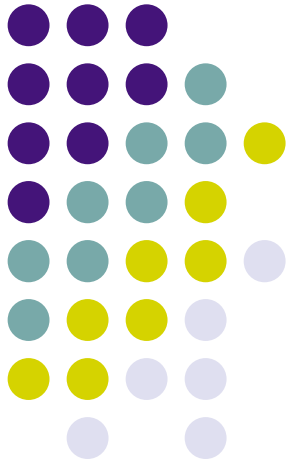
XACML 3.0 Enhancements

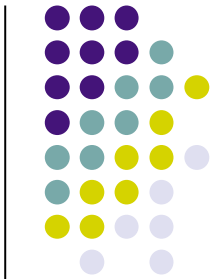
Gerry Gebel
Axiomatics
gerry@axiomatics.com



kantara INITIATIVE™

AXIOMATICS

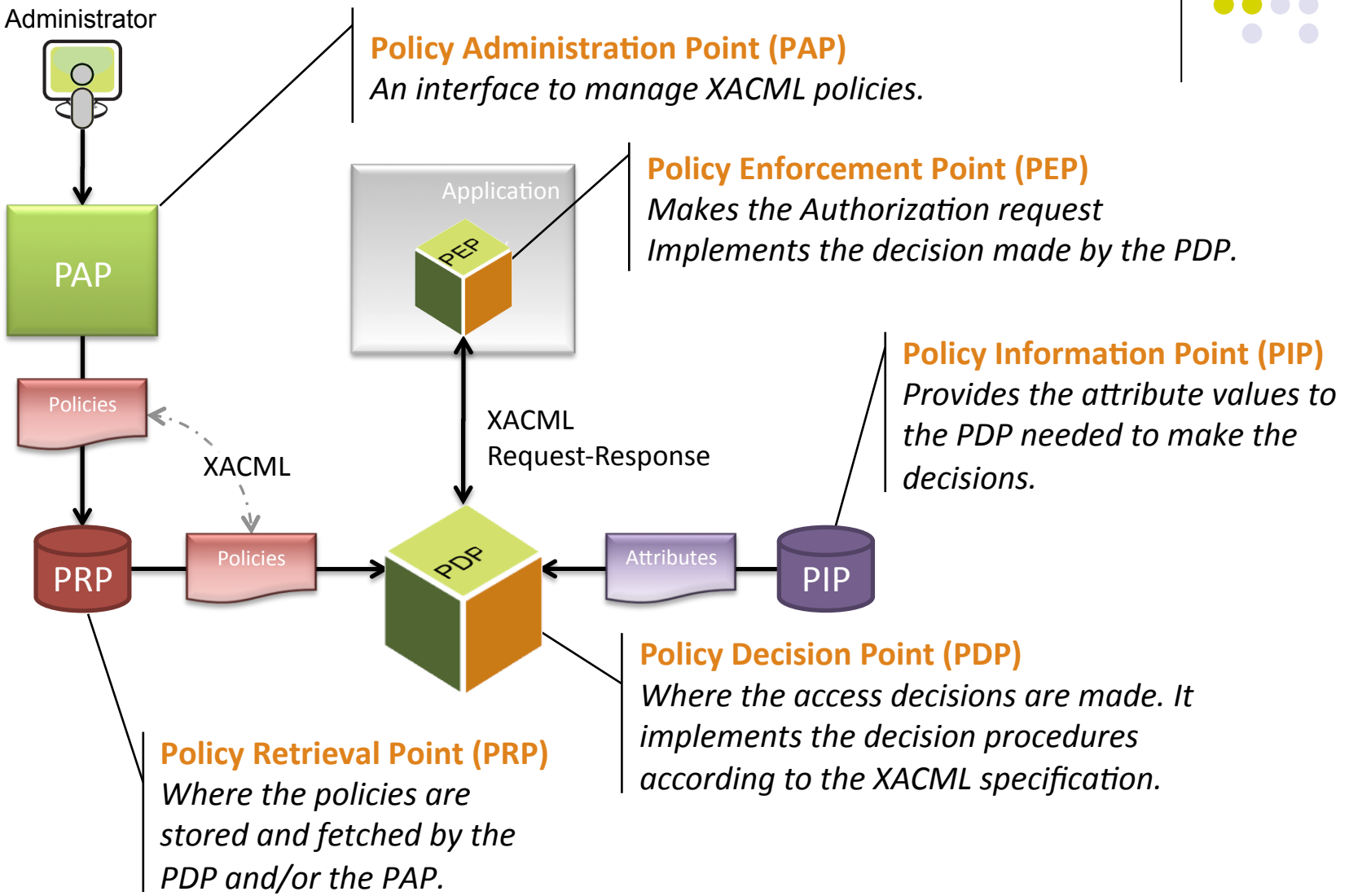
XACML – a quick intro



- An abstract architecture
- A policy language
- A request – response protocol

kantara INITIATIVE™

XACML Architecture



Policy Administration Point (PAP)
An interface to manage XACML policies.

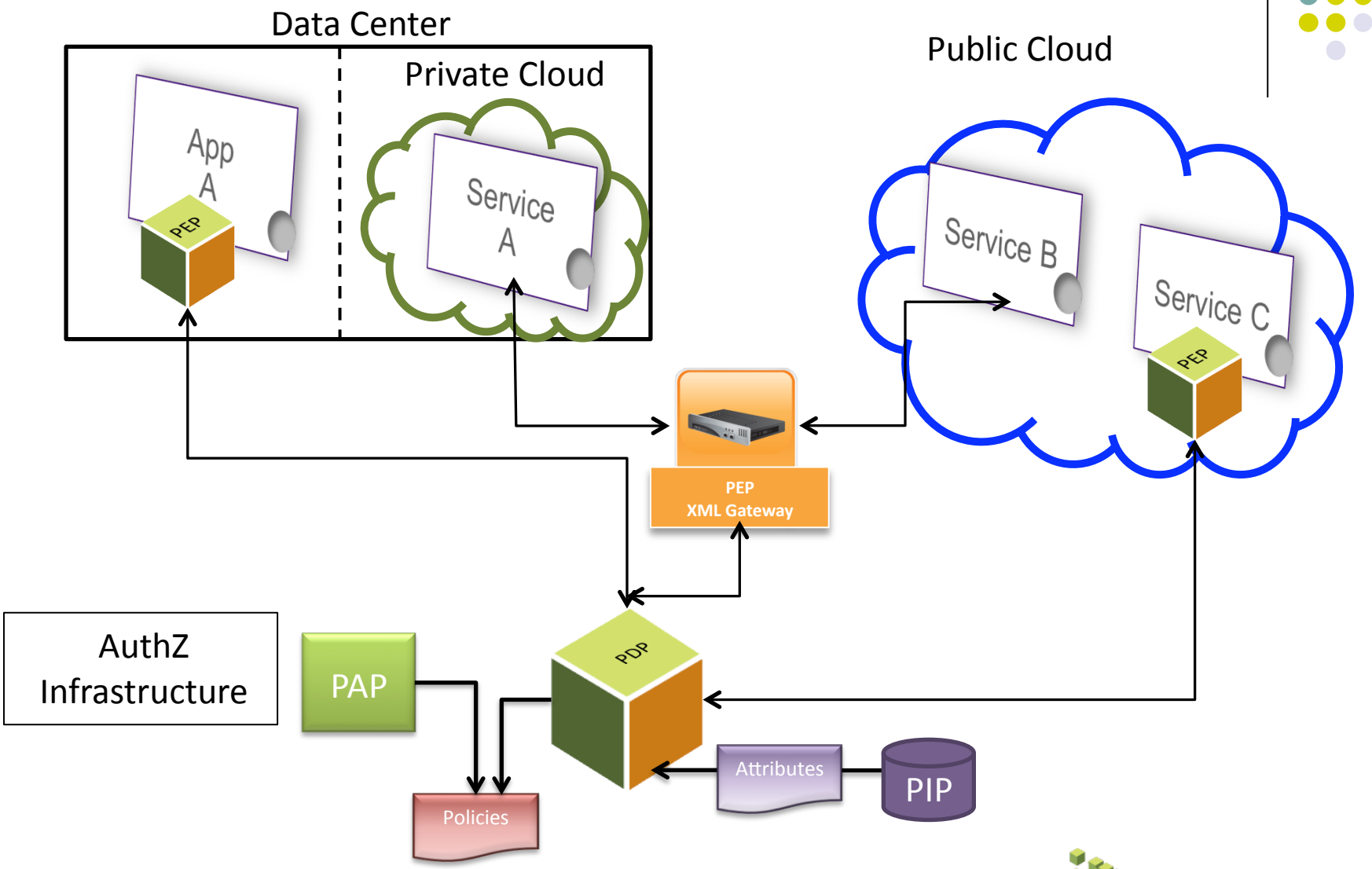
Policy Enforcement Point (PEP)
Makes the Authorization request
Implements the decision made by the PDP.

Policy Information Point (PIP)
Provides the attribute values to the PDP needed to make the decisions.

Policy Decision Point (PDP)
Where the access decisions are made. It implements the decision procedures according to the XACML specification.

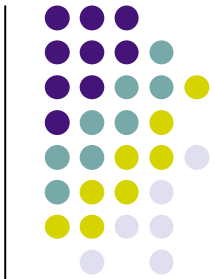
Policy Retrieval Point (PRP)
Where the policies are stored and fetched by the PDP and/or the PAP.

Anywhere Application Architecture



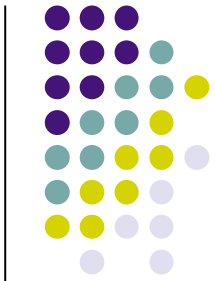
AXIOMATICS

XACML 3.0 Status



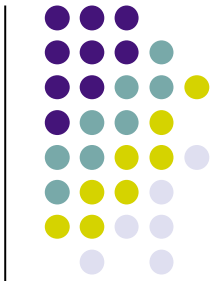
- Currently a Committee Draft
  - Core spec is at CD 4
  - There have been 2 public review periods
  - Formal ratification expected before end of 2010
- Previous versions
  - XACML 1.0 – February 2003
  - XACML 2.0 – February 2005

New in XACML 3.0



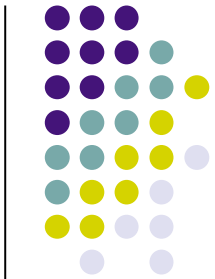
- Bug fixes
  - General errata, typos XPATH namespace issues
- Optimizations
  - Confined XPATH to each section in a request – makes multi decision processing more efficient
- XACML syntax compatibility
  - Version 3.0 is very similar to 2.0
  - Version 3.0 supports all previously defined functionality
  - Only XPATH expressions must be rewitten

New Attribute Categories



- Add your own generic attribute categories
  - Version 2.0 only defined Subject, Action, Resource, and Environment categories
  - Version 3.0 has <Attributes Category="ABC">
  - Two new standard categories to support delegation
- New Target matching capabilities
  - <Target> contains <AnyOf> and <AllOf> instead of <Subjects>, <Subject>, etc.

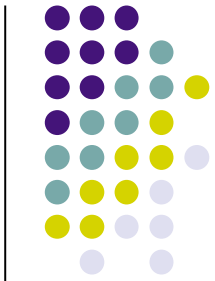
Example of a user-defined category



```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:cd-01">
 <Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
  <Attribute
   AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">alice</
    AttributeValue>
  </Attribute>
 </Attributes>
 <Attributes Category="http://example.com/myproject/Service">
  <Attribute
   AttributeId=" http://example.com/myproject/attr/Color">
   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Green</
    AttributeValue>
  </Attribute>
 </Attributes>
</Request>
```

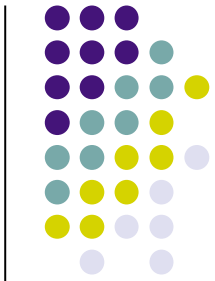
User-defined category

New – Obligation Expressions



- Version 2.0 only returned static expressions
- Now, obligation expressions can fetch values from the request and transform them before returning them with the “Permit” or “Deny”
- Note: PEP must enforce decision and carry out the obligation
  - “Log elevated access request”
  - “Send email notification to data owner”

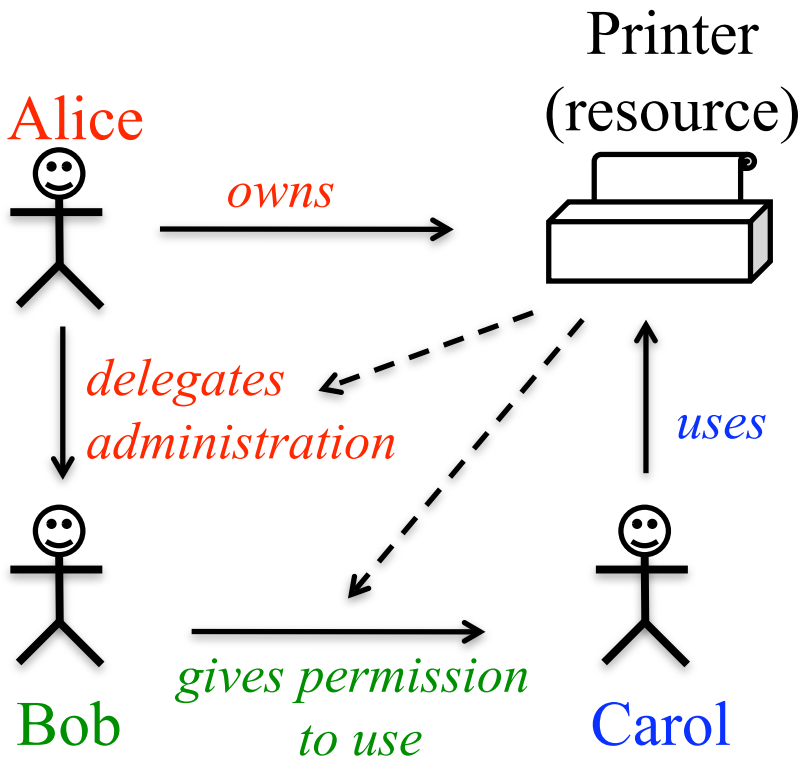
New - Advice



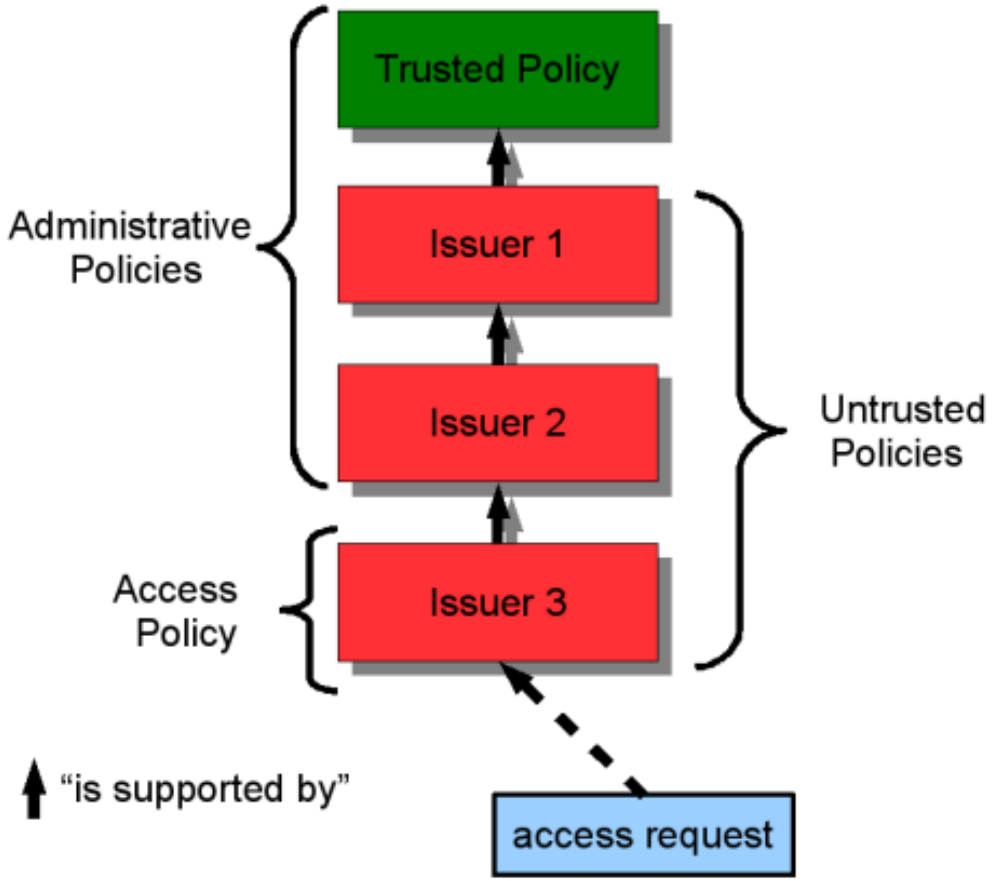
- Functionally the same as an “Obligation”
- However, “Advice” can be safely ignored by the PEP

New - Delegation

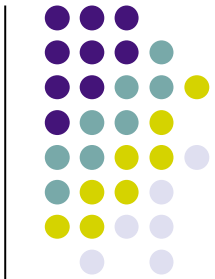
- Decentralization of authZ management
- Owner-centric authorization
  - Resources have owners
  - Owners can delegate (parts of) their administration rights
- PDP needs to verify delegations
  - Check if Bob had the right to give access

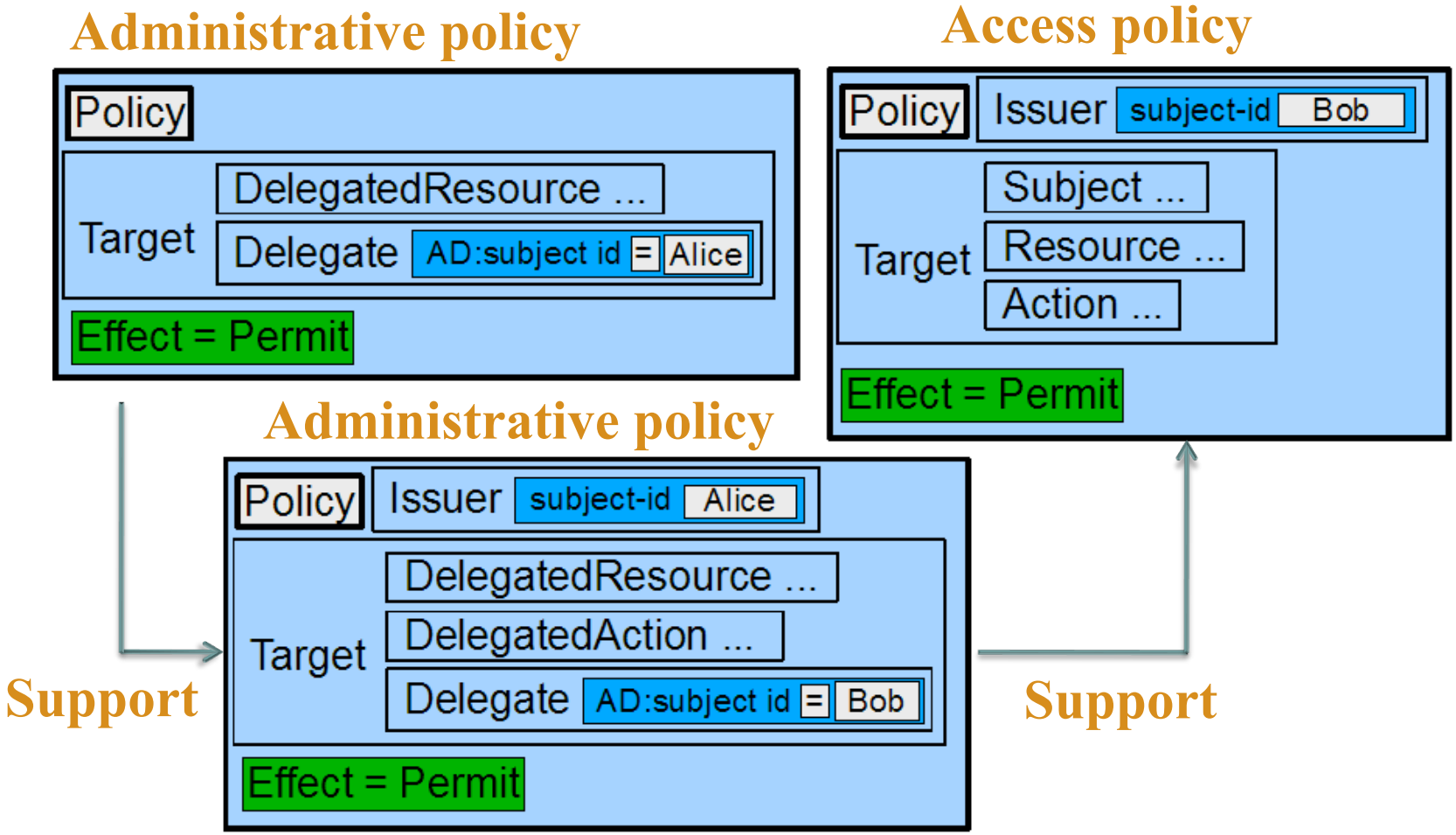


Delegation: Behind the Scenes

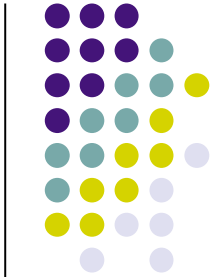


Delegation Chain





Delegation Example



1. Organisation A creates delegation policy that allows Organisation B to give their employees access to the simulator

Organisation A (experts in material simulation)

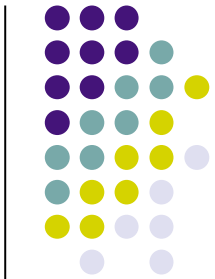
Organisation B (produces airplane components)

2. Organisation B can administrate access for their employees on its own

Supercomputer for simulation

3. Employee of organisation B uses the simulator

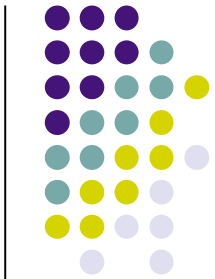
New – Export Control Profile



- Export Administration Regulations
  - EAR
  - Defined by US Dept of Commerce
  - Non-military goods, services, and information
- International Traffic in Arms Regulations
  - ITAR
  - Defined by US Dept of State
  - Military goods, services, and information

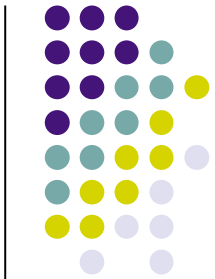
http://www.oasis-open.org/committees/document.php?document_id=38509&wg_abbrev=xacml

Export Control Profile



- EC Profile defines
  - Resource attributes
    - Classification
    - ECCN (Export Control Classification Number)
    - USML (US Munitions List)
  - Subject attributes
    - Nationality
    - Location
    - Organization
    - U.S. Person

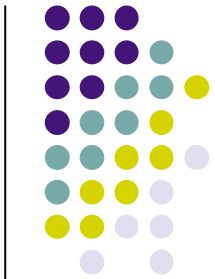
New – Intellectual Property Control Profile



- Protection schemes for
  - Copyright
  - Patent
  - Trademark
  - Trade Secret

http://www.oasis-open.org/committees/document.php?document_id=38510&wg_abbrev=xacml

IP Control Defines



- **Resource attributes:**
  - IPC-Type
  - IPC-Data
  - IP-Owner
  - IP-Designee
  - EC-US
  - License
- **Subject attributes:**
  - Nationality
  - Organization

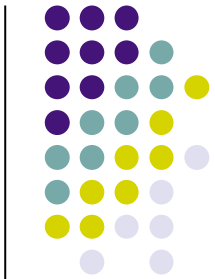
Environment attribute:

- Location

Action attributes:

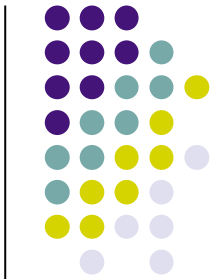
- Storage
- Physical transmission
- Electronic transmission
- Encryption type
- Marking
- Disposal
- Authority

Update – Multiple Decision Profile



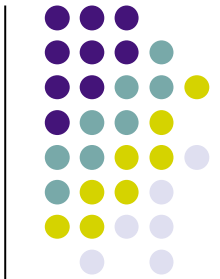
- Was called Multiple Request in version 2.0
- PEP can bundle more than one request in a message to the PDP
  - When individual requests are not practical – such as processing 50 authZ requests before rendering a portal page
- PDP can return individual decisions in a single response
- PDP can return a combined decision

Update – Policy Combining Algorithms



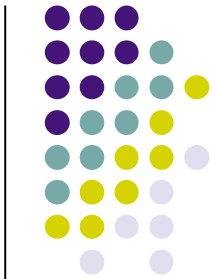
- Many 2.0 combining algorithms were biased to turn an “Indeterminate” response into a “Deny” response
  - To hide errors
  - Version 3.0 algorithms operate more consistently
- Added new algorithms, can create your own combining algorithms

Update – Hierarchical Resource Profile



- Allows XACML policies to be used on resources that are organized in hierarchies
  - Identify nodes in a hierarchy
  - Request access to nodes
  - Build policies that apply to nodes
- New scheme to encode hierarchy as URI

More Information



- www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml