InCommon FEDERATION

Recommended Practices and New Developments
in the InCommon Federation

Tom Scavo
Operations Manager
InCommon.org

@trscavo

Why are we here?

- To help create a **community of trust and sharing** in higher education
  - within higher education
  - between higher education and vendor partners
  - between higher education and government
- To make it **easier and safer for users** to use our computer systems

What we do

- Focal points:
  a. federated identity
  b. identity assurance
  c. multifactor authentication
- Service offerings:
  a. InCommon Federation
  b. Certificate Service (Comodo)
  c. Multifactor Service (Duo Security)

How we do it

- Standardized on SAML protocols and SAML metadata format but **these are not required** to run a federation
- We do not distribute or require particular software

InCommon != Shibboleth

@trscavo

Operating Principles

Basic operating principles:

1. ***T****rust*
2. ***I****nteroperability*
3. ***P****rivacy*

Join us! **TIP** the scales in favor of federation!

@trscavo

Trust

Trust-related activities:

- Metadata registration, administration, production, distribution, and consumption
- IdP deployment strength
  - enforce key size (at least 2048 bits)
  - promote proper key handling
  - XML signature on assertions using SHA-256
- Multifactor

Interoperability

Recommended practices lead to interop:

- SAML software
- saml2int deployment profile
- attribute support
- federated user experience

Goal: Near-100% coverage (or penetration)

Privacy

All InCommon participants agree to basic privacy principles (see: PA, section 9)

Other aspects of the privacy issue:

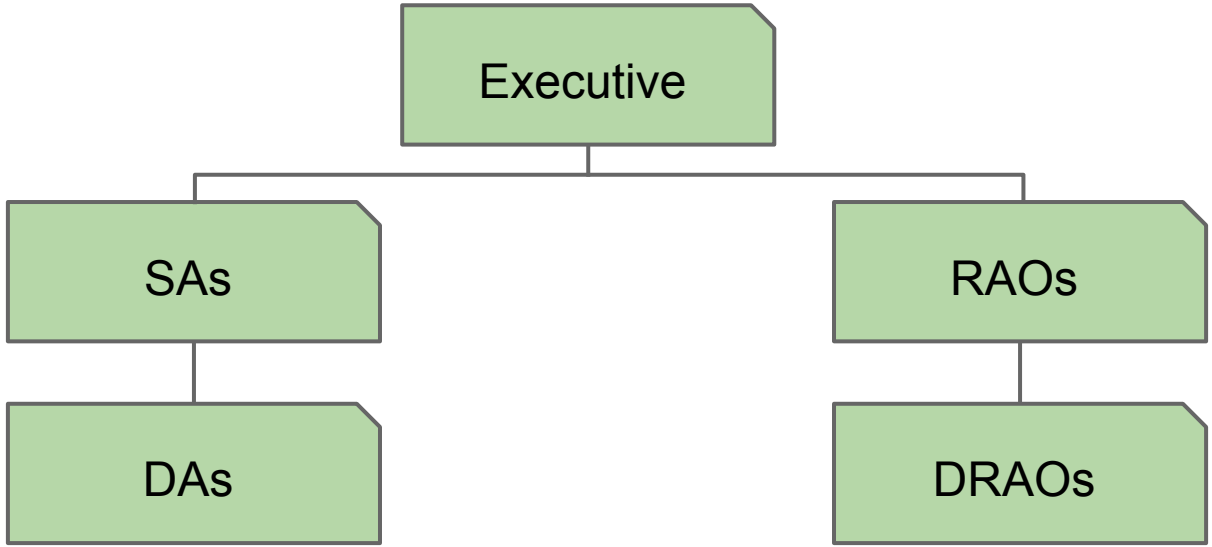
- we do not require IdPs to share particular attributes
- we do not store user attributes
- message-based encryption
- service categories

Internet2 Collaboration Wiki Spaces

https://spaces.internet2.edu
Space: InC-Federation

@trscavo

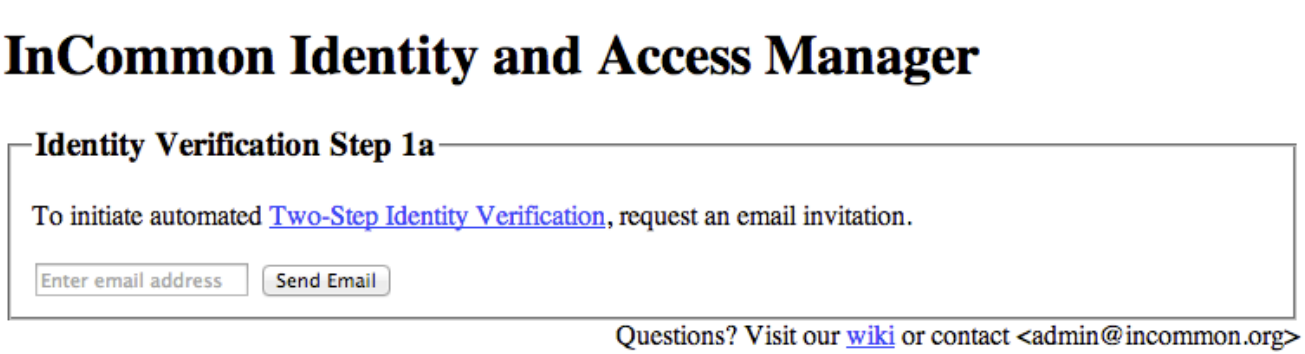
InC Ops IAM

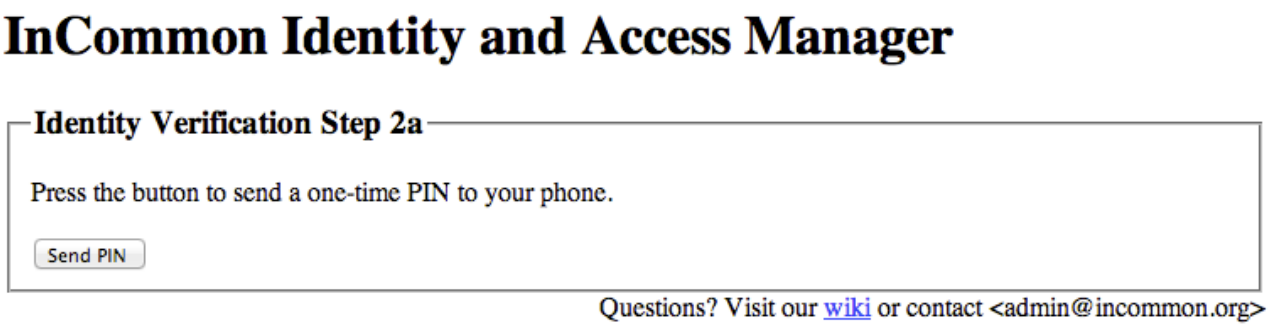


“A pharmacist doesn’t care who a doctor really is
when s/he can’t even read the handwriting ;-) “
@Steve_Lockstep

@trscavo

Identity Verification





@trscavo

InCommon FEDERATION

Delegated Administration

https://spaces.internet2.edu/x/7ZiKAQ

@trscavo

Delegated Administration?

- A Delegated Administrator (DA) is provisioned by a Site Administrator (SA)
- The SA delegates the administration of SP metadata to the DA
- The SA must approve any metadata update request made by the DA
- DAs log into the FM w/ a *federated password*

What? No IdP?

Sites that don’t deploy an IdP can use the new **Google Gateway**...

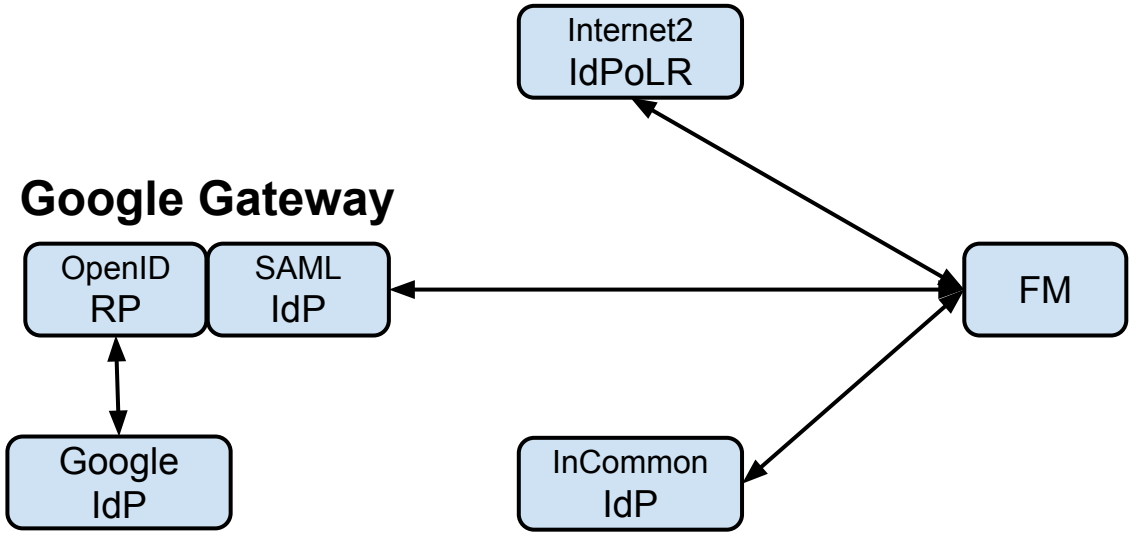
InCommon FEDERATION

Announcement

A *Delegated Administrator*
may now log into the *Federation Manager*
with a *Google* account

@trscavo

InCommon/Internet2 Google Gateway



In production since October 13, 2013

Powered by Cirrus Identity and Internet2

Federating the FM and the CM

@trscavo

Federating the FM

- All DAs log into the FM with a federated password **now**
- All RAs log into the FM with two factors **now**; all RAs will log in with a federated password by the end of Q1 2014
- All SAs will eventually log into the FM with a federated password and a mobile device

Federating the CM

- A staging instance of the CM that supports federated login is being tested **now**
- Eventually all MRAOs, RAOs, and DRAOs will log into the CM with a federated password; all MRAOs and RAOs will be required to log in with a mobile device as well

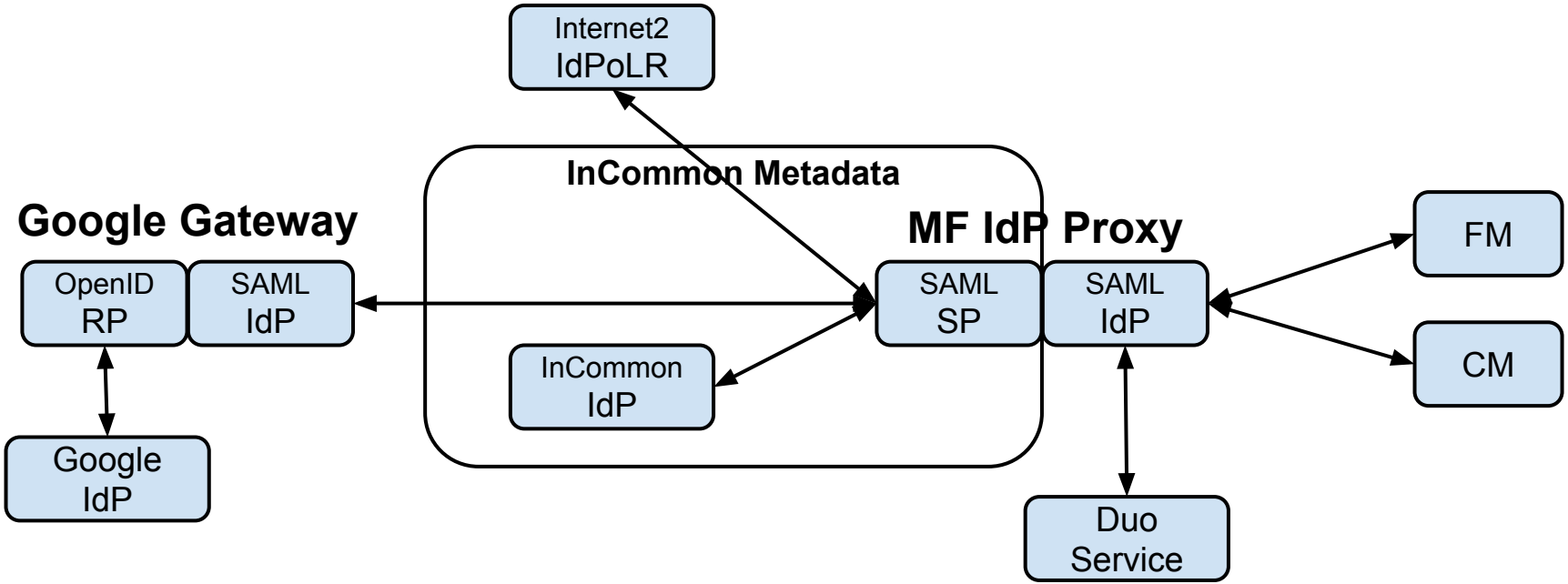
InCommon FEDERATION

Announcement

A *Multifactor IdP Proxy* will be running in production by the end of Q1 2014

@trscavo

InCommon Multifactor IdP Proxy



Powered by Cirrus Identity, Duo Security, Comodo, and Internet2

@trscavo

Multifactor IdP Proxy

- The Multifactor IdP Proxy is a SAML-to-SAML gateway that implements *distributed multifactor authentication*.
- The MF IdP Proxy is integrated with the Duo Security mobile-based authentication solution.
- Staging instance of MF IdP Proxy is being tested **now**.
- The MF IdP Proxy is built (by Cirrus Identity) using simpleSAMLphp and is deployed in the cloud (AWS).

InCommon FEDERATION

Service Categories

https://spaces.internet2.edu/x/fgVOAg

Research & Scholarship

- Primary goal: *Streamline attribute release*
- The Research & Scholarship Category
  - “Candidates for the Research and Scholarship (R&S) Category are Service Providers that support research and scholarship as an essential component”
- International standardization effort:
  - The REFEDs R&S Category specification

R&S SPs

- Service Providers apply for R&S
  - R&S SPs satisfy a modest set of requirements
  - An *attribute bundle* is associated with R&S
  - InCommon staff vet and approve R&S applications
- R&S SPs are tagged in metadata
  - An entity attribute is inserted into SP metadata

R&S IdPs

- Identity Providers declare support for R&S
  - IdPs agree to release a minimal subset of the R&S attribute bundle
  - IdPs specify attribute release policy using entity attributes (not entityIDs)
- R&S IdPs are tagged in metadata
  - Like SPs, an entity attribute is inserted into IdP metadata

Federated User Experience

- IdP Discovery (SP)
- Federated Login (IdP)
- User Consent (IdP)
- Error Handling (SP)

InCommon FEDERATION

Metadata Distribution WG

https://spaces.internet2.edu/x/zRBOAg

@trscavo

Metadata Refresh

- *Refresh and verify metadata at least daily*
- https://spaces.internet2.edu/x/JwQjAQ
- Metadata refresh has important security and interoperability implications
- Ensure your federation partners refresh their metadata

@trscavo

Big Changes Coming!

- New metadata server
- New metadata aggregates
- New metadata endpoints
- SHA-256-based XML signature
- https://spaces.internet2.edu/x/5IOZAg

New Metadata Aggregates

- On Dec 18, 2013, two new metadata aggregates will become available:
  - http://**md.incommon.org**/InCommon/InCommon-metadata.xml
  - http://**md.incommon.org**/InCommon/InCommon-metadata-fallback.xml
- The current aggregate will be phased out:
  - http://**wayf.incommonfederation.org**/InCommon/InCommon-metadata.xml

More Big Changes!

- Per-entity metadata
  - A signed metadata file for each IdP and SP
- Metadata for interfederation
  - Consume eduGAIN metadata
  - Consume UKf metadata