Getting Started With InCommon

Steve Thorpe, MCNC
thorpe@mcnc.org

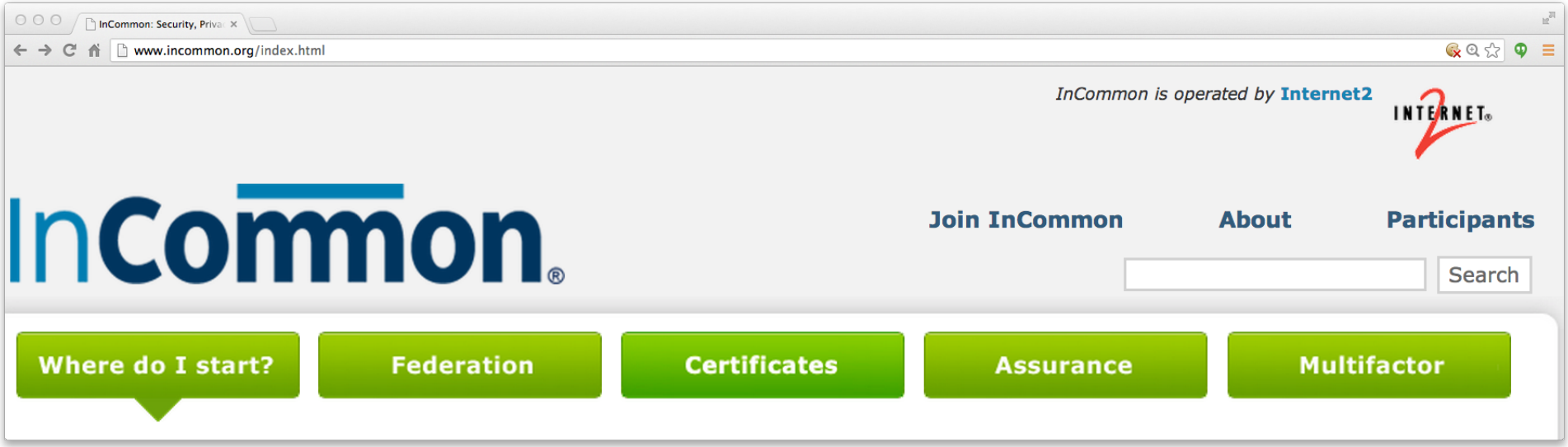
Slides are here: **http://bit.ly/HLCu54**

InCommon camp
Campus Architecture & Middleware Planning

Pre-Conference

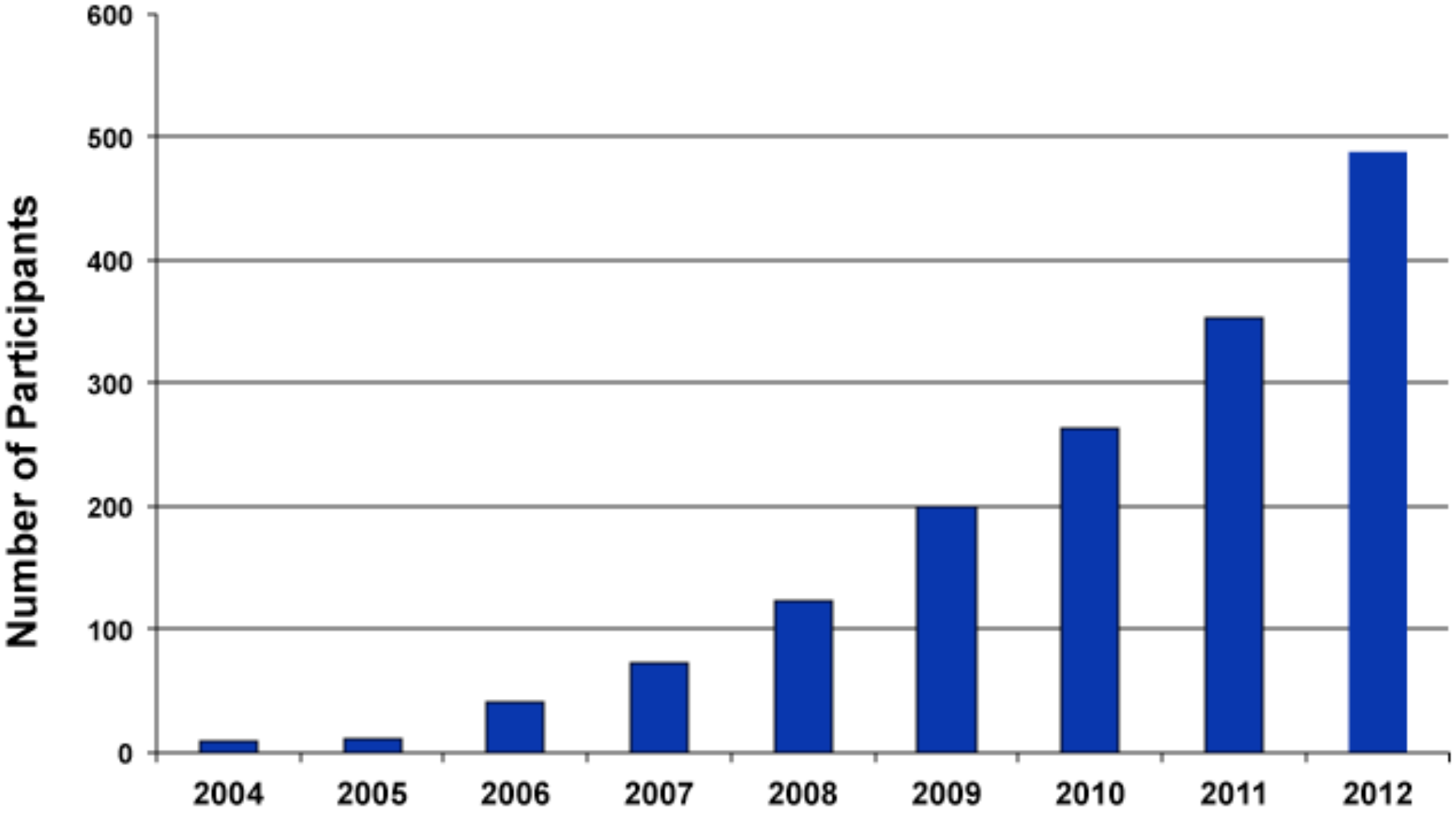
Getting Started with Federated Identity Management
Wednesday, November 13, 2013
San Francisco, CA

Where do I start?



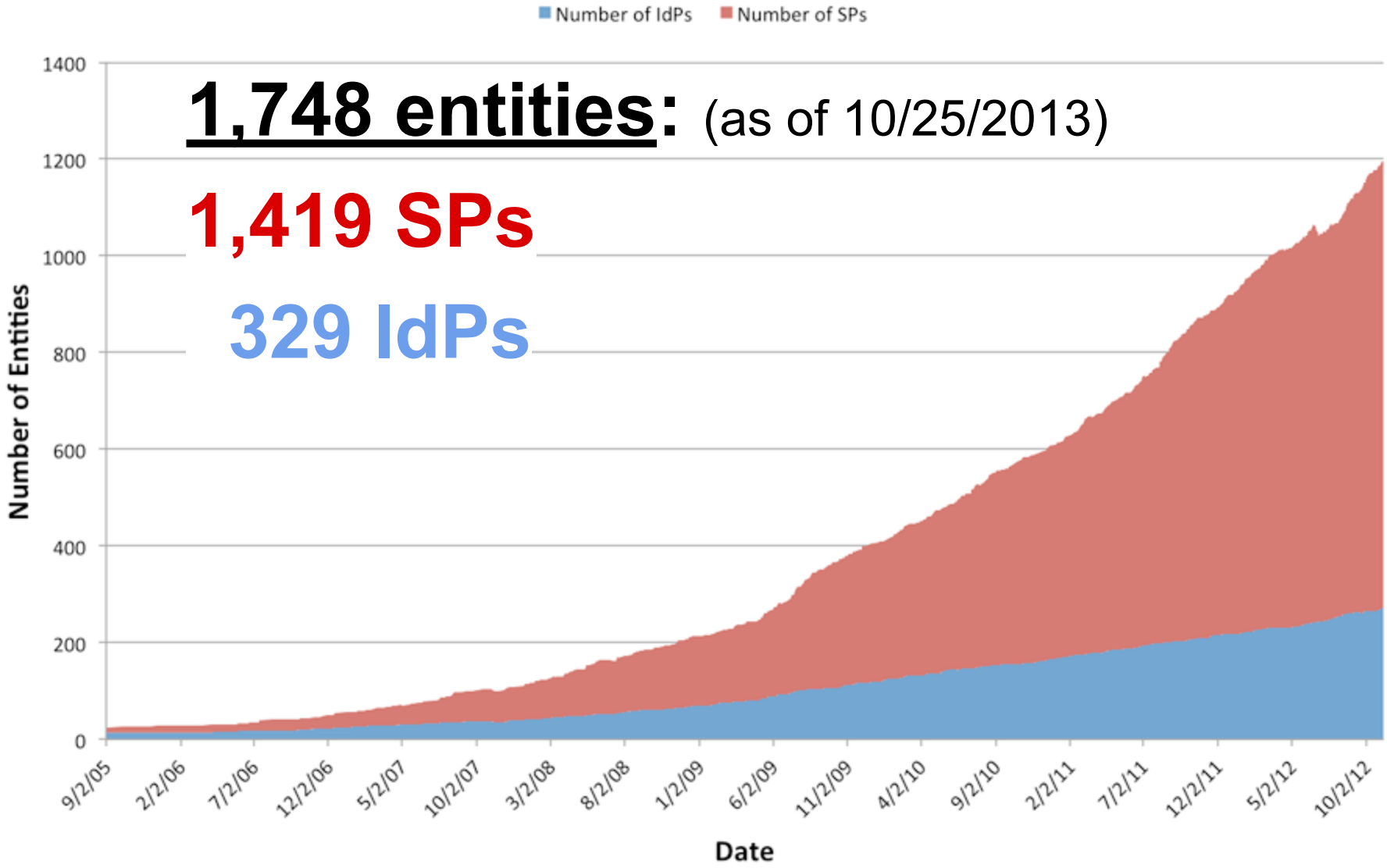
InCommon, operated by Internet2, provides a secure and privacy-preserving trust fabric for research and higher education, and their partners, in the United States. InCommon operates an identity management federation, a related assurance program, and offers certificate and multifactor authentication services.

InCommon Participant Growth



http://www.incommon.org/newsletter/images/participants_2012.png

InCommon Metadata Entity Growth



1,748 entities: (as of 10/25/2013)

1,419 SPs

329 IdPs

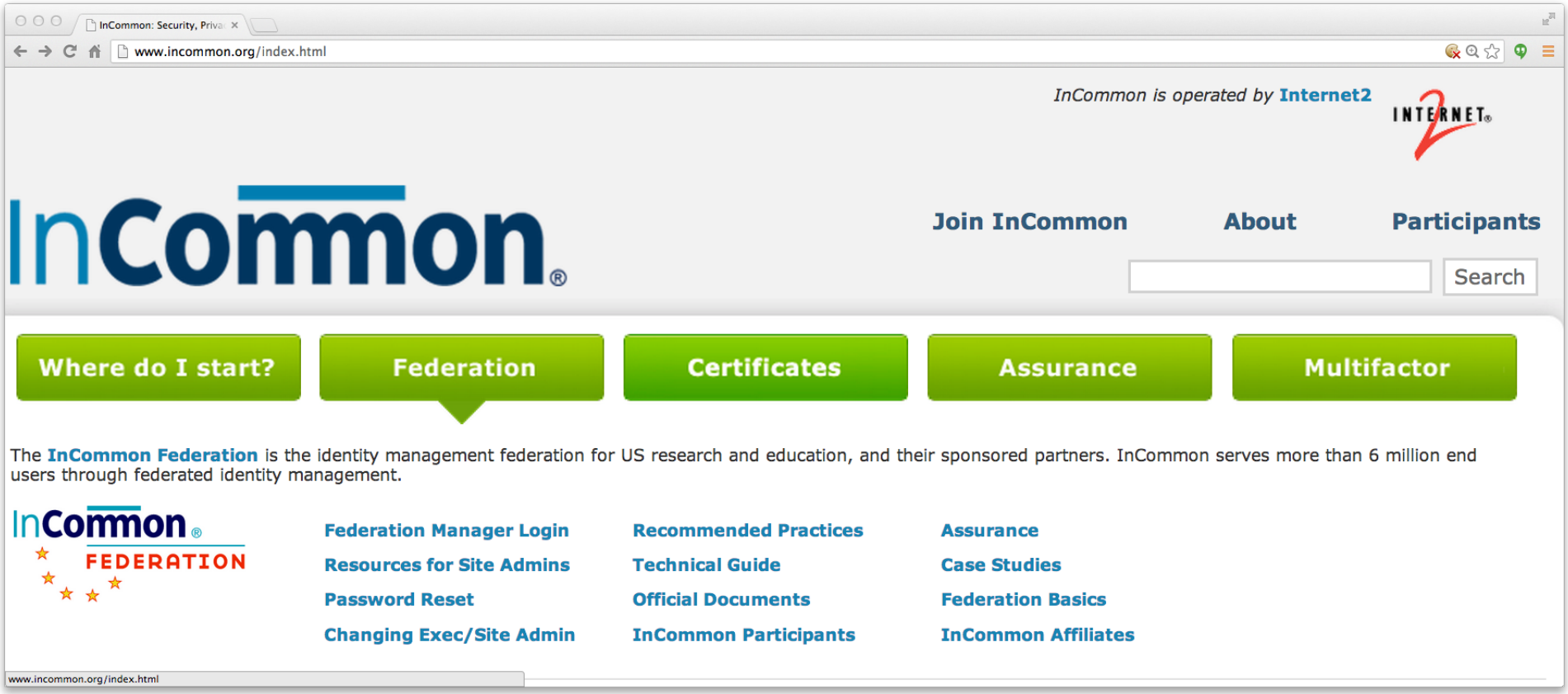
http://www.incommon.org/newsletter/images/entities_2012.png

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

See your "InCommon Basics and Participating in InCommon" Handout

- InCommon Basics
  - Federated Id Management Checklists
  - IdP: Identity Management Preparation
  - IdP: Identity Attribute Provisioning
  - Service Provider Preparation
- Joining InCommon
  - Complete PoP
  - Become sponsored if necessary
  - Submit completed agreement and payment
  - Executive & administrator registration / Id proofing
- Add / manage your entities in the InCommon Metadata

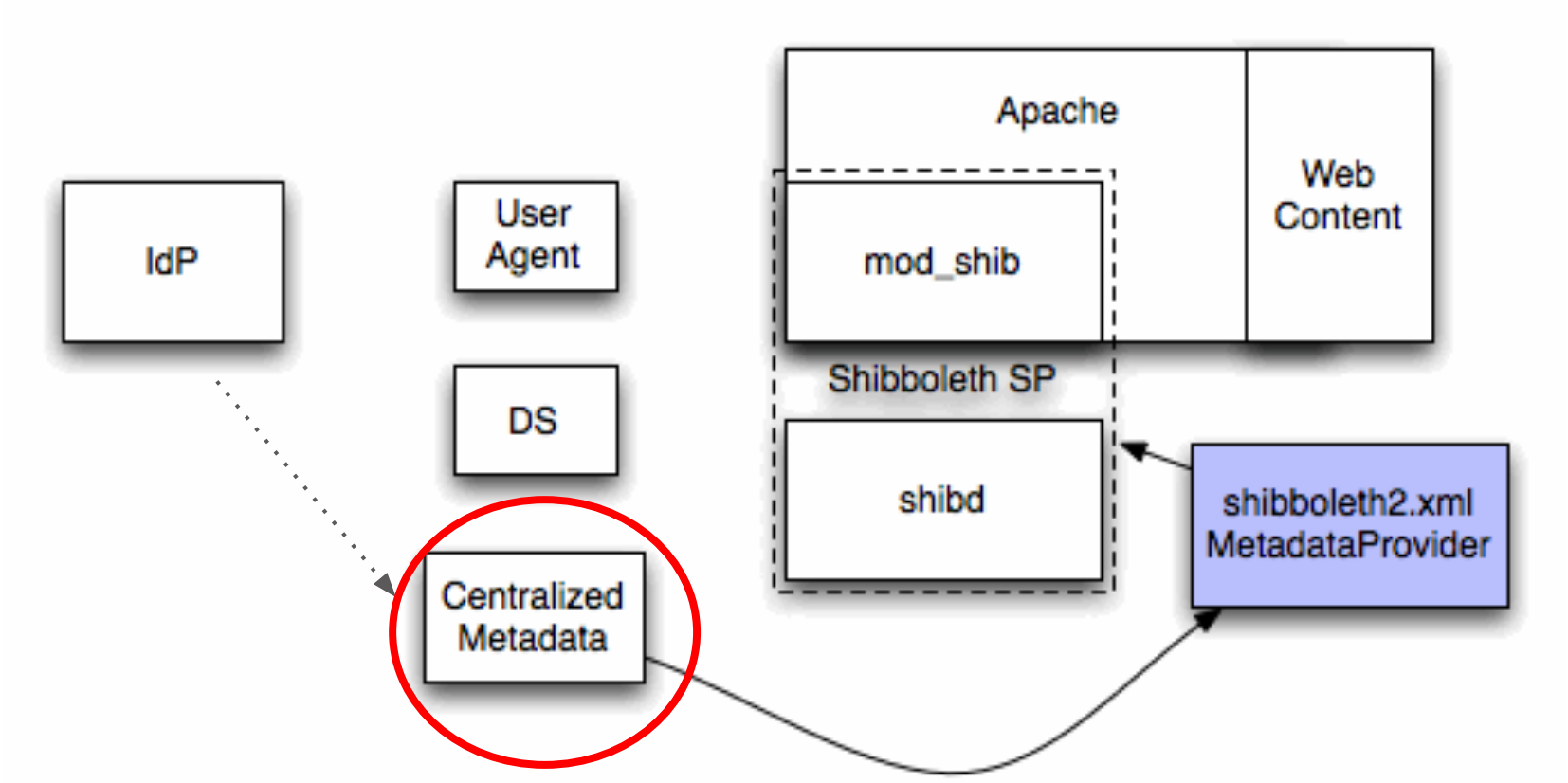
Federation


InCommon: Security, Priva
www.incommon.org/index.html
InCommon is operated by Internet2
INTERNET2
InCommon
Join InCommon
About
Participants
Search
Where do I start?
Federation
Certificates
Assurance
Multifactor
The InCommon Federation is the identity management federation for US research and education, and their sponsored partners. InCommon serves more than 6 million end users through federated identity management.
InCommon FEDERATION
Federation Manager Login
Resources for Site Admins
Password Reset
Changing Exec/Site Admin
Recommended Practices
Technical Guide
Official Documents
InCommon Participants
Assurance
Case Studies
Federation Basics
InCommon Affiliates
www.incommon.org/index.html

InCommon Metadata: the technical glue that enables federating

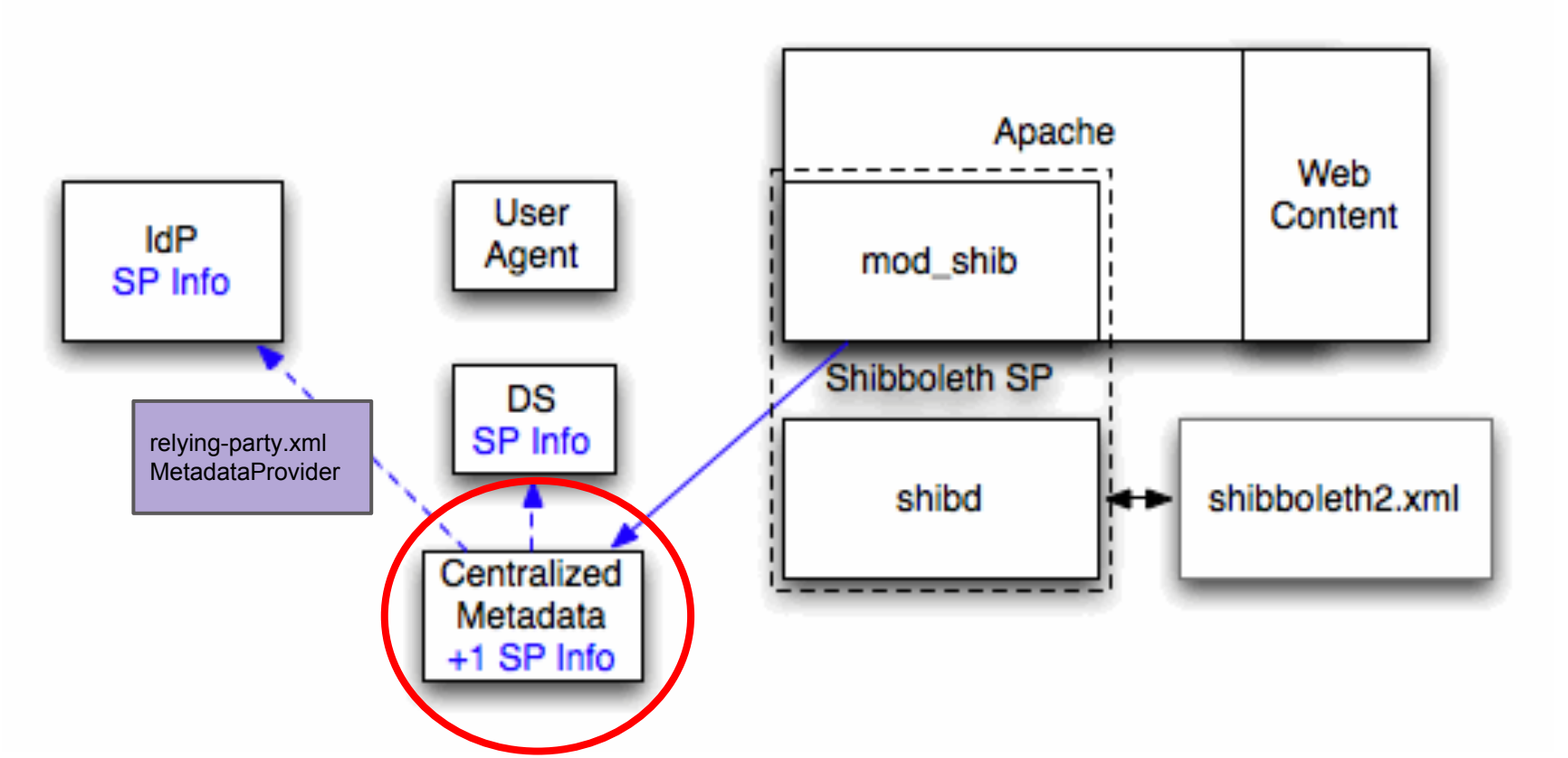
- Like a phonebook and caller-ID function rolled into one
  - Where can I find your IdP and SPs?
  - How do I recognize your IdP and SPs?
- InCommon makes this process easy among its membership, by eliminating the need for one-off bilateral information exchanges
- It is totally up to the members as to whether to actually exchange data with other entities

SP Recognizes IdPs Via Metadata



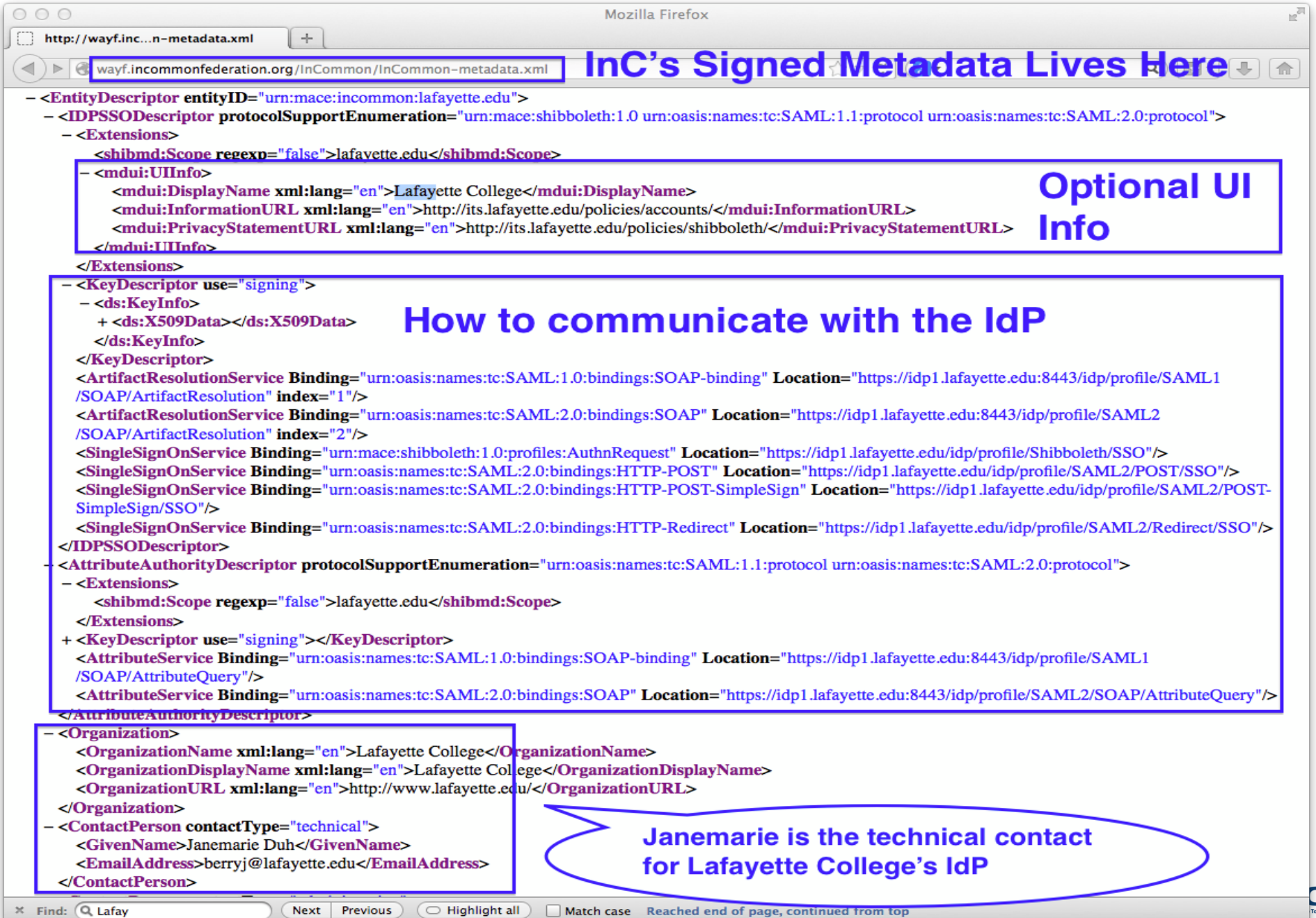
Source: https://spaces.internet2.edu/display/ShibInstallFest/Shibboleth+Workshop+Series+-+Linux+Service+Provider+%28CentOS+6.2%29

IdP Recognizes SPs Via Metadata



Source: https://spaces.internet2.edu/display/ShibInstallFest/Shibboleth+Workshop+Series+-+Linux+Service+Provider+%28CentOS+6.2%29

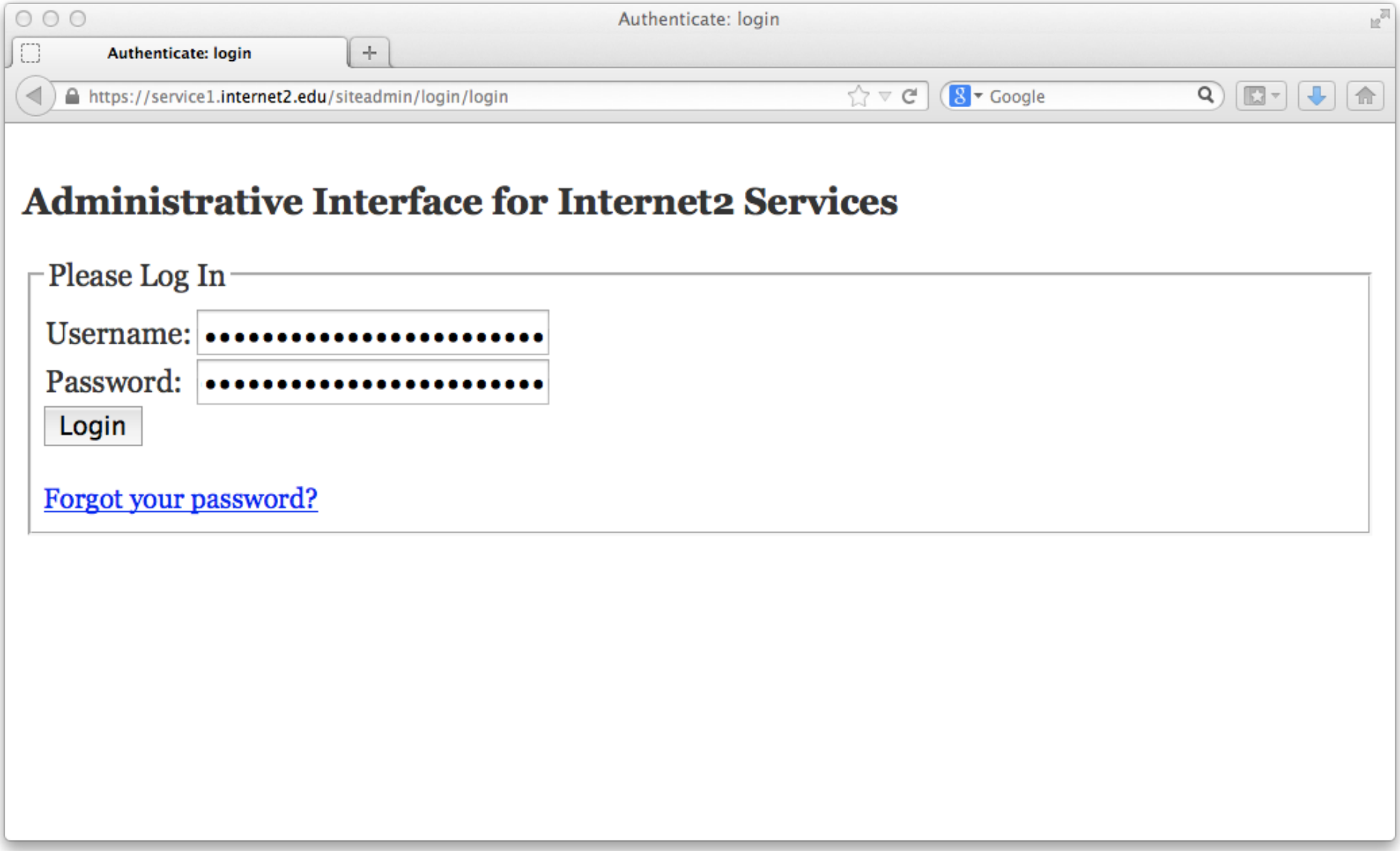
InCommon Metadata - 100,000 Foot View




```
– <EntityDescriptor entityID="urn:mace:incommon:lafayette.edu">
  – <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">lafayette.edu</shibmd:Scope>
      – <mdui:UIInfo>
          <mdui:DisplayName xml:lang="en">Lafayette College</mdui:DisplayName>
          <mdui:InformationURL xml:lang="en">http://its.lafayette.edu/policies/accounts/</mdui:InformationURL>
          <mdui:PrivacyStatementURL xml:lang="en">http://its.lafayette.edu/policies/shibboleth/</mdui:PrivacyStatementURL>
        </mdui:UIInfo>
      </Extensions>
    – <KeyDescriptor use="signing">
      – <ds:KeyInfo>
          + <ds:X509Data></ds:X509Data>
        </ds:KeyInfo>
      </KeyDescriptor>
      <ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding" Location="https://idp1.lafayette.edu:8443/idp/profile/SAML1
      /SOAP/ArtifactResolution" index="1"/>
      <ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://idp1.lafayette.edu:8443/idp/profile/SAML2
      /SOAP/ArtifactResolution" index="2"/>
      <SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest" Location="https://idp1.lafayette.edu/idp/profile/Shibboleth/SSO"/>
      <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://idp1.lafayette.edu/idp/profile/SAML2/POST/SSO"/>
      <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign" Location="https://idp1.lafayette.edu/idp/profile/SAML2/POST-
      SimpleSign/SSO"/>
      <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://idp1.lafayette.edu/idp/profile/SAML2/Redirect/SSO"/>
    </IDPSSODescriptor>
  – <AttributeAuthorityDescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol">
    – <Extensions>
        <shibmd:Scope regexp="false">lafayette.edu</shibmd:Scope>
      </Extensions>
    + <KeyDescriptor use="signing"></KeyDescriptor>
      <AttributeService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding" Location="https://idp1.lafayette.edu:8443/idp/profile/SAML1
      /SOAP/AttributeQuery"/>
      <AttributeService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://idp1.lafayette.edu:8443/idp/profile/SAML2/SOAP/AttributeQuery"/>
    </AttributeAuthorityDescriptor>
  – <Organization>
      <OrganizationName xml:lang="en">Lafayette College</OrganizationName>
      <OrganizationDisplayName xml:lang="en">Lafayette College</OrganizationDisplayName>
      <OrganizationURL xml:lang="en">http://www.lafayette.edu/</OrganizationURL>
    </Organization>
  – <ContactPerson contactType="technical">
      <GivenName>Janemarie Duh</GivenName>
      <EmailAddress>berryj@lafayette.edu</EmailAddress>
    </ContactPerson>
```

Managing Your InCommon Metadata

- Here is a sneak preview of what you can expect when you start managing your organization's InCommon metadata


Authenticate: login
Authenticate: login
https://service1.internet2.edu/siteadmin/login/login
Google
Administrative Interface for Internet2 Services
Please Log In
Username:
Password:
Login
Forgot your password?

InCommon Site Admin: MCNC

(Logout)

Home

x.509 Certificates (IdP only)

Identity Provider Metadata Wizard

Service Provider Metadata Wizard

Delegated Administrators

POPs

Your Account

Documentation

FM Change Log

Your Current Roles:

- InCommon Administrator for MCNC

Questions? Visit our wiki or contact <admin@incommon.org>.

InCommon Site Admin: MCNC

(Logout)

Home

x.509 Certificates (IdP only)

Identity Provider Metadata Wizard

Service Provider Metadata Wizard

Delegated Administrators

POPs

Your Account

Documentation

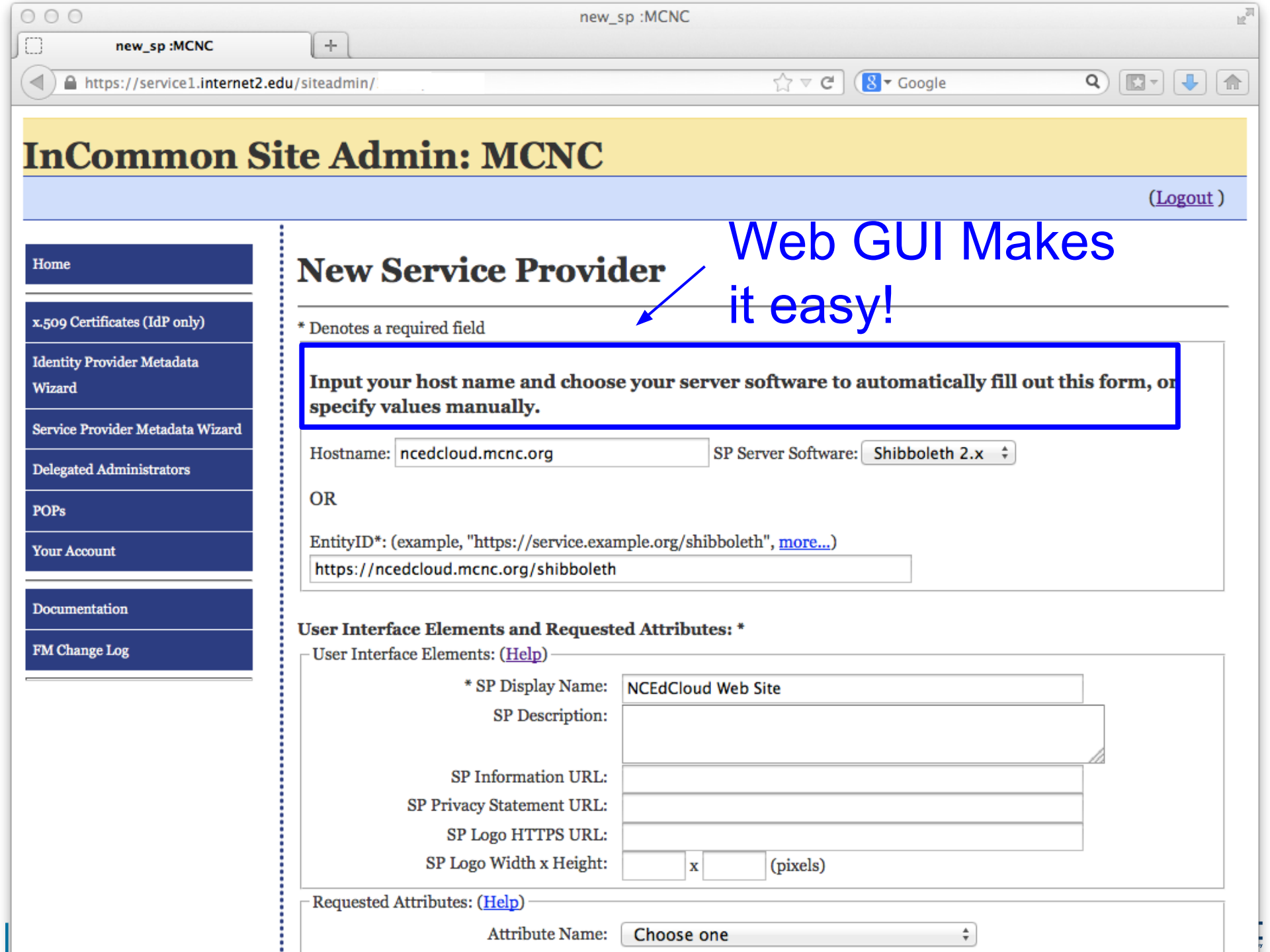
FM Change Log

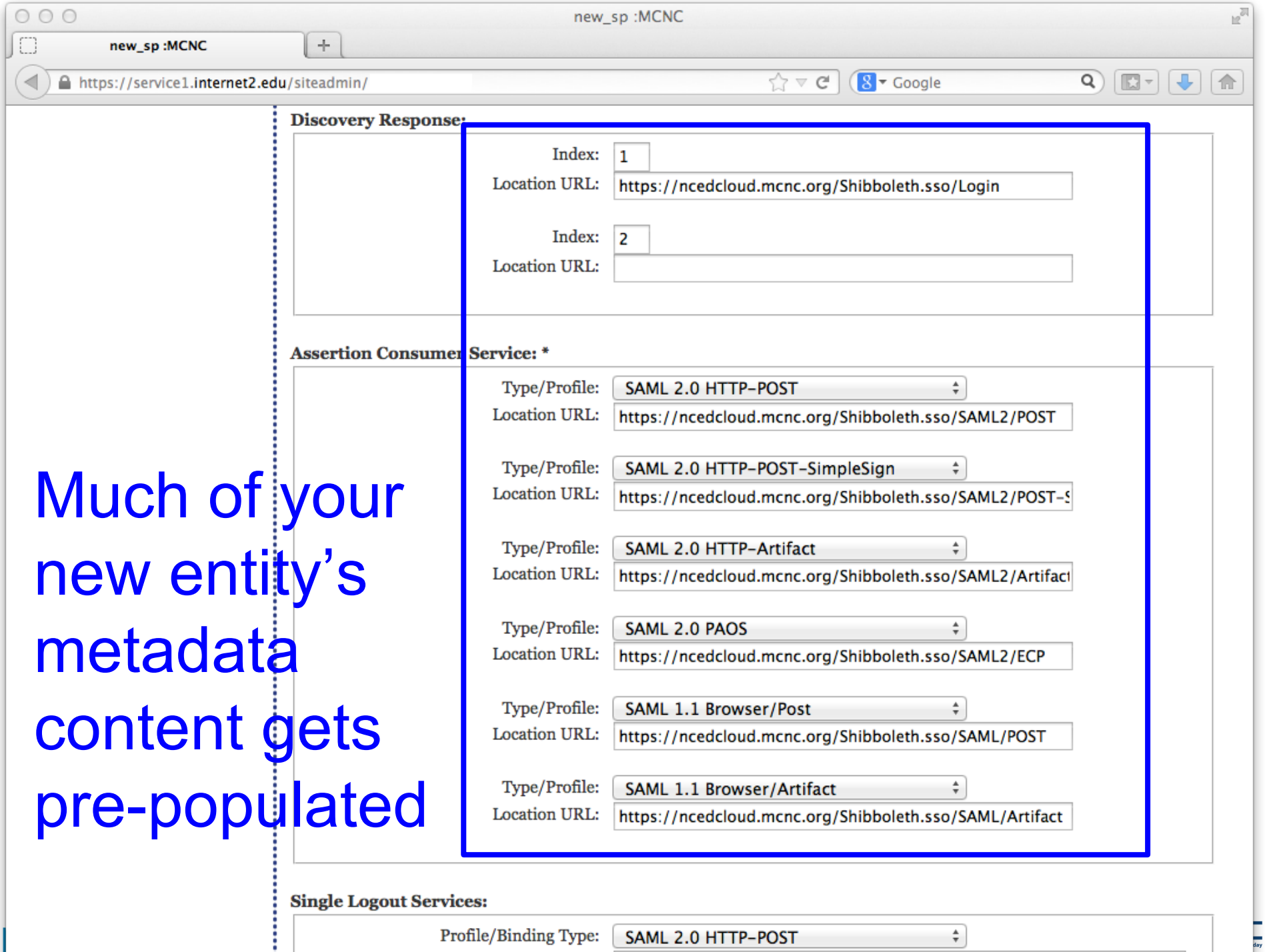
Your Service Providers

Add a New Service Provider

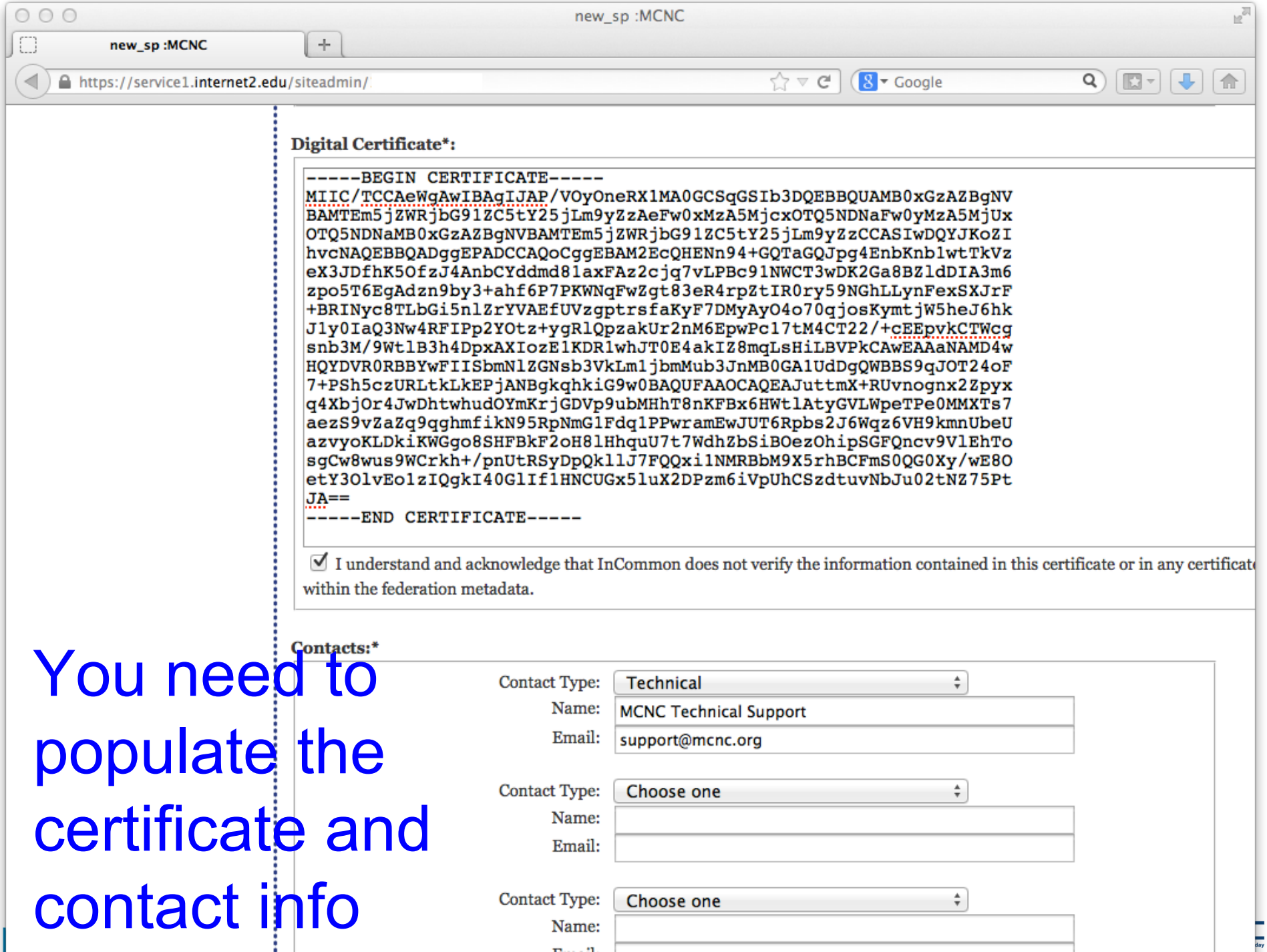
Existing Service Providers

1. https://cacti.mcnc.org/shibboleth
2. https://db-backup.ncren.net/shibboleth
3. https://db-beta.ncren.net/shibboleth
4. https://db.ncren.net/shibboleth
5. https://db-test.ncren.net/shibboleth
6. https://dev.grnoc.ncren.net/shibboleth
7. https://dns.mcnc.org/shibboleth
8. https://dnsui-test-01.mcnc.org/shibboleth
9. https://edspace-test-01.mcnc.org/shibboleth
10. https://edspace-test-02.mcnc.org/shibboleth
11. https://edspace-test.mcnc.org/shibboleth
12. https://footprints-test-01.mcnc.org/shibboleth

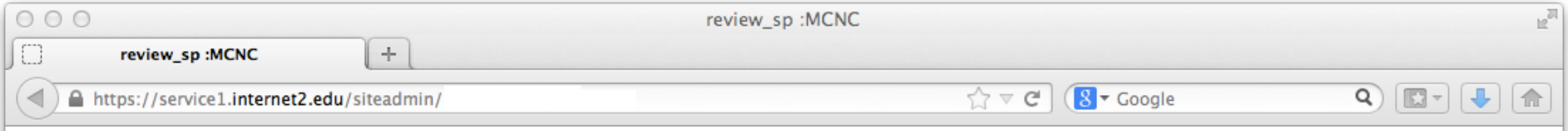

new_sp :MCNC
new_sp :MCNC
https://service1.internet2.edu/siteadmin/
Google
InCommon Site Admin: MCNC
(Logout)
Home
x.509 Certificates (IdP only)
Identity Provider Metadata Wizard
Service Provider Metadata Wizard
Delegated Administrators
POPs
Your Account
Documentation
FM Change Log
New Service Provider
Web GUI Makes it easy!
* Denotes a required field
Input your host name and choose your server software to automatically fill out this form, or specify values manually.
Hostname: ncedcloud.mcnc.org
SP Server Software: Shibboleth 2.x
OR
EntityID*: (example, "https://service.example.org/shibboleth", more...)
https://ncedcloud.mcnc.org/shibboleth
User Interface Elements and Requested Attributes: *
User Interface Elements: (Help)
* SP Display Name: NCEdCloud Web Site
SP Description:
SP Information URL:
SP Privacy Statement URL:
SP Logo HTTPS URL:
SP Logo Width x Height: x (pixels)
Requested Attributes: (Help)
Attribute Name: Choose one



Much of your new entity's metadata content gets pre-populated



You need to populate the certificate and contact info



InCommon Site Admin: MCNC

(Logout)

- Home
- x.509 Certificates (IdP only)
- Identity Provider Metadata Wizard
- Service Provider Metadata Wizard
- Delegated Administrators
- POPs
- Your Account
- Documentation
- FM Change Log

Review Service Provider

Please review then click on the Submit button to complete the metadata update request.
Requests are typically processed within one Internet2 business day.

Provider ID: https://ncedcloud.mcnc.org/shibboleth

User Interface Elements and Requested Attributes:

User Interface Elements

Display Name:	NCEdCloud Web Site
Description:	
Information URL:	
Privacy Statement URL:	
Logo URL:	
Logo Width and Height:	

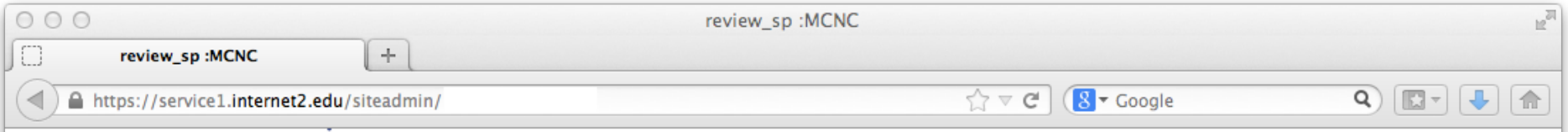
Discovery Response Endpoints:

Index: 1
URL: https://ncedcloud.mcnc.org/Shibboleth.sso/Login

Assertion Consumer Service Endpoints:

Type: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
URL: https://ncedcloud.mcnc.org/Shibboleth.sso/SAML2/POST

Type: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign



Digital Certificates:

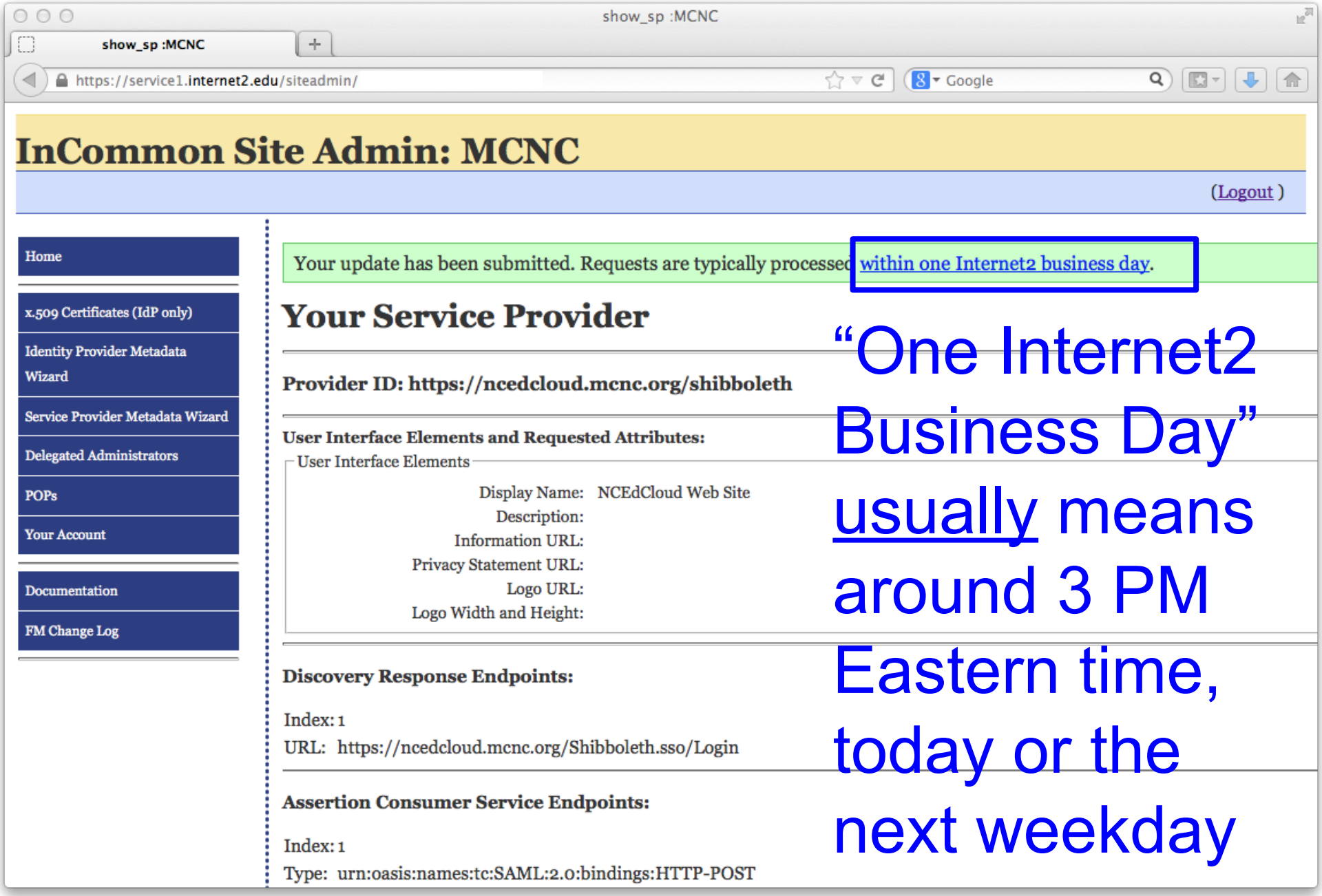
Subject: ncedcloud.mcnc.org
Fingerprint (SHA1): 23:44:2A:E1:44:F0:CB:D2:3F:B7:94:9B:CD:F6:C4:7D:25:71:84:46
Expires at: 2023-09-25 19:49:43 UTC

Contact Type: Technical
Contact Name: MCNC Technical Support
Contact Email: support@mcnc.org

Submit By clicking this submit button, I agree that the information submitted is accurate and is not intentionally misleading, false or fraudulent or otherwise does not infringe on any copyright, patent or trademark rights.

XML Metadata

```
<EntityDescriptor entityID="https://ncedcloud.mcnc.org/shibboleth" xmlns="urn:oasis:names:tc:SAML:2.0
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:t
    <md:Extensions xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
      <DiscoveryResponse xmlns="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol" Binding=
      <mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
        <mdui:DisplayName xml:lang="en">NCEdCloud Web Site</mdui:DisplayName>
      </mdui:UIInfo>
    </md:Extensions>
    <md:KeyDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <!-- Serial No. 18434705674030618101, expires on Mon Sep 25 19:49:43 2023 GMT -->
          <ds:X509Certificate>
MIIC/TCCAeWgAwIBAgIJAP/VOyOneRX1MA0GCSqGSIb3DQEBBQUAMB0xGzAZBgNV
BAMTEm5jZWRjbG91ZC5tY25jLm9yZzAeFw0xMzA5MjcxOTQ5NDNaFw0yMzA5MjUx
OTQ5NDNaMB0xGzAZBgNVBAMTEm5jZWRjbG91ZC5tY25jLm9yZzCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAM2EcQHENn94+GQTaGQJpg4EnbKnb1wtTkVz
eX3JDfhK5OfzJ4AnbCYddmd81axFAz2cjq7vLPBc91NWCT3wDK2Ga8BZldDIA3m6
```



"One Internet2 Business Day" usually means around 3 PM Eastern time, today or the next weekday

Metadata update request confirmation for MCNC - Inbox

Inbox | Metadata update reque...

Get Mail | Write | Chat | Address Book | Tag | Quick Filter | Search... <⌘K>

From do-not-reply@incommon.org

Subject **Metadata update request confirmation for MCNC**

Reply | Reply All | Forward | Archive | Junk | Delete

4:37 PM

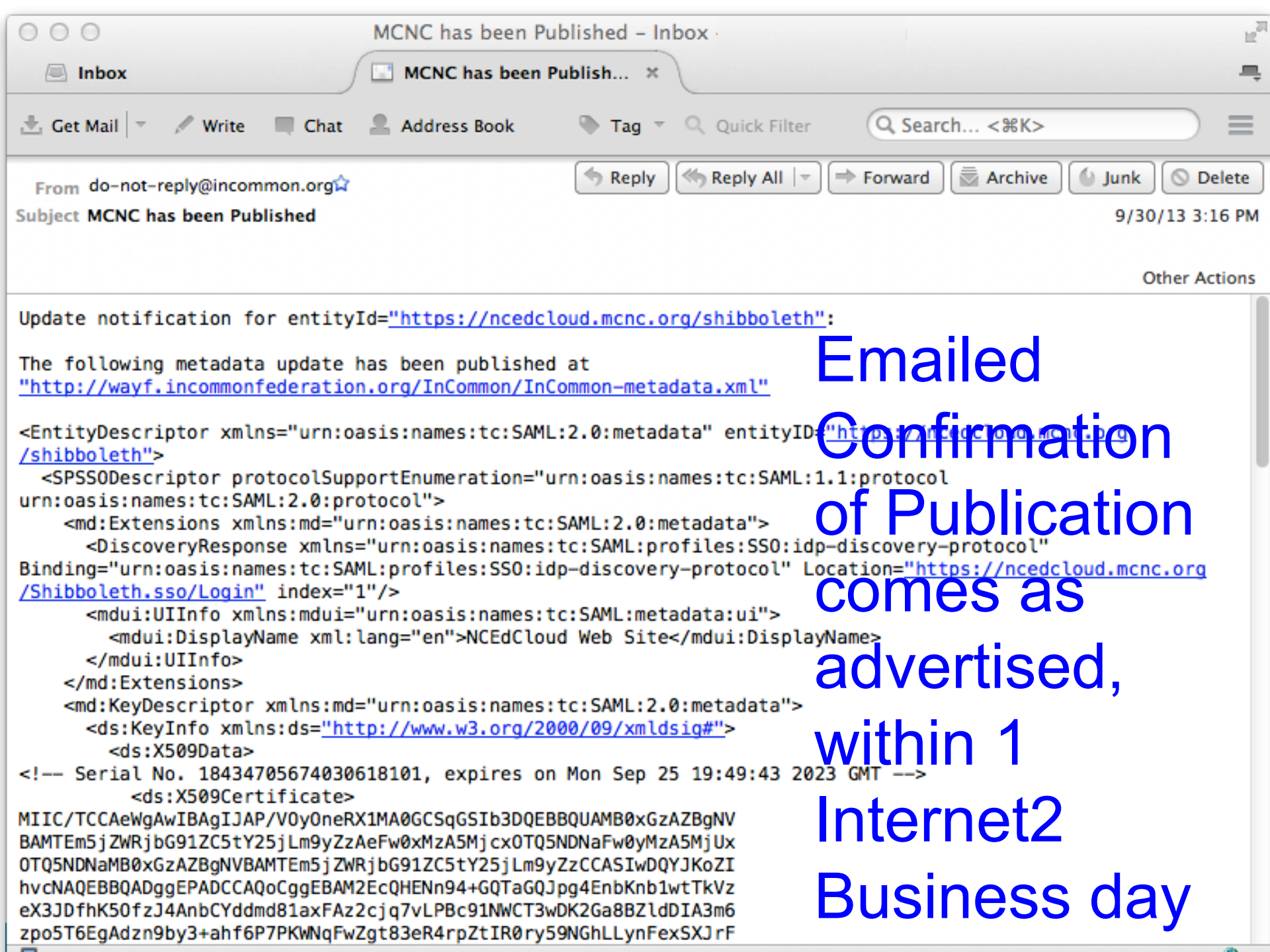
Other Actions

The following metadata update request was submitted
by Steve Thorpe.

Your metadata will be updated as soon as possible, typically within one Internet2
business day "http://www.incommonfederation.org/ops/hours.html". If you have any
questions, please email us at admin@incommon.org.

<EntityDescriptor entityID="https://ncedcloud.mcnc.org/shibboleth" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
<SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol">
<md:Extensions xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
<DiscoveryResponse xmlns="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol"
Binding="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol" Location="https://ncedcloud.mcnc.org/Shibboleth.sso/Login" index="1"/>
<mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
<mdui:DisplayName xml:lang="en">NCEdCloud Web Site</mdui:DisplayName>
</mdui:UIInfo>
</md:Extensions>
<md:KeyDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<!-- Serial No. 18434705674030618101, expires on Mon Sep 25 19:49:43 2023 GMT -->
<ds:X509Certificate>
MIIC/TCCAeWgAwIBAgIJAP/VOyOneRX1MA0GCSqGSIb3DQEBBQUAMB0xGzAZBgNV
BAMTEm5jZWRjbG91ZC5tY25jLm9yZzAeFw0xMzA5MjcxOTQ5NDNaFw0yMzA5MjUx
OTQ5NDNaMB0xGzAZBgNVBAMTEm5jZWRjbG91ZC5tY25jLm9yZzCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAM2EcQHENn94+GQTaGQJpg4EnbKnb1wtTkVz
eX3JDfhK5OfzJ4AnbCYddmd81axFAz2cjq7vLPBc91NWCT3wDK2Ga8BZldDIA3m6
zpo5T6EgAdzn9by3+ahf6P7PKWNqFwZgt83eR4rpZtIR0ry59NGhLLynFexSXJrF
+BRINyc8TLbGi5nlZrYVAEfUVzgptrsfaKyF7DMyAyO4o70qjosKymtjW5heJ6hk
J1y0IaQ3Nw4RFIPp2YOtz+ygRlQpzakUr2nM6EpwPc17tM4CT22/+cEEpvkCTWcg
snb3M/9WtlB3h4DpxAXIozE1KDR1whJT0E4akIZ8mqLsHiLBVPkCAwEAAaNAMD4w
HQYDVR0RBBYwFIISbmNlZGNsb3VkLm1jbmMub3JnMB0GA1UdDgQWBBS9qJOT24oF
7+PSh5czURLtkLkEPjANBgkqhkiG9w0BAQUFAAOCAQEAJuttmX+RUvnognx2Zpyx
q4XbjOr4JwDhtwhudOYmKrjGDVp9ubMHhT8nKFBx6HWtlAtyGVLWpeTPe0MMXTs7
aezS9vZaZq9qghmfikN95RpNmG1Fdq1PPwramEwJUT6Rpbs2J6Wqz6VH9kmnUbeU
azvyoKLDkiKWGgo8SHFBkF2oH8lHhquU7t7WdhZbSiBOezOhipSGFQncv9VlEhTo
sgCw8wus9WCrkh+/pnUtRSyDpQkllJ7FQQxi1NMRBbM9X5rhBCFmS0QG0Xy/wE8O
etY3OlvEo1zIQgkI40GlIf1HNCUGx5luX2DPzm6iVpUhCSzdtuvNbJu02tNZ75Pt
JA==
</ds:X509Certificate>
</ds:X509Data>

Confirmation of submission comes right away by email



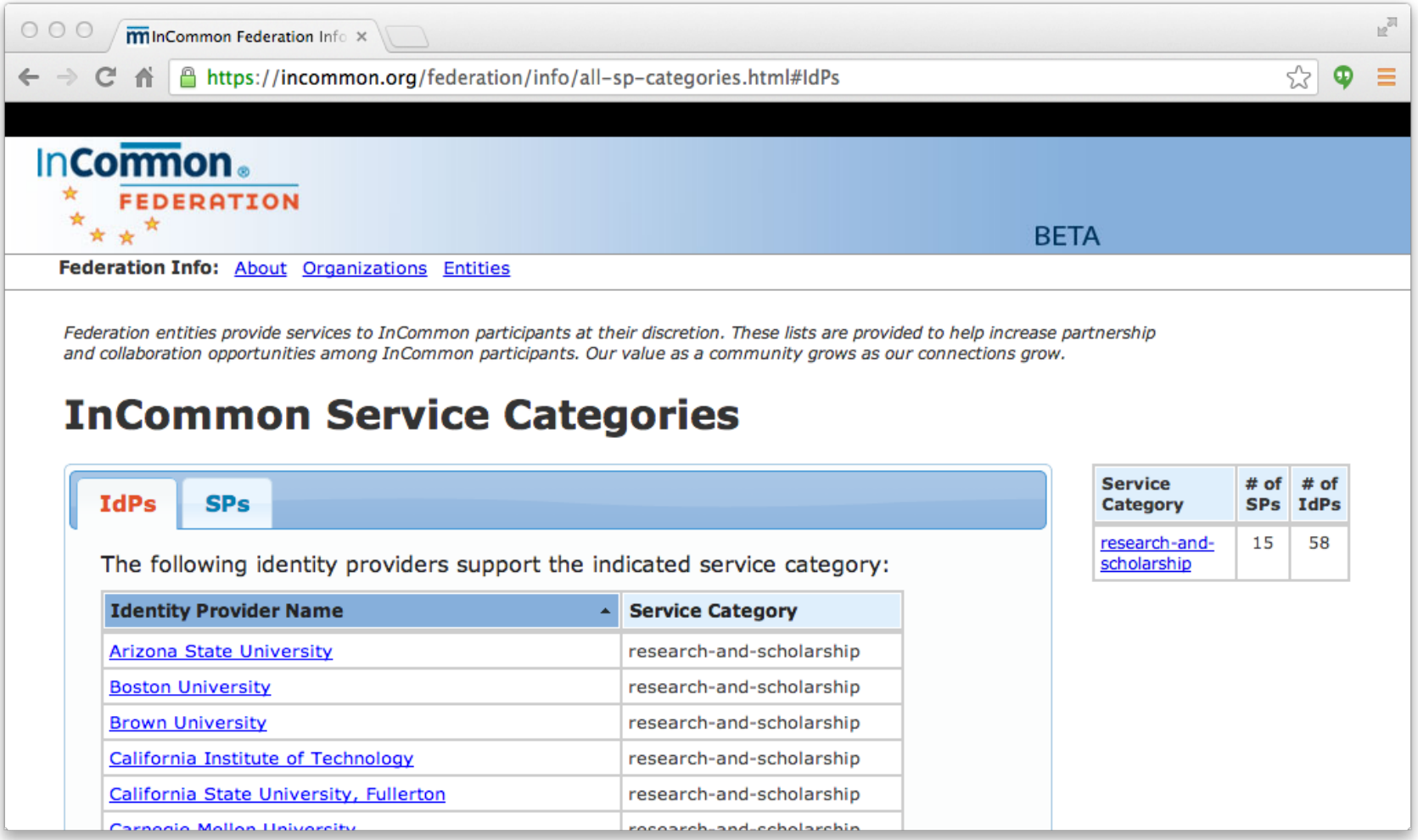
Emailed Confirmation of Publication comes as advertised, within 1 Internet2 Business day

InCommon Service Categories

- Research and Scholarship Category
  - Eases collaboration by reducing the policy interpretation, inter-institutional agreements, and system configuration needed for those services
  - IdP's can make a one-time config change to release certain attributes to all InCommon R&S entities
  - A simpler and more scalable approach than negotiating such release bilaterally with every service provider

58 Research and Scholarship IdPs

(as of October 4, 2013)



15 Research and Scholarship SPs

(as of October 4, 2013)

InCommon Service Categories

IdPs | SPs

The following service providers belong to the indicated service category:

Service Provider Name	Service Category
CarmenWiki	research-and-scholarship
CILogon	research-and-scholarship
Collaboration Wiki Spaces at Internet2	research-and-scholarship
FileSender	research-and-scholarship
GENI Experimenter Portal	research-and-scholarship
GPN/UM Dropoff Services	research-and-scholarship
Indiana CTSI HUB	research-and-scholarship
LIGO CBC Wiki	research-and-scholarship
LIGO Wiki	research-and-scholarship
Multi-Factor Authentication (MFA) Cohortium Registry	research-and-scholarship
Multi-Factor Authentication (MFA) Cohortium Wiki	research-and-scholarship
Narada Metrics	research-and-scholarship
Open Science Data Cloud Console	research-and-scholarship
Penn State WikiSpaces	research-and-scholarship
UW-Milwaukee CGCA Wiki	research-and-scholarship

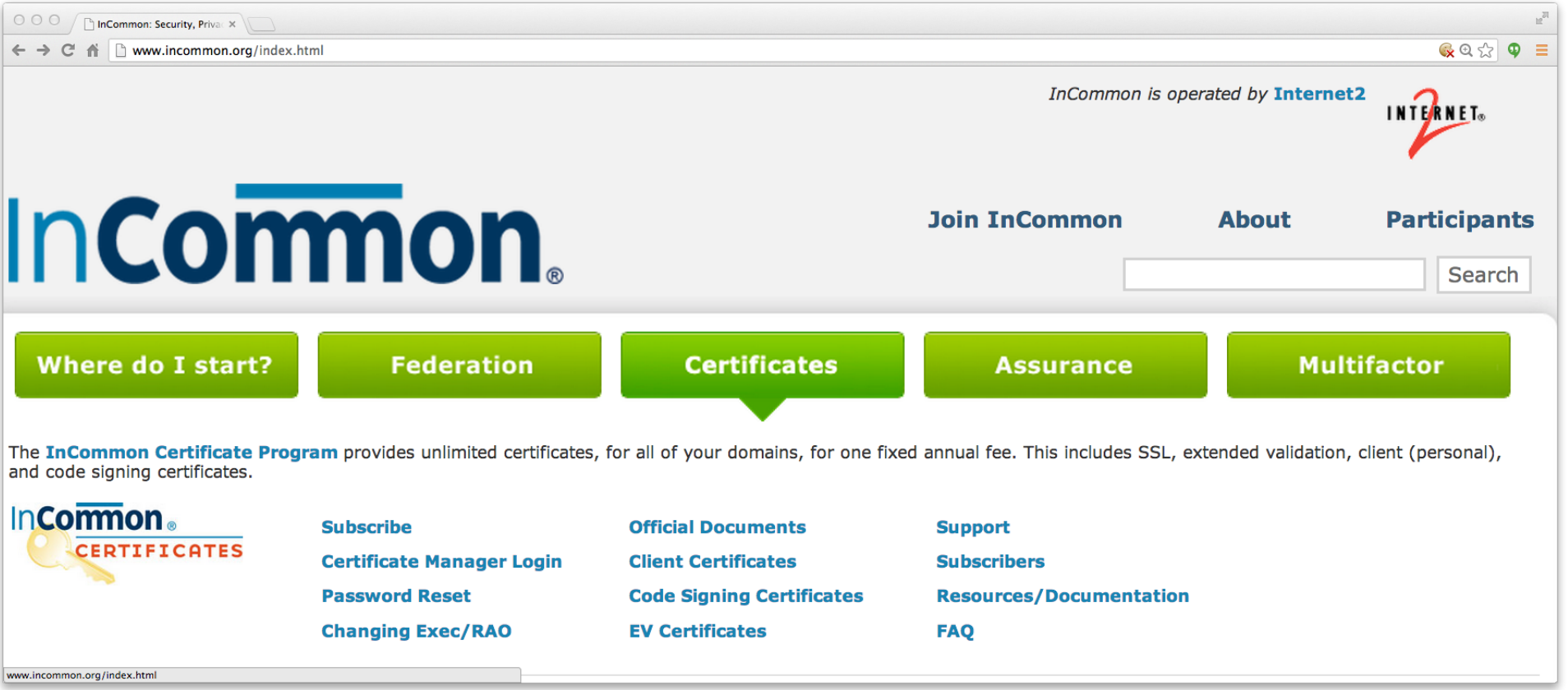
Importance of Vendor Arm-Twisting

- The more vendors support SAML / Shibboleth / InCommon, the better
  - Eases service adoption by peer campuses
  - Expands market for service providers
  - It's a win-win!

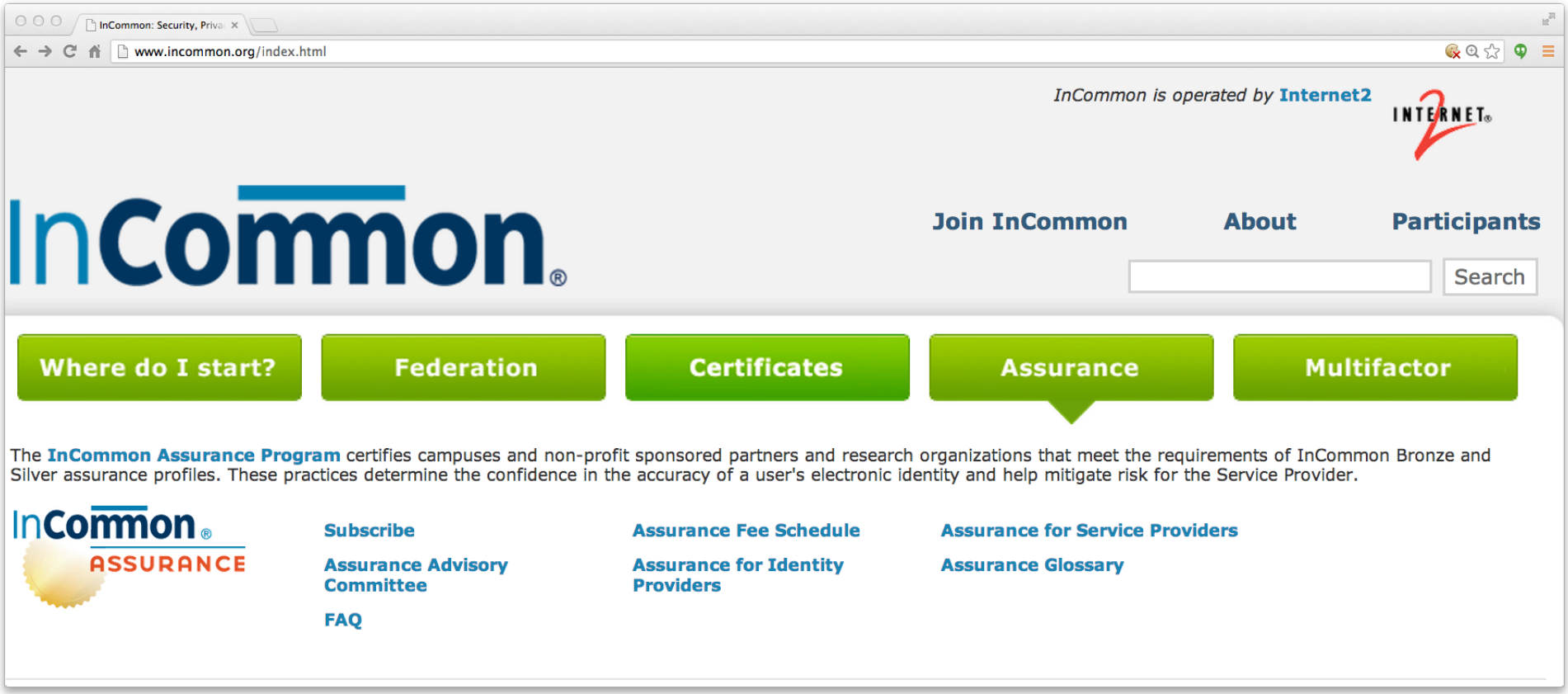
- Consider making it a requirement
  - Build it into your contracts

InCommon® CERTIFICATES

(Janemarie case study?)



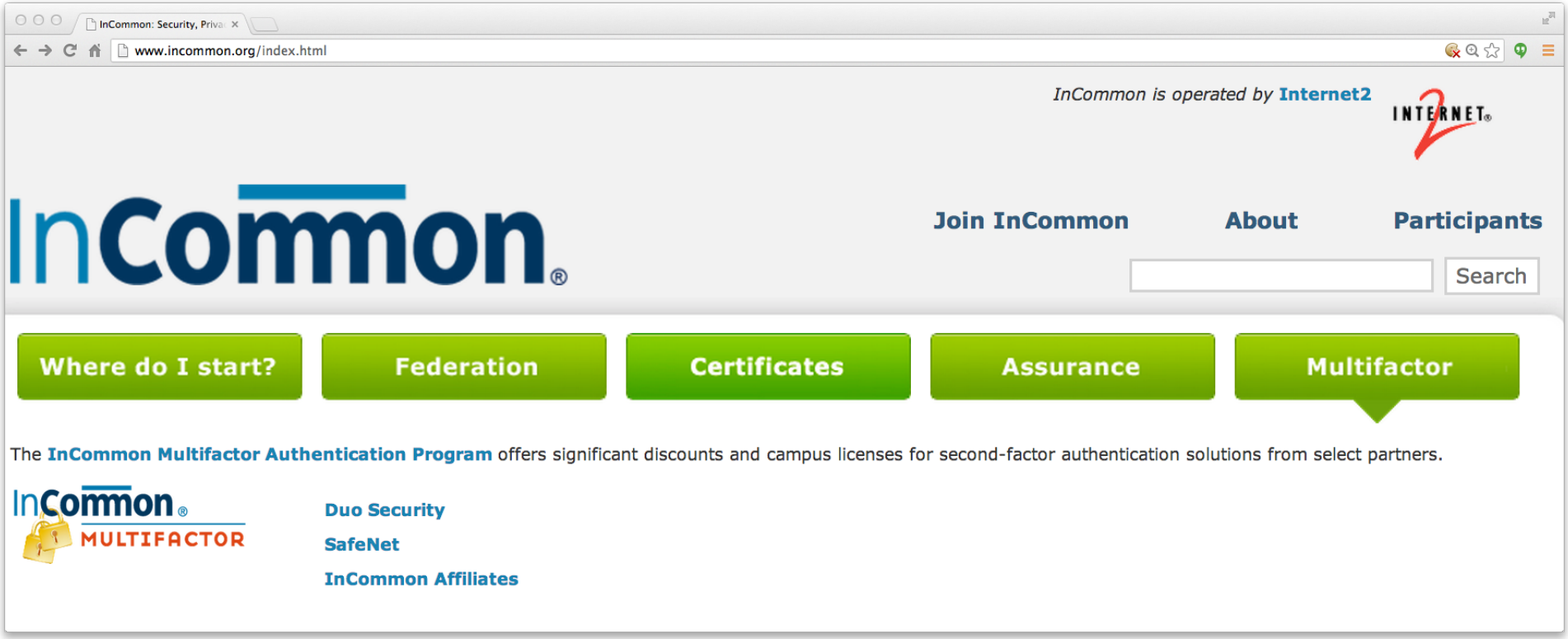
Assurance


InCommon: Security, Priva
www.incommon.org/index.html
InCommon is operated by Internet2
INTERNET2
InCommon
Join InCommon
About
Participants
Search
Where do I start?
Federation
Certificates
Assurance
Multifactor
The InCommon Assurance Program certifies campuses and non-profit sponsored partners and research organizations that meet the requirements of InCommon Bronze and Silver assurance profiles. These practices determine the confidence in the accuracy of a user's electronic identity and help mitigate risk for the Service Provider.
InCommon ASSURANCE
Subscribe
Assurance Advisory Committee
FAQ
Assurance Fee Schedule
Assurance for Identity Providers
Assurance for Service Providers
Assurance Glossary

Assurance Categories

- Identity Providers in InCommon Metadata would include Identity Assurance Qualifiers (for InCommon-certified IdPs)
- **Bronze provides provides reasonable assurance that a particular credential represents the same person each time it is used**
- Silver has identity-proofing requirements that provide reasonable assurance of individual identity. **Silver provides a security level roughly appropriate for basic financial transactions**.
  - Virginia Tech is the pioneering member of Silver

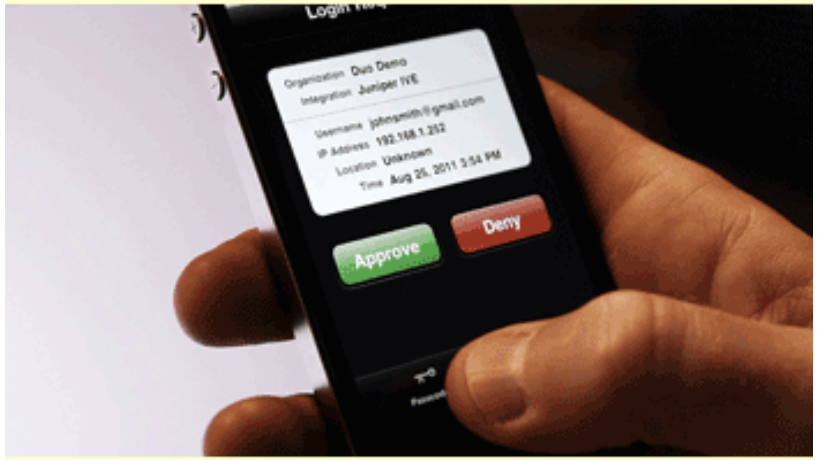
Multifactor



InCommon® MULTIFACTOR

Authentication Solutions

DUO

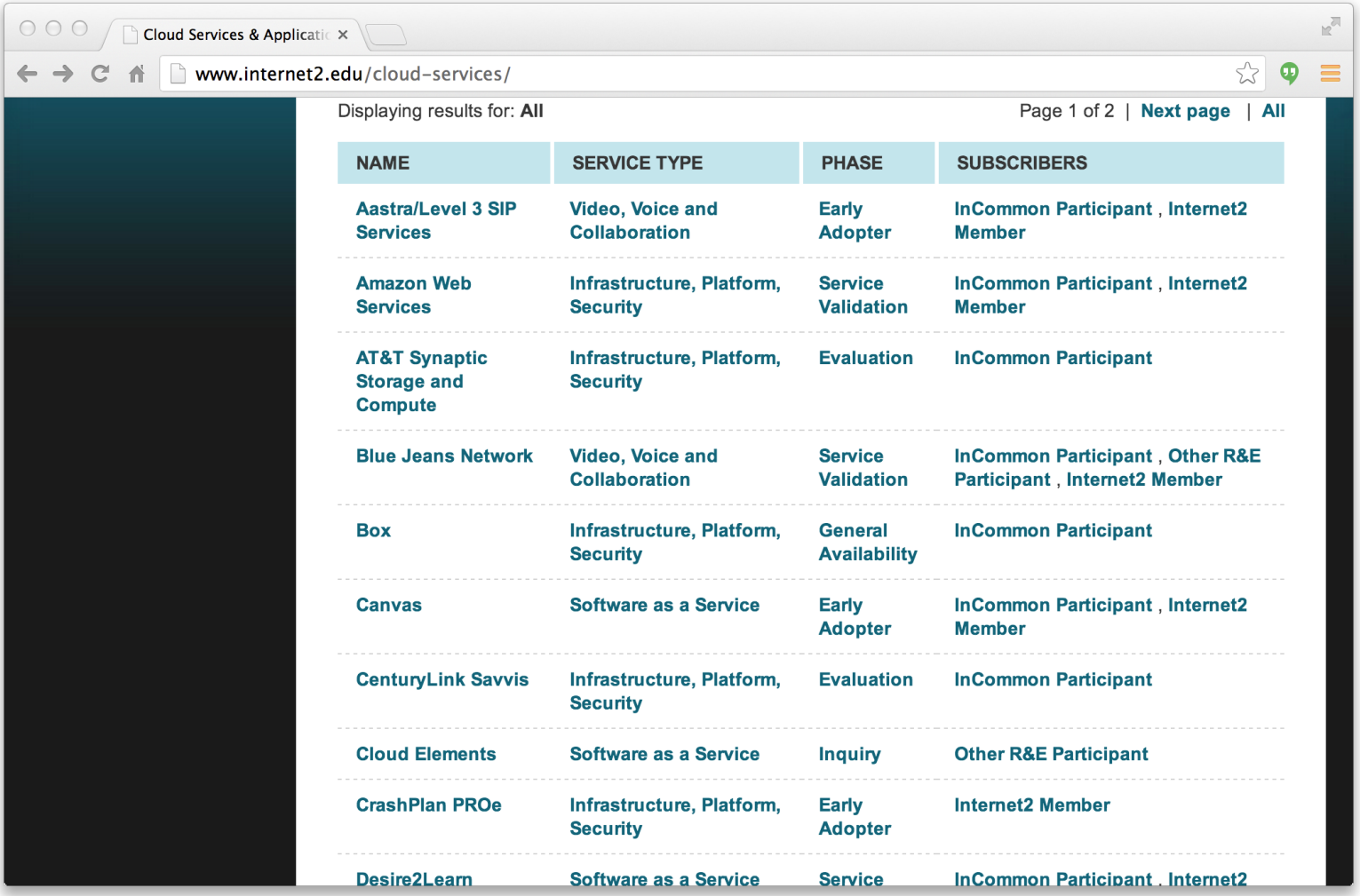


InCommon and Duo Security offer affordable campus licenses for phone-based second-factor authentication.

SafeNet. THE DATA PROTECTION COMPANY

The InCommon/SafeNet program offers smart cards and USB-format hard tokens at a significant discount.

Netplus - Cloud Service Portfolio Utilizing InCommon Infrastructure



Displaying results for: **All**

Page 1 of 2 | **Next page** | **All**

NAME	SERVICE TYPE	PHASE	SUBSCRIBERS
Aastra/Level 3 SIP Services	Video, Voice and Collaboration	Early Adopter	InCommon Participant , Internet2 Member
Amazon Web Services	Infrastructure, Platform, Security	Service Validation	InCommon Participant , Internet2 Member
AT&T Synaptic Storage and Compute	Infrastructure, Platform, Security	Evaluation	InCommon Participant
Blue Jeans Network	Video, Voice and Collaboration	Service Validation	InCommon Participant , Other R&E Participant , Internet2 Member
Box	Infrastructure, Platform, Security	General Availability	InCommon Participant
Canvas	Software as a Service	Early Adopter	InCommon Participant , Internet2 Member
CenturyLink Savvis	Infrastructure, Platform, Security	Evaluation	InCommon Participant
Cloud Elements	Software as a Service	Inquiry	Other R&E Participant
CrashPlan PROe	Infrastructure, Platform, Security	Early Adopter	Internet2 Member
Desire2Learn	Software as a Service	Service	InCommon Participant , Internet2

NCTrust Case Study

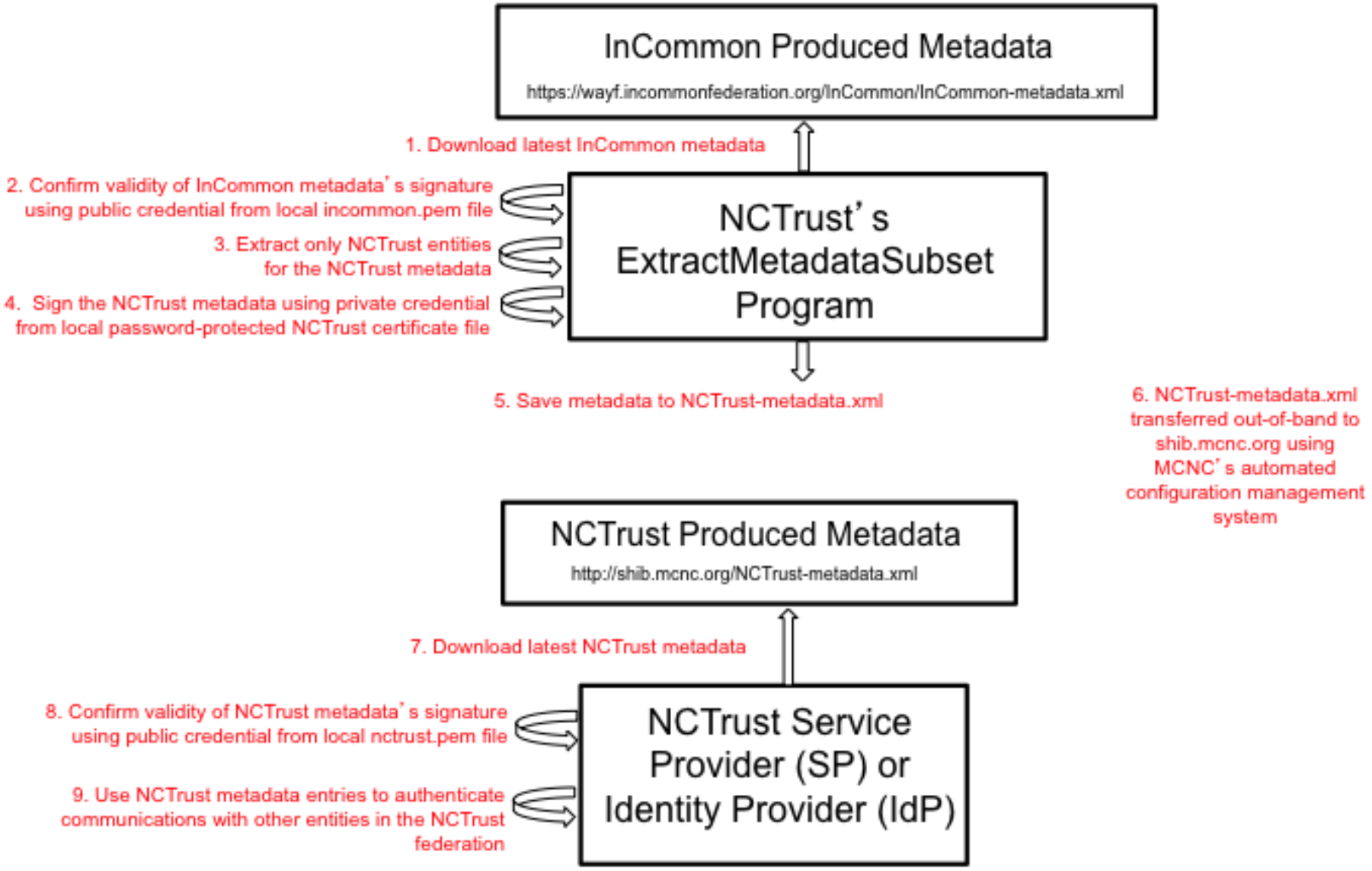
The NCTrust Federation was a pilot project to model a K-20 federation for the state of North Carolina, and included participants from:

- Public and Private 4-year Universities
- 2-yr Community Colleges
- K-12 school districts (LEAs)
- The NC Department of Public Instruction (DPI)
- MCNC (Sponsor and member)

NCTrust Built Using InCommon

- The administrative effort, including the legal framework / documentation / policies / procedures for asserting our various participant responsibilities. This is a HUGE effort, and by joining InCommon we were able to piggy-back on their work.
- InCommon also provided some technical support, as did the community of people responding to questions posed to the Internet2 Shib-Users list.
- Additionally, they had a running SP we could authenticate against (Internet2 Collaboration Wiki site)

NCTrust Federation Metadata Process



NCTrust Partners and Friends

InCommon® Shibboleth Training

- Two-day workshop covers Identity Provider and Service Provider
- Self-paced technical installation and configuration
- Install under Linux (CentOS) or Microsoft Windows environment
- http://www.incommon.org/shibtraining/

Thank you

Questions?