



Videoconferencing Middleware Architecture

v0.01, November 1, 2001

Ken Klingenstein

Project Director, Internet2 Middleware Initiative

Chief Technologist, University of Colorado at Boulder



Architectural Principles

- *Authentication of users happens in their own security domains, i.e. the client authenticates to its home service.*
- *Authorization decisions are usually made at the target. The target requests attributes from the source to make the authorization decision.*
- *The service where the authorization decisions are made need not be co-located with where the decisions are enforced.*
- *The exchange of information between the origin and the target should be secure, encrypted and authenticated.*
- *The target should be provided the minimal set of attributes necessary to make its decision.*



Desktop Video

- *Resource discovery*
 - finding/authenticating the target (i.e. IP address)
 - finding an appropriate gatekeeper, VRVS, etc.?
- *Connection establishment*
 - authenticated user
 - authenticated target?
 - target authorizes connection (and negotiates parameters)
 - security domains and intermediaries authorize the connection
- *Need for ongoing authentication/authorization services?*
- *Need for middleware for connection closure?*

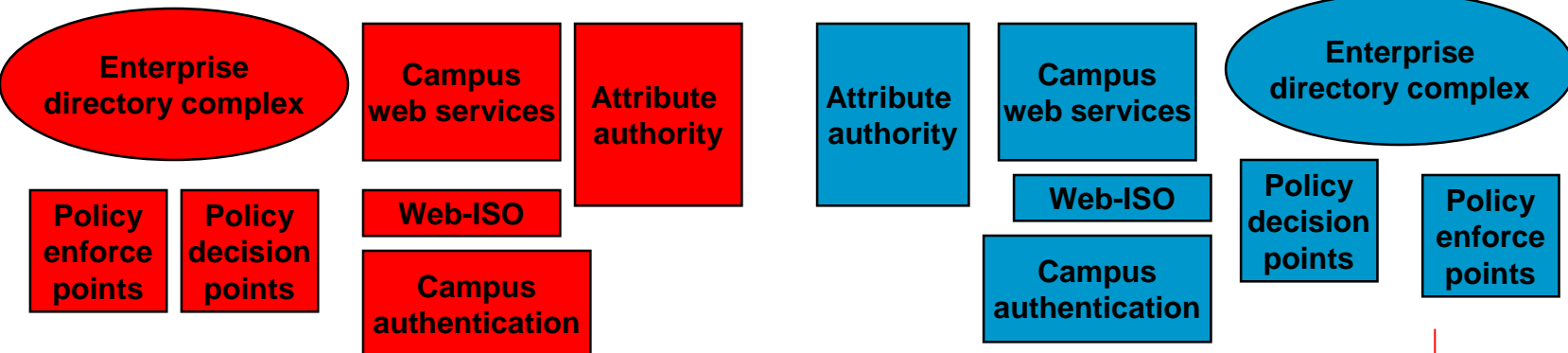


Videoconferencing Architectural Model

Most components within each security domain have existing interfaces.

MCU and/or other intermediaries

Arrows, i.e. protocols or APIs, can be drawn between security domains for almost any components shown. Wisdom suggests otherwise.





Resource Discovery Options

- *use DoDHE or ViDoDHE*
- *link or chain campus video directories*
- *search within video client*
- *use external search facility*
- *note registration of IP address issues*



Authentication Issues - Videoconference Originator

- *How to authenticate?*
 - through web interface?
 - direct access from client?
 - use of existing credentials (cookies, Kerberos tickets, certs)?
- *What identifier to authenticate against?*
- *What identifier to pass to target for authorization decision?*
- *What authorization decisions need to be made by the originating security domain? Where will the decision be made?*
- *Do inter-realm communications go through AA or through client or...*
- *What is the relationship between the video directory and the enterprise directory?*



Architectural Issues - Videoconference Target

- *How to permit service requests, and how to have service requests presented?*
- *How to communicate authorization decision to origin?*
- *What is the relationship between the video directory and the enterprise directory?*
- *How do resources like MCUs get represented in a directory?*



Inter-realm Architectural Issues

- *How to do resource discovery?*
- *Between what origination and target components should flows of information happen?*
- *What are the attributes and object classes necessary to achieve the required functionality?*
- *If the MCU or intermediaries are in other security domains, what are the authentication and authorization issues involved?*