A Security Framework Supporting Domain-Based Access Control in Distributed Systems

Nicholas Yialelis and **Morris Sloman**

Email: {ny, mss}@doc.ic.ac.uk

Department of Computing
IMPERIAL COLLEGE
180 Queen's Gate
LONDON SW7 2BZ

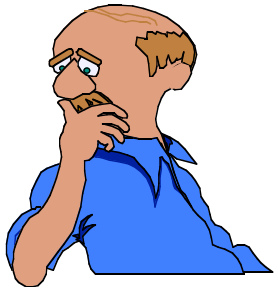
Security in Commercial Distributed Object Systems

Problem

Distributed Object Systems may:-

- support a large number of objects
- cross organisational boundaries
- exhibit complex trust relationships

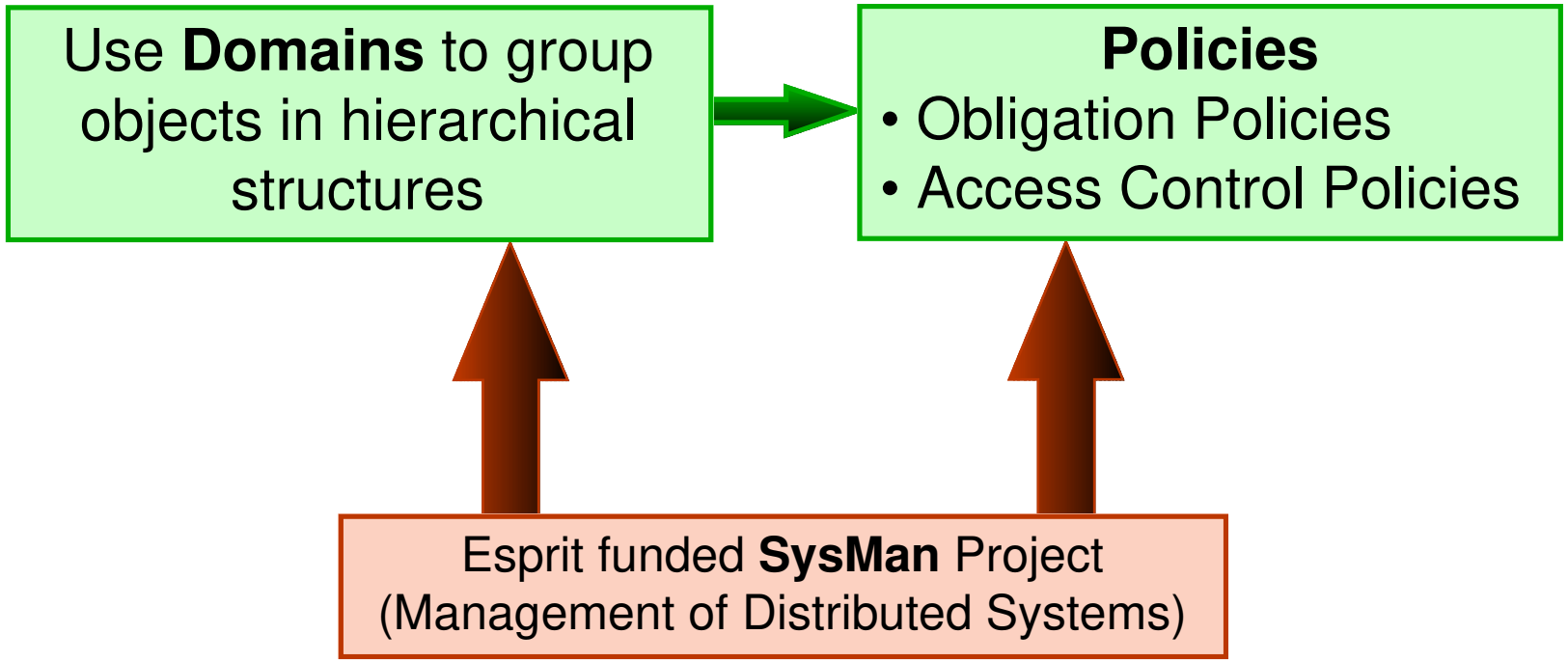
Difficult to Manage!



Outline

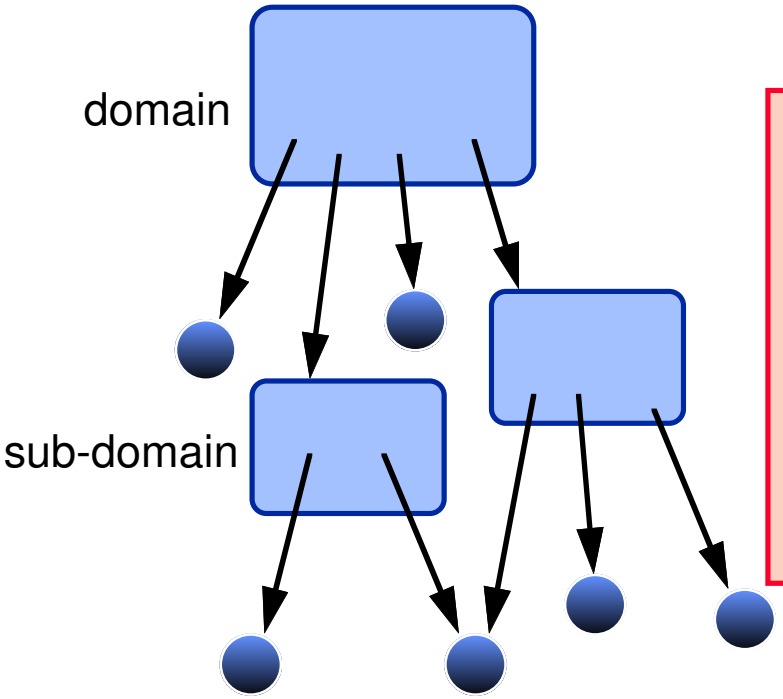
- Our Approach
  - Domains
  - Access Control Policies (+ Delegation)
- System Overview
  - Domain Service
  - Policy Service
  - Authentication Service
  - Security Agents
- Conclusions and Future Work

Our Approach



Domains

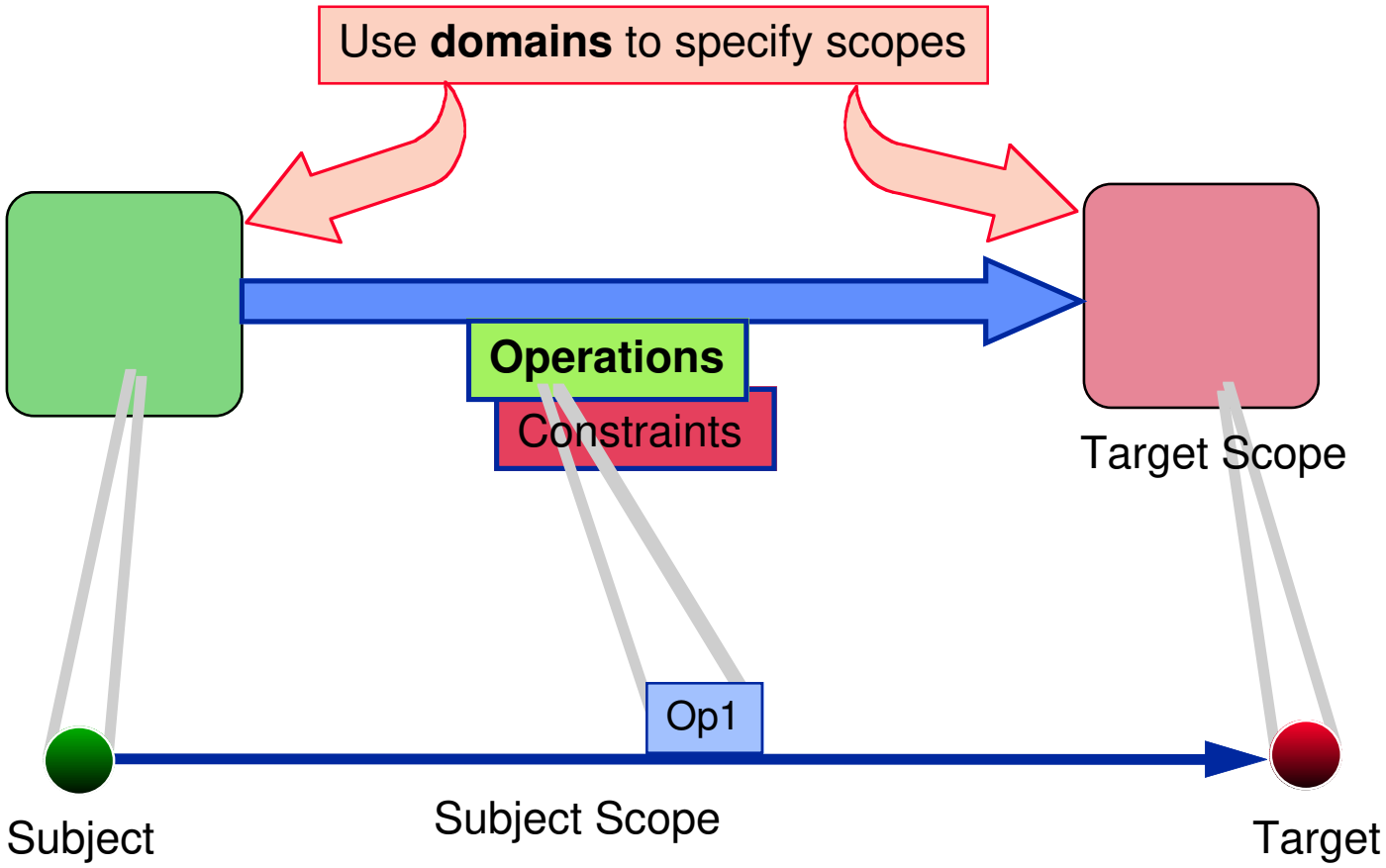
A management **domain** is an object which maintains a list of references to objects that have been explicitly grouped together for the purposes of management



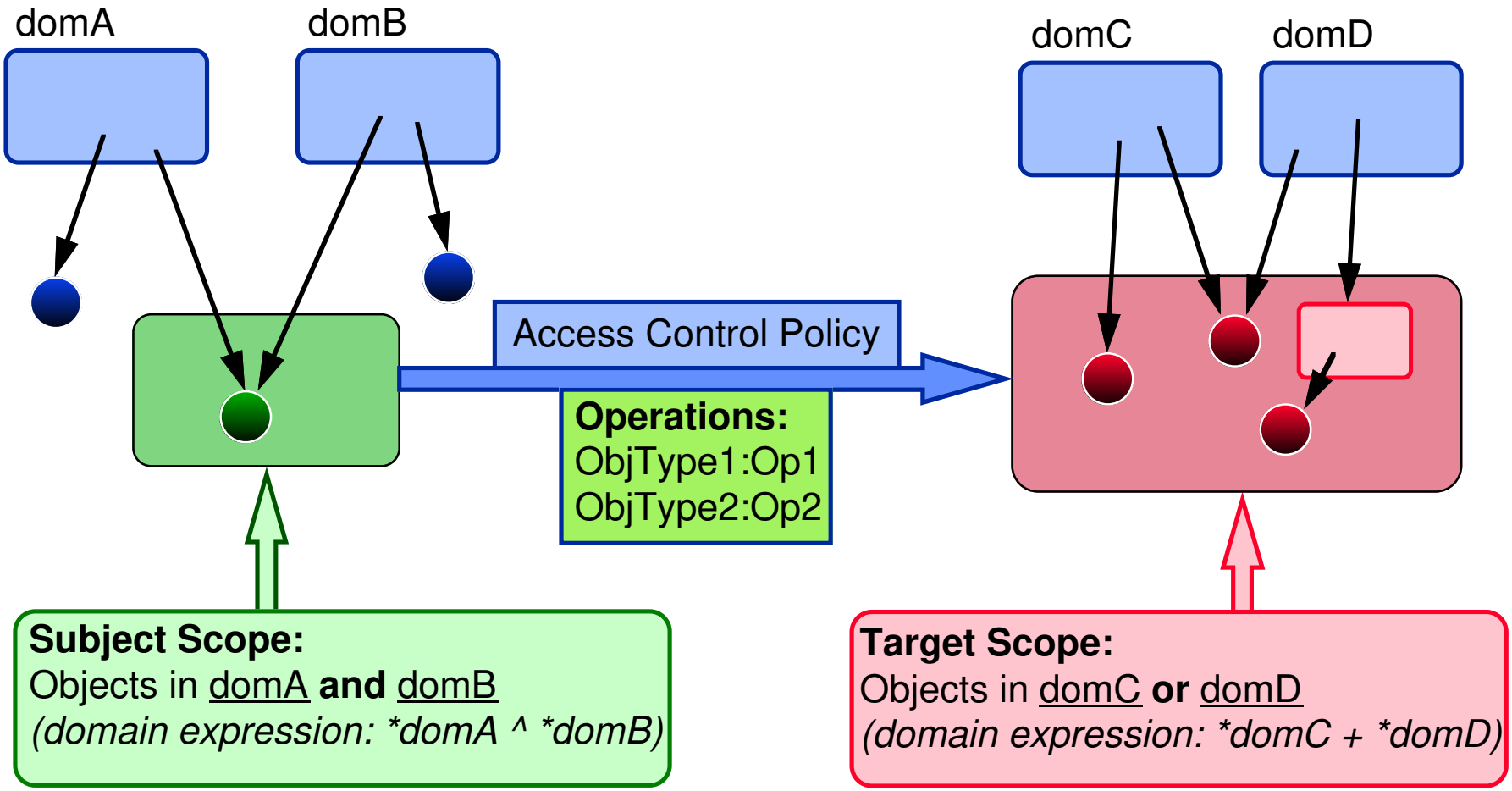
Domains can be used to group objects in a hierarchical structure to

- reflect organisational, geographical or trust structure,
- apply a common security policy,
- partition the security management in order to cope with the complexity of large distributed systems

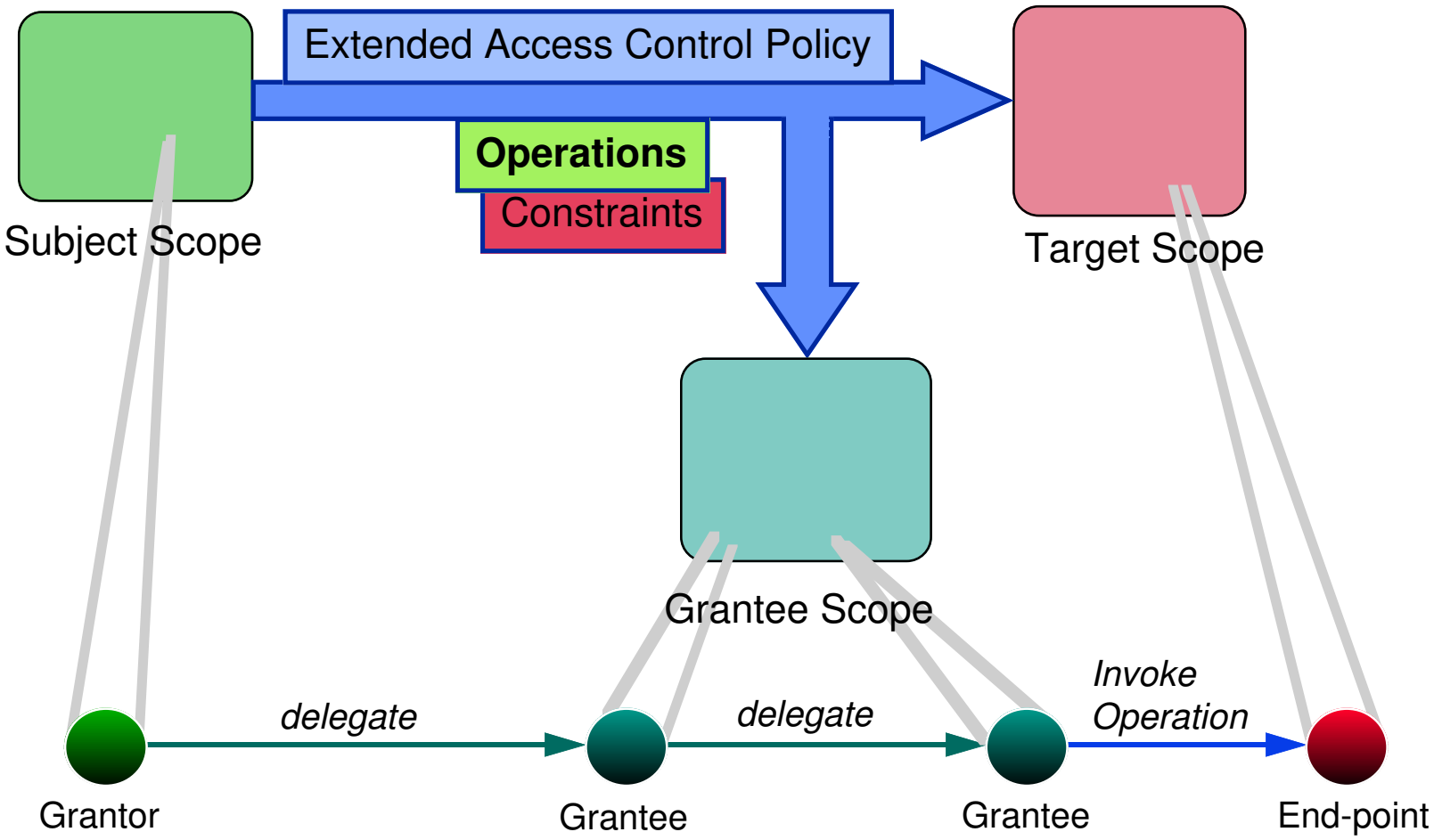
Access Control Policies



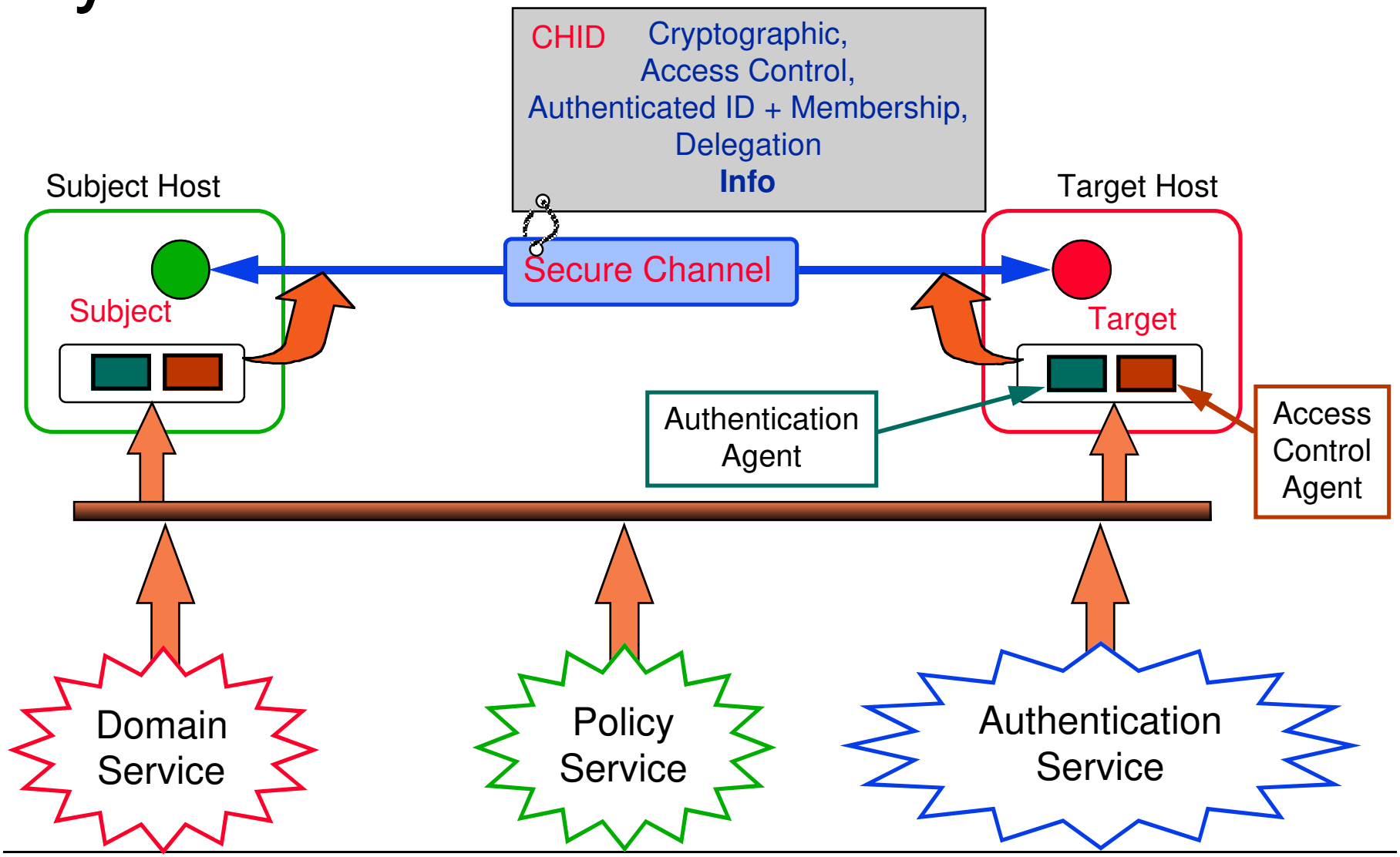
Access Control Policies (cont'd)



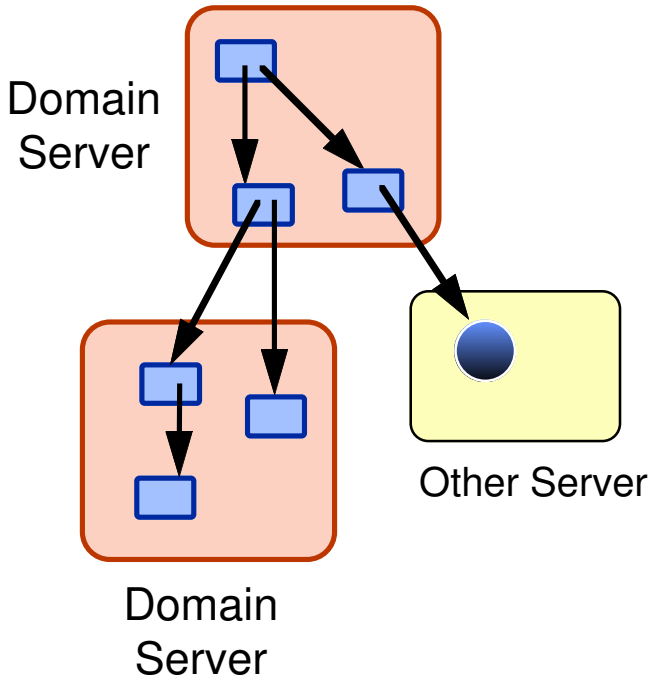
Controlling Delegation



System Overview



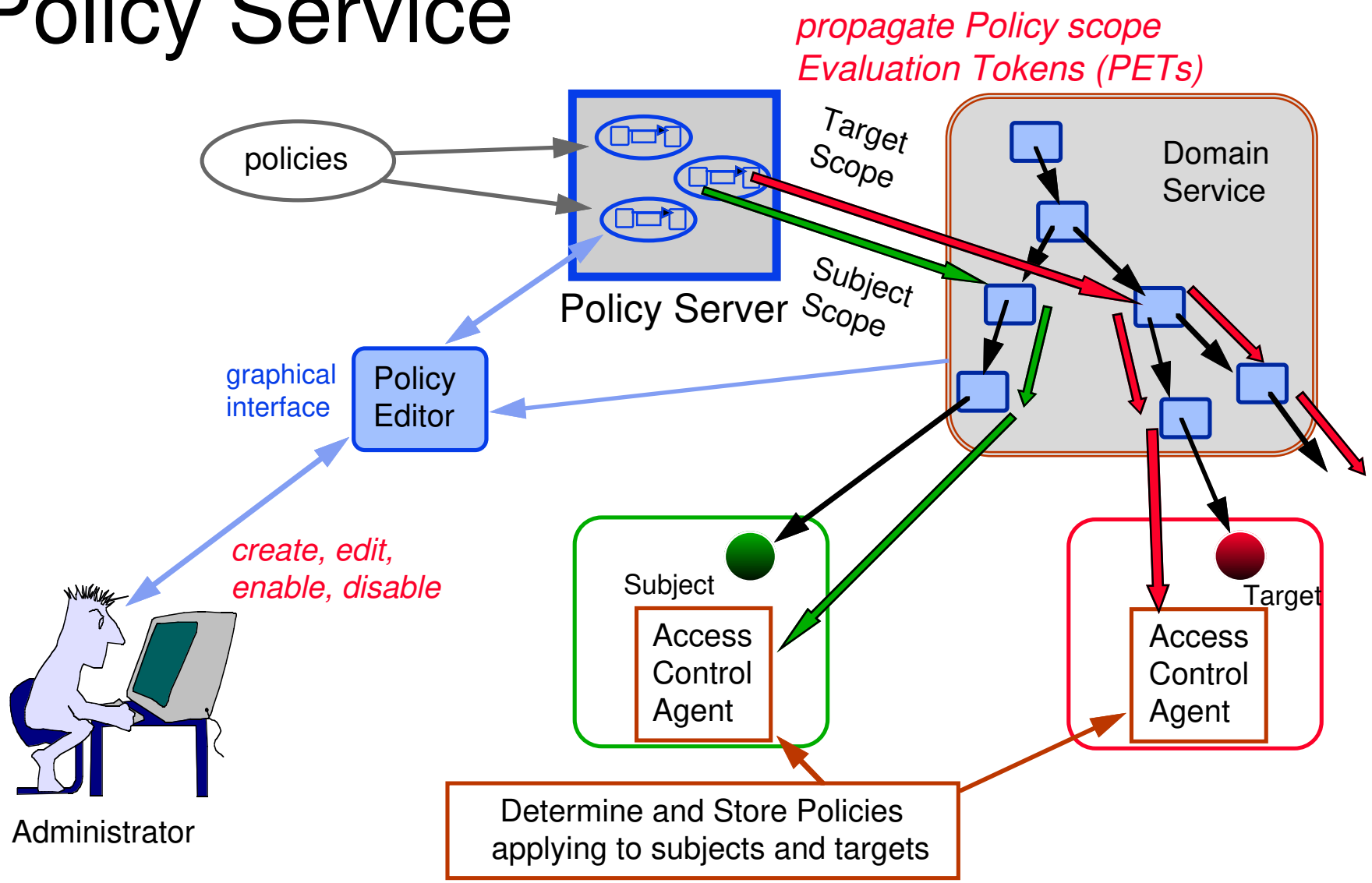
Domain Service



- Domain Service is **distributed** to reflect management distribution
- Distribution increases
  - the performance
  - the availability
  - the security

A domain server is trusted to certify membership of objects in the domains it maintains

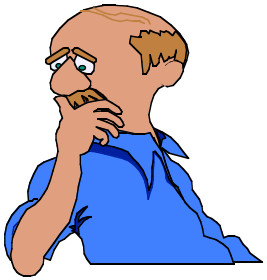
Policy Service



Authentication Service

- Access Control is based on domain membership
- Support Delegation

Large number of certificates and delegation tokens to be verified (especially when cascaded delegation is encountered)



Goal: Reduce cryptographic overhead

Authentication Service (cont'd)

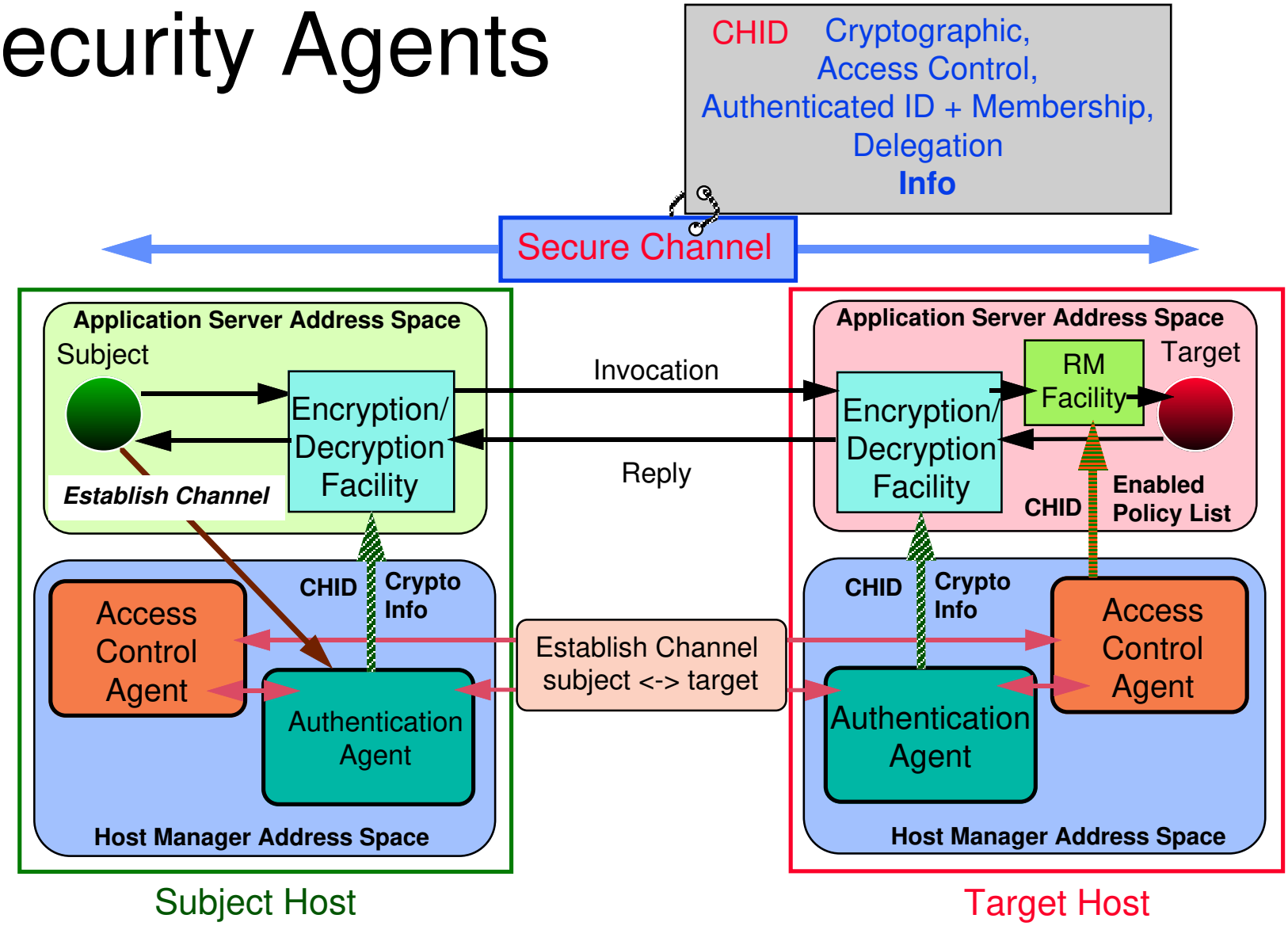
Intra-Realm Authentication:

- Based on **symmetric** encryption
  - reduced cpu-time for en/decryption compared to asymmetric
  - more flexible in terms of crypto-algorithms
- Use **replicated servers** with **minimal state** (Davis and Swick, 1990)
  - no server state consistency problems
  - simple authentication servers
  - key translation service - relay (simulate asymmetric encryption)
    - Delegation Tokens
    - verification of Domain membership
- Register Authentication Agents and Users (not application objects)
  - reduced security database size and update rate

Drawbacks

- stolen Master key compromises all keys
- increased network traffic

Security Agents



Implementation

Prototype in CORBA-compliant Orbix™ environment

- Domain Service
- Policy Service

⟹ policy propagation

- Graphical Interfaces using Tcl/Tk
  - Domain Browser
  - Policy Editor
- Access Control Agent, Reference Monitor

Conclusions and Future Work

The problem:

- Difficult to manage large distributed systems

Our Approach:

- Use domains to group objects in hierarchical structures
- Access Control (+ Delegation) Policies in terms of domains

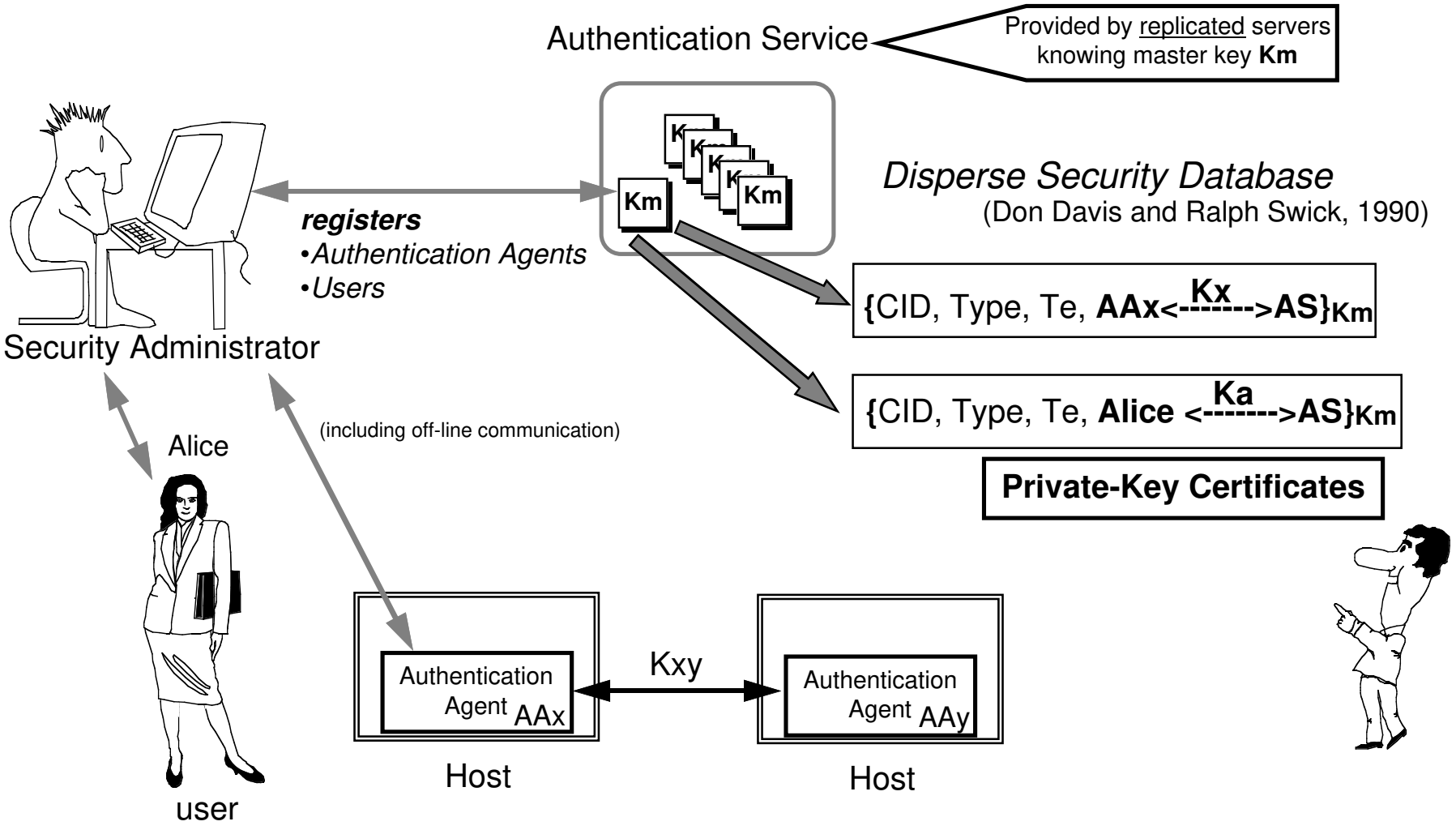
System:

- Distributed Domain Service to reflect distribution of management
- Policy Service
  - Dynamic Policy Scope Evaluation
- Authentication based on symmetric cryptography
  - Reduce en/decryption overhead
- Use of Security Agents on a per host basis
  - Reduce number of registered principals
  - Transparency of Security

Future Work:

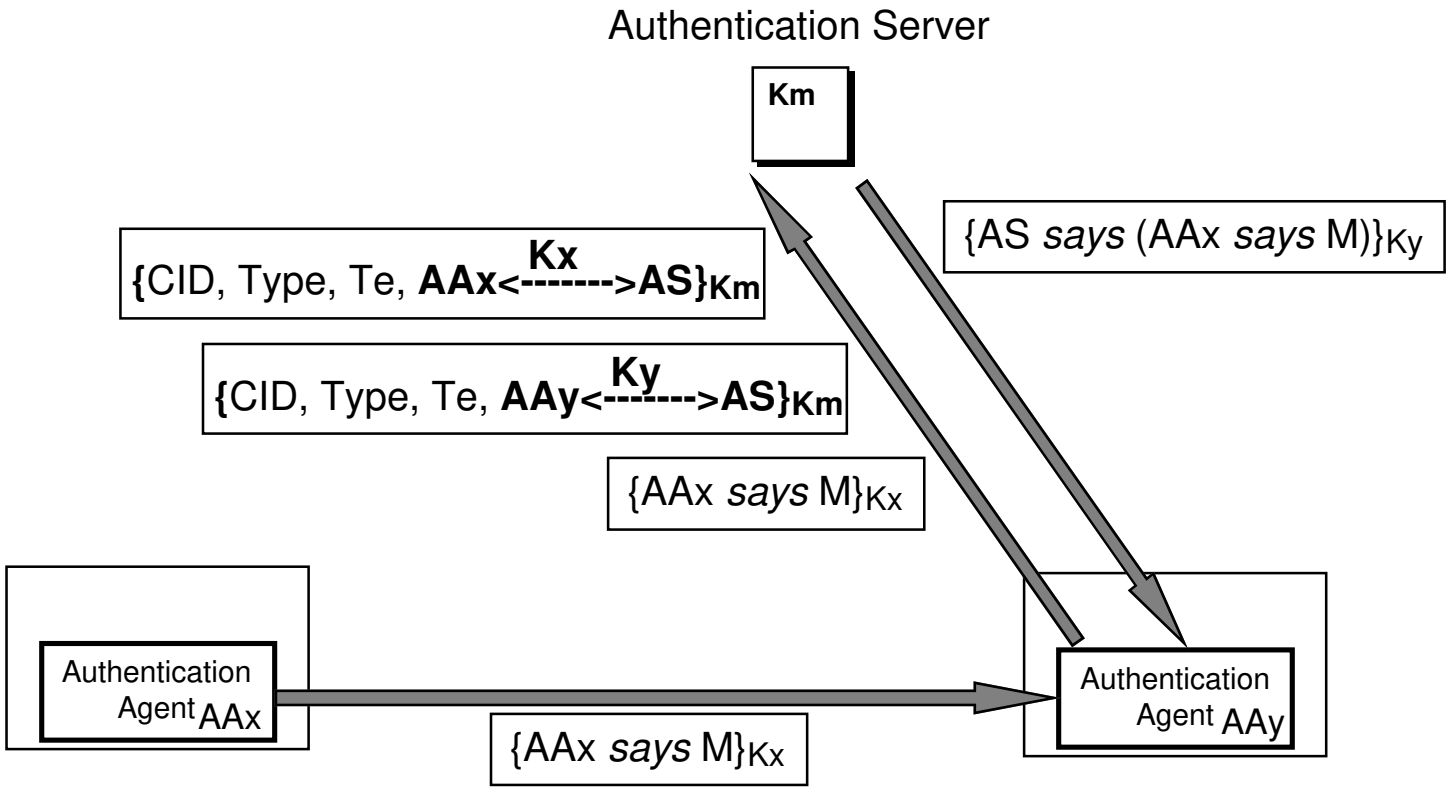
- Roles
- Auditing
- Intra-Realm Authentication

Authentication Service (cont'd)



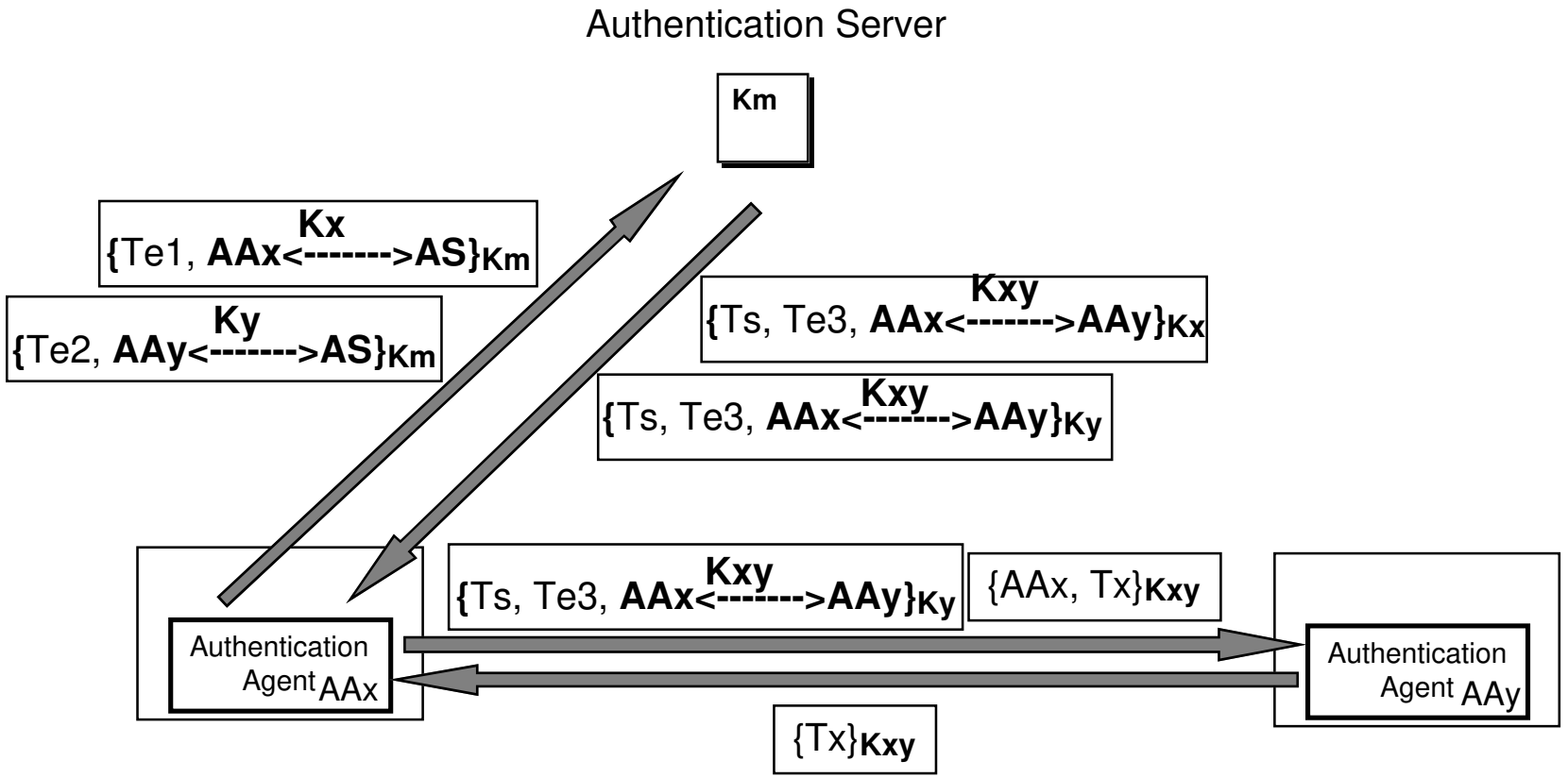
Authentication Service (cont'd)

Relay (key-translation service)

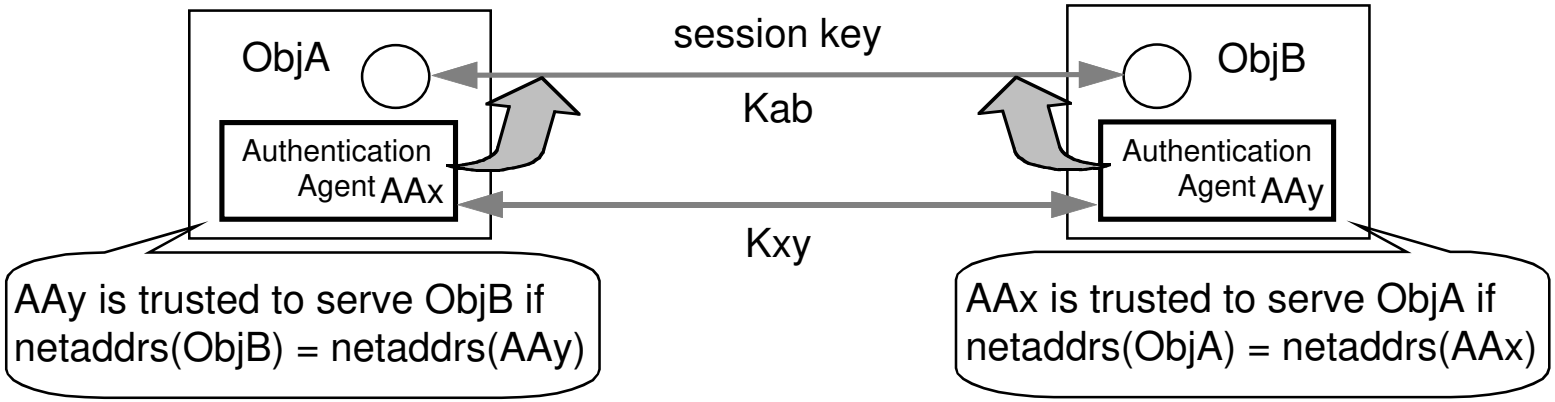


Authentication Service (cont'd)

Authentication Protocol



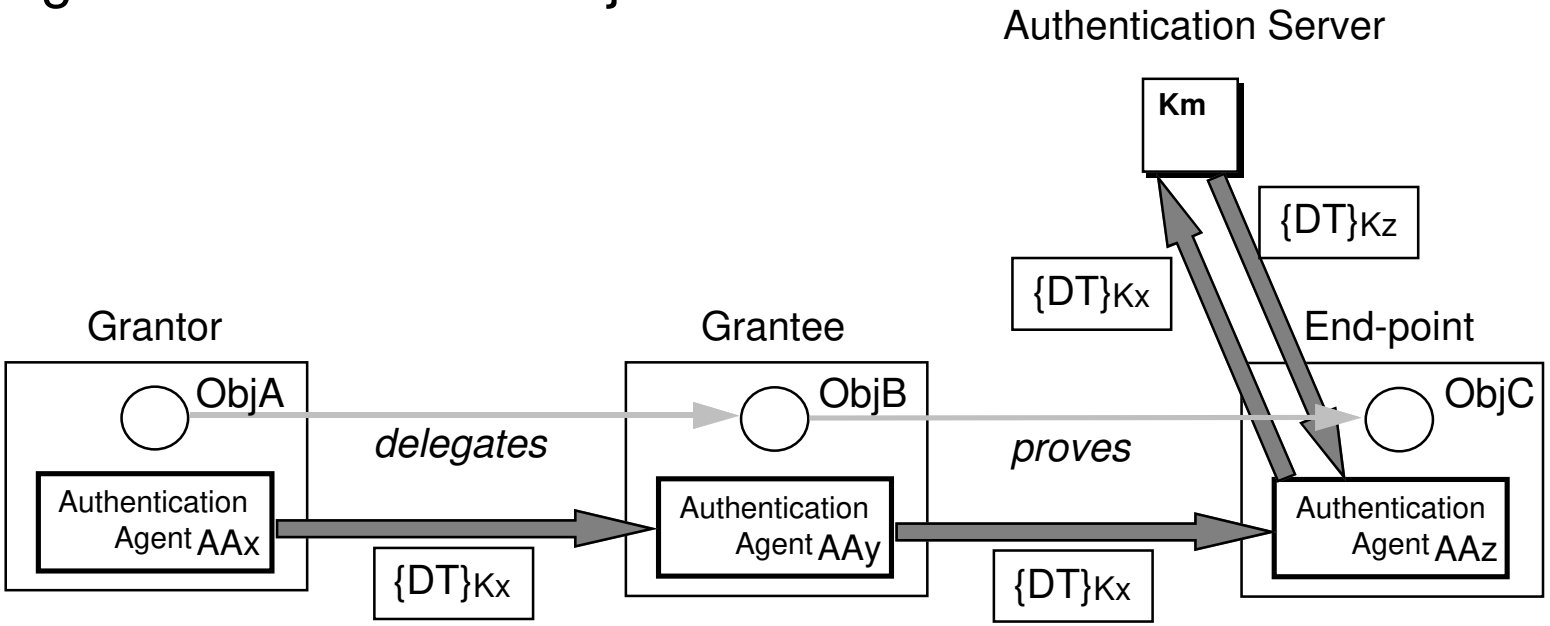
Authentication Service (cont'd)



Authentication Agents are trusted to serve objects on their hosts

Authentication Service (cont'd)

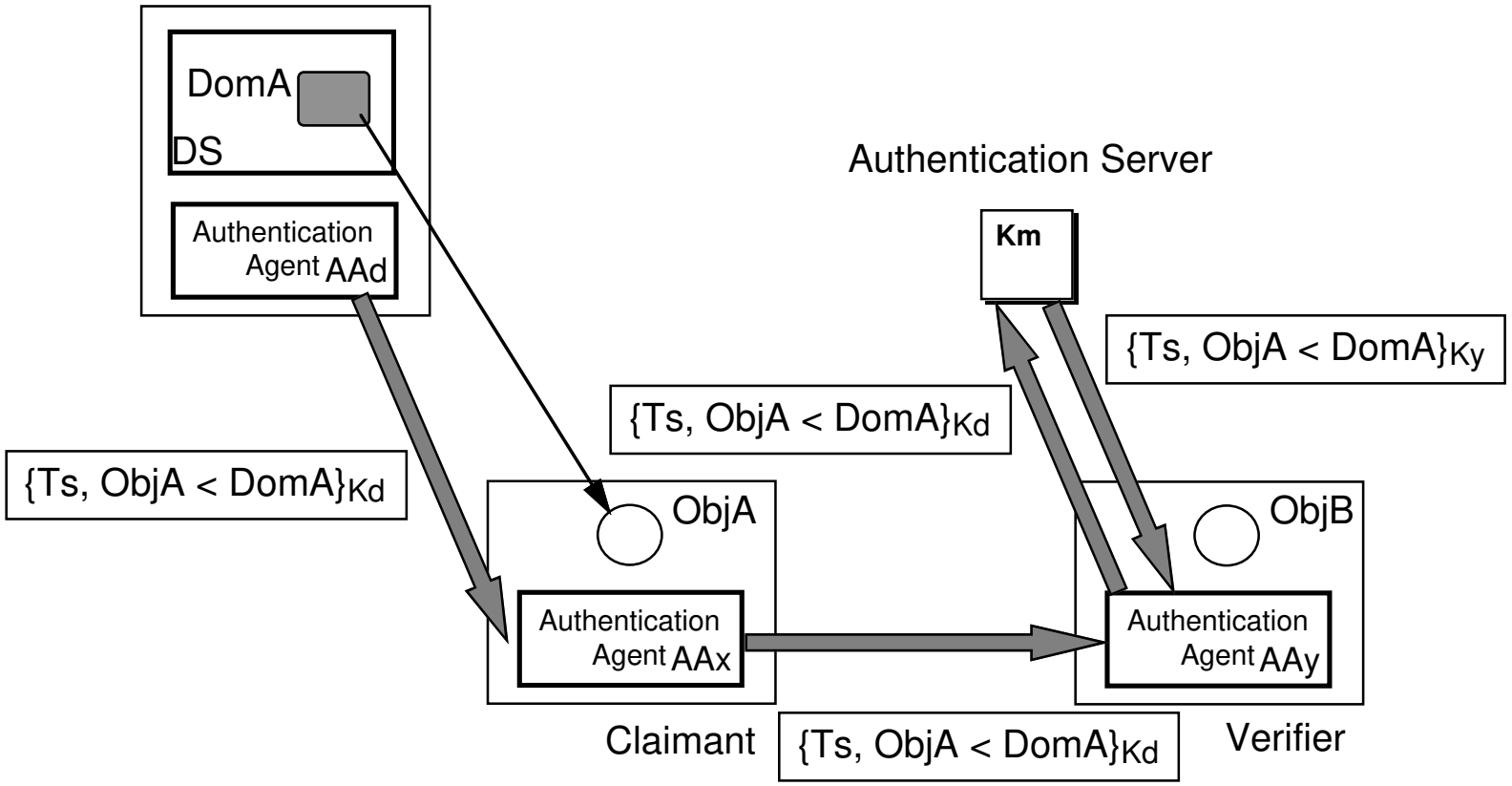
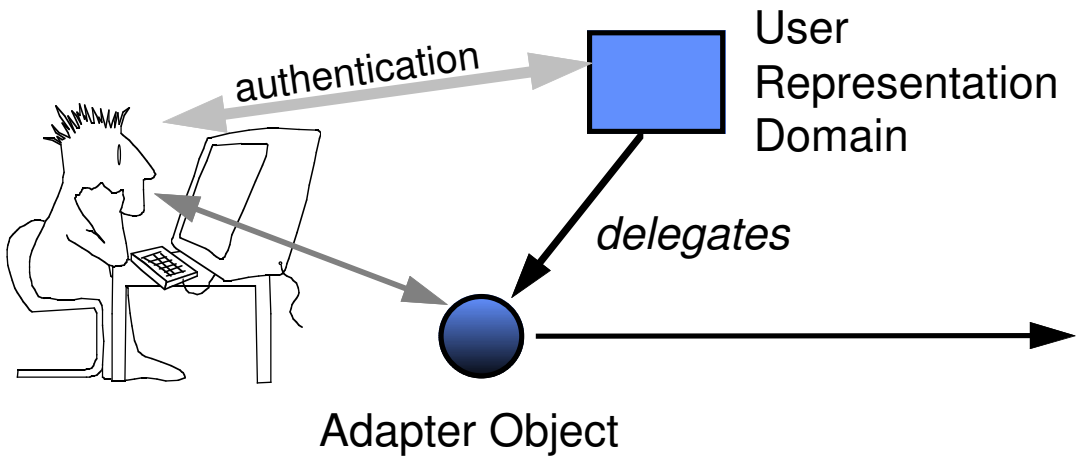
Delegation to a remote object



DT: [DID, PDT, Tde, DAR, Grantor, Grantee]

Authentication Service (cont'd)

Domain Membership Verification (push method)



User Authorisation