InCommon Federation ~~Best~~ ~~Golden~~ ~~Good~~ (Recommended) Community Practices

InCommon CAMP June 2011

Columbus, Ohio

~~RL "Bob" Morgan~~

Tom Barton, Scott Cantor

InCommon TAC

InCommon is Growing Up

- Now 500 SPs, 200 IdPs, 300 participant organizations
- Some participant sites are more than 6 years old
- Federation is evolving:
  - SAML 1 -> SAML 2
  - Shibboleth 1.x to 2.x; other SAML software choices
  - more sophisticated use of attributes
  - non-web solutions
  - higher-profile applications and services (e.g. NIH)

How Do We Move Forward Together?

- Contractual vs non-contractual arrangements
  - typically, when a federated relationship is covered by a contract, dedicated technical work to support the arrangement is justifiable, (though even in these cases consistency among sites is good)
  - in non-contractual situations (e.g. many research/academic collaborations) it is crucial that federation "just works"
- It's a communication issue
  - participants need more/better/easier information from InCommon about the right things to do to make federation work better
  - InCommon needs more/better/richer information from participants about problems, solutions, barriers

Organizational: POP

- “Mandatory” Participant Operational Procedures document
- Think of it as training wheels for Silver
- Touches on other recommendations:
  - Privacy Policies
  - Attribute Release Process for IdPs
  - Requested Attributes for SPs

Organizational: Contacts

- Primary function has turned out to be inter-participant communication, **not** end-user contact
- A critical unmet need is ability for an SP to tell an end user who to contact for attribute release issues
- Proposal:
  - technical: system support between participants
  - administrative: attribute release, meat-space issues between participants
  - support: end user issues
  - security: proposed extenstion for incident response

Organizational: Incident Response

- CIC-developed outline for integrating federated security incident response into local practices for incident response
- Recognizes need for a new type of contact dedicated to incident response
- Federated incidents treated on par with local incidents
- Acknowledges special responsibilities partners have to support each other's incident processes

Tech: Endpoints in Metadata

- TLS/SSL, obviously
- Bindings (Redirect to IdP, POST to SP)
- ECP (SOAP to IdP) if you can
- Avoid unnecessary SAML 2 AttributeService endpoints
- SP keys to support XML Encryption
- Firm prohibitions under discussion
  - require TLS for IdPs?

Tech: Certificates in Metadata

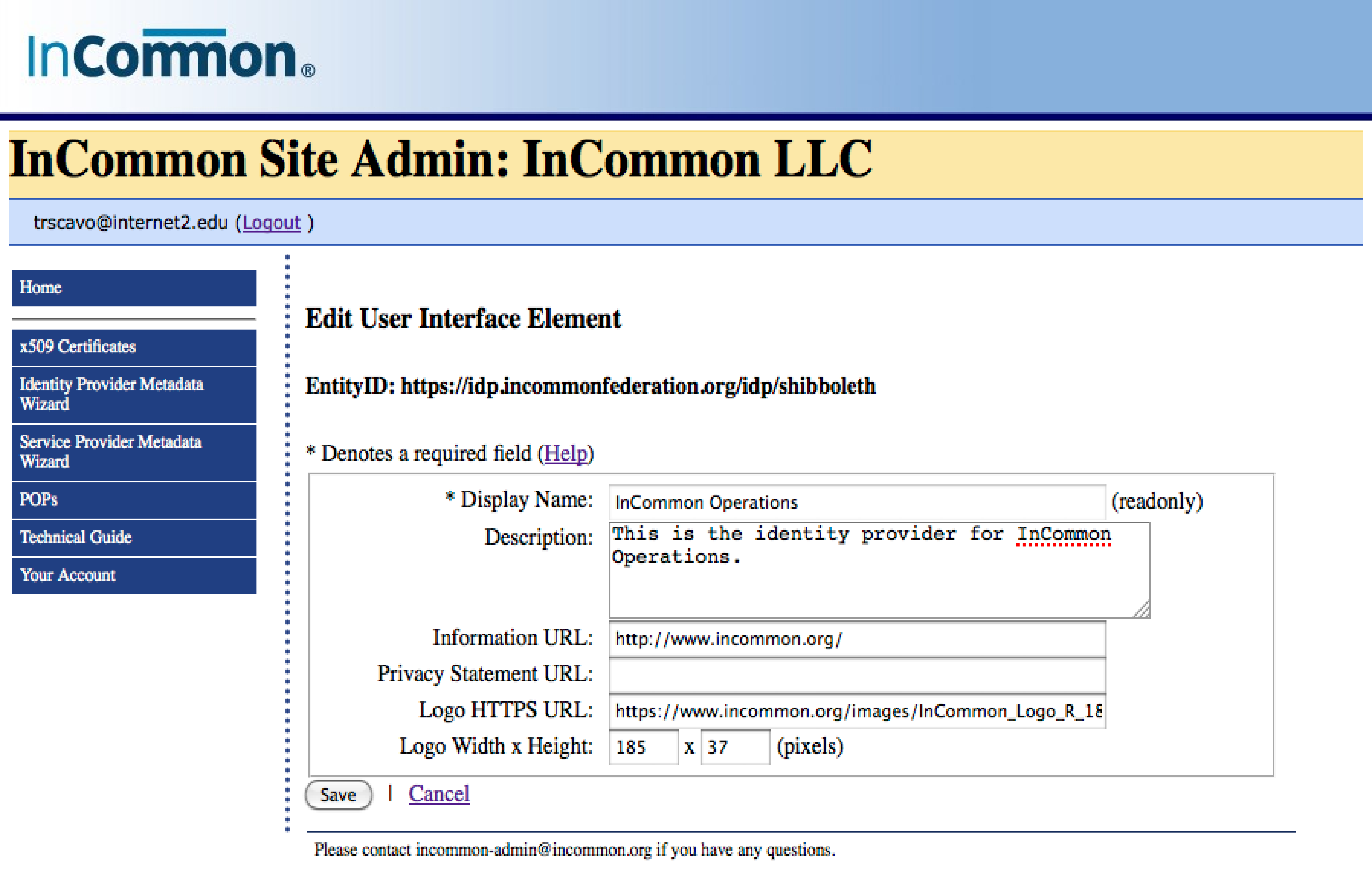
- Public keys wrapped in ASN.1:
  - 2048 bit RSA
  - self-signed
  - long lived, not expired
  - avoid CDP or OCSP extensions
- Controlled key migration:
  - https://spaces.internet2.edu/x/vAEFAQ
- Track partners with non-compliant metadata behavior
  - Federation could assist with this

Tech: Metadata Consumption

- SAML 2.0 standard + OASIS Metadata Interoperability Profile V1.0
  - http://wiki.oasis-open.org/security/SAML2MetadataIOP
  - Key management via metadata
- Depends on metadata carrying a reasonable “validUntil” attribute at the root, and software to enforce it along with the metadata signature
- Little vendor adoption, primary reason Shibboleth remains the only “supported” software in the federation

Tech: User Interface Metadata

- Information supplied by participants via InCommon admin interface
  - display names and logos, descriptions
  - privacy and attribute release policies
- Aids IdPs and SPs in maintaining a coherent “story” throughout the login process
- Discovery pages show IdPs, reference SP
- Login and consent pages reference SP



InCommon Site Admin: InCommon LLC

trscavo@internet2.edu (Logout)

Edit User Interface Element

EntityID: https://idp.incommonfederation.org/idp/shibboleth

* Denotes a required field (Help)

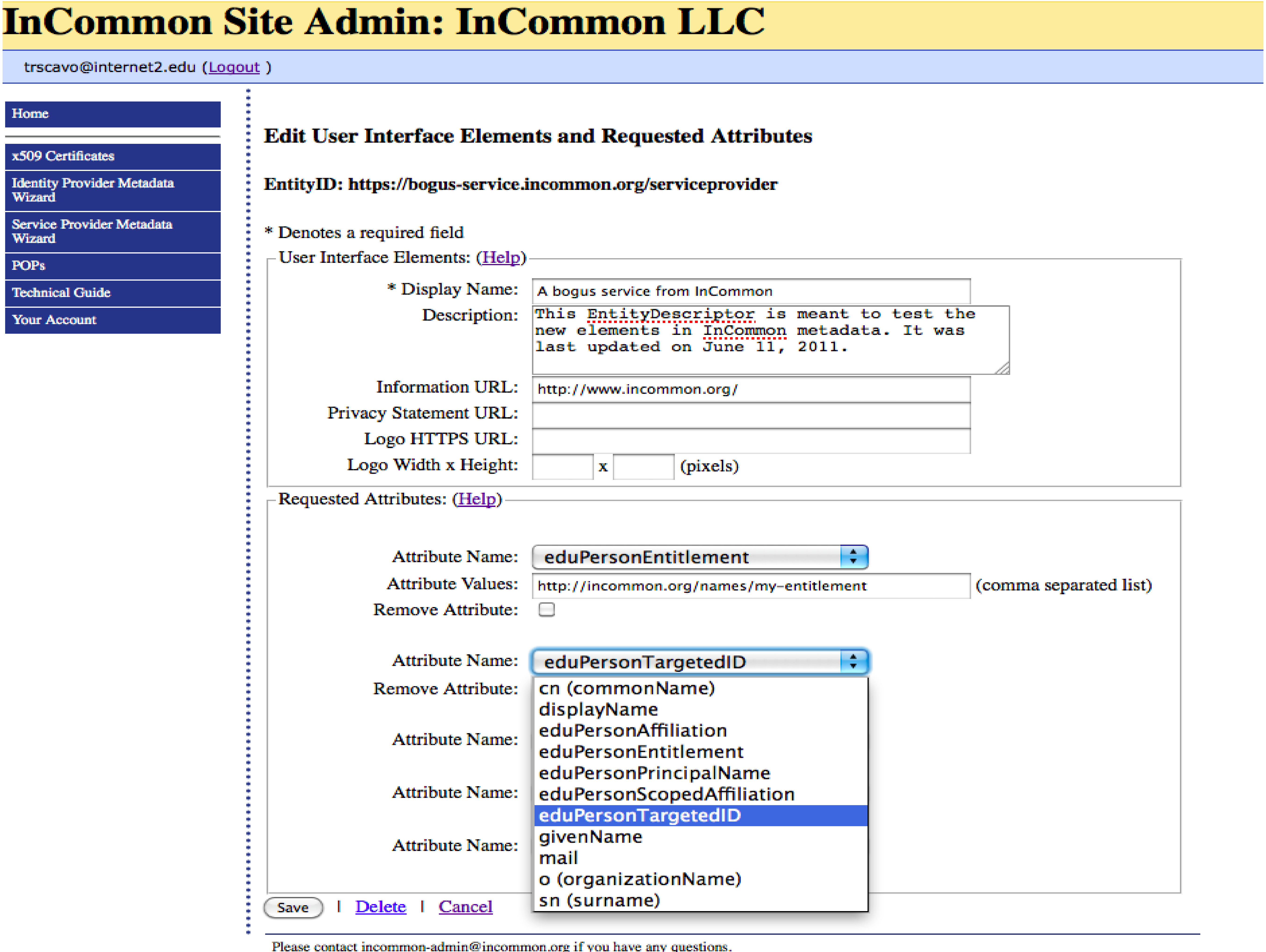
* Display Name:	InCommon Operations	(readonly)
Description:	This is the identity provider for InCommon Operations.	
Information URL:	http://www.incommon.org/	
Privacy Statement URL:		
Logo HTTPS URL:	https://www.incommon.org/images/InCommon_Logo_R_18	
Logo Width x Height:	185 x 37	(pixels)

Save | Cancel

Please contact incommon-admin@incommon.org if you have any questions.

Tech: Requested Attributes

- Movement toward “long-tail”, “promiscuous” federation, services looking for any identities they can get.
- Recommendation to IdPs to move toward opt-in or opt-out attribute release models.
- Common factor: automating discovery of attributes the SP needs.
- InCommon admin wizard handles basic attributes important to common use cases
- Future enhancements will address more complex applications



InCommon Site Admin: InCommon LLC

trscavo@internet2.edu (Logout)

Home
x509 Certificates
Identity Provider Metadata Wizard
Service Provider Metadata Wizard
POPs
Technical Guide
Your Account

Edit User Interface Elements and Requested Attributes

EntityID: https://bogus-service.incommon.org/serviceprovider

* Denotes a required field

User Interface Elements: (Help)

* Display Name:	A bogus service from InCommon
Description:	This EntityDescriptor is meant to test the new elements in InCommon metadata. It was last updated on June 11, 2011.
Information URL:	http://www.incommon.org/
Privacy Statement URL:	
Logo HTTPS URL:	
Logo Width x Height:	x (pixels)

Requested Attributes: (Help)

Attribute Name:	eduPersonEntitlement
Attribute Values:	http://incommon.org/names/my-entitlement (comma separated list)
Remove Attribute:	☐
Attribute Name:	eduPersonTargetedID
Remove Attribute:	
Attribute Name:	
Attribute Name:	
Attribute Name:	

Please contact incommon-admin@incommon.org if you have any questions.

Maturity: Software Maintenance

- Monitor lists, apply patches, you know the drill
  - For Shibboleth, monitor the “announce” list
- Web-based systems have unique and stubborn vulnerabilities, do not expect this to change
- Assurance programs are predicated on sound systems management practices
- Federation remains on an evolutionary path

Maturity: Error Handling

- How do you know an SP isn’t serious?
  - When you see the Gryphon (*)
- How do you know an SP **really** isn’t serious?
  - When you see a missing image instead of the Gryphon.

- (*) Shibboleth Project sites excepted.

Maturity: Error Handling

- Regardless of software:
  - look and feel
  - don’t expect IdP help desk to support your SP
  - for production, error pages focused on user self-help
- For Shibboleth:
  - In SP, templates are a fall back, redirectErrors to app script is much more powerful
  - In IdP, templates (JSP or Velocity) are fully programmable
- Remapping error messages really helps…

Maturity: User Experience

- Understanding of how federation should work is very different in 2011 vs. 2001, documentation has not kept up.
- Early adopters got lots of things wrong, and deserve our thanks.
- One size fits most, and consistency is king.
- If apps favor local accounts, so will users.

Maturity: User Experience

- Login link in upper right.
- Embedded or stand-alone discovery with reference to SP.
  - include all login options, not just InCommon or just federation
  - search as you type, not list (unless list is very small)
  - previous or favored choices shown at top, not automatically reused
- IdP login/consent pages reference back to SP.
- SP handles missing attributes via IdP administrative contact.

Maximizing Value: Persistent Identifiers

- eduPersonPrincipalName
  - generally short, email like, readable
  - activity correlates across services
  - reassigned after fallow periods by some organizations
- eduPersonTargetedID / SAML “persistent” NameID
  - so-called “directed” identifier
  - longer, unwieldy for humans, opaque/ugly
  - generally uncorrelatable except by “affiliated” services
  - never reassigned

Maximizing Value: Persistent Identifiers

- Supporting ePTID historically rare, increasingly important
- All IdPs are urged to support it:
  - generate and store in a database if you prefer
  - compute via a hash if you can't
- Consider release of ePTID for “most” users to “most” SPs
  - discussions active around definitions of “most”

Maximizing Value: Attribute Release Process

- Opt-In
  - Full power of consent add-ons like uApprove set a high bar
  - Less powerful approaches seem worth consideration
- Opt-Out
  - Relaxing default release of basic attributes for “some” users to “some” SPs
  - Federation can deliver compelling value in delivering assurance of which SPs are “some”

Maximizing Value: Attribute Release Process

- Document a process and link to it via <PrivacyStatementURL>
- Provide an administrative contact whose job is to make release happen when it should