

# Lotus knows.

Smarter software for a Smarter Planet.

## ID105 What's New in IBM® Lotus® Notes™ Client Security

**John Banks-Binici** | Program Director  
**Srinivas Rao** | Senior Software Engineer  
**Jennifer Moore** | Advisory Software Engineer



## Financial Disclaimer

The information on the new product is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information on the new product is for informational purposes only and may not be incorporated into any contract. The information on the new product is not a commitment, promise, or legal obligation to deliver any material, code or functionality. The development, release, and timing of any features or functionality described for our products remains at our sole discretion

## Agenda

- Introductions and Overview
- Security infrastructure available for plug-in's in Lotus Notes
- Security model for plug-in components in Lotus Notes
- Application plug-in's we ship with Lotus Notes and their Security Model
- Administering this plug-in security infrastructure
- Lotus strategy for keeping abreast of new security threats
- Summary & References
- Q & A

# Introductions

- Who we are
- What we do
- Focus of this presentation

## Security can be Complex and Frustrating for Developers, Administrators, and End Users

Secure Password Storage

Code Validation

Authentication

Certificate Management

SSL

Trust

Reverse Proxies

Single Sign On



**Lotus Notes can simplify security for you!**

## Agenda

- Introductions and Overview
- Security infrastructure available for plug-in's in Lotus Notes
- Security model for plug-in components in Lotus Notes
- Application plug-in's we ship with Lotus Notes and their Security Model
- Administering this plug-in security infrastructure
- Lotus strategy for keeping abreast of new security threats
- Summary & References
- Q & A

## Accounts framework

- Accounts document in personal address book persist connection related properties that are required to make a connection to and communicate with a local or remote server
  - Server URL
  - Username and Password
  - Authentication method to be used
  - Other connection details
- Accounts framework integrates these accounts with Java™ Authentication and Authorization Service (JAAS) to provide seamless Single Sign-On to Applications
- Account documents can be managed via programmatic API's, end user Accounts framework UI (user interface) or any custom application UI

## Accounts UI

**New Account**

Accounts provide the information needed by components to connect to servers. Create a new account to connect to a service not provided by default, such as a personal mail or news service.

**Basics**

Account Name:

Description:

Type:

Server:

**Log in information**

☒ Use direct log in or single sign-on:

Name:

Password:

☒ Use Domino single sign-on if available

Domino single sign-on server:

☐ Allow other accounts to use this log in information

☐ Use name and password of an existing account.

Account:

**- Advanced properties**

Home Portal URL:

Authentication URL:

Authentication Type:

**+ Notes Locations**

Portal Form (advanced)

TAM SPNEGO (advanced)

TAM Form (advanced)

J2EE Form (advanced)

HTTP Basic

OK Cancel



# Authentication Types supported by Accounts framework

- Basic authentication
- Form based authentication
  - J2EE-FORM
  - PORTAL
  - Tivoli Access Manager™ (TAM)
  - SiteMinder™
- TAM with SPNEGO Authentication (Simple and Protected GSSAPI Negotiation Mechanism)
- Domino LTPA (Lightweight Third Party Authentication)

# Client Side SSL and Proxy authentication support

## Client side SSL

- Cross-Certificates are stored in personal address book
  - Trust decisions made based on cross-certificates stored in the personal Address book
  - Certificates and Cross Certificates can be provisioned or imported manually by the user
- Users are prompted for trust decisions when an untrusted server certificate is presented

## Proxy authentication

- supports NTLM, NTLMv2 and proxy with authentication

## Signed Plugin Validation

- Lotus Notes client is a highly extensible platform
  - Malicious third party plug-in code could be installed by end user
- Signed plugin validation provides the administrator with control over what can and can not be installed on a Lotus Notes client based on code signer
  - Trusted Certificates are stored in personal address book
  - Certificates can be provisioned
  - Lotus Notes Client can be configured to Allow, Prompt, or Deny untrusted, expired, or unsigned code
- With Lotus Notes 8.5.1, a plugin's timestamp signature is now honored
  - validates that a signing certificate was valid at the time of signature, even if the certificate is now expired

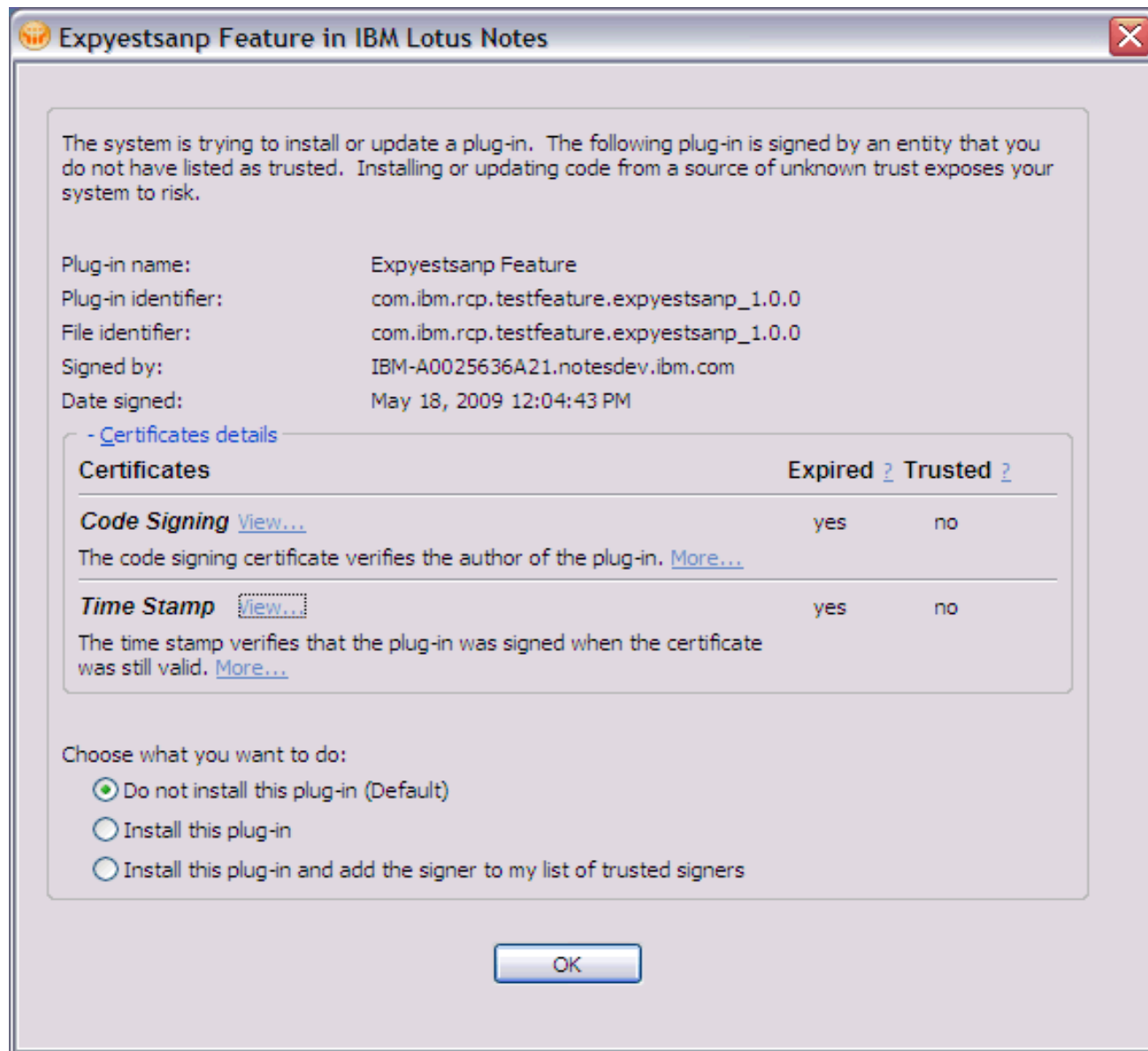
## Signed Plugin Validation UI (Tampered Jar file)



## Signed Plugin Validation UI (Unsigned Jar file)



## Signed Plugin Validation UI (Untrusted Jar file)



## Agenda

- Introductions and Overview
- Security infrastructure available for plug-in's in Lotus Notes
- Security model for plug-in components in Lotus Notes
- Application plug-in's we ship with Lotus Notes and their Security Model
- Administering this plug-in security infrastructure
- Lotus strategy for keeping abreast of new security threats
- Summary & References
- Q & A

## Web Container

What is it?

- A Web Server that runs Web Applications (Servlets, JSPs, etc.)

What is the security model?

- Server Side Authentication Support
  - Basic and Forms based authentication
- Transport Level SSL Server Sockets
  - Server Side Certificates Configured by user provided trust stores
- Pluggable back end credential repository
  - Default OSGi UserAdmin Service
  - LDAP, Active Directory, and other repositories can be used by implementing an interface and extending an extension point





## Embedded Browser

### What is it?

- Embedded browser is a configurable and manageable browser that you can embed in a client application
  - provides APIs that you can use to implement a web browser view
- Supports Internet Explorer on Windows® and Mozilla on Linux®

### What is the security model?

- APIs are provided that you can use to customize it and configure the Embedded Browser's security
  - Examples of configurable security settings:
    - List of domains from which a user cannot download unsolicited files.
    - List of domains for restricting navigation.
    - Turn on or off Java2 Applets, Bookmarks, local file access
    - List of domains for restricting unsolicited popups.
- Provides Single Sign On via integration with Accounts framework



## My Widgets (what is widgets and live text)

- A widget is a tool housed in My Widgets sidebar panel
  - can consist of one or more components and actions
  - actions can optionally contain a wired content type and recognizer to define the Live Text pattern to act on and specifically how to act on that Live Text
  - Widgets might include Notes Applications, Google Gadgets, services performed in Web pages, or feeds
- Live Text is a text string (e.g., address, part number, zip code) within any Lotus Notes document (e-mail, application, etc) that has been configured to be recognized as a certain type
- A widget can also be designed to provision eclipse plug-ins to Client

## My Widgets (what is the security model?)



- Widgets are deployed using a Notes database called catalog
  - Users can browse catalog and pick functionally
  - Administrator can Manage widgets, recognizers and actions
- Administrator can use desktop policy to
  - push categories of widgets to users
  - Whether Live Text is turned on
  - Who gets to install / create widgets
- Eclipse plug-in signatures are verified for trust before being installed on Client
- Widgets leverage accounts framework for authentication needs

### Desktop Settings

[Basics](#) | [Smart Upgrade](#) | [Applications](#) | [Widgets](#)

#### Widget Settings

Widget catalog server:	<input type="text"/>
Widget catalog application name:	<input type="text" value="toolbox.nsf"/>
Widget catalog categories to install:	<input type="text"/>
Enable Live Text:	<input type="text" value="Enable"/>
Show the My Widgets panel in the sidebar:	<input type="text" value="No"/>
Restrict the addition of widgets to specific types:	<input type="text" value="Disable"/>
Restrict provider IDs for installation/execution:	<input type="text" value="Disable"/>
Restrict extension point IDs for installation/execution:	<input type="text" value="Disable"/>
Create and manage an action:	<input type="text" value="Enable"/>
Create and manage recognizers and content types:	<input type="text" value="Yes"/>
Enable default recognizers:	<input type="text" value="Enable"/>
Send widgets using e-mail:	<input type="text" value="Enable"/>
Install widgets from e-mail or other:	<input type="text" value="Enable"/>
Install widgets from catalog:	<input type="text" value="Enable"/>
Publish to catalog so others can browse (subject to catalog ACLS):	<input type="text" value="Enable"/>



## My Widgets (what is the security model?)

- Widgets are defined by an Extension.xml file which does not contain the actual HTML/Javascript
  - This is simply an XML markup that specifies the
    - URL of where the widget is, for example a feed from cnn.com or the URL to a Google Gadget
    - ids of content types to bind to for livetext
  - Importing or exporting extension.xml does not export any confidential information, and is completely controllable by administrative policy
- Content of the widget is rendered in a sandboxed stand-alone single instance of the embedded browser
  - conforming to the industry standard web browser security model
  - All browser security policies restricting activeX, javascript execution within IE/Mozilla apply to the embedded browser



## Feed Reader

What is it?

- Feed reader side bar panel allows you to subscribe and manage your feeds subscriptions
- Feed subscriptions allow you to update Web content without requiring you to actively check for it

What is the security model?

- Feed reader in IBM Lotus Notes follows industry standard web browser security model
- All html content, including javascript, activeX controls, images are rendered in a web security sandbox, provided by the embedded browser control, provided by Microsoft IE on Windows, and Mozilla XULRunner on Mac and Linux



## Feed Reader (Security model)

- Previewing a feed
  - opens a separate single isolated browser control and the content of the feed is placed into this empty browser control
  - content is rendered in standard Internet Zone
  - any active/harmful content from a feed description element is filtered out, so that it will not be executed when displayed in the feeds preview window
- All applicable security restrictions imposed by Internet Explorer policies on windows are applied
  - If the security policies for IE disable ActiveX, Javascript, displaying images, all those same policies apply and will restrict the embedded browser and feed preview pane in IBM Lotus Notes



## Xpages Runtime (what is it?)

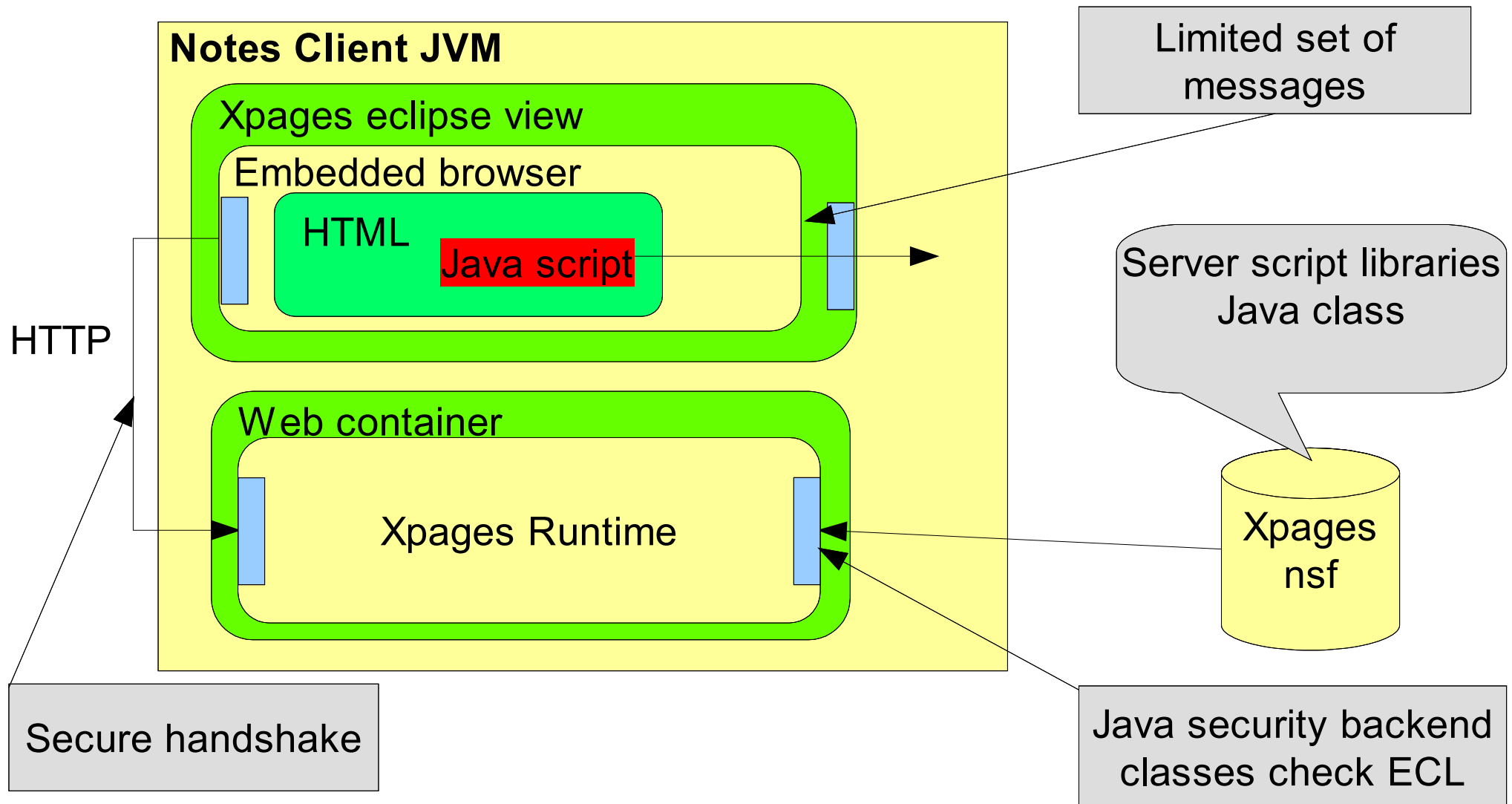
- XPages Runtime is a Java Servlet that run within the Notes client Web Container
  - Xpages Is a Web Application Framework based on JSF (JavaServer Faces)
  - XPages applications run within web container and display the user interface as an HTML application in a window running an embedded browser
- XPages applications are
  - distributed as an NSF, launch properties indicate the application is to be run using the XPages Runtime
  - rendered using the embedded browser and displayed in an Eclipse View component within the Notes Client

## Xpages Runtime (what is it?)

- Xpages technology allows developers to create rich internet applications that run in both a Web Browser and in the Notes Client
- XPages in the Notes Client is enhanced to provide better integration with the Notes Client
  - Dialog boxes for alerts, warnings, and info messages use rich client components to provide a better user experience
  - XPages application can run as a component in a Composite Application and interact with the other components through Property Broker by publishing events to other consumer components



## Xpages Runtime (Security Model)



## Xpages Runtime (Security Model)

- A secure 'handshake' happens between the Client (Xpages viewpart hosting the embedded browser control) and the Server (XPages Runtime in the Web Container) to verify the authenticity of requests to the XPages Runtime
- Property broker requests on behalf of browser are only allowed after a security check using the Notes backend classes is done to determine if all the singers of the XPages application have the capability to read and write to Property Broker
- Xpages runtime allows limited access to Java platform capabilities from JavaScript
- Active content filtering is leveraged to remove possibly malicious active content( scripts, tags ) in an input/output text control

## Xpages Runtime (Security Model)

- XPages on the Notes Client uses a number of existing Notes security features
  - Access to the Notes Client is protected by a Notes ID
  - Access to the XPages application and data is governed by an Access Control List (ACL)
  - Encryption can be enabled for a local application to prevent unauthorized users from accessing application data
  - XPages application design elements are all signed
  - Execution of security sensitive operations is controlled by an Execution Control List (ECL)
    - uses the capabilities granted under the "Using Workstation" tab for User Security to grant/deny capabilities to signers of XPages application
  - Java libraries check with a Java Security Manager whenever a security sensitive operation is performed

## Composite applications

- Composite Applications allow you to create and aggregate components on the screen to present content from multiple systems in a unified interface for the end user
  - provides collaboration in context, providing the information your people need, when they need it
- Allows you to Exploit IT investments and strategy with heterogenous technologies
  - Notes applications/databases
  - Lotus Component Designer components
  - Portlets and WSRP
  - Eclipse components (e.g. embedded browser)
  - other component types , including desktop applications

## Composite applications (Security Model)

- Composite applications that contain portlets leverage Home Portal account to implement SSO
- Administrator can push down policy to create the Home portal account settings
- Security model depends on what technology is used to create the component

The screenshot shows the 'Preferences' dialog box with the 'Home Portal Account' section selected in the left-hand tree. The right-hand pane displays the configuration for the Home Portal Account. It includes a description, a 'Basics' section with fields for Name, Description, Type, and Server, a 'Log in information' section with fields for Name and Password, and an 'Advanced properties' section with fields for Home Portal URL, Authentication URL, TAM junction, and Authentication Type. There is also a checkbox for 'Show Synchronization in Open list and in Preferences' and a 'Clear Home Portal Account' button.

**Preferences**

type filter text

- Accounts
- Basic Notes Client Configuration
- Calendar and To Do
- Composite Application Editor
- Contacts
- Feeds
- Fonts and Colors
- Home Portal Account
- IBM Lotus Symphony
- Live Text
- Locations
- Log Settings
- Logging Monitor
- Lotus Connections
- Mail
- Notes Ports
- Regional Settings
- Replication
- Search
- Spell Check
- Toolbar
- Web Browser
- Widgets
- Windows and Themes

**Home Portal Account**

The Home Portal Account is used to connect to the home portal server. You cannot change the name of this account but you can edit the description, the server address and authentication type you use to connect to the home portal server.

**Basics**

Name: Home Portal Account

Description: Home Portal Account

Type: HTTP

Server: http://myportal.com

**Log in information**

Name:

Password:

**Advanced properties**

Home Portal URL: http://myportal.com

Authentication URL: http://myportal.com

TAM junction (obtain from your Help Desk):

Authentication Type: PORTAL-FORM

☐ Show Synchronization in Open list and in Preferences

Clear Home Portal Account

OK Cancel

## Agenda

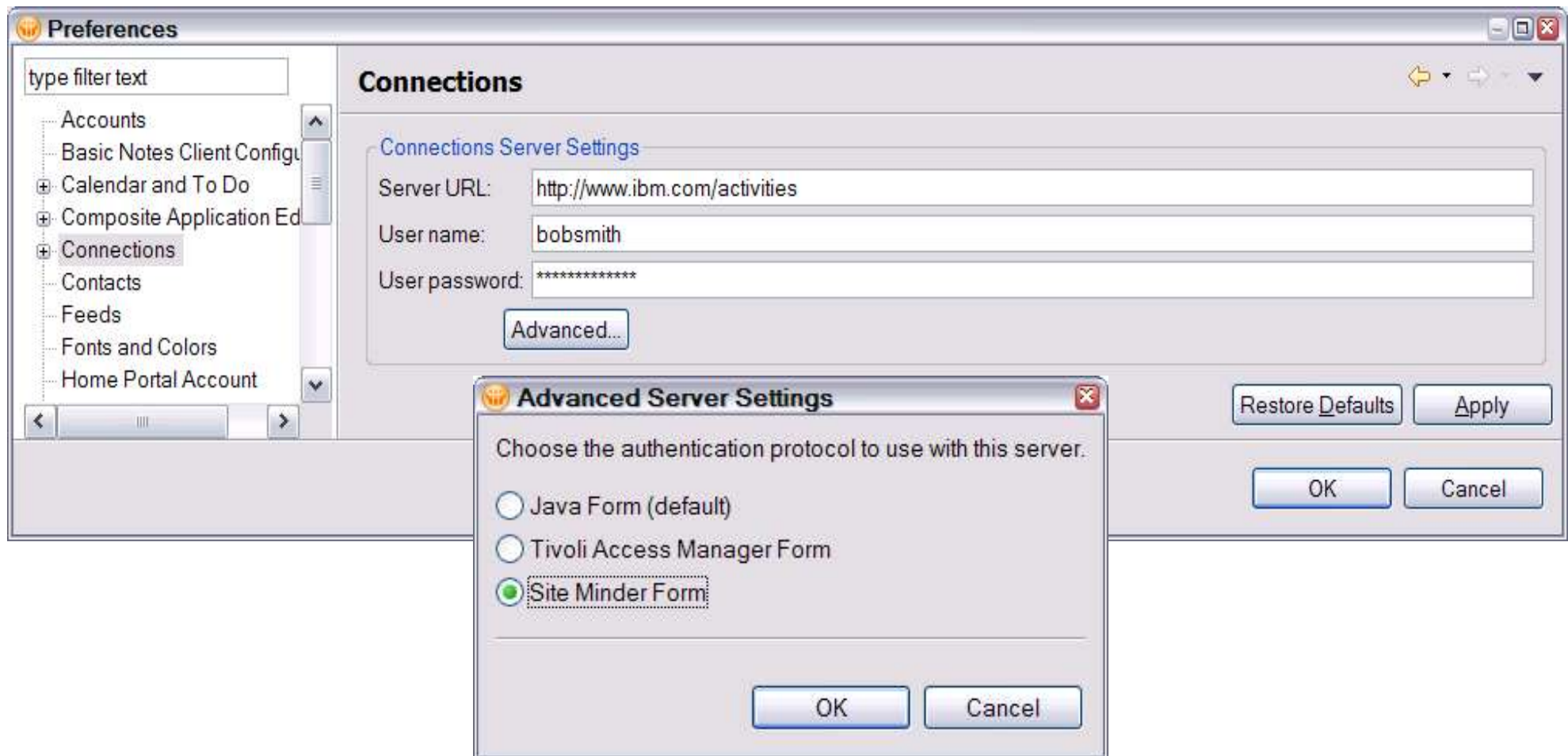
- Introductions and Overview
- Security infrastructure available for plug-in's in Lotus Notes
- Security model for plug-in components in Lotus Notes
- Application plug-in's we ship with Lotus Notes and their Security Model
- Administering this plug-in security infrastructure
- Lotus strategy for keeping abreast of new security threats
- Summary & References
- Q & A





## IBM Lotus Connections™

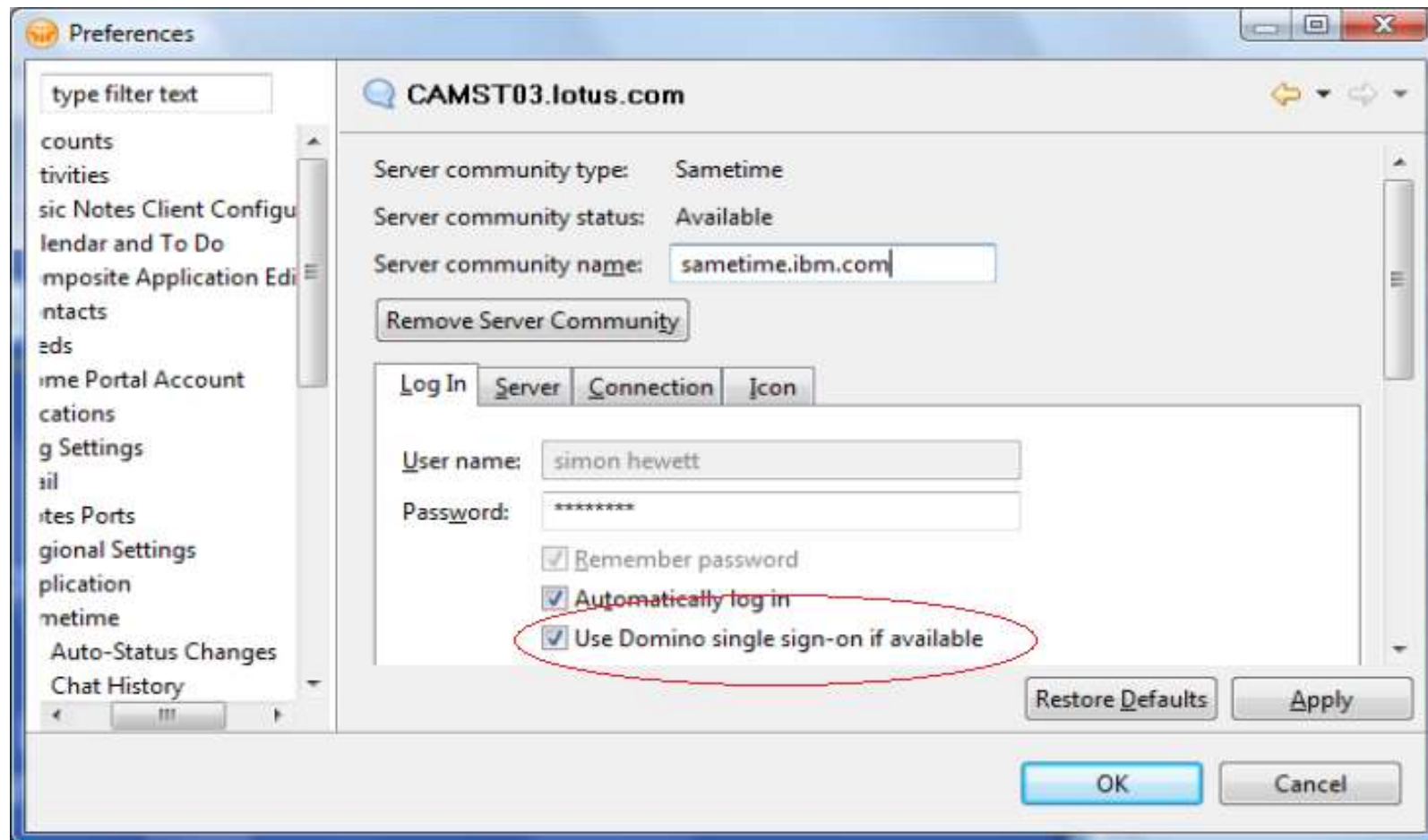
- Accounts to store credentials and connection information
- Java Authentication and Authorization Service (JAAS) to securely authenticate with the Lotus Connections server



## IBM Lotus Sametime™



- Accounts used to store credentials and connection information (v. 8)
- JAAS, using the Domino LTPA login module, as an optional authentication mechanism





## Agenda

- Introductions and Overview
- Security infrastructure available for plug-in's in Lotus Notes
- Security model for plug-in components in Lotus Notes
- Application plug-in's we ship with Lotus Notes and their Security Model
- Administering this plug-in security infrastructure
- Lotus strategy for keeping abreast of new security threats
- Summary & References
- Q & A



## Administrator Policy Settings (Signed plug-ins)

### Security Settings

[Basics](#) | 
 [Password Management](#) | 
 [Execution Control List](#) | 
 [Keys and Certificates](#) | 
 [Signed Plug-ins](#) | 
 [Portal Server](#) | 
 [ID Vault](#) | 
 [Proxies](#) | 
 [Comments](#) | 
 [Administration](#)

Signed Plug-in Basics		How to apply this setting:	Inherit from parent policy:	Enforce in child policies:
Installation of plug-ins that are expired or not yet valid:	<input checked="" type="radio"/> Ask the user <input type="button" value="v"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Installation of unsigned plug-ins:	<input checked="" type="radio"/> Ask the user <input type="button" value="v"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Installation of plug-ins signed by an unrecognized entity:	<input checked="" type="radio"/> Ask the user <input type="button" value="v"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Trust IBM plug-in signing certificate:	<input checked="" type="radio"/> Always trust for install <input type="button" value="v"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Ignore expiration for time stamping certificate:	<input checked="" type="radio"/> Always install <input type="button" value="v"/>	<input type="checkbox"/> Don't set value	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

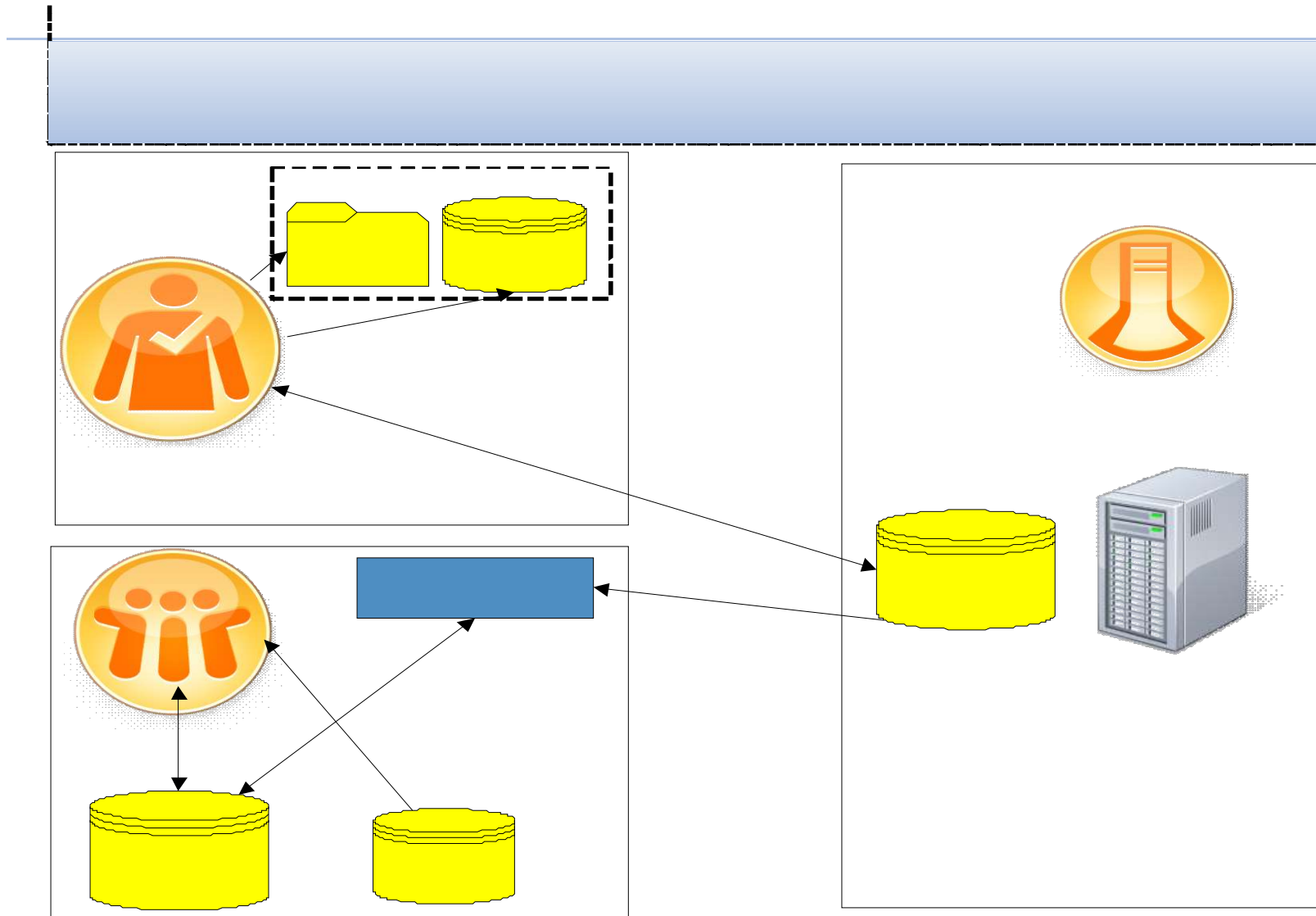
## Managing Administrative Trust Defaults (Purpose & Scope)

- Customers have a lot of administrative trust defaults defined in their public address book, internet certificates and cross-certificates from companies they trust
  - they need the ability to keep those certificates in sync with Client PNAB
  - if a certificate expires and they get a new one from the companies outside they need an easy way to distribute them to the clients PNAB
- Usage scenario's which benefit from pushing down trust defaults
  - silent deployment of signed plug-ins via catalogue
  - SSL, SMIME...

# Managing Administrative Trust Defaults (Supported Scenarios)

- Pushing down administrative trust defaults via domino policy
- Pushing down administrative trust defaults via media kit
  - Supports deployment which do not leverage policies
  - Provides means to bootstrap trust defaults for any form of rolling out traditional installs via SMS etc

## Managing Administrative Trust Defaults (Overview)





## Managing Administrative Trust Defaults (Policy UI)

Earliest allowable key creation date: 08/0

Spread new key generation for all users over this many days: 180

Maximum number of days the old key should remain valid after the new key has been created: 365

**Document/Mail Encryption Settings**

Encryption requirements: ☐ Use (requi

**Certificate Expiration Settings**

Warning Period: 21

Custom Warning Message:

**On-line Certificate Status Protocol (OCSP)**

☐ Enable OCSP checking

**Administrative Trust Defaults**

Update Links

Select the certificates to trust

Notes Cross Certificates | Internet Cross Certificates | Internet Certifiers

Select All

- ☐ Baltimore CyberTrust Mobile Root/CyberTrust/Baltimore/IE
- ☐ Baltimore CyberTrust Root/CyberTrust/Baltimore/IE
- ☐ CyberTrust JAPAN Root CA/CyberTrust Japan, Inc./JP
- ☐ CyberTrust JAPAN Secure Server CA/CyberTrust Japan, Inc./JP
- ☐ Entrust.net Certification Authority (2048)/(c) 1999 Entrust.net Limited/www.entr
- ☐ Entrust.net Client Certification Authority/(c) 1999 Entrust.net Limited/www.entr
- ☐ Entrust.net Client Certification Authority/(c) 2000 Entrust.net Limited/www.entr
- ☐ Entrust.net Secure Server Certification Authority/(c) 1999 Entrust.net Limited/
- ☐ Entrust.net Secure Server Certification Authority/(c) 2000 Entrust.net Limited/
- ☐ GTE CyberTrust Global Root/GTE CyberTrust Solutions, Inc./GTE Corpora
- ☐ GTE CyberTrust Root 2/GTE CyberTrust Solutions, Inc./GTE Corporation/L
- ☐ GTE CyberTrust Root 3/GTE CyberTrust Solutions, Inc./GTE Corporation/L
- ☐ GTE CyberTrust Root 4/GTE CyberTrust Solutions, Inc./GTE Corporation/L
- ☐ GTE CyberTrust Root 5/GTE CyberTrust Solutions, Inc./GTE Corporation/L
- ☐ GTE CyberTrust Root/GTE Corporation/US
- ☐ IBM Certification Authority/International Business Machines Corporation/US
- ☐ VeriSign Class 1 Public Primary Certification Authority - G3/(c) 1999 VeriSign
- ☐ VeriSign Class 2 Public Primary Certification Authority - G3/(c) 1999 VeriSign
- ☐ VeriSign Class 3 Public Primary Certification Authority - G3/(c) 1999 VeriSign
- ☐ VeriSign Class 4 Public Primary Certification Authority - G3/(c) 1999 VeriSign
- ☐ WAP CA/(c) 1999 Entrust.net Limited/www.entrust.net/WAPCPS incorp. by re
- ☐ EMAIL=certificate@trustcenter.de/OU=TC TrustCenter Class 0 CA/O=TC T

OK

Cancel

The screenshot shows the IBM Lotus Notes Domino Administrator interface. The left sidebar displays the 'Domino Directory' tree with 'Certificates' selected under 'Policies'. The main window shows a list of certificates. A context menu is open over the list, showing options like 'Apply Delegation to All Selected Entries', 'Export Certificates to Deploy Database', and 'Import Internet Certificates'. The certificate list includes entries from 'TC TrustCenter' and 'Thawte Consulting'.

**Domino Directory Tree:**

- People
  - by Organization
  - by Client View
  - Alternate Location
  - Certificate Entries
- Policies
  - Dynamic Policies
  - Settings
- Groups
- Configuration
  - Servers
  - Messaging
  - Replication
  - Directory
  - Policies
    - Dynamic Policies
    - Settings
  - Web
  - Clusters
  - Security
    - Certificates**
    - ID Vaults
  - Standard Client
    - Accounts
  - Miscellaneous
  - Standard-Client

**Context Menu Options:**

- Apply Delegation to All Selected Entries
- Edit Directory Profile
- Edit Administration ECL
- Set Secure Internet Password
- Add Admin Roles to Access Control List
- Remove Directory Profile
- Update AutoDialer Schedule
- Export Certificates to Deploy Database**
- Import Internet Certificates
- Edit Document
- Send Document
- Forward
- Move To Folder...
- Remove From Folder
- View Options
- Preview in Web Browser

**Certificate List:**

Issued To	Issued To
cate@trustcenter.de/OU=TC TrustCenter Class 0 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE	cate@trustcenter.de/OU=TC TrustCenter Class 0 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE
cate@trustcenter.de/OU=TC TrustCenter Class 1 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE	cate@trustcenter.de/OU=TC TrustCenter Class 1 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE
cate@trustcenter.de/OU=TC TrustCenter Class 2 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE	cate@trustcenter.de/OU=TC TrustCenter Class 2 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE
cate@trustcenter.de/OU=TC TrustCenter Class 3 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE	cate@trustcenter.de/OU=TC TrustCenter Class 3 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE
cate@trustcenter.de/OU=TC TrustCenter Class 4 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE	cate@trustcenter.de/OU=TC TrustCenter Class 4 CA/O=TC TrustCenter for Security in Data Networks GmbH/L=Hamburg/ST=Hamburg/C=DE
nal-basic@thawte.com/CN=Thawte Personal Basic CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA	nal-basic@thawte.com/CN=Thawte Personal Basic CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA
nal-freemail@thawte.com/CN=Thawte Personal Freemail CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA	nal-freemail@thawte.com/CN=Thawte Personal Freemail CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA
nal-premium@thawte.com/CN=Thawte Personal Premium CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA	nal-premium@thawte.com/CN=Thawte Personal Premium CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA
nal-premium-server@thawte.com/CN=Thawte Premium Server CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA	nal-premium-server@thawte.com/CN=Thawte Premium Server CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA
EMAIL=server-certs@thawte.com/CN=Thawte Server CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA	EMAIL=server-certs@thawte.com/CN=Thawte Server CA/OU=Certification Services Division/O=Thawte Consulting/L=Cape Town/ST=Western Cape/C=ZA
EMAIL=webmaster@belsign.be/CN=BelSign Class 1 CA/OU=BelSign Class 1 Certificate Authority/O=BelSign NV/L=Brussels/C=BE	EMAIL=webmaster@belsign.be/CN=BelSign Class 1 CA/OU=BelSign Class 1 Certificate Authority/O=BelSign NV/L=Brussels/C=BE
EMAIL=webmaster@belsign.be/CN=BelSign Class 2 CA/OU=BelSign Class 2 Certificate Authority/O=BelSign NV/L=Brussels/C=BE	EMAIL=webmaster@belsign.be/CN=BelSign Class 2 CA/OU=BelSign Class 2 Certificate Authority/O=BelSign NV/L=Brussels/C=BE
EMAIL=webmaster@belsign.be/CN=BelSign Class 3 CA/OU=BelSign Class 3 Certificate Authority/O=BelSign NV/L=Brussels/C=BE	EMAIL=webmaster@belsign.be/CN=BelSign Class 3 CA/OU=BelSign Class 3 Certificate Authority/O=BelSign NV/L=Brussels/C=BE
EMAIL=webmaster@belsign.be/CN=BelSign Object Publishing CA/OU=BelSign Object Publishing Certificate Authority/O=BelSign NV/L=Brussels/C=BE	EMAIL=webmaster@belsign.be/CN=BelSign Object Publishing CA/OU=BelSign Object Publishing Certificate Authority/O=BelSign NV/L=Brussels/C=BE
EMAIL=webmaster@belsign.be/CN=BelSign Secure Server CA/OU=BelSign Secure Server Certificate Authority/O=BelSign NV/L=Brussels/C=BE	EMAIL=webmaster@belsign.be/CN=BelSign Secure Server CA/OU=BelSign Secure Server Certificate Authority/O=BelSign NV/L=Brussels/C=BE
Entrust.net	Entrust.net
IE	IE
JP	JP
US	US



# Lotus Notes Media Kit Security Policy Settings

- `com.ibm.rcp.security.update/EXPIRED_SIGNATURE_POLICY=PROMPT`
- `com.ibm.rcp.security.update/UNSIGNED_PLUGIN_POLICY=PROMPT`
- `com.ibm.rcp.security.update/UNTRUSTED_SIGNATURE_POLICY=PROMPT`
- `com.ibm.rcp.security.update/TRUST_CERTIFICATE_AUTHORITIES=false`
- `com.ibm.rcp.security.update/TSAEXPIRED_SIGNATURE_POLICY=ALLOW`

## Agenda

- Introductions and Overview
- Security infrastructure available for plug-in's in Lotus Notes
- Security model for plug-in components in Lotus Notes
- Application plug-in's we ship with Lotus Notes and their Security Model
- Administering this plug-in security infrastructure
- Lotus strategy for keeping abreast of new security threats
- Summary & References
- Q & A

## Agenda

- Introductions and Overview
  - Security infrastructure available for plug-in's in Lotus Notes
  - Security model for plug-in components in Lotus Notes
  - Application plug-in's we ship with Lotus Notes and their Security Model
  - Administering this plug-in security infrastructure
  - Lotus strategy for keeping abreast of new security threats
- Summary & References
- Q & A

## Summary & References

- Summary
- Lotusphere Sessions:
  - AD205      Developing and Deploying Secure Java Applications with IBM Lotus Notes Client
  - ID207      IBM Lotus Protector for Mail Security: Spam and Content Protection
  - ID602      Lotus Brings Security to the Cloud with IBM
  - ID204      Getting the Most from IBM Lotus Domino Security

## Questions and Answers...



## Legal Disclaimer

© IBM Corporation 2009. 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, and Lotusphere are trademarks of International Business Machines Corporation 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.