

Introducing MIT Touchstone

IS&T Leadership

October 18, 2007

Paul B. Hill, ISDA



Information Services & Technology



Massachusetts
Institute of
Technology

What is MIT Touchstone?

- Suite of technologies
 - A web logon server
 - Communicating information about the authentication to appropriate web servers
 - Account management beyond the MIT core community
- Focused on Web authentication



Why are we introducing MIT Touchstone?

- Support a wider variety of authentication methods
- Minimize the exposure of passwords
- Provide a consistent methodology for web developers and system administrators
- Provide a maintainable approach to introducing evolving authentication technologies
- Provide the ability to use other identity providers



How will MIT Touchstone improve the user experience?

- Users will be able to use a variety of authentication mechanisms
- Users will be able to traverse Touchstone enabled web sites and resources transparently
- Ultimately, less information about the user will have to be released to many web sites



What technologies are used?

- Login server is Stanford's WebAuth server
- Shibboleth developed by Internet2
- Account management for "external users"
 - User ID based on email address
 - Supporting username/password and OpenID
 - Self-service account creation and sponsored accounts



Timeline

Pilot started on October 11th

- Login server (without certificates)
- Shibboleth IdP for MIT users
- Stellar

By end of IAP 2008

- Login server including certificates
- Initial pilot of new account management system

Fall of 2008

- Full production



Scope of the pilot

- Any MIT user of a pilot application will have the option of using Touchstone to authenticate
- During the pilot only a limited number of applications will be allowed to integrate with MIT Touchstone
- Initial pilot applications will prompt for a certificate by default just as they do today.
- Certificate authentication to Touchstone login server temporarily removed. It will be returning.



Applications expected to be in the pilot

- Stellar – October 11th
- Jira – October 15th
- Confluence wiki system (now wiki.mit.edu) – later today
- Dates to be determined:
 - Dspace
 - Thalia
 - Alfresco
 - And one NIST application to be determined

Support

- Users will not be expected to distinguish between Touchstone components or services and the application they are trying to access
- User will contact the support group that they normally contact for a given application. Typically the help desk.
- Determine if the problem is with Touchstone or the use of the application and resolve or escalate as appropriate



Touchstone contact points

- RT queue: ISDA::touchstone-support
- Mailman: touchstone-support



Federated Authentication

- Accepting authentications from a selected set of partners
 - Also how we will handle our own collaboration accounts
- Other partners will accept our authentications as well
- Fewer “guest accounts”



Demo

- <http://stellar.mit.edu/S/project/isda>

Thanks to:

- Robert Basch – lead developer
- The Stellar Team –
 - Craig Counterman, Joanna Proulx, Arti Shama
- Carter Snowden
- CSS Help Desk Team –
 - Barbara Goguen, Oliver Thomas
- NIST –
 - Mark Silis, Jeff Schiller
- ITAG, TRB, and the IdM-sc
- Internet 2 and Stanford

