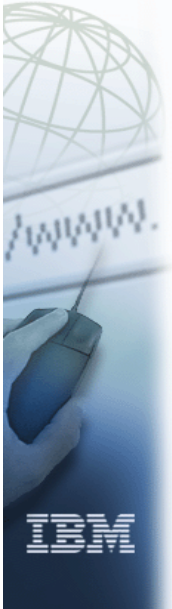


ibm.com



e-business



Powerful and secure infrastructures with WebSphere Application Server for z/OS

Securing WebSphere using Local and Remote Registries



Redbooks

International Technical Support Organization

© Copyright IBM Corp. 2003. All rights reserved.

Holger Wunderlich / wunderl@us.ibm.com

Notices

This information was developed for products and services offered in the U.S.A.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

Affinity™
AIX®
CICS®
DB2®
eServer™
eServer™
Everyplace™
IBM®
IMS™

IMS/ESA®
MQSeries®
MVS™
MVS/ESA™
Notes®
OS/2®
OS/390®
Parallel Sysplex®
Redbooks™

Redbooks(logo)™
RACF®
S/390®
SecureWay®
SOM®
Tivoli®
WebSphere®
z/OS™
zSeries™

The following terms are trademarks of other companies:

Intel, Intel Inside (logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

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

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

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



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Objectives

Securing WebSphere using Local and Remote Registries

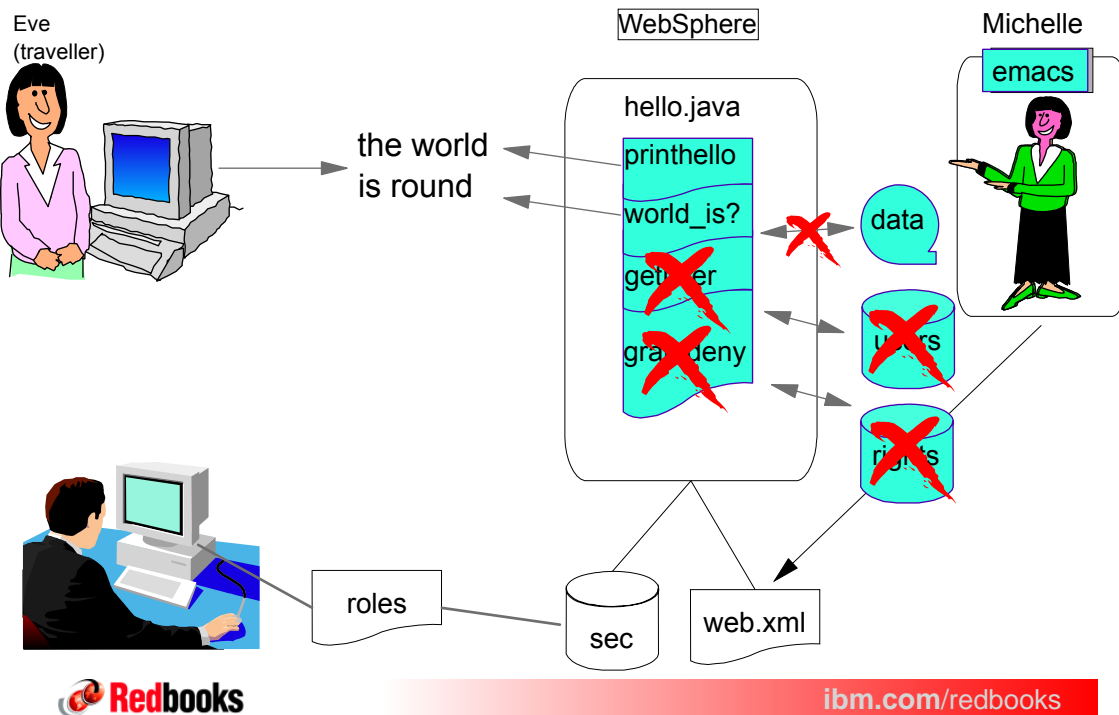
- Overview
- Authentication/Authorization Concepts
- Login mechanisms and methods
- Local Registry concepts
 - Authc, Authz, Auditing
- Trust Association Interceptor
- Remote Registry concepts
 - Using LDAP and Native Authentication
 - Using Custom User Registries
 - Incorporating Tivoli Access Manager
 - declarative
 - programmatic
- Summary
- Questions



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Pythagoras' guide to security frameworks



Why does WebSphere need a registry?

access decisions are based on:

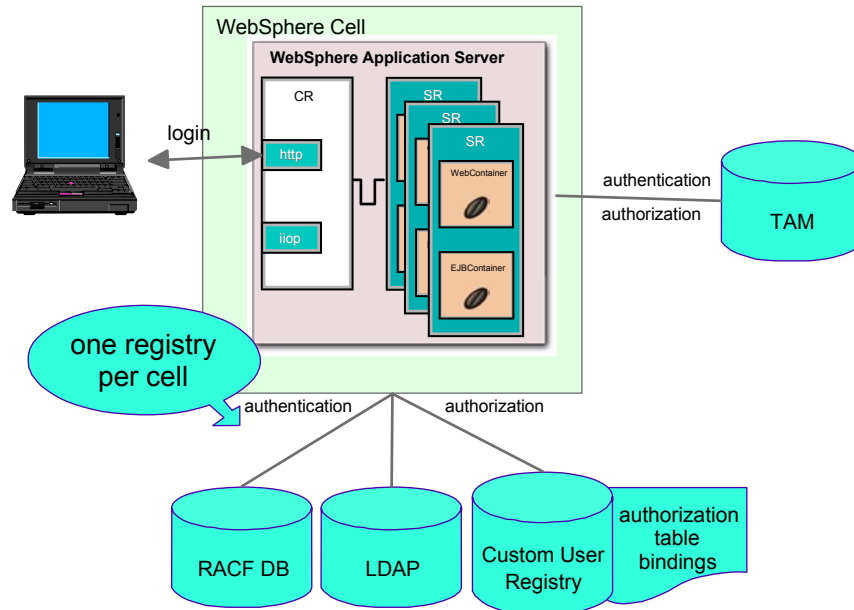
Authentication

- Who are you?
 - ID/Password
 - PassTickets
 - Digital Certificates, Identity mapping

Authorization

- What are you allowed to see / execute
 - group memberships
 - role to user mappings
 - protected resources (EJB and Web container)

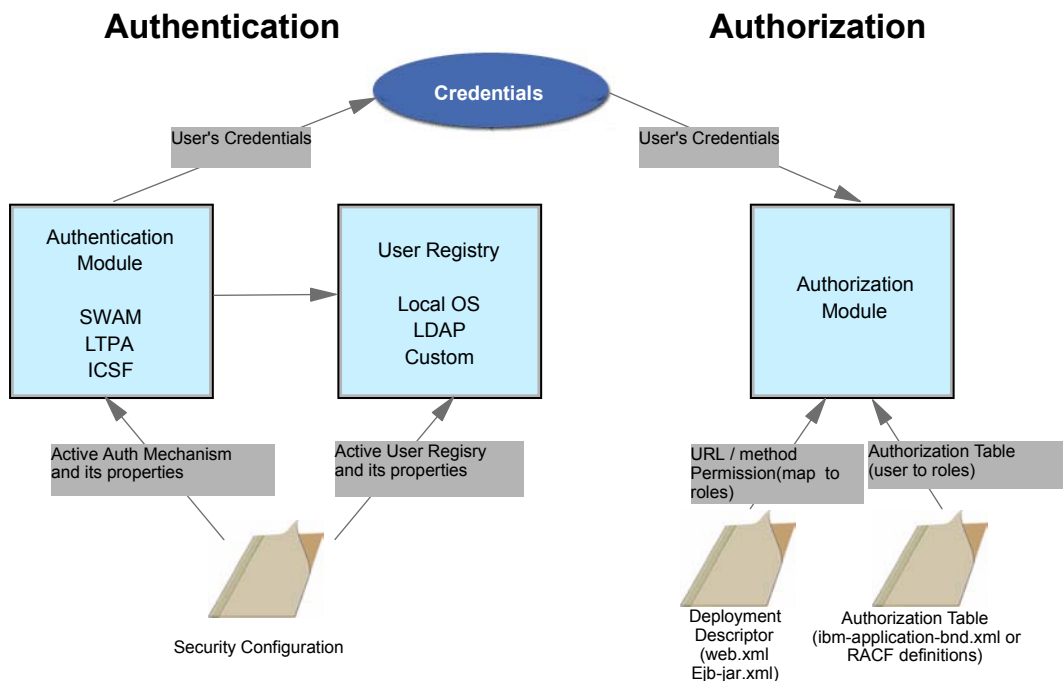
Multiple Registries



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Authentication Mechanisms and Registries

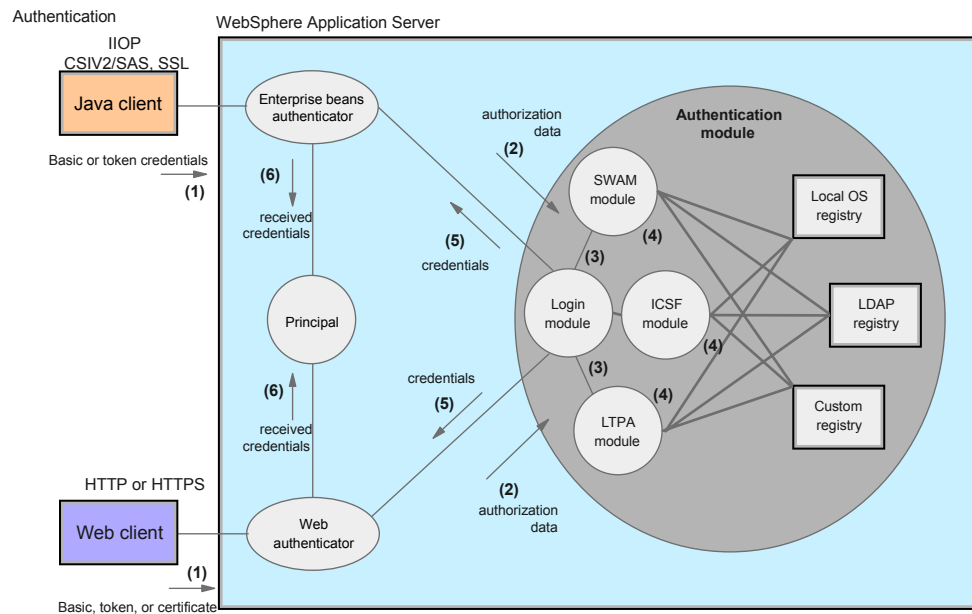


ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Authentication in Detail: HTTP & IIOP

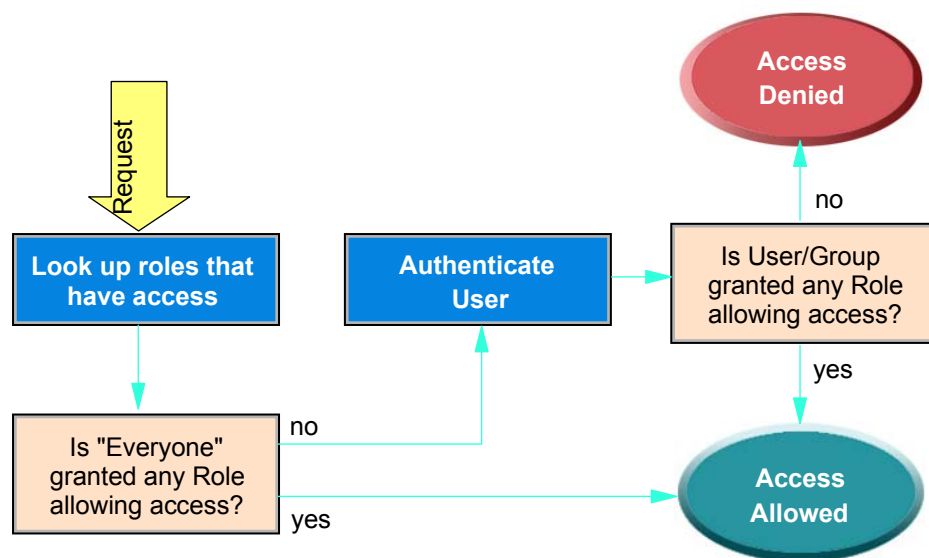
Authentication Process



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Authorization Flow

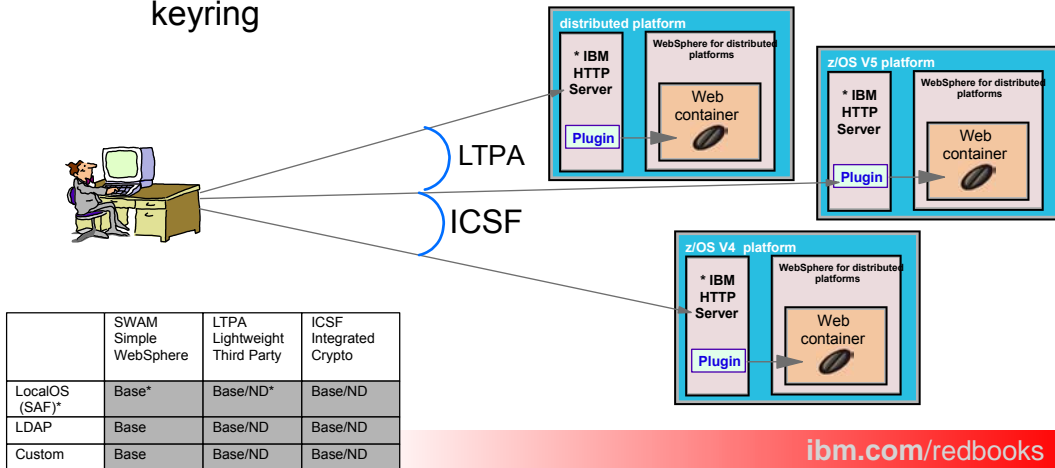


ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Authentication Mechanisms

- ▶ SSO
 - ▶ SWAM, No security token created
 - ▶ LTPA, Security token created by WebSphere using configured keys
 - ▶ ICSF, Security token created by ICSF using keys from SAF keyring



© Copyright IBM Corp. 2003. All rights reserved.

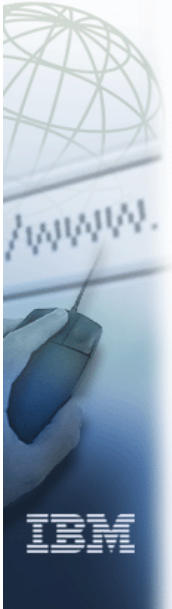
AUTHc AUTHz

- ▶ HTTP / Web Container
 - ▶ Authentication
 - ▶ Basic
 - ▶ Form based
 - ▶ Client certificate
 - ▶ Authorization
 - ▶ Role based
 - ▶ EJBROLES
 - ▶ bindings
 - ▶ Declarative or programmatic
 - ▶ isUserInRole("Frequent Writer")
 - ▶ getUserPrincipal()
- ▶ IIOP / EJB container
 - ▶ zSAS (local OS)
 - ▶ CSiv2
 - ▶ Authentication
 - ▶ Basic (userid/password)
 - ▶ Passticket
 - ▶ Client certificate
 - ▶ Asserted identity
 - ▶ Kerberos
 - ▶ Authorization
 - ▶ Role based
 - ▶ EJBROLES
 - ▶ bindings
 - ▶ Declarative or programmatic
 - ▶ isCallerInRole("Residence Leader")
 - ▶ getCallerPrincipal()

ibm.com



e-business

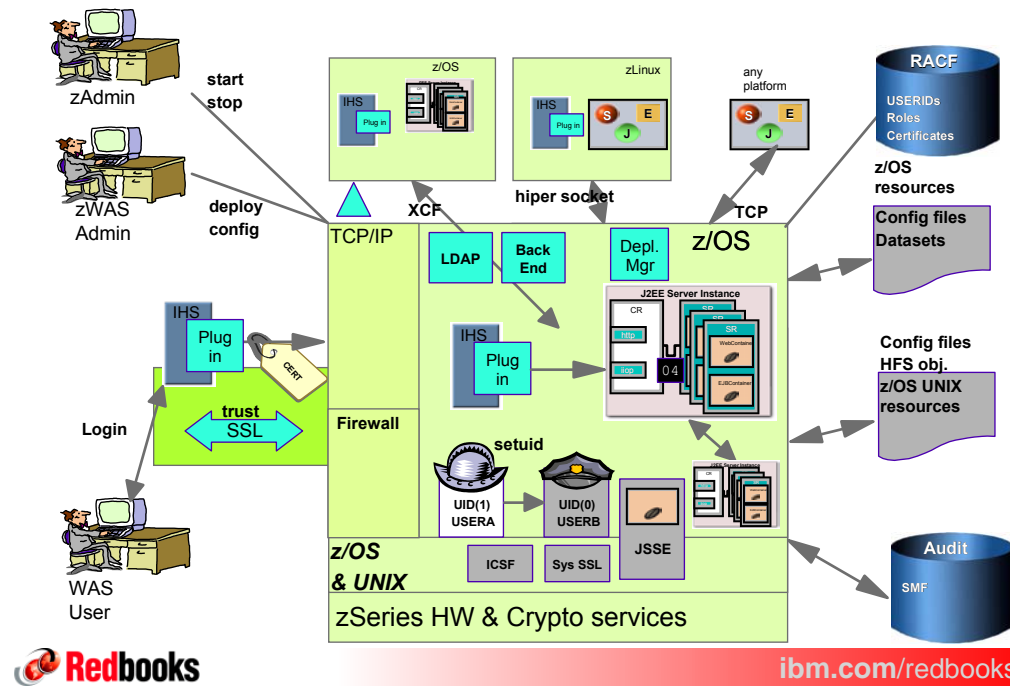


Local Registry Concepts



© Copyright IBM Corp. 2003. All rights reserved.

SAF is more than a WebSphere registry!



© Copyright IBM Corp. 2003. All rights reserved.

When should I use a local registry?

- ▶ When the authenticated users are present in the local registry(intranet)
- ▶ When best performance is mandatory
- ▶ When comprehensive end-to-end security is needed (userid present in the Web server, Web container, EJB container and backend system)
- ▶ When auditing is needed
- ▶ When the users and application security needs to be managed by the RACF security administrators
- ▶ For the Admin console
- ▶ When zSAS is needed (Passtickets, zWAS 4 interoperability)
- ▶ For SAF based run-as/RunAs role

When can I use a local registry?

- ▶ Authenticated or mapped users are in the SAF DB
- ▶ User to Role mappings are in the SAF DB



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

during authentication / expired passwords

RACF allows your passwords to expire. Not all authentication methods support expired passwords nicely, in fact RFC or Java standard conform implementations fail to deliver expired password support. If you need this functionality you can chose between following methods:

- ▶ Tivoli Access Manager for e-Business WebSeal front-end connected to LDAP running on z/OS backed by a RACF database.
- ▶ Enhanced Form based login
- ▶ Basic authentication front-ended by an IBM HTTP Server running in the same RACF plex that has the expired password support installed



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

during/after authentication / AS creation

■ Credentials are created

- ▶ z/OS: Submit, Start, Logon (certificate, passticket, kerberos, DCE.....)
- ▶ WebSphere:
 - Start, RACO, Asserted Identity, passticket, CSIV2
 - Authentication Mechanism: login, certificate, TAI,.....

■ Accessor Environment Element (ACEE)

- ▶ Assigned when a user logs onto the system, the user ID is assigned an ACEE credential, which it uses to identify the user
- ▶ Always setup when an address space is created
- ▶ Follows the process within the operating system
- ▶ Available to identify the authenticated user ID during access control authorization checking and for auditing purposes.

■ RACF Object (RACO) / environment element: transportable form of ACEE

- ▶ Can be acquired by an authorized application
- ▶ Can be transported from one address space to another on the same system (not between images in a sysplex)
- ▶ WebSphere on z/OS creates RACO's and transports them between its daemon and server address spaces.

■ Java Principal

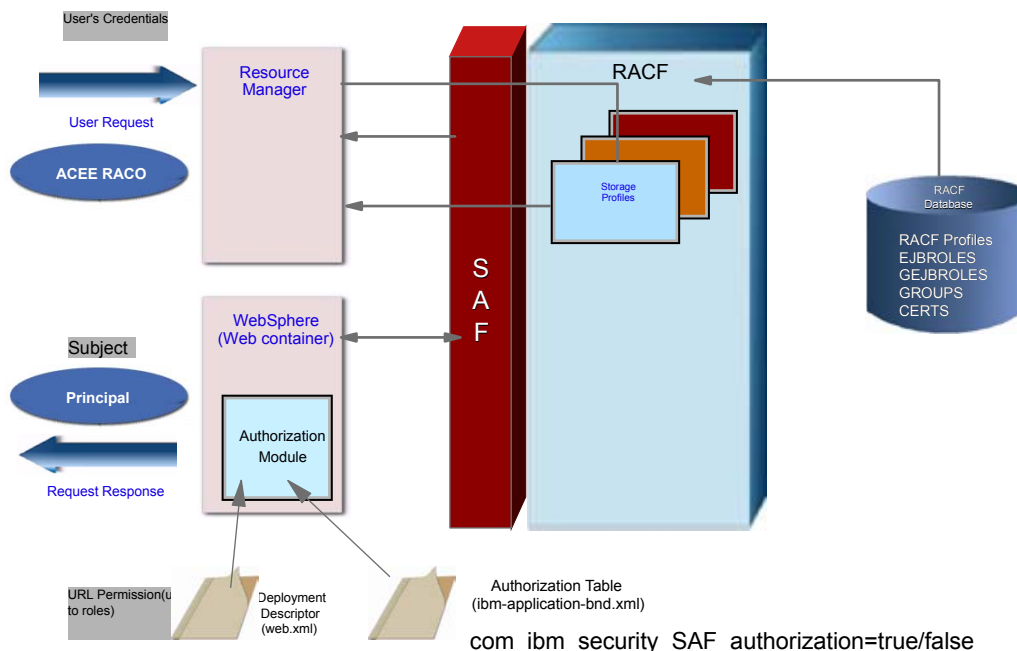
- ▶ Identity & Credential assigned to an request, stored in an object called subject



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

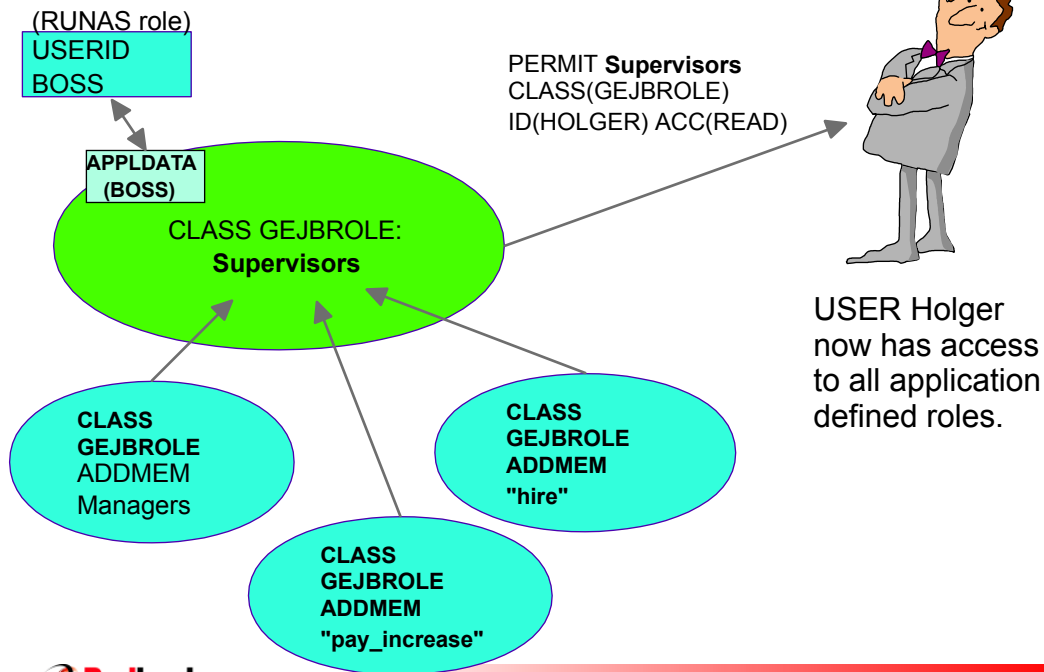
Authorization with a local registry



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

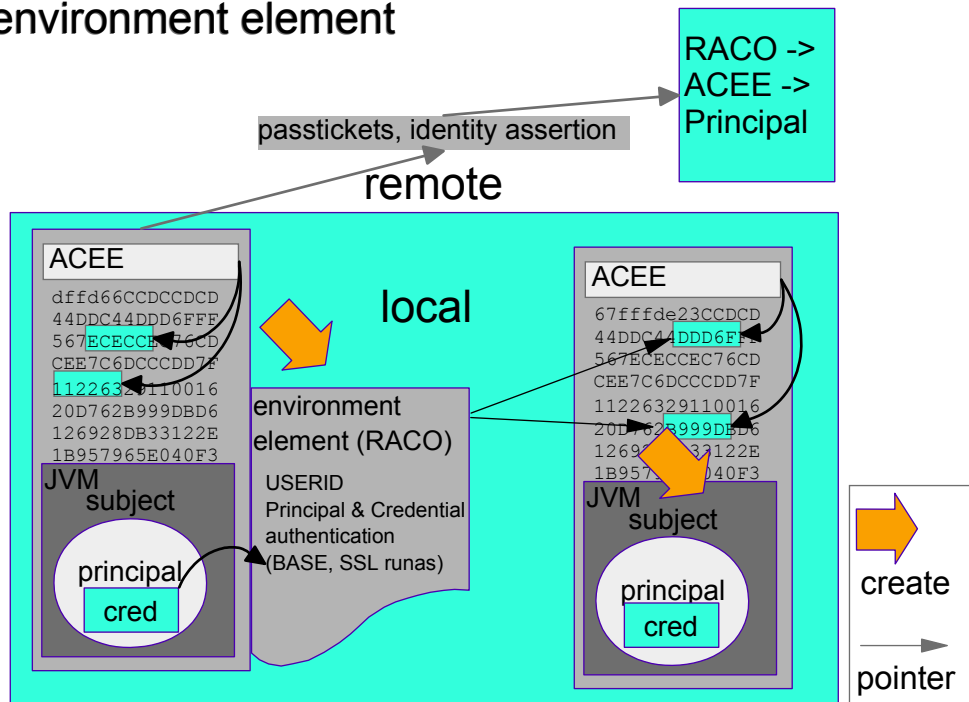
LOCAL OS authorization specifics



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

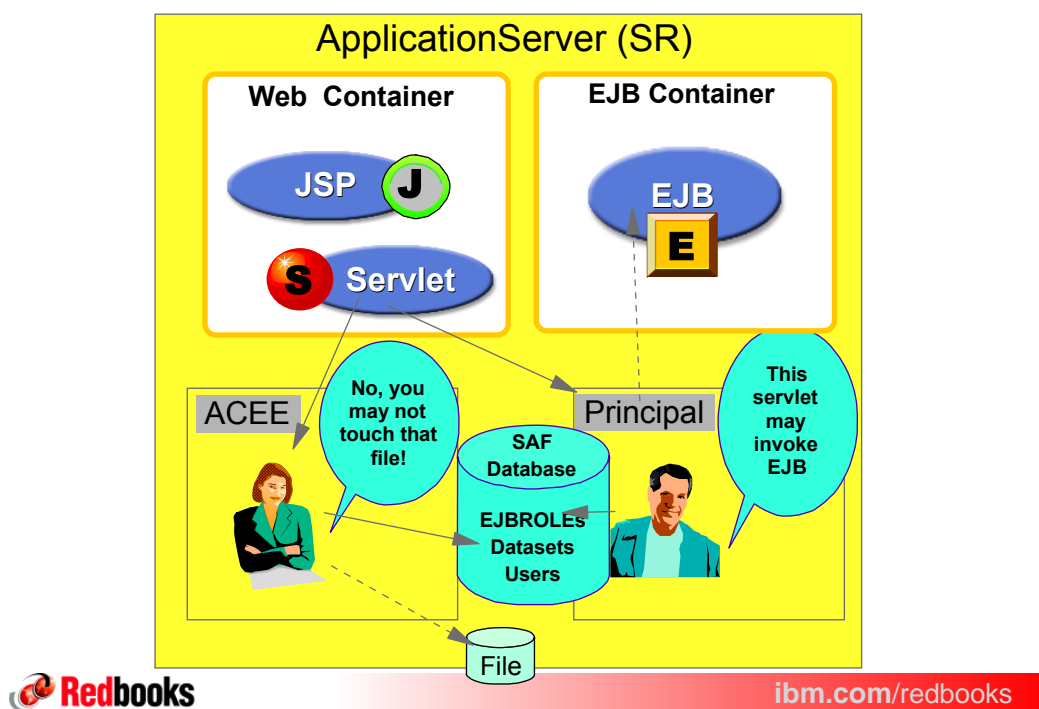
environment element



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

schizophrenic



First monster is tamed Synch to OS Thread allowed

- Synch-to-OS-thread
 - ▶ JDBC connectors only
 - ▶ Sets the OS task (thread) ACEE to the J2EE RunAs identity (stored in the RACO)
- No longer supported for applications



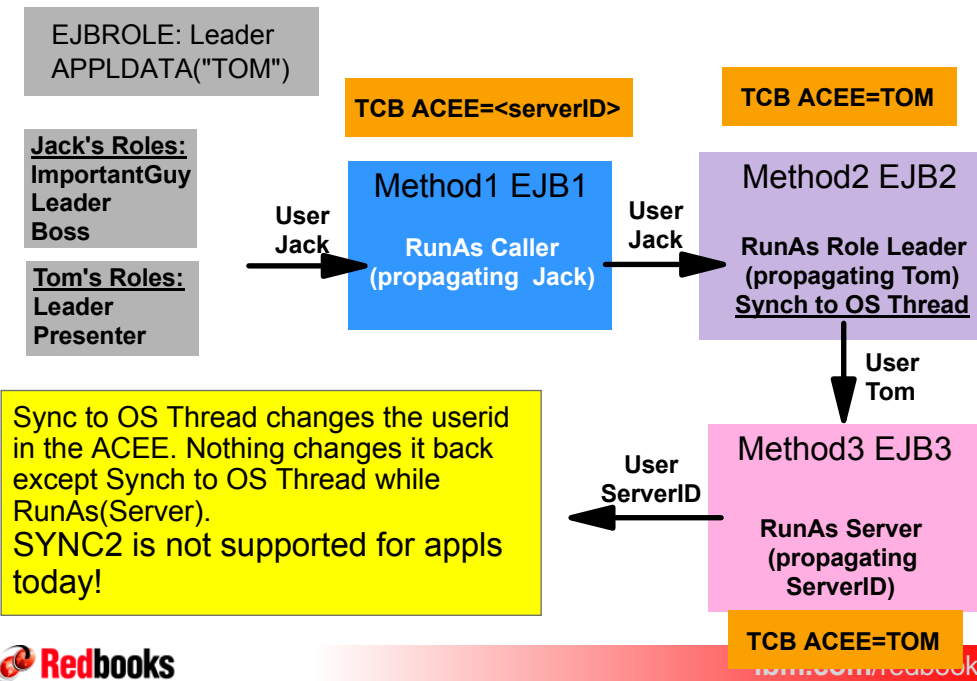
Global Security >

z/OS Global Security Options

This panel specifies z/OS Global Security Options. [1]

Configuration	
General Properties	
Remote Identity	WASDFTU
Local Identity	WASDFTU
Synch to OS Thread Allowed	<input checked="" type="checkbox"/>
Apply OK Reset Cancel	

RunAs and Synch to OS Thread



RunAs role with a local registry

[Local OS User Registry >](#)

Custom Properties

Specifies arbitrary name/value pairs of data, where the name is a property configuration properties: [\[1\]](#)

Total: 3

☐ Filter

☐ Preferences

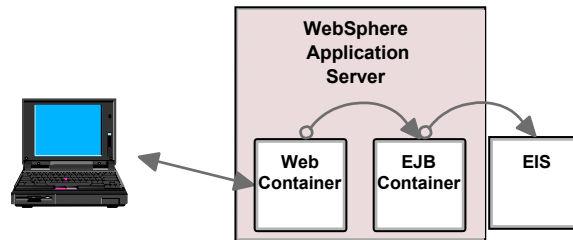
<input type="checkbox"/> Name	<input type="checkbox"/> Value
<input type="checkbox"/> com.ibm.security.SAF.authorization	true
<input type="checkbox"/> com.ibm.security.SAF.delegation	true
<input type="checkbox"/> com.ibm.security.SAF.unauthenticated	WSQUEST

recap:

- ▶ users are mapped to roles in the deployment descriptor or
- ▶ in the GEJBROLE profile
- ▶ if you RunAs role, the role needs to be mapped back to an identity with is available in the configured registry

the appldata field in the (G)EJBROLE profile does this mapping
(unless SAF.delegation is set to false)

Identity Propagation Local OS



- Identities are propagated forward to EJB container and the EIS subsystem



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Special subjects

WebSphere Application Server for z/OS Version 5 SAF authorization does not support authorization subjects such as Everyone and AllAuthenticate

Bypass: by giving UACC READ to an EJBROLE profile and having the assigned RunAs userid set to RESTRICTED



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

auditing

- ▶ information can be written to SMF 80 (SAF audit records)
- ▶ information to audit:
 - ▶ failed logins
 - ▶ sensitive users (*ALTUSER TARZAN UAUDIT*)
 - ▶ connections made to your server (default failures for CBIND)
 - ▶ authorizations by EJBROLES
 - ▶ you would need to: *RALTER EJBROLE <role_name> AUDIT(ALL)*
 - ▶ you should: *SEARCH CLASS(EJBROLE) CLIST('RALTER EJBROLE ' ' AUDIT(ALL)')*
 - ▶ and execute the CLIST: *EXEC EXEC.RACF.CLIST*
- ▶ x.500 field in SMF 80



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

SMF unload

```
//MARNELAD JOB
(POK,999),'uuuh',CLASS=A,REGION=0M,NOTIFY=&SYSUID
//SMFDUMP EXEC PGM=IFASMFDP
//SYSPRINT DD SYSOUT=*
//ADUPRINT DD SYSOUT=*
//SMFDATA DD DISP=SHR,DSN=SYS1.SC59.MAND
//OUTDD DD DISP=OLD,DSN=MARNEL.SC59.IRRADU00
//SYSUDUMP DD SYSOUT=*
//SMFOUT DD
DISP=(NEW,CATLG,DELETE),DSN=MARNEL.SC59.SMFDATA,
//
SPACE=(CYL,(10,2,0)),DCB=(LRECL=32760,BLKSIZE=0,RECFM=VB),
//
UNIT=SYSALLDA
//SYSIN DD *
INDD(SMFDATA,OPTIONS(DUMP))
OUTDD(SMFOUT,TYPE(080:080))
USER2(IRRADU00) USER3(IRRADU86)
/*
```



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

```
//RACFICE EXEC PGM=ICETOOL,PARM='MSGPRT=ALL'
//TOOLMSG DD SYSOUT=*
//PRINT DD SYSOUT=*
//DFSMSG DD SYSOUT=*
//ADUDATA DD DISP=SHR,DSN=MARNEL.TEMP.IRRADU00
//TEMP0001 DD DISP=(NEW,DELETE,DELETE),SPACE=(CYL,(20,5,0)),UNIT=SYSALLDA
//TOOLIN DD *
SORT FROM(ADUDATA) TO(TEMP0001) USING(EJBR)
DISPLAY FROM(TEMP0001) LIST(PRINT) -
PAGE -
TITLE('EJBR: USE OF EJBROLES') -
DATE(YMD/) -
TIME(12:) -
BLANK -
ON(14,8,CH) HEADER('Qualifier') -
ON(32,10,CH) HEADER('Date') -
ON(23,8,CH) HEADER('Time') -
ON(184,8,CH) HEADER('Jobname') -
ON(286,30,CH) HEADER('Role')
/*
//EJBRCNTL DD *
SORT FIELDS=(10,08,CH,A)
INCLUDE COND=(5,8,CH,EQ,C'ACCESS',AND,
578,8,CH,EQ,C'EJBROLE')
OPTION VLSHRT
```

authorization report



- 1 -	EJBR: USE OF EJBROLES	03/07/30	02:49:02 pm	
Qualifier	Date	Time	Jobname	Role
SUCCESS	2003-07-30	12:45:32	WASD5S	administrator
SUCCESS	2003-07-30	12:45:35	WASD5S	administrator
SUCCESS	2003-07-30	12:45:37	WASD5	monitor
SUCCESS	2003-07-30	12:45:37	WASD5	monitor
SUCCESS	2003-07-30	12:45:37	WASD5	monitor

user to role, counter good for accounting?

```
//TOOLIN DD *
OCCURS FROM(TEMP0001) LIST(PRINT) -
PAGE -
TITLE('Role Access Count') -
DATE(YMD/) -
TIME(12:) -
BLANK -
ON(63,8,CH) HEADER('User ID ') -
ON(286,30,CH) HEADER('Role ') -
ON(VALCNT) HEADER('Number of Access')
//EJBRCNTL DD *
SORT FIELDS=(10,08,CH,A)
INCLUDE COND=(5,8,CH,EQ,C'ACCESS',AND,
578,8,CH,EQ,C'EJBROLE ')
OPTION VLSHRT
```

- 1 -	Role Access Count	03/08/13	01:09
User ID	Role	Number of Access	
MARELI	administrator	677	
MARELI	monitor	1806	
MARELI	operator	18	
MARELI	Employee	1	
SEC2	Employee	17	



authentication x.500 field

WebSphere uses the X500NAME audit field to contain information about the authentication mechanisms used by the user. The RACF type 80 records contain this X500NAME information in the X500_ISSUER and X500_SUBJECT fields. The values that these fields may contain are:

Authentication Mechanism\$	Service\$ (X500_ISSUER)\$	Authenticated (X500_SUBJECT)\$
Custom Registry\$	WebSphere Custom Registry \$	Custom registry principal name\$
Kerberos\$	WebSphere Kerberos\$	Kerberos principal name\$
RunAs Rolename\$	WebSphere role name\$	Role name\$
RunAs Server\$	WebSphere Server Credential\$	MVS user ID\$
RunAs User ID with no password\$	WebSphere Authorized Login\$	MVS user ID\$
RunAs User ID / Password\$	WebSphere Userid/Password\$	MVS user ID\$
RunAs Unauthenticated User\$	WebSphere Unauthenticated User\$	UNAUTHENTICATED\$



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

authc/authz report

```

DISPLAY FROM(TEMP0001) LIST(PRINT) -
PAGE -
TITLE('EJBR: USE OF EJBROLES') -
DATE(YMD/) -
TIME(12:) -
BLANK -
ON(14,8,CH)    HEADER('Qualifier') -
ON(32,10,CH)   HEADER('Date') -
ON(23,8,CH)    HEADER('Time') -
ON(63,8,CH)    HEADER('User ID') -
ON(1597,16,CH) HEADER('X500 Subject') -
ON(1853,20,CH) HEADER('X500 Issuer ') -
ON(286,30,CH)  HEADER('Role')
//EJBRCTL DD *
SORT  FIELDS=(10,08,CH,A)
INCLUDE COND=(5,8,CH,EQ,C'ACCESS',AND,
              578,8,CH,EQ,C'EJBROLE ')
OPTION VLSHRT

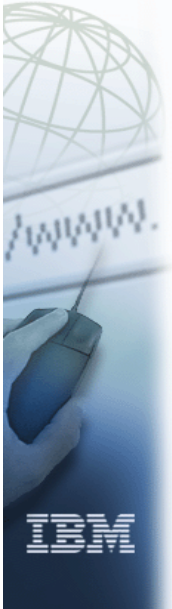
```

Qualifier	Date	Time	User ID	X500 Subject	X500 Issuer	Role
INSAUTH	2003-08-13	09:50:01	MARELI	MARELI	WebSphere Userid/Password	CICSServletManager
INSAUTH	2003-08-13	09:50:25	SEC2	SEC2	WebSphere Userid/Password	CICSServletManager
INSAUTH	2003-08-13	13:48:33	WASDFTU	UNAUTHENTICATED	WebSphere Unauthenticated User	administrator
INSAUTH	2003-08-13	14:01:35	MARNEL	MARNEL	WebSphere Userid/Password	CEO
INSAUTH	2003-08-13	14:31:19	TAI	TAI	WebSphere Authorized Login	monitor
SUCCESS	2003-08-13	13:58:05	MARELI	MARELI	WebSphere Authorized Login	operator
SUCCESS	2003-08-13	14:11:24	WDS2STU	WDS2STU	WebSphere Server Credential	operator

ibm.com



e-business



Trust Association



© Copyright IBM Corp. 2003. All rights reserved.

Trust Association Interceptor

- ▶ A plug point in the authentication flow where one can insert their own code to achieve whatever authentication outcome they desire.
- ▶ Authentication takes place in a front-end authentication server (typically a reverse proxy)
- ▶ WebSphere accepts and acts on this authentication process, rather than driving its own authentication process
- ▶ TAI is a Java class that implements the interface called TrustAssociationInterceptor
- ▶ Trust needs to be established
- ▶ Can be selective, its not all an all or nothing approach
- ▶ It is powerful (and dangerous if you do not know what you are doing)



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Why should you use TAI?

TAI itself allows your infrastructure to offload only the authentication process to an front-end authentication server. TAI will work together with any registry you select, remote or local! It might be the right option if you:

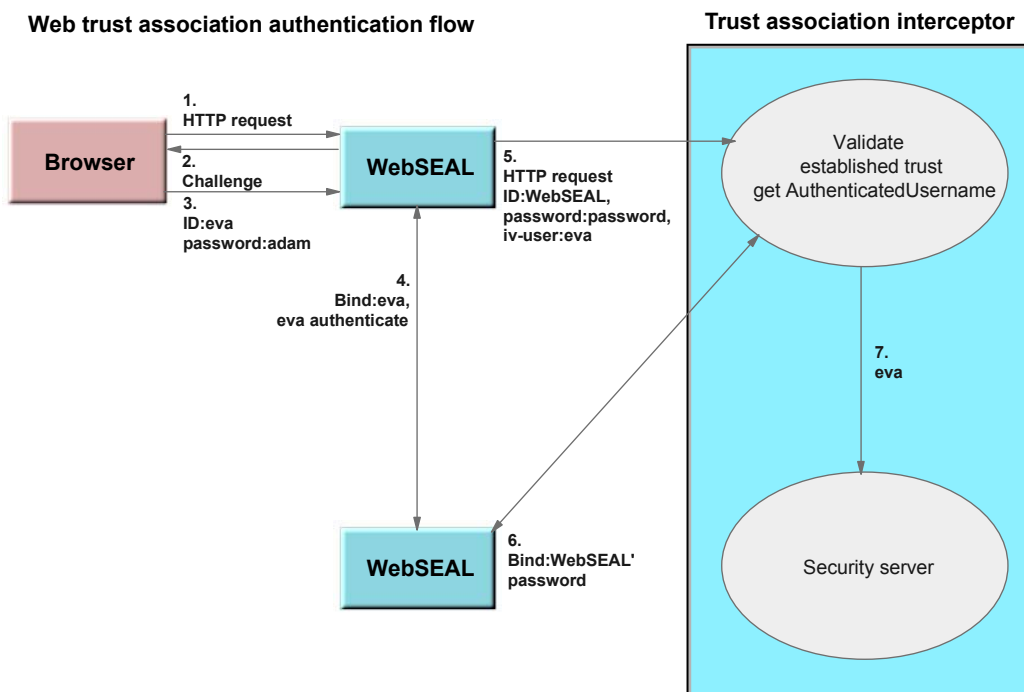
- ▶ Authenticate in the DMZ and can build trust between WebSphere and the authenticating Server
- ▶ Your authentication server shares the same user registry as your WebSphere Application Server Cell (not required)
- ▶ In Tivoli Access Manager for e-Business scenarios
- ▶ You need to Integrate with other registry solutions



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

TAI and an authentication server



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Where can you get a TAI?

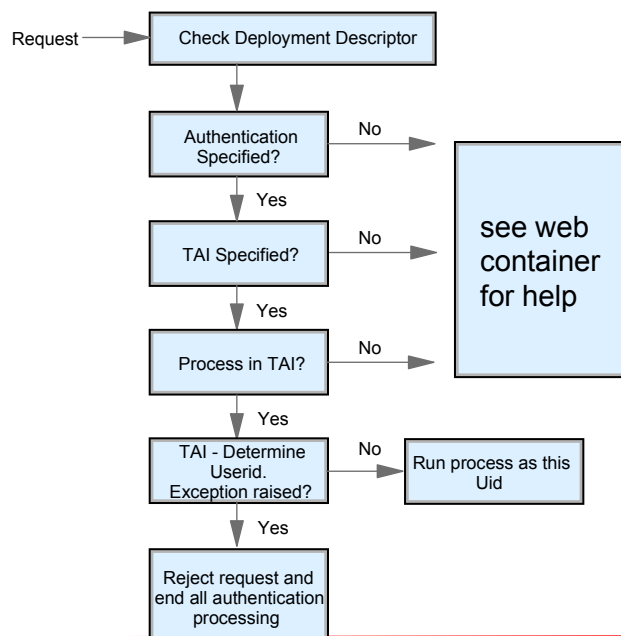
- Write it yourself in Java (using WSAD)
 - ▶ See TrustAssociationInterceptor class contained in the Java package com.ibm.websphere.security
- A TAI may be provided by a third-party product that is performing authentication
- Might be a combination of these two
- Use one of the samples created for the Redbook
 - ▶ See ftp site for Redbook SG24-6846
<ftp://www.redbooks.ibm.com/redbooks/SG246846/pokltsoTai1.jar>, [pokltso2.jar](ftp://www.redbooks.ibm.com/redbooks/SG246846/pokltso2.jar), [pokltso3.jar](ftp://www.redbooks.ibm.com/redbooks/SG246846/pokltso3.jar)



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

external TAI flow



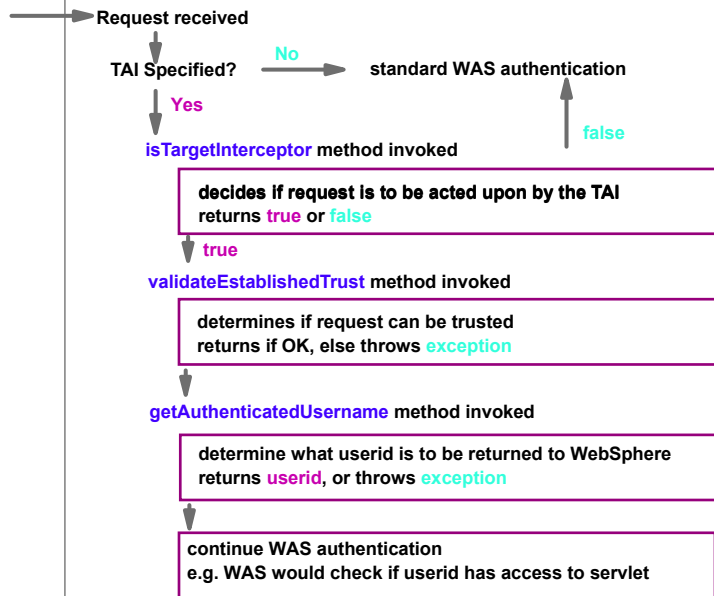
ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

internal TAI flow

WebSphere - Web Container

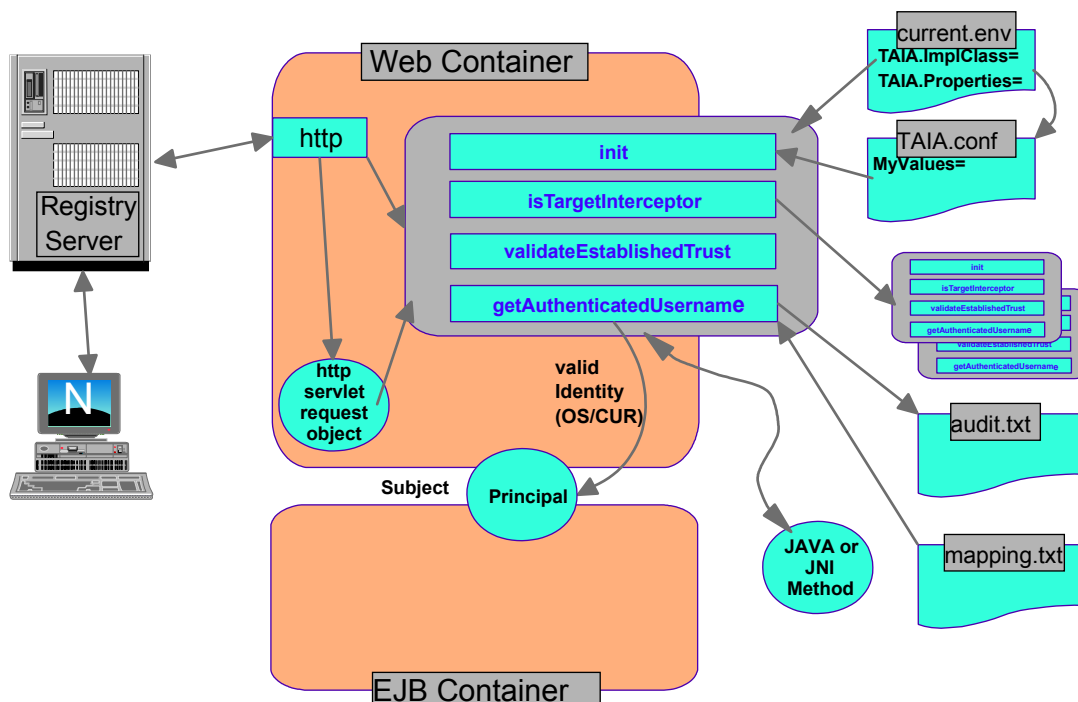
```
com.ibm.ws.security.web.WebSealTrustAssociationInterceptor
```



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

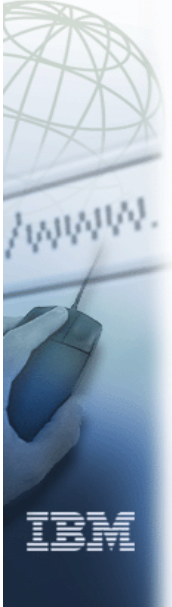
TAI Complete Picture



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

ibm.com

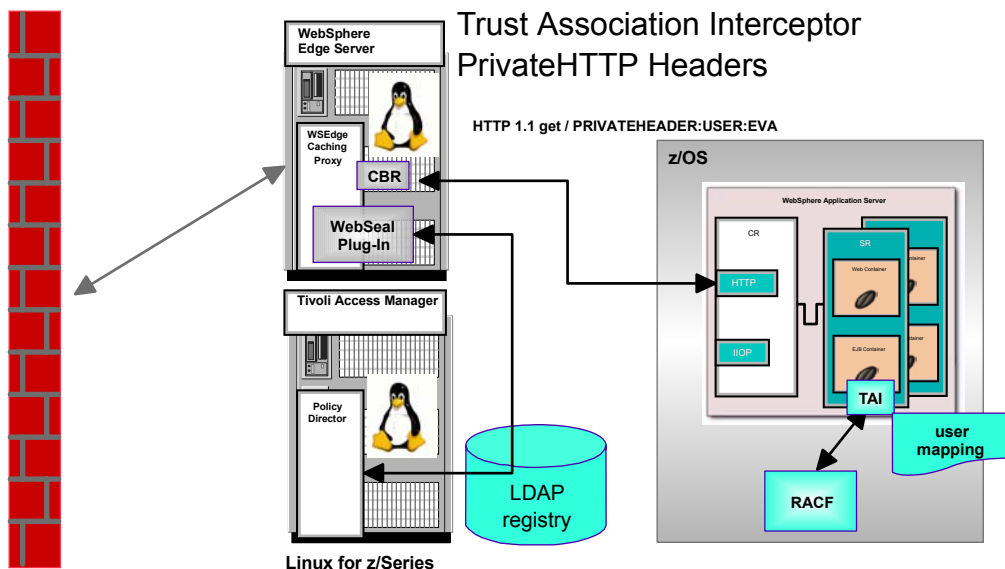


LDAP Native Authentication & Tivoli Access Manager for e-Business WebSEAL



© Copyright IBM Corp. 2003. All rights reserved.

Trust Association Interceptor Using any remote user registry



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Using z/OS LDAP and Native Authentication

When would you choose this scenario?

- you have a pre-existing LDAP server
- you have the need for a central user registry (single sign on)
- you want the ability to reuse RACF userids/pwds
- you are looking to front end WAS/390 with a security product like TAM

Sample User:

```
cn=secl, o=itso
objectclass=top
objectclass=person
objectclass=organizationalPerson
objectclass=ibm-nativeAuthentication
cn=secl
sn=User
```

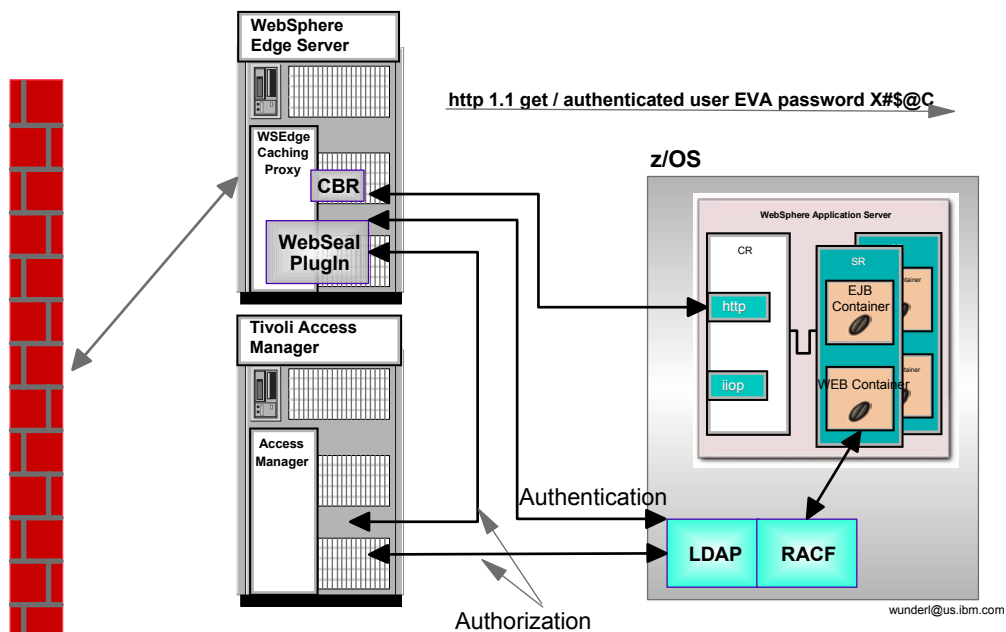
Note that no user password is stored for RACF users



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

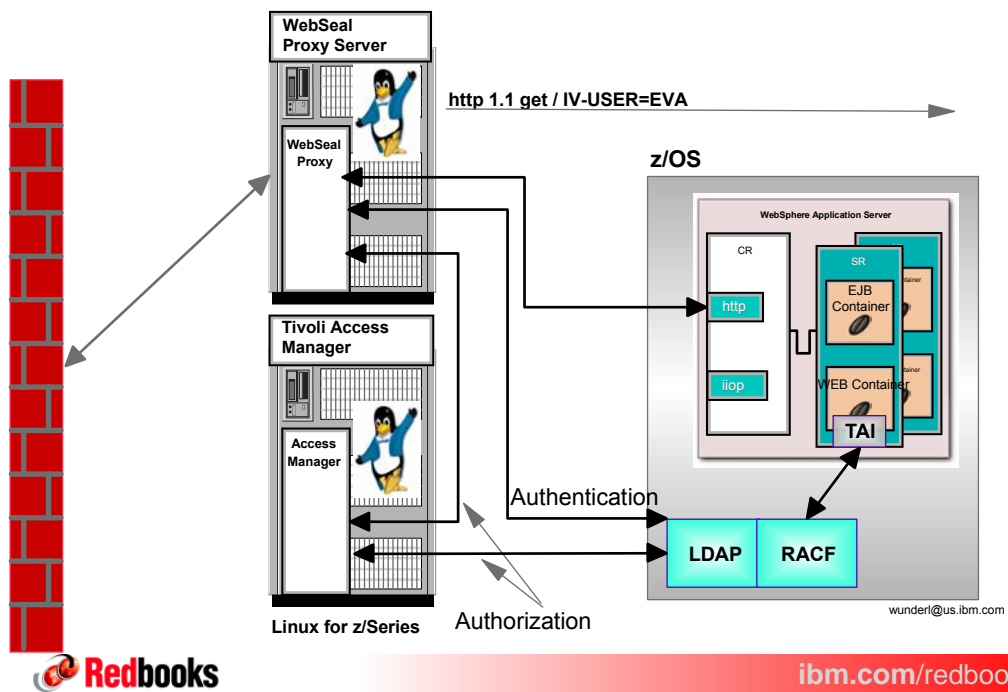
WebSeal Plugin Scenario with LNA exported local registry



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

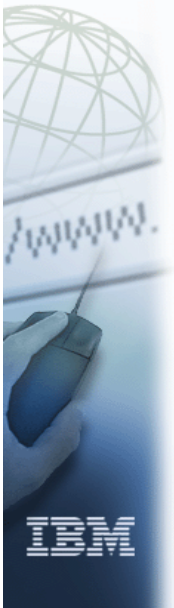
WebSeal Proxy and TAI Scenario



ibm.com



Remote Registries & Cross Platform Security



© Copyright IBM Corp. 2003. All rights reserved.

Why use a Remote Registry?

► Remote registries can offer the following benefits...

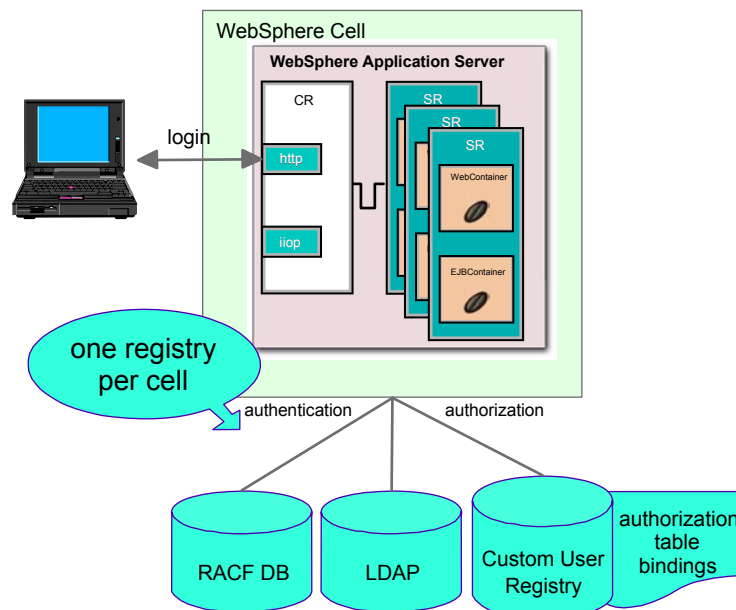
- Single Sign On Solutions
 - one userid to maintain across multiple environments through LDAP or CUR
- Custom User Registries allows you to delegate the declarative and programmatic security requirements to a remote enterprise security registry. Thus, it allows WebSphere Application server to integrate seamlessly into almost any security infrastructure
- If you want to leverage a non local registry for your non-local (internet) clients
- By providing the APIs, IBM allows you to develop a security solution that fits exactly to your needs
- By providing this pluggable interface, IBM allows other vendors to enable their security solutions for WebSphere
- Identity Mapping Capabilities
 - Using IDI to map one user to the equivalent user behind the scenes



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

again: freedom of choice



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Custom User Registry in z/OS

- ▶ Allows authentication against a remote registry from the WebContainer
- ▶ Authentication takes place in the WebContainer only
- ▶ Authorization table is used for access checks
- ▶ Derived USERID is not RACF and cannot be checked against EJBROLES
- ▶ Do not allow IIOP clients to connect to an CUR secured J2EE server.
 - To avoid remote IIOP clients to access an CUR controlled J2EE server set RACF class CBIND CB.BIND.servername and CB.servername to UACC(NONE)
- ▶ The CUR userid does not get propagated nicely into the EJB container or JCA connector. The principal is actually the serverid, so the authorization table needs to be modified accordingly.

Remember: Even if you configure IBM WebSphere Application Server for z/OS to operate with a remote registry, it will still use the System Authorization Facility (SAF) to secure its own runtime, and its accesses to operating system resources.



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

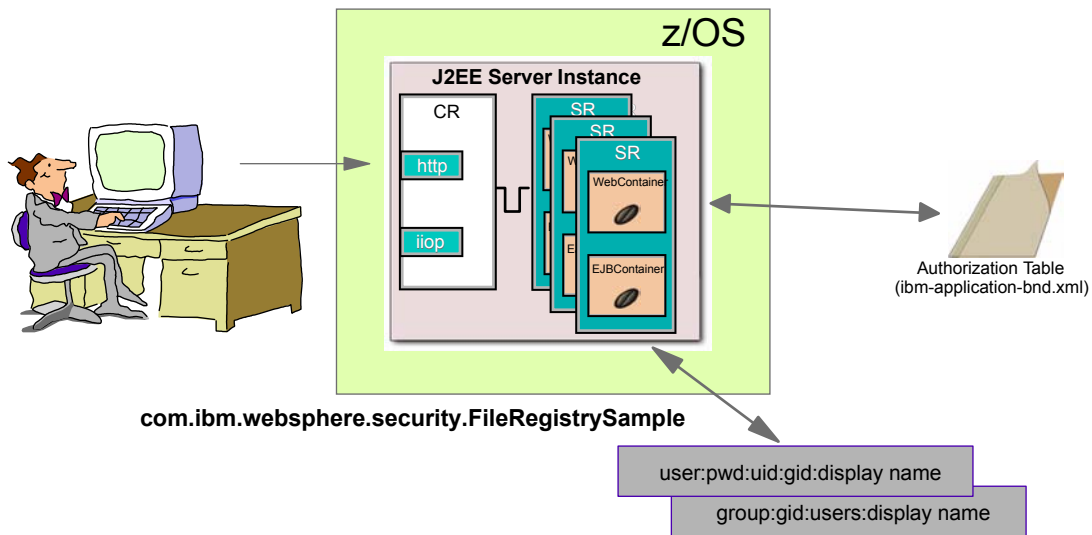
CUR implementation

- file based implementation
 - user and group files are created and stored in the HFS to be used by WAS
 - file must be updated manually
- Remote datasource
 - TCP/IP enabled registry (TAM, LDAP...)
 - DB2 (or other brands) databases can be configured to provide userid/pwd and group information to WebSphere



ibm.com/redbooks

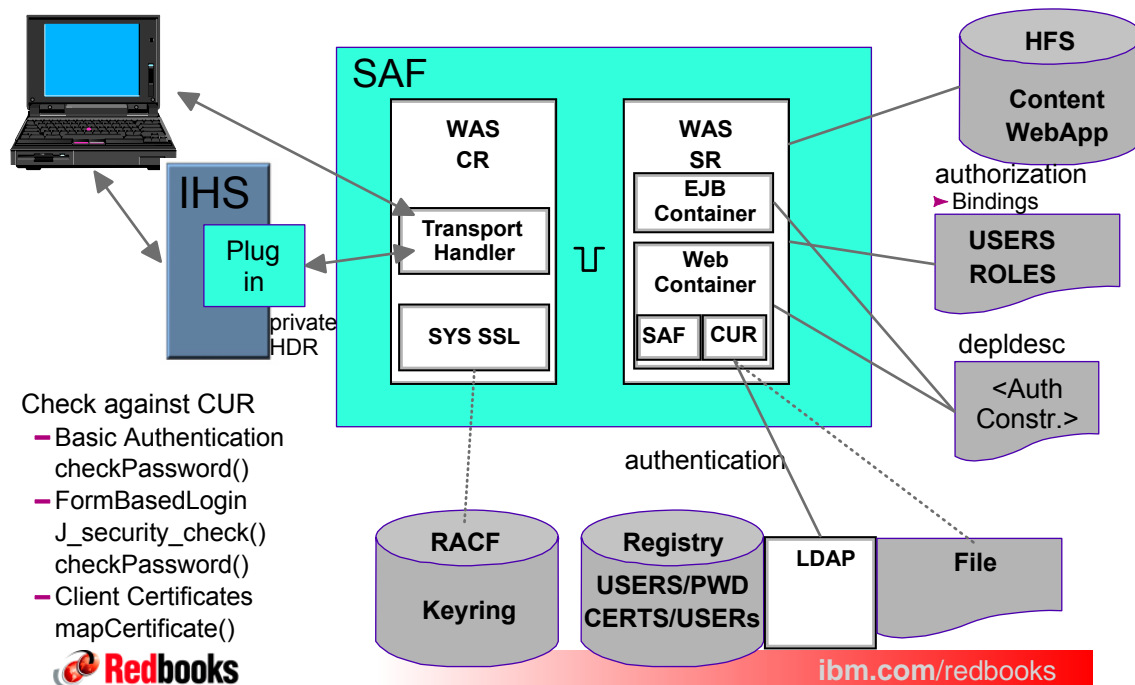
© Copyright IBM Corp. 2003. All rights reserved.



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Custom User Registry Overview



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

CUR user to role mapping

The admin interface looks up the CUR to allow you selecting users for the mapping

Lookup users/groups

Lookup user and/or groups

The following roles will be mapped to the items in the selected list.

Worker

To search for users/groups, type in a limit (number) and a search pattern and click the "Search" button (e.g. a*):

limit (number of items) 20

Search String * Search

Select users/groups below in the "Available" list. Move them to the "Selected" list by clicking on the >> button

Available:

- Holger
- Eva
- server
- WSADMIN

Selected:

- Holger
- Eva

/WebSphere/BS0F/appserver/config/cells/cdfsc59/applications/SWIPEV5.ear/deployments/SWIPEV5/META-INF/:

ibm-application-bnd.xml

```
<authorizations xmi:id="RoleAssignment_4">
  <users xmi:id="User_3" name="Holger"/>
  <users xmi:id="User_4" name="Eva"/>
  ....
```



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

RunAs role to user mapping

[Enterprise Applications](#) > [SWIPEV5](#) >

Mapping RunAs Roles to Users

Map RunAs roles to users

The Enterprise beans you are installing contain predefined RunAs roles. RunAs roles are particular role to be recognized while interacting with another Enterprise bean.

username: WSADMIN

password: *****

Apply

Remove the RunAsUser user name and password from the selected roles.

Remove

Role	User Name
<input type="checkbox"/> CEO	
<input checked="" type="checkbox"/> Manager	

OK Cancel

recap:

- ▶ users are mapped to roles in the deployment descriptor or
- ▶ if you RunAs role, the role needs to be mapped back to an identity with is available in the configured registry

this is done in ibm-application-bnd.xml:

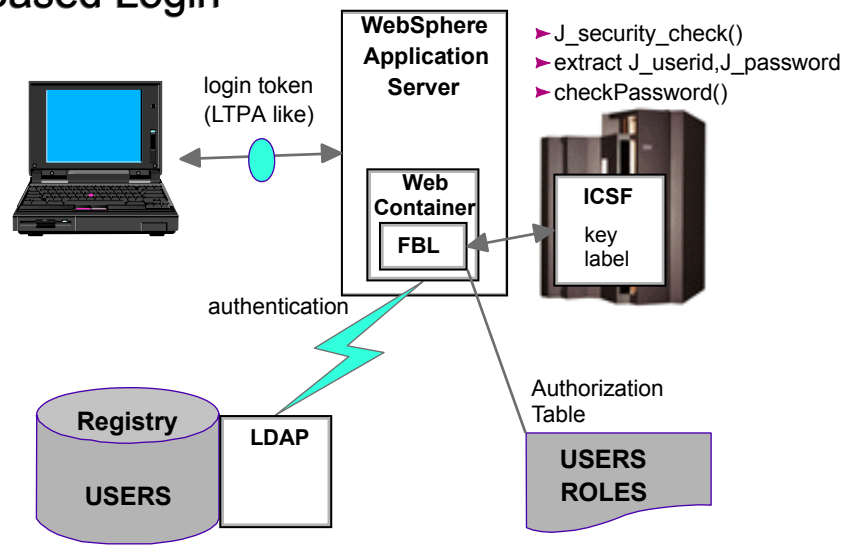
```
<runAsMap >
  <runAsBindings xmi:id="RunAsBinding_2">
    <authData xmi:type="commonbnd:BasicAuthData" xmi:id="BasicAuthData_2"  userId="WSADMIN"
    password="{xor}NzAzPCot"/>
    <securityRole href="META-INF/application.xml#SecurityRole_1"/>
  </runAsBindings>
```



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Custom User Registry Form Based Login



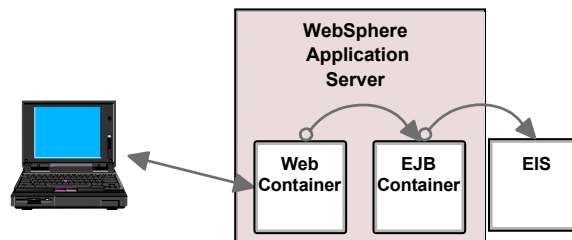
- ▶ Independent from local registry (RACF)
- ▶ RACF userid not available!



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Identity Propagation CUR



- ▶ WebContainer authenticates and sets current userid (principal) to remote userid (not RACF)
- ▶ Collocated EJBs use CUR identity (RunAs caller propagation), therefore the EJB container need to access the authorization table.
- ▶ Remote EJBs get either
 - ▶ servers USERID propagated
 - ▶ or the USERID defined in WebAuth.CustomRegistry.SAFPrincipal=
- ▶ JCA security is defined by res-auth and the RunAs mode of the calling EJB. RunAs Caller/res-auth container in an collocated environment would propagate an invalid USERID. In consequence only res-auth application/servlet is supported



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

auditing

- ▶ authorization is not under control of CUR and cannot be logged today
- ▶ for authentication you can build in your own logging procedures like logj or jni calls to SMF(). Also x500 access report carries some info.



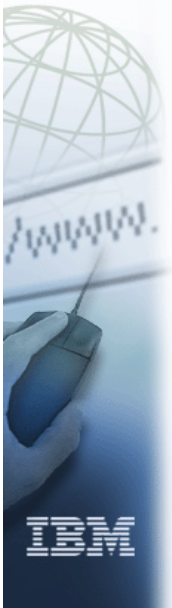
ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

ibm.com



e-business



Tivoli Access Manager for e-Business integration



Redbooks

International Technical Support Organization

© Copyright IBM Corp. 2003. All rights reserved.

Product Overview

Tivoli Access Manager for e-Business

- WebSeal Plug-in
- Caching Proxy Plug-in
- Policy Server / Authorization Server
- PD Authorization Services for z/OS
- AMWAS/PDWAS WebSphere Plug-in

Tivoli Directory Server

- LDAP Server



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Front Ending WAS with TAM

Why would you want to implement Tivoli Access Manager?

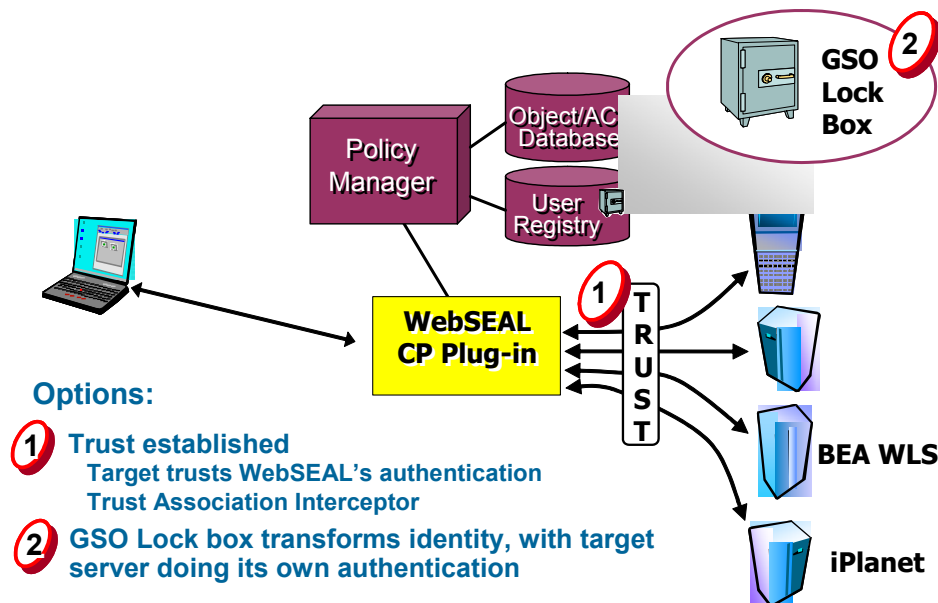
- Global Sign On (GSO) solutions
- Single Sign On (SSO) solutions
- Security management
 - Coarse Grained Authorization
 - protects basic web resources
 - Fine Grained Authorization
 - allows security calls to be made from within an application to protected resources within a web page
 - User/Group Administration
 - immediate administration for adding users and groups to the secure space
- High Availability
 - replicas of various servers are supported
 - WebSEAL can junction to many http ports intelligently
 - uses a "least busy" sorting algorithm
- Centralized user and group management
- Centralized authorization management for J2EE applications



ibm.com/redbooks

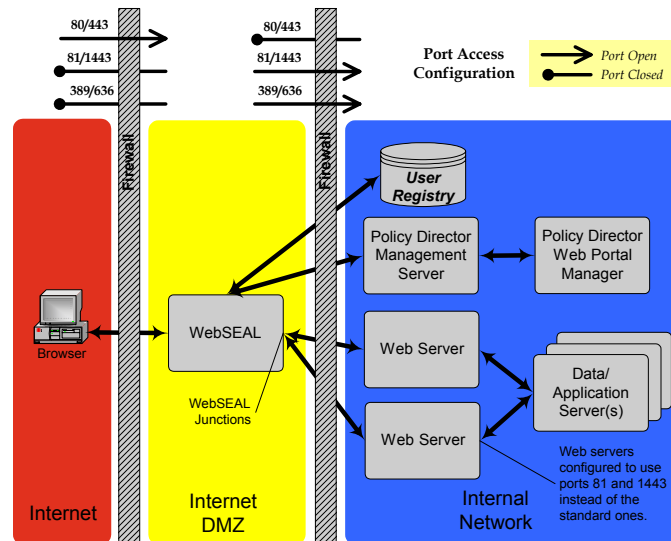
© Copyright IBM Corp. 2003. All rights reserved.

Global Sign On

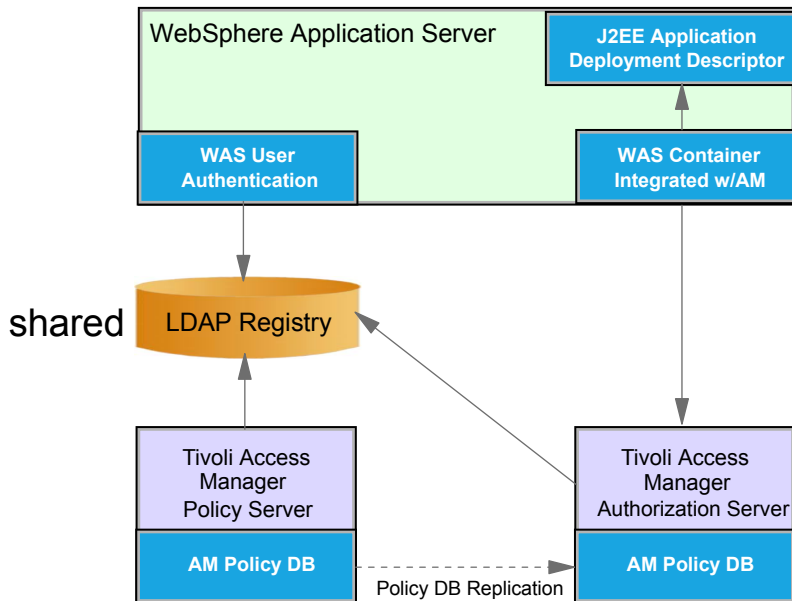


Caching Proxy and WebSeal Plug-in

An Example Policy Director WebSEAL Architecture



Tivoli Access Manager for e-Business AMWAS / PDWAS

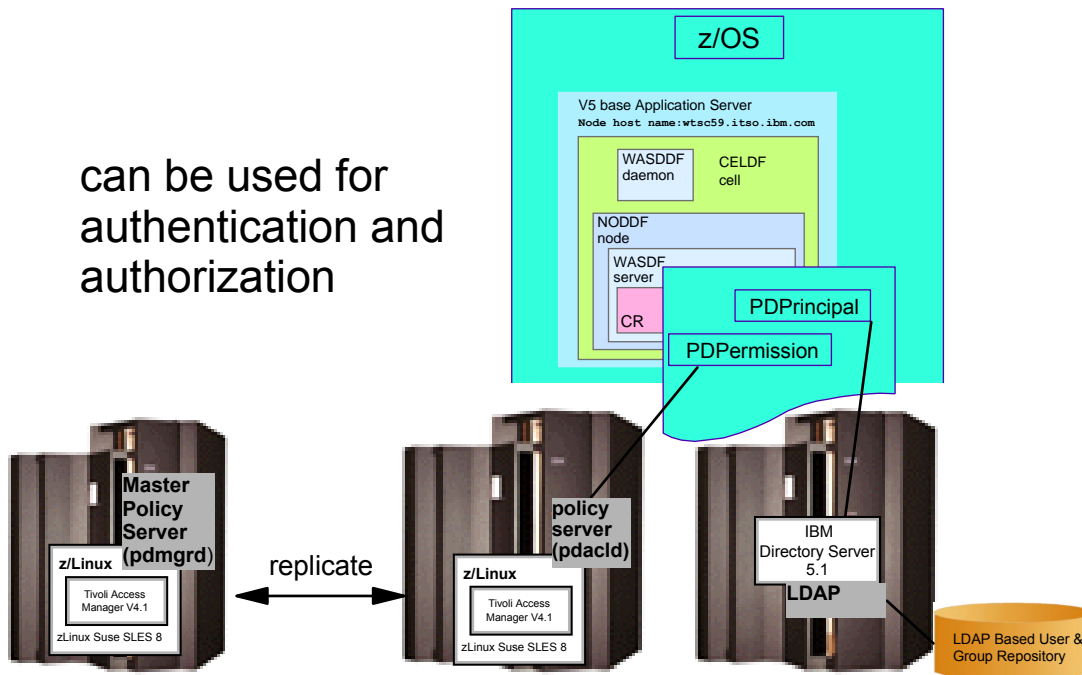


ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Policy Director Authorization Services for z/OS JAVA API

can be used for
authentication and
authorization



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Policy Director Authorization Services for z/OS JAVA API

The TAM Java and Administration APIs at a TAMEb 3.9 and TAMEb 4.1 level are available as a Small Programming Enhancement (SPE) via PTF UA02702(APAR OA02022).

In order to apply the PTF, you must have IBM Policy Director Authorization Services for z/OS and OS/390 installed (5655F95).

Policy Director Authorization Services is available at no charge to customers who have a license for OS/390 V2.10 (5647-A01) or z/OS V1.1 (5694-A01) or later.

If you are only using the Java APIs, you have to install Policy Director Authorization Services, but you don't have to configure it. You would only have to do the necessary configuration for the Java Administration and Authorization APIs after you installed the SPE.



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Policy Director Authorization Services for z/OS JAVA API

The PDLoginModule class manages authentication with Access Manager. Applications can use PDLoginModule to authenticate an Access Manager user, create a corresponding PDPrincipal object, and a PDCredential object containing the user's credentials. The PDPrincipal class implements the java.security.Principal interface.

PDPermission can be used to access Access Manager for authorization decisions. PDPermission can locate the current Subject, extract the authentication information, and contact Access Manager to determine if the Subject has permission to access the resource in the particular way (read, write, invoke, etc.). PDPermission accesses Access Manager's authorization server over SSL. A future version of Access Manager will provide local access. Servlets, EJBs, or utility code can use these classes according to the JAAS standard. However, non-JAAS applications can also use them.

PDPermission's API is quite simple. The constructor takes a target resource name within Access Manager's object space and an Access Manager access mode or set of actions as parameters. The permission is then checked by a Java2 Security Manager, which throws an AccessControlException if the principal is not allowed access to the target resource based on the requested action. Listing 1 is a very simple example



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Summary

Registry configured	Authentication		Authorization	
	Web container	EJB container	Web container	EJB container
Local OS, container	Transport Handler: <ul style="list-style-type: none"> SAF with TAI: <ul style="list-style-type: none"> anywhere Reverse Proxy WebSeal TAM CP plug-in => map to SAF mutual SSL: <ul style="list-style-type: none"> SAF IHS HTTP PI (RACF plex) =>map to SAF USERID (1) <ul style="list-style-type: none"> IHS HTTP PI (in a nonshr registry) =>map to SAF USERID (2)	<ul style="list-style-type: none"> SAF 	<ul style="list-style-type: none"> EJBROLES, GEJBROLES or bindings 	<ul style="list-style-type: none"> EJBROLES, GEJBROLES or bindings
programmatic options with Local OS	<ul style="list-style-type: none"> JAAS against SAF 	<ul style="list-style-type: none"> JAAS against SAF 	<ul style="list-style-type: none"> getUserPrincipal isUserInRole TAM Java API's against remote registry 	<ul style="list-style-type: none"> getCallerPrincipal isCallerInRole TAM Java API's against remote registry



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Registry configured	Authentication		Authorization	
	Web container	EJB container	Web container	EJB container
Custom User Registry & LDAP, container	Transport Handler <ul style="list-style-type: none"> gets resolved in supplied registry (TCP/IP or local file) with TAI: <ul style="list-style-type: none"> anywhere Reverse Proxy WebSeal TAM CP plug-in => map to CUR mutual SSL: <ul style="list-style-type: none"> CUR IHS HTTP PI (same registry than CUR) => map to CUR USER (8) IHS HTTP PI (in a nonshr registry, like the RACFplex) =>map to CUR USERID (9) 	<ul style="list-style-type: none"> not available today, Note: container need to be protected against connecting IIOP clients when running in CUR mode with WAS 5.02 against supplied registry 	<ul style="list-style-type: none"> bindings, checking against CUR/LDAP authenticated user 	<ul style="list-style-type: none"> bindings, checking against SAF server ID with WAS 5.02 checking bindings against CUR/LDAP authenticated user
programmatic options with Custom User Registry & LDAP	<ul style="list-style-type: none"> JAAS against CUR interface (TCP/IP or local file) 	<ul style="list-style-type: none"> JAAS against CUR interface (TCP/IP or local file) 	<ul style="list-style-type: none"> getUserPrincipal isUserInRole TAM Java API's against remote registry 	<ul style="list-style-type: none"> getCallerPrincipal isCallerInRole TAM Java API's against remote registry
AMWAS container (WAS 5.02)	<ul style="list-style-type: none"> Tivoli Access Manager 	<ul style="list-style-type: none"> Tivoli Access Manager 	<ul style="list-style-type: none"> Tivoli Access Manager ACL 	<ul style="list-style-type: none"> Tivoli Access Manager ACL
programmatic options with AMWAS (APAR OA02022)	<ul style="list-style-type: none"> JAAS 	<ul style="list-style-type: none"> JAAS 	<ul style="list-style-type: none"> getUserPrincipal isUserInRole TAM Java API's against remote registry 	<ul style="list-style-type: none"> getUserPrincipal isUserInRole TAM Java API's against remote registry

Footnotes

- (1)After handshake was successful you can be sure that the certificate is already in SAF and can be mapped to an valid identity
- (2)If IHS WebSphere HTTP Plug-in uses a different registry, the certificate that is forwarded to WAS might not be available in the SAF registry. Certificate needs to be mapped to an SAF USERID
- (3)After handshake was successful you can be sure that the certificate is already in CUR and can be mapped to an valid identity
- (4)SSL handshake based on cert which is in RACF, needs to mapped to an non RACF user available in CUR



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Questions?



ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.