IBM Commerce

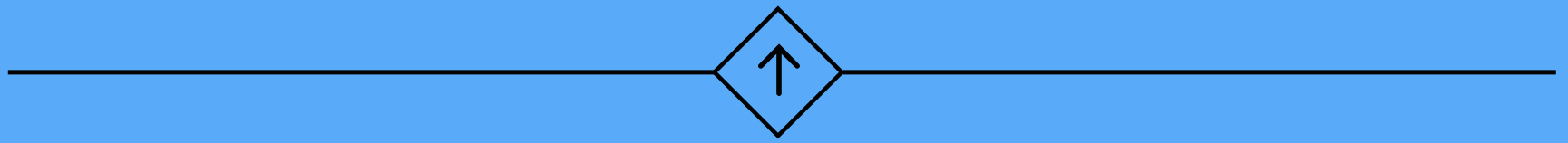
# Digital Experience Security Overview & Hardening

Thomas Hurek, Digital Experience Lab Services, IBM USA

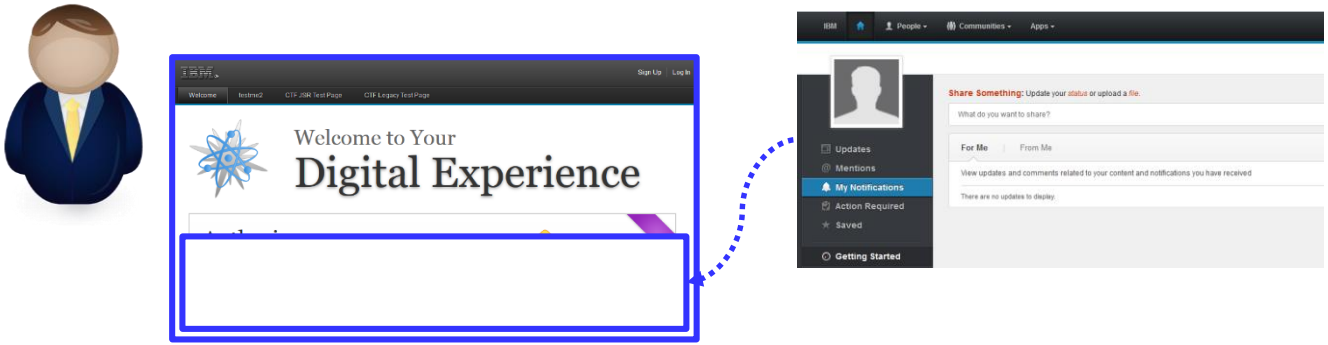
# Agenda

- SSO
  - FrontSide
    - Transient users
    - VP scoping
  - BackEnd
    - HTTPOutbound
    - Seemless integrate Cloud data
- Portal features
  - StepUp / Preview / Impersonation
  - VMM and adapters
  - Portal Access Control
- Portal Hardening
  - Secure portal
  - Secure communication
  - Custom Code

# SSO



# Seemless integrate Cloud data

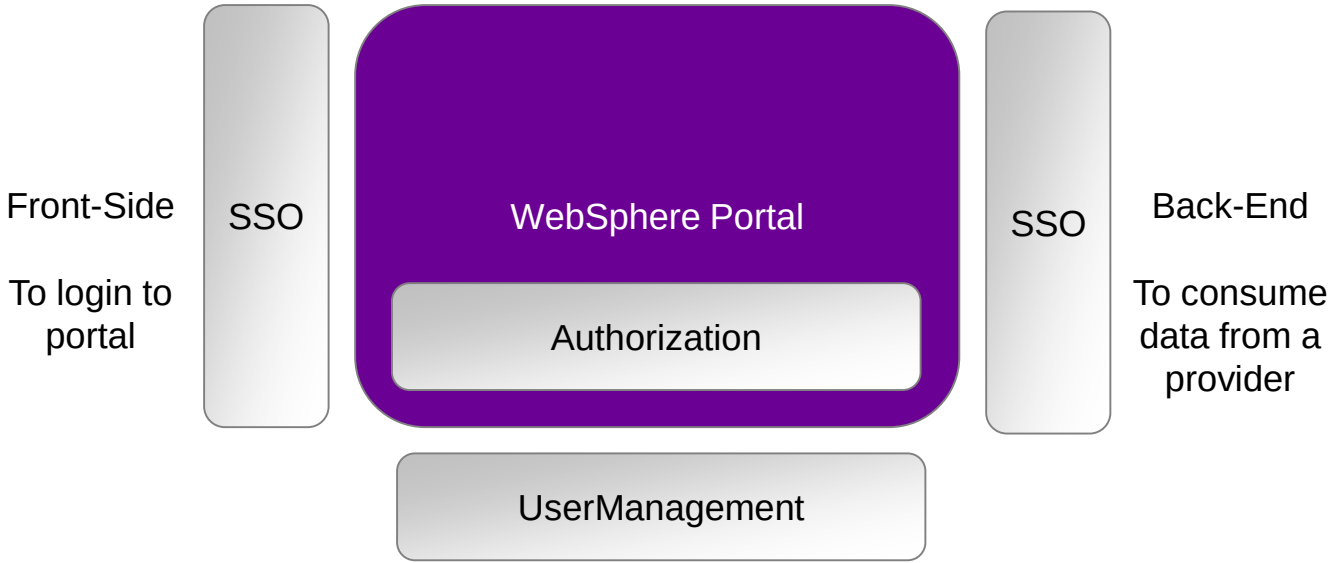


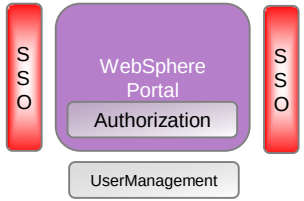

**Integrate data seamless** into the portal.

New questions appear...

- How to login?
- Is information user-scoped?
- How to consume?
- Who owns the backend system?

# Overview





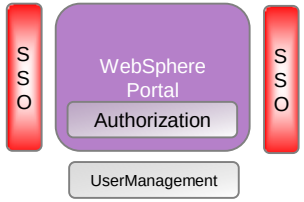

# Single Sign-On - simple

Alice

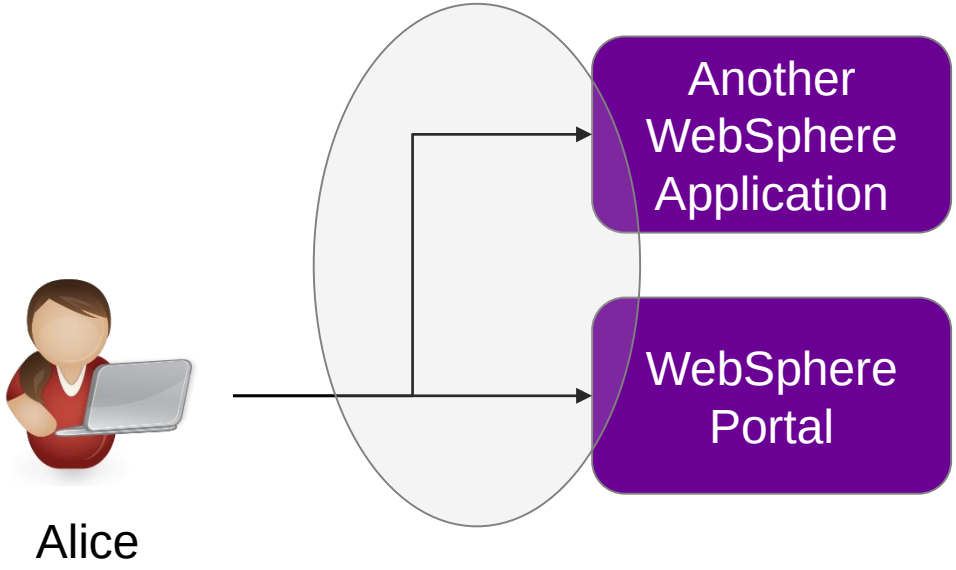
Simple login

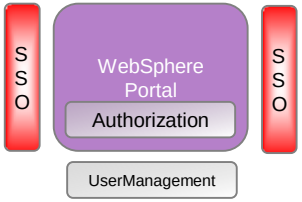
WebSphere Portal

TAI
JAAS
Portal LoginFilters (implicit/explicit)

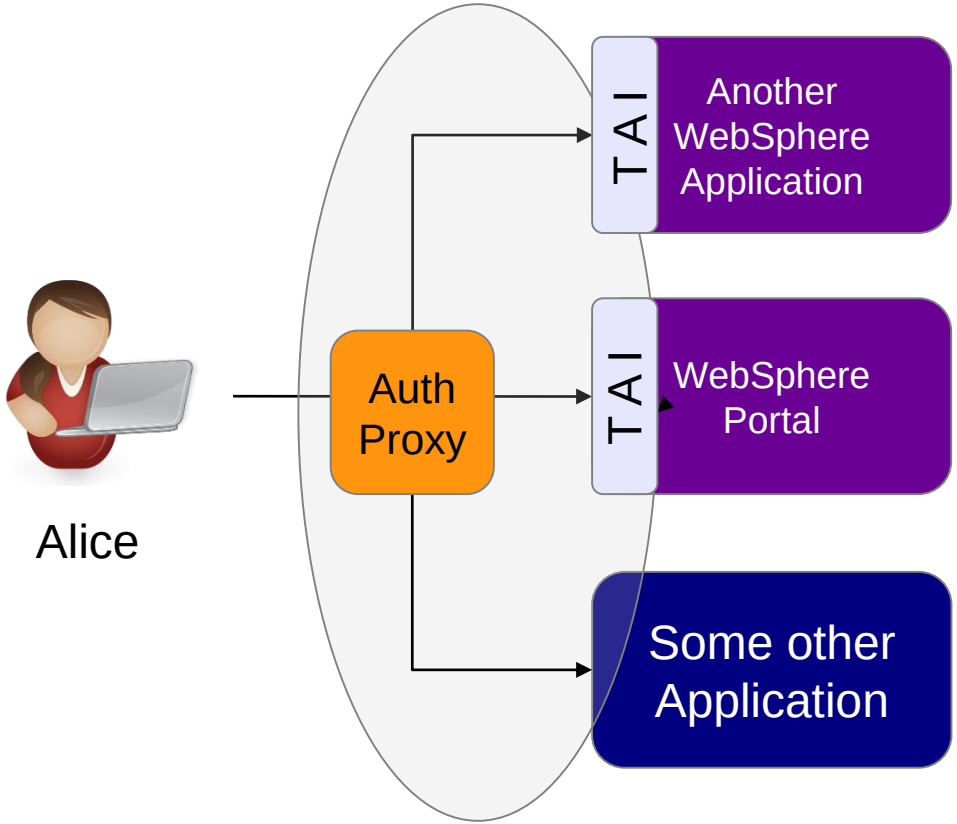


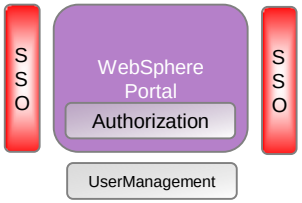

# Single Sign-On - LTPA



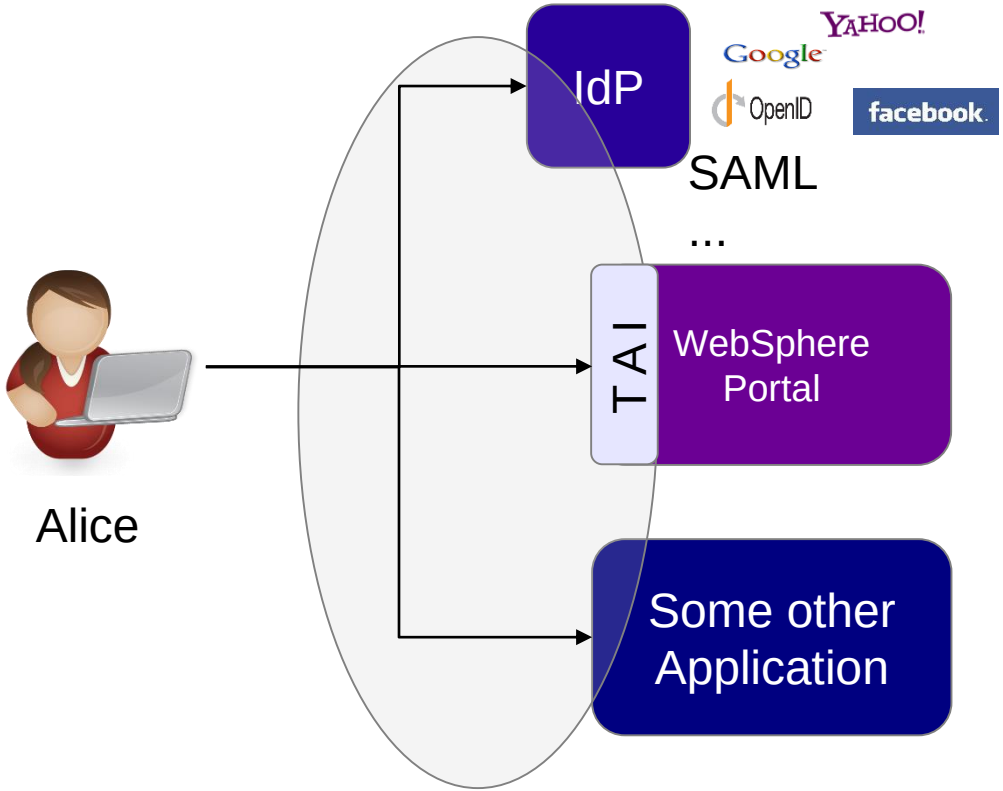



# Single Sign-On – Auth Proxy



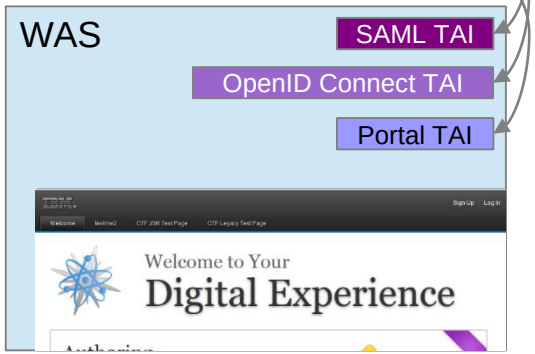



# Single Sign-On – Identity Provider



# Front Side SSO details

Login to your Digital Experience using the account of **your** choice.
Using new flexible SSO integration options.




facebook — Login still valid by portal TAI

Google+ — Changed from OpenID to **OpenId Connect 2015**

SAML — **Enhancement for Service Provider initiated flow (2015)**

OpenId Provider — Login still valid by portal TAI

OpenID Connect — **New since 2015**

# Protocol Overview – just as reference

## OpenId

http://en.wikipedia.org/wiki/OpenID

## Oauth

http://en.wikipedia.org/wiki/OAuth

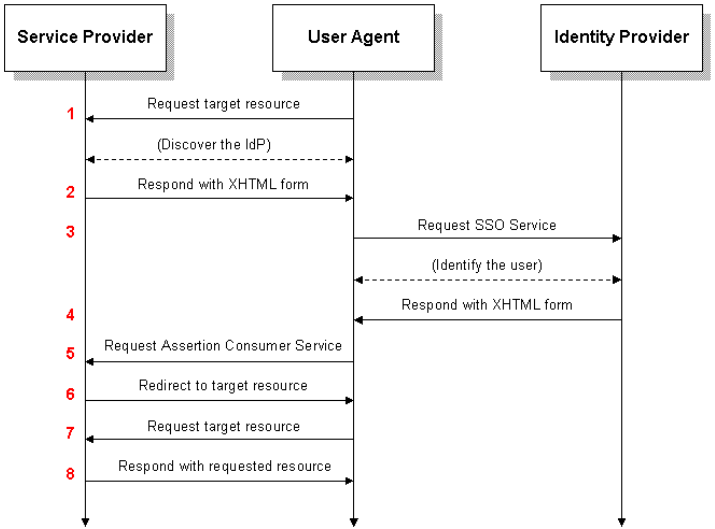
## OpenId connect

http://en.wikipedia.org/wiki/OpenID_Connect

## SAML

http://en.wikipedia.org/wiki/SAML_2.0

SP POST Request; IdP POST Response

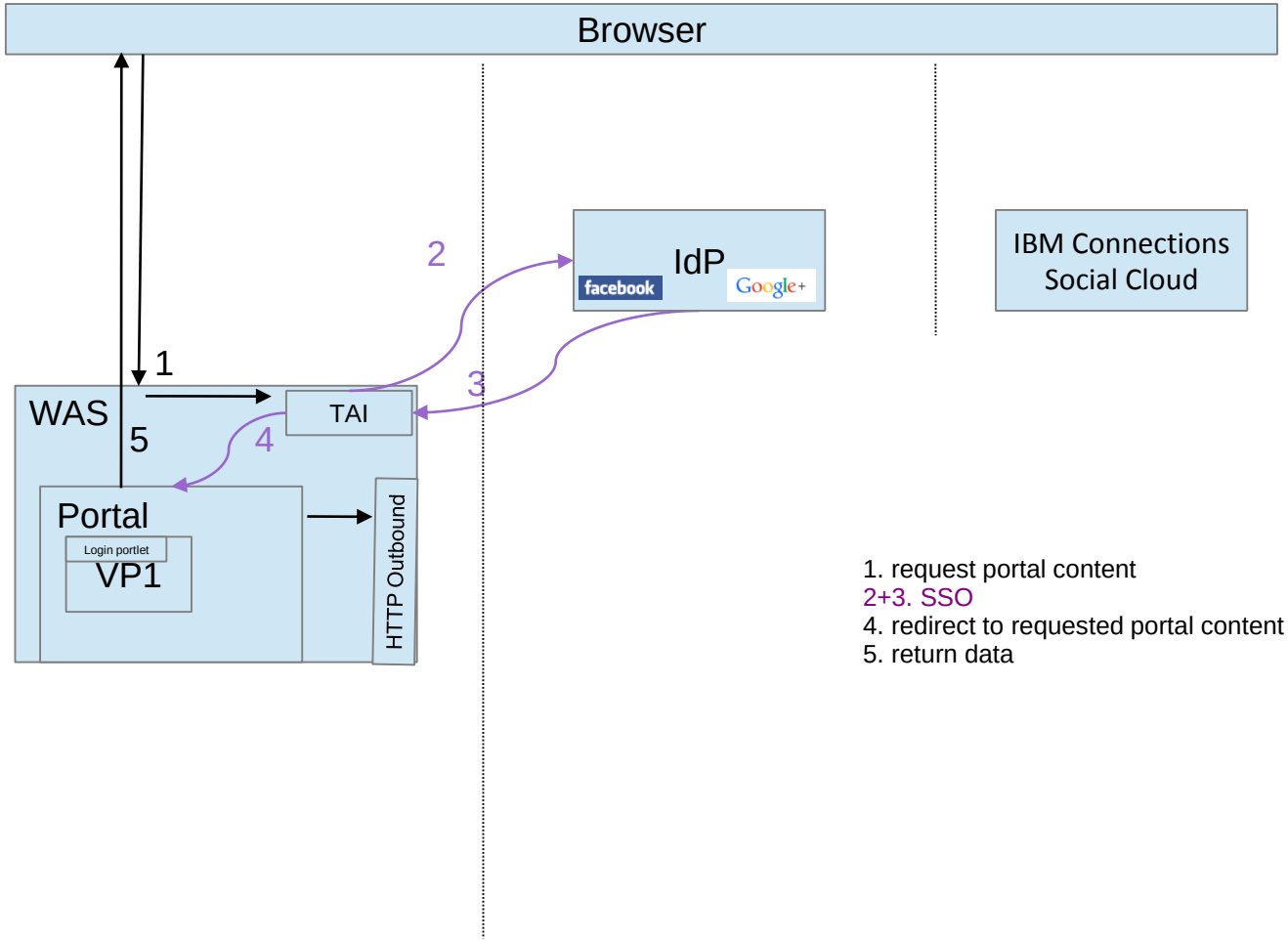


# SP initiated vs. IdP initiated

- HTTPOutbound works with IdP initated flows.
- The technical flow may not be recognized by a user – even the technical footprint differs.
- In example the WAS SAML TAI can get configured to work with IdP initiated flows. In case the authorization is not available a error page is displayed which is in fact the IdP login page.
- Given that a User recognize it as SP initated flow – but it is a IdP started flow.

- Since 2015 the WAS SAML TAI can also get configured to support a real SP initated flow, here some custom code need to create the SP scoped details (AuthnRequest, RelayState,..) and the login procedure works as defined in the spec.

https://www.ibm.com/developerworks/community/blogs/8f2bc166-3bdc-4a9d-bad4-3620dbb3e46c/entry/how_to_configure_was_saml_tai_to_work_with_portal_in_a_sp_initiated_flow?lang=en




1. request portal content
2+3. SSO
4. redirect to requested portal content
5. return data

# Transient users

With this option you, can provide a personalized view to unregistered users while still providing benefits to fully registered users.

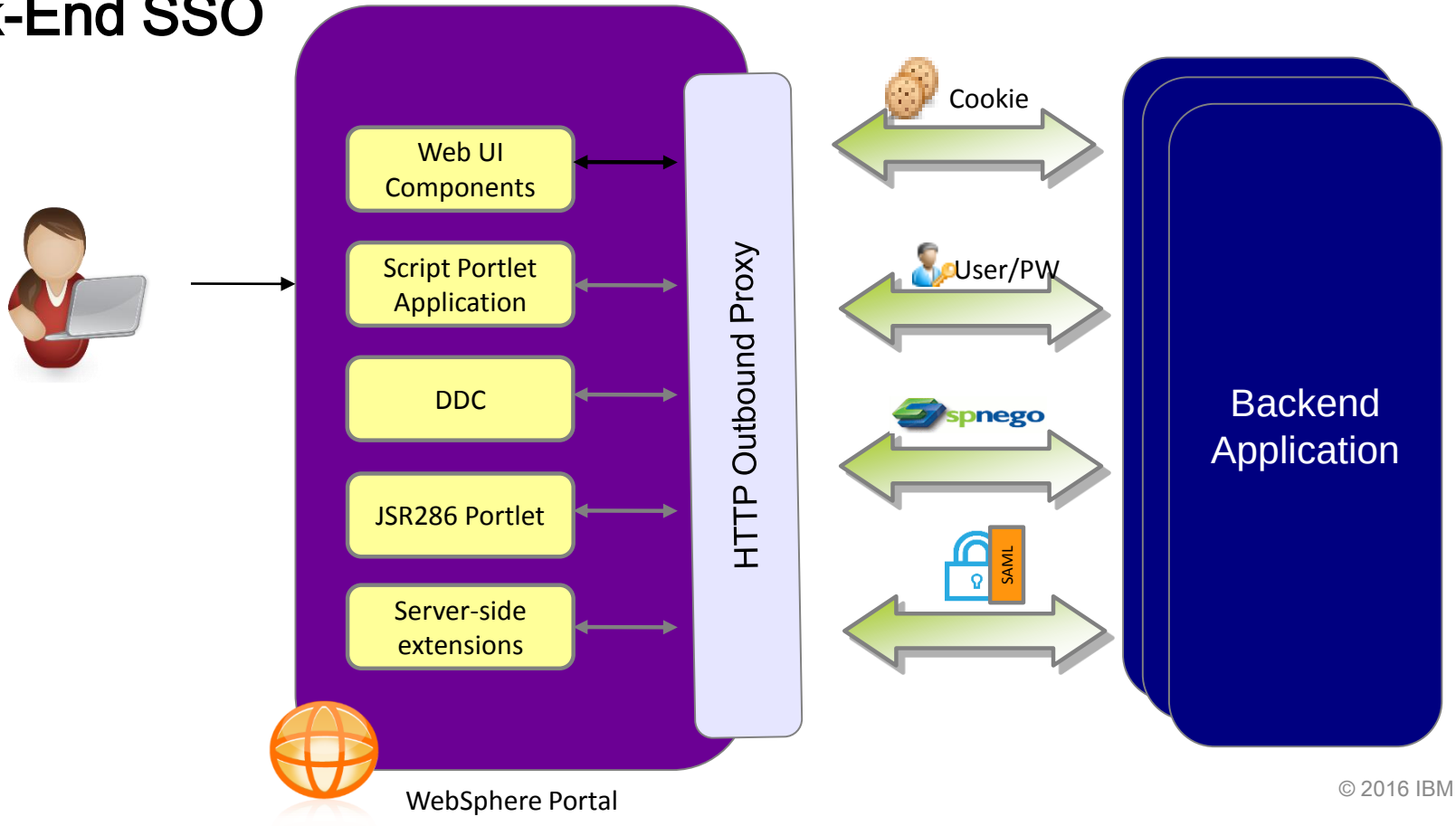
Portal config documented in KC

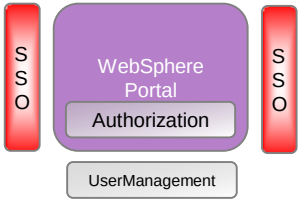
TAI config is on WAS level

Example code provided in developerWorks

https://www.ibm.com/developerworks/community/blogs/8f2bc166-3bdc-4a9d-bad4-3620dbb3e46c/entry/portal_transient_user_support_with_was_saml_tai_business_case_clarification?lang=en
http://www-01.ibm.com/support/knowledgecenter/SSHRKX_8.5.0/mp/security/openid_trans_users.dita?lang=en

# Back-End SSO






# Outbound HTTP Connections

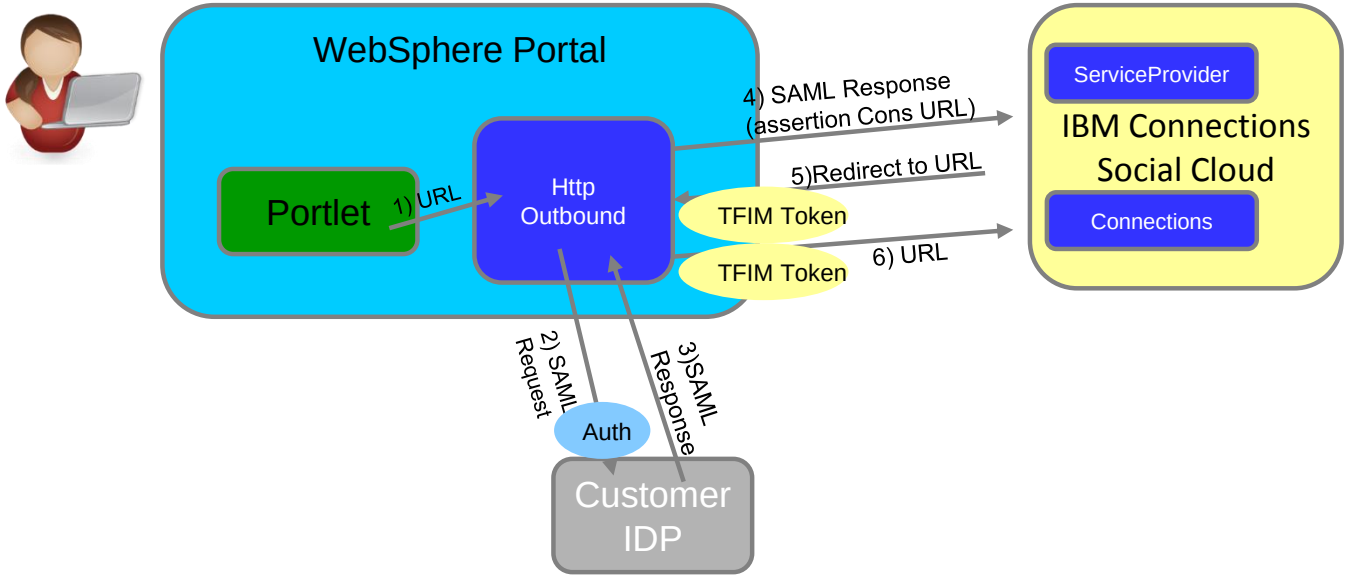
- Central control for outbound HTTP connections
- Functions for authentication and cookie handling
- Administration via model APIs or configuration tasks
- Custom outbound service filter possible

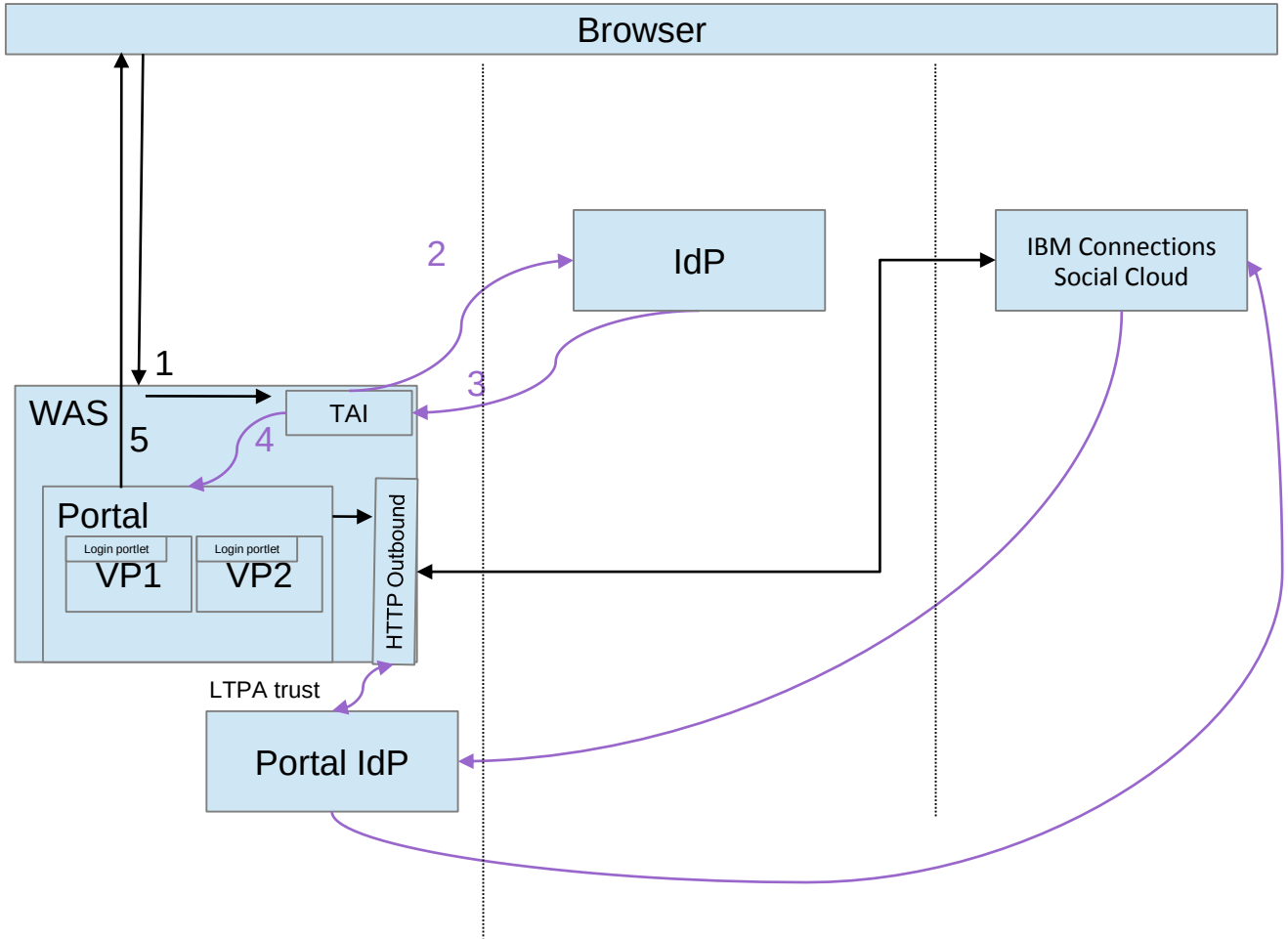
http://www-01.ibm.com/support/knowledgecenter/SSHRKX_8.5.0/mp/dev-portlet/outbhttp_cust_srvc_filtrs.dita

- Since 8.5 streamlined
- Use one code base for all flows
- Use one configuration for all flows

# Back-End SSO

1) Portal calls a myproxy configured endpoint
(LTPA is already available in the security context of the caller)
2) SSO1 (LTPA, Form, BasicAuth, SPNEGO) from portal to IdP to get SAML assertion
3) redirect including SAML assertion to SP
4) SSO2 (SAML) to get security token for Cloud
5) redirect including security token (LTPA') to data-provider
6) SSO3 (LTPA') to get required data

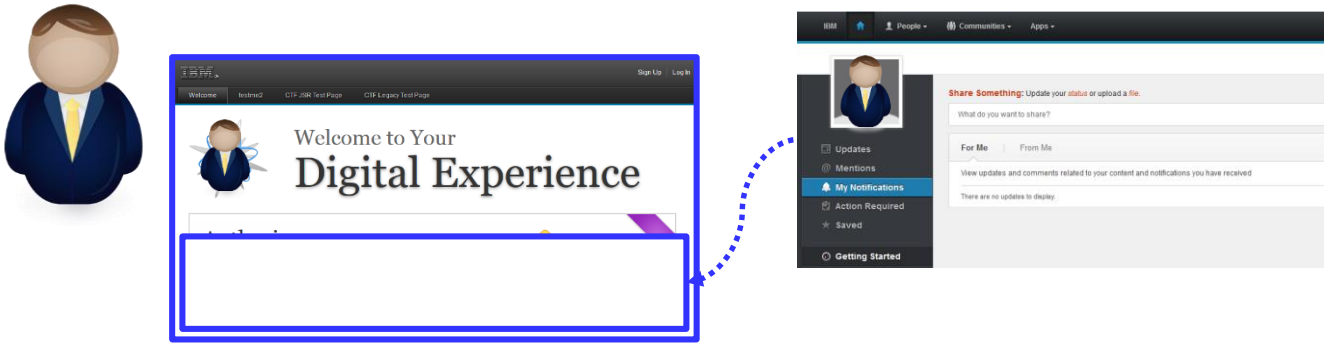



Browser
1
2
3
4
5
IdP
IBM Connections
Social Cloud
WAS
TAI
Portal
Login portlet
VP1
Login portlet
VP2
HTTP Outbound
LTPA trust
Portal IdP

# Setup SAML Outbound best practice

- There are different layers involved, so several areas to check for missconfigurations.
  - Test IdP flow directly in Browser (also check for cookies)
    - Login to ADFS and check cookie + scoping *(if ADFS environment)*
    - Use form to start IdP initated login flow
    - Only if this works browser based it may work via HTTPOutbound
      - SAMLResponse format, user lookup, certificates (SSL, signer)
  - Test for connectivity from portal server to involved servers
  - Check flow with tracing

# Seemless integrate Cloud data - solved




**User based SSO** from portal to BackEnd to integrate data seamless into the **data model** (e.g. DDC).

Now you are able to work with e.g. the IBM Connections Social Cloudoffering in the same manner as a local Connections Server can get aggregated into your WebSphere Portal

http://www-01.ibm.com/support/knowledgecenter/SSHRKX_8.5.0/mp/dev-portlet/outbhttp_auth_est_sso_saml_tok.dita
http://www-01.ibm.com/support/knowledgecenter/SSHRKX_8.5.0/mp/dev-portlet/known_limitations_sc4sb.dita

# Authorization requires SSO context

In case of SSO it needs to be **sure** that a user in portal (that benefits from SSO) is in the connected system the **same** user.

Often eMail is used as identifier – then make sure **eMail attribute** is not allowed to get changed by the user itself without **validation**.

# Reuse IdP information

## Profile information

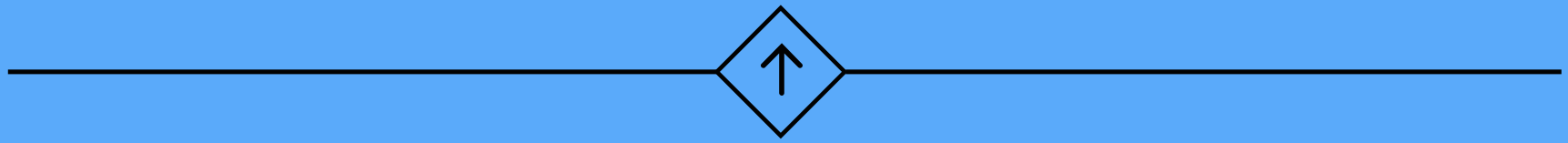
- It is possible to get profile information from the IdP or ID-provider. Those needs to get mapped to portal attributes.

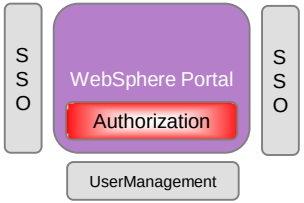
## Groups

- Groups may be handy for AC settings.
- Portal can get configured to reuse the WSSubject groups

http://www-01.ibm.com/support/knowledgecenter/SSHRKX_8.5.0/mp/admin-system/reuse_group_info.dita?lang=en

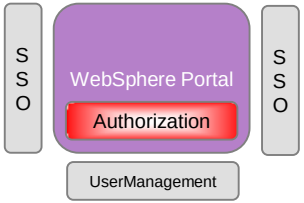
# Portal Features





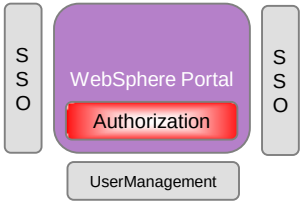

# StepUp

- Predefined authentication levels: identified, authenticated, standard
- Allows to plug custom code for enforcing custom levels
  - e.g. enforce SSL or client-side certificate
- Authentication levels can be set for portlets and pages



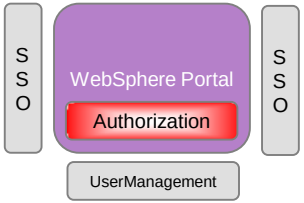

# RememberMe

- Persistent cookie to recognize user without manual login (DN used)
- After logout, a user is treated as “identified”
- Portlets can show personalized content
- For accessing protected resources, user has to authenticate
- Administration of authentication levels
  - Via UI (Portal Administration >...> Resource Permissions)
  - Via XML Access



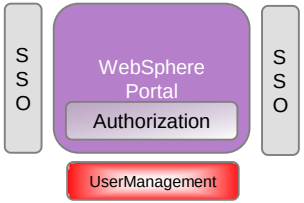

# Preview

- See the content like another user
  - Portal changes the puma response to the user
  - Other systems will only recognize „real“ user (e.g. WebSphere via LTPA)
- Protected by Access Control
  - Control who can start preview for whom



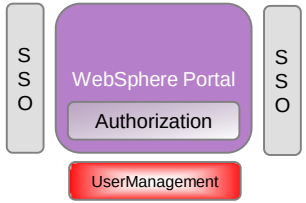

# Impersonation

- Acting as a different user
  - Portal tracks information about original user
  - Other systems will only recognize impersonated user (e.g. WebSphere via LTPA)
- Protected by Access Control
  - Control who can be impersonated by whom
- Public APIs to identify Impersonator

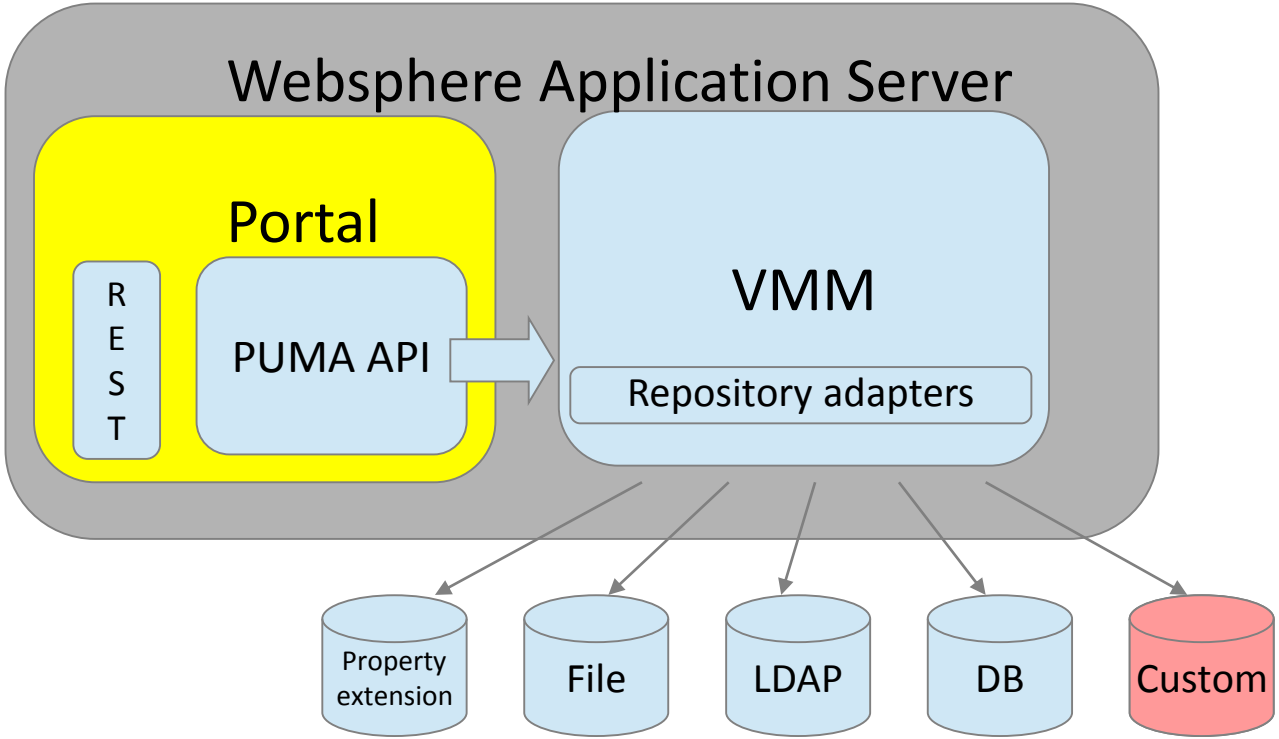


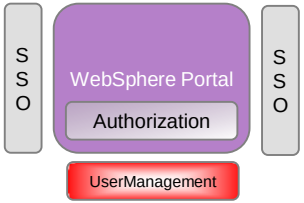

# User Management

- Accessing different user repositories (VMM)
  - LDAP
  - DB
  - RACF
  - Custom
- Provide ability to manipulate Registry data for Application purpose
- Separate Users for Multiple VP's
- Helping you to cleanup if you move your environment




# Virtual Member Manager






# Dynamic Groups

- Rule-based usergroups
- Not managed by standard user repository
- Available since 8.0 or via Solution Catalog (7.0)

AllManagersInGermany

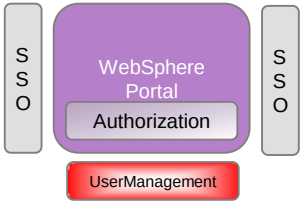
&(c="Germany")(isManager="Y")

Alice

C: Germany
isManager: Y
....

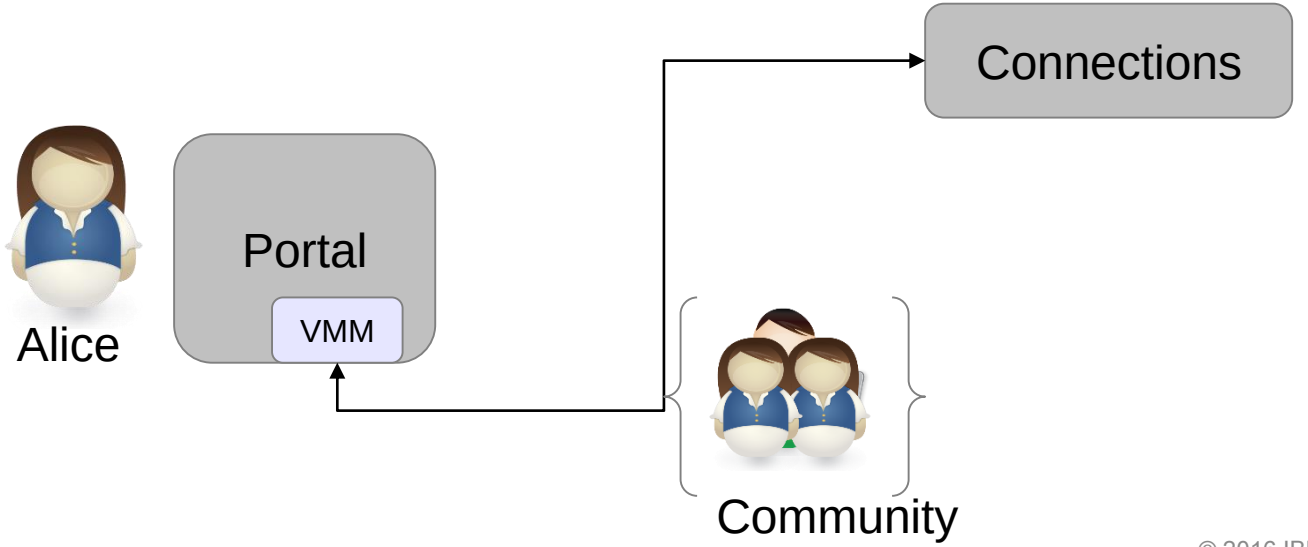
Michelle

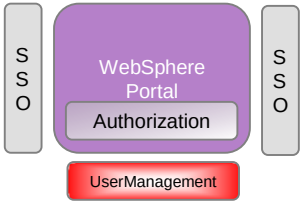
C: Germany
isManager: N
....




# Community Integration

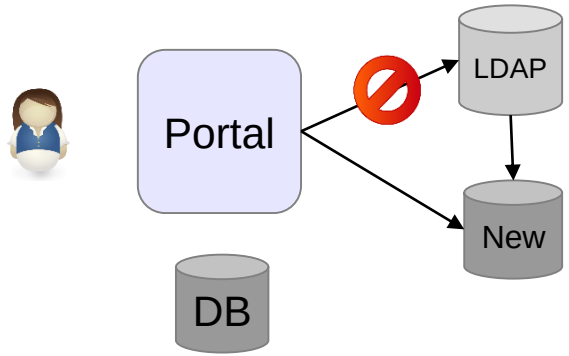
- Communities are available at Portal
  - For AC groups
  - Via Puma
  - Via VMM

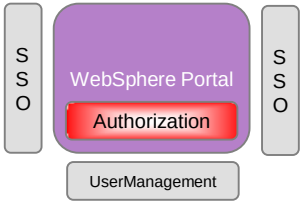





# Cleanup End User Artifacts

- Two tools to use
  - UserCleanup via XMLAccess
  - Memberfixer for WCM content
- Helping you to keep end user customization after user backend changes
  - DN changes
  - UniqueID changes
  - Cleanup or Data migration






# What is Portal Access Control

Authentication → Get Unique User ID

Authorization → Use Unique User ID

**Who**

is allowed to perform

which **action**

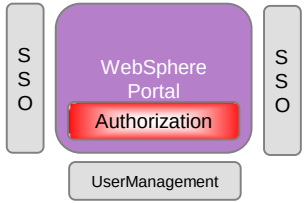
Examples: view, edit, delete

on which **resource**?

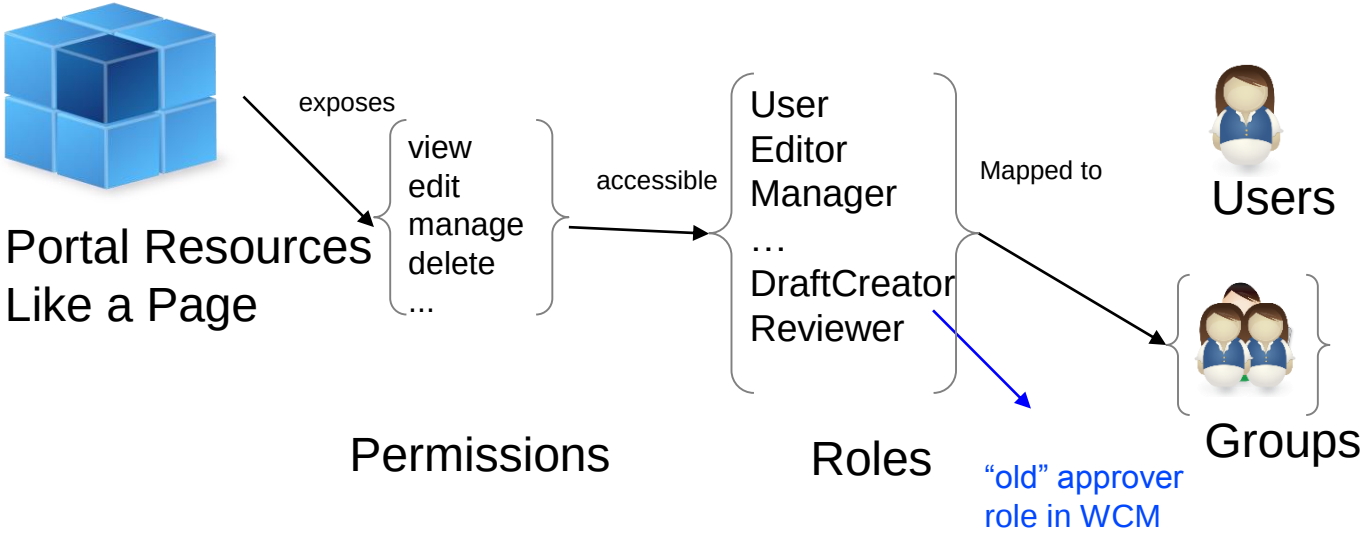
Portal Resources

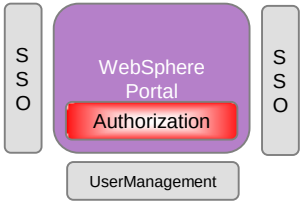
Examples: page, portlet

Access Control in Portal is **role based** e.g. Alice is Editor@PageA and User@PortletB

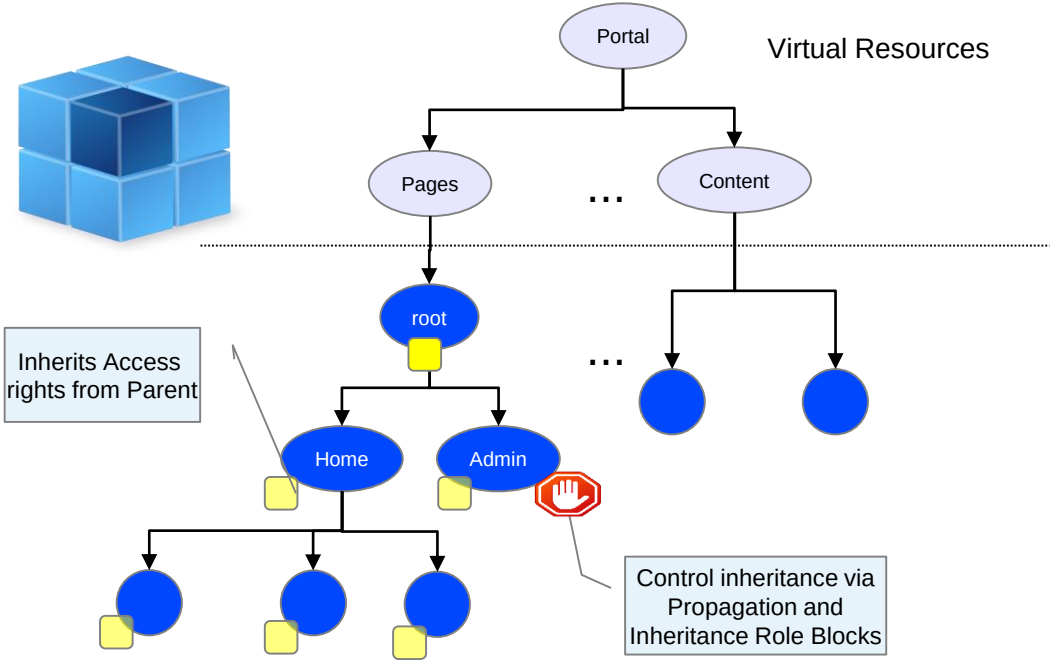



# Access Control Model





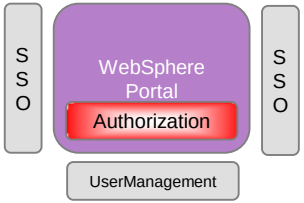

# Access Control Model




Users

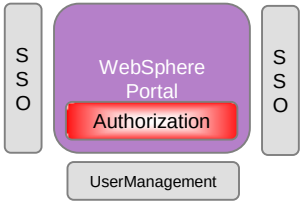
Groups

# Delegated Administration




- Your Company has multiple facilities
- Each of them should be able to maintain separate content at a globally defined spot

- The content will be managed and controlled by people inside of the facility
- These user may or may not also control who can see the content within their facility

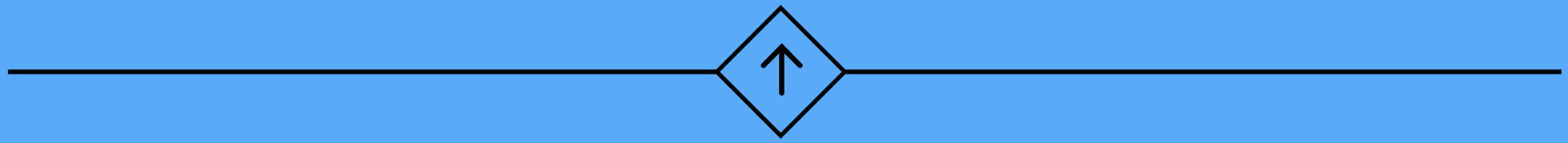



# Attribute Based Security

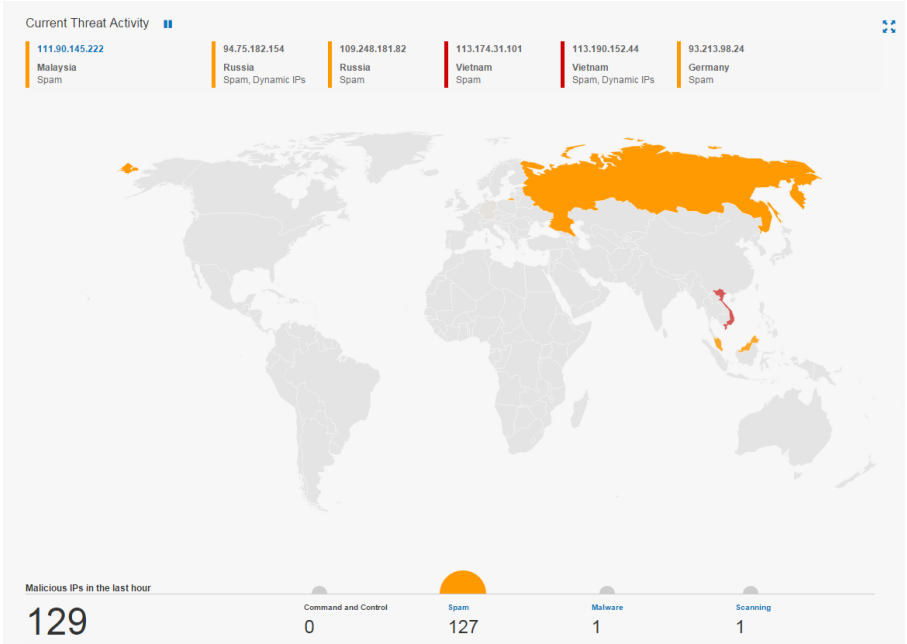
- For WCM content
- Permission can be granted in addition to user/group based rights
- Public API plug point for custom code in Core Access Control Layer
- Custom code can decide based on attributes controlled by business users
- Since 8.5

https://www.ibm.com/developerworks/community/groups/service/html/communityview?communityUuid=8f2bc166-3bdc-4a9d-bad4-3620dbb3e46c#fullpageWidgetId=Wc5d73787a343_444e_a578_049379d72276&file=d898a782-82e5-43a1-86f1-4d983b342256

# Portal Hardening



# Security in focus




http://xforce.ibmcloud.com

# Secure portal

- Every IBM WebSphere Portal installation is unique
- Security needs differ, e.g.
  - Intranet/Internet
  - Content
  - User population
  - Related Systems

More details in the Security Hardening Guide

http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Security_Hardening_Guide_for_IBM_WebSphere_Portal

# Session Security Integration

- New Default “enable” since v85
  - Prevents that a user can access the WAS session of another user on WAS
- UnauthorizedSessionRequestException
  - session.security.use.errorcode (WP ConfigService)
  - session.security.redirecturl (WP ConfigService)
- Session Management > Custom Properties
  - InvalidateOnUnauthorizedSessionRequestException
    - Possible to activate since v8.0.0.1

https://www.ibm.com/developerworks/community/blogs/PortalL2Thoughts/entry/why_does_userb_see_usera_s_data

# LoginURL

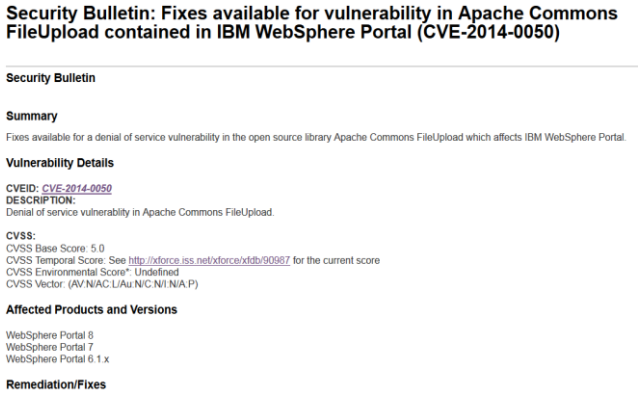
- Not a new thing, but well known
  (every user can find it on google)

http://wpsbvt.boeblingen.de.ibm.com:10039/wps/portal/cxml/04_SD9ePMtCP1I800I_KydQvyHFUBADPmuQy?userid=wpsadmin&password=wpsadmin

- Handy but not really secure if users leverage it via HTTP
  - PI13472 introduced the option to disable it (8001 CF 12 + 85 )
    - AuthenticationService.properties
    - authentication.isLoginUrlActive = true (/ false)

# Security Fixes

- Install security fixes
  - Identify security fixes
    - Overview of installed software
    - Channels to use (IBM: E.g. PSIRT Blog/My Notifications)
  - Define processes to install security fixes
    - Responsibilities
    - Time frame
- Proactive: Use current maintenance levels



**Security Bulletin: Fixes available for vulnerability in Apache Commons FileUpload contained in IBM WebSphere Portal (CVE-2014-0050)**

**Security Bulletin**

**Summary**

Fixes available for a denial of service vulnerability in the open source library Apache Commons FileUpload which affects IBM WebSphere Portal.

**Vulnerability Details**

**CVEID:** CVE-2014-0050
**DESCRIPTION:**
Denial of service vulnerablity in Apache Commons FileUpload.

**CVSS:**
CVSS Base Score: 5.0
CVSS Temporal Score: See http://xforce.iss.net/xforce/xfdb/90987 for the current score
CVSS Environmental Score*: Undefined
CVSS Vector: (AV:N/AC:L/Au:N/C:N/I:N/A:P)

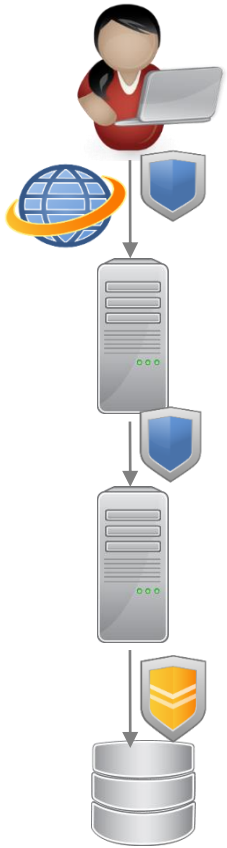
**Affected Products and Versions**

WebSphere Portal 8
WebSphere Portal 7
WebSphere Portal 6.1.x

**Remediation/Fixes**

# Secure Communication

- Usage of TLS/HTTPS
- Some scenarios:
  - Never (probably not the best idea)
  - For passwords
  - Logged In
  - Always



# Custom Code

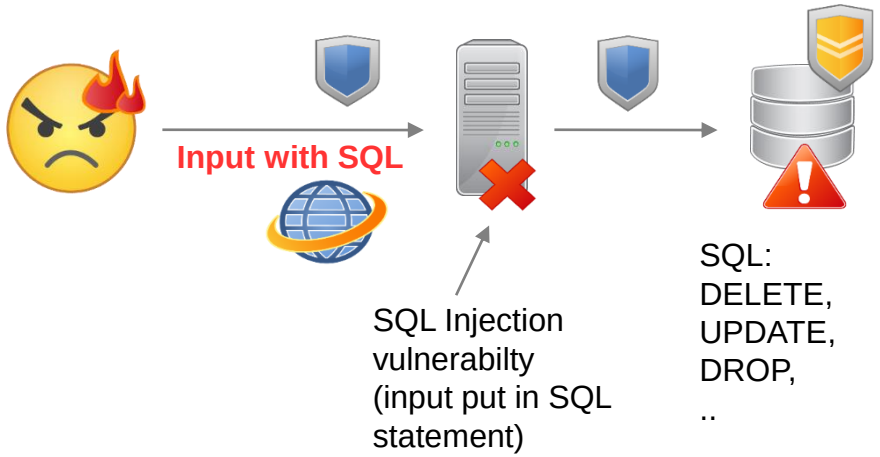
- Raise development's awareness
  - Training
  - Documentation
  - Reviews
- Prevent introduction of potential vulnerabilities
  - Coding guidelines
  - Frameworks/APIs
  - Automated test tooling (AppScan)

# Custom Code

- Security Vulnerabilities in Web Applications
  - Cross Site Scripting
  - Unvalidated Redirects/Forwards
  - SQL Injection
  - ..

Open Web Application Security Project
https://www.owasp.org

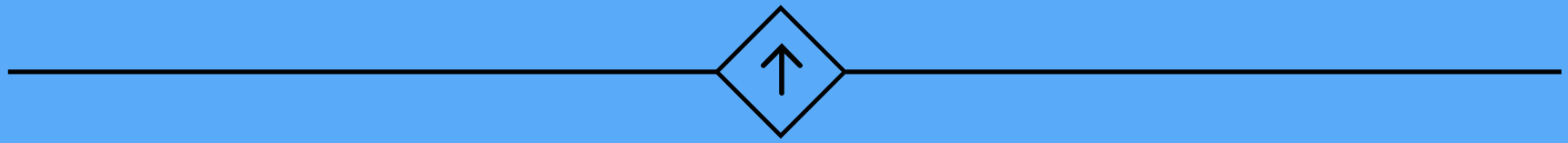
- OWASP Top 10



# DeveloperWorks Community of Portal Security Team

https://www.ibm.com/developerworks/community/groups/community/PortalSecurityTeam

# Vielen Dank



# Thomas Hurek, Digital Experience Lab Services, IBM USA

Join the conversation
Blog, YouTube, Twitter and Facebook

IBM Commerce