e-Authentication & Authorization
Presentation to the EA2 Task Force

March 6, 2007

What is Meteor?

- Web-based universal access channel for real-time inquiry of financial aid information
- Aggregated information to assist Financial Aid Professionals, students and borrowers with debt counseling and the aid process in general
- Collaborative effort of leading FFELP providers
- Freely available software and access to the network

The Meteor Project Components

- The Meteor Software
- The Meteor Network
- The Meteor Federation

Meteor Software Features

- Information from multiple data providers is aggregated in real-time to assist the FAP and the borrower with the financial aid process, repayment and default aversion.
- Meteor is a collaborative effort utilizing leading-edge technology and access is provided at no charge.

Meteor Software Features

- Access timely, student-specific financial aid information from multiple sources
- One-stop, common, online customer service resource

Types of Data Available

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

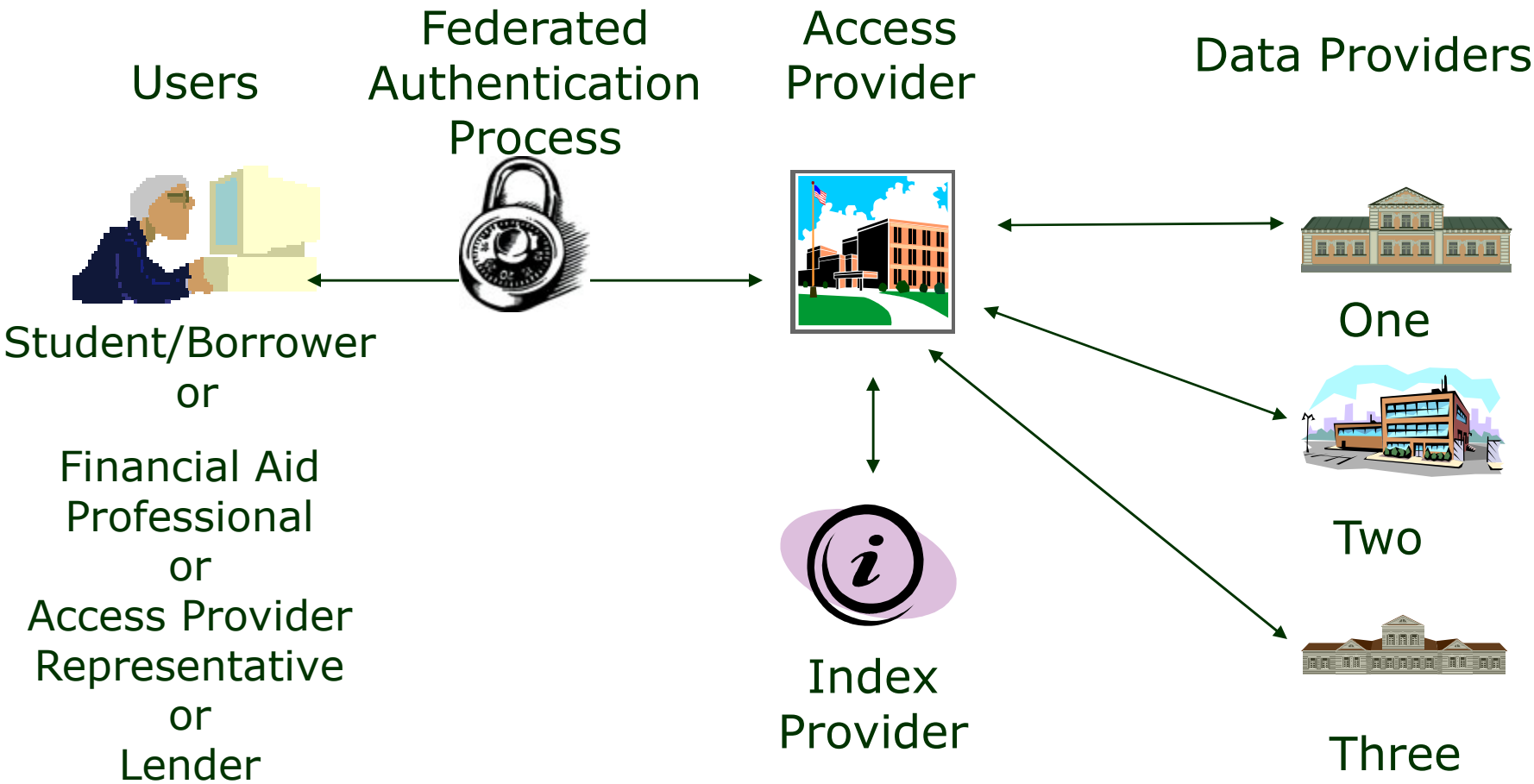
The Meteor Network

- Meteor
  - Federated Model: Transitive Trust
  - Multiple points of access
- User Roles
  - School
  - Student/Borrower
  - Customer Service Representatives
  - Lenders

Use of data approved by FSA

- FSA approval for use of real-time data
  - Collaborative effort to bring about change to the requirements for schools to solely rely on NSLDS
  - Allows schools to resolve discrepancies by using real time data that comes directly from the loan holders databases

The Meteor Process



E-Authentication

- The MAT worked with the Shibboleth project, a project of Internet2/Mace, in developing architectures, policy structures, practical technologies, and an open source implementation to support inter-agency sharing of web resources.
- Shibboleth project participants include Brown University, Ohio State, Penn State and many other colleges and universities.

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 Gramm-Leach-Bliley Act (GLBA), and individual state privacy laws.
- The analysis revealed that Meteor complied with both GLB and known state privacy provisions.

Building Trust and Integrity

- Federated model of authentication
  - Meteor Participant Certification
  - Conditions of Use
  - Authentication protocol review
  - Use of Data Exception Policy

Reliability and Security

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

Meteor's Authentication Objectives

- Provide a flexible, easy to implement authentication system that meets the needs of the provider organizations and their customers.

- Ensure compliance with the Gramm-Leach-Bliley Act (GLBA), federal guidelines, and applicable state privacy laws.

Meteor's Authentication Objectives

- Assure data owners that only appropriately authenticated end users have access to data.
- Ensure compliance to participant organizations internal security and privacy guidelines.

Authentication

- No central authentication process
- Utilizes transitive trust model
- Each Access Provider uses their existing authentication model (single sign-on)
- Level of trust assigned at registration

The Meteor Authentication Model

- Each Access Provider uses their existing authentication model (single sign-on)
- Meteor levels of assurance are assigned at registration
  - Level 0 (Unique ID)
  - Level 1 (Unique ID & 1 piece of validated public data)
  - Level 2 (Unique ID & 2 pieces of validated public data)
  - Level 3 (Unique/User ID & shared secret)
- Meteor Level 3 complies with the NIST Level 2

Meteor's Authentication Requirements

- User is required to provide an ID and a shared secret.
- Assignment and delivery of shared secret must be secure.
- Assignment of shared secret is based on validated information.
- Reasonable assurances that the storage of the IDs and shared secrets are secure.

E-Authentication Policies

- Access provider must ensure appropriate authentication for each end user and provide traceability back to that user
- Access provider must provide authentication policy to central authority
- Access provider must provide central authority with 30 day advance notice of changes to authentication policy
- Access provider must agree to appropriate use of data

The Meteor Authentication Process

- End user authenticates at access provider site or through a Meteor approved third party Authentication Agent
- Access provider creates authentication assertion (SAML)
- Access provider signs authentication assertion with digital certificate
- Control is passed to Meteor software

The Meteor Authentication Process

- Index and data providers verify assertion using the access provider's public key stored in the registry.
- End user is provided access to the aggregated data

SAML Assertion Attributes

- Role of end user
- Social Security Number
- Authentication Process ID
- Level of Assurance
- Opaque ID
- School OPEID (Summer 2007)

Current Status

- 1 Index Provider
- 20 Data Providers
- 15 Access Providers
- 1 Authentication Agent

Meteor Usage

- Meteor Usage
  - FAA Statistics
    - Usage has been increasing since FSA announcement about use of real time data
  - Borrower Statistics
  - Meteor…not just an inquiry network
    - In addition to providing access to and aggregation of financial aid award information, the Meteor software can also be used by organizations to enhance their current services.
      - MYF integration
      - Internal usage of the software at member organizations

Authentication and Authorization

- Authentication is the process of determining the identity of a user that is attempting to access a system.
- Authorization is the process of determining what types of activities are permitted.

Authentication and Authorization

- Once you have authenticated a user, they may be authorized different types of access or activity.
  - Meteor Roles
    - Financial Aid Professional
    - Student/Borrower
    - Customer Service
    - Lender

Authentication Process:

- Student logs into Access Provider site (i.e. school, lender, servicer or guarantor)
  - Access Provider authenticates student
  - Access Provider messages the Meteor Registry for validation, attaching the security assertion
  - Registry validates the provider and sends the request to the Meteor Index for processing.
  - The index identifies potential data providers who receive a message including the security assertion
  - Data providers return data to the access provider provided that the applicable authentication level meets their requirements.

What's Next?

- Continue to monitor the development of XML, transport and authentication standards
- Review of multi-layer authentication
- Clock synchronization across the network for timing out of assertions for additional security
- Alignment with the NIST levels of assurance

Contact Information

Tim Cameron
Meteor Project Manager
NCHELP
703-969-8565
meteor@nchelp.org