
Getting Started With InCommon®

Steve Thorpe, MCNC
thorpe@mcnc.org

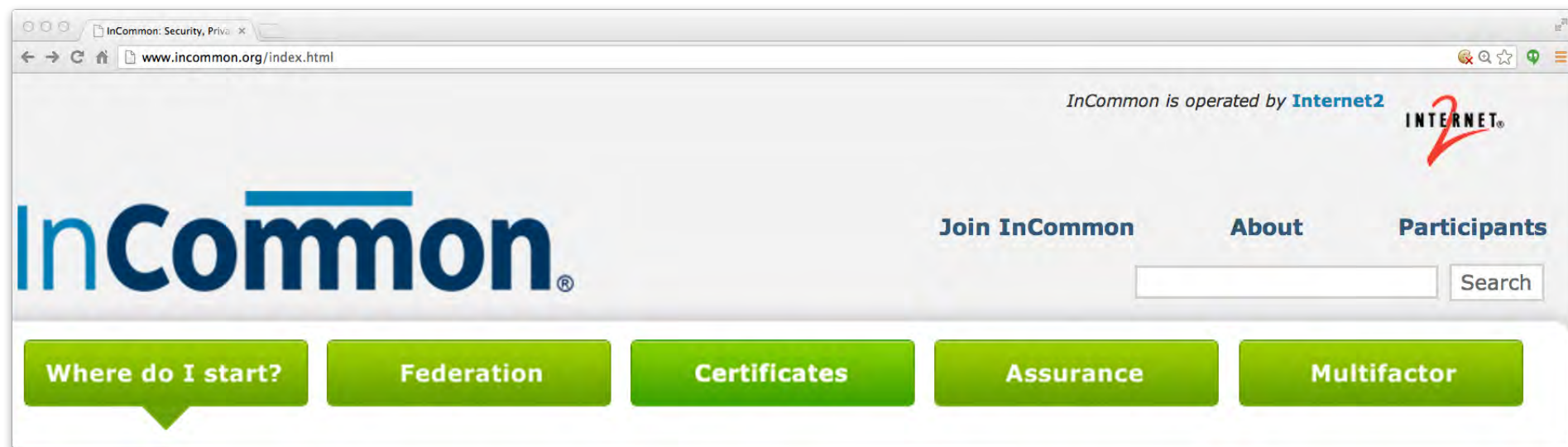


Slides are here: <http://bit.ly/HLCu54>



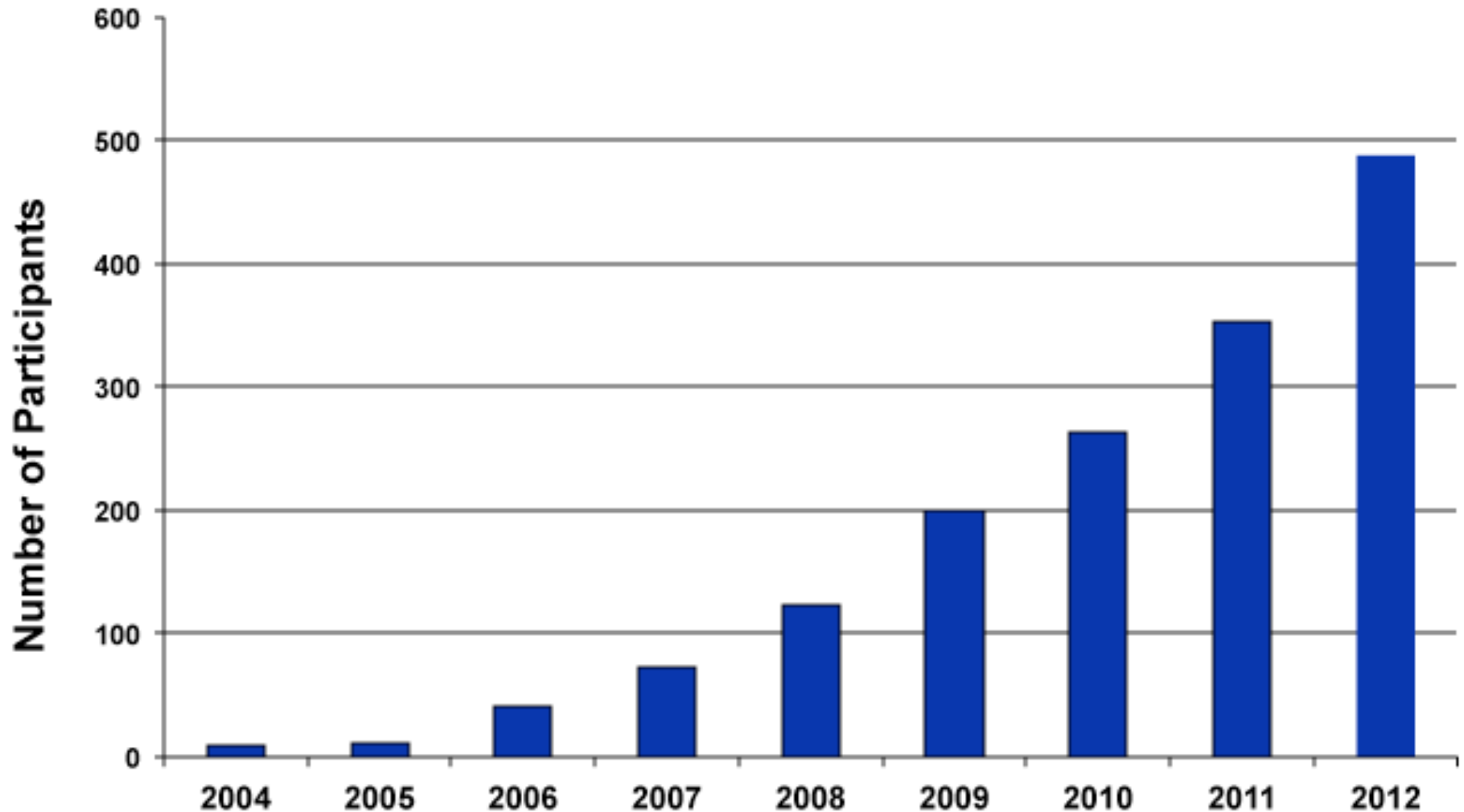
Getting Started with Federated Identity Management
Wednesday, November 13, 2013
San Francisco, CA

Where do I start?



InCommon 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.

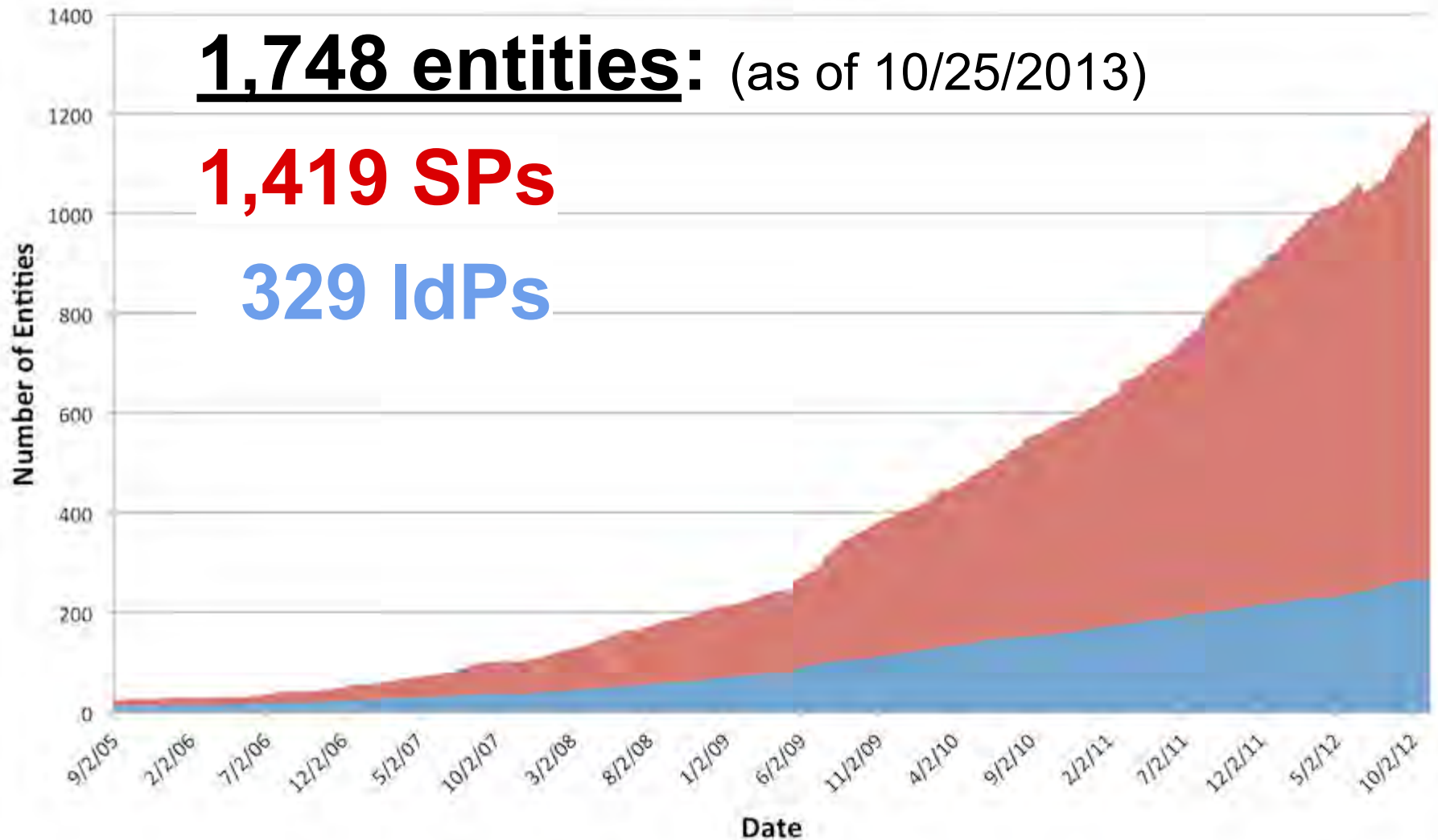
InCommon Participant Growth



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

InCommon Metadata Entity Growth

■ Number of IdPs ■ Number of SPs



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

The screenshot shows the InCommon website interface. At the top, the browser address bar displays "www.incommon.org/index.html". The main header features the InCommon logo on the left, the text "InCommon is operated by Internet2" with the Internet2 logo on the right, and navigation links for "Join InCommon", "About", and "Participants". A search bar is located below these links. A row of five green buttons is displayed: "Where do I start?", "Federation", "Certificates", "Assurance", and "Multifactor". The "Federation" button is highlighted with a white speech bubble. Below this row, a paragraph states: "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." Underneath the paragraph is the InCommon Federation logo, which includes the text "InCommon FEDERATION" and five stars. To the right of the logo is a grid of links organized into three columns: "Federation Manager Login", "Resources for Site Admins", "Password Reset", and "Changing Exec/Site Admin" in the first column; "Recommended Practices", "Technical Guide", "Official Documents", and "InCommon Participants" in the second column; and "Assurance", "Case Studies", "Federation Basics", and "InCommon Affiliates" in the third column. The footer of the browser window shows the URL "www.incommon.org/index.html".

InCommon is operated by **Internet2**

InCommon®

[Join InCommon](#) [About](#) [Participants](#)

[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

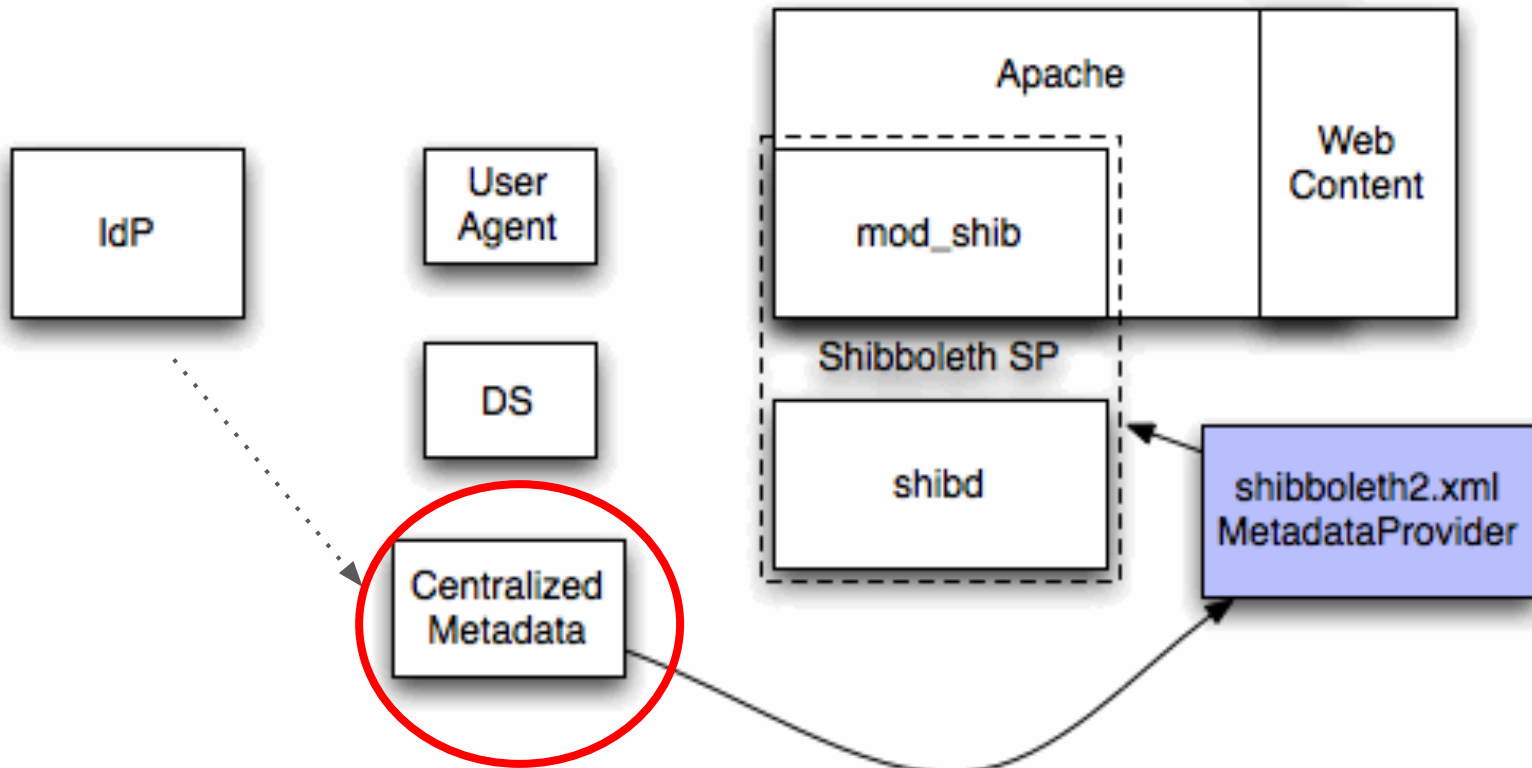
- [Federation Manager Login](#)
- [Resources for Site Admins](#)
- [Password Reset](#)
- [Changing Exec/Site Admin](#)
- [Recommended Practices](#)
- [Technical Guide](#)
- [Official Documents](#)
- [InCommon Participants](#)
- [Assurance](#)
- [Case Studies](#)
- [Federation Basics](#)
- [InCommon Affiliates](#)

www.incommon.org/index.html

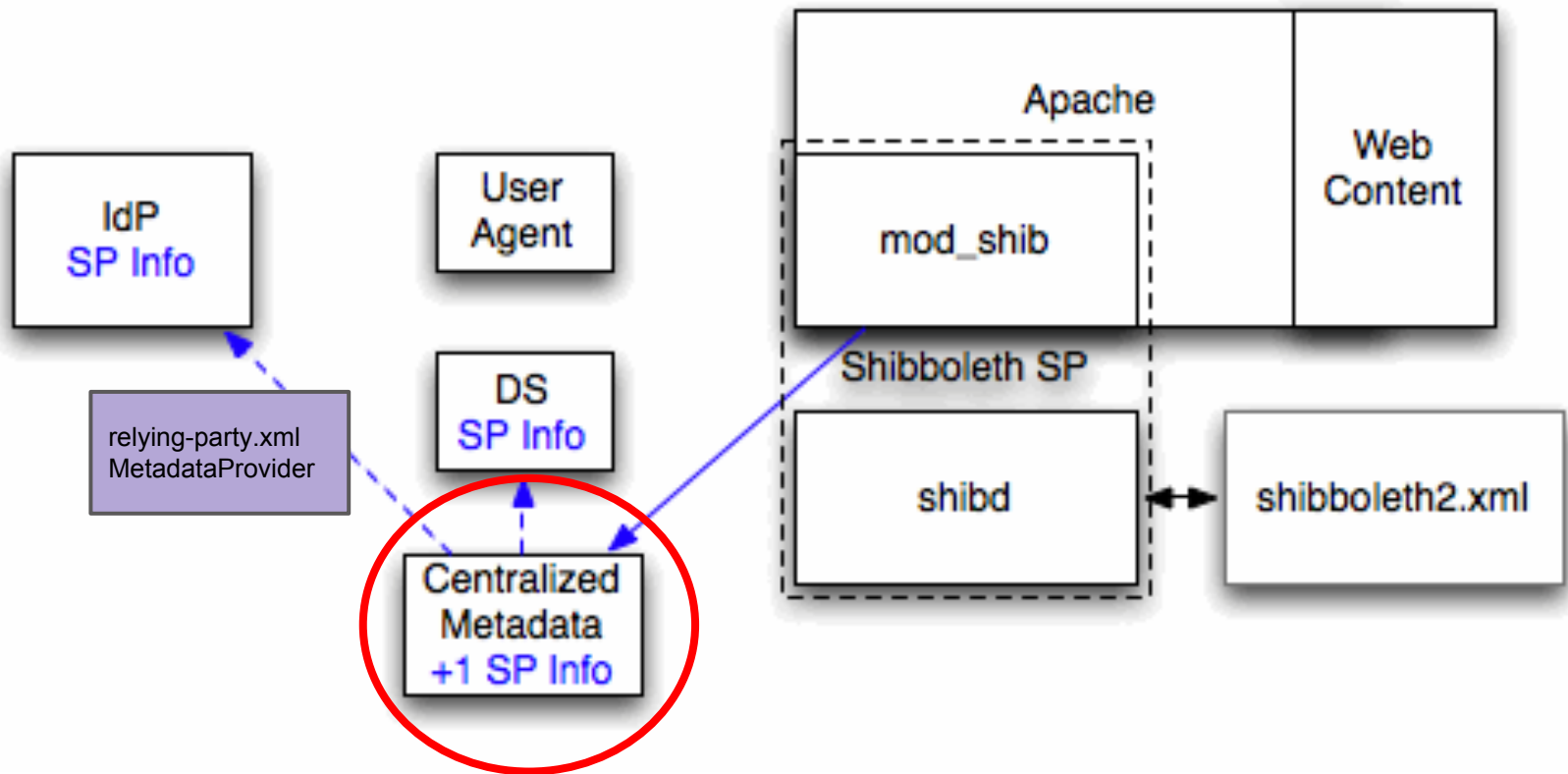
InCommon[®] Metadata: the technical glue that enables federating

- 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



IdP Recognizes SPs Via Metadata



InCommon Metadata - 100,000 Foot View

Mozilla Firefox

http://wayf.inc...n-metadata.xml
wayf.incommonfederation.org/InCommon/InCommon-metadata.xml

InC's Signed Metadata Lives Here

```
- <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>berrj@lafayette.edu</EmailAddress>
</ContactPerson>
```

Optional UI Info

How to communicate with the IdP

Janemarie is the technical contact for Lafayette College's IdP

Managing Your InCommon[®] Metadata

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



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

[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>

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: SP Server Software:

OR

EntityID*: (example, "https://service.example.org/shibboleth", [more...](#))

User Interface Elements and Requested Attributes: *

User Interface Elements: ([Help](#))

* SP Display Name:

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:

Discovery Response:

Index:	1
Location URL:	https://ncedcloud.mcnc.org/Shibboleth.sso/Login
Index:	2
Location URL:	

Assertion Consumer Service: *

Type/Profile:	SAML 2.0 HTTP-POST
Location URL:	https://ncedcloud.mcnc.org/Shibboleth.sso/SAML2/POST
Type/Profile:	SAML 2.0 HTTP-POST-SimpleSign
Location URL:	https://ncedcloud.mcnc.org/Shibboleth.sso/SAML2/POST-S
Type/Profile:	SAML 2.0 HTTP-Artifact
Location URL:	https://ncedcloud.mcnc.org/Shibboleth.sso/SAML2/Artifact
Type/Profile:	SAML 2.0 PAOS
Location URL:	https://ncedcloud.mcnc.org/Shibboleth.sso/SAML2/ECP
Type/Profile:	SAML 1.1 Browser/Post
Location URL:	https://ncedcloud.mcnc.org/Shibboleth.sso/SAML/POST
Type/Profile:	SAML 1.1 Browser/Artifact
Location URL:	https://ncedcloud.mcnc.org/Shibboleth.sso/SAML/Artifact

Single Logout Services:

Profile/Binding Type:	SAML 2.0 HTTP-POST
-----------------------	--------------------

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

Digital Certificate*:

```
-----BEGIN CERTIFICATE-----  
MIIC/TCCAeWgAwIBAgIJAP/VOyOnerX1MA0GCSqGSIb3DQEBBQUAMBOxGzAZBgNV  
BAMTEm5jZWRjbG91ZC5tY25jLm9yZzAeFw0xMzA5MjcOTQ5NDNaFw0yMzA5MjUx  
OTQ5NDNaMB0xGzAZBgNVBAMTEm5jZWRjbG91ZC5tY25jLm9yZzCCASIwDQYJKoZI  
hvcNAQEBBQADggEPADCCAQoCggEBAM2EcQHENn94+GQTaGQJpg4EnbKnblwtTkVz  
eX3JDfhK5OfzJ4AnbCYddmd81axFAz2cj7vLPBc91NWCT3wDK2Ga8BZldDIA3m6  
zpo5T6EgAdzn9by3+ahf6P7PKWNqFwZgt83eR4rpZtIR0ry59NGhLLynFexSXJrF  
+BRINyc8TLbGi5nlZrYVAEfUVzgpTrsfaKyF7DMYAyO4o70qjosKymtjW5heJ6hk  
Jly0IaQ3Nw4RFIPp2Y0tz+YgRlQpzakUr2nM6EpwPc17tM4CT22/+cEEpvkCTWcg  
snb3M/9Wt1B3h4DpxAXIozElKDR1whJT0E4akIZ8mqLsHiLBVPkCAwEAAANAMD4w  
HQYDVR0RBBywFIIISbmNlZGNSb3VkLm1jbmMub3JnMB0GA1UdDgQWBBS9qJOT24oF  
7+PSH5czURLtkLkEPjANBqkqhkiG9w0BAQUFAAOCAQEAJuttmX+RUvnognx2Zpyx  
q4XbjOr4JwDhtwhudOYmKrijGDVp9ubMHhT8nKFBx6HWt1AtyGVLWpeTPe0MMXTs7  
aezS9vZaZq9qghmfikN95RpNmG1Fdq1PPwramEwJUT6Rpbs2J6Wqz6VH9kmnUbeU  
azvyoKLDkiKWGgo8SHFBkF2oH8lHhquU7t7WdhZbSiBOezOhipSGFQncv9V1EhTo  
sgCw8wus9WCrkh+/pnUtRSyDpQk1lJ7FQQxi1NMRBbM9X5rhBCFms0QG0Xy/wE8O  
etY30lvEolzIQgkI40G1If1HNCUGx5luX2DPzm6iVpUhCSzdtuvNbJu02tNZ75Pt  
JA==  
-----END CERTIFICATE-----
```

I understand and acknowledge that InCommon does not verify the information contained in this certificate or in any certificate within the federation metadata.

Contacts*:

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

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
URL: <https://ncedcloud.mcnc.org/Shibboleth.sso/SAML2/POST-SimpleSign>

Final
Review
Before
Submit

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: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:2.0:bindings:HTTP-POST"
        <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:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>
    </SPSSODescriptor>
  </EntityDescriptor>
```

MIIC/TCCAeWgAwIBAgIJAP/VOyOneRX1MA0GCSqGSIb3DQEBBQUAMB0xGzAZBgNV

BAMTEm5jZWRjbG91ZC5tY25jLm9yZzAeFw0xMzA5Mjc0OTQ5NDNaFw0yMzA5MjUx

OTQ5NDNaMB0xGzAZBgNVBAMTEm5jZWRjbG91ZC5tY25jLm9yZzCCAS1wDQYJKoZI

hvcNAQEBBQADggEPADCCAQoCggEBAM2EcQHEnn94+GQTaGQJpg4EnbKnblwtTkVz

eX3JDfhK5OfzJ4AnbCYddmd81axFAz2cj7vLPBc91NWCT3wDK2Ga8BZldDIA3m6

zpe5F6EgAdgn9bu3+ahf6P7BKWNgFwZat82eP4rre7+TP0ru59NChILunEoxSYIre

InCommon Site Admin: MCNC

Home

x.509 Certificates (IdP only)

Identity Provider Metadata Wizard

Service Provider Metadata Wizard

Delegated Administrators

POPs

Your Account

Documentation

FM Change Log

Your update has been submitted. Requests are typically processed within one Internet2 business day.

Your Service Provider

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:

Index: 1
 Type: urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST

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

Inbox

Metadata update requ...

Get Mail Write Chat Address Book Tag Quick Filter

Search... <⌘K>

From do-not-reply@incommon.org

Reply

Reply All

Forward

Archive

Junk

Delete

Subject Metadata update request confirmation for MCNC

4:37 PM

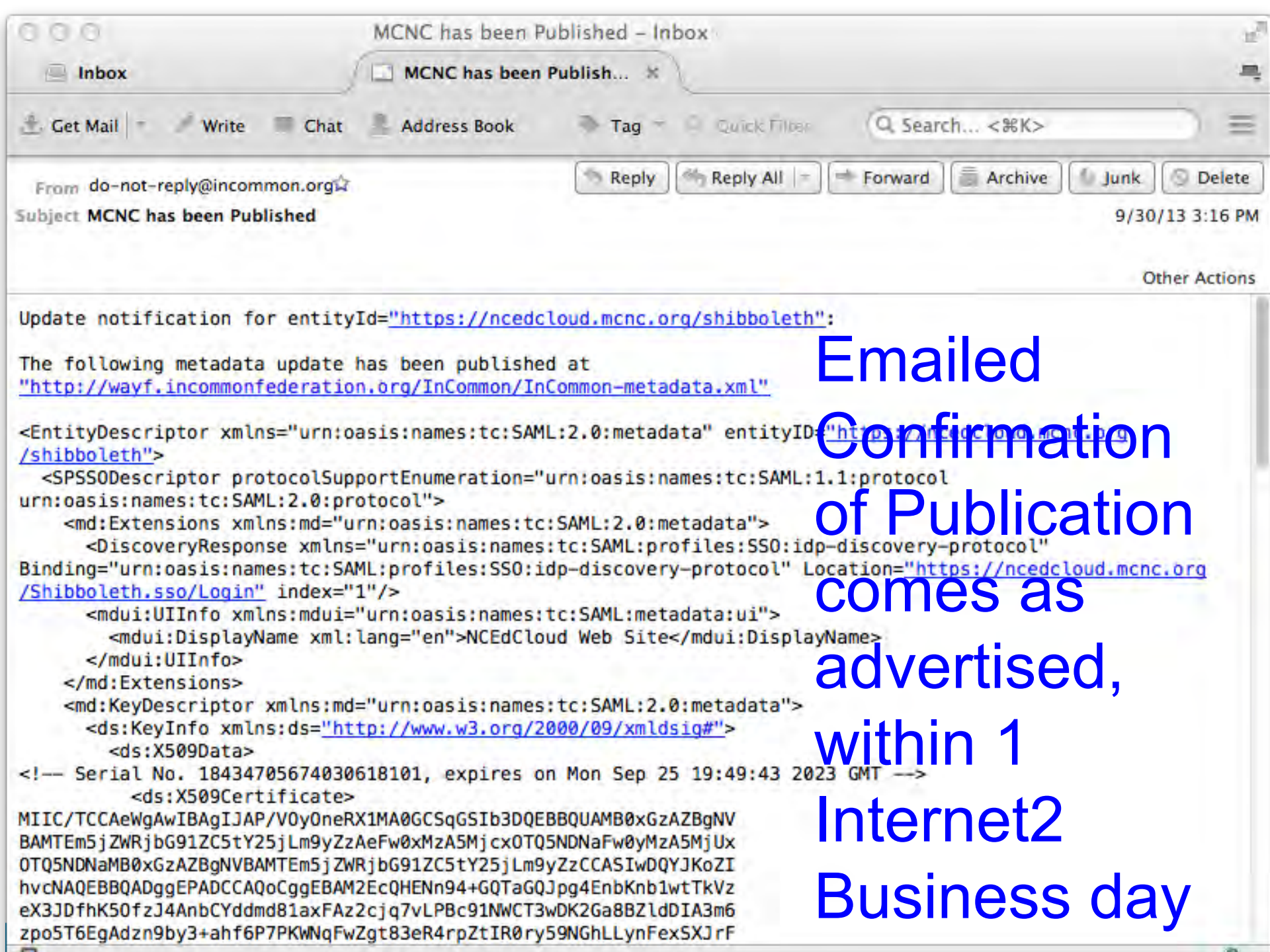
Other Actions

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/V0y0neRX1MA0GCSqGSIb3DQEBBQUAMB0xGzAZBgNV
BAMTEm5jZWRjbG91ZC5tY25jLm9yZzAeFw0xMzA5Mjc0OTQ5NDNaFw0yMzA5MjUx
OTQ5NDNaMB0xGzAZBgNVBAMTEm5jZWRjbG91ZC5tY25jLm9yZzCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAM2EcQHENn94+GQTaGQJpg4EnbKn1wtTKVz
eX3JDfhK50fzJ4AnbCYddmd81axFAz2cj7vLPBc91NWCT3wDK2Ga8BZldDIA3m6
zpo5T6EgAdzn9by3+ahf6P7PKWnqFwZgt83eR4rpZtIR0ry59NGhLLynFex5XJrF
+BRINyc8TLbG15nLzrYVAEfUVZgptrsfaKyF7DMYAy04o70qjosKymtjW5heJ6hk
J1y0IaQ3Nw4RFIPp2Y0tz+ygRlQpzakUr2nM6EpwPc17tM4CT22/+cEEpvkCTWcg
snb3M/9WtLB3h4DpxAXIozE1KDR1whJT0E4akIZ8mqLshILBVPkCAwEAANAMd4w
HQYDVR0RBBywFIIISbmlZGNsb3Vklm1jbmMub3JnMB0GA1UdDgQWBBS9qJ0T24oF
7+Psh5czURLtkLKEPjANBgkqhkiG9w0BAQUFAA0CAQEAJuttmX+RUvnoGnx2Zpyx
q4XbjOr4JwDhtwhudOYmKrjGDVp9ubMHHt8nKFBx6HwtLAtyGVLWpeTpe0MMXts7
aezS9vZaZq9qghmfikN95RpNmG1Fdq1PPwramEwJUT6Rpbs2J6Wqz6VH9kmmUbeU
azvvoKLDkiKWGgo8SHFBkF2oH8lHhquU7t7WdhZb5iB0ez0hipSGFQncv9V1EhTo
sgCw8wus9WCrk+/pnUtrSyDpQklLJ7FQqxi1NMRBbM9X5rhBCFmS0QG0Xy/wE80
etY30lvEo1zIQgKI40GLI1fHNCUGx5luX2DPzm6iVpUhcSzdTuvNbJu02tNZ75Pt
JA==
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
  </SPSSODescriptor>
</EntityDescriptor>
```

Confirmation
of submission
comes right
away by email



From do-not-reply@incommon.org

Reply Reply All Forward Archive Junk Delete

Subject MCNC has been Published

9/30/13 3:16 PM

Other Actions

Update notification for entityId=["https://ncedcloud.mcnc.org/shibboleth"](https://ncedcloud.mcnc.org/shibboleth):

The following metadata update has been published at ["http://wayf.incommonfederation.org/InCommon/InCommon-metadata.xml"](http://wayf.incommonfederation.org/InCommon/InCommon-metadata.xml)

<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityId=["https://ncedcloud.mcnc.org/shibboleth"](https://ncedcloud.mcnc.org/shibboleth)>
 <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"](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#"](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/V0y0neRX1MA0GCSqGSIb3DQEBBQUAMB0xGzAZBgNV
 BAMTEm5jZWRjbG91ZC5tY25jLm9yZzAeFw0xMzA5MjcxOTQ5NDNaFw0yMzA5MjUx
 OTQ5NDNaMB0xGzAZBgNVBAMTEm5jZWRjbG91ZC5tY25jLm9yZzCCASIwDQYJKoZI
 hvcNAQEBBQADggEPADCCAQoCggEBAM2EcQHENn94+GQTaGQJpg4EnbKnblwtTkVz
 eX3JDfhK50fzJ4AnbCYddmd81axFAz2cjq7vLPBc91NWCT3wDK2Ga8BZldDIA3m6
 zpo5T6EgAdzn9by3+ahf6P7PKWNqFwZgt83eR4rpZtIR0ry59NGhLLynFex5XJrF

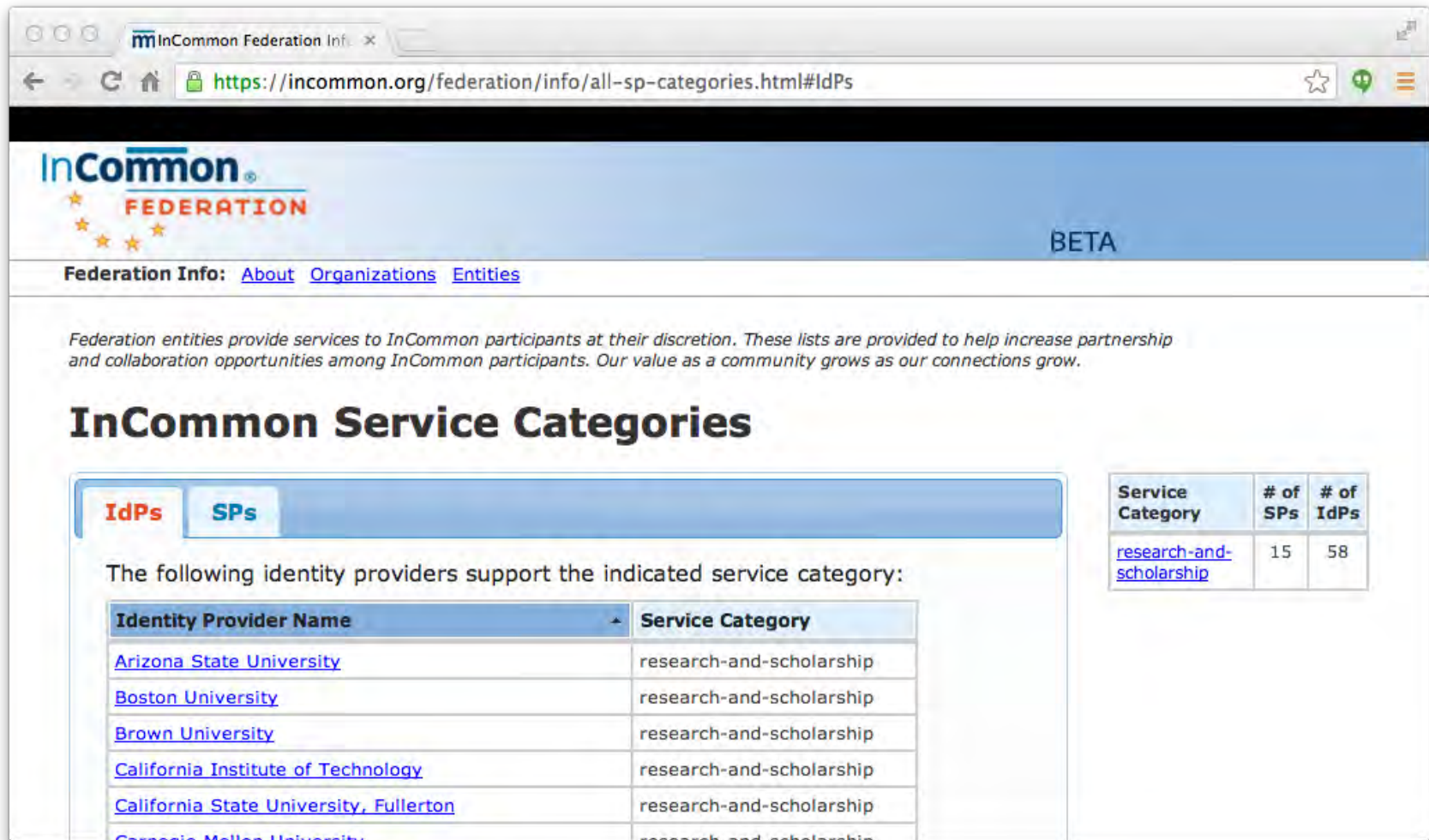
Emailed
Confirmation
of Publication
comes as
advertised,
within 1
Internet2
Business day

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)



The screenshot shows a web browser window with the URL <https://incommon.org/federation/info/all-sp-categories.html#IdPs>. The page header includes the InCommon Federation logo and a "BETA" label. Below the header, there are navigation links for "About", "Organizations", and "Entities". A paragraph of text explains the purpose of the federation entities. The main heading is "InCommon Service Categories". There are two tabs: "IdPs" (selected) and "SPs". Below the tabs, a text block states: "The following identity providers support the indicated service category:". To the right, a small table summarizes the data. Below the text, a larger table lists the identity providers and their associated service categories.

InCommon Federation BETA

Federation Info: [About](#) [Organizations](#) [Entities](#)

Federation entities provide services to InCommon participants at their discretion. These lists are provided to help increase partnership and collaboration opportunities among InCommon participants. Our value as a community grows as our connections grow.

InCommon Service Categories

IdPs **SPs**

The following identity providers support the indicated service category:

Identity Provider Name	Service Category
Arizona State University	research-and-scholarship
Boston University	research-and-scholarship
Brown University	research-and-scholarship
California Institute of Technology	research-and-scholarship
California State University, Fullerton	research-and-scholarship
Carnegie Mellon University	research-and-scholarship

Service Category	# of SPs	# of IdPs
research-and-scholarship	15	58

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




(Janemarie case study?)

The screenshot shows the InCommon website interface. At the top right, it says "InCommon is operated by Internet2" with the Internet2 logo. The main navigation includes "Join InCommon", "About", and "Participants". A search bar is present. Below the navigation is a row of five green buttons: "Where do I start?", "Federation", "Certificates", "Assurance", and "Multifactor". The "Certificates" button is highlighted with a white speech bubble pointing to it. Below this row, a paragraph states: "The InCommon Certificate Program provides unlimited certificates, for all of your domains, for one fixed annual fee. This includes SSL, extended validation, client (personal), and code signing certificates." Below the paragraph is a grid of links. On the left is the InCommon CERTIFICATES logo. The links are organized into three columns:

Subscribe	Official Documents	Support
Certificate Manager Login	Client Certificates	Subscribers
Password Reset	Code Signing Certificates	Resources/Documentation
Changing Exec/RAO	EV Certificates	FAQ

Assurance


InCommon is operated by **Internet2** 

InCommon[®]

[Join InCommon](#) [About](#) [Participants](#)

[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.

 **ASSURANCE**

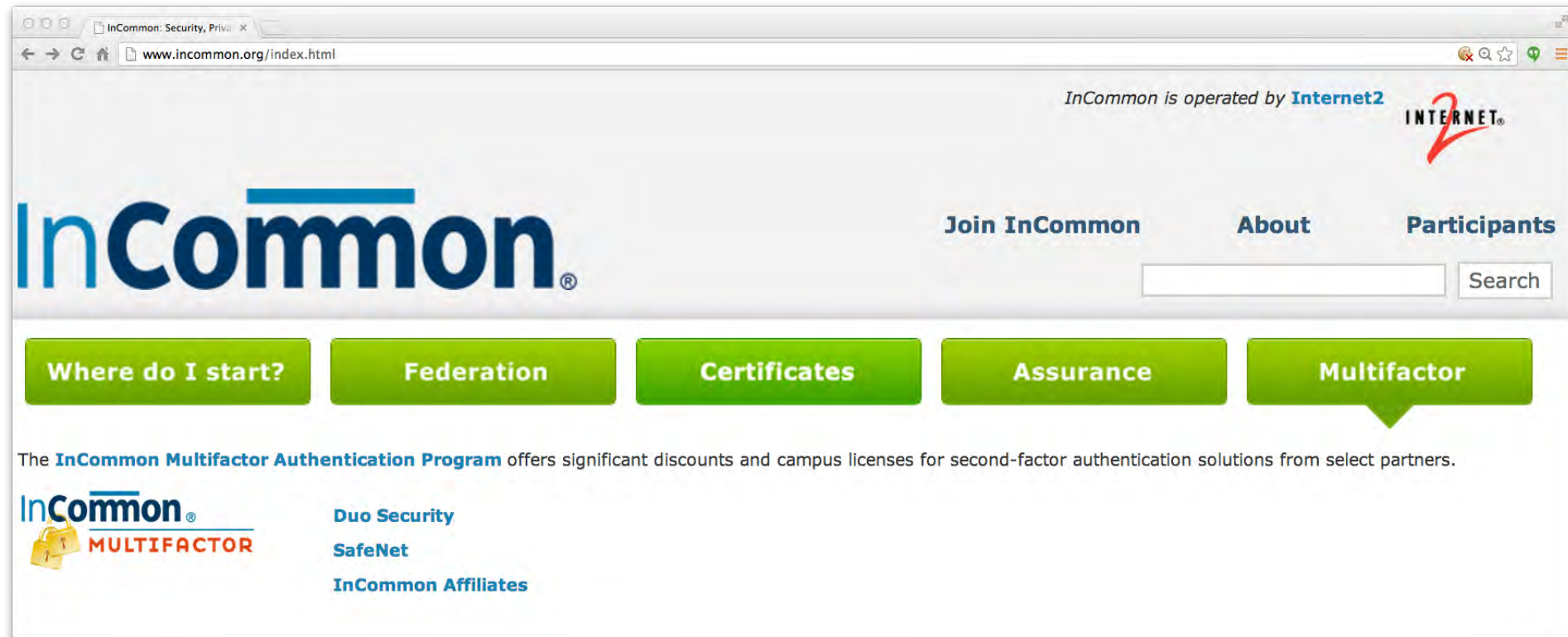
- [Subscribe](#)
- [Assurance Advisory Committee](#)
- [FAQ](#)
- [Assurance Fee Schedule](#)
- [Assurance for Identity Providers](#)
- [Assurance for Service Providers](#)
- [Assurance Glossary](#)

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



The screenshot shows the InCommon website interface. At the top, it says "InCommon is operated by Internet2" with the Internet2 logo. The main navigation includes "Join InCommon", "About", and "Participants". A search bar is present. Below the navigation is a row of green buttons: "Where do I start?", "Federation", "Certificates", "Assurance", and "Multifactor". The "Multifactor" button is highlighted with a white speech bubble. Below this, a text block states: "The InCommon Multifactor Authentication Program offers significant discounts and campus licenses for second-factor authentication solutions from select partners." Underneath, there is a logo for "InCommon MULTIFACTOR" and a list of partners: "Duo Security", "SafeNet", and "InCommon Affiliates".

InCommon is operated by **Internet2**

InCommon®

[Join InCommon](#) [About](#) [Participants](#)

[Where do I start?](#) [Federation](#) [Certificates](#) [Assurance](#) [Multifactor](#)

The **InCommon Multifactor Authentication Program** offers significant discounts and campus licenses for second-factor authentication solutions from select partners.

InCommon®
MULTIFACTOR

- [Duo Security](#)
- [SafeNet](#)
- [InCommon Affiliates](#)

Authentication Solutions



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

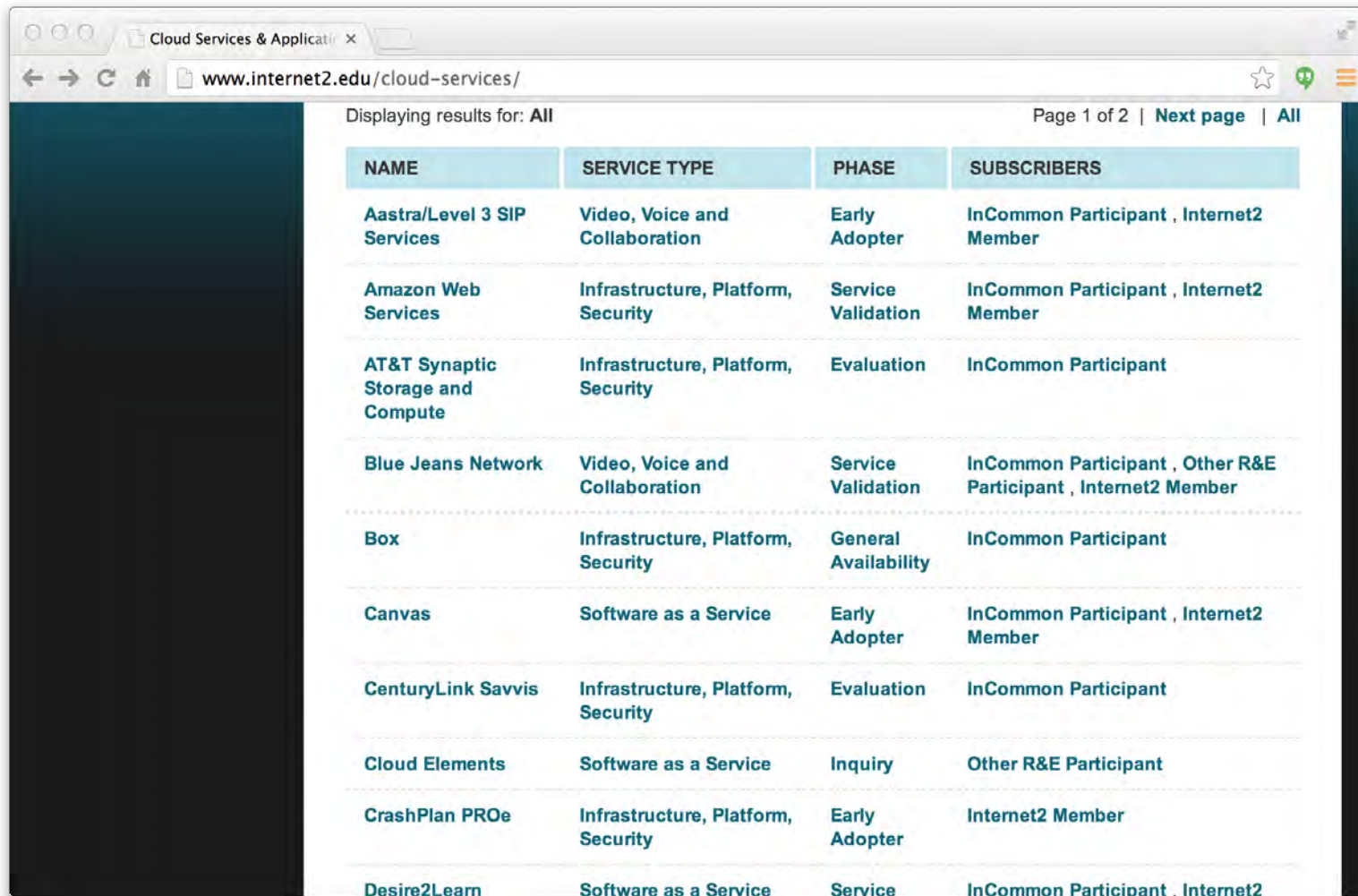


THE
DATA
PROTECTION
COMPANY



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

Netplus - Cloud Service Portfolio Utilizing InCommon Infrastructure



The screenshot shows a web browser window with the address bar displaying "www.internet2.edu/cloud-services/". The page content includes a table of cloud services. Above the table, it says "Displaying results for: All" and "Page 1 of 2 | Next page | All". The table has four columns: NAME, SERVICE TYPE, PHASE, and SUBSCRIBERS. The rows list various services such as Aastra/Level 3 SIP Services, Amazon Web Services, AT&T Synaptic Storage and Compute, Blue Jeans Network, Box, Canvas, CenturyLink Savvis, Cloud Elements, CrashPlan PROe, and Desire2Learn.

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

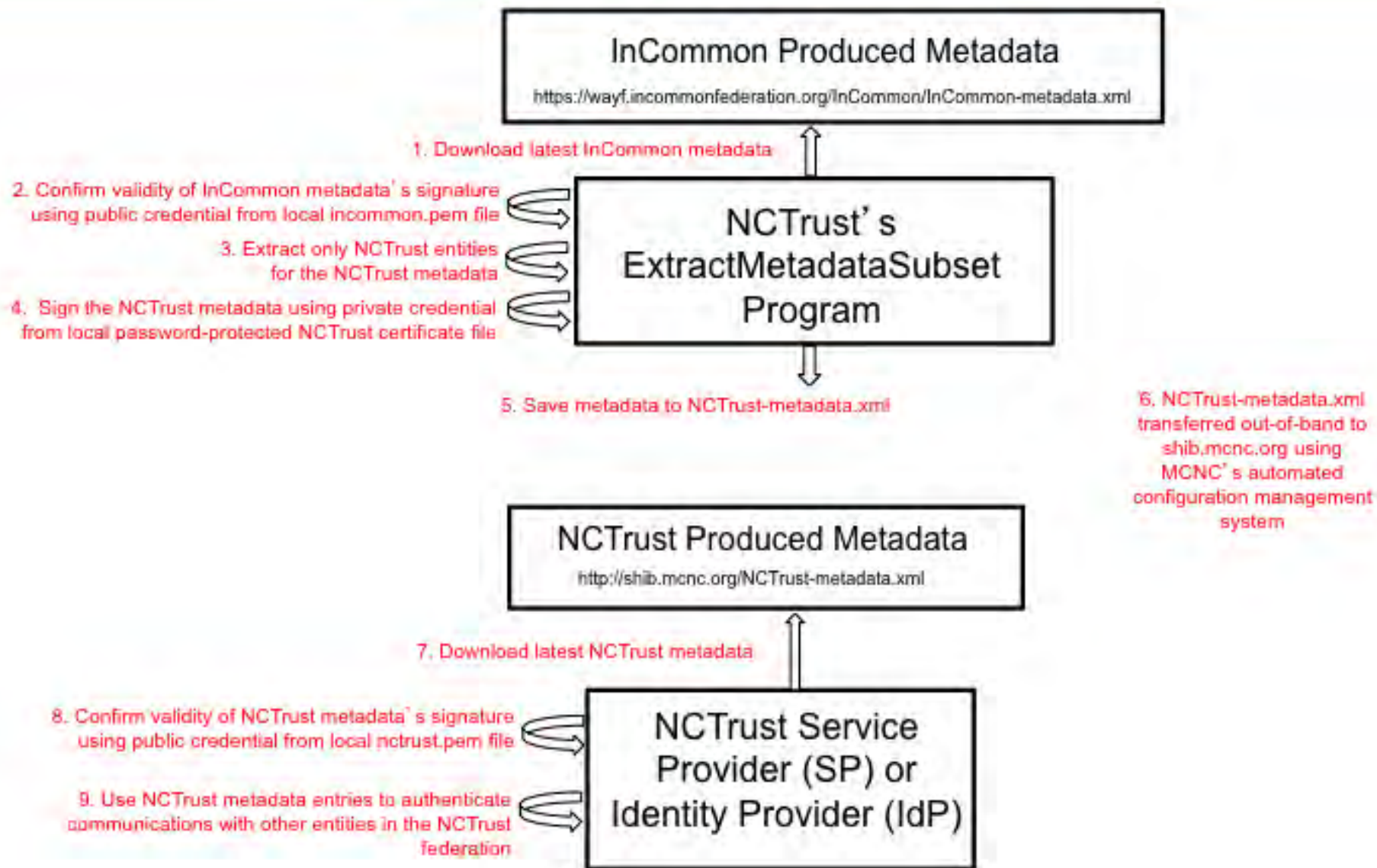
The NCTrust Federation was a pilot project to model a K-20 federation for the state of North Carolina, and included participants from:

- 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®



NC
DPI



North Carolina
Learning Object Repository



THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL



UNIVERSITY of NORTH CAROLINA
GREENSBORO

UNC-GA is a "Friend of NCTrust"



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?