
Secure real-time audio/video communication – H.350, Encryption & Gatekeeper/Proxy – using H.323 (...and a bit SIP)

Tutorial/workshop session
- H.350 directory services -

**19th APAN Meeting
Bangkok, Thailand
January 2005**

The Problem

- Managing Users and Workflow becomes the biggest issue once deployment scales up.
 - Requesting gatekeeper/proxy server entry
 - Requesting white pages listing for dialing info
 - How to do reliable billing
 - How to implement classes of service
 - Getting configuration information right in endpoints
- The Hardest and Most Expensive Part of Video / VoIP

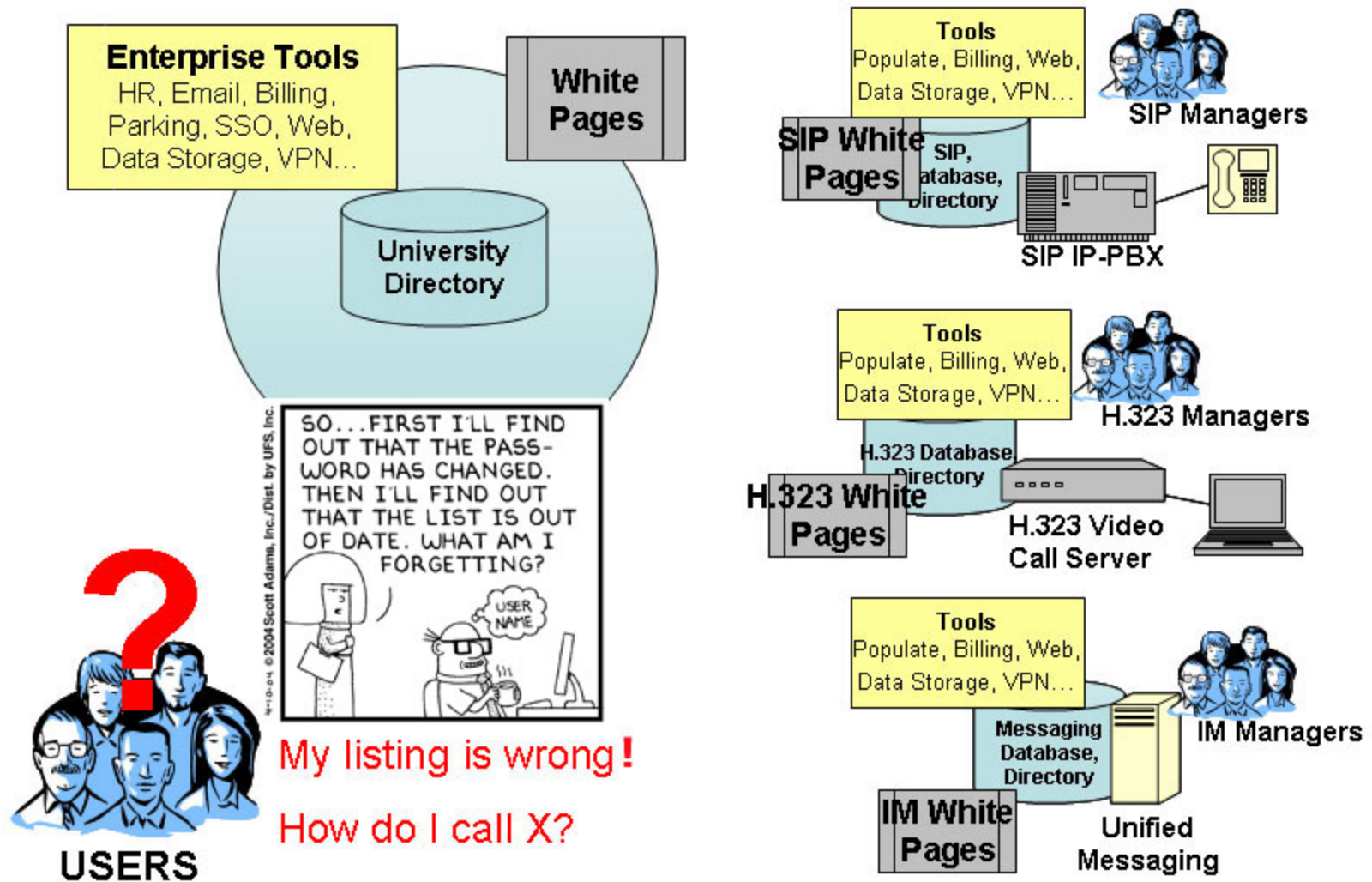
Resource Discovery

- How do I find people and endpoints?
- How do I find MCUs and gateways?
- Do I discover or 'register' resources?

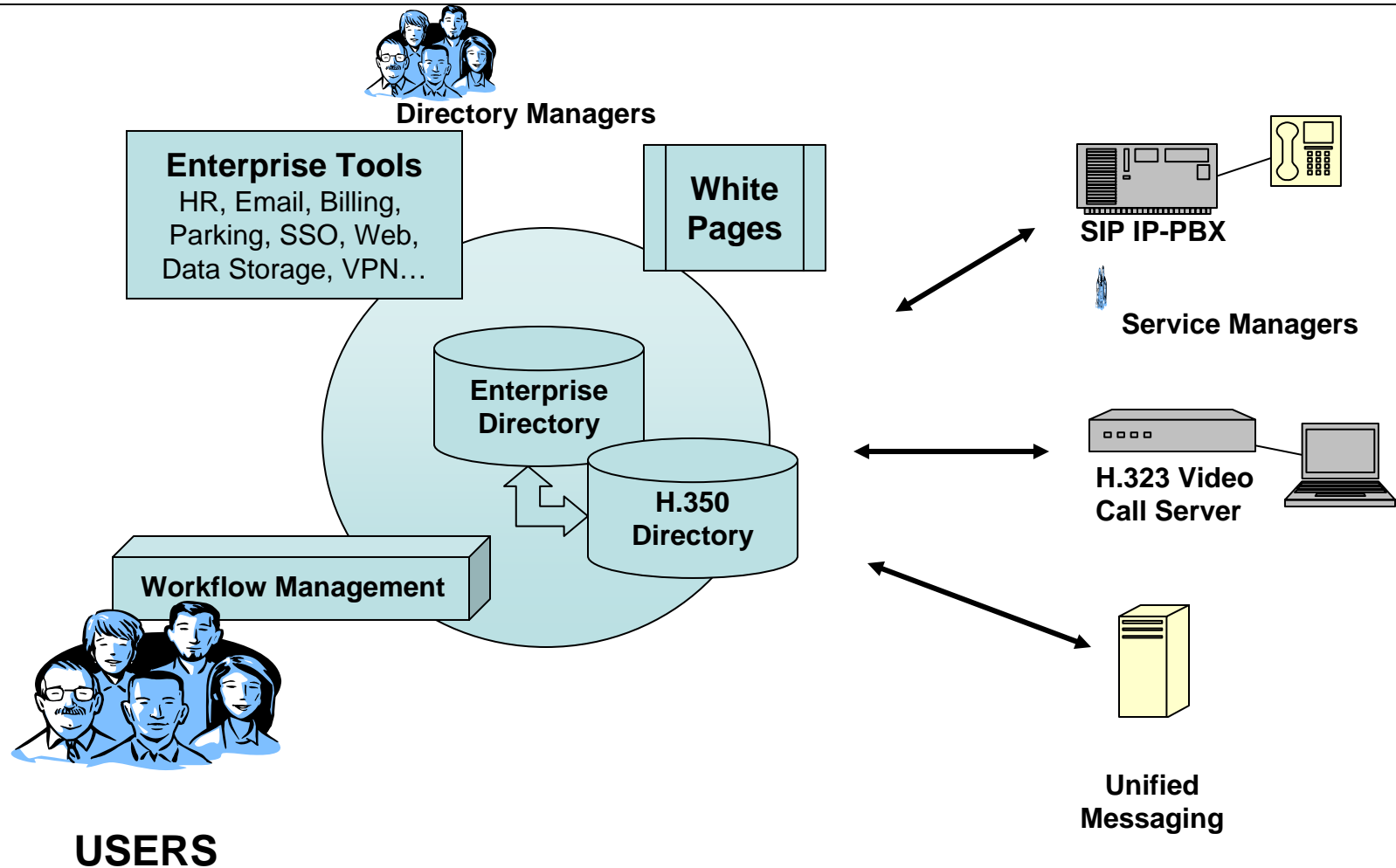
What Operational Needs?

- Universities are building central, authoritative user directories – Use this identity management system, don't require vendor's (often proprietary) directory
- Standardize storage of protocol-specific data to ease updates and migrations; one central data store for multiple protocols
- Leverage identity management for reliable USER (not device) authentication

Technology Silos → Redundant Processes & Confusion



The Solution: Directory-Enabled Video / VoIP

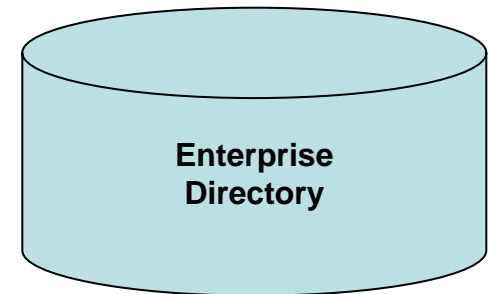


The Solution: Video Conferencing Directory Services

- Directories emerged as a key element of VC services
 - E.g. in ViDeNet
- White Pages function is critical
- Directory as canonical data source is essential for large scale enterprise deployments
 - Can't afford separate organizational unit to manage video 'accounts'
 - Rely on existing HR data management

Using: The Enterprise Directory

- Central stores of information about people associated with an institution
- Authoritative (eg: Human Resources, Registrar; Telecommunications)
- ONE consolidated list – duplicate identities resolved
- Benefits:
 - Correct and current
 - Single location to disable account
 - Single location to reset password
- Video/VoIP manager – reinvent this wheel?



Using: LDAP

- **Lightweight Directory Access Protocol**
- A protocol describes messages used to access certain types of data
- LDAP provides a data model (schema) that standardizes data naming and organization for global unique naming
- Derived from OSI X.500
- LDAP V3 ([IETF RFC 3377](#)) includes important security enhancements (SSL...)
- Features: Central Name Space & Identity Mgmt
- Highly flexible architecture
- Fast database, but specialized
- Can Enable: White Pages, Authentication, User / account management, Endpoint management

Benefits From Standardized Identity Management for Video / VoIP

- Without re-working business process, you can
 - Change vendor platforms
 - Have multi-vendor services
 - Integrate more than just video/voice (e.g. email, web)
- Leverage existing identity management tools
 - Most call server manufacturers not expert at identity management
 - LDAP tools are mature, secure, flexible, open

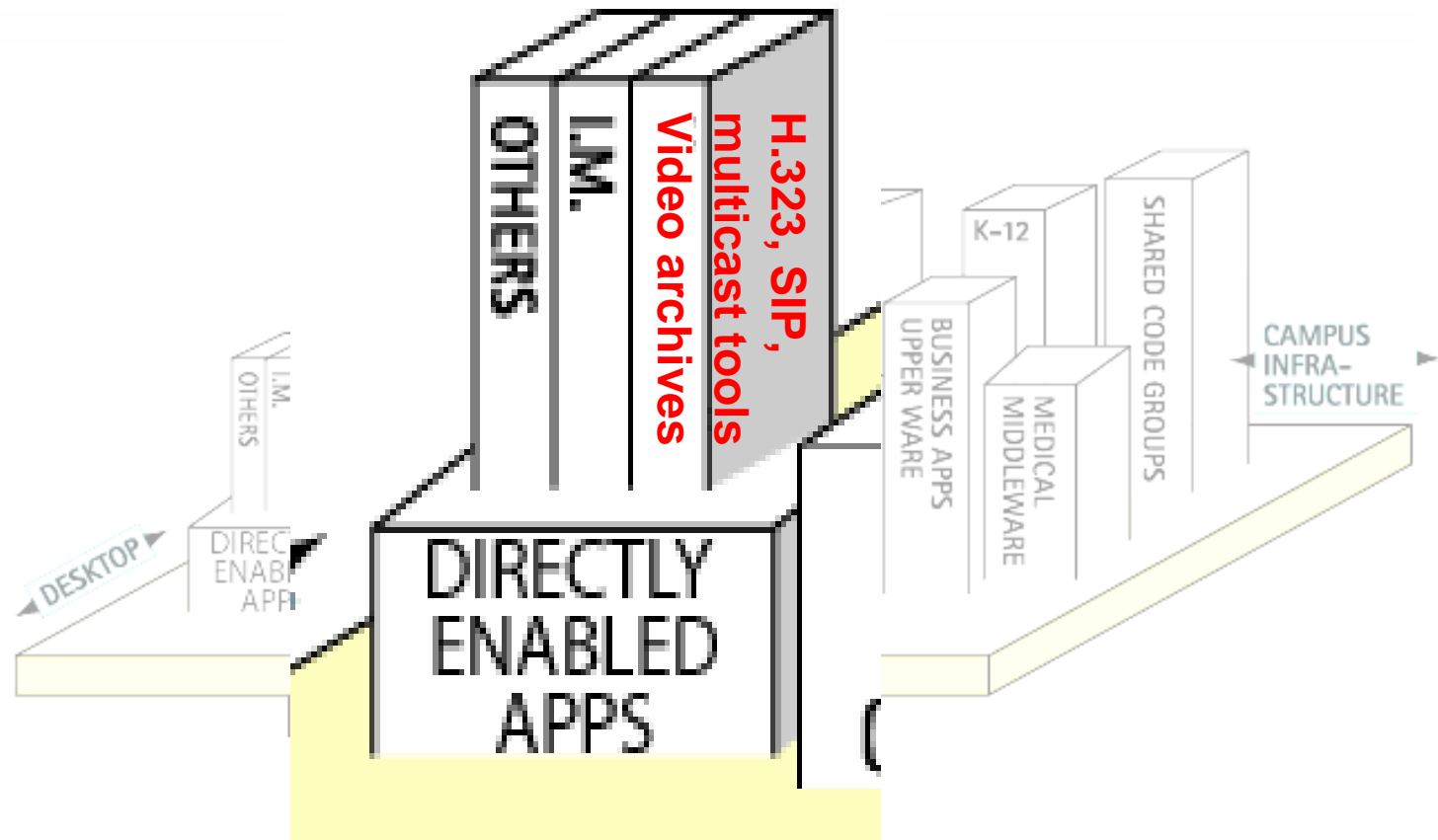
The Start

- Operational need for directory-enabled video/voice led to Video Middleware working group “vidmid-vc” (Internet2 Middleware and ViDe joint initiative)
<http://middleware.internet2.edu/video/>
- Project with NSF grant to UAB with partners CGU, SURFnet, UNC, and RADVISION
- Architecture proposed to ITU-T, accepted and ratified as H.350 in August 2003, also IETF informational

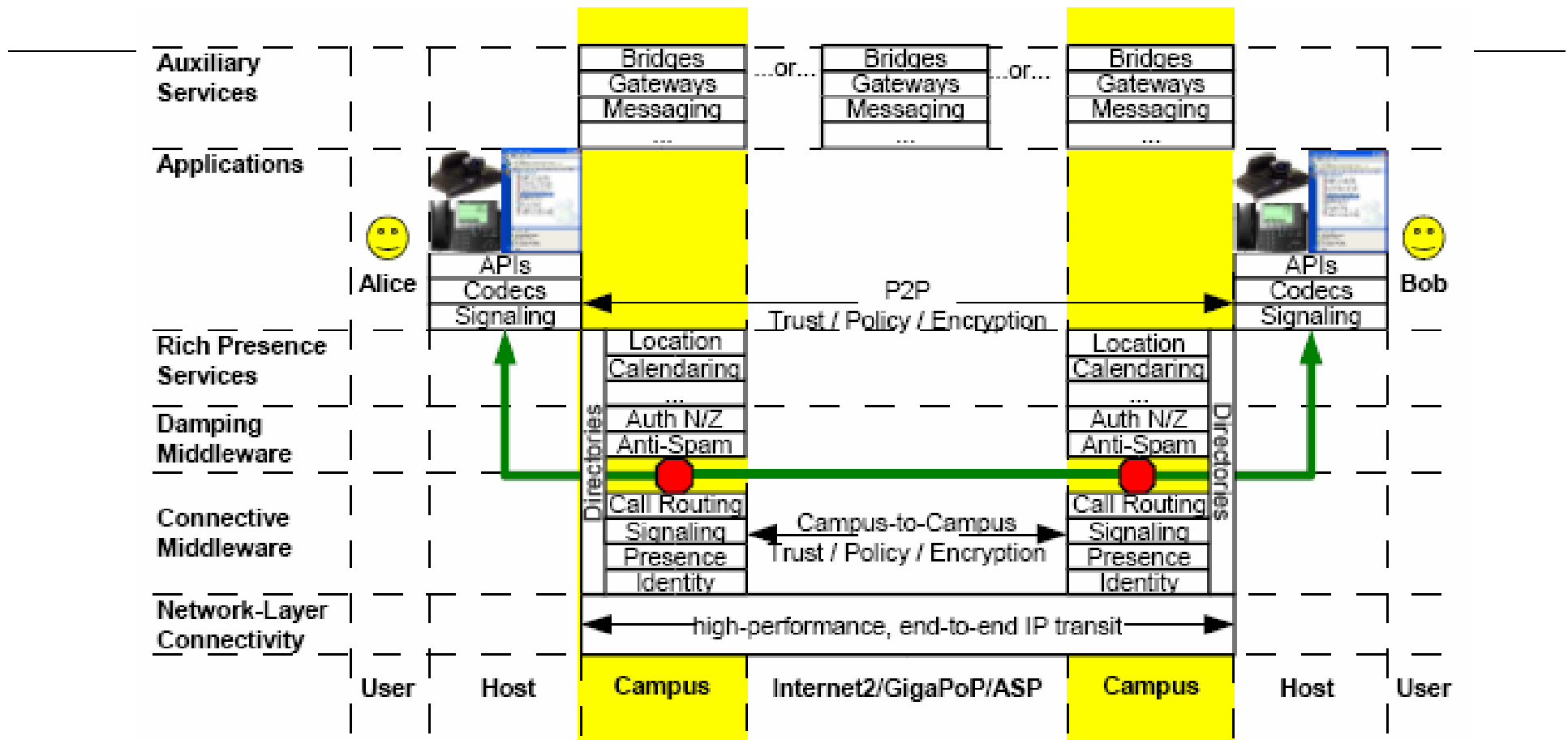
Video middleware

- Room for improvement. Today's VC apps:
 - No resource discovery – need to already know address of gatekeeper/proxy, target, gateway
 - Non-existent or unreliable authentication (who is calling?)
 - No authorization (all users have same access)
 - No security (eavesdropping)
- Develop Middleware Strategies and Prototype Working Code for
 - **FEDERATED** (No Root Authority; multiple policy)
 - **SECURE** (Authenticated Users; Ability to apply Usage policies; no eavesdropping)
 - **VIDEOCONFERENCING** (H.323 and SIP) Services

Where are we?



Communication middleware



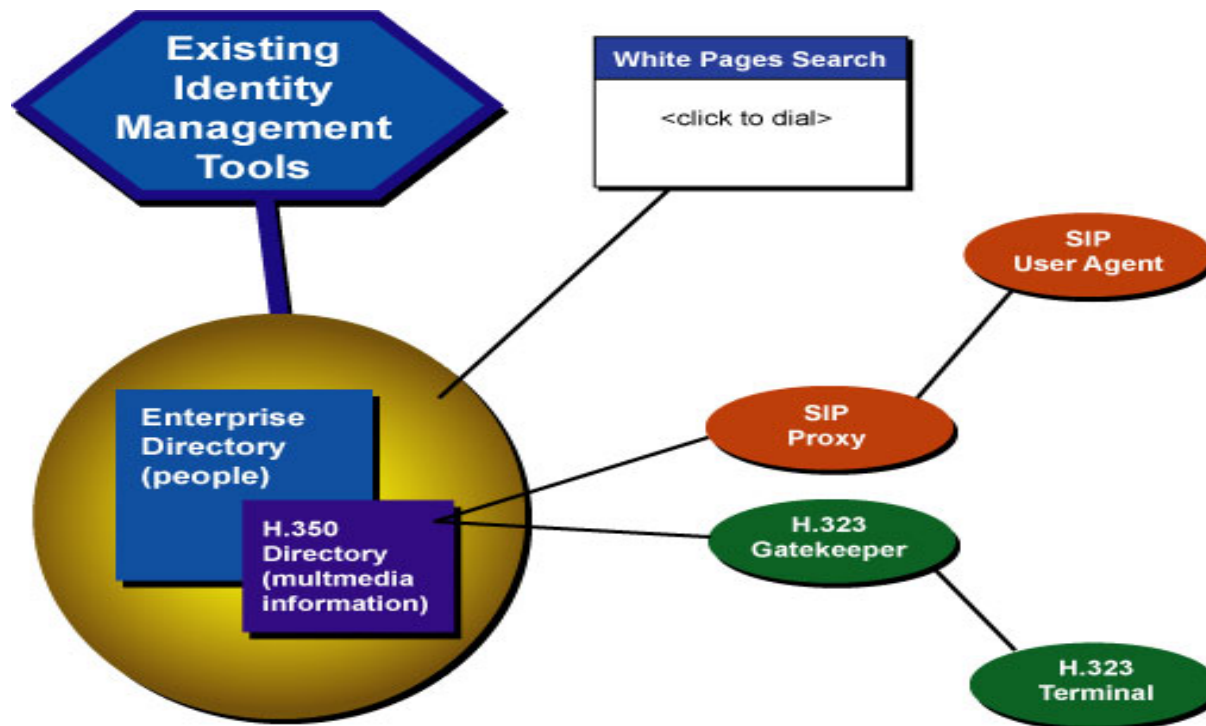
- Learn from “*Connective Middleware for Voice and Integrated Communications*” [Ben Teitelbaum, Internet2]

VC Directory Services Design Goals

- Associate endpoints with people
- Enable online searchable "white pages"
- Store all data in central directory (not call server); draw from authoritative source & avoid duplication
- Multiple endpoints/user; multiple protocols/endpoint
- Provide or auto-load per-user configuration
- Extensible
- "Lightweight" impact on enterprise directory
- Support global white pages "portals"

The Outcome

H.350 Architecture Components



What Is H.350 ?

- H.350 is
 - An LDAP schema
 - Standardized way to store information
 - Simple, basic elements are defined
 - Extensible – can include proprietary elements
 - Multi - protocol
- H.350 is not
 - A protocol
 - Just for H series protocols

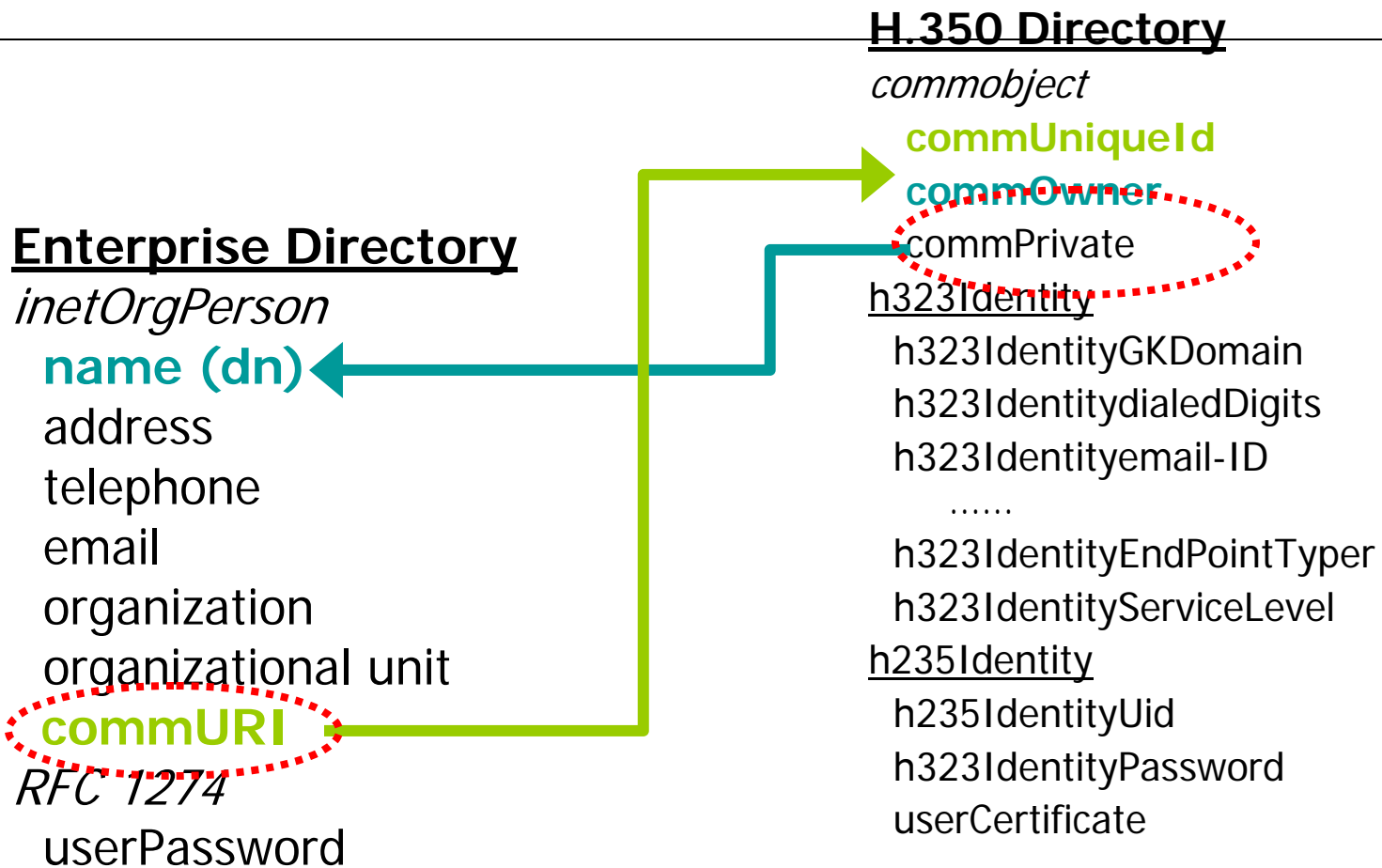
H.350 Series Recommendations

- **H.350** - Directory services architecture for multimedia conferencing
 - Base architecture
- **H.350.1** – Directory services architecture for H.323
- **H.350.2** – Directory services architecture for H.235
- **H.350.3** – Directory services architecture for H.320
- **H.350.4** – Directory services architecture for SIP
- **H.350.5** – Directory services architecture for non-standard protocols
- **H.350.6** – Directory services architecture for call forwarding and preferences
- **H.350.7** – Directory services architecture for Presence Information (XMPP)
- **H.350 Implementers Guide**

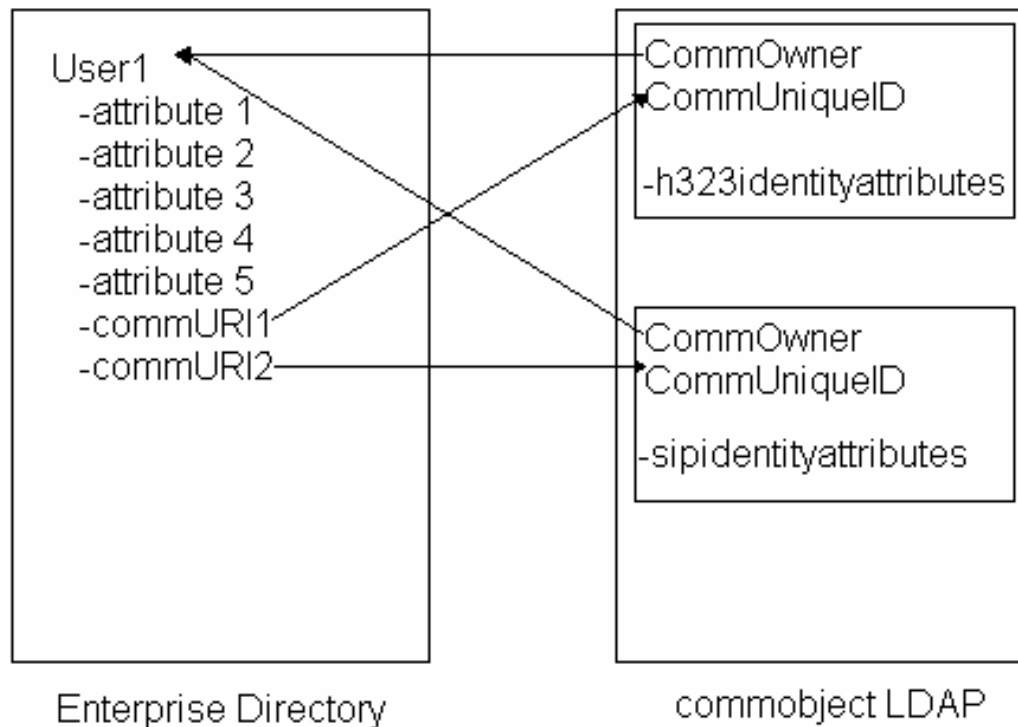
What About Presence?

- Call forwarding and Call preference *is not* presence
- sip.edu (an Internet2 project) uses presence and didn't think much of H.350.....until they scaled up their service and decided configuration storage and autoconfiguration were “good things”.

A Peek Inside H.350



Flexible Architecture

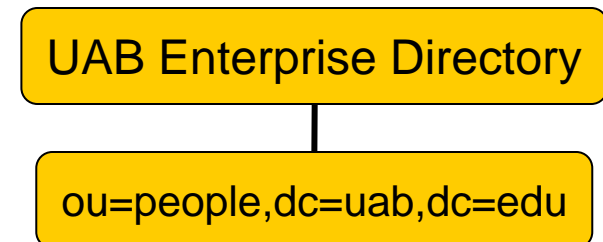
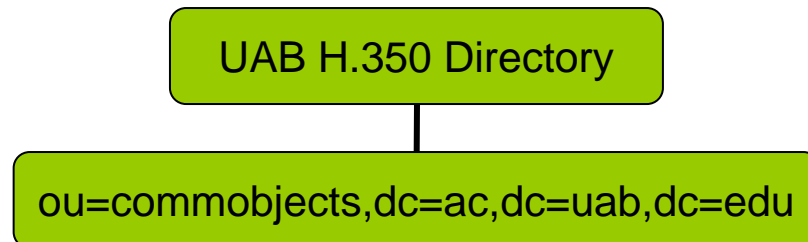
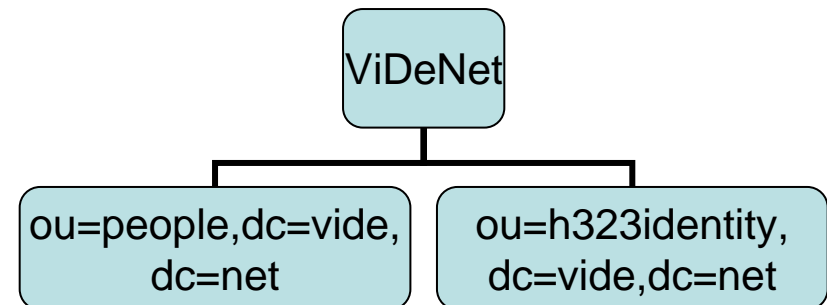


One person can be associated with more than one commURI (ie, device)

One person can be associated with multiple protocols, eg. H.323 *and* SIP

Flexible Deployment

- Enterprise and H.350 directories can be two branches of a single DIT *OR*
- May be implemented as two separately administered directories
- Enterprise entry needs only commURI



H.350.6 Call Forwarding and Preferences

- URI + Label
 - URI points to location where call forwarding address can be found
 - Label specifies type of forwarding and wait time
- Potential Targets
 - Another number
 - Unified messaging number
 - CPL script
 - mailto:
 - Web form ‘Sorry we missed your call. Please fill out this form and we’ll have someone call you back’
 - whack_a_mole.jsp video game

What about Rooms?

- Depends on objects available in enterprise directory
- Open question: if authentication is used, who should authenticate?
 - The device
 - The conference moderator
 - Everyone in the conference
 - All of the above

UAB Electronic Phonebook

<http://www.uab.edu/phonebook/>



Jill B Gemmill

BlazerID/Phonebook alias: **JGemmill**

Internet Email address: JGemmill@uab.edu

University department: **Academic Computing**

University job title: **Asst Dir Academic Computing**

Physical location of office: [Administration Building](#)

AB 719

Paper mail address of office: **1530 3RD AVE S
BIRMINGHAM AL 35294-0107**

Office telephone number: **(205) 975-2850**

Office hours: **9-6**

Current project(s): **Internet2, Secure Internet videoconferencing, ViDe**

Other colleges attended: **Antioch College**

URL for WWW use: <http://www.dpo.uab.edu/~jgemmill/>

Fraternity or sorority: **never have liked them much**

Degrees earned: **B.A.; M.S. ; MSEE**

Multimedia contact info:

- [\[H323\] My Desktop](#)
- [\[H323\] AB 7th Floor Room Unit](#)

Change Information



[H323] My Desktop

Attribute	Value
commOwner	jgemmill
h323IdentitydialedDigits	00115490000
h323IdentityEndpointType	Terminal

Search for a person

http://videnet.unc.edu/vidе-dod/index.phtml

The screenshot shows the ViDeNet search interface. At the top is the ViDeNet logo and a navigation bar with 'My ViDeNet' and a 'Help' dropdown. Below this is the 'University of Alabama' header. The main content area is titled 'Zone Essentials' and contains a search box with 'Jill' entered. A red arrow points to the 'Search ViDeNet' button. Below the search box are links for 'Click here for an Advanced Search.', 'Reset My Zone', and 'Need Help? - Call Your Zone Administrators'.

Enter name; Search

The screenshot shows the search results page. At the top is the ViDeNet logo and a navigation bar with 'My ViDeNet', 'Help', and a dropdown menu set to 'Zone Administrators Only'. Below this is the title 'ViDeNet Search Engine - Results - List' and a subtitle 'Your search returned the following from 2 unique user(s)'. A table displays the search results for 'jill'.

ViDeNet Search Engine - Results - List
Your search returned the following from 2 unique user(s).

You searched for: 'jill'	Endpoint Name	Name/Owner	Institution	Department
Jill Gemmill	My Desktop	Jill Gemmill	University of Alabama at Birmingham (UAB)	Academic Computing
Jill Gemmill	AB 7th Floor Room Unit	Jill Gemmill	University of Alabama at Birmingham (UAB)	Academic Computing
Jill Gemmill	No Endpoint Defined Yet	Jill Gemmill	University of Alabama at Birmingham (UAB)	Computer and Information Sciences

[New Search!](#) [Back](#)

Result: Associated with multiple endpoints

Other Searches Possible

ViDeNet Search Engine

Word or Phrase for Search:

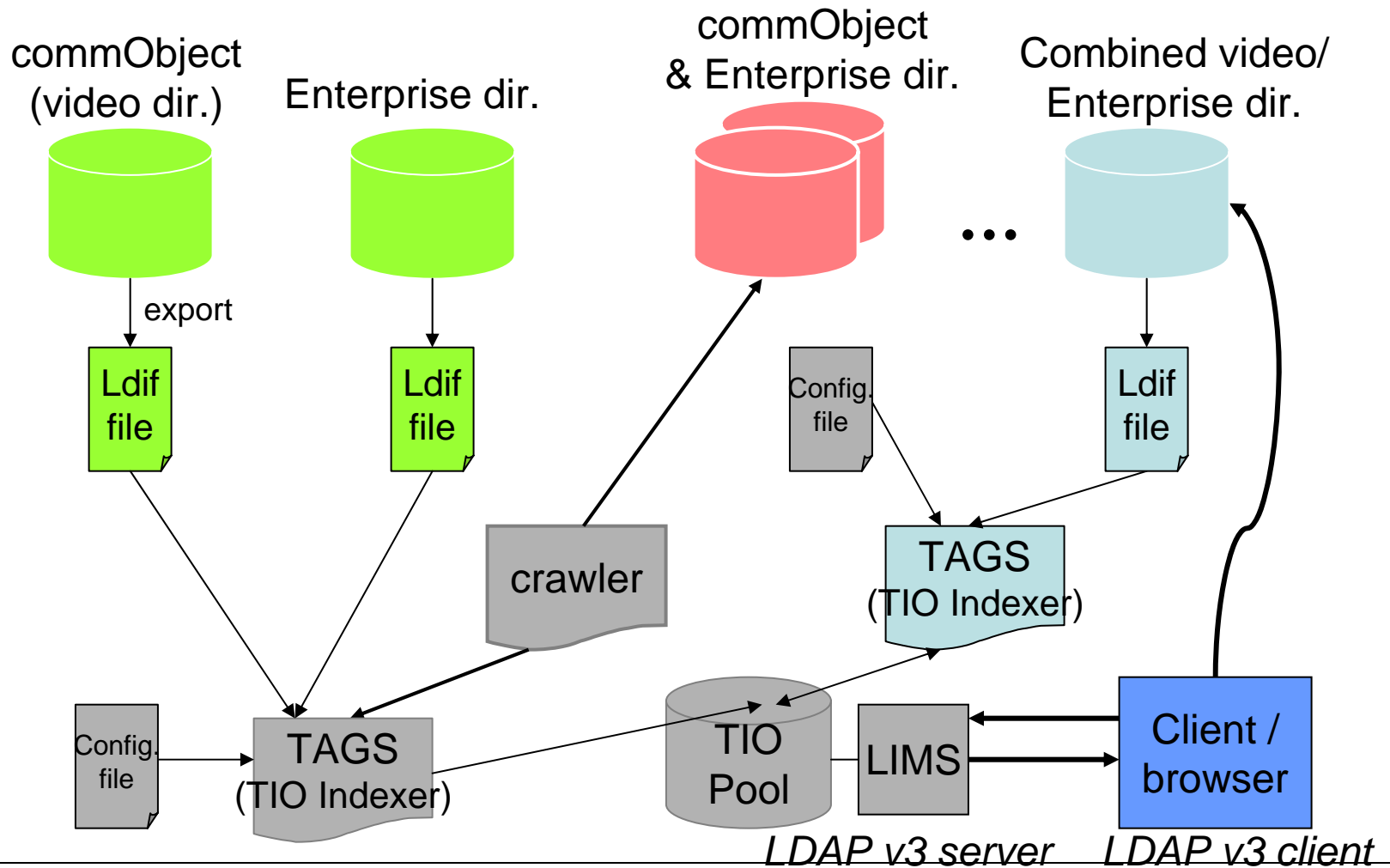
Select Field to Search:

From the Following Location:

ViDeNet Search Engine - Results - List
Your search returned the following from 5 unique user(s).

You searched for: 'UAB'	Endpoint Name	Name/Owner	Institution	Department
UAB	Endpoint Number 1	David Shealy	UAB	Physics
University of Alabama at Birmingham (UAB)	No Endpoint Defined Yet	Jill Gemmill	University of Alabama at Birmingham (UAB)	Computer and Information Sciences
University of Alabama at Birmingham (UAB)	My Desktop	Jill Gemmill	University of Alabama at Birmingham (UAB)	Academic Computing
University of Alabama at Birmingham (UAB)	AB 7th Floor Room Unit	Jill Gemmill	University of Alabama at Birmingham (UAB)	Academic Computing
UAB	No Endpoint Defined Yet	Julio Rivera	UAB	Accounting and Information Systems
UAB, CGU, UNC-CH, SURFNet, RADVISION	MCU Meeting Number	vnet ViDe.Net Middleware Protect	UAB, CGU, UNC-CH, SURFNet, RADVISION	National Science Foundation Grant

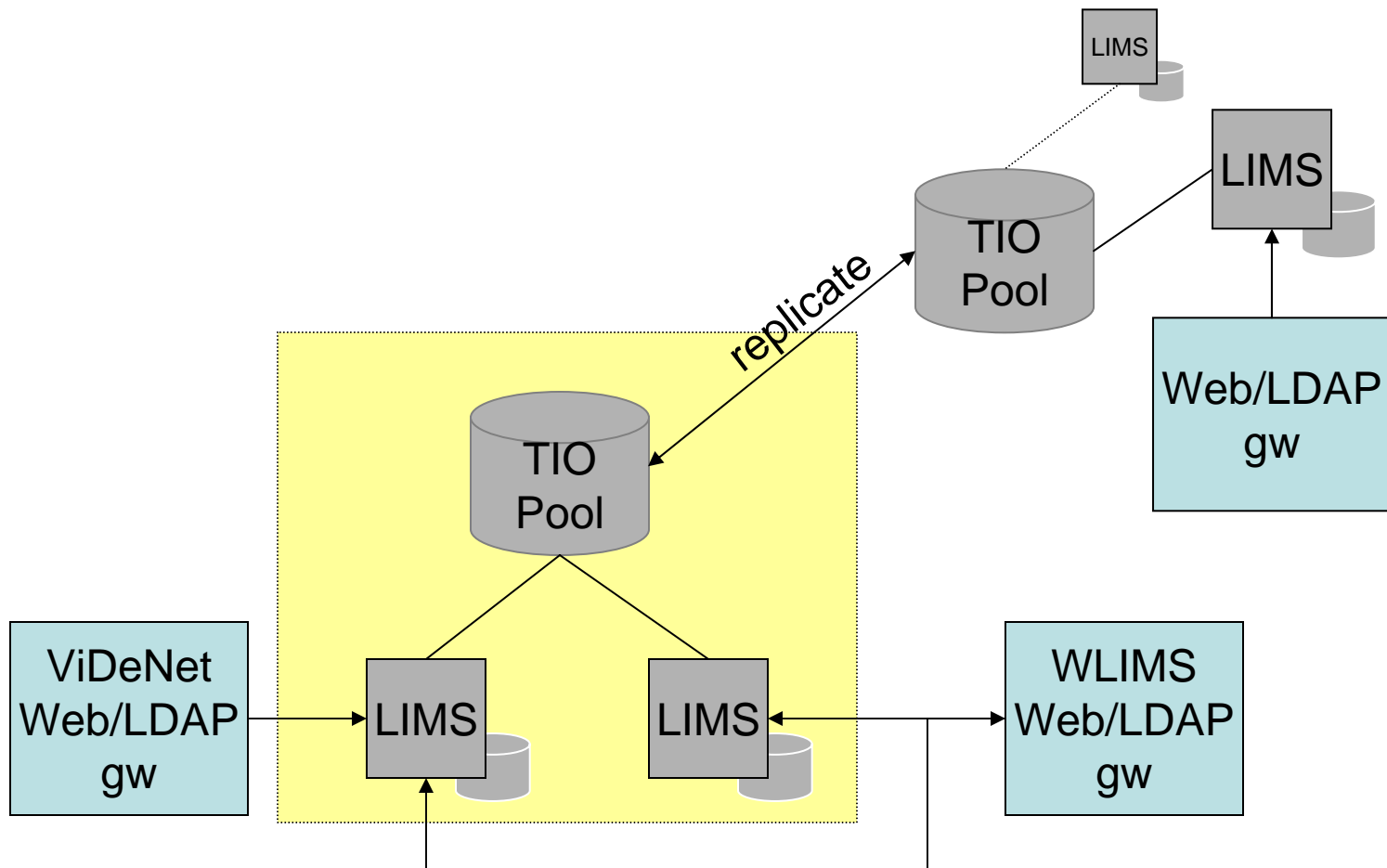
Global Directory Services



Directory of Directories Search

- [Simple Java Directory Search](#) searches public attributes in predefined list of directories.
- Under Development: scalable approach indexes remote directories (LIMS/TIO). A “google-like” repository linking back to distributed entries.

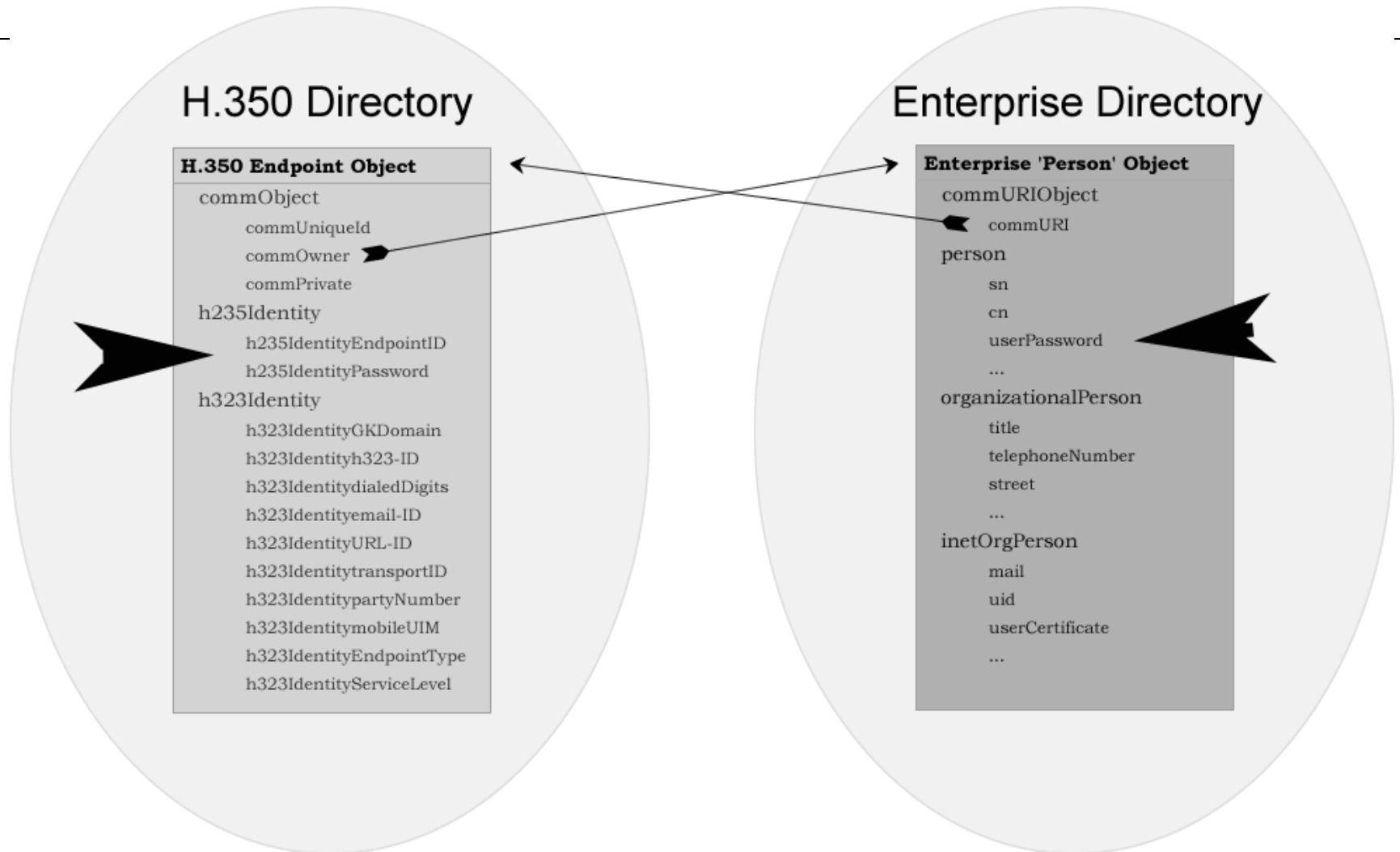
Distributed TIO pool



Software

- TAGS
 - LDIF to TIO converter
 - Roland Hedberg (Catalogix.se)
 - Open source
- LIMS (LDAP Index Metadata Server)
 - TIO/LDAPv3 index server
 - Roland Hedberg
 - Open source
- SUDALIS
 - LDAP crawler
 - Peter Gietz (DAASI)
 - Open source, but availability restricted
- WLIMS
 - Web/LDAP gateway
 - Stig Venaas (Uninett, Norway)
 - Open source

Security Credential Storage (H.235 and SIP)



Security Mechanisms in Voice&VC

H.323/H.235

- Annex D - Baseline Security Profile
 - Hop-by-hop processing
 - Password based security
- Annex E - Signature Security Profile
 - Certificate Based Security (PKI)

SIP

- End-to-end mechanisms
 - Basic authentication
 - Digest authentication
 - Message body encryption using S/MIME
- Hop-by-hop mechanisms
 - Transport Layer Security (TLS)
 - IP Security (IPSec)
 - The SIPS URI schema

Endpoints Implementing H.350 can...

- Lookup correct configuration information and load it.
Solves big user support issue!
- No matter what protocol or brand, necessary data can be managed in an organized way.
- Do white pages search via LDAP protocol – receive answers; ‘click to dial’ if supported.

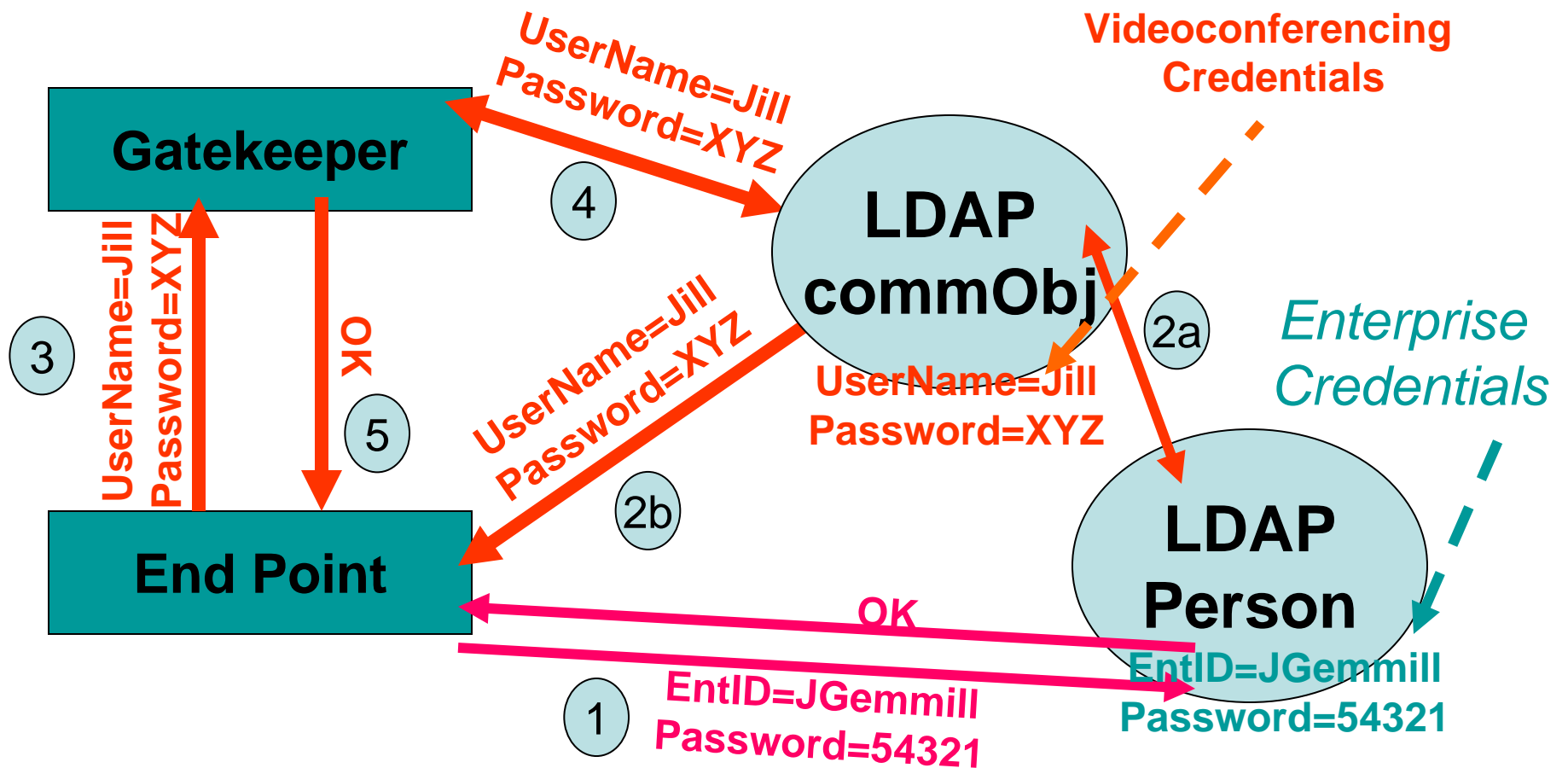
Endpoints Implementing H.235 can...

- Lookup correct configuration information and load it.
Solves big user support issue!
- No matter what protocol or brand, necessary data can be managed in an organized way.
- Do white pages search via LDAP protocol – receive answers; ‘click to dial’ if supported.

Call Servers Implementing H.350 can...

- Pull information from canonical store
 - Solves manual data entry problems
 - Can convert canonical to proprietary if needed on the fly
- Use `XIdentityServiceLevel` attribute to provide levels of authorization
- Scale up video/voip operations

Enterprise Authentication with H.350



So, does any of this stuff work
and exist in the real world?

Prototypes Developed

- ViDeNet and “early adopter” directory entries
- H.350-aware H.323 endpoint: RadVision
- H.350-aware gatekeeper: RadVision
- H.350-aware SIP user agent: CGU
- H.350-aware SIP Proxy server: HCL
- Automated configuration for endpoints
- Enterprise authentication used to obtain protocol-specific password
- White pages and “Directory of directories”

H.350 Enabled SIP User Agent

- Built by Samir Chatterjee and his Network Convergence Lab at Claremont Graduate University
- Built on Java Media Framework
- Uses DynamicSoft stack
- User agent available for download
<http://ncl.cgu.edu/sipclient/index.php>

Industry Uptake? Yes!

NetworkWorldFusion Search / Docfinder: [] Advanced search | Help | Site map

HOME | WHITE PAPERS | SPECIAL REPORTS | EVENTS | WEBCASTS | BOOKS/TRAINING | VENDOR VIEW | SUBSCRIBE | STORE

RESEARCH CENTERS

- Applications
- Careers
- Convergence
- Data Center
- LANs
- Net/Systems Mgmt.
- NOSes
- Outsourcing
- Routers/Switches
- Security
- Service Providers
- Small/Med.Business
- Storage
- WAN Services
- Web/e-commerce
- Wireless/Mobile

SITE RESOURCES

- Daily News
- Newsletters
- This Week in NW
- Tests/Reviews
- Buyer's Guides
- Opinion
- Forums
- Special Issues
- How to/Primers
- Case Studies
- Encyclopedia
- IT Briefings

XML

Layer 1

- Safe
- Pals
- votin
- mach
- More

TODAY

- Cour
- anti-
- Euro
- Focu
- MCI
- BMC

Convergence /
Vide Conferencing vendors embrace H.350

By [Jason Meserve](#)
 Network World, 03/22/04

RELATED LINKS | BREAKING NEWS

SEND | PRINT | FEEDBACK | REPRINT

In an effort to ease management of large IP video or even voice deployments, videoconferencing vendors are rallying around a new specification that standardizes the way endpoint addressing information is stored.

[H.350](#), the IEEE specification ratified in September for storing IP video and audio contact information in a central directory, is appearing in commercial products, most recently Radvision's [Enhanced Communications Server 3.5](#) gatekeeper release, a server that authorizes endpoints on a network and provides dialing plans such as mapping a standard four-digit extension to a device's IP address.

Advertisement:
 Brought to you by: [NetworkWorld](#)

Unlike many "h-dot" standards, H.350 is not a protocol, but a

FREE
 Subscription to Network World!
 \$255⁰⁰ value

Dimension
 Free Analyst White Paper from Check Point

Special Report
 Should you spend time and money pursuing IT certifications? Find out in NW's Special Report: It Pays to Certify

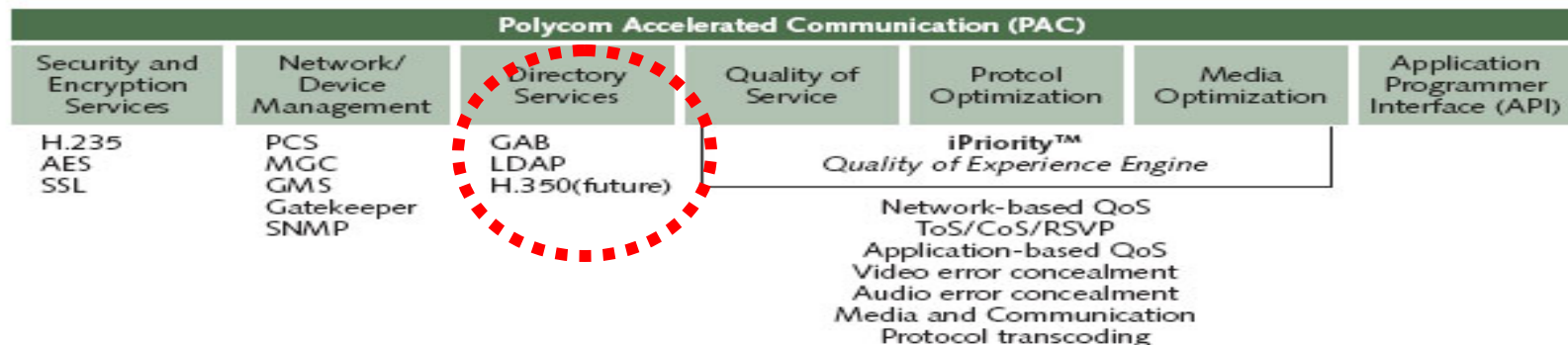
Download your free copy (registration required).

Advertiser Showcase
 Automated Patch Management for Microsoft Software

- RADVISION ECS
- VCON MXM (Q2 2004)
- Tandberg TMS 8.0
- HCL SIP Proxy
- Aethra

Exhibit 5 Polycom Accelerated Communications (PAC)

Source: Polycom, Inc., 2004




K. Stoeckigt, E. Verharen, kewin@acm.org, egon.verharen@surfnet.nl


ViDe H.350 Cookbook <http://lab.ac.uab.edu/vnet/>



quick links


 Cookbook for Videoconferencing Middleware:


- [HTML](#)
- [Version 0.5 pdf](#)
- [Version 0.64 pdf](#)
- [Version 0.73 pdf](#)
- [Version 1.0 pdf](#)


 H.350 Brochures


- [university](#)
- [vendor](#)

 [H.350 LDIF Files](#)

 [CGUsip Client v1.1](#)

 [Search](#) the ViDeNet proof of concept H.350 directory

 [Register](#) in the ViDeNet proof of concept H.350 directory

 [Search](#) the ViDeNet global video directory of directories prototype

May 27, 2004

[Version 1.0](#) of the ViDe H.350 Cookbook has been released!

April 08, 2004

Presentations for the 6th Annual SURA/ViDe Workshop and the H.350 Workshop are now available on the [presentations](#) page.

December 15, 2003

The [Video Middleware Cookbook 0.5](#) has been released for [National Science Foundation Middleware Initiative \(NMI\)](#).

March 19, 2003

Press releases are now featured on the [links](#) page.

March 19, 2003

The [CGUsip Client v1.1](#) is now available.

Questions and Comments: [Jason L. W. Lynn](#)
last updated Thursday, May 27, 2004 13:05

K. Stoeckigt, E. Ver... [http://lab.ac.uab.edu/vnet/](#)

ViDe H.350 Cookbook

- 60+ pages of text and 200 pages with step by step instructions and examples
 - Detailed description and example use of each attribute in all H.350 objects
 - LDIF files ready to use for iPlanet, OpenLDAP, and Active Directory
 - H.350 installation and server configuration instructions
- Included in [National Science Foundation Middleware Initiative \(NMI\) Releases 4 & 5](#)

Conclusions

- Videoconferencing Services are growing
- Managing these services well provides scalability and ease of use
- H.350 plus cookbook are valuable tools

Acknowledgments

Colleagues: Tyler Miller Johnson, Samir Chatterjee, Jill Gemmill, Jason Lynn
Internet2 Middleware Architects (MACE) and Video Middleware (VidMid) Working Groups
SURA Southeastern Universities Research Association

RADVISION, Cisco

NSF ANI-022710 “*ViDe.Net: Middleware for Scalable Video Services for Research and Higher Education*” (Gemmill (PI), Chatterjee, Johnson)

NSF ANI-0123937 “*NSF Middleware Initiative*” **via SURA-2002-103** “*UAB Middleware Testbed Program: Integrated Directory Services, PKI, Video, and Parallel Computing*”, Subcontract (Shealy, Gemmill (Technical Lead))

NSF EPS-0091853 via UA-01-016 “*Alabama Internet2 Middleware Initiative*”, NSF EPSCoR (Shealy, Gemmill (co-PI))

Any opinions, findings or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Links

- TNC2003 presentation on European VC services and GDS and H.350
<http://www.carnet.hr/CUC/tnc-cuc2003/program/slides/s6a1.pdf>
- ViDe.Net project
[http:// metric.it.uab.edu/vnet /](http://metric.it.uab.edu/vnet/)
- ViDeNet
<https://videnet.unc.edu/>
- ViDeNet dir. of video dir.s
<http://videnet.unc.edu/vid-dod/index.phtml>
- Vidmid-vc
<http://middleware.internet2.edu/video/>
- Presentations
 - Vidmid
<http://www.internet2.edu/presentations/spring02/20020507-VidMid-Verharen.ppt>
 - H.323 and Approaches to Authentication
http://www.dpo.uab.edu/%7Ejgemmill/Presentations/Year_2002/Internet2AUthNZ2002.pdf
 - Secure videoconferencing
http://www.vide.net/conferences/spr2003/presentations/day_one/jill_gemmill