

IBM® WEBSHERE® PORTAL 6.1
Deliver Exceptional User Experiences

WebSphere software ibm.com/websphere/portal



【IBM SOA講堂】 Lotus動員協作： Portal 6.1 SSO 應用

鄭志傑
IBM 資深資訊工程師
chengcc@tw.ibm.com

IBM Certified System Administrator
WebSphere Portal

Agenda

- ① What's SSO
- ① WebSphere Portal v6.x Security Overview
- ① How to do web based SSO by using Portal
- ① What's new in v6.1



Single Sign-on 目的

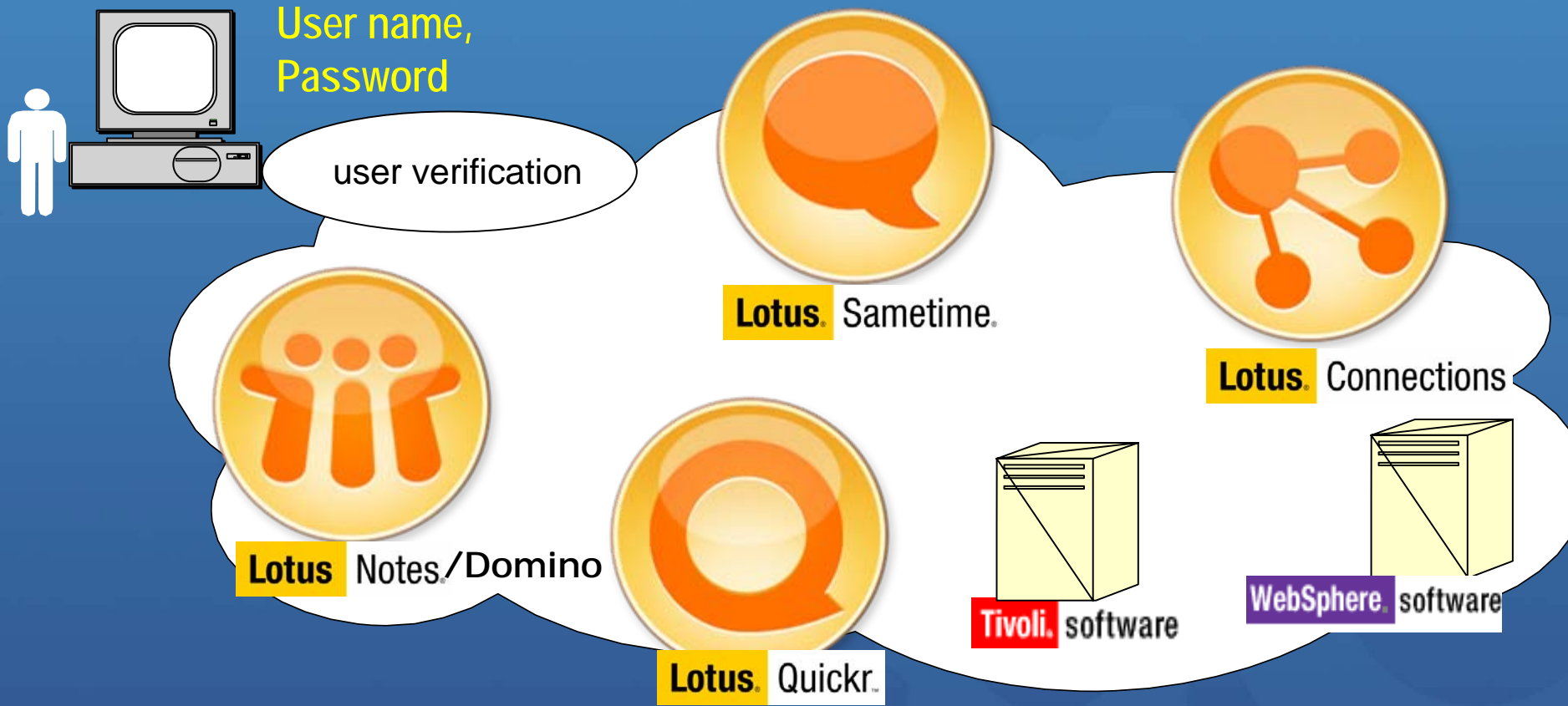
- Fewer password prompts, fewer passwords in general
 - Happy users!
 - Helpdesk and administrators have less work.



- Good security



Login once per session



A logged-in user accesses the SSO environment without repeating login steps.

Lightweight Third Party Authentication (LTPA)

- LTPA is one of IBM's SSO solutions

Lotus software

WebSphere software

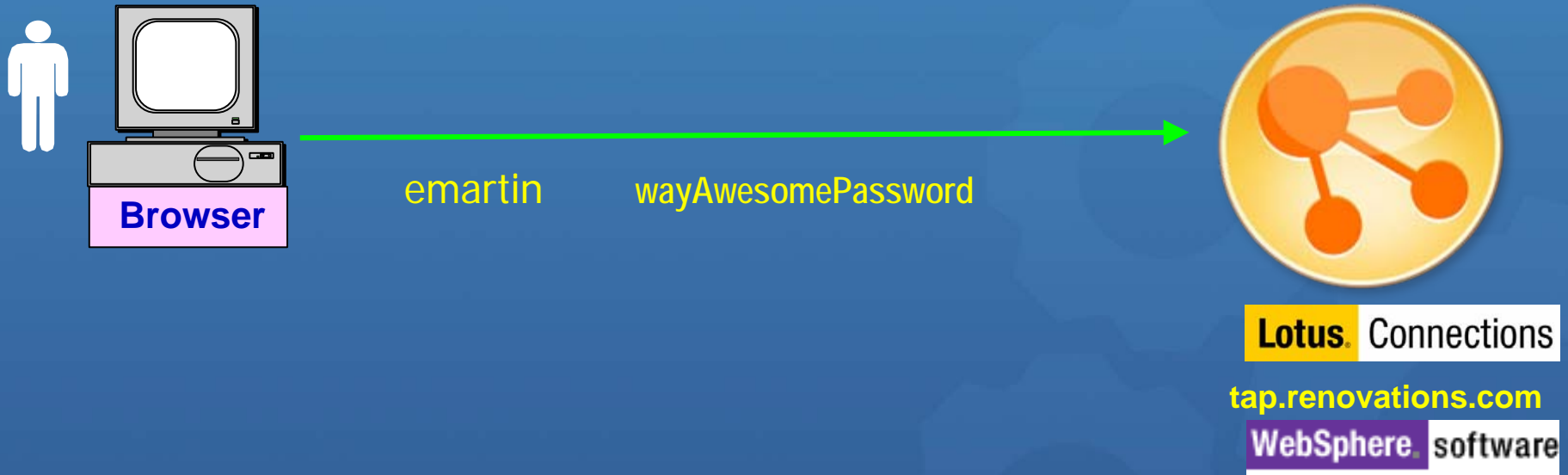
Tivoli software

- Open architecture for interoperability with other SSO
 - IBM Lotus Domino®, IBM WebSphere Application Server® and IBM Tivoli Access Manager® allow integration of other SSO applications.
 - IBM continues to improve LTPA integration with **Windows desktop and Kerberos security.**



LTPA encoded token represents a logged in user

<https://dogear.tap.renovations.com/atom/tag=coolStuff&email=ctaylor@renovations.com>



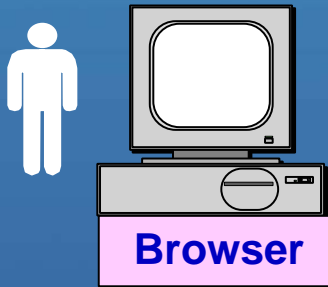
User provides login name and password.

Server looks up the user in the directory and verifies password.



LTPA encoded token represents a logged in user

<https://dogear.tap.renovations.com/atom/tag=coolStuff&email=ctaylor@renovations.com>



Connections content



Lotus Connections

tap.renovations.com

WebSphere software

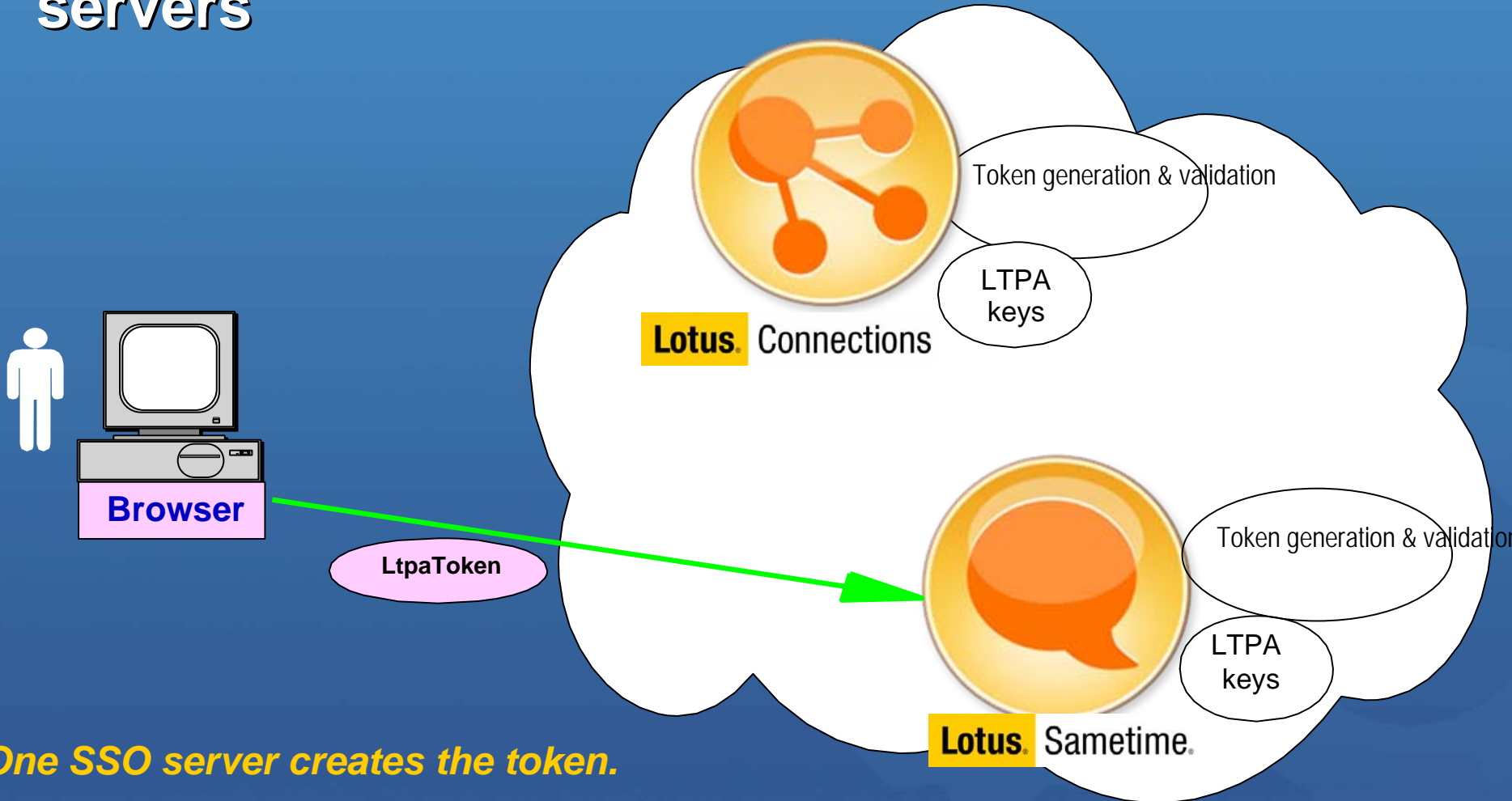
```

cookie:
  LtpaToken
value:
  <encoded>
domain:
  renovations.com
    
```

Server creates and returns an LTPA token containing user's name.



Valid LTPA token identifies user to various IBM servers



One SSO server creates the token.

Others servers validate the token using shared cryptographic keys.

Agenda

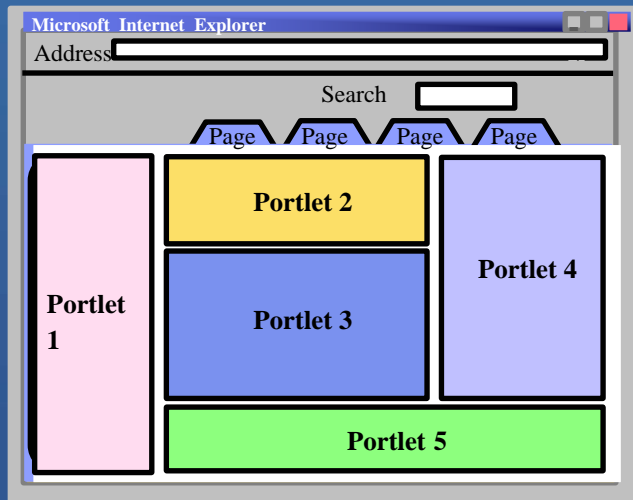
- ① What's SSO
- ① WebSphere Portal v6.x Security Overview
- ① How to do web based SSO by using Portal
- ① What's new in v6.1



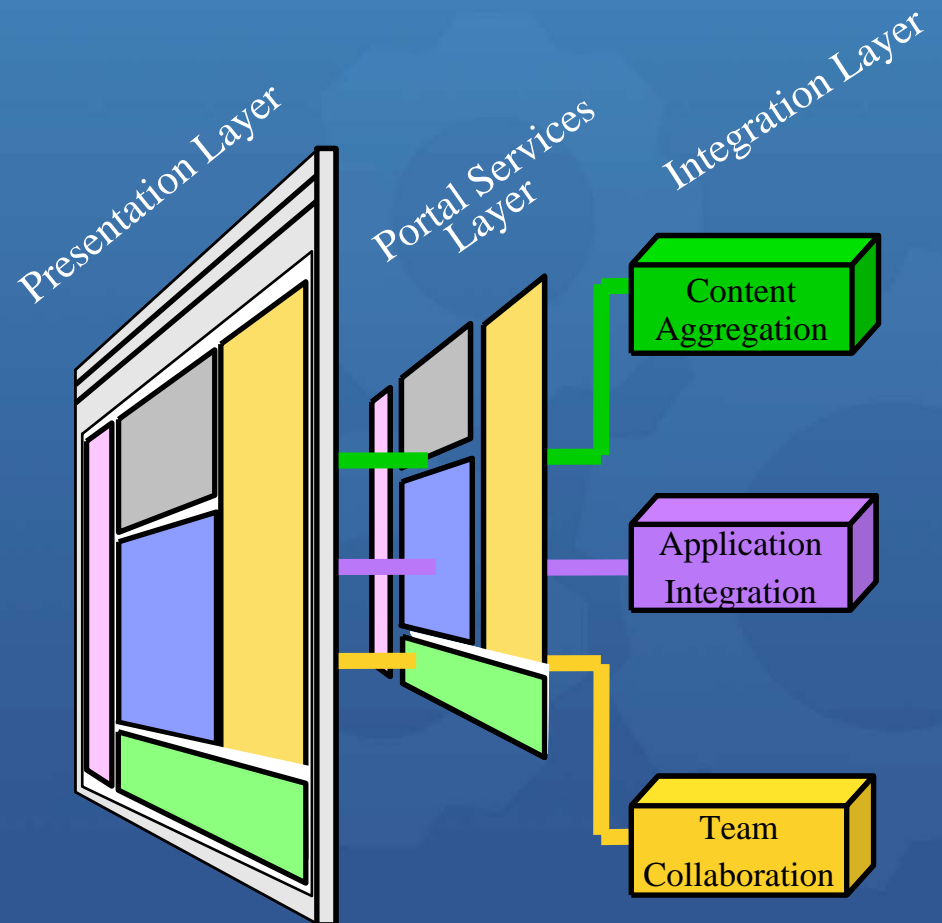
Portal 基本概念：談論到...

user interface...

- a UI framework for integrating "other" applications, content and processes.
- includes additional infrastructure like search, single sign-on, directory management, etc.



...and Integration



Portal 概念：安全(Security)

- **Authentication** – Portal relies on WAS for authentication
 - WAS supports LDAP, WMM or Custom registry for user authentication
 - WAS provides authentication exits in TAI
- **Authorization** – Portal uses PAC (Portal Access Control)
 - Roles Based (role = roletype@resource; eg. Editor@MyNews); Roles are assigned to principals (user or user groups)
 - Portal provides ability to externalize security to Siteminder and Tivoli
- **Default SSO implementation uses LTPA**

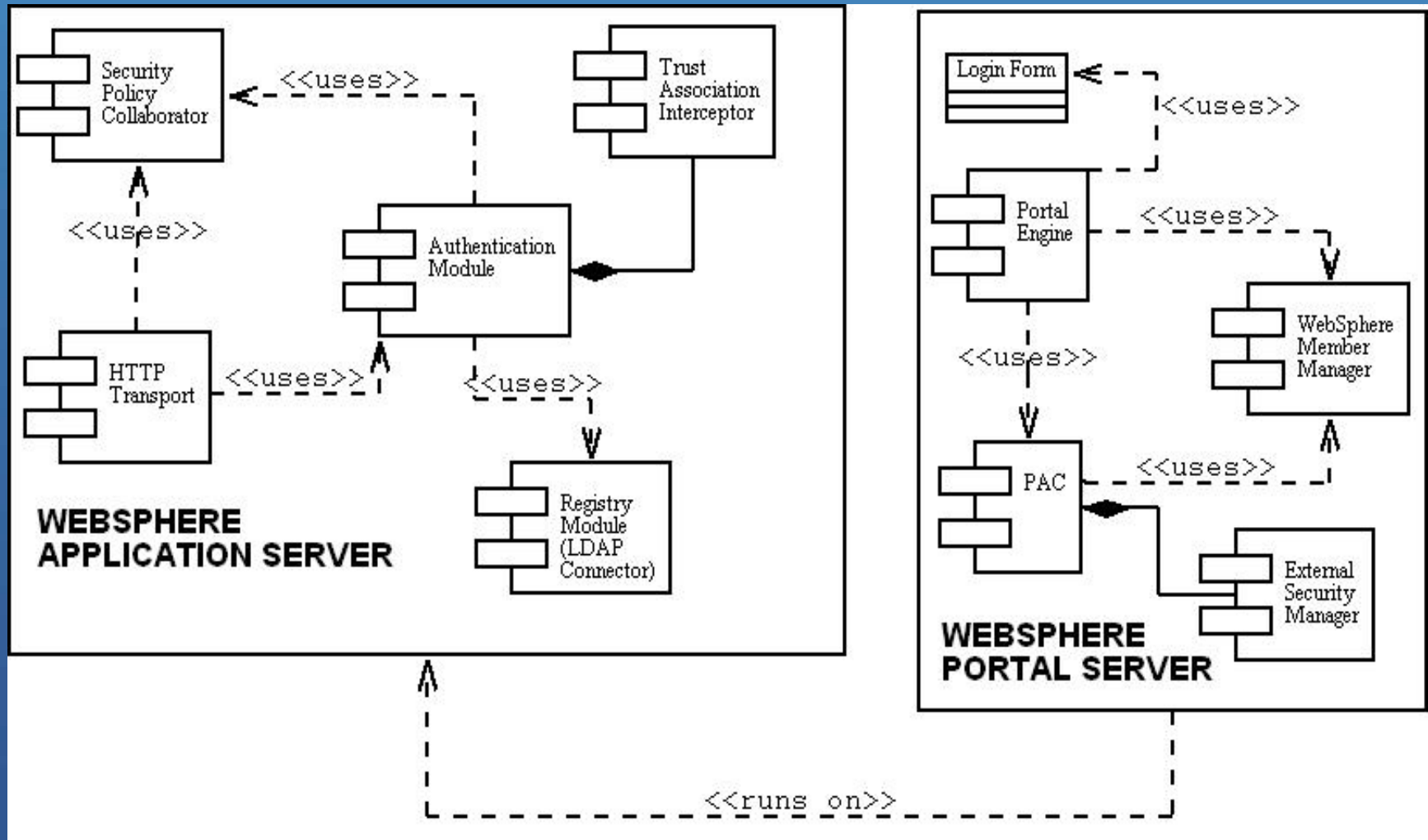


Portal 概念：安全(Security)

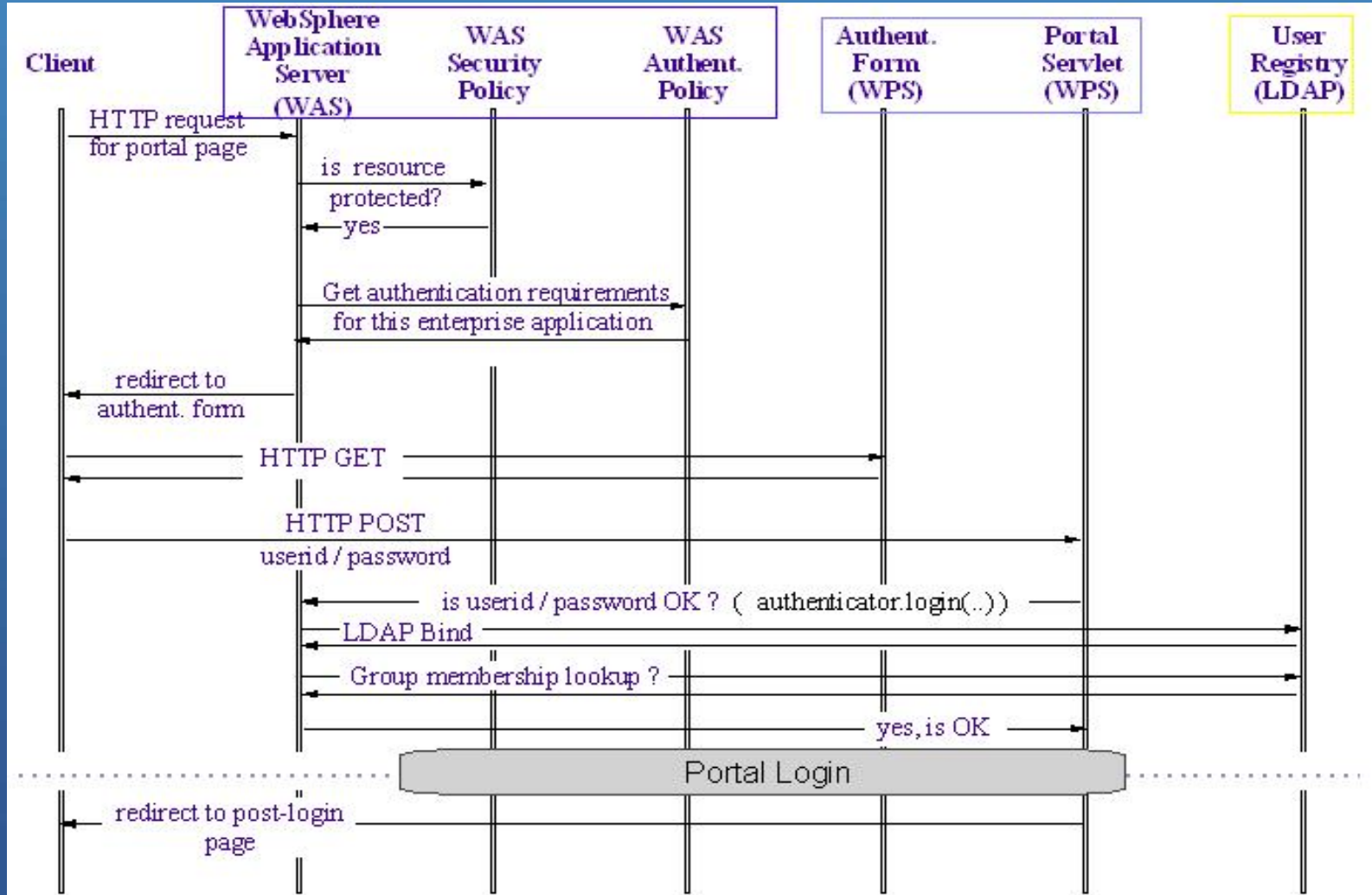
- **WMM – WebSphere Member Manager** – used in user and group lookups
 - Provides an abstraction to underlying user store (can be LDAP, DB or LDAP+DB)
- Portal provides **Credential Vault** to map user identities within Portal, hence providing backend SSO capabilities
 - Credential Vault is implemented as a Portlet Service



Portal 概念 :Component Diagram (authentication)



Portal 概念 : Sequence Diagram (authentication)

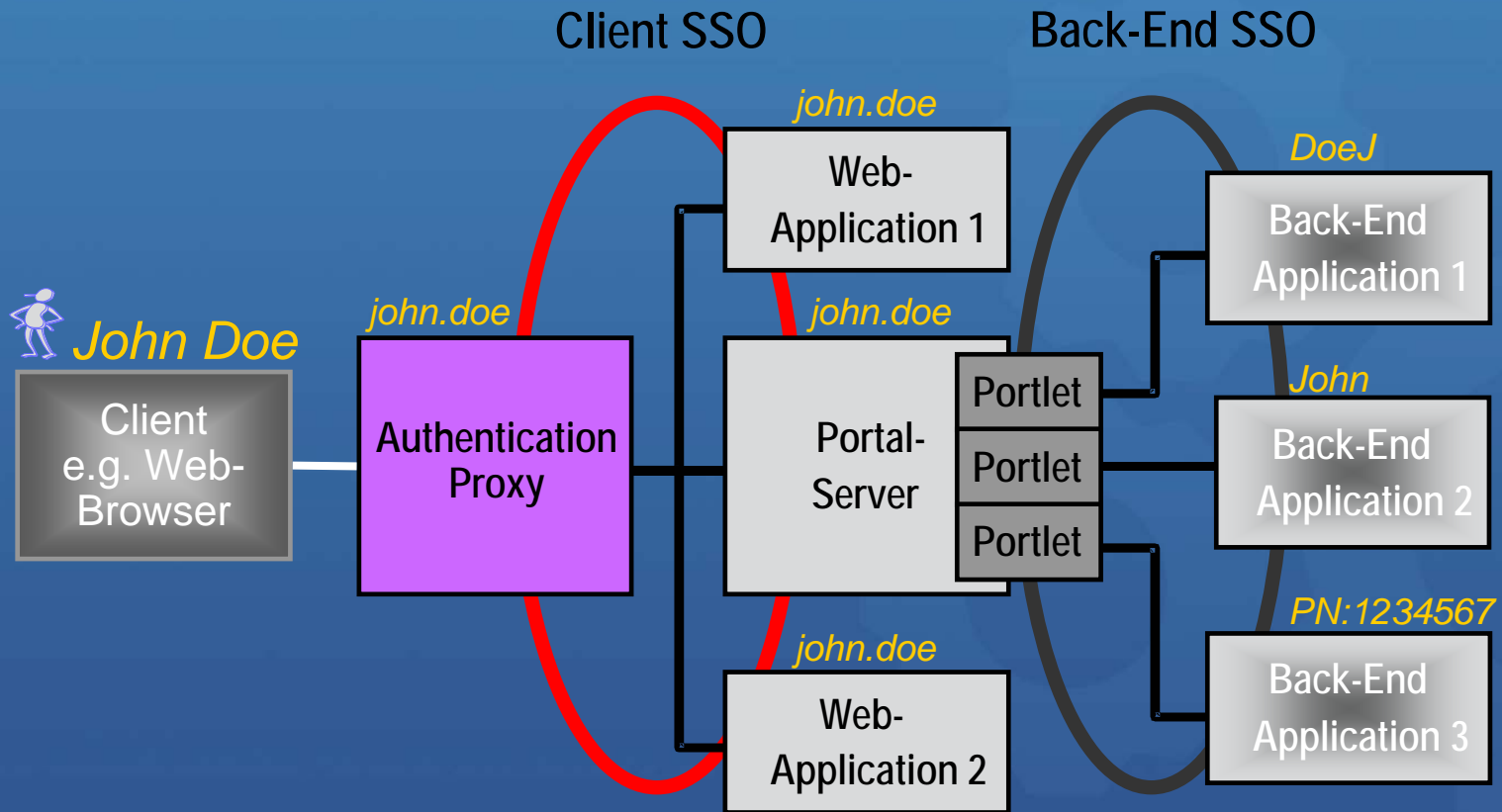


Agenda

- ① What's SSO
- ① WebSphere Portal v6.x Security Overview
- ① How to do web based SSO by using Portal
- ① What's new in v6.1

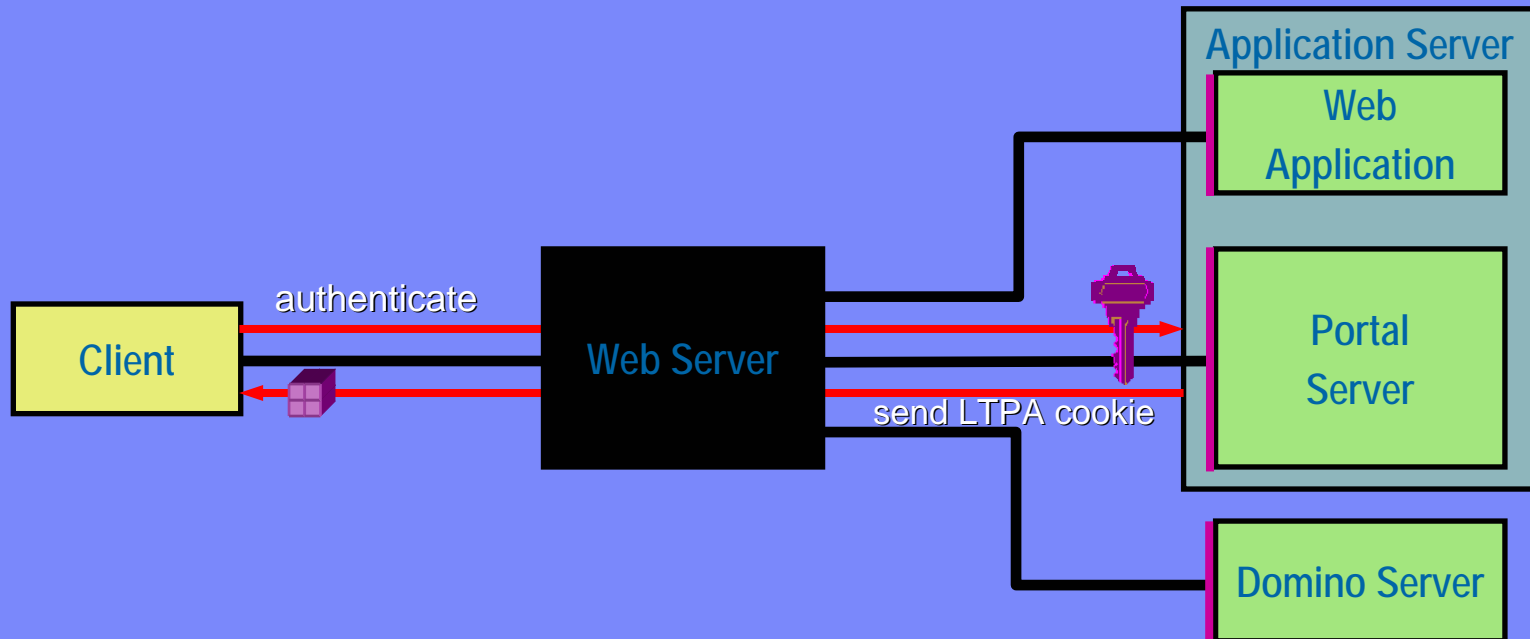


Portal Single Sign-On Realms



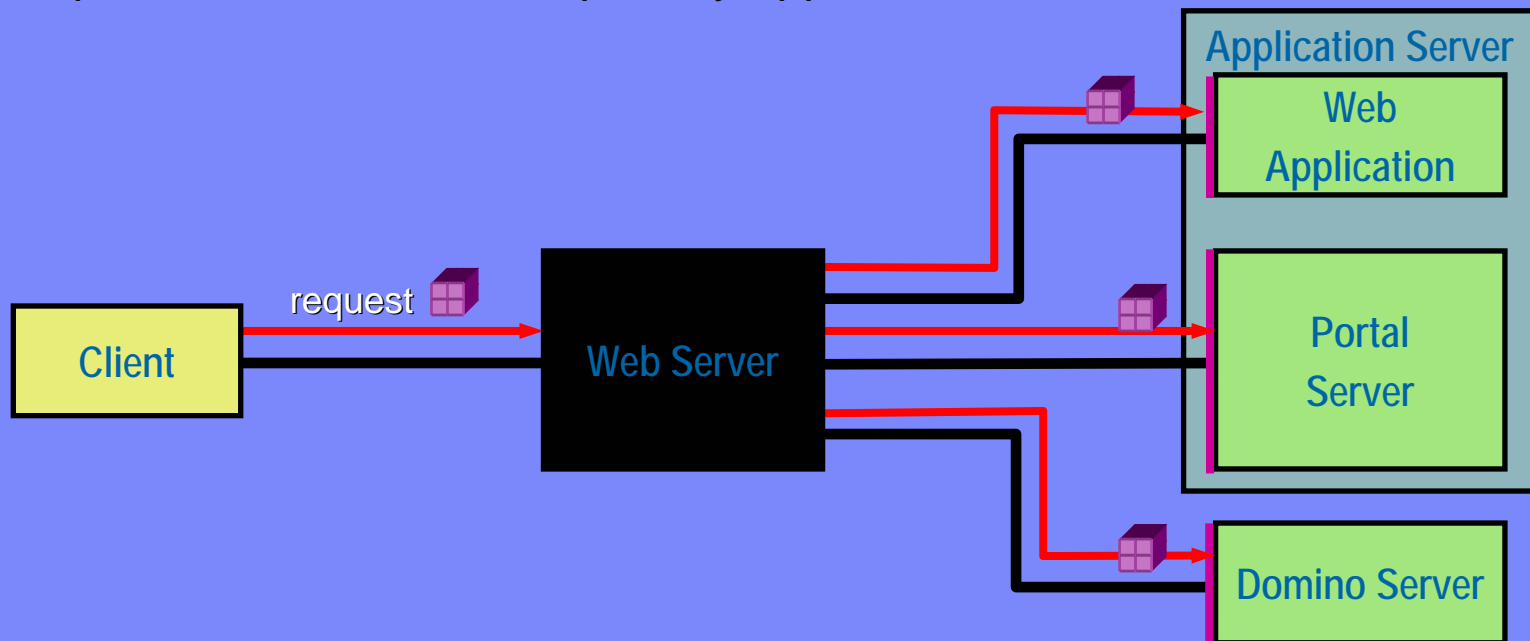
Version 1: WebSphere LTPA Single Sign-On

Step 1: User authenticates



Version 1: WebSphere LTPA Single Sign-On

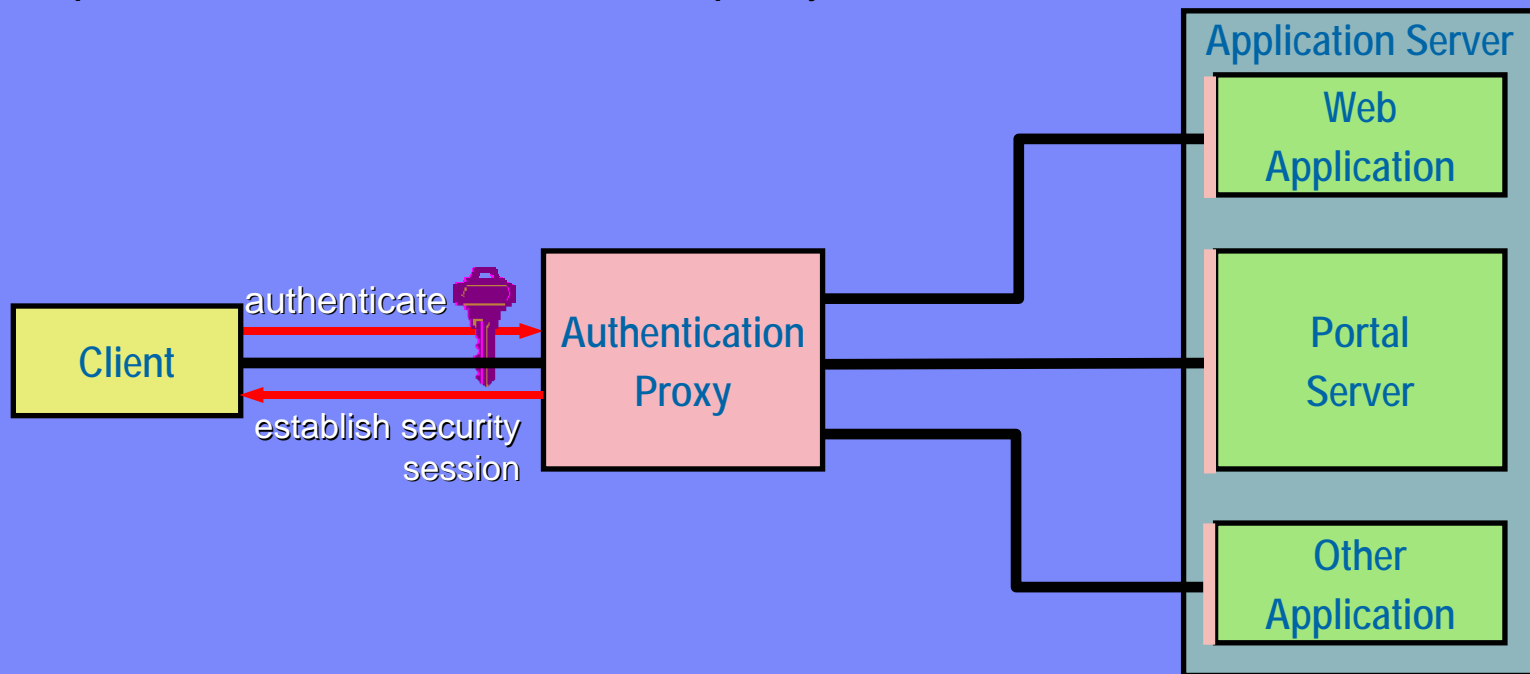
Step 2: LTPA token is accepted by applications



 LTPA token contains encrypted user ID

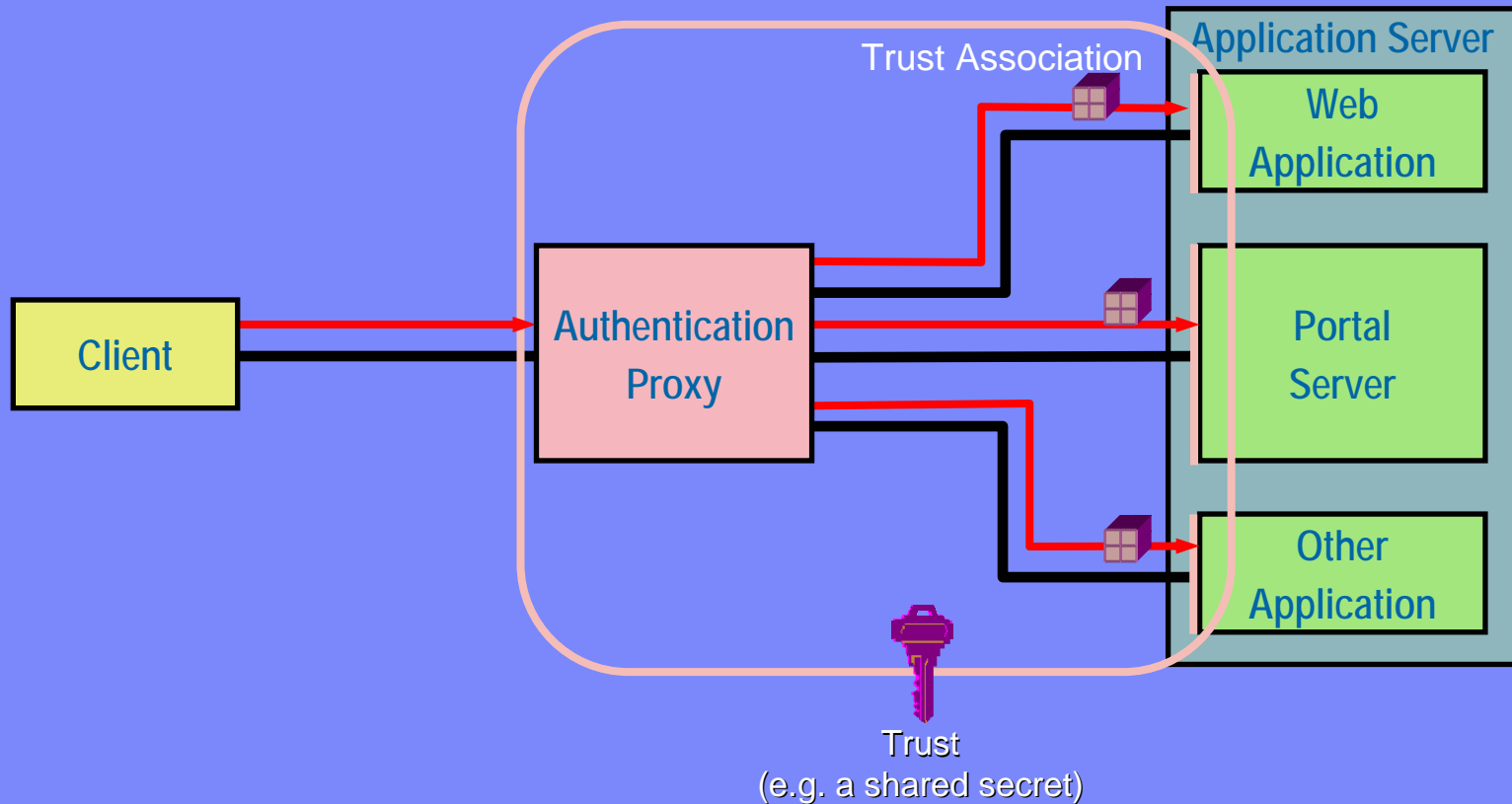
Version 2: Authentication Proxy SSO (via TAI)

Step 1: User authenticates at the proxy



Version 2: Authentication Proxy SSO (via TAI)

Step 2: Proxy tokens are accepted by applications

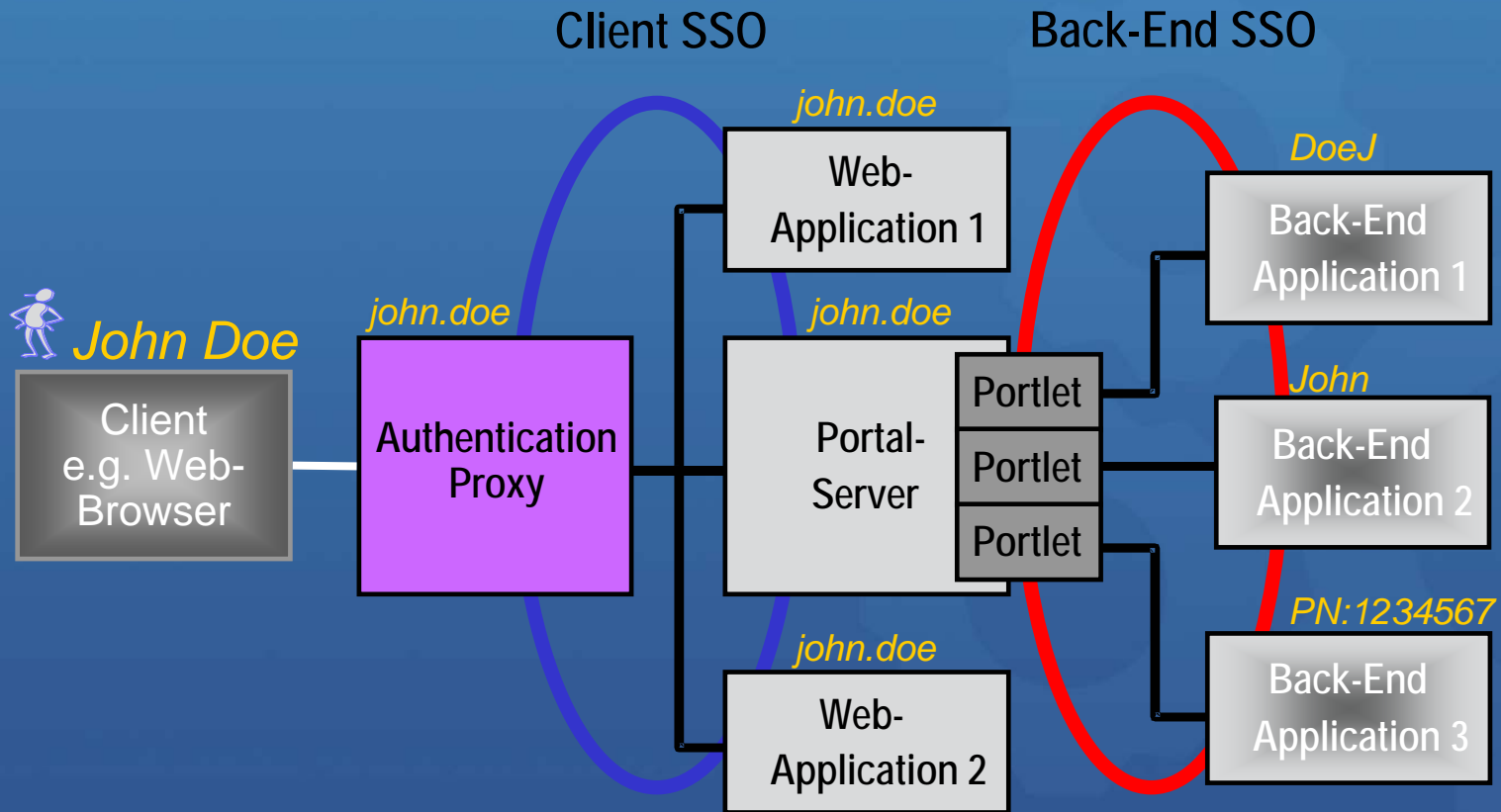


Portal/Windows SSO

- Supported out-of-the-box by Tivoli Access Manager
 - WebSEAL supports SPNEGO to ask for AD/Kerberos Ticket in an HTTP Header
 - Requires SPNEGO enabled browser (e.g. MS IE)
- Not supported out-of-the-box by WAS/Portal standalone
 - But well known how to do so via ISSW services
 - SPNEGO TAI++ implementation already built by ISSW
 - ✓ Not all the building blocks are officially supported
- SmartCard authentication supported by Tivoli Access Manager or via Windows SSO ...



WP to Backend SSO: The Portal Credential Vault



Portal to Backend SSO: WP Credential Vault

A Portlet Service for storing and retrieving SSO Credentials including the user's JAAS Subject that was built during login.

+

A vault adapter interface to integrate vault implementations like the Tivoli Access Manager Global Sign-On Lockbox

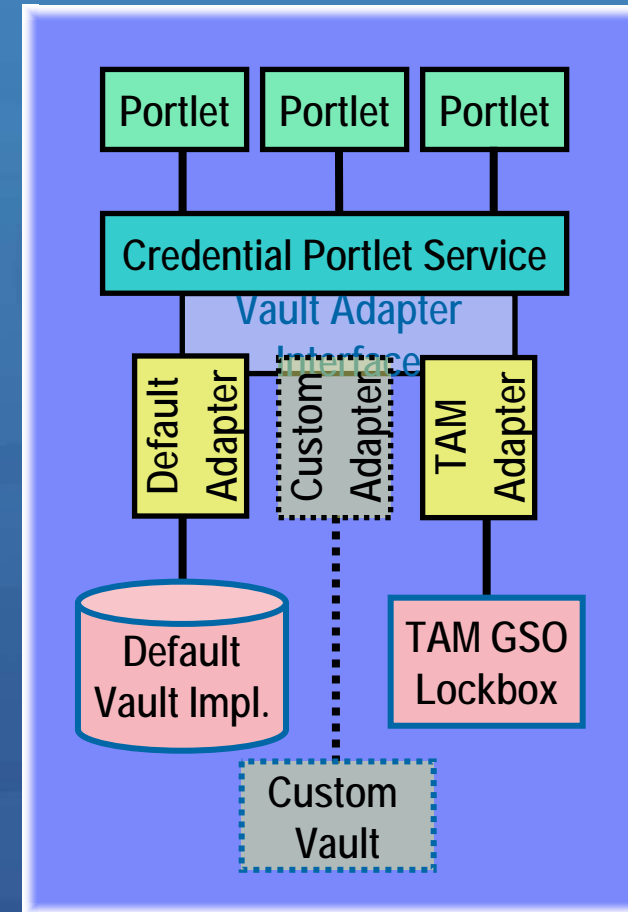
+

A basic default vault implementation

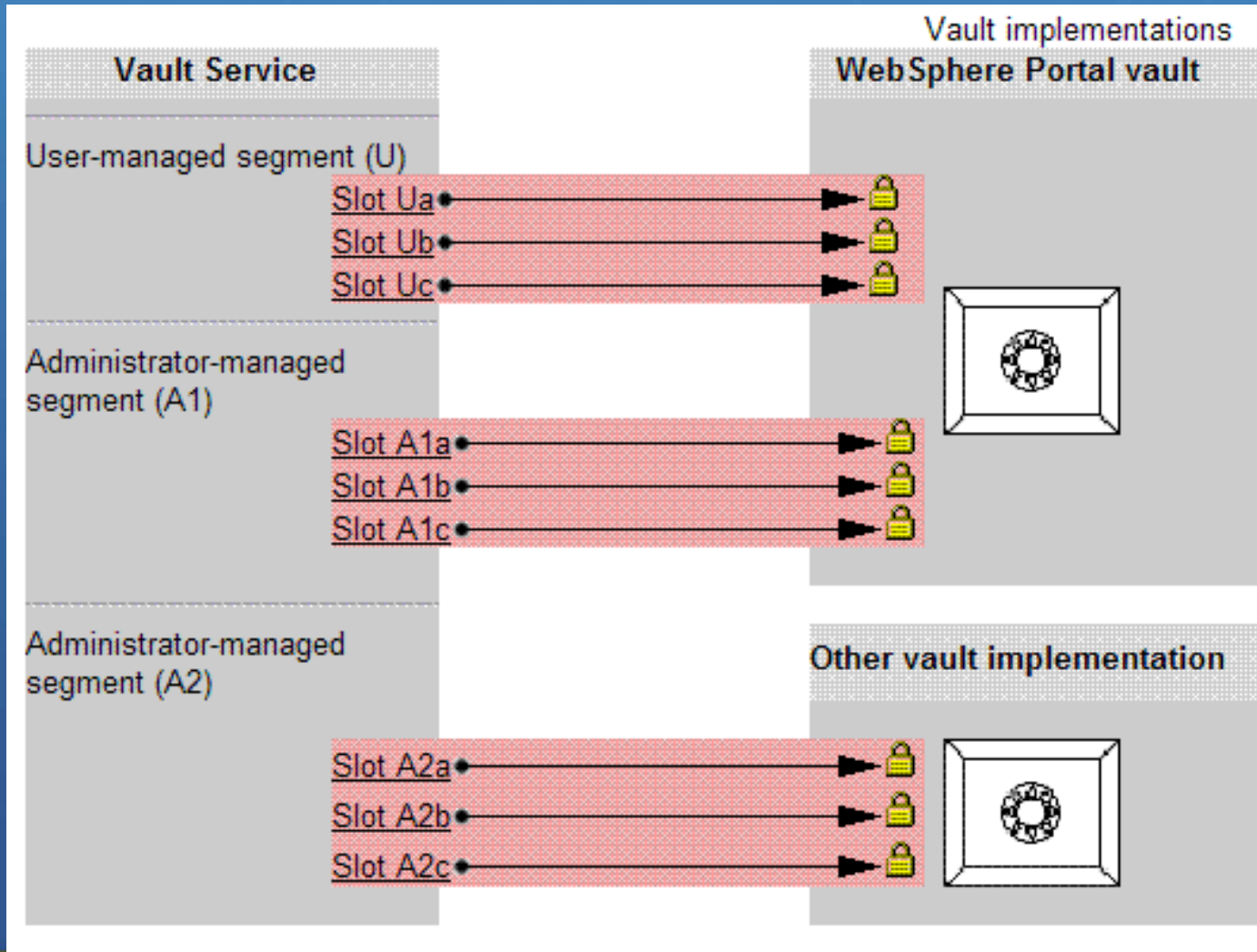
- base64 encoding
- public encryption exit
- migration challenge

+

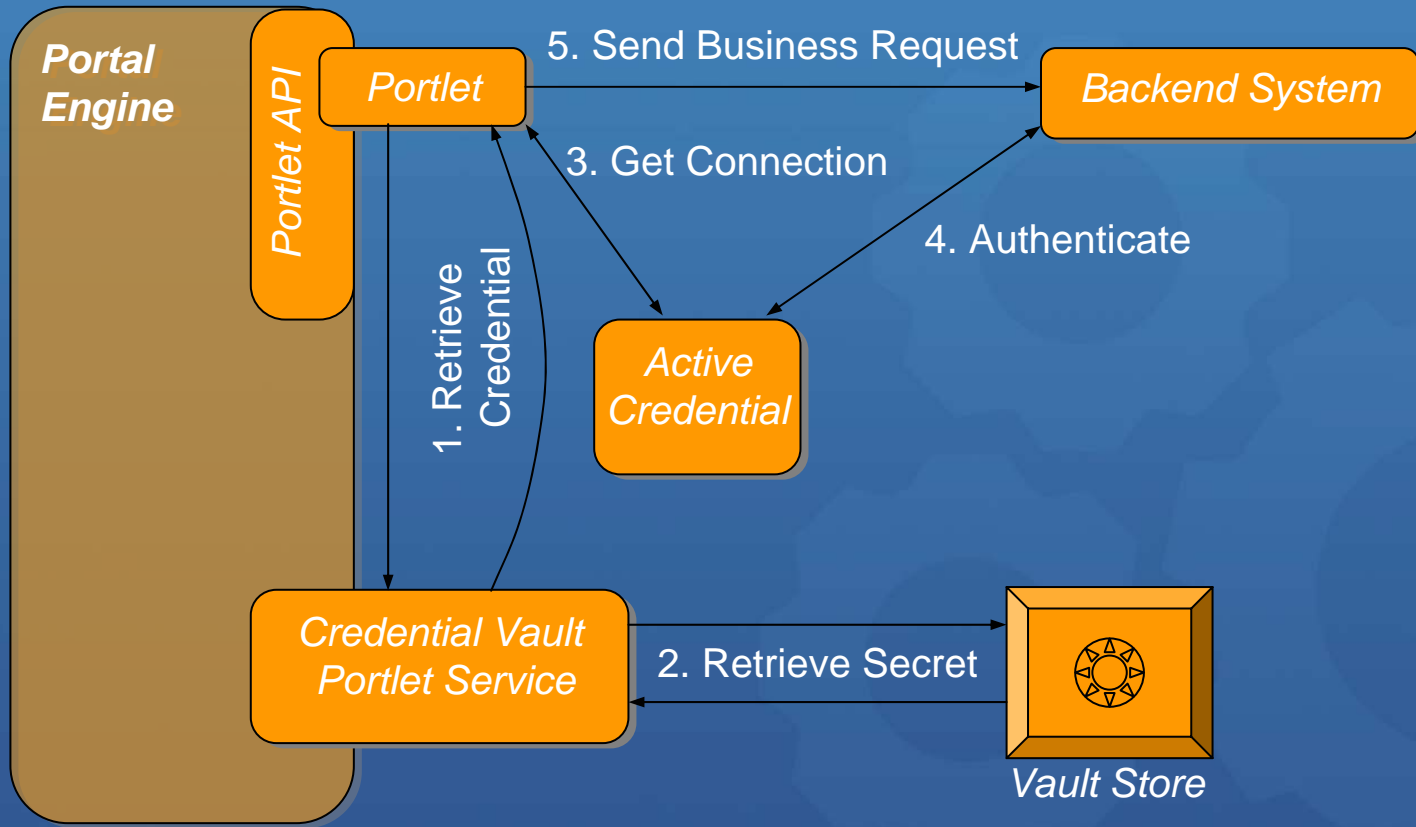
A vault adapter interface to integrate vault implementations like the Tivoli Access Manager Global Sign-On Lockbox



Credential Vault: Internal Org



Using Active Credential Objects



Agenda

- ① What's SSO
- ① WebSphere Portal v6.x Security Overview
- ① How to do web based SSO by using Portal
- ① What's new in v6.1



在 WebSphere Portal 6.1 安全性增強部分

- ◎ Greatly improved Security Configuration
- ◎ SPNEGO support (Windows® Desktop SSO)
- ◎ Reuse Group information from WebSphere
- ◎ Replace WMM with VMM
- ◎ Remember Me Cookie Support



WebSphere Portal 6.1 安全性增強介紹

◎ Greatly improved Security Configuration

- Less steps involved in frequent tasks like switching to LDAP (no disable/enable security required anymore)
- Easier to use SSL and Key Management
- Predefined Security profiles for WSRP
- Easy to Setup and Use Federated User Repositories

◎ SPNEGO support (Windows® Desktop SSO)

◎ Reuse Group information from WebSphere

◎ Replace WMM with VMM

◎ Remember Me Cookie Support

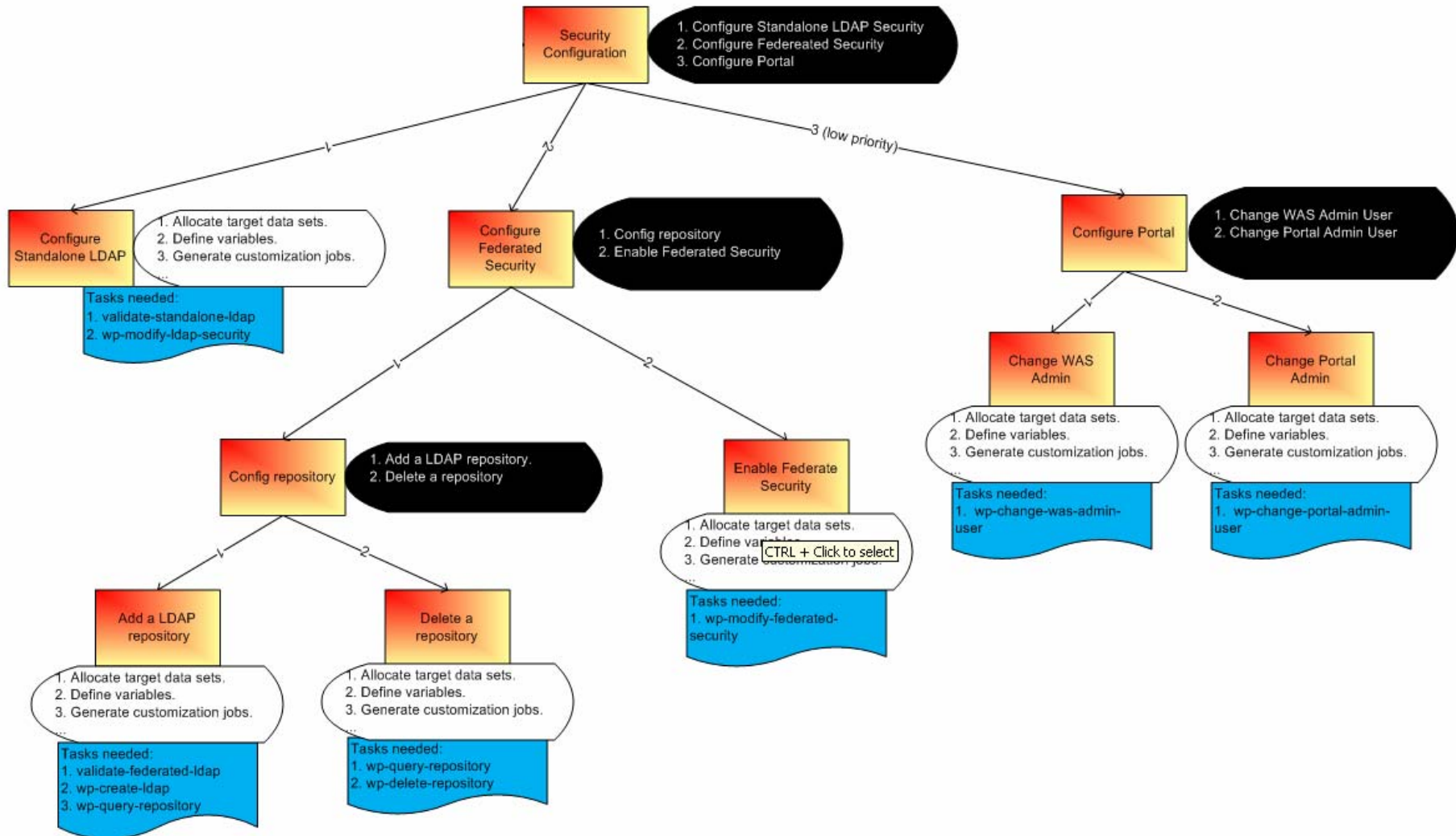


安全性設定上更加容易

- Introducing a new more flexible configuration path
- No need to disable security anymore
- Reduction of execution time
 - General task execution time between 10 and 20 minutes



新的設定方式一覽表



跟安全性設定的 ConfigEngine 工作 (1)

- **Enabling and configuring federated repository security**, e.g. user registry class name
 - wp-modify-federated-security
- **Configuring federated repositories**
 - VMM Federated LDAP – creating/updating the LDAP configuration in VMM
 - ✓ wp-create-ldap
 - ✓ wp-update-federated-ldap
 - VMM Federated DB – creating/updating the DB configuration in VMM
 - ✓ wp-create-db
 - ✓ wp-update-db
 - VMM Federated CUR – creating/updating the VMM user registry configuration
 - ✓ wp-create-cur
 - ✓ wp-update-federated-cur
 - VMM Delete federated repository
 - ✓ wp-delete-repository
- **Configuring stand-alone security**
 - VMM Stand-alone LDAP configuration
 - ✓ wp-modify-ldap-security
 - ✓ wp-update-standalone-ldap
 - VMM Stand-alone CUR configuration
 - ✓ wp-modify-cur-security
 - ✓ wp-update-standalone-cur



跟安全性設定的 ConfigEngine 工作 (2)

Configuring a lookaside or property extension repository

- wp-configure-la-complete
- wp-add-la-property

Configuring VMM realms

- wp-create-realm
- wp-update-realm
- wp-delete-realm
- wp-default-realm
- wp-add-realm-baseentry
- wp-delete-realm-baseentry
- wp-query-realm-baseentry
- wp-modify-realm-defaultparents

Configuring VMM repository base entries

- wp-create-base-entry
- wp-update-base-entry
- wp-delete-base-entry

Changing the administrative users

- wp-change-was-admin-user
- wp-change-portal-admin-user



What do we have OOTB

- ◉ **WebSphere Portal does use a File as User Registry**
 - Easy simple repository for POC and Development environment
- ◉ **WebSphere Application Security is enabled**
 - As in 6.0 WebSphere Portal bases on this environment setup
 - We use Federated as OOTB UserRegistry of WAS



在 WebSphere Portal 6.1 安全性增強部分

- ◎ Greatly improved Security Configuration
- ◎ **SPNEGO support (Windows® Desktop SSO)**
 - Automatically authenticate the user if logged into his desktop
- ◎ Reuse Group information from WebSphere
- ◎ Replace WMM with VMM
- ◎ Remember Me Cookie Support



在 WebSphere Portal 6.1 安全性增強部分

- ◎ **Greatly improved Security Configuration**
- ◎ **SPNEGO support (Windows® Desktop SSO)**
- ◎ **Reuse Group information from WebSphere**
 - Better integration in WebSphere Security infrastructure
 - Membership of a User can be driven by security infrastructure
- ◎ **Replace WMM with VMM**
- ◎ **Remember Me Cookie Support**

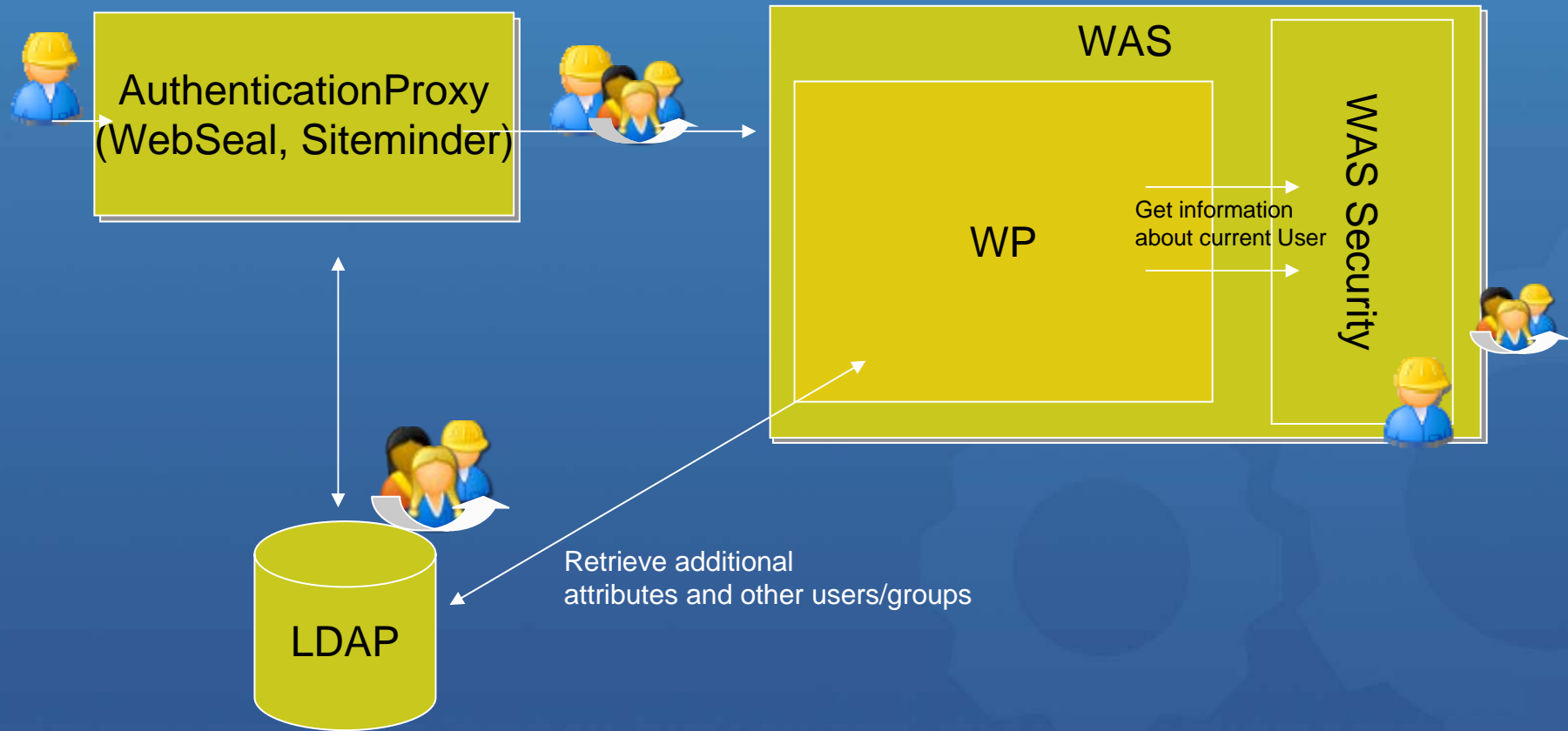


Reuse Group information from WebSphere

- Better integration in WebSphere Security infrastructure
 - WebSphere TAI++ enables you to establish trust w/o verification
 - With WebSphere Portal 6.1
- Membership of a User can be driven by security infrastructure



Reuse Group information from WebSphere



Describe the different approaches that can be taken into consideration. Give a short description, and state pros and cons for each design alternative.

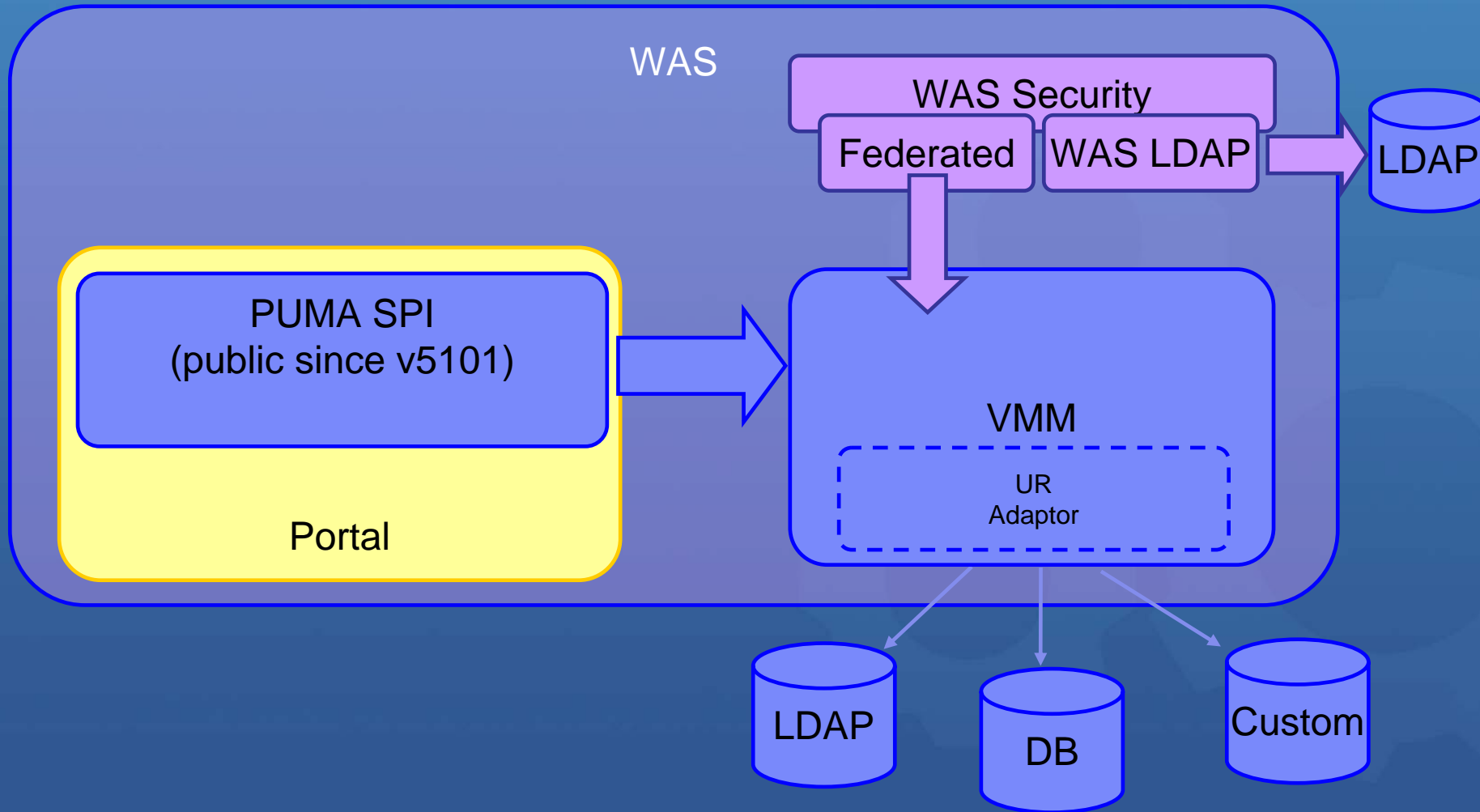


在 WebSphere Portal 6.1 安全性增強部分

- ◎ **Greatly improved Security Configuration**
- ◎ **SPNEGO support (Windows® Desktop SSO)**
- ◎ **Reuse Group information from WebSphere**
- ◎ **Replace WMM with VMM**
 - Reusing new WebSphere Infrastructure for Users and Groups
 - Puma will be continued
- ◎ **Remember Me Cookie Support**



VMM Integration in WP V6.1



Virtual Member Manager

- Integrated in WebSphere Application Server V6.1
- Replaces the WebSphere Member Manager (WMM) that came with WebSphere Portal prior to release V6.1
- VMM User Registry (UR) adapter acts as the integration point between WAS security and VMM
 - `com.ibm.ws.wim.registry.WIMUserRegistry`
- Out of the box VMM adapters for
 - File-based repository
 - LDAP repository
 - Database repository



Public available Custom Adapter

- Public API for Custom Adapter
 - For Portal still possible to provide VMM adapter and CUR adapter
- VMM API is based on Service Data Objects (SDO)
- Config tasks available

see notes section for resources



在 WebSphere Portal 6.1 安全性增強部分

- ◎ Greatly improved Security Configuration
- ◎ SPNEGO support (Windows® Desktop SSO)
- ◎ Reuse Group information from WebSphere
- ◎ Replace WMM with VMM
- ◎ **Remember Me Cookie Support**
 - User can select the website to remember them for delivering personalized content without login
 - Also provides step-up Authentication Framework for customer authentication levels



StepUp and RememberMe

RememberMe Cookie

- Persistent cookie allows portal to recognize user without login
 - ✓ → Portal can show a personalized welcome page
- If cookie is present, portal treats the user as „**identified**“ but not yet „**authenticated**“
 - ✓ User can only see resources available for the anonymous user
- Access to protected resources requires the user to authenticate.



The screenshot shows a login dialog box with the following elements:

- User ID:
- Password:
- Remember me on this computer
- Not registered? [Sign up](#)
- Log in
- Cancel

A large black arrow points from the top right towards the 'Remember me on this computer' checkbox.

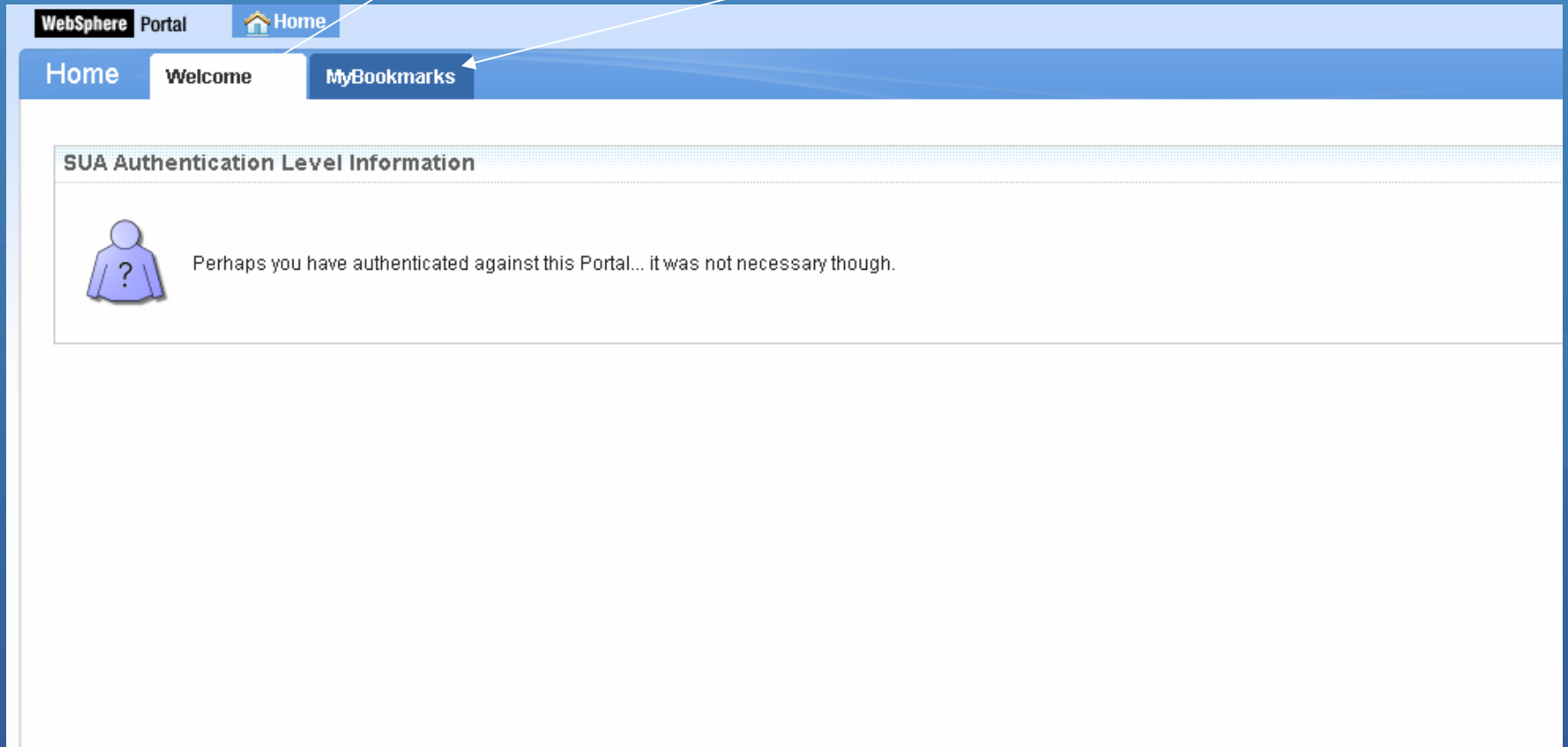
StepUp Framework

- Enables you to enforce another authentication level for specific pages and/or portlets
- Framework to **plug in additional Levels of Authentication Strength**
 - ✓ E.g. enforce SSL for specific services, or client certificate certificates,...
- Available for Pages and Portlets
- Required authentication strength can be managed using the Resource Permission Portlet



No authentication level

Remember me level assigned




The screenshot shows a WebSphere Portal interface. At the top, there is a navigation bar with "WebSphere Portal" and a "Home" button. Below this, there are three tabs: "Home", "Welcome", and "MyBookmarks". The "MyBookmarks" tab is selected. The main content area is titled "SUA Authentication Level Information". It contains a blue icon of a person with a question mark and the text: "Perhaps you have authenticated against this Portal... it was not necessary though." Two white arrows point from the text above to the "MyBookmarks" tab and the "SUA Authentication Level Information" section.

WebSphere Portal Home

Home Welcome MyBookmarks

SUA Authentication Level Information

 Perhaps you have authenticated against this Portal... it was not necessary though.

Home

Login

User ID:

Password:

Remember me on this computer


Not registered? [Sign up](#)



WebSphere Portal | Home | Applications | Search Center

Home | Welcome | MyBookmarks | Feeds

SUA Authentication Level Information

 You have at least provided a valid Remember Me Cookie to authenticate against this Portal.

Remember Me Cookie Portlet

Using the Portlet Service **RememberMeCookieService**, the following information has been retrieved:

Remember Me enabled:	true
Remember Me Cookie set:	true
User ID:	uid=stefan,o=defaultWIMFileBasedRealm
Remember Me Cookie revocation URL:	/wps/myportal/!ut/p/c/5/04_SB8K8xLLM9MSSzPy8xBz9QJ_...
	Revoke the Remember Me Cookie.

Using the Portlet Service **PumaHome** and the **PumaProfile**, some user attributes have been obtained:

cn: Stefan Schmitt
uid: stefan

Bookmarks

- [WebSphere Portal Security Home](#)
- [Portal Security Zone](#)
- [Resource Permission](#)


wps/portal/mybookmarks

wps/myportal/mybookmarks

WebSphere Portal [Home](#)

Home **Welcome** MyBookmarks

SUA Authentication Level Information



You have at least provided a valid Remember Me Cookie to authenticate against this Portal.

Remember Me Cookie Portlet

Using the Portlet Service **RememberMeCookieService**, the following information has been retrieved:

Remember Me enabled: true
Remember Me Cookie set: true
User ID: uid=stefan,o=defaultWIMFileBasedRealm
Remember Me Cookie revocation URL: [wps/portal/ut/p/c/5/04_SB8K8xLLM9MSSzPy8xBz9QJ_89...](#)
[Revoke the Remember Me Cookie.](#)

Using the Portlet Service **PumaHome** and the **PumaProfile**, some user attributes have been obtained:

cn: Stefan Schmitt
uid: stefan


Bookmarks

- [Portal Security Zone](#)
- [Resource Permission](#)

WebSphere Portal [Home](#) Applications Search Center

Home **Welcome** MyBookmarks **Feeds**

SUA Authentication Level Information



You have at least provided a valid Remember Me Cookie to authenticate against this Portal.

Remember Me Cookie Portlet

Using the Portlet Service **RememberMeCookieService**, the following information has been retrieved:

Remember Me enabled: true
Remember Me Cookie set: true
User ID: uid=stefan,o=defaultWIMFileBasedRealm
Remember Me Cookie revocation URL: [wps/myportal/ut/p/c/5/04_SB8K8xLLM9MSSzPy8xBz9QJ_...](#)
[Revoke the Remember Me Cookie.](#)

Using the Portlet Service **PumaHome** and the **PumaProfile**, some user attributes have been obtained:

cn: Stefan Schmitt
uid: stefan

Bookmarks

- [WebSphere Portal Security Home](#)
- [Portal Security Zone](#)
- [Resource Permission](#)



Custom Level Sample

Custom Level

WebSphere Portal Home Applications Search Center

Home Welcome MyBookmarks Feeds

SUA Authentication Level Information



You have at least provided a valid Remember Me Cookie to authenticate against this Portal.

Remember Me Cookie Portlet

Using the Portlet Service **RememberMeCookieService**, the following inf

Remember Me enabled: true
Remember Me Cookie set: true
User ID: uid=stefan,o=defaultWIMFileB
Remember Me Cookie revocation URL: /wps/myportal/!ut/p/c5/04_SBE
[Revoke the Remember Me Cookie](#)

Level Authentication Challenge

uid: stefan

Bookmarks

- WebSphere Portal Security Home
- Portal Security Zone
- Resource Permissions

Requested Content

The screenshot shows a 'Questionnaire' portlet with an aerial view of a building. Below it, the 'IBM Redbooks' section lists articles such as 'Implementing an IBM/Brocade SAN with 8 Gbps Directors and Switches' and 'Enterprise Multipatform Auditing'. The 'IBM Press Releases' section includes a release about 'IBM Delivers the Next Wave of Business Social Networking: IBM Lotus Connections & IBM Atlas'.



Questions





IBM® WEBSHERE® PORTAL 6.1
Deliver Exceptional User Experiences

WebSphere software ibm.com/websphere/portal



Thank You!