



Federal Student Aid

Software Developers Conference

August 3, 2006



START HERE
GO FURTHER
FEDERAL STUDENT AID



eAuthentication in Higher Education

Tim Bornholtz



START HERE
GO FURTHER
FEDERAL STUDENT AID



What is eAuthentication?

- What is eAuthentication?
- What is a Federation?
- What is Transitive Trust?
- How are they different?





Let's Start with A Math Lesson

- Transitive property of equality

If $a = b$ and $b = c$

Then $a = c$





Translate That To Trust

Christopher trusts Nicholas
Nicholas trusts Stephanie

Christopher will (usually) trust Stephanie





Boundaries of Trust

- These trust relationships can only go so far.
- We probably would not trust a friend of a friend of a friend of a friend.
- There are not indefinite levels of trust.
- The boundaries of your trust make up the Federation.





Federation

- A Federation is a group of organizations that have agreed to trust each other.
- All members of the federation trust all other members within the federation.
- Separate agreements with each and every member are not necessary.





Rules of a Federation

- All members of a federation agree to abide by the rules of the federation.
- Each federation has some sort of “steering committee” that decides on the rules:
 - Legal rules – who can participate and what can they do within the federation.
 - Technical rules – technical infrastructure and specifications necessary to communicate with other federation members.





A Federation Must Provide

- Privacy
- Strength of identity proof
- Regulation / policies
- Ease of use
- Audit
- Indemnification





So What Is eAuthentication?

- eAuthentication is a Federation of US government agencies and private sector organizations.
- GSA is coordinating the federation
 - Determined the legal policies required for joining the network.
 - Specified the technical requirements to participate.





Federal eAuthentication

- Leverages many existing NIST standards
- Set standards for
 - Identity proofing
 - SAML bindings
 - Credential Assessment Framework
 - Risk Assessment
- Interoperability lab
- As of 6/30/06
 - Sixteen agencies signed up as Relying Party
 - Twelve Relying Parties in production
 - Six Credential Service Providers





Electronic Authentication Partnership

- EAP is a multi-industry partnership that is bringing together both the public and private sector.
- Replacing custom bilateral agreements with a uniform set of rules.
- Developing a standard evaluation process for credentials and setting uniform approaches and minimum requirements for authentication.





Authentication vs. Authorization

- Members of a federation determine what to trust and for what purposes on an application level basis.
- Authenticate locally.
- Passwords **never** go over the wire.





eAuthentication Levels of Risk

- Each application needs to determine its level of risk.
 - A public service to reserve campgrounds is a very low risk.
 - A financial application for grants and loans is a higher risk, but there is no risk of loss of life.
 - The security codes to access a nuclear warheads is a very very high risk.





eAuthentication Credential Strength

- NIST has defined four levels of user authentication in M-04-04.
 - Level 1: little or no confidence
 - Level 2: Some confidence
 - Level 3: High confidence
- Level 4: Very high confidence
- These are based on the strength of identity proofing and strength of credentials.
 - Something you know (e.g. password)
 - Something you have (e.g. ID badge)
 - Something you are (e.g. fingerprint)





Shibboleth

- Shibboleth is open source software which provides Web Single SignOn (SSO).
- Uses Security Assertion Markup Language (SAML) as defined by OASIS.
- Access control based on attributes
 - Users can usually decide which attributes are released to each service provider.
 - Each service provider can specify a minimum set of requirements necessary to grant access.





InCommon

- Federation to support a common framework to access online resources in support of education and research.
- Uses Shibboleth as the federating software.
- Provides standard conduct for all members to collaborate.
- Economies of scale for contractual agreements.





Members of InCommon

- The Ohio State University
- The University of Chicago
- University of California, Los Angeles
- University of California, Office of the President
- University of California, Riverside
- University of California, San Diego
- University of Rochester
- University of Southern California
- University of Virginia
- University of Washington
- Case Western Reserve University
- Cornell University
- Dartmouth
- Georgetown University
- Internet2
- Miami University
- Napster, LLC
- OhioLink - The Ohio Library & Information Network
- Penn State
- Stanford University
- SUNY Buffalo





Other Shibboleth Federations

- University of Maryland – 16 campuses
- University of Texas – 23 campuses
- University of California system
- California State system
- The Ohio State University





Prominent International Federations

- FEIDE – Norway
 - Educational sector in Norway.
- HAKA Federation – Finland
 - Identity federation of Finnish universities, polytechnics and research institutions
- SDSS – United Kingdom
 - Federation for managing access to UK academic online resources
- SWITCH – Switzerland
 - Eleven universities - more than 140,000 users
 - More than 80 resources - primarily in the field of e-learning





Inter-Federation Models

- Some organizations will join several federations and manage them as distinct groups.
- A more streamlined approach, though more difficult, is to create peering arrangements between the distinct federations.
 - These peering arrangements allow all members of one federation to access the resources of the other federation.
 - Some peering arrangements may be bilateral – meaning the sharing works both ways.





InCommon and eAuthentication

- InCommon and the federal eAuthentication are working on a peering agreement to allow members to interoperate
 - High priority effort by PMO
 - One group working on policy
 - One group working on the technology
 - Hoping for agreement by 9/30/06
 - Looking to demo in 12/06





InCommon and eAuthentication Phases

- Phase 1)
 - Use the existing SAML 1.0 profile
 - NSF FastLane
 - Department of Education systems
 - Small number of campus users
- Phase 2)
 - Upgrade to the SAML 2.0 profile
 - More agency applications and more agencies
 - More campuses





Horizontal vs. Vertical Federations

- Most federations take a horizontal slice of the application space
 - The federation deals with authentication and authorization but does not care about the actual business process.
- Some federations take a vertical slice of a business process
 - The federation deals with one specific line of business or one specific application within a line of business.



A Vertical Federation for Student Aid

- Meteor is an effort to provide financial aid professionals and students with online aggregated financial aid award information from various industry participants.
- Meteor enables students to obtain detailed, real time student aid information directly from the web.
- Meteor enables the financial aid professional to supplement their counseling services.



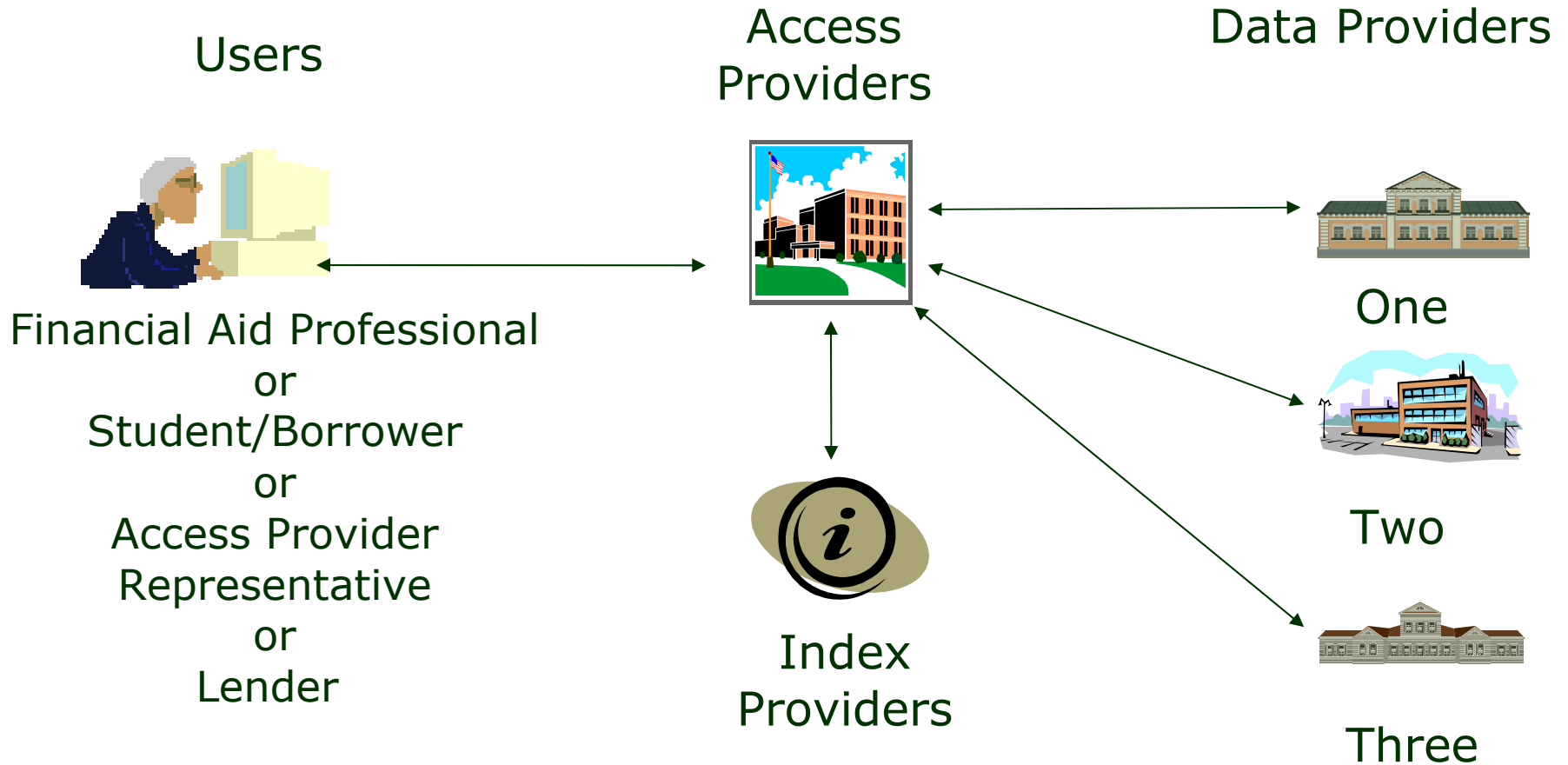
Types of Data Available

- FFELP
- Alternative/Private Loans
- State Grants & Scholarships (Summer 2006)
- Perkins (In development)
- Direct Loans (Planned)
- Pell Grants (Planned)





The Meteor Process





Authentication Process:

- Student logs into Access Provider site (i.e. school, lender, servicer or guarantor)
- Access Provider follows their local authentication procedures, assigns a role and retrieves the appropriate assurance level from the Meteor Registry
- Access Provider builds the security assertion
 - AP Unique ID
 - User Role
 - End User Identifier
 - Authentication Process ID
 - Assurance Level





Authentication Process:

- Access Provider digitally signs the request and queries the Index Provider
- Index Provider validates the provider (digital certificate) against the Registry;
- Index Provider builds a response message and digitally signs and sends the request to the Access Provider





Authentication Process:

- Access Provider receives the response and validates the provider against the Registry; validates the digital signature; validates assurance levels for Data Provider requirements; builds, signs, and sends the request message
- The same validation process continues for the Data Provider's receipt and response and the Access Provider's receipt and display of the Meteor messages.





Clearinghouse as Index Provider

- 100% of FFELP guarantee volume
- Over 5.6 million Direct Loan Program accounts
- Over 13.2 million FFELP servicer accounts
- Over 1.6 million Perkins/Private/Alternative Loan servicer accounts (including some managed by schools themselves)





Meteor Customization

- Meteor screens can be customized to blend with the service providers current web services
- Meteor allows a service provider to customize the use of the data provided in the Meteor Network
 - e.g. MYF Exit Counseling application
 - Not a standard Meteor implementation
 - Customized screens
 - Further integration is possible!
- Meteor software can be used in other internal applications with approval from the MAT





Reliability and Security

- Data is sent directly from the data provider's system and is not altered in any way within the Meteor software
- All data is electronically transmitted securely using SSL encryption
- Independent audit showed no serious vulnerabilities with the software





Building Trust and Integrity

- The Meteor Advisory Team sought input and expertise regarding privacy and security from the sponsoring organizations and the NCHELP Legal Committee.
- Analysis was provided in relation to GLB and individual state privacy laws.
- The analysis revealed that Meteor complied with GLB, FERPA, and known state privacy provisions.





Creating the Federation

Challenges and Opportunities

- Policy
 - Provider eligibility
 - Security and privacy
 - Removal from the network
- Consensus Building
 - Over 40 providers (challenge!)
- Collaboration
 - Over 40 providers (opportunity!)





Lessons learned

- The policy work is much harder than the technical work.
- The legal staff at every member will need to review the policies.
- Usually need to be educated:
 - Why federations work
 - Why they are secure





Benefits of Federations

- Business process optimization.
- No need to manage large userid database.
- Get the authentication information from the very best source!





Possible Future Directions

- Identity Providers
 - College Board and ACT
 - More schools
 - FAMS vendors
- Service Providers
 - Department of Education
 - Lenders, Guarantors, Servicers
 - School Information Systems
 - Many many others





Questions, Comments, Suggestions





Contact Information

Tim Bornholtz

Phone: 540-446-8404

Email: tim@bornholtz.com

Web: <http://www.bornholtz.com>

Federal eAuthentication - <http://cio.gov/eauthentication>

Electronic Auth Partnership - <http://eapartnership.org>

InCommon - <http://incommonfederation.org>

Shibboleth - <http://shibboleth.internet2.edu>

Meteor - <http://nchelp.org/Meteor.htm>

