IDtrust 2011
10th Symposium on Identity and Trust on the Internet
Program with Presentations

Notes

Transportation
There will be a shuttle bus leaving the Gaithersburg Holiday Inn at 8:00 a.m. Wednesday and Thursday morning to travel to NIST. The shuttle will return to the hotel at the end of the poster reception on Wednesday (7:30 PM) but there will not be a return shuttle bus on Thursday. NIST has regular shuttle service to the Shady Grove Metro station.

Wireless
802.11b Wireless access points will be available.

Blogging
Participants and observers are encouraged to use the tag "idtrust2011" when blogging and tweeting about the symposium.

Program

Wednesday, April 6, 2011 - Full Day

8:00 Bus Departs from Gaithersburg Holiday Inn for NIST
8:30 - 9:00 Registration and Continental Breakfast
9:00 - 9:15 Welcome
How the World has Changed - IDtrust 10th Anniversary Retrospective: Ken Klingenstein, *Internet2* (Slides: ppt)

9:15 - 9:45 Invited Talk
Whither Identity Management?: Tim Brown, *CA Technologies* (Slides: pdf)

Identity management has gone through a number of transitions and continues to evolve. This session will discuss: Where has identity management been? What have we learned? What are the challenges we face? Where is it going?

9:45 - 10:45 Panel - Usability Issues in Identity Management: Improving the engagement ceremony between users and services

Panel Moderator: Trent Adams, *Internet Society* (Slides: ppt)

Larry Drebes, *JanRain* (Slides: pdf)
Paul Trevithick, *Azigo* (Slides: pdf)
Ken Klingenstein, *Internet2* (Slides: ppt)
Don Thibeau, *Open ID Foundation*

Asking users to know the protocol running a system's identity management solution is like asking them to list the constituent elements that make up the air we breathe. In most cases, users just want to get into a system quickly and easily (often to the detriment of security). This panel brings together cross-protocol practitioners (e.g. OpenID, SAML, OAuth) working on usable solutions that attempt to balance issues such as utility, efficiency, and security. Among the topics to be discussed are technical and usability issues surrounding identity provider discovery.

10:45 - 11:15 Break

11:15 - 12:45 Panel - Privacy: An Emerging Landscape

Panel Moderator: Carl Ellison, *Independent* (Slides: pptx)

Trent Adams, *ISOC* (Slides: pdf)
Al Zarate, *National Center for Health Statistics* (Slides: ppt)
Ken Klingenstein, *Internet2* (Slides: ppt)
Brian LaMacchia, *Microsoft* (Slides: pptx)

Privacy, like security, is emerging as a broad and diverse landscape, and advances are happening in several areas. After an opening talk that describes this landscape, talks will drill down into the most important developments in technical and policy activities. We will look at the failure of anonymization technologies for large data sets and its consequence on research. Consent for the release of personal attributes is becoming real in federated and social identity and we will look at perspectives in both the US and Europe. We will also look at new technologies that provide selective personal information release and how they fit into the landscape.

12:45 - 1:45 Lunch
1:45 - 2:15 Keynote Talk

National Strategy for Trusted Identities in Cyberspace: Jeremy Grant, *NIST* (Slides: pptx)

The National Strategy for Trusted Identities in Cyberspace (NSTIC) is a White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of sensitive online transactions.

The Strategy calls for the development of interoperable technology standards and policies - an "Identity Ecosystem" - where individuals, organizations, and underlying infrastructure - such as routers and servers - can be authoritatively authenticated. The goals of the Strategy are to protect individuals, businesses, and public agencies from the high costs of cyber crimes like identity theft and fraud, while simultaneously helping to ensure that the Internet continues to support innovation and a thriving marketplace of products and ideas.

The Strategy was developed with substantial input from the private sector and the public. It calls for the effort to be led by the private sector, in partnership with the federal government, consumer advocacy organizations, privacy experts, state and local agencies, and others.

NIST has been asked by the White House to lead the implementation of NSTIC. NIST's Jeremy Grant will give an overview of the soon-to-be-released Strategy and detail the role NIST will play in collaborating with the private sector to move NSTIC forward.

2:15 - 3:30 Panel - Privacy and Security Research Challenges for Biometric Authentication

Panel Moderator: Elaine Newton, *NIST* (Slides: ppt)

Ross Micheals, *CSC* (Slides: pdf)
Stephanie Schuckers, *Clarkson University* (Slides: ppt)
Terrance Boult, *University of Colorado* (Slides: ppt)
For biometric technologies to be deployed in support of identity assurance, it is essential to distinguish between the role that biometric technologies can play in Identity Proofing (establishment of identity) versus Identity Authentication (affirmation of the holder of a credential or identifier by which the user is known

to the system), as each of these functions typically have differing policies (i.e. in-person versus remote); technology availability (i.e. full desktop system versus embedded scanner); and security and privacy considerations. Biometric systems are typically used as part of an overall security system. Stolen biometric information are a security risk, may be non-revocable, and contain privately identifiable information. Development of countermeasures is needed to minimize vulnerabilities of these systems.

Specific R&D challenges that will be noted in this discussion include: biometric template protection algorithms, revocable/cancelable biometrics, anti-spoofing/liveness detection testing, and best practices for e-authentication and the treatment of biometrics in an identity assurance framework.

3:30 - 4:00 Break
4:00 - 5:15 Panel - Successful Implementation of Identity Management Systems Integration

Panel Moderator: Steve Whitlock, *Boeing*

Vijay Takanti, *Exostar* (Slides: pptx)
Mollie Shields-Uehling, *SAFE-Biopharma* (Slides: ppt)
Debbie Bucci, *National Institutes of Health* (Slides: pptx)
Over sixty years have passed since the discovery of public key concepts and thirty years since the development public key algorithms. In the last twenty years governments, corporations, universities and individuals have spent fortunes in resources and lifetimes in the process of conversion from concepts and ideals to technologies, products and services that enable e-services.

This panel will focus on success stories and examples of working implementations from several different communities.

5:15 - 7:30 Poster Session / Reception at NIST

IDtrust did not have a peer review process this year, but we did want to have a more informal process to let people offer some ideas to share. So we invited poster submissions, and the following will be at the reception.

Efficient Transmission of DoD PKI Certificates in Tactical Networks

Sean R. O'Melia, *MIT Lincoln Laboratory*
Roger I. Khazan, *MIT Lincoln Laboratory*
Dan Utin, *MIT Lincoln Laboratory*

Draft FIPS 201-2 Discussion Point

Bill MacGregor, *NIST*
Hildy Ferraiolo, *NIST*
Ketan Mehta, *NIST*
Sal Francomacaro, *NIST*
Ramaswamy Chandramouli, *NIST*
Towards a method for managing distributed access entitlement and access certification (Can we trust that AuthZ attribute?)

Corinne Irwin, *NASA*
Dennis Taylor, *NASA/ASRC Primus Solutions*
Trust in National Identity Systems: Exploring Citizen Risk Perception

Adrian Rahaman, *University College London*
Angela Sasse, *University College London*
PKAuth: A Social Login Protocol for Unregistered Apps

Francisco Corella, *Pomcor*
Karen Lewison, *Pomcor*
System Diagram of Federated Identity, Authentication and Authorization using X.509 Certificates and SAML

Robert Cope, *Homeland Security Consultants*

7:30 Bus Departs for Gaithersburg Holiday Inn

Thursday, April 7, 2011 - Half Day

8:00 Bus Departs from Gaithersburg Holiday Inn for NIST
8:30 - 9:00 Registration and Continental Breakfast
9:00 - 9:30 Invited Talk
Unified Identity for Access Control: Carl Ellison, *Independent* (Slides: ppt)

There is much debate over the nature of identity and how it relates to authenticators, identifiers, attributes, named groups, etc. Taken in isolation, these debates rely on near-philosophical concepts of identity. Rather than be another voice in those debates, on those terms, we look here at the functional needs of access control in large scale industrial environments. From those needs, we show a need for more than one form of identifier or attribute, but where each is established in a single statement from some authority on that particular statement. We also show that chains of such statements will be

required in normal access control decisions. We then give a single representation of such statements that captures all of the different kinds of statement and an algorithm over chains of those representations that establishes the truth of a chain. The algorithm for proving validity of deductions is not confined to a single organization, so it gives implicit federation not just of identifier but of attributes.

9:30 - 11:00 Panel - 2 Factor Authentication and Higher Level-of-Assurance Issues
Panel Moderator: Ken Klingenstein, *Internet2*

Elaine Newton, *NIST* (Slides: ppt)
William MacGregor, *NIST* (Slides: ppt)
Paul Donfried, *Verizon Business Solutions* (Slides: pptx)

Invited Talk
Digital Signatures - Current Barriers: Simson Garfinkel, *Naval Postgraduate School* (Slides: pdf)

11:00 - 11:30 Break
11:30 - 12:45 Panel - Creating the Attribute Ecosystem
Panel Moderator: Peter Alterman, *NIH*

Jack Suess, *InCommon Steering & UMBC* (Slides: ppt)
Debbie Bucci, *National Institutes of Health* (Slides: pptx)
Ken Klingenstein, *Internet2* (Slides: ppt)
With the focus of identity management shifting from authentication to the attributes being shared across the ecosystem, key issues around the creation and consumption of attributes are emerging. In those domains where regulation defines roles and permissions, such as pharmaceuticals and financials, attribute schema can be modeled in both syntactic and semantic standards by the federations that operate in those sectors. In the broader public sector, key attributes for many federated uses cases, including "over legal age", citizenship, physical limitations, and at least a few others lack a mechanism for such normalization. This session will look at key issues of the ecosystem (attribute LOA, sources of authority and delegation trails, query languages, inter-state and inter-national jurisdictional issues), the development of attribute schema in some verticals such as government and R&E, and discuss processes for normalization of public and marketplace attributes.

12:45 - 1:00 Wrap Up

Program Chair: Carl Ellison, *Independent* (Slides: pptx)

See Also

This workshop is part of the IDtrust Symposium Series

- •2011: 10th Symposium on Identity and Trust on the Internet (IDtrust 2011)
- •2010: 9th Symposium on Identity and Trust on the Internet (IDtrust 2010)
- •2009: 8th Symposium on Identity and Trust on the Internet (IDtrust 2009)
- •2008: 7th Symposium on Identity and Trust on the Internet (IDtrust 2008)
- •2007: 6th Annual PKI R&D Workshop
- •2006: 5th Annual PKI R&D Workshop
- •2005: 4th Annual PKI R&D Workshop
- •2004: 3rd Annual PKI R&D Workshop
- •2003: 2nd Annual PKI Research Workshop
- •2002: 1st Annual PKI Research Workshop

INTERNET2™

“Ten Years Ago… on a cold dark night”

Welcome

Acknowledgments and thanks

Security Acronymny: then and now

What's working

What's proving hard

Acknowledgments

NIH and NIST – Peter Alterman, Tim Polk and Bill Burr

NSF – Early Adopters and NSF Middleware Initiative

Internet2 Membership

PKI Labs, PKI Advisory Board, Neal McBurnett

Program Committee and Sean Smith

Security Acronymny circa 1998

PKI

X.500

X.509

CRL

RSA

PGP

Security Acronymny circa 2002

PKI
X.500
X.509
CRL
OCSP
LDAP
RSA
PGP
XKMS
SPKI

GXA
Liberty
Magic Carpet
SAML
Shibboleth
XML
HEBCA
FBCA

Security Acronymny circa 2002

E-authentication

9-11-01

OGSA

GSS

E-SIGN

E-LOCK

ACES

CAM

DAVE

Observations

I was really ignorant in 1998

This is proving really hard

There are a lot more approaches, if only because there are lots more needs

Partitioning the problem space may be better than the unified solution

What's working

At the core, the math of PKI remains extremely elegant

The standards, protocols and processes of PKI are open

PKI attracts really smart people

What's proving hard

Scaling: virtual organizations, federations, bridged hierarchies

Trust: collaborative versus legal

Integrating security and privacy

Mechanics: mobility, archiving, key escrow, identity

Authorization: role based versus atomic rights

Reconciling humans and lawyers

Interrealm Trust Structures

Federated administration

- basic bilateral (origins and targets in web services)
- complex bilateral (videoconferencing with external MCU's, digital rights management with external rights holders)
- multilateral

Hierarchies

- may assert stronger or more formal trust
- requires bridges and policy mappings to connect hierarchies
- appear larger scale

Virtual organizations

- Grids, digital library consortiums, Internet2 VideoCommons, etc.
- Share real resources among a sparse set of users
- Requirements for authentication and authorization, resource discovery, etc need to leverage federated and hierarchical infrastructures.

The Continuum of Trust

Collaborative trust at one end…

- can I videoconference with you?
- you can look at my calendar
- You can join this computer science workgroup and edit this computing code
- Students in course Physics 201 @ Brown can access this on-line sensor
- Members of the UWash community can access this licensed resource

Legal trust at the other end…

- Sign this document, and guarantee that what was signed was what I saw
- Encrypt this file and save it
- Identifiy yourself to this high security area

Dimensions of the Trust Continuum

Collaborative trust

handshake

consequences of breaking trust more political (ostracism, shame, etc.)

fluid (additions and deletions frequent)

shorter term

structures tend to clubs and federations

privacy issues more user-based

Legal trust

contractual

consequences of breaking trust more financial (liabilities, fines and penalties, indemnification, etc.)

more static (legal process time frames)

longer term (justify the overhead)

tends to hierarchies and bridges

privacy issues more laws and rules

The Trust Continuum, Applications and their Users

Applications and their user community must decide where their requirements fit on the trust continuum

Some apps can only be done at one end of the continuum, and that might suggest a particular technical approach.

Many applications fit somewhere in the middle and the user communities (those that trust each other) need to select a approach that works for them.

Integrating Security and Privacy

Balance between weak identity, strong identity, and attribute-based access (without identity)

Balance between privacy and accountability – keeping the identity known only within the security domain

Reconciling Humans and Lawyers

Non-repudiation has had a very high bar set…

Human nature has been "refined" over a long time

We tend to talk globally, think locally and act inconsistently…

Conference Outcomes

Refine our understandings of security

Cross-pollinate PKI research

Identify experiments that should be conducted

Why PKI?

Single infrastructure to provide all security services

Established technology standards, though little operational experience

Elegant technical underpinnings

Serves dozens of purposes - authentication, authorization, object encryption, digital signatures, communications channel encryption

Low cost in mass numbers

Why Not PKI?

High legal barriers

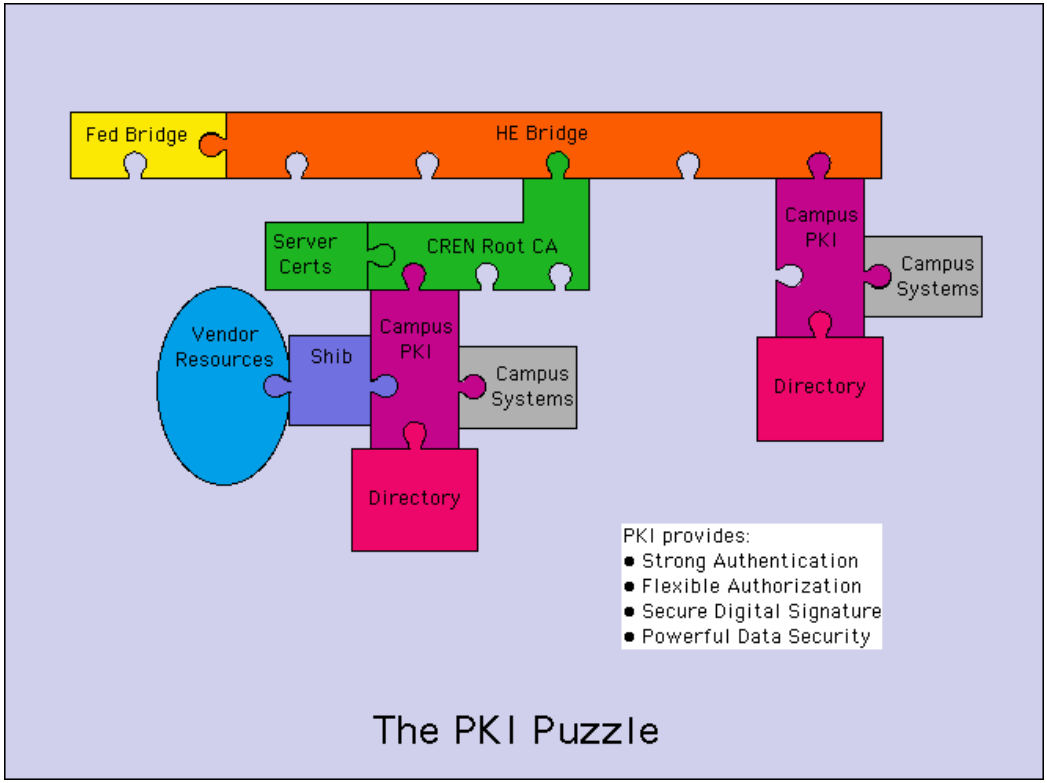
Lack of mobility support

Challenging user interfaces, especially with regard to privacy and scaling

Persistent technical incompatibilities

Overall complexity

D. Wasley's PKI Puzzle



Federal Activities

fBCA

NIH Pilot

ACES

fPKI TWG

Others – federal S/MIME work

Internet2/NIH/NIST research conference

...

The Industry

What's the problem with PKI then? It all boils down to one thing: Complexity.

Wanted: PKI Experts
By Scot Petersen

July 18, 2001

The Industry

Baltimore in peril

PKIforum slows down

OASIS-SAML work (XML to leaven PKI) gains buzz

RSA buys Securant

Ten Years Forward…

The issues here have become immensely important

The cutting edge is being blunted by the demands of deployment

It's too important for us to be doing it…

10TH SYMPOSIUM ON IDENTITY AND TRUST ON THE INTERNET (IDTRUST 2011)

Identity and Access Management

"Near the Horizon, Just Over the Horizon"

Tim Brown

SVP Distinguished Engineer

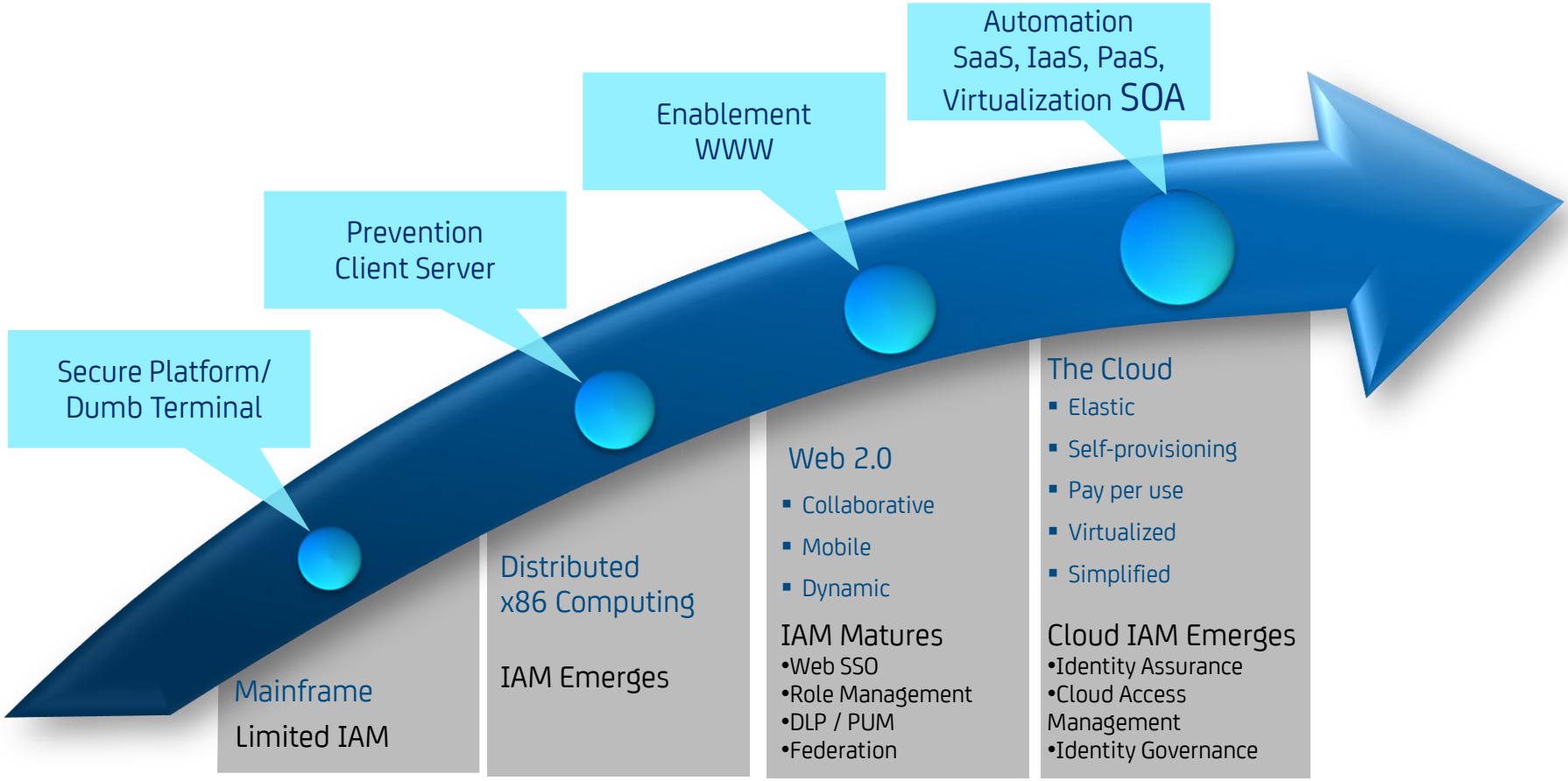
CA Technologies

timothy.brown@ca.com

ca technologies

Identity and Access Management transitions along with technology and the threat environment

Technology and the Threat Landscape is evolving



Near the Horizon

- Huge amount of information and applications available from anywhere
- Multi-Use Identities emerge beyond communities of trust
  - Facebook, Google, Yahoo
- Many communities of trust emerge utilize Cloud based Identities
  - Healthcare, State and Local Govt,
- NSTIC is a Catalyst– National Strategy for Trusted Identity in Cyberspace will be announced on April 15th
  - Cooperation between standards organizations
    - OpenID, Kantara, OIX,
  - Community Frameworks such as TSCP emerge to solve specific problems

Near the Horizon

- Acceptance of online credentials as legally binding
  - Commonwealth of Virginia – Enabling digital signing of documents
- Emergence of “Trusted Identity Providers” that assume some liability
  - Governments, Banks, Independent entities
- Move to claims based Identity Models and away from simple username and password
- Increased use of mobile device as identity and transaction enabler (Stronger Auth necessary in Cloud apps)
- Continued increase in sophisticated threat: Insiders take center stage
- Privacy and Identity becoming more linked

Just Over the Horizon

- Security moves closer to the data
  - Policy based just in time access control with no static roles or groups
  - All access is granted based on current level of risk and the objects policy
  - Digital rights management based on encryption
- "There's an App for that" creating the next generation of IAM issues
- Identity information will flow between devices and become enable the next generation of social networking
- Use of true identity and biometrics increasing. Facial recognition, DNA scans etc (Passport control, India Identity project)
- Global standards emerging (Maybe)?
- Cloud will drive vendors to have better controls and identity systems that enable collaboration

What's Next

- An Identity centric world
  - That enables the appropriate level of authentication to be used based on risk
  - That requires the minimal amount of information to be shared for a transaction
  - That grants access to information only for the time necessary
  - That is easy to use and acceptable to the masses
- Enable the right people to have the right access to the right data at the right time

Questions?

the Internet is for everyone

Usability Issues in Identity Management

Improving the engagement ceremony between users and services

Panel Moderator: J. Trent Adams (adams@isoc.org)

Internet Society

InternetSociety.org

Usability Issues in Identity Management:

Improving the engagement ceremony between users and services

Asking users to know the protocol running a system's identity management solution is like asking them to list the constituent elements that make up the air we breathe. In most cases, users just want to get into a system quickly and easily (often to the detriment of security).

Users just want in.

Usability Issues in Identity Management: *Panelists*

- J. Trent Adams, Internet Society *(Moderator)*
- Larry Drebes, JanRain
- Paul Trevithick, Azigo
- Don Thibeau, Open ID Foundation
- Ken Klingenstein, Internet2

Usability Issues in Identity Management: *Topics*

- What is the role of automated IdP discovery, and why does it matter to issues such as adoption, conversion, usability?
- What solutions currently exist for IdP discovery? How are they similar and different? How widely deployed are they today, and is there a future roadmap?
- What are the goals of the various stakeholders who are interested in IdP discovery? What are the differences between the solutions supporting end users, enterprise, and government, and can they effectively be aligned?
- How do solutions interface with legacy systems? Is there a difference in approach for wired, wireless, and mobile systems?
- How do the solutions address issues of user privacy? Is it possible to automate IdP discovery in way that minimizes information leakage?
- How does IdP discovery relate to attribute discovery, or the discovery of service meta-data? Is there work being done to explore attribute exchange as distinct from IdP?

the Internet is for everyone

Thank you.

Questions? Comments? Send them to:

J. Trent Adams (adams@isoc.org)

The Internet Society:

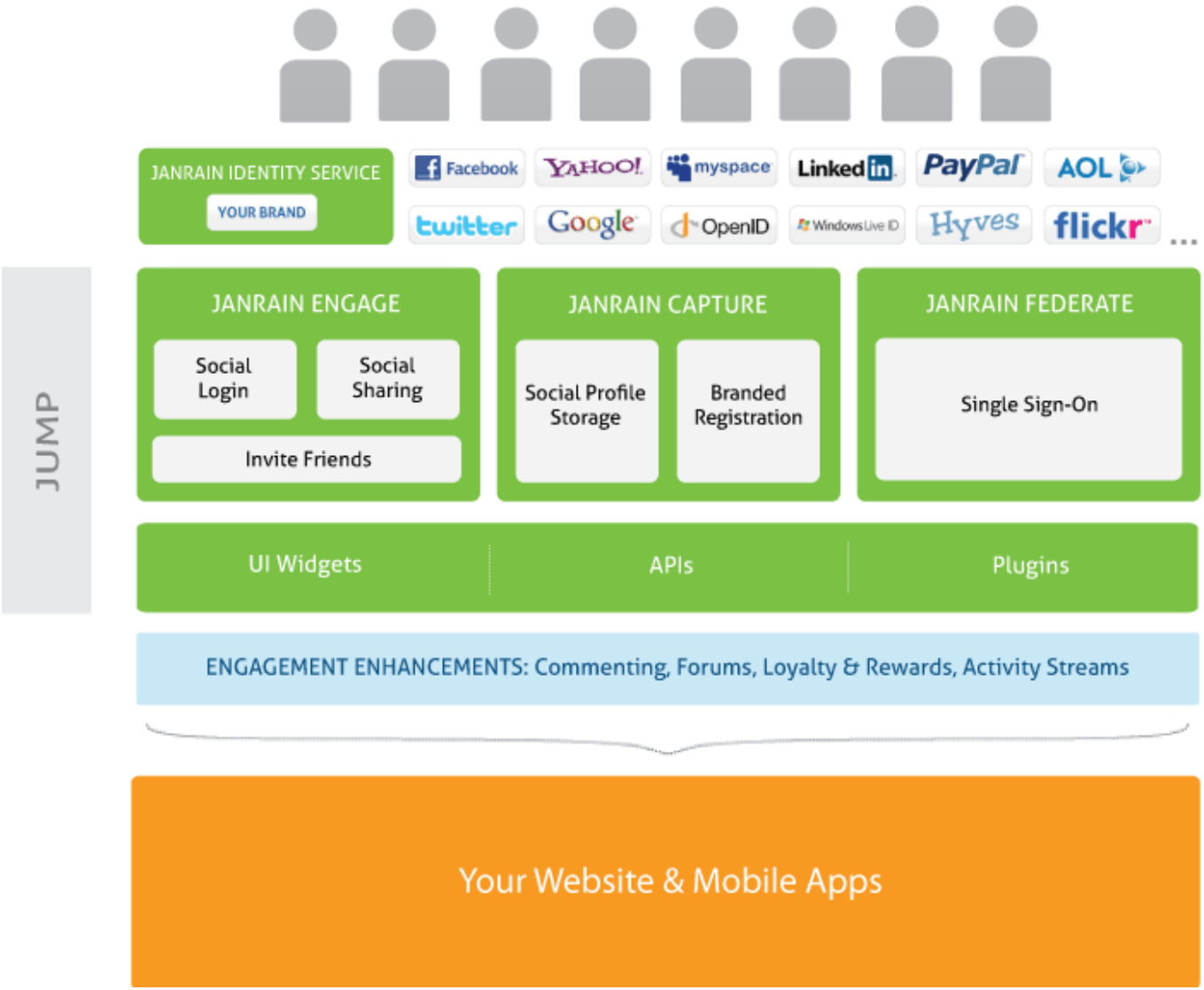
- InternetSociety.org
- info@InternetSociety.org

Internet Society

InternetSociety.org

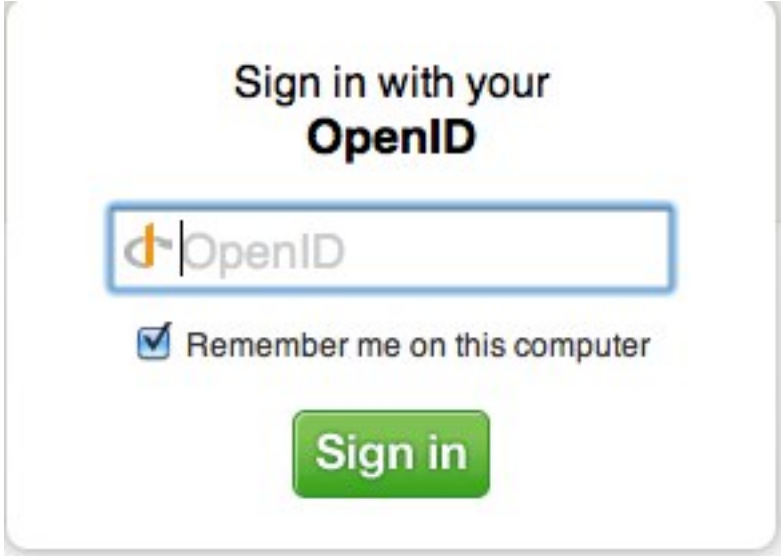
Janrain

Janrain User Management Platform

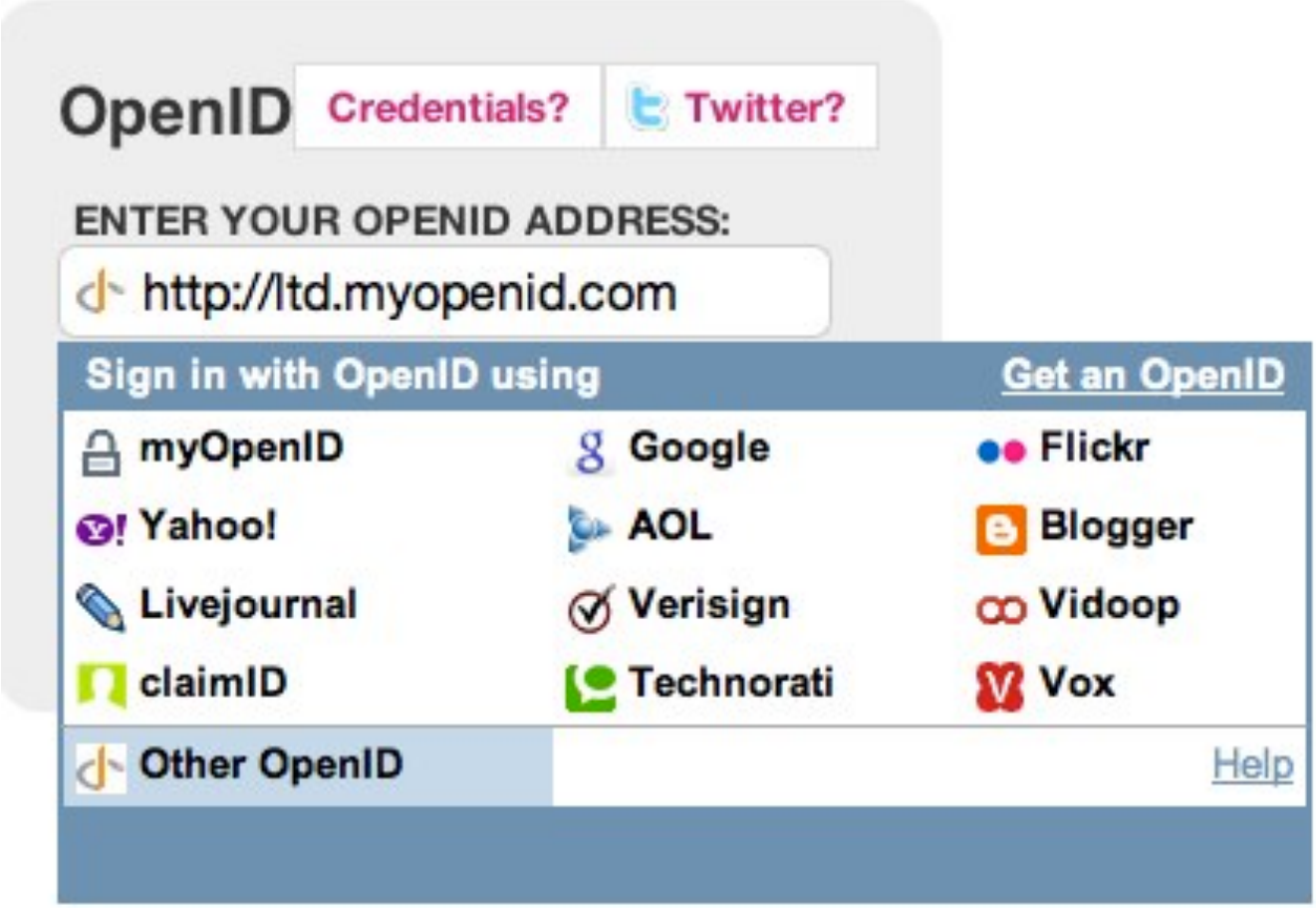



BEST BUY
Parents.
Kmart
NATIONAL GEOGRAPHIC CHANNEL
GET SATISFACTION
Sears
twitter feed
Citysearch
NING
fitness
Mind, Body + Spirit
THE DAILY SHOW WITH JON STEWART
Vht
TRIBUNE INTERACTIVE
NASDAQ
Kodak
IdeaScale
where ideas come to life
EMI
schülerVZ
Blackbaud
UNIVERSAL
UNIVERSAL MUSIC GROUP
WISER EARTH
npr
PayPal
savings.com
MTV
MUSIC TELEVISION
KickApps
meredith
THE BODY SHOP.
Tungle
DIESEL
FOR SUCCESSFUL LIVING
cigar aficionado
THE DR. OZ SHOW
THE BALTIMORE SUN
Free People
URBAN OUTFITTERS
PAULA DEEN
Regence
BELO
bizjournals
THE COLBERT REPORT
Los Angeles Times
divine caroline
GAP
Katy Perry
white pages
adaptu
bizjournals
SCRIPPS
TakingITGlobal
INSPIRE INFORM INVOLVE
KIA
KIA MOTORS
HABBO
Better Homes and Gardens
YellowPages
TRITON MEDIA
QYPE
FIND IT. SHARE IT
50 CENT
NEW YORK STATE SENATE
Deutsche Telekom
SCOUT 24
Autodesk
FOX 5 SAN DIEGO
Associated Northcliffe Digital
part of Daily Mail and General Trust plc
Mahalo
AboutUs
Awana
The Annenberg Foundation

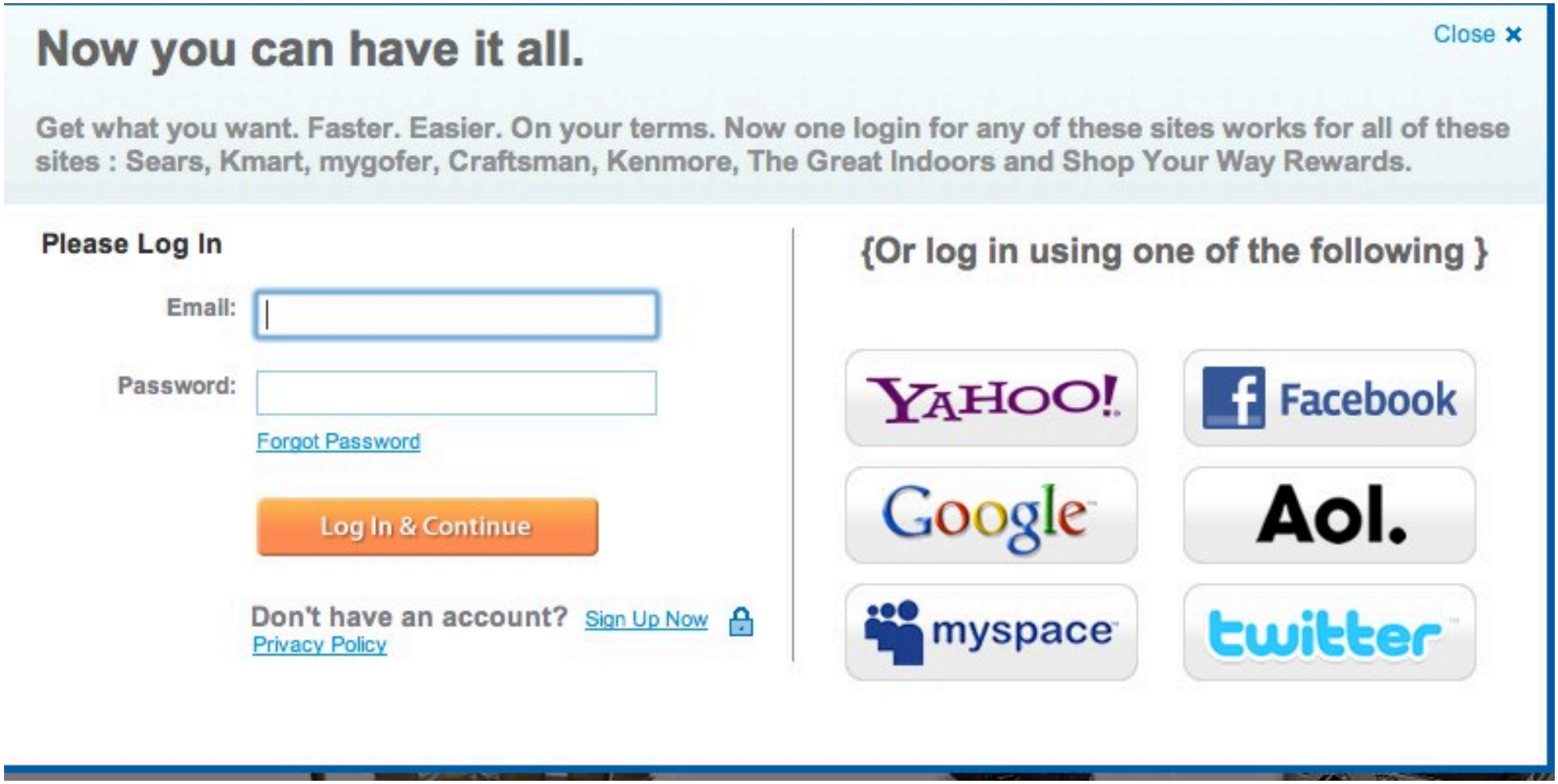
Original UI


Sign in with your
OpenID
OpenID
Remember me on this computer
Sign in

UI Helper


OpenID
Credentials?
Twitter?
ENTER YOUR OPENID ADDRESS:
http://ltd.myopenid.com
Sign in with OpenID using
Get an OpenID
myOpenID
Google
Flickr
Yahoo!
AOL
Blogger
Livejournal
Verisign
Vidoop
claimID
Technorati
Vox
Other OpenID
Help

Current UI


Close
Now you can have it all.
Get what you want. Faster. Easier. On your terms. Now one login for any of these sites works for all of these sites : Sears, Kmart, mygofer, Craftsman, Kenmore, The Great Indoors and Shop Your Way Rewards.
Please Log In
Email:
Password:
Forgot Password
Log In & Continue
Don't have an account? Sign Up Now
Privacy Policy
{Or log in using one of the following }
YAHOO!
Facebook
Google
Aol.
myspace
twitter

Return Experience

Now you can have it all.

Close ✖

Get what you want. Faster. Easier. On your terms. Now one login for any of these sites works for all of these sites : Sears, Kmart, mygofer, Craftsman, Kenmore, The Great Indoors and Shop Your Way Rewards.

Please Log In

Email:

Password:

Forgot Password

Log In & Continue

Don't have an account? Sign Up Now

Privacy Policy

{Or log in using one of the following }

Facebook

not you?

Welcome back, Larry Drebes

Sign In »

use another account

User Acquisition: Users Prefer Interacting On Multiple Platforms

User Data Management: Breadth of Profile Data By Provider

Network	Email	Name	Location	Birth Date	Gender	Friends/ Contacts	Profile Photo	Interests	Social Publishing
facebook	X	X	X	X	X	X	X	X	X
Google	X	X	X			X			X
twitter		X				X	X		X
YAHOO!	X	X	X	X	X	X	X		X
LinkedIn		X	X	X		X	X	X	X
myspace		X	X	X	X	X	X	X	X
Windows Live	X	X		X	X	X	X		
PayPal	X	X							
Aol.	X	X	X	X	X				

User Data Management: Depth of Social Data By Provider

Facebook — Configured

The following features are supported. Enabling features with a checkbox will prompt users for permission to that part of their profile when they authenticate.

Basic Profile
Read access to the users' profile data. Returned by the auth_info API call.

Off Address	Ask Birthday	Ask Verified Email
Display Name	Family Name	Formatted Name
Gender	Given Name	Homepage
Preferred Username	Profile Photo	Time Zone

Extended Profile
Read access to the users' extended profile data. Returned by the auth_info API call.

Ask About Me	Off Addresses	Off Current Location
Ask Emails	Ask Interests	Off Organizations
Off Photos	Off Relationship St...	Ask Status
Books	Friends List	Interested In M...
Last Updated	Movies	Music
TV Shows	URLs	

Contacts
Read access to the users' friends. Returned by the get_contacts API call.

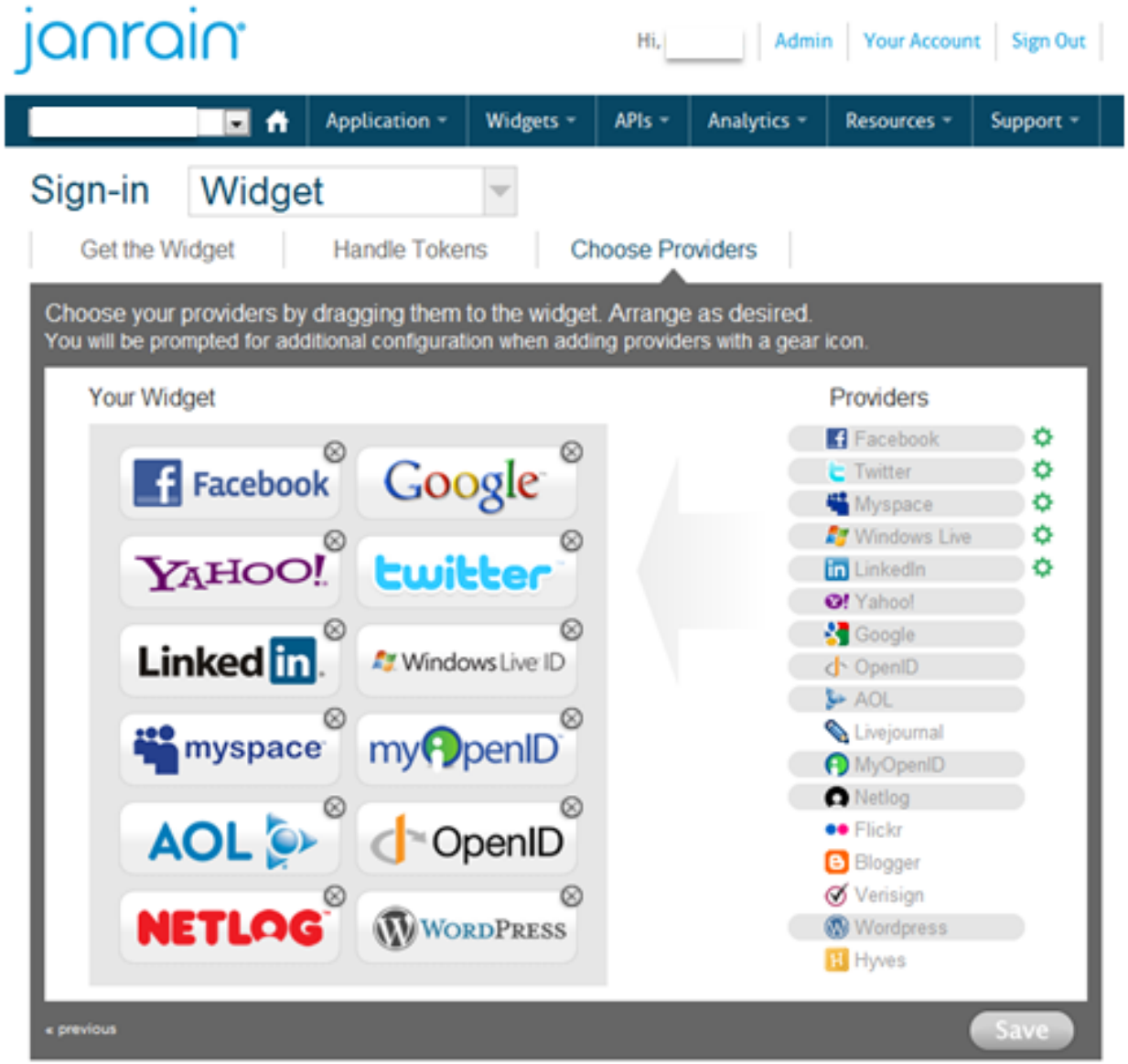
Off About Me	Off Address	Off Addresses
Off Birthday	Off Current Location	Off Interests
Off Organizations	Off Photos	Off Relationship St...
Off Status	Books	Display Name
Family Name	Formatted Name	Gender
Given Name	Homepage	Interested In M...
Last Updated	Movies	Music
Preferred Username	Profile Photo	Time Zone
TV Shows	URLs	

Social Sharing
Ask Post content, comments, or likes to a user's stream.
Required for the social widget. Also works with the activity and set_status API calls (Pro only).

Facebook
Google
LinkedIn
Myspace
PayPal
Twitter
Windows Live
Yahoo!
AOL
Blogger
Flickr
Hyves
Livejournal
MyOpenID
Netlog
Verisign
Wordpress

Full List of Available Profile Data – www.janrain.com/providerguide

Configuring the UI is "drag and drop"



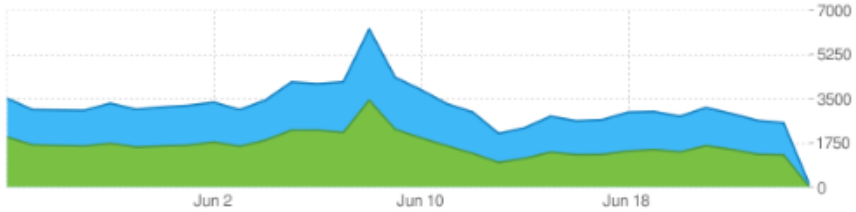
Gain Insight through Actionable Analytics

Sign-In Analytics

Daily sign-ins and new users

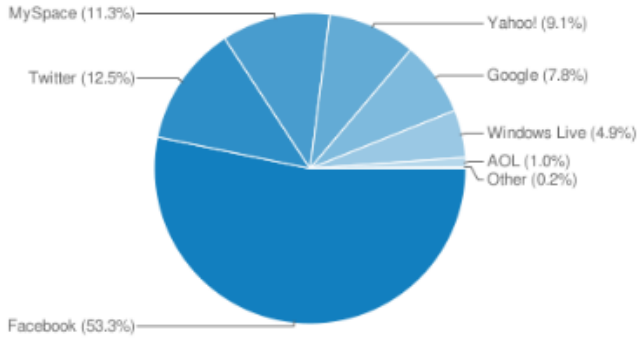
May 25 - Jun 25

Last 30 Days



Login stats by day.

Distribution of providers used for sign-in



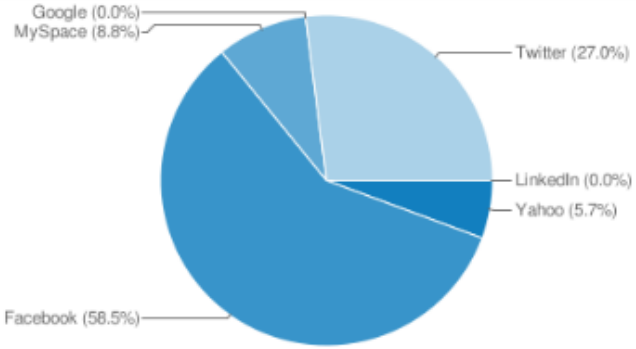
Social Publishing Analytics

Daily posts and referrals

May 25 - Jun 25

Last 30 Days

Distribution of posts by provider



Universal Login Experience

Kantara Initiative

Co-chair: Philippe Clement (Orange)

Co-chair: Bob Morgan (University of Washington)

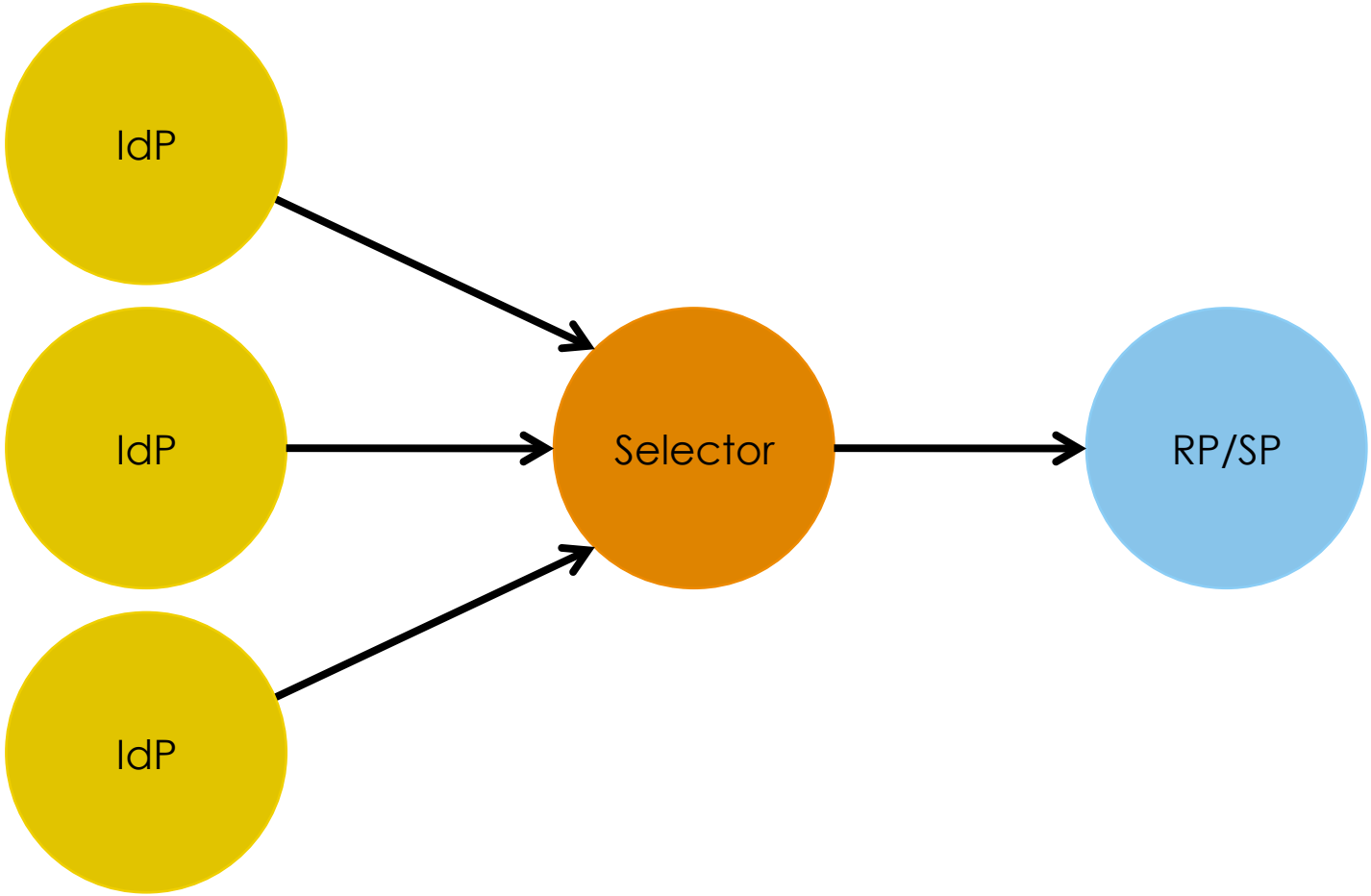
Co-chair: Paul Trevithick (Azigo)

User Experience Architect: Valeska O'Leary (Azigo)

Objectives

- Focus on user experience
  - Ignore technical feasibility (at least at first)
  - Multi-language
  - Support people with various disabilities
- Protocol-agnostic
  - OpenID, SAML, Infocard, Webfinger, userid/password
  - Could be extended to Facebook Connect, and others
- Three deployment architectures
  - RP-embedded selector
  - Selector agent web service
  - Active client

Conceptual Architecture



Mozilla Firefox Start Page

http://www.ncbi.nlm.nih.gov/pubmed/

PubMed Home

NCBI Resources How To My NCBI | Sign In

PubMed.gov
U.S. National Library of Medicine
National Institutes of Health

Search: PubMed Limits Advanced search H

Search

Sign in to **PubMed**
with 1 of the 6 accounts below

What is this?

NCBI Google EQUIFAX PayPal Windows Live YAHOO!

or enter your account provider

Welcome to PubMed

PubMed comprises more than 19 million citations for biomedical articles from MEDLINE and life science journals. Citations may include links to full-text articles from PubMed Central or publisher web sites.

Using PubMed

- PubMed Quick Start
- New and Noteworthy
- PubMed Tutorials
- Full Text Articles
- PubMed FAQs

PubMed Tools

- Single Citation Matcher
- Batch Citation Matcher
- Clinical Queries
- Topic-Specific Queries

More Resources

- MeSH Database
- Journals Database
- Clinical Trials
- E-Utilities
- LinkOut

Done valeskaUX YSlow

Mozilla Firefox Start Page

http://www.ncbi.nlm.nih.gov/pubmed/

PubMed Home

NCBI Resources How To My NCBI | Sign In

PubMed.gov
U.S. National Library of Medicine
National Institutes of Health

Search: PubMed Limits Advanced search H

Search

Welcome to PubMed

PubMed comprises more than 19 million citations for biomedical articles from MEDLINE and life science journals. Citations may include links to full-text articles from PubMed Central or publisher web sites.

Sign in to **PubMed**
with 1 of the 6 accounts below

What is this?

NCBI Google EQUIFAX PayPal Windows Live YAHOO!

F

Florida Memorial University
Florida State University Orlando, FL
Florida State University Palm Springs, FL
Florida Metropolitan University
FMU -
fmuniv.edu-

Using PubMed

PubMed Quick Start
New and Noteworthy
PubMed Tutorials
Full Text Articles
PubMed FAQs

PubMed Tools

Single Citation Matcher
Batch Citation Matcher
Clinical Queries
Topic-Specific Queries

M

MeSH Database
Journals Database
Clinical Trials
E-Utilities
LinkOut

Done valeskaUX YSlow

Mozilla Firefox Start Page

http://www.ncbi.nlm.nih.gov/pubmed/

PubMed Home

NCBI Resources How To My NCBI | Sign In

PubMed.gov
U.S. National Library of Medicine
National Institutes of Health

Search: PubMed Limits Advanced search H

Search

Recently you signed in to **PubMed**
using this account ...

Google

more options

Welcome to PubMed

PubMed comprises more than 19 million citations for biomedical articles from MEDLINE and life science journals. Citations may include links to full-text articles from PubMed Central or publisher web sites.

DEMO

Using PubMed

- PubMed Quick Start
- New and Noteworthy
- PubMed Tutorials
- Full Text Articles
- PubMed FAQs

PubMed Tools

- Single Citation Matcher
- Batch Citation Matcher
- Clinical Queries
- Topic-Specific Queries

More Resources

- MeSH Database
- Journals Database
- Clinical Trials
- E-Utilities
- LinkOut

Done valeskaUX YSlow

Learnings

- Let the RP/SP use its own UI to initiate login (e.g. “login” button)
  - Don’t impose a standard button or icon
- Ended up with a UI “theme with variations”
  - E.g. If more than N IdPs than include the search widget
  - E.g. if support Webfinger then allow email address entry
  - Lists vs. use icons
- Allow search provider name AND keywords

Logic drives the UI

```
If (number-of-accepted-IdPs is less than TBD1) then
{
  Display all of them as a set of icons
} else if (number-of-accepted-IdPs is less than TBD2) then
{
  Display all of them by name in a vertical list
} else
{
  // there is either a large (i.e. more than TBD2) fixed set of acceptable IdPs
  // or there is an unknowably sized set of acceptable IdPs (e.g. the RP supports WebFinger)
  If (RP supports WebFinger AND RP supports a fixed set of acceptable IdPs) then
  {
    Display a text entry widget whose label says
       "type an email address OR the name of an identity provider"
  } else if (RP supports a fixed set of acceptable IdPs) then
  {
    Display a text entry widget whose label says "find your identity provider"
  } else if (RP supports WebFinger) then
  {
    Display a text entry widget whose label says "type an email address"
  }
}
```

Next Steps: Metadata

- Describing the RP/SP policies to the Selection Agent
  - What providers are trusted?
  - What claims are required?
- Describing the IdPs to the Selection Agent
  - Icons (if available)
  - Claims supported
- [Maybe] Expand to non-login use cases
- [Maybe] Expand to "multi-IdP" claims aggregation
  - User selects multiple IdPs to gain all necessary claims

Discovery and Federated Identity

INTERNET®

Topics

- Life today and the pull-down list from Hell
- Hints at the wrong layer suck
- The importance of keeping the continuity of experience
  - Staying with the story
- How does the likely path of interfederation affect discovery

Life Today

- Workarounds
  - Initiating at the IdP – e.g. PSU get to NIH through the PSU research web site.
  - Hand out Per-IdP URLs (e.g. Google)
  - Assume one IdP, "click here if you're a weirdo" in its login UI
- Models
  - SP/Embedded – e.g .Elsevier
  - Centralized/Shared
    - SP-centric - e.g. NIH Federated Login gateway vs. federation/IdP centrice.g. WAYF, InCommon

Grab File Edit Capture Window Help (95%) Mon 4:20 PM

Identity Provider Selection

https://spaces.internet2.edu/shibboleth-ds/WAYF?entityID=https%3A%2F%2Fspaces.internet2.edu%2Fshibboleth&return=https%3A%2F%2Fspaces.internet2.edu%2FShibboleth.sso%2FLo

Google Maps Wikipedia

Select an Identity Provider

The Internet2 Wiki Service requires that you identity yourself. Please select a trusted identity provider from the list below, or simply begin typing in the edit box.

Enter institution name:

Search

Choose from a list:

Federation	Organization
US Higher Education	AAF standalone attribute authorities
UK Federation	AARNet
Australian Access Federation	Aberdeen College
SWAMID Test Federation	Aberdeen College Staff
Austria - ACOnet	Aberystwyth University
France - CRU	Abingdon and Witney College
Servicio de Identidad de RedIRIS (SIR)	Academy of Fine Arts Vienna
Switzerland - SWITCHaai	Accrington & Rossendale College
All Sites	ACOnet
	ACOnet OpenIdP (Self-Asserted Identity)

Select Remember for session

Need assistance? Send mail to spaces-admin@internet2.edu with description.

Loading "https://spaces.internet2.edu/shibboleth-ds/WAYF?entityID=https%3A%2F%2Fspaces.internet2.edu%2Fshibboleth&return=https%3A%2F%2Fspaces.internet2.edu%2FShibboleth.sso%2FLogin%3FSAMLDS%3D1%26os_destination%3D%252Fdashboard.action%26target%3Dcookie%253Aa986e7e1", completed 3 of 4 items

Done

Grab File Edit Capture Window Help (95%) Mon 4:24 PM

Atlases – High Resolution Pathology Images

muni.cz https://atlases.muni.cz/en/index.html

Most Visited Getting Started Latest Headlines

OneView Internet Login | CNN.com – Breaking News, U.S.,... | Washington Dulles Internationa... | Program – 10th Symposium on... | Dashboard – Internet2 Wiki | Atlases – High Resolution Path...

Atlases - PATHOLOGY IMAGES

Collection of high resolution histological images

Lang:

Registered users: 16229

Hypertext atlas of Dermatopathology

version 10.96, November 2010

Hypertext Atlas of Dermatopathology contains thousands of clinical and histological images of skin diseases. Virtual microscope interface is used to access histological images available in very high resolution. The Atlas is available in English and Czech.

Hypertext atlas of Fetal Pathology

version 2.22, September 2010

Hypertext Atlas of Fetal Pathology contains clinical and histological images of various form of developmental anomalies. Virtual microscope interface is used to access histological images available in very high resolution. The Atlas is available in English and Czech.

Hypertext atlas of Neonatal Pathology

version 1.11, September 2010

Hypertext Atlas of Neonatal Pathology contains clinical and histological images of various forms of neonatal pathology. Virtual microscope interface is used to access histological images available in very high resolution. The Atlas is available in English and Czech.

Hypertext atlas of Bone Marrow Pathology

version 1.10, February 2010

Hypertext Atlas of Bone Marrow Pathology Pathology contains clinical and histological images of various forms of bone marrow diseases. Virtual microscope interface is used to access histological images available in very high resolution. The Atlas is available in English and Czech.

Hypertext atlas of Rare Lymphomas

version 0.83, September 2010

Hypertext Atlas of Rare Lymphomas contains clinical and histological images of some rare hematologic/lymphatic malignancies of children. Virtual microscope interface is used to access histological images available in very high resolution. The Atlas is available in English and Czech.

Hypertext atlas of Pathology

version 2.50, November 2010

Hypertext Atlas of Organ Pathology contains teaching materials for pre-graduate students. It is under construction and in full version so far available in Czech language only. The English version contains only chapters with images to enable image sharing (see bellow). The interface is similar to the Atlas of Dermatopathology. Many macroscopic and microscopic images are available, as well as images from CT and MRI scanners and endoscopes.

Demo pages of the Atlases

This page demonstrates technologies used in the Atlas on selected images (activation of arrows, sharpening, virtual microscope). This page does not require registration.

In order to have an access to the **high resolution** images you have to **LOGIN** below:

If you have an account in one of the following **identity federation**, click on the logo.

If you are not member of any listed identity federation, click on the button below:

Local account

Contact us | Privacy | How to cite Atlases

Done

kjk@internet2.edu

Grab File Edit Capture Window Help (93%) Mon 4:15 PM

Select your identity provider

terena.org https://login.terena.org/wayf/module.php/discopower/disco.php?entityID=https%3A%2F%2Fterena.org%2Fsp&return=https%3A%2F%2Flogin.terena.org%2Fwayf%2Fmodule.php%2Fsaml%2Fsp%2Fdisco

Most Visited Getting Started Latest Headlines

OneView Internet Login | CNN.com – Breaking News, U.S.,... | Washington Dulles Internationa... | Program – 10th Symposium on... | Select your identity provider

SELECT YOUR IDENTITY PROVIDER

English | Bokmål | Nynorsk | Sámegiella | Dansk | Deutsch | Español | Svenska | Suomeksi | Français | Italiano | Nederlands | Luxembourgish | Czech | Slovenščina | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 | 中文 | ελληνικά | Lietuvių kalba | Åarjelh-saemien giele

You have previously chosen to authenticate at **Internet2**

Login at Internet2

All | Nordic countries | Spain | UK | eduGAIN | Social networks | Guest providers | Miscellaneous

Incremental search...

- Internet2
- Arnes
- AAI@EduHr (Croatia)
- Aberdeen College
- Aberdeen College Staff
- Aberystwyth University
- Abingdon and Witney College
- Accrington & Rossendale College
- Adam Smith College
- AESIR
- aitta2.funet.fi Shibboleth 2
- Anglia Ruskin University

Done

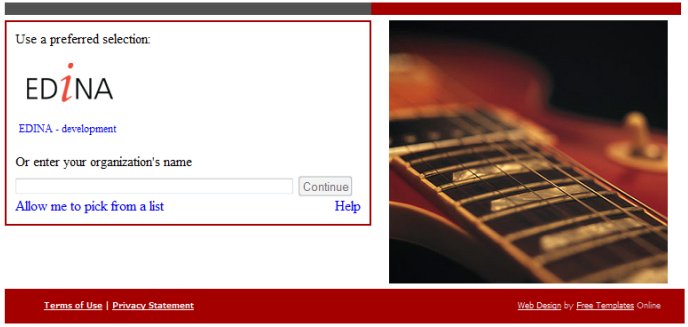


Figure 2: Initial IdP selection page embedded in SP webpage

2.2.1 Preferred IdP Pane

The top portion of the EDS, known as the preferred IdP pane, displays a set of "preferred" IdPs. An IdP is preferred if either the EDS deployer has specifically stated it as preferred in their configuration, or if the user has previously selected the IdP. The EDS will always display the SP configured preferred IdPs first, but it will always reserve at least one spot for a user selected IdP. So, for example, if the preferred IdP pane has three IdPs in it, and the SP has configured 4 preferred IdPs, only the first two will be shown and the third slot will be a user selected IdP. The preferred IdPs are represented by both an image button, bearing the logo of the IdP, as well as a textual link bearing the IdP's name (see Associated Metadata Changes for the origins of this data).

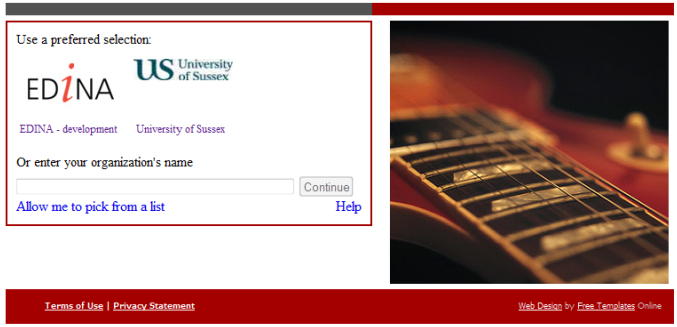


Figure 3: IdP selection page showing previously selected IdP to the right of SP configured preferred IdP

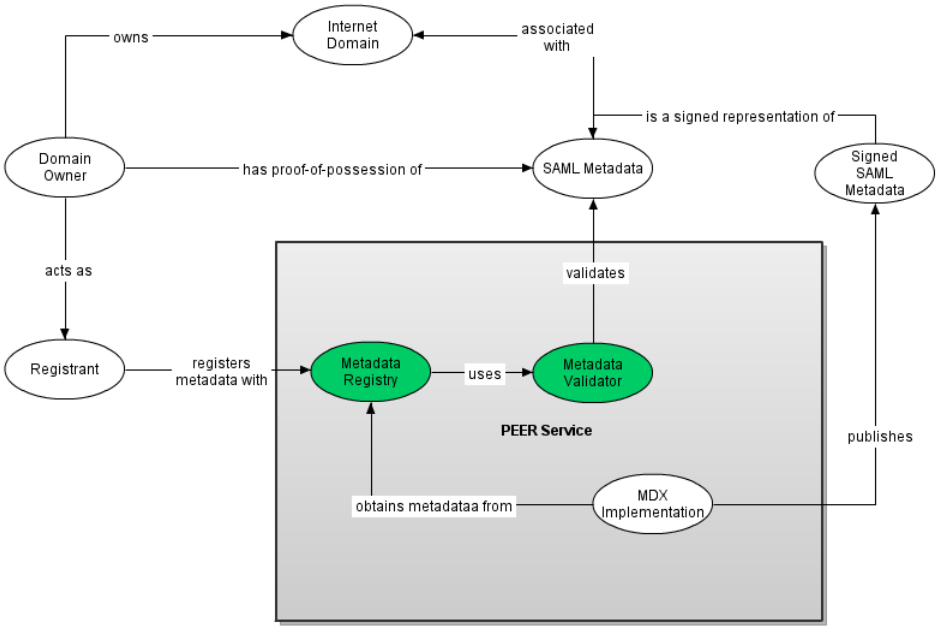
Moving from /etc/hosts to interfederation

- Connecting autonomous federations
- Critical for global scaling, accommodating state and local federations, integration across vertical sectors
- Has technical, financial and policy dimensions
- Technical solutions include eduGAIN and MDX
- Policy activities in eduGAIN, Kalmar2 Union, Kantara, Terena

MDX – metadata exchange protocol

- Institutions and organizations will pick a registrar to give their metadata to
- Institutions and organizations will pick an aggregator (or several) to get their partners metadata from
- Aggregators exchange metadata with each other and registrars
- If this sounds like DNS registration and routing, it is, one layer up

PEER Big Picture



Implications for discovery

- So many IdP's…
  - Can sub-select at the SP
  - Can get sticky at the SP
- Discovery for non-web apps
  - Pop up a browser
  - Sticky on the device (cookie, cert,…)

Privacy Panel

- Trent Adams, Internet Society
- Al Zarate, National Center for Health Statistics
- Ken Klingenstein, Internet2
- Brian LaMacchia, Microsoft Research

Three Forms

- American – subject takes responsibility for her own privacy – don’t share any data, but if you do share data, it’s free for everyone
- European – recipient of personal data takes responsibility for the subject’s privacy – share data with people you trust to respect your privacy
- Census – distillation of useful data from databases while destroying personal data – share anonymized data with those you don’t trust

the Internet is for everyone

Online Privacy – *A Global Perspective*

ID Trust Symposium, April 6, 2011

J. Trent Adams (adams@isoc.org)

Internet Society

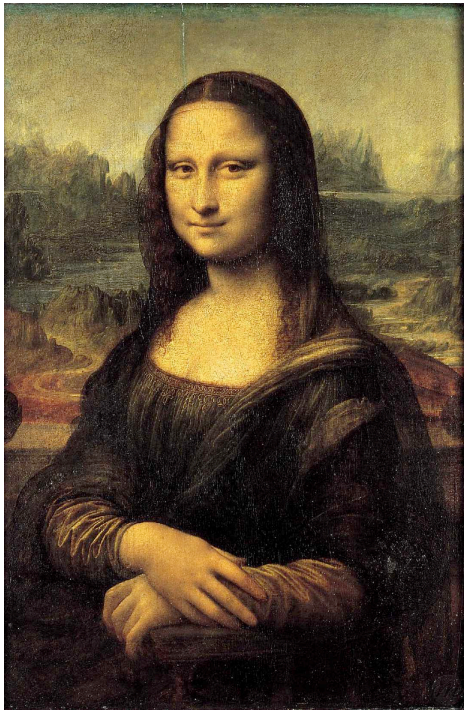
InternetSociety.org

Online Privacy – *A Global Perspective*

- Framing Online Privacy
- Survey of Global Membership
- International Policy & Regulatory Activities
- The Bumper Sticker

Privacy Overview – *"I'll know it when I see it."*

- A definitive definition of "**privacy**" is as elusive as one for "**art**"



Privacy Overview – *An OECD Definition*

- **OECD defines privacy as a concept that applies to data subjects:**
  - "It is the status accorded to data which has been agreed upon between the person or organisation furnishing the data and the organisation receiving it and which describes the degree of protection which will be provided."
  - **NOTE:** *This definition is from the OECD "Glossary of Statistical Terms", which is maintained as a "comprehensive set of definitions of the main data items collected by the organisation." … though this definition is not frequently cited, and there is no other concise definition within the OECD.*

http://stats.oecd.org/glossary/detail.asp?ID=6959

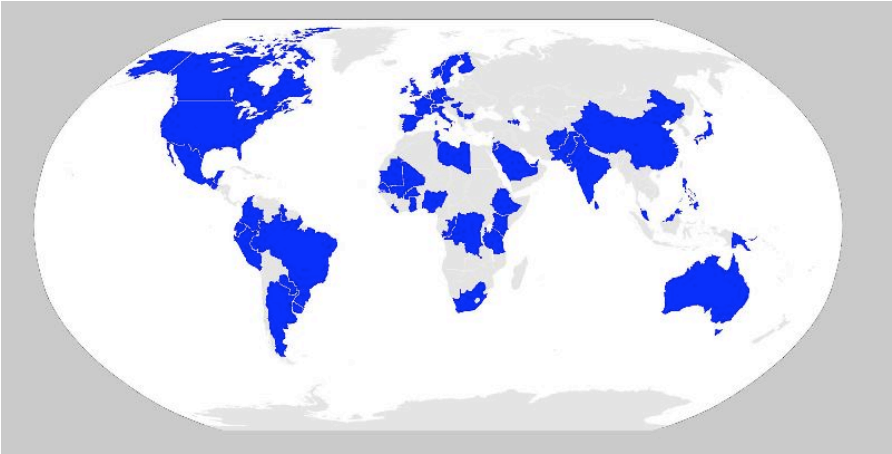
Privacy Overview – *Unpacking a Concept*

Online Privacy = { **Sharing** (data) in an explicit **context** with an expectation of **scope**. }

Privacy Overview – *Striking a Balance*

- **Privacy Protection in the Context of Personal Data on the Internet**
  - Supports confidence in the overall network
  - Network Confidence = Usability (Privacy + Security + Reliability)

Privacy Overview – *International ISOC Member Survey*



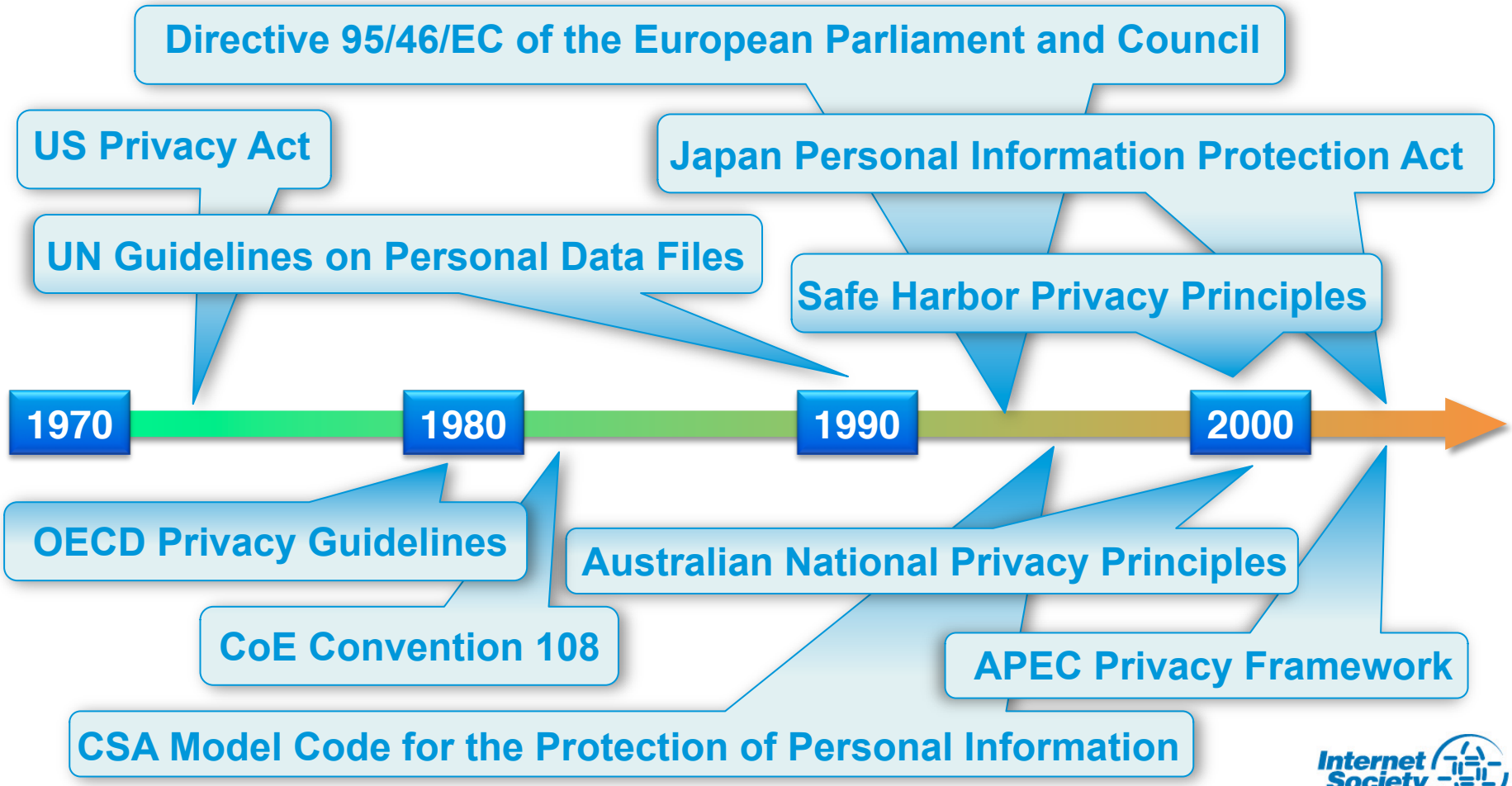
- **Regional Differences Emerged, Including:**
  - **Societal** – *Responses from Asia tended to focus on security of personal data.*
  - **Regulatory** - *Responses from countries with well-established privacy laws tended to be more specific with policy suggestions.*
  - **Priority** - *Respondents in countries with low Internet penetration prioritized connectivity over privacy concerns.*

Full Report: http://www.isoc.org/internet/issues/privacy.shtml

Privacy Overview – *International ISOC Member Survey*

- **Emerging Challenges Included:**
  - **Data Durability** – *How to effectively manage long-lived personal data.*
  - **Economics of Privacy** – *What is the value of personal data, and how to balance the transborder flow of legal economic activity & privacy.*
  - **Ownership, Control and Responsibility** – *Who owns what data, how is it controlled, and who is the responsible party.*
  - **Surveillance** – *How to protect individuals from intrusive observation from governments and enterprise.*
  - **Transparency and Understanding** – *How to ensure adequate understanding of how personal data is collected and used.*
  - **Unauthorised Access and Use** – *How to address issues related to the illegal and/or unauthorised access to or use of personal data.*

Privacy Overview – *Some Useful Regulatory Foundations*



Privacy Overview – *International Regulatory Activities*

- **OECD**
  - Preparing an anniversary report on the evolving privacy landscape.
- **Council of Europe**
  - Considering how to modernize Convention 108 for the Protection of Individuals with regard to "Automatic Processing of Personal Data"
- **European Commission**
  - Reviewing general legal frameworks on personal data protection such as Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Privacy Overview – *International Regulatory Activities (2)*

- **APEC Data Privacy Pathfinder Project**
  - Building on the guidance of APEC data privacy principles, they are developing and testing practical elements of a system to enable accountable cross-border data flows

- **International Conference of Data Protection and Privacy Commissioners**
  - 2009 – "Madrid Resolution" Statement on The Necessity of International Frameworks in Support of The Protection of Privacy and Personal Data
  - 2010 – "Jerusalem Declaration" calls for the an intergovernmental conference to develop a binding international instrument on privacy and the protection of personal data

Privacy Overview – *Hot-Topic Issues*

- **Issues Discussed in International Regulatory Bodies:**
  - "Right to be Forgotten"
  - "Privacy by Design" & "Privacy by Default"
  - "Transparency" & "Informed Consent"
  - "Identification" vs. "Correlation"
  - "Data Minimization"
  - "Data Protection"
  - "Jurisdiction of Origin & Use"
  - "Online Activity Tracking"
  - "Defining Personal Data"

Privacy Overview – *What's the Bumper Sticker?*

Privacy Overview – *What's the Bumper Sticker?*

(since we're dreaming anyway…)

Privacy Overview – *What's the Bumper Sticker?*

Online Privacy = { **Sharing** (data) in an explicit **context** with an expectation of **scope**. }

Privacy ~ Secrecy *-and-* **Privacy != Secrecy**

Online Privacy is more than just the web

Privacy. I'll know it when I see it.

the Internet is for everyone

Thank you.

Questions? Comments? Send them to:

J. Trent Adams (adams@isoc.org)

The Internet Society:

- InternetSociety.org
- info@InternetSociety.org

Internet Society™

InternetSociety.org

Achieving Anonymity in Micro Data Files

10th Symposium on Identity and Trust on the Internet
April 6-7, 2011
Privacy: An Emerging Landscape

Alvan O. Zarate, Ph.D.

Scientific Data Analyst

National Center for Health Statistics

NCHS Health E-Stats

CDC SAFER • HEALTHIER • PEOPLE™

NCHS – the Federal Government's Principal Health Statistics Agency – Data Collection,

- Population Based surveys
  - Health Interview Survey
  - Clinical Examination
  - Family Formation
- Records Based data collection
  - Vital Statistics
  - Hospital, Nursing home, MDs.

Data Collected I

- Coroner's reports
- Cause of fetal death
- Other cause: suicide, hiv
- Drug & alcohol use
- Sexual experiences & preference
- Sexually transmitted disease
- Income
- Genetics

Data Collected II

- Date of birth, gender
- Occupation
- Education
- Race
- Geographic area (street, county, state)
- Household characteristics

Two Requirements

- **"...shall publish ... and disseminate ... [it's] ... statistics on as wide a basis as is practicable."**

- **No *identifiable* information ... may be used for any purpose other than the purpose for which it was supplied nor may it be released to any party not agreed to by the supplier.**

Public Health Service Act of 1974

Applicable Law

- Privacy Act
- FOIA (Exceptions for identifiable data)
- Public Health Service Act (308(d)) Upheld in Appellate Court
- E-Govt. Act (Title V - Confidential Information Protection and Statistical Efficiency Act (CIPSEA)

Terms and Concepts

Privacy

Informed Consent

Confidentiality

Disclosure

Identifiability

De-identification

Re-identification

Privacy

"Informational privacy encompasses an individual's freedom from excessive intrusion in the quest for information and

an individual's ability to choose the extent and circumstances under which his or her" information "will be shared with or withheld from others." Private Lives and Public Policy 1993

Informed Consent

- agreement to allow personal data to be provided for research and statistical purposes. … based on full exposure of the facts the person needs to make the decision intelligently,
- (including possible linkage to other information and identities of other parties who would be given access to identifiable data.)

Informed Consent - consequences

- A binding contract – strictly observed
- Ability to restrict access not authorized
  - for NCHS denial of congressional claim upheld by U.S. Court of Appeals
- Basis of claim to stewardship responsibility

Confidentiality

"A quality or condition accorded to information as an obligation not to transmit that information to an unauthorized party."
National Research Council 1991

"…the promises … made to a data provider …regarding the extent to which the data provided will allow others to gain specific information about the data provider or data subject." Private Lives and Public Policy 1993

Disclosure

- Inappropriate (cf. consent) attribution of information to a data subject.

  - *Information disclosure*: sensitive information about an individual revealed

  - *Identity disclosure*: data provider identified together with associated sensitive information

Identifiable Information

- *Data which can be used to establish individual identity, whether directly - using items such as name, address or unique identifying number - or indirectly - by linking data about a respondent with other information that uniquely identifies them*

Direct and Indirect Identifiability

Direct identifier: Information that is uniquely associated with a person or the person's family. Readily available and leads directly to them with few intermediary steps.

Indirect identifier: Information items which, *in combination* are uniquely associated with a person. Information which facilitates such associations.

Re-identification by Matching

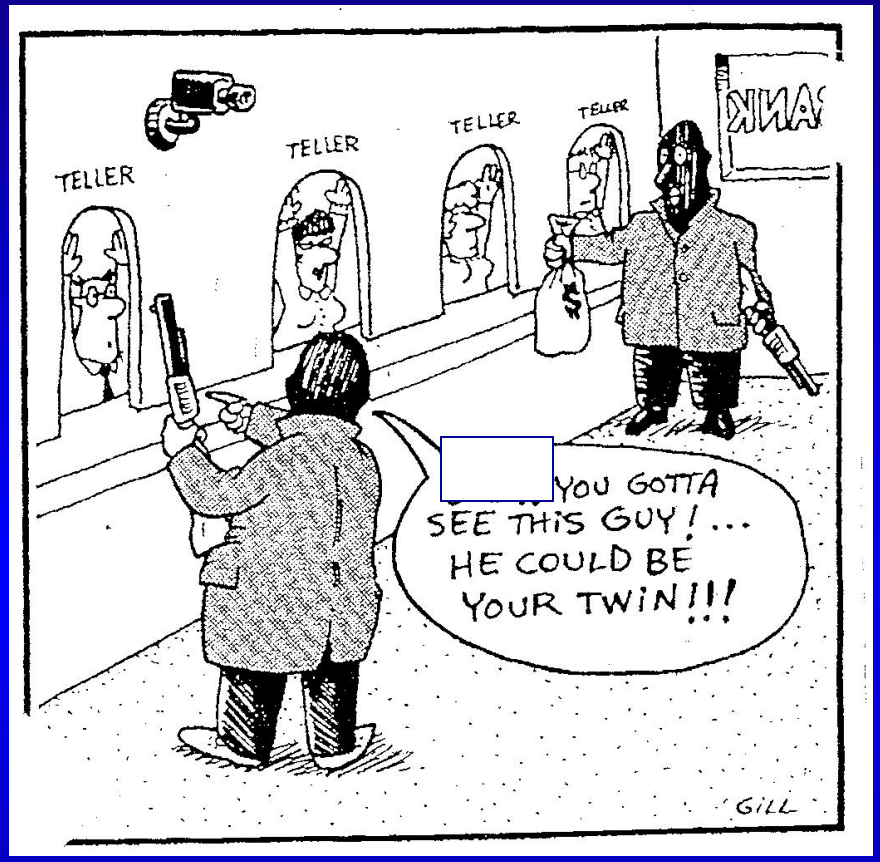
“De-identification”

Identified file Name abcdefghijkl
Identifier deleted abcdefghijkl

“Re-identification”

Public use file abcdefghijkl
External file abcdefgmno Name


TELLER
TELLER
TELLER
TELLER
BOB!! YOU GOTTA SEE THIS GUY! ... HE COULD BE YOUR TWIN!!!
GILL


TELLER
TELLER
TELLER
TELLER
YOU GOTTA SEE THIS GUY! ... HE COULD BE YOUR TWIN!!!
GILL

Data in Combination

- Month, day and year of birth
- Gender
- Zip code

Unique-ness Using Three Variables

Variables	% Unique in voter registration list
Birthdate alone	12
Birthdate + gender	29
Birthdate + Zip (5)	69
Birthdate + Zip (9)	97

Sweeney, 1997

Data Release

- Unrestricted (public use)
- Restricted (identifiable/confidential)
  - Collaborators
  - Other researchers/agencies
  - Data Center/Enclave (use but no release)

Data Release – Public Use

Unrestricted (de-identified)

- "…when … microdata are released to anyone who wants them, with *no restrictions or conditions of any kind…*"

(Jabine, 1993. Emphasis added)

Disclosure Review - Steps

- Study documentation
- Check list
- Consultation with Confidentiality Officer
- Submission to DRB
- Presentation/discussion at DRB
- Follow-up as necessary
- Decision

Disclosure Risk Checklist

- Series of questions designed to help determine the suitability of releasing data.
  - geographic detail – explicit & implicit
  - statistical outliers re selected variables (age, race, occupation, income, household type)
  - intentional & unintentional error
  - other data bases containing similar data

Assessing Disclosure Risk - I

- Key variables (age, gender, occupation, marital status, income …)
- Variables unique to this file (not available for population)

  - collected by no one else

  - collection process not replicable

  (clinical samples, attitudes)
- Addition of external data – “enrichment”

Assessing Disclosure Risk - II

- Geographic detail – explicit and implicit
- Proportion of study population included (all v. sample)
- Amount of error in data - target and population (e.g. income)
- Data sensitivity

Data Protection

- Remove direct identifiers
- Restrict geography
- Code to remove detail – larger categories, top coding
- Variable suppression (e.g. place of birth)
- “Unusual” case suppression (small frequency)
- Special handling of data from external sources (esp. area data)
- Statistical modification (“noise”)

DRB Deliberation

- Discussion/Questions re issues raised by data collection program or DRB.
- Most resolved at initial meeting
- Some require follow up to determine
- - frequencies of cases in sample v. general population.
- - effect on key statistics of data protection methods employed.

Decision

- Release/Do not release
  - decision covers ongoing surveys for three years when there is no change in content or frequencies. After that, new review.
- Data use agreements*
- Research Data Center

* Consent permitting

References/Resources I

When Data Sharing is Required: I. What is this Requirement? II. HIPAA and Disclosure risk Issues III. Meeting the Challenge. de Wolf V, Sieber JE, Steel P and Zarate AO. *IRB: Ethics & Human Research*. 27/6 28/1 and 28/2. 2005-2006.

References/Resources II

- American Statistical Association, Privacy, Confidentiality and Data Security web site

http://www.amstat.org/comm/cmtepc/index.cfm?fuseaction=main

- Disclosure Potential Checklist

http://www.fcsm.gov/committees/cdac/index.html

Data release problems and resolution -1

Data System	Problem/Resolution
-NSFG (contextual)	Area detail – RDC
-NEHIS	Establishment/linkage with external files – RDC
-NHANES	Heavy publicity – PSU modification, 2 yrs file, recodes

Data release problems and resolution -2

Data System	Problem/Resolution
-NHANES (kids)	Clinical report/RDC
-NSFG (kids)	Parents knowledge /statistical “noise”
-NHIS size of SMSA	Research evidence of disclosure risk/restrict release to 500,000+

Data release problems and resolution -3

Data System	Problem/Resolution
-NHIS data detail disease condition,	Recoding of occupation income, race
-Survey sample detail	Recombination of info.
-Surveys linked with mortality data	Linkage with external files/RDC
-Vital Statistics	Geographic detail – in process

The “Culture” of Confidentiality

- Individual employee as the most important element
- Awareness of responsibility as an ethical as well as legal imperative
- Continuous awareness
- Seen as protective of study participants *and* responsive to the research community

Issues and Challenges

- Synthetic Data Sets
- Offsite Designated Agents
- Web data dissemination
- Data Stewardship/Data centralization
- Assessment of security breaches

Privacy – Three Definitions

- Privacy/Secrecy *Basic. Required by law/ethics*
- Privacy of Shared Data *Authorization required (consent) Both parties responsible. Sanctions. Tight agreements.*
- Anonymization of Data

  Not easy but possible. More research needed. Restricted access

Consent and Federated Identity

INTERNET®

Topics

- Consent
  - Where and when
  - How the interface looks today
  - Where it needs to go
- Informed consent
  - Setting the bar
  - Engaging the SP's
  - Educating the User

Jurisdictional Issues at the Start

- At least three policy spaces at play
  - IdP location
  - SP location
  - User's national and local laws
- Known exploits exist today…

Consent

- At the point of collection of information
  - “We intend to use what you give us in the following ways”
- At the point of release of information
  - “I authorize the release of this data in order to get my rubber squeeze toy…”

User interface

- Provide users with control, and guidance, over the release of attributes
  - Includes consent, privacy management, etc.
- Basic controls (uApprove) now built into Shibboleth, but largely untapped in deployments.
- Additional technical developments would help scalability
- Human interface issues largely not yet understood – getting the defaults right, putting the informed into informed consent, etc.

SWITCH aai

About AAI : FAQ : Help : Privacy

This is the Digital ID Card to be sent to '**https://aai-demo.switch.ch**':

Digital ID Card

Surname	**SWITCHaai**
Given name	**Demouser**
Unique ID	**234567@example.org**
User ID	**demouser**
Home organization	**example.org**
Home organization type	**other**
Affiliation	**staff**
Entitlement	**http://example.org/res/99999** **http://publisher-xy.com/e-journals**

☐ Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future.

Cancel Confirm

Firefox

Inbox (5) - marc_doughty@brown.ed... | VMware Communities: VMware Work... | null

https://sso.brown.edu/uApprove/Controller?returnurl=https%3A%2F%2Fsso.brown.edu%2Fidp%2Fprofile%2FSAML2%2FRedirect%

Brown University

Authentication Required

Terms of Use

By submitting this form you agree to continue to abide by the Brown University Acceptable Use Policy outlined at www.brown.edu/cis/policy/aup.php.

☐ I accept the terms of use

Decline | Confirm

Brown Home | Help | myAccount | **New Users:** Activate your account now

The face of web authentication at Brown is changing! You are using Brown's new web authentication service, Shibboleth. During 2009, Shibboleth will gradually replace WebAuth as Brown's Single Sign-on web authentication service. Shibboleth is more useful, more secure, and more widely used throughout higher education.

Shibboleth.

Shibboleth is different - learn how to safely and securely use Shibboleth.

Additional information regarding Brown's Shibboleth implementation is located on the CIS documentation wiki.

Firefox

Inbox (5) - marc_doughty@brown.ed... | VMware Communities: VMware Work... | null

brown.edu https://sso.brown.edu/uApprove/Controller?terms-agree=on&terms-confirm=Confirm

vmware workstation 2.6.38

Brown University

Authentication Required

To use 'spaces.internet2.edu', their system needs to receive some information about you in the form of a Digital ID Card. You will need to agree to send the following information to access their services. All this information is needed or access to the service will not be granted.

Digital ID Card	
email	Marc_Doughty@brown.edu
eduPersonPrincipalName	mdoughty
storedIdOracle	ujbMRsDo5eeKRrsOItCcvMsrF50=
displayName	Marc P. Doughty

☐ Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future to this site as well as to other services I will access.

Cancel | Confirm

Brown Home | Help | myAccount | **New Users:** Activate your account now

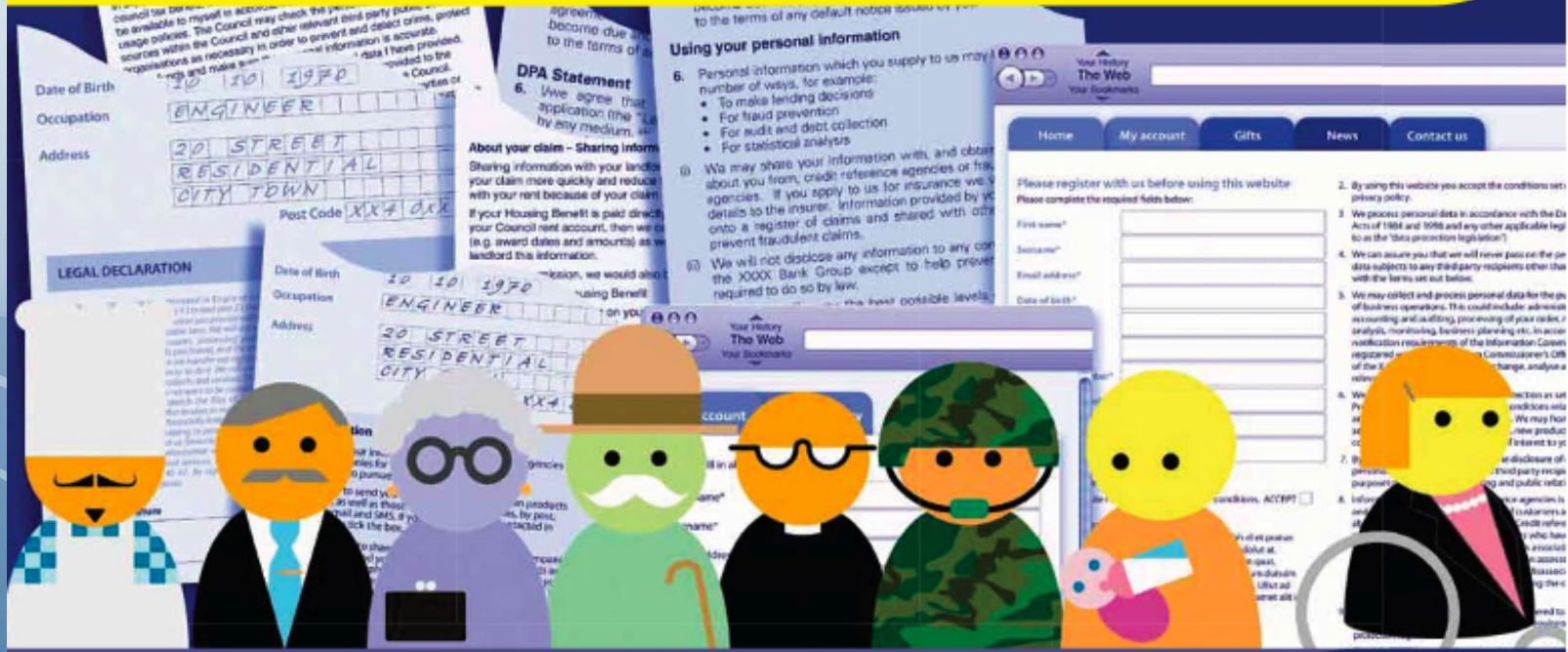
Shibboleth.

The face of web authentication at Brown is changing! You are using Brown's new web authentication service, Shibboleth. During 2009, Shibboleth will gradually replace WebAuth as Brown's Single Sign-on web authentication service. Shibboleth is more useful, more secure, and more widely used throughout higher education.

Shibboleth is different - learn how to safely and securely use Shibboleth.

Additional information regarding Brown's Shibboleth implementation is located on the CIS documentation wiki.

Privacy notices code of practice



Promoting public access to official information
and protecting your personal information

Information Commissioner's Office

Informed Consent

Next | Back | Print | Quit

Contents

Examples:

The final part of this code consists of a set of examples based on real privacy notices that we have seen. They illustrate good practice to adopt, such as giving people appropriate choices that are easy to exercise, and bad practice to avoid, such as using confusing language. The examples are illustrative extracts only and should not be used as templates. They cannot cover every type of information collection, but they will help organisations to draft privacy notices whatever their line of business. Please note that the formats shown may not meet accessibility requirements.

Date of Birth 10 10 1970

Occupation ENGINEER

Address 20 STREET
RESIDENTIAL
CITY TOWN

Post Code XX4 0XX

How information about you will be used

We may share your information with credit reference agencies and other companies for use in credit decisions, for fraud prevention and to pursue debtors.

We would like to send you information about our own products and services, as well as those of selected third parties, by post, telephone, email and SMS. If you agree to being contacted in this way, please tick the relevant boxes.

Post ☐ **Phone** ☐ **email** ☐ **SMS** ☐

We would also like to share your information with other companies so that they may send you information about their products and services, by post, telephone, email and SMS. If you agree to your information being shared in this way, please tick the box. ☐

If you need any further information please write to us at 10 Street Name, Town Name, County Name AB12 3CD.

Customer Signature **Date**

Simple language, clear font and style.

Clear opportunity to agree to marketing.

Prior consent sought.

Alternative 'opt out' version:

We would like to send you information about our own products and services, as well as those of selected third parties, by post. If you **do not** agree to being contacted in this way, please tick the box. ☐

Clear opportunity to opt out of marketing.

Specific rules for marketing by email, telephone and SMS apply. Please see our guidance on the Privacy and Electronic Communications Regulations 2003.

Date of Birth 10 10 1970

Occupation ENGINEER

Address 20 STREET
RESIDENTIAL
CITY TOWN

Post Code XX4 0XX

LEGAL DECLARATION

X Limited is a company incorporated in England and is a member of the X Retail Group ("the Group"). The Group ("we/us") also includes Y Limited and Z Limited and their associated companies from time to time. The personally identifiable information you provide will be processed in accordance with the Data Protection Acts 1984 and 1998 and other applicable laws. We will use your information so that we can process your order. This includes administering any accounts, processing your bank/credit card details in order to obtain payment, arranging delivery of any goods purchased, and the prevention and detection of fraud. We can hand over your information to anyone to whom we transfer our rights and duties under our agreement with you or if we have a duty to do so and the law allows us to do it. We will use your information for market research and the marketing of our own and third parties' products and services. This may include contacting you by post, telephone, email or SMS unless you indicate you do not want to be contacted in any of these ways by calling us on 0870 23 45 67. We will use your information to search the files of credit reference agencies who will record that search. This information may be used by other lenders in making credit decisions about you, members of your household and those with whom you may be financially linked. Information held about you by the credit reference agencies may already be linked to records relating to people with whom you are financially linked. For the purposes of credit searching, you may be treated as financially linked and you will be assessed with reference to any associated records. We will share your information with other companies, for the purposes of market research and the marketing of their products and services, unless you indicate that you wish to be excluded from such uses by contacting us on 0870 23 45 67. By signing this form, you consent to the information you provide being processed for the above purposes.

Customer Signature **Date**

Confusing and legalistic language. Closely spaced text, small italic font in light grey.

Unnecessary – means little to public.

Raises Privacy and Electronic Communications Regulations problems and 0870 number does not provide easy means to opt-out consistent with the medium (script).

Confusing language.

Unexpected use. Good practice would be to obtain consent.

Next Steps

- Normalize the “presentation of the attributes” language
- Field test – get the defaults right
- Sift through what really needs consent
  - Need to complete the business transaction
  - Europe model more sophisticated but is compounded by national issues
  - Federations as vehicle for national consent management
  - ePTID – opaque, non-correlating. Does it need consent?
  - Cookie consent?
- Attribute bundles

New Results using Anonymous Credentials: Constrained Delegation and Revocation

Brian A. LaMacchia
Director, XCG Security & Cryptography, Microsoft Research

Agenda

- Basics of anonymous credentials
- Using anonymous credentials in security policy languages
  - Anonymous credential delegation
  - Anonymous principals for the SecPAL language
- Making anonymous credentials revocable
  - Problem definition
  - Accumulators
  - Using accumulators as privacy-preserving CRLs
  - Revocable delegable anonymous credentials

Anonymous Credentials

- An anonymous credential allows a *principal* to prove possession of one or more *attributes* without revealing the principal's identity or other additional information.

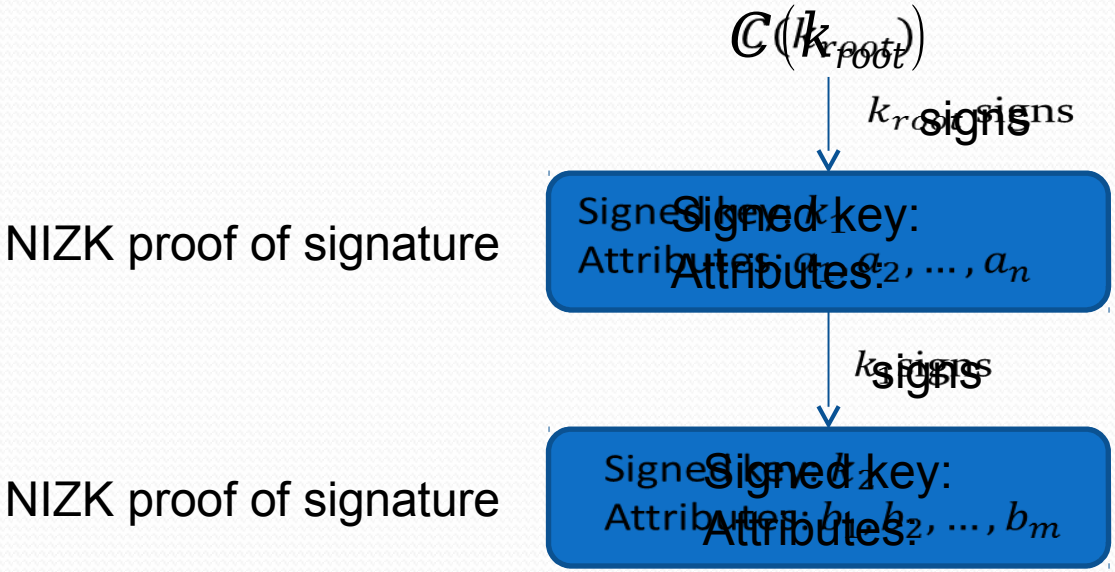
- Examples of attributes:
  - "is a US citizen", "age > 18", "is an employee of Fabrikam"

- *Unlinkability* is a key requirement
  - Should not be able to link multiple uses of a credential

- One technique: Non-Interactive Zero-Knowledge (NIZK) proofs
  - Prove you have a dig sig from an issuer of the desired attribute
  - Re-randomize the proof to hide identity & provide unlinkability
  - Uses Groth-Sahai proofs (Belenkiy et al., Crypto '09)

Anonymous Credential Delegation

- Keys for anonymous credentials have two forms
  - Private: held by bearer
  - Public: a commitment to the key (can re-randomize)
- Credential chains:



SecPAL: Security Policy Assertion Language

- A security policy language for decentralized authorization
  - Supports constrained delegation
  - Logical framework for reasoning about authorization

- Principals are defined by keys
  - E.g., public key of RSA key pair
  - Principals sign statements (signed credentials)
  - Issuer says Subject can Verb Object

- Some simple examples:
  - Azure STS says Hospital possess accountName: “hospital”
  - Hospital says Pharmaco can read, write file://localhost/hospital/drugtrialdocuments/
  - Storage Tenant says Hospital can read, write file://localhost/hospital/ if Hospital possess accountName: “hospital”

Anonymous Principals for SecPAL

- A principal that proves its ID with an anonymous credential
  - Simple version like a group of principals
    - E.g., Any US citizen can enter the country
  - But can also merge with delegation
    - E.g., OS says <1> can say %x can write to /var
      <1> says <2> can write to /var
- Notation
  - "<i>": principal of credential at delegation level i
- Delegation levels of credentials map to policy
  - Public attributes in credentials are SecPAL statements

Efficiency and Ephemeral Keys

- Anonymous signatures slower than public key
- Solution: bootstrap into public key using ephemeral keys
  - E.g., OS says <1> can write /var
    <1> says RSAKey can act as <1>
  - Now RSAKey can write to /var
  - STS converts to limited, normal token for RSAKey
- Principal can create new RSA key
  - Individual keys are unlinkable

Revocation for Anonymous Credentials

- The ability to revoke is an integral part of all systems built on digital signatures (e.g. PKI certificates)
  - We want this capability for anonymous credentials also
- But how do we revoke an anonymous credential without identifying it explicitly?
  - If we identify it (e.g. list an ID number) then users would also have to reveal that same information to allow relying parties to perform revocation checks linkability
- We need a mechanism that allows an RP to see if a credential is revoked without requiring the reveal of a unique ID
  - Answer: Use an accumulator

Accumulators

- An accumulator is a mathematical object that aggregates a set of elements into a single value.
  - represents the set without revealing the individual elements in the set
- Accumulators allow both *membership* and *non-membership* proofs.
  - Membership Proof: Prove that an element is accumulated in , without revealing .
  - Non-Membership Proof: Prove that an element is NOT accumulated in , without revealing .
- If the contents of the set accumulated in changes, and all the associated proofs can be updated efficiently.

An accumulator is a mathematical object that aggregates a set of elements into a single value.
V represents the set $\{a_i\}$ without revealing the individual elements in the set
Accumulators allow both *membership* and *non-membership* proofs.
Membership Proof: Prove that an element y is accumulated in V, without revealing y.
Non-Membership Proof: Prove that an element y' is NOT accumulated in V, without revealing y'.
If the contents of the set accumulated in V changes, V and all the associated proofs can be updated efficiently.

Accumulators for Blacklisting with Privacy

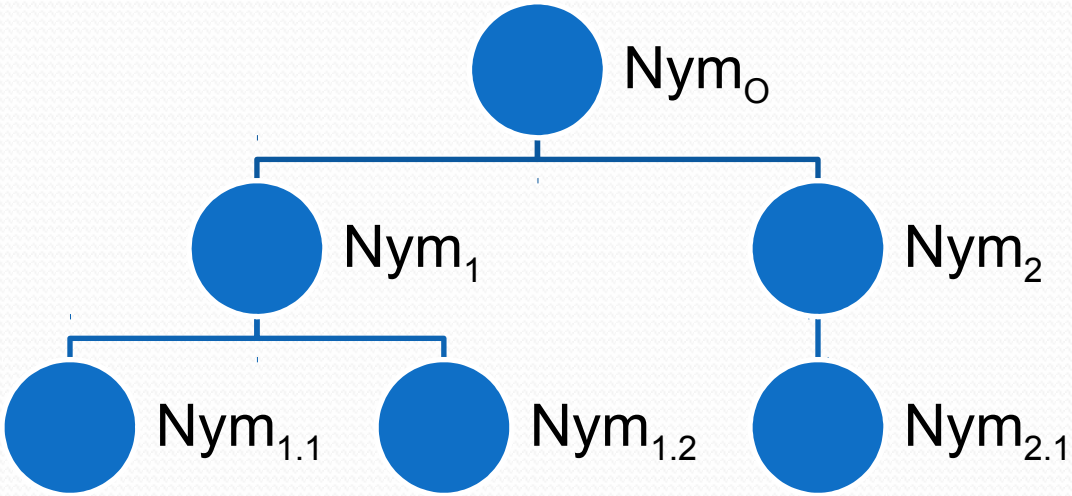
- Main idea: Build a privacy-preserving blacklist of revoked credentials using an accumulator.
  - Like a CRL
- Build an accumulated value V containing all of the revoked credentials.
- When a credential is presented to the RP, the RP can use a non-membership proof to check that the presented credential is not in V.
  - ⇒ If the proof succeeds, then the element is not revoked
- Checking a non-membership proof does not reveal the element
  - ⇒ Privacy protection
- Challenge for authorization delegation:
  - Can a non-membership proof be delegated without revealing the element?
  - Even when the set of accumulated elements changes?

Accumulators with Delegable Non-Membership Proofs (ADNMP)

- ADNMP satisfy the following properties:
- **Delegatability**: y's owner can delegate the ability to prove that y is not accumulated
  - Even when the accumulated set changes, and
  - Without revealing y (reveal a delegating key instead)
- **Unlinkability**: The delegating keys of different elements are indistinguishable.
- **Re-delegatability**: A delegate can re-delegate the proving ability further to other users.
- **Validity**: Correctness of delegating keys are verifiable.

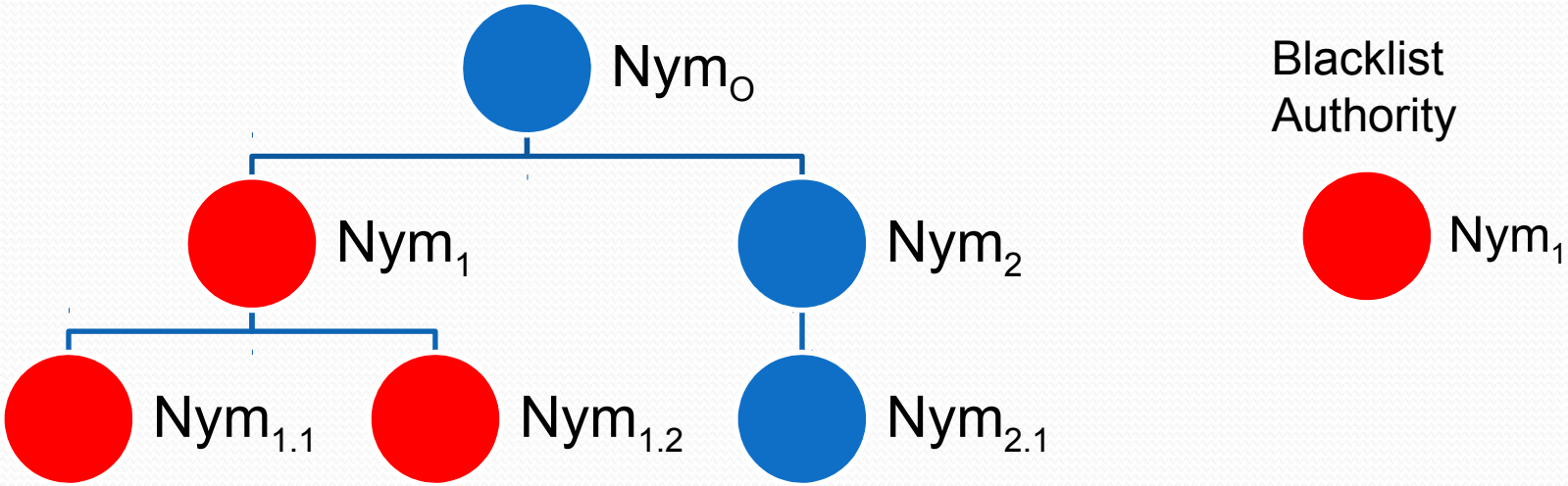
ADNMP satisfy the following properties:
Delegatability: y's owner can delegate the ability to prove that y is not accumulated
Even when the accumulated set changes, and
Without revealing y (reveal a delegating key instead)
Unlinkability: The delegating keys of different elements are indistinguishable.
Re-delegatability: A delegate can re-delegate the proving ability further to other users.
Validity: Correctness of delegating keys are verifiable.

Delegatable Anonymous Credentials



- In a DAC system, pseudonyms form a tree – each link between nodes is a delegation.
- $Nym_{1.1,}Nym_{1.2}$ and $Nym_{2.1}$ can each anonymously prove that she has a credential, which is delegated 2 levels away from $Nym_{O.}$

Revocable Delegatable Anonymous Credentials (RDAC)



- Nym_1 is revoked.
- $Nym_{1.2}$ can no longer prove that she has the credential
  - Her only path to the root is gone.
- $Nym_{2.1}$ can still prove anonymously that
  - She has a credential, which is delegated 2 levels away from $Nym_{O.}$
  - All of her ancestors (Nym_O, Nym_2) are not blacklisted.

Summary

- Anonymous credential delegation can be used to enable anonymous principals in an authorization language
  - We can still have constrained delegation even when anonymous
- Accumulators can be used to build a privacy-preserving revocation mechanism for anonymous credentials
- For more information:
  - Tolga Acar and Lan Nguyen, “Revocation for Delegatable Anonymous Credentials,” no. MSR-TR-2010-170, 22 December 2010
  - SecPAL: http://research.microsoft.com/projects/SecPAL/

Questions?

National Strategy for Trusted Identities in Cyberspace

Jeremy Grant

NIST

April 6, 2011

What is NSTIC?

Called for in President's Cyberspace Policy Review (May 2009):
a "cybersecurity focused identity management vision and strategy"

Guiding Principles

- Privacy-Enhancing and Voluntary
- Secure and Resilient
- Interoperable
- Cost-Effective and Easy To Use

NSTIC calls for an **Identity Ecosystem**,
"an online environment where individuals
and organizations will be able to trust each other
because they follow agreed upon standards to obtain
and authenticate their digital identities."

The Problem Today

Usernames and passwords are broken

- Most people have 25 different passwords, or use the same one over and over
- Even strong passwords are vulnerable…criminals can get the "keys to the kingdom"
- Rising costs of identity theft
  - 123% increase in financial institution Suspicious Activity Reports in last 6 years (FINCEN)
  - 11.7 million est. victims over 2 years (BJS, 2008)
  - $17.3 billion est. cost to economy over 2 years (BJS, 2008)
- Cybercrime is also on the rise
  - Incidents up 22% from 2009 to 2008 (IC3 report)
  - Total loss from these incidents up 111%, to $560 million.

The Problem Today

Identities are difficult to verify over the internet

- Numerous government services still must be conducted in person or by mail, leading to continual rising costs for state, local and federal governments

- Electronic health records could save billions, but can't move forward without solving authentication challenge for providers and individuals

"No one knows you're a dog"

- Many transactions, such as signing an auto loan or a mortgage, are still considered too risky to conduct online due to liability risks

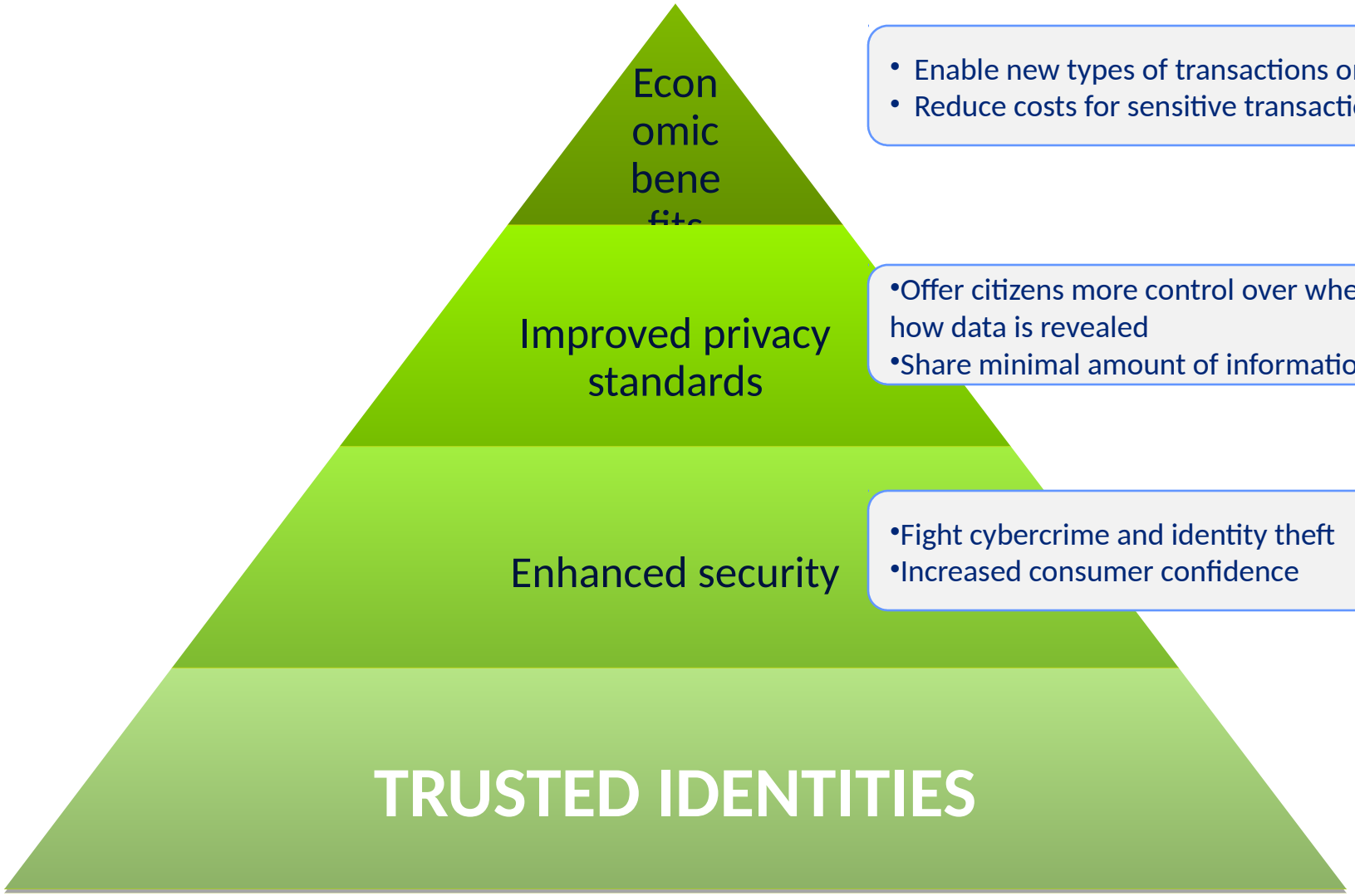
The Problem Today

Privacy remains a challenge

- Individuals often must provide more personally identifiable information (PII) than necessary for a particular transaction
  - This data is often stored, creating “honey pots” of information for cybercriminals to pursue

- Individuals have few practical means to control use of their information

Trusted Identities provide a foundation



- Enable new types of transactions online
- Reduce costs for sensitive transactions

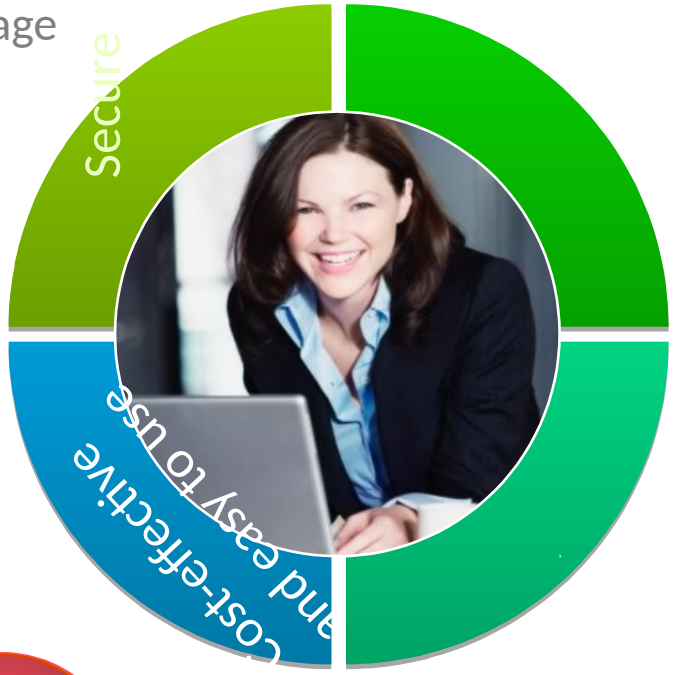
- Offer citizens more control over when and how data is revealed
- Share minimal amount of information

- Fight cybercrime and identity theft
- Increased consumer confidence

January 1, 2016

The Identity Ecosystem: Individuals can choose among multiple identity providers and digital credentials for convenient, secure, and privacy-enhancing transactions anywhere, anytime.

Sign mortgage with digital signature



Alternative payment mechanisms; convenient transactions

Trustworthy critical service delivery

Single Sign-On to her corporate portal

Security 'built-into' the system to reduce user error

Privately post location to her friends

We've proven that Trusted Identities matter

But Barriers Exist

- High assurance credentials come with higher costs and burdens
- They've been impractical for many organizations, and most single-use applications.
- Metcalfe's Law applies – but there are barriers (standards, liability, usability) today that the market has struggled to overcome.

DoD Led the Way

- DoD network intrusions fell 46% after it banned passwords for log-on and instead mandated use of the CAC with PKI.

What does NSTIC call for?

Private sector will lead the effort

- Not a government-run identity program
- Industry is in the best position to drive technologies and solutions
- Can identify what barriers need to be overcome

Federal government will provide support

- Help develop a private-sector led governance model
- Facilitate and lead development of interoperable standards
- Provide clarity on national policy and legal framework around liability and privacy
- Act as an early adopter to stimulate demand

Privacy and Civil Liberties are Fundamental

Increase privacy

- Minimize sharing of unnecessary information
- Minimum standards for organizations - such as adherence to Fair Information Practice Principles (FIPPs)

Voluntary and private-sector led

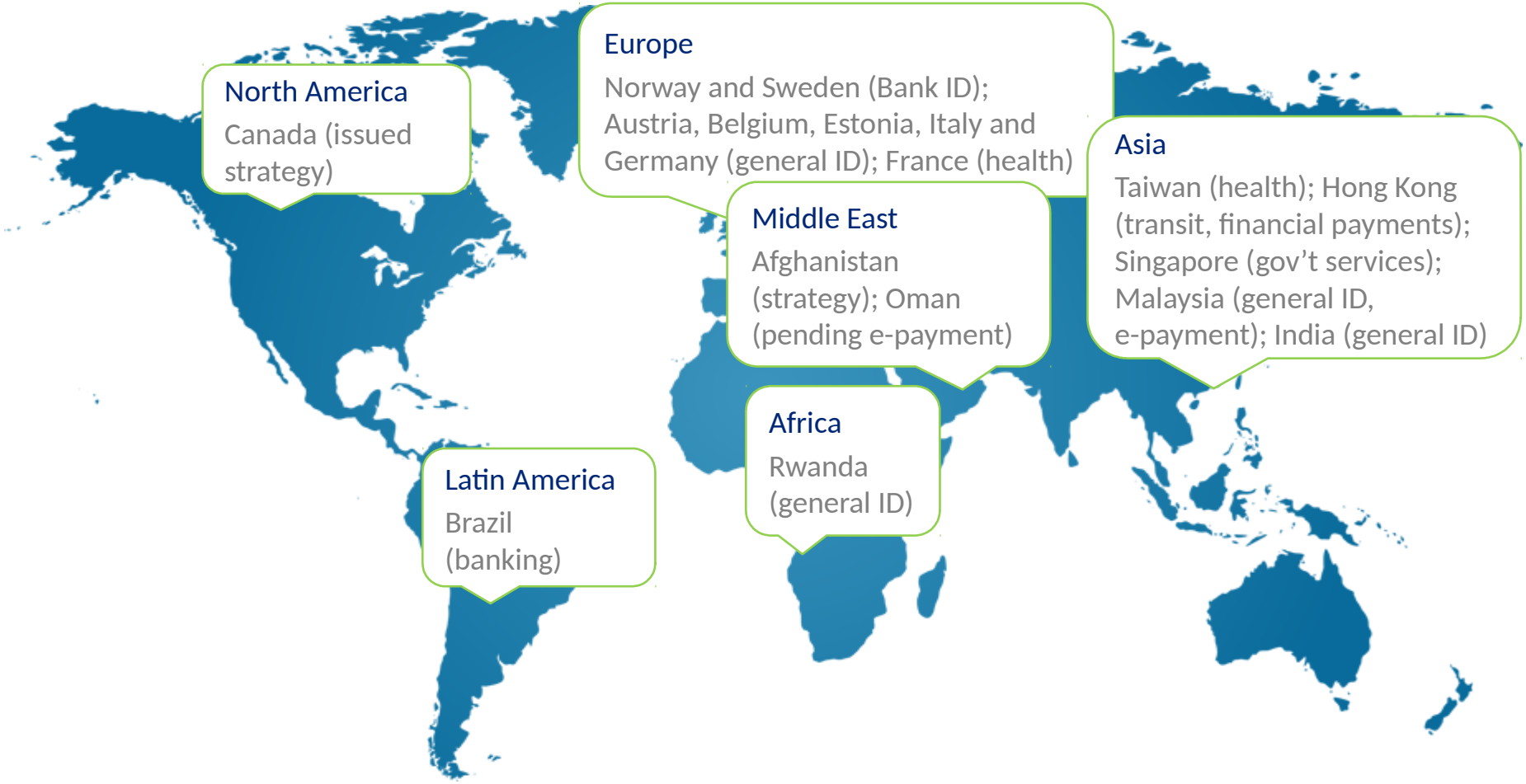
- Individuals can choose not to participate
- Individuals who participate can choose from public or private-sector identity providers
- No central database is created

Preserves anonymity

- Digital anonymity and pseudonymity supports free speech and freedom of association

Other countries are moving forward

NSTIC is unique in that it is led by the private sector.



Industry and Privacy Support

Key members of the U.S. technology industry, the privacy community, and the security industry have expressed support for NSTIC

"NSTIC has the opportunity to tip the balance of the conversation and focus on identity to socio-economic benefit from what is often today one of identity fraud and identity theft. In doing so trusted identities can improve the delivery and lower the cost to the public of financial services, health care, e-commerce and reduce the federal budget."

Salvatore D'Agostino, CEO, Idmachines LLC

"The Administration to my view has, has conducted a very open process here....I think that there's a model here perhaps for the broader question of cybersecurity."

Jim Dempsey, Vice President for Public Policy at the Center for Democracy & Technology

"Our industry strongly supports the goals outlined in the Strategy, and we see a vital role for a National Program office to work with industry and government in its finalization and implementation."

Letter to Sec. Locke, White House Cybersecurity Coordinator Howard Locke, and Patrick Gallagher from TechAmerica, Business Software Alliance, and Information Technology Industry Council; additional signatures included leadership from Microsoft, Symantec, PayPal, CA, CSC, RSA/EMC, Infineon , Unisys, Verisign and Gemalto and other technology firms

BSA. Business Software Alliance | Information Technology Industry Council | TechAmerica WHERE THE FUTURE BEGINS

March 3, 2011

The Honorable Gary F. Locke
Secretary of Commerce
U.S. Department of Commerce
Washington, D.C. 20230

The Honorable Howard A. Schmidt
Special Assistant to the President
Cybersecurity Coordinator
Executive Office of the President
Washington, D.C. 20500

The Honorable Patrick D. Gallagher
Director
National Institute of Standards and Technology
Department of Commerce
Gaithersburg, MD 20899

Dear Secretary Locke, Mr. Schmidt, and Mr. Gallagher:

On behalf of the U.S. technology industry, we write to express our support for the development of a national strategy to address the significant challenges currently associated with online identity management. Therefore, we eagerly await the issuance of the National Strategy for Trusted Identities in Cyberspace (NSTIC) and the establishment of a national program office to help ensure its success.

The industry recognizes a clear and pressing need for strong, trusted identities online as part of a larger effort to support continued robust growth in online transactions and communications, enhance cybersecurity and protect personal privacy. As the Administration has recognized, this goal will be achieved only with robust private-sector involvement in finalizing the strategy and with industry's leadership in its implementation.

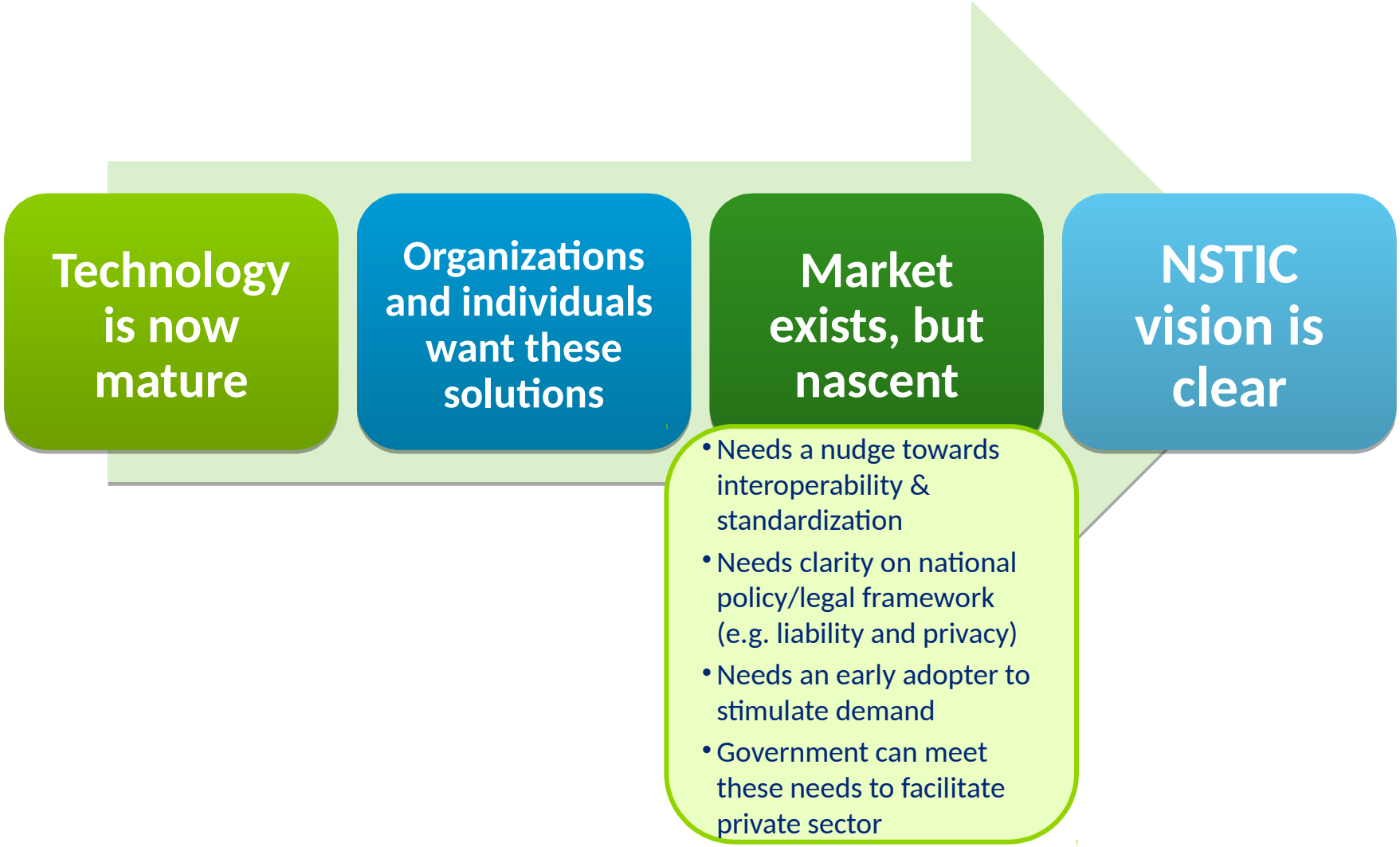
Our members support the need for a national strategy to provide individuals and "organizations secure, efficient, easy-to-use and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation."

Mr. Schmidt, as you have highlighted, $30.8 billion was spent in online transactions during the 2010 holiday season, a 13 percent increase over 2009. If we are to continue to see such rapid growth in online industries such as e-commerce, we must do more to ensure and maintain the trust of consumers and companies in the security of online transactions. In addition, as you have noted, we must ensure that new technologies for identity management improve not only the security of transactions, but also the privacy of consumers engaging in these transactions.

The improved online identities resulting from NSTIC solutions can help achieve those goals by addressing concerns about identity theft, online fraud, intellectual property, privacy and cybersecurity without creating a centralized or government-managed system. Having participated in multiple discussions with the Administration about this program, we believe the government is acutely aware of the necessity for the private sector to lead in developing secure online identities.

We strongly urge that the final strategy be aimed at fostering the growth of an open marketplace that provides consumers and businesses with a choice of credentials and identity management solutions developed and offered by the private sector. That marketplace should be expected to encourage the development of an ecosystem that offers a wide array of identity management technology solutions with a variety of security and privacy options depending upon the nature and sensitivity of the transaction, from anonymity to strong identity assurance and authentication. It is important that these

The Time is Now



Next Steps

Convene the Private Sector

- Workshops on governance, privacy and technology

FY11 Focus

- Establish Governance model
  - Private sector led; multi-stakeholder collaboration
  - Enable expedited focus on consensus standards and operating rules
  - Explore models for addressing liability
- Pilots:
  - Develop criteria for selection
  - Assess potential programs
  - Prepare for formal pilot launches with funding in FY12

Government as an early adopter to stimulate demand

- Ensure government-wide alignment with the Federal Identity, Credential, and Access Management (FICAM) Roadmap
- Increased adoption of Trust Framework Providers (TFP)

Questions?

Jeremy Grant

jgrant@nist.gov

202.482.3050

IDTrust 2011:
Privacy and Security Research Challenges for Biometric Authentication

Moderator: Elaine Newton, PhD
NIST
elaine.newton@nist.gov

National Institute of Standards and Technology

A Generic Biometric System

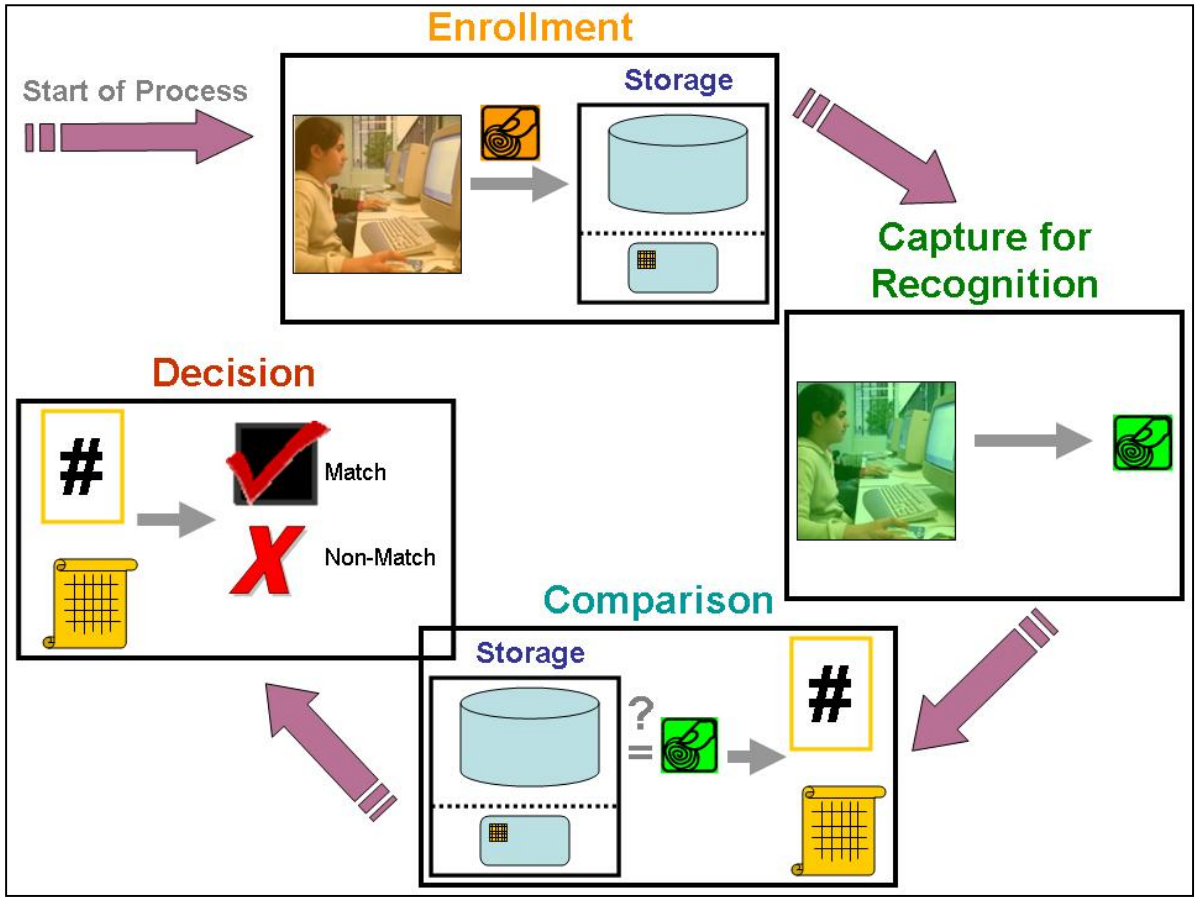
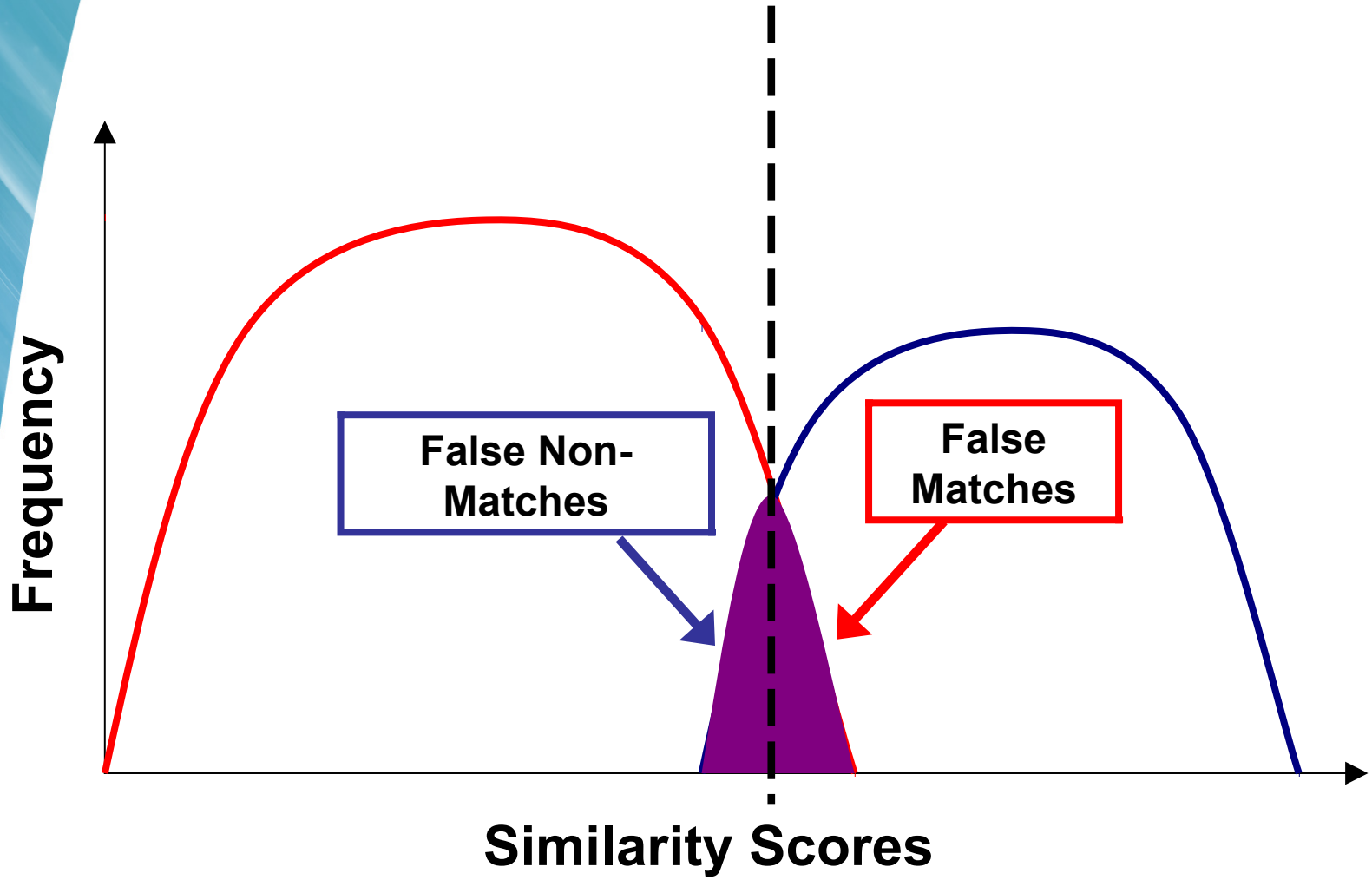


Image from: Newton, Elaine. *Biometrics and Surveillance: Identification, De-Identification, and Strategies for Protection of Personal Data*, PhD Dissertation, Carnegie Mellon University, Dept of Engineering and Public Policy, ProQuest UMI, May 2009.

Notional Histogram of Genuines (Blue) and Imposters (Red)



NIST Biometric Testing

- Fingerprint
  - Ongoing Proprietary Fingerprint Test (PFTII) and MINEX (MINutiae EXchange) testing using various databases of 120K+ subjects
  - Software development kit (SDKs) –based testing
- Face
  - Data from grand challenges and vendor tests
  - DOS Database of 37K subjects
  - Algorithm-based testing
- Iris
  - Data from grand challenges and vendor tests
  - Algorithm-based testing

Authentication Use Case Comparison

For law enforcement, immigration, etc.

- Enrollment and subsequent recognition attempts
  - highly controlled
  - Supervised / Attended
- Successful recognition
  - Answers the question, “Has this person been previously encountered?”
  - Is a unique pattern

For online transactions, e.g. banking, health, etc.

- Enrollment
  - Less controlled
  - Probably not in person
- Subsequent recognition attempts
  - Unattended
- Successful recognition
  - Answers the question, “How confident am I that this is the actual claimant?”
  - Is a tamper-proof rendering of a distinctive pattern

Passwords v. Biometric Data

- P: Known only to the end-user
- B: Potentially known by anyone who can encounter the individual in-person or virtually

- P: Can be (easily) changed if compromised and periodically renewed to mitigate risk
  - Can be lengthened to increase security
- B: A pattern with some degree of robustness over time that can be used to distinguish individuals

- P: Many possibilities for users to choose different credentials for different domains, which could be randomly generated or otherwise have no personally identifying information
- B: A presentation of the same biometrics for any application, and many can be used for identification

- P: Deterministic
- B: Probabilistic

Biometric Security Issues

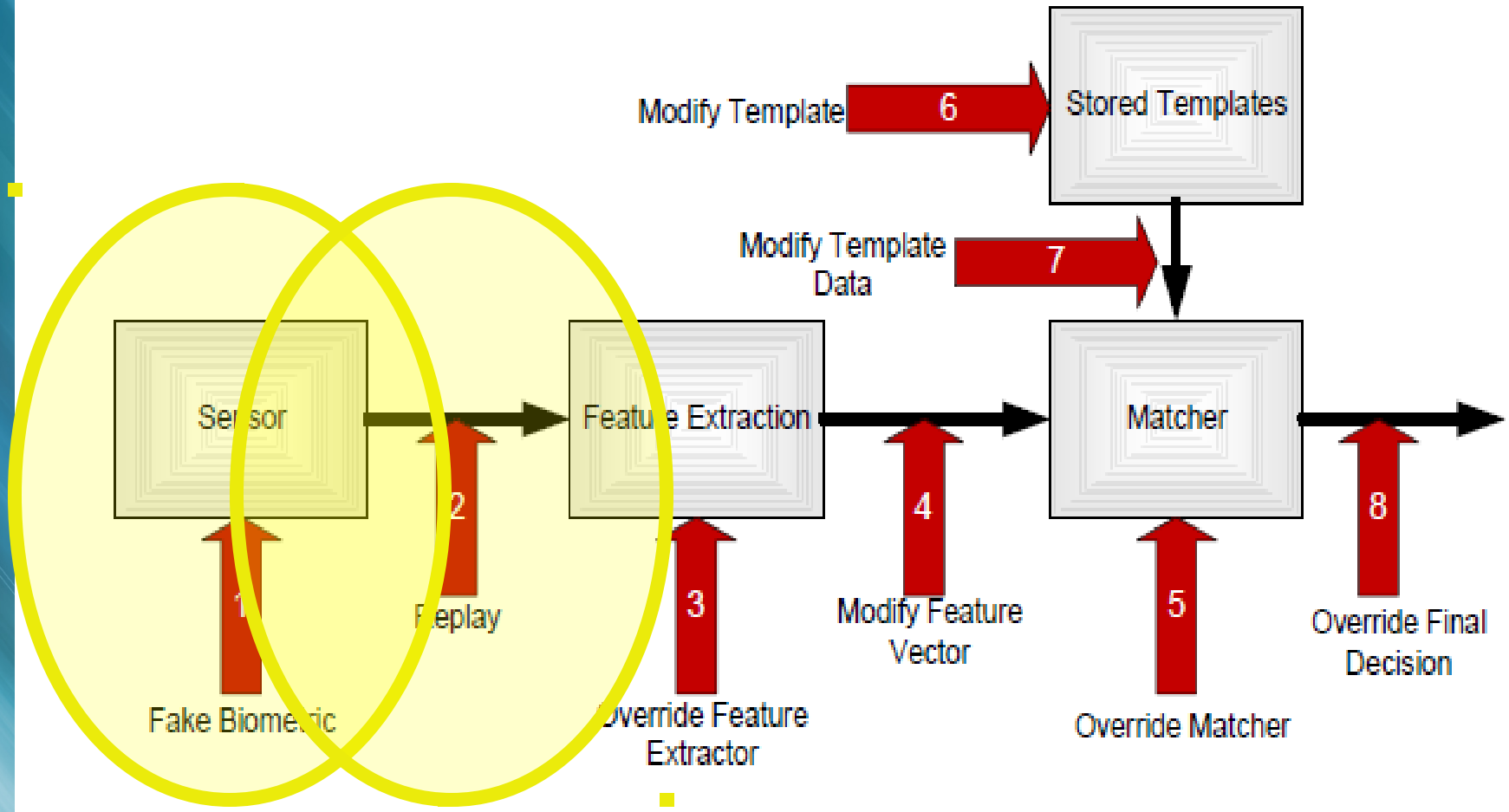


Figure by Nalini Ratha, IBM

Thank you

And now for our panel:

Ross Micheals, PhD

Terry Boult, PhD

Stephanie Schuckers, PhD

Biometrics & eAuth

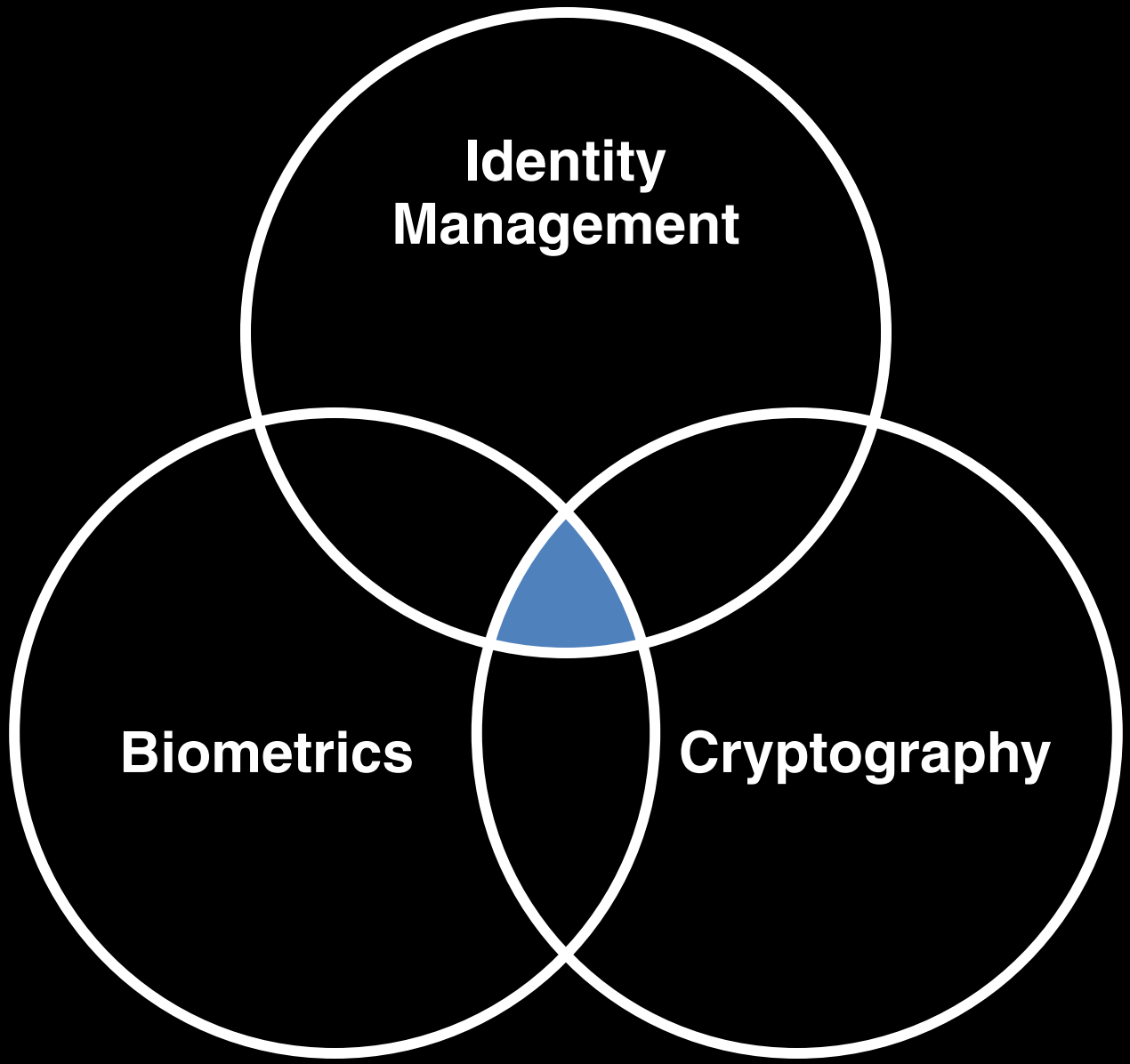
Ross J. Micheals / NIST

revocable biometric (n.)

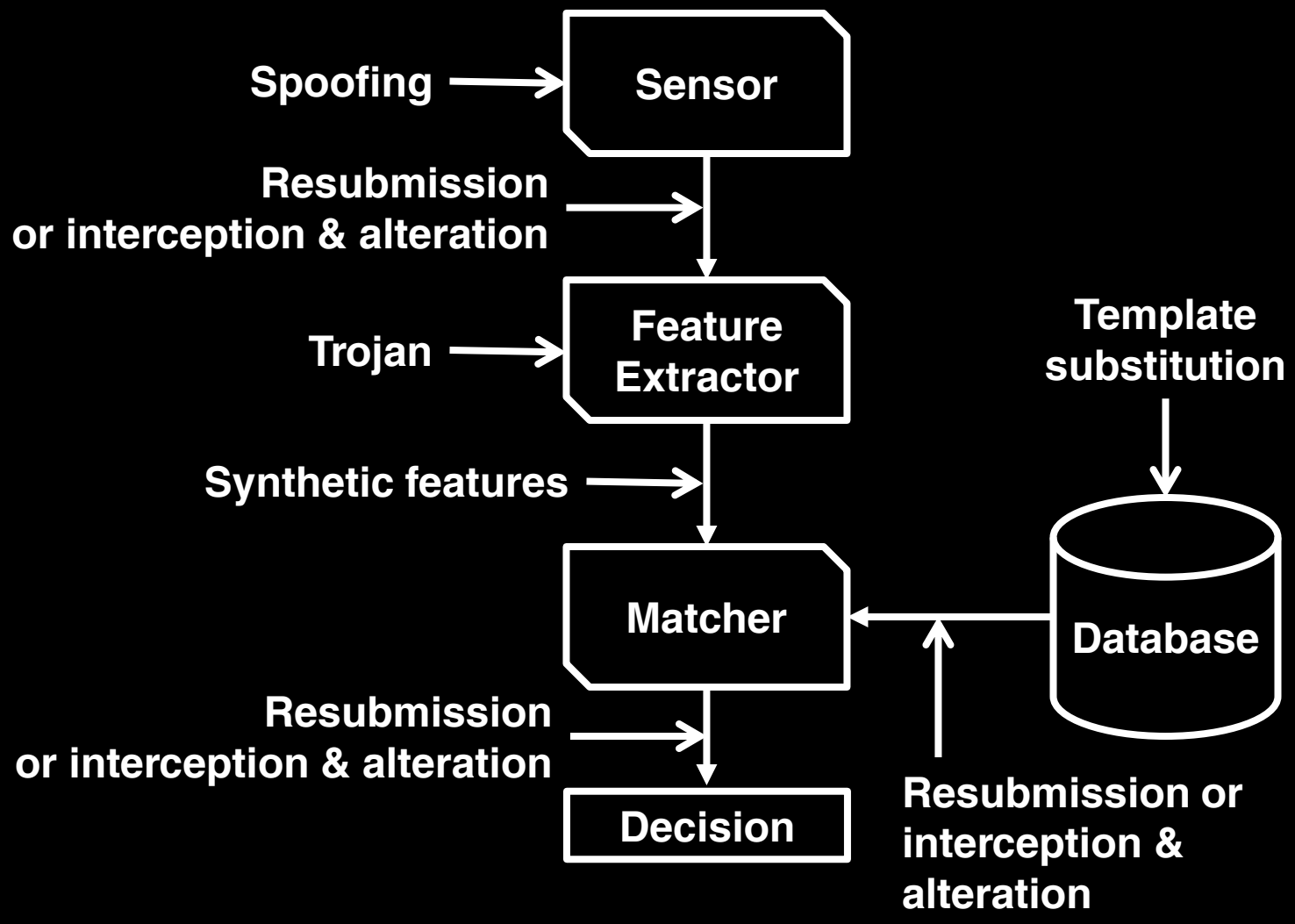
ri·vō'·cə·bəl bi·ō·'me·trik

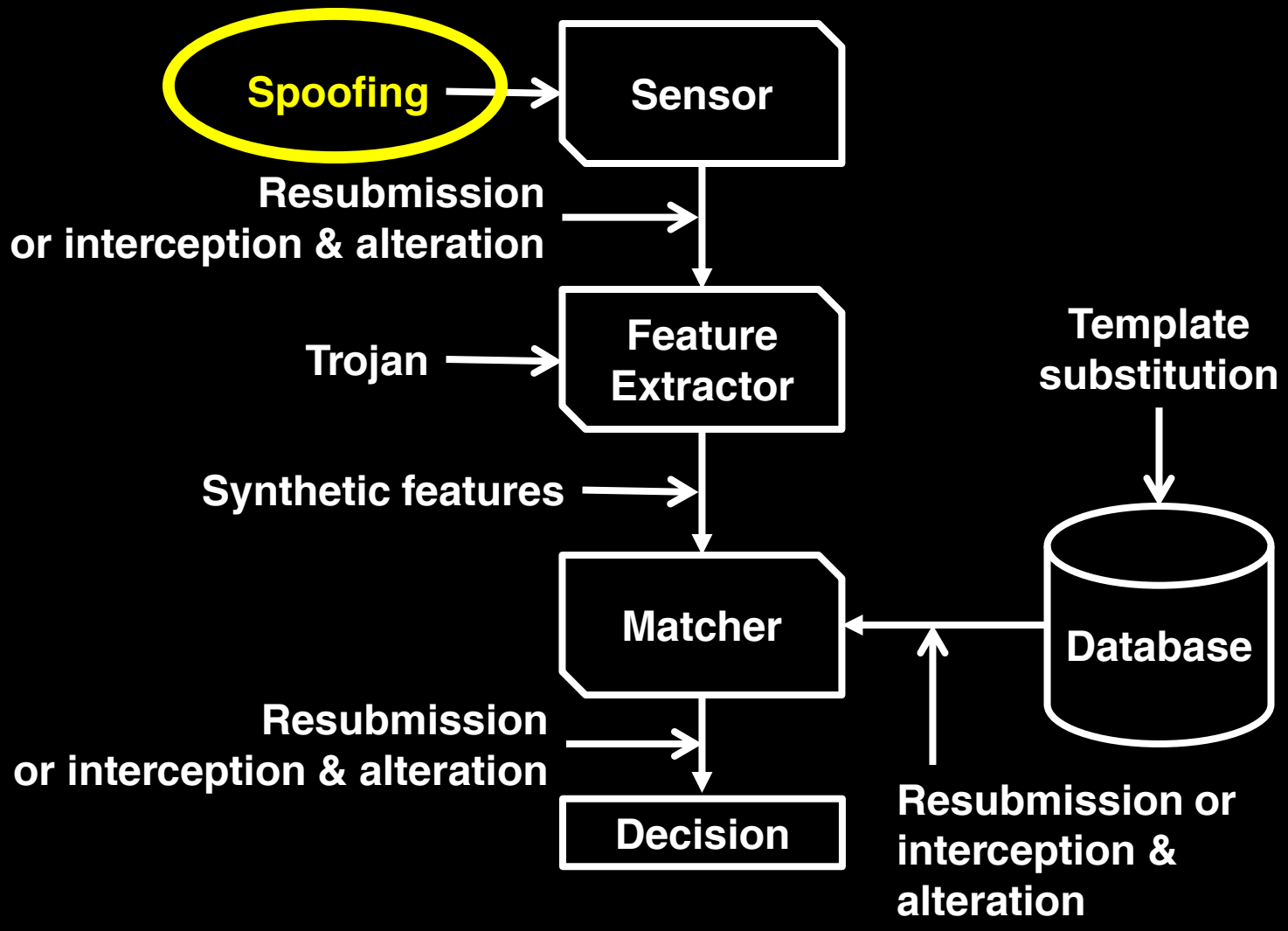
“I can get another credential.”

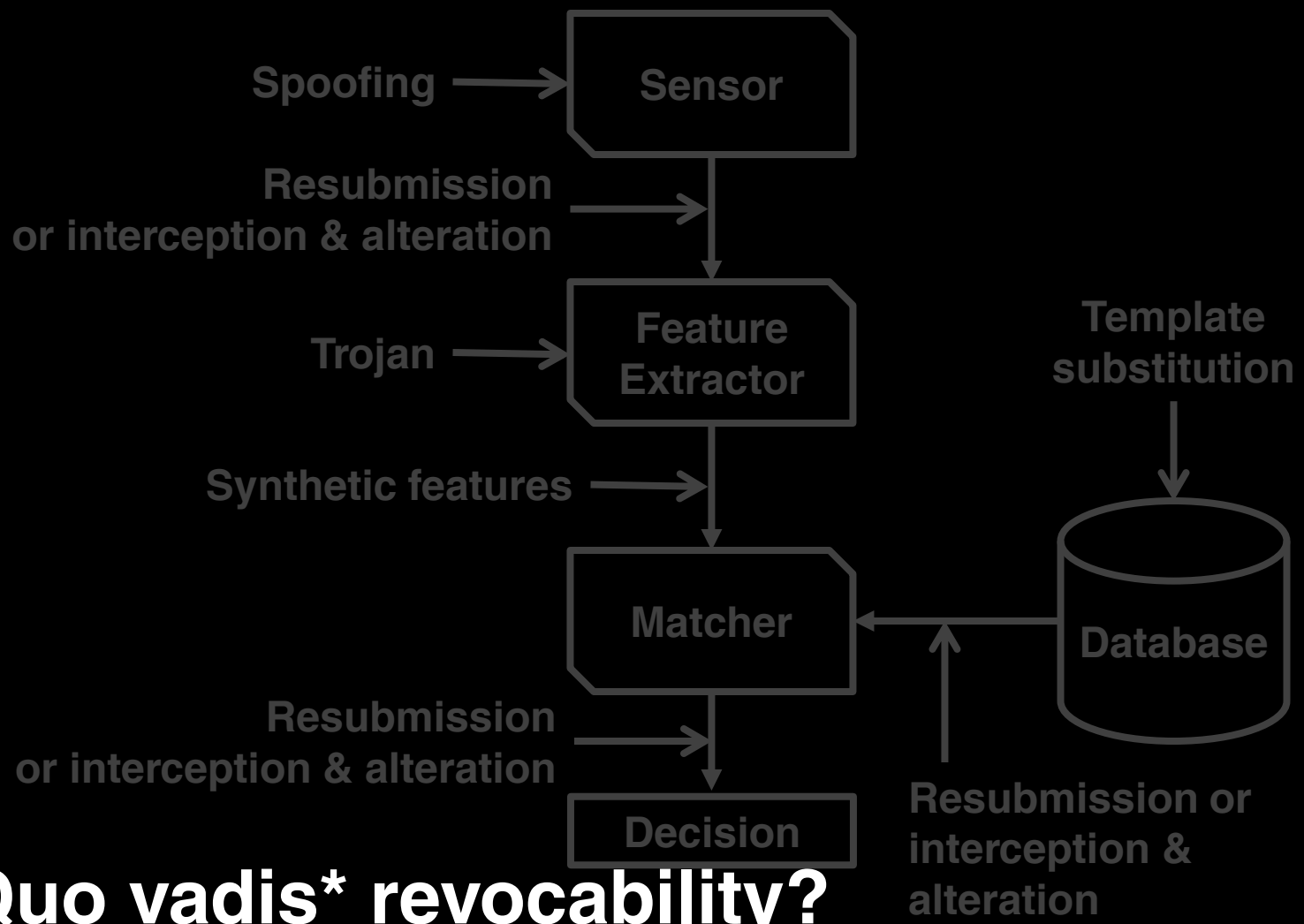
How can biometrics become a viable option for remote multifactor authentication?


Identity
Management
Biometrics
Cryptography

U. Uludag and A.K. Jain, “Attacks on biometric systems: a case study in fingerprints,” In *Proc. SPIE, Security, Steganography and Watermarking of Multimedia Contents VI*, volume 5306, pp. 622-633, 2004.

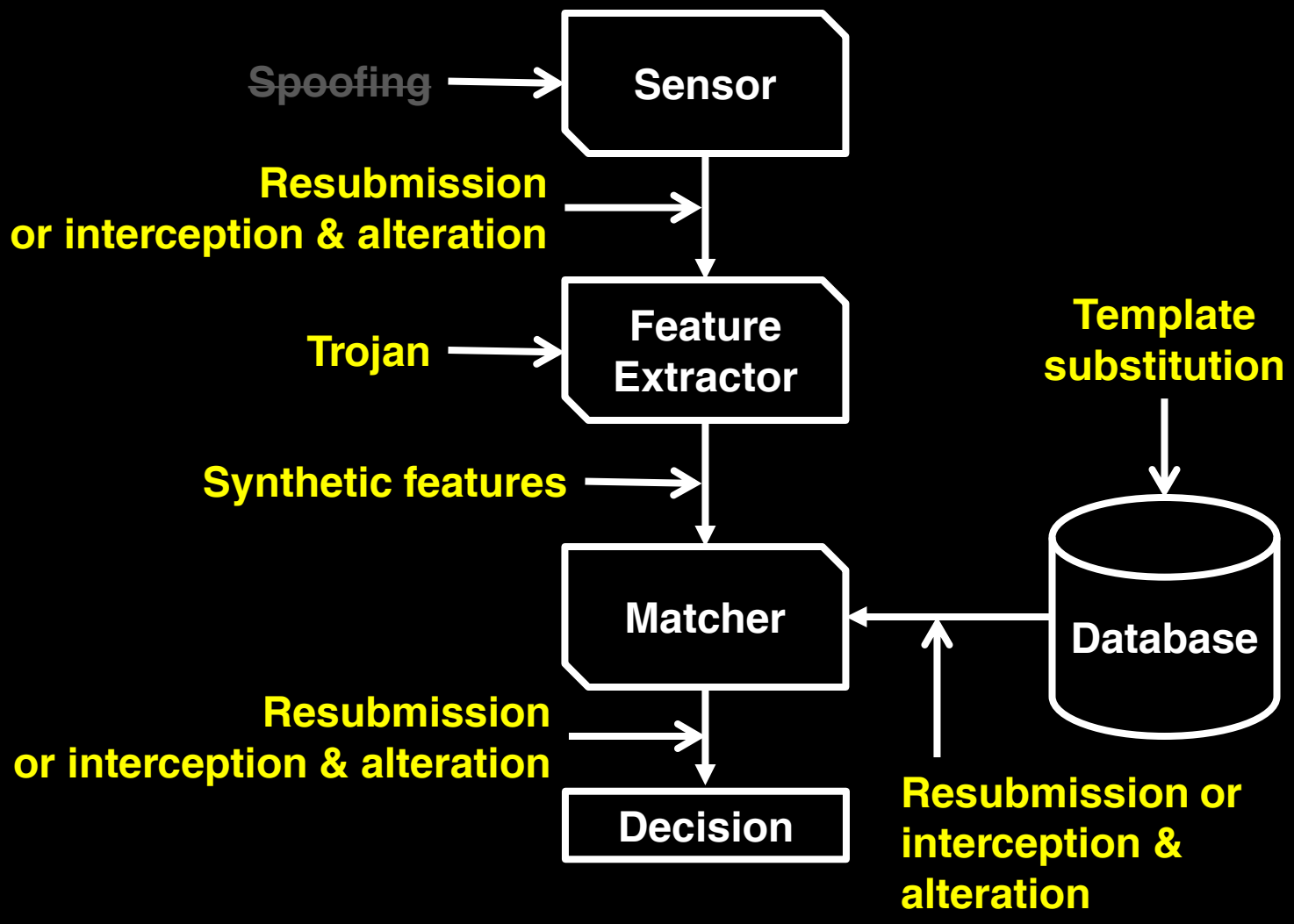

Spoofing
Sensor
Resubmission
or interception & alteration
Trojan
Feature
Extractor
Template
substitution
Synthetic features
Matcher
Database
Resubmission
or interception & alteration
Decision
Resubmission or
interception &
alteration


Spoofing
Sensor
Resubmission
or interception & alteration
Trojan
Feature
Extractor
Template
substitution
Synthetic features
Matcher
Database
Resubmission
or interception & alteration
Decision
Resubmission or
interception &
alteration



Quo vadis* revocability?

(Unnecessary use of Latin inspired by National Academies "Whither Biometrics" Project and related papers.)


Spoofing
Sensor
Resubmission
or interception & alteration
Trojan
Feature
Extractor
Template
substitution
Synthetic features
Matcher
Database
Resubmission
or interception & alteration
Decision
Resubmission or
interception &
alteration

Terrance Boult
University of Colorado at Colorado Springs

Stephanie Schuckers
Clarkson University

What does it mean to be “multifactor?”

Know

Have

Are

Transparent Hardware

Biometric Cryptographic Tokens

ross.micheals@nist.gov

Evaluation of Liveness or Anti-spoofing in Biometric Systems

Presented by Stephanie Schuckers

Contributors to the research; Bozhao Tan, Aaron Lewicke, Peter Johnson, Joseph Sherry, David Yambay, Rachel Wallace, Greta Collins, Dominic Grimberg, Laura Holsopple, Arun Ross, Emanuela Marasco

Funding provided by

National Institute of Standards and Technology (NIST), National Science Foundation (NSF), Dept. of Homeland Security (DHS), and the Center for Identification Technology Research (CITeR)

The Center for Identification Technology Research (CITeR)

Clarkson UNIVERSITY defy convention

NSF Industry/University *Cooperative* Research Center (IUCRC) focused on Integrative Identification Research since 2001

- *importance of individuals in a global society*

Research Scope – Physiological, Behavioral, and *Molecular* Biometrics. Current Emphasis:

- 2001: WVU Founding Site, MSU Partner, 5 Founding Affiliates
  - Automated Biometric Recognition
- 2006: University of Arizona becomes 2nd Site, 10+ Universities
  - Credibility, psychophysiological and behavioral deception detection
- 2010: Clarkson Plans 3rd Site, over 20 Affiliates
  - Logical and cyber identity, intelligence

CITeR's Affiliates

- Accenture
- Booz Allen Hamilton
- Computer Science Corporation
- DIA/DACA-Defense Academy for Credibility Assessment
- Department of Defense—Biometric Task Force
- Department of Defense—DDR&E
- Department of Defense—USSOCOM/SOALT
- Department of Homeland Security—S & T 3 memberships (1 Clarkson)
- BORDERS DHS COE
- Federal Aviation Administration, Information Systems Security (2 memberships)
- Federal Bureau of Investigation
- Irvine Sensors

- Laurea Ltd.
- Lockheed Martin
- National Institute of Standards and Technology (NIST)--pending
- National Security Agency 2 organizations (1 Clarkson)
- Northrop Grumman
- OU Center for Applied Social Research
- Raytheon (2 organizations)
- Morpho Trac Inc.
- Sandia National Labs
- SRC
- Science Applications International Corporation (SAIC)
- US Army Picatinny Arsenal
- US Army CERDEC/SBInet Indep. Test Team
- West Virginia High Technology Consortium Foundation

Spoofing

- In 2009, publicized fingerprint spoof attack at Japanese border by a Korean woman
- Highlighted vulnerability in fingerprint systems used for identity management
- Number of successful spoofing events is unknown

Spoofing

- **Spoofing: "The process of defeating a biometric system through the introduction of fake biometric samples.**
- **Artificially created biometrics:**
  - lifted latent fingerprints
  - artificial fingers
  - image of a face or iris
  - high quality voice recordings
  - worst case—dismembered fingers
- **Famous 'gummy fingers' by Matsumoto 2002**
- **Mythbusters episode in 2007**
- **Spoof attack in early 2009 at Japanese border by a Korean woman**

Biometric Spoofing in Popular Media

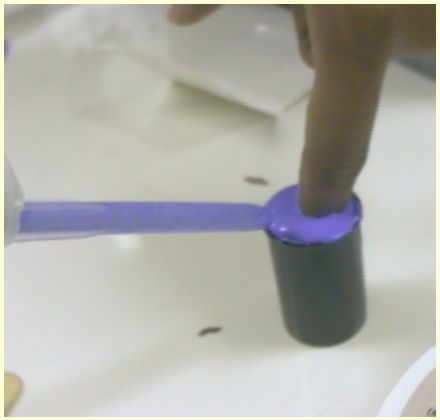
Tom Cruise, Minority Report

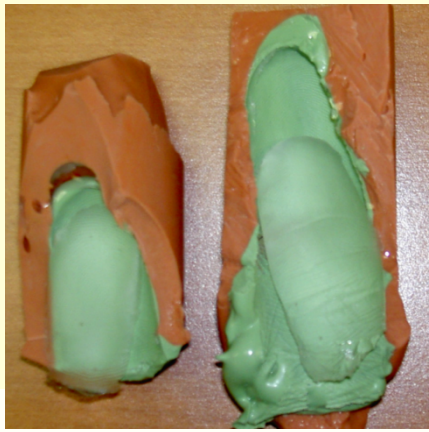
Cameron Diaz, Charlies Angels

Mythbusters, 2007

Spoofing Techniques in our Lab

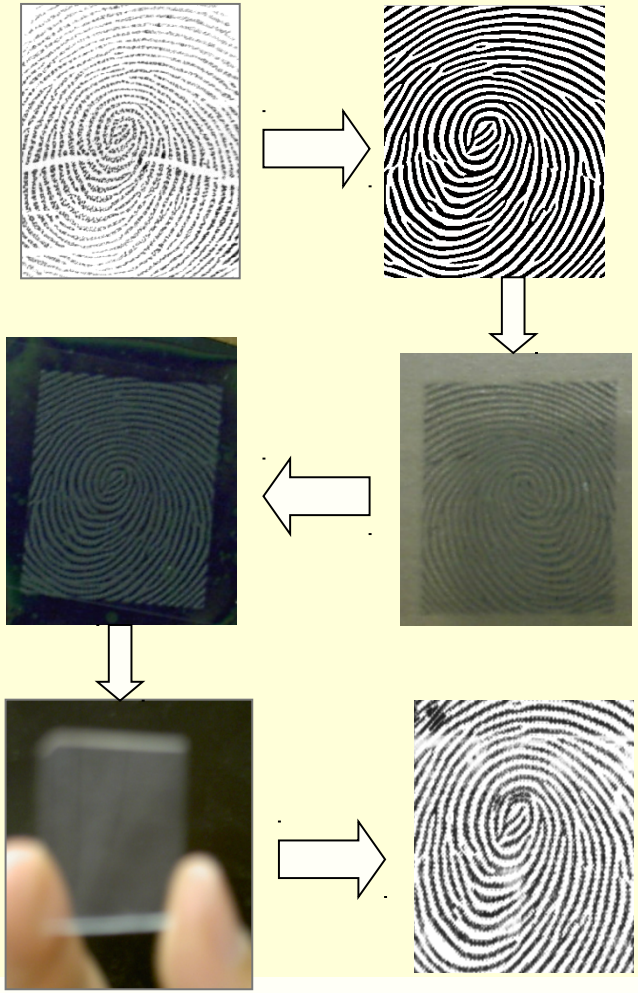
- Dental materials for casts
- Cooperative, high quality casts
- Mold made from cast, also termed ‘replica’, ‘spoof’, ‘fake finger’
- Materials for Mold: Play-Doh, gelatin, silicon rubber, paint, caulk, wood glue, paper, latex rubber, paper
- Cadaver fingers





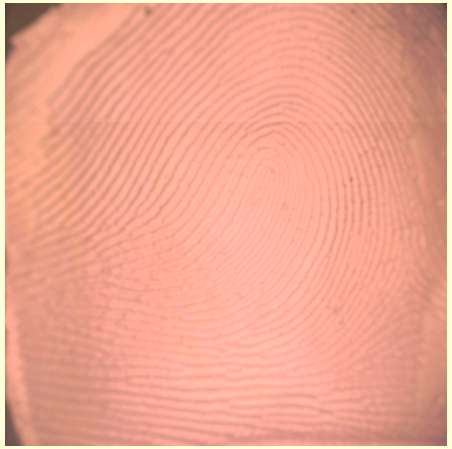
Spoof Techniques in our Lab

- Uncooperative
- Lifted latent print, stolen fingerprint image
- Fingerprint mask generation
- Print on transparent film
- Expose negative photosensitive silicon wafer
- Develop to form cast
- Pour silicone or other liquid material to form mold



Example Photos of Spoof Fingers

Caulk



Paint

Playdoh

Silicon

Photos of spoof fingers made from various materials

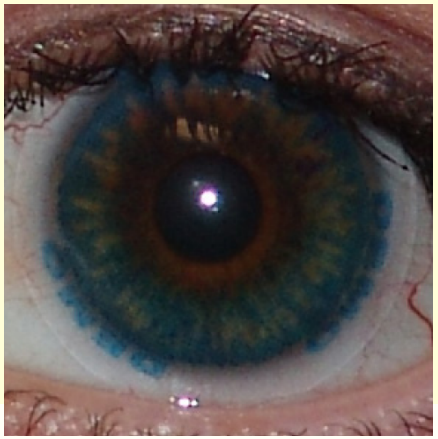
Same scanner (optical)
Different spoof materials

Top row, left to right:
latex painter's caulk.
gelatin,
latex paint.

Bottom Row:
playdoh.
latex rubber.
silicon.

Spoofing versus Obfuscation

- **Spoofing—posing as another individual**
  - Positive identification applications
- **Obfuscation—hiding your identity**
  - Negative identification applications
  - May form ‘new’ identity for positive identification
  - Mutilation of fingerprint
  - Texture-contact lens to hide iris pattern
  - Theatre makeup/putty to change facial characteristics



Minimizing Spoofing Risk

- **Application-specific risk assessment**
  - What is the role of biometrics in my application? (Is it needed?)
  - Does it improve upon former methods of identity management?
  - What is the impact of spoofing vulnerability?
  - What is the public perception of spoofing vulnerability?
- **Ways to mitigate risk**
  - Multi-factor authentication—password, smart card
  - Multi-biometrics—require multiple biometrics
  - Liveness detection or anti-spoofing

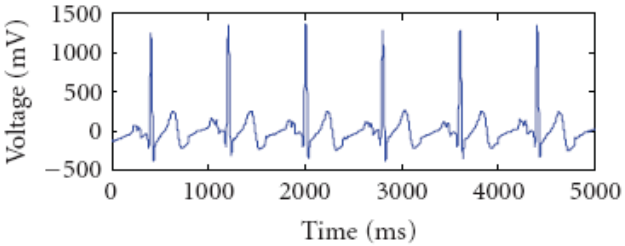
Liveness Detection

- **Also termed**
  - 'Vitality Detection'
  - 'Anti-Spoofing'
- **Definition: to determine if the biometric being captured is an actual measurement from the authorized, live person who is present at the time of capture**
- **"It is 'liveness', not secrecy, that counts," Dorothy Denning**
  - Your fingerprint is NOT secret.
  - Cannot reasonably expect it to be absolutely secret
  - Therefore, must ensure measurement is of the 'real' biometric and not a replica.
  - True for most other biometrics, with some exceptions to be discussed
- **Typically treated as a two class problem—live or spoof**

Liveness Detection

- **Rarely does biometric sensor measure 'liveness', that is, liveness is not necessary to measure the biometric**
- **Hardware-based**
  - Requires specialized hardware design
  - Integrated with biometric sensor
- **Software-based**
  - Uses information already measured from biometric sensor
  - Additional processing needed to make a decision
- **Liveness inherent to biometric**
  - Must be 'live' to measure it, e.g., electrocardiogram

- M2SYS-M2-S1



(a) 5 seconds of ECG from subject A

Hardware-based Fingerprint Liveness Detection

- **Hardware-based**
  - Temperature
  - Pulse
  - Blood pressure
  - Odor
  - Electrocardiogram
  - Multispectral imaging, spectroscopy
- **Should be integrated carefully so spoof cannot be combined with any live finger to be accepted**
  - e.g. translucent spoof fooling light-absorption-based pulse oximeter

- The Lumidigm J110 Anti-Spoof scanner
- MultiSpectral imaging with varying illumination and polarization

Example Hardware: Multispectral

The Lumidigm J110 Anti-Spoof scanner

- MultiSpectral imaging with varying illumination and polarization
- Commercial system which protects from spoofing
- Hardware approach
- Tradeoff—larger and more expensive

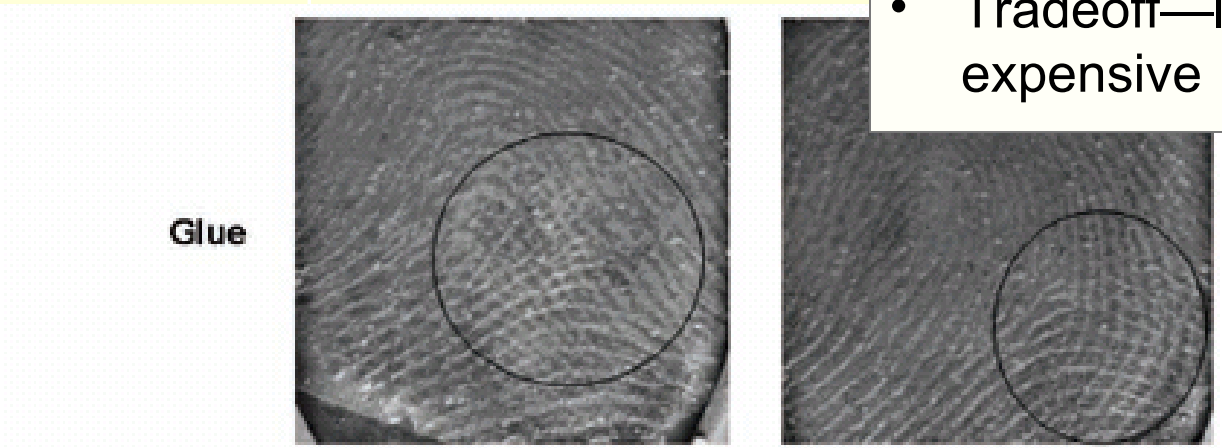
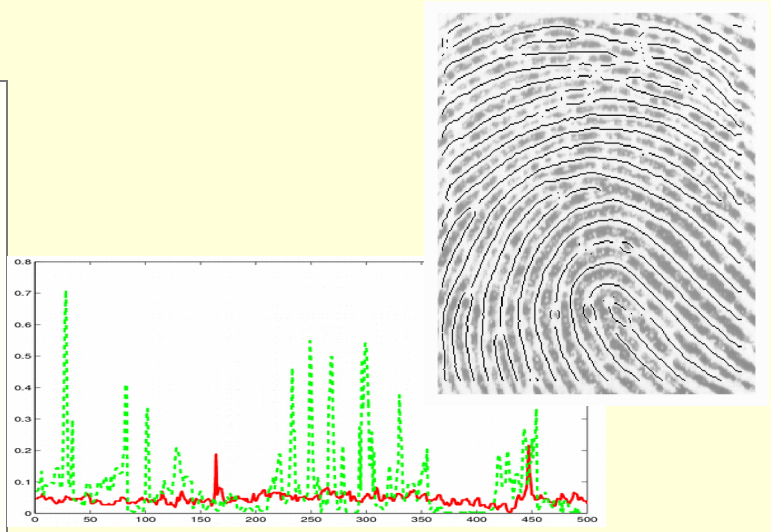


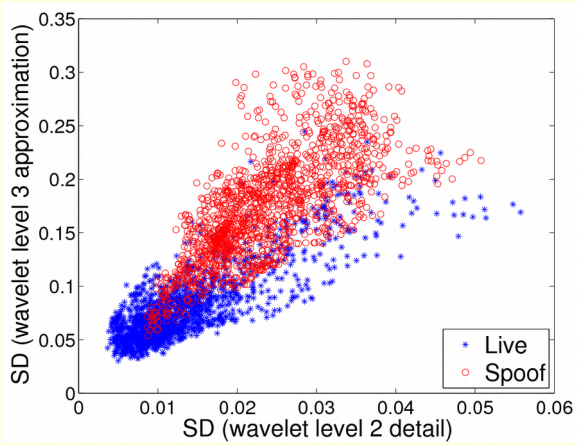
Fig. 9. Example images of various thin, transparent spoofs placed on real fingers. The elliptical marks highlight areas in which unnatural textures are clearly apparent. The automated texture analysis techniques incorporated in the MSI sensor are sensitive to much subtler variations of texture.

Rowe et al. Advances in Biometrics, 2008,

Software-based Fingerprint Liveness Detection

- **Examples proposed**
  - Skin deformation
  - Elasticity
  - Pores
  - Perspiration pattern
  - Power spectrum
  - Noise residues in valleys
  - Combining multiple features
- **Must represent variability of live subjects (dry, moist, variable environments, ages, ethnicity)**
- **Reliance on the properties of spoof materials**
- **Must stay one step ahead of would-be attacker—software upgrade**



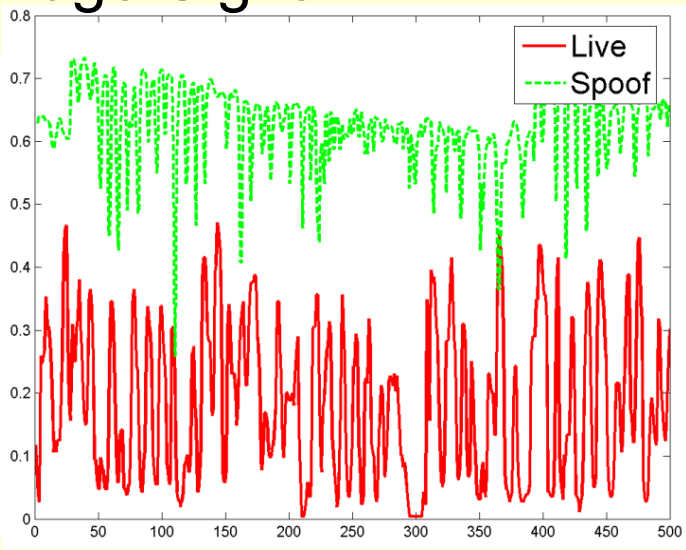


Example Software: Ridge/Valley Features

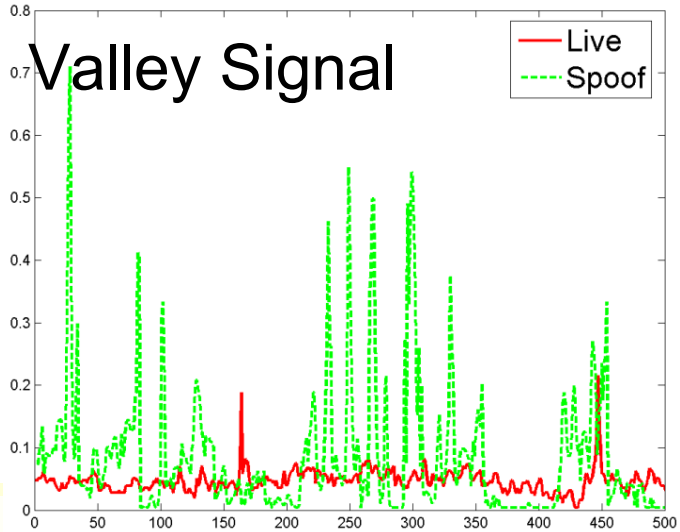
Clarkson UNIVERSITY

- Relies on differences in ridge/valley structure between live and spoofs
- Uses features measured from ridges and valleys separately
- Sensitive to the sensor being used
- Impacted by environmental conditions
- Must represent large diversity in both spoof and live images

Ridge Signal

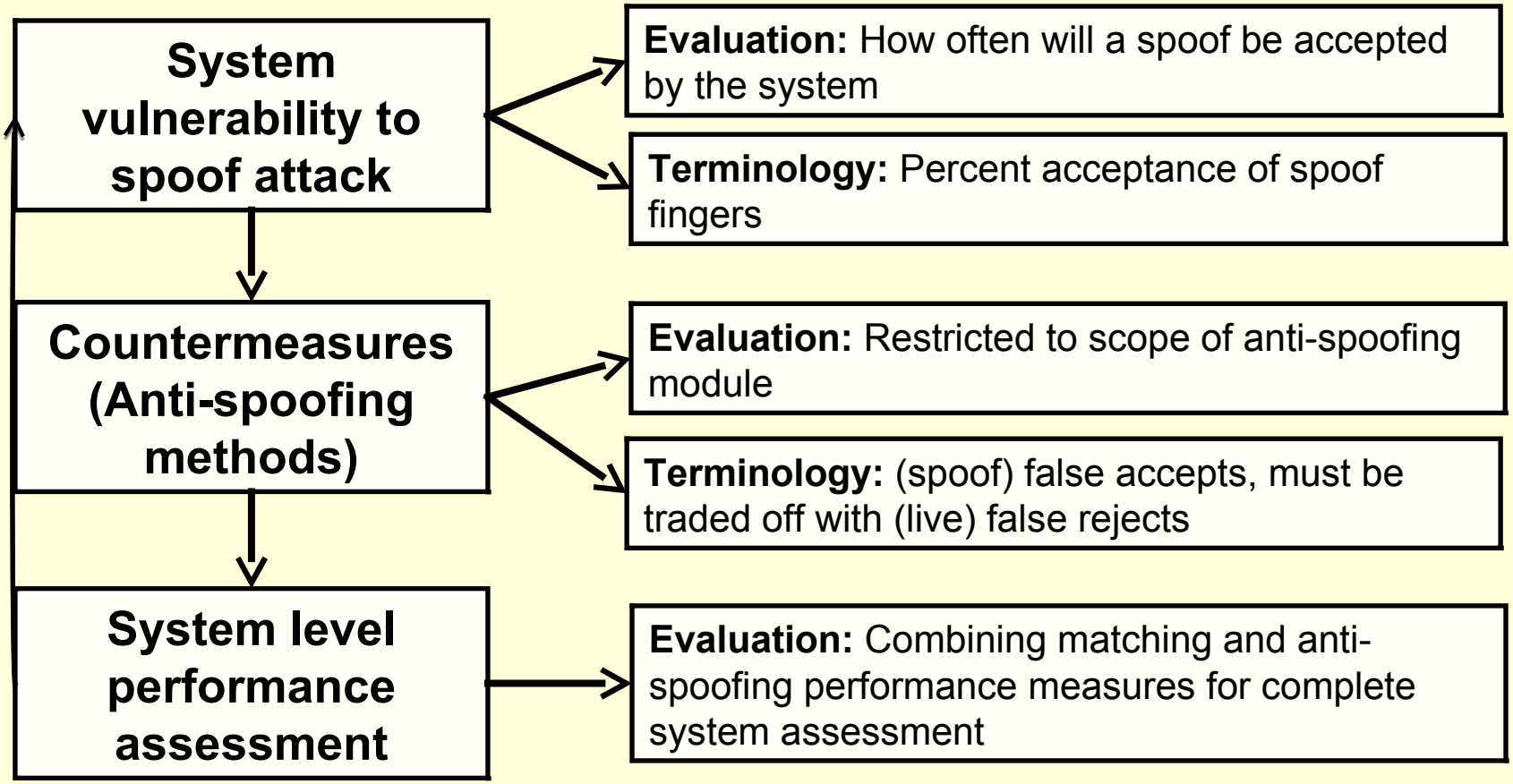


Valley Signal



Tan, et al, CVPR, 2006
Ulchida, et al, LN in CS, 2004

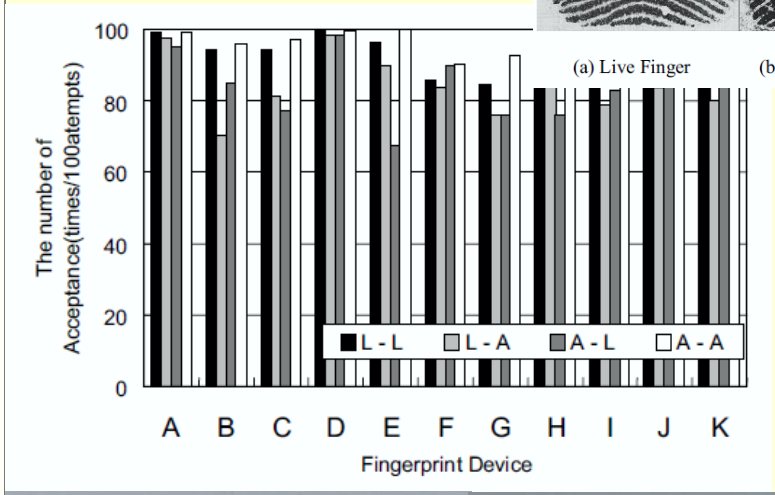
Assessment of Spoofing Vulnerability and Countermeasures

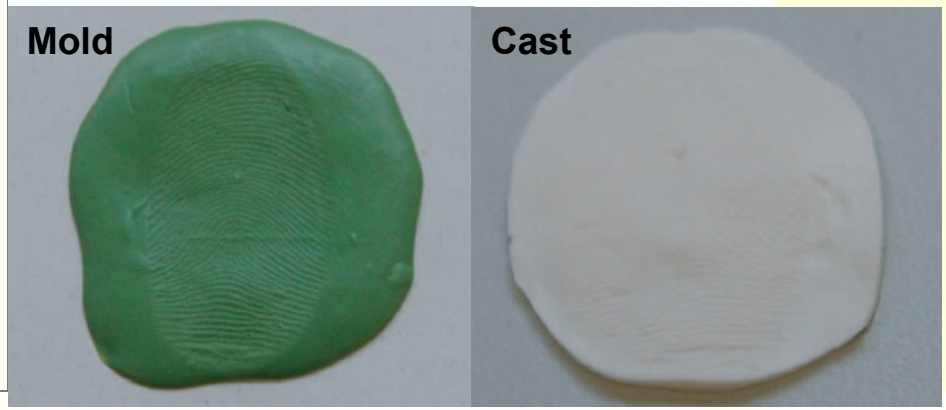


Spoof Testing on Conventional Systems

- **Matsumoto et al., 2002**
  - Method: (1) enroll live, test live; (2) enroll live, test spoof; (3) enroll spoof, test live; (4) enroll spoof, test spoof (all genuine matches)
  - Data: Live, silicone, and gelatin fingers
  - Evaluation: Percent accepted in terms of matching performance
- **Galbally et al., 2006**
  - Method: (1) enroll and test with live fingers; (2) enroll and test with spoof; (3) enroll live, test spoof
  - Data: Live and silicone fingers
  - Evaluation: FAR and FRR in terms of matching performance

(a) Live Finger (b) Gummy Finger





Testing of Liveness Algorithm Module

Algorithm	No. Spoofs	No. Live	No. impressions	No. frames	Live Performance	Spoof Performance
Perspiration with Fourier space	18	18	1	2	88.89%	88.89%
Surface coarseness	10 gelatin 24 plastic clay	23	1	1	100%	100%
Distortion Analysis	40 (10 silicone, 10 gelatin, 10 latex, 10 wood glue)	45 (2 fingers)	10	20	88.76%	88.76%
Perspiration with wavelet space	80	58	1	1	80% - 100%	80% - 100%

State of Liveness Performance Evaluation

- Performance metrics for biometric systems – adapted unmodified for anti-spoofing assessment
  - Classification rate (percent correctly classified)
  - FAR/FMR – false accept rate/false match rate
  - FRR/FNMR – false reject rate/false non match rate
  - TAR/GAR – true accept rate/genuine accept rate
  - EER – equal error rate
  - ROC – receiver operating characteristic
  - DET – detection error trade-off
- Need to distinguish "**false accepts**" in ***matching*** from "**false accepts**" in ***spoofing***
  - Need common set of vocabulary

Performance Vocabulary

- **Biometric performance terminology**
  - False reject rate—Error associated with rejecting an ‘genuine’ user
  - False accept rate—Error associated with accepting an un-authorized, ‘imposter’ user
    - Zero-effort attempt—no willful attempt
- **Anti-spoofing terminology**
  - ***False reject rate***—similar to above, now anti-spoofing detection algorithm may reject ‘genuine’ authorized user
  - ***Spoof false accept rate***—error associated with accepting the presentation of a spoof
    - Non-zero effort attempt—willful attempt

State of Liveness Performance Evaluation

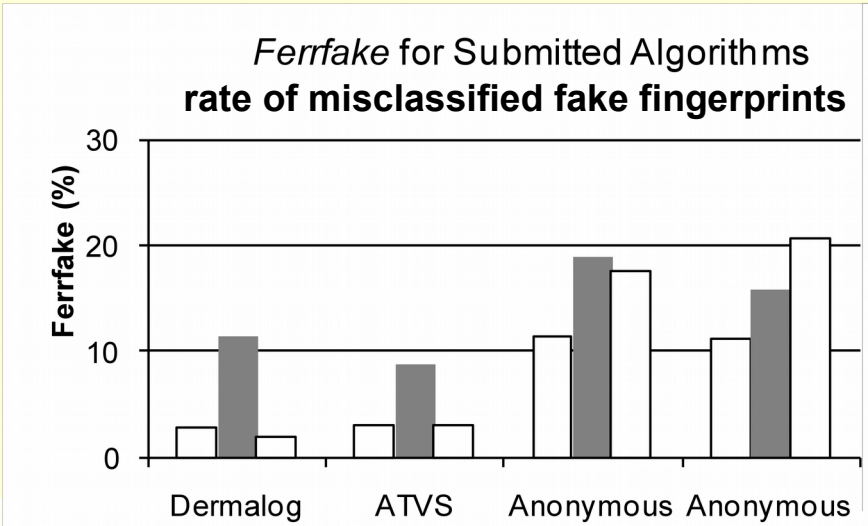
- Need for performance metrics to assess liveness and systems which incorporate liveness
- Need to distinguishing false accepts in matching from spoof false accepts
- Must be clear on anti-spoofing impact on false reject rates
- Fusion of match scores and “liveness” scores

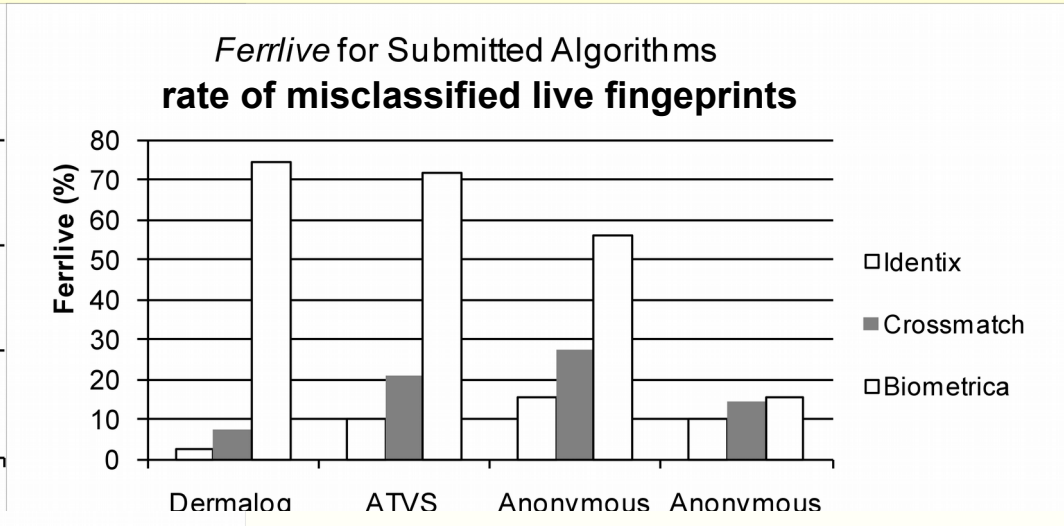
Next issue

- Testing procedures—it depends on how you perform spoofing

Liveness Detection Competition—LivDet 2009

- ***First liveness detection competition at ICIAP 2009 with a public liveness database***
- Collaboration with Univ. of Cagliari
- Focusing on software-based fingerprint liveness
- Scanners used: CrossMatch, Identix, Biometrika
- 2000 live and spoof samples for each scanner
- Four participants





Announcing LivDet II

- To compare different methodologies for software-based and system-based fingerprint liveness detection
  - Algorithm—training set provided, sequestered test set
  - System—hardware/software system submitted and tested
- To become a reference event for academic and industrial research in software-based and system-based fingerprint liveness detection
- To raise the visibility of this important research area in order to decrease risk of fingerprint systems to spoof attacks
- Results to be presented as part of International Joint Conference on Biometrics (IJCB) 2011

Factors impacting performance testing

- Material for spoof
- Material for mold
- Variability in recipes
- Individual variability
- “Spoofer” variability
- Number of attempts
- Placement, pressure, etc.
- Cooperative or non-cooperative collection of fingerprint pattern
- Known versus unknown attacks

Others developing methods for performance assessment of liveness

- **Communications-Electronics Security Group (CESG)**
  - Branch of Government Communications Headquarters (GCHQ) – UK
  - Developing a methodology for biometric security testing
- **Federal Office for Information Security (BSI) – Germany**
  - Common Criteria Certification
  - Protection Profiles for anti-spoofing evaluation
- **Korea Information Security Agency**
  - Methodology designed to evaluate the objective performance of spoof detection technology
- **Developing ISO Standards**

Liveness Methods Impact on Standard Biometric Characteristics

- **Ease of Use**
  - Dynamic, time delay
  - User assisted
- **Collectability**
  - User assisted
- **User acceptance**
  - Measurement which requires medical information may not be acceptable to individuals
- **Universality**
  - Perspiration differences may not be measurable in some individuals
  - Some individuals require lotion for fingerprint
- **Permanence**
  - Environmental impact

Conclusions

- Spoof FAR needs to be considered for non-zero effort false accept
  - FAR accounts only for zero effort false accept rate
  - Real spoof attempts are ‘rare’ events, likely much smaller than error with detection
  - Can be used as a flag to ‘secondary’
- Testing
  - Common terminology
  - Agreed upon framework for testing
  - Standards for levels of assurance
  - System level versus module level testing
- Liveness detection or anti-spoofing will impact overall performance of biometric system

Clarkson UNIVERSITY

Thank you!

Questions?

References

- C. Jin, H. Kim, S. Elliot, “Liveness Detection of Fingerprint Based on Band-Selective Fourier Spectrum,” *Lecture Notes in Computer Sciences,* vol. 4817, pp. 168-179, 2007.
- K. Uchida, “Image-Based Approach to Fingerprint Acceptability Assessment,” *Lecture Notes in Computer Sciences,* pp. 294-300, 2004.
- A. Antonelli, R. Cappelli, D. Maio, D. Maltoni, “Fake Finger Detection by Skin Distortion Analysis,” *IEEE Transactions on Information Forensics and Security,* vol. 1, no. 2, pp. 360-373, September 2006.
- J. Jia, L. Cai, “Fake Finger Detection Based on Time-Series Fingerprint Image Analysis,” *Lecture Notes in Computer Sciences,* vol. 4681, pp. 1140-1150, 2007.
- Parthasaradhi S, Derakhshani R, Hornak L, Schuckers SAC, Time-Series Detection of Perspiration as a Liveness Test in Fingerprint Devices, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 35, pp. 335- 343, 2005.
- B Tan, S Schuckers, Liveness Detection for Fingerprint Scanners Based on the Statistics of Wavelet Signal Processing, Computer Vision and Pattern Recognition Workshop, 2006 Conference on, Page(s):26 – 26, 17-22 June 2006.
- Baldisserra, Denis, Annalisa Franco, Dario Maio, and Davide Maltoni. “Fake Fingerprint Detection by Odor Analysis ,.” In Advances in Biometrics, 265-272, 2005.

References--continued

- C. Jin, H. Kim, S. Elliot, “Liveness Detection of Fingerprint Based on Band-Selective Fourier Spectrum,” *Lecture Notes in Computer Sciences,* vol. 4817, pp. 168-179, 2007.
- Miura, Naoto. “Feature Extraction of Finger Vein Patterns Based on Iterative Line Tracking and Its Application to Personal Identification.” 29 June 2009.
- Wubbeler, Gerd. “Verification of Humans using the Electrocardiogram.” 26 June 2009.
- Rowe, Robert K., Paul W. Butler, and Kristin A. Nixon. "Multispectral Fingerprint Image Acquisition." Advances in Biometrics, 2008.
- Andy Adler, Stephanie Schuckers, Security and Liveness: Overview, in Encyclopedia of Biometrics, editor: Stan Li, Springer Reference, 2009.
- Stephanie Schuckers, Liveness: Fingerprint, in Encyclopedia of Biometrics, editor: Stan Li, Springer Reference, 2009 .

Addressing Privacy and Security Research Challenges for Biometric Authentication via the BKI: Biocrytographic Key Infrastructure

Terrance E. Boult

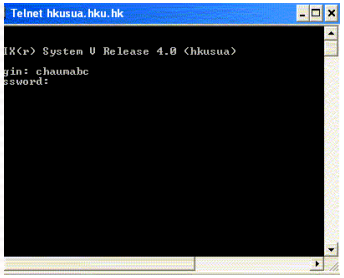
El Pomar Professor of Innovation and Security
University of Colorado at Colorado Springs
and
CEO/CTO Securics Inc

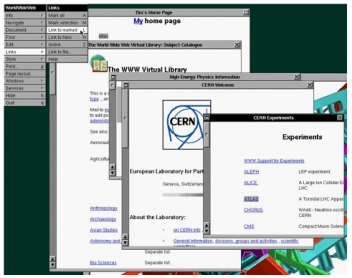
tboult@securics.com 719 963 0573 (Cell)

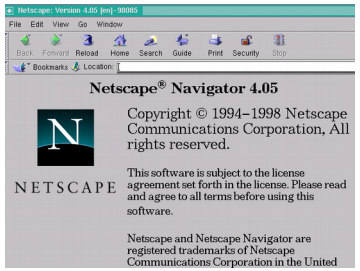
Securics®

Engineering Entrepreneurship Communications Globalization
UCCS
Bachelor of Innovation™
www.innovation.uccs.edu

Remember the 80s and 90s?







- Huge explosion in new Internet protocols
  - Email, Remote Connections, The Web,…
- Security of these protocols was an afterthought!
  - We need cryptography to protect insecure channels
  - How can Alice verify a server?
  - How do we share encryption keys?

Solution: Public Key Infrastructure

Online Identity Problems…

- Public Key Infrastructure enabled early e-commerce through secure communication
- But Identity and transactions are between people, not machines. How do we "certify" parties in a transaction? ID/Passwords?
  - **Certificates help machines, few people.**

  - **How many people even know what is a valid certificate?**
  - **Malware/Bot attacks directly capture passwords from machine and browser, sidestepping PKI certificates**

PKI resolve <u>Identity</u> by what you have

What makes an ID trusted?

1. Good protocols for ID management.
2. Strong (levels of) assurance that only intended users can use that ID. (Verifier)
3. *Strong link between claimed identity and other attributes (bank account, age, schooling, etc..) (Registration authority)*
4. *Validity of registration authority/delegate*
5. *Must have liability for failures in #1-3*

Identity Limitations of PKI

- Ellison and Schneier (2000)*
  - "Risk #1: Who do we trust, and for what?"
  - "Risk #2: Who is using my key?"
  - "Risk #4: Which John Robinson is he?"
  - "Risk #6: Is the user part of the security design?"
  - "Risk #8: How did the CA identify the certificate holder"?

*C. Ellison and B. Schneier, "Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure," *Computer Security Journal*, 16(1):1-7, 2000.

“Three factor” of Authentication security

1. ***Something you know (passwords,attributes)***
   Easily changed, easily shared,
   moderate/easy forgotten/lost

2. ***Something you have (e.g. card, cert)***
   Moderate to change, moderate to share
   easily forgotten/lost

3. ***Something you “are” (e.g. biometric)***
   Hard to share, hard to forget/lost,
   Traditionally impossible to change!

Traditional Biometric "Security"

Standard Templates ARE effectively invertible!

Vendor claims of security because templates are are "non-invertible" is like saying a noisy ROT13 is encryption:

formally true, practically meaningless.

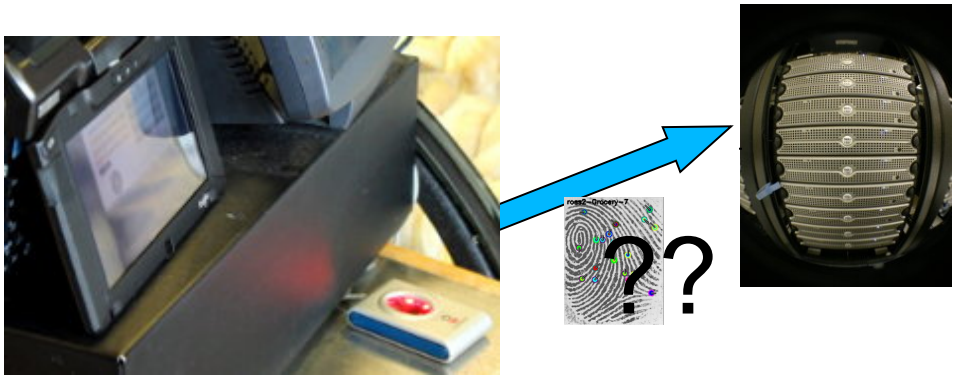
Recovering images from ISO minutiae templates allowed successful attacks against nine different systems

- 81% highest security
- 90% normal security

Wong/Jain ICB09 improved to > 95% .

Cappelli et al. PAMI, Sept. 2007
http://biolab.csr.unibo.it

Biometrics for Verified Web-Identity?



Biometrics provide identity assurance, convenient & low cost but

- Cannot revoke a fingerprint like a password or credit card!
- Like symmetric encryption both sides need the “secret”
- Only matching party can really trust match happened, other party must trust the matcher with their data!

The TRUSTED identity on the web needs a radically different and asymmetric identity approach.

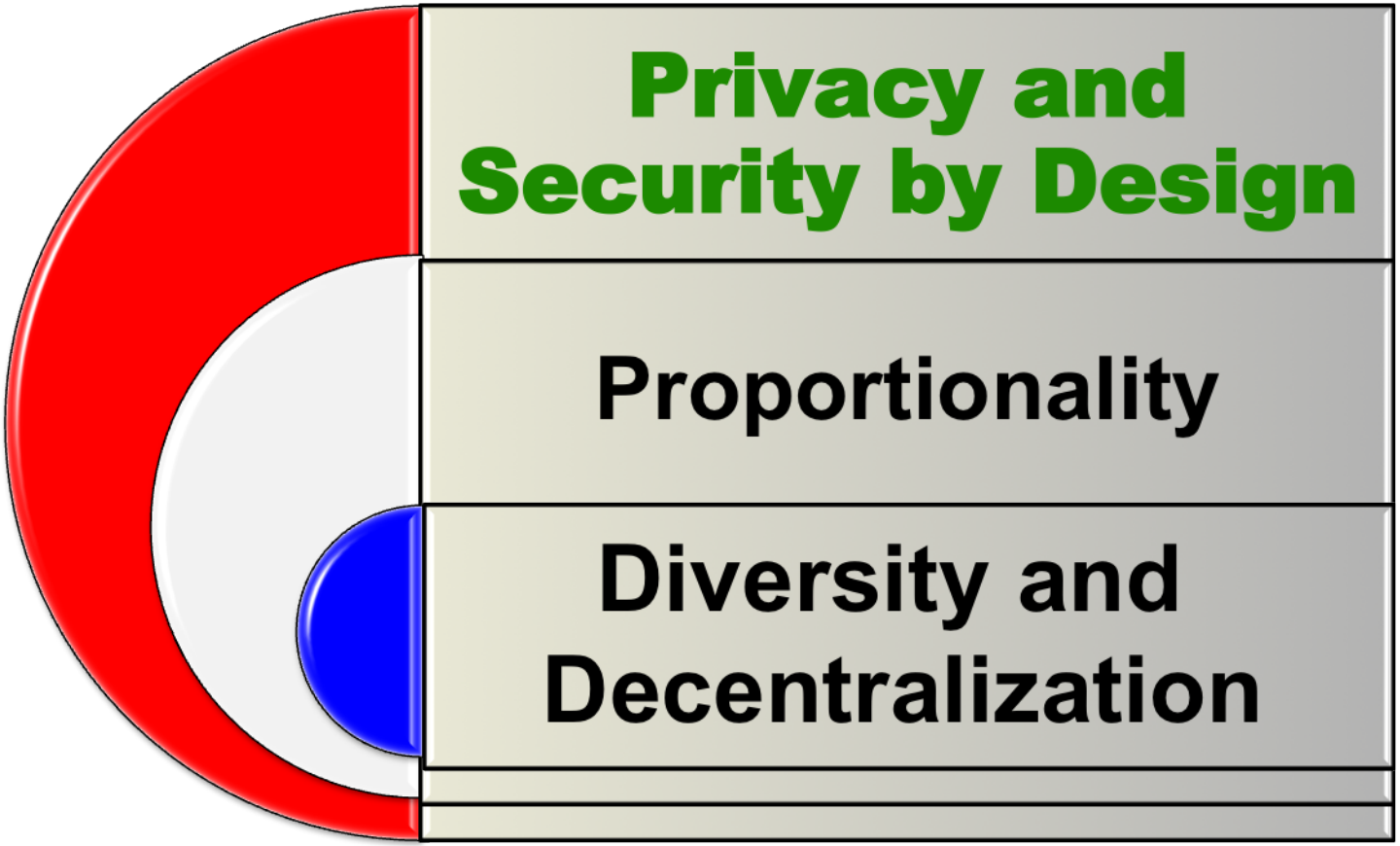
Biometrics and Security

- Traditional biometrics must be decrypted to match
- Even if not a “secret”, it still must be protected
- Cannot change/revoke traditional biometrics.
- Strong personal identity, and only strong solution to detect attempts to have multiple identities.

Biometrics and Privacy

- Concerns of Function creep
- Cross DB linking/Surveillance.
- Improper impact of innocents from false-matches
- Some issues addressed by revocable/cancellable biometrics, fuzzy extractors & other template protection technology

National Workright Institute Guidelines for IMS



What you are: online requirements

TB's Requirements for effective biometric-based identity for web:

1) Asymmetric with strong 2-party confirmed non-repudiation

2) Revocable with different token on each transaction!

3) Support for multi-factor "verification only" tokens (no search)

4) Protocols that never send biometric data or tokens from client machine (Enrollment is special case)

5) Strong "verification" of individual issuing credentials

6) Application or even transaction specific accuracy support

7) Should support but not need "central" identity management.

8) Should support various levels of "Spoof" Detection

9) Should support option of secure sensor communication

10) Low-cost or a range of costs

Case Study: Revocable Biotokens

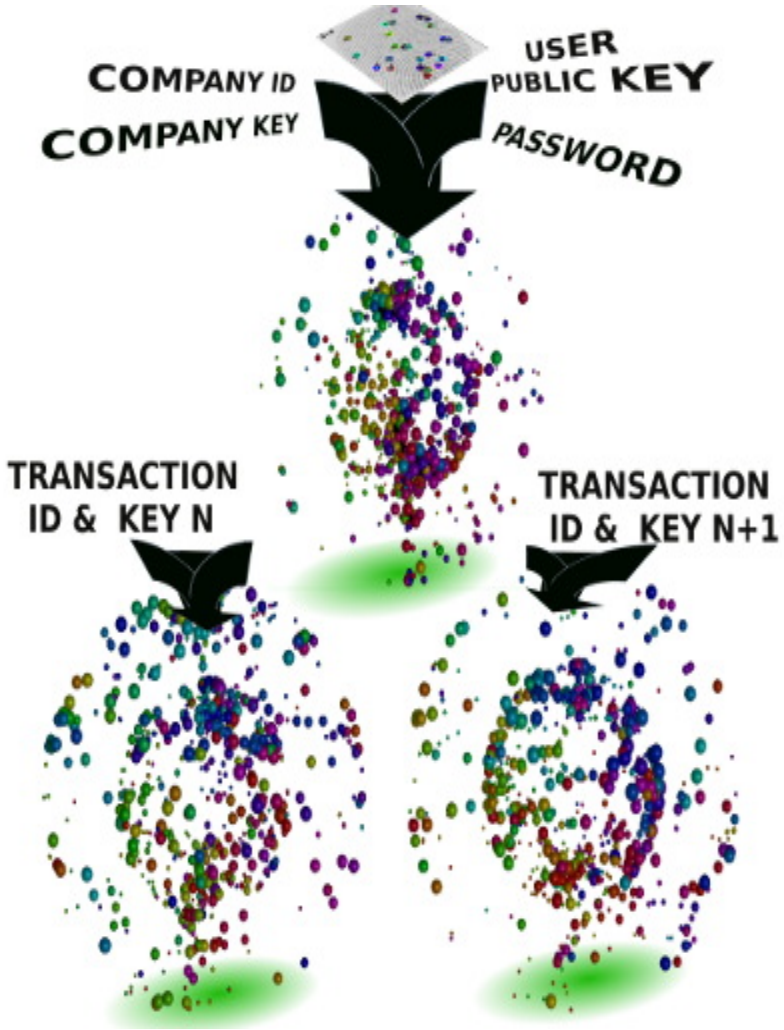
- Boult et al. 2007*
  - Assume a biometric produces values v Each is transformed via scaling and translation " $v' = (v - t) * s$
  - Split v' into stable component q and residual component r
  - For user j, leave the residual obscured: $r_j(v')$
  - Encrypt q with public key or hash P : $w_{j,1}(v', P)$

*T. Boult, W. Scheirer and R. Woodworth, "Revocable Fingerprint Biotokens: Accuracy and Security Analysis," CVPR 2007.

The Biotope Biotoken

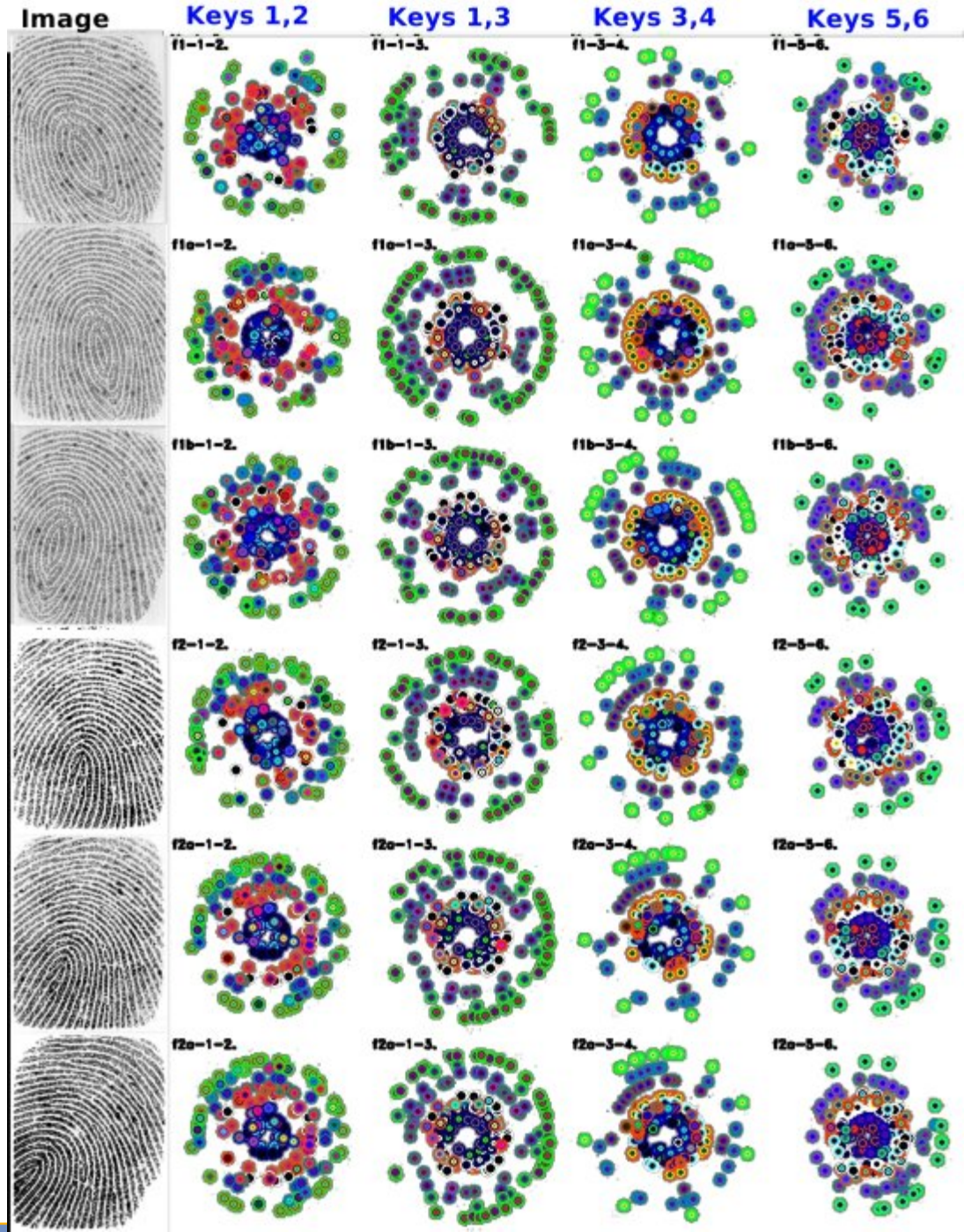
Multi-factors are mixed

- **Base Biotope mixes biometric data, Company ID/Key , User Public Key.**
- **Uniquely addresses issues of protecting noisy biometric data**
- **Can re-transform with transaction ID and embedded new keys for each traction.**
- **Can have a multiple non-searchable BKI databases**



Biotope Visualization

- Each column is different keys.
- Note the differences across keys for same image!
- Keys more similar than “people”!
- Revoke by changing any key



Securics

Nesting Property

- w_j is re-encoded using a transformation function T

  1st encoding: $w_{j,1}(v', P)$

  2nd encoding: $w_{j,2}(w_{j,1}, T_2)$

  nth encoding: $w_{j,n}(w_{j,n\text{-}1}, T_n)$

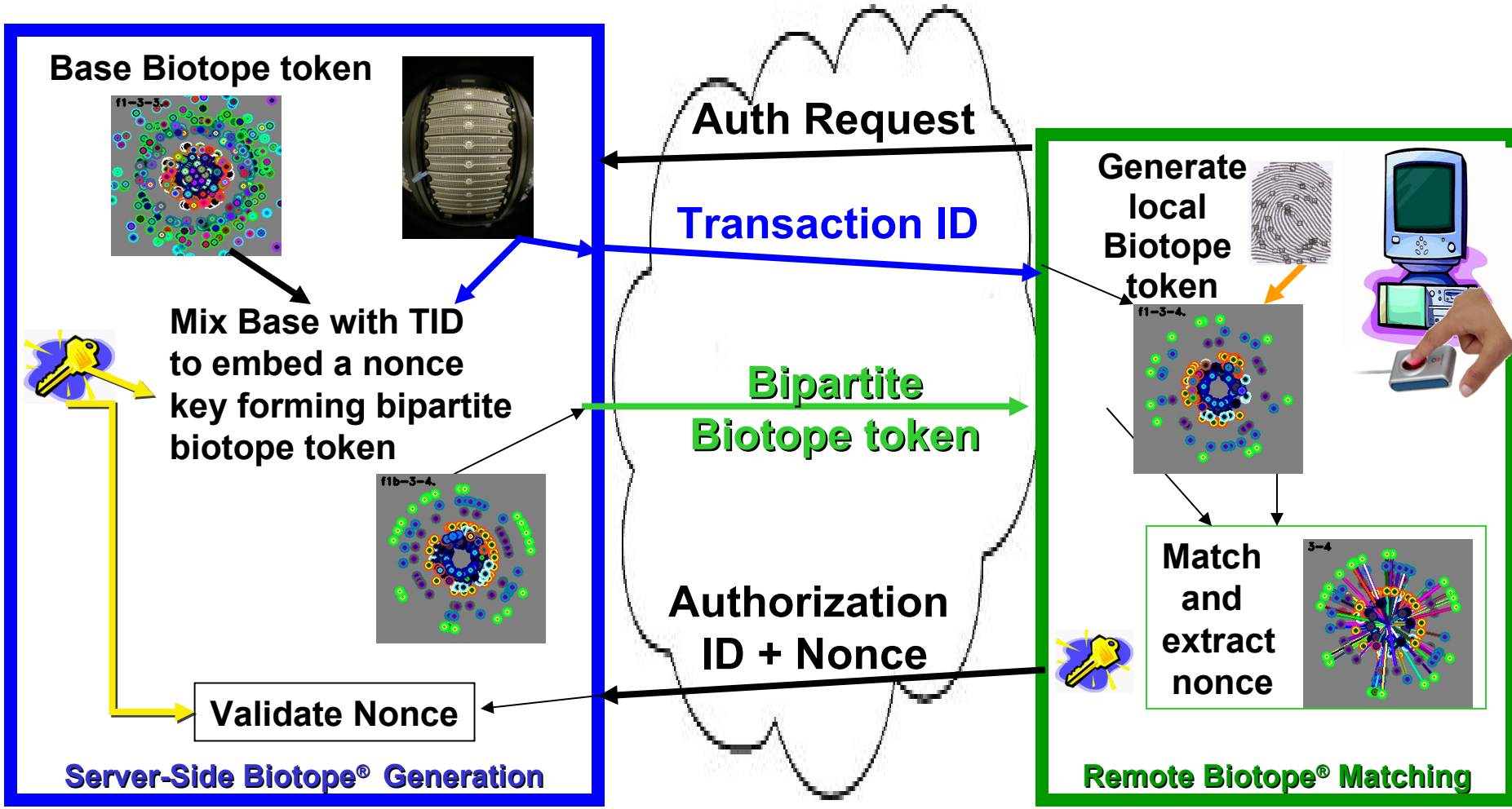
- The nesting process can be formally invertible via the keys, but cryptographically secure
- Revocable + nesting = Asymmetric ID

Bipartite Biotokens

- Scheirer and Boult 2009*
  - Let B be a revocable biotoken. A bipartite biotoken B_p is a transformation $bb_{j,k}$ of user j's k^{th} instance of B. Any bipartite biotoken $B_{p,k}$ can match any revocable biotoken B_k for the same user that uses the same transformations.
  - $bb_{j,k}$ must allow the embedding of some data d into B_p
    - $bb_{j,k}(w_{j,k}, T_k, d)$
  - If $B_{p,k}$ and B_k match, d is released

*** W. Scheirer and T. Boult, "Bipartite Biotokens: Definition, Implementation, and Analysis," ICB 2009.**

Bipartite Biotope® Process



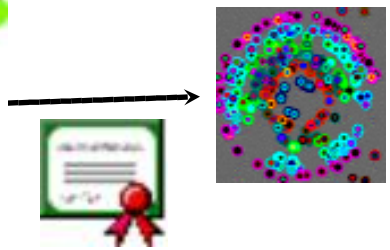
- Solves "asymmetry" of matching, Man in the Middle, Phishing and remote device hacks on "match" yes/no. Can be use "offline" with sync or to store encryption keys.

Flat BKI verification with Central Challenges

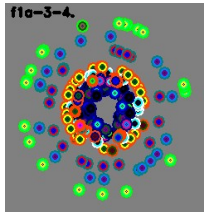
Enroll Biometric

Enroll

Create and Store a revocable identity BKI token CB



Derive transaction token with Embed Nonce

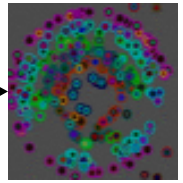


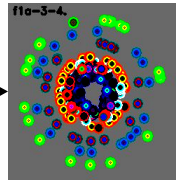
Return Nonce as proof of match

Biometric Matching in *Secure Encoded Space*

Transaction Biometric

Authenticate



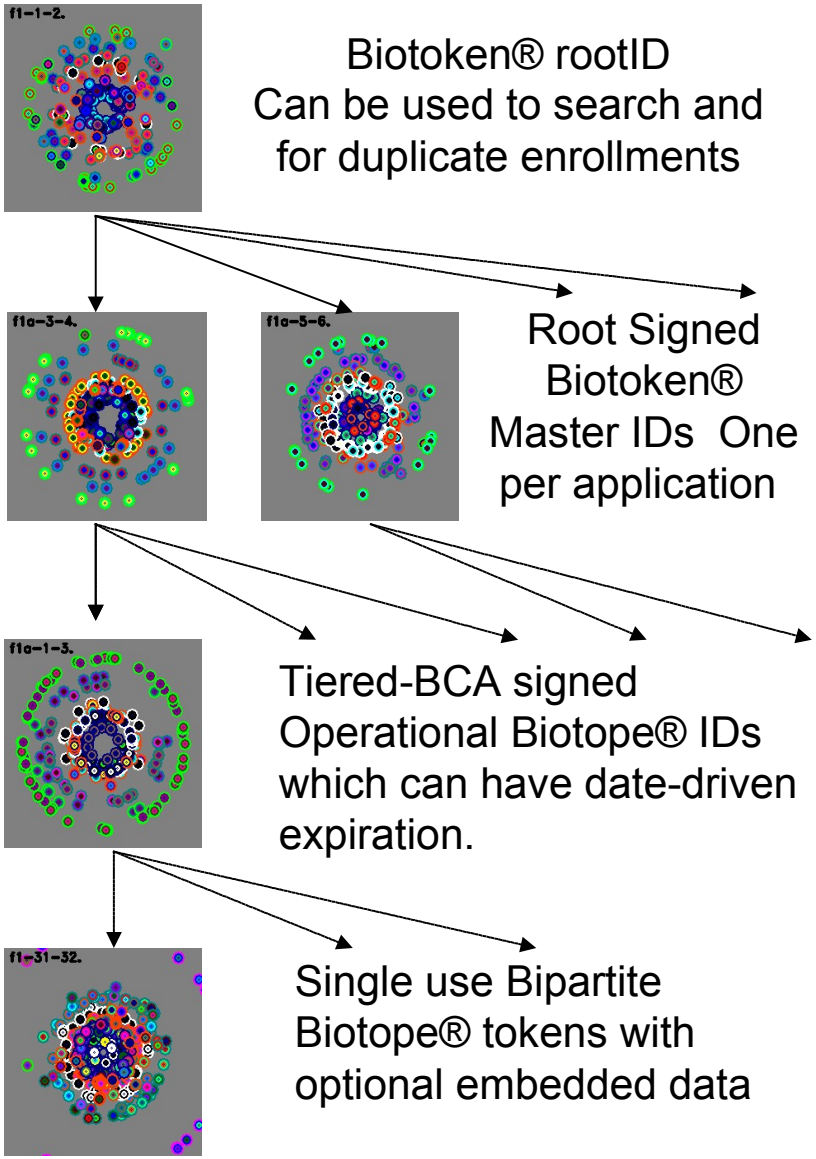


Match and decode

Device Generates a revocable identity token (may include password + EIN)

Retransform with TranID

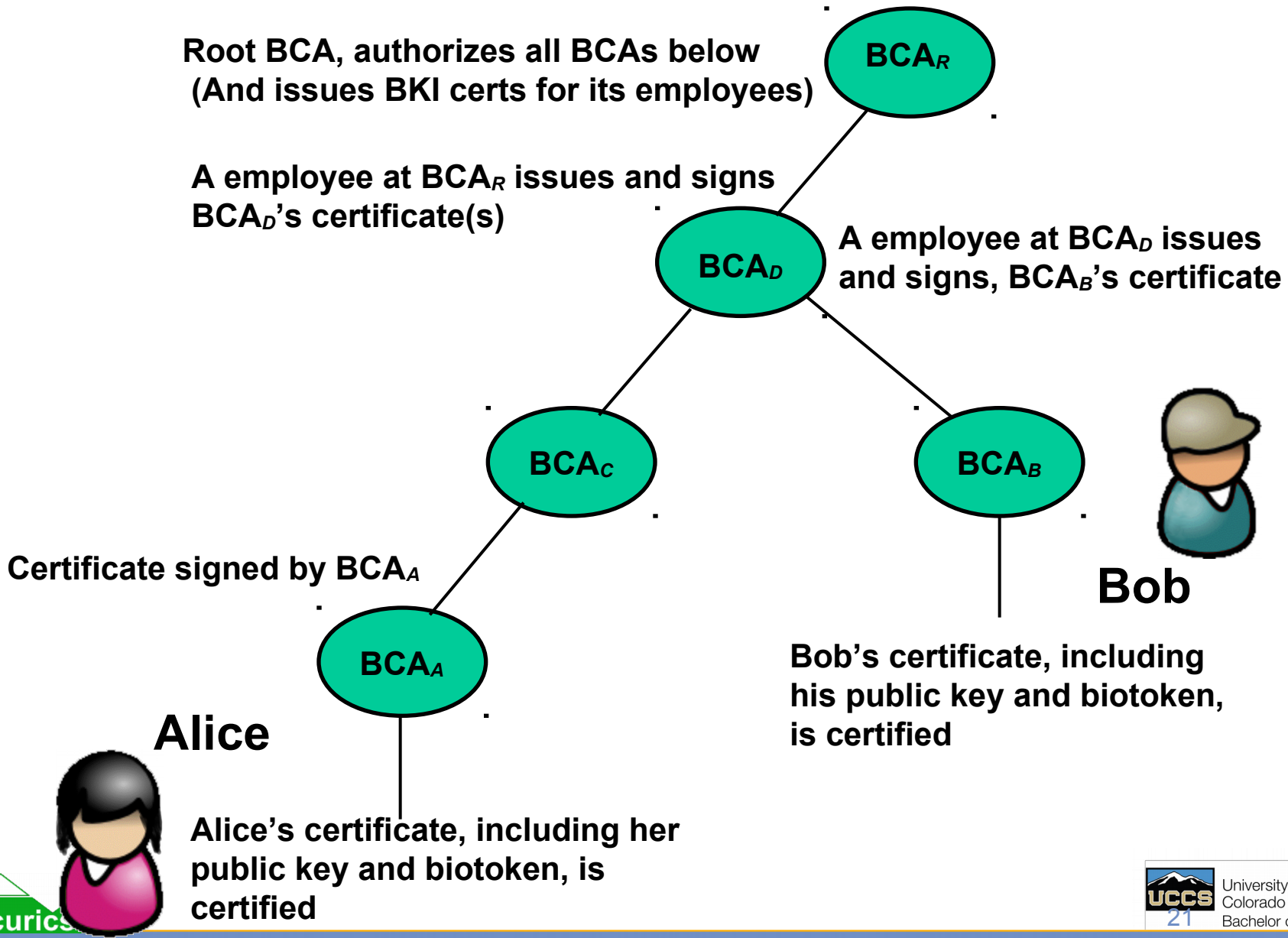
BKI: Biotope Key Infrastructure



- Add Biotope fields & dates in X509 v3 Cert extension fields.
- BCA proofs ID, issues and signs user's "root" certificate
- BCA derives operational certificate and return it or publishes in a private or public directory.
- Alice can locate Bob's cert, derives new transaction certificate with embed key. She signs cert and sends to Bob.
- Bob can validate the message, use biometrics to extract key use or sign it to validate transaction and identities.

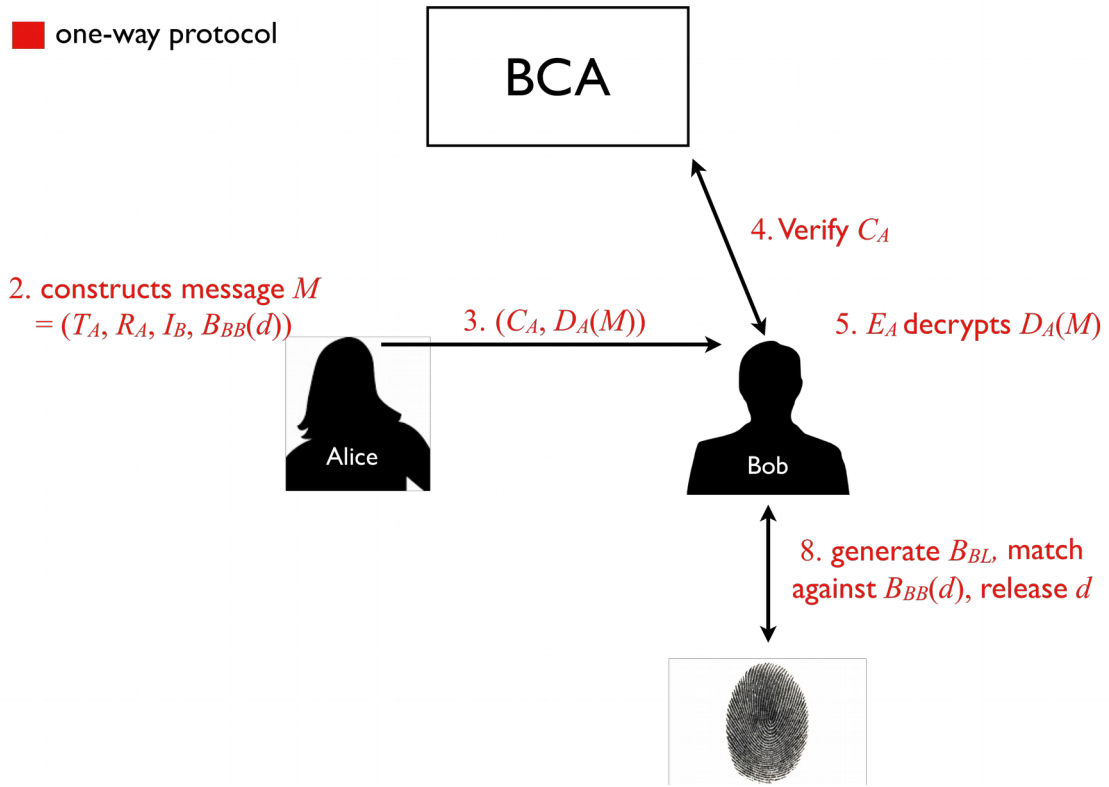
*** W. Scheirer, W. Bishop and T. Boult "Beyond PKI: The Biocyptographic Key Infrastructure," IEEE WIFS 2010 Wksp on Information Forensics and Security**

A BKI Tree "example"



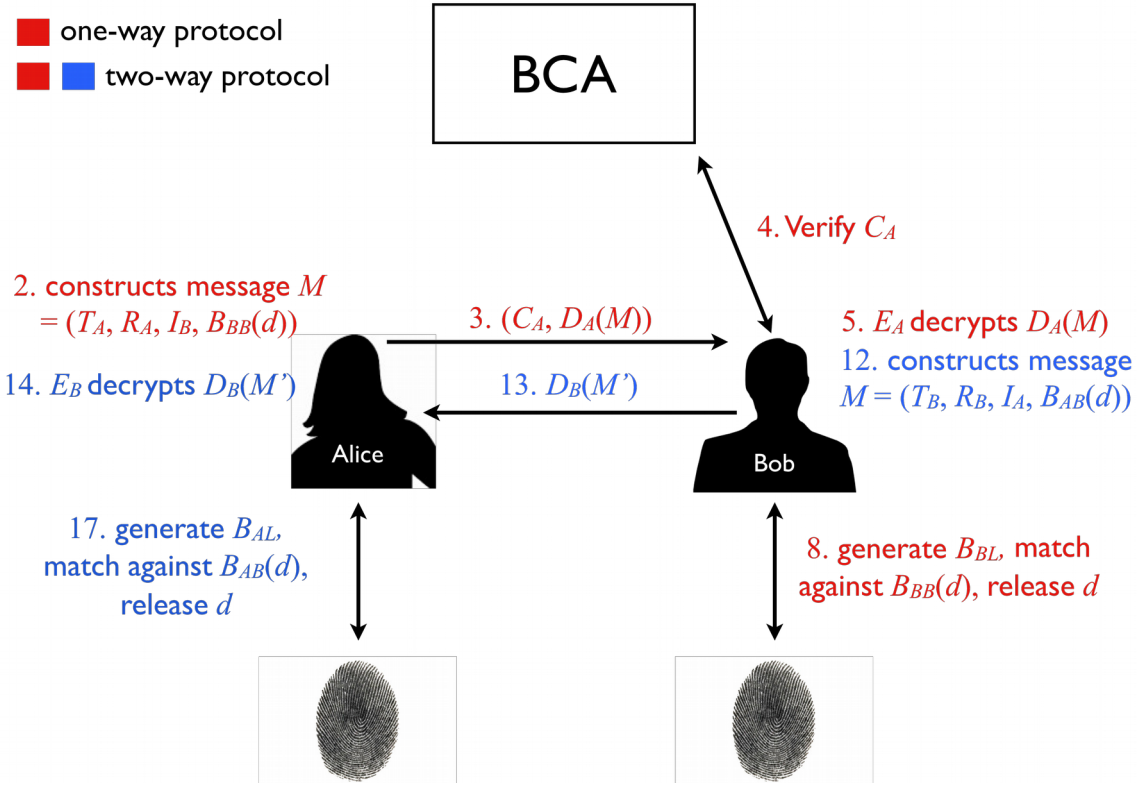
One-Way Protocol

- **Sender creates bipartite biotoken using Receiver's public certificate**
- **Establishes identity & trust of message Receiver**
- **Provides secure one-way data channel**



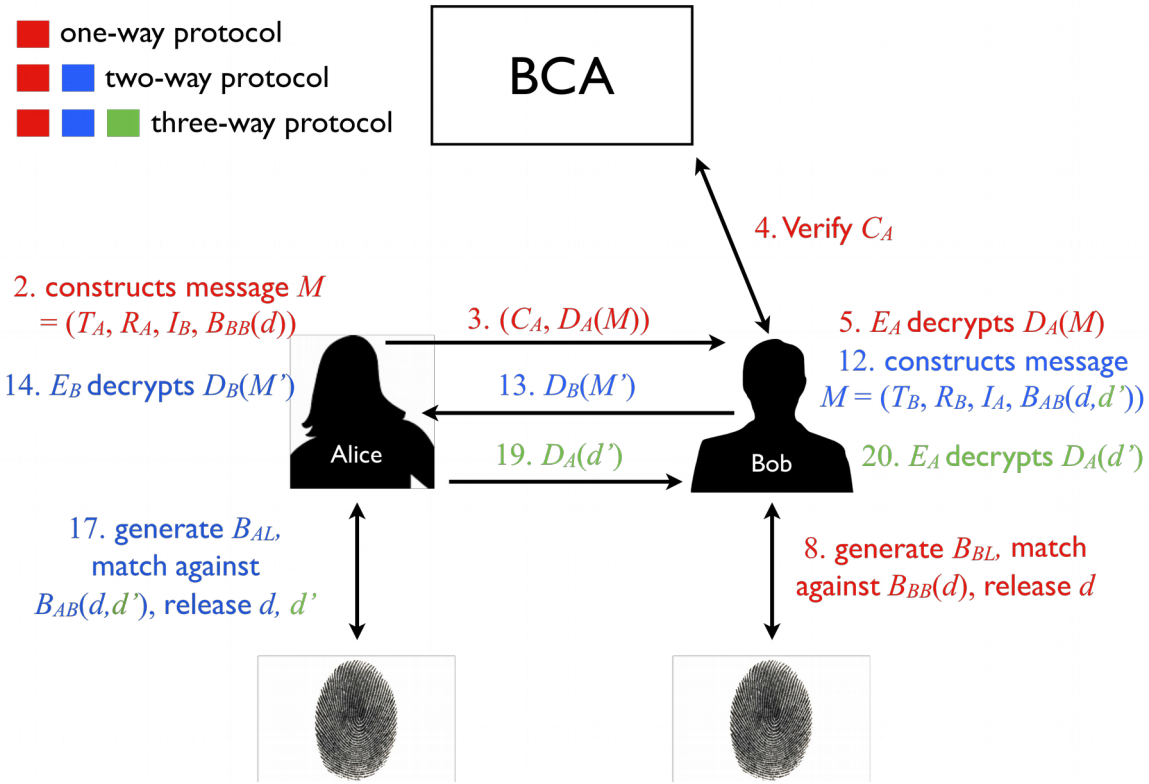
Two-Way Protocol

- **Provides Sender assurance that the Receiver is not an impostor**
- **Strongly Validates one identity in the transaction**



Three-Way Protocol

- **Provides Receiver assurance that the Sender is not an impostor**
- **Strongly Validates both identities in the transaction**

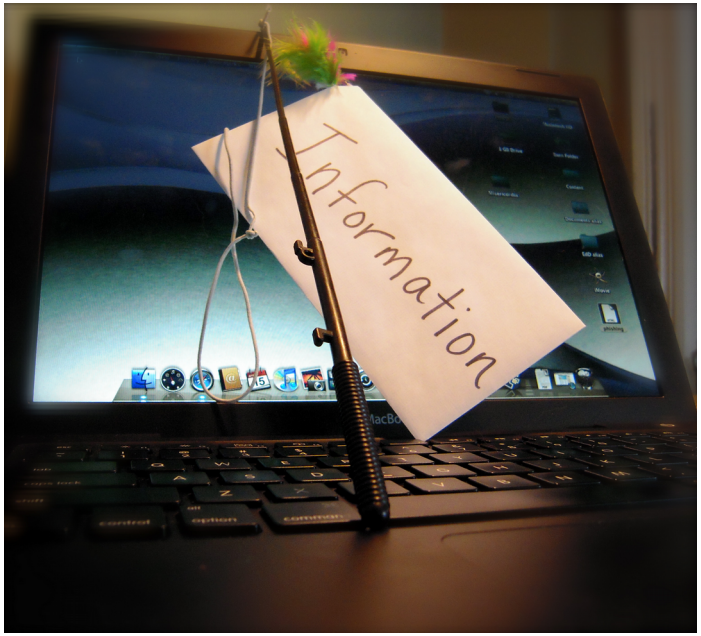


Certificate Revocation/Reissue

- We must consider certificate *and* biometric re-issue
- Scenario 1: Manual re-issue
  - Certificate owner generates a new public-private key pair and a new biotoken
- Scenario 2: Automatic re-issue of biotoken
  - BCA retains transformation keys, reverts public biotoken to a lower level, issues new transformation keys and public biotoken
- Scenario 3: Automatic re-issue of key-pair
  - BCA issues new key-pair, transmits secret key to owner via bipartite biotoken

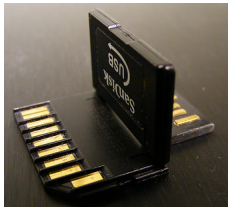
New Applications/Protocols

- Financial Payments/PayPal
- Key-Exchange
- Bio-Kerberos
- Bio-S/Key
- BKI-enabled LDAP
- Biometric Digital Signatures



Other Examples of BKI Enabled Services

- Financial Transactions
- Age Verification
- Remote-web access
- Secure Documents
- Strong anonymous identity
- Healthcare IT
- Anonymous E-Voting
- Multi-use ID Cards
- Multi-factor Signatures
- Key-management
- Data-at-Rest Solutions



Privacy and De-Duplication

- Many ID proofing process require one ID per person (for security or anti-fraud)
- De-duplication requires recognition
  - → Invades Privacy !!
  - → New types of security risks !!

Is there a way to support de-duplication and yet ensure that the ID system data may not be abused. In particular can we make it impossible to search with latents or use data to plant (or generate) a fakeprint?

id-privacy example

(2,0)-id-privacy → P(R) = chance

(2,0)-id-privacy → P(R) >> chance

id-privacy

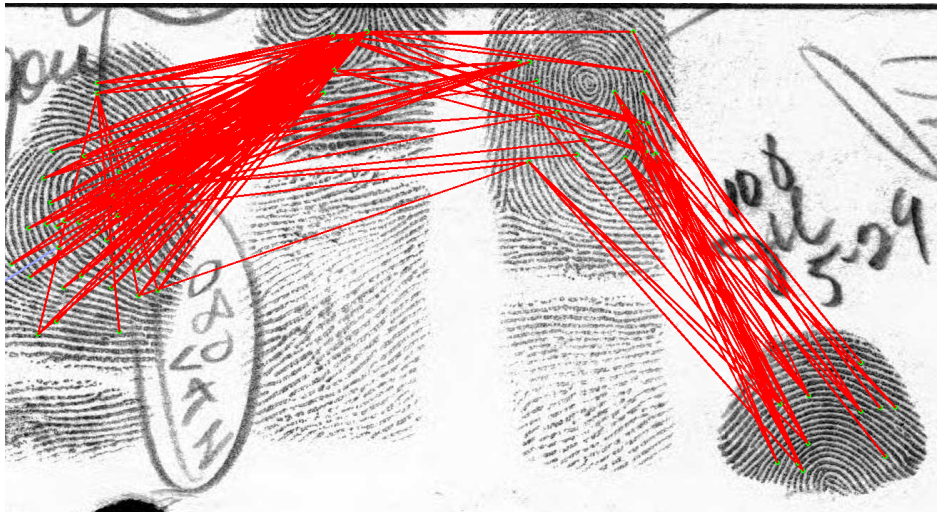
*A recognition representation is said to have id-privacy when using less than **i** items for the search input, the stored data cannot identify subjects with probability **d** greater than random chance, yet when **i** or more distinct items are present, the subject can be recognized at substantially above chance.*

- *This is statement about representation i.e. d = 0, no algorithm can do recognition with less than i inputs.*
- *For d > 0, algorithms/experiments can provide approximate estimate/bound on d.*

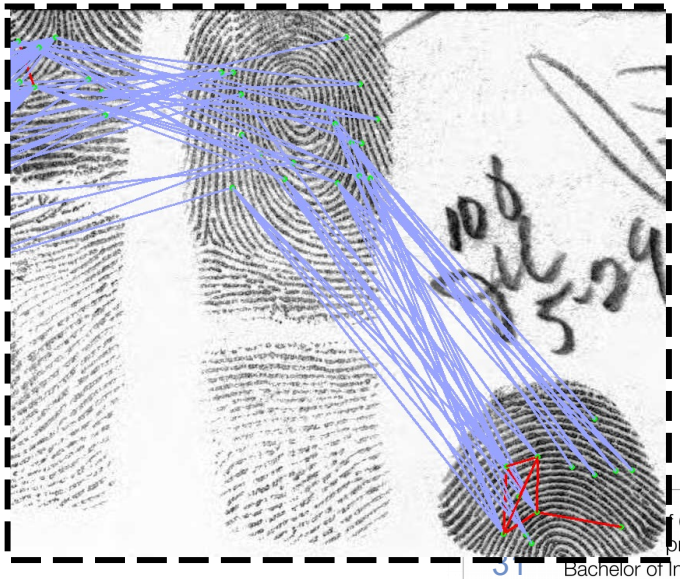
- *Broader and more precise definition than k-anonymity*
- *Defines a new class of problems/representations*

An algorithm for fingerprint *id*-privacy

- Use only intra-finger features. Forest algorithm directly applies, just limit choice of data in pairs.



- Can also allow some local feature pairing, resulting in d>0 but improved accuracy.



BE-Verified?

Optional Check BKI Signature

BE-Verify Code Released

id-privacy Rep

Crypto-Keys

SSN# PersonalPin?

Multi-Finger Bipartite Biotope

Multi-finger Decoding Biotope

BKI Signed

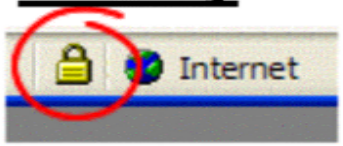
Crypto-Keys

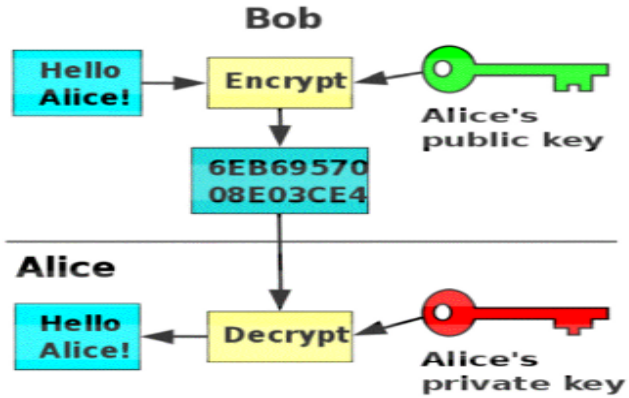
SSN# PersonalPin?

BE-Verify Code Embedded

Summary

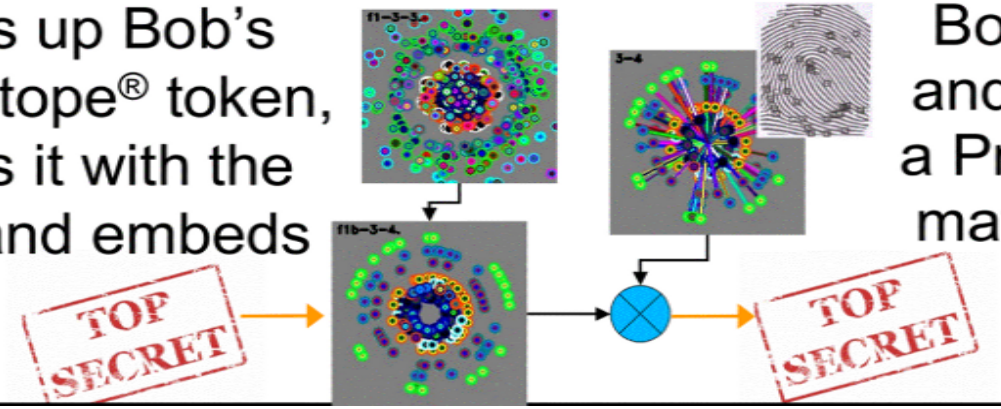
Public Key Infrastructure enables asymmetric secure communication and digital signatures, but **it does not solve <u>Identity</u> Issues**





Our BKI is the first asymmetric identity verification

Alice looks up Bob's Public Biotope® token, transforms it with the Trans-Id and embeds the secret



Bob's Fingerprint and keys generate a Private token and matching releases the secret

The revocable BKI technology is to biometrics what PKI/RSA was to encryption – a disruptive innovation based on asymmetric protection of information

EXOSTAR®

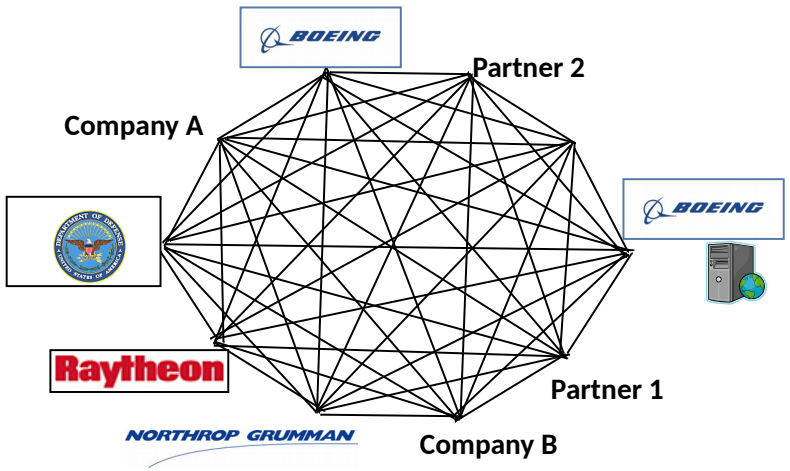
Successful Implementation of Identity Management Systems Integration

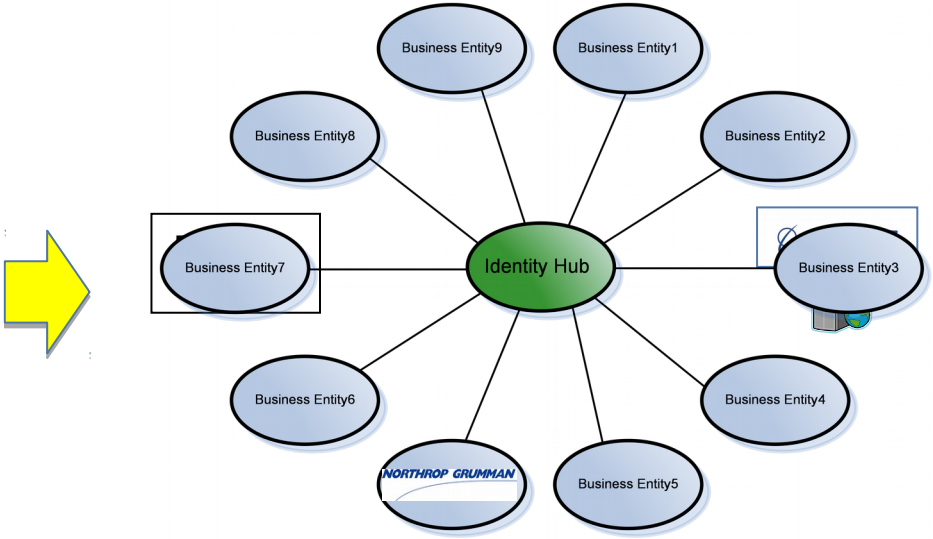
ID Trust 2011: "Near the Horizon, Just Over the Horizon"

Vijay Takanti
Vice President Security & Collaboration Services
Exostar

April 6, 2011

Identity Hub





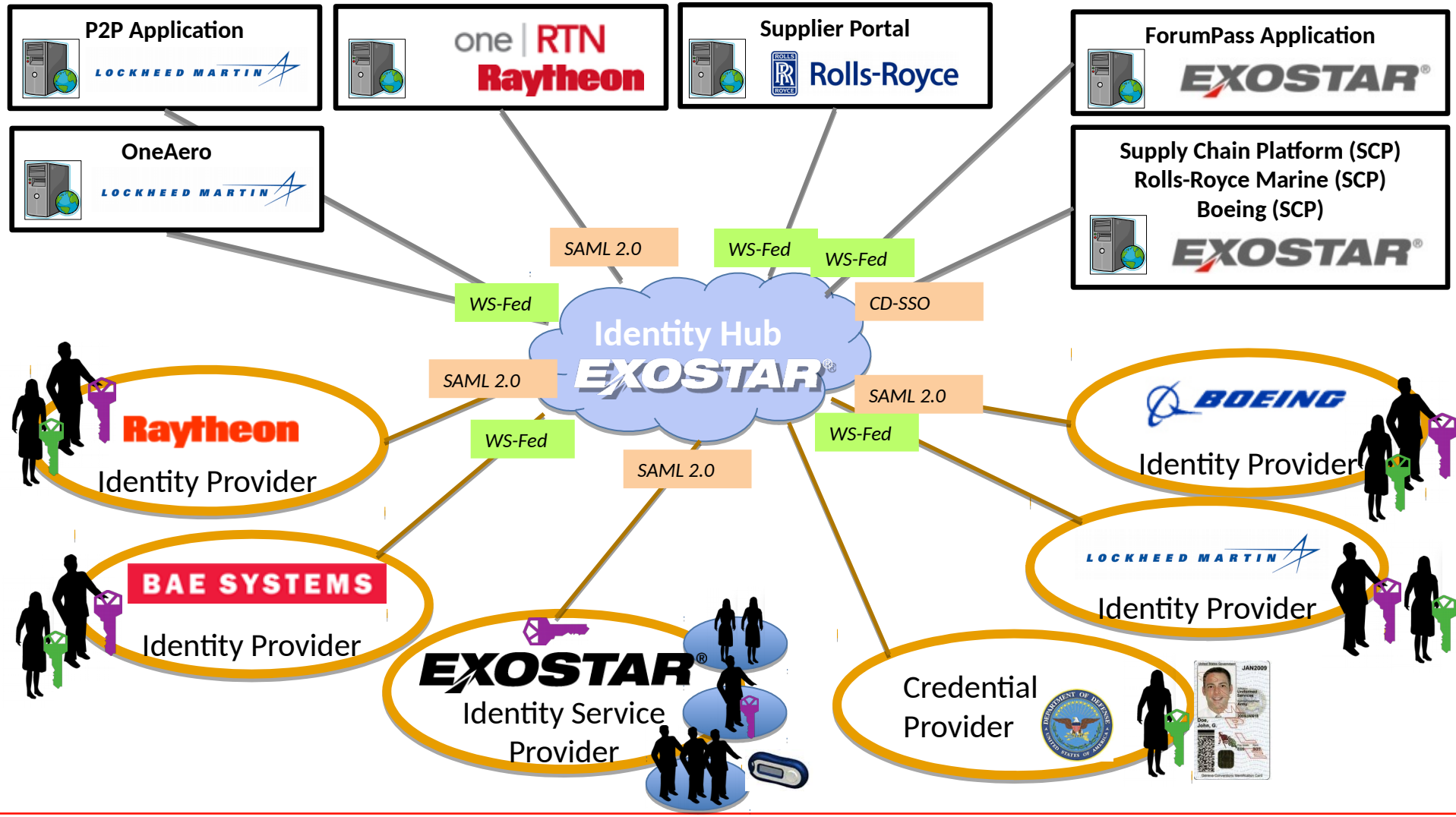
Typical Federation:

X user account provisioning systems
X life cycle management systems
multiple protocols (SAML, WSFED, etc)

Federation through Exostar:

Single interface to an identity hub

The Exostar Identity Hub "In Action"



EXOSTAR®

Thank You

SAFE-BioPharma™

SAFE-BioPharma Association
Signatures and Authentication for Everyone

Overview of the SAFE-BioPharma Digital Identity and Signature Standard

10th Annual Symposium on Identity and Trust on the Internet

April 6th, 2011

NIST

SAFE-BioPharma™
SAFE-BioPharma Association
Signatures and Authentication for Everyone

Moving BioPharma and Its Partners into the Digital Age: SAFE-BioPharma I

- **December 2003, industry IT professionals from Top Ten Pharma companies saw the need for identity management and digital signatures as fundamental to move pharma processes into the electronic realm**
  - Revolutionary changes underway in medical research and in healthcare
  - Cost and complexity has created crisis in R&D productivity
  - Need for rapid, close collaboration between pharma, healthcare providers, research institutions, government and global partners
  - FDA and EMA moving to fully electronic submission, review and response
- **Series of Working Groups established the SAFE-BioPharma standard**
  - Standard – PKI based, liability, contracts, regulatory participation
  - Medium Assurance/Hardware – smartcard

SAFE-BioPharma™

SAFE-BioPharma Association
Signatures and Authentication for Everyone

SAFE-BioPharma II

- **Member-governed non-profit collaboration: SAFE-BioPharma Association July 2005**
- **Policy Approval Authority approved interoperable standard Sept 2005**
  - Trusted identity and non-repudiable digital signature
  - Single interoperable digital identity across industry
  - Technology and vendor neutral
  - Based on leading government technical and identity proofing standards
  - Interoperable with Federal agencies
  - Wrapped in a legal, governance and risk mitigation model
  - Recognized by world's leading regulatory authorities – FDA and EMA
- **SAFE-BioPharma Bridge operational**
- **Pilots and implementations**
  - Pfizer, GSK clinical, Astra Zeneca regulatory; Firebird Pilot – National Cancer Institute, pharma, medical insts.

SAFE-BioPharma III: 2007-2010

- **Improving usability**
  - Pilots and early adopters: resulted in expansion of the standard – basic, software, roaming
  - Improvements in identity proofing process and digital signing options
  - Growth in certified products and applications
- **Building the interoperable network:**
  - Expansion of commercial firms offering credentials and related services
  - Cross-certification with FBCA & establishment of 4BF (4 Bridges Forum)
  - EU qualified certificates; Safe Harbor certification
- **Growing use and use cases**

SAFE-BioPharma™

SAFE-BioPharma Association
Signatures and Authentication for Everyone

SAFE-BioPharma Members

- Alkermes
- Allergy & Asthma Inst.
- Amarin
- Amgen
- Abbott
- AstraZeneca*
- Bristol-Myers Squibb*
- Eli Lilly
- Forest Labs
- GlaxoSmithKline
- IPS Research
- J&J*
- Merck*
- McDougall Scientific
- MWB Consulting
- National Notary Assn.
- Oxford Outcomes
- PDC Biotech
- Pfizer*
- Premier Purchasing
- Roche
- Sanofi-Aventis*
- SNAP Diagnostics
- St. Renatus
- Veroha

*Board members

SAFE-BioPharma™

SAFE-BioPharma Association
Signatures and Authentication for Everyone

SAFE-BioPharma Vendor Community

Vendor Partners

- ✓ Adobe*
- ✓ Arcot*
- ✓ ARX*
- ✓ Gemalto*
- ✓ Gemini Security
- ✓ Hitachi
- ✓ IBM
- ✓ IntraLinks
- ✓ IDBS*
- ✓ LCSP
- ✓ Microsoft
- ✓ Safenet*
- ✓ Surety
- ✓ Symyx*

Vendor Partners

- ✓ Tricipher*
- ✓ Verizon
- ✓ Waters Inc.*

Issuers

- ✓ Citibank
- ✓ Exostar
- ✓ IdenTrust
- ✓ J&J
- ✓ Symantec
- ✓ TransSped

SAFE-BioPharma™

SAFE-BioPharma Association
Signatures and Authentication for Everyone

A Non-Profit, Member-Driven Standards Association

Board of Directors & PAA
Rick Yborra, BMS, Chair

CEO
Mollie Shields-Uehling

SAFE-BioPharma Member Consortium

STAFF
- Jon Schoonmaker, Chief, Ops
- Gary Wilson, Prog Mgr
- Rich Furr, Head, Reg Afrs
- Tanya Newton, Mgr, Reg Afrs
- Kevin Chisholm, Exec Asst
- John Weisberg, PR & Comm
- Kay Bross, Member & Vendor Progs

- Legal, Financial, Admin

SAFE-BioPharma Japan Advisory Group

Astellas

Working Groups

Technology WG
Justin Bovee, J&J
Keith Respass, Merck

- **Federation TF, Pfizer/Merck**
- **Users Group, Lilly/Pfizer**
- **Issuers Group**

Global Business & Reg
Betsy Fallen, Merck

SAFE-BioPharma European Union Advisory Group,

Isabelle Davias, Sanofi-Aventis

Hans van Leeuwen, Merck

SAFE-BioPharma™
SAFE-BioPharma Association
Signatures and Authentication for Everyone

SAFE-BioPharma Association – Non-Profit Standards Collaboration

Standards	Standards-Related Services Supporting Innovation	Collaborative Association
►**Standard Development & Maintenance** ►**Governance/legal framework** ►**Certification:** - Products - Issuers ►**Standards engagement: HL7, CDISC, IHE, Kantara** ►**Working Groups** –Technical –Federation –Users Group –Global Business & Reg –SAFE EU Advisory Council –Japan Advisory Council ►**Regulatory alignment:** –FDA; EMEA; NCAs, PMDA	►**Operation of SAFE-BioPharma bridge** ►**Cross-cert with FBCA** ►**Participation in CPWG** ►**4BF – network of trusted bridges** ►**Implementation tools** ►**EU Safe Harbor – data privacy** ►**Antecedent Data ID Proofing** ►**EU qualified digital identities** ►**Process improvements** ►**Vendor partner program**	►**Stakeholder outreach** ►**Education & advocacy** ►**Policy engagement** ►**Industry awareness & engagement** ►**Information/Best Practices Forum** ►**Policy forums** ►**Media: local, national, trade, international**

SAFE-BioPharma™
SAFE-BioPharma Association
Signatures and Authentication for Everyone

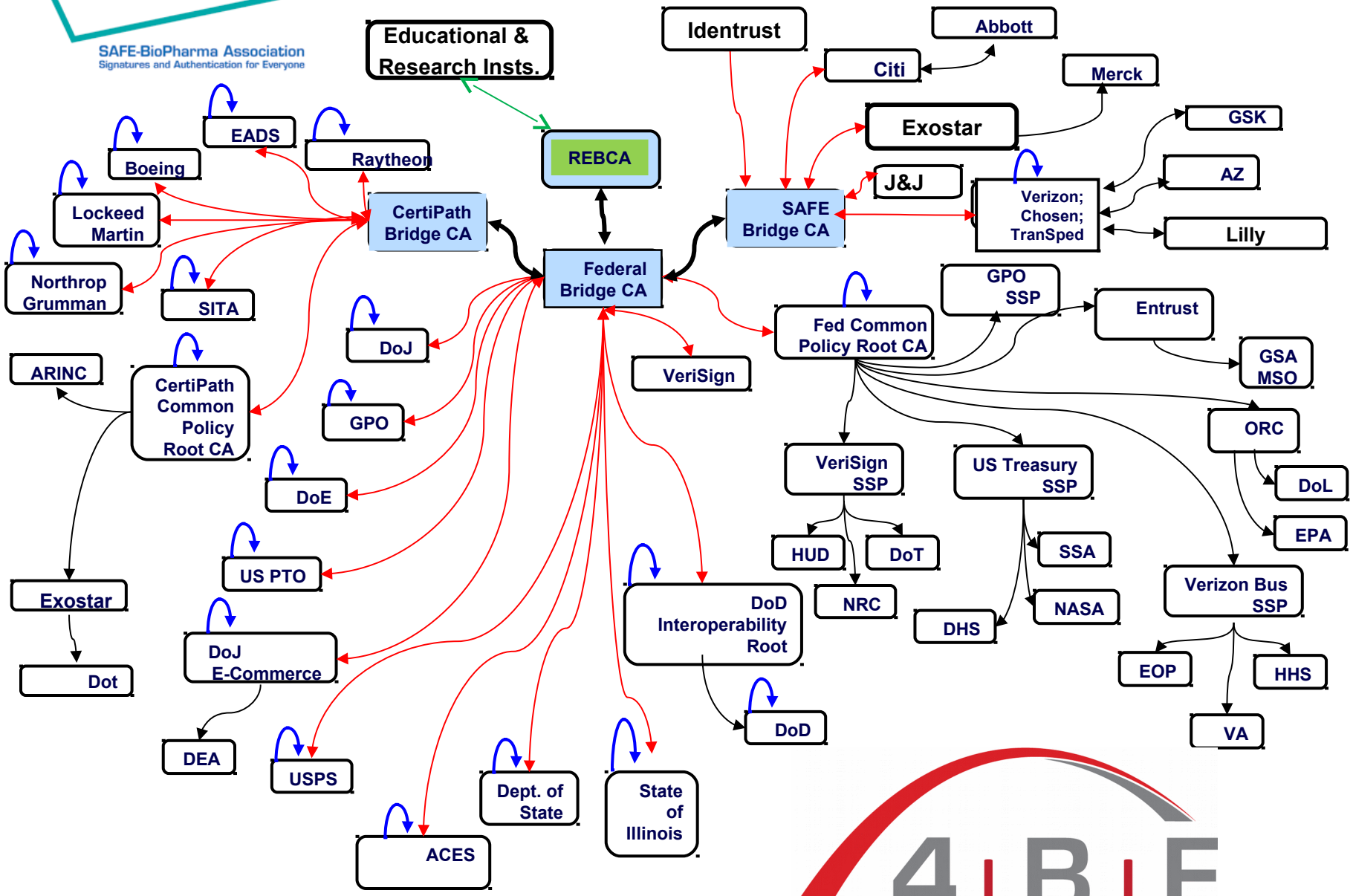
SAFE-BioPharma and Regulators

- **EMA and FDA are on a publicly-announced paths to requiring fully electronic submissions within the next few years**
- **FDA helped write SAFE-BioPharma standard**
  - CIO, PDUFA IT Team, 21CFR11 Council, CDER, CBER
  - Training program; compliance matrix; CIO meetings
  - FDA has received 10,000s of SAFE-BioPharma submissions since 9/06
- **EMA helped write standard**
  - 2009 eCTD pilot – 5 companies submitted eCTDs to EMA; evaluation report
  - Accepting fully electronic eCTD submissions
- **SAFE-BioPharma in Japan**
  - JPMA has established Task Force on SAFE-BioPharma digital signatures – includes JMA and PMDA
  - Hitachi supporting SAFE-BioPharma implementations in Japan
  - Successful pilot with 3 hospitals and Astellas signing pharmacovigilance documents
  - Pilot underway with five Japanese companies

SAFE-BioPharma™

SAFE-BioPharma Association
Signatures and Authentication for Everyone

4BF –Network of Trusted Cyber-Communities



4 B F

4BF – 4 Bridges Forum

www.The4BF.com

- **Collaboration between GSA (USG), SAFE-BioPharma, Certipath and Higher Education to raise awareness and promote use of new network of trusted cyber-communities**
  - SAFE-BioPharma example: Bristol-Myers Squibb, National Cancer Institute, and medical research institutions collaborating on variety of projects using Federal and SAFE digital IDs and signatures
  - Certipath: facilities access to DOD secure facilities
  - Higher Education Bridge: NIH grant applications; encrypted e-mail for university and govt. collaborations involving GSA: facilities access; network access; validate credentials from external parties; authentication to Level 3 & 4 applications by USG and private sector
  - Federal Bridge: Logical and physical access; digital signatures; collaboration among agencies and with external parties
- **Phase II underway – communications and discussion forum –** now includes the PIV-i providers – Verisign, Entrust, Verizon

SAFE-BioPharma IV: Greater Need for Standard and Many New Uses – 2011

- **Dramatically changing external environment**
  - Industry facing patent cliff; downsizing; mergers; global collaborations
  - Clinical trials shift to India, China
  - Translational medicine – research-clinical practice-research cycle
  - USG payments for EHRs and forms of “MU” – meaningful use
  - DEA requirements for 2-factor for ePrescribing of controlled substances
  - Strengthened HIPAA (privacy) standards; EU data privacy standards
- **Commercial technology providers moving into healthcare**
  - Cloud-based solutions; mobile; multiple form factors
  - Credentials as commodities – value added services leveraging credentials
  - 4 Bridges – network of linked cyber-communities
- **Growing use and use cases:**
  - ELNs (basic laboratory research)
  - Regulatory submissions
  - Workflow between several/many partners for auth & signing

SAFE-BioPharma™
SAFE-BioPharma Association
Signatures and Authentication for Everyone

Examples of How SAFE-BioPharma Is Being Used

Use Case	Company
ELNs – basic research	Abbott (including China), BMS, GSK, Pfizer, SA/Aventis Pasteur (vaccines)
Contracts, SOWs	J&J, GSK, Premier, Oxford, MWB Consulting, IPS, Allergy & Asthma Inst.
Physician Signatures	SNAP Diagnostics
ePrescribing (authentication and dig sig)	3 ePrescribing applications companies
Purchasing	Premier
Clinical Research	Sanofi-Aventis, BMS, National Cancer Inst.
Research Collaboration	BMS, National Cancer Institute, Sanofi-Aventis
Alliance Management	BMS, GSK
Regulatory Submissions	AZ, BMS, GSK, SA, Eli Lilly, Forest, J&J, Alkermes
Document management system	McDougall Scientific
Legal signatures	Veroha
Paperless business/regulatory environment	Amarin, MWB Consulting, SAFE-BioPharma

SAFE-BioPharma™
SAFE-BioPharma Association
Signatures and Authentication for Everyone

Pfizer eLabNotebooks

Company Profile:

- **Largest *research-based* pharmaceutical**
- **Founding member, SAFE-BioPharma Assoc.**
- **Global research organizations**

- **Challenges**
  - Productivity
  - Regulatory compliance
    - HIPAA
    - 21 CFR Part 11
  - Patent defense

Chemistry electronic notebook

Scope:

- **Paper lab notebook**
  - Chemist, witness signatures
  - Patent implications
- **Replace paper with electronic**
  - SAFE-BioPharma digital signatures
  - TriCipher mySignatureBook
- **Using digital signatures**
- **Flattened PDF for distribution**
- **Electronic records management**

Steven.C.Trudel
1 Facsimile of Original Digital Signature

Steven.C.Trudel
Reason: I am the author of this document.
Date: 2007-05-15 17:11:32 -0400

Michael.B.Tollefson
2 Facsimile of Original Digital Signature

Michael.B.Tollefson
Reason: I have read and understood the contents of this document.
Date: 2007-05-16 08:23:51 -0400

SAFE-BioPharma™
SAFE-BioPharma Association
Signatures and Authentication for Everyone

Pfizer ELN Results and Benefits

Results:

- **Less time on paperwork, more in the lab**
  - > 3300 researchers in 280 departments in 20 countries;
  - > 550,000 documents signed
  - >1,000,000 digital signatures!
- **3.3 million pages *not* printed!**
  - >16 tons of paper saved
- **Better patent defense**
  - Signed, time-stamped in timely manner
- **Better compliance with internal regulations**
- **Easier access to research**
  - Electronic search of records
- **Faster research cycles**
  - More time in lab, less on paperwork; No more delays to collect witness signatures

SAFE-BioPharma™
SAFE-BioPharma Association
Signatures and Authentication for Everyone

SNAP Diagnostics

Company Profile:

- Leader in diagnostic technology for detection of sleep apnea and analysis of snoring problems
- Provides physicians in the U.S., EU, and Latin America with proprietary diagnostic equipment used in home settings

Scope:

- Records of at-home tests analysis by company physicians who advise referring physicians re therapeutic approach
- Digital forms used in this process digitally signed

Results:

- Eliminated paper in day-to-day reviews of diagnostic information
- Eliminated costs associated with handling, signing, shipping, storing and accessing paper

SAFE-BioPharma™
SAFE-BioPharma Association
Signatures and Authentication for Everyone

GSK eSubmissions

- **Move towards fully electronic submissions to FDA**
- **Reduce Waste**
  - Costs
  - Time
  - Transport
- **Efficiency Gains**
- **FDA Forms signed with Digital Signatures**
  - No printing of paper copy to sign
  - Supports production across sites
  - No scanning of the signed FDA Form
  - No extra storage in USRA Archives (currently stores paper copy of Form along w/ e-sub.)

SAFE-BioPharma™
SAFE-BioPharma Association
Signatures and Authentication for Everyone

GSK Strategic Decisions

- **How to Credential (in-house, outsource, via SAFE-BioPharma)**
- **Who should be a Trusted Agent?**
- **Limits on signing?**
  - Who should/can sign? What type(s) of document(s)?
- **What tool(s) to use for signing?**
- **Meaning of Signature**
  - A corporate signature on an FDA form is required

    AND
  - Signatory has a legal obligation as expressly written on the FDA form, <u>and</u> within the CFR sections that apply
- **What to sign?**
  - Initial and supplemental NDA, BLA, eCTD; CBE and CBE-30; annual Reports' other

SAFE-BioPharma™
SAFE-BioPharma Association
Signatures and Authentication for Everyone

GSK: Benefits/Cost Savings

- **Savings in scanning, storing, transporting [over initial 9mo.]**
  - Reduced monthly # of in-scope application forms using wet signature from 100% to 20%
  - Reduced cycle time from preparation of form to inclusion in submission (from average of 8 hrs to minutes)
  - Reduced records management/archival effort [approx 36 days or $6.1K / £4.1K Cost Savings]
  - Scanning and printing costs [approx. $.74 / £0.5K]
  - Enabled cross-site & virtual operations

SAFE-BioPharma™
SAFE-BioPharma Association
Signatures and Authentication for Everyone

Pilot Study:

Bristol-Myers Squibb
National Cancer Institute-Cancer Therapy Evaluation Program (CTEP)

- **Working example of how secure, online trusted identities can be used to save time and costs over the hard copy paper systems currently used for clinical trials**
- **Employs *interoperable digital identities, digital signatures* and *cloud computing* to eliminate reliance on paper forms when starting clinical trials**
- **Pilot study goals**
  - accelerate initiation of clinical trials
  - eliminate reliance on paper forms
  - lower costs
- **In line with principles of National Strategy for Trusted Identities in Cyberspace (NSTIC)**

SAFE-BioPharma™
SAFE-BioPharma Association
Signatures and Authentication for Everyone

NCI-CTEP

- **Mission: improve the lives of cancer patients by finding better ways to treat, control and cure cancer**
- **World's largest sponsor of cancer treatment clinical trials**
  - 900+ active clinical trials testing new cancer treatment regimens
  - activates 130 new protocols per year
  - each protocol produces many signed and exchanged documents among multiple participants
  - 100,000 pages in 2010
- **Mandates**
  - initiate clinical trials to patient accrual more quickly
  - reduce costs
  - streamline document management while assuring greater document security
  - have environmentally sound procedures

NATIONAL® CANCER INSTITUTE

SAFE-BioPharma™
SAFE-BioPharma Association
Signatures and Authentication for Everyone

Bristol-Myers Squibb

- Global biopharmaceutical company
- Mission: discover, develop and deliver innovative medicines that help patients prevail over serious diseases
- At leading edge of cancer research and treatment since 1970's

Bristol-Myers Squibb

Many documents are signed, transmitted, countersigned

- Prior to study, process was delayed by sending physical documents via courier or fax for signature
- During study, electronic documents were stored in the cloud where researchers could access and sign immediately using digital signatures based on interoperable digital identities

Paper Use

SAFE-BioPharma™

SAFE-BioPharma Association
Signatures and Authentication for Everyone

Many documents are signed, transmitted, countersigned

- Prior to study, process was delayed by sending physical documents via courier or fax for signature
- During study, electronic documents were stored in the cloud where researchers could access and sign immediately using digital signatures based on interoperable digital identities

SAFE-BioPharma™

SAFE-BioPharma Association
Signatures and Authentication for Everyone

Results

- **Cost Savings**

  - Substantial cost savings anticipated as pilot moves to production
  - On average, 10% of the documents are shipped overnight and 10% by courier service.
  - Estimated savings: $500 per user

- **Time Savings**

  - Significant time savings
  - 3 to 5 business days per signature is typical
  - Pilot demonstrates that each signature can take minutes

- **Document Loss**

  - Pilot demonstrates elimination of lost or misplaced documents.
  - Using digital signatures establishes audit trail of when the document was uploaded, of the email sent to alert the signatory that the document is available for signature, and when the document was actually signed

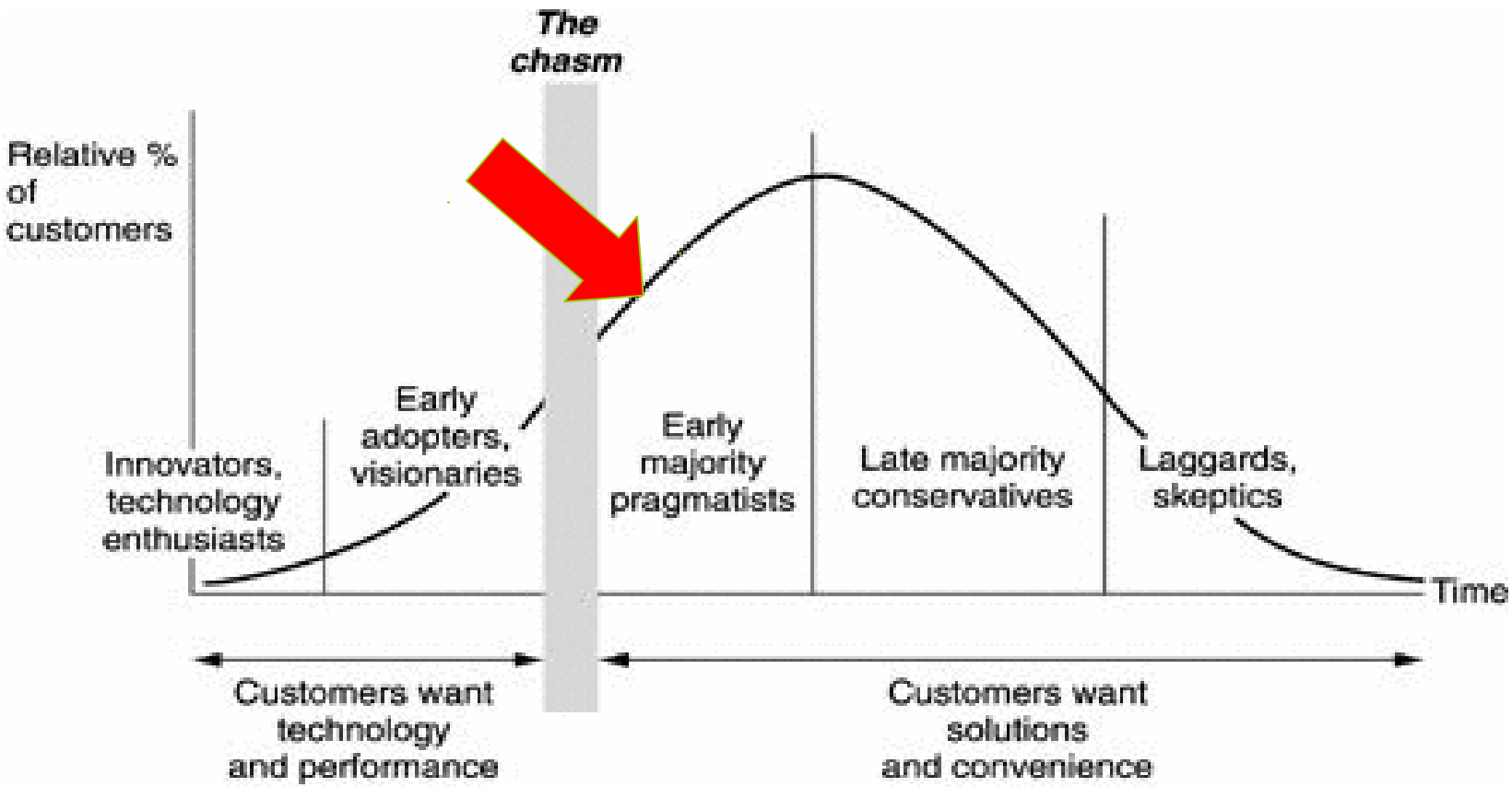
- **Reduced Environmental Impact**

  - Moving to electronic process eliminates use of paper and ink, eliminates document shipment; minimizes storage and retrieval

SAFE-BioPharma 2011

- **Focusing on Projects that Demonstrate Interoperability**
  - BMS-NCI/CTEP pilot; move to production by end of year
  - Expand to other areas of NIH
  - Federation – 3-4 SAFE-BioPharma Members and NIH
  - DEA ePrescribing projects
- **Expand the standard/rules**
  - ICAM lower levels of trust
- **Continue to align internationally – EU, Japan, China**

From Concepts and Ideals to Technologies, Products & Services



SAFE-BioPharma™

SAFE-BioPharma Association
Signatures and Authentication for Everyone

- ✓ *Please visit the SAFE-BioPharma website*: http://safe-biopharma.org/
- ✓ *Please visit the 4BF website:* http://www.the4bf.com/
- ✓ *Watch the SAFE-BioPharma introductory video: http://www.safe-biopharma.org/video.htm*

- ✓ *Contact us for more information:*

Mollie Shields Uehling
CEO
mollie@safe-biopharma.org
(201) 849-4544
(201) 925-2173 (cell)

Kay Bross, Director
Member/Vendor Progs
kbross@safe-biopharma.org
(513) 489-3840 (o)
(513) 673-2344 (c)

Tanya Newton
Manager, Reg Afrs
(908) 213-1069
tanya.newton@safe-biopharma.org

Jon Schoonmaker
Chief of Operations & Technical Program
(301) 610-6060
jon.schoonmaker@safe-biopharma.org

Kevin Chisholm, Admin.
Kevin.Chisholm@SAFE-BioPHarma.org
(201) 849-4545

Rich Furr
Head, Reg. Afrs.
RFurr@SAFE-BioPharma.org
(980) 236-7576

Gary Wilson
Prog. Mgr
(781) 962-3172
Gwilson@safe-biopharma.org

Jon Weisberg
Communications
801-359-9977 o
801-860-9977 m
jweisberg@safe-biopharma.org

Single Sign-On and Federated Authentication at NIH and Beyond

Debbie Bucci
National Institutes of Health

CIT
Center for Information Technology

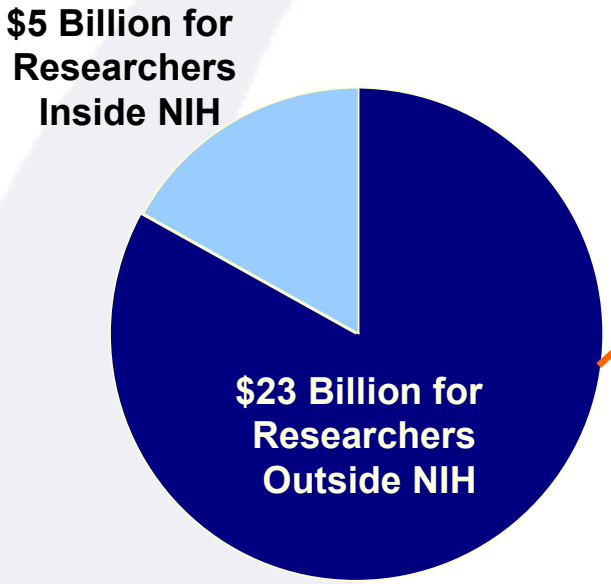
About NIH

- National Institutes of Health (NIH)
- Operating division of the U.S. Department of Health & Human Services (HHS)
- Primary Federal agency for conducting and supporting biomedical research

CIT
Center for Information Technology

External Users

- NIH provides financial support to researchers around the world.
- NIH invests **over $28 billion** in medical research each year.



83% goes to almost 50,000 competitive grants that support over 325,000 researchers **outside NIH**.

CIT
Center for Information Technology

Authentication Services at NIH

NIH iTrust

Multifunction single sign-on (SSO) and federated authentication service consisting of:

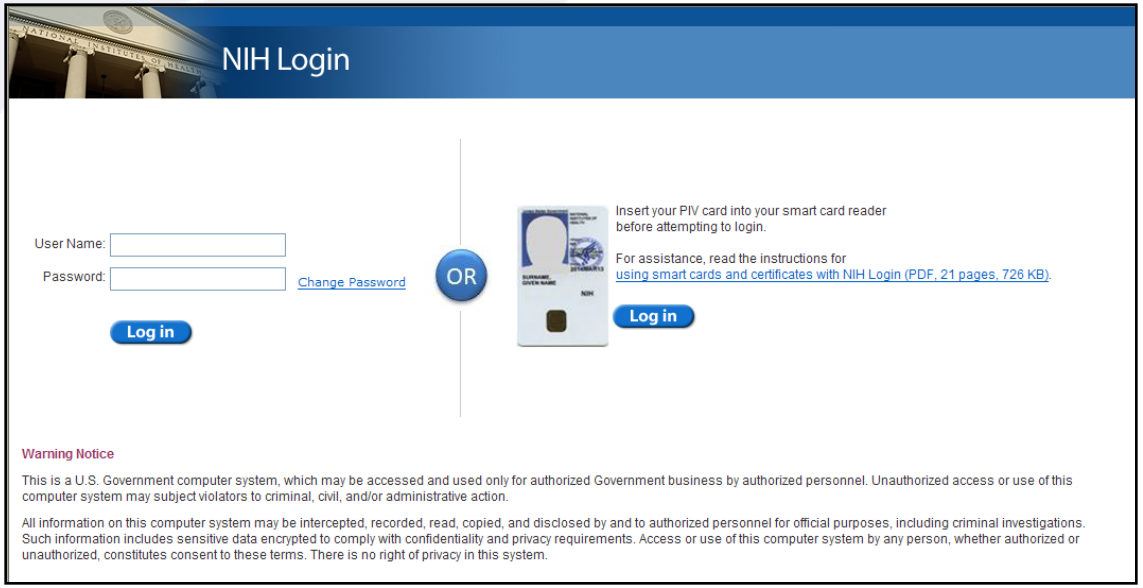
- **NIH Login** – links internal users at NIH to internal and departmental (HHS) applications and electronic resources
- **NIH Federated Login** – links external users to NIH and departmental (HHS) applications and resources

Federated Authentication Partners

- **Government Departments and Agencies**
- **InCommon Federation** – identity and access management federation for the higher education and research communities; nearly 50 major universities access NIH resources through InCommon.
- **Open Identity Exchange (OIX), OpenID, and Information Card Foundations** are working with industry leaders such as AOL, Equifax, Google, PayPal, VeriSign, and Yahoo to provide access at Levels of Assurance (LOA) 1-4.

NIH Login

- In production since 2003
- Over 55,000 NIH users, 275 applications, 700 URLs
- 1.7 -2.4 million transactions per day
- Single Sign-On (SSO), including use of Personal Identity Verification (PIV) Cards
- Authenticated web services

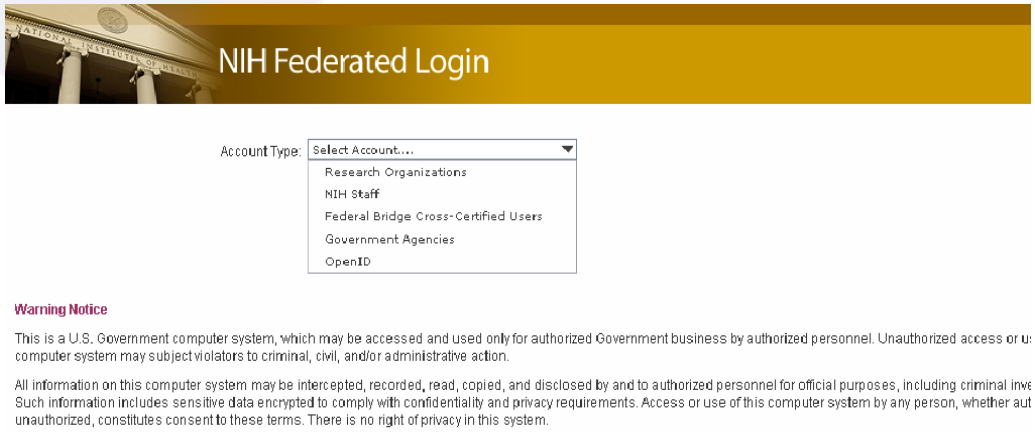


- June 2008 mandated for all new web applications
- May 2010 all Login apps must support PIV
- Dec 2010 all sensitive applications must use two factor
  - Delayed to June 2011- issues with Citrix, VPN and legacy applications, desktops and laptops and Non PIV Holders

CIT
Center for Information Technology

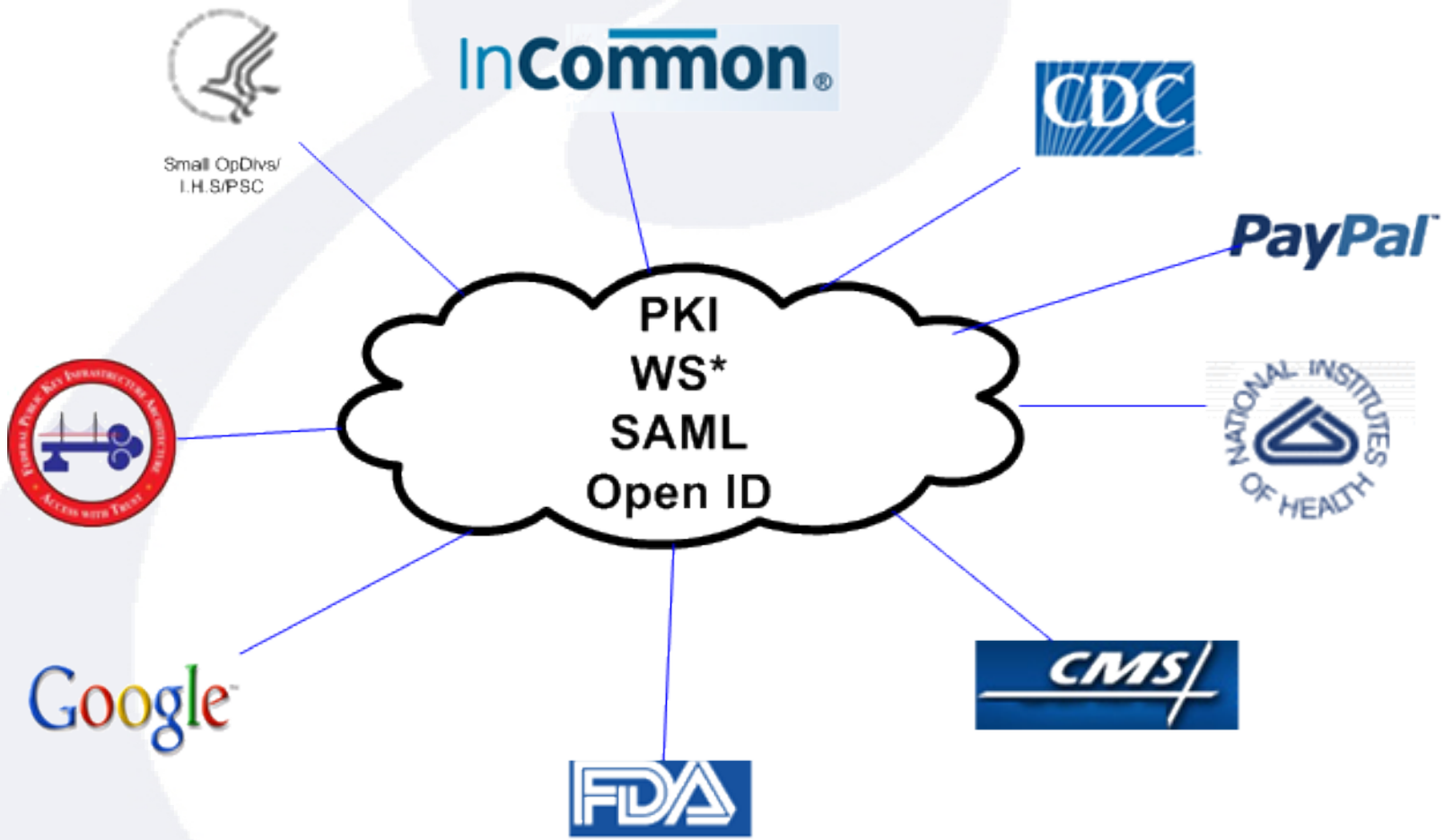
NIH Federated Login

- In production since 2008
- 60 Federated applications
- University participation up 240%
- Over 72,000 external credentials averaging 2-3000 users a week
- Scaled to support 1 Million users on track to support over 500,000 external users by end FY11:
  - wikis, SharePoint, Grids, Library services Acquisition services
  - Cross-agency, government-wide collaborations
  - Enterprise/departmental applications



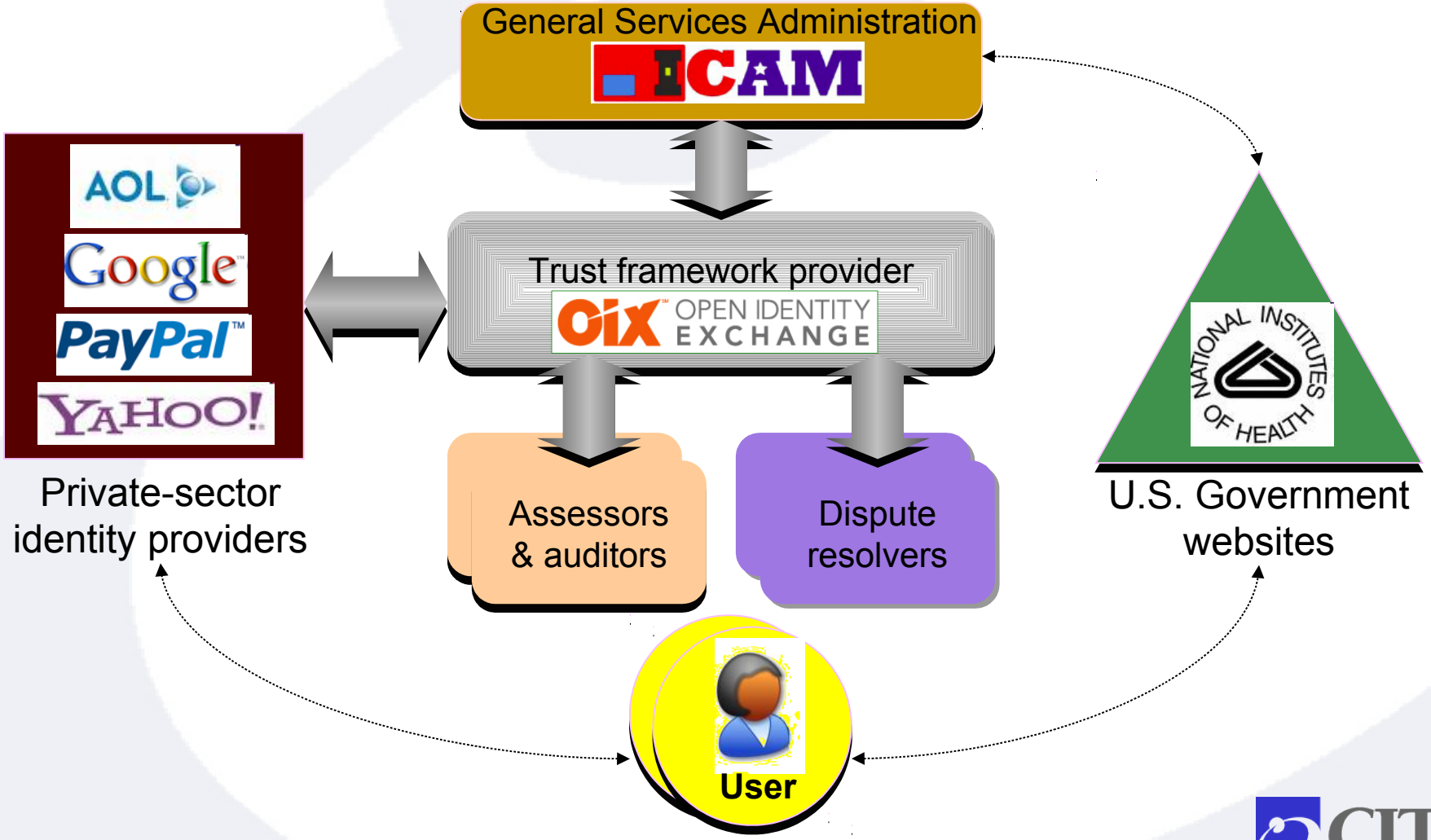
CIT
Center for Information Technology

Federated View



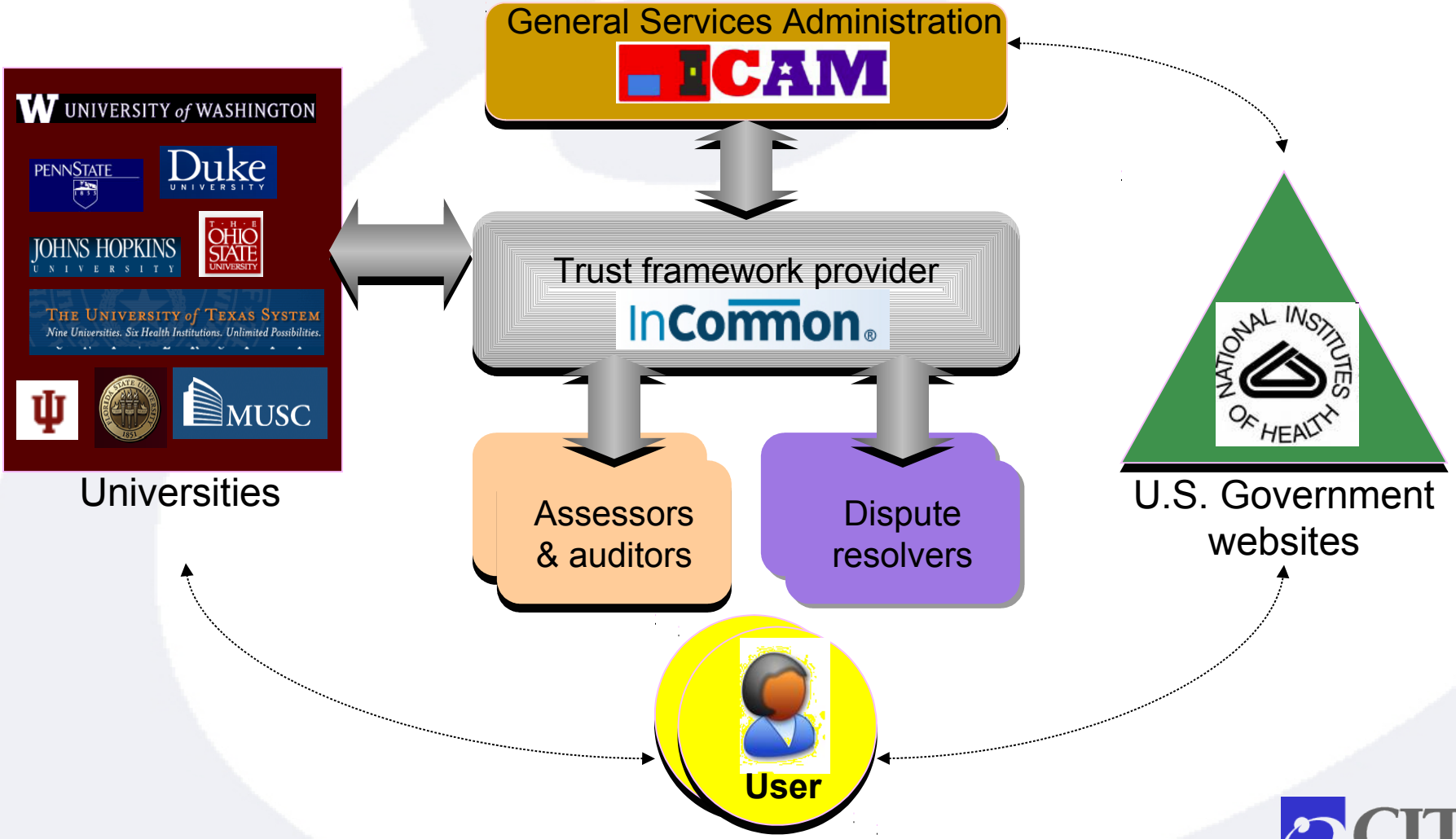
CIT
Center for Information Technology

Federated Authentication at NIH



CIT
Center for Information Technology

Federated Authentication at NIH



Federal Mandates

Mandates for Federated Authentication and Personal Identity Verification (PIV) Card and Common Access Card (CAC) across the Federal Government:

- HSPD-12 “Policy for a Common Identification Standard for Federal Employees and Contractors”
- FIPS 201-1 “Personal Identity Verification of Federal Employees and Contractors”
- NIST SP-800-63 “Electronic Authentication Guideline”
- OMB M-04-04 “E-Authentication Guidance for Federal Agencies”
- OMB M-06-16 “Protection of Sensitive Agency Information”
- OMB M-11-11 “ Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors “

NIH iTrust Key Points

- Aligns with FICAM's IdM reference segment architecture
- Integrates with HHS Operating Divisions and other departments and agencies
- Promotes both interoperability and standards
- Meets the needs of researchers and clinicians
- Offers quick implementation

Current Integration Projects

- **NIH eVIP (electronic Vendor Invoicing Program)**
  - Over 30,000 users and 7,000 vendors across the country will submit invoices, receive payment, and complete other transactions using their own identity credentials
- **NIH eRA (electronic Research Administration)**
  - Over 250,000 researchers and 9,500 institutions worldwide will apply for grants and access funding, while helping eRA monitor grant disbursement
- **National Library of Medicine PubMed Database**
  - Secure access for users with OpenID credentials such as Google and Yahoo
  - 12,000 OpenID users registered in the first six weeks

Current Integration Projects

- **Healthcare Reform Implementation Tracking Tool (HRITT)**
  - HHS, CMS, White House, and other agencies will use MS Project Server to track implementation of the 400+ provisions of the 2010 Patient Protection and Affordable Care Act
- **National Interagency Confederation for Biological Research (NICBR)**
  - Federated access to a group of applications used by researchers from the National Cancer Institute, National Institute of Allergy and Infectious Diseases, Army, Navy, Department of Homeland Security, CDC, and USDA at Ft. Detrick, MD

For Further Information

Debbie Bucci
Manager, Integration Services Center
Division of Enterprise and Custom Applications
Center for Information Technology
National Institutes of Health
Debbie.Bucci@nih.gov

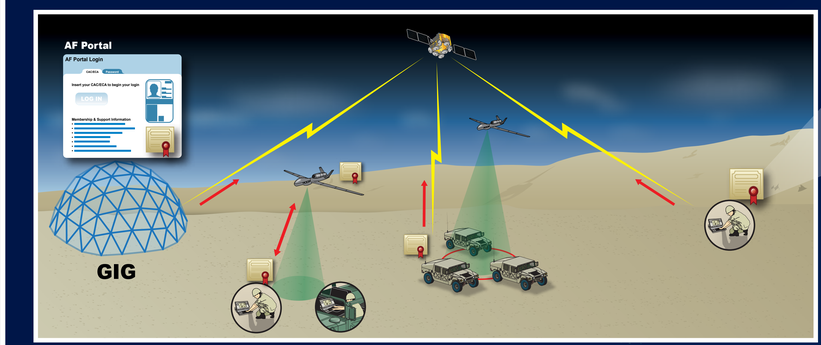
NIH Integration Services Center
NIHISCSupport@mail.nih.gov

NIH Center for Information Technology
www.cit.nih.gov

CIT
Center for Information Technology

Efficient Transmission of DoD PKI Certificates in Tactical Networks

Secured Communications at the Tactical Edge

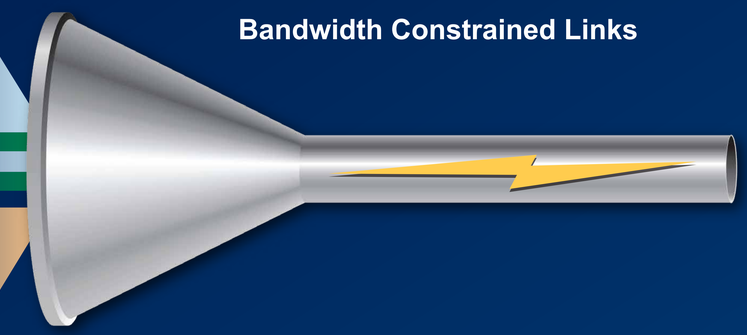


Certificate Profile

- Basic Metadata Fields
- Public Key
- Extension Fields
- Signature
- Application Data

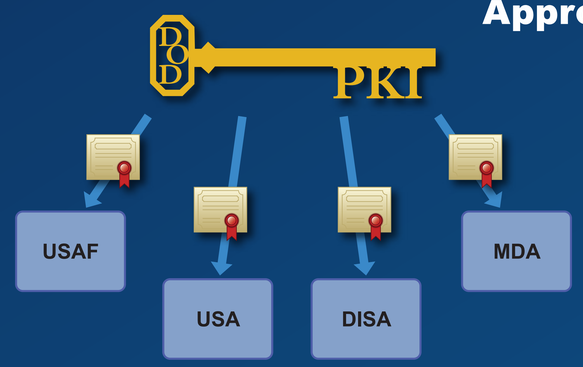
Legend:
- Metadata (human readable)
- Random-appearing data

Bandwidth Constrained Links



Frequent certificate transmission consumes scarce bandwidth
Goal: reduce certificate sizes → more bandwidth for application data

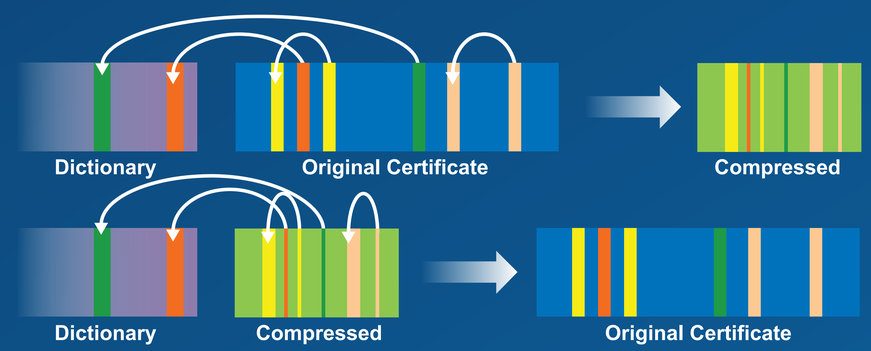
Approach: standard data compression with preplaced dictionary



Similar profiles lead to redundancies in metadata across DoD PKI certificates

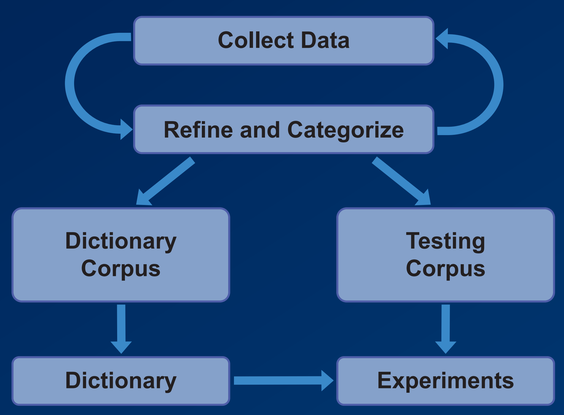
Dictionary

Contains metadata elements common across DoD PKI certificates



Standard data compression removes internal data redundancies
Additional redundancies removed using preplaced dictionary

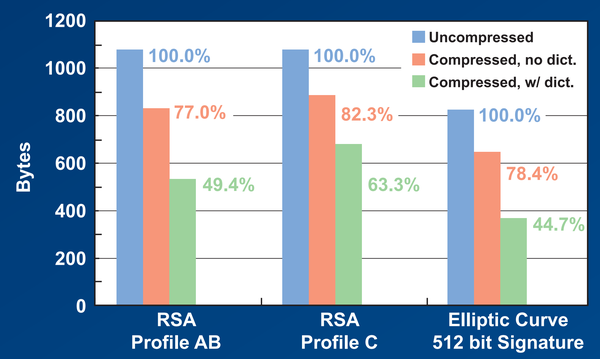
Methodology



Data Set

- Certificates obtained from DoD Global Directory Service
  - 189 for dictionary corpus, 169 for testing corpus
- Drawn from 22 organizations across DoD
- Categorized into distinct profiles
  - Profile AB: RSA 1024 bit signature, ~7 KB dictionary size
  - Profile C: RSA 2048 bit signature, ~11 KB dictionary size

Average Certificate Sizes



Dictionary-aided compression can reliably reduce transmission overhead of DoD PKI certificates

Lincoln Laboratory POC: Sean O'Melia, sean.omelia@ll.mit.edu, Roger Khazan, rkh@ll.mit.edu, and Dan Utin, danu@ll.mit.edu

This work is sponsored by the United States Air Force under Contract FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the authors and are not necessarily endorsed by the United States Government.

445601.ai

1951–2011
LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

themes. There will also be breakouts for each subcommittee to meet individually. The agenda may change to accommodate Committee business. The final agenda will be posted on the Smart Grid Web site at *http://www.nist.gov/smartgrid.*

DATES: The SGAC will hold a meeting on Thursday, March 24, 2011, from 8:30 a.m. until 5 p.m. The meeting will be open to the public.

ADDRESSES: The meeting will be held in the Lecture Room C, in the Administration Building at NIST in Gaithersburg, Maryland. Please note admittance instructions under the **SUPPLEMENTARY INFORMATION** section of this notice.

FOR FURTHER INFORMATION CONTACT: Dr. George W. Arnold, National Coordinator for Smart Grid Interoperability, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8100, Gaithersburg, MD 20899–8100; telephone 301–975–2232, fax 301–975–4091; or via e-mail at *nistsgfac@nist.gov.*

SUPPLEMENTARY INFORMATION: The Committee was established in accordance with the Federal Advisory Committee Act (5 U.S.C. App.).

Background information on the Committee is available at *http://www.nist.gov/smartgrid/committee.cfm.*

Pursuant to the Federal Advisory Committee Act, 5 U.S.C. App., notice is hereby given that the Smart Grid Advisory Committee (SGAC) will hold a meeting on Thursday, March 24, 2011, from 8:30 a.m. until 5 p.m. The meeting will be held in the Lecture Room C, in the Administration Building at NIST in Gaithersburg, Maryland. The primary purpose of this meeting is to review the early findings and observations of each Subcommittee, strategize the Table of Contents for the Committee report to NIST, agree on the page limit for each subcommittee, and look for any common overarching themes. There will also be breakouts for each subcommittee to meet individually. The agenda may change to accommodate Committee business. The final agenda will be posted on the Smart Grid Web site at *http://www.nist.gov/smartgrid.*

Individuals and representatives of organizations who would like to offer comments and suggestions related to the Committee's affairs are invited to request a place on the agenda by contacting Cuong Nguyen at *cuong.nguyen@nist.gov* or (301) 975–2254 no later than March 17, 2011. On March 24, 2011, approximately one-half hour will be reserved at the end of the meeting for public comments, and speaking times will be assigned on a first-come, first-serve basis. The amount of time per speaker will be determined by the number of requests received, but is likely to be about 3 minutes each. Questions from the public will not be considered during this period. Speakers who wish to expand upon their oral statements, those who had wished to speak but could not be accommodated on the agenda, and those who were unable to attend in person are invited to submit written statements to the Office of the National Coordinator for Smart Grid Interoperability, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8100, Gaithersburg, MD 20899–8100; fax 301–975–4091; or via e-mail at *nistsgfac@nist.gov.*

All visitors to the NIST site are required to pre-register to be admitted. Anyone wishing to attend this meeting must register by close of business Thursday, March 17, 2011, in order to attend. Please submit your name, time of arrival, e-mail address, and phone number to Cuong Nguyen. Non-U.S. citizens must also submit their country of citizenship, title, employer/sponsor, and address. Mr. Nguyen's e-mail address is *cuong.nguyen@nist.gov* and his phone number is (301) 975–2254.

Dated: March 2, 2011.

Charles H. Romine,

Acting Associate Director for Laboratory Programs.

[FR Doc. 2011–5250 Filed 3–7–11; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 110124059–1058–02]

Announcing Draft Federal Information Processing Standard (FIPS) 201–2, Personal Identity Verification of Federal Employees and Contractors Standard, Request for Comments, and Public Workshop on Draft FIPS 201–2

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice and request for comments.

SUMMARY: The National Institute of Standards and Technology (NIST) publishes this notice to request comments on Draft Federal Information Processing Standard (FIPS) Publication 201–2, "Personal Identity Verification of Federal Employees and Contractors Standard." Draft FIPS 201–2 amends FIPS 201–1 and includes clarifications of existing text, removal of conflicting requirements, additional text to improve clarity, adaptation to changes in the environment since the publication of FIPS 201–1, and specific changes requested by Federal agencies and implementers. NIST has received numerous change requests, some of which, after analysis and coordination with the Office of Management and Budget (OMB) and United States Government (USG) stakeholders, are incorporated in the Draft FIPS 201–2. Before recommending FIPS 201–2 to the Secretary of Commerce for review and approval, NIST invites comments from the public concerning the proposed changes. NIST will hold a public workshop at NIST in Gaithersburg, MD to present the Draft FIPS 201–2. Please see admittance instructions in the **SUPPLEMENTARY INFORMATION** section below.

DATES: Comments must be received by June 6, 2011. The public workshop will be held on April 18–19, 2011. Pre-registration must be completed by close of business on April 11, 2011.

ADDRESSES: Written comments may be sent to: Chief, Computer Security Division, Information Technology Laboratory, ATTN: Comments on Revision Draft FIPS 201–1, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899. Electronic comments may be sent to: *piv_comments@nist.gov.* Anyone wishing to attend the workshop in person, must pre-register at *http://www.nist.gov/allevents.cfm.* Additional workshop details and webcast will be available on the NIST Computer Security Resource Center Web site at *http://csrc.nist.gov.*

FOR FURTHER INFORMATION CONTACT: William MacGregor, (301) 975–8721, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930, e-mail: *william.macgregor@nist.gov,* or Hildegard Ferraiolo, (301) 975–6972, e-mail: *hildegard.ferraiolo@nist.gov,* or Ketan Mehta, (301) 975–8405, e-mail: *ketan.mehta@nist.gov.*

SUPPLEMENTARY INFORMATION: FIPS 201 was issued in February 2005, and in accordance with NIST policy was due for review in 2010. In consideration of changes in the environment over the last five years and specific requests for changes from USG stakeholders, NIST determined that a revision of FIPS 201–1 (version in effect) is warranted. NIST has received numerous change requests, some of which, after analysis and coordination with OMB and USG stakeholders, are incorporated in the Draft FIPS 201–2. Other change requests

incorporated in the Draft FIPS 201–2 result from the 2010 Business Requirements Meeting held at NIST. The meeting focused on business requirements of Federal departments and agencies. The following is a summary of changes reflected in the Draft FIPS 201–2. Please note that the proposed revision of the document has caused a renumbering of several sections of FIPS 201–1 (version in effect). The section references below are consistent with Draft FIPS 201–2. The changes in Draft FIPS 201–2 are:

• Changes to clarify requirements and editorial corrections are incorporated throughout the document. These changes are not intended to modify the substantive requirements in FIPS 201–1.

• Specific modifications that potentially change an existing requirement or add a new requirement are reflected in the following list.

—In Section 2.1, the second bullet is *replaced* with "A credential is issued only after the National Agency Check with Written Inquiries (NACI) or equivalent is initiated and the FBI National Criminal History Check (NCHC) is completed," to eliminate an inconsistency that was inadvertently introduced by the FIPS 201–1 revision.

—In Section 2.2, the text is *replaced* with a reference to the memorandum from Linda Springer, Director Office of Personnel Management (OPM), dated 31 July 2008, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD–12." The purpose of this change is to update the identity credentialing requirements in accordance with OPM guidance issued after the FIPS 201–1 was published.

—Section 2.3 is *modified* to directly incorporate the content from the I–9 form that is relevant to FIPS 201. This change is made to eliminate confusion that has resulted from I–9 content that is not used by FIPS 201–1 processes; it also provides a more precise requirement statement for the two forms of identity source documents.

—Section 2.3 is *modified* to introduce the concept of a "chain-of-trust," maintained by a PIV Card Issuer, further described in Sections 2.4, 2.5 and 4.4.1. The "chain-of-trust" allows the holder of a PIV Card to obtain a replacement for a compromised, lost, stolen, or damaged PIV Card through biometric authentication. This capability is requested by Federal agencies because the alternative, complete re-enrollment, is time-consuming and expensive. The "chain-of-trust" method can only be used if the PIV Card Issuer has retained biometric data through which an individual can be authenticated.

—Section 2.4 is *added* to define a 1-to-1 biometric match. A 1-to-1 biometric match is necessary to associate a presenting individual with their 'chain-of-trust' record. The objective is to reduce replacement cost to agencies for lost, stolen, or damaged PIV Cards, to reduce the amount of data gathering, and minimize in-person visits without compromising the security objectives of HSPD–12.

—Section 2.4 is *modified* to increase the maximum life of PIV Card from 5 years to 6 years. This revision is made in response to agency requests to synchronize lifecycles of card, certificates, and biometric data.

—Section 2.4.1 is *added* to introduce a special rule for pseudonyms, clarifying the conditions under which pseudonyms may be approved by the sponsoring agency (*i.e.,* for the protection of the cardholder). FIPS 201–1 does not specify requirements for issuing PIV credentials under pseudonyms. This use-case requires a normative list of minimum requirements within the standard.

—Section 2.4.2 is *added* to introduce a grace period for the period between termination of an employee or contractor and re-employment by the USG or a Federal contractor. If re-employment occurs within the grace period, to obtain a new PIV Card, an NCHC is required and a complete NACI is not required. For example, an employee may be detailed to a special assignment for a brief time period and, upon completion of the assignment, return to the original agency. In another case, the PIV Cardholder may move from one Federal agency to another within a short period of time. In each of these situations, repeating the entire identity proofing and identity vetting process when all the necessary information about the individual was previously collected in accordance with FIPS 201–1 is inefficient. The grace period to allow reuse of the existing records held by an agency addresses this inefficiency.

—Section 2.5 is *modified* to restructure the PIV Card maintenance procedures slightly. "Renewal" of a PIV Card to re-collect biometric data, currently a facial image and two fingerprint templates, is required once every twelve years, to update files to account for normal aging. Subsequent to the issuance of FIPS 201–1 and based on comments received by NIST, it is apparent that terms such as "renewal", "reissuance", "replacement", "registration", etc., are used interchangeably and inaccurately and that FIPS 201–1 needs to clearly state the purpose and circumstances under which identity credential renewal is required. Draft FIPS 201–2 introduces normative text to address this ambiguity.

—Section 2.5.2.1 is *added* to recognize legal name changes. Name change is a very common occurrence, and it represents a major change in identity source documents. Specific requirements to manage and record legal name changes correctly and consistently across identity management systems were identified and are included.

—Sections 2.5.3 and 2.5.4 are *added* to provide requirements for post-issuance updates made to the PIV Card after it is issued to the cardholder. These requirements are added in response to agency requests.

—Section 2.5.5 is *added* to provide details on reset procedures for PIN, biometrics or other types of resettable data as per agency requests.

—Section 4.1.4 is *added* to provide visual card topography zones and color specifications from SP 800–104 "A Scheme for PIV Visual Card Topography." SP 800–104 was developed after FIPS 201–1 was published to enhance the uniformity of colors and additional zones needed by agencies.

—Section 4.1.4.1 is *modified* to allow longer names (70 characters) to be printed on the card in the existing zone. This change is made to enable printing of complete names for required accuracy.

—Section 4.1.4.3 is *added* to provide requirements for compliance with Section 508 of the Americans with Disabilities Act. The U.S. Access Board, an independent Federal agency devoted to accessibility for people with disabilities, requested improvements in FIPS 201 to facilitate the use of the PIV Card by people with impaired vision or manual dexterity. For example, an improvement could allow an unsighted person to quickly and positively orient the card by touch when presenting the PIV Card to a card reader.

—Section 4.1.6.1 is *modified* to revise the list of mandatory and optional PIV logical credentials. This section is modified based on the inputs received during the 2010 Business Requirements Meeting described above. The section adds a requirement to collect alternate iris images when

an agency cannot capture reliable fingerprints. This section also specifies a mandatory asymmetric card authentication key as part of PIV logical credentials and adds an optional On-card biometric comparison as a means of performing card activation and PIV authentication mechanism. The section includes hooks for additional keys if they are needed for secure messaging. In addition, NIST proposes that specific key references and their use will be defined in a future special publication.

—Section 4.1.7.1 is *modified* to allow a PIN or equivalent verification data (e.g., biometric data) to activate a PIV Card to perform privileged operations. The requirement that all PIV System cryptographic modules be tested and validated to FIPS 140–2 Security Level 2 (logical) or Security Level 3 (physical) is not changed.

—Section 4.3 is *modified* to make the NACI Indicator optional and to deprecate its use. The NACI Indicator originally was included in the PIV Authentication Certificate to inform relying systems that the background investigation had not been completed before issuing the PIV Card. Since the issuance of FIPS 201–1, timely completion of background investigations has improved, online status checking services are now available, OPM requirements for background investigations have been revised, and OMB reporting requirements are in place. These improvements provide sufficient controls to make the need for storing NACI Indicator on the PIV Card optional and to deprecate its use.

—Section 4.3 is *modified* to add an option to include country(ies) of citizenship of Foreign Nationals in the PIV Authentication Certificate. This change reflects the desirability of electronically reading the affiliation of Foreign Nationals.

—Section 4.5.3 is *added* to allow a possible future inclusion of an optional ISO/IEC 24727 profile that enables middleware a degree of independence from credential interfaces and vice versa and thus provides adaptability and resilience to PIV card evolution.

—Sections 6.2.2, 6.2.3.1, and 6.2.3.2 are *modified* to remove the qualifier "(Optional)" from the requirement for signature verification and certificate path validation in the CHUID, BIO, and BIO–A authentication mechanisms. These signature verification and path validation functions would be mandatory under FIPS 201–2 to achieve the authentication assurance confidence levels shown in Tables 6–2 and 6–3.

—Section 6.2.5 and 6.2.6 are *added* to provide authentication mechanisms based on optional PIV data elements. Specifically, an On-card biometric comparison authentication mechanism is added in Section 6.2.5 and a symmetric card authentication key authentication mechanism is added in Section 6.2.6.

—Appendix A is *removed.*

FIPS 201–1 and Draft FIPS 201–2 are available electronically from the NIST Web site at: *http://csrc.nist.gov/publications/fips/index/html.*

NIST will hold a public workshop on Draft FIPS 201–2 on Monday and Tuesday, April 18 and 19, 2011 at NIST in Gaithersburg, Maryland. The workshop may also be attended remotely via webcast. The agenda, webcast and related information for the public workshop will be available before the workshop on the NIST Computer Security Resource Center Web site at *http://csrc.nist.gov.* This workshop is not being held in anticipation of a procurement activity. Anyone wishing to attend the workshop in person, must pre-register at *http://www.nist.gov/allevents.cfm* by close of business Monday, April 11, 2011, in order to enter the NIST facility and attend the workshop. In accordance with the Information Technology Management Reform Act of 1996 (Pub. L. 104–106) and the Federal Information Security Management Act of 2002 (FISMA) (Pub. L. 107–347), the Secretary of Commerce is authorized to approve Federal Information Processing Standards (FIPS). Homeland Security Presidential Directive (HSPD) 12, entitled "Policy for a Common Identification Standard for Federal Employees and Contractors", dated August 27, 2004, directed the Secretary of Commerce to promulgate, by February 27, 2005, " * * * a Federal standard for secure and reliable forms of identification (the 'Standard') * * * ," and further directed that the Secretary of Commerce "shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies."

E.O. 12866: This notice has been determined not to be significant for purposes of E.O. 12866.

Dated: February 17, 2011.

Charles H. Romine,

Acting Associate Director for Laboratory Programs.

[FR Doc. 2011–5259 Filed 3–7–11; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

Proposed Information Collection; Comment Request; Marianas Trench Marine National Monument Knowledge and Attitudes Survey

AGENCY: National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice.

SUMMARY: The Department of Commerce, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to take this opportunity to comment on proposed and/or continuing information collections, as required by the Paperwork Reduction Act of 1995.

DATES: Written comments must be submitted on or before May 9, 2011.

ADDRESSES: Direct all written comments to Diana Hynek, Departmental Paperwork Clearance Officer, Department of Commerce, Room 6616, 14th and Constitution Avenue, NW., Washington, DC 20230 (or via the Internet at *dHynek@doc.gov*).

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of the information collection instrument and instructions should be directed to Dr. Stewart Allen, (808) 944–2186 or *Stewart.Allen@noaa.gov*.

SUPPLEMENTARY INFORMATION:

I. Abstract

President George W. Bush established the Marianas Trench Marine National Monument (Monument) on January 6, 2009, by Presidential Proclamation 8335. The monument includes approximately 95,216 square miles within three units in the Mariana Archipelago. The Mariana Trench Unit is almost 1,100 miles long and 44 miles wide and includes only the submerged lands. The Volcanic Unit consists of submerged lands around 21 undersea mud volcanoes and thermal vents along the Mariana Arc. The Islands Unit includes only the waters and submerged lands of the three northernmost Mariana Islands: Farallon de Pajaros or Uracas; Maug; and Asuncion, below the mean low water line. Within the Islands Unit of the monument, commercial fishing is prohibited but sustenance, recreational, and traditional indigenous fishing can be allowed on a sustainable basis.

The Secretary of the Interior has management responsibility for the monument, in consultation with the Secretary of Commerce who, through

Towards a method for managing distributed access entitlement and access certification (Can we trust that AuthZ attribute?)

Problem:

Federation agreement documents may authorize access rights for collaboration partners, yet they alone do not fulfill compliance requirements for authorization. If we must produce audit data for internal access certification, aren't audit data also required for ABAC and distributed AuthZ?

Example Control Requirements:

- NIST SP 800-53 Rev 3 AC-3 ACCESS ENFORCEMENT: Control Enhancements...(2) The information system enforces dual authorization, based on organizational policies and procedures...Dual authorization mechanisms require two forms of approval to execute.
- Payment Card Industry (PCI) Data Security Standard: Implement Strong Access Control Measures

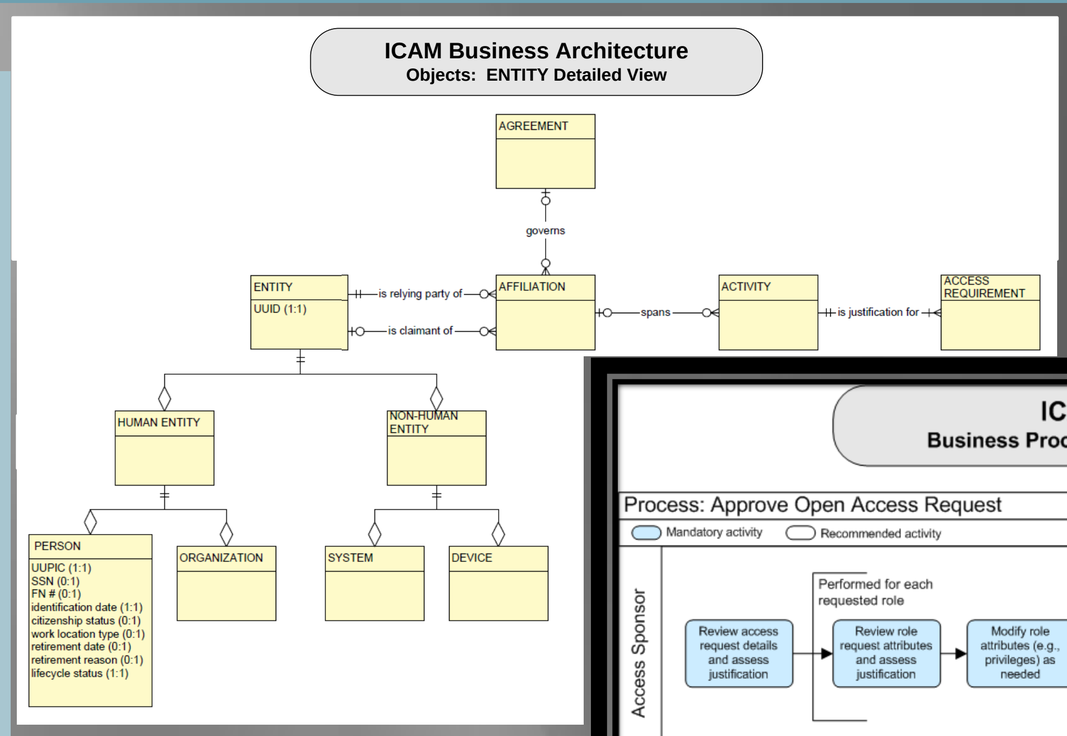
Requirement
7: Restrict access to cardholder data by business need to know
7.1.3 Requirement for a documented approval by authorized parties specifying required privileges.
7.1.3 Confirm that documented approval by authorized parties is required (in writing or electronically) for all access, and that it must specify required privileges.

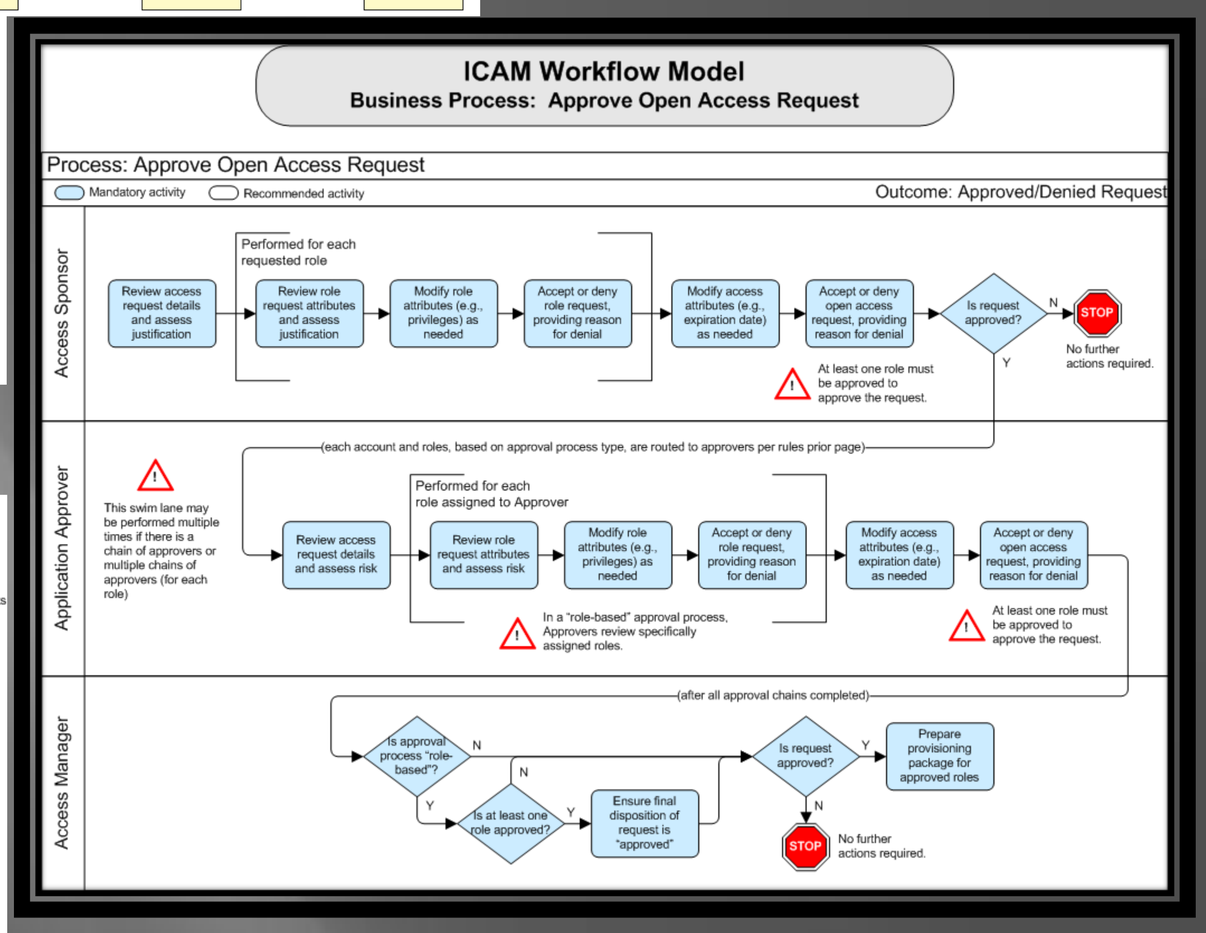
Description/As-Is:

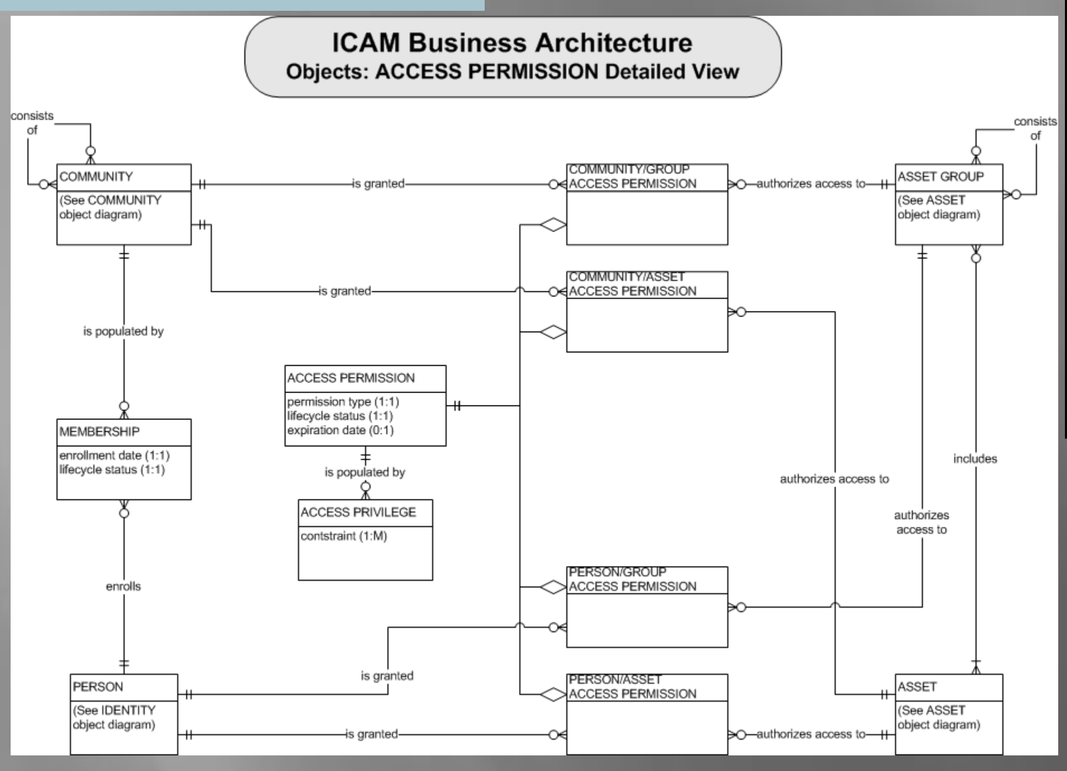
The As-Is architecture already supports the ability to associate a Person with an affiliation through an agreement.

The As-Is architecture also addresses the requirement for explicit Access Permission to be granted, enforcing separation of duties. This can be done on a person-by-person basis, or through access granted to a Community.

As implemented today, there is an implicit assumption that the person involved in requesting, sponsoring, and approving access requests is a "NASA" Person.







A simplified table entry illustrates that for each Access Permission granted, there is an auditable entry in the Policy Administration Point that shows who requested, sponsored, and approved the access.

Access Permission	User	Requestor	Sponsor	Approver
AssetAPrivilegeB	Person:1234567	2345678	3456789	4567890
AssetAPrivilegeA	Community:1234	2345687	3456798	4567890

Requirements Mapping/To-Be:

Access Permission	User	Requestor	Sponsor	Approver
AssetAPrivilegeB	Organization:Agreement:Person:1234567	Organization:Agreement:2345678	Organization:Agreement:3456789	Organization:Agreement:4567890
AssetAPrivilegeA	Organization:Agreement:Community:1234	Organization:Agreement:2345687	Organization:Agreement:3456798	Organization:Agreement:4567890

Proposition:

Extend the current architecture to support registration of Access Permissions to federated People and Communities

Register federation agreements in Policy Administration Points
Add organization/agreement attributes to Access Permission registries
Send info in SAML assertion; register table entry in NAMS at point of access.

Questions:

- What is the best person identifier from an external source? We assume UUID, although many organizations do not support UUID today.
- Do we need standard organization identifiers? FASC-N can be used for Federal entities; it gets more complicated in the non-Federal space.
- What happens when we federate with a federation?
- How do we know freshness? Do we do it every time we have a transaction? How "sticky" should the authorization be?

Next Steps:

- Achieve consensus on the problem space and compliance requirements
- Explore technical approaches
  - SAML Profile, attribute schemas
  - SPML
  - BAE
- Define federation agreements/interface definition agreements
- Define Interconnection Security Agreement (ISA) / modifications

Corinne S. Irwin, NASA
Corinne.S.Irwin@nasa.gov
202-358-0653

Dennis C. Taylor, NASA/ASRC Primus Solutions
Dennis.C.Taylor@nasa.gov
301-286-4290

TRUST IN NATIONAL IDENTITY MANAGEMENT SYSTEMS: EXPLORING CITIZEN RISK PERCEPTIONS

Adrian Rahaman and Professor M. Angela Sasse
Human-Centered Security, Privacy, Identity and Trust (HC-SPIT) University College London, UK

Current Trust Research. Trust is needed in situations of risk [1]. While there has been some work in exploring combined trust-risk models [2][3], the available trust model for N-IDMS is absent of risk [4]. Furthermore, the N-IDMS trust model is focused on intrinsic qualities of the individual (beliefs, attitudes, and personalities); it does not link trust development to the "design" of the N-IDMS.

Our Research. How do individuals perceive N-IDMSs?
How to individuals risk perceptions develop, and how might that influence their intentions to trust and accept an N-IDMS?

There is currently no guidance on how to develop N-IDMSs that are trustworthy and acceptable. This study aims to fill this gap, by developing an understanding of how individual's perceive risk in N-IDMSs, and how it may impact their trusting intentions towards such systems.

Findings. The research shows that individuals' tendency to accept an N-IDMS may be swayed by their perception of risk; developed through: problem evaluation, system assessment, and security concerns

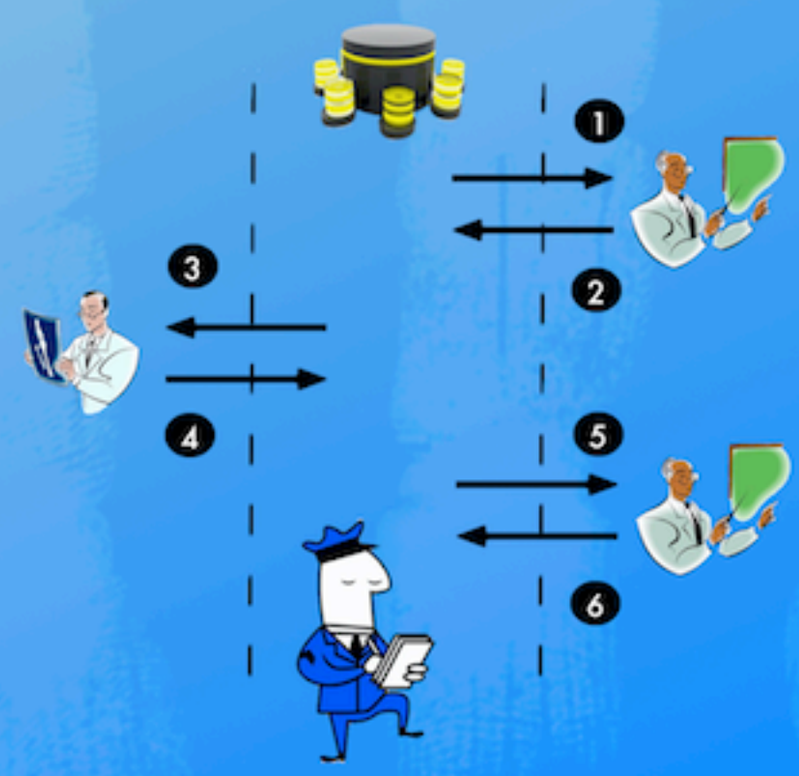
[1] Riegelsberger, J., Sasse, M. A., & Mccarthy, J. D. (2005). The mechanics of trust: A framework for research and design. International Journal of Human-Computer Studies, 62(3), 381-422

[2] Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. International Journal of Electronic Commerce. ME Sharpe.

[3] Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' Information Privacy Concerns (IUIPC): the construct, the scale, and a causal model. Information Systems Research, 15(4), 336-355

[4] Li, X. (2004). Trust in national identification systems: a trust model based on the TRA/TPB.

Methodology. 14 focus groups 3 participants each 6 sceaniors developed to aid discussion *



1. Teacher is concerned about child. Checks database, no records.

2. Enters notes about concerns into child's entry on the database.

3. Doctor has suspicions of abuse. Checks database, not enough convincing evidence.

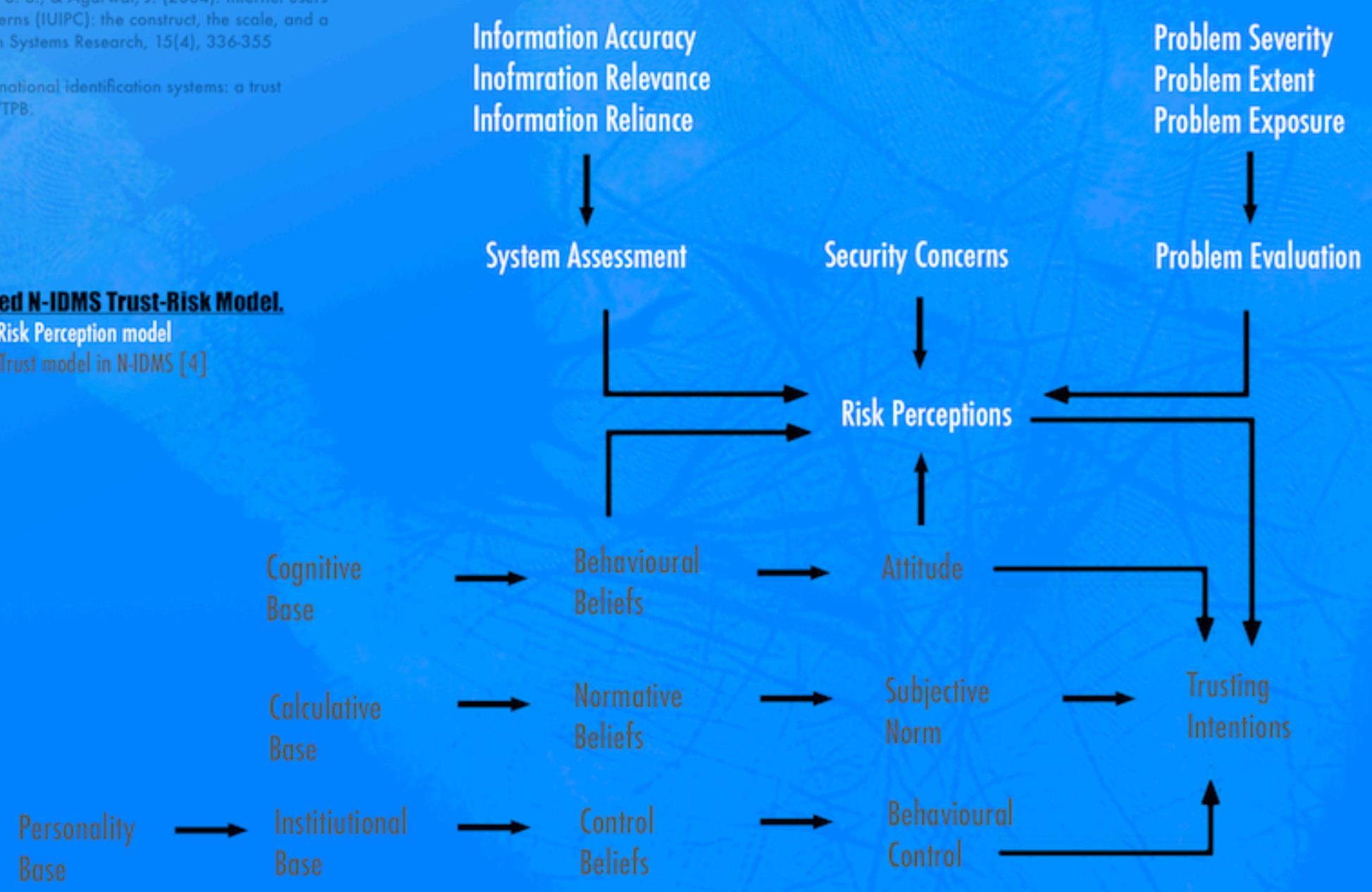
4. Notes suspicions on child's record on the database.

5. Teacher is further concerned. Finds similar indications in database.

6. Informs authorities.

* Scenarios: child abuse (illustrated above); personal debt; obesity; welfare fraud; crime; national identity cards.

Combined N-IDMS Trust-Risk Model.
Proposed Risk Perception model
Li (2004) Trust model in N-IDMS [4]



a.sallehabrahaman@cs.ucl.ac.uk a.sasse.ucl.ac.uk
ADRIAN RAHAMAN | M. ANGELA SASSE | University College London

PKAuth: A Social Login Protocol for Unregistered Apps

Francisco Corella and Karen Lewison
Pomcor

Dangers of Social Login

Social login allows an application to delegate authentication to a social site and gain access to the user's social context. Examples: Login with Facebook, Twitter, LinkedIn, etc.

Social login is becoming very popular. But social login uses OAuth, and OAuth requires **registration of the application with the site**. And a social site has become dominant (Facebook).

Login with Facebook may become the **de facto standard** for user authentication on the Web. Then:

- All applications will have to **register with Facebook** just to be able to authenticate their users.
- **Facebook will have the power to disable any Web application by revoking its registration.**

Dire Consequences

Compulsory application registration is very bad for:

- Web applications, which can be disabled by Facebook
- Users who lose access to an application if Facebook revokes the application's registration
- Facebook competitors, who will be at a great disadvantage
- The government, which may have to step in
- Facebook, which may face government regulation

We Need a Social Login Standard…

- …that does not require registration of the application with the site
- …that allows the user to choose any site (federation)
- …that does not have the phishing vulnerabilities and other security flaws of OAuth and OpenID

A Candidate: PKAuth

PKAuth relies on the **Web's PKI** rather than registration to authenticate the application and identify it to the user

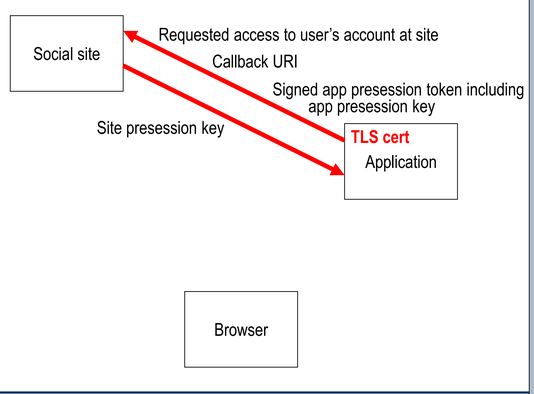
	OAuth	PKAuth
Application authentication based on…	Shared secret established by registration	App's existing TLS certificate and private key
Identification of application to the user based on…	Information obtained by registration	Information contained in TLS certificate

PKAuth Protocol Flow

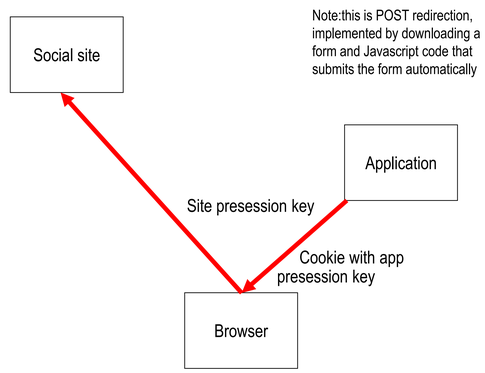
Step 1: User specifies social site

Step 2: Application obtains site info from well-known file

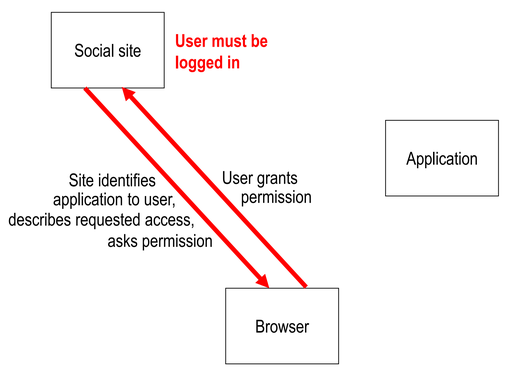
Step 3: Application sends direct request



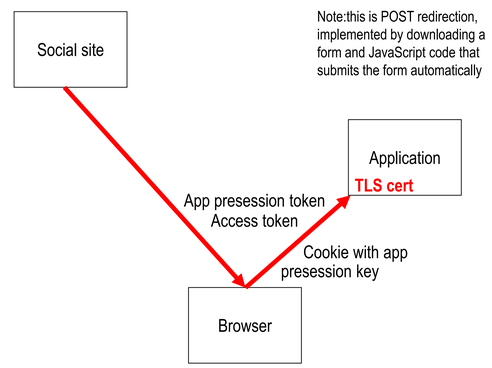
Step 4: Application redirects browser to site



Step 5: Site verifies user is logged in, identifies application to user, asks permission

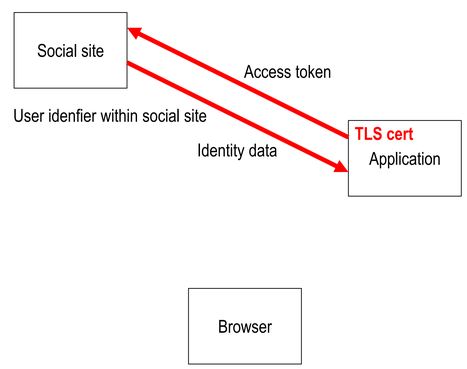


Step 6: Site redirects browser to application



Application verifies presession token signature.
Application verifies that presession key is in presession token.

Step 7: Application gets user identity data

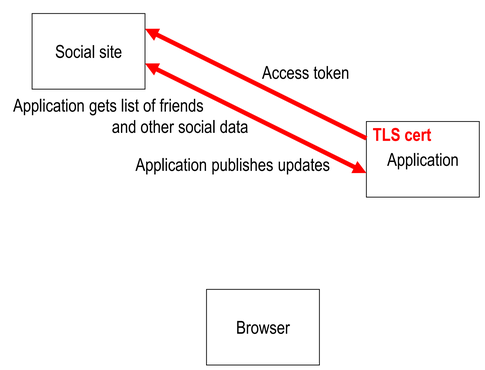


Site verifies association between access token and certificate

Step 8: Application logs user in

User ID within application = user ID within site + site domain name
Identity data used to update or create user account

Step 9: Application accesses user's social context



Site verifies association between access token and certificate

Browser-Resident Applications

Include AJAX applications implemented in JavaScript, rich applications implemented in Flex or Silverlight.

TLS cert and private key reside in server-side component.

Steps 3, 7, 9: connections from browser to site proxied through server-side component, which authenticates with TLS certificate and private key.

Step 4: client-side component creates form in window, tab or frame, and submits form.

Step 6: server-side component receives redirected request and downloads it to client-side component.

Native Applications

Each application instance running in a user's machine has its own TLS client certificate and private key, used in steps 3, 7 and 9. The instance certificate is backed by an application certificate.

Step 4: application instance launches external browser.

Step 6: the callback URI is a local URI, or a URI with a custom scheme, or a URI that targets and ancillary Web server. If a Web server is used, it uses the same application certificate that backs the instance certificates as a TLS server certificate.

Security Properties

Protection against phishing attacks: user is never asked to provide credentials on the fly.

Protection against CSRF attacks on the site: traditional countermeasure works because user is logged in.

Protection against CSRF attacks on the application: provided by presession key in cookie

Protection against DOS attacks on callback endpoint: provided by signed presession token.

Protection against DOS attacks by storage exhaustion: neither site nor application keep storage allocated while waiting for input from an unauthenticated user.

To Do

Produce a formal specification.

Create open source reference implementations.

Use PKAuth to implement decentralized social networks.

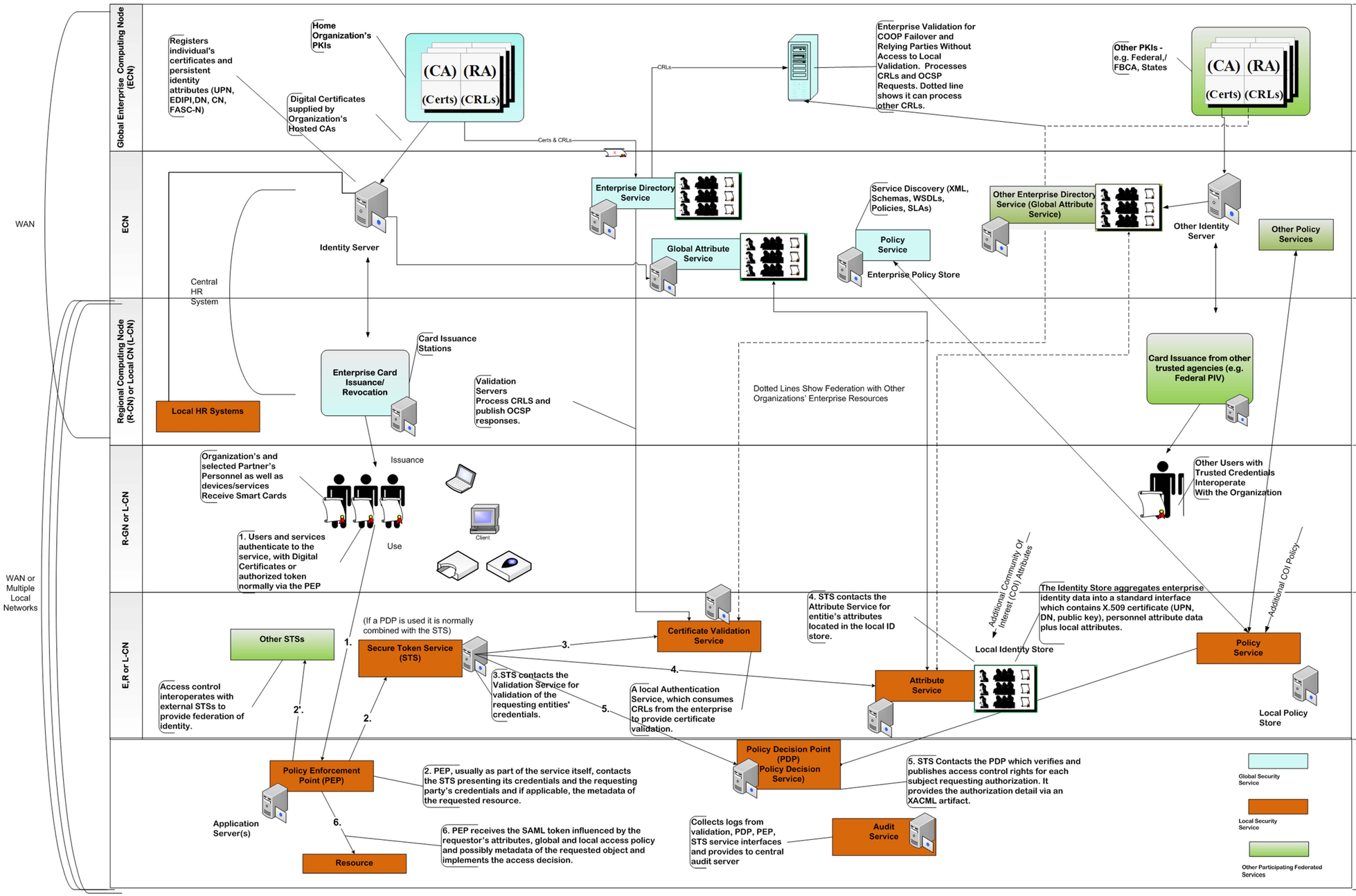
Have PKAuth adopted as a social login standard.

Paper Available At…

http://pomcor.com/whitepapers/PKAuth.pdf.

http://HomelandSecurityConsultants.net
Robert.Cope@homelandsecurityconsultants.net

System Diagram of Federated Identity, Authentication and Authorization using X.509 Certificates and SAML



Some Relevant Standards (Not Exhaustive and Some can show up in Multiple Layers)

Enterprise Infrastructure & Trust Anchors

RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework)
RFC 3874 (SHA2)
RFC 3280 (Certificate and CRL Profile)
RFC 2560 (Online Certificate Status Profile)
RFC 5055 (Server-based Certificate Validation Protocol)
OASIS Enterprise Key Management Infrastructure and Protocol

Enterprise Identity Issuance and Discovery Infrastructure

FIPS 201
OASIS Service Provisioning Markup Language
OASIS Universal Description Discovery and Integration
GSA Backend Attribute Exchange
OASIS WS-Policy
HSPD12 Backend Attribute Exchange Architecture and Interface Specification

Enterprise Credentialing

ISO7816 identification card standard
ISO 14443 RFID cards
Global Platform - The Standard for Smart Card Infrastructure
Telecommunications standard
NIST SP 800-73 Interfaces for Personal Identity Verification
International Committee for Information Technology Standards 378 fingerprint template
OASIS Service Provisioning Markup Language

Relying Parties – Individuals and Services

ISO7816 identification card standard
ISO 14443 RFID cards
Telecommunications standard
NIST SP 800-73 Interfaces for Personal Identity Verification
International Committee for Information Technology Standards 378 fingerprint template
OASIS Service Provisioning Markup Language
NIST SP 800-116 Use of PIV Credentials for PACS

Authentication and Access Control

OASIS Security Assertion Markup Language
OASIS WS-Security Policy
OASIS WS-Policy Attachment
OASIS WS Trust
OASIS eXtensible Access Control Markup Language
OASIS WS-SecureConversation
NIST
X.509 Attribute Sharing Profile (XASP)
Assertions and Protocols for the OASIS
Security Assertion Markup Language (SAML) V2.0

Access Control/Auditing

NIST Special Publication (SP) 800-92, Guide to Computer Security Log Management
FICAM Framework PACS & LACS Modernization
NSTIC Framework
. NIST SP 800-116 Use of PIV Credentials for PACS
FIPS 201-1 Information Assurance Levels for Logical and Physical Access
FICAM Framework Access Control Convergence

Unified Identity for Access Control

Carl Ellison

7 April 2011

IDtrust

Trust Insiders

Instruct Outsiders

This electronic message contains information from the law firm of _____. The contents may be privileged and confidential and are intended for the use of the intended addressee(s) only. If you are not an intended addressee, note that any disclosure, copying, distribution, or use of the contents of this message is prohibited.

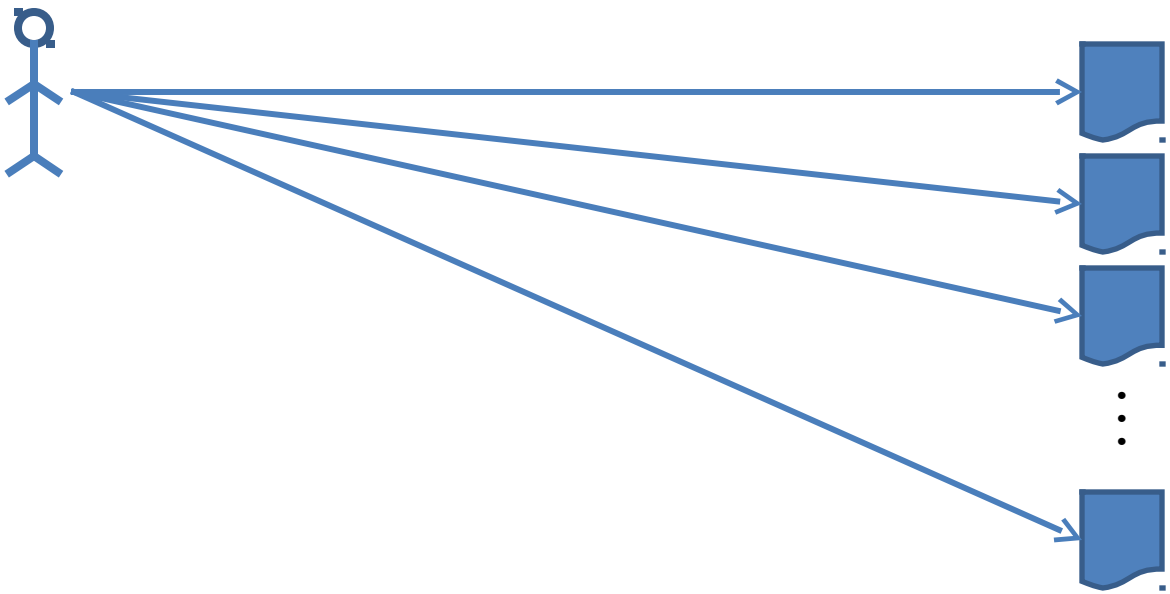
If you have received this e-mail in error, please delete this message and any attachments and contact me at _____.com.

Enforcement by Technical Means

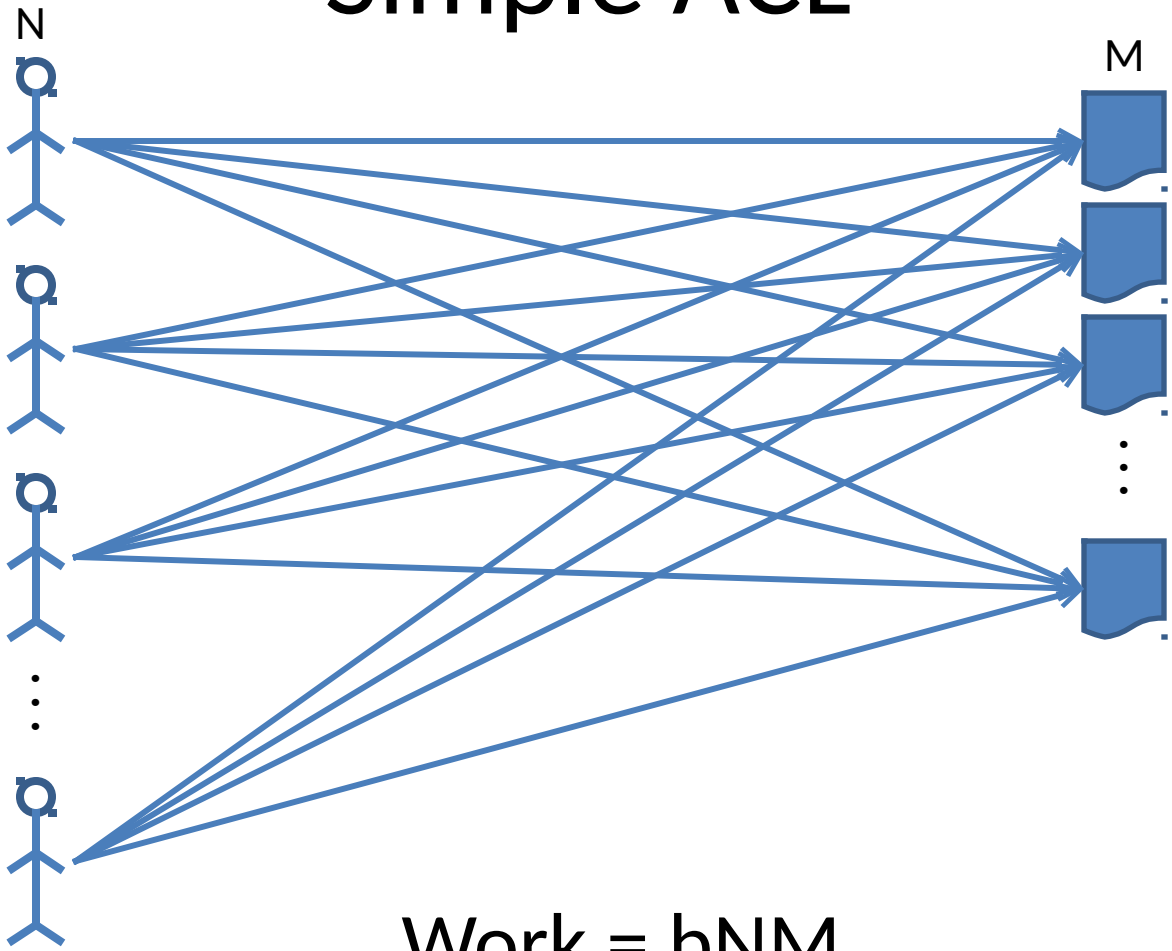
- Specific access control:
  - Account login
  - Session with cached ID(s)
  - ACLs on files
- Simple ACL, one per file
  - List of IDs of those permitted to access the file
  - If one of your cached IDs matches one on the ACL then you get access.

Simple ACL

Simple ACL



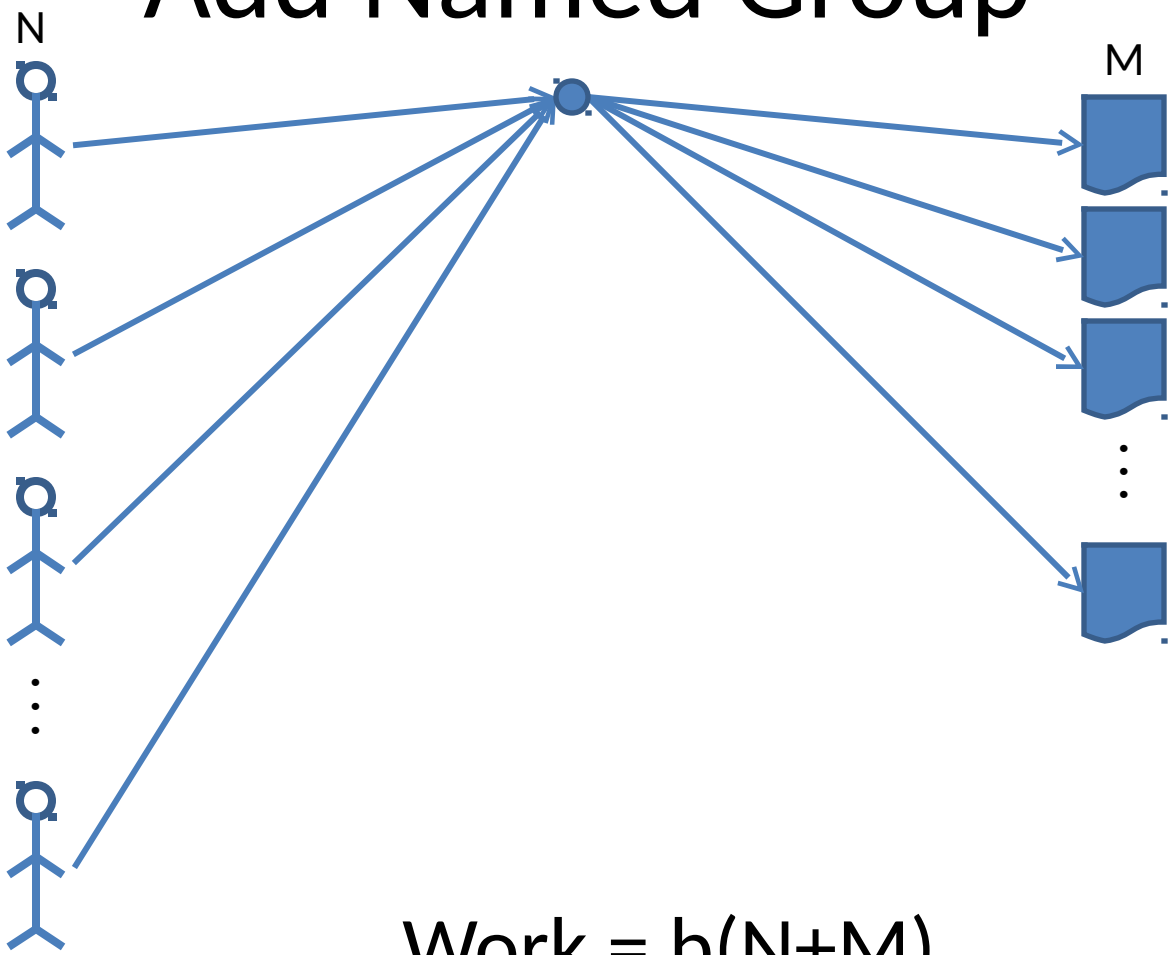
Simple ACL



Work = bNM

b=30 sec; N=5e4; M=3e5; Work ≈ 60000 man-yrs

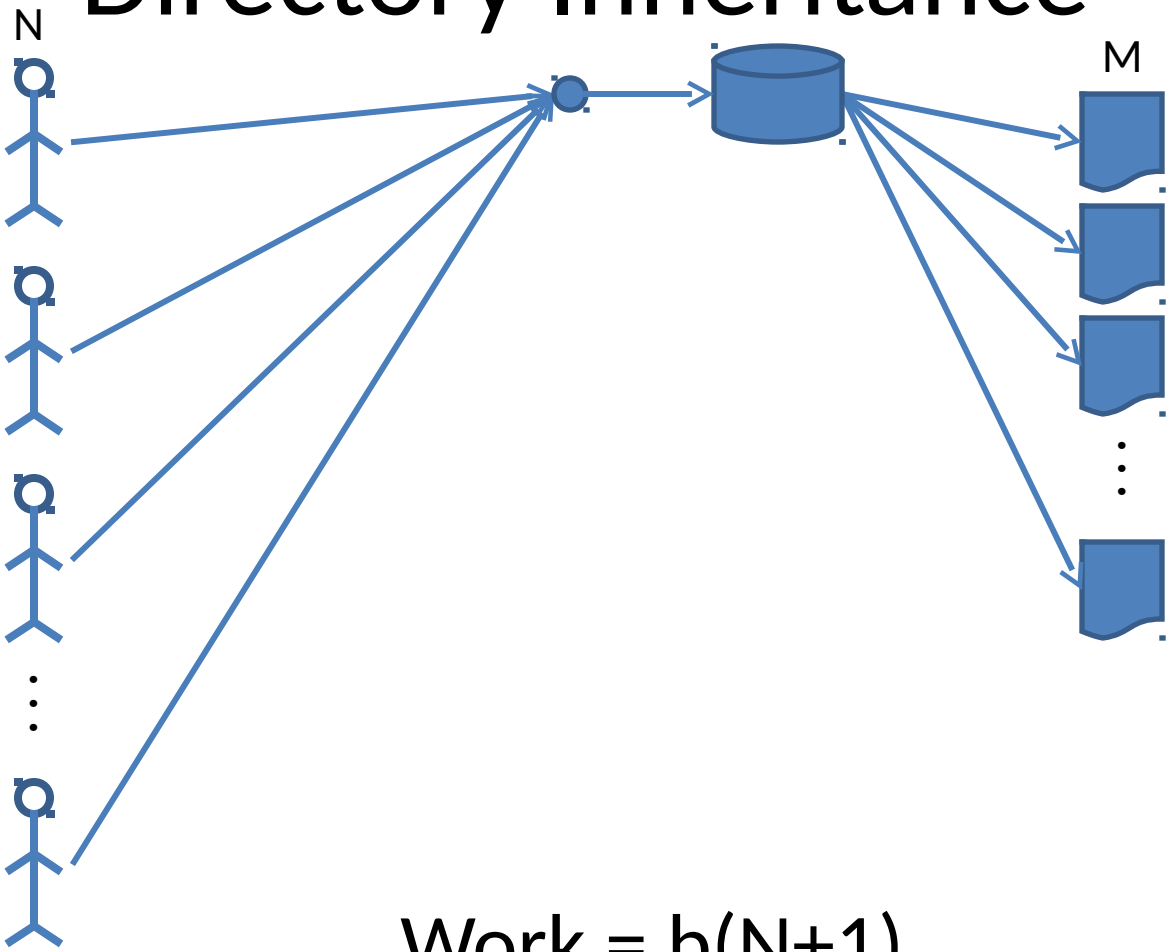
Add Named Group



Work = b(N+M)

b=30 sec; N=5e4; M=3e5; Work ≈ 73 man-wks

Directory Inheritance



Work = b(N+1)

b=30 sec; N=5e4; M=3e5; Work ≈ 10 man-wks

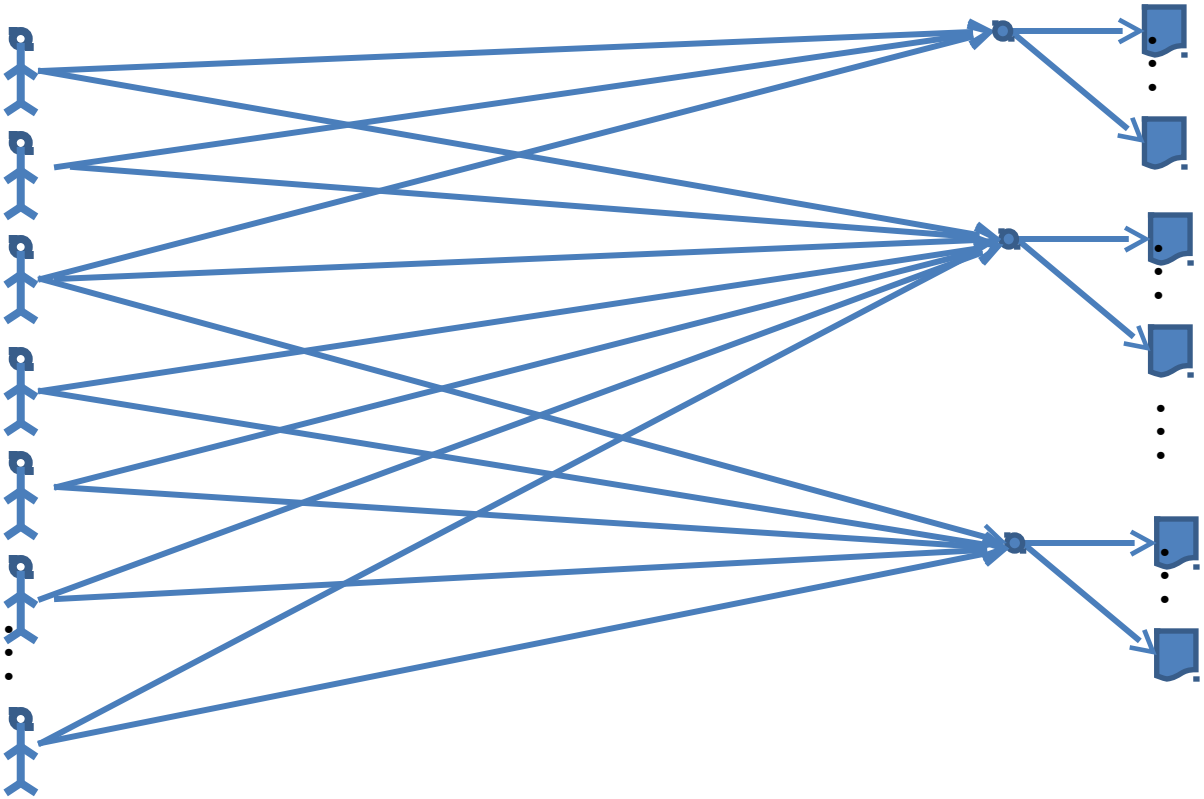
Machinery To Do ACLs and Groups

- Security IDs (SIDs)
- Implemented within the OS
- Each OS does it differently, but I'll use a subset of Windows™ as the example here
  - It is very common.
  - It includes both group definitions and directory inheritance.

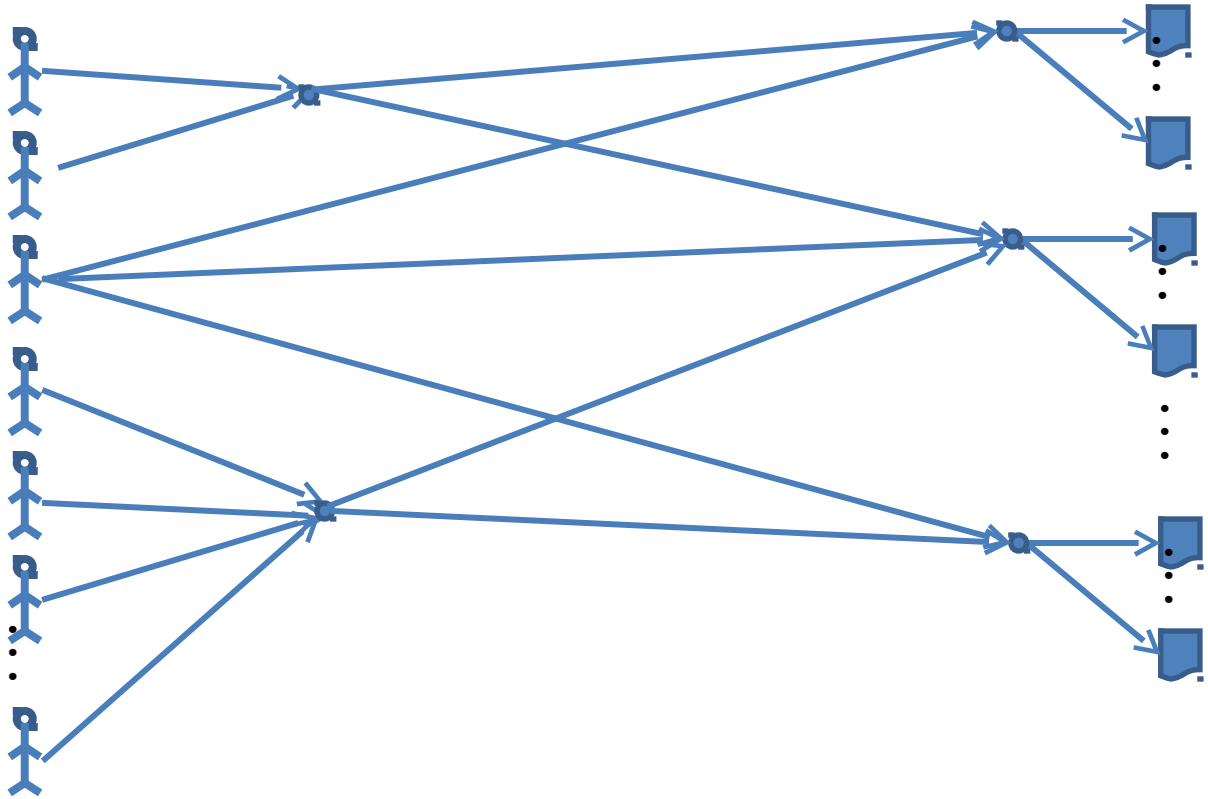
Group Definition in Windows™ Today

- SID = (Domain ID, Relative ID) = (D, R)
  - Each SID has a printable name, local to the Domain, but we don't deal with that here.
- Same SID format for individuals and groups
- ACL is list of SIDs; Group is a list of SIDs
- Groups are defined in Active Directory™ by:
  - "(D, R_1) is member of (D, R_2)"
  - only a domain administrator of D may make or delete that definition.

Multiple Projects



Equivalent Graph



Same graph, but fewer links, so less cost.

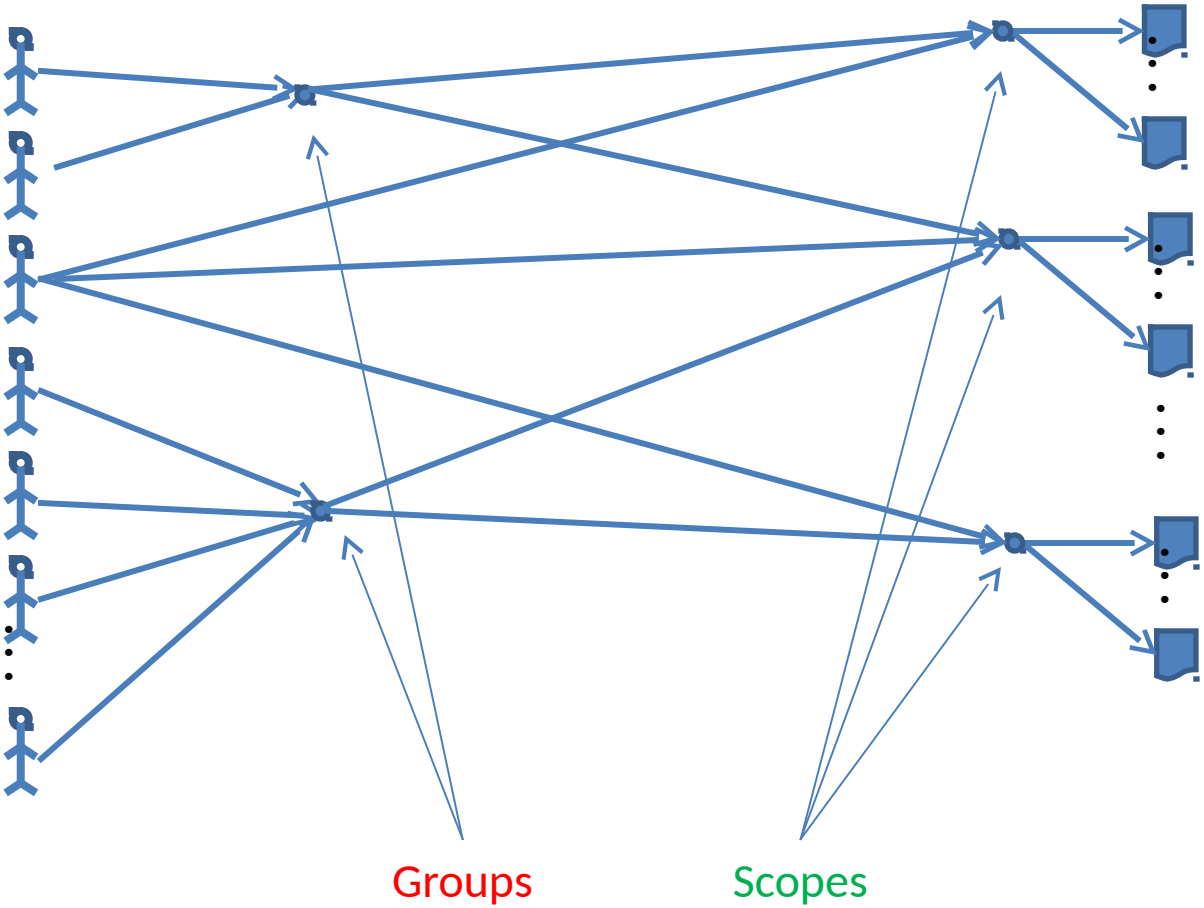
Groups as Org Chart

- Nested named groups allow us to capture the relevant levels of an org chart, for example:
  - Software Developers
    - Core Operating System
      - File system
      - Scheduler
      - Crypto
    - Shell
      - Explorer
      - Control Panel
- It is often easier to express policies in terms of those org chart groups rather than individuals.
- If we want RBAC, we can express roles as SIDs, using the group machinery.

Scopes

- On the resource side, we can also lump files together in groups of resources, called **scopes**
  - This can be done with directories, if all files are on one machine, with propagation of ACLs down the directory structure.
  - If the files span multiple machines, then scopes can be defined using the group mechanism, as we show in our examples here.

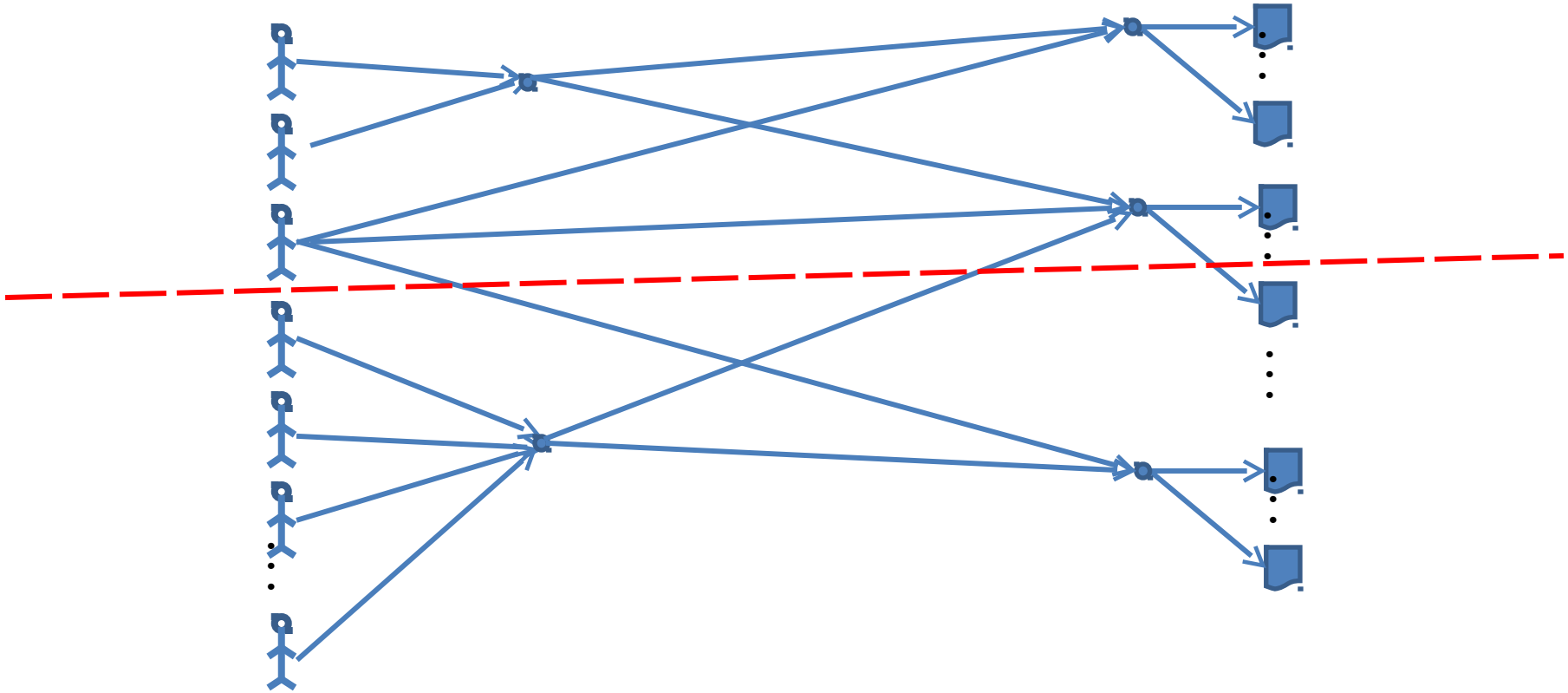
Groups and Scopes



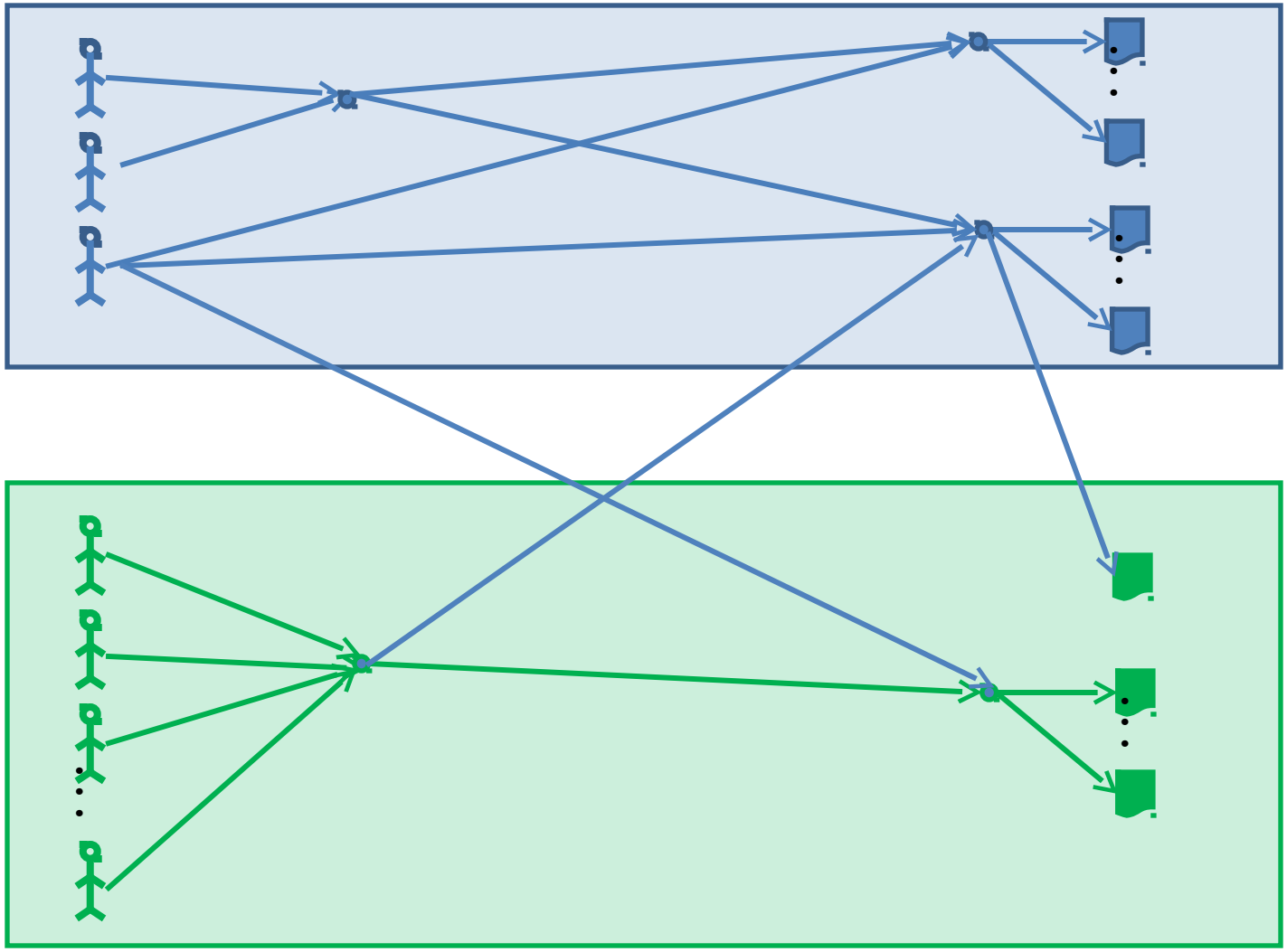
Pretty Good Stuff

- With the machinery we have today, we get SIDs for IDs, groups, roles and scopes.
- Groups and scopes can be nested as deeply as we want.
- We can represent an org chart with nested groups.
- We can represent a project hierarchy of files with nested scopes.
- So, what’s the problem?

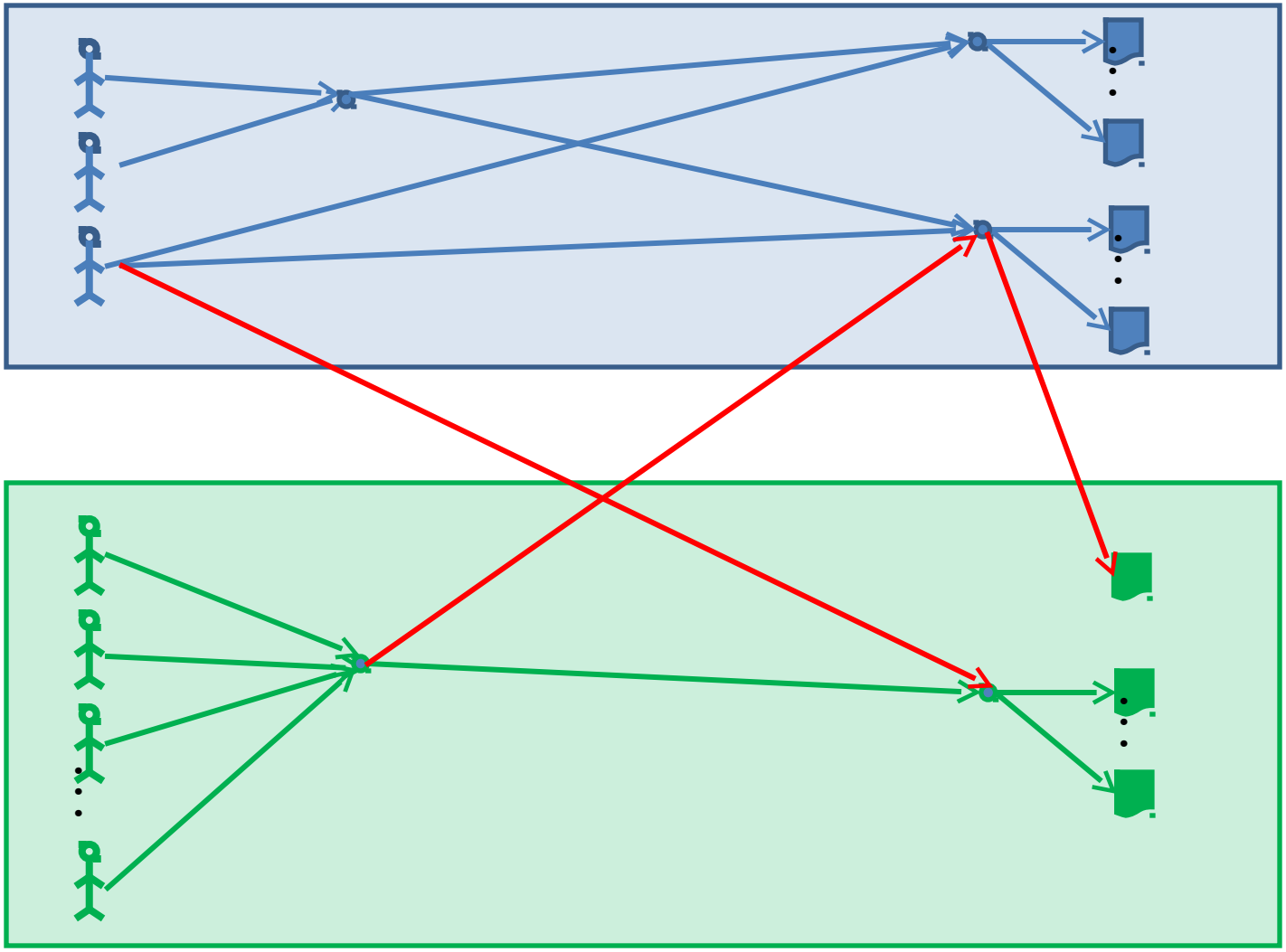
Multiple Organizations



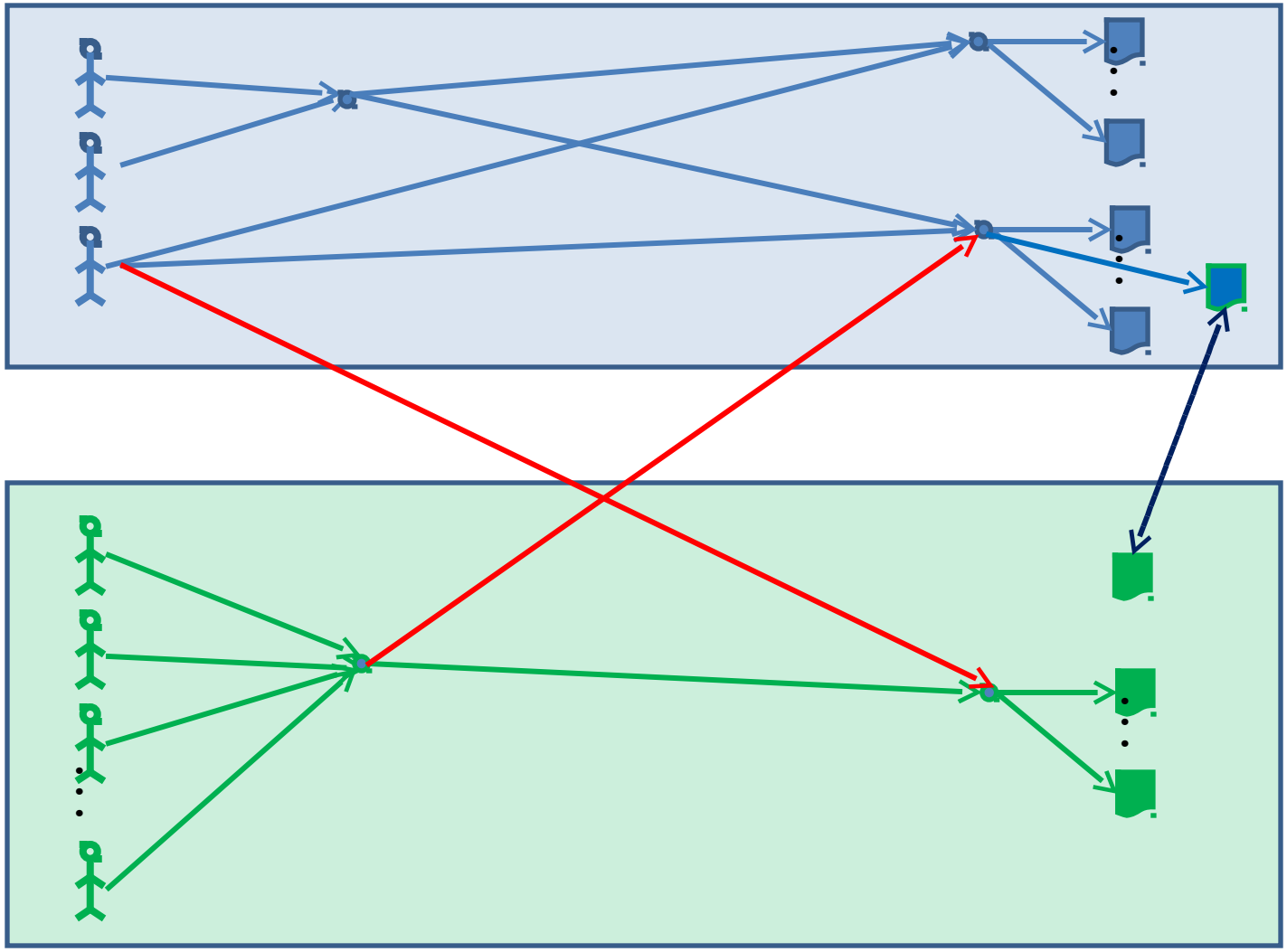
Crossing Organization Boundaries



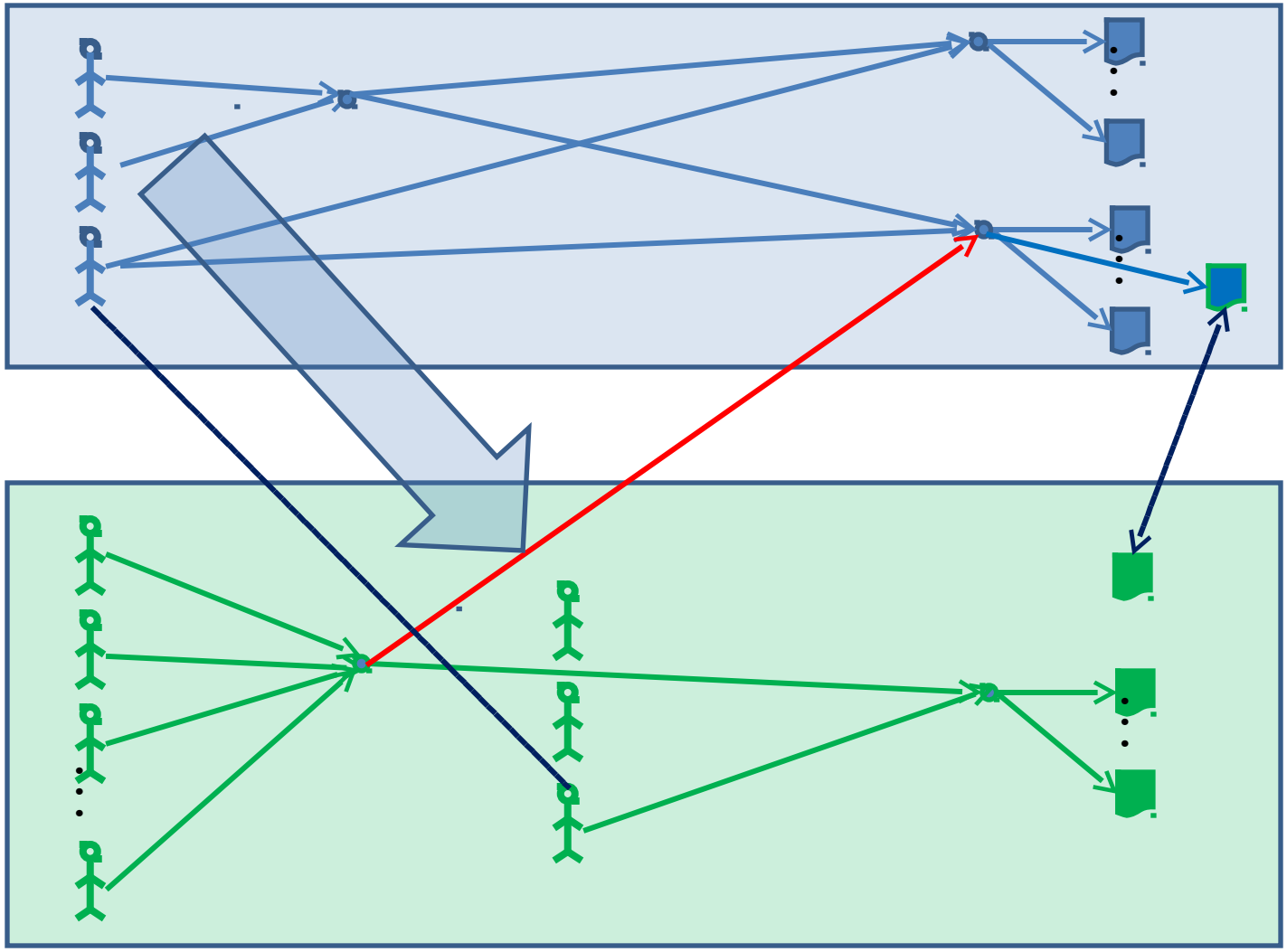
Crossing Organization Boundaries



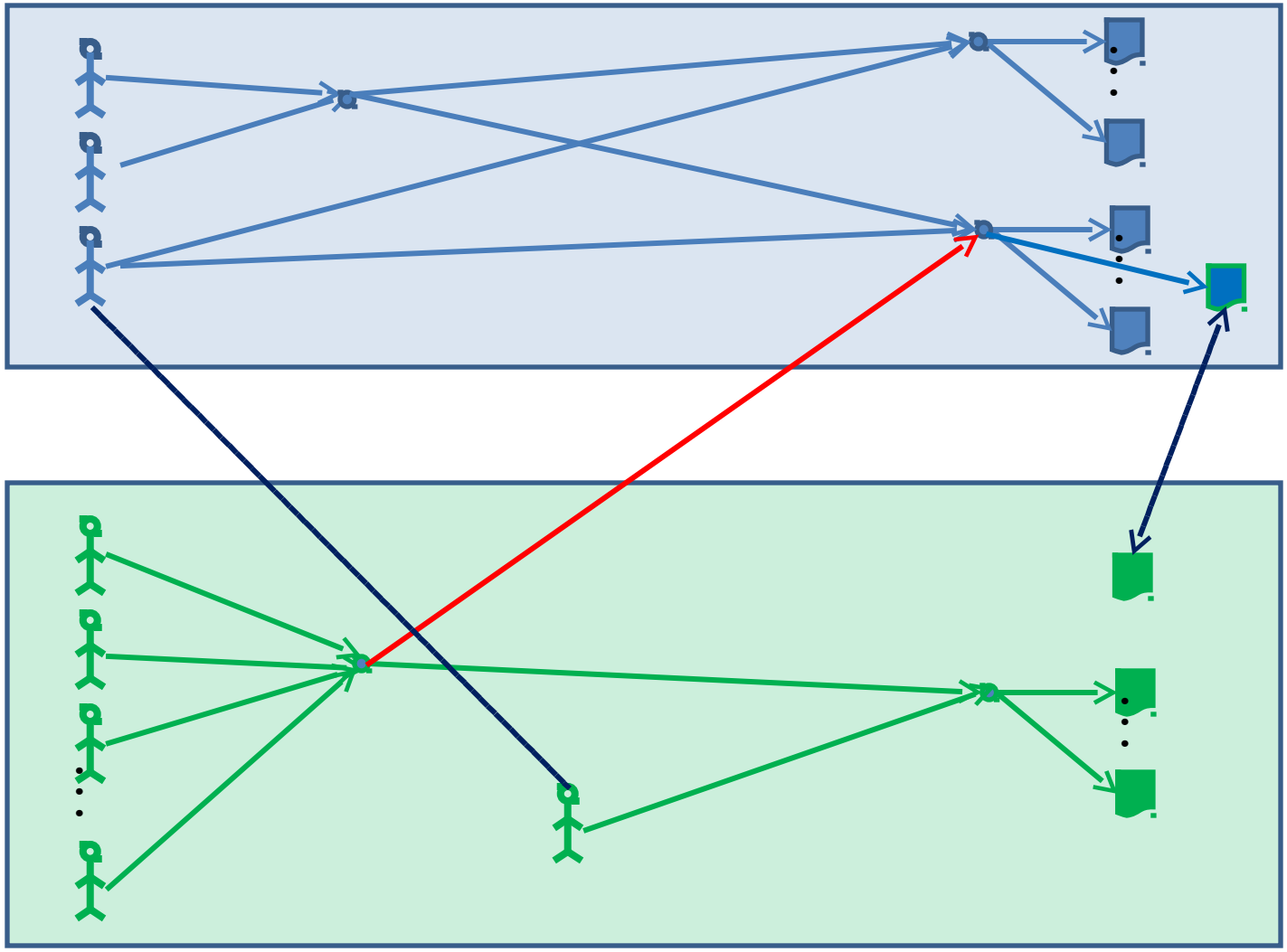
Crossing Organization Boundaries



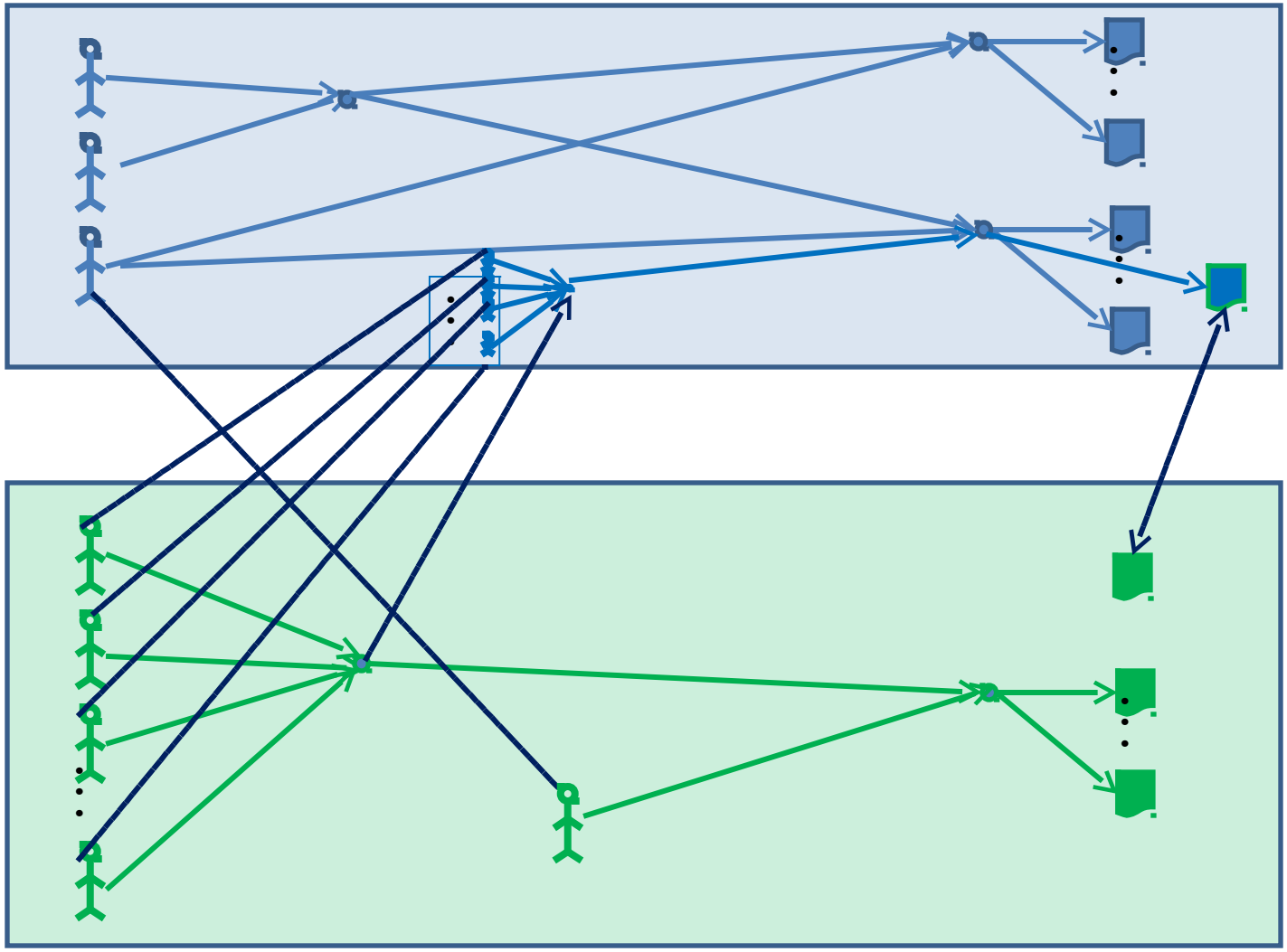
Crossing Organization Boundaries



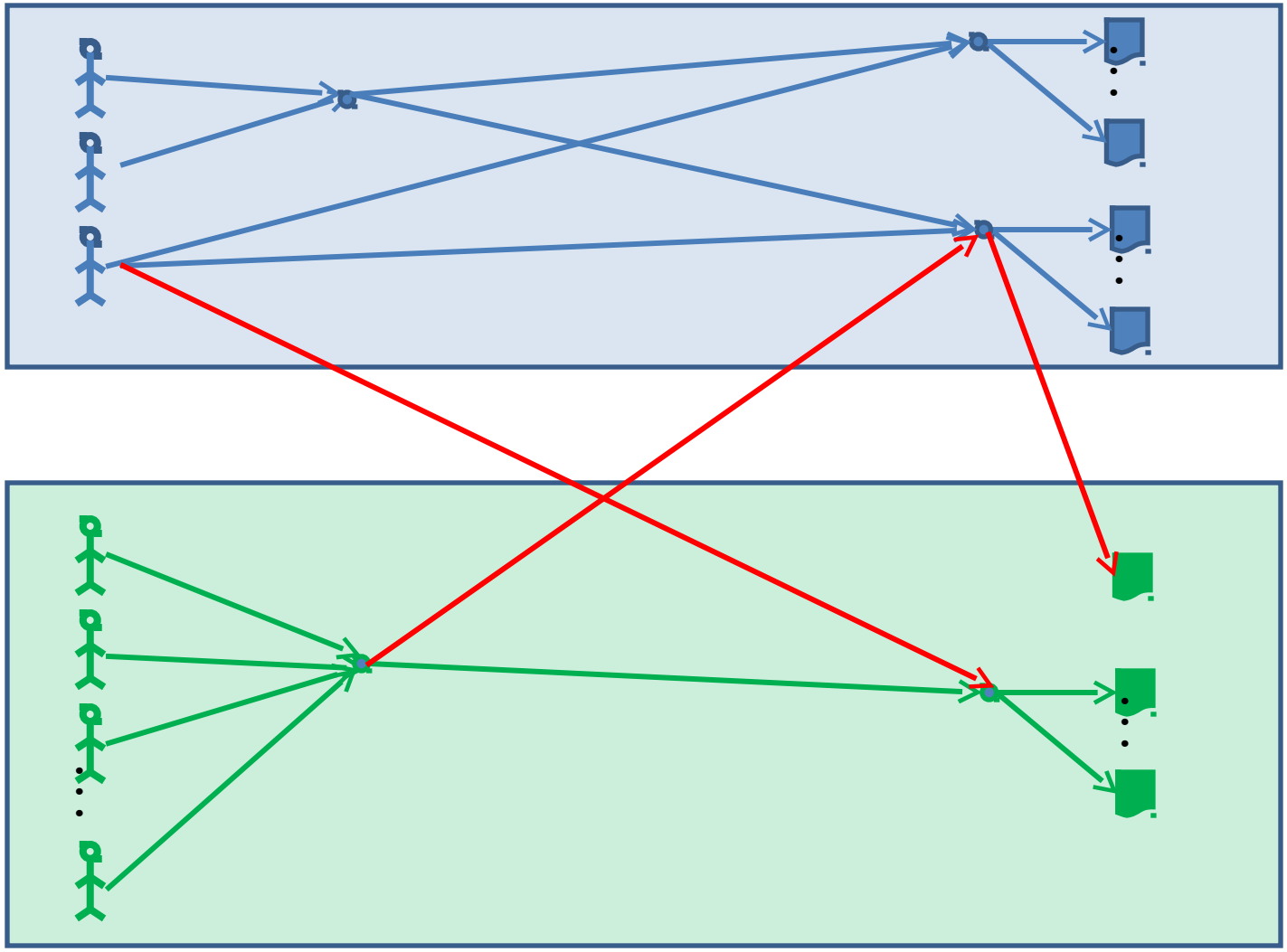
Crossing Organization Boundaries



Crossing Organization Boundaries



Crossing Organization Boundaries



Group Definition – Review

- SID = (Domain ID, Relative ID) = (D, R)
- D is a globally unique ID; R is unique within D
- Same format SIDs for individuals and groups.
- ACL is list of SIDs; Group is a list of SIDs
- Groups are defined in Active Directory™ today by:
  - "(D, R_1) is member of (D, R_2) **says** D"

Extended Group Definition

- SID = (D, R), as before
- D is a globally unique ID or a public key
- Group membership is defined by:
  - "(D_1, R_1) is a member of (D_2, R_2) **says** D_2"
    - When Ds differ, we express the red links from that graph.
  - The administrator of D_2 has the responsibility for making or deleting that definition.
  - If D_2 is a public key, then "says D_2" is a digital signature and this group membership statement can be a certificate or SAML token.

Extensions

- With just what we've presented so far, we get what we need most – efficient and secure groups, roles and attributes across organization boundaries, without anything special for federation.
- However, there are other extensions that are easy to provide in this scheme:
  - Attribute-value pairs
  - Root stores, cross-certification and bridges
  - Group definition expressions with $\wedge$, $\leq$, $\geq$, etc.

Attribute, Value Pairs

- Giving a user an attribute A and value V makes her a member of a group of all users who have attribute A and value V.
- Like all other names, A should be a SID: (D, R)
- So, generalize the SID
  - From (D, R)
  - To (D, R, V) which stands for (A, V) = ((D, R), V)
- We can say, for example:
  - "(K_S) is a member of (K_{CA}, Eva) says K_{CA}"
  - "(K_{CA}, Eva) is a member of (K_1, Age, 15) says K_1"
  - "((K_1, Age) < 21) is a member of (K_2, Minor) says K_2"
  - This user's SIDs include: (K_S), (K_{CA}, Eva), (K_1,Age,15),(K_2,Minor)

Notation Summary

- Use "→" to mean "is a member of"
- Let (D, R) mean (D, R, *)
- Let (D) mean (D, *)
- D can be a public key, so we can write:
  - (K, R, V)
  - (K, R)
  - (K)
- "$(K_S) \rightarrow (K_{DoD}$, Clearance, SECRET) says K_{DoD}"

Root Stores and Bridge CAs

- X.509 gives us "$(K_S) \rightarrow (K_{CA}, DN)$ says K_{CA}"
- But, we don't define groups with:
  - "$(K_{CA}, DN) \rightarrow (D, R)$ says D"
- Instead, we say:
  - "$DN \rightarrow (D, R)$ says D"
- To capture this behavior in our notation, we have to create the symbol δ and say:
  - "$(\delta, DN) \rightarrow (D, R)$ says D"
  - where δ means "some K in the local root store or descended from the store by a chain of CA certificates or cross-certificates"
- This introduces vulnerabilities (cf., the Comodo RA attack) but matches current practice.

Group Definition Expressions

- Groups defined as above are of the form:
  - Group = $SID_1 \vee SID_2 \vee SID_3 \vee \ldots \vee SID_N$
- Groups can be defined by other expressions:
  - $\wedge$ as well as $\vee$
  - "$(K_1, R_1) \wedge (K_2, R_2) \rightarrow (K_3, R_3)$ says K_3"

Good News, Bad News

- The good news is that none of this (except possibly group definition expressions) requires anything new in protocols or over-the-wire data structures.
  - Claims-based IDPs should be able to handle all this.
- The bad news is that none of this is achievable merely by defining a new protocol or wire data structure.
- This requires changes inside an OS, file server or PDP.

Not covered in these slides (for time) but the designs exist

- Level of Assurance
  - Applied at each node and edge in the graph
  - Carried by an attribute for use in access decisions
- Human readable names
- Human interface tools
- Certificate chain discovery
- Authorization decision logic
  - We're just providing the material for that decision.

Feedback and Discussion Welcome

Send any comments or questions to:

- cme@panix.com

and/or

- cme@acm.org (sometimes drops mail)

NIST Update: Part Deux

Elaine Newton, PhD
NIST
elaine.newton@nist.gov

National Institute of Standards and Technology

Outlook for Identity Management

- WH Initiative on the National Strategy for Trusted Identities in Cyberspace (NSTIC)
  - Aims to improve the security of online transactions of consumers (e.g. online banking)
    - Remote access for more services, available anytime, anywhere
    - Risk-based choices of factors and methods
    - Open standards, interoperable platforms

Multi-Factor Authentication (MFA) Initiative

- Supported by the Comprehensive National Cybersecurity Initiative (CNCI)
  - Objective:

    To improve cyber security through strengthening authentication assurance by
    - Advancing multi-factor authentication
    - Shifting the predominance of the username-password paradigm for online transactions
    - Addressing major gaps for remote authentication for higher risk online transactions

Authentication Use Case Comparison

For law enforcement, immigration, etc.

- Enrollment and subsequent recognition attempts
  - highly controlled
  - Supervised / Attended
- Successful recognition
  - Answers the question, “Has this person been previously encountered?”
  - Is a unique pattern

For online transactions, e.g. banking, health, etc.

- Enrollment
  - Less controlled
  - Probably not in person
- Subsequent recognition attempts
  - Unattended
- Successful recognition
  - Answers the question, “How confident am I that this is the actual claimant?”
  - Is a tamper-proof rendering of a distinctive pattern

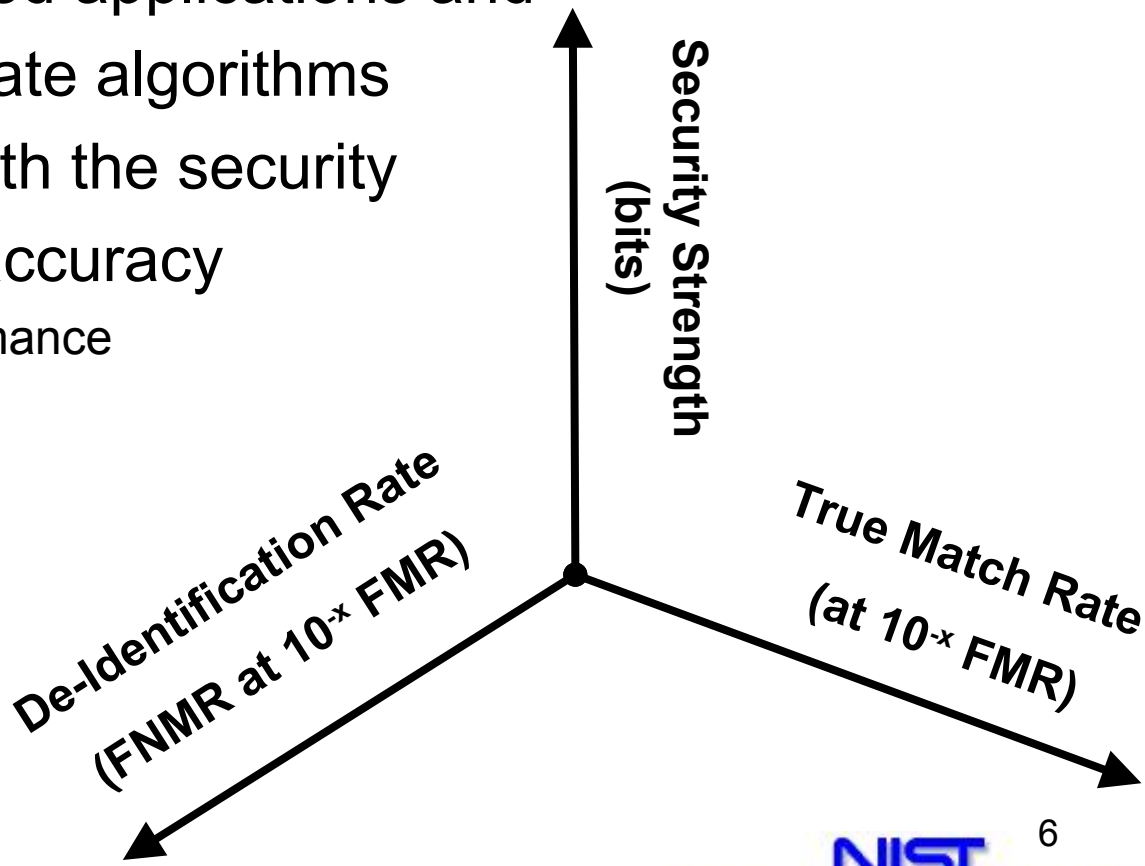
Biometric Template Protection (1 of 3)

- EU funded a 3 year project known as TURBINE (TrUsted Revocable Biometric IdeNtitiEs)
  - “To develop an innovative, privacy enhancing technology solution for electronic identity (eID) authentication through fingerprints biometrics, and
  - “To demonstrate the performance and security of this solution…”

http://www.turbine-project.eu/

Biometric Template Protection (2 of 3)

- Testing will need to address
  - Scale for intended applications and
  - Metrics to evaluate algorithms incorporating both the security properties and accuracy
    - Biometric Performance
    - De-Identification
    - Irreversibility
    - Others



Biometric Template Protection (3 of 3)

- Testing will need to address
  - Scale for intended applications and
  - Metrics to evaluate algorithms

    incorporating both the security

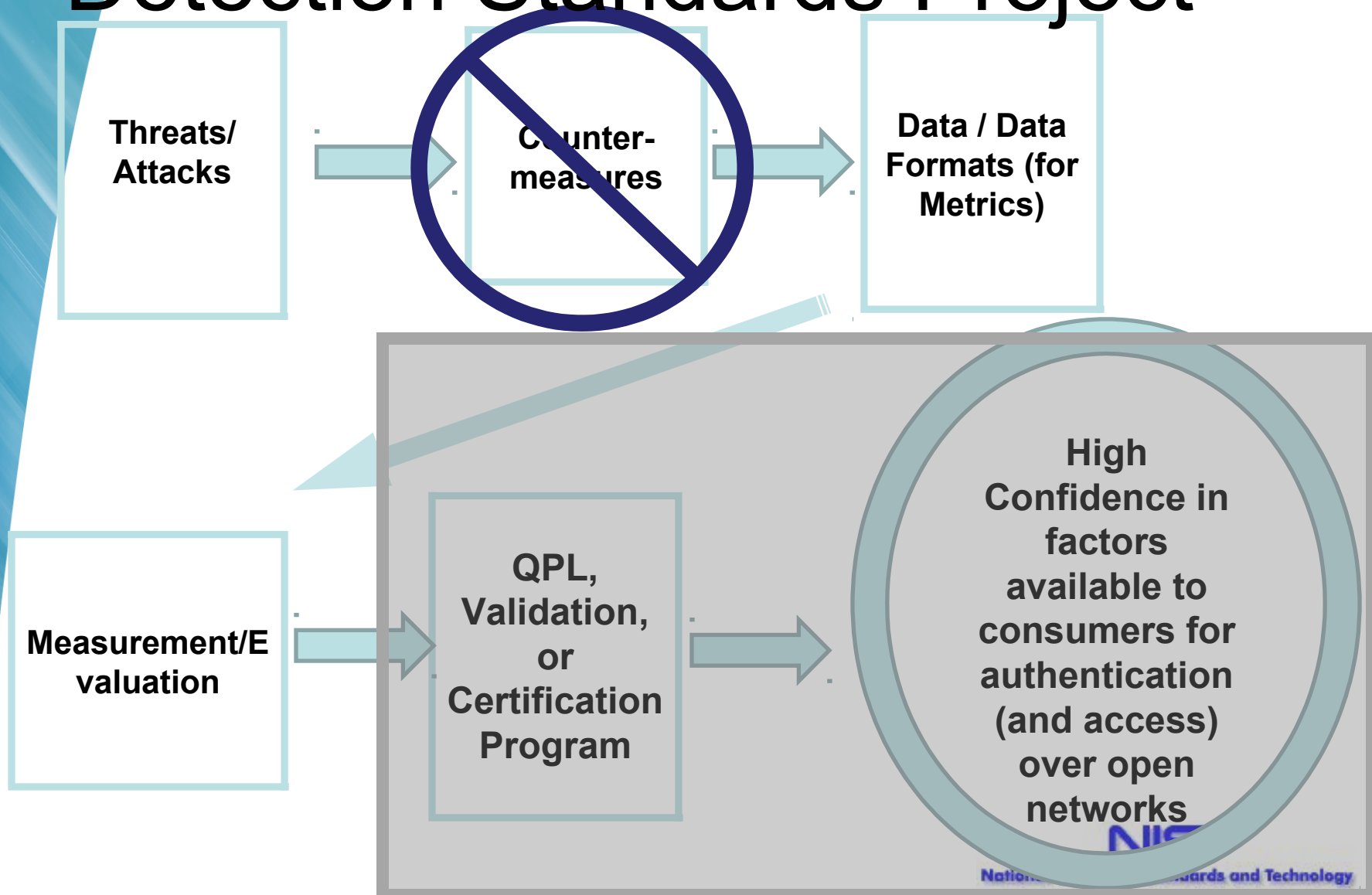
    properties and accuracy

← Fingerprint databases at NIST are the largest and can provide scale.

← NIST funding biometric and security experts to develop metrics, using a NIST Twiki to engage the security and biometric communities.

- Metrics will be used to develop testing protocol

Anti-Spoofing/Liveness Detection Standards Project



Credential Revocation

- No standard methods to revoke an Identity Provider (IdP)s' issued credential or its associated attribute(s).
  - > Investigating techniques for credential and attribute revocation.
  - >Defining use cases and profiles for revocation.
- Lead/PoC: Hildy Ferraiolo (NIST)

hferraio@nist.gov, 1-301-975-6972

MFA Biometrics Projects Summary

- Metrics for a Benchmarking-Framework to Rank Biometric Template Protection Algorithms (starting FY11)
- Anti-Spoofing/Liveness Detection (starting FY11)
  - Evaluation approaches for fingerprint recognition systems
  - Leading international standard project in ISO/IEC (SC 37)
- Credential Revocation (starting FY11)
- Drafting guidelines and requirements for the use of biometrics as a second factor for remote authentication
- On-Card-Comparison Testing
  - Final report available at http://biometrics.nist.gov/cs_links/minex/minexII/minex_report.pdf
- Standards and reference implementation for web services (Draft 1 available at bws.nist.gov)

Thank you

Questions?

Elaine Newton, PhD
elaine.newton@nist.gov
1-301-975-2532

National Institute of Standards and Technology

A Quick Tour of the FIPS 201 Revision

William I. MacGregor
NIST ITL Computer Security Division
william.macgregor@nist.gov

NIST, Gaithersburg
7Apr2011

National Institute of Standards and Technology

HSPD-12 Implementation

- First the eggs, then the chickens…
  - PIV Cards are the eggs
  - Applications are the chickens
- How many eggs? Roughly,
  - 4.6M PIV Cards issued to employees (80%)
  - 1.6M PIV Cards issued to contractors (30%)
- Now it's time for chickens…
  - "Federal Identity Credentialing and Access Management (FICAM) Roadmap and Implementation Guidance"
  - Part A: ICAM Segment Architecture completed Sep2009
  - Part B: Implementation Guidance work-in-progress

Useful URLs

- http://www.whitehouse.gov/omb/e-gov/hspd12_reports/ **- OMB quarterlies**
- http://csrc.nist.gov/groups/SNS/piv/standards.html **- FIPS 201 & NIST pubs**
- http://www.idmanagement.gov/ **- ICAMSC & GSA ID management resources**
- http://www.idmanagement.gov/drilldown.cfm?action=hspd12_faqs **- FAQs**
- http://fips201ep.cio.gov/ **- HSPD-12 Evaluation Program (APL)**
- http://www.nist.gov/itl/iad/ **- NIST biometrics resources**
- http://www.whitehouse.gov/omb/memoranda_default/ **- OMB Memoranda**

- There are now dozens of OMB Memoranda, NIST publications, CIO Council publications, Federal PKI Policy Authority publications, GSA documents, OPM documents, and others relevant to HSPD-12.
- And, of course, OMB M-11-11.

The Larger Context

- Built on DoD Common Access Card experience.
- Enhanced to scale US Government-wide:
  - Simple, self-contained app, with assurance processes.
  - Authenticate, Encrypt/Decrypt, Sign/Verify.
  - Defined issuance processes, limited crypto capabilities.
- Expanding to other communities:
  - PIV Interoperable (PIV-I) Cards issued by Non-Federal Issuers.
  - PIV-I uses same blank card stock as PIV.
  - The Federal Bridge unifies the trust model for all participants.
- After five years, new requirements are being heard!

The Revision of FIPS 201-1

- NIST was obligated to consider the need for revision of FIPS 201 five years after publication (i.e., in 2010).
- NIST determined that FIPS 201-1 should be revised, and prepared Draft FIPS 201-2.
- The revision was announced in the Federal Register on 8Mar2011.
- On the same day, Draft FIPS 201-2 was available on the NIST website for a 90 day public comment period.

The Revision of FIPS 201-1

- 2010: NIST studied the need for revision
- 8Mar2011: revision was launched

- See the launch announcement
  - http://csrc.nist.gov/news_events/index.html#mar8
  - Leads to Draft FIPS 201-2 (clean & diff)
  - Also Federal Register Notice (a handy index)_
- Workshop at NIST on **18-19Apr2011**
  - Attend in person, registration fee $160
  - Watch & listen via webcast, free
- Comments must be received by **6Jun2011**

Selected Changes
Proposed

1. Make card lifecycle management more efficient
   - Synchronize card, cert, and biometric data lifetimes
   - Allow biometric reconnect to identity chain-of-trust
   - Add additional biometric modality, iris
   - Allow all newly-issued cards to have max lifetime
   - Replace NACI Indicator with online status check (cond)
2. Remove ambiguity in implementation of PKI
   - Make asymmetric CAK mandatory, symmetric optional
   - Make signature verification and PDVAL mandatory
3. Introduce New Functional Capabilities
   - On Card Comparison for card activation & authentication
   - Improve adaptability and resilience of readers
   - Secure Sessions from reader or application to PIV Card
   - Trust Anchors for readers or applications

NIST is often asked…

- Shouldn't smartphones, USB tokens, tablets, and form factors be supported?
- If mutually authenticated secure sessions are added, what are the End Entities?
- Could authentication mechanisms become location-aware?
- Shouldn't the credential protect the user against unnecessary disclosure of sensitive information?

Multi-Factor Authentication and Higher LOA Issues

10th Symposium on Identity and Trust on the Internet

Paul Donfried
CTO – IAM
Universal Identity Services

April 7, 2011

Remember when we were young…

Operators □ Skype

Cisco Unified Communications 500 Series

A new wave of disruptive technology is transforming the dynamics of global business

Our vision is to empower individuals with seamless and secure access

A New Mobile Mindset

"I need better tools for managing my digital personals and profiles—not just Facebook but retail, bank, and travel accounts.
I want value based relationships with loyalty programs"

"I want my profile to be useable across the brands and relationships I value. I want them to value me and only send relevant rewards or incentives"

"To stay connected I need the ability to move from work to my personal life without worrying about which password to use"

"My local government and healthcare providers are too slow and inaccessible. There are too many forms and redundancies"

Consumer Community

Friend Family

Employee Colleague

Citizen Patient

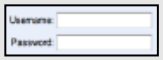
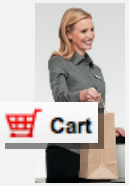
Seamless and secure access to anyone, anywhere on any device

verizon

Giving power to your end users leads to customer insights, context and repeat business

verizon

UIS Market Facing Services

People	Identity Form Factors (Verizon & 3rd Party Issued)	Open Standards	Services You Need	Open Standards	Relying Parties
	      	LDAP X.509 SMS OTP RADIUS OATH	 Identity Issuance Services  Authentication Gateway Federation  Risk Services	Info Cards/Open ID Microsoft® Active Directory® WS-Trust LDAP OIX SAML RADIUS Kerberos Shibboleth X.509/OCSP	 Work Login  Healthcare  Shopping  Banking

We need an identity ecosystem in the cloud.

UIS Profile Management

Account | Credit Cards

First Name: Peter
Last Name: Graham
Email Address: ptrgraham@aol.com change
Subscriptions: Manage email subscriptions
Change profile picture
Choose File No file ch
Time Zone: (GMT-07:00) Arizona

Change Your Password

New Password
Retype Password

Connections

Facebook: Connect
Starfish

Developer API

Api Token(s): Get Your API Client ID

Save Changes

About Me

My gender is:
Male Female
Show me deals near ZIP/postal code:
I was born on:
Month Day Year

My Favorite Deals

Health and Beauty
- Dental, vision, and m
- Salon services
- Spa services, massa

Food and Drink
- Bars and clubs
- Cafes, dessert, and
- Casual restaurants
- Fine dining
- Meal preparation and

Retail and Service
- Automobile
- Clothing, fashion, an
- Groceries
- Home and garden
- Pets

My Background

Education: Bachelor's degree
Employment status: Employed full time
Income range: Prefer not to share
Own a home? Yes No
Relationship status: Married
Have children? Yes No

One Time Password (OTP) Delivery Settings

One Time Password Setting

EMAIL

By clicking on a check box here you will be enabling the respective email address to receive a one time password (OTP) for authentication.

HOME	peter.graham@verizonbusiness.com	☐

SMS (Text Message)

By clicking on a check box here you will be enabling the respective phone number to receive a one time password (OTP) as a text message (SMS). Please ensure this telephone number is capable of receiving text messages (SMS). Standard SMS text rates may apply based on your service provider.

HOME	(520) 576-7083	☐
HOME	(520) 762-9518	☐

IVR (Voice Call)

By clicking on a check box here you will be enabling the respective phone number to receive an automated phone call with instructions for authentication. Please ensure the telephone number is capable of receiving voice calls.

HOME	(520) 762-9518	☐
HOME	(520) 576-7083	☐

verizon

Scale

	2011	2012	2013
UID Users	100 million	200 million	

Consumer Value

- Improved user experience
- Reduced identity risk
- Reduced fraud
- More control

Discussion

Digital Signatures: Current Barriers

Simson L. Garfinkel
Associate Professor, Naval Postgraduate School

April 7, 2011

http://simson.net/

NPS is the Navy's Research University.

Location: Monterey, CA [& Arlington, VA]

Campus Size: 627 acres

Students: 1500

- US Military (All 5 services)
- US Civilian (Scholarship for Service & SMART)
- Foreign Military (30 countries)
- All students are fully funded

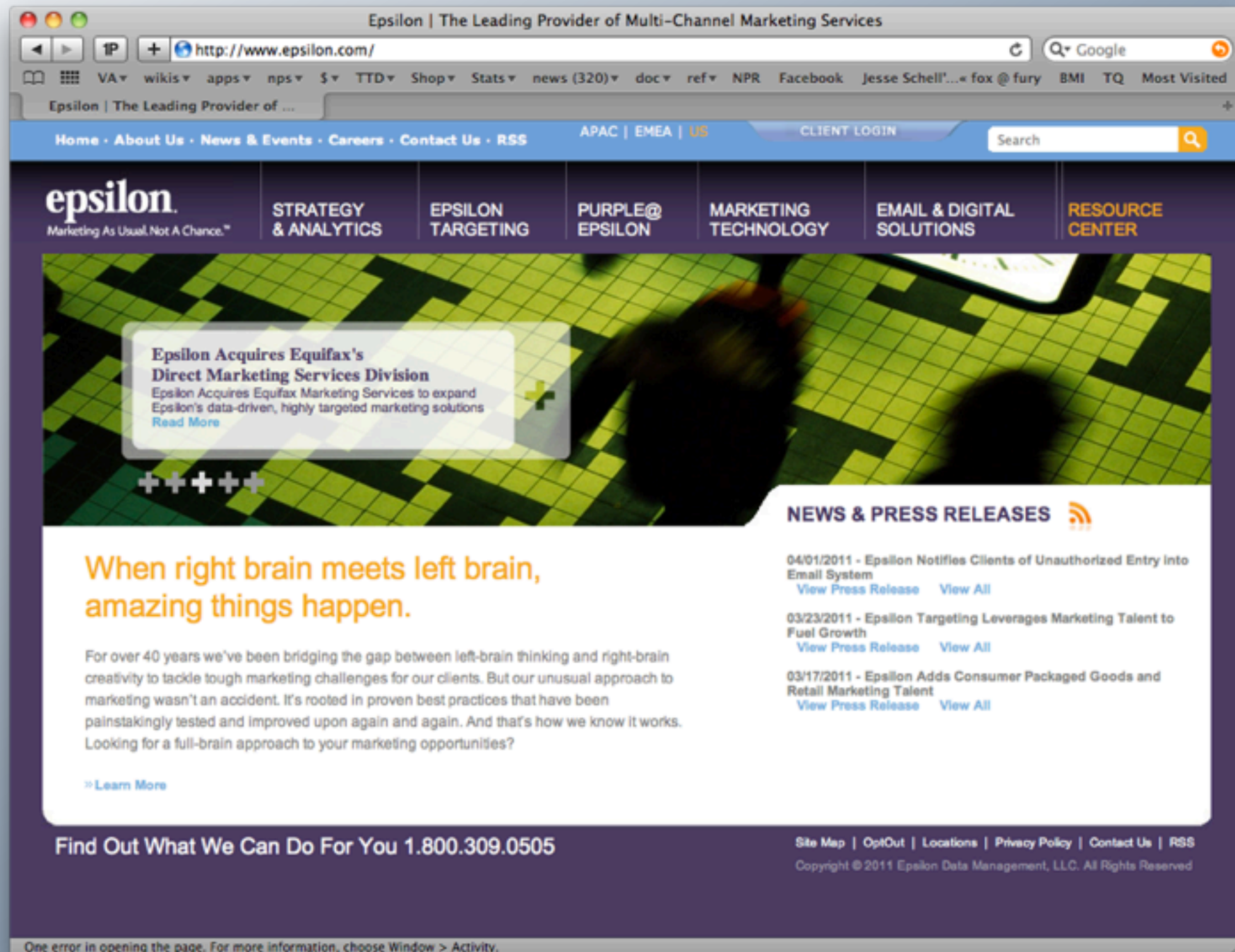
Schools:

- Business & Public Policy
- Engineering & Applied Sciences
- Operational & Information Sciences
- International Graduate Studies

Personal Opinion Disclaimer

This document was prepared as a service to the DoD community. Neither the United States Government nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process disclosed, or represents that its use would not infringe privately owned rights.

Reference herein to any specific commercial products, process, or service by trade name, trademark manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The opinions of the authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.



Enhancing mail security with digitally signed mail.

April 2011: Epsilon Data Management LLC announces millions of customer email addresses stolen.

Epsilon provides email services for:

- Chase
- Capital One
- Citibank
- etc.

If email from banks was digitally signed:

- The hacker would have gotten the private key.
- The private key would then be invalidated.
- Anti-spam systems would reject mail signed with invalidated key.

Epsilon email hack: millions ...| Technology | guardian.co.uk

Epsilon email hack: millions of cu...

Epsilon email hack: millions of customers' details stolen

Customers of Barclaycard US, Capital One and other companies warned after attack on marketing email provider Epsilon

Josh Halliday
guardian.co.uk, Monday 4 April 2011 18.16 BST
Article history

Epsilon email hack: customers of Barclaycard US had their names and email addresses stolen. Photograph: David Levene for the Guardian

Computer hackers have stolen the names and email addresses of millions of people in one of the largest internet security breaches in US history.

Why don't banks sign their mail?
From 2003 to 2006, I met with 5 banks to find out why.

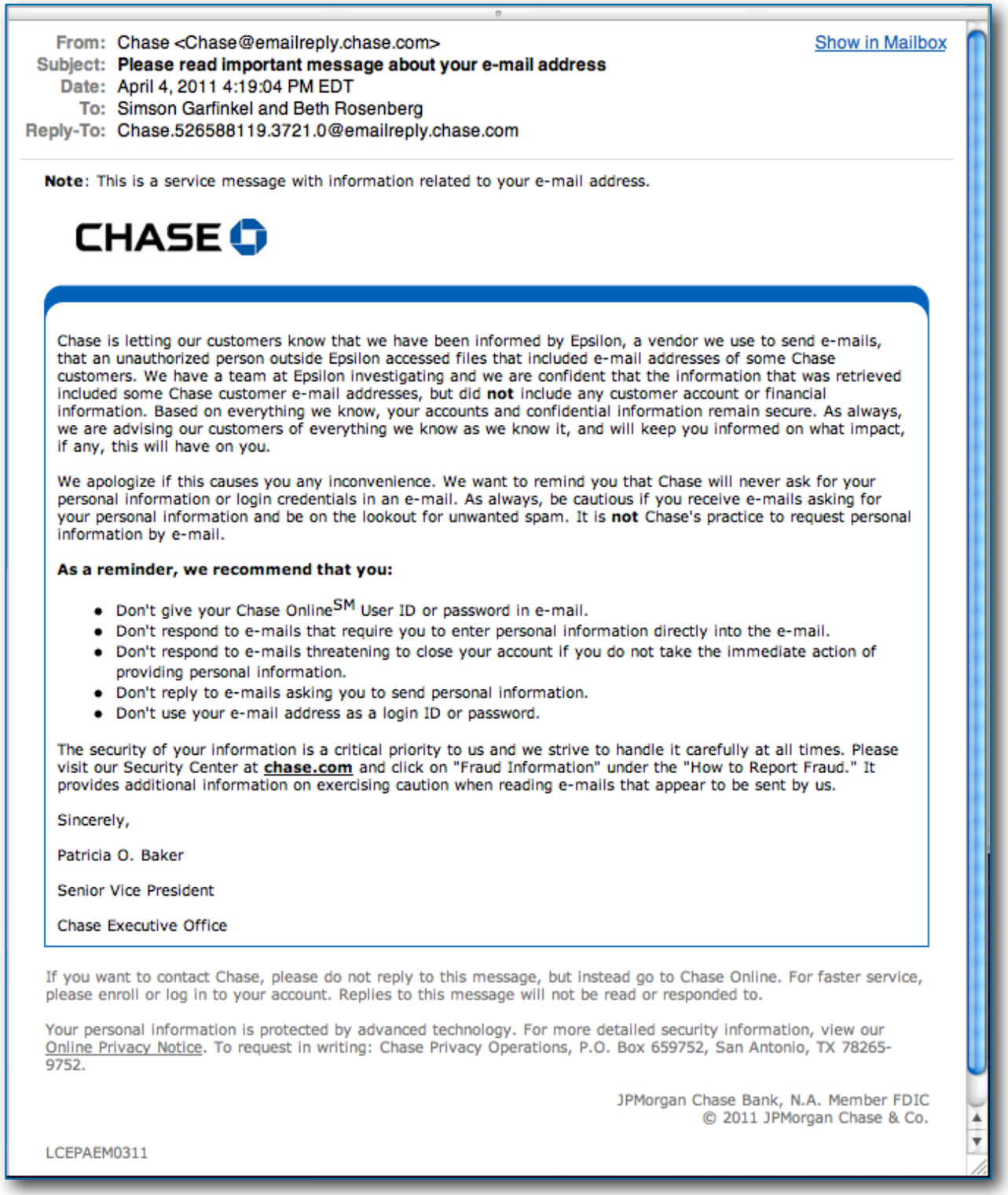
"No other banks sign their mail."

"Email is a marketing function."

"We use digital signatures internally, but federal regulations prohibit sending signed mail to our customers."

"Most of our customers use web mail, and web mail doesn't work with digital signatures."

"Nobody has PGP."



From: Chase <Chase@emailreply.chase.com>
Subject: **Please read important message about your e-mail address**
Date: April 4, 2011 4:19:04 PM EDT
To: Simson Garfinkel and Beth Rosenberg
Reply-To: Chase.526588119.3721.0@emailreply.chase.com

Show in Mailbox

Note: This is a service message with information related to your e-mail address.

CHASE

Chase is letting our customers know that we have been informed by Epsilon, a vendor we use to send e-mails, that an unauthorized person outside Epsilon accessed files that included e-mail addresses of some Chase customers. We have a team at Epsilon investigating and we are confident that the information that was retrieved included some Chase customer e-mail addresses, but did **not** include any customer account or financial information. Based on everything we know, your accounts and confidential information remain secure. As always, we are advising our customers of everything we know as we know it, and will keep you informed on what impact, if any, this will have on you.

We apologize if this causes you any inconvenience. We want to remind you that Chase will never ask for your personal information or login credentials in an e-mail. As always, be cautious if you receive e-mails asking for your personal information and be on the lookout for unwanted spam. It is **not** Chase's practice to request personal information by e-mail.

As a reminder, we recommend that you:

- Don't give your Chase Online℠ User ID or password in e-mail.
- Don't respond to e-mails that require you to enter personal information directly into the e-mail.
- Don't respond to e-mails threatening to close your account if you do not take the immediate action of providing personal information.
- Don't reply to e-mails asking you to send personal information.
- Don't use your e-mail address as a login ID or password.

The security of your information is a critical priority to us and we strive to handle it carefully at all times. Please visit our Security Center at **chase.com** and click on "Fraud Information" under the "How to Report Fraud." It provides additional information on exercising caution when reading e-mails that appear to be sent by us.

Sincerely,

Patricia O. Baker

Senior Vice President

Chase Executive Office

If you want to contact Chase, please do not reply to this message, but instead go to Chase Online. For faster service, please enroll or log in to your account. Replies to this message will not be read or responded to.

Your personal information is protected by advanced technology. For more detailed security information, view our Online Privacy Notice. To request in writing: Chase Privacy Operations, P.O. Box 659752, San Antonio, TX 78265-9752.

JPMorgan Chase Bank, N.A. Member FDIC
© 2011 JPMorgan Chase & Co.

LCEPAEM0311

Public key cryptography was invented nearly 30 years ago to secure electronic mail.

Since then we have spent a *lot* of effort on this issue.

1976 – Public Key Cryptography (Diffie & Hellman)

1977 – RSA Encryption (Rivest, Shamir & Adelman)

1978 – Certificates (Kornfelder)

1987 – Privacy Enhanced Mail

1992 – PGP

1998 – S/MIME

2005 – Domain Keys

2009 – National Strategy for Trusted Identities in Cyberspace

By 1999 there were two email security standards: PGP and S/MIME

Support for S/MIME was built into every mainstream mail client:

- Outlook Express
- Outlook
- Mozilla Thunderbird
- Evolution
- Apple Mail

S/MIME support in Outlook Express, circa 2001

PGP requires a plug-in

#1 problem with S/MIME: Two-Party Agreement

Encrypted mail:

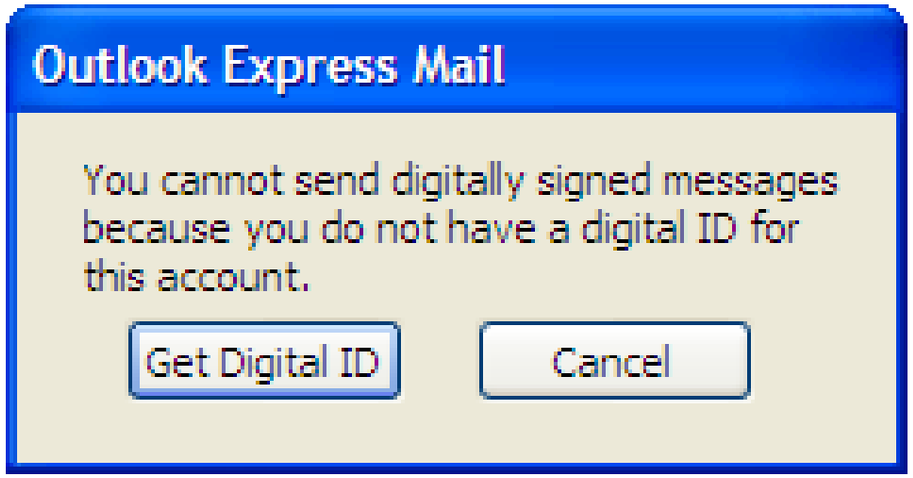
- Recipient must have a certificate
- Sender must get recipient's certificate

Sending signed mail:

- Sender must have a certificate.

Replying to signed mail:

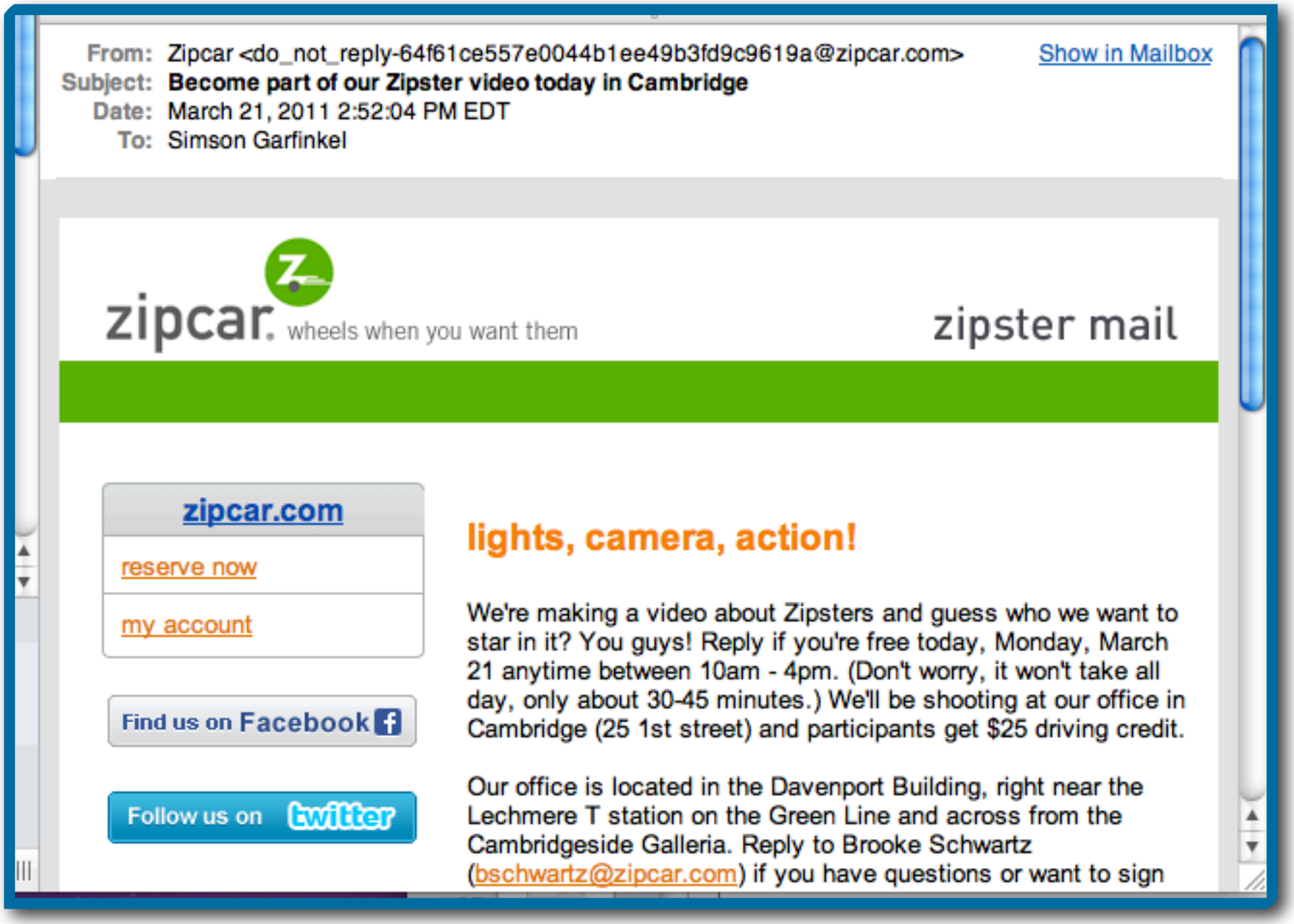
- Recipient-come-sender must have a certificate:



But no certificate is required to receive digitally signed mail...

My goal: digital signatures for do-not-reply email

Lots of companies send “do-not-reply” email:



From: Zipcar <do_not_reply-64f61ce557e0044b1ee49b3fd9c9619a@zipcar.com> Show in Mailbox
Subject: **Become part of our Zipster video today in Cambridge**
Date: March 21, 2011 2:52:04 PM EDT
To: Simson Garfinkel

zipcar. wheels when you want them

zipster mail

zipcar.com
reserve now
my account

Find us on Facebook

Follow us on twitter

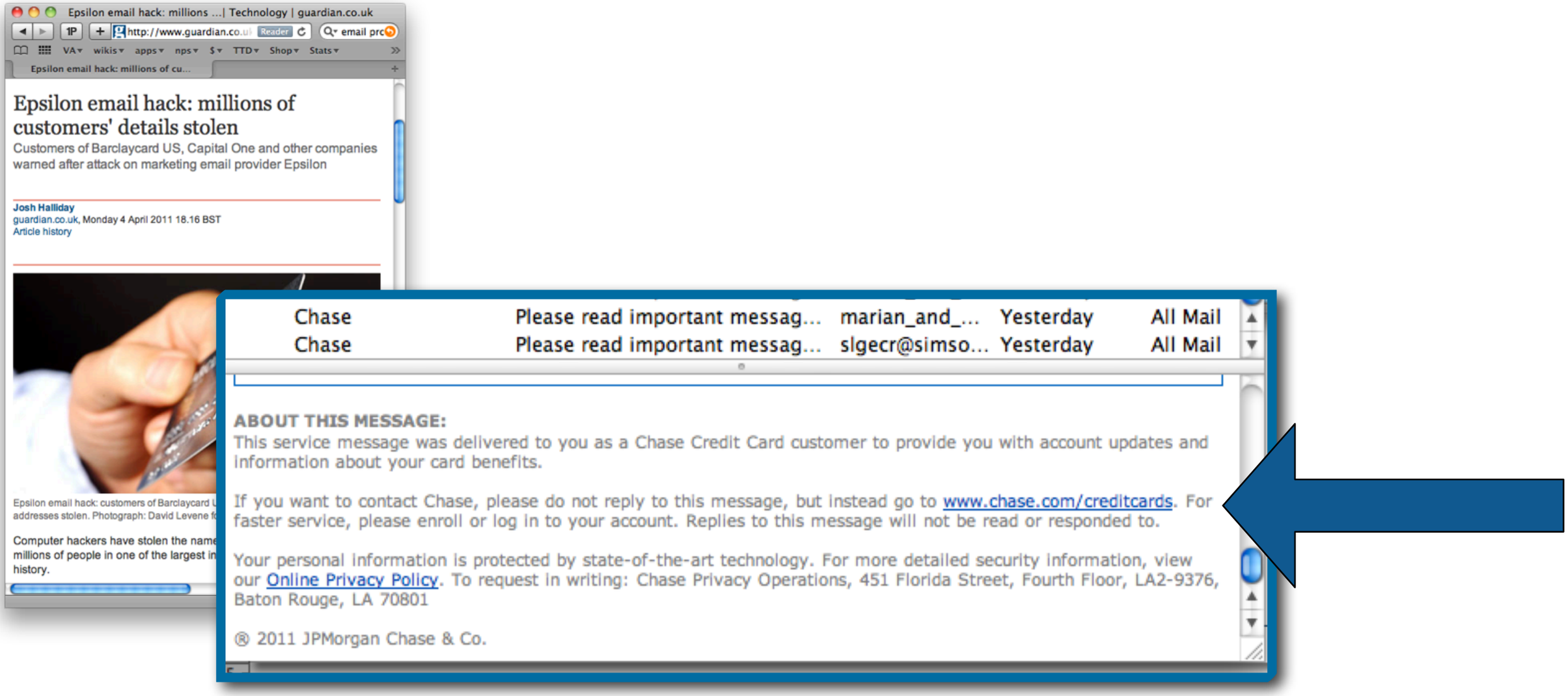
lights, camera, action!

We're making a video about Zipsters and guess who we want to star in it? You guys! Reply if you're free today, Monday, March 21 anytime between 10am - 4pm. (Don't worry, it won't take all day, only about 30-45 minutes.) We'll be shooting at our office in Cambridge (25 1st street) and participants get $25 driving credit.

Our office is located in the Davenport Building, right near the Lechmere T station on the Green Line and across from the Cambridgeside Galleria. Reply to Brooke Schwartz (bschwartz@zipcar.com) if you have questions or want to sign

You can either ignore it, or click the links.

Much (most?) of the mail that Epsilon sent is do-not-reply mail



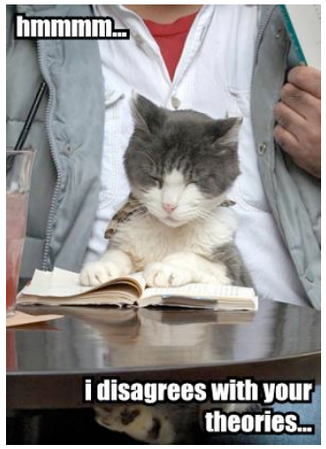
"If you want to contact Chase, please do not reply to this message, but instead go to www.chase.com/creditcards."

Outline of this talk

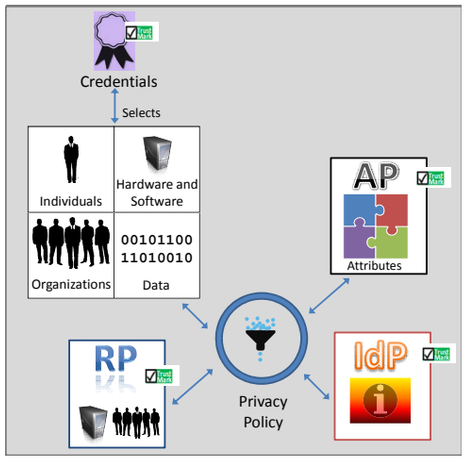
Digital signatures today

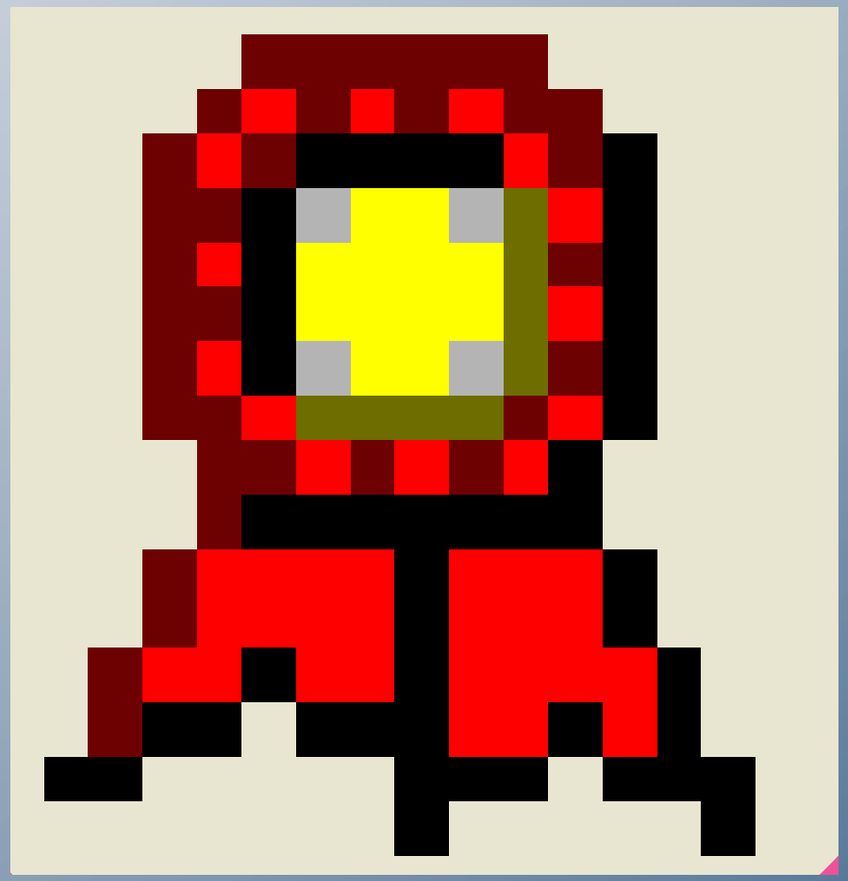
- Good news!
- Not-so-good news.
- Really bad news.

Theories regarding the use of digital signatures.



Suggestions for moving forward.



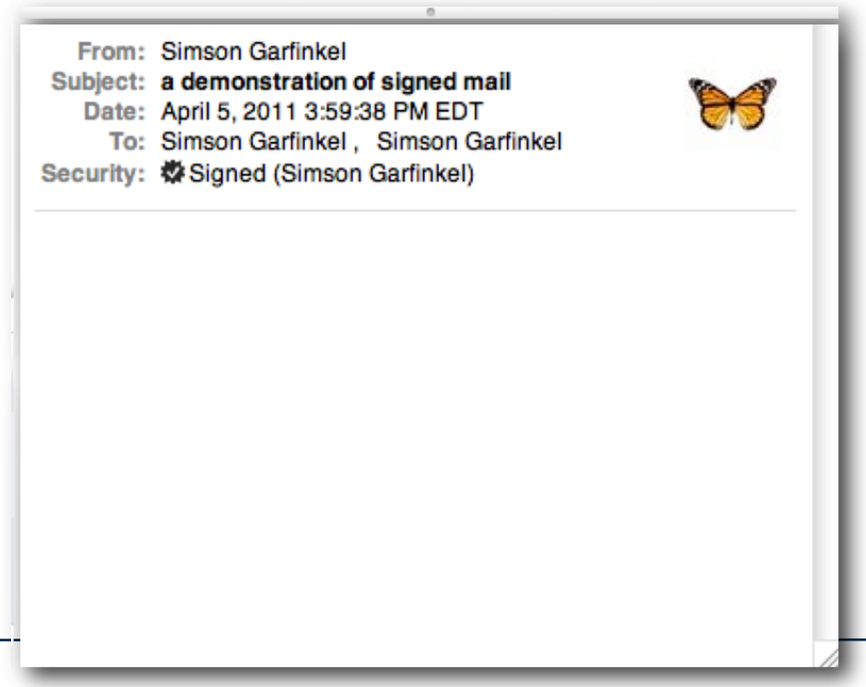


Good News!

Good news about digital signatures!

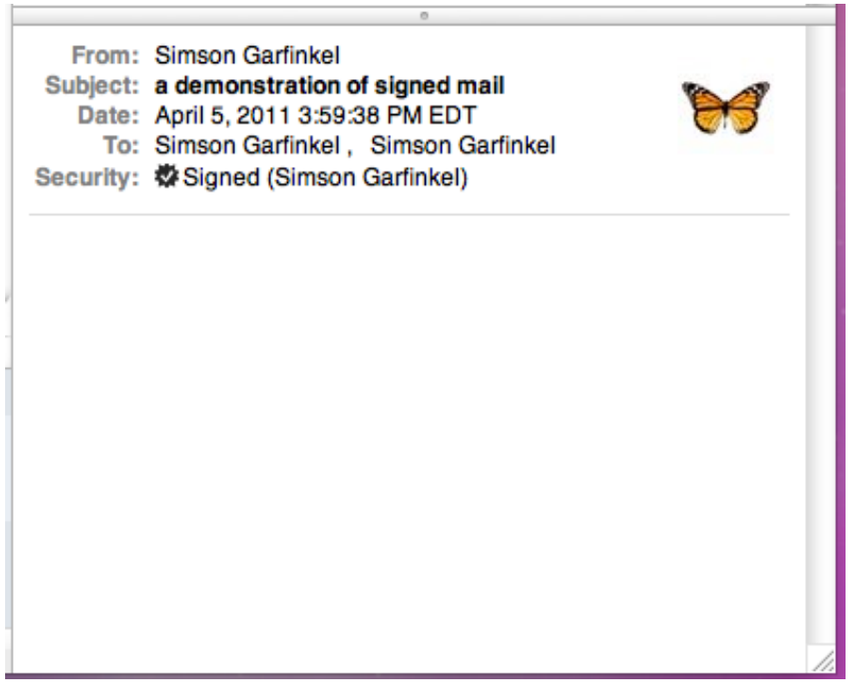
I get signed email messages *every day* from DoD employers using Microsoft Outlook

Apple Mail can verify the signatures

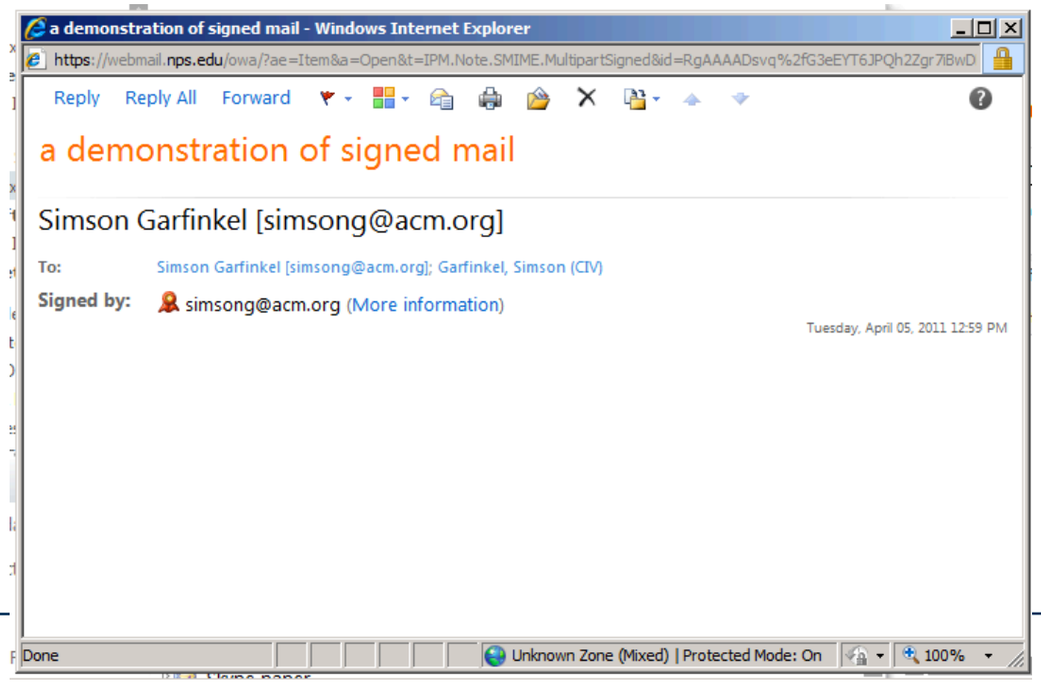


Good news about digital signatures!

I get signed email messages *every day*:



It even works in Microsoft Outlook Webmail:



DoD has issued every employee & warfighter a “CAC” (Common Access Card).

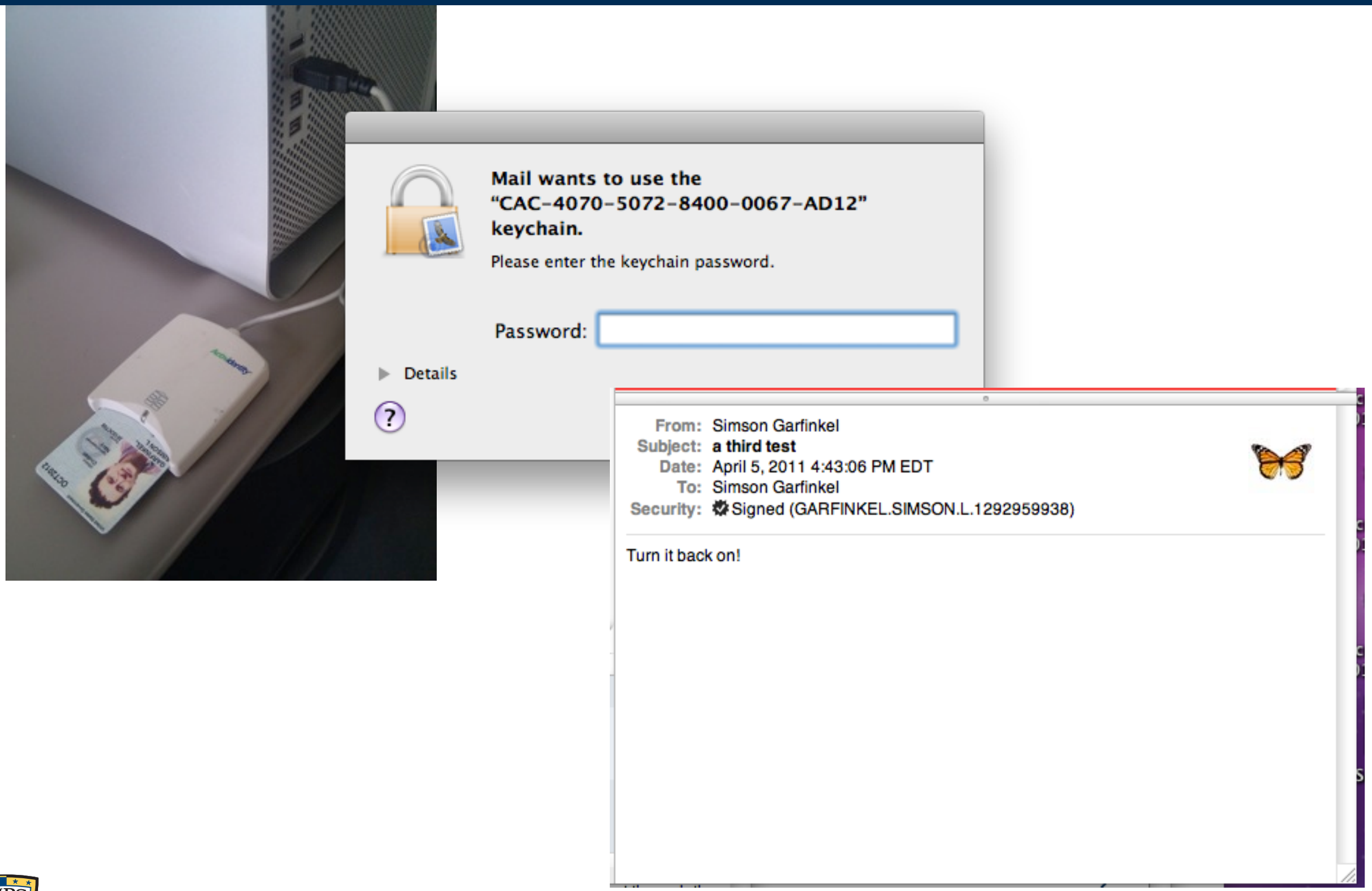
HSPD-12 compliant

- Email Encryption key (with key escrow)
- Email Signing key
- Identity Key

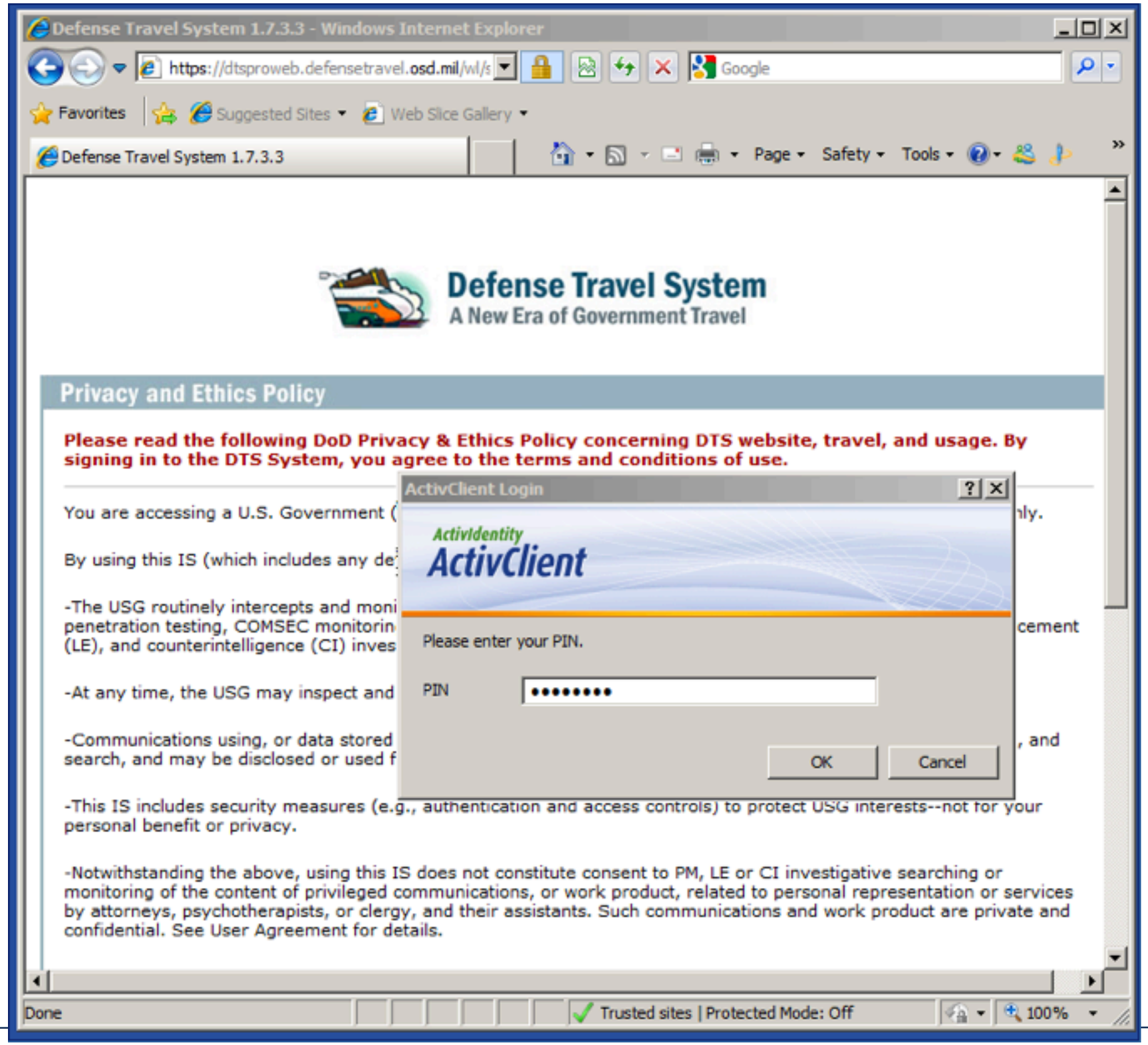
Widely used today for:

- Identity badge at DoD facilities.
- Email signing & encryption
- Access to websites.
- etc.

CAC interoperates with Apple Mail



Defense Travel System (DTS) uses CAC for authentication.



DD1351-2 is a standard form for travel reimbursement.

TRAVEL VOUCHER OR SUBVOUCHER

Read Privacy Act Statement, Penalty Statement, and Instructions on back before completing form. Use typewriter, ink, or ball point pen. PRESS HARD. DO NOT use pencil. If more space is needed, continue in remarks.

1. PAYMENT
☐ Electronic Fund Transfer (EFT)
☐ Payment by Check

SPLIT DISBURSEMENT: The Paying Office will pay directly to the Government Travel Charge Card (GTCC) contractor the portion of your reimbursement representing travel charges for transportation, lodging, and rental car if you are a civilian employee, unless you elect a different amount. Military personnel are required to designate a payment that equals the total of their outstanding government travel card balance to the GTCC contractor.

☐ Pay the following amount of this reimbursement directly to the Government Travel Charge Card contractor: $ _____

2. NAME *(Last, First, Middle Initial) (Print or type)*

3. GRADE

4. SSN

5. TYPE OF PAYMENT *(X as applicable)*
☐ TDY ☐ Member/Employee
☐ PCS ☐ Other
☐ Dependent(s) ☐ DLA

6. ADDRESS. a. NUMBER AND STREET | b. CITY | c. STATE | d. ZIP CODE

e. E-MAIL ADDRESS

7. DAYTIME TELEPHONE NUMBER & AREA CODE

8. TRAVEL ORDER/AUTHORIZATION NUMBER

9. PREVIOUS GOVERNMENT PAYMENTS/ ADVANCES

10. FOR D.O. USE ONLY
a. D.O. VOUCHER NUMBER
b. SUBVOUCHER NUMBER
c. PAID BY
d. COMPUTATIONS

11. ORGANIZATION AND STATION

12. DEPENDENT(S) *(X and complete as applicable)*
☐ ACCOMPANIED ☐ UNACCOMPANIED

a. NAME *(Last, First, Middle Initial)*	b. RELATIONSHIP	c. DATE OF BIRTH OR MARRIAGE

13. DEPENDENTS' ADDRESS ON RECEIPT OF ORDERS *(Include Zip Code)*

14. HAVE HOUSEHOLD GOODS BEEN SHIPPED? *(X one)*
☐ YES ☐ NO *(Explain in Remarks)*

15. ITINERARY

a. DATE		b. PLACE *(Home, Office, Base, Activity, City and State; City and Country, etc.)*	c. MEANS/ MODE OF TRAVEL	d. REASON FOR STOP	e. LODGING COST	f. POC MILES
	DEP					
	ARR					
	DEP					
	ARR					
	DEP					
	ARR					
	DEP					
	ARR					
	DEP					
	ARR					
	DEP					
	ARR					

e. SUMMARY OF PAYMENT

(1) Per Diem	
(2) Actual Expense Allowance	
(3) Mileage	
(4) Dependent Travel	
(5) DLA	
(6) Reimbursable Expenses	
(7) Total	
(8) Less Advance	
(9) Amount Owed	
(10) Amount Due	

16. POC TRAVEL *(X one)* ☐ OWN/OPERATE ☐ PASSENGER

17. DURATION OF TRAVEL
☐ 12 HOURS OR LESS
☐ MORE THAN 12 HOURS BUT 24 HOURS OR LESS
☐ MORE THAN 24 HOURS

18. REIMBURSABLE EXPENSES

a. DATE	b. NATURE OF EXPENSE	c. AMOUNT	d. ALLOWED

19. GOVERNMENT/DEDUCTIBLE MEALS

a. DATE	b. NO. OF MEALS	a. DATE	b. NO. OF MEALS

20.a. CLAIMANT SIGNATURE | b. DATE

c. REVIEWER'S PRINTED NAME | d. REVIEWER SIGNATURE | e. TELEPHONE NUMBER | f. DATE

21.a. APPROVING OFFICIAL'S PRINTED NAME | b. SIGNATURE | c. TELEPHONE NUMBER | d. DATE

22. ACCOUNTING CLASSIFICATION

23. COLLECTION DATA

24. COMPUTED BY | **25. AUDITED BY** | **26. TRAVEL ORDER/ AUTHORIZATION POSTED BY** | **27. RECEIVED** *(Payee Signature and Date or Check No.)* | **28. AMOUNT PAID**

DD FORM 1351-2, MAR 2008

PREVIOUS EDITION MAY BE USED UNTIL SUPPLY IS EXHAUSTED.

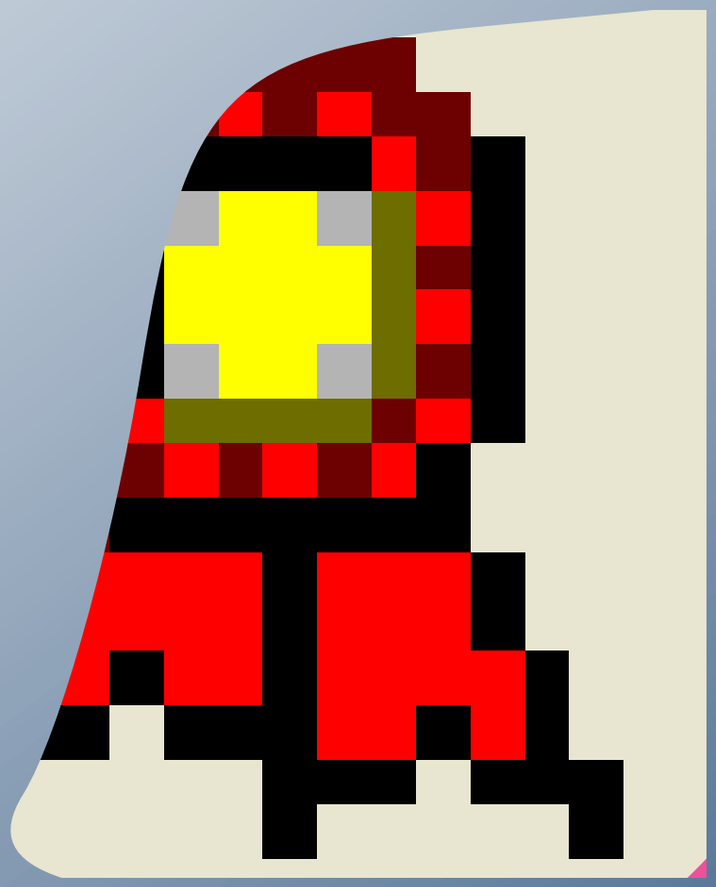
Exception to SF 1012 approved byGSA/IRMS 12-91.
Adobe Designer 7.0

I signed my DD1351-2 “Travel Voucher or Subvoucher” on my MAC with a CAC and Adobe Acrobat.

20.a. CLAIMANT SIGNATURE

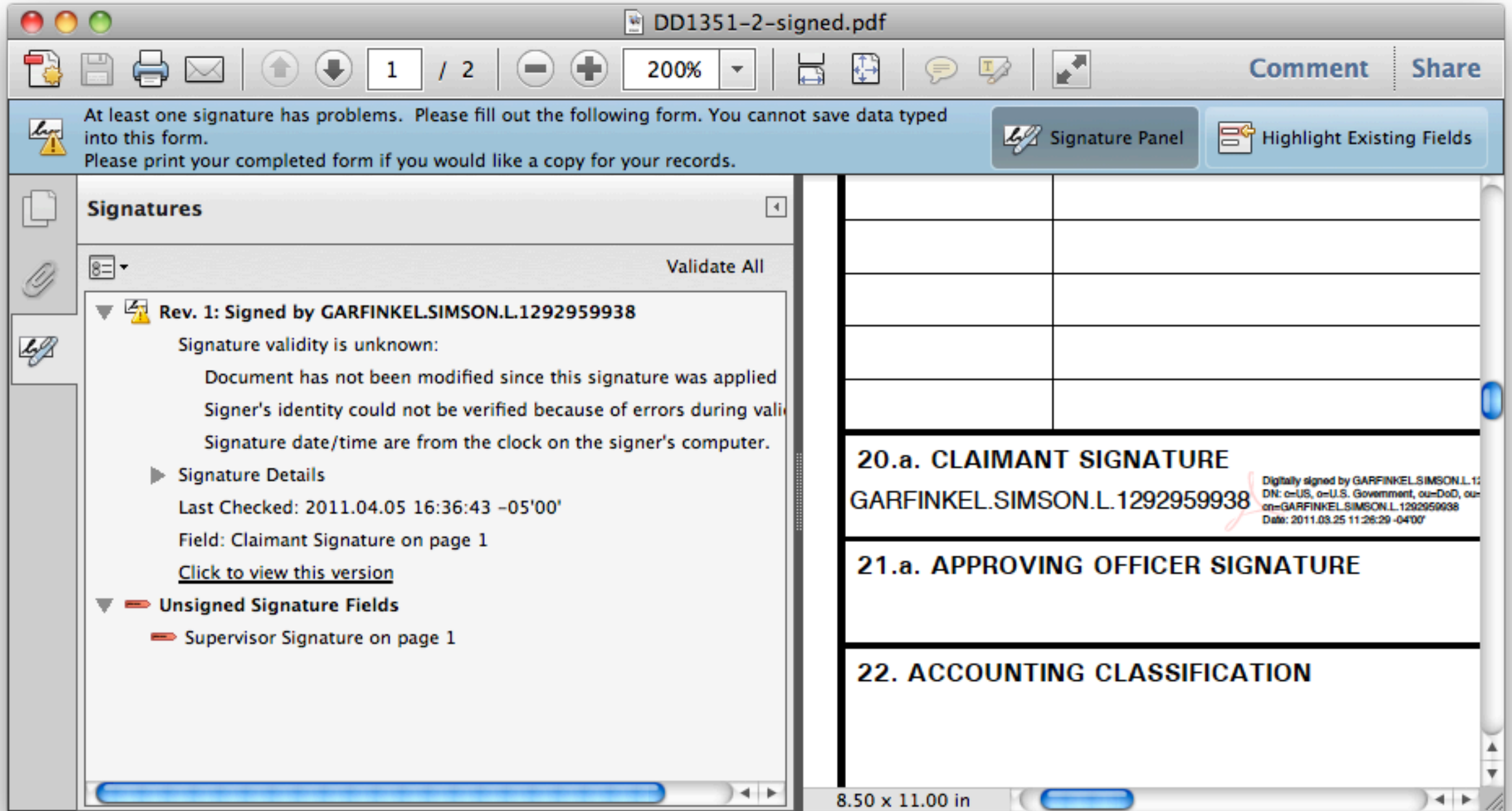
GARFINKEL.SIMSON.L.1292959938

Digitally signed by GARFINKEL.SIMSON.L.1292959938
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=GARFINKEL.SIMSON.L.1292959938
Date: 2011.03.25 11:26:29 -04'00'



Not-so-good news

DoD's CA isn't part of Acrobat Reader



DoD has taught people to *ignore* signature warnings.

Actually, DoD CA's aren't part of *any standard software.*

DoD may have largest PKI deployment on the planet.

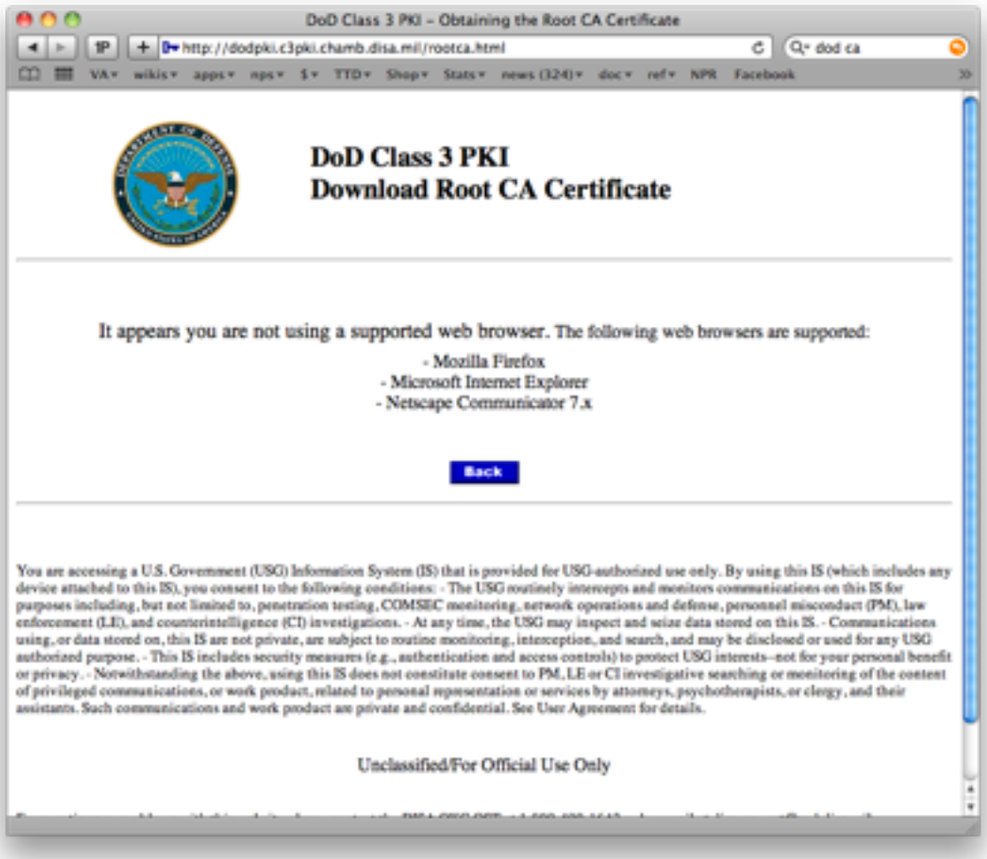
- 3 million employees with CACs.
- Millions of contractors

But DoD requires that root CA's be installed:

- On every fresh operating system install
- On home machines
- On public machines used to contact DoD systems.

DoD could:

- Get roots installed in IE & Firefox
- Cross-certify with VeriSign "bridge."



DTS isn't 100% compatible with MacOS

Firefox on Macintosh allows you to *create* travel orders, but not sign.

This is pretty weird...

Most signed messages are valid on Windows but not on Mac due to disagreements over S/MIME standard.

Original problem: Common Name vs. RFC 822 Name

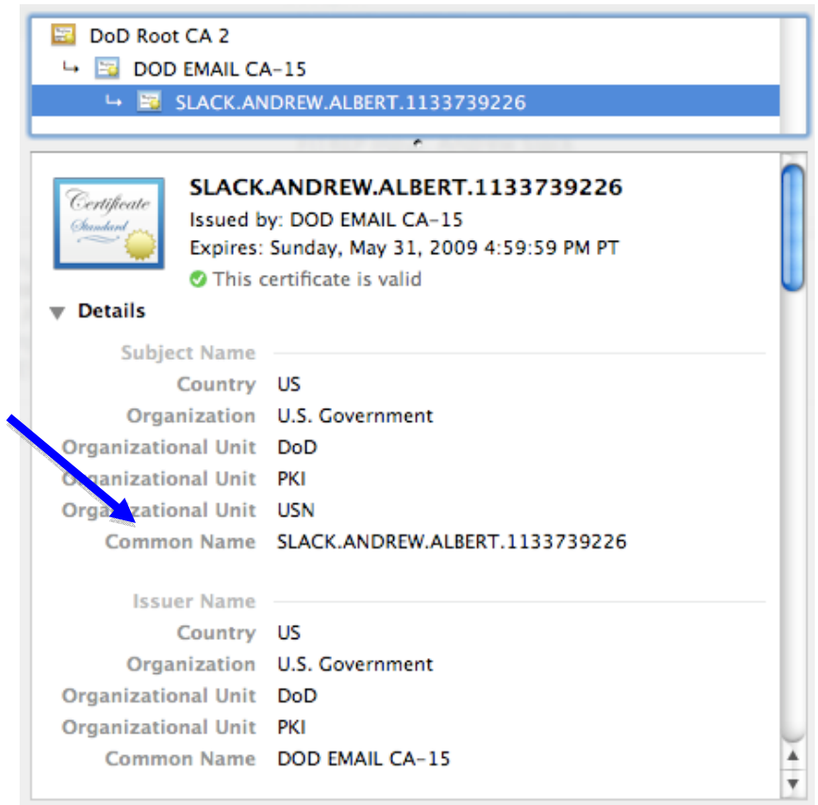


Figure 2. DoD CAC Certificate

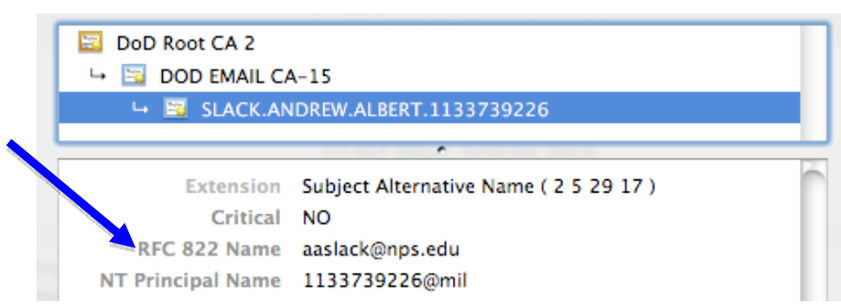


Figure 3. DOD Email Certificate (RFC 822 Name)

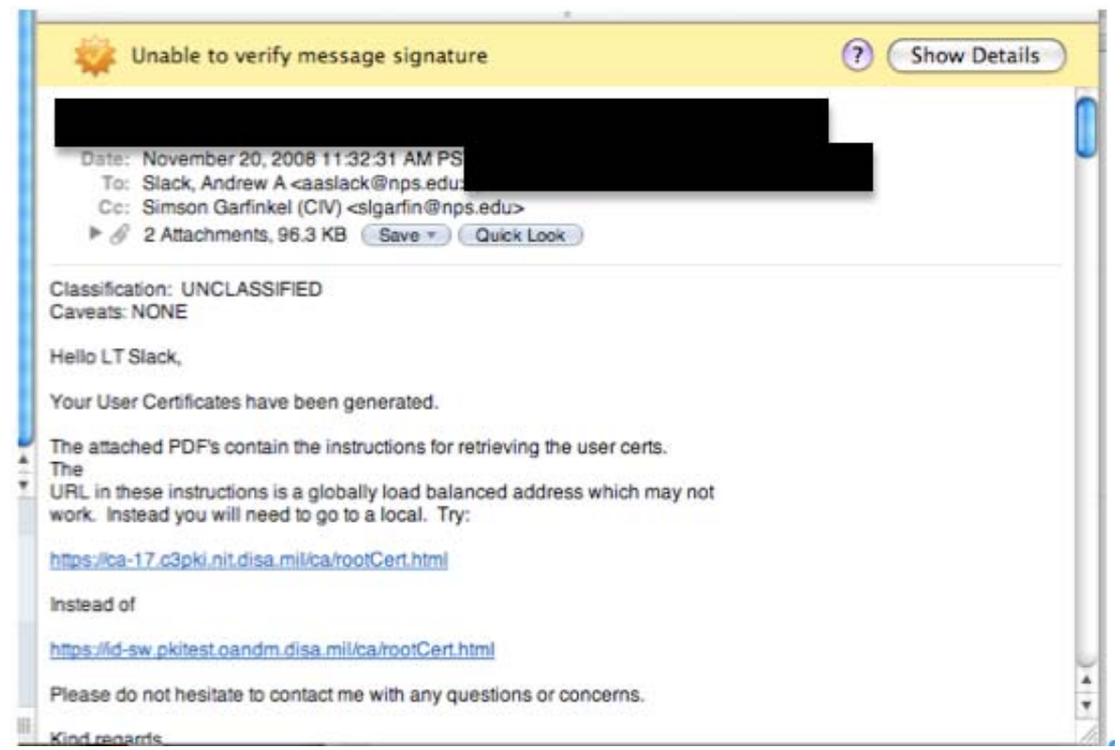
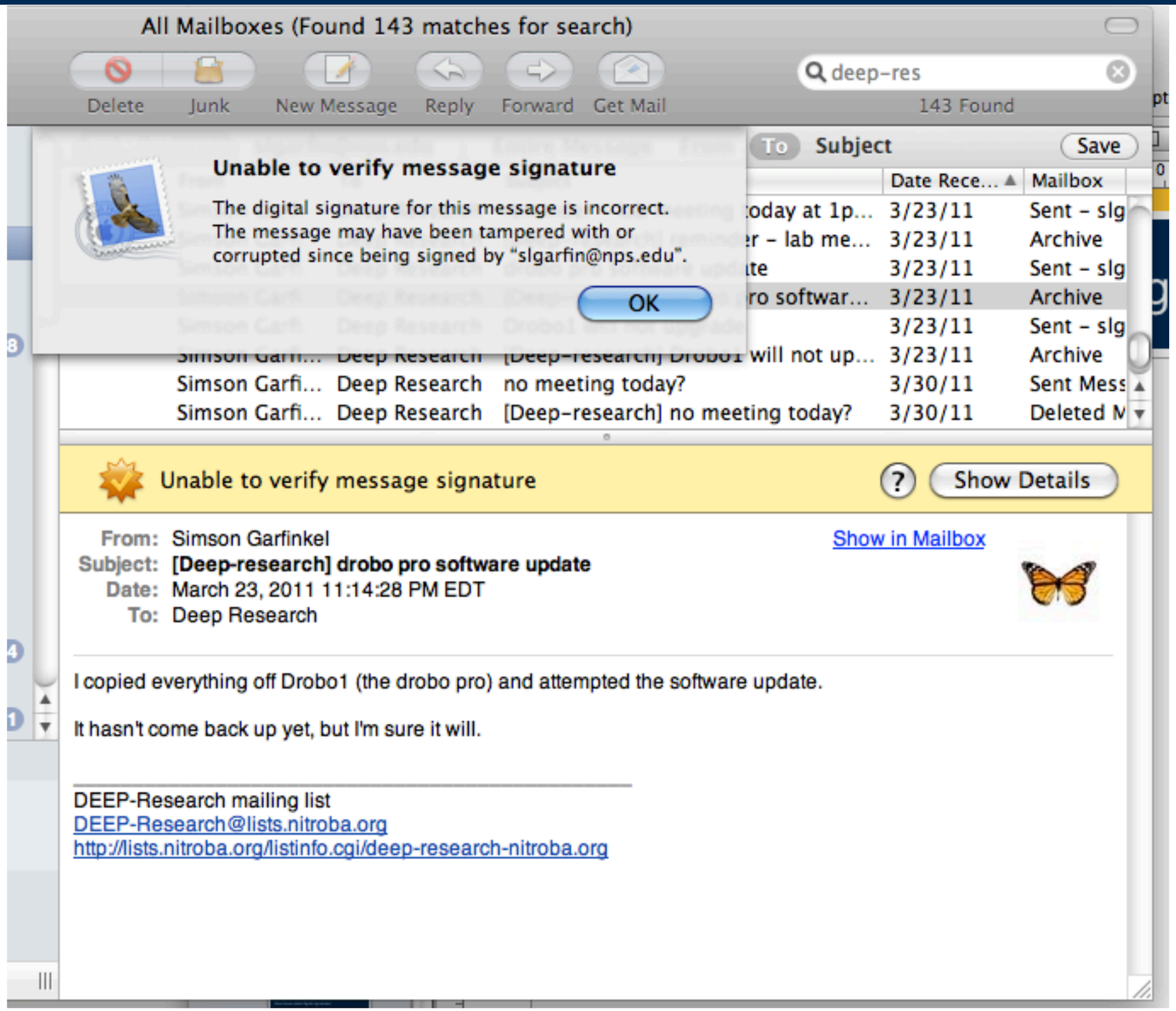
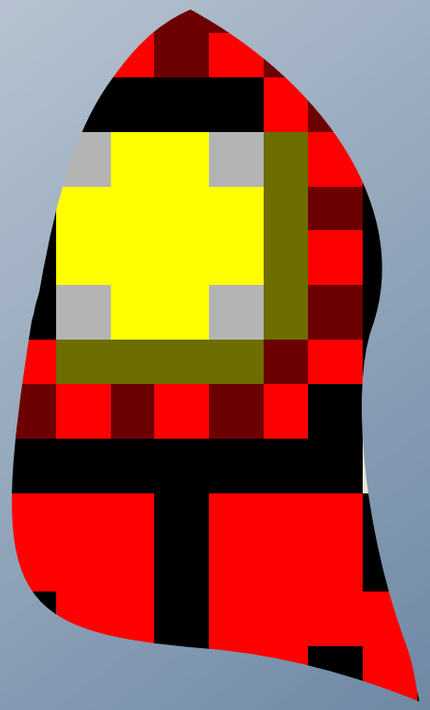


Figure 4. Apple Mail Digital Signature Error

Current problem: slgarfin@nps.edu != SLGarfin@nps.edu

Mailing lists corrupt digital signatures





Really bad problems

To date, we have been unable to get a DoD certificate to sign do-not-reply email.

"Role-Based Certificates" would seem to be the ideal mechanism.

... But DoD's policy requires that private keys be held by a *person*, not a *program*.

- Paperwork assumes that a *person* is sending out the mail.
- Not clear who the responsible party is!
  - *The programmer?*
  - *The person running the program?*
  - *The system manager?*

This makes no sense!

- We issue SSL certificates to websites (e.g. https://webmail.nps.edu)
- Has put deployment plans on hold.

PGP Confusion

S/MIME clients are *widely deployed,* but...

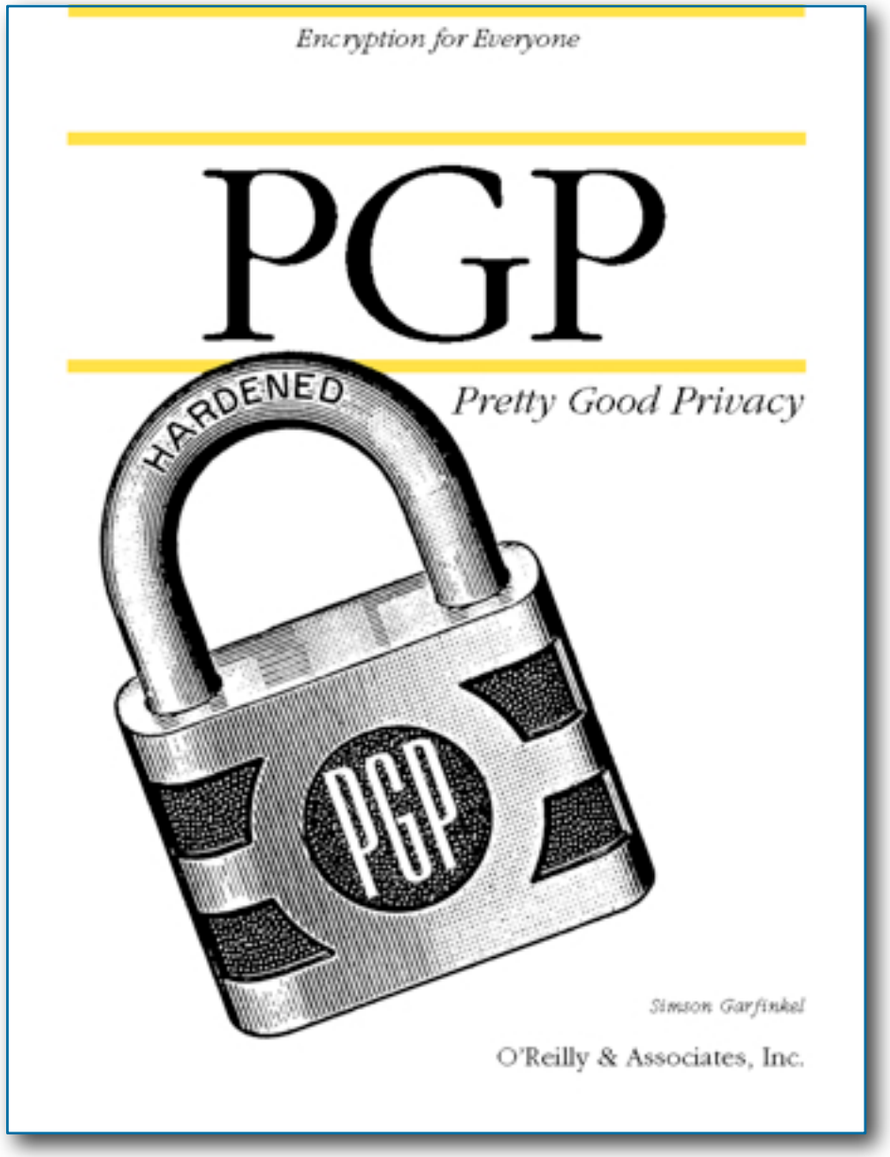
- Security “thought leaders” continue to use PGP.
- Code distributions are signed with PGP.

We have now conclusively shown that...

- PGP’s “Web of Trust” doesn’t scale.
- PGP’s model doesn’t work against most adversaries.

Nevertheless...

- People like making their own keys.
- Even “free” S/MIME keys are too hard to get.

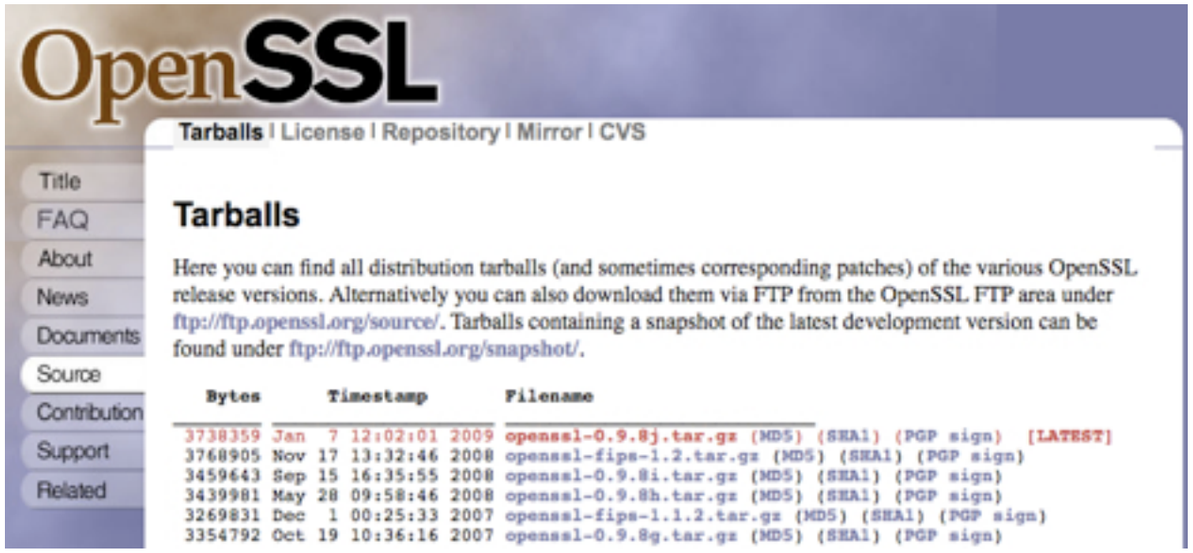


OpenSSL and Bouncy Castle

We have complete S/MIME implementations in C and Java.

- OpenSSL
- Bouncy Castle

These systems are dramatically harder to use than PGP/GPG



Gmail, Hotmail & Yahoo Mail: no support for S/MIME.

Gmail – a signed message sent to gmail – simsong@gmail.com

https://mail.google.com/mail/?shva=1#mbox/1

Gmail Calendar Documents Photos Reader Web more

Search Mail

Mail
Contacts
Tasks

Compose mail

Priority Inbox
Inbox
Buzz
Starred
Chats
Sent Mail
Drafts (11)
All Mail
Spam (1767)
Trash

[Imap]/Drafts
Apple Mail To Do
Deleted Messages
Jobs (3)
Junk
Notes
NPS
Patent 661 (5)
Sent Messages (98)
1 more

Send SMS
Phone number

IT Help Desk Software - Advanced help desk tools. - 30-day Trial.

« Back to Priority Inbox | Archive | Report spam | Delete

More actions

a signed message sent to gmail Inbox | X

Sent Messages | X

show details 8:49 PM (0 minutes ago) Reply

a test

smime.p7s
5K Download

Reply Forward

Loading "https://mail.google.com/mail/?shva=1#mbox/12f2d6fe06ac000f", completed 6 of 7 items

Domain keys didn't help with the Epsilon hack.

Sign up for FREE Account Alerts — SLG Archive 2010

Delete Junk Reply Reply All Forward Print To Do

From: Chase Mortgage
Subject: **Sign up for FREE Account Alerts**
Date: October 29, 2010 2:58:46 PM EDT
To: Simson Garfinkel and Beth Rosenberg
Reply-To: HLD <16e929563layfovciar5jlzaaaaaaacbwog4cdiuhvmyaaaaa@chasehf.bfi0.com>

If you are having trouble viewing this message, please click here. E-mail Security Information.

CHASE

STAY IN CONTROL OF YOUR FINANCES WITH
FREE ACCOUNT ALERTS.

CHASE GIVES YOU MORE.

```
Received: from bigfootinteractive.com (arm-ei106.bigfootinteractive.com [216.33.63.106])
     by godfather.dreamhost.com (Postfix) with ESMTP id 1E8711B00DA
     for <slgecr@simson.net>; Fri, 29 Oct 2010 11:59:12 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha1; d=email.chase.com; s=ei; c=simple/simple;
     q=dns/txt; i=@email.chase.com; t=1288378751;
     h=From:Subject:Date:To:MIME-Version:Content-Type;
     bh=jNOzuXpYWUjARvRuT3WdyI3KWUQ=;
     b=VZaJIaIBb1YTcefMpOuIgSubEbtUWCQbPV7hR5sEEh03Vwt4eoBJ7RuEprhvTclJ
     cLvQduq9ckXIMG+Gfx7WX094UcjzOHN4Jjyp0/v5+BeCqVw7tVIgsGRpulP9uwCE
     rlbhrtcIw4a9oydl+J5HRz+g3kAEM5MifeuEL4dRg1o=;
DomainKey-Signature: q=dns; a=rsa-sha1; c=nofws;
     s=ei; d=email.chase.com;
     h=Received:Reply-To:Bounces_to:Message-ID:X-SS:X-BFI:Date:From:Subject:To:MIME-Version:Content-Type;
     b=AlCXta6UCf9WNYeGrTBb/CbsTbqMZZXi1nTHXIXcsyyw+iKpPnqslkyHxLG1JiaT
     xVT674RqaVBLYJDgie6kqadzSX4OfaX6nMDSKnzkbYh3NE5B+NC8iOODVju1IjEc
     /NPGucMg/NZb6SPCNJ8NIArhnQdY/n81oFmBbEDM6EA=
Received: from [192.168.2.232] ([192.168.2.232:63855] helo=pimailer110)
     by pimta04.epsiloninteractive.com (envelope-from
<16e929563layfovciar5jlzaaaaaaacbwog4cdiuhvmyaaaaa@email.chase.com>)
     (ecelerity 2.2.2.45 r(34222M)) with ESMTP
     id AD/22-19159-F791BCC4; Fri, 29 Oct 2010 14:59:11 -0400
```

- Click "Update Alerts" to save your changes.

30 days

We appreciate your business. If you have questions about Account Alerts, please call us toll-free at 1-800-848-9136.

We've received your payment

Sincerely,
Chase Online Services

Your payment is due

BEFORE HACK

Please read important message about your e-mail address — Inbox

Delete Junk Reply Reply All Forward Print To Do

From: Chase <Chase@emailnotify.chase.com>
Subject: **Please read important message about your e-mail address**
Date: April 4, 2011 3:34:23 PM EDT
To: marian_and_simson@simson.net
Reply-To: Chase.254787031.3720.0@emailnotify.chase.com

Note: This is a service message with information related to your e-mail address.

CHASE

Chase is letting our customers know that we have been informed by Epsilon, a vendor we use to send e-mails, that an unauthorized person outside Epsilon accessed files that included e-mail addresses of some Chase customers. We have a team at Epsilon investigating and we are confident that the information that was retrieved included some Chase customer e-mail addresses, but did **not** include any customer account or financial information. Based on everything we know, your accounts and confidential information remain secure. As always, we are advising our customers of everything we know as we know it, and will keep you informed on what impact, if any, this will have on you.

We apologize if this causes you any inconvenience. We want to remind you that Chase will never ask for your personal information or login credentials in an e-mail. As always, be cautious if you receive e-mails asking for

```
X-Spam-Flag: NO
X-Spam-Score: 3.401
X-Spam-Level: ***
X-Spam-Status: No, score=3.401 tagged_above=-999 required=999
     tests=[HTML_MESSAGE=0.001, SARE_FORGED_CHASE=3.4] autolearn=disabled
Received: from deathwish.dreamhost.com ([208.97.132.72])
     by localhost (diehard.dreamhost.com [208.97.132.157]) (amavisd-new, port 10024)
     with ESMTP id C50kEPHdL8SM for <marian_and_simson@simson.net>;
     Mon,  4 Apr 2011 12:34:29 -0700 (PDT)
Received: from jpmchase.com (imhvf4.jpmchase.com [159.53.46.159])
     by deathwish.dreamhost.com (Postfix) with ESMTP id 614B09409C
     for <marian_and_simson@simson.net>; Mon,  4 Apr 2011 12:34:18 -0700 (PDT)
Received: from ([169.111.6.6])
     by imhvf4.jpmchase.com with ESMTP  id 90CHCH1.413329769;
     Mon, 04 Apr 2011 04:12:01 -0400
```

If you want to contact Chase, please do not reply to this message, but instead go to Chase Online. For faster service, please enroll or log in to your account. Replies to this message will not be read or responded to.

Your personal information is protected by advanced technology. For more detailed security information, view our Online Privacy Notice. To request in writing: Chase Privacy Operations, P.O. Box 659752, San Antonio, TX 78265-9752.

JPMorgan Chase Bank, N.A. Member FDIC
© 2011 JPMorgan Chase & Co.

LCEPAEM0311

This e-mail was sent to: marian_and_simson@simson.net

AFTER HACK

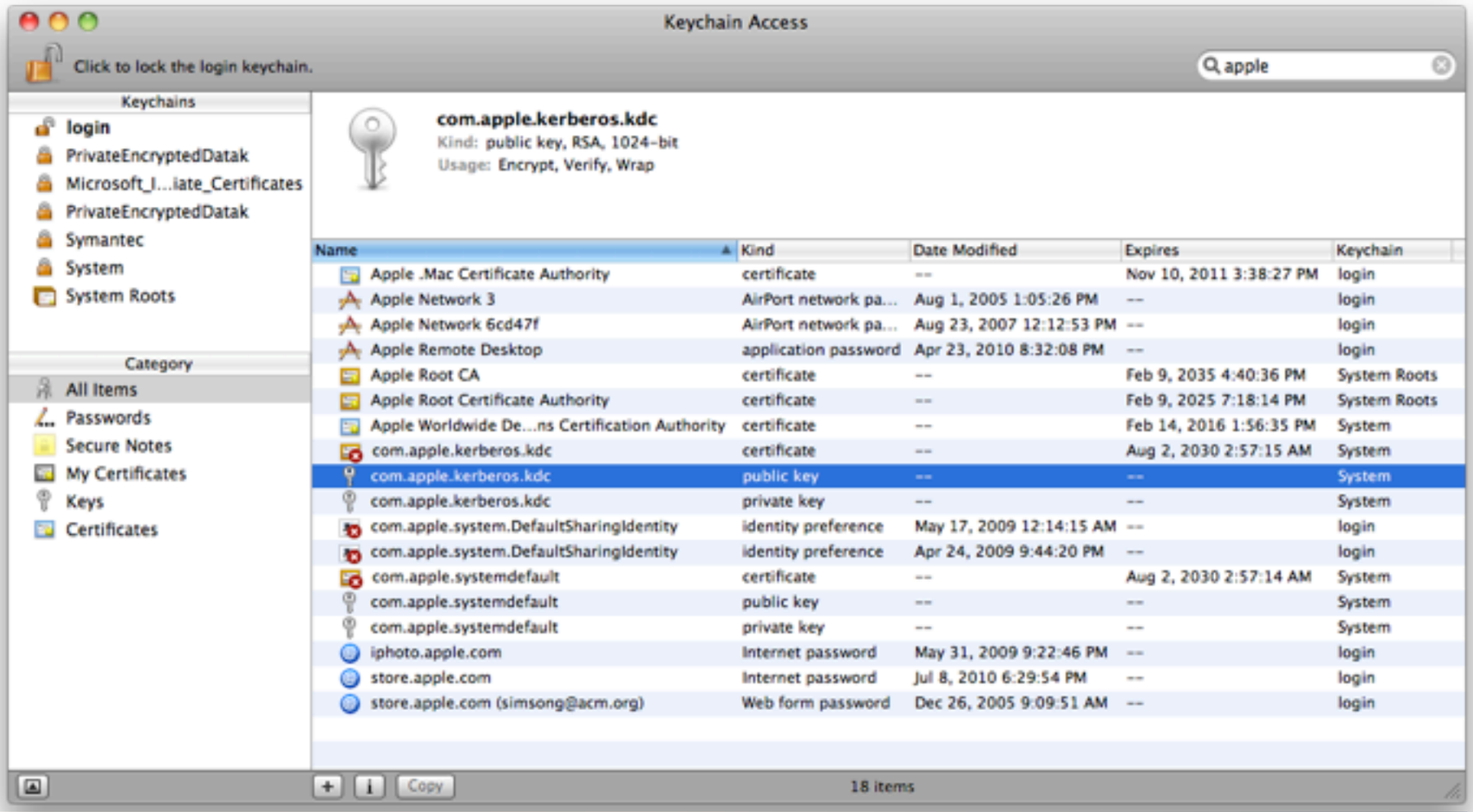
Theories regarding the use of digital signatures.

Usability is the #1 barrier to use.

People will use it if there is *no cost* and *no time commitment.*

People use PKI with:

- SSL (bad example)
- Skype
- Apple iChat



There is widespread ignorance regarding the technology.

Decision makers largely do not understand:

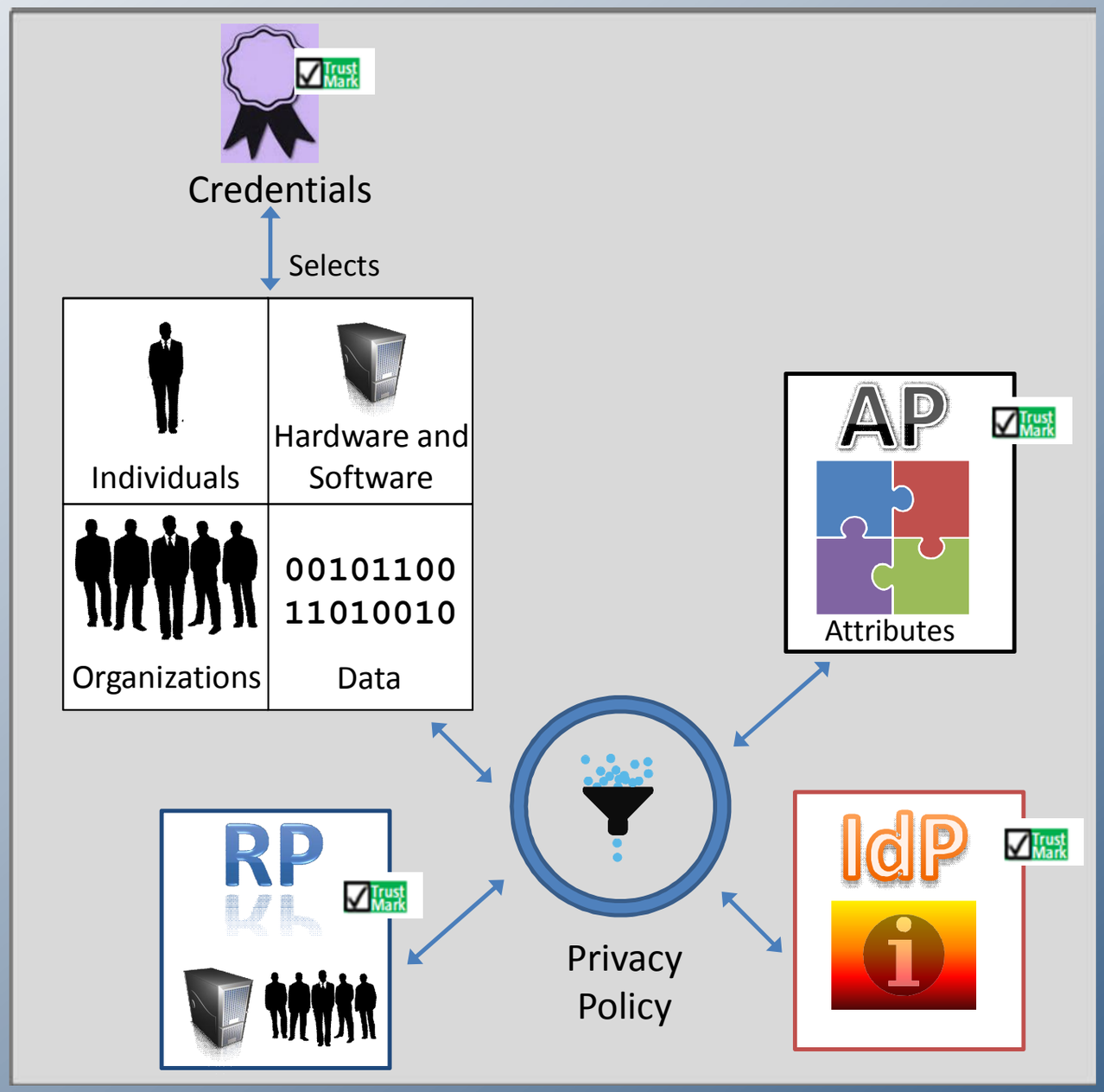
- What digital signatures do.
- Why they should be used.

Technologies largely do not understand:

- The differences between:
  - *S/MIME*
  - *PGP*
  - *DomainKeys*
- How to choose between the *technical* alternatives.
- How to choose a vendor / software package / ideology.
- How to get certificates.

Nobody is sure:

- Who are the *customers* and who are the *users.*
- The necessity of deploying a technology *before* it's used.

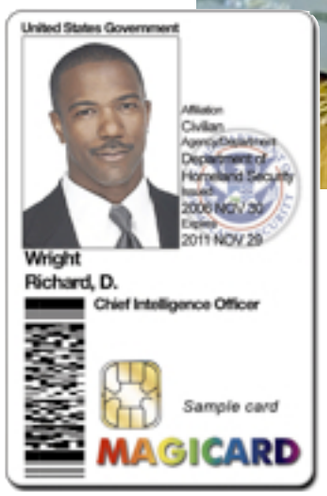


Suggestions for moving forward...

Recommendation:
Deploy and and mandate for *senders*.

USG must demand that vendors use PKI.

- Require that email sent to USG employees be digitally signed.
  - —*Mandate both* S/MIME and DomainKeys
- Accept HSPD-12 cards for authentication.
- Don't let vendors issue usernames & passwords.



DOD should get its certificates in browsers

- Microsoft; Mozilla Firefox; Apple; Android; Blackberry

Secure email plans should emphasize *signatures,* not *encryption*.

- Phishing and spam are the major risks.
- Email interception is a relative rare occurrence.

"If you've got them by the **inbox** their hearts and minds will follow."

—*Not quite John Wayne*

Questions?

The Application and the Ecosystem

Acknowledgments

- https://spaces.internet2.edu/display/fedapp/Home
  and Scott Cantor

Federating Applications

- What are the issues apps are finding in adapting to a federated world?
- What issues will they need to learn about in an attribute ecosystem
  - Sooner
  - Later

Federated Applications – The Core Issue

- We are still treating federation as an afterthought when this design would improve all web applications.
- The core problem is application developers still think their application must reimplement common business logic better resolved elsewhere – its not just passwords we should externalize.

Topics Areas Being Worked on Today

- Authentication
- IdP Discovery
- Logout
- User Identification
- Sessions
- Identity Assurance
- Attributes
- Boarding Process
- Provisioning (incl. Account Activation / Linking)
- Groups
- Authorization / Access Control
- [Error Handling]
- [Federation Trust Management]

Applications and Federated Life - Today

- IdP discovery
- User Identification
- Session Management
- The Boarding Process
- Interfederation

IdP Discovery – The Problem Space

- Federation creates the IdP discovery problem – where do you send them to authenticate?
  - In federations, we cannot expose user credentials to authentication systems controlled by unrelated organizations.
- As a result, the authentication source has to be selected before credentials are supplied, either explicitly through user choice, or by deriving something from a user identifier.
- Need better coordination amongst providers before this becomes too complex for users.

IdP Discovery Models

Models

- SP/Embedded – e.g .Elsevier
- Centralized/Shared
  - SP-centric - e.g. NIH Federated Login gateway vs. federation/IdP centrice.g. WAYF, InCommon

•Common UI "trigger" for consistency

IdP Discovery Work Arounds

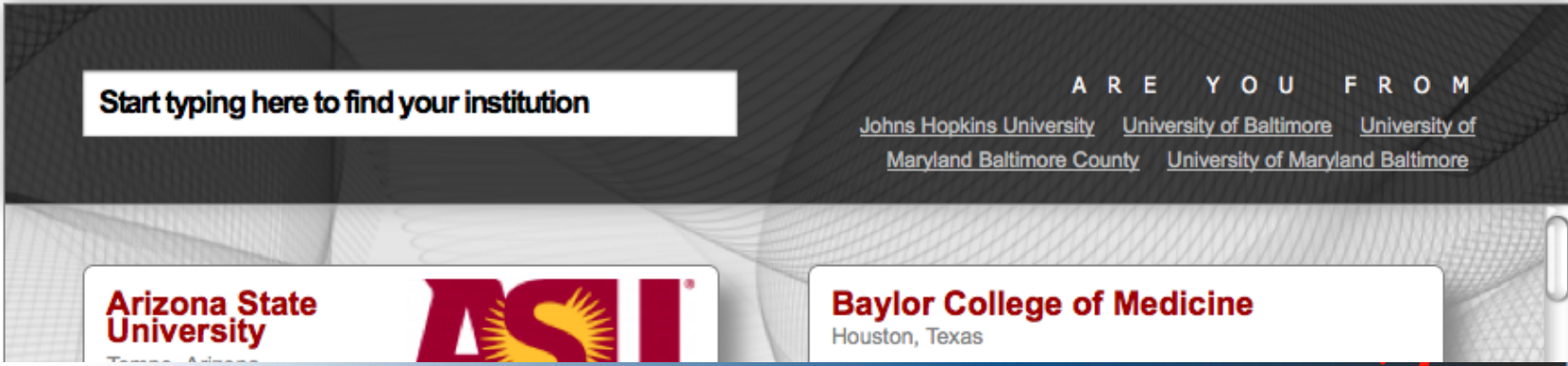
- Workarounds
  - Initiating at the IdP – e.g. PSU gets to NIH through the PSU research web site.
  - Hand out Per-IdP URLs (e.g. Google)
- Shared hints
  - Limiting discovery to expected IdPs
  - Geolocation

GeoLocation Hints - EDUCAUSE

EDUCAUSE recently began establishing trust relationships with members of The InCommon Federation. The relationships will increase security and streamline access among a group of web sites that EDUCAUSE creates and maintains for its members. If your organization is listed below, you can use this service to authenticate via your home institution's credentials. If you are a member of InCommon and would like more information on how to setup your identity provider for use with EDUCAUSE, please visit our IdP Setup page for more information.

To learn more about this service, please review background information about the EDUCAUSE/InCommon partnership.

If you run into any problems with the service, please contact support@educause.edu



Oasis Work on Discovery

SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0

Committee Specification Draft 01

14 December 2010

Specification URIs:

This Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/csd01/sstc-saml-metadata-ui-v1.0-csd01.odt (Authoritative)
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/csd01/sstc-saml-metadata-ui-v1.0-csd01.html
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/csd01/sstc-saml-metadata-ui-v1.0-csd01.pdf

Previous Version:

N/A

Latest Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/sstc-saml-metadata-ui-v1.0.odt (Authoritative)
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/sstc-saml-metadata-ui-v1.0.html
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/sstc-saml-metadata-ui-v1.0.pdf

Technical Committee:

OASIS Security Services (SAML) TC

Chair(s):

Thomas Hardjono, M.I.T.
Nate Kingenstein, Internet2

Editor(s):

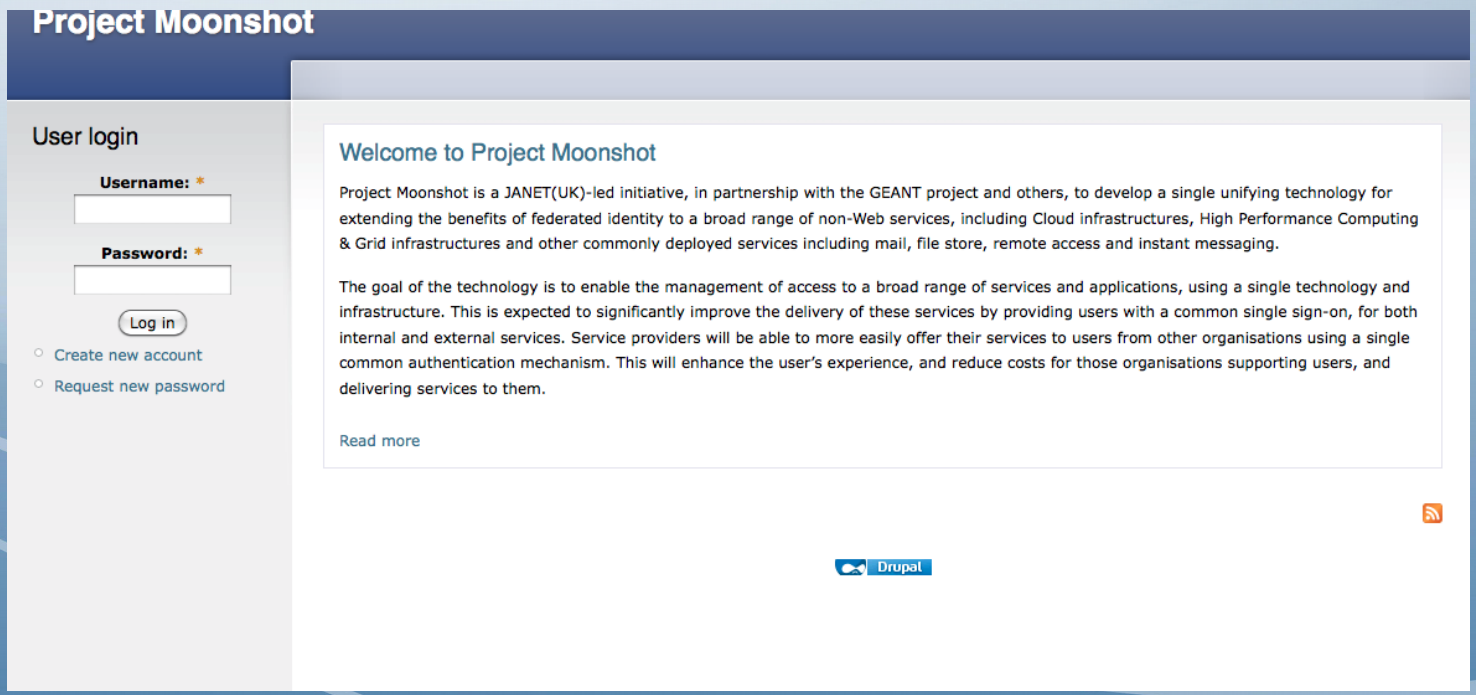
Web Authentication – Problem Space

- Web authentication involves proving the identity of a client and server to each Invokes lots of issues when externalized
  - Discovery
  - Authentication attributes & practices
  - Error Handling
  - Logout
  - Timers

Non-Web Authentication – Problem Space

- Authentication for non-web
  - TLS
  - OTP over TLS
  - SASL / GSS-API
    - Project Moonshot
    - Tie to web authentication – iTunes example.

Project MoonShot –project-moonshot.org



Identity Assurance – Problem Statement

- Does 800-63 assurance levels adequately reflect good risk abatement techniques in a federated world, especially outside gov.
  - If not, is there anything better to use?
- Transitive trust arrangements
- LOA over time
- Self-service password resets

The Next Round of Application Issues

- Logout
- Provisioning and Deprovisioning
- Metadata exchange - uApprove
- Account Linking – transitive trust
- Identity Assurance from the app view
- Error handling
- Federated Security Incident Handling

Acknowledgments

- https://spaces.internet2.edu/display/fedapp/Home and Scott Cantor

Attributes

Debbie Bucci
National Institutes of Health

CIT
Center for Information Technology

NIH Person

- Staff tracking initiative 2009 common bio sketch
- EA to investigate common attributes/data values across systems and sources
  - Clinicaltrials.gov
  - iEdison
  - My bibliography
  - NSF/USDA/NIH – FDP work
  - AAMC – multi affiliations
- NIH External Researcher Conceptual Data Model – June 2010
- ARRA funding – need to track investments across government
- Starting the work all over again – common biosketch across the government

Attribute Tiger team

- Input for various initiatives
- Competing interest
  - What is the scope?
    - Authentication/authorization/entitlements?
    - G2G, B2G, C2G
- 3 submissions – external to government
- Additional input from DHS/DOD Tiger Team
- Lead to 12 other sources
- Common concerns
  - Name
  - PII/Biographic
  - Contact (Emergency, employer, technical, support, adminstrative, supervisor, business, home)
  - Clearance
  - IDP, AP
  - Organization
  - Employment

The Attribute and the ecosystem

Topics

- Basics
- Common Schema
  - LOA of attributes
  - Privacy
  - Naming
- Complexity and Extensibility
  - Tagging
  - Complexity vs Metadata
- IdP releasing vs SP asking
  - Query languages
- Dealing with Aggregation

Killer Attributes
(and the applications that love them)

- Human readable identifiers
  - Email address, eppn, display name, etc
- Opaque identifiers
  - ePTID
- Affiliation
- Citizenship
- Over legal age

Types of attributes

- Institutional
  - Organizational
  - Reassertion of Official attributes
  - Temporal – geolocation, etc.
- Community or collaboration asserted
  - Formal – Virtual organizations, groups
  - Informal – reputation systems, FoF
- Self-asserted

Common Schema

- NIEM – National Information Exchange Model – www.niem.gov
- eduPerson -http://middleware.internet2.edu/eduperson/
- http://www.terena.org/activities/tf-emc2/schac.html
- Accessability schema - http://www.w3.org/WAI/ and http://www.w3.org/WAI/intro/uaag.php
- http://doc.esd.org.uk/IPSV/2.00.html

Eve Maler's Attribute Assurance Matrix

Identity, Access Management, and Privacy: Concepts and Technologies
The Attribute Assurance Matrix

Thinking about identity data used in your applications for authorisation or personalisation, for each identity data item:

What is the nature of the data?

What is the nature and role of the application in your organisation?

What effect does the data have on application behavior?

What are the consequences if the data is incorrect?

What party is truly authoritative for that data?

Is there a role for self-assertion or self-service in data provisioning and updating?

If you are not the authoritative party, how and how often do you get the data today?

What is your business relationship with the authoritative party?

What is your remediation strategy and workflow for incorrect data?

Naming

- Oids vs URNs vs URLs vs URI's vs
- Registering name spaces

Privacy

- Which attributes are PII?
  - ePTID – opaque, non-correlating, but 1-1
  - IP address
- Which jurisdiction applies?
  - IdP? SP? Nationality of user?
- Which require consent and for what purpose?

Authorization – Problem Statement

- In a federated landscape, with scale in mind, groups more than identities control access
- But attributes may express, in addition or instead, a user's relationship with the authenticating organization, membership in groups, or possession of roles or entitlements that signify permission to access application resources. In such cases, authorization may be delegated or distributed to the authenticating organization, or even across additional organizations. This is a relatively common pattern when the authorization policy is simple (typically all or nothing) and applies to large numbers of users at multiple organizations. It is less common as policies become more complex and fine-grained.

Groups

- Local Groups
  - User Identification
  - Provisioning (and Deprovisioning)
- Representation
  - isMemberOf
  - eduPersonEntitlement
- Groups with Federated Members
- Federated Groups
- Privacy Implications
  - Visibility of members to other members
  - Sharing groups across services

Of Entitlements and Attributes

- In entitlements, SP community passes business logic to IdP's, who compute authorization and pass entitlement
  - To scale, must have common license terms
  - SP's need to be willing to expose business logic
- In attributes, IdP's pass attributes to SP for authorization
  - Raises privacy issues
  - To scale, must have shared community attributes

Some key issues

- Which schema
- Knowing which IdP to ask for which attributes, especially as we get into aggregation
- How to ask, e.g. over 18
- Making values extensible, so that they can be tagged, like validation, date, terms of use

Attribute Release

- SP Asking vs. IdP Releasing
- Specifying requirements (queries, metadata, policy files, web pages, etc.)
- Consent

Attribute aggregation

- At the IdP
  - Already doing internal aggregation
  - Can arrange bulk feeds – e.g. IEEE member
- At the SP
  - Already in the Shib code
- At an intermediate point
  - Portals and gateways do this now
  - Can greatly simplify trust

“Over legal age”

- Use cases are legion and confusing
  - Legal age of the web site country
  - Legal age of the IdP country
  - Legal age of the identity holder’s country

- Authoritative sources and delegation
- Query languages

Complexity and Extensibility

- Complexity
  - Tagging within attribute vs use of metadata vs context
- Extensibility
  - The ability to add new controlled values
- How much flat attribute proliferation can be managed through a structured data space?
- DRM of metadata

Principles of the Tao 属性之道

- Least privilege/minimal release
- Using data “closest” to source of authority
- Late and dynamic bindings where possible
- Dynamic identity data increases in value the shorter the exposure. If identity data is cached away from the source there is increased likelihood of staleness and over-exposure which can lead to privacy and data accuracy concerns.

kjk@internet2.edu

Beyond the first horizon

- LOA of attributes
  - Specifying semantic rules
- Shifting from attribute values as text strings to rich signed data
  - Terms of use
  - Time limits
  - etc

Thanks

Program Committee

- Abbie Barbir
- Trent Adams
- Peter Alterman
- David Chadwick
- Elaine Newton
- Ken Klingenstein
- Neal McBurnett
- Radia Perlman
- Richard Wilsher
- Sara Caswell
- Kent Seamons
- Jon Solworth
- Stephen Whitlock
- Tom Greco
- Tony Nadalin
- Von Welch

Special Thanks

- Sara Caswell
- Peter Alterman
- Neal McBurnett
- Elaine Newton
- Ken Klingenstein