Lotusphere 2012
Business. Made Social.

New Single Sign-on Options for IBM® Lotus® Notes® & Domino®
IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM’s sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.
Agenda

- Standards based SSO using SAML
- SAML for IBM Lotus Domino web server and IBM Lotus iNotes®
- SAML for IBM Lotus Notes client
User accesses many different IBM services with browser or Lotus Notes.

User doesn't want multiple password prompts.
User might also access third party services.

User doesn't want multiple password prompts.
SSO Mission: Fewer password prompts, fewer passwords in general

- We need SSO because:
  - High administrative cost for managing passwords.
  - Users can't remember a lot of passwords.
  - Password prompts are annoying.
  - Many “different” passwords leads to lower security.

- If we use cryptographic mechanisms instead of passwords, we can improve security and minimize cost.

- For best interoperability across IBM and third party applications, we look to adopt standards based SSO.
Security Assertion Markup Language (SAML)

- Standard to address Internet SSO.
- OASIS publishes the standards documents.

- Many implementations available, including open source.
- SSO across cooperating domains and across cooperating corporations.

- IBM LotusLive® Notes implements SAML.
SAML identity assertion

- Security is based on PKI.
  - User's identity is represented in a signed XML assertion.
  - Private key, public key pair:
    - Server creating the assertion signs it using its private key.
    - Servers processing assertions validate signature using the trusted signer's public key.
  - Standards based, Internet certificates and keys are used.

- Service identifies the user based on the user's assertion.
  - Assertion contains the authenticated user's name (e.g. email address).
SAML Identity provider (IdP) authenticate:

- IdP implements “federated identity”.
  - Knows about user names, passwords.
  - Might be able to authenticate the user via SPNEGO/Kerberos, or alternate non-password method.
  - Prepares credentials (SAML identity assertion) for the user to target service.
    - IdP authenticated user x at time y
  - Can be used by services from different vendors.

- Common IdPs
  - IBM Tivoli® Federated Identity Manager (TFIM®)
  - Microsoft® ADFS® 2.0 integrated with Active Directory®
  - many others
Federated Identity using SAML assertions

Why is it a good thing for security?
- Minimized use of password (only handled by IdP, if required).
- Authenticate once to IdP. The IdP may “remember” the user.
- Customers can use/control their own on-premises IdP.
- Less user data redundancy.
- Goal: password info is unavailable to crackers wanting to launch an offline password guessing attack
Services accepting SAML assertions

- SAML service provider (SP) receives authentication decision from the IdP.
- SP authenticates a user by successful verification of the user's SAML assertion.
Remove risk using SSL

- HTTP protocols in use
- If SSL (HTTPS) is not used to encrypt the channels
  - Eavesdropper steals user login information, e.g. password.
  - Eavesdropper steals the identity assertion.
    - Good for short period of time.
  - Eavesdropper steals any cookies.
    - Good for configured period of time.
Agenda

- Standards based SSO using SAML
- SAML for IBM Lotus Domino web server and IBM Lotus iNotes
- SAML for IBM Lotus Notes client
Domino SP receives authentication decision from the IdP.

Domino authenticates a user by successful verification of the user's SAML assertion.
Web client: user accessing Domino via browser.

User browses to a protected Domino URL, but hasn't logged in yet.
Web client: user accessing Domino via browser

Domino redirects the browser to the IdP's URL with a SAML request.
URL might look something like this

Browser redirects to SAML IdP.
User may be prompted to authenticate to IdP, or the IdP may be configured to authenticate user with non-password method (e.g. SPNEGO/Kerberos).
Web client: user accessing Domino via browser.

IdP has authenticated the user and sends the SAML assertion.
SAML assertion received at Domino is verified using the IdP's public key. Domino needs to map the name in the assertion to user's Domino name.
User is logged in at Domino. User's browser now has credentials to access protected Domino URLs.
Now the user will see the protected Domino URL.

http://domino1.renovations.com/db.nsf
User accesses other Domino SAML servers

IdP remembers the user, and issues SAML assertions transparently to the user.

Each Domino server can use SAML assertion and issue the user a single server session cookie. SSO achieved by use of common IdP.
Administrator sets up Domino SAML in environment with non-SAML IBM servers

Instead of a single server session cookie, Domino SAML is configured to use an LTPA session cookie that can be shared with other IBM servers.
Administrator has registered the on-premises IdP with Facebook®, so that Facebook can verify SAML assertions from the IdP.
iNotes may authenticate the user via SAML assertion

- HTTP flows (as shown in previous slides) to authenticate
iNotes secure mail: Using SAML to avoid password to Notes id file

The ID vault server using new Notes RPC channel to receive user's assertion, and to return user's unlocked id file to iNotes.
Deployment steps for Domino web server SAML

- Deploy a SAML IdP on-premises.
  - (Optimal) To avoid password prompting by the IdP, configure IdP for SPNEGO/Kerberos user authentication.
  - Tell the IdP about each participating Domino server.

- Configure Domino.
  - Domino web server settings for SAML.
  - Declare trust in the IdP to login Domino users.
  - Set up name mapping (map user's email address to a Domino distinguished name).
  - (for iNotes secure mail users) Deploy security policy for id file in ID vault.
  - (for iNotes secure mail users) Declare trust in the IdP to authenticate to ID vault.
Agenda

- Standards based SSO using SAML
- SAML for IBM Lotus Domino web server and IBM Lotus iNotes
- SAML for IBM Lotus Notes client
Notes Shared Login providing SSO at Notes startup

- Notes Shared Login is a great feature.
  - User does not have a Notes password.
  - User's id file can be managed in the ID vault.
  - Administrator's policy determines which users have Notes Shared Login.

- Notes Shared Login can't be used in virtual environments (e.g. Citrix).
  - SAML may provide a useful alternative.
Notes on Citrix: Virtual environment

Windows Domain Controller
(Kerberos security, ADFS IdP)

ID vault
ID Files

Lotus Domino

Active Directory
Administrator has picked one of these policy choices to enforce for user:
- User is a SAML user.
- User should be prompted for password.
Notes on Citrix can leverage the Windows environment for a SAML user.

For Citrix Windows environment, it may be convenient to deploy Microsoft ADFS 2.0 for the SAML IdP.
Notes on Citrix: Use SAML to avoid password prompt to start Notes

- Notes embedded browser handles authentication to SAML IdP via SPNEGO/Kerberos over HTTP.

User has already logged into Windows. User doesn't need to prove who he is to the Microsoft ADFS IdP.
Notes on Citrix: Use SAML to avoid password prompt to start Notes (by retrieving unlocked id file)

- Send SAML assertion to ID vault server via Notes RPC channel.
- ID vault server returns user's unlocked id file via Notes RPC channel.

ID vault server evaluates whether the assertion comes from trusted IdP.
Deployment steps for Notes client use of SAML at startup

- **Deploy a SAML IdP on-premises.**
  - (Optimal) To avoid password prompting by the IdP, configure IdP for SPNEGO/Kerberos user authentication.
  - Tell the IdP about the Domino SAML service provider for the ID vault.

- **Configure server settings.**
  - Deploy security policy to assign SAML users, and managing id files in ID vault.
  - Declare trust in the IdP to login Notes users by SAML authentication to ID vault.
  - Set up name mapping (map user's email address to a Domino distinguished name).
User accesses many different IBM services with Notes

IBM Sametime
IBM Connections
LotusLive Engage
Lotus Domino
Lotus Quickr

User doesn't want multiple password prompts.
Notes plug-ins

- After login to Notes, Notes may attempt authentication to Internet servers.
  - Notes sidebars:
    - Sametime
    - Activities (Connections)
    - Feeds.....
    - Browser applications running in Notes
Notes plug-ins

- After login to Notes, Notes may attempt authentication to Internet servers.
  - Notes sidebars:
    - Sametime
    - Activities (Connections)
    - Feeds.....
    - Browser applications running in Notes

- Authentication mechanism is specified in Notes account
  - In user's personal Name and Address book
Notes plug-ins

- After login to Notes, Notes may attempt authentication to Internet servers.
  - Notes sidebars:
    - Sametime
    - Activities (Connections)
    - Feeds.....
  - Browser applications running in Notes

- Authentication mechanism is specified in Notes account
  - In user's personal Name and Address book

- Notes already has an option for SAML to LotusLive Notes
Optimally Notes plug-ins can use SAML in the future

- Notes embedded browser can make requests to an IdP.
  - No login prompts if IdP using SPNEGO/Kerberos.
  - Issue: not all target servers will be able to accept a SAML assertion.

- Notes could send a SAML assertion to Domino to authenticate and receive a session token (LTPA) for use by Notes plug-in.
8.5.2 Notes managed accounts

- Administrator manages Account documents in Domino Directory.
  - Domino policy mechanism pushes accounts to Notes client.
  - We may need some tweaks to Account documents for SAML.
Legal disclaimer

© IBM Corporation 2012. All Rights Reserved.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM’s current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM’s sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

IBM, the IBM logo, Lotus, Lotus Notes, Notes, Domino, Quickr, Sametime, Lotuslive, WebSphere, UC2, PartnerWorld and Lotusphere are trademarks of International Business Machines Corporation in the United States, other countries, or both. Unyte is a trademark of WebDialogs, Inc., in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Facebook is a registered trademark of Facebook, Inc in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

All references to Renovations refer to a fictitious company and are used for illustration purposes only.
Questions?