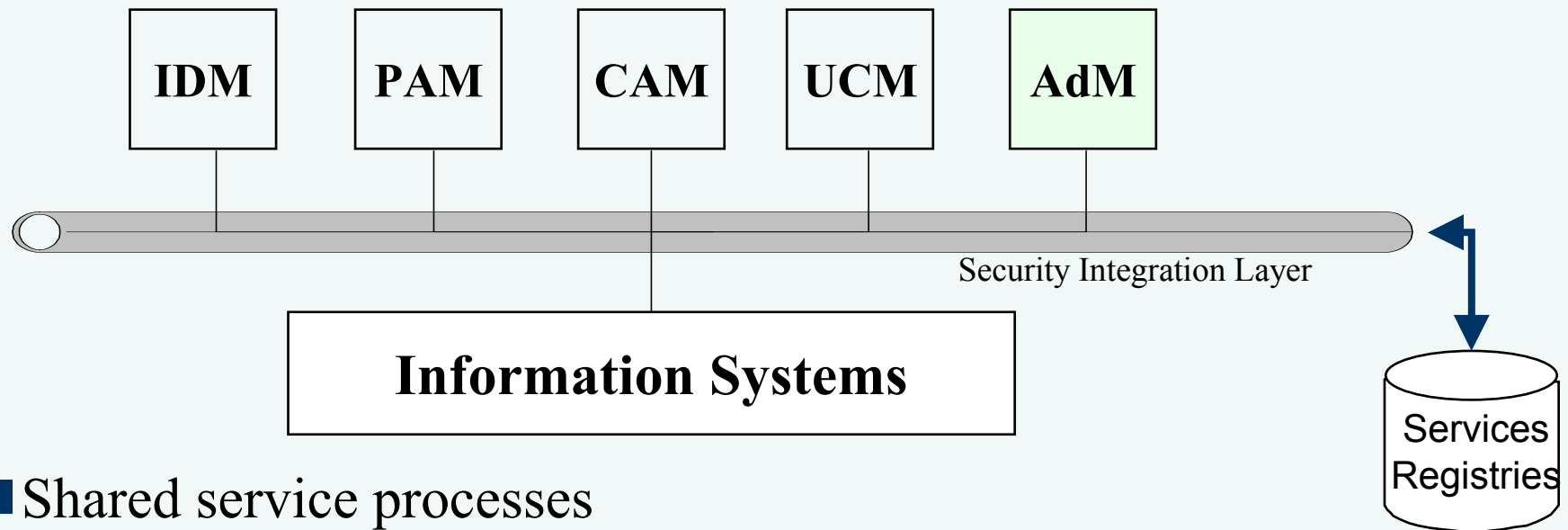
The Administration Management (AdM), The IAM transaction monitor



Adm provides distributed administrative means for IAM stores



Security Integration Layer

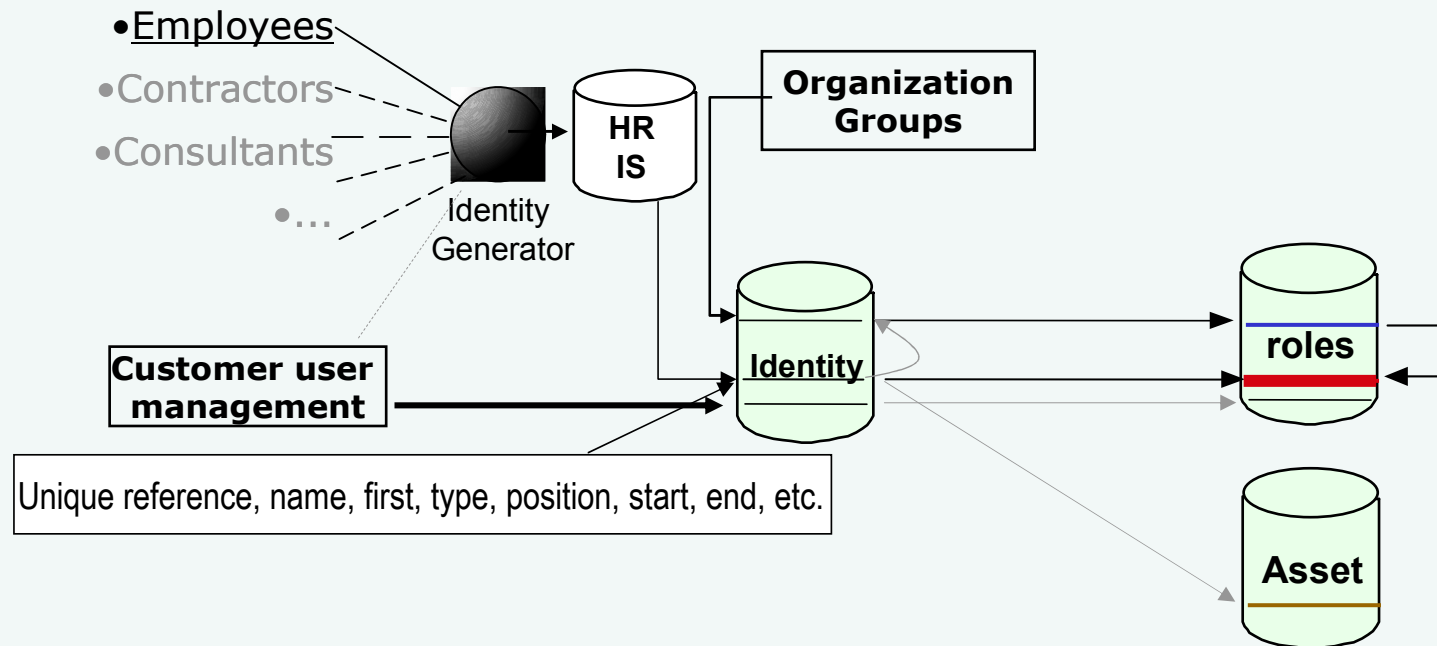


- Shared service processes
- Process governance
 - Consumer management
 - Information management
 - Policies
- Service management (capacity, configs, changes, etc.)
- Monitoring and Incident controls

Process understanding

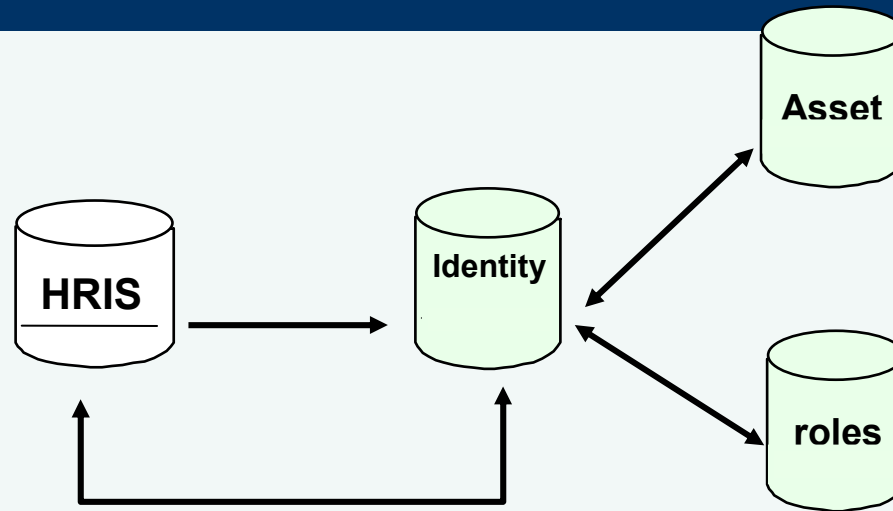
- Entry process
- Exit process
- Change process

Entry process understanding



Organisation & Security
in Information Management
www.ogерis.be

Exit process understanding



- Status alignment
- End date updated
- Subsequent removal of roles and asset ownership

Progress ↓

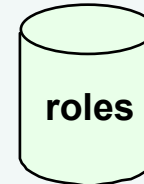
HR record may persist



Identity may also persist



Roles are suspended, then revoked



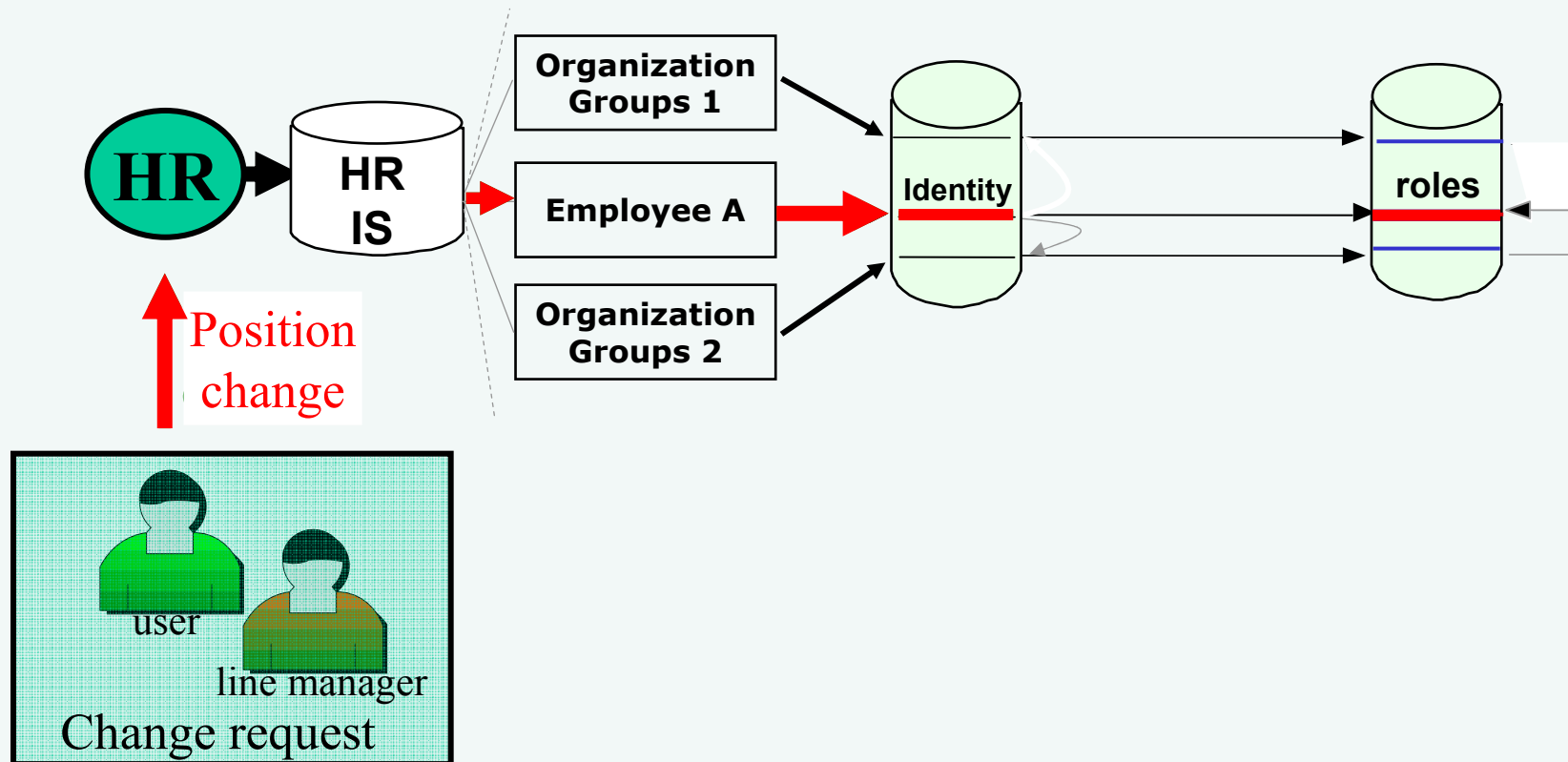
Asset are returned



Ogeris

Organisation & Security
in Information Management
www.oggeris.be

Change process understanding



Success Factors

- Staffing and ability to deliver
- Assurance of private data protection
- Perceived simplification: cheaper and faster access to service
- Effective simplification of administrative burden
- Trust relationship between Service Consumers, Service Providers, Service Suppliers

Conclusions

- A process driven approach
- An independent model
- A need for physical decoupled processes of IdM, PAM, CAM, UCM
- A model that needs judgments: Need to be adapted to the context.
Help to developing specific IAM
- The model fits to new trend of software developments
- The model provides synergies and return
- A mature reference but still on progress
- Products are available around the world

Access Management

Questions

To get more

- www.ogeris.be
- www.iso.org

Tel. : 0477/22.59.53

e-mail : cstenuit@ogeris.be

