IAM Online

Multifactor Authentication in Higher Education
Tuesday, December 6, 2011 – 3 p.m. ET

Steven Burke, Federal Student Aid, US Dept. of Education
Shilen Patel, Senior IT Analyst, Duke University
Miguel Soldi, Information Security Policy and Resourcing Analyst,
    University of Texas System
Rodney Petersen, EDUCAUSE
Two-Factor Authentication

An EDUCAUSE Information Security Guide Resource

Miguel Soldi, HEISC Governance, Risk, and Compliance Working Group
Why a Resource About Two-Factor Authentication?

- Two-factor authentication has been around for a good while…
- Most people are familiar with it….though some may not know it.
- But, we have come to realize that…
  - Staff and faculty, in their official capacity, have access to systems and databases with an increasing amount of confidential information,
  - Confidential information highly desirable and actively sought by the curious and the criminal,
  - Passwords safeguarding information can frequently be easily guessed or compromised through phishing or hacking, and
  - The increased use of single sign on has also increased the value and risks of those passwords

Why a Resource About Two-Factor Authentication?

- Two-factor authentication has been around for a good while...
- Most people are familiar with it...though some may not know it.
- But, we have come to realized that...
  - it makes good business sense to consider two-factor authentication as an alternative to the use of userid / passwords by themselves, and
  - compliance requirements are increasingly motivating us to come to that realization...a bit quicker.

A Word About the Resource.

- High-level overview document that touches on the business reasons for using an additional factor, characteristics of available technology, and a discussion of biometrics.
- It is intended as a starting point for those who are just starting to think about it and a “springboard” to further explore alternatives, characteristics, and risks.
- It is not a roadmap for implementation or an endorsement for any particular technology.
- It not perfect either. Feedback, comments, and other input are welcomed and appreciated.
Two-Factor Authentication Resource – Next Steps

Common Barriers to Implementation of Two-Factor Authentication

• No explicit federal or state requirement.
• Who owns the process? Who pays for it? What about decentralized IT?
• False sense of security. “Have not had a breach so we must be doing things right.”
• Trying to do too much at once.
• Cost and difficulty to demonstrate/articulate benefit.
• IT and IT help desk may not want to support it.
• Inconvenience. One more thing to carry and worry about.
• Privacy concerns regarding biometrics in particular
How Can I Approach Implementing Two-Factor Authentication?

• What do we need and why?
  – Is there a specific compliance requirement?
  – Is it only for physical access to buildings and data centers, access to data, or both?
  – Do we need to target specific users, applications, locations, all of the above?
  – What mix of technology and deployment architectures is needed / desired?

• What can we afford?
  – What is the incremental benefit of one technology over another?
  – Full vs Incremental implementation.

• What can we sustain?
  – Integrated solution covering all requirements?
  – Manageable help desk workload to handle user questions, training, lost devices, renewals, revocations, etc?
  – Will users accept and utilize our solution?
Contact Information

We appreciate your feedback and comments.

Email: msoldi@utsystem.edu

THANK YOU!
Multifactor AuthN

Shilen Patel, Duke University
Multimode Multifactor Authentication

• Traditional single-mode multifactor authentication is a non-starter.
  – Authmech = f(organization)

• Authmech = f(app,user) (or even f(app,user,location))
  – f() = Max(user(app), app(user), institution(app, user))

• Prof W. can self-select a higher bar for his logins to his blog, while we can raise the bar for logins to grant mgt.
Low-hanging fruit strategy

• Start with the IDP
  – 700+ on-campus SPs and growing already
  – If we’re careful, most SPs won’t need to do anything and their users won’t notice anything
  – Infrastructure behind the IDP can be reused
  – New apps are largely web-based; older apps continue to grow better web interfaces
New IDP external authmech

- Pluggable interface for custom credential verifiers
- Recognizes different strength values for different credential types
- Computes required strength based on claimed identity and SP making request.
New IDP external authmech

• IDP Login Extensions
  – ajaxy and context sensitive
  – authN options depend on user capabilities and preferences
  – constrained feedback to defeat incremental attacks
New IDP external authmech

- Data repositories for rules and preferences
  - IDP stores mech strength rules locally
  - LDAP stores user, SP specific data
  - Considering Grouper as replacement for one or both to enhance generality
Single sign-on

• SSO becomes an issue across disparate SPs
• Built-in previous session handler doesn’t understand strength
• We disable it and supply SSO in the external authmech itself
Single sign-on

- Record authN strength factor (sum) in login context (auth method)
- SSO implements $\geq$ semantics -- SSO succeeds iff previous session method strength $\geq$ current requirement
- On SSO failure, require all new creds from user
Novel Use Cases

- Sometimes a password may not be required (WS)
- If no one specifies anything, UI can look just like before
- If an SP explicitly lowers its expectations, new options arise
  - Default numeric strength requirement = 1 (equiv to “password only”)
  - Allow OpenID gateway as option for SPs requiring strength < 1
Other Considerations

• User requires a higher strength value for an SP, but forgets his second factor when going to a conference.

• Strength requirement for self service tool.

• Other authentication mechanisms.
Manage your personal preferences

You can choose what level of authentication is required when you access NetID protected web sites.

Preferred authentication methods:
- [ ] Password
- [x] TiQR
- [x] x509

Minimum requirement for all web sites: Medium

Individual site specific requirements:
- Test Service Provider 3: Medium
- Test Service Provider 1: High
- Test Service Provider 2: Medium

Update Preferences
Duke University
NetID Services

Please identify yourself to NetID service handleservice at host shibboleth.duke.edu.

Please enter your NetID:

NetID: [Enter]
Password: [Enter]

Don't know what a NetID is? Not sure if you have one? Find out.

Forgot your password? Click here.
Duke University NetID Services

Please identify yourself to NetID service handleservice at host shibboleth.duke.edu.

Please enter your NetID:

NetID: shilen
Password: 

+ TiQR
+ x509

Enter

Don't know what a NetID is? Not sure if you have one? Find out.

Forgot your password? Click here.
Please enter your NetID:

NetID:  shilen
Password: 

Start your TiQR smartphone application and direct your smartphone camera to the image below to continue authenticating

If you have not yet registered with the TiQR service, you can do so by clicking here
Duke University
NetID Services

Please identify yourself to NetID service handleservice at host shibboleth.duke.edu.

Please enter your NetID:

NetID:  
Password:  

Enter

Don't know what a NetID is? Not sure if you have one? Find out.

Forgot your password? Click here.

Guest Access
Duke University Guest login

Choose an account to login with

Google

Yahoo!
Accounts

Shib-test.oit.duke.edu is asking for some information from your Google Account. To see and approve the request, sign in. Learn more

Sign in

Email

Password

Sign in

Stay signed in

Can't access your account?
Contact Information

We appreciate your feedback and comments.

Email: shilen@duke.edu
Two-Factor Authentication

Steven Burke, Federal Student Aid, US Department of Education
Project Overview

To comply with the White House through the United States Office of Management and Budget (OMB) mandate, Memorandum M07-16 attachment 1, and as part of our ongoing efforts to ensure the security of Federal Student Aid data systems, the U.S. Department of Education, is required to implement a security protocol through which all authorized users will enter two forms of “authentication” to access Federal Student Aid systems via the Internet.

This process is referred to as Two-Factor Authentication (TFA).
Keyloggers, Malicious Threats

• Keyloggers
  • What is it and how does it exploit a Web Application?
  • What can be captured?
  • Why is it desirable?
What is Two-Factor Authentication?

Two Factor Authentication is a process which requires each authorized user to log into FSA systems with two types of information:

Something that you **know** is the First Factor: **User ID and Password**

Something that you **have** is the Second Factor: **Token with a One Time Password**

- The One Time Password (OTP) will be generated by a small electronic device known as the TFA Token that is in the physical possession of the user

- To generate the OTP, a user will press the “power” button on the front of the token.

- A different OTP will be generated each time the button is pressed.

**Alternative Methods of obtaining OTP without TFA Token:**
A) Answer 5 Challenge Questions online
B) Have the OTP sent to your Smart Phone
How do I register my token?

• Once you receive your token you must register it for each system for which you have access to and utilize

• Each FSA System Web site will be slightly different when logging in and registering your token

Next Steps:
Click on the following link.

https://fafsa.ed.gov/FOTWWebApp/faa/faa.jsp

Then click on the Register/Maintain token URL on the top right hand side of the screen.
• **Step One** – Enter general identifying profile information
  
  • If you ever forget your assigned password or misplace your token, you may choose to complete the cell phone information to receive this information via “text” message
**Step Two** – Enter the Token Serial Number located on the back of the token

- The credential will begin with three letters and nine numbers (i.e. AVT800000000)
> **Step Three** – Complete five separate questions and responses
  
  • You may not repeat questions nor may any question have the same response

![Step Three: Choose Challenge Questions and Enter Responses](image)
TFA Terms of service

Step Three continued – You must read the Terms of service before checking the acknowledgment statement and proceeding.
TFA – Security Code

• You will then be directed to the security code entry screen

• You must enter two consecutive security codes successfully

• Please note: a new code is generated once every 30 seconds and will require you to click the “On Button” in between attempts
TFA Registration Complete

- Registration Completion – When successful you will receive confirmation and your security token will now be ready for use.
Once your token is registered you must log in using both factors of authentication:

- Factor one – Assigned User ID and Password
- Factor two – One-Time generated Password (OTP)
Token Registration Process – CPS

Token Registration Process - CPS

CPS
https://faaccesse.gov/FTOWWebApp/faa/faq.jsp

NSLDS
https://www.nslsifap.ed.gov/nsls_FAP/secure/login.jsp

Registration Profile Screen

Step 1: Profile Information
- First Name
- Last Name
- Office Desk Number
- Cell Phone Number
- Confirm Cell Phone Number
- Email

Step 2: Enter Token Serial Number
- Serial Number [S/N]
- Confirm Serial Number

Step 3: Choose Challenge Questions and Enter Responses

Step 4: Terms of Service, click the checkbox, and click "Submit"

Security Code (CIF)
Entry:
- Security Code #1
- Security Code #2
Click "Submit"

Success message, Close browser,

CPS
Enter Application

NSLDS
Enter Application

Start Here
Go Further
Federal Student Aid

39
Token Registration Process – COD

COD
https://cod.ed.gov/cod/loginPage

Click the link under "To register a new token or maintain your FSA token profile"

Login Page – Common Origination & Disbursement Two-Factor

Enter COD User ID and Password, click "Login"

New Token Registration screen

Step 1: Profile Information
- First Name
- Last Name
- Office Desk Number
- Cell Phone Number
- Confirm Cell Phone Number
- Email

Registration Profile Screen

Step 2: Enter Token Serial Number
- Serial Number
- Serial Number (S/N)

Step 3: Choose Challenge Questions and Enter Responses

Step 4: Read Terms of Service, click the checkbox, and click "Submit"

Security Code (OTP) Entry:
- Security Code #1
- Security Code #2

Click "Submit"

Success message, click "here" to return to COD login page

COD Login Page
Token Registration Process – EDconnect/SAIG

1. Start EDconnect software on desktop
2. EDconnect Login Page
3. Click “Register/Maintain Token”
4. Login – AIMS TFA Portal screen
5. Enter User ID and Password, click “Login”
6. New Token Registration screen

**Registration Profile Screen**

**Step 1: Profile Information**
- First Name
- Last Name
- Office Desk Number
- Cell Phone Number
- Confirm Cell Phone Number
- Email

**Step 2: Enter Token Serial Number**
- Serial Number (S/N)
- Confirm Serial Number

**Step 3: Choose Challenge Questions and Enter Responses**

**Step 4: Read Terms of Service, click the checkbox, and click “Submit”**

**Security Code (OTP) Entry**
- Security Code #1
- Security Code #2

Click “Submit”

Success message, close browser.

EDconnect / SAIG Enter Application
Primary Systems Impacted Across the Enterprise

- CPS FAA Web Access  4/20/2011
  (Central Processing System)
- COD  10/23/2011
  (Common Origination and Disbursement System)
- NSLDS move Behind AIMS  12/18/2011
  (National Student Loan Data System)
- Participation Management  2/12/2012
- SAIG/ EDconnect  2/12/2012
  (Student Aid Internet Gateway)
- Ombudsman  2/12/2012
# Token Deployment Schedule 2011-2012

<table>
<thead>
<tr>
<th>Group</th>
<th>Implementation</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group 1</td>
<td>Q4 2011</td>
<td>DE, MD, VA, WV</td>
</tr>
<tr>
<td>Group 2</td>
<td>Q1 2012</td>
<td>NC, NJ, NY, SC</td>
</tr>
<tr>
<td>Group 3</td>
<td>Q2 2012</td>
<td>KY, MI, NE, NH, OH, PA, RI, VT</td>
</tr>
<tr>
<td>Group 4</td>
<td>Q2 2012</td>
<td>CA, FL</td>
</tr>
<tr>
<td>Group 5</td>
<td>Q3 2012</td>
<td>AK, ID, MN, ND, OK, OR, SD</td>
</tr>
<tr>
<td>Group 6</td>
<td>Q3 2012</td>
<td>AR, CO, GA, KS, MO, MS</td>
</tr>
<tr>
<td>Group 7</td>
<td>Q3 2012</td>
<td>AZ, CT, IA, IL, IN, LA, TX</td>
</tr>
<tr>
<td>Group 8</td>
<td>Q4 2012</td>
<td>AL, AS, FC, FM, GU, HI, MA, ME, MH, TN</td>
</tr>
<tr>
<td>Group 9</td>
<td>Q4 2012</td>
<td>MT, NM, NV, PR, PW, UT, WA, WI, WY</td>
</tr>
</tbody>
</table>
TFA – Token Deployment Status

- Phase 1 FSA – Citrix users 1,300 completed 5/1/2011
- Phase 2 Dept. of ED Staff 5,200 completed 7/1/2011
  - FSA Contractors completed 10/28/11

- Phase 3 International users at Foreign Schools
  - Group 0 – Foreign Schools
    - 650 confirmed users 11/28/2011
  - Group 0 – DeVry University
    - 820 confirmed users 11/28/2011
  - Group 1 – DC, DE, MD, VA, WV
    - 2,622 estimated users
    - Complete attestation and ship tokens by 12/31/2011

- Groups 2-9 11/16/2012
Two Factor Authentication Next Steps

Action Items and Next Steps (Internal)
• Contractor /Vendor attestation of Developers, Testers and Call Center Representatives (CSRs)
• FSA Project Team to provide information on confirmation processes, TFA training and tokens
• Contractor /Vendor are to register tokens
• FSA to TFA Enable Systems

Action Items and Next Steps (External)
• Primary Destination Point Administrator (PDPA) and COD Security Administrators (CSA) attestation of (FAA, Servicers and Guaranty Agencies, etc.) associated with their account and who are working on behalf of their institution
• FSA Project Team to provide information on confirmation processes, TFA training and tokens
• Institutions are to register tokens
Contact Information

We appreciate your feedback & comments.

- Phone: 202-377-4683 (Steven Burke)
- E-mail: TFA_Communications@ed.gov
Evaluation
Please complete the evaluation of today’s IAM Online.

IAM Online Announcement List
Email sympa@incommon.org with the subject: subscribe iamonline

Thank you to InCommon Affiliates for helping to make IAM Online possible.

Brought to you by InCommon, in cooperation with Internet2 and the EDUCAUSE Identity and Access Management Working Group