Security Domain Membership Management

CORBA Specification Submission Overview

Konstantin Beznosov, Concept Five Technologies

March 29, 2001

Presentation Outline

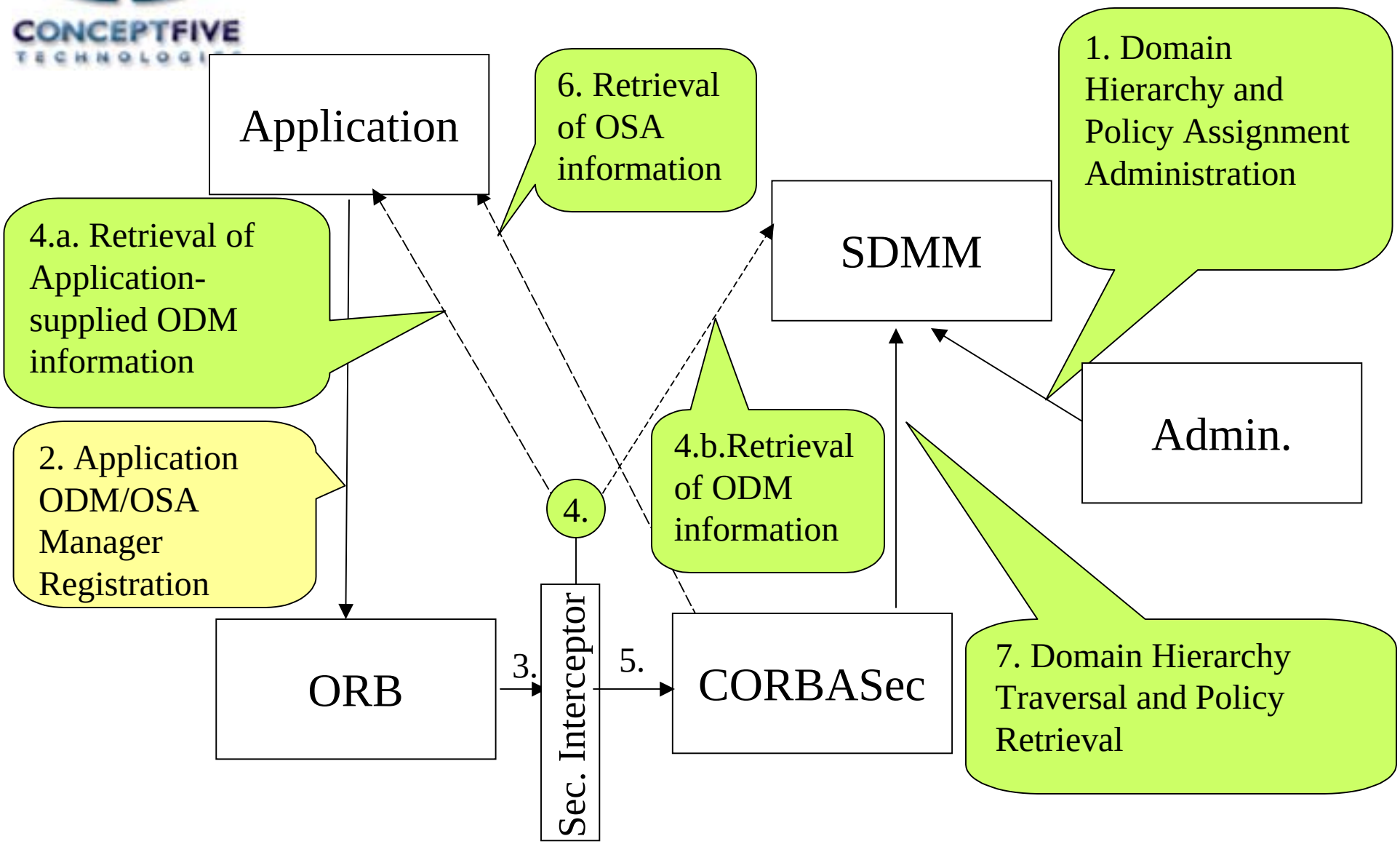
- Architecture overview
- Object Domain Mapping
- Object Security Attributes
- Domain Administration

Architecture Overview

Main Parts of the Architecture

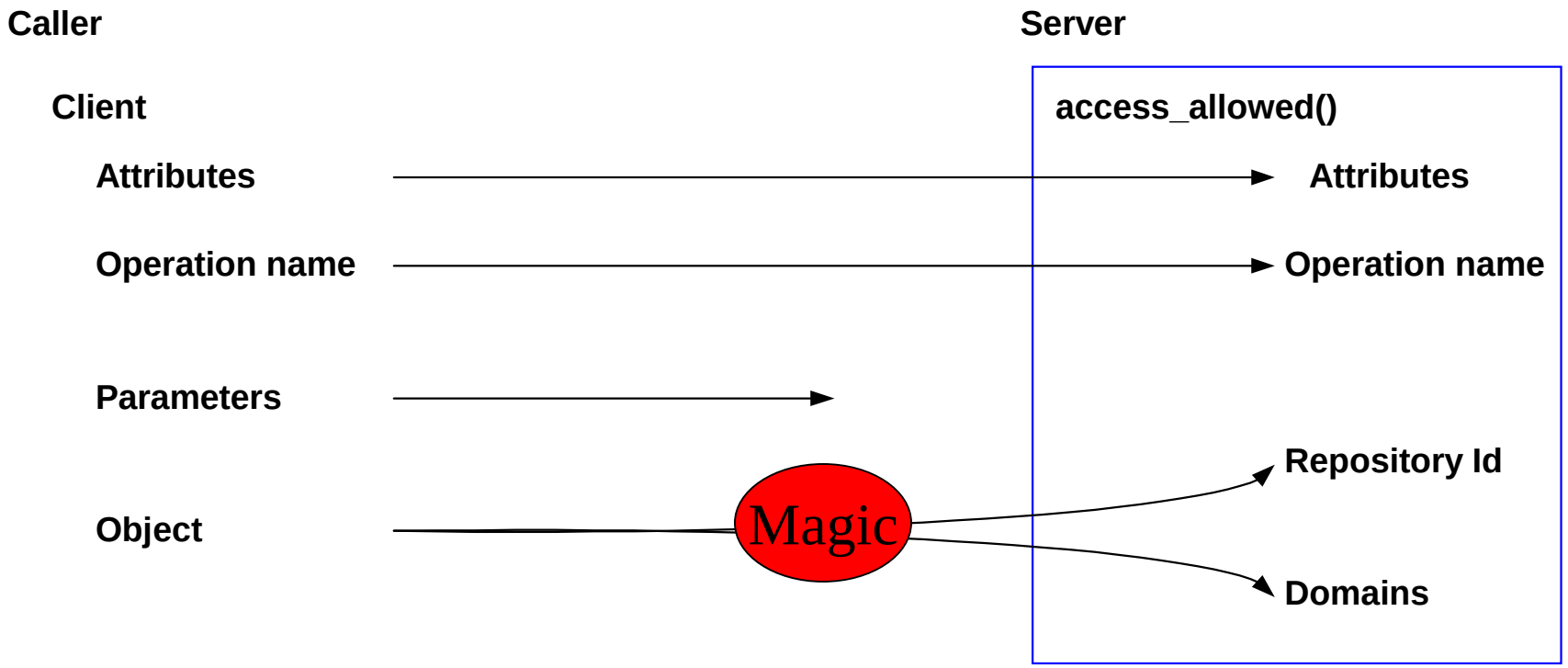
1. Object Domain Mapping:
   What domains does the object belong to?
   - object to domain mapping (ODM) information retrieval run-time mechanisms
2. Object Security Attribute Retrieval
   What security-related attributes does the object have?
   - Object security attribute (OSA) retrieval run-time mechanisms
3. Domain Administration
   - Administration of domain hierarchies
   - Administration of domain-to-policy associations
   - Run-time computation of security policy composition according to the domain hierarchy

Specified Mechanisms

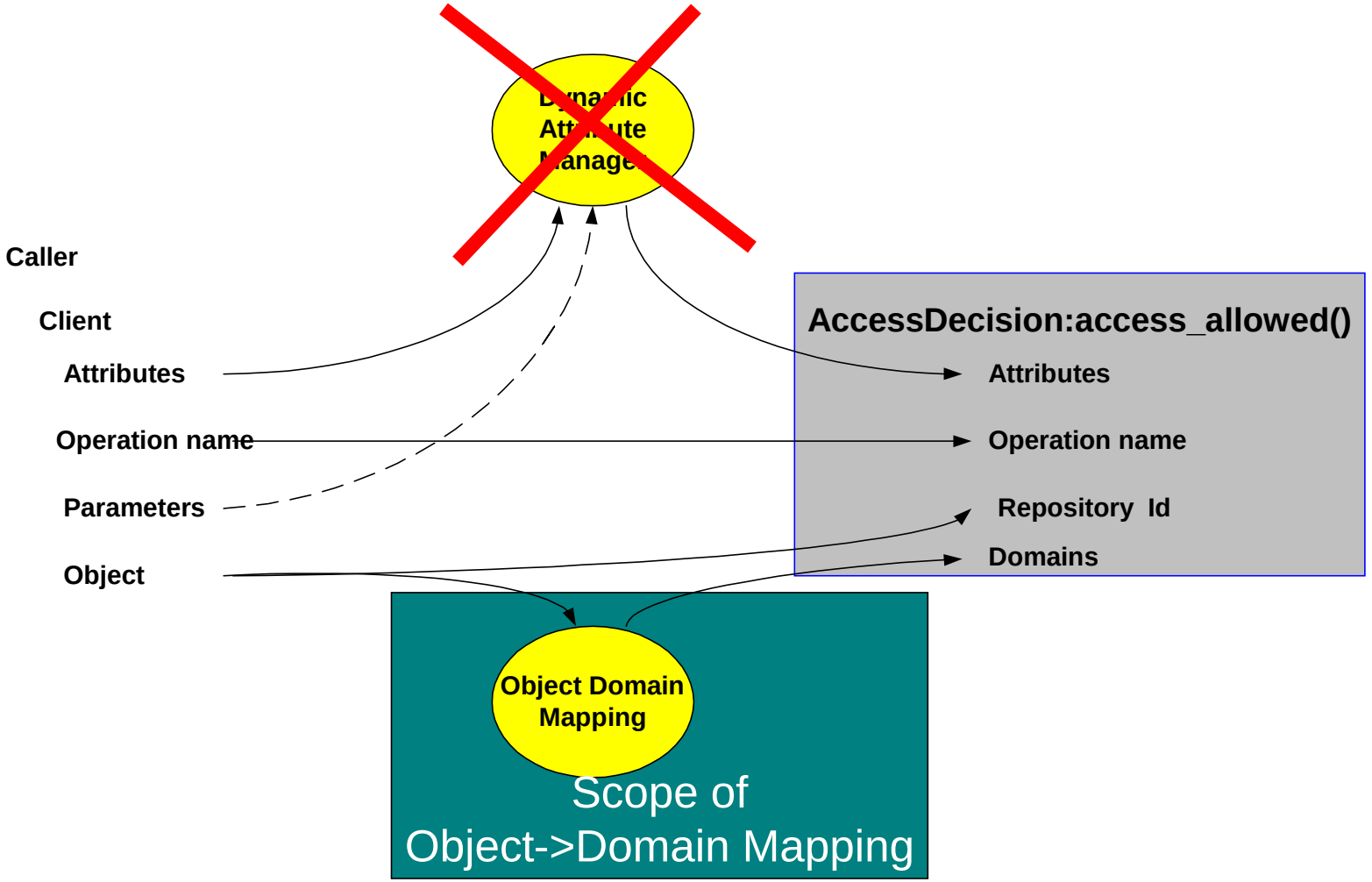


Object-Domain Mapping

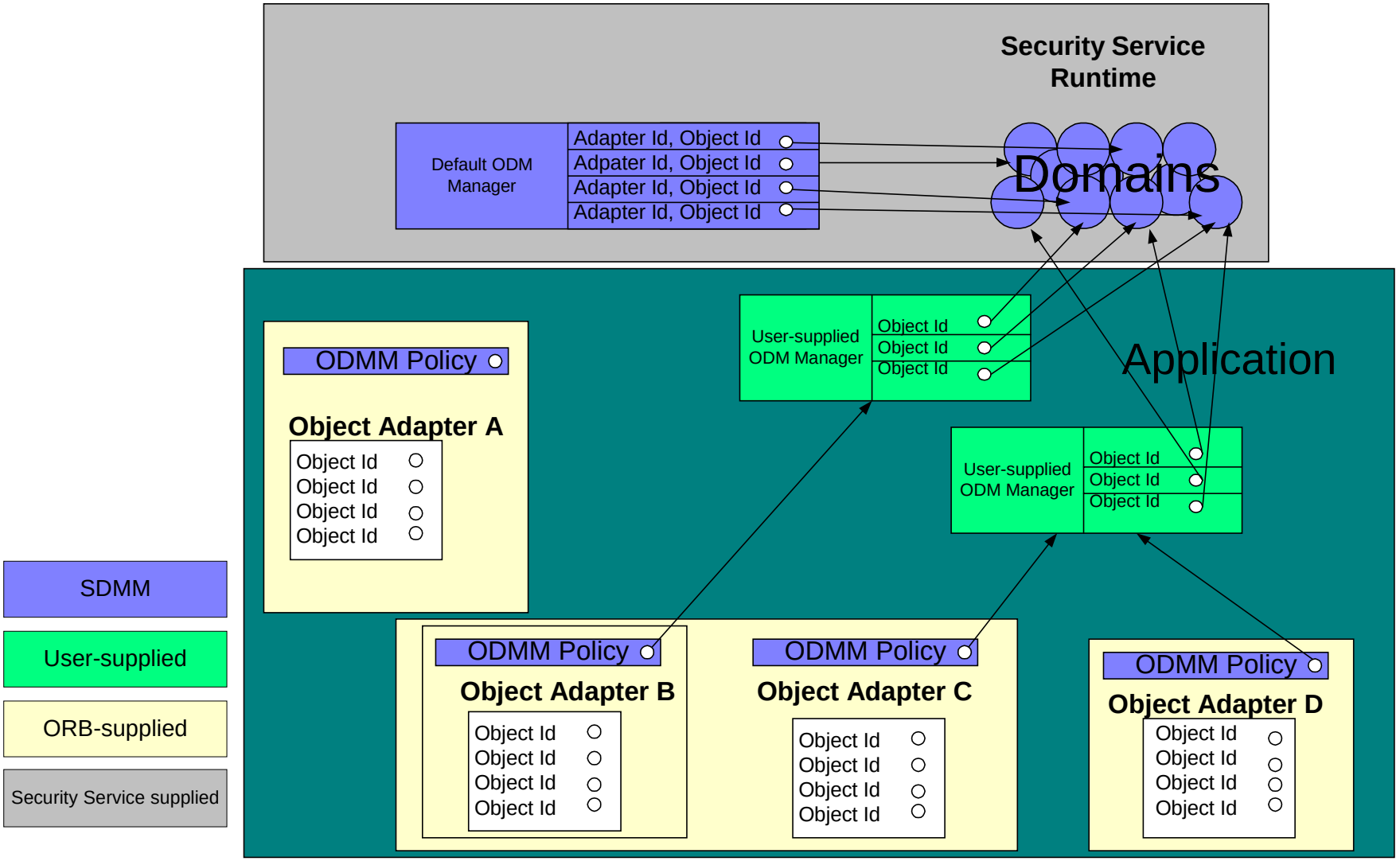
Access Decision Information Flow



The Scope of ODM as defined by the submission



ODM Managers and Policies

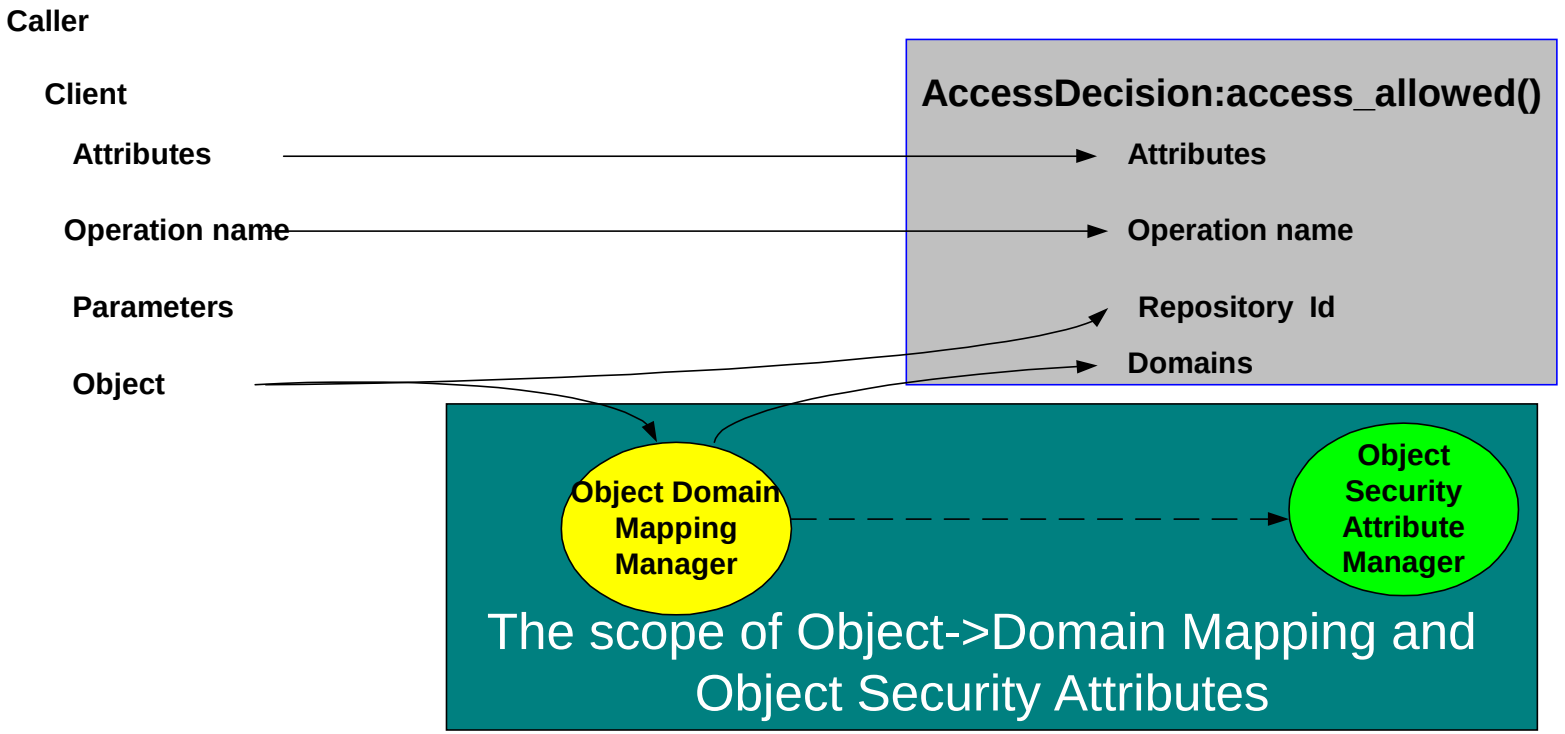


Object Security Attribute Retrieval

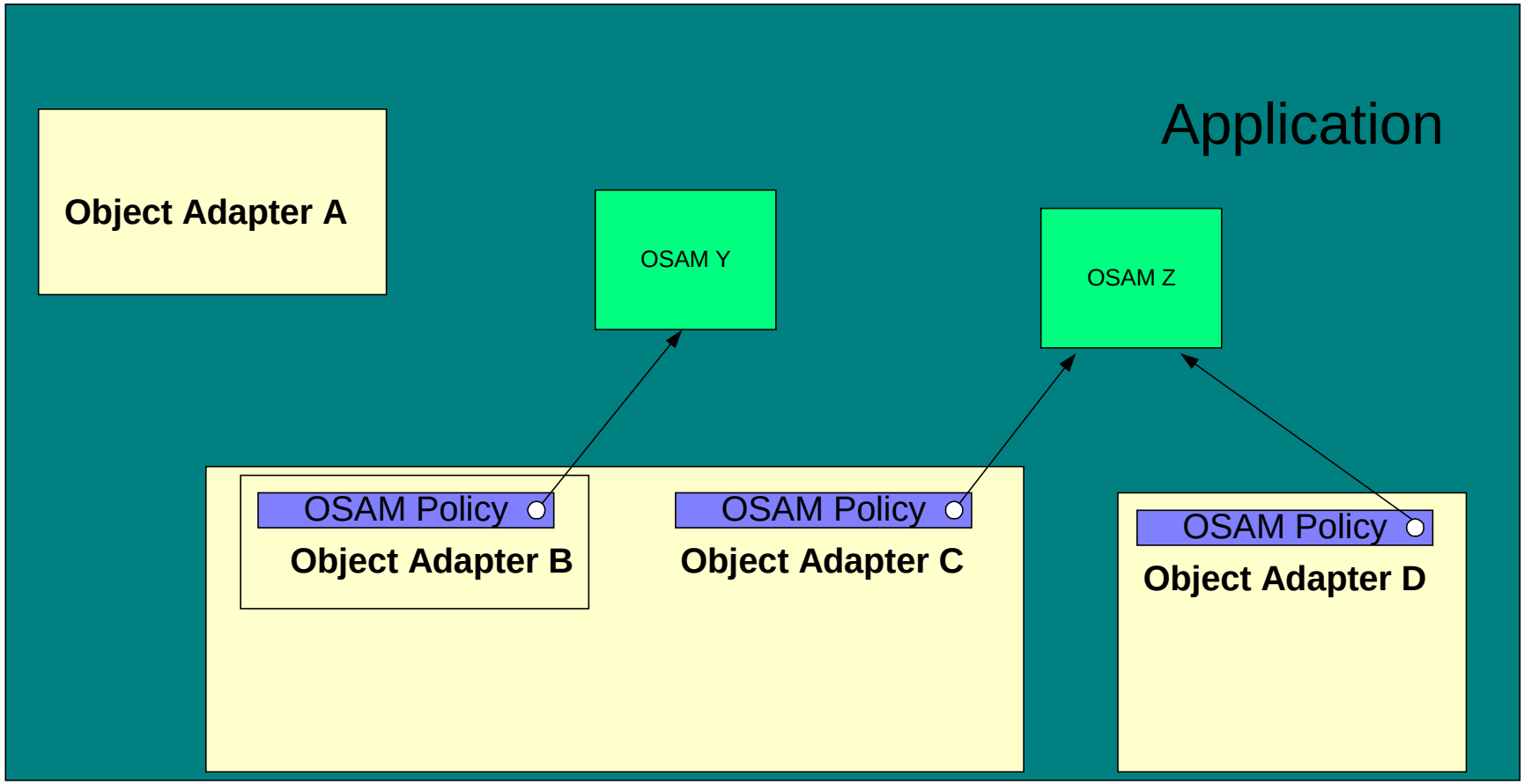
Why Object Security Attributes

- Make Object->domain mapping specific to application domain and yet isolated from the application implementation
- Separation of responsibilities:
  - Security service – security vendor
  - ODM Manager -- application owner or security vendor/integrator
  - Security-related attributes -- application vendor
- Examples:
  - bank account objects
    - account #
    - State in which the account was opened
  - phone account objects
    - hone area code for
  - owner identity

The Scope of ODM and OSA as defined by the submission

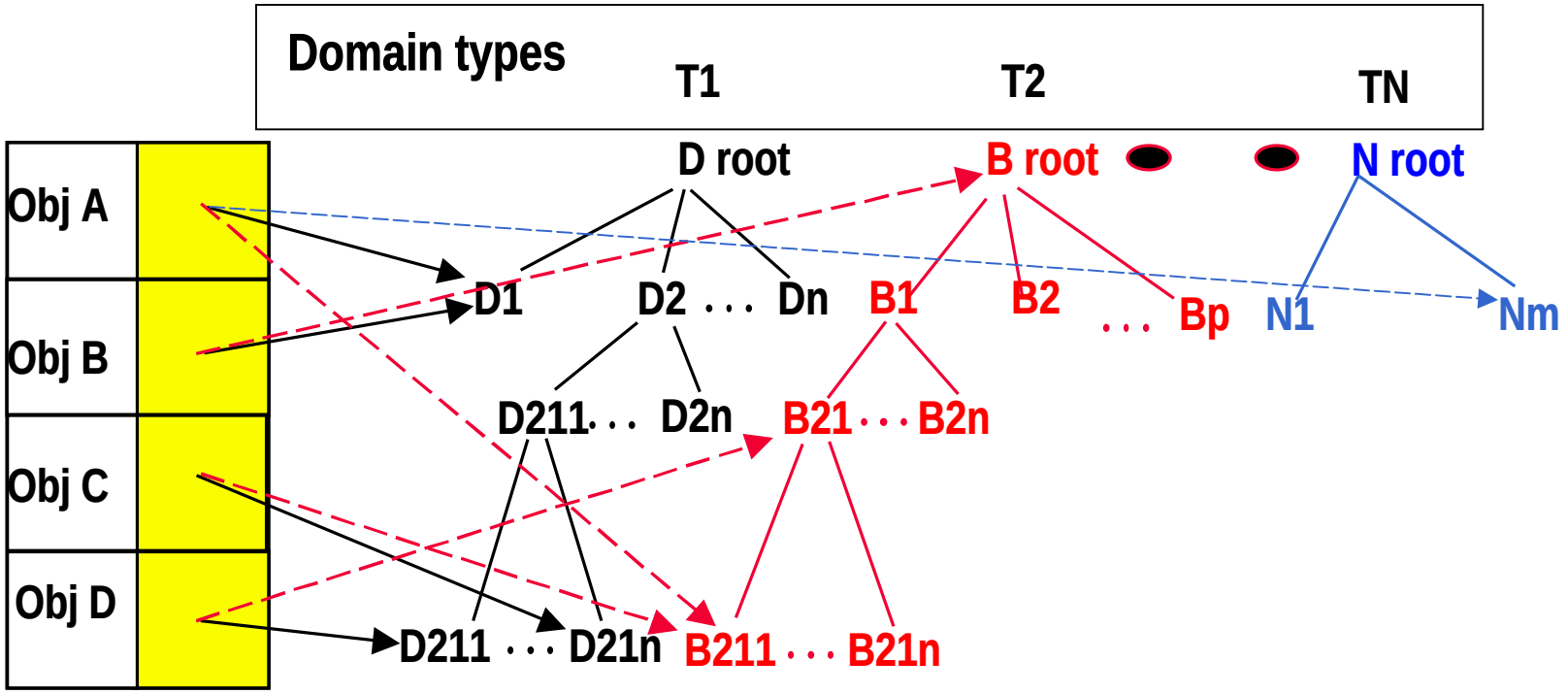


OSA Managers are Provided only by Application



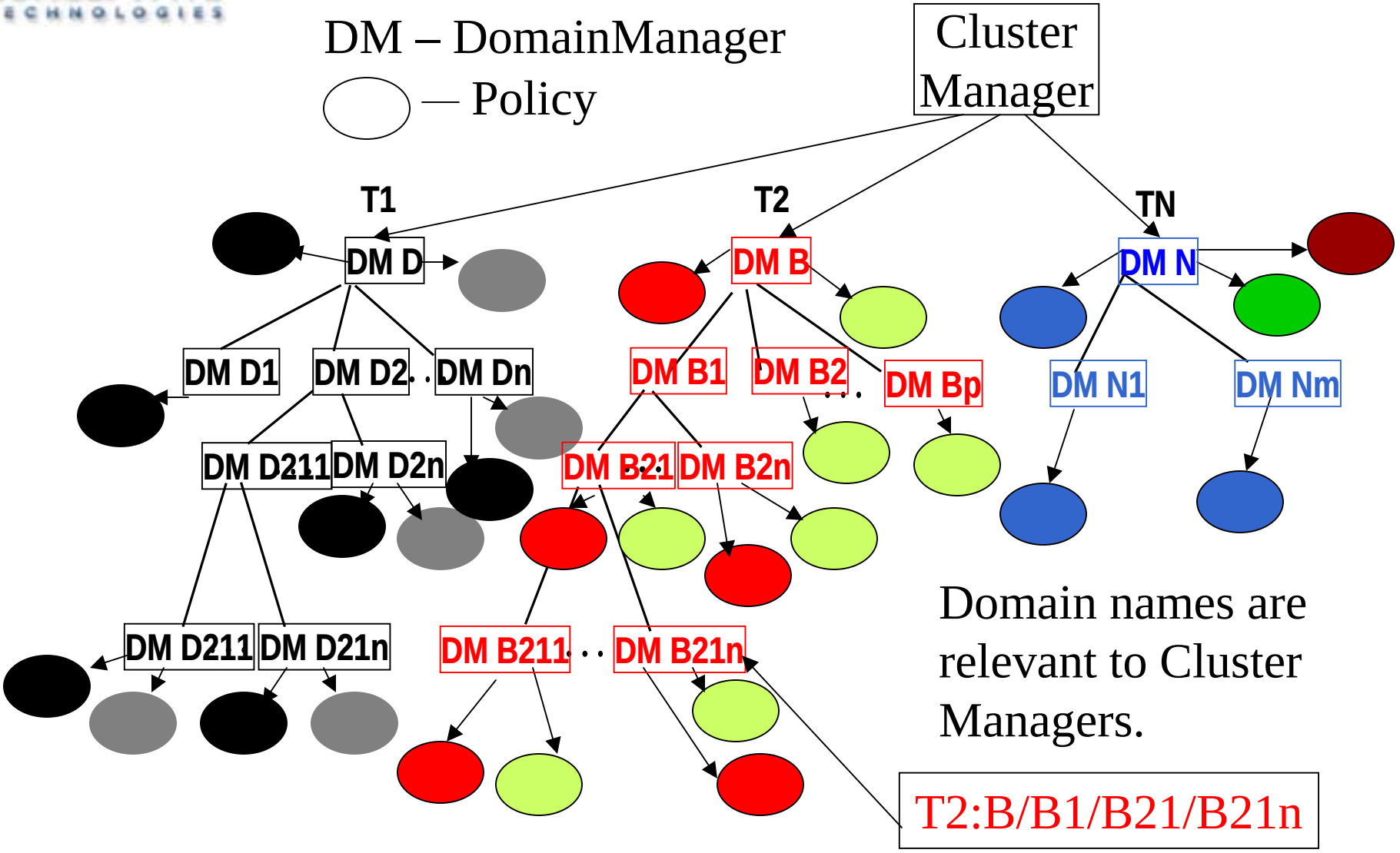
Domain Administration

Objects and Domains

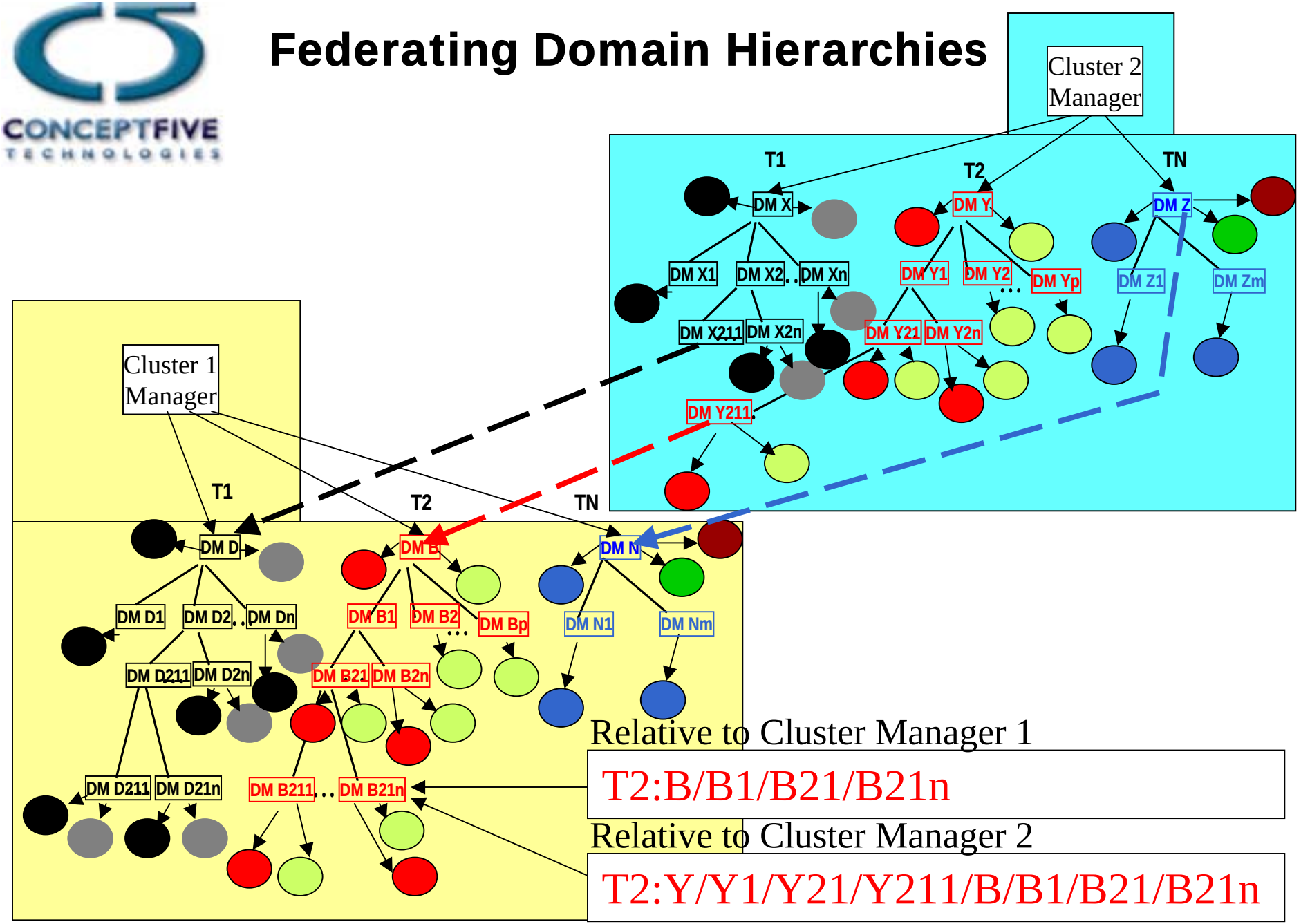


Object A domain membership: D1, B211, Nm

Domains and Policies



Federating Domain Hierarchies



Relative to Cluster Manager 1

T2:B/B1/B21/B21n

Relative to Cluster Manager 2

T2:Y/Y1/Y21/Y211/B/B1/B21/B21n

Notes on Domain Hierarchies

- Domain Managers can come and go, i.e. IORs are not very long living, but
  - Cluster Managers and domain names are significantly more static
- Cluster probably implemented by the same vendor
  - Possible run-time optimization inside of clusters

Documents

- Original RFP

  OMG document number: orbos/98-11-24
- Current Submission:

  OMG document number: orbos/2001-02-01
- Next version of the submission in April