



Entitlements Access Management for Software Developers



Market Environment

The use of fine grained entitlements and obligations control for access to sensitive information and services in software applications is a rapidly emerging requirement in the global IT market.

The requirement is driven by government security and privacy legislation.

The developing standard is the XACML based fine grained access control framework.

Application developers are faced with critical decisions and costs if they are to compete in the market where XACML based Entitlements Management will be a requirement

This is fast becoming a necessity rather than an option



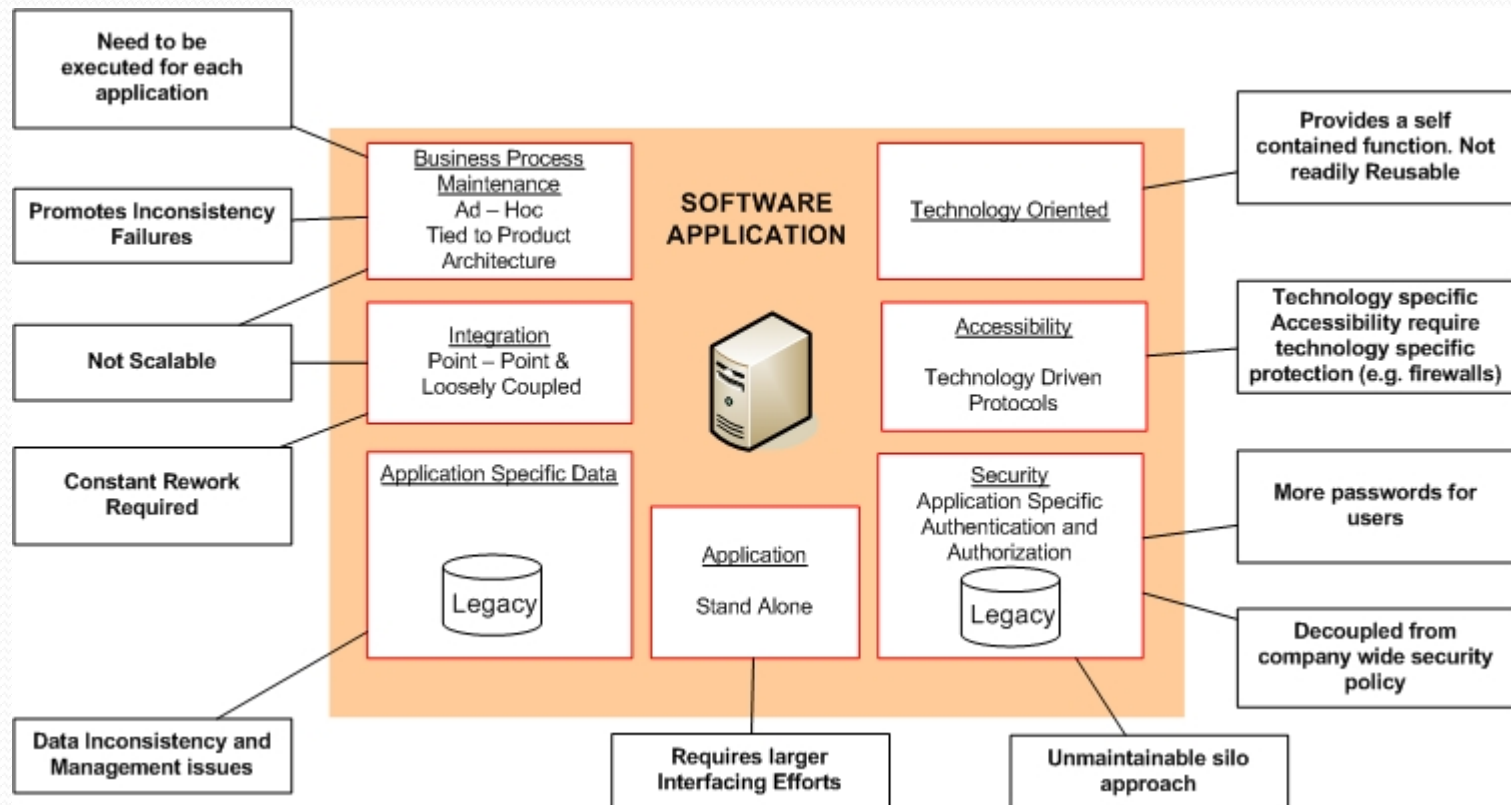
Technology / Product Driven Architecture

- Increased:
 - Management Cost
 - Data Duplication
 - Auditing Efforts
 - Security Risks
 - Inconsistency
 - Difficulty to prove compliancy



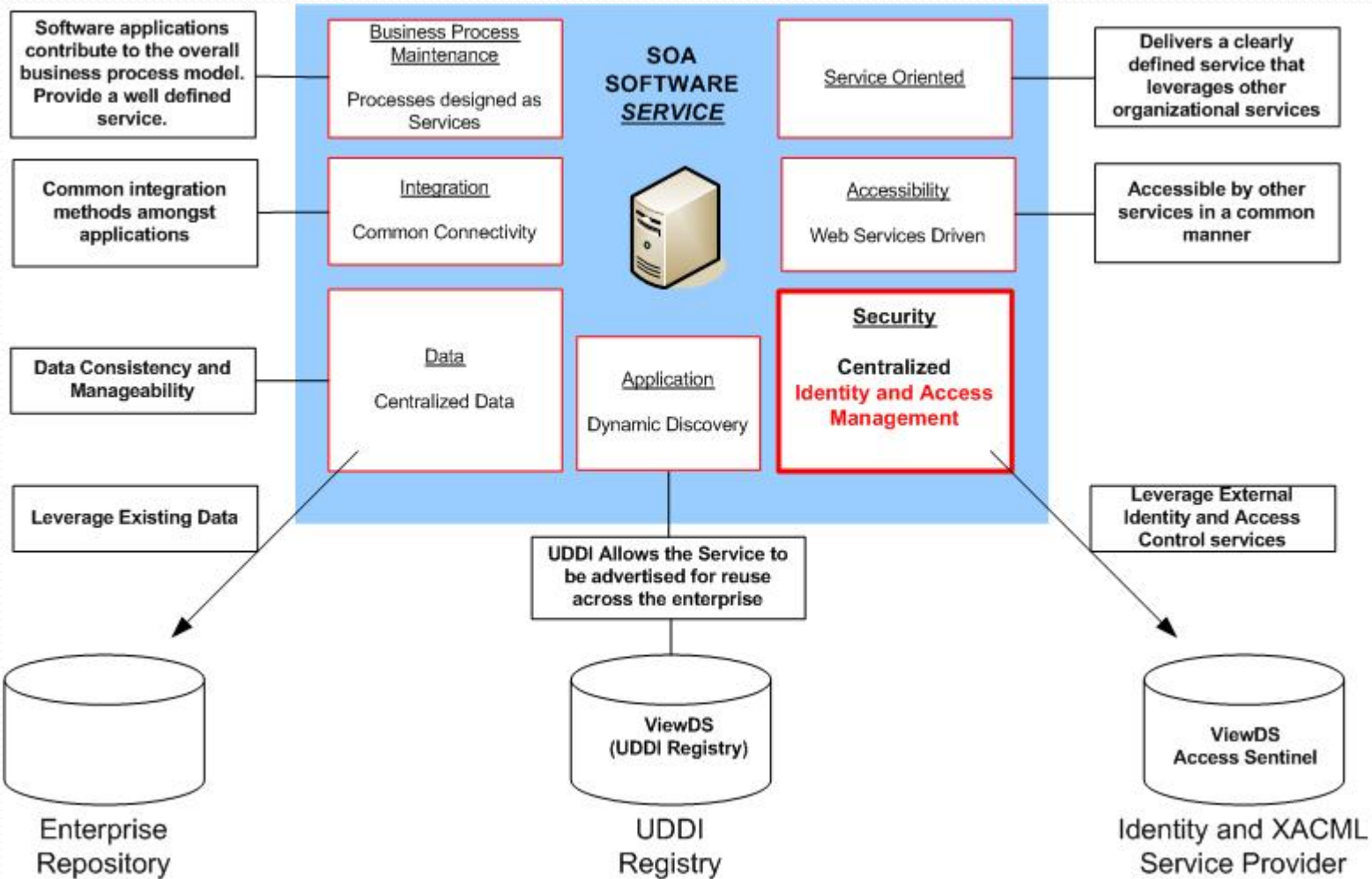


Technology / Product Driven Architecture





Service Oriented Architecture

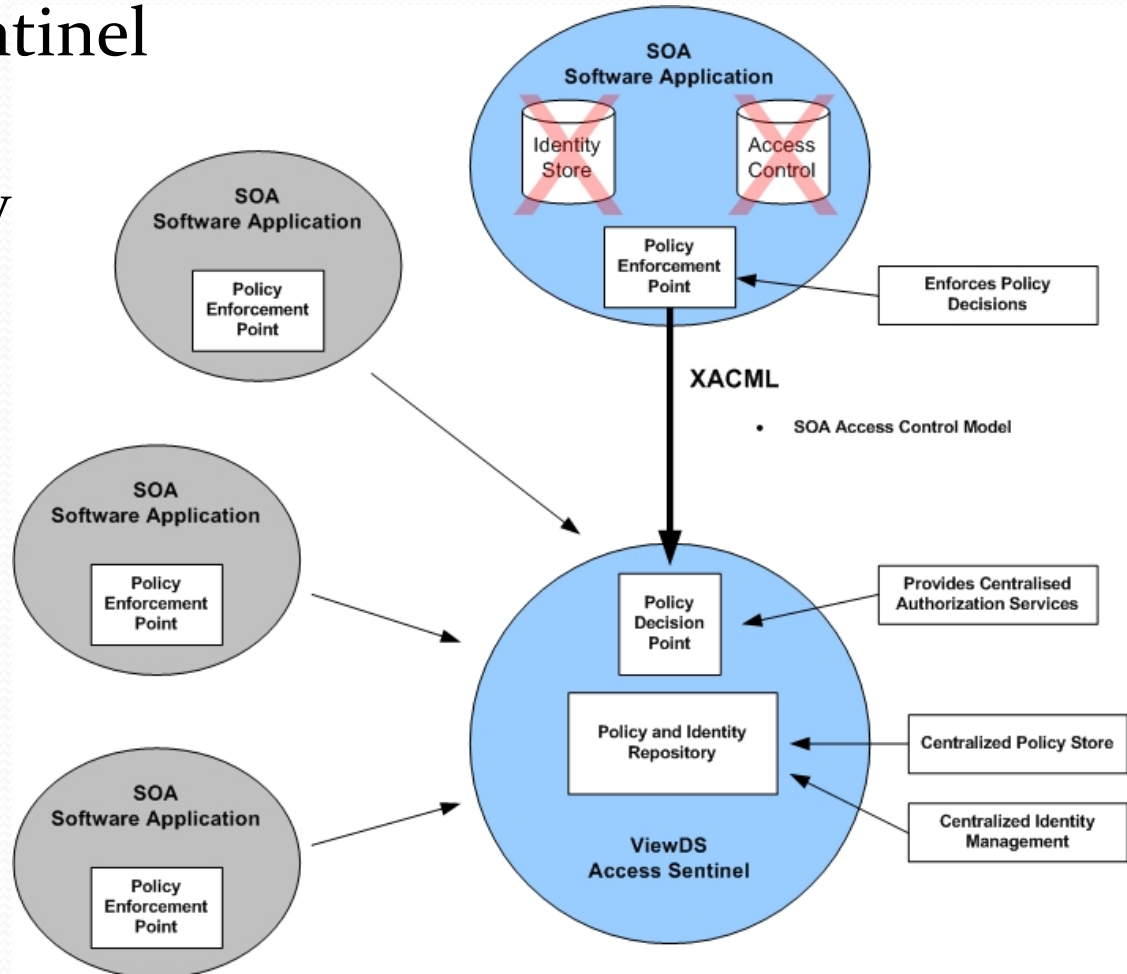




Service Oriented Architecture

- ViewDS Access Sentinel

- Centralised Policy and Identity Store
- Offers Scalable SOA Access Control Services
- Standards based





Entitlements Management Considerations

How to implement in new and legacy software products

Implement a standards-based architecture rather than having to implement access control solutions in every new product?

Reduce development costs by (re-)using standards-based components?

Avoid the continuing need to alter the application's business logic whenever policy requirements change?

Fit with major vendors' architectures



Entitlements Management Considerations

Build or buy?

Rely on major vendors' deployments?

- If so, which one?
- Re-engineer for each vendor?

XACML Expertise

Time to deliver

Few independent mature products

Maintaining evolving standards



eNitiatives Proposition

A ready-made component that can be interfaced and tailored to applications

Version already delivered to major European software developer

XACML standards based

Rapid time to deliver

Continuous maintenance for evolving standards

OEM or Reseller model

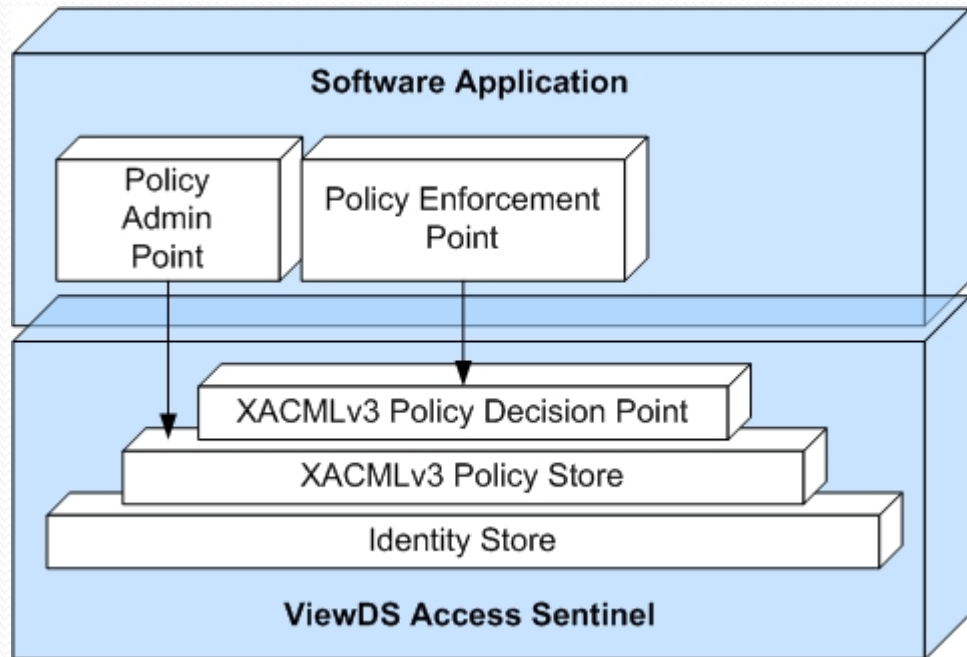
Called Access Sentinel

eNitiatives Proposition

Let ViewDS Access Sentinel handle Authorization using XACMLv3

Policy Admin and Enforcement modules available for your platform

A reusable, scalable and standards based solution





Access Sentinel

- is based on the XACMLv3 (eXtensible Access Control Markup Language) standard
- provides the policy decision point and the policy administration point access at a **single source** of policy, identity and entitlement information: this capability is unique in the market to-day.
- a unique architecture : it is the only product that combines both the identity store and the policy store in one repository.
- consequent major advantages in data integrity, maintenance and support, performance, energy use and system design.
- current competitor solutions require additional databases to store access control policies, identity information and roles and entitlements.
- current competitors are unable to manage delegations and distribution of policy information to multiple access control policy servers.



Conclusion

- Access Sentinel is a "one-stop shop" for authentication and authorization across an enterprise's applications
 - With a variety of solutions for integrating enterprise application servers
- Combining the PDP, PAP, PIP and Identity Provider functionality into a single system component provides:
 - A fully unified enterprise view of authorization policy
 - Easier deployment and administration
 - Fewer discrete components
 - Higher performance
 - from the elimination of external messaging
 - Fault tolerance, load balancing and local access will be provided through policy engine replication
- For OEM Application customers, Access Sentinel provides an easy method for implementing XACMLv3 fine grained entitlements control
- Licencing is available on a perpetual or per application basis



Engagement

If Entitlements Management is an imminent requirement,
need to decide soon

Determine strategy and architecture.

If a “buy” component approach is taken, eNitiatives can
provide a low cost, standards-based component

sales@enitiatives.com.au

+613 9851 8600



For the Technical



What is XACML?

- eXtensible Access Control Markup Language
 - Role Based Access Control
 - Attribute Based Access Control
 - Obligations
- Centralized Authorization Service
 - Delegated administration of policies
 - Reusable throughout the organization
- Standardized
 - Security Policies represented in a Standards Based manner
 - Auditable, Scalable, Accepted and Compliant



XACML Policies

- Policies are defined with a collection of Rules
- Rules are made up of Subjects, Resources, Actions and Environment
 - Subject: The Entity requesting access
 - Resource: Data, or a service or a system component
 - Action: The type of access requested on the Resource
 - Environment: Additional information (e.g. Time of Day)
- Attribute Based
 - Subjects, Resources and Actions may be identified by their attributes
 - This is in addition to referencing by ID, Group Membership and Role membership
 - Provides a greater level of flexibility and extensibility

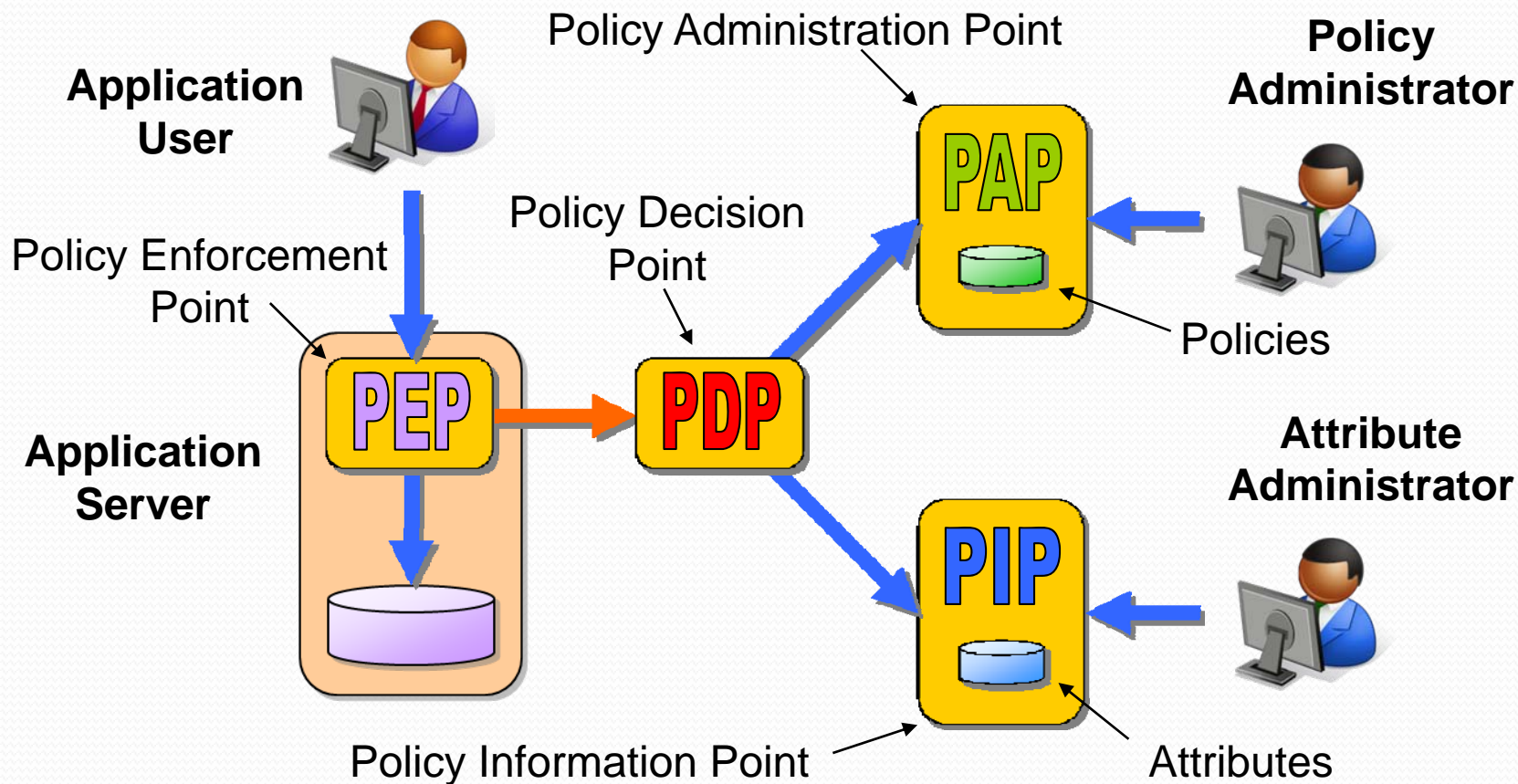


XACML Architecture

- Policy Administration Point [PAP]
 - An interface that allows policies to be maintained
- Policy Information Point [PIP]
 - An information repository holding information about subjects, actions and resources
- Policy Decision Point [PDP]
 - The access control decision making service. Upon receiving an authorization request, the PDP will assess the policies and information available to make an access control decision
- Policy Enforcement Point [PEP]
 - An XACML enabled application's access control module. When an application needs an access control decision to be made, it will use its PEP to request a decision from the PDP. Upon receiving the decision, the PEP will enforce the decision and any associated obligations.

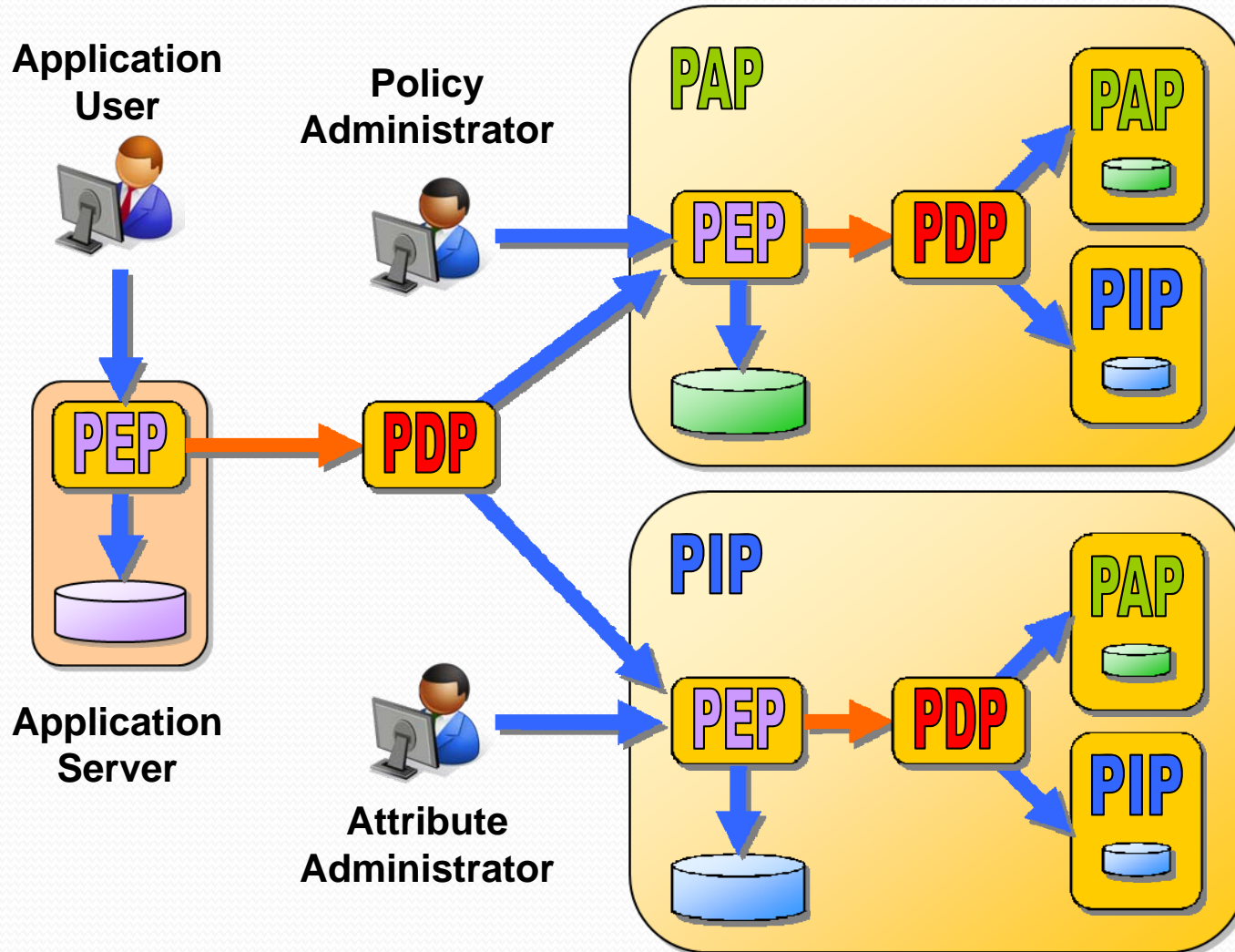


XACML Dataflow Model





The Real Dataflow Model





The Complete Access Sentinel Picture

