Multi-Factor Authentication, Assurance, and the Multi-Context Broker

IAM Online
April 30, 2014

Keith Wessel, University of Illinois, Urbana-Champaign
David Langenberg, University of Chicago
David Walker, InCommon Technical Advisory Committee

INTERNET2

InCommon

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

aegisIDENTITY
the identity software company
www.aegisidentity.com | @aegisidentity

FISCHER INTERNATIONAL

IDM integration

Microsoft

UNICON

Brought to you by Internet2's InCommon in cooperation with
the Higher Education Information Security Council

Overview

- The Multi-Context Broker
- Multi-Factor Authentication at the University of Illinois at Urbana-Champaign
- Multi-Factor Authentication and Assurance at the University of Chicago

The Multi-Context Broker (MCB)

David Walker

Why Do We Need a Multi-Context Broker?

Campus would like their authentication service to

- use multi-factor for internal services
- address risk needs of different campus services by supporting multiple levels of credential security, from email to budget distribution
- access higher-risk services where the external service provider needs confidence of higher-security credential practices

And don't we want to develop custom code...

What Is the Multi-Context Broker?

- A Shibboleth Identity Provider plugin to make it easier to orchestrate multiple authentication methods within your IdMS. Uses include:
  - Multi-factor authentication
  - Assurance profiles
- Goal is very easy deployment with no programming, just configuration.
- Funded by the InCommon Assurance Program and the National Strategy for Trusted Identities in Cyberspace (NSTIC).

How Does It Work?

1. The service provider requests an authentication context (an authentication method, plus potential other criteria like identity proofing processes)
2. The MCB checks the IdMS to see if the user is certified to use the requested context, or some other context that satisfies the requirements of the requested context.
3. If additional authentication is required, the MCB invokes the appropriate authentication method.
4. Assuming success, the MCB returns the requested context to the service provider.

Variations on the Theme

- There may be multiple authentication methods that can satisfy a service provider's request. In that case, the user is given a choice.
- On a per-user basis, information in the IdMS can be set to require multi-factor authentication, even if the service provider does not specifically request it.
- The service provider can request multiple authentication contexts in priority order. User choices are ordered accordingly.

Current Status of the MCB

- Available now.
- Documentation and download:
  - https://spaces.internet2.edu/x/BozFAg
- Supported Authentication Methods
  - Username / Password (JAAS)
  - PKI
  - Duo Security
  - Very easy to build new submodules (fewer than 200 lines of Java for the Duo submodule).
- Engaged user community on the shib-users list.

The University of Illinois at Urbana-Champaign

Keith Wessel

The Back Story

- Two SSOs needing to work together
- Remote User login handler did the trick
- A session in one took care of a session in the other

The Problem

- Along came Duo
- The Shib Duo login handler works with JAAS but not remote user
- Do we write our own login handler?
- How do we easily allow SPs to request MFA?

The Solution

- MCB has login submodules for remote user and Duo
- Make remote user the required initial authn method
- Allow SPs to request a specific context if they want optional or required MFA

ILLINOIS LOGIN

You must log in to continue.

Enter your **NetID:**

Enter your **Active Directory (AD) password:**

Login

Forgot your Active Directory password?

To change or reset your Active Directory password, go to the CITES Password Manager.

More Information

Where to Get Help

Contact the CITES Help Desk at consult@illinois.edu.

What Is a NetID?

Your NetID serves as your login to many University computing and networking services and also determines your University email address, which is netid@illinois.edu.
For more information, see the Your Network ID (NetID) page.

Technical Information

This login service uses the following server:

test.auth.uillinois.edu

This page's URL should start with https:// followed by the server listed above.

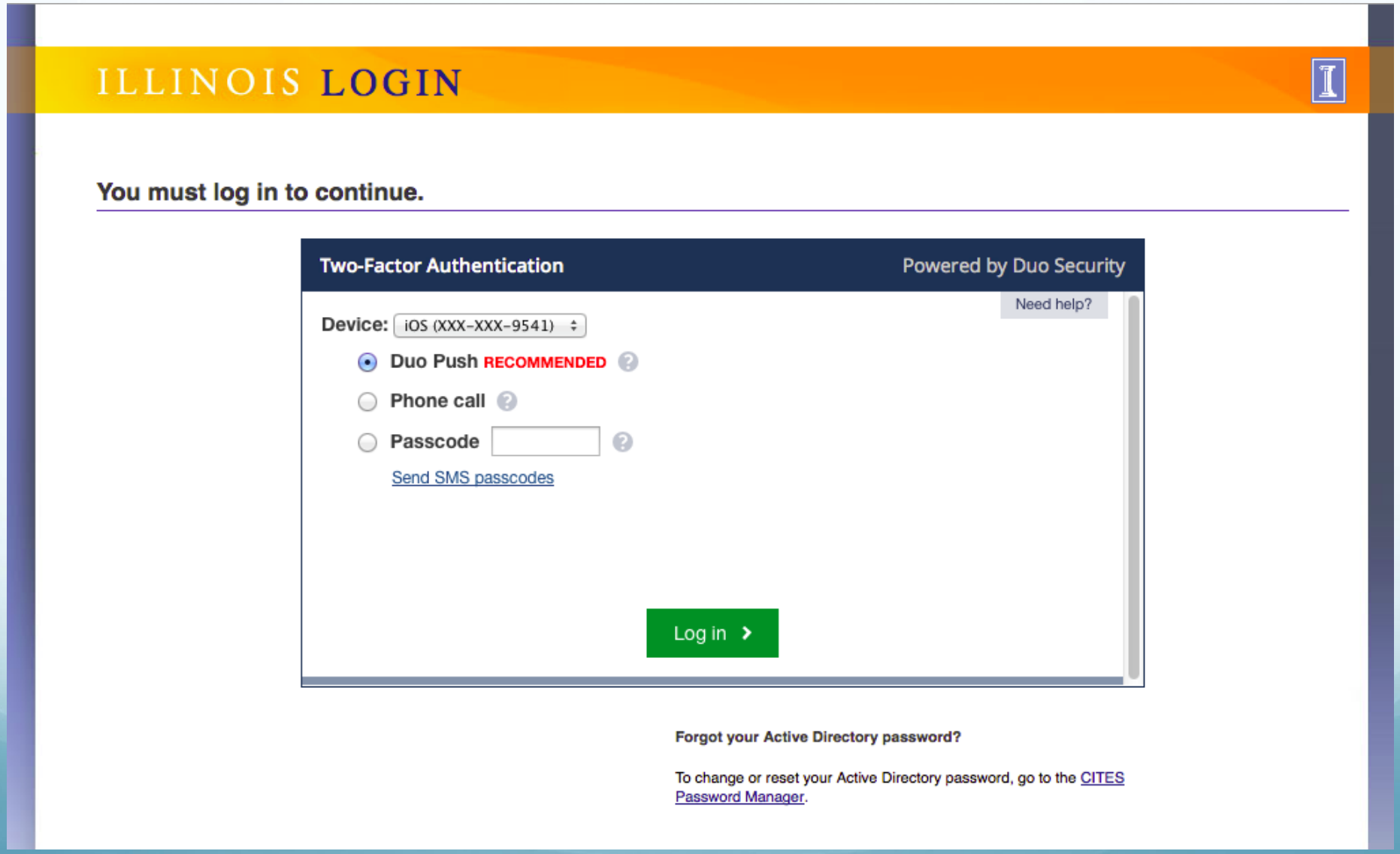
Target:

HTTPS://shib-test-idp.cites.illinois.edu/idp/Authn/RemoteUser

For most web browsers, the security padlock icon for this page should be closed/locked.

To maximize security, quit your browser when done using this application.

SM-U-IL-001


ILLINOIS LOGIN
You must log in to continue.
Two-Factor Authentication
Powered by Duo Security
Need help?
Device: iOS (XXX-XXX-9541)
Duo Push RECOMMENDED
Phone call
Passcode
Send SMS passcodes
Log in
Forgot your Active Directory password?
To change or reset your Active Directory password, go to the CITES Password Manager.

INTERNET2

InCommon

THE UNIVERSITY OF CHICAGO

David Langenberg

davel@uchicago.edu

Use Cases

- InCommon Silver
- Duo Security
  - Services opt-in to requiring users to 2FA
  - Users opt-in to requiring 2FA for all services
- Desire to require a user to have to enter credentials only once per SSO Session

Demo

Evaluation

Please complete the evaluation of today's webinar
https://www.surveymonkey.com/s/IAM_Online_April_2014

Active Directory and Best Practices: A Revised Cookbook

Best practices for authentication

Active Directory and Assurance profiles

Wednesday, May 7, 2014
Noon ET | 11 am CT | 10 am MT | 9 am PT

http://internet2.adobeconnect.com/incforum

Save the Date!

Identity Week 2014 will take place at the Internet2 Technology Exchange

Advance CAMP, CAMP, Trust and Identity

October 26-30, 2014 - Indianapolis, Indiana

http://events.internet2.edu/2014/technology-exchange/

InCommon Shibboleth Installation Workshops

July 24-25 - Indiana University - Indianapolis, IN

September 29-30 - New Jersey Institute of Technology - Newark, NJ

Details and registration at www.incommon.org/shibtraining

INTERNET2

InCommon

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

aegisIDENTITY
the identity software company
www.aegisidentity.com | @aegisidentity

FISCHER INTERNATIONAL

IDM integration

Microsoft

UNICON

Brought to you by Internet2's InCommon in cooperation with
the Higher Education Information Security Council