IAM

André Mariën

There is a problem with IAM

- IAM projects are high-risk projects and at the same time critical improvement projects
  - High failure rates do not inspire management confidence and will stress the relationship, between IT and business once more
  - Organizations that do not fail often find that many of the expected benefits have not materialized
- The necessity of tackling the IAM problems facing all organizations, and especially larger ones, makes finding the root cause of the difficulties that undeniably exist a worthwhile quest
  - Do we lack the right tools or the silver bullet model?
  - Is the complexity inherently too high to cope with?
  - Are the people incompetent or badly trained?
  - Or do we look for solutions in the wrong place?

Business objectives

- Know you users
  - Manage their identities
- Ensure compliance
  - Accountability, data protection, duty segregation
- Prevent unauthorized access
  - Authenticated, Authorized, access control
- Affordable
  - Fit with business and IT reality
  - Maintainable and mostly automated

Security lingo objectives

- Ensure confidentiality
  - Confidentiality is often equated with encryption
  - But access control is key for confidentiality, while encryption and key management are one form of support for access control
- Ensure accountability
  - The link between the physical world (people of flesh and blood) with technical world (userID/password, certificate, token, claim, …) is a crucial part
  - Manage privileges, but also manage privilege management
  - Accurate and comprehensive reporting
- Avoid conflict of interest
  - Identifying conflict of interest situations and defining duties with segregation constraints
  - Identity management must be enterprise wide: link all logical instances to the actual, physical principal
- Ensure least-privilege
  - Only privileges that are needed, but when needed
  - Organizational agility: acquiring and dropping privileges follows business changes immediately

Objectives - approaches

Objectives:

- Risk driven?
- Compliance driven?
- Business driven?
- Efficiency?
- Response time?
- Complexity?

Approaches:

- A BIG IAM vendor and integrator
- Best of breed:
  - SSO, Provisioning, IDM, Workflow
- Custom made – product oriented
- Differentiator – utility
- Management of accounts? Of identities? Self-service? Federation?
- Data replication or integration
- Process centric
- Transversal: across units
- Context dependent authorization
- Architecture input

Your first decisions may put the whole program at risk

- Classify it as an IT project
  - All will go well in the development and implementation phase
  - Nothing but trouble near roll-out and production
- Decide on a company wide model, and use for instance RBAC as a safe choice
  - Proof-of-concept test succeed
  - Roll-out and maintenance slowly turn into nightmare
- Pick a product, configure, do some role mining, done
  - Great plan
  - Try outs seem to work
  - Role mining produces on larger scale are less convincing
  - No underpinning of roles, so how to maintain?

- Let’s move one step back, and think

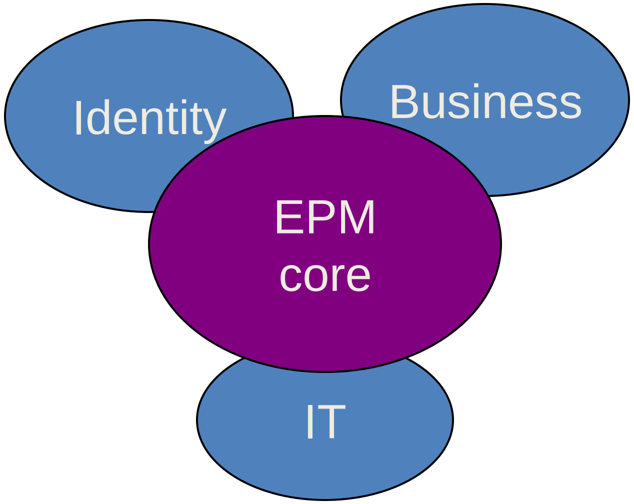
Observations

- Identity space
  - There are multiple systems managing identity information, spread across the organization, from different vendors with different purposes, and they are here to stay
  - Fundamental to “identity” is it’s uniqueness, but many views coexist
- Business view
  - There are many ways business look at controlling access: based on functions, based on tasks, based on organizational structure. Any attempt to force this into one way only is sure to meet resistance
  - Business needs drive authorization and access control: the business need leads to authorizations and access granting
- Technology space
  - Every application, service, package comes with its interface to account repositories, supports some authorization and access control model(s) like userIDs with semantics, RBAC, groups, ACLs, …
  - Some systems are immutable, really inert, whereas others come and go, or are replace by new ones with a different vision

Four domains

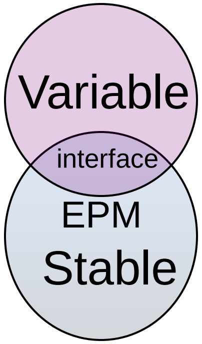
- Divide and conquer: Four domains
  - Identity management
  - Business privilege management
  - Technical authentication and access control
  - Enterprise privilege management: the domain linking it all together

- Core activities
  - Entity registration and correlation
  - Business privilege modeling and model population
    - May include role mining
  - Access control solutions and provisioning
    - Includes credential management, SSO
    - Includes repository synchronization, credential distribution, self-management
  - Privilege management and privilege use
    - Authorizations
    - Authorization management
    - Conflict of interest, segregation of duty management
    - Policy Information Point service
    - Policy Decision Point service
    - Access Control service
    - Provisioning drivers



Four domains: do

- The three satellite domains must be able to evolve independently
  - Keep the center very stable
  - Maintain interfaces as much as possible
  - Absorb changes in the mapping on the borders (hinges)
- Minimize impact on other domains from
  - Changes in identity management solutions
  - Business unit reorganization, model for privilege management changes
  - Technology changes: new solutions, other provisioning, other repositories



Identity management

- Approaches
  - Registration authority, with local registration agents
  - Correlation extensions in the various solutions
  - “Master data management” approach
- Principle: Identity as root
  - Identity-rooted data modeling
  - Specific extensions
    - Technical identities, and link with accountable identity
    - Third party stub identities , and link with accountable identity

Privilege: a central concept

- Privilege Definition
  - Privileges are a business concept: no techno gibberish
  - What privileges exist in the enterprise?
  - Identification, categorization and modeling of the different types of privileges that exist within an enterprise
- Privilege Assignment
  - Mapping privileges to identities
  - The act of creating a linkage between instances of parties and privileges.
- Permission definition
  - Permission as abstraction of access differentiation as supported by the system
  - “consult”, “update”, “approve”, “admin”: regardless of how it is implemented
- Privilege Provisioning
  - Translate privileges into permissions into provisioning data
  - Translate privileges into implementation-specific permission statements
  - Feed provisioning system with translated data
- Privilege Control
  - Check if required permissions for the given context and operation are assigned to the requesting entity for the resource
  - Security function which provides the ability to permit or deny the use of a particular resource by a particular party in line with the defined and assigned privileges.

Business privilege management

- Rooted in business
  - The privileges of an entity are a consequence of the business context
- Business units have multiple privilege models
  - Organizational Roles
  - Organizational structure
  - Task based
  - Professional certification or authorizations
  - Unstructured subsets (for instance workload driven)
- High level differences between
  - Unit type: HR, finance, sales, IT
  - Business: bank, insurance, trading
- Primary schemes:
  - Chain: Role, organization and credential to tasks to privileges
  - Direct: Identity to privileges

- Approach:
  - Map business model to a limited subset , for instance functions, tasks, organizational units, accreditations
  - Map this subset to privileges: authorization step

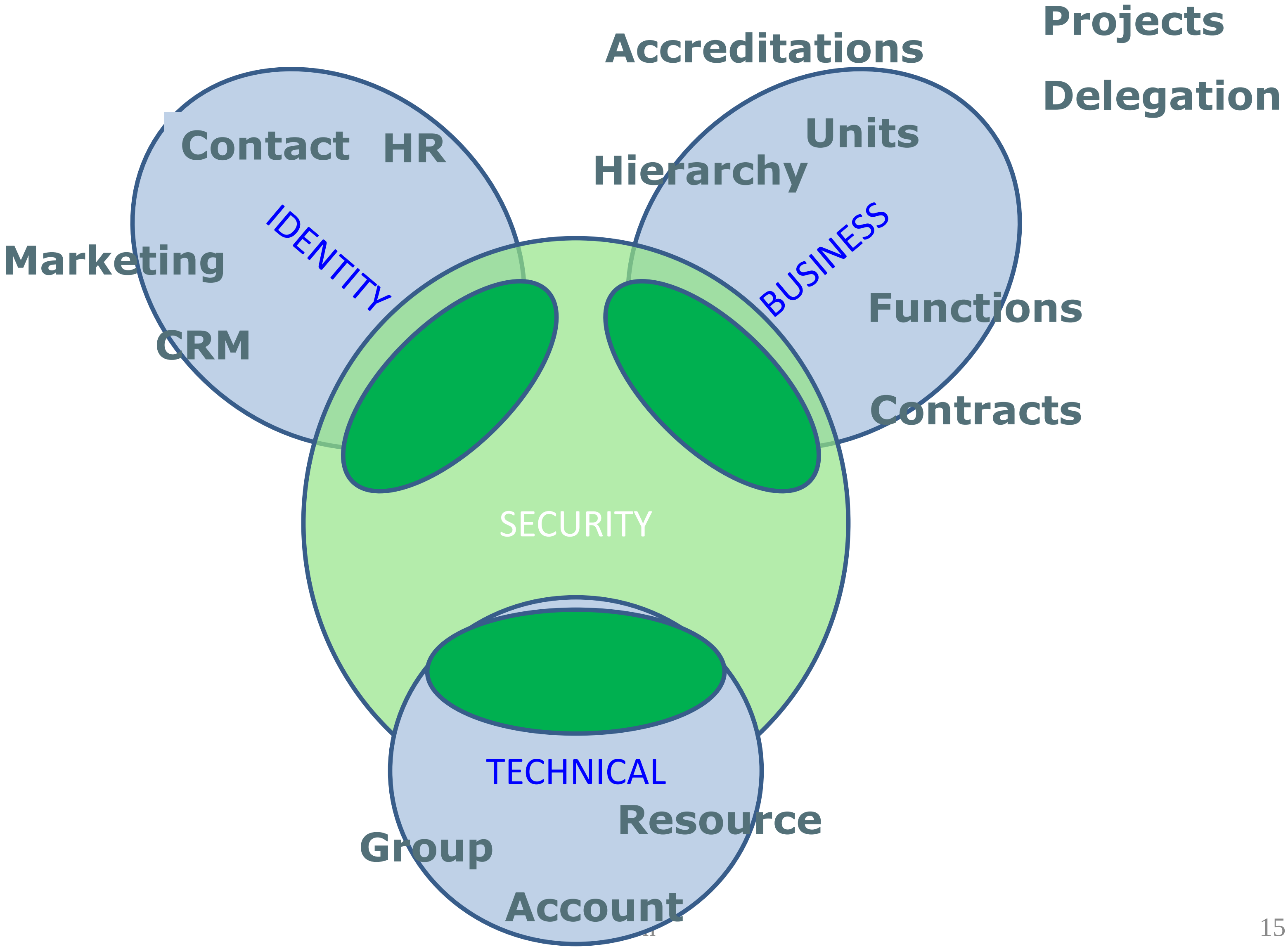
Technical authentication and access control

- Account management
  - Accounts as a consequence of privilege assignments
  - You get an account because you have the authorization to do something
- Authorization often hidden inside applications
  - Model per application
  - No model at all
- Technical privilege modeling
  - Permissions: abstract specific implementation
  - Three distinctions to make: user, supervisor, manager; implementations can vary:
    - Three classes of userIDs (Uxxx, Sxxx, Mxxx)
    - userID must be member of the right group
    - ACL contains userID
- Access control models
  - OASIS model provides solid base: policy (enforcement, decision, information, administration) points: PDP, PEP, PIP, PAP
  - Provide increasing levels of integration
    - EPM as a PAP: externalized management
    - EPM as only a PIP: minimal integration
    - EPM as a PIP and a PDP: externalized access control
- Provisioning, SSO, federation, exceptions, credential management

Four domains: don’t

- Don’t attempt to enforce one identity management system
  - HR, CRM, partner management, providers: not the same
- Don’t attempt to force business to think in one model about privileges
  - Ok to make them consider alternatives
  - Ok to separate concerns
- Don’t use a technological one-size-fits-all, end-to-end solution
  - Legacy solutions do not follow newer models
    - Group based, Account based, role based, … exist
- Don’t think that because you can accommodate everything in one model, it is a good idea to do so
  - A good engineer can accomplish anything with anything, but it may be very ugly, and the TCO may be prohibitive
- Don’t underestimate the effort to create an enterprise solution
  - Human factor, processes, legacy, transitions, …
- Don’t believe that you can take a snap-shot, model and deploy in an atomic step
  - Before the snap-shot is finished, it is outdated
  - Reverse engineering may be bad engineering: consolidate the errors
  - A conversion will take years, going faster will delay it more

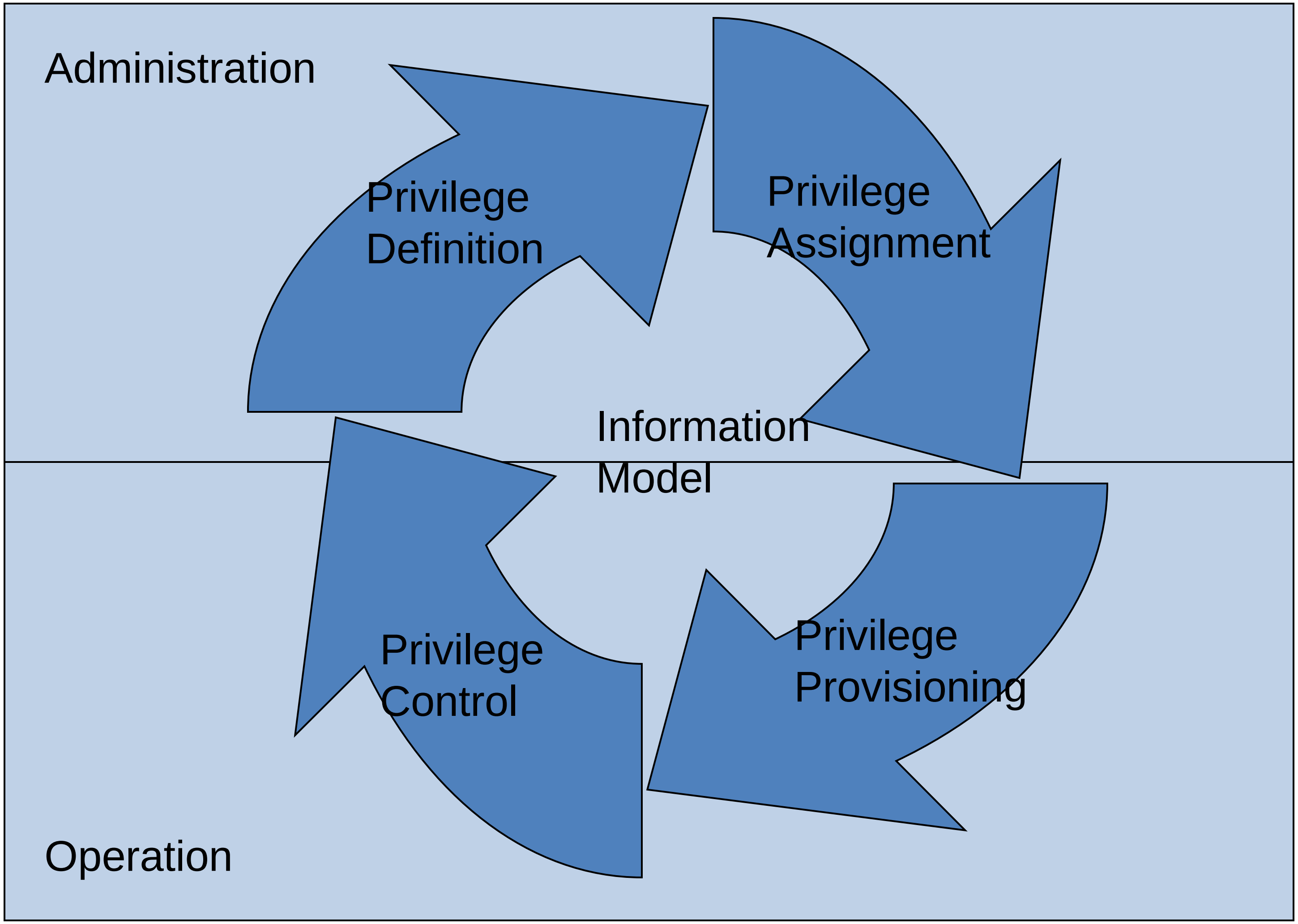
The four-world model



Process: business drives

- Processes and process design matter, a lot
- Move away from “request access”
  - Access granting is based on business decisions
    - No need to ask for an account
    - No need to check business reason for a request
  - Revert thinking: business decision implies granting access
    - Not: ask for access as a separate process
    - Changes in business imply granting the necessary access
- Task assignment, work unit assignment, … are business events at the basis of privilege changes
  - Should lead to privilege changes
  - Privilege changes should lead to account requests or removal
  - No need to “request” new or delete old privilege

Privilege processes



Sub problems and Aspects

	Definition	Assignment	Use
Identity	What is it? Where is it? Kind of identity	How to introduce? When to assign? When to end?	Crosslink Existance Identity reference
Account	Realms Systems Types	Account management	Authentication
Rights	Model Model instances	Authorization	Access control

Automation

- Process: Three steps
  - Legitimate request for access?
    - Implied by business decision.
    - Derive situation from business data
  - Authorize access
    - Principle-based authorization, not case-based.
    - Modeling exercise: define privileges and mapping onto business attributes
  - Enable access
    - (Provisioning)
    - Update access control repositories to allow access.
    - Update account repositories
    - Update access control component database (PIP, PDP implementation)

- Business privilege assignment
  - Based on principles
    - “All employees are authorized to access email”
    - “Only personnel in HR has access to personnel records”
    - “Only managers have access to evaluation reports”
  - Based on business information sources
    - “is an employee”
    - “works in HR”
    - “is a manager”
    - “is a certified accountant”
- Automatic:
  - No approval delays for automated privilege assignment
  - Privilege removal: as soon as business context changes
- Responsibility:
  - Direct impact on operational rights
  - Change throttling/buffering

Additional complexity

- Constraints
  - Incompatible privileges cannot be combined
  - Important objective for business
  - Issues: where to check? When to check? Override?
- Contexts (mobile workforce, different commercial contexts)
  - Privileges assigned in context require context verification (acting for, from, …)
- Delegation (illness, holiday)
  - Delegation as normal business practice
    - Not exceptional
    - Not via credential passing
- Transitions (function change, role change, in/out)
  - Transitions as normal business practice
    - Start working, move to different unit, move to different function
  - Change takes time
    - coexistence of two situations
    - Controlled move
- Parameterization
  - Opaque parameters for specific business information transfer to access control components
  - Context information

Planning - components

- Identity management
  - MDM projects for all identity data
  - Identification of repositories
  - Registration coordination and authorities
  - Correlation and assurance
- Business
  - Empowered
  - Made responsible: directly steering IAM
  - Identification & formalization of master data
  - Completeness of information required
- Privileges
  - Identification and formalization of privileges
  - Mapping business attributes to privileges
  - Mapping privileges to access control abstractions
- Process
  - Process redesign
  - Processes and workflow
- User involvement
  - Transparency
  - One-door: portal for IAM
- Access control data repositories
  - Identification of repositories
  - MDM style
  - Repository Integration style
    - Provisioning approach when relevant
    - Application adaptations when relevant
    - Fronting when relevant (proxy, filter, …)
  - Permission modeling

Some existing authorization models

- Access control basics:
  - Mandatory Access Control (MAC)
  - Discretionary Access Control (DAC)
- Identity/User & Group Based Access Control
  - Access permissions are directly associated with a user or user group (e.g. ACLs)
- Role-Based Access Control (RBAC)
  - Access permissions are based on the role(s) a subject is performing
    - model extensions: adminstration (ARBAC), context-awareness, constraints, privacy, SoD, additional layers of abstraction …
- Context-Based Access Control
- Content-Based Access Control
- Rule (RuBAC) & Attribute (ABAC) Based Access Control Access decisions are based on the evaluation of rules expressed in terms of attributes of the subject, action, resource and environment
- ORBAC

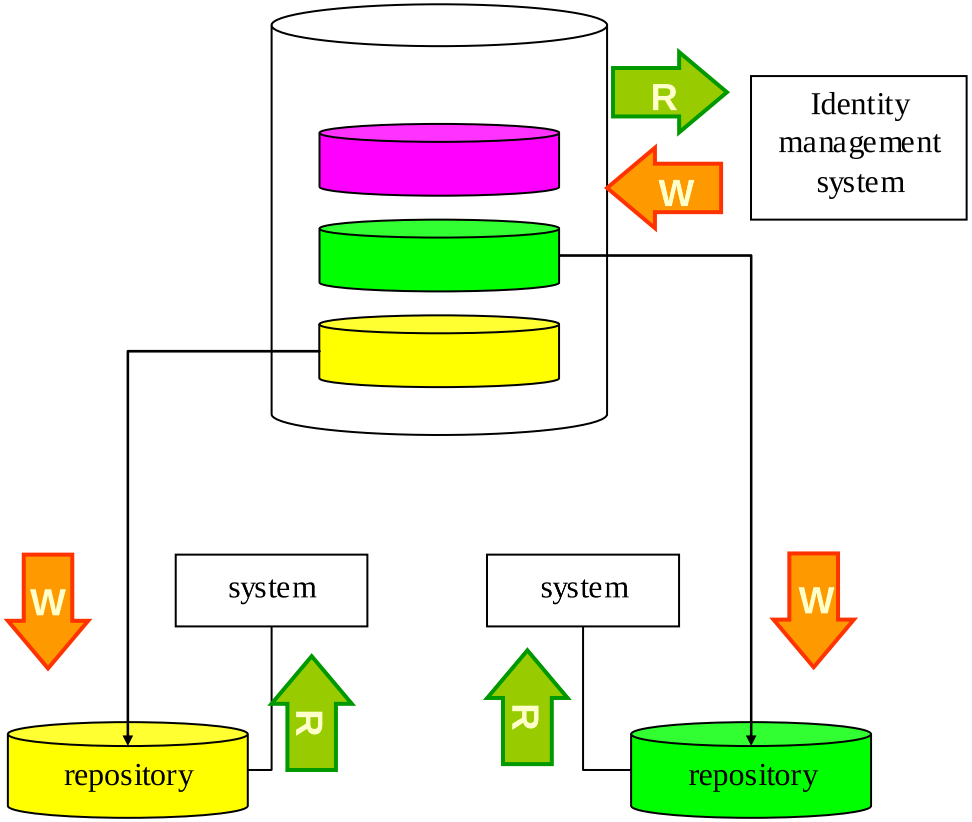
The 3 IAM layers
Policies – Model – Implementation

Component	Description	Scope	Governance
Security Policies	•The definition of the security goals, the managerial and administrative mechanisms to achieve them	•The whole of the Business organization including the Security Actors - BSO	•Exerted by Regulatory entities, Audit and Compliance
Security Model	•The scheme for specifying and enforcing the security policies. Typically founded upon a formal model of access rights	•Identification and certification •Logical Access Control	•Exerted by ISM and its branch IAM •Operationally enforced by Business Line Management
Security Implementation	•The realization or execution of the security model. The act of carrying out and enforcing the security policy and making it tangible	•User and ID certification •Access and rights management •Target asset authorization	• Service Desk Security Services • Operationally implemented by Business Lines Security Organization and actors

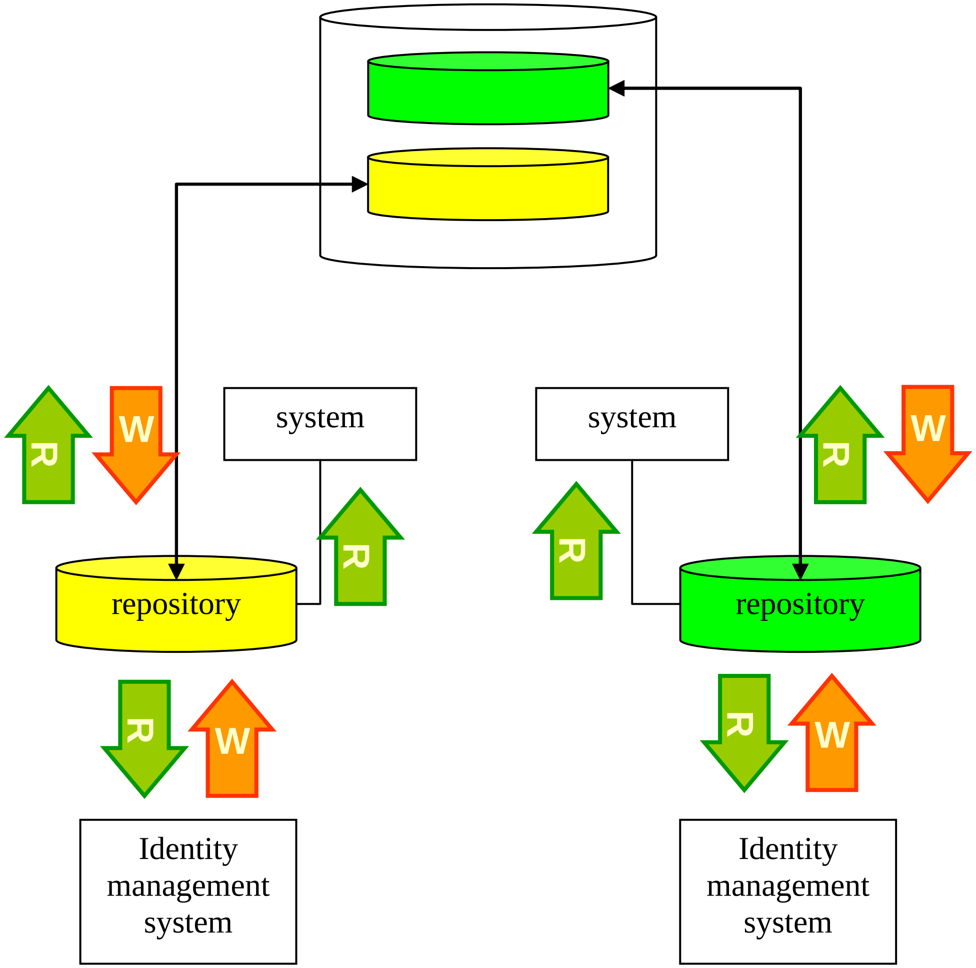
Master data management

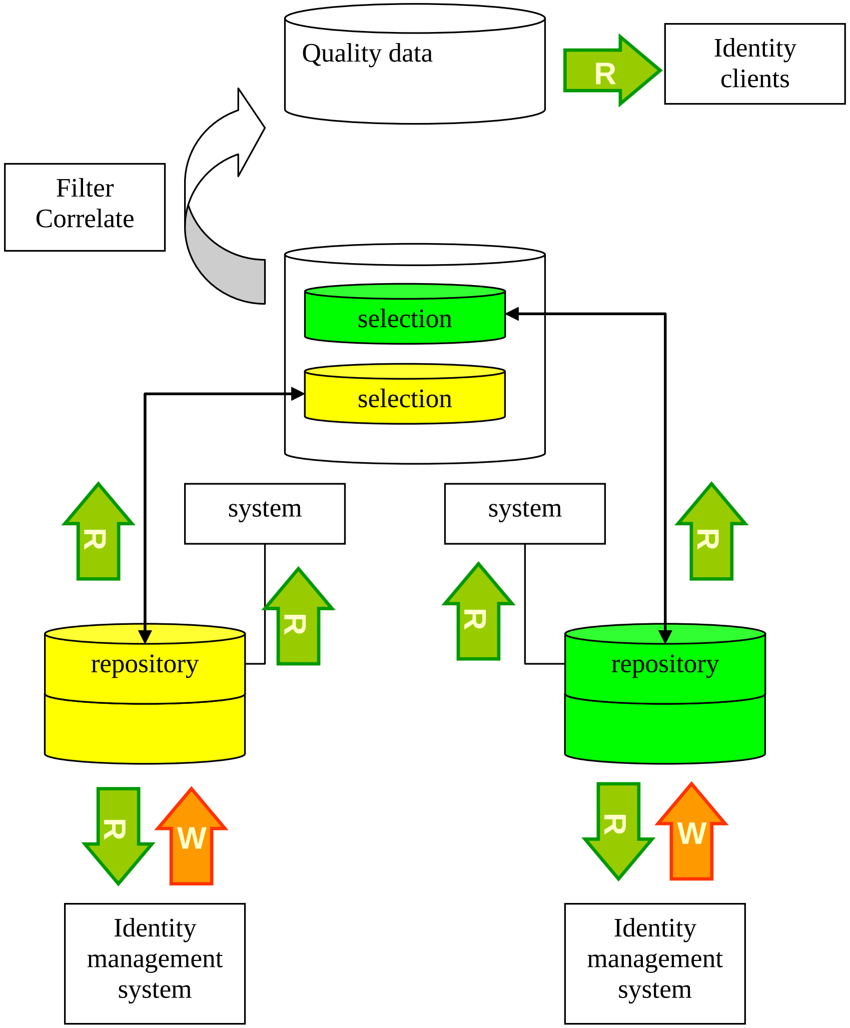
- One master
- Clearly determine which is the master
- Various set-ups possible

Management master with provisioning to slaves



Distributed repositories and management, with consolidation

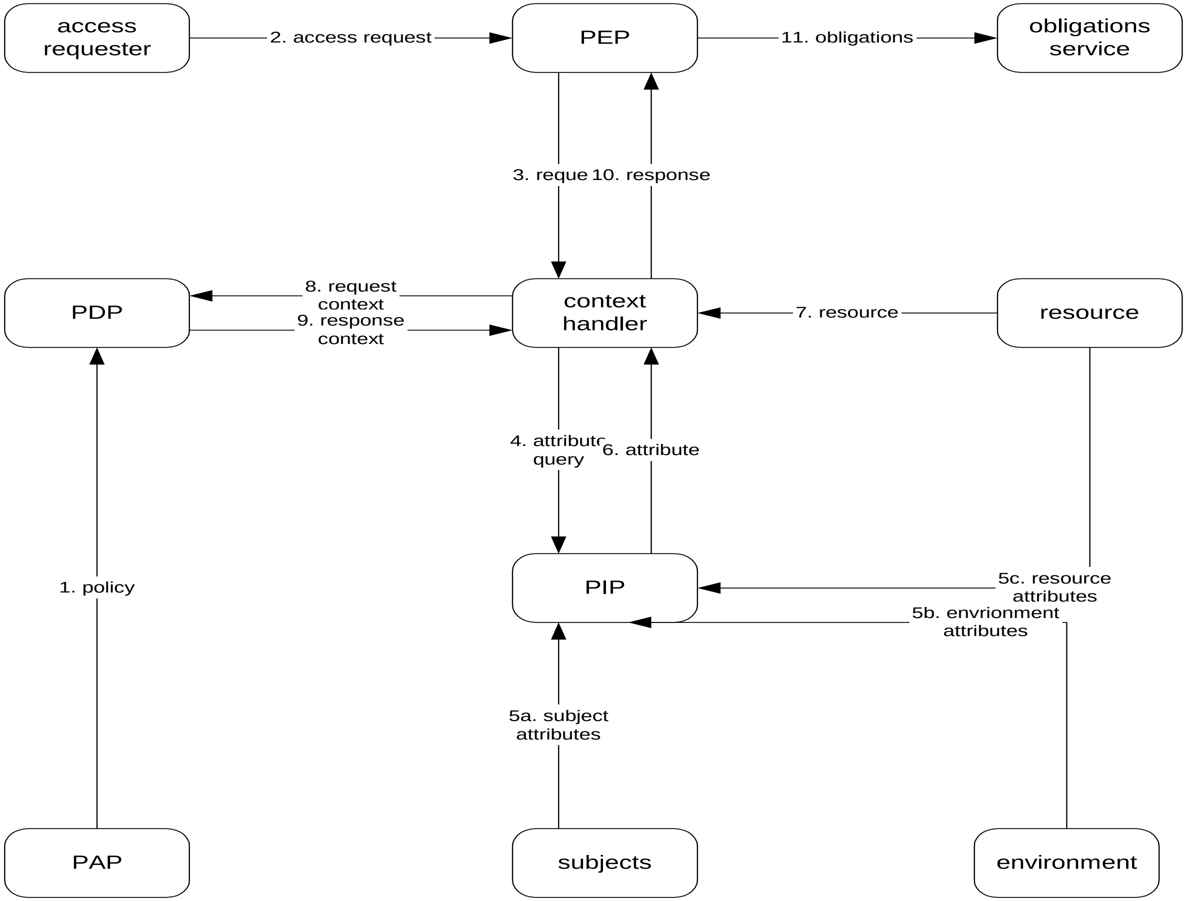



Quality data
R
Identity
clients
Filter
Correlate
selection
selection
R
system
system
R
R
R
repository
repository
R
W
R
W
Identity
management
system
Identity
management
system

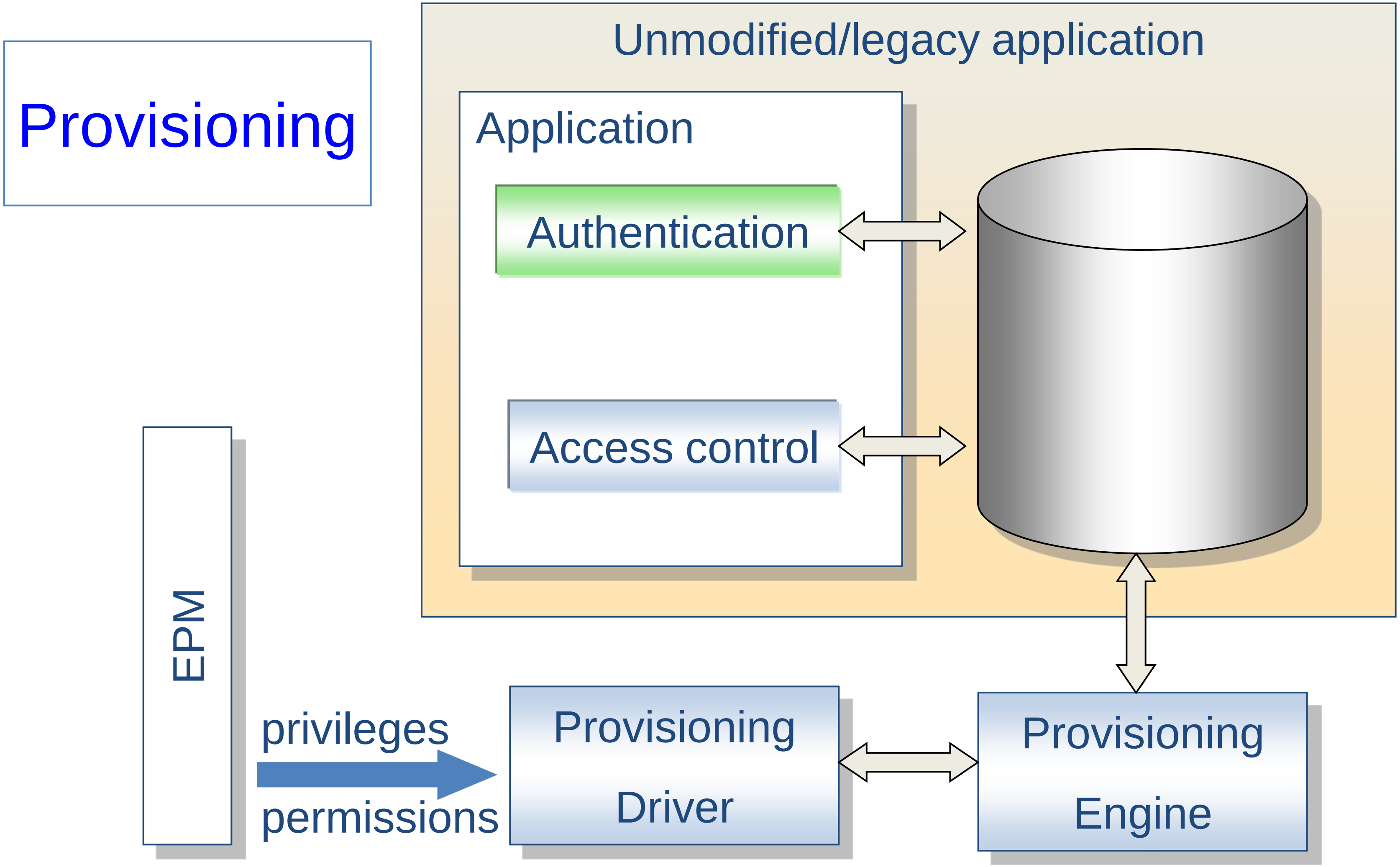
OASIS XACML based view

- Differentiation: location of the Access Control Enforcement Point (PEP), Decision Point (PDP), Administration Point (PAP) and Information Point (PIP):
  - Provisioning Model (PAP[, PIP]):
    - privileges are translated into realm permissions and provisioned towards the different realm masters.
    - PDP, PEP: in the applications
  - Privilege Information Retrieval Model (PAP,PIP):
    - PDP, PEP: in the applications
    - But: PIP consulted to take decision
  - Centralized Privilege Control (PAP,PDP[,PIP]):
    - PEP: in the applications
    - PDP is externalized
    - possibly PIP consulted to take decision

XACML Data Flow Model

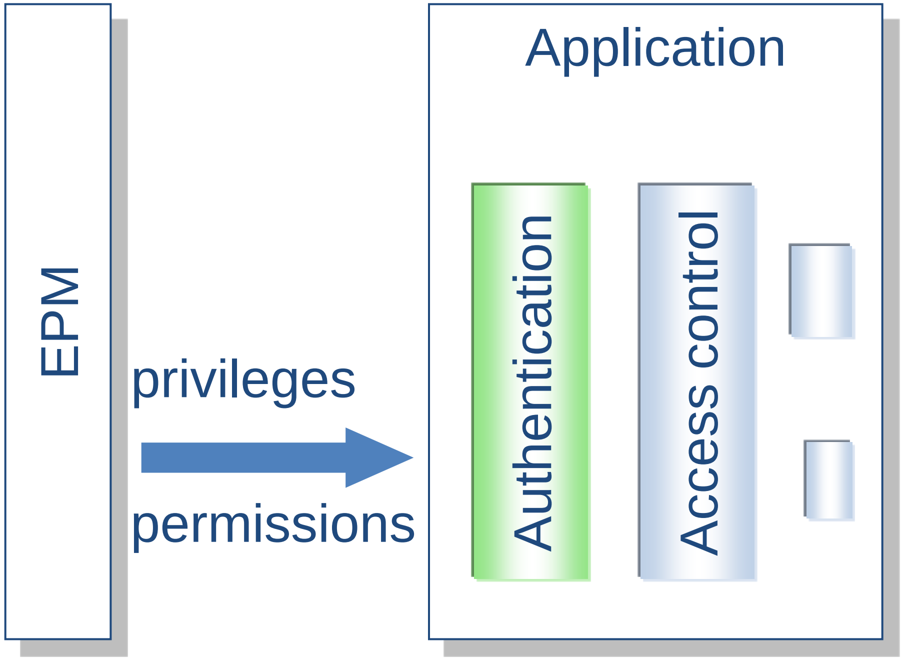


Application interaction patterns



Application interaction patterns

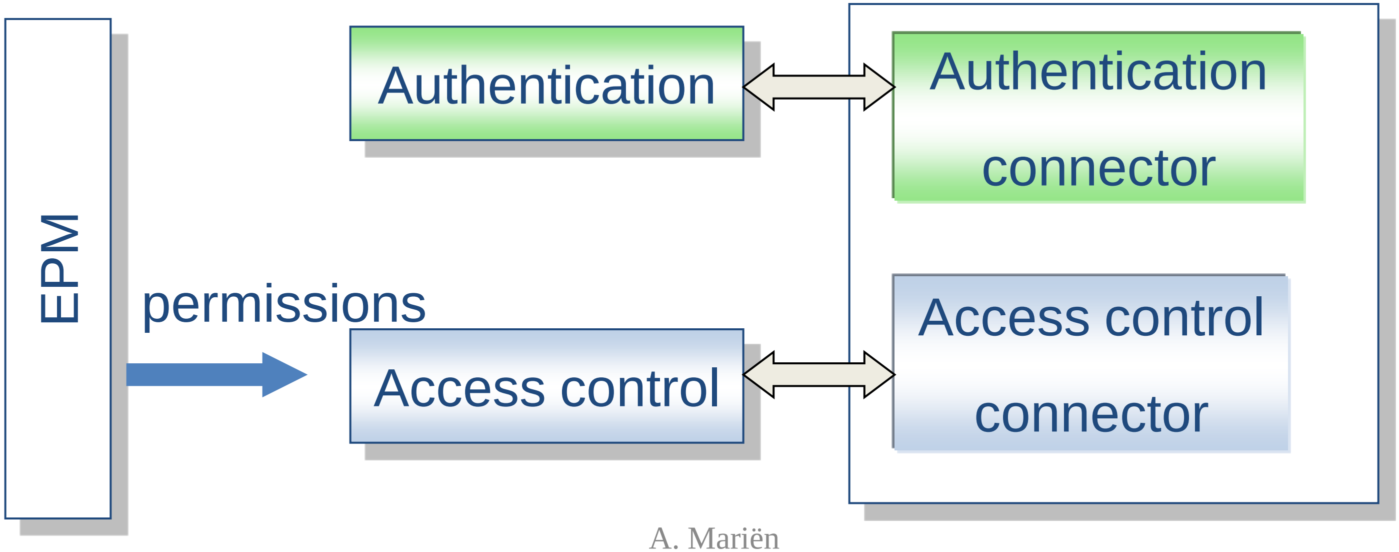
- EPM
  - Maps account to permissions
  - Provides permissions to the application
- Application
  - Request permissions for an account
  - Interprets the permissions, and possibly other elements, to check if access is granted



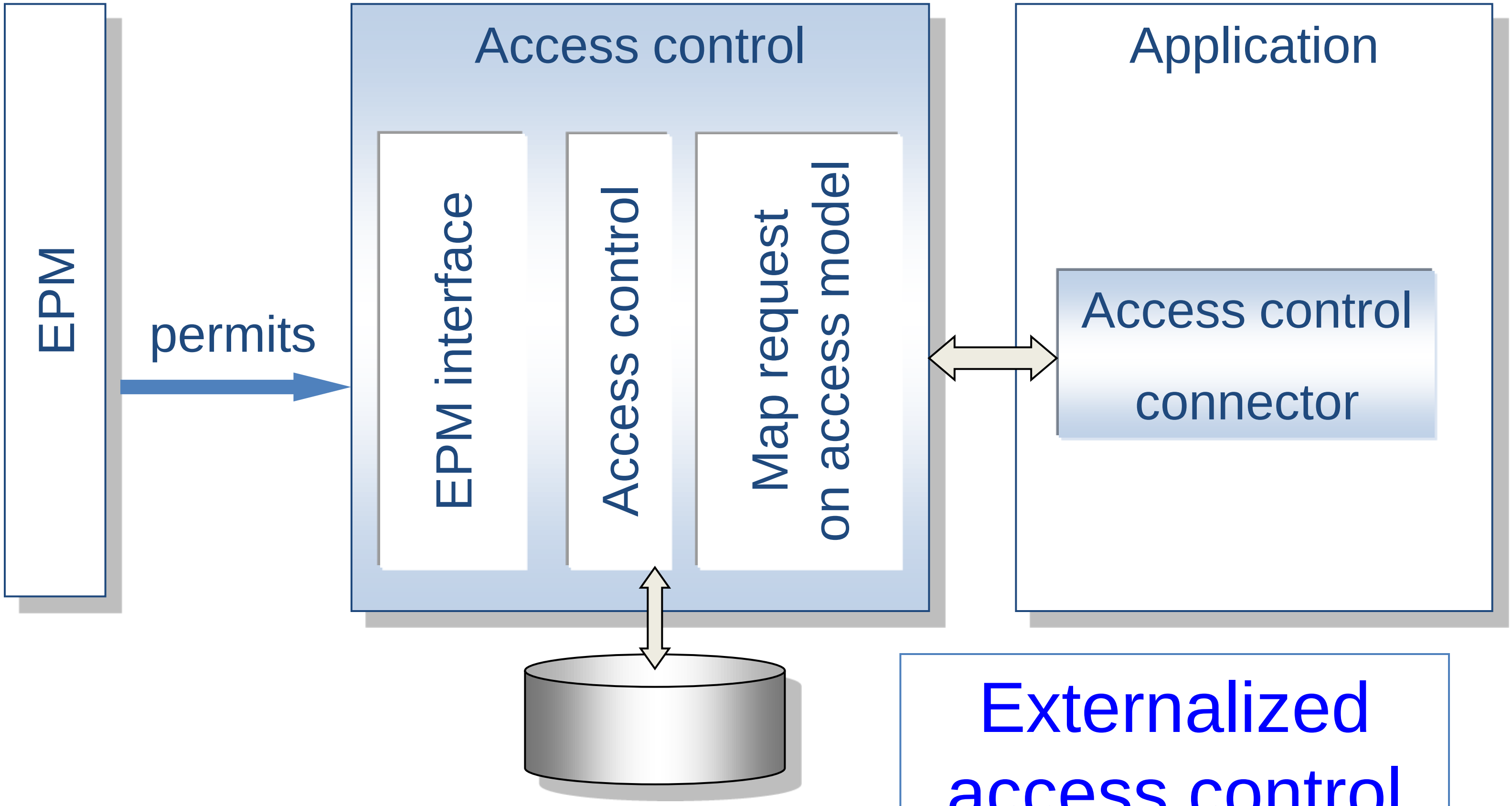
Privilege information consumer internal access control

Application interaction patterns

- EPM
  - Maps account to permissions
- Access control component
  - Gets access request information (account, parameters)
  - Obtains permissions (with parameters) from EPM
  - Takes access control decision
- Application
  - Uses the access control component to get a decision

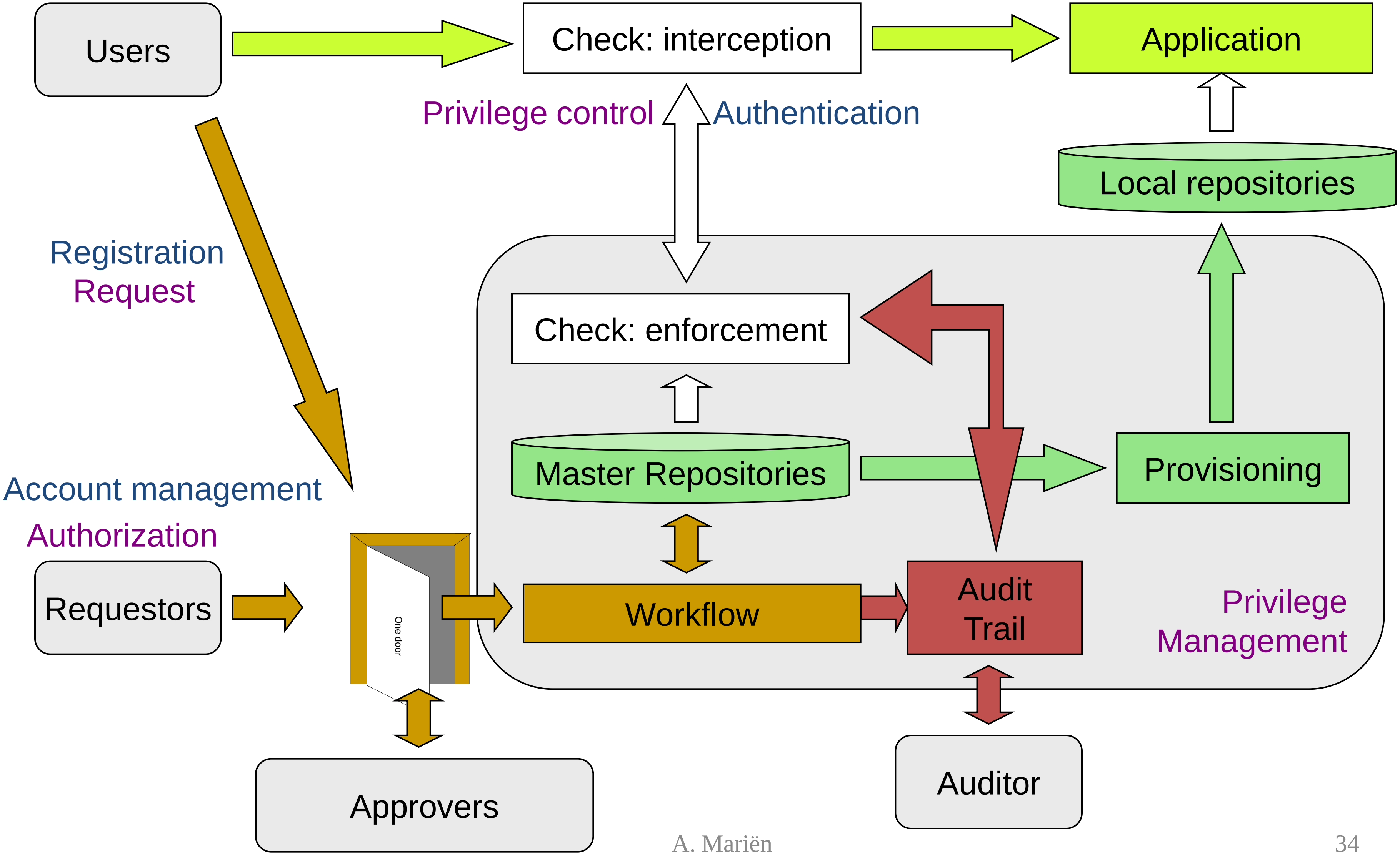


Application interaction patterns



Externalized
access control

High level security architecture



Users

Check: interception

Application

Privilege control

Authentication

Local repositories

Registration
Request

Check: enforcement

Master Repositories

Provisioning

Account management

Authorization

Requestors

Workflow

Audit
Trail

Privilege
Management

Approvers

Auditor

Conclusion

- EPM is a big undertaking, touching many parts of the organization
- Unless all of aspects are addressed, the objectives will at best be partially met
- Both the inertia of an organization and its dynamics claim their rights: ignoring either is a high risk
- Business, not IT, should be in the driving seat
- Business processes and models are much more important than technical access control models

- A man warned is forearmed

Questions?