

Identity Management -- Background Concepts, Goals and Jargon

Joe St Sauver, Ph.D.

MAAWG Senior Technical Advisor (joe@uoregon.edu)

MAAWG Vienna, Klimt 2&3

1-2 PM, Wednesday, June 5th, 2013

<http://pages.uoregon.edu/joe/maawg-id-mgmt/>

Disclaimer: Any opinions expressed in this presentation are those of the author and not necessarily those of any other entity.

1. Introduction

MAAWG's New Identity Management SIG

- Michael O'Reirdan, now MAAWG Chairman Emeritus, came up with the idea of a MAAWG Identity Management Special Interest Group at the Spring 2013 meeting in San Francisco. His idea was enthusiastically received by the MAAWG Board, and Mike has been good enough to allow me to co-lead that activity with him.
- This session has been designed to provide a little backfill relating to identity management so that we're all "on the same page," hopefully allowing us to collectively get traction on this topic.
- While I've put together some slides, I'd prefer this to be an interactive session so please feel free to bring up topics or ask questions at any time, seminar-style. We know that many of you have significant expertise in this field and are well positioned to make significant contributions to MAAWG's work in this area.

A Disclaimer and a Little About My \$DAYJOB

- Part of my normal daily work is with Internet2 and InCommon under contract through UO Information Services, however I'm not speaking on behalf of any of those entities today, nor am I articulating any official position of MAAWG.
- I mention Internet2 and InCommon in particular because at least some of the work we're going to talk about today involves open source identity management software that originated with Internet2 (e.g., Shibboleth), and similarly, the primary higher education identity federation in the United States, InCommon, is administered by InCommon, a unit of Internet2. I want you to know about my affiliations so you can understand my perspective/biases, if any.

MAAWG Does Have Some History When It Comes to Identity Management...

- Even though MAAWG's Identity Management SIG is brand new, MAAWG's Public Policy working group did submit a couple of pages of comments back in July 2010 in response to a request for feedback on the "National Strategy for Trusted Identities in Cyberspace," see http://www.maawg.org/sites/maawg/files/news/MAAWG_DHS_NSTIC_2010-07.pdf
- For those who may not have noticed NSTIC when it first turned up...

NSTIC ("EN-stick" not "NYST-ick")

- NSTIC is the "National Strategy for Trusted Identities in Cyberspace" project, see <http://www.nist.gov/nstic/>
- The NSTIC site says, among other things:

"The National Strategy for Trusted Identities in Cyberspace (NSTIC) envisions a cyber world - the Identity Ecosystem – that improves upon the passwords currently used to log-in online. It would include a vibrant marketplace that allows people to choose among multiple identity providers - both private and public - that would issue trusted credentials that prove identity."

The NSTIC-Envisioned Identity Ecosystem

- An example of what the "Identity Ecosystem" means from the NSTIC web site:

"For example, student Jane Smith could get a digital credential from her cell phone provider and another one from her university and use either of them to log-in to her bank, her e-mail, her social networking site, and so on, all without having to remember dozens of passwords. If she uses one of these credentials to log into her Web email, she could use only her pseudonym, "Jane573." If however she chose to use the credential to log-in to her bank she could prove that she is truly Jane Smith. People and institutions could have more trust online because all participating service providers will have agreed to consistent standards for identification, authentication, security, and privacy."

NSTIC Identity Ecosystem Steering Group

- The Identity Ecosystem Steering Group (IESG) was created by NSTIC to "administer the development of policy, standards, and accreditation processes for the Identity Ecosystem Framework," see <http://www.idecosystem.org/>
- Anyone can become a member, see the form that's at:
<http://www.idecosystem.org/page/join-idesg-0>
- Once you're a member, you can participate in the work of the IESG committees by joining the committee mailing lists, and you can also participate in upcoming events.

2. But What Is "Identity Management?"

Is It Really About NSTIC's Identity Ecosystem?

Or Is It Just Usernames and Passwords?

From the POV of Some Users, Identity Management IS Just All About Usernames/PWs

- Everyone has got **too dang many** usernames and passwords. We just can't keep them all straight unless we write them down (and we know that we probably shouldn't be doing that)
- Half the time we're forced to pick **crazy passwords** that are so complex we can't even remember them
- **Resetting our passwords** (e.g., when we forget it/lock ourselves out) can be a real PITB – except when it feels ***too*** easy to us...
- **Using passwords doesn't really feel very safe to many of us** given all the computer viruses out there that are trying to mine stuff from the various password stores that may be on our computers
- Then there's the worry that **someone's trying to phish us**, and the worry that we've accidentally gone to some "look-alike" site
- As users, we ***hate*** usernames and passwords!

Identity Management From Some Providers' POV

- **Users resist signing up** for accounts (*OR* they want **a dozen accounts** instead of just the one we want them to consistently use)
- **We never know who anyone *really* is**, which is a pain for many reasons (especially if they're trying to buy stuff from us)
- Users are always **forgetting** or mis-entering their username and password, resulting in their getting locked out (which means that we then have to help them somehow **reset their passwords**)
- Users are always getting their **credentials guessed or stolen**, and then our service ends up abused
- **Users never tell us when they die or otherwise stop using our service**, so we've got tons of stale accounts, thereby keeping new users from getting "good" usernames and serving as potential targets for abusers looking for accounts they can hijack
- As providers, we ***hate*** managing usernames and passwords!

In Reality, However...

- Identity management is a lot more than "just" usernames and passwords.
- Let's consider an example of how student identities get managed in higher ed...

Academic (Student) Identity Management Lifecycle

- An applicant becomes interested in a school and creates an initial account so that they can begin getting and submitting info
- The applicant's status transitions to accepted/waitlisted/rejected, enrolled, and (eventually) graduated/transferred/withdrawn. Then we have new alumni/alumnae, or in some cases graduate students...
- Password reset requests need to be handled
- Attributes need to be set (example: academic major and minor, local address, cell phone number, 3rd party email address, etc.)
- An online directory needs to be populated, while honoring any directory information restriction requests made under FERPA
- Legal name changes need to be handled (e.g., marriages/divorces)
- Account holds need to be processed (example: student account gets hacked and begins sending spam, so account gets disabled, etc.)
- And there are many more identity management tasks...

A Canonical Identity Source, Or Chaos?

- Ideally, in the preceding student example, authoritative identity management information about the student will be maintained in a canonical system, such as the university's Student Information System (perhaps part of a larger integrated campus ERP system).
- In the case of faculty/staff, comparable information might reside in the university's Human Resources System, and for alumni, that data might be stored in a parallel Alumni Relations System.
- When identity management gets handled badly, however, multiple non-authoritative identity management systems may get turned up (for example, in individual departments and offices), and the data in those shadow systems tends to quickly become inconsistent, out-of-date, and unavailable for use by other applications.
- Shadow systems of that sort get created because authoritative identity data isn't being managed in the right sort of way. When you notice shadow systems, they should serve as a warning to you.

Contemporary Identity Management

- In modern practice, identity management is also (or should also be) about improving the "user experience," including:
 - Reducing the number of usernames and passwords a user has to create, remember and manage. This can be done through the effective use of federation and trust relationships. This reduces the amount of time users need to spend creating accounts and logging in, while simplifying things like online purchases.
 - Allowing users better control over their online privacy, while also offering "high assurance" identity credentials where necessary or appropriate for sensitive applications such as banking or health care.

3. Why An Identity Management SIG Now? Why Is Identity Management a "MAAWG Thing?"

Why Identity Management Now? Social Media

- Social media applications (such as Facebook and Google+) are becoming increasingly central to Internet activity, and of course, social applications are, at their core, all about your online identity:
 - 845 million active users on Facebook during a typical month
 - 465 million Twitter accounts
 - 135 million LinkedIn users

That's a LOT of user identities, from my POV...

Source: <http://www.jeffbullas.com/2012/04/23/48-significant-social-media-facts-figures-and-statistics-plus-7-infographics/>

Social Media Can Help Establish Your Online Identity -- But Also Increase Your Risk of ID Theft

- There's a tension when it comes to use of social media.
- On the one hand, your social network presence includes a "web of trust" consisting of friends and other individuals who know and interact with you. By doing so, they provide "proof" of your legitimacy. This is a web of "social trust" that may remind you of PGP/Gnu Privacy Guard's web of "cryptographic trust." We know that you really exist because other Facebook users friend you. :-;
- On the other hand, use of social media will result in details of your personal and professional life being publicly exposed and that may increase your risk of having your identity stolen (trivial example: if your password reset question is "What high school did you attend?" and your social media page talks about the fact that you will be attending the Lincoln High School reunion in August, well...)

Facebook Posts Help Credit Bureaus Sniff Out Fraudsters

By Danielle Kucera - May 30, 2013 7:29 PM GMT+0200



COMMENTS

QUEUE



Credit bureaus and payment companies are testing ways to use social media -- say, a [Facebook Inc. \(FB\)](#) post about a recently purchased Corvette -- to verify a person's identity and even assess consumer creditworthiness.

[Equifax Inc. \(EFX\)](#), [EBay Inc. \(EBAY\)](#)'s [PayPal](#) and [Intuit Inc. \(INTU\)](#) have begun trials to see whether social posts can help prove identities, and, in some cases, detect whether customers are lying about their finances.

Enlarge image



Consumers may share photos of new cars they've purchased on Facebook, check in on expensive flights and post pictures of items they own on Pinterest, all data that may show if a person is being truthful about disposable income. Photographer: Daniel Acker/Bloomberg

Users of Facebook, Pinterest Inc. and Twitter Inc. share personal details every day through public postings, status updates and location check-ins. That information is proving useful in validating identity, evaluating whether to make a loan and sniffing out fraud that cost U.S. online retailers \$3.5 billion last year, according to [CyberSource Corp.](#) EBay set aside \$580 million, or 4.1 percent of net revenue, to cover transaction and loan losses last year.

"We are investing a lot in how can we use unstructured data that is sitting out there in social media that can help us understand a little more about identity," [Rajib Roy](#), president

of Equifax Identity and Fraud Solutions, said in an interview.

Why Identity Management Now? The Cloud

- Many organizations want to take advantage of "cloud-based services" delivered by 3rd parties entities, which increases the importance of scalable online identity management beyond traditional organizational boundaries.
- You really don't want each new cloud-based service to have its own new username and password, right? That's what makes users go crazy/get confused/reuse the same password everywhere.
- Other options are even worse, including periodically copying passwords from some master system over to the the cloud based service(s) – wow, now *there's* a nightmare.
- You really want a federated approach, where the cloud-based service provider will *trust* the local identity provider to authenticate the user in question on their behalf.

Example: AWS and Federated ID Management

The screenshot shows a blog post from the AWS TypePad blog. The header includes navigation icons (back, forward, search, etc.) and the URL: aws.typepad.com/aws/2013/05/aws-iam-now-supports-amazon-facebook-and-google-identity-federation.html. The main content features the Amazon Web Services logo and a sidebar listing recent customer success stories. The post title is "AWS IAM Now Supports Amazon, Facebook, and Google Identity Federation". It is attributed to Jeff Wierer, a Principal Product Manager for AWS IAM. The post discusses how AWS IAM supports identity federation by allowing developers to grant temporary security credentials to users managed outside of AWS, specifically mentioning support for web identity federation with Facebook, Google, and the newly launched Login with Amazon service.

RECENT AWS
CUSTOMER SUCCESS
STORIES & VIDEOS

[Mentor Graphics](#)
[Choice Logistics](#)
[tadaa](#)
[Trinity Mirror plc](#)
[AEG](#)
[D-Link](#)
[EyeEm](#)
[LogMyCalls](#)
[Neowiz](#)
[Zedo](#)
[Bristol-Myers Squibb](#)
[GE](#)
[NASDAQ OMX](#)
[Backupify](#)
[Seven Bridges Genomics](#)
[WeTransfer](#)
[Universal Church](#)
[Getty Images](#)
[Autodesk.](#)

« [Verbalizelt - Scaling a SaaS Platform for the Shark Tank](#) | [Main](#) | [Amazon Route 53 Adds ELB Integration for DNS Failover](#) »

AWS IAM Now Supports Amazon, Facebook, and Google Identity Federation

[Jeff Wierer](#), Principal Product Manager on the AWS Identity and Access Management (IAM) team sent along a guest post to introduce a powerful new federation feature.

-- Jeff;

In a previous blog post we discussed how [AWS Identity and Access Management \(IAM\)](#) supports [identity federation](#) by allowing developers to grant temporary security credentials to users managed outside of AWS. Today we're expanding this capability with support for [web identity federation](#). Web identity federation simplifies the development of cloud-backed applications that use public identity providers such as [Facebook](#), [Google](#), or the newly launched [Login with Amazon](#) service for authentication. For those of you not yet familiar with Login with Amazon, it's a new service you can use to securely connect your websites and apps with millions of Amazon.com customers. If you're interested in learning more about Login with Amazon, please visit their launch [page](#).

Web identity federation enables your users to sign in to your app using their Amazon.com, Facebook, or Google identity and authorize them to seamlessly access AWS resources that are managed under your AWS account. If you are building a mobile or a client-based application, you can now integrate these three popular identity providers and authorize users without any server-side code and without distributing long-term credentials with the app. To support this scenario, this release introduces a new AWS Security Token Service (STS) API, [AssumeRoleWithWebIdentity](#). This API lets you request temporary security credentials for your customers who have been authenticated by Amazon.com, Facebook, or Google. Your app can then use the temporary security credentials to access AWS resources such as Amazon Simple Storage Service (S3) objects, DynamoDB tables, or Amazon Simple Queue

Why Identity Management Now? Do Not Track

- For a long time, regular cookies, Flash cookies and other persistent identifiers made it relatively easy for marketers and others to track user identities over time... but that tradition of tracking online activity is now being challenged as a result of things like community "Do Not Track" efforts and free technical browser anti-tracking/tracker-blocking tools such as Ghostery.
- The trustworthiness of online tracking identifiers is also being eroded by things like "Persistent ID" cloning tools for Apple iTunes, potentially allowing multiple iTunes installations to appear to have the same Persistent ID.

Do Not Track

Universal Web Tracking Opt Out

Overview



Do Not Track is a technology and policy proposal that enables users to opt out of tracking by websites they do not visit, including analytics services, advertising networks, and social platforms. At present few of these third parties offer a reliable tracking opt out, and tools for blocking them are neither user-friendly nor comprehensive. Much like the popular Do Not Call registry, Do Not Track provides users with a single, simple, persistent choice to opt out of third-party web tracking.

Do Not Track signals a user's opt-out preference with an HTTP header, a simple technology that is completely compatible with the existing web. [Several large third parties](#) have already committed to honor Do Not Track, but many more have been recalcitrant. We believe regulation is necessary to verify and enforce compliance with a user's choice to opt out of tracking.

Did you know...



Behavioral advertising accounts for [less than 5%](#) of U.S. online advertising revenue. ☺

For users

Your browser **supports** Do Not Track ✓

You **have enabled** Do Not Track ✓

How to enable: [Firefox](#), [Internet Explorer](#), [Safari](#)

Developer resources

[Cookbook](#): how to build third-party advertising, analytics, and social features without tracking

[Draft Standard Specification](#)

[FourthParty Web Measurement Platform](#)

[Reference Browser Extensions](#)

[Web Application Templates](#)

[Web Server Configurations](#)

Policy materials

[FTC Comment](#): comprehensive policy statement

[Annotated Bibliography of Related Work](#)

Stay on top

[Follow @donottrack on Twitter](#)

www.ghostery.com

Ghostery™

DOWNLOAD NOW  ABOUT GHOSTERY PRIVACY POLICY SUPPORT GHOSTERY BLOG



Detect

Ghostery™ sees the invisible web - tags, web bugs, pixels and beacons. Ghostery tracks the trackers and gives you a roll-call of the ad networks, behavioral data providers, web publishers, and other companies interested in your activity.



Learn

After showing you who's tracking you, Ghostery™ also gives you a chance to learn more about each company it identifies. How they describe themselves, a link to their privacy policies, and a sampling of pages where we've found them are just a click away.



Control

Ghostery™ allows you to block scripts from companies that you don't trust, delete local shared objects, and even block images and iframes. Ghostery puts your web privacy back in your hands.



CONNECT WITH GHOSTERY

 Follow Us On Twitter
 Friend Us on Facebook

FEATURED ON

The New York Times
THE GLOBE AND MAIL
The Washington Post

OUR PROMISE

NO ADWARE, SPYWARE OR MALWARE...EVER.

Ghostery is free to download and use - plus you have our promise that Ghostery will never be used for advertising. In fact, Ghostery is now part of Evidon, whose mission is to enable a more transparent, trusted environment for

Why Identity Management Now? Account Hijacks

- "The way we daisy-chain accounts, with our email address doubling as a universal username, creates a single point of failure that can be exploited with devastating results. Thanks to an explosion of personal information being stored in the cloud, tricking customer service agents into resetting passwords has never been easier. [* * *] This summer, hackers destroyed my entire digital life in the span of an hour. My Apple, Twitter, and Gmail passwords were all robust—seven, 10, and 19 characters, respectively, all alphanumeric, some with symbols thrown in as well—but the three accounts were linked, so once the hackers had conned their way into one, they had them all."

"Kill the Password: Why a String of Characters Can't Protect Us Anymore," Matt Honan, Wired, 11.15.12,
www.wired.com/gadgetlab/2012/11/ff-mat-honan-password-hacker/

24 April 2013 Last updated at 14:06

Share

AP Twitter account hacked in fake 'White House blasts' post

The Associated Press has said its Twitter account has been hacked, after the posting of a bogus post about explosions at the White House.

The news agency's account was suspended and it advised all tweets should be ignored until further notice.

The false message said: "Breaking: Two Explosions in the White House and Barack Obama is injured."

US markets were spooked by the tweet; the Dow Jones Industrial Average dropped 150 points as it was retweeted.

On Tuesday evening, the FBI said it was investigating the incident.



Dr Herb Lin, a cyber security expert, says media agencies are likely to make security changes to their Twitter account

Related Stories

[The problem with](#)

[See also: <http://www.zerohedge.com/news/2013-04-23/twitter-hack-compete-evaporation-all-market-liquidity-one-chart>]

Why Identity Management Now? Passwords Are "Dead"

- "Passwords are dead."
 - Bill Gates, RSA, 2004
- Or are they? Passwords seem to have lingered onwards for nearly ten years in Bill Gate's authentication purgatory, never ascending into heaven or descending into hell.
- *"The sad truth is that passwords are a problem that nobody really wants to solve. Users want to do whatever is easiest, and don't want to be burdened by the inconvenience of strong authentication. System owners don't want to spend any money on stronger authentication, and lack the will to enforce an unpopular mechanism on users."* <http://blogs.gartner.com/jay-heiser/2012/08/01/passwords-are-dead-long-live-the-password/>

Why Identity Management Now? The Promise of Much-Hyped "Big Data"

- Finally, we need to recognize that identity management underlies and supports much of the interest in "big data" -- whether you're a marketer who's delighted by what you've been able to accumulate, or a privacy advocate horrified at the loss of online privacy.
- Identity management is a double edged sword that can cut both directions, helping advertisers to better track your preferences and interests so as to better meet your needs (whether latent or expressed), while also potentially allowing you to reduce the amount of information shared with third parties (for example, a federated approach to identity may allow your email identity to be kept confidential, with only relevant attributes being released to third parties who have a legitimate need-to-know)

In Other Communities, Identity Management Is Being Driven By Problems With "Leaks"

www.fiercegovernmentit.com/story/intel-chief-looks-metadata-identity-management-prevent-wikileaks-redux/2012-01-29

Intel chief looks to metadata, identity management to prevent WikiLeaks redux

January 29, 2012 | By David Perera

SHARE

Email

TOOLS

Comment

Print

Contact Author



James Clapper speaks Jan. 26, 2012 at a CSIS event in Washington, D.C.

The intelligence community has embarked on a 5 year metadata and identity management effort meant to prevent a repeat of incidents such as the WikiLeaks disclosure of State Department cables, said James Clapper, director of national intelligence.

Clapper spoke Jan. 26 at an event held by the Center for Strategic and International Studies in Washington, D.C.

"Over the next, say, five years I think we will have made some serious and noticeable changes," Clapper said. Robust identity management is needed to ensure that only bona fide recipients of information receive data shared electronically, while the tagging of data should permit the wider sharing of that information among legitimate consumers, he explained.

SIGN UP FOR NEWSLETTER

EMAIL ADDRESS

FierceGovernmentIT tracks the latest developments in the U.S. government's 24,000 decision makers and IT execs. Subscribe to our free thrice weekly e-newsletter today!

POPULAR STORIES —

MOST READ **MOST SHARED**

DoD decision on Vista disappointing
NAVY delays NGEN award to Juniper
GAO: Social Security needs to make changes or face trouble
TRACON air traffic control modernization prospect of more schedule, cost increases
PortfolioStat reflects OMB concern over authority

THE LIBRARY: WEBINARS

Why Identity Management at MAAWG?

- MAAWG member companies already enable hundreds of millions of user identities worldwide. Everyone who sends email (or who uses a smart phone or other mobile device) already has an "online identity" in the form of an email address or phone number, right?
- Creating and administering those identities is both a huge potential expense and a potentially invaluable treasure trove of marketing information – IF you're the organization providing and logging the use of those identities.
- Online identities are also the focus of identity thieves, e.g., phishing/social engineering, and credential harvesting by crimeware such as Zeus or Brasilian banker trojans.
- It seems clear that identity management is really quite central to much of the work that MAAWG and its membership worries about.

Identity Management and... Personal Reputation?

- MAAWG and its members have worked on many different reputation-related areas, including IP address reputation and domain reputation – maybe the time has come for user-level reputation work, too? After all, if MAAWG members could confidently tie mail to actual users, that would be a very fine-grained reputation accumulation mechanism, right?
- This topic ties closely to issues such as use of PGP/Gnu Privacy Guard, or the use of S/MIME for per-user cryptographic message signing (but are people actually willing to swallow the message-level crypto pill?) [Note that we've previously talked about client certs and using S/MIME at MAAWG, see "Client Certs and S/MIME Signing and Encrypting: An Introduction," Feb 2012, <http://pages.uoregon.edu/joe/maawg24/maawg24.pdf>]

4. Stepping Back For a Minute, How Did We Get Where We Are Today?

At The Dawn Of The Modern Era...

- In "the beginning" -- let's say fifty years ago -- there was no identity management because computers were accessed directly, e.g., you computed in person.
- Identifying approved users was easy, because only a small number of people had physical access to those early systems, and users needed to be physically present to run jobs (unless they were using a system where they'd turn in their jobs to a computer operator who'd then run it for them)
- It was easy to recognize authorized users: the number of people interested in using those systems (and skilled enough to practically do so) was small.

A Computer From That Era: The IBM 704



Credit: http://en.wikipedia.org/wiki/File:IBM_Electronic_Data_Processing_Machine_-_GPN-2000-001881.jpg

A Brief Geek Digression on the IBM 704

- First mass-produced computer with floating point hardware, a big deal to computationally-oriented guys of the time.
- 123 were sold from 1955-1960
- Vacuum tube-based
- (Real) core memory (4K 36-bit words)
- Programs entered via punched cards; output via printer or (an optional) 21" long persistence phosphor CRT display
- 4K instructions per second
- FORTRAN was created for use with this system
- Access to the system? As we mentioned, go to the computer....
- Lots more at http://en.wikipedia.org/wiki/IBM_704

Local Usernames/Passwords and Local Files

- Now let's make this scenario just a little more complicated.
- Let's pretend that this is still the old days, but not quite as far back. At that point, maybe you're using a 110 baud ASR33 teletypewriter or a 300 baud DECwriter to connect to a remote time sharing computer, dialing in with an acoustical coupler or modem.
- On the remote system, inbound modems would have been connected directly to serial ports on the system (Ethernet wasn't part of the picture at that point).
- You would have an identity on that timesharing system, but it existed primarily to track/limit your usage, and to allow files you'd saved to be connected to (and charged against) your quota.

When Was The First Username/Password?

- This is a bit of an open question. In 2012, Wired magazine ran an article crediting MIT CTSS, see www.wired.com/wiredenterprise/2012/01/computer-password/ which noted:

According to Fernando Corbató [the person who was responsible for the CTSS project] even though the MIT computer hackers were breaking new ground with much of what they did, passwords were pretty much a no-brainer. "The key problem was that we were setting up multiple terminals which were to be used by multiple persons but with each person having his own private set of files," he told Wired. "Putting a password on for each individual user as a lock seemed like a very straightforward solution."

Why Else Should We Recall CTSS?

 www.multicians.org/thv/mail-history.html

The History of Electronic Mail

Tom Van Vleck

Computer mail and messaging have probably been independently invented many times. I do not know who first invented these applications, and I haven't found any documented versions that precede the ones I helped create in 1965. This note describes my knowledge of the history of electronic mail and instant messaging.

(I don't really like to use the term "e-mail" or "email." I usually just call it "mail." The use of electrons for mail may someday become quaint, replaced by photons or quarks; should we prepare to speak of "p-mail" or "q-mail"?)

CTSS

The [Compatible Time-Sharing System \(CTSS\)](#) was begun at the MIT Computation Center in 1961. By 1965, there were hundreds of registered users from MIT and other New England colleges, and CTSS service was provided every day to up to 30 simultaneous users on each of the Computation Center and Project MAC IBM 7094s.

CTSS allowed users to log into MIT's [IBM 7094](#) from remote dial-up terminals, and to store files online on disk. This new ability encouraged users to share information in new ways. When geographically separated CTSS users wanted to pass messages to each other, they sometimes created files with names like `to tom` and put them in "common file" directories, e.g. `M1416 CMFL03`. The recipient could log into CTSS later, from any terminal, and look for the file, and print it out if it was there.

Mail

A proposed CTSS `MAIL` command was described in an undated Programming Staff Note 39, "[Minimum System Documentation](#)"  by Pat Crisman, Glenda Schroeder, and Louis Pouzin. Numerical sequence places the note in either Dec 64 or Jan 65. PSN 39 proposed a plan for documenting the CTSS system as many of its developers transitioned to the Multics development project. Among other topics, PSN 39 suggested creation of a facility that would allow any CTSS user to send a message to any other. The proposed uses were communication from "the

Link Between Identity Management & Messaging

- That early connection between identity management and messaging is natural, and, I'd argue, a virtually inescapable one.
- If you have multiple users of a shared system, there needs to be a way to map each resource owners to their stuff, limit access to private resources, and account for usage. That implies a need for identities.
- Once you have multiple users on a shared resource, the desire for those users to communicate with each other also becomes inescapable, if only for things like griping about some colleague hogging too much in the way of shared resources, or asking an operator about the status of submitted jobs, etc.
- Thus, it is entirely natural and appropriate that MAAWG should continue to develop a thread of work around identity management. Messaging and identity management just go together well!

User IDs and Group IDs

- Coming back to our remote access example, that system, assuming it was running some version of Unix, would have had a unique numeric identifier (a user ID) for each user, defined in /etc/passwd (plus /etc/shadow later). Each user also was also assigned to a particular numeric group ID (as defined in /etc/group). For example, all users from the chemistry department might be in one group, all users from the physics department might be in another; users with special admin privileges might be in the "wheel" group.
- Group IDs are nice examples of a couple of features that we'll see pop up again in other identity management-related contexts:
 - group memberships
 - attributes or assertions about users ("jsmith is an administrator," or "sallyjones is a member of the Physics Department")

Exporting Files, Sharing Authentication

- Now let's make things just a *bit* more complicated still...
- Instead of one system and some locally attached disk, assume we're talking about a set of "powerful" networked Unix scientific workstations, perhaps a lab of Sun SPARCstation 2 systems from 1990 or thereabouts.
- Those nodes are going to share a set of usernames and passwords (so that a user can login to any of those nodes) and a network file system mounted on all the nodes (so that the user can work on the same set of files regardless of what node he or she is logged into).

NFS and NIS/YP

- To export the files, let's use NFS v2, created circa 1989 (see http://en.wikipedia.org/wiki/Network_File_System#NFSv2)
- To manage the identities, let's use NIS/YP (see http://en.wikipedia.org/wiki/Network_Information_Service)
- Identity management is still "tiny scale:" a lab of local systems, perhaps with a few hundred users, all within the same administrative domain. You may see people running this architecture even today (even though NIS has severe security limitations, see https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/3/html/Security_Guide/s1-server-nis.html)
- At the same time, other developments were taking place. For example, imagine providing dial in service to multiple time sharing systems from a shared pool of modems connected to a terminal server, and those users would also need to be authenticated...

RADIUS

- RADIUS (Remote Authentication Dial In User Service) was created by Livingston Enterprises to handle authentication, authorization and accounting for Merit Networks dial in users circa 1991. An extensive suite of RFCs document the protocol, see <http://en.wikipedia.org/wiki/RADIUS#RFCs>
- RADIUS is still in use today for enterprise AAA chores, with the most popular implementation probably being <http://freeradius.org/>
- Because RADIUS supports the use of different realms, it can also be used to support cross-ISP roaming users.
- RADIUS was *supposed* to be replaced by Diameter ("Diameter is twice RADIUS!"), but largely hasn't been, except in mobile network contexts (e.g., 3G, LTE and IMS). See RFC6733 for more about the Diameter protocol.

Other Enterprise AAA Technologies

- LDAP (Lightweight Directory Access Protocol, see en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol) includes the ability to "bind" (authenticate) users, and contributes a lot to what you'll see later in this talk when we talk about federated authentication, including things like schemas.
- Kerberos is another enterprise AAA technology, see RFC4120. Kerberos may be deployed in classic Unix form (MIT Kerberos), or in the form of Active Directory, as used by Microsoft Windows.
- And then there's CAS (Central Authentication Service), a popular web-based single sign on option, see <http://www.jasig.org/cas>
- Clearly there are a lot of enterprise-scale authentication options...

Auth Drives Architectural Choices And (Easily Integrated) Application Options

- You will notice by this point that at this point there is the potential for a bit of a battle when it comes to who will do identity management for the organization, and with potentially very high stakes -- if you control the enterprise identity management infrastructure, you have a real leg up when it comes to guiding the direction of the rest of your architecture.
- That is, for example, if you decide to do Microsoft Active Directory in the enterprise, that might push you toward different enterprise application choices than if you're using LDAP or RADIUS as a core authentication technology, perhaps.

5. The Inter-Domain, Non-Enterprise Case (Really, The World Wide Web)

We Don't Need Identity Management For All Internet Applications, Just For The Web

- To a first approximation, for most users, "the Internet" is synonymous with what they can access via the web.
- Thus, at least if we're talking about typical users, they don't care about things like ssh command line access, or pretty much anything except the web (even their email and other messaging probably happens within a web browser, rather than using a dedicated POP or IMAP client).
- Thus, the goal these days, at least when it comes to "Internet" authentication and authorization for normal users," we just need to handle the web-based case. (I know this seems like an incredible oversimplification, but I think it is likely an accurate one)

Public, Internal, and Private Web Access

- If you're just accessing publicly available web pages, no authentication or authorization is normally required.
- If you're accessing non-public "internal only" web pages (what's often referred to as an organizational "intranet"), authorization and access control is often handled by hosting the web server on non-routable address space, or by explicitly limiting access to the company's IP address blocks, with off site access being handled through use of a VPN
- If you're accessing personal web pages (for example, a web email account), you'll normally login with some sort of credential, hopefully over a TLS/SSL protected/encrypted channel, at which point the server will normally set a "cookie" on your browser, thereby logging your browser in. That cookie may be persistent, or a temporary cookie that's discarded when your session's over.

Single Sign On (SSO) and OpenID

- Users working from dedicated personal laptops also want to be able to "stay signed on," and not have to repeatedly login just to access other applications from the same provider.
- Thus, for example, a Google user, once they've signed on to access Gmail, will want to be able to access other Google person-specific resources without having to repeatedly "re-login" – and they can. This is true not just for Google accounts, but also for accounts from other providers, such as Yahoo, too – once logged in, your credentials will work for all (or virtually all) applications offered by that provider.
- The question, though, is "What of third party providers?" For example, what if you want to access some third party provider's service, authenticating to that service with your Google account or your Yahoo account? Yes, that can be done, too.

6. Federated Authentication With OpenID

We're Not Going To Rehash The Step-By-Step Process By Which OpenID Works

- If you want a nice step-by-step summary of how OpenID works, see the discussion and diagrams that are available at <https://developers.google.com/accounts/docs/OpenID>
- I also rather like:
"Single Sign-On For the Internet: A Security Story,"
<https://www.blackhat.com/presentations/bh-usa-07/Tsyrklevich/Whitepaper/bh-usa-07-tsyrklevich-WP.pdf>

While this is a 2007 document, it does a nice job of summarizing not just how OpenID is meant to work, but some of the ways that OpenID could potentially be abused (at least if people are casual about how they implement/use it)

Federated Login for Google Account Users

Third-party websites and applications can now let visitors sign in using their Google user accounts. Federated Login, based on the [OpenID](#) standard, frees users from having to set up separate login accounts for different web sites--and frees web site developers from the task of implementing login authentication measures. OpenID achieves this goal by providing a framework in which users can establish an account with an OpenID provider, such as Google, and use that account to sign into any web site that accepts OpenIDs. This page describes how to integrate Google's Federated Login for a web site or application.

Note: If you are planning to provide a "sign-in with Google" feature, we recommend using [Google+ Sign-in](#), which provides the OAuth 2.0 authentication mechanism along with additional access to Google desktop and mobile features.



Sign in with Google

Google supports the OpenID 2.0 protocol, providing authentication support as an OpenID provider. On request from a third-party site, Google authenticates users who are signing in with an existing Google account, and returns to the third-party site an identifier that the site can use to recognize the user. This identifier is consistent, enabling the third-party site to recognize the user across multiple sessions. Google also supports the following extensions:

OpenID Attribute Exchange 1.0 allows web developers to access, with the user's approval, certain user information stored with Google, including user name and email address.

OpenID User Interface 1.0 supports alternative user experiences for the authentication process. The default experience requires the web application to redirect users away from the application site to Google's authentication pages. This extension allows web developers to open Google authentication in a popup window and includes favicon support for a smoother experience.

OpenID+OAuth Hybrid protocol lets web developers combine an OpenID request with an [OAuth authentication](#) request. This extension is useful for web developers who use both OpenID and OAuth, particularly in that it simplifies the process for users by requesting their approval once instead of twice.

Google Is Not the Only OpenID Provider, But It Is Probably the Most Widely Used One

- There are literally hundreds of OpenID providers out there, although just a handful account for the vast majority of OpenID logins, see <http://janrain.com/blog/what-are-most-popular-networks-social-login-and-sharing-web/> which quotes the values:

<i>Google:</i>	38%	38% (cumulative %)
Facebook:	27%	65%
Yahoo:	14%	79% (top 3 providers = ~80%)
Twitter:	7%	86%
Windows Live:	6%	92%
Other:	8%	100%

- That same article notes that OpenID provider popularity varies according to the type of web site that's being accessed.



Surprise! You may already have an OpenID.

If you use any of the following services, you already have your own OpenID. Below are instructions on how to sign in with each of the following providers on an OpenID enabled website. (When you see bold text, you should replace it with your own username or screenname on that service.)



Look for the "Sign in with a Google Account" button or use your [Google Profile URL](#).



Look for the "Sign in with Yahoo" button.



Look for the "Yahoo! JAPAN
IDでログイン" button.



Enter
"username.livejournal.com"



Click the "Sign in with Hyves" button.



Enter your blog URL:
"blogname.blogspot.com"



Look for the "Sign in with Yahoo" button or use your photostream URI.



Click the "Sign in with Orange" button or enter "orange fr"



[mixi](#) is a web service that allows users to communicate with their friends and acquaintances



Look for the "Login with MySpaceID" button or enter "www.myspace.com/username"



Enter your WordPress.com URL, for example:
"username.wordpress.com"

Look for a "Sign in with AOL" button or enter openid.aol.com/screenname

Other Well Known & Simple Providers

In addition, there are several dedicated OpenID providers that are generally recommended by various members of the community. While not a comprehensive list, each of these providers offers a free and secure OpenID to use across the web.



Not All OpenID Providers Will Necessarily Work The Way Originally Intended...

- For example, imagine an OpenID provider that provides a redirection layer between an OpenID, concealing/protecting a user's real email address from disclosure... This is not a hypothetical service – this is exactly what LiquidID does, see <http://liquidid.net/home.php> (does this remind you of privacy/proxy domain name registrations? It sure strikes a chord for me in this respect...)
- Even more "interestingly," imagine an OpenID provider that offers completely anonymous "throw away" OpenID credentials, much in the way that Mailinator offers completely anonymous throw away email addresses...

Anonymous OpenID

brought to you by...



What is this?

In short: automatic, anonymous, registration-less & disposable OpenID log-ins.

OpenID is a solution to the problem of having to keep track of usernames and passwords for sites that require log-ins. Many sites are now OpenID enabled and allow visitors to log in using only the URL of their profile on an OpenID provider such as AOL, Blogger and so on.

OpenID.Anonymity.com is an OpenID provider just like them, but we do it differently. No one has got a fixed profile here, and you don't have to sign up or register any accounts whatsoever. Rather, any OpenID profile given such as <http://openid.anonymity.com/anythingHere> will automatically be validated for you as an authentic log-in by Anonymity.com. If the site that you log in to ask for a name, we simply give it a randomized name such as "AnonEceSAqo." In short, OpenID.Anonymity.com is to OpenIDs what Mailinator is to e-mails.

How do I use it?

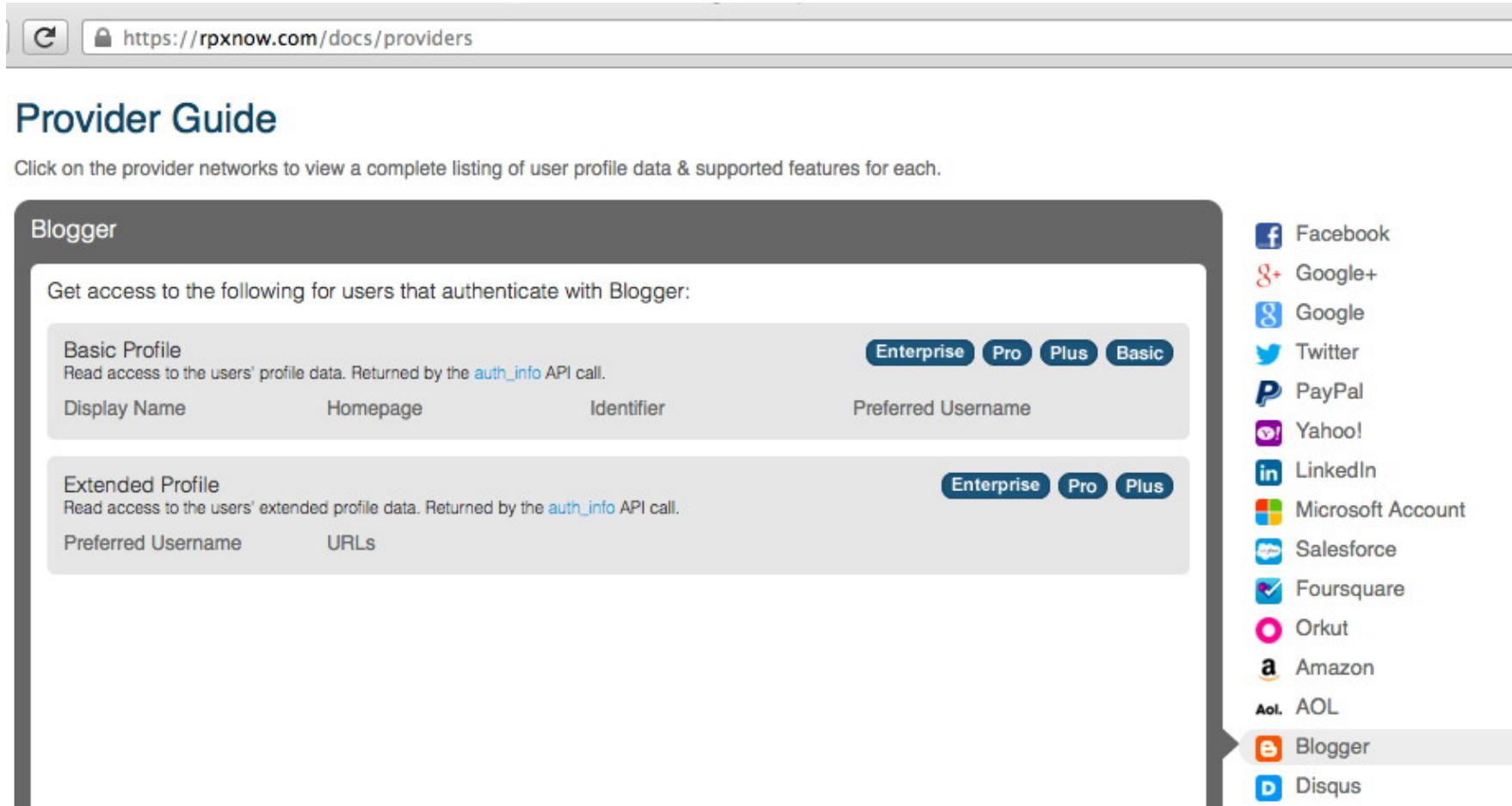
When you would like to log in to a site that you would rather not give your online identity to, look for the OpenID icon or an option to log in using OpenID. If the site accepts OpenID, it should ask you for the URL to your OpenID-enabled profile (provider). Now, rather than giving up your AOL or LiveJournal URL, simply type in <http://openid.anonymity.com/whateverhere>, substituting the *whateverhere* part with any letters and numbers of your choosing. Submit, enter in the characters on the captcha image, submit again, and that's it! The site should now recognize you as a logged in account under a fictitious name indicating your anonymity.

Your disposable OpenID

<http://openid.anonymity.com/CiraHoG>



So What DOES Gets Shared When OpenID Is Used? Answer: It Varies By Provider. Blogger?

A screenshot of a web browser window displaying the "Provider Guide" for the Blogger provider on the rpxnow.com website. The URL in the address bar is https://rpxnow.com/docs/providers. The page title is "Provider Guide". A sub-section for "Blogger" is shown, with a note: "Get access to the following for users that authenticate with Blogger:". Below this, two sections are listed: "Basic Profile" and "Extended Profile". Each section has a "Read access to the users' profile data. Returned by the auth_info API call." note. Under "Basic Profile", there are four columns: "Display Name", "Homepage", "Identifier", and "Preferred Username". To the right of these columns are four buttons: "Enterprise", "Pro", "Plus", and "Basic". Under "Extended Profile", there are two columns: "Preferred Username" and "URLs". To the right of these columns are three buttons: "Enterprise", "Pro", and "Plus". To the right of the main content area is a vertical list of other provider icons and names, each with a small arrow pointing towards the "Blogger" button.

-  Facebook
-  Google+
-  Google
-  Twitter
-  PayPal
-  Yahoo!
-  LinkedIn
-  Microsoft Account
-  Salesforce
-  Foursquare
-  Orkut
-  Amazon
-  AOL
-  Blogger
-  Disqus

"Display Name, Homepage, Identifier, Preferred Username, URLs" 57

Facebook? LOTS More Gets Shared

https://rpxnow.com/docs/providers

Facebook

Get access to the following for users that authenticate with Facebook:

Basic Profile		Enterprise Pro Plus Basic	
Read access to the users' profile data. Returned by the auth_info API call.			
Display Name Name	Gender Preferred Username	Homepage UTC Offset	Identifier

Extended Profile		Enterprise Pro Plus	
Read access to the users' extended profile data. Returned by the auth_info API call.			
About Me Books Games Interests Photos Religion URLs Name	Activities Current Location Groups Movies Political Views Sports Videos Profile URL	Addresses Emails Heroes Music Quotes Status Id	Albums Friends List Interested In Meeting Organizations Relationship Status TV Shows Last Updated

Contacts		Enterprise Pro	
Read access to the users' friends. Returned by the get_contacts API call.			
About Me Albums Display Name Gender Homepage Movies Preferred Username Sports Videos	Activities Birthday Family Name Given Name Interested In Meeting Music Profile Photo Time Zone Id	Address Books Formatted Name Groups Interests Music Quotes TV Shows Name	Addresses Current Location Games Heroes Last Updated Photos Relationship Status URLs Profile URL

Social Sharing		Enterprise Pro Plus Basic	
Write access to the users' activity stream. Works with the activity and set_status API calls (Pro only).			
Activity/Status Message Media	URL	Title	Description

Facebook  **Google+**  **Google**  **Twitter**  **PayPal**  **Yahoo!**  **LinkedIn**  **Microsoft Account**  **Salesforce**  **Foursquare**  **Orkut**  **Amazon**  **AOL**  **Blogger**  **Disqus**  **Flickr**  **Hyves**  **Instagram**  **Livejournal**  **Mixi**  **MyOpenID**  **Myspace**  **Netlog**  **Renren**  **Sina Weibo**  **SoundCloud**  **Tumblr**  **Verisign** 

58

Is Disclosing More Information About Users A Good Thing, or A Bad Thing?

- If a legitimate service is relying on an OpenID for authentication, having more information about a user helps them to potentially identify and manage problematic users.
- On the other hand, if I'm a bad site attempting to leverage OpenID to mine information about users, the more information that gets shared with them, the bigger the potential risk to user privacy.
- Presumably privacy-aware users would prefer to use whatever OpenID identity provider releases the LEAST information about me (while still being acceptable to the services I use), but most users just don't seem to know/care.
- One more point: virtually all of these user attributes are "self-asserted"/"user-supplied" – should you even bother paying attention to them anyway? What if users simply choose to lie?

Other Issues: Does OpenID Have "Critical Mass?" Perhaps Not, At Least For Drupal

#85

Posted by [c960657](#) on May 29, 2013 at 3:54pm

I agree with the previous comments.

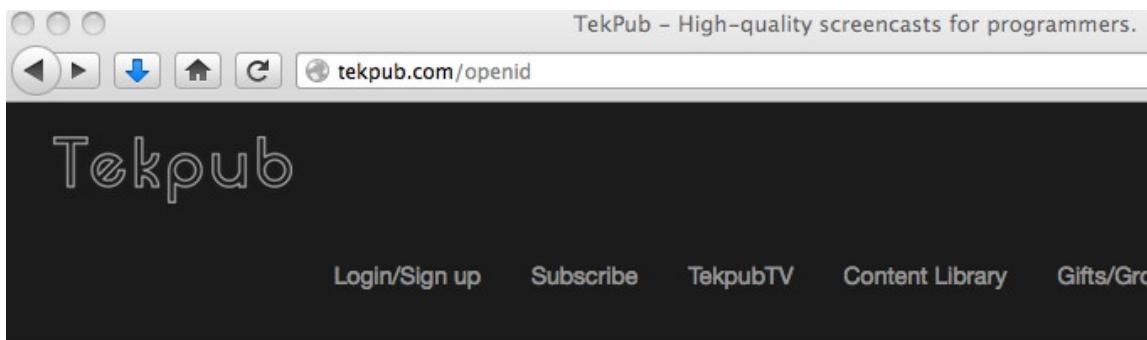
I have much sympathy for OpenID, and I really hoped that it would take off. But so far it has not become the one solution to rule them all, and the future of this field is very uncertain, so even if the module was well-maintained, I think it has lost its relevance as a core module. In my opinion, no standard currently has so wide-spread support that we should support it in core.

If you take a look into the code in the OpenID module, it's pretty clear that Drupal makes it very difficult to create an authentication module that integrates nicely with the existing login forms, the account creation flow etc. I think the core efforts should be spent on making it easy for contrib modules to work as authentication providers (and allow disabling the built-in authentication mechanism). Support for different login frameworks can be developed in contrib based open standards (OpenID), proprietary systems (Facebook) or enterprise single sign-on systems (Drupal.org bakery). Site-owners should be able to install one or more authentication modules that matches the target audience of the web site.

"Remove OpenID from core,"
<https://drupal.org/node/556380>

Still Others Have Tried Supporting OpenID, And Have Ended Up Transitioning Away From It For Process-Related Reasons

- Consider the following commentary from Tekpub...



What Happened To OpenID?

Long story short, We've completely removed OpenID/OpenAuth/3rd Party Auth from Tekpub. Hopefully this didn't surprise you. If it did, read on...

Why We Did It

Many developers love the idea of OpenID and Single Signon. So did we, until we used it full time with Tekpub. In the beginning it's all we had! **We didn't want to store anything about you that we didn't need to.**

As neat of an idea as that sounds, it quickly became a complete nightmare that resulted in:

- People losing their orders when they changed their OpenID
- Providers changing people's OpenID URLs for them
- Providers going out of business, stranding our users
- Our authenticator, JanRain, going offline - locking our users out

I [Wrote about it here](#) if you would like to read more.

I'd Love To Hear What You All Think About OpenID Based on Your Own Experiences...

- Are you using OpenID to login? Are you accepting it for authentication on your web site? Do you like it? Is OpenID the federated web authentication solution you like and need?
- Beyond OpenID, there are other federated web authentication solutions. One of these is Shibboleth, a SAML-based federated identity solution.

7. Federated Authentication: Shibboleth

Shibboleth

- "Shibboleth is among the world's most widely deployed federated identity solutions, connecting users to applications both within and between organizations. Every software component of the Shibboleth system is free and open source."
- "Shibboleth is an open-source project that provides Single Sign-On capabilities and allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner."
- <http://shibboleth.net/>

Shibboleth Relies on SAML ("SAM-uhl")

- SAML stands for "Security Assertion Markup Language."
- SAML is too complex to describe in detail here, but
<http://saml.xml.org/wiki/saml-introduction> links both to an "executive overview" (seven pages long!),
<https://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf>
as well as to a 51 page "technical overview," see
<https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf>

How Shibboleth Works (In A Nutshell)

Step 1: User Accesses A Resource

Step 2: Service Provider Issues Authentication Request

Step 3: User Authenticated at Identity Provider

Step 4: Identity Provider Issues Authentication Response

Step 5: Service Provider Checks Response

Step 6: Resource Returns Content

<http://shibboleth.net/about/basic.html> goes over these steps in more detail...

A Higher Ed Use Case

- Imagine a situation where an institution (like UO) contracts for access to a proprietary web database, licensed for use by all faculty.
- The database provider needs some way for UO faculty, and only UO faculty, to "login" to access that database, but the provider and the university don't want to use a single shared common password that everyone will know (shared passwords quickly leak to unauthorized users), nor does the university or the provider want to set up per-user, per-database credentials.
- Federated authentication, if supported by both the institution and the database provider, is perfect for this sort of application. The service provider trusts the identity provider to authenticate university users, and the provider then applies normal business rules to determine what access is legitimately authorized.
- Authentication gets decoupled from authorization

Authentication vs Authorization

- Authentication (often referred in "shorthand" within the community as "AuthN") is the question, "Have we identified who this is?"
- Authorization (in shorthand, "AuthZ") is a separate question, e.g., "Are they allowed access to this resource?"
- Staying with a university context, imagine a student who is delinquent in paying her tuition and fees. We may still have total confidence that we know who that student is when she authenticates with her university-supplied credentials, but that non-paying student may not be authorized access to any classes or campus resources until she settles her pending bill.

Two Federation Roles: IdPs vs SPs

- **IdPs, or Identity Providers**, supply user information. For example, a university might be an identity provider for its faculty, staff and students. IdPs create and manage user identities/accounts.
- **SPs, or Service Providers**, consume user information. (SPs are also sometimes known as "relying parties.") A common example of a service provider is our online subscription database example: it wants to allow access from organizational subscribers, but deny access from non-subscribers.
- An IdP can also be an SP, providing and consuming identity data. For example, maybe a university has a federated wiki, as well as offering federated identity data for faculty, students and staff members.

A Sample Federation With IdPs and SPs

- InCommon is the US higher education community's identity federation. InCommon currently has 295 IdPs and 1,128 SPs, as listed at <https://incommon.org/federation/info/all-entities.html> and it services just under 6 million users (admittedly tiny compared to typical national or international-scale commercial ISPs, but non-trivial in size compared to some local/regional federations).
- There's an InCommon page that has a listing of all InCommon participants, by type... The first two categories are pretty self-explanatory (high ed institutions, and non-profits/government labs/etc.); the third category, sponsored participants, represents commercial entities that have been sponsored by an existing community member because the community would like to be able to access services offered by that commercial entity with federated authentication. See the next page...

Current InCommon Participants

Below is a complete list of InCommon Participants. There are also lists available for:

- **Identity and Service Providers** deployed in the federation (and other metadata-driven pages)
- **Certificate Service** subscribers

The IdP and SP pages include links to more-detailed information on each entity—just go to the IdP or SP list and click on the name of the IdP or SP you are interested in. **InCommon serves almost 6 million end-users through federated identity management.**

Higher Education Participants (359)	Government and Nonprofit Laboratories, Research Centers, and Agencies (29)	Sponsored Partners (144)
A. T. Still University Allegheny College American University Amherst College Arizona State University Arkansas State University Auburn University Augsburg College Azusa Pacific University Ball State University Barry University Bay De Noc Community College Baylor College of Medicine Baylor University Beaufort County Community College Bloomburg University of Pennsylvania Boise State University Boston College Boston University Brandeis University Bridgewater College Brigham Young University Brown University Bucknell University California Community Colleges Chancellors Office	Ames Laboratory Argonne National Laboratory Brookhaven National Laboratory ESnet Fermilab GENI Project Office Idaho National Laboratory Internet2 Jefferson Lab Lawrence Berkeley National Laboratory LIGO Scientific Collaboration LTERN (Long Term Ecological Research Network) Marine Biological Laboratory Moss Landing Marine Laboratories National Institutes of Health National Science Foundation NERSC (National Energy Scientific Computing Center) Oak Ridge National Laboratory Open Cloud Consortium (OCC) Open Science Grid Pacific Northwest National Laboratory Sandia National Labs	Academic Works, Inc. Acatar Accessible Information Management, LLC Advantage Connect Pro Inc. ALEKS Corporation Alexander Street Press American Psychological Association Apple - iTunes U AppointLink Portal Solutions, Inc. ARTstor Association for Computing Machinery AT&T Services AthenaOnline.com Atlas Systems, Inc. Atomic Learning Benelogic BioOne, Inc. BioRAFT Blackboard, Inc. Blatant Media Corporation Cambridge University Press CampusEAI Cayuse, Inc. Cengage Learning, Inc. CenturyLink <small>Cincinnati Children's Hospital Medical Center</small>

Higher Ed Identity Federations Worldwide

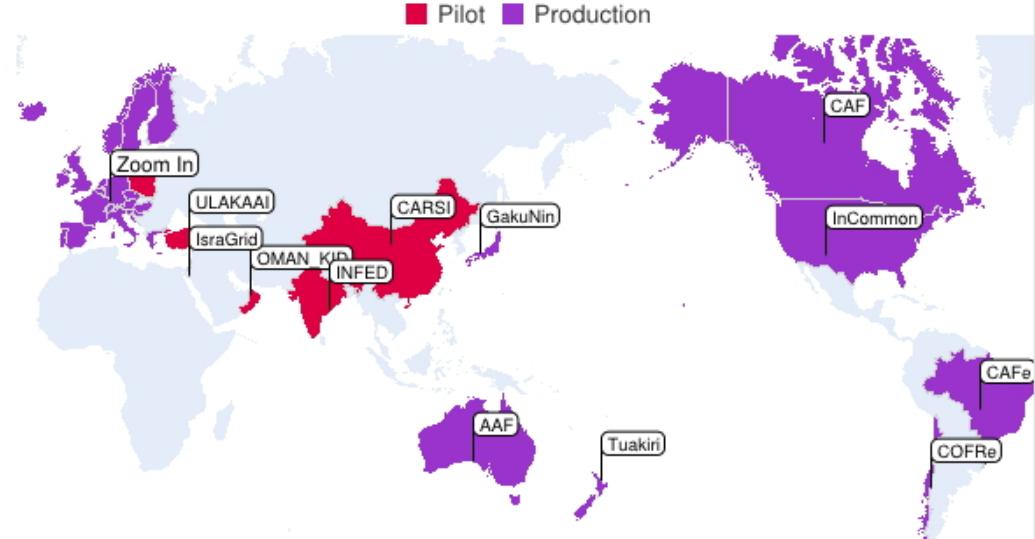
- REFEDS is a TERENA activity (<http://www.terena.org/about/>) that is meant to be "the voice that articulates the mutual needs of research and education identity federations worldwide."
- You can see from the following REFEDS map how many countries currently have R&E identity federations, either in production or in pilot.

 **REFEDS**

The map below shows the **identity federations** around the world that work with REFEDS. Note that the federations shown on the map may not offer full national coverage even if the whole country is coloured. Most of these federations focus on higher education and research communities.

For information on which federation participates in the existing inter-federations initiatives, please visit [eduGAIN web site](#) and [Kalmar2 website](#).

■ Pilot ■ Production



Research and Education Federations Map
[Download High-quality Printable Map](#)

<https://refeds.org/resources.html>

There Are Non-Higher Ed SAML Federations, Too

The screenshot shows a web browser window with the following details:

- Title Bar:** Federated Identity and Privilege Management
- Address Bar:** https://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1179
- Header:** Justice Information Sharing, U.S. Department of Justice, Office of Justice Programs
- Navigation Bar:** Home, Global Justice, Global Information Sharing Toolkit (highlighted), National Initiatives, Privacy & Civil Liberties, Policy & Practice, Implementation Assistance
- Left Sidebar (National Initiatives):**
 - Fusion Centers and Intelligence Sharing
 - Global Reference Architecture
 - National Information Exchange Model
 - Global Justice XML (Archive)
 - Federated Identity and Privilege Management** (highlighted)
- Main Content Area:** Global Federated Identity and Privilege Management
- Section:** Introduction
- Text:** Achieving information sharing objectives requires that partners establish wide-scale electronic trust among the caretakers of critical information and those who need and are authorized to use that information. The information is sensitive-inappropriate sharing is just as dangerous as lack of sharing. That is where a new and rapidly maturing technology called federated identity comes in. Federated identity allows a user's roles, rights, and privileges to be communicated securely in the justice community and, in particular, to those who hold the information required to effectively safeguard our nation.
- Section:** Site Tools
- Links:** Events Calendar, FAQ, Document Library, News Archive, Site Map, RSS Feeds & Podcasts, Contact Us, BJA Twitter
- Right Sidebar:** The Global Federated Identity and Privilege Management (GFIPM) framework provides the justice community and partner organizations with a standards-based approach for implementing federated identity. The concept of globally understood metadata across federation systems is essential to GFIPM interoperability. Just as a common Extensible Markup Language (XML) data model was the key to data interoperability, a standard set of XML elements and attributes about a federation user's identities, privileges, and authentication can be universally communicated. The GFIPM metadata and framework support the following three major interoperability areas of security in the federation:
- Identification/Authentication - *Who is the end user and how were they authenticated?*
 - Privilege Management - *What certifications, clearances, job functions, local privileges, and organizational affiliations are associated with the end user that can serve as the basis for authorization decisions?*
 - Audit - *What information is needed or required for the purposes of auditing systems, systems access and use, and legal compliance of data practices?*

How Shibboleth Practically Works: IdP Discovery Pages ("WAYF?")

- When a user runs into a service provider that offers Shibboleth federated login, the user needs to use an "IdP discovery page" (often referred to as a "Where are you from?" page) to get the user of the service to the IdP they'd like to use.
- FWIW, I have some worries about the scalability of this sort of thing – long lists of sites to choose from can quickly get unwieldy, but we're still at a do-able number of sites at this point...
- For example...

Sample WAYF Page

The screenshot shows a web browser window with the URL <https://spaces.internet2.edu/shibboleth-ds/WAYF?entityID=https%3A%2F%2Fspaces.internet2.edu>. The page title is "Select an identity provider". A message states: "The Service you are trying to reach requires that you authenticate with your home organization, enter the name below." Below this is a search form with a text input field and a "Search" button. The section "Enter institution name:" is followed by a "Search" input field and a "Search" button. The section "Or choose from a list:" contains two columns: "Federation" and "organization". The "Federation" column includes links for "US Higher Education", "UK Federation", "SWAMID Test Federation", "Austria - ACOnet", "France - CRU", "Servicio de Identidad de RedIRIS (SIR)", "Switzerland - SWITCHaai", "Social Providers (Beta)", and "All Sites". The "organization" column lists various institutions: Aberdeen College, Aberdeen College Staff, Aberystwyth University, Abingdon and Witney College, Academy of Fine Arts Vienna, Accrington & Rossendale College, ACOnet, ACS Schools, Adam Smith College, and AESIR. At the bottom are "Select" and "Remember for session" buttons. A footer message says: "Need assistance? Send mail to [administrator's name](#) with description." A logo placeholder is at the bottom right.

Select an identity provider

The Service you are trying to reach requires that you authenticate with your home organization, enter the name below.

Enter institution name:

Search

Or choose from a list:

Federation	organization
US Higher Education	Aberdeen College
UK Federation	Aberdeen College Staff
SWAMID Test Federation	Aberystwyth University
Austria - ACOnet	Abingdon and Witney College
France - CRU	Academy of Fine Arts Vienna
Servicio de Identidad de RedIRIS (SIR)	Accrington & Rossendale College
Switzerland - SWITCHaai	ACOnet
Social Providers (Beta)	ACS Schools
All Sites	Adam Smith College
	AESIR

Select Remember for session

Need assistance? Send mail to [administrator's name](#) with description.

logo

Another Sample WAYF Page

Log In From Your Institution | EDUCAUSE.edu – (Private Browsing)

<https://www.educause.edu/user/wayf?entityID=https%3A%2F%2Fwww.educause.edu%2Fshibboleth-sp&return=https%3A%2F%2Fwww.educause.edu%2Fsh>

Home > Federated Login > User account > Log In From Your Institution ★ Favorite

LOGIN TO 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

Start typing here to find your institution

ARE YOU FROM
University of Vermont, Vermont State Colleges

<p>Amherst College Amherst, Massachusetts</p>  <p>AMHERST COLLEGE</p>	<p>Arizona State University Tempe, Arizona</p> 
<p>Auburn University Auburn University, Alabama</p> 	<p>Baylor College of Medicine Houston, Texas</p>
<p>Baylor University Waco, Texas</p>	<p>Bloomsburg University of Pennsylvania Bloomsburg, Pennsylvania</p> 

A Federal WAYF Page

MAX.gov Login

Office of Management and Bu... (US) | https://login.max.gov/cas/login?service=https%3A%2F%2Fmax.omb.gov%2Fcommunity%2Flogin.action%3F

 MAX.GOV LOGIN [Don't Have a MAX ID Yet?](#) [Register Now](#)

Home Manage Password Contact Us

LOGIN WITH YOUR....

User ID & Password [?](#)

User ID
Your registered email address

Password

[Forgot or change your password?](#)

PIV or CAC Card [?](#)

Please make sure your card is plugged into the reader



LOGIN WITH YOUR
PIV OR CAC

Agency Federated Partner Login [?](#)

 NASA  DOJ  HHS  MCC  USAID

Use this Agency Login every time I log into MAX

WARNING: This system contains U.S. Government Data. Unauthorized use of this system is prohibited.

Institutional Login Pages

- Once the user selects their home institution, they are then redirected to/shown their home institution's federated login page
- Each school's federated login page will normally be localized according to traditional institutional look-and-feel, using institutional logos and colors, etc., and secured with https (SSL/TLS), and will be located at/show the institutional URL in the user's browser bar
- Once the user authenticates, a cookie will be set and then the user will be taken...
 - back to the page they were originally trying to visit (if login was successful) or
 - to an error page (if login failed or the required attributes weren't configured to be released for this site)

Sample Institutional Login Page

The screenshot shows a web browser window with the following details:

- Title Bar:** UO Web Sign On Service
- Address Bar:** https://shibboleth.uoregon.edu/idp/Authn/UserPassword
- Toolbar:** Includes icons for back, forward, search, and other browser functions.
- Header Bar:** UNIVERSITY OF OREGON (with a large white 'O' icon) and links for UO Home and Dept Index.
- Main Content Area:**
 - Section Title:** UO Web Sign On Service
 - Text:** Log in using your [Duck ID](#) to access the application that redirected you here. After login, you will be returned to the application. In addition you will be enabled for Single Sign-On with other applications that use the University of Oregon's Shibboleth web sign on system.
 - Form Fields:** Username (text input field containing a yellow placeholder) and Password (text input field containing a yellow placeholder).
 - Buttons:** Login (button) and clear (button).

For security reasons, please Log Out and Exit your web browser when you are done accessing services that require authentication.

Another Sample Institutional Login Page

The screenshot shows a web browser window with the following details:

- Title Bar:** LBNL Central Login Facility – (Private Browsing)
- Address Bar:** https://login.lbl.gov/idp/Authn/UserPassword
- Header:**
 - BERKELEY LAB** logo with the text "BERKELEY LAB" below it.
 - LAWRENCE BERKELEY NATIONAL LABORATORY** text.
 - U.S. DEPARTMENT OF ENERGY** logo with the text "U.S. DEPARTMENT OF ENERGY" below it.
 - A-Z INDEX | PHONE BOOK | JOBS | SEARCH** links.
- Sub-header:** CENTRAL LOGIN FACILITY
- Form:**
 - USERNAME:**
 - PASSWORD:**
 - Login** button

Please login below with your LBNL LDAP username and password:

Are you wondering how you ended up here?

A service offered by EDUCAUSE, but without more descriptive details, has requested that we authenticate you. Because your username and password will not be transmitted to this service, you should feel relatively safe logging in here.

If you have concerns about the legitimacy of this site, please contact the Help Desk at x4357 or help@lbl.gov.

Attributes

- Each federated user has a set of common attributes associated with them. In higher ed's case, these are defined via **eduPerson**, an LDAP schema developed and maintained by MACE, an Internet2 working group that focuses on directories and identity issues.
- Attributes have officially assigned OIDs (Object IDs), see for example <http://middleware.internet2.edu/oid-mace/> and <http://middleware.internet2.edu/dir/edu-schema-oid-registry.html>
- A summary list of eduPerson attributes can be seen at <http://www.incommon.org/federation/attributesummary.html>
- Attributes include **eduPersonScopedAffiliation** (student, faculty, staff, alumni, etc.), **sn** (surname), **givenName** (first name), **mail** (email address), **eduPersonPrincipalName** (aka EPPN), **eduPersonTargetedID**, and multiple **eduPersonEntitlement's** (a list of URIs representing licenses, permissions, rights, etc.)

Email Addresses vs. ePPNs vs. ePTIDs

- While many may assume that most users are identified by their email address, in federated authentication, at least in InCommon, the unique identifier is actually normally the ePPN (eduPersonPrincipalName), see
<http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-201203.html#eduPersonPrincipalName>
- While ePPNs look like an email address (having a user@domain form), and will be consistently shown to each SP, they should not be assumed to be a published/deliverable addresses. They may also change from time to time (example: name changes due to marriage)
- The eduPersonTargetedID (ePTID) is an even more privacy-preserving "opaque identifier," consisting of a stable blob of characters, although the ePTID will usually be different for different SPs, preventing potential cross-SP identification and tracking.

Why Not Just Use Email Addresses?

- Email addresses don't preserve the user's privacy: many email addresses are effectively a version of the user's real life name, and may connect the user to his/her behavior more than it should.
- At the same time, there's nothing that prevents a person from picking a completely misleading email address – Jane Smith could choose the email address `bobdoe@example.com` if she wanted to.
- Email addresses aren't perpetual. An email address that exists today might be gone tomorrow. Even worse, email addresses also aren't guaranteed against reassignment, either: `johns@example.com` may be John Smith today, but John Samuelson tomorrow
- Some may have N email addresses (... and thus N identities?)
- Some might not use email (perhaps preferring some sort of instant messaging), but the use of email addresses as a default identifier conflates their role as an identifier with a protocol, e.g., email, "forcing" people to sign up for a service they might never use... 85

Attributes and "Need to Know"

- You may notice that this sort of scheme puts a substantial emphasis on only releasing the attributes that the service provider "needs to know" -- not all SPs will have access to all potentially available user attributes (including email addresses!) by default.
- IdPs, in negotiation with each SP, determine which attributes they're willing to release to those SPs.
- Sometimes that may mean an SP know a lot about an authenticated user, while other times you may know very little. It can also mean that some IdPs may not be able to authenticate to some services.
- This privacy-preserving property is an important aspect of Shib-based federated authentication, both in higher education, and in more serious government contexts.
- A government federated authentication example may help illustrate this...

Law Enforcement/Intelligence "Need to Know"

- Assume that you're a law enforcement agency working to combat illegal drugs Your team includes drug cops from state and local police departments, federal LEOs, international partners, and even members of the intelligence community.
- Intelligence sharing entities don't want to have to create usernames and passwords for each user, and users don't want per-site creds.
- More importantly, from an opsec POV, you don't want "everything" about each officer to be exposed by default to all service providers – at least some of those officers may be working undercover.
- Attributes may also be important: some officers may hold Top Secret or Secret security clearances, while others may not.
- Federated authentication is a perfect fit for this case: it allows each officer to be authenticated by their home agency, with only required attributes getting released to the intelligence sharing site.

Federal Law Enforcement Doesn't Use eduPerson

- Law enforcement agencies needed a schema with attributes that aren't in eduPerson.
- The most widely known law enforcement federated ID schema is GFIPM, from the Department of Justice.

The screenshot shows a web browser window with the URL "gfipm.net/standards/metadata/2.0/" in the address bar. The page has a blue header with the "DEPARTMENT OF JUSTICE" seal on the left. The main title "GFIPM Metadata 2.0" is in large white font, followed by the subtitle "Global Federated Identity and Priviledge Managment (GFIPM)". Below the header is a black navigation bar with links: Home, User Attributes, Entity Attributes, Resource Attributes, Action Attributes, Environment Attributes, and Code Sets.

GFIPM Metadata 2.0 Contents

The GFIPM Metadata 2.0 specification includes metadata attributes about users, system entities, information resources, information-sharing actions, and environmental conditions within an information-sharing federation. Its core content (comprising attributes and code sets) is available online here. In addition, artifacts from the spec (including a compressed archive of the entire spec) are available below for download.

NOTE: To better serve the needs of multiple independent GFIPM federations, and also to more adequately meet the needs of GFIPM federations that include one or more trusted identity brokers (TIBs), several changes have been made to the GFIPM Metadata 2.0 Spec as of January 2011. Please see the addendum document for a full description of these changes.

Metadata Attributes and Code Sets

- [User Attributes](#)
- [Entity Attributes](#)
- [Resource Attributes](#)
- [Action Attributes](#)
- [Environment Attributes](#)
- [Code Sets](#)

Artifacts Available for Download

- [GFIPM Metadata 2.0 Overview and Usage Document \(PDF\)](#)
- [GFIPM Metadata 2.0 Spec \(MS Excel\)](#)

GFIPM Is Long and Very Inclusive

- If you look at the user attributes defined in <http://gfipm.net/standards/metadata/2.0/> you'll see that it defines a large number of user attributes. Some are familiar (such as "Full Name" or "Telephone Number")
- Others are more unique to the law enforcement and intelligence community ("Fingerprint Set Image", "Security Clearance Level Code," "Sworn Law Enforcement Officer Indicator," "Counter Terrorism Data Agency Search Home Privileged Indicator," and many more...)
- You can look at each of these attributes, and what they mean, if you're curious...

gfpmp.net/standards/metadata/2.0/user.html

Primary Language Name	Text
<u>Photo Image</u>	Base-64 Binary
<u>Digitized Signature Image</u>	Base-64 Binary
<u>Fingerprint Set Image</u>	Base-64 Binary
<u>Emergency Contact Full Name</u>	Text
<u>Emergency Contact Telephone Number</u>	Text
<u>Emergency Contact Email Address Text</u>	Text
<u>Security Clearance Level Code</u>	Clearance Code
<u>Security Clearance Effective Date</u>	Date
<u>Security Clearance Expiration Date</u>	Date
<u>Security Clearance Sanction Text</u>	Text
<u>Security Clearance Granting Agency Name</u>	Text
<u>Sworn Law Enforcement Officer Indicator</u>	Boolean
<u>Public Safety Officer Indicator</u>	Boolean
<u>NCIC Certification Indicator</u>	Boolean
<u>28 CFR Certification Indicator</u>	Boolean
<u>NCIC Criminal History Privilege Indicator</u>	Boolean
<u>NCIC Hotfile Privilege Indicator</u>	Boolean
<u>FBI IAFIS Privilege Indicator</u>	Boolean
<u>FBI III Privilege Indicator</u>	Boolean
<u>NICS File Privilege Indicator</u>	Boolean
<u>NDEx Privilege Indicator</u>	Boolean
<u>LEO Privilege Indicator</u>	Boolean
<u>NIPP Sector Code</u>	NIPP Sector Code
<u>Emergency Support Function Code</u>	Emergency Support Function Code
<u>Military Status Code</u>	Military Status Code

28 CFR Certification Indicator

Full Formal Attribute Name

gfipm:2.0:user:28CFRCertificationIndicator

Abbreviated Formal Attribute Name

28CFRCertificationIndicator

Definition

True if the user has been trained and certified in the handling of criminal intelligence data in accordance with Code of Federal Regulations Title 28 (28 CFR) Part 23, false otherwise.

Data Type

Boolean

Metadata Version

2.0

Usage Information

Assertion of this privilege requires the user to have been trained and certified in the handling of criminal intelligence data in accordance with Code of Federal Regulations Title 28 (28 CFR) Part 23. One way for a user to meet this requirement is by having taken and passed the online 28 CFR Part 23 training course and certification exam offered by the U.S. Department of Justice Bureau of Justice Assistance (BJA) via its Secured National Criminal Intelligence Resource Center (NCIRC) Web Site (<http://www.ncirc.gov/securedwebsite.cfm>). Alternatively, a user may meet this requirement by having taken and passed an equivalent offline 28 CFR Part 23 training course, offered by the Institute for Intergovernmental Research (IIR). (See <http://www.iir.com/28cfr/Training.htm> for details.)

Legal values for this attribute are "true", "false", "1", and "0", where "1" indicates true and "0" indicates false.

GFIPM: A Top 10 DOJ BJA Global Achievement

|The Department of Justice's (DOJ) Top Ten Global Accomplishments

9. The [Global Federated Identity and Privilege Management](#) (GFIPM) framework provides the justice community and partner organizations with a standards-based approach for implementing federated identity (i.e., allowing a user's identities, privileges, and authentication to be universally communicated). GFIPM effectively breaks down the traditional barriers of stove-piped systems to better safeguard our nation.

<https://www.bja.gov/Publications/GlobalTop10.pdf>

Coming Back to InCommon: Metadata

- "InCommon metadata is the basis for trust within the InCommon Federation. In a very real sense, SAML metadata powers the federation. Without metadata, trusted operations within the Federation would grind to a halt. Put another way, SAML metadata represents the trust backbone of the InCommon Federation. Within the federation, trust is based on what effectively is a SAML-based PKI (as opposed to a more traditional X.509 Certificate-based PKI) built on top of trusted SAML metadata. Federation participants trust InCommon to vet the metadata content submitted by other participants. In turn, InCommon vouches for the integrity of the metadata it makes available to participants. This implicit trust agreement underlies and strengthens the security of the SAML protocol exchanges used throughout the Federation."

<http://www.incommon.org/federation/metadata.html>

What Does Metadata Look Like?

```
<!-- University of Oregon -->
<EntityDescriptor entityID="https://shibboleth.uoregon.edu/idp/shibboleth" xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <IDPSSODescriptor protocolSupportEnumeration="urn:mace:shibboleth:1.0 urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol">
    <Extensions>
      <shibmd:Scope regexp="false">uoregon.edu</shibmd:Scope>
      <mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
        <mdui:DisplayName xml:lang="en">University of Oregon</mdui:DisplayName>
        <mdui:Description xml:lang="en">University of Oregon's Shibboleth Identity Provider</mdui:Description>
        <mdui:Logo height="239" width="200" xml:lang="en">https://shibboleth.uoregon.edu/images/
Large_UO_Logo.jpg</mdui:Logo>
      </mdui:UIInfo>
    </Extensions>
    <KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
          <!-- Serial No. 468082133872964124381250680193044146864260986, expires on Mon Aug 21 17:07:58 2028 GMT --
          <ds:X509Certificate>
MIIDQjCCAiqgAwIBAgITFP1Rwp3clPykVwEUThiy/rAHejANBgkqhkiG9w0BAQUF
[etc]
```

Some Metadata Repositories

- <http://wayf.incommonfederation.org/InCommon/InCommon-metadata.xml> (6.5 MB)
- <http://metadata.ukfederation.org.uk/ukfederation-metadata.xml> (12MB)
- *Note:* while some federations may only sign and publish metadata a couple times a day, each participating site will commonly conditionally retrieve a copy of the relevant metadata file every hour, raising interesting scaling considerations if metadata were to be highly dynamic (e.g., if it were to change every hour), or the number of sites were to increase by orders of magnitude.
- *Also note:* if for any reason a site cannot retrieve metadata, they typically continue to use their current copy by default. This means that meta data doesn't represent a centralized single point of failure.

POP Statements

- The process of doing federated authentication involves more than just technology – it also involves policies. Policies will typically be created by a governance group such as a steering committee or board (in the case of federation policies), or by local administrative authorities (in the case of local POPs).
- To make this concrete...
 - The federation as a whole has a federation operating policy and practices ("FOPP") statement, for example, see <https://www.incommon.org/docs/policies/InCommonFOPP.pdf>
 - Each individual participant also publishes a POP (Participant Operational Practice) statement; you can see an outline for a typical POP at https://www.incommon.org/docs/policies/incommonpop_20080208.pdf

Finding Specific Policies in InCommon

InCommon Federation Info: Entities

https://incommon.org/federation/info/all-entities.html#IdPs_O

Ohio State University
Ohio Technology Consortium (OH-TECH)



Identity Provider: **Ohio State University** [more technical info](#)

Information URL: <https://webauth.service.ohio-state.edu/info.html>

Privacy Statement URL: <http://ocio.osu.edu/policy/policies>

Technical Contacts: "Authentication Support" <webauth-admin@lists.service.ohio-state.edu>

Administrative Contacts: "Authentication Support" <webauth-admin@lists.service.ohio-state.edu>

Support Contacts: "IT Service Desk" <8help@osu.edu>

Site Administrators: Visit the wiki for documentation regarding [MDUI elements](#) and [contacts](#) in IdP metadata.

This InCommon Identity Provider is owned by:
[Ohio State University](#)

Questions? Visit our [FAQ](#) or contact
<info at incommon dot org>


[ROCKINGHAM COUNTY SCHOOLS](#)
[Rutgers, The State University of New Jersey](#)

OSU's Specific Information URL

The screenshot shows a web browser window titled "OSU Web Login Service". The address bar displays the URL <https://webauth.service.ohio-state.edu/info.html>. The page content includes the Ohio State University logo, the title "OSU Web Login Service", and a paragraph describing the service's purpose. Navigation links like Help, Buckeye Link, Map, Find People, and Webmail are visible at the top.

OSU Web Login Service

The OSU Web Login Service enables web sites within and outside the university to provide secure and/or personalized services or data by leveraging [enterprise accounts issued to faculty, staff, students, and guests.](#)

Attributes and Privacy

Our default privacy policy permits us to release "public" information about most users that access services registered directly with our login service, or that are registered within the [InCommon Federation](#). This information includes a globally unique username, official e-mail address of record, and a legal name. Some accounts may not have all of that data associated with them.

An exception exists for those students (or former students) who have elected to suppress their personal information in our campus directory under the FERPA statute. No personally identifiable information will be released for such individuals to outside services except by special arrangement.

For technical staff, a complete list of data elements supported for use by authorized applications can be found [here](#). Applications should be aware that authentication alone does not constitute a guarantee or implication of any kind as to the account holder's relationship with the university. Accounts may be issued to anybody at any time for any reason.

Official information on university policies is [available](#).

Technical Support

Information on system outages or known problems may be found on the official [System Status](#) site.

Users who encounter problems logging into an application should always refer to local support contacts associated with an application. This may be, but often will not be, the [IT Service Desk](#). Contacting the Service Desk may result in a referral to an

Security Response to Incidents Involving Federated Authentication

- One side effect of doing federated authentication is that you, as a service provider, may not be able to directly identify a problematic user – you may only have a subset of the user's attributes, not including the user's real identity or even their username.
- Thus, working security incidents observed by a Service Provider will typically require the cooperation of the Identity Provider.
- Point of contact information is included in each IdP's metadata (e.g., look back at the Ohio State example just shown)

8. Some Additional Interesting Bits (Including Work In Progress)

Grouper (Remember those UIDs, GIDs?)

- Grouper helps collaboration to work in a federated environment by allowing groups to be managed in a centralized and scalable way, see <http://www.internet2.edu/grouper/>
- For a MAAWG-related example, consider MAAWG working groups. If those working groups were managed using a tool like Grouper, once someone was added to a particular working group, their status would also be made known to things like associated wiki pages (so they could be automatically allowed to edit them), and to associated mailing lists (so that they would be automatically subscribed to that working group's mailing list). Similarly, if a person wanted to stop being part of that working group, removing them from that group would reverse all those settings.
- Grouper enables delegation, too, so a subcommittee chair could be authorized by a committee chair to handle their own subcommittee groups

Scaling Attribute Release

- In the federated model, each IdP needs to permit the release of required attributes to each SP, which means that there would be $N(\text{IdP})$ times $N(\text{SP})$ attribute release policies that might need to be negotiated (if every IdP was used in conjunction with every SP).
- To simplify this, and to improve the scalability of attribute release, one approach that is currently being tried is the use of communities such as InCommon Research and Scholarship (R&S) community, <https://spaces.internet2.edu/display/InCFederation/Research+and+Scholarship+Category>
- In a nutshell, IdPs can decide that they will release a standard set of attributes (the ones that are normally needed by most service providers) to all service providers of a defined type.
- An SP then just needs to get approved as an R&S SP to automatically get access to standard attributes from all R&S IdPs.

What About Handling Potential Users Who Don't Have A "Home" IdP?

- Many times higher education people assume that everyone who wants to do federated authentication will "belong" to an institution that is Shibboleth enabled, but obviously that's not always going to be the case:
 - Some users may not be from a university.
 - Some users may be from a university, but one that doesn't offer a Shibboleth IdP service.
- What do we tell users in those sort of categories? How do we help them use Shibboleth?
- For a long time, we'd recommend that users get a free ProtectNetwork individual account, see
<https://app.protectnetwork.org/registration.html?execution=e1s1>

(Experimental) Social-to-SAML Gateways

- A more recent experimental approach to dealing with unaffiliated folks involves using Social-to-SAML gateways.
- Social-to-SAML gateways would allow you to trust a social identity, such as one from Facebook, Google, LinkedIn, PayPal, Twitter, VeriSign, Windows Live, Yahoo, etc., and then gateway that identity across to a traditional SAML-based environment.
- See <https://samlgwtest.theotislab.com/servDetails.html> and <https://spaces.internet2.edu/display/socialid/Social-to-SAML+Gateway+FAQ>
- **Should MAAWG be encouraging deployment of Social-to-SAML Gateways by social identity providers themselves?**

NIST 800-63 Levels of Assurance (LOAs)

- NIST 800-63-1, Electronic Authentication Guideline, see <http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf> defines four levels of assurance. Grossly oversimplifying:
- **LOA-1:** Self-asserted user identity, basically just assurance that this is the same user from session-to-session, simple password/PIN works okay, no identity proofing is required.
- **LOA-2:** Strong passwords required, proof of identity required (drivers license or passport), can be done remotely or in person
- **LOA-3:** Multifactor auth required, identity documents must be verified through record checks, can be done remotely or in person
- **LOA-4:** Cert-based multifactor on hard tokens or smart cards, extremely strong identity proofing (multiple documents, in person, verified via record checks, biometric data collected to prevent repudiation, in person only)

An Example of an LOA-4 Type Credential

- Some of you traveling today may be familiar the US "Trusted Traveler" program, which is associated with various efforts such as Global Entry, NEXUS, Sentri, TSA PreCheck, see:
<http://www.globalentry.gov/>
- If you sign up for that program, you can normally avoid long lines at Customs coming into the United States (or depending on the programs you sign up for, when travelling to Canada or Mexico), and if you're exhausted from traveling, this is just wonderful.
- On the other hand, the semi-painful part about the Trusted Traveler program is that you need to complete a long application and submit a lot of information about your identity, so it can be verified and so that Customs and Border Protection can tell you're not a criminal, and you need to appear in person for identity proofing and for biometric data collection. Why? These are LOA-4 class credentials, one of the few you may routinely run into in civilian circles.

Assurance Within InCommon

- For the most part, in the InCommon federation, sites trust their colleagues to satisfy their articulated policies and practices. That is, there is not any sort of formal assurance program involving audits or other formal compliance checks.
- InCommon is working on deploying an assurance program, beginning with "Bronze," a NIST 800-63 LOA-1-like self-asserted assurance standard, and "Silver," a NIST 800-63 LOA-2-like audited standard, see <http://www.incommon.org/assurance/>
- Currently one site, Virginia Tech, has been certified for both, but we know that many other schools are currently working to get certified for Bronze and/or Silver. There's a nice write up for VaTech meet the applicable assurance requirements at <https://spaces.internet2.edu/display/InCAssurance/Assurance+Implementation+Example+-+Virginia+Tech>

Thanks For the Chance To Talk Today!

Are There Any Questions?