

SURA/ViDe Digital Video Workshop *and*
ACM Computer Services Management Symposium
March 23, 2004

“ViDe.Net: Middleware for Scalable Video Services for Research and Higher Education”

Jill Gemmill, UAB

Tyler Miller-Johnson, UNC

May 2002-2004



Acknowledgement

- This material is based upon work supported by the National Science Foundation under Grant No. ANI-0222710 “*ViDe.Net: Middleware for Scalable Video Services for Research and Higher Education*”
 - Jill Gemmill (*PI*), *University of Alabama at Birmingham*
 - Samir Chatterjee, *Claremont Graduate University*
 - Tyler Miller-Johnson, *University of North Carolina-Chapel Hill*
 - Egon Verharen, *SURFnet*
- Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation

“Our Vision”

- Voice and video over IP to every person on Earth
- ViDeNet testbed provides managed ‘video and voice Internet’ for several hundred universities and research networks worldwide
(<https://videnet.unc.edu>)

Videoconferencing/VoIP is not just for geeks anymore

- Millions of people use VoIP in unmanaged, point-to-point calls everyday
- Managed services are growing
 - VoIP service providers w. > 100K customers
 - Higher education and K-20

Application Space

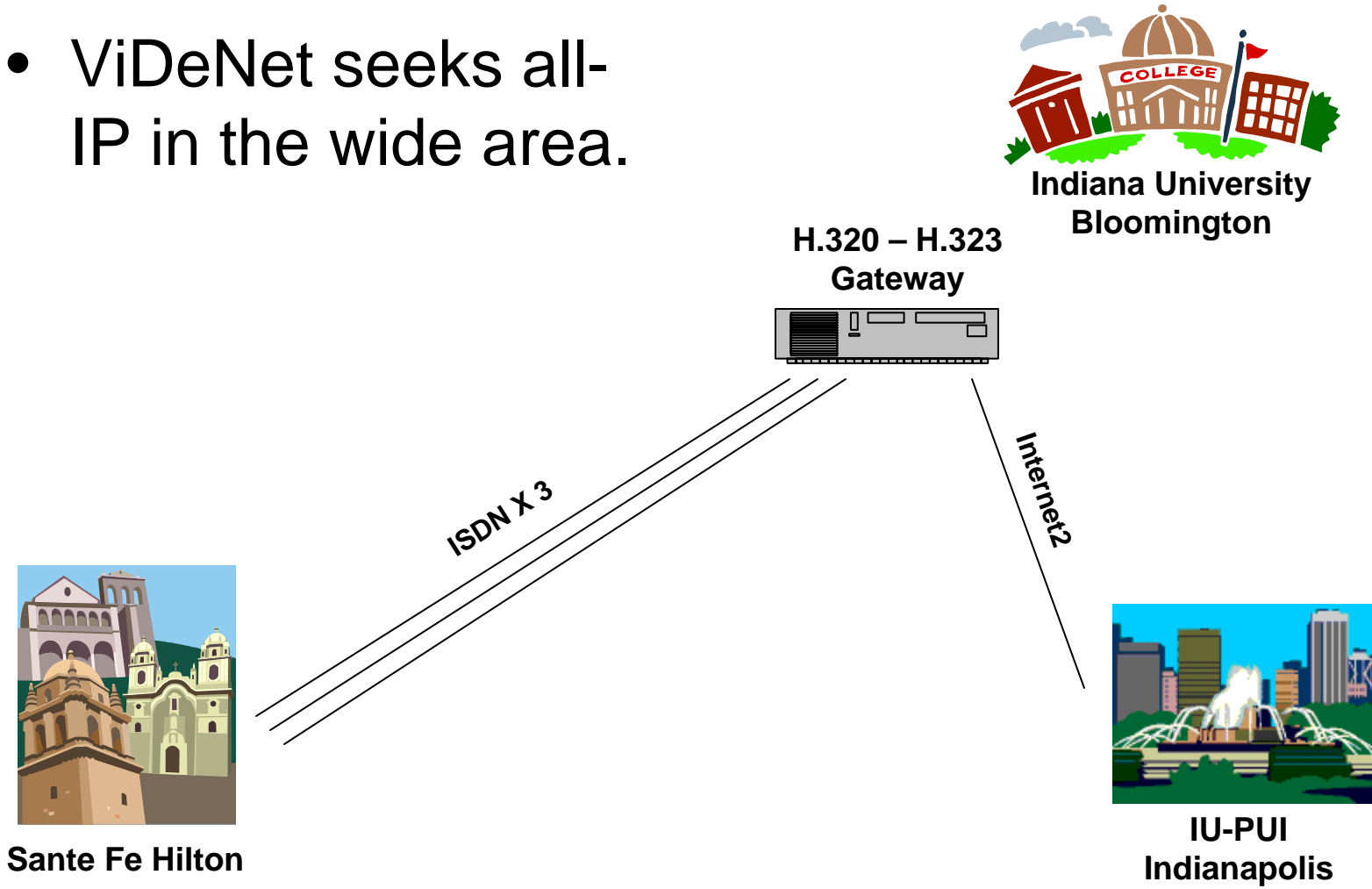
- Distributed classrooms
 - no longer limited by number of “special rooms”
 - Convenience (no distance to technology)
- Scientific Collaborations
 - Many large, multi-disciplinary centers
 - Regular planning, coordination, communication
- Higher-Education/K-12 Cooperation
- Telemedicine
 - Dermatology, Psychiatry, Prisoners, “E-Health”
- Administrative Meetings
 - Within University Systems
 - Across Universities

What is ViDeNet?

- **Test bed** promoting highly scalable and robust (standards-based) networked IP video and voice technologies.
- Over 156 **advanced voice and video networks**: higher education, some industry, K-12, and research organizations. 25 national zones.
- ViDe.Net architecture serves as the **core architecture** for the Internet2 Commons service
- **Mesh** of interconnected H.323 zones, now with SIP bridging.
- A **community** of video conferencing experts interested in sharing their knowledge and in working together to achieve better services for their user communities.

Today's Conference

- ViDeNet seeks all-IP in the wide area.



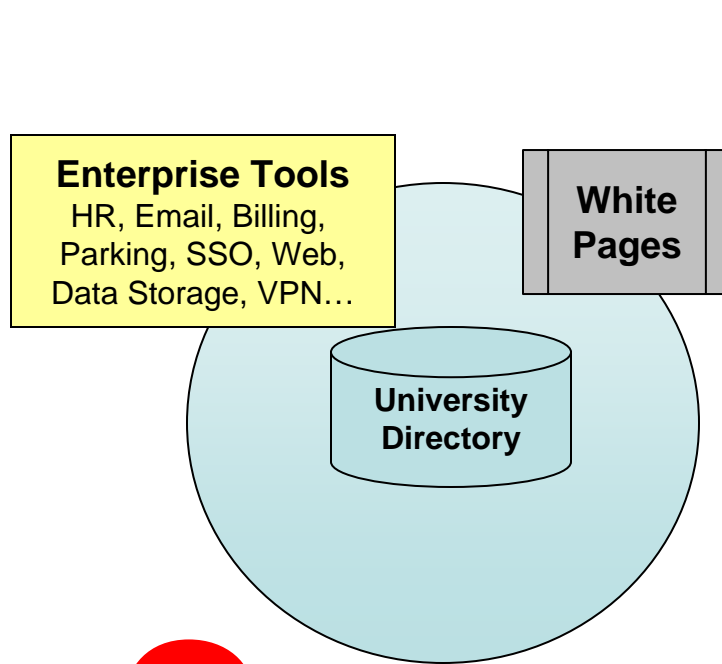
The Hardest and Most Expensive Part of Managed Video / VoIP

- Not the protocols – they work pretty well
- Not calls servers and endpoints – they work well and are reasonably priced
- Once deployment scales up, management difficulties multiply

Why H.350? What problems did ViDeNet want to solve?

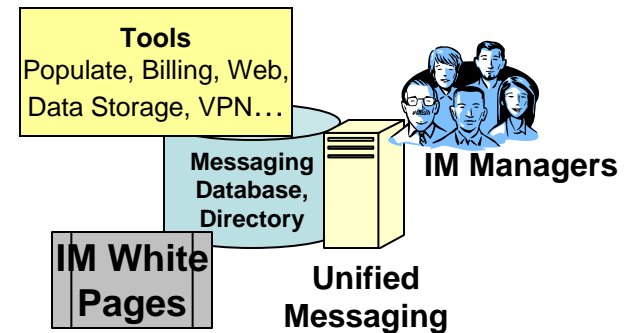
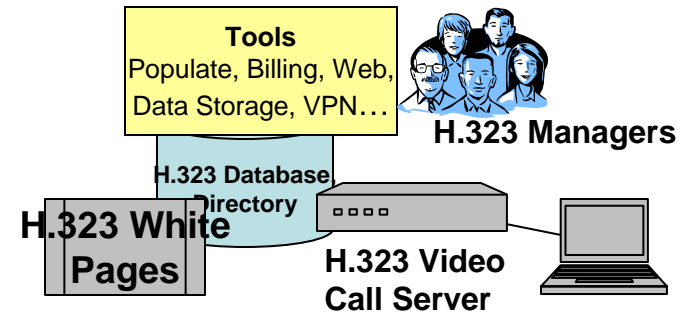
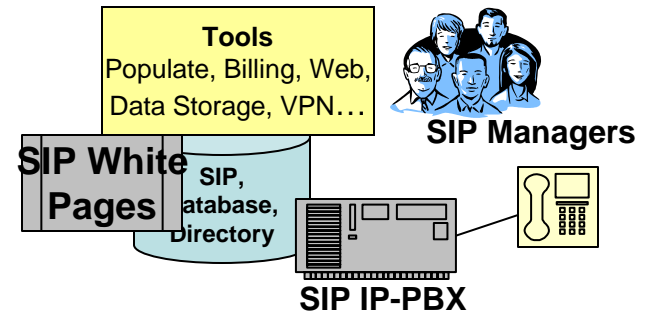
1. Application wants listing of authorized users;
 - Application provides “silo” directory
2. People want VC/VoIP “address books”
 - How do you find a ‘number’ you don’t already know?
3. Endpoints require some initial configuration; Call Servers store configuration information;
 - Parameters are protocol-specific, but storage format is all over the map
 - Separate storage facility needed for each brand of equipment
4. User authentication was poor or non-existent

Technology Silos = Redundant Processes



“My listing is wrong!”

“How do I call X?”



Solution Path

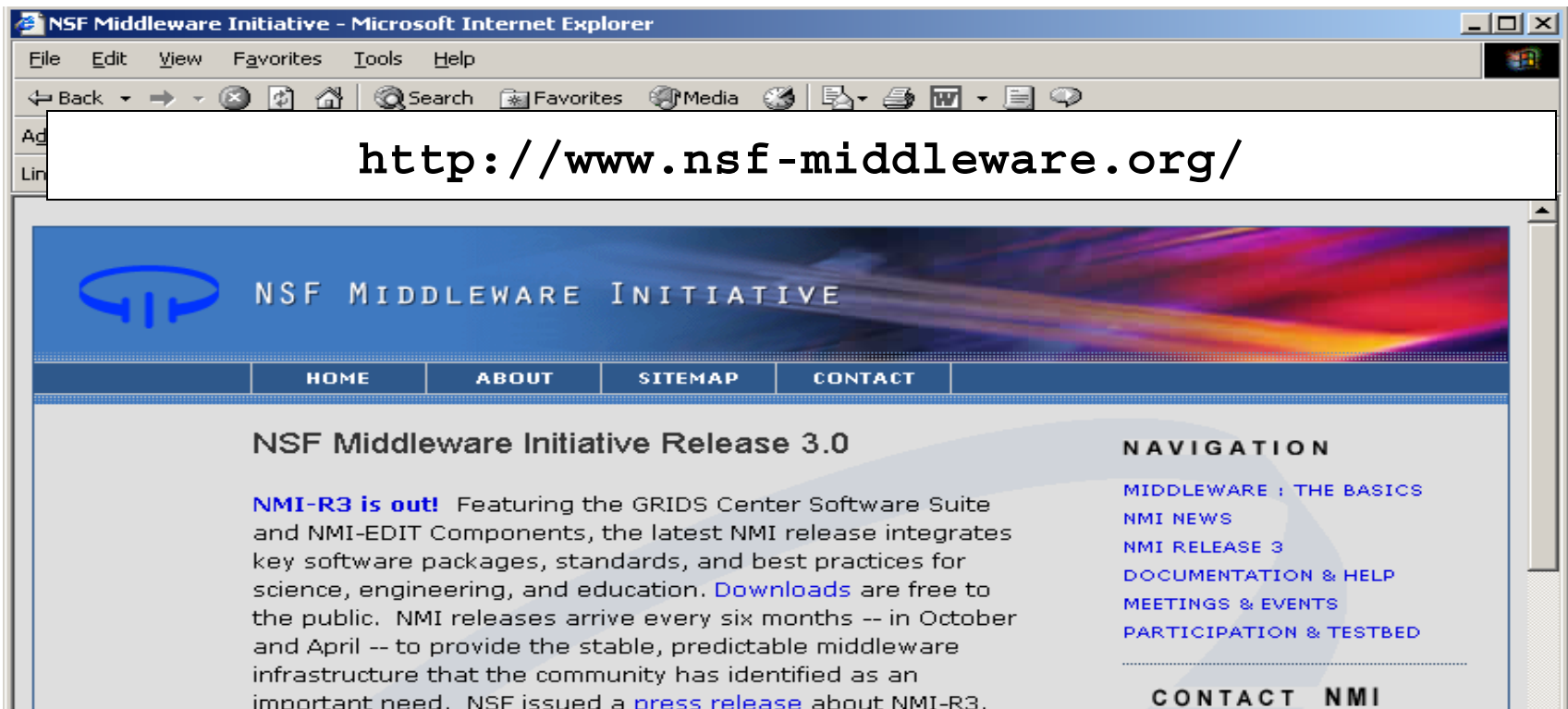
1. Universities are developing central, authoritative directories
 - Use these existing identity management solutions
 - avoid replicating into (proprietary) silos
2. Standardize a storage format for protocol-specific data
 - one central store for multiple protocols
 - ease updates/migrations
3. Leverage identity management for reliable multimedia authentication and authorization

Other drivers

- COTS – (Commercial, Off-The-Shelf)
The solution should be palatable to vendors so they would implement it.
 - Therefore, adoption as a standard was necessary
- H.323/SIP have existing security protocols
 - use those, without requiring modifications
- Solution should be useful for non-standards based conferencing (MPEG2 / Access Grid / VRVS)
- Interested in evaluating applicability of “federated administration model” for managing videoconferencing/voip

What is “NMI”?

- **National Science Foundation
Middleware Initiative**





Grid Research Integration Deployment and Support Center

Define, **Develop**,
Deploy, and
Support an
Integrated
national middleware
infrastructure
supporting
21st Century
science and
engineering
Applications

nmi-edit

Enterprise and Desktop Integration Technologies



Result:



H.350 : New ITU-T Standard

- H.350 was born out of Internet2 Video Middleware working group (Internet2 Middleware and ViDe joint initiative)
- H.350 was introduced in NMI Release 2 as commObject, an NMI-EDIT component
- “Research/Higher-education initiated design ratified as international standard August 2003
- Sent by ITU for informational review to IETF in October 2003

What Is H.350 ?

- **H.350 is**
 - An LDAP schema
 - Standardized way to store information
 - Simple – includes basic elements
 - Extensible – can include proprietary ‘fancy’ elements
 - Multi - protocol
- **H.350 is NOT**
 - A protocol
 - Just for H series protocols

H.350 Directory Organization

Enterprise Directory

inetOrgPerson

name (dn)

address

telephone

email

organization

organizational unit

commURI

RFC 1274

userPassword

commObject

commUniqueId

commOwner

commPrivate

h323Identity

h323IdentityGKDomain

h323Identityh323-ID

h323IdentitydialedDigits

h323Identityemail-ID

.....

h323IdentityEndPointTyper

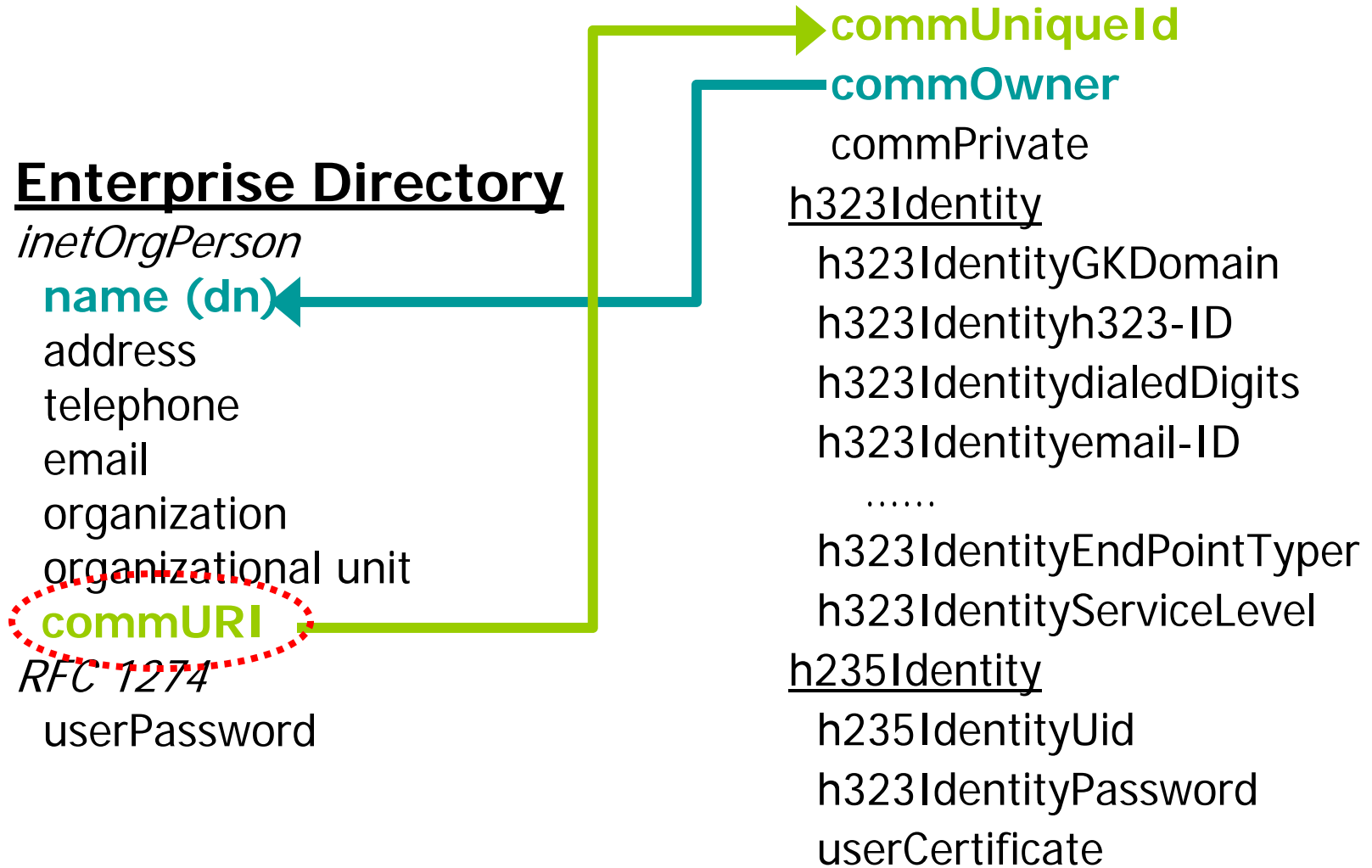
h323IdentityServiceLevel

h235Identity

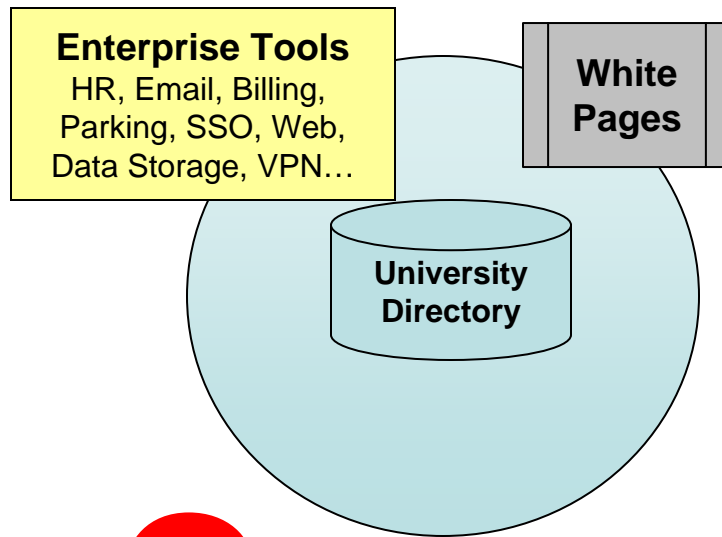
h235IdentityUid

h323IdentityPassword

userCertificate

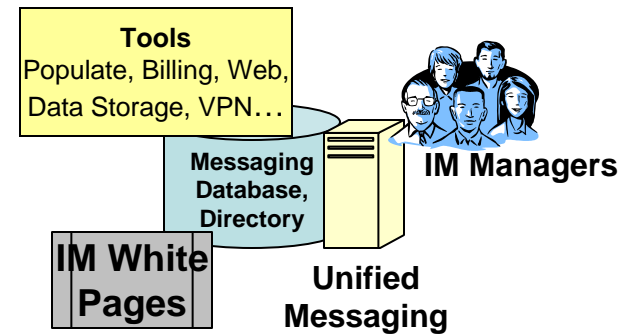
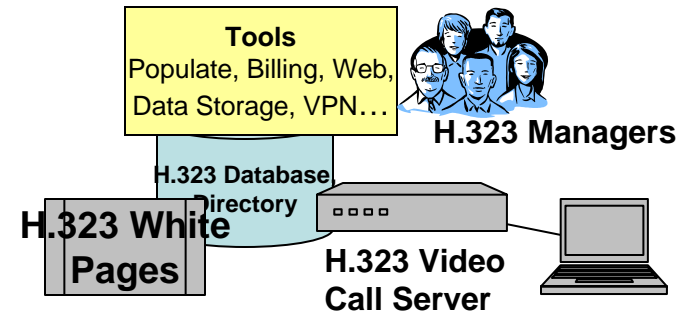
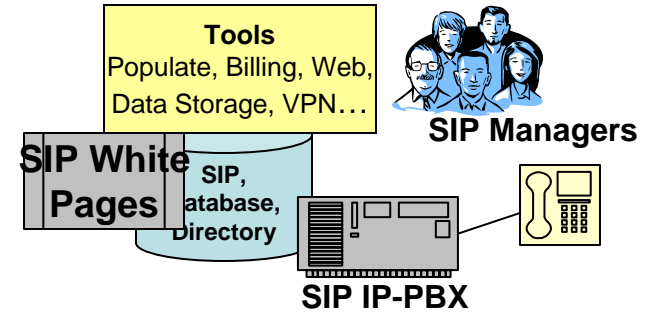


Technology Silos = Redundant Processes

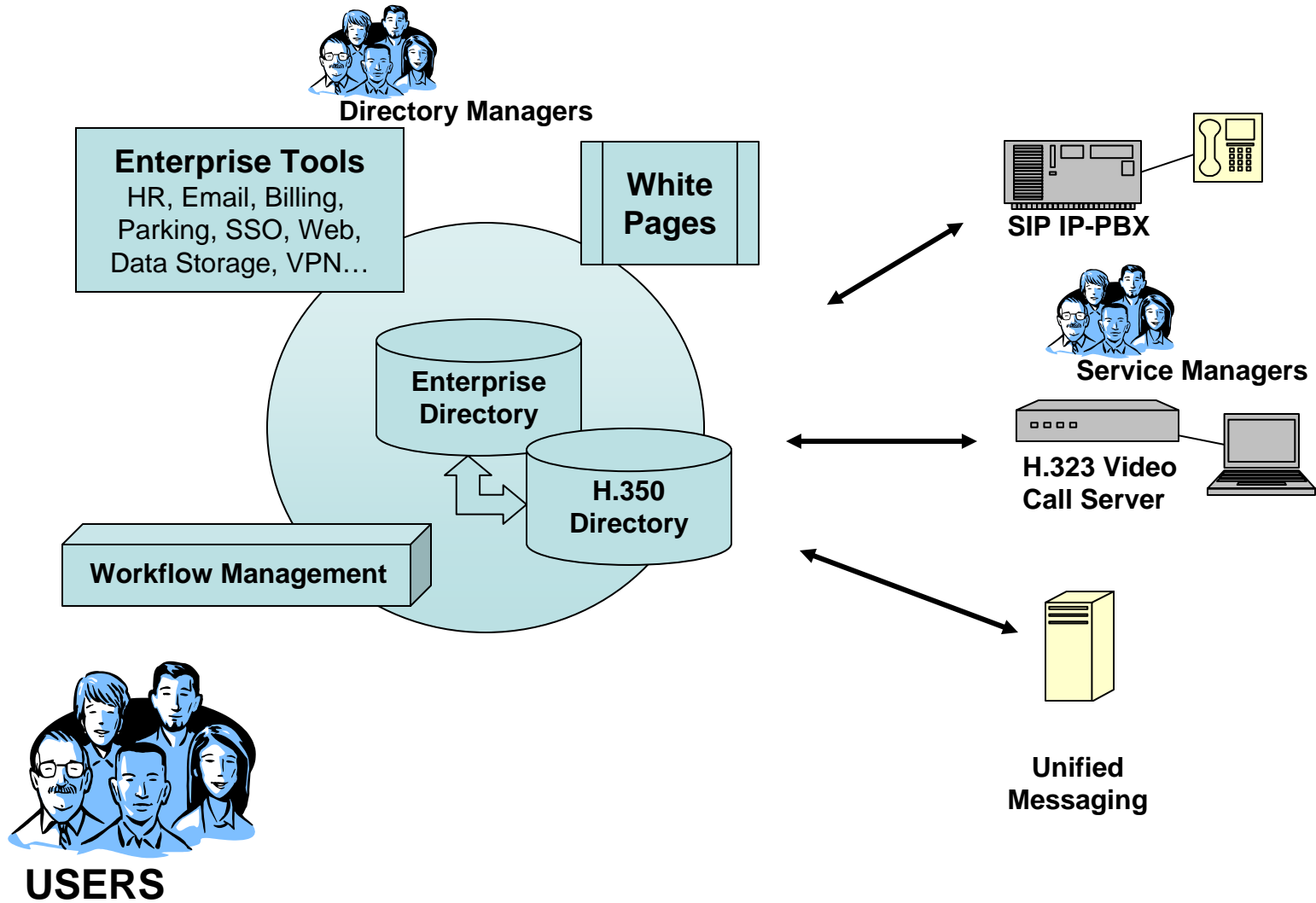


“My listing is wrong!”

“How do I call X?”



Directory-Enabled Video / VoIP



H.350 Provides These New Service Features

- White Pages
- Directory of Directories
- User Support / Contact Management
- Endpoint configuration
- Embedded address books
- Clickable Dialing
- Secure conferencing
- Standard and proprietary conferencing
- Authorization and Billing

UAB Electronic Phonebook

Copyright © 1997-2004 University of Alabama at Birmingham



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](#)

**Scalability:
 solves big user
 support issue**



[H323] My Desktop

Attribute	Value
commOwner	jgemmill
h323IdentitydialedDigits	00115490000
h323IdentityEndpointType	Terminal

Representing an Access Grid User



genericIdentity ProtocolIdentifier:	Access Grid
generic Identity Message:	See ' http://www.accessgrid.org/documentation/ for locations and connection instructions.

Other Queries Are Possible

ViDeNet

My ViDeNet Help Zone Administrators Only

ViDeNet Search Engine

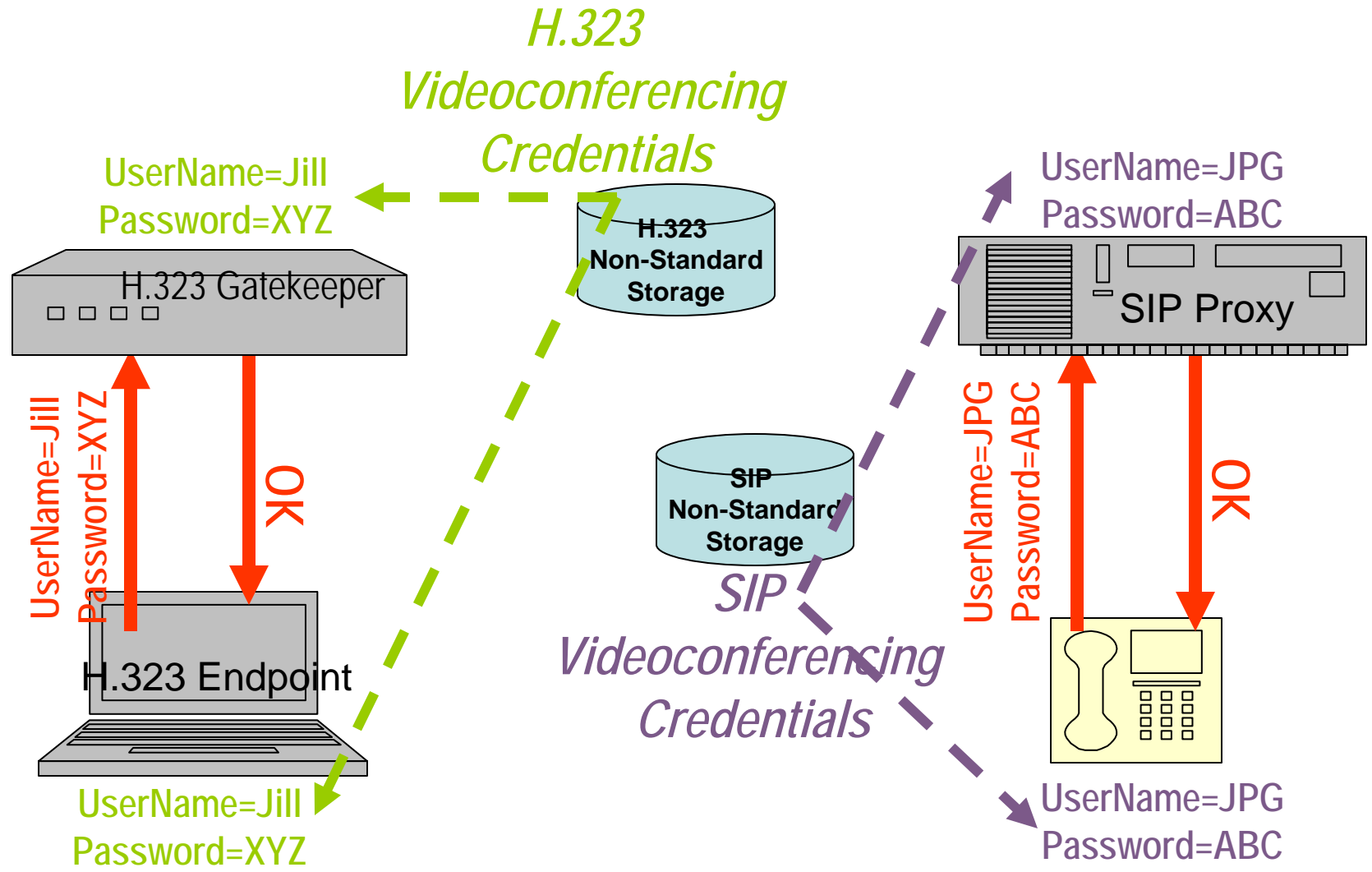
Word or Phrase for Search: UAB

Select Field to Search: Institution

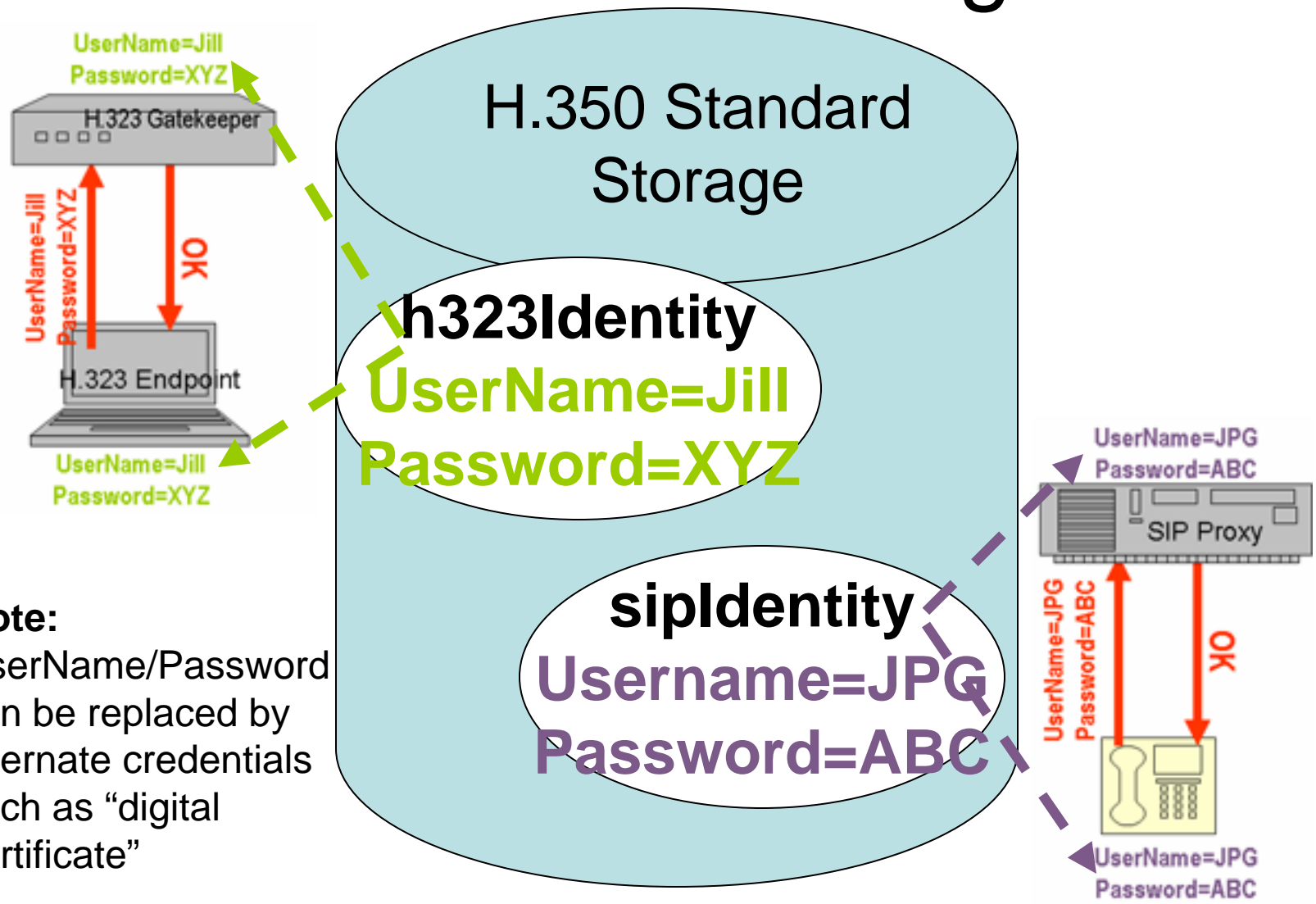
From the Following Location: All Countries

Search!

Non-Standard Credential Storage Means Multiple Logins/Password



H.350 (Standard) Credential Storage

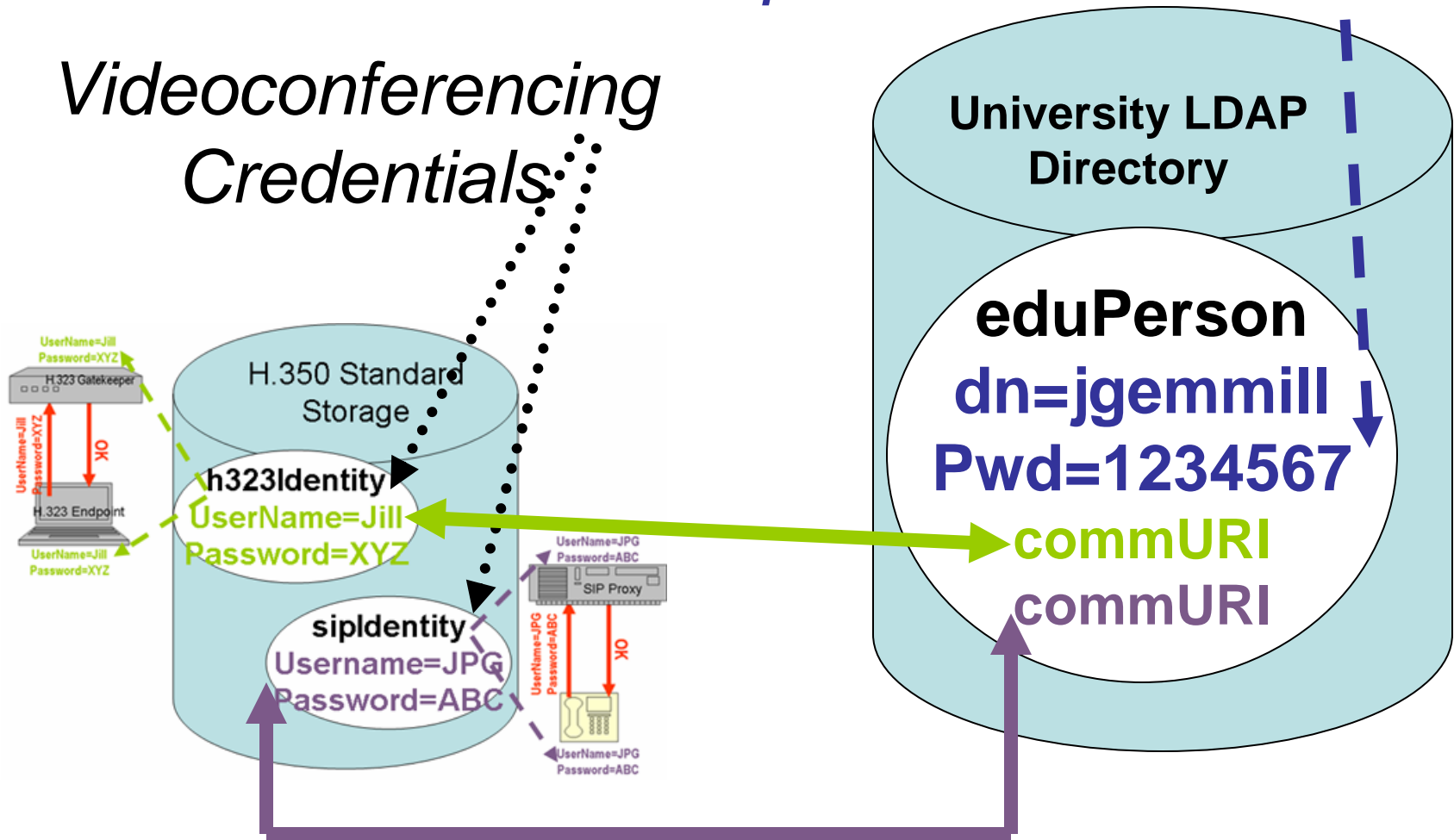


Note:
UserName/Password
can be replaced by
alternate credentials
such as “digital
certificate”

Enterprise Authentication with H.350

Enterprise Credentials

Videoconferencing Credentials



Prototypes We've Developed

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

Commercial Implementations

- RADVISION ECS Gatekeeper
- HCL SIP Proxy Server
- Tandberg Management Server
- < others currently under development >

- Who will drive H.350? YOU!! Ask for it in your RFP's.

Video Middleware Cookbook

Version 0.5 included in NMI Release 4

<http://lab.ac.uab.edu/vnet/cookbook/>

- 66 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
- Version 1.0 (March 2004) will include code snippets for developers and global indexing instructions.

ViDeNet Project Web Site

<http://lab.ac.uab.edu/vnet/>

The screenshot shows a Microsoft Internet Explorer browser window displaying the ViDe.Net website. The browser's address bar shows the URL <http://lab.ac.uab.edu/vnet/>. The website header features the "ViDe.Net" logo with the tagline "VIDEO DEVELOPMENT INITIATIVE" and the word "Middleware" to its right. Below the header is a navigation menu with links: home, about, deliverables, publications, presentations, publicity, meetings, minutes, schedule, and links.

The main content area is divided into two columns. The left column, titled "quick links", contains several items:

- Vnet Cookbook for Videoconferencing Middleware:**
 - [html](#)
 - [pdf](#)
- Vnet H.350 Brochures:**
 - [university](#)
 - [vendor](#)
- Vnet H.350 LDIF Files**
- Vnet CGU.sip Client v1.1**
- Vnet Search** the ViDeNet proof of concept H.350 directory

The right column displays a list of news items, each with a date header:

- 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 [CGU.sip Client v1.1](#) is now available.

The browser's status bar at the bottom shows "Done" and "Internet".

H.350 Development Process

- First recognized within ViDeNet as a vague general 'issue'
- SURFNet and UNC tossed schema ideas around
- Internet2 VidMid VC took on the work item
 - Focused the effort
 - Brought video and directory experts together
- Completed draft submitted to ITU-T
- ITU-T accepted it as work item H.350
- Study Group 16 worked for about a year
- Ratified
- Vendor adoption begins
- Enterprise adoption begins

International Telecommunication Union

- The ITU is an inter-governmental organization under the umbrella of the United Nations (www.itu.int)
 - currently has over 450 members from industry
 - has more than 2800 Recommendations in force
- Study Group 16
 - multimedia service definition and multimedia systems, including the associated terminals, modems, protocols and signal processing.
 - Multimedia Services, Systems and Terminals
 - e-business and e-commerce
 - Selected Recommendations
 - H.320
 - H.323
 - H.264
 - H.350
- US Representation through US State Department

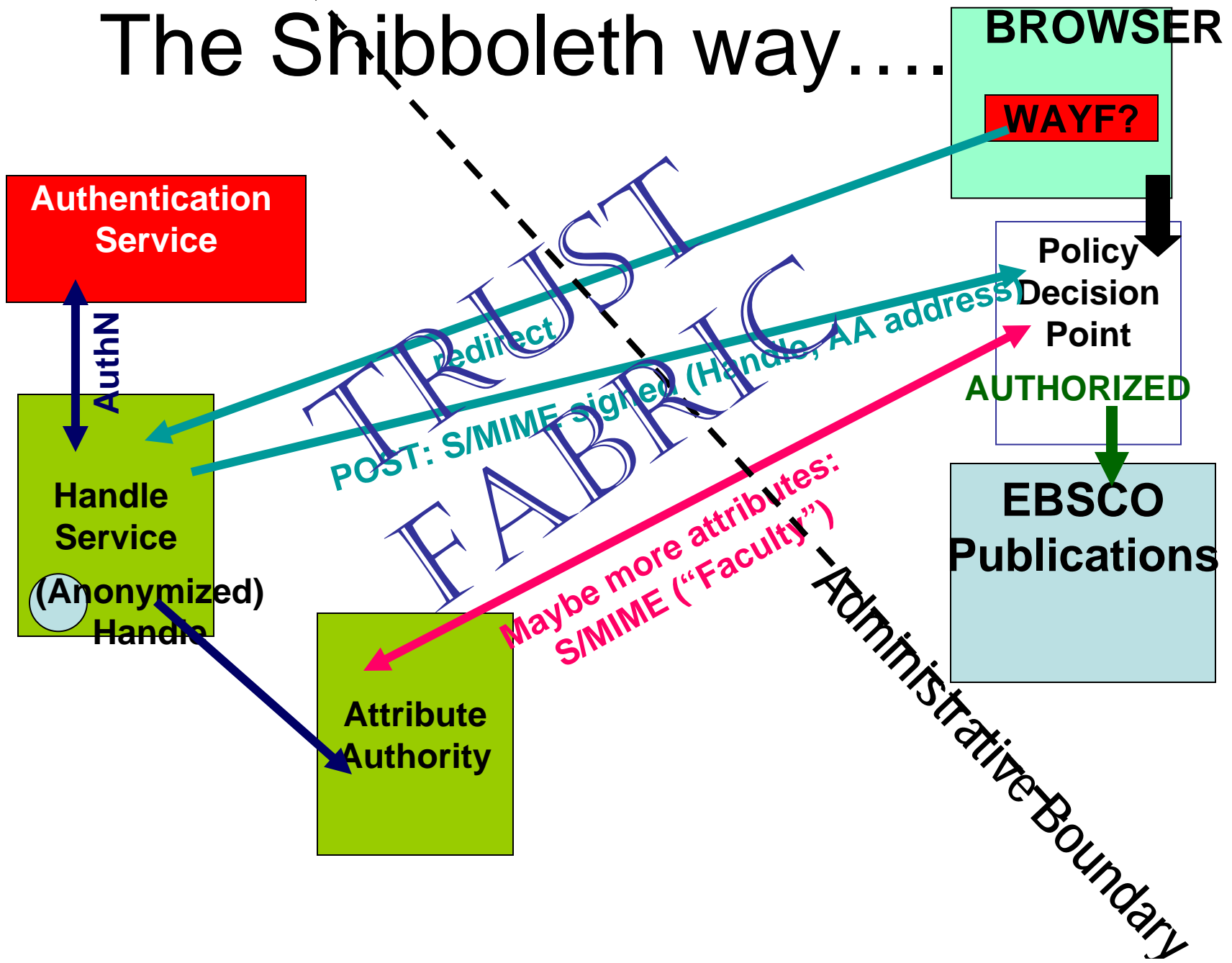
Why Standardization Process Was Helpful

- Caused the academic community to be extremely thorough
 - In terms of accuracy, scope and scenario development
 - Forced examination of real world implementation hurdles
 - Important linking between researchers and technologists
 - Implementation not valued in the computer science community
 - Leads to less rigour
 - Higher education thus abandons its voice
 - Private industry not shy to speak up, but may not deliver desired results
- Diverse expert input
- Thorough review by many eyes
- Difficulty getting enterprise acceptance without standardization (i.e. we'll munge our own)
- Difficulty getting vendor acceptance because each implementation different
- Educational community not a large enough market segment to drive development
- Paves the way for other vendor partnerships
 - An interesting alternative to open source

Federated Administration

- *OLD: Everyone belongs under a single root authority*
- Multiple, independent authorities
- *OLD: Cross-domain requires same authentication system (Kerberos OR Microsoft Active Directory OR Passport OR Novell Directory Services OR Grid Security Infrastructure OR PKI...)*
- Authenticate however you like at home

The Shibboleth way....



Federated Administration for Video/VoIP

- Policy Decision Points
 - Endpoints, Call Servers, Gateways
- Video/VoIP not web application – Shibboleth API's needed
- Can Assertions (Credentials) be of the same type as those already used in the protocols? (X.509 cert and S/MIME message)

How Federated Administration Overlaps with Security

- Basis of any complex authorization decision is
 - Who is this person?
 - Is the information source to be trusted?
 - Is there enough information to make a decision?
 - Appropriate policy
 - Enough attributes
 - Enough trust

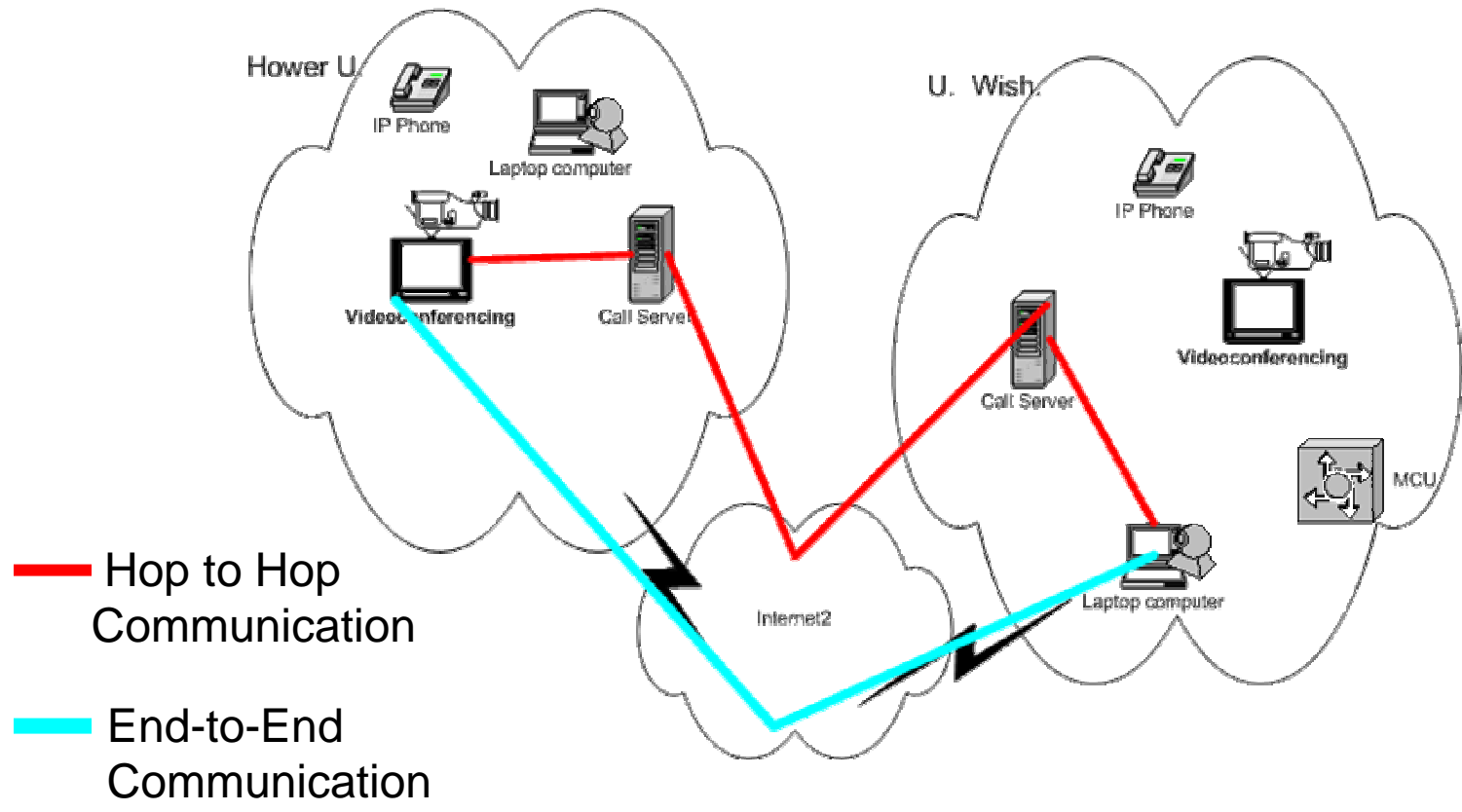
What is meant by “videoconference security”?

- At a “gut level”, we might think of:
 - No eavesdropping
 - No denial of service or break-ins
 - No “spamming” (video/voice from unwanted visitors)
 - Making sure resources like PBX gateways and MCU’s are used only by those authorized

Standard Security Mechanisms ITU X.800 IETF and RFC 2828

- Encryption
- Digital Signature
- Access Control
- Data Integrity
- Authentication Exchange
- Traffic Padding
- Routing Control
- Notarization
- Trusted Functionality
- Security Label
- Event Detection
- Security Audit Trail
- Security Recovery

Videoconferencing uses both hop-to-hop and end-to-end style communication



Model for both H.323 and SIP architectures

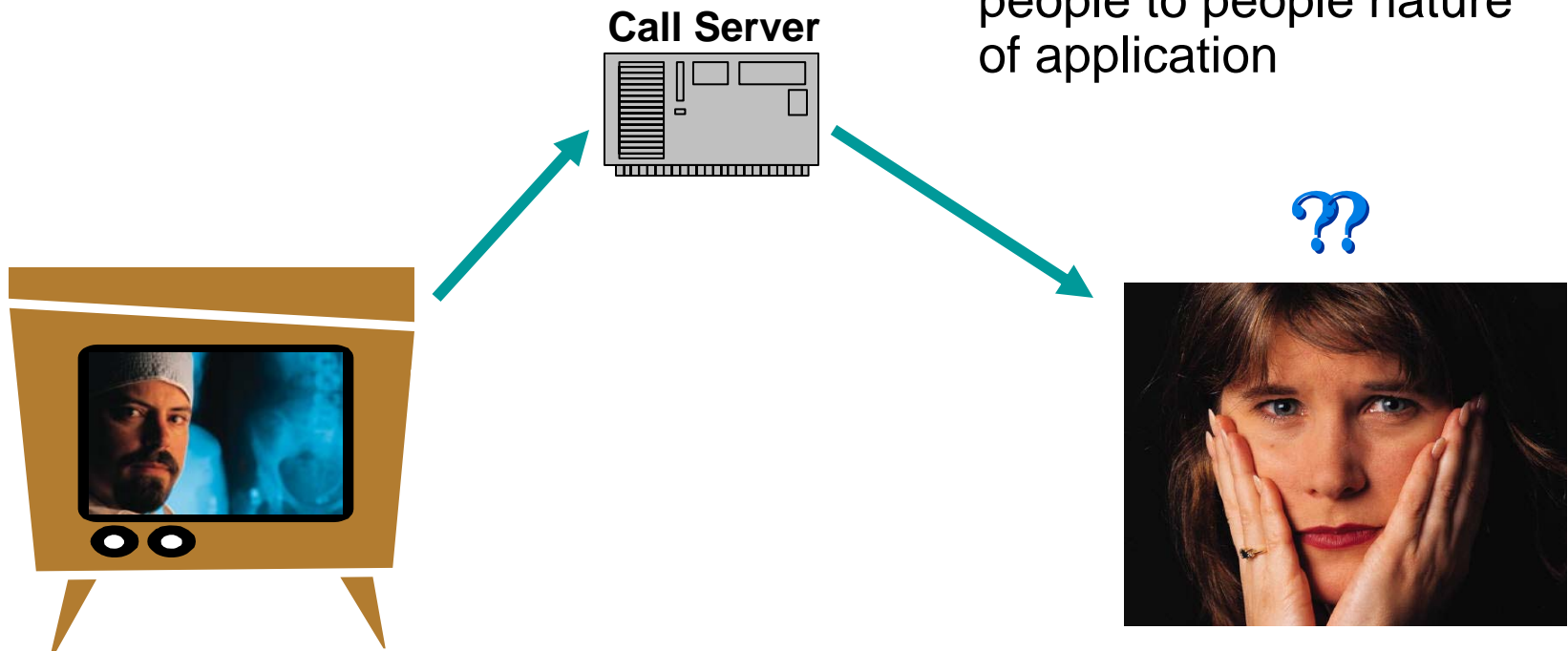
E2M Security

- Pros

- Ensures nobody steals service provider's resources
- Ensures you pay your bill

- Cons

- Doesn't allow you to access resources in other realms
- Doesn't provide caller ID
- Doesn't recognize true people to people nature of application



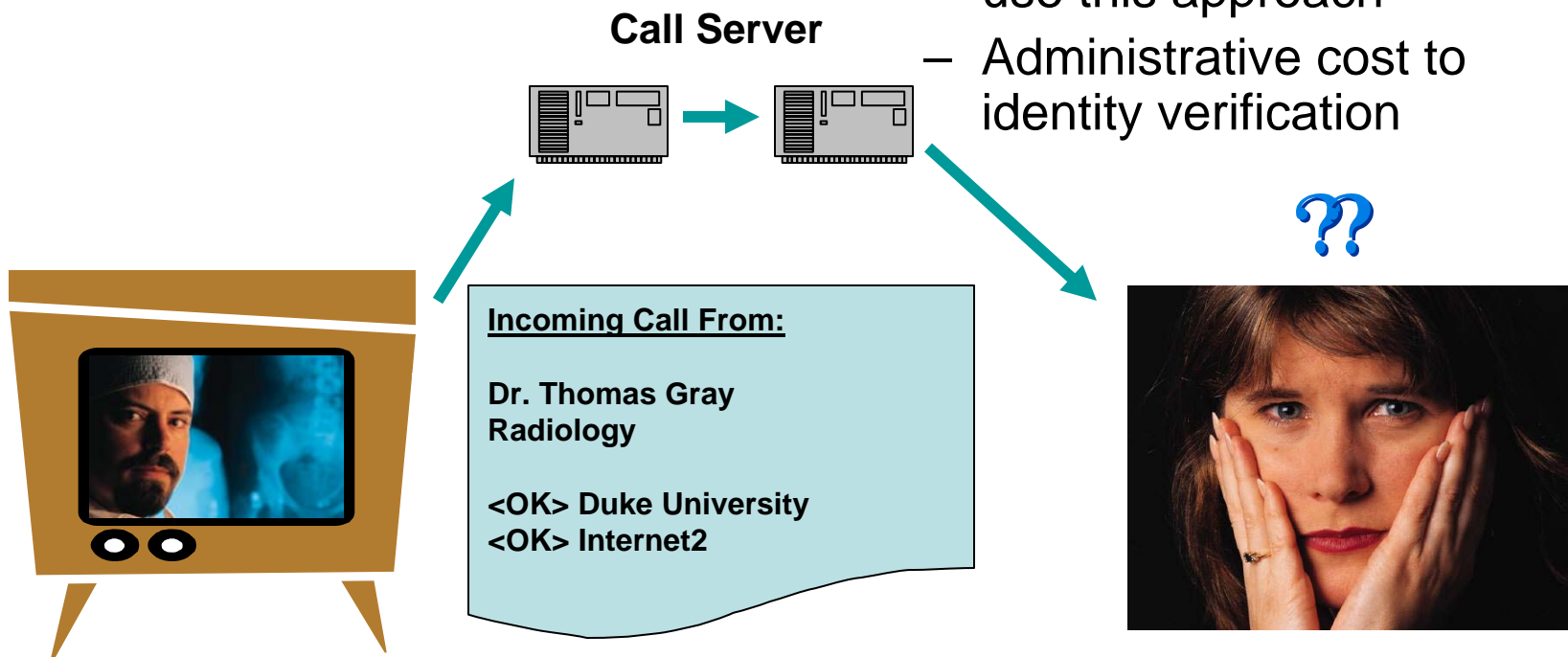
E2E Security

- Pros

- Confirms your identity to the called party
- Works across realms

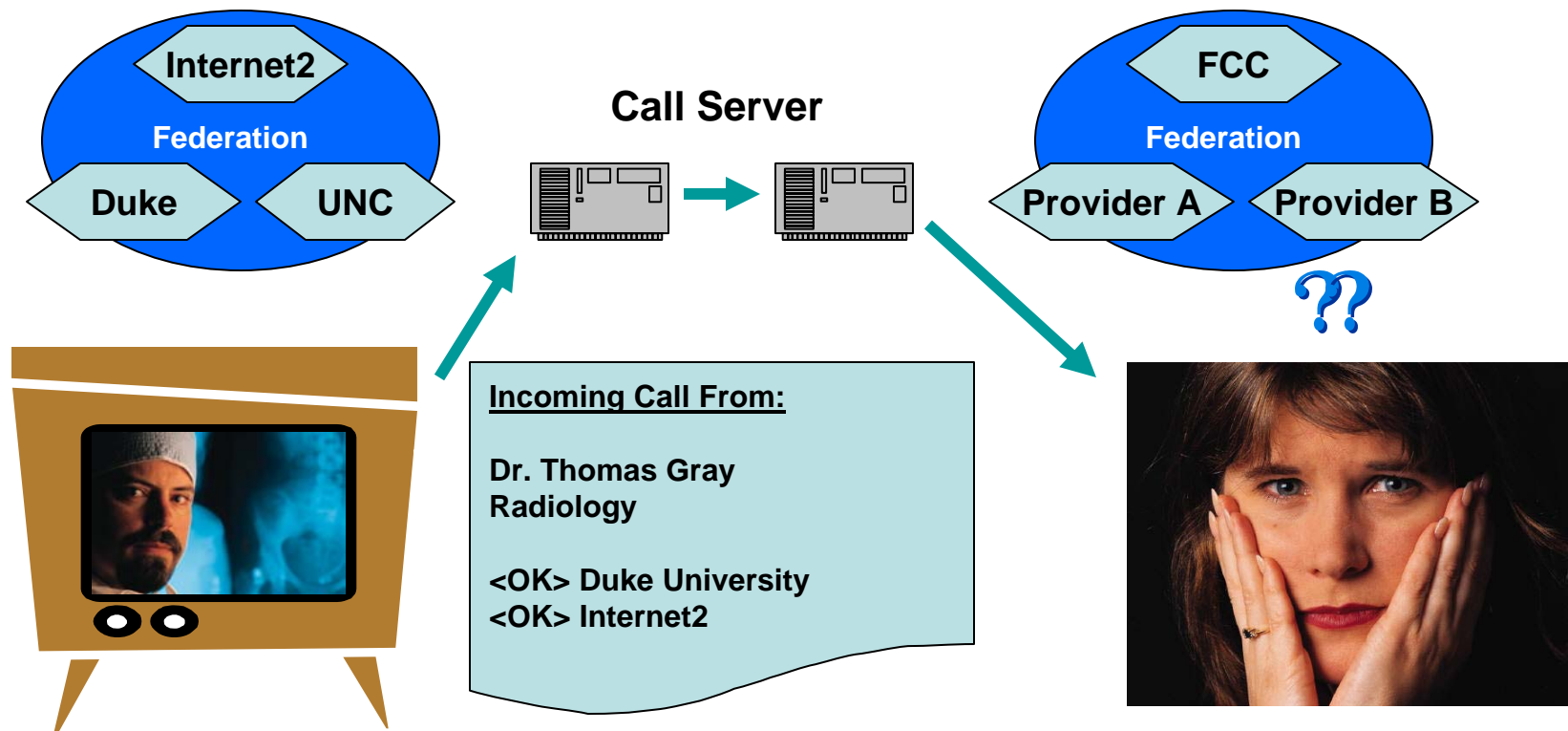
- Cons

- Requires common authentication across realms
- Other applications don't use this approach
- Administrative cost to identity verification

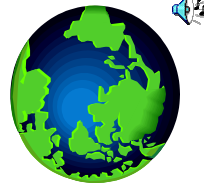


How Does Federation Help

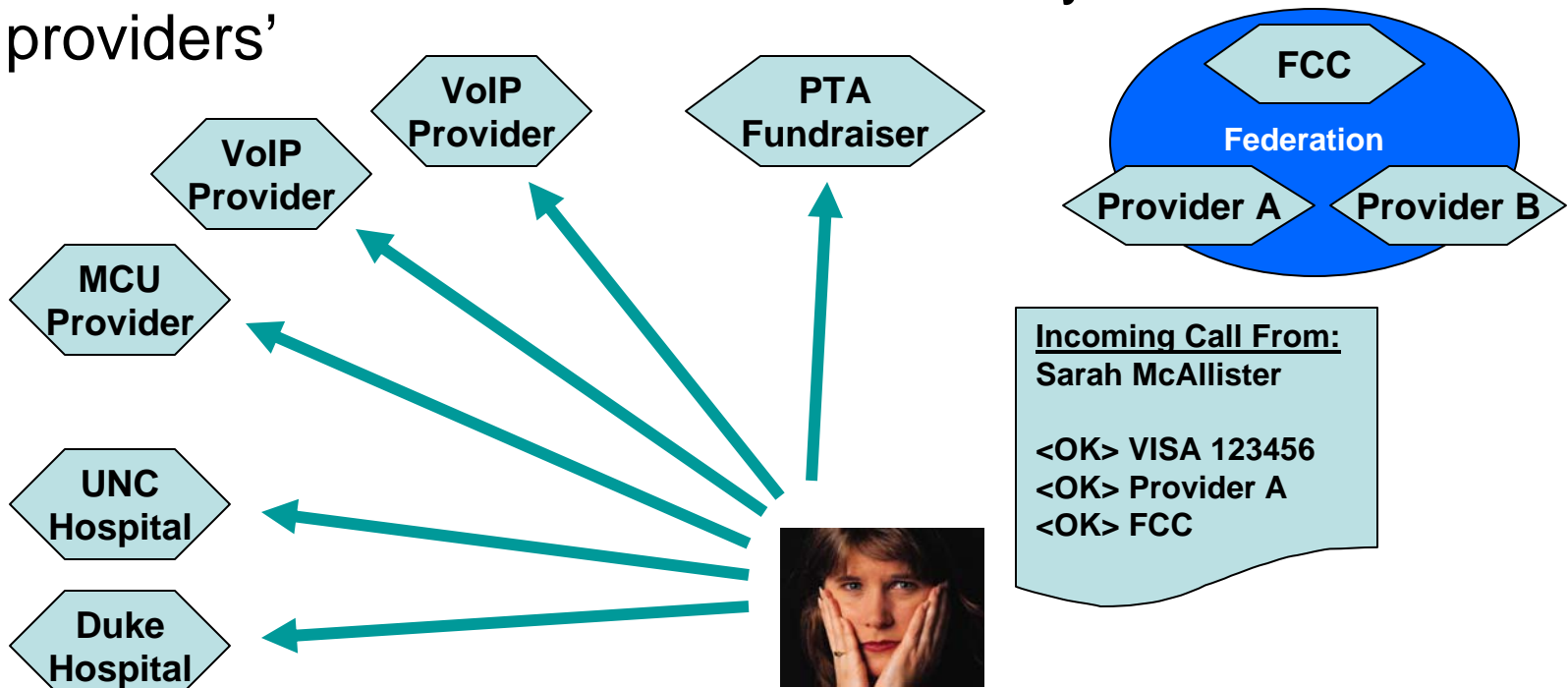
- E2E security features
- Still implement your own authentication methods
- Recognizes the world is a messy place



This Changes Everything



- Access to many service providers
- Not necessarily required to pre-establish accounts
- Call signaling and networks can be un-secured
- ITU-T NGN 'unfettered access to many service providers'



More shameless advertising...
www.vide.net/conferences/h350/



What?	Who?	Why?	Where?	Register
Program	Travel & Hotel	Sponsors	Contact	Resources

One Day Workshop on H.350

Directory services for multimedia networks

Opening Reception and Buffet Dinner
 Wednesday, March 24, 2004
 6:00 to 9:00 PM

Workshop Speaker Sessions
 Thursday, March 25, 2004
 8:00 AM - 5:00 PM

University Place Conference Center and Hotel, IUPUI
 Indianapolis, Indiana

The Video Development Initiative (ViDe) is offering a one-day workshop on the new H.350 "Directory Services Architecture for Multimedia Conferencing" standard ratified in August 2003 by the International Telecommunications Union (ITU).



This workshop is a post-conference special event following the [6th Annual SURA/ViDe Digital Video Workshop](#).

More about ViDe

- I2 Commons
- Megaconference
- ViDeNet
- Video Metadata (Moving Image Collection Project)
- Digital Rights Management (DRM) for video assets
- MPEG-4 activities
- Contribute to cookbooks

Q & A

Copyright Jill Gemmill and Tyler Johnson 2004

This work is the intellectual property of the authors. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.