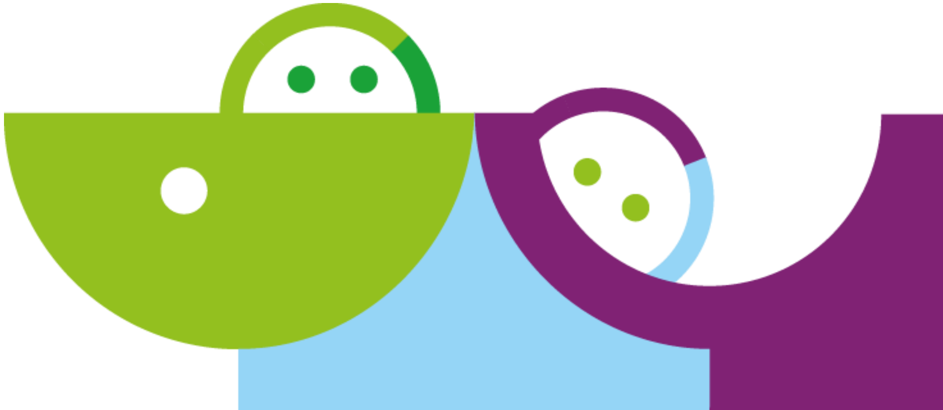
DIGITAL NAIV ODER DIGITAL NATIVE?

Egal! Hauptsache, Sie sind digital präsent, überall und jederzeit!



WEBSPHERE PORTAL AUTHENTICATION AND AUTHORIZATION IN CLOUD

SECURITY FOR PORTAL

Sascha Schefenacker, Portal Security

Please Note

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.

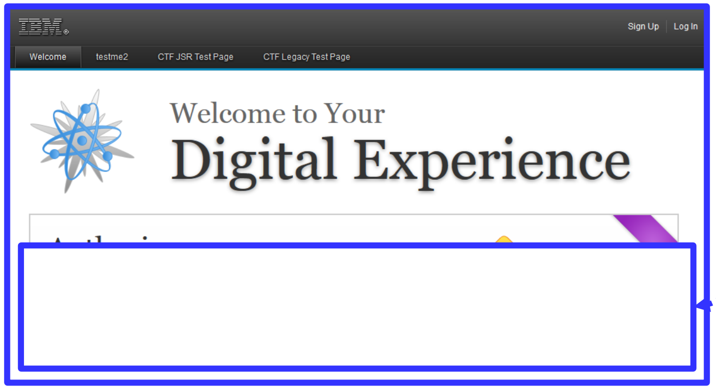
The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features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

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user’s job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

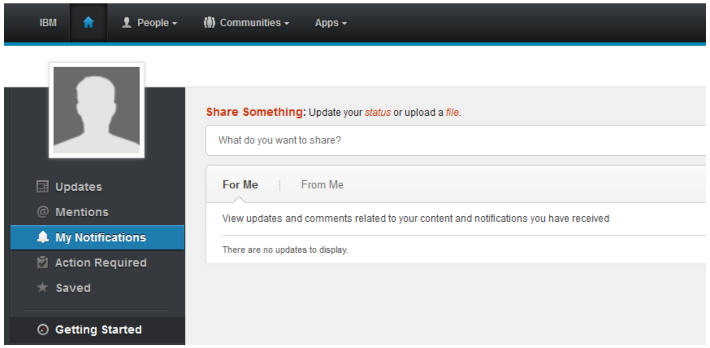
Agenda

- Seemless integrate Cloud data
- SSO FrontSide
  - Transient users
  - VP scoping
- SSO BackEnd
  - HTTPOutbound
- Portal Hardening

Seemless integrate Cloud data



Welcome to Your
Digital Experience



Share Something: Update your *status* or upload a *file*.

What do you want to share?

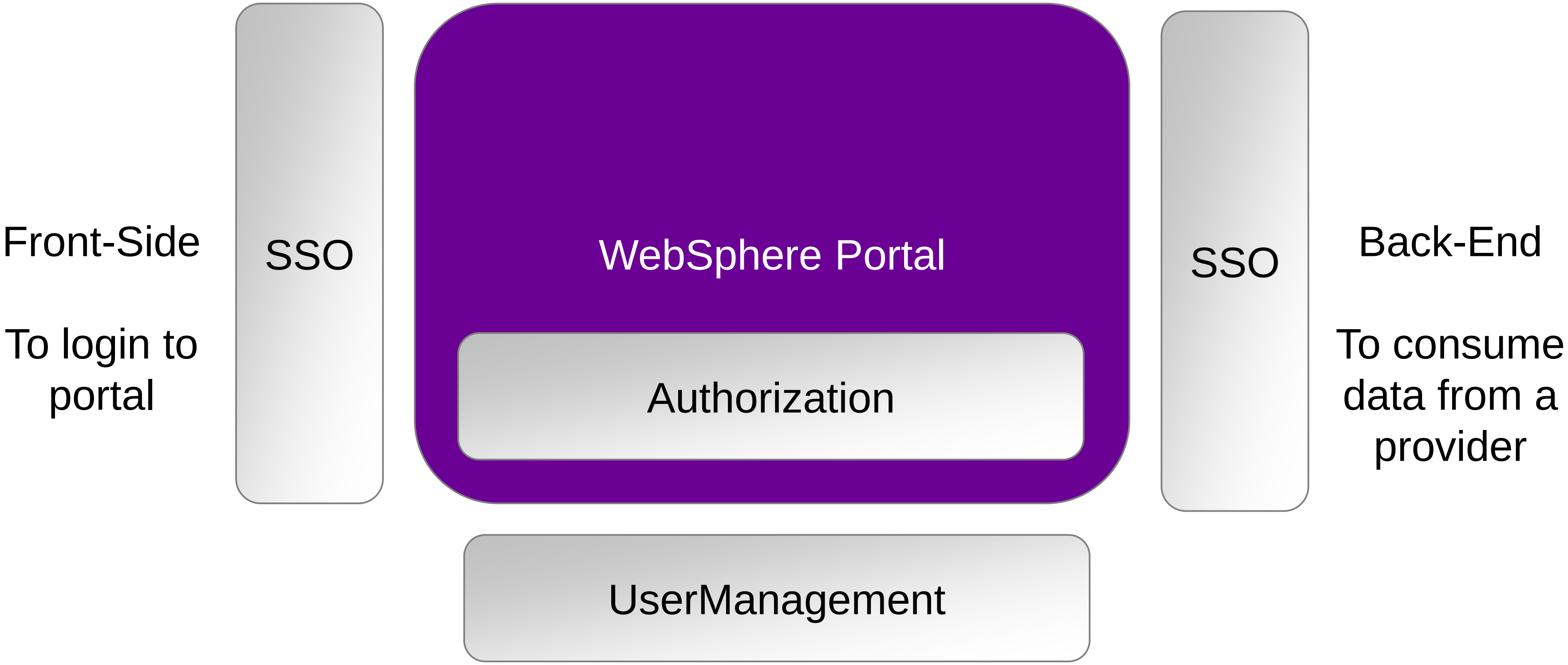
View updates and comments related to your content and notifications you have received

There are no updates to display.

Integrate data seamless into the portal.

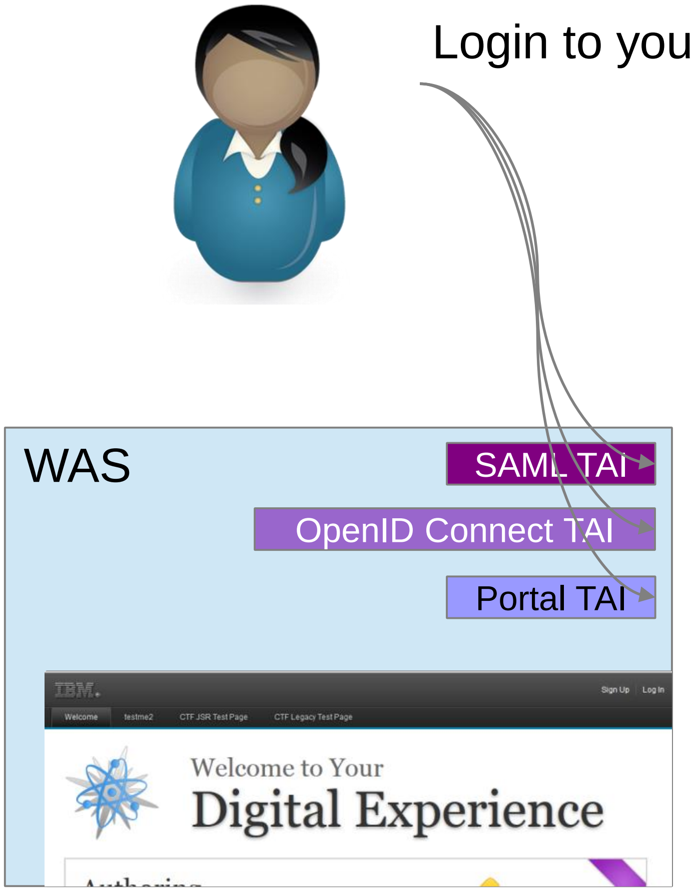
New questions appear...
How to login?
Is information user-scoped?
How to consume?

Login and SSO in different areas



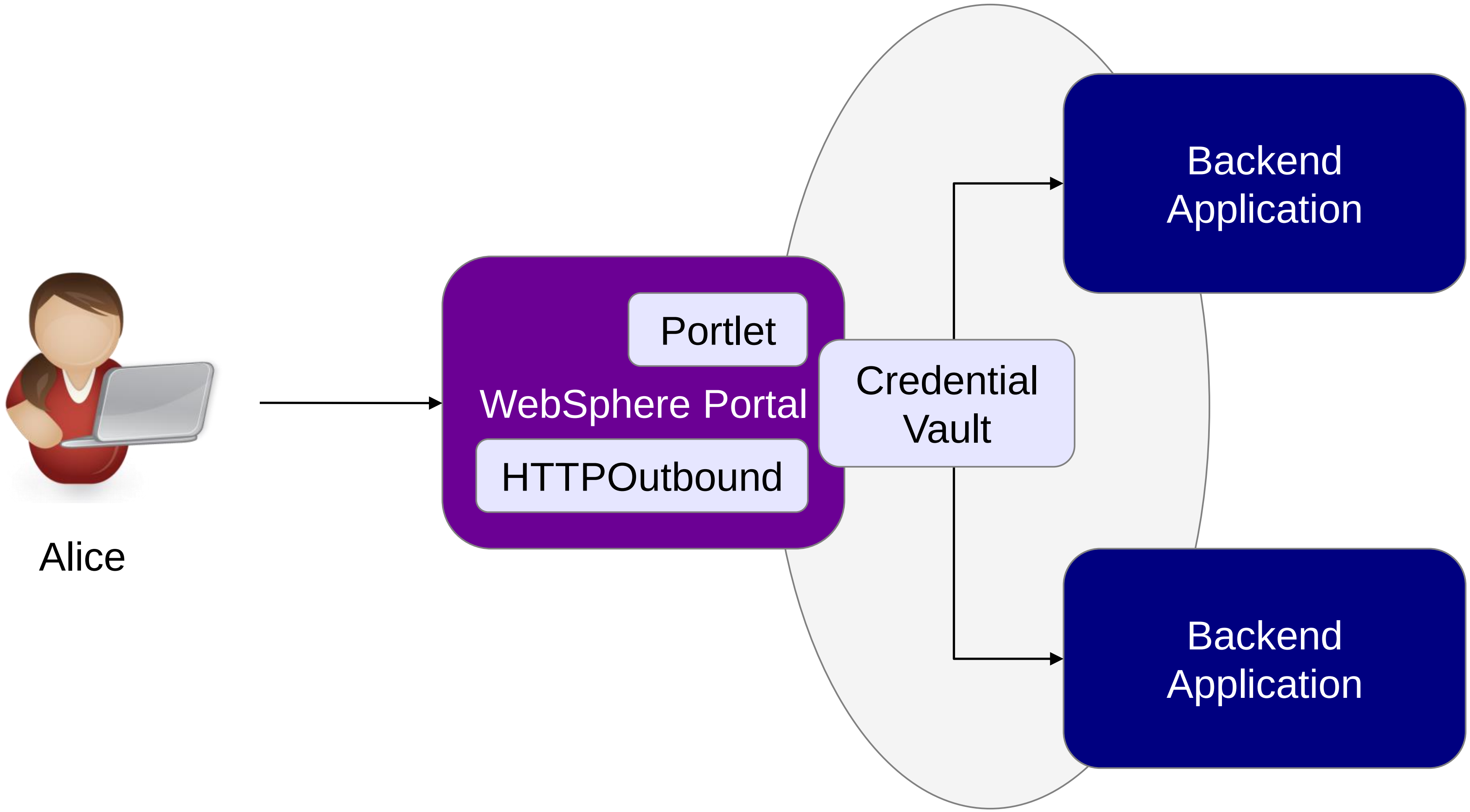
Front Side SSO

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**

Back-End SSO


Alice
Portlet
WebSphere Portal
HTTPOutbound
Credential Vault
Backend Application
Backend Application

Protocol Overview

OpenId

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

Oauth

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

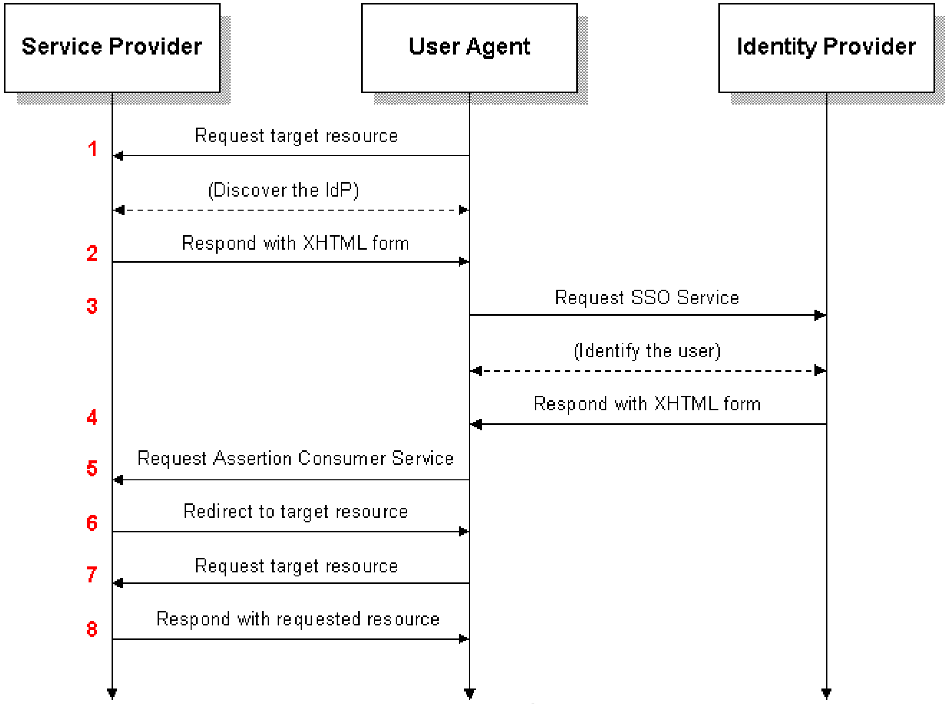
OpenId connect

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

SAML

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

SP POST Request; IdP POST Response



Service Provider

User Agent

Identity Provider

1 Request target resource

(Discover the IdP)

2 Respond with XHTML form

3 Request SSO Service

(Identify the user)

4 Respond with XHTML form

5 Request Assertion Consumer Service

6 Redirect to target resource

7 Request target resource

8 Respond with requested resource

SP initiated vs. IdP initiated

HTTPOutbound works with IdP initated flows.

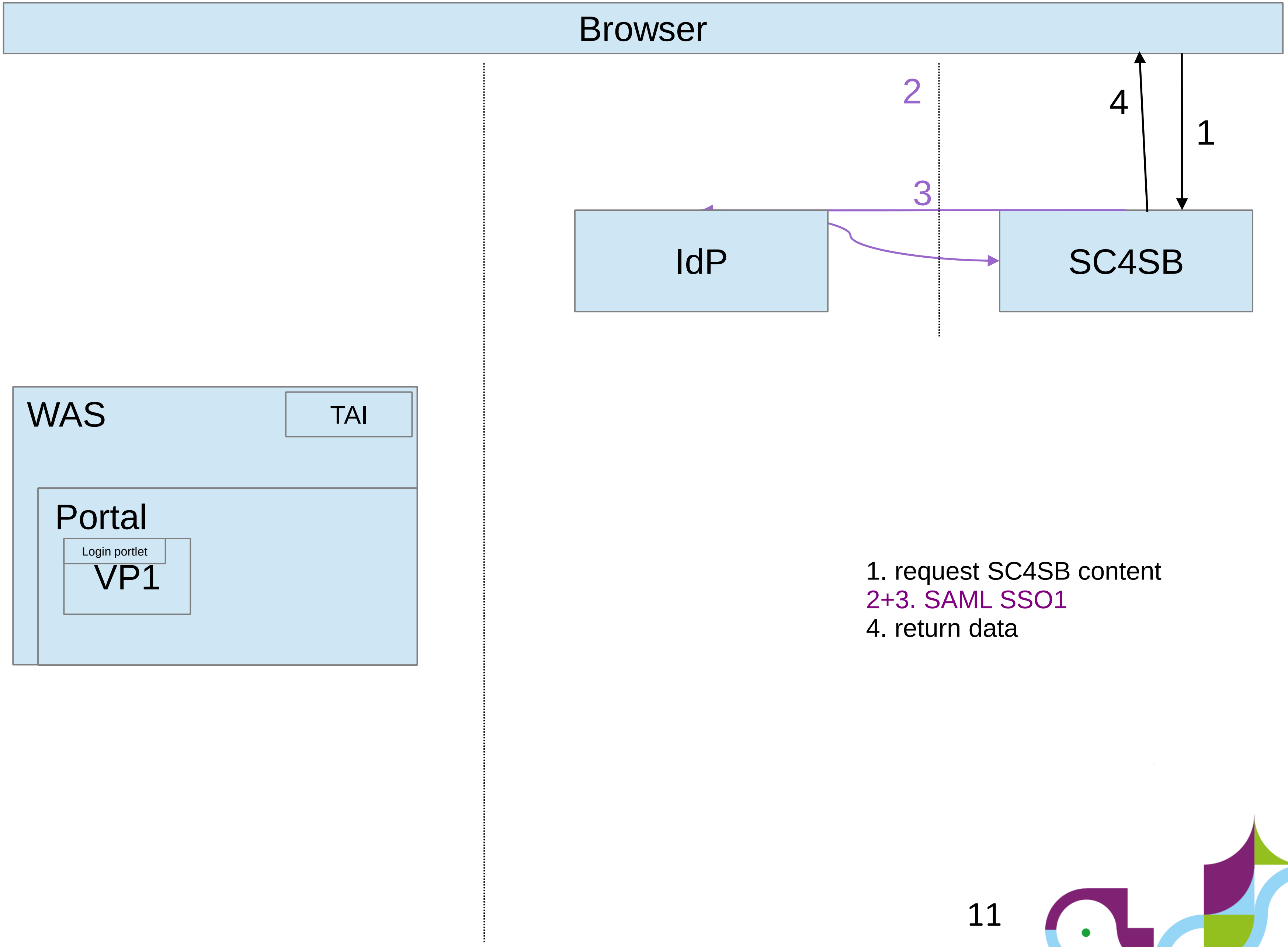
The technical flow may not be recognized by a user – even the technical footprint differs.

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.

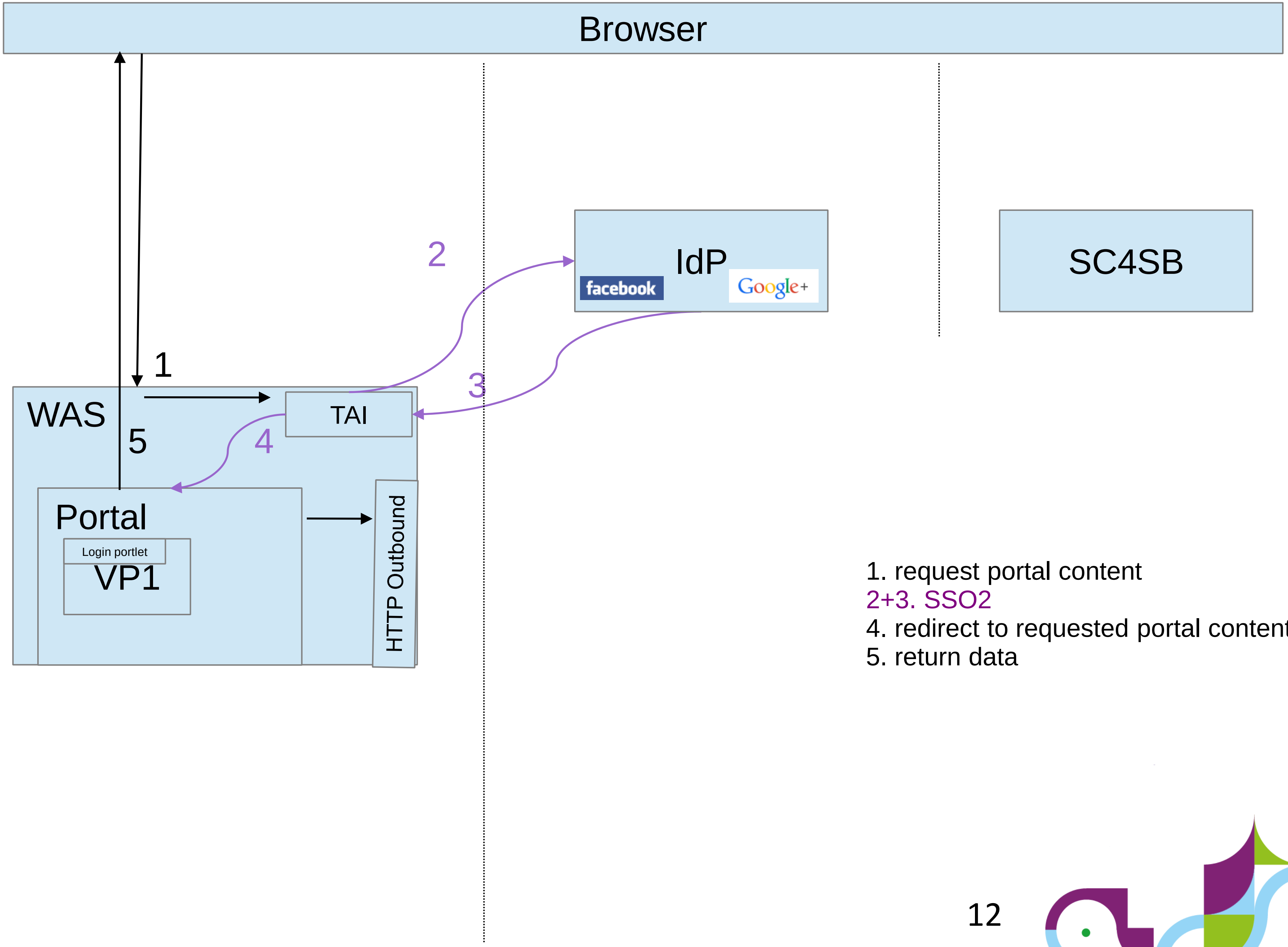
Given that a User recognize it as SP initated flow – but it is a IdP started flow.

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 SC4SB content
2+3. SAML SSO1
4. return data



1. request portal content
2+3. SSO2
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

Virtual Portal scoping

Even if a user is found in the connected repositories the user still may not be valid for the current VP realm.

A user might be valid for VP1 but still is a transient user for VP2.

A transient users of VP1 should not be automatically allowed to visit VP2 as transient user as well.

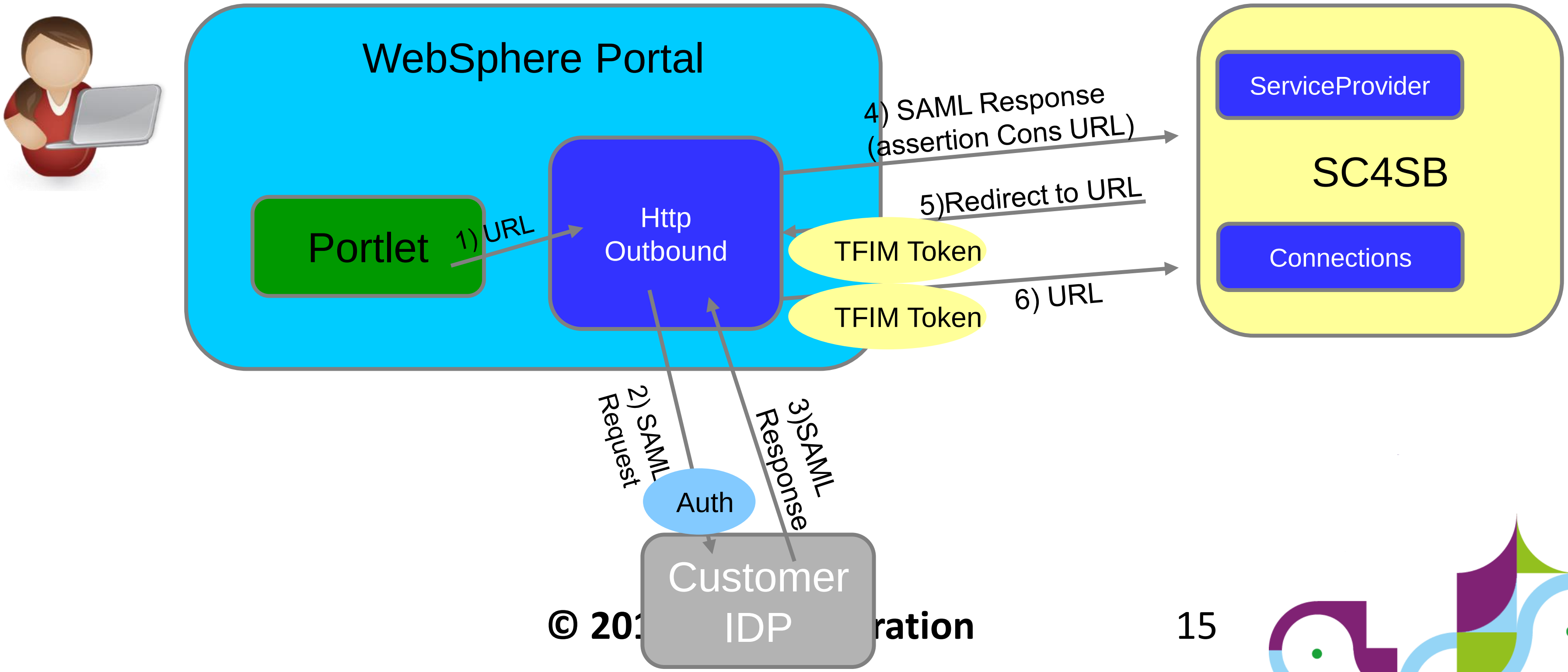
Restart after config neccessary

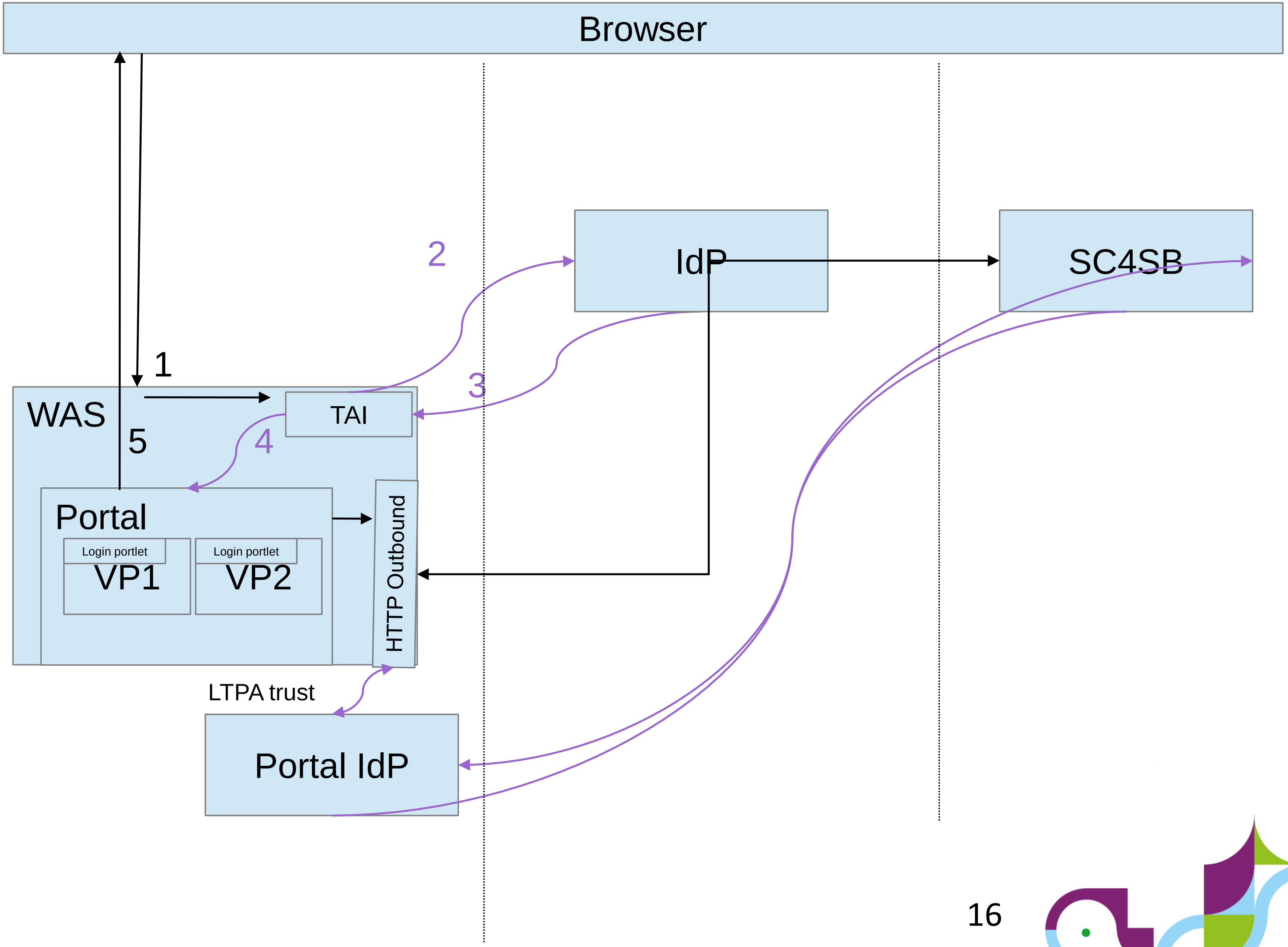
TAI config on WAS level

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

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
2
IdP
SC4SB
1
3
WAS
TAI
5
4
Portal
Login portlet
VP1
Login portlet
VP2
HTTP Outbound
LTPA trust
Portal IdP

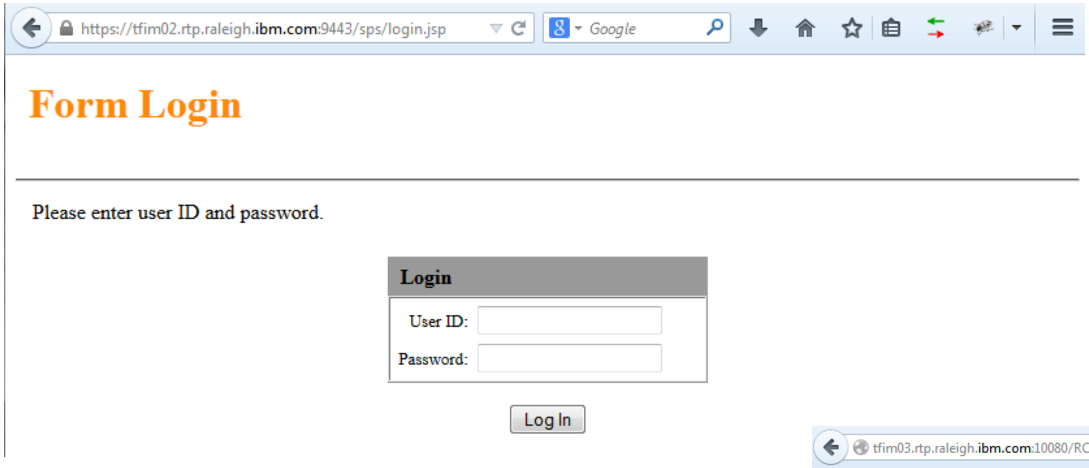
Setup / Error finding best practice

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

IdP Flow

https://tfim02.rtp.raleigh.ibm.com:9443/sps/LibertyFlow/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://tfim03.rtp.raleigh.ibm.com:9443/sps/LibertySP/saml20&TARGET=https://tfim03.rtp.raleigh.ibm.com:10080/RCSSTest&NameIdFormat=Email



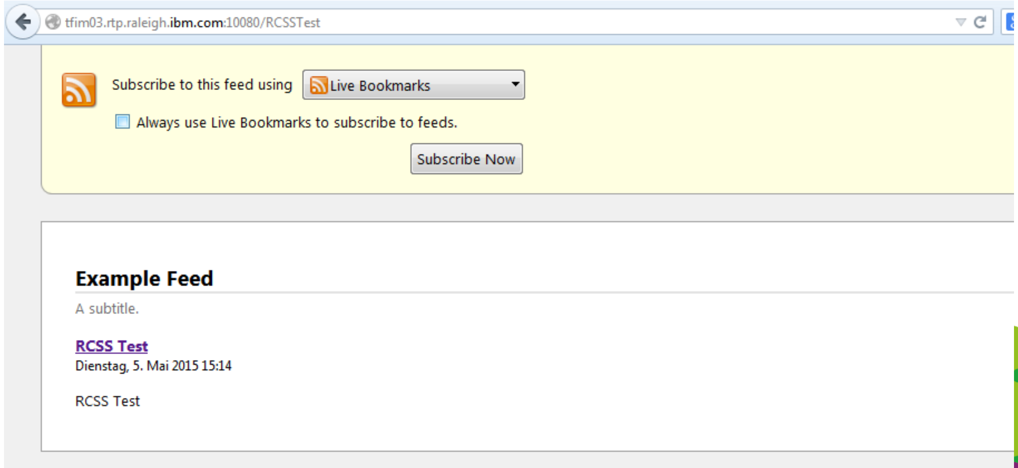
https://tfim02.rtp.raleigh.ibm.com:9443/sps/login.jsp

Form Login

Please enter user ID and password.

Login

User ID:	
Password:	



tfim03.rtp.raleigh.ibm.com:10080/RCSSTest

Subscribe to this feed using Live Bookmarks

☐ Always use Live Bookmarks to subscribe to feeds.

Example Feed

A subtitle.

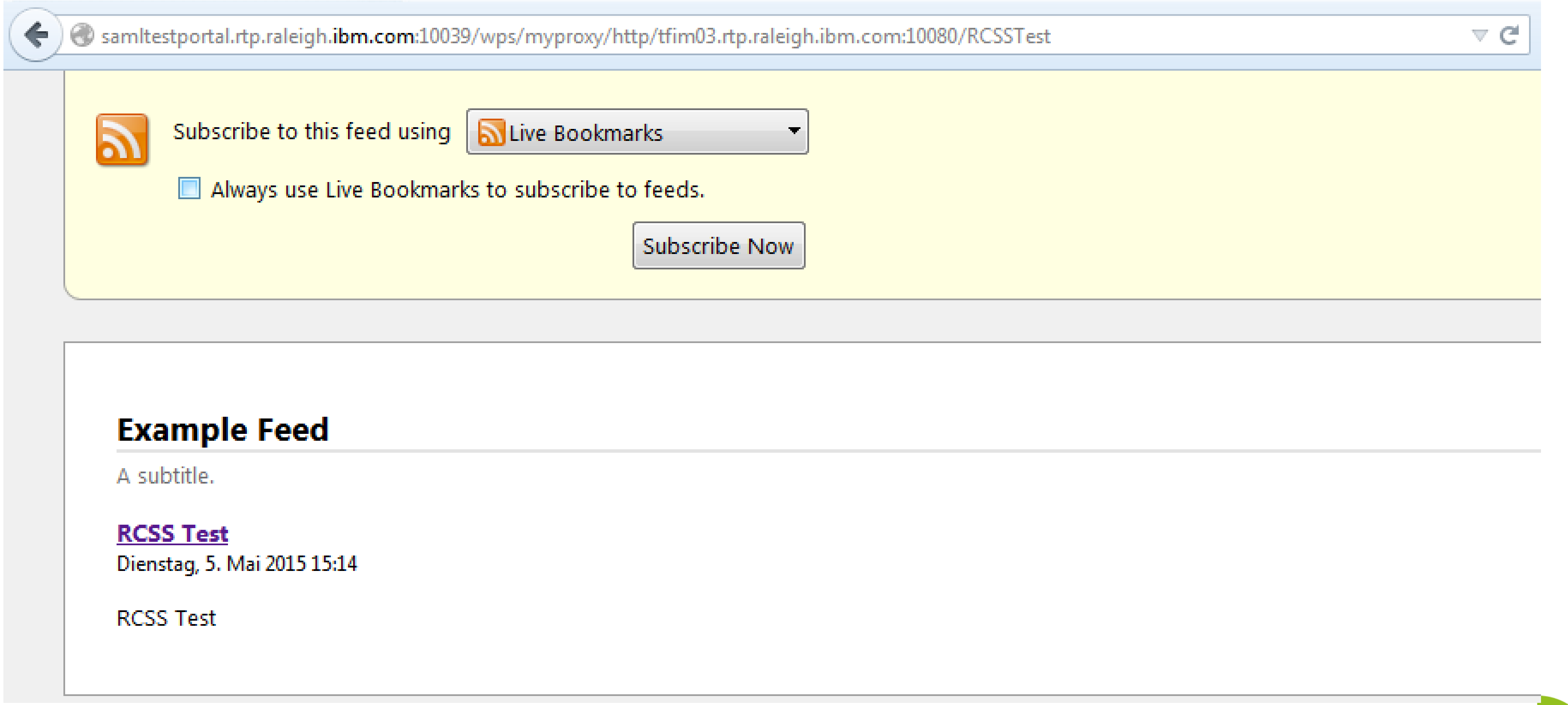
RCSS Test

Dienstag, 5. Mai 2015 15:14

RCSS Test

HTTPOutbound Flow

http://samltestportal.rtp.raleigh.ibm.com:10039/wps/myproxy/http/tfim03.rtp.raleigh.ibm.com:10080/RCSSTest



samltestportal.rtp.raleigh.ibm.com:10039/wps/myproxy/http/tfim03.rtp.raleigh.ibm.com:10080/RCSSTest

Subscribe to this feed using Live Bookmarks

□ Always use Live Bookmarks to subscribe to feeds.

Subscribe Now

Example Feed

A subtitle.

RCSS Test

Dienstag, 5. Mai 2015 15:14

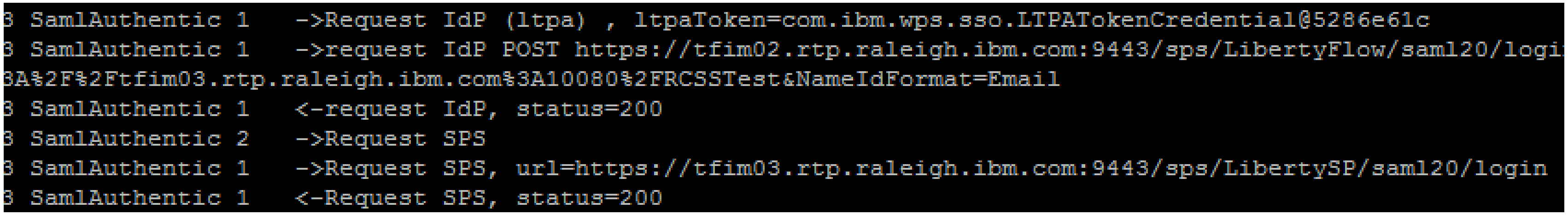
RCSS Test

Tracing of SAML HTTPOutbound

Added a new traceing support by using different trace levels to allow tracing on systems with high load (e.g. cloud instance)

com.ibm.wps.proxy.saml.SamlAuthenticationFilter=**FINE**

Shows the flow to IP and SP including status code



```
3 SamlAuthentic 1   ->Request IdP (ltpa) , ltpaToken=com.ibm.wps.sso.LTPATokenCredential@5286e61c
3 SamlAuthentic 1   ->request IdP POST https://tfim02.rtp.raleigh.ibm.com:9443/sps/LibertyFlow/saml20/logi
3A%2F%2Ftfim03.rtp.raleigh.ibm.com%3A10080%2FRCSSTest&NameIdFormat=Email
3 SamlAuthentic 1   <-request IdP, status=200
3 SamlAuthentic 2   ->Request SPS
3 SamlAuthentic 1   ->Request SPS, url=https://tfim03.rtp.raleigh.ibm.com:9443/sps/LibertySP/saml20/login
3 SamlAuthentic 1   <-Request SPS, status=200
```

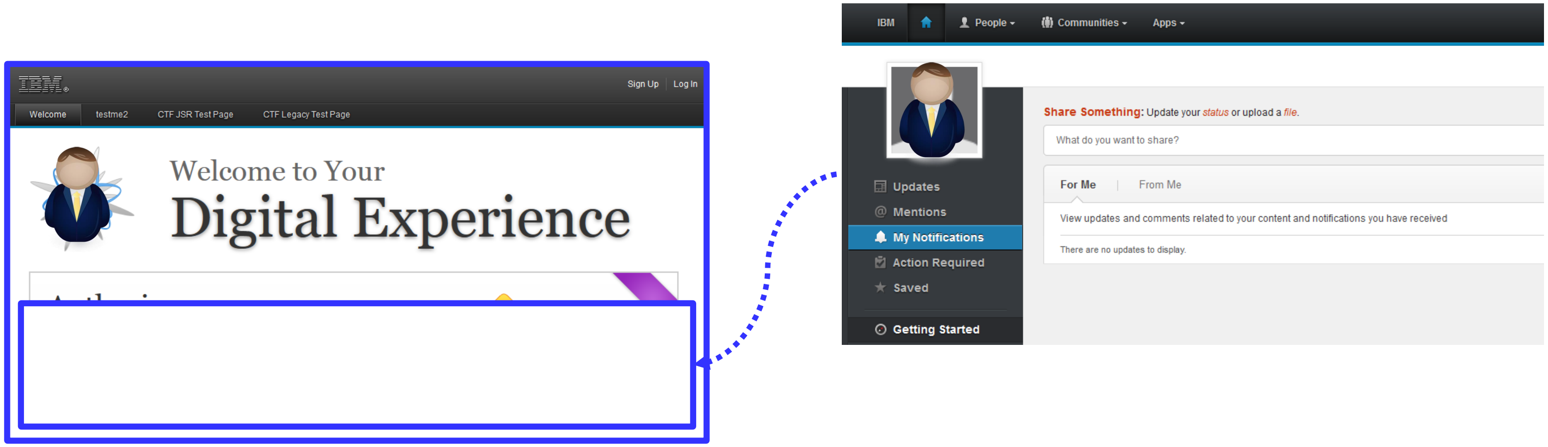
com.ibm.wps.proxy.saml.SamlAuthenticationFilter=**FINER**

Shows the regular flow and information

com.ibm.wps.proxy.saml.SamlAuthenticationFilter=**all/FINEST**

Adds additional information for 401 handling on Backend

Seemless integrate Cloud data - solved



Share Something: Update your *status* or upload a *file*.

What do you want to share?

View updates and comments related to your content and notifications you have received

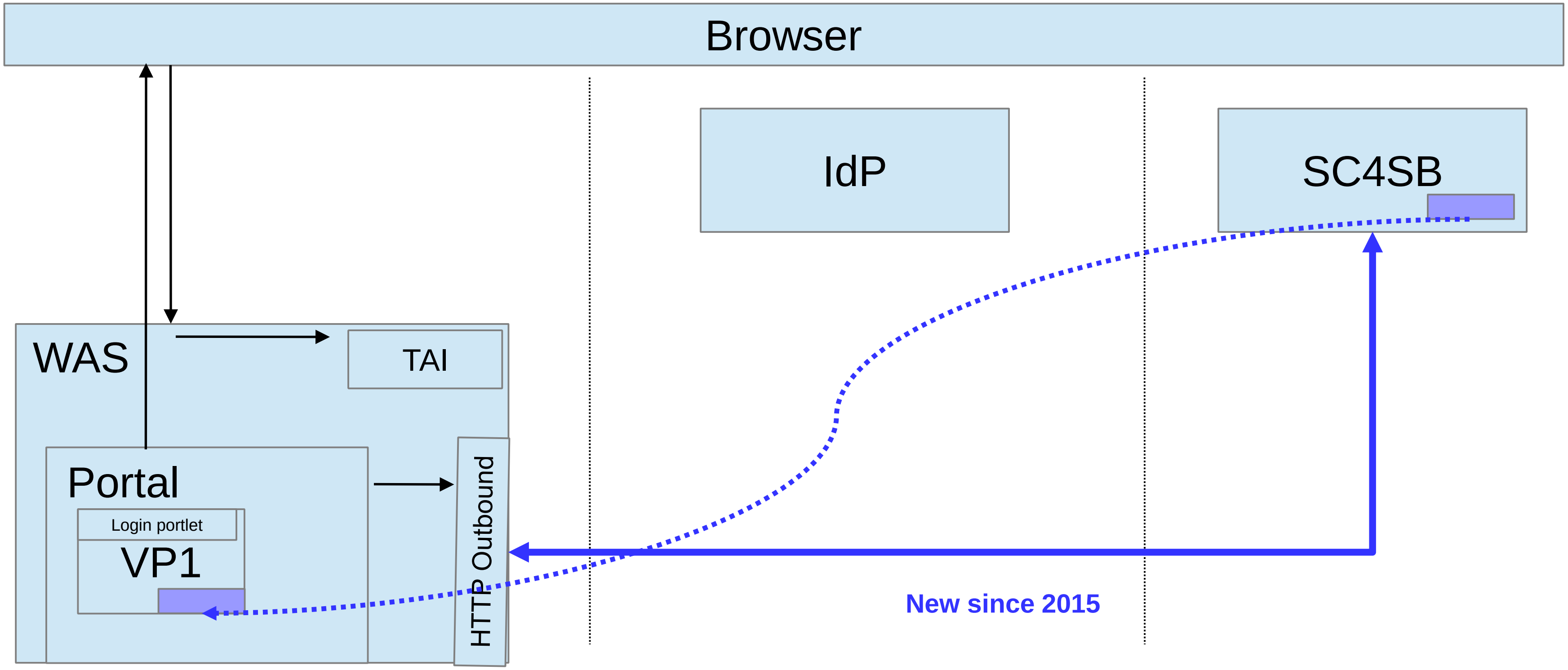
There are no updates to display.

User based SSO from portal to BackEnd to integrate data seamless into the **data model** (e.g. DDC : TECH-D07).

Now you are able to work with e.g. the SC4SB offering 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

Seemless integrate Cloud data



User based SSO from portal to SC4SB to integrate data seamless into the data model (DDC).

Own code vs. using HTTPOutbound

- HTTPOutbound is the streamlined architecture for backend data retrieval
- Use one code base for all flows
- Use one configuration for all flows

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

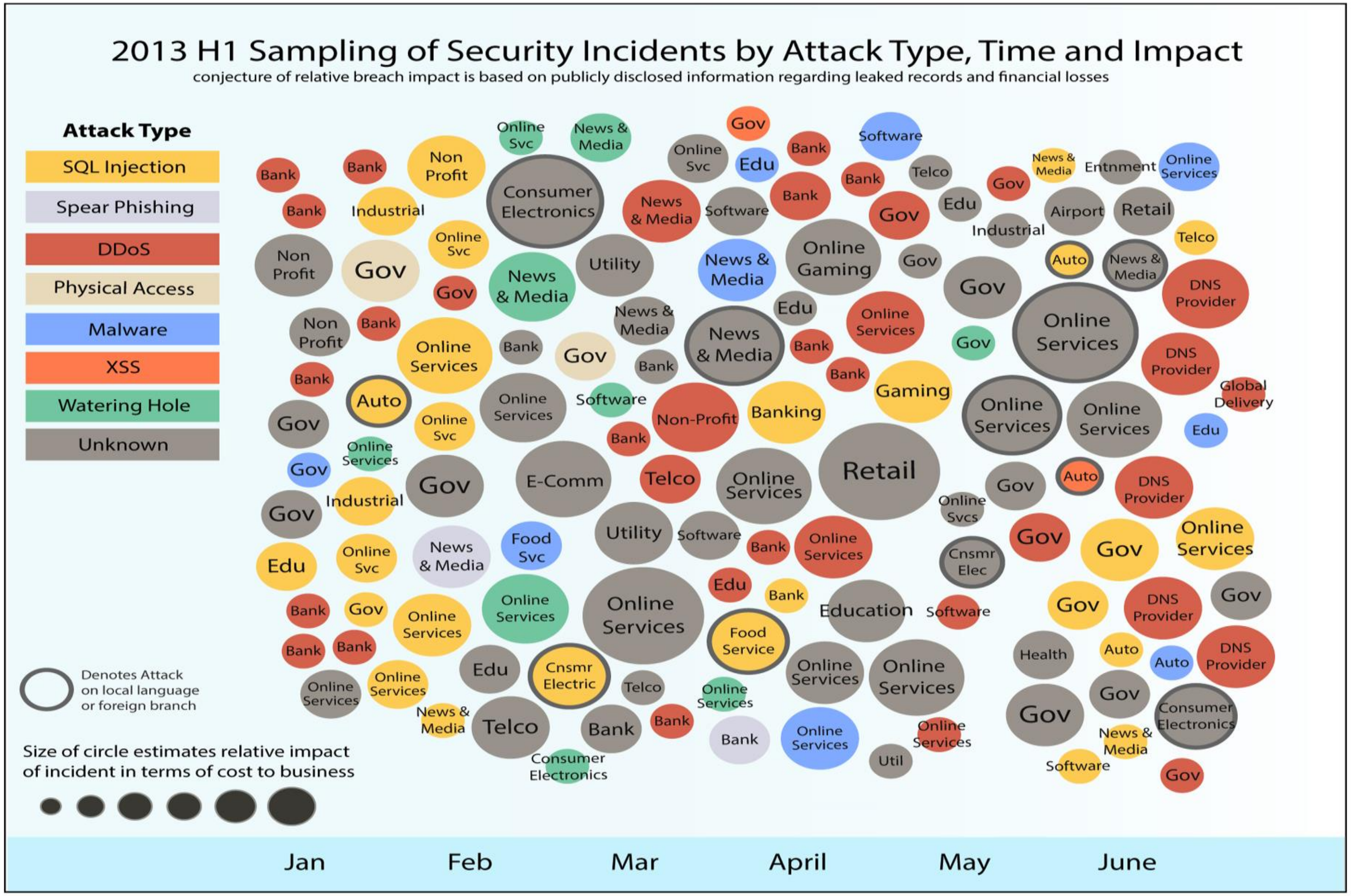
- It is possible to get profile information from the IdP or ID-provider. Those needs to get mapped to portal attributes.

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

Security in focus


2013 H1 Sampling of Security Incidents by Attack Type, Time and Impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

Source: IBM X-Force® Research and Development

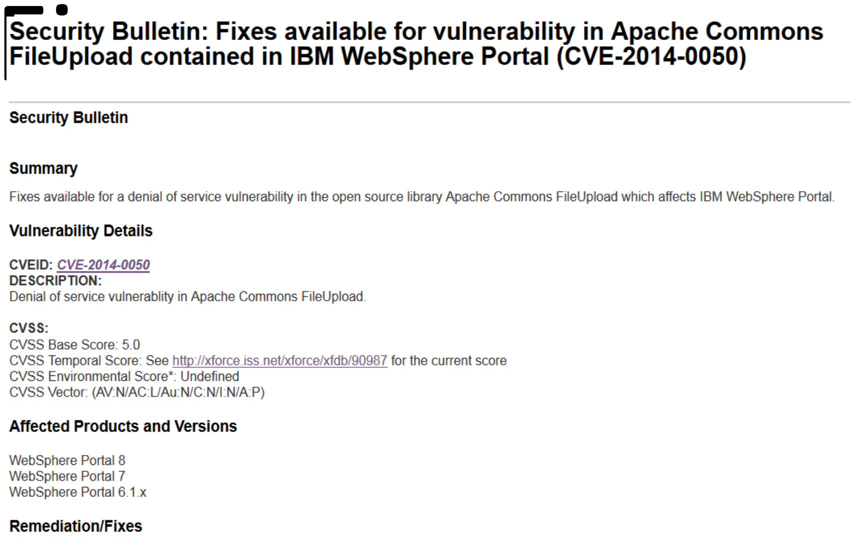
Secure portal

- 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

Security Fi



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

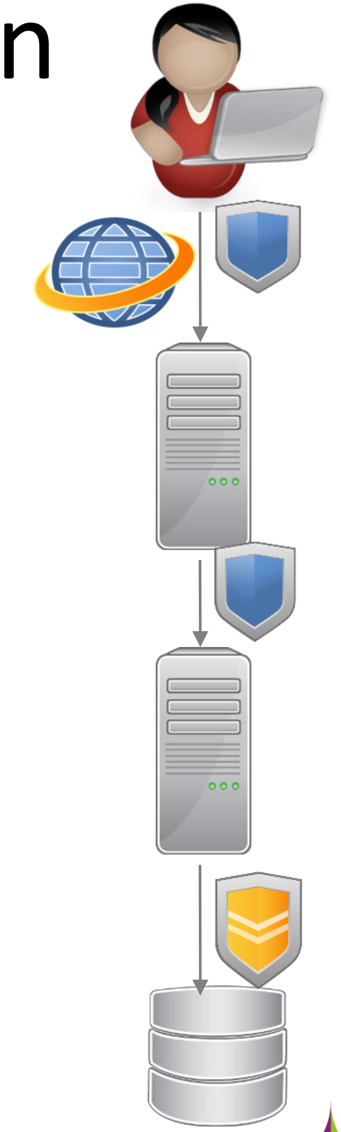
WebSphere Portal 8
WebSphere Portal 7
WebSphere Portal 6.1.x

Remediation/Fixes

- 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

Secure Communication

- Usage of TLS/HTTPS
- Some scenarios:
  - Never
  - For passwords
  - Logged In
  - With any input data
  - Always

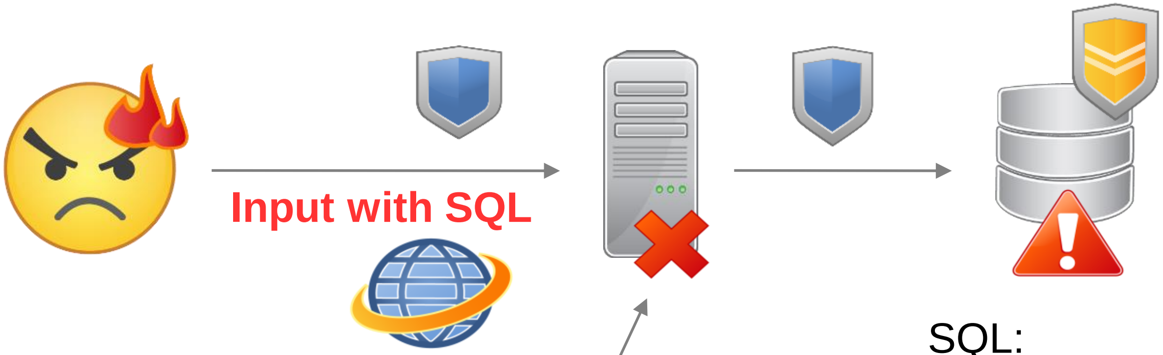


Custom Code

- 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
  - ..



SQL Injection vulnerabilty (input put in SQL statement)

SQL:
DELETE,
UPDATE,
DROP,
..

- OWASP Top 10

- **IBM Digital Experience Solutions**

  http://www-01.ibm.com/software/collaboration/digitalexperience

- **DeveloperWorks Community of Portal Security Team**

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

- **WebSphere Portal and IBM Web Content Manager Information Center Wiki**

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

- **IBM Digital Experience Demonstrations:**

  http://www.youtube.com/user/IBMXWebX

- **IBM Digital Experience Developer**

  http://developer.ibm.com/digexp

- **IBM Software Business Solutions Catalog**

  https://greenhouse.lotus.com/catalog/