E-Authentication
...in Student Aid...

Can it:
• Deliver Service?
• Provide Value?
• Achieve Results?
Agenda

...the State of E-Authentication...

Definitions / Terminology / Standards  
Mike Sessa, PESC

FSA Update and Perspective  
Charlie Coleman, FSA

Industry Perspective  
Charles Miller, RIHEAA

School Perspective  
Nicholas Zinser, Northeastern University

Discussion...what does E-Authentication mean for all of us...???
...
Definitions and Terminology

- **Authentication** – is the process of identifying an individual*.

- **Authorization** – is the process of giving individuals access based on their identity (once they have been authenticated).

- **Identity** – is a unique name of a person, device, or the combination of both that is recognized by a system.

- **Security** – is a process or technique to ensure that data stored cannot be read or compromised by any individuals without authorization.
Definitions and Terminology

- **Privacy** – is freedom from unauthorized access.
- **Trust** – is firm reliance on integrity, ability, or character.
- **Federated Identity** – use of agreements, standards, and technologies, to make identity and entitlements portable across loosely coupled, autonomous identity domains. (Burton Group 8/30/04)
- **Transitive Trust** – circle of trust, multi-domain single sign-on.
  A trusts B. B trusts C. A trusts C.
The Business Problem in Higher Education

- Students must access multiple online systems and service providers that are not connected or related.
- Different access requirements are burdensome and confusing.
- Students circumvent security provisions by using the same passwords and/or passwords are left in the open and are unsecured.
A Look at the ATM Model

- Provide access to funds from multiple locations using combination of token and PIN.
- Available, simple to use, a customer convenience, a commodity.
- BUT, the ATM network had to be built. Policies, procedures, network, and rules of engagement had to be developed and agreed upon by a significant number of banks.
- Banks are not required to have ATMs.
- Customer experience and standards have set the ATM process.
Guiding Market and Consumer Principles

- Students must be able to access necessary information whenever needed.
- Process must be simple, easy, and must be market and user acceptable.
- Process must protect privacy.
- Students will access higher education services through any of the suppliers that are servicing them...multiple “starting points.”
Guiding Market and Consumer Principles

- Process must not rely on one specific technology.
- Process must support multiple schemes (SAML, Liberty, Shibb).
- Process must be secure and reliable.
www.CIO.gov/eAuthentication

- Assists agencies in determining their authentication needs for electronic transactions.
- Directs agencies to conduct e-authentication risk assessments on electronic transactions to ensure that there is a consistent approach across government.
- Provides the public with clearly understood criteria for access to Federal government services online.
The Federal Perspective

Four Assurance Levels:

- Level 1 – Little or no confidence in the asserted identity’s validity.
- Level 2 – Some confidence in the asserted identity’s validity.
- Level 3 – High confidence in the asserted identity’s validity.
- Level 4 – Very high confidence in the asserted identity’s validity.
The Federal Perspective

- NIST Special Publication 800-63 January 2004 – states specific technical requirements for each of the four levels of assurance:
  - Identity proofing, registration, and delivery of credentials.
  - Tokens for proving identity.
  - Remote authentication mechanisms (credentials, tokens, and protocols used to establish that a claimant is in fact the subscriber claimed to be).
  - Assertion mechanisms used to communicate the results of a remote authentication to other parties.
The Federal Perspective

Burton Group Report

- An independent program review of technical architecture, interoperability, and trust characteristics
- EAP
- Available through www.CIO.gov/eAuthentication
Electronic Authentication Partnership (EAP)

www.EAPartnership.com

- Formed by CSIS, OMB, and GSA.
- EAP is “the multi-industry partnership working on the vital task of enabling interoperability among public and private electronic authentication systems.”
What’s needed?

- Standard policies, procedures, and rules.
- Electronic standards.
- Agreement from service providers to engage in a circle of trust.
- Awareness, communication, and collaboration.
- Market and consumer satisfaction.
FSA Update and Perspective

Charlie Coleman
Does your workstation look like this?
Today...

Financial Aid Office

(Multiple User IDs & Passwords per FAA)

CPS

DLSS

DLCS

COD

NSLDS

eCB

IFAP

eZ-Audit

Financial Aid Office

(Multiple User IDs & Passwords per FAA)
Future…

Financial Aid Office

(Fewer User IDs & Passwords per FAA)

Authentication & Access Management

- CPS
- DLSS
- DLCS
- COD
- NSLDS
- eCB
- IFAP
- eZ-Audit

Financial Aid Office
Target Vision
<table>
<thead>
<tr>
<th>#1</th>
<th>…Meets customers expectations for simplified web access</th>
</tr>
</thead>
<tbody>
<tr>
<td>#2</td>
<td>…Improves the security / privacy of student aid data with fewer IDs and simpler management</td>
</tr>
<tr>
<td>#3</td>
<td>…Reduces costs to FSA, schools, etc</td>
</tr>
</tbody>
</table>
Then...Now...Next

2003 EAC
FSA Access Management Team Established

2004 EAC
Open Standards/ Product Selected
E-Authentication Risk Assessments of Gov’t Systems

2005 EAC
FSA’s Access Management High level design (shared with industry and PESC)
Standards & Products

(Fewer User IDs & Passwords per FAA)

Tivoli Identity Manager (TIM)

Tivoli Access Manager (TAM)

Authentication & Access Management

Financial Aid Office

FSA

DLSS

DLCS

COD

NSLDS

eCB

IFAP

EZ-AUDIT

CPS
Moving to Self Service Access...

Centralized Administration

FSA SYSTEMS

School A (Berkeley)  School B (Harvard)

Delegated Administration

FSA SYSTEMS

School A (Syracuse)  School B (Northeastern)
Transitive Trust / Federated Identity

#1 Transitive Trust and Federated Identity…the practice of accepting a third-party identity based on mutual consent between two direct parties.

#2 The concept looks like:

#3 FSA plans to participate…not lead
Federal E-Authentication Framework Initiative

Policy: E-Authentication Guidance for Federal Agencies (OMB M-04-04)

Documents and information at: www.cio.gov/eauthentication
In Summary FSA is...

#1 …moving forward with the Access Management Team.

#2 …testing Tivoli Identity Manager (TIM) and Tivoli Access Manager (TAM) as open standard products.

#3 …moving to a ‘Delegated Administration’ model.

#4 …participating in the Transitive Trust discussions…not leading.
Remember...

What Happens in Vegas, Stays in Vegas...
Industry Perspective

Charles Miller
Overview of Authentication

- Simple example of authentication and transitive trust using SAML.
- Industry initiative that is using transitive trust with SAML. (Meteor)
- How it works.
- Future transitive trust possibilities.
E-Authentication Objectives

- Provide a flexible, easy to implement authentication system that meets the needs of your organization and your clients.
- Ensure compliance with the Gramm-Leach-Bliley Act (GLBA), federal guidelines, and applicable state privacy laws.
E-Authentication Objectives

- Assure data owners that only appropriately authenticated end users have access to data.
- Ensure compliance to internal security and privacy guidelines.
Requirements for Secure e-Authentication

- User must be 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 shared secrets are secure.
Secure E-Authentication Process

- End user authenticates at member site
- Member creates authentication assertion (SAML)
- Member signs authentication assertion with digital certificate (XML Signature)
- Control is passed to partner site
I need a book for my class.

Checked out book from ACME Library.

Don’t have that book. Try my partner, ACME Library.

I have that Book.

Mr. SAML says you’re ok.

You can trust me! (SAML)

ACME Library

Simple Example of Transitive Trust & E-authentication

I need a book for my class.

Sign On

Your schools Library

Simple Example of Transitive Trust & E-authentication

I need a book for my class.

ACME Library

Simple Example of Transitive Trust & E-authentication

I need a book for my class.

ACME Library

Simple Example of Transitive Trust & E-authentication

I need a book for my class.
Industry Example – Meteor

- Web-based universal access channel for financial aid information
- Aggregated information to assist the FAP with counseling borrowers and with the aid process in general
- Collaborative effort
- A gift to schools and borrowers
The Meteor Process

Access Providers

Data Providers

Financial Aid Professional/Student

Index Providers

One

Two

Three
Security Assertion Markup Language (SAML)

- SAML defines an XML framework for exchanging security information and attributes.
- SAML communicates this information in the form of Assertions.
  - Assertions contain information about subjects (people or computers) which have an identity in the network.
  - Assertions are issued by SAML authorities - authentication authorities, attribute authorities, and policy decision points.
SAML Assertions

- Authentication
  - Previous authentication acts
  - Assertions should not usually contain passwords

- Attributes
  - Profile information
  - Preference information

- Authorization
  - Given the attributes, should access be allowed?
Typical Assertion

- Issuer ID and issuance timestamp
- Assertion ID
- Subject
- Name and security domain
- Conditions under which the assertion is valid
- Assertion validity period
- Audience restrictions
- Target restrictions (intended URLs for the assertion)
- Application specific conditions
Additional Assertion Attributes

- Role of end user
- Social Security Number
- Authentication Process ID
- Level of Assurance
- Opaque ID
Securing SAML Assertions with XML Signatures

- The SAML assertion is signed by the entity that created it.

- When signed, all irrelevant white-space is removed.

- Once signed, the document may not be modified without invalidating the XML signature.
Future transitive trust possibilities.

Acme Lender

Acme Guarantor

Acme Sevicer

Schools Auth. System

Schools system

Security assertion

Financial Aid Professional

ACME School

DLCS

NSLDS

DLSS

IFAP

PEPS

COD

eCB

CPS
School Perspective

Nicholas Zinser
Northeastern & myNEU

- Launched myNEU in Fall of 2002 to current student population
- Expanded to include admitted full-time undergraduate students in January 2004
- Quickly becoming the hub of student transaction activity
myNEU & Student Financial Services

- Launched real-time financial aid information site in January 2004
  - Authenticated via myNEU
  - Office available when students are

- Launched job search, application, and timesheet program in July 2004
  - Authenticated via myNEU
  - Increased service to students
myNEU & Student Financial Services – Online Aid Information

- First implementation of a .NET product at Northeastern
- Had to merge portal user authentication with aid database identifiers
- Update scheduling poses the question – When do you take down the Internet?
Branding is consistent with portal graphics

Personalized Experience

Generic Messages
myNEU & Student Financial Services – Jobs in the Portal

- New FWS system required knowledge of both students and supervisors
  - Students authenticated by the portal prevent non-NU students from applying for jobs
  - Supervisors need a non-portal method of managing their jobs as some employers are not NU employees
Branding unique, but echoes portal

Warning about non-portal access
Authentication Issues

- Namespace
  - As the University expands, available names in standard naming convention decreases
  - Flexibility allows for differentiation
    - husky.n
    - husky.nu
    - husky.northeastern
  - Central data warehouse for IDs created
Authentication Issues

- Technology
  - New products arriving to market are written in newer, constantly changing code
  - Several implementations have been the first of their kind at NU
  - Constant communication with IS staff and outside vendors is important
Other Authentication Initiatives

- Meteor access for students
  - Track loan borrowing information throughout academic program
  - Continued focus through alumni portal post-graduation
- Federal Perkins Loan MPN
  - Complete via the portal
  - Increase completion rate for MPN
...Thank You...Thank You Very Much...

...Questions / Comments / Thoughts...
Contact Info

Michael Sessa
202-293-7383 (o)
617-694-2716 (c)
sessa@pesc.org

Charles Miller
401-736-1100 (o)
cmiller@riheaa.org

Charlie Coleman
202-377-3512 (o)
202-549-9955 (c)
charlie.coleman@ed.gov

Nicholas Zinser
617-373-5830 (o)
n.zinser@neu.edu
http://www.myneu.neu.edu/