ibm.com

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

J2EE server security options

Redbooks

International Technical Support Organization

Holger Wunderlich
wunderl@us.ibm.com

© Copyright IBM Corp. 2003. All rights reserved.

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 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.

© 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:

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.

© Copyright IBM Corp. 2003. All rights reserved.

HTTP Security Options and Configurations

WebSphere AS for z/OS: HTTP and Web container security options

Does your IBM HTTP Server on z/OS deliver the security infrastructure for your Web applications? Do you trust in its wonderful and unique capabilities to deliver thread-level security and SAF integration?

And do you realize, when WebSphere V 5 comes along--that all this will be history?

In WebSphere 5, security for your Web applications is managed within the Web Container of the WebSphere runtime--and WebSphere can manage your security with a wide range of choices! In this session, we explain the security possibilities that are available when your Web applications run in WebSphere 5, and detail how security will be inherited by your EJB Container. We also examine cross-platform security models within this context.

© Copyright IBM Corp. 2003. All rights reserved.

cheat sheet

SSO	Single Sign On
GSO	Global Sign On
LTPA	Light Weight Third Party Authentication
CUR	Custom User Registry
CSIv2	Common Secure Interoperability Version 2
zSAS	z/OS Security Association Service
SAS	Security Association Service (IIOP) Security Attribute Service (CSIv2)
TAI	Trust Association Interceptor
PAM	Pluggable Authentication Module

Authentication Mechanism: SWAM, LTPA, ICSF

Authentication Method: Basic, FBL, SSL...

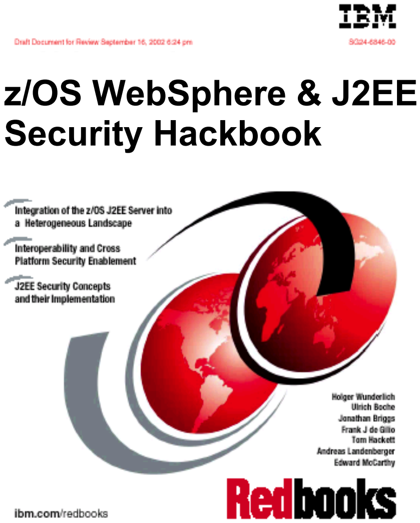
© Copyright IBM Corp. 2003. All rights reserved.

Objectives

- A Brief History of Web(Sphere) Security
- Web Container Authentication Concepts
  - ROLES
  - Runas, ThreadID, resauth
  - Subjects and Principals
- Web Container Authentication Models
  - basic, form-based, client certificates, TAI & CUR

© Copyright IBM Corp. 2003. All rights reserved.

Based on: z/OS WebSphere and J2EE Security Handbook, SG24-6847/6086



Draft Document for Review September 16, 2002 6:24 pm

IBM

SG24-6846-00

z/OS WebSphere & J2EE Security Hackbook

- Integration of the z/OS J2EE Server into a Heterogeneous Landscape
- Interoperability and Cross Platform Security Enablement
- J2EE Security Concepts and their Implementation

Holger Wunderlich
Ulrich Boche
Jonathan Briggs
Frank J de Gilio
Tom Hackett
Andreas Landenberger
Edward McCarthy

Redbooks

ibm.com/redbooks

What do you think of when someone mentions z/OS security? Probably of something that is trustworthy, or even impenetrable. Perhaps you also think of something that is a little complex and challenging to administer.

What comes to mind when someone mentions Internet security? Perhaps you think of prominent Web sites that have been "hacked" or credit card numbers that have been stolen.

Using working examples of code and configuration files, in this IBM Redbook we explain how you can run your Web-enabled applications with as high a level of security as other z/OS applications and subsystems--even if those applications were written or originally deployed on another platform--by using the Java TM 2 Platform Enterprise Edition (J2EE) programming model and the IBM WebSphere Application Server for z/OS and OS/390.

This redbook will help application programmers, WebSphere and security administrators, and application and network architects to understand and use these products.

http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg246846.pdf

http://wtscpok.itso.ibm.com/~redpiece/PDF/SG246086.PDF

Redbooks

ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

ibm.com

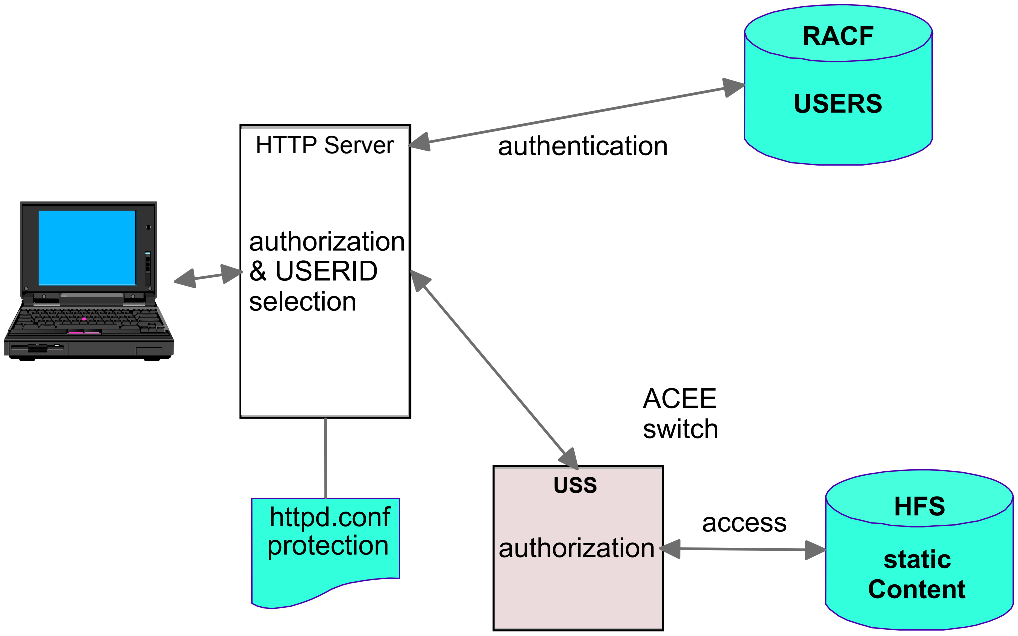
A Brief History of Web(Sphere) Security

Redbooks

International Technical Support Organization

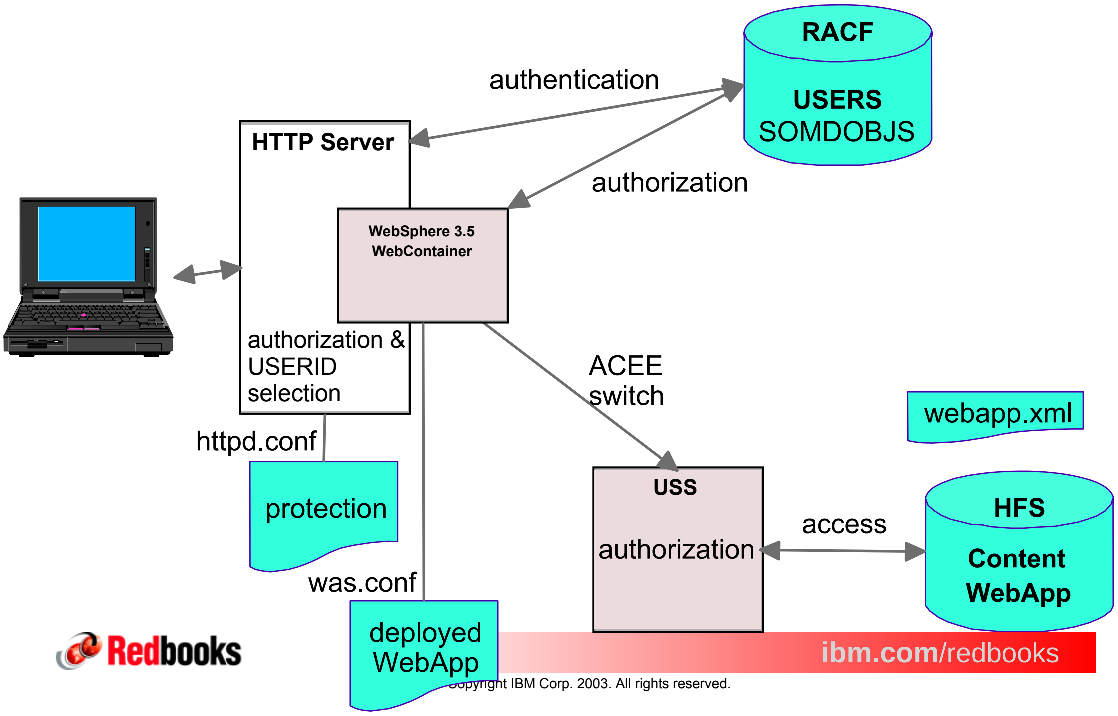
© Copyright IBM Corp. 2003. All rights reserved.

WebServer Security in z/OS



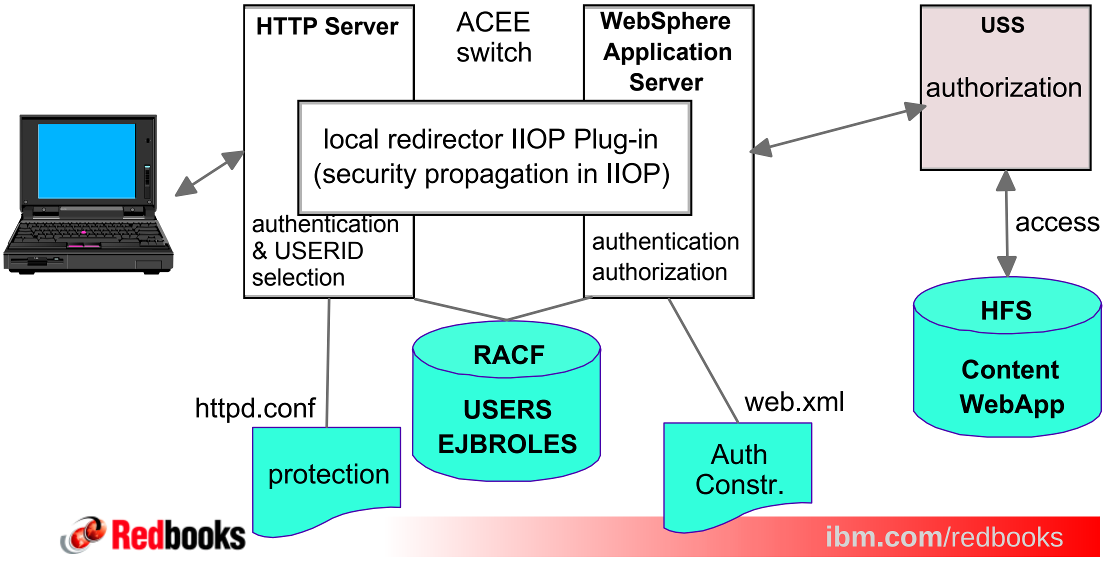
Redbooks
ibm.com/redbooks
© Copyright IBM Corp. 2003. All rights reserved.

WebSphere 3.5 Security



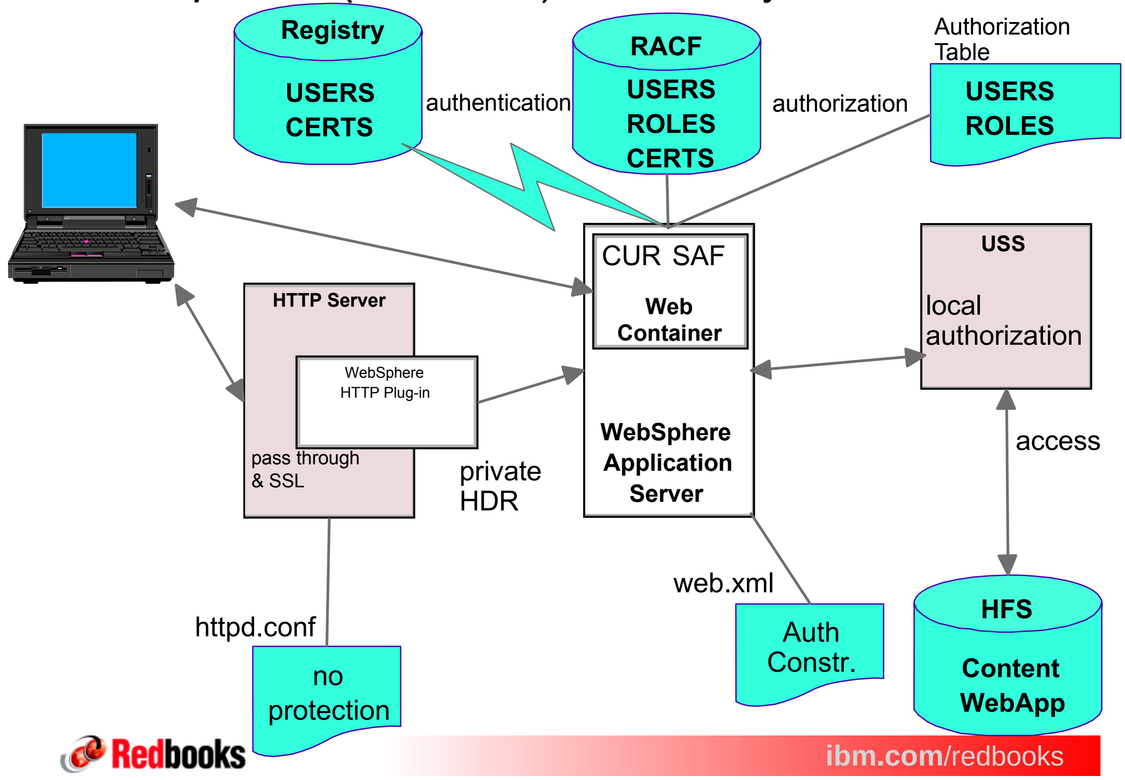
Redbooks
ibm.com/redbooks
© Copyright IBM Corp. 2003. All rights reserved.

WebSphere 4 Security: IIOP Plug-In



© Copyright IBM Corp. 2003. All rights reserved.

WebSphere 4(UQ90049) / 5 Security



© Copyright IBM Corp. 2003. All rights reserved.

ibm.com

WebContainer Security Concepts

Redbooks

International Technical Support Organization

© Copyright IBM Corp. 2003. All rights reserved.

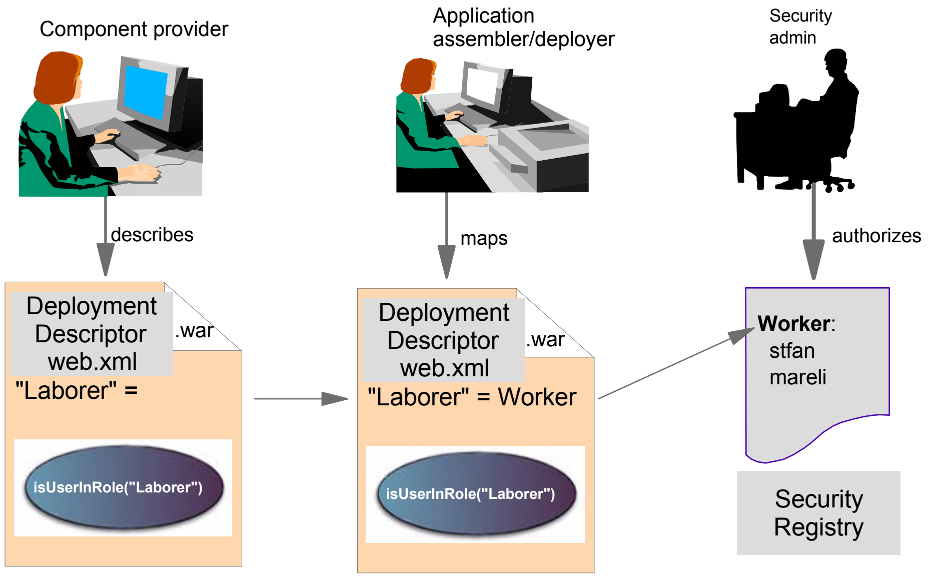
Web Application Authorization

- registry independent:
- Programmatic: javax.servlet.http.HttpServletRequest interfaces
  - Access control within the program, fine grained
  - getUserPrincipal
    - Which identity am I running under?
  - isUserInRole()
    - Is the identity authorized to the role?
- Declarative: Security Constraints in DD (web.xml)
  - Container handles access control, based on method / URL
  - Web Resource Collections
  - Authorization Constraint one or more roles authorized to the urls in the Web Resource Collection
  - User data constraint to enforce SSL for specific URLs

© Copyright IBM Corp. 2003. All rights reserved.

authorization tooling

isUserInRole("Laborer") ?



© Copyright IBM Corp. 2003. All rights reserved.

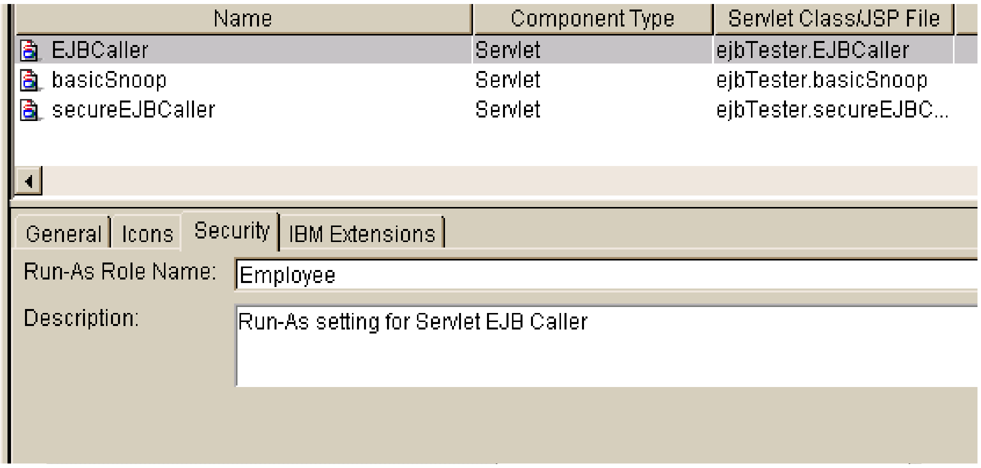
run-as in the WebContainer (V5)

- run-as for the WebContainer was introduced in J2EE 1.3, which is supported in V5.
- The J2EE 1.3 specification is at the component level only
- run-as allows caller (default) or role to be specified
- role needs to be mapped back to an user

© Copyright IBM Corp. 2003. All rights reserved.

Delegation: servlet Run-as

- ➤ Does not change current Principal, only propagation identity.
- ➤ Applies also to unauthenticated requests.
- ➤ No support in WSAD.



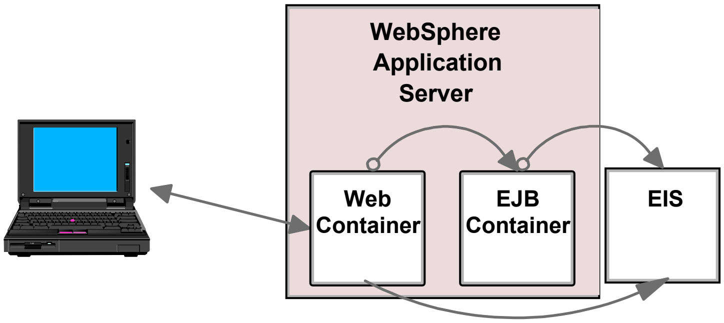
Name	Component Type	Servlet Class/JSP File
EJBCaller	Servlet	ejbTester.EJBCaller
basicSnoop	Servlet	ejbTester.basicSnoop
secureEJBCaller	Servlet	ejbTester.secureEJBC...

Run-As Role Name: Employee

Description: Run-As setting for Servlet EJB Caller

© Copyright IBM Corp. 2003. All rights reserved.

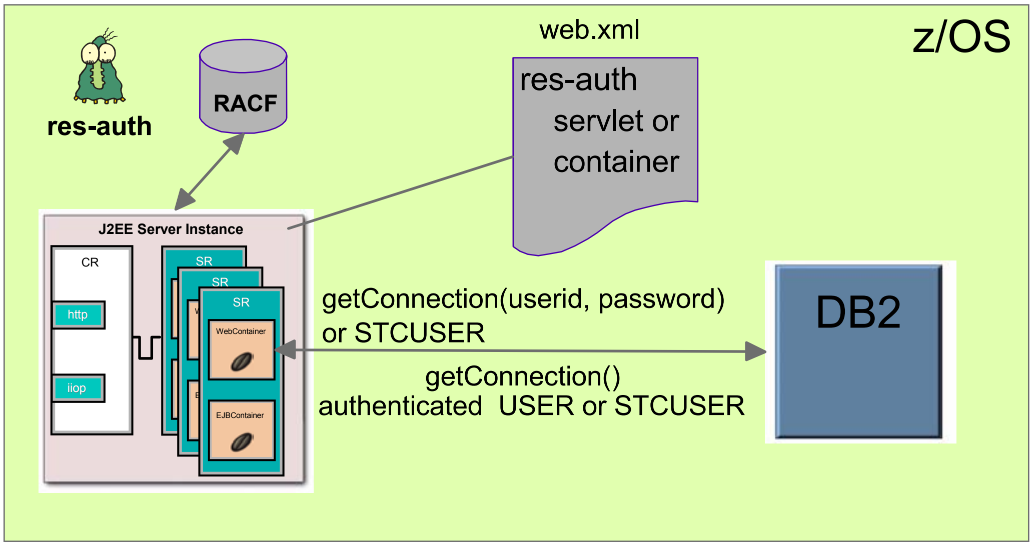
WebSphere WebContainer Identity Propagation



- ➤ Local
  - ➤ WebContainer authenticates
  - ➤ sets current userid (principal)
  - ➤ and propagates run-as id for downstream authorization
- ➤ Custom
  - ➤ WebContainer authenticates
  - ➤ sets current userid (principal)
  - ➤ and propagates server id or
  - ➤ WebAuth.CustomRegistry.SAFPrincipal for downstream authorization

© Copyright IBM Corp. 2003. All rights reserved.

res-auth: JDBC Access from the WebContainer



z/OS

res-auth

RACF

web.xml

res-auth servlet or container

J2EE Server Instance

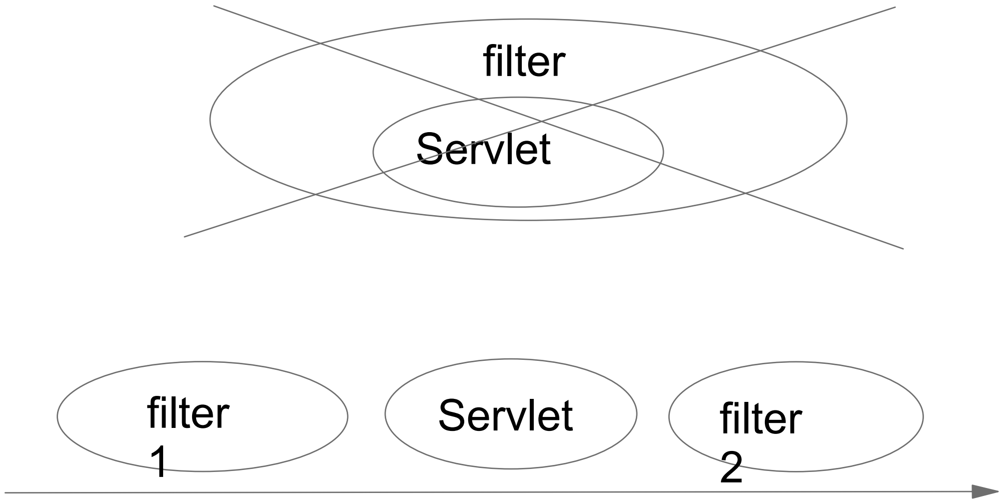
getConnection(userid, password) or STCUSER

getConnection() authenticated USER or STCUSER

DB2

© Copyright IBM Corp. 2003. All rights reserved.

Servlet Filters



Servlet filters can be used for additional authentication or processing. Both form-based login and servlet filters are supported by the Web container. The form-based login servlet performs the authentication and servlet filters perform additional authentication, auditing, or logging information. The servlet filters are invoked either before or after the login actions (CustomLoginServlet)

© Copyright IBM Corp. 2003. All rights reserved.

ibm.com

Authentication

Redbooks

International Technical Support Organization

Holger Wunderlich
wunderl@us.ibm.com

© Copyright IBM Corp. 2003. All rights reserved.

WAS Authentication Mechanisms

SWAM

- non forwardable tokens, no Single SignOn
- not supported with ND
- uses an HTTP session to manage the FB login token

LTPA

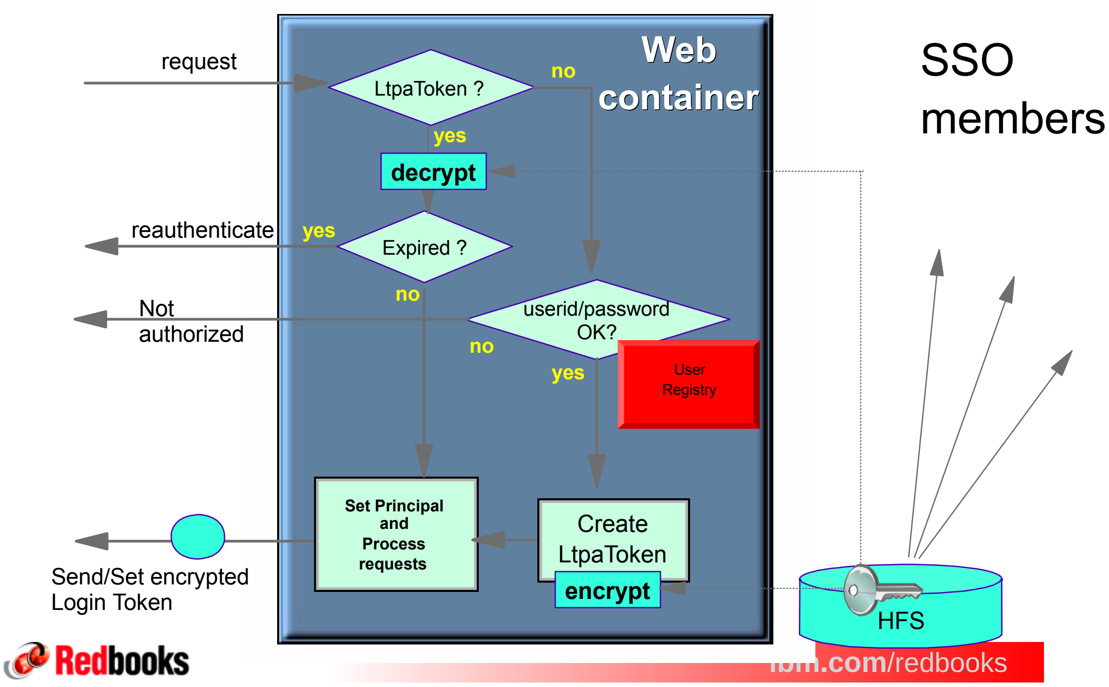
- forwardable token: "LtpaToken" cookie. Possible SSO with DP.
- encrypt the token with JCE keys. Can be exported/imported.

ICSF

- forwardable token: "LtpaToken" cookie. Possible SSO with v4 z/OS
- encrypt the token with ICSF keys.

© Copyright IBM Corp. 2003. All rights reserved.

LTPA
Lightweight Third Party Authentication



request

LtpaToken ?

no

yes

decrypt

Web container

SSO members

reauthenticate

yes

Expired ?

no

Not authorized

userid/password OK?

no

yes

User Registry

Set Principal and Process requests

Create LtpaToken

encrypt

Send/Set encrypted Login Token

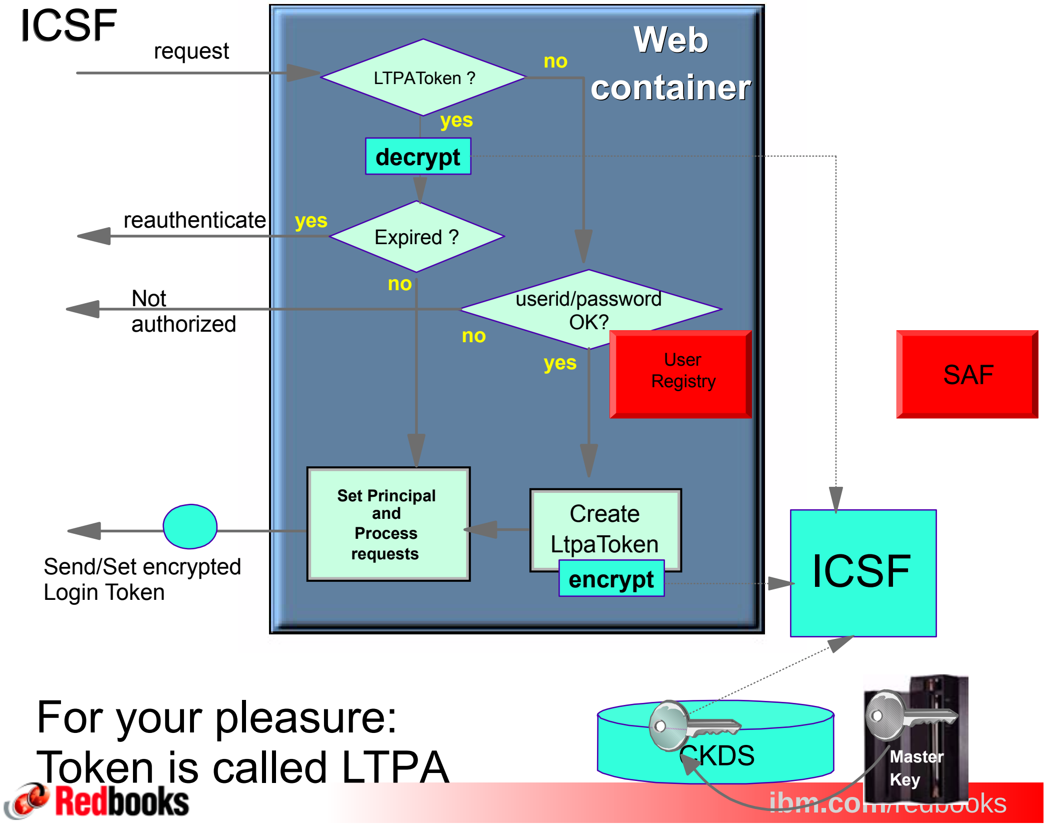
HFS

Redbooks

ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

ICSF



request

LTPAToken ?

no

yes

decrypt

Web container

reauthenticate

yes

Expired ?

no

Not authorized

userid/password OK?

no

yes

User Registry

SAF

Set Principal and Process requests

Create LtpaToken

encrypt

ICSF

Send/Set encrypted Login Token

CKDS

Master Key

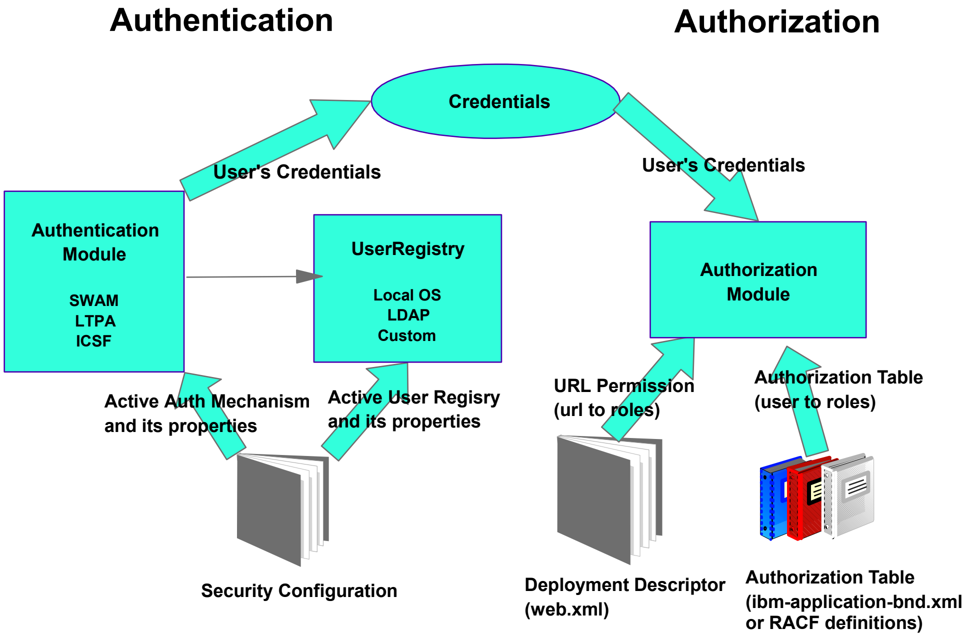
For your pleasure:
Token is called LTPA

Redbooks

ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

WebSphere Implementation


Authentication
Authorization
Credentials
User's Credentials
User's Credentials
Authentication Module
SWAM
LTPA
ICSF
UserRegistry
Local OS
LDAP
Custom
Authorization Module
Active Auth Mechanism and its properties
Active User Regisry and its properties
URL Permission (url to roles)
Authorization Table (user to roles)
Security Configuration
Deployment Descriptor (web.xml)
Authorization Table (ibm-application-bnd.xml or RACF definitions)

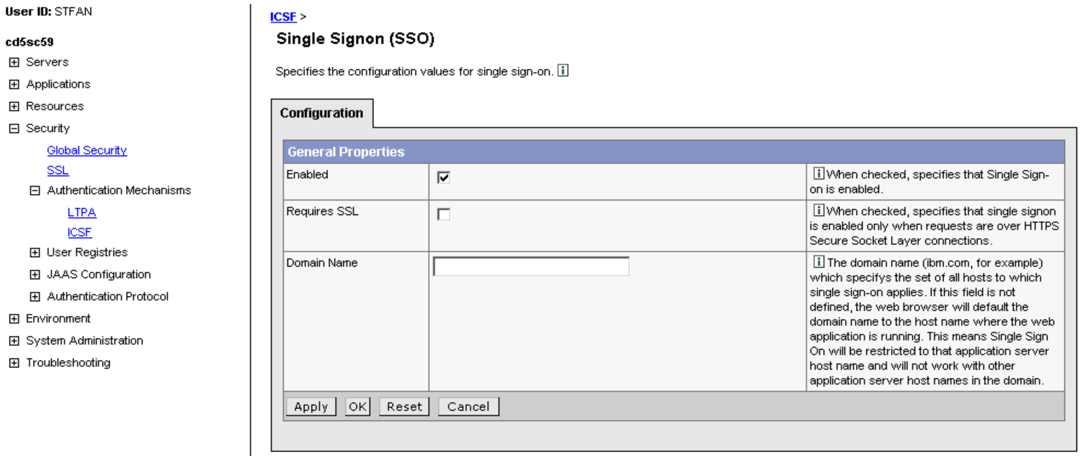
Redbooks ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Single Sign On

Provided by forwardable LtpaToken (LTPA or ICSF)

... domain needs to share LtpaToken encryption and key mechanism.



Single Signon (SSO)

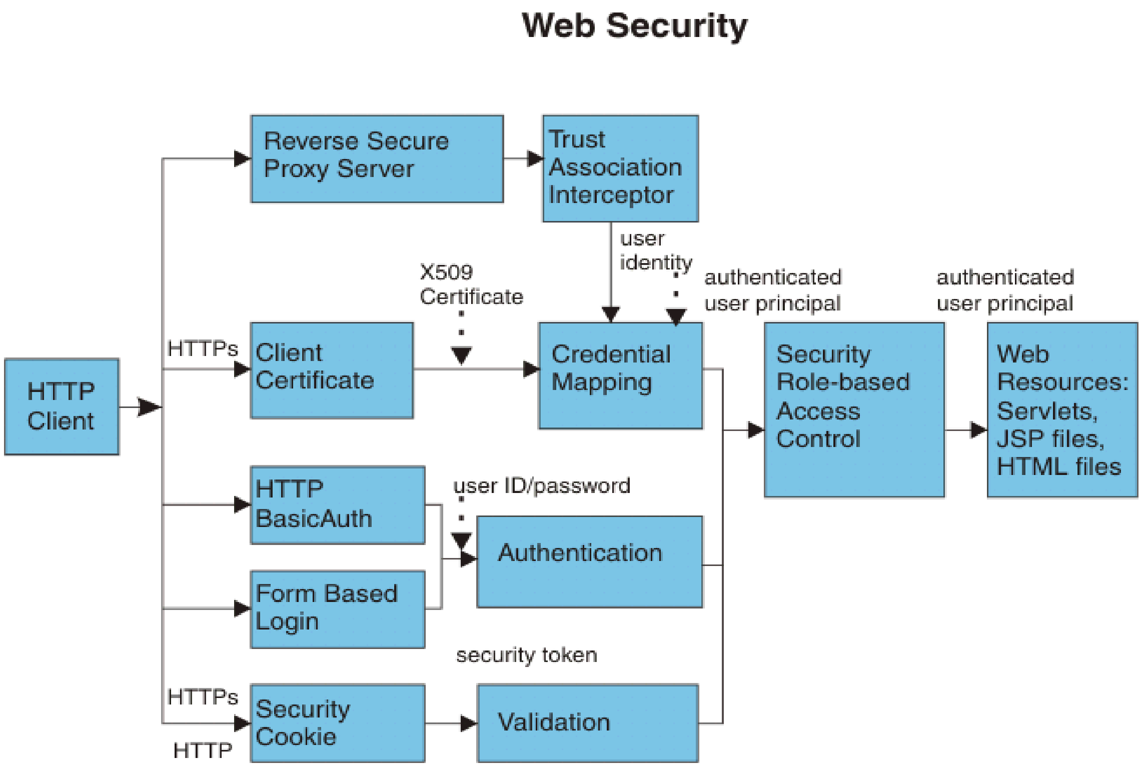
Specifies the configuration values for single sign-on.

General Properties		
Enabled	☑	When checked, specifies that Single Sign-on is enabled.
Requires SSL	□	When checked, specifies that single signon is enabled only when requests are over HTTPS Secure Socket Layer connections.
Domain Name		The domain name (ibm.com, for example) which specifies the set of all hosts to which single sign-on applies. If this field is not defined, the web browser will default the domain name to the host name where the web application is running. This means Single Sign On will be restricted to that application server host name and will not work with other application server host names in the domain.

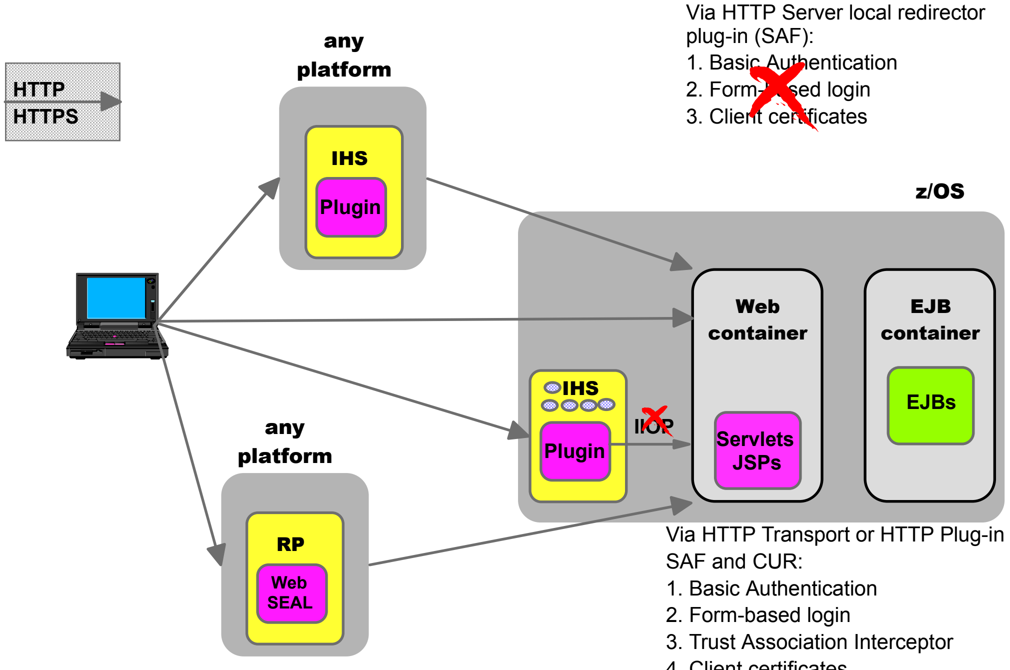
Redbooks ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

WebSphere HTTP Authentication



Authentication options: HTTP Server and HTTP Transport



Via HTTP Server local redirector plug-in (SAF):

1. Basic Authentication
2. ~~Form-based login~~
3. Client certificates

Via HTTP Transport or HTTP Plug-in SAF and CUR:

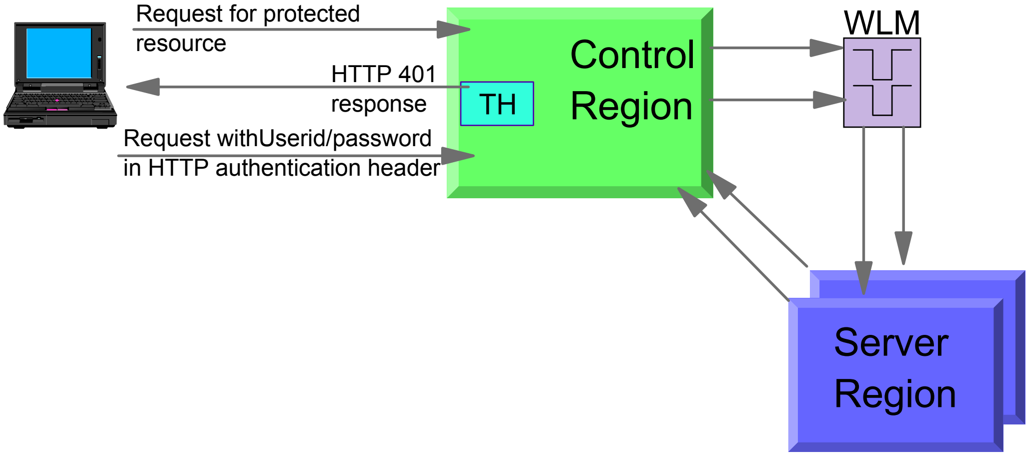
1. Basic Authentication
2. Form-based login
3. Trust Association Interceptor
4. Client certificates

Redbooks

ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

HTTP Transport Handler



Request for protected resource

HTTP 401 response

Request withUserid/password in HTTP authentication header

TH

Control Region

WLM

Server Region

© Copyright IBM Corp. 2003. All rights reserved.

Basic Authentication

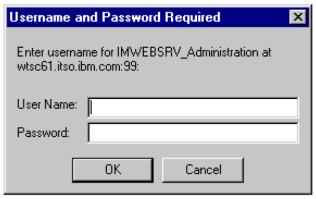
1. User clicks on link to protected page

Request: GET http://server/restricted.html

2. Server checks authority and rejects request

Response: Status 401
Realm "IMWEBSRV_Administration"

3. Browser pop-up window prompts user for userId and password



Username and Password Required

Enter username for IMWEBSRV_Administration at wtsc61.itso.ibm.com:99:

User Name:

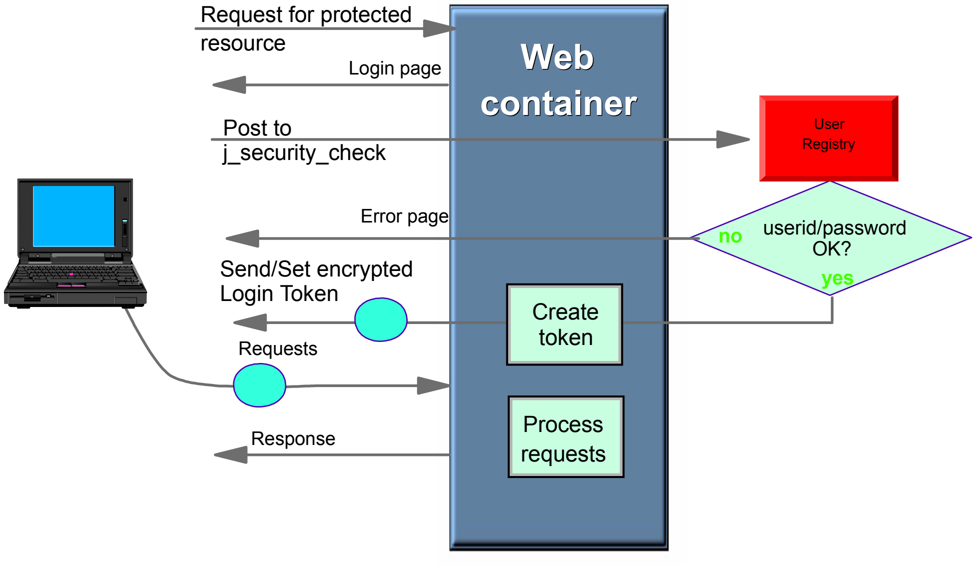
Password:

4. Browser resends request with userid/password in request header

```
Request: GET http://server/restricted.html
```

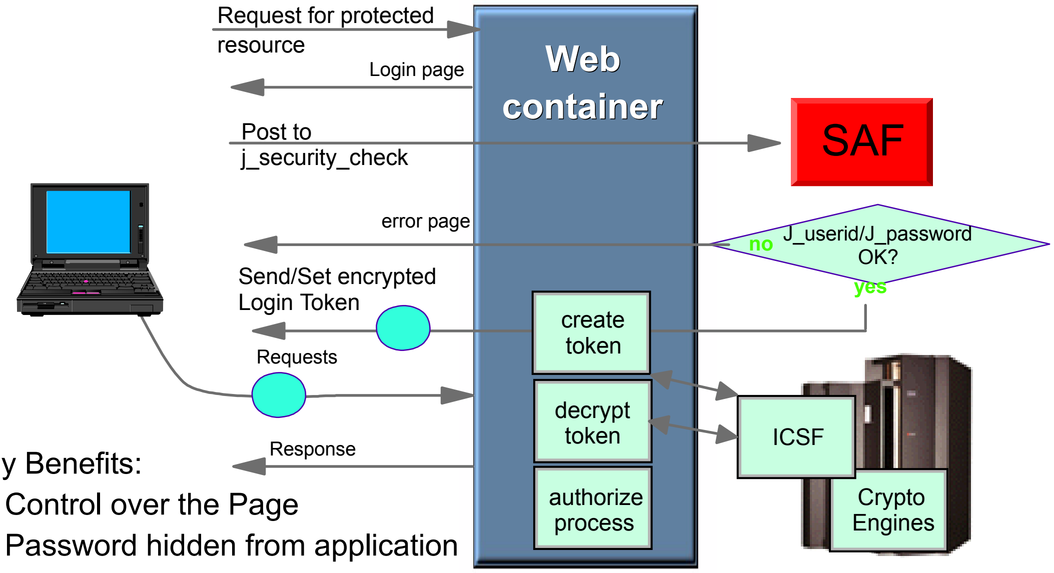
© Copyright IBM Corp. 2003. All rights reserved.

Form based



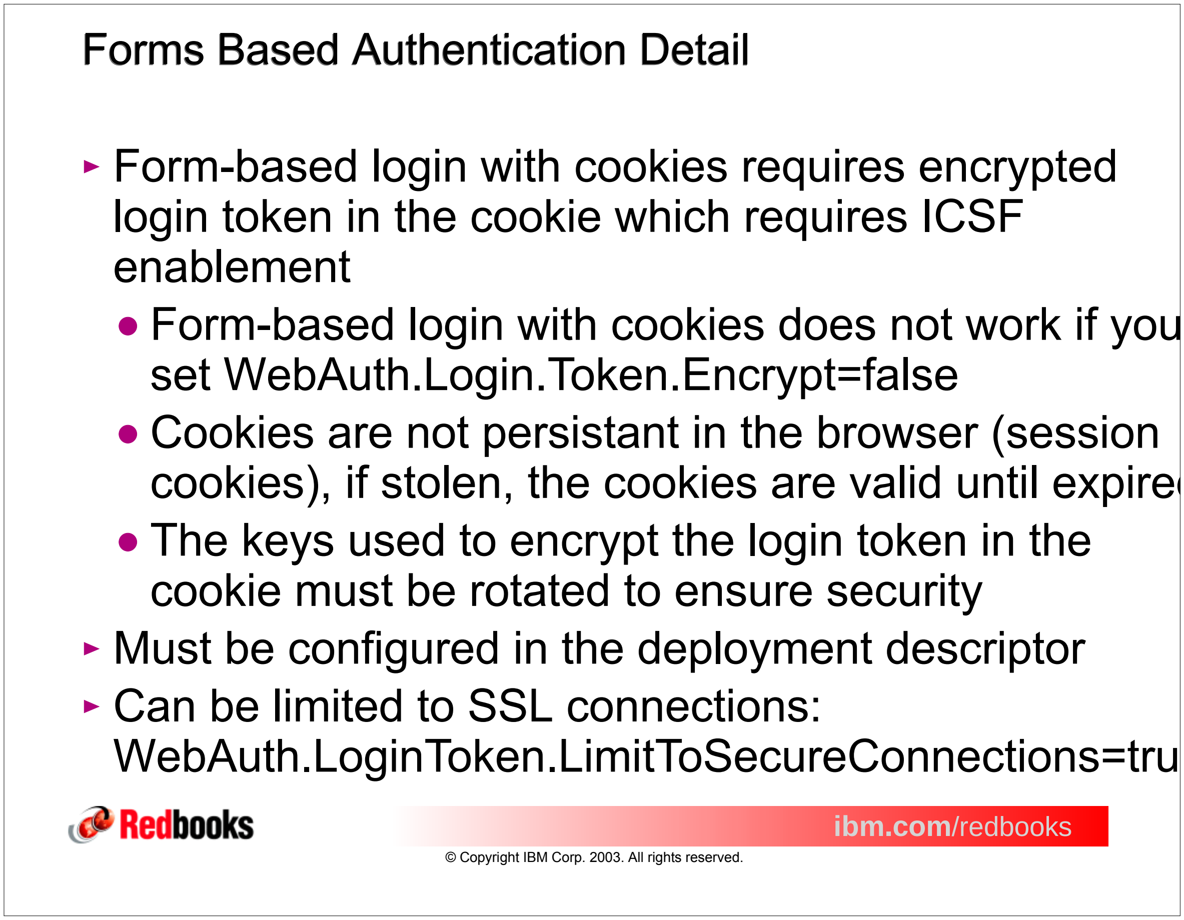
© Copyright IBM Corp. 2003. All rights reserved.

Form based login with SAF and ICSF



- Key Benefits:
  - Control over the Page
  - Password hidden from application
- Comments:
  - Requires cookies, requires encryption, SAF user present

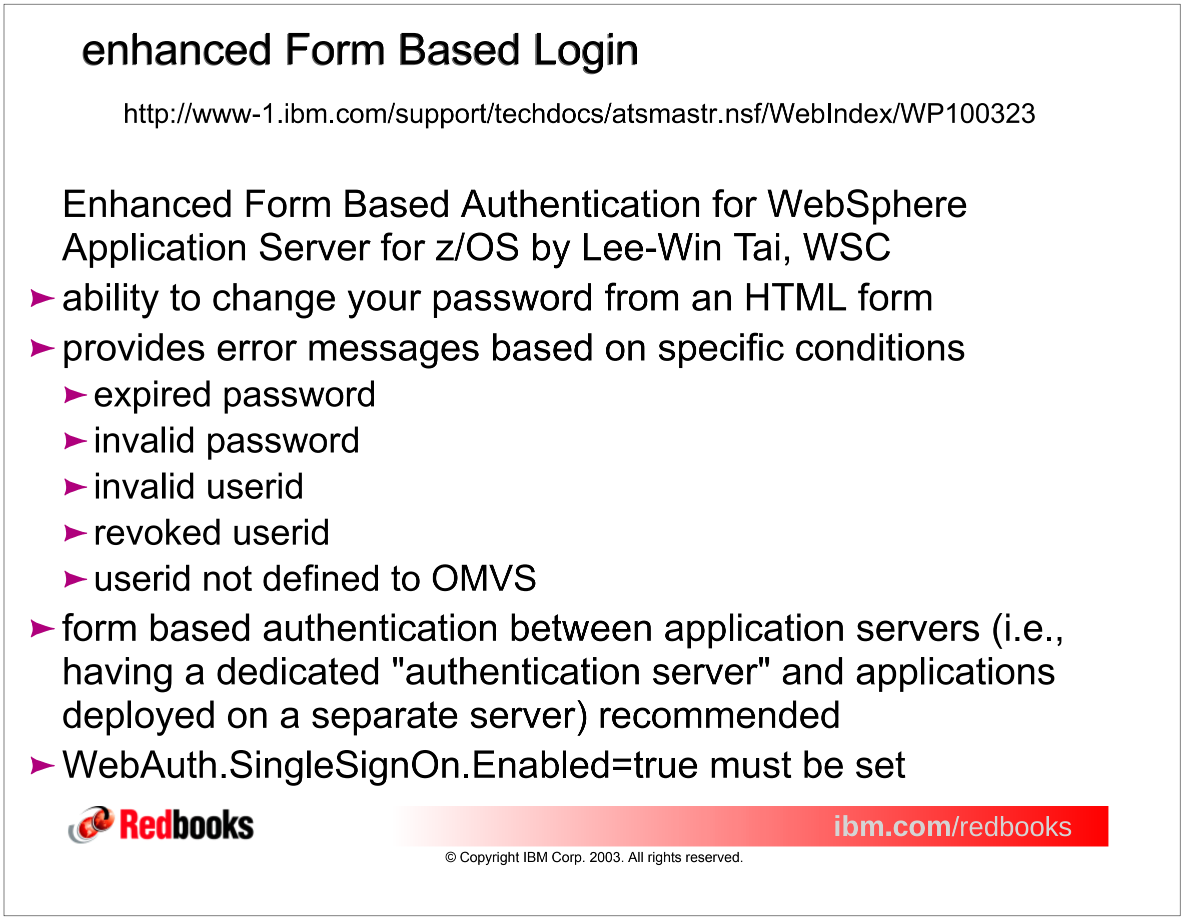
© Copyright IBM Corp. 2003. All rights reserved.



Forms Based Authentication Detail

- Form-based login with cookies requires encrypted login token in the cookie which requires ICSF enablement
  - Form-based login with cookies does not work if you set WebAuth.Login.Token.Encrypt=false
  - Cookies are not persistant in the browser (session cookies), if stolen, the cookies are valid until expire
  - The keys used to encrypt the login token in the cookie must be rotated to ensure security
- Must be configured in the deployment descriptor
- Can be limited to SSL connections: WebAuth.LoginToken.LimitToSecureConnections=tru

© Copyright IBM Corp. 2003. All rights reserved.



enhanced Form Based Login

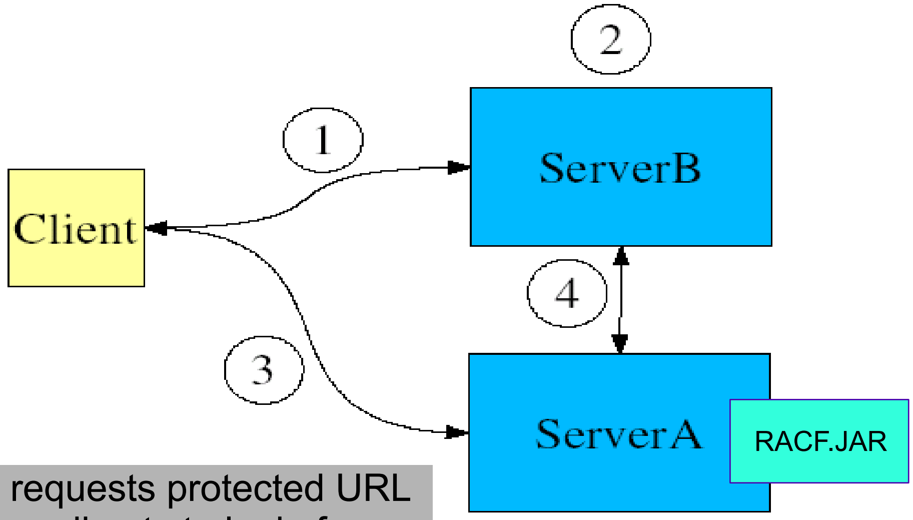
http://www-1.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100323

Enhanced Form Based Authentication for WebSphere Application Server for z/OS by Lee-Win Tai, WSC

- ability to change your password from an HTML form
- provides error messages based on specific conditions
  - expired password
  - invalid password
  - invalid userid
  - revoked userid
  - userid not defined to OMVS
- form based authentication between application servers (i.e., having a dedicated "authentication server" and applications deployed on a separate server) recommended
- WebAuth.SingleSignOn.Enabled=true must be set

© Copyright IBM Corp. 2003. All rights reserved.

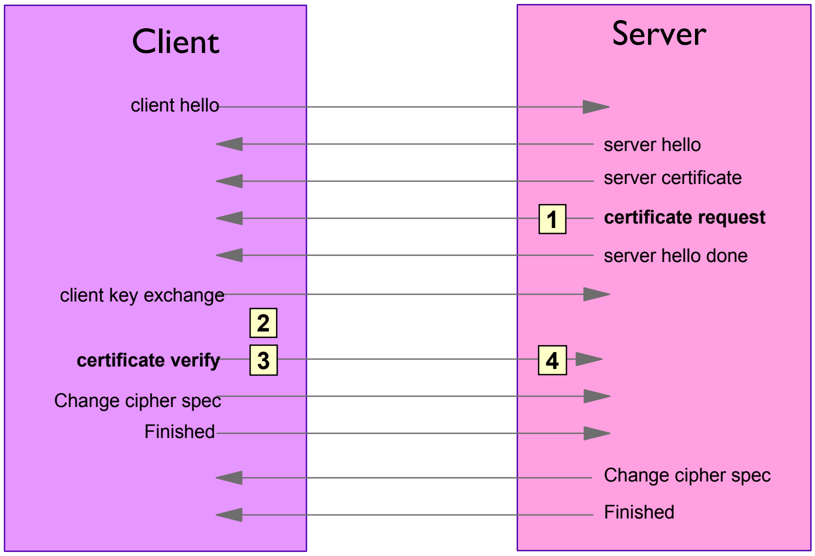
eFBL



1 Client requests protected URL
2 Server redirects to login form
3 Client submits form to authentication server
4 Client is redirected to originally requested URL

© Copyright IBM Corp. 2003. All rights reserved.

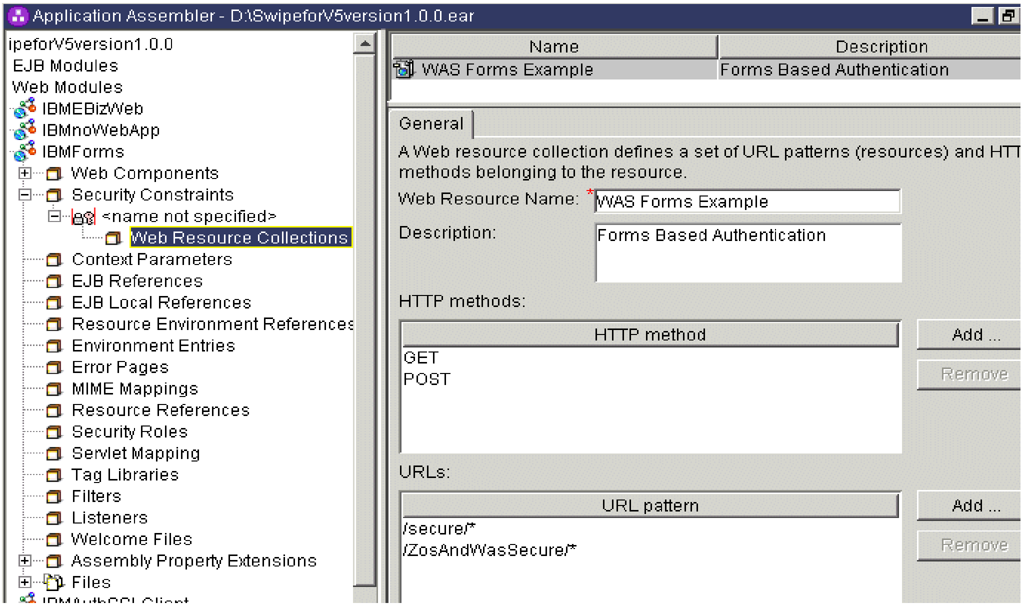
Certificates



HTTP custom prop. MutualAuthCBindCheck should control RACF certificate mapping.

© Copyright IBM Corp. 2003. All rights reserved.

URL Protection



Name	Description
WAS Forms Example	Forms Based Authentication

A Web resource collection defines a set of URL patterns (resources) and HTT methods belonging to the resource.

Web Resource Name: * WAS Forms Example

Description: Forms Based Authentication

HTTP methods:

HTTP method
GET
POST

URLs:

URL pattern
/secure/*
/ZosAndWasSecure/*

Redbooks

© Copyright IBM Corp. 2003. All rights reserved.

web.xml: Security Constraints

```
<security-constraint>
    <web-resource-collection>
        <web-resource-name>Secure Urls</web-resource-name>
        <description></description>
        <url-pattern>/secure/*</url-pattern>
        <http-method>GET</http-method>
        <http-method>PUT</http-method>
    </web-resource-collection>
    <auth-constraint>
        <description></description>
        <role-name>Manager</role-name>
    </auth-constraint>
    <user-data-constraint>
        <transport-guarantee>INTEGRAL</transport-guarantee>
    </user-data-constraint>
</security-constraint>
<login-config>
    <auth-method>BASIC</auth-method>
    <realm-name>SimpleRealm</realm-name>
</login-config>
<security-role>
    <description>Manager role</description>
    <role-name>Manager</role-name>
</security-role>
```

Redbooks

© Copyright IBM Corp. 2003. All rights reserved.

ibm.com

e-business

IBM

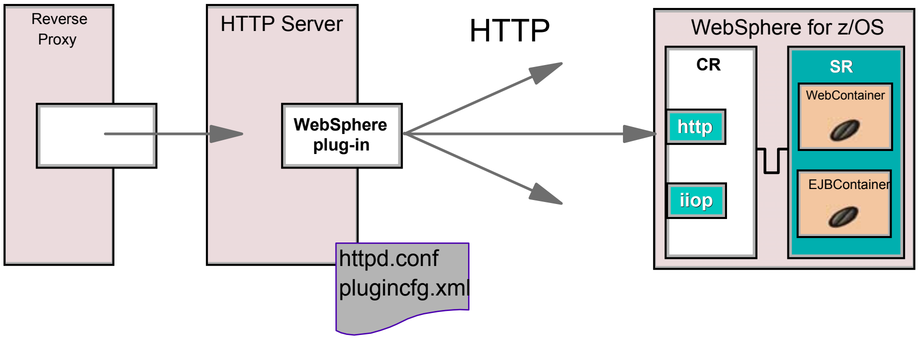
HTTP Plug-in

Redbooks

International Technical Support Organization

© Copyright IBM Corp. 2003. All rights reserved.

WAS 4/5 HTTP(S) plug-in (security aspects)



Reverse Proxy

HTTP Server

WebSphere plug-in

httpd.conf
pluginCfg.xml

HTTP

WebSphere for z/OS

CR

http

iiop

SR

WebContainer

EJBContainer

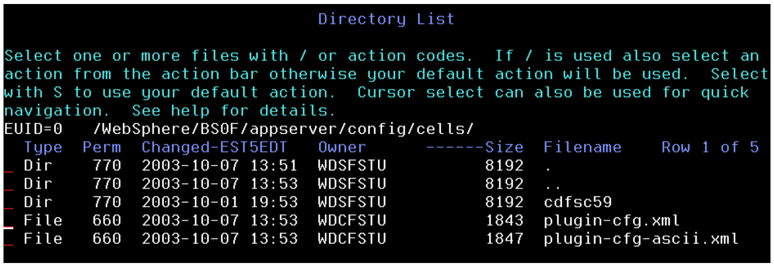
- ➤ SSL endpoint
- ➤ Authentication
- ➤ DMZ Integration
- ➤ Private WebSphere Headers

~~BBOC_HTTP_MODE=INTERNAL~~
TrustedProxy=true
~~BBOC_HTTP_SSL_MODE=INTERNAL~~
TrustedProxy=true

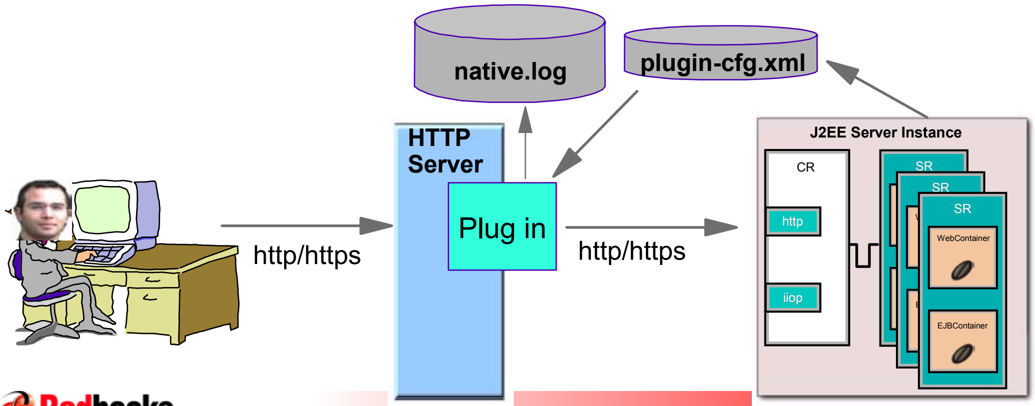
Private Headers contain:
certificate
remote user
remote host

© Copyright IBM Corp. 2003. All rights reserved.

HTTP Plugin



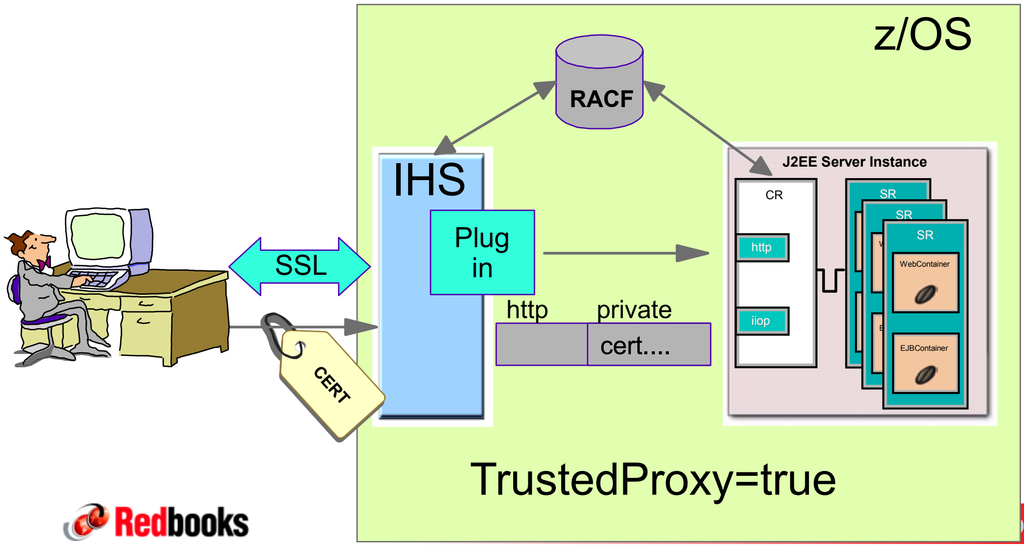
```
                         Directory List

Select one or more files with / or action codes.  If / is used also select an
action from the action bar otherwise your default action will be used.  Select
with S to use your default action.  Cursor select can also be used for quick
navigation.  See help for details.
EUID=0   /WebSphere/BSOF/appserver/config/cells/
  Type  Perm  Changed-EST5EDT   Owner       ------Size  Filename    Row 1 of 5
_ Dir    770  2003-10-07 13:51  WDSFSTU           8192  .
_ Dir    770  2003-10-07 13:53  WDSFSTU           8192  ..
_ Dir    770  2003-10-01 19:53  WDSFSTU           8192  cdfsc59
_ File   660  2003-10-07 13:53  WDCFSTU           1843  plugin-cfg.xml
_ File   660  2003-10-07 13:53  WDCFSTU           1847  plugin-cfg-ascii.xml
```



© Copyright IBM Corp. 2003. All rights reserved.

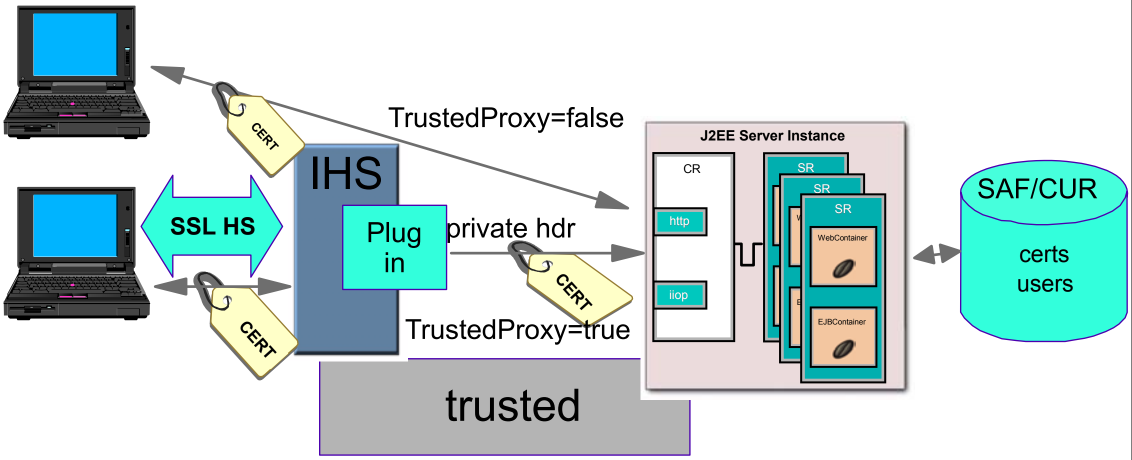
z/OS IHS Plug-in

- ➤do not use protection setups (%%CLIENT%%)
- ➤extattr +p ihs390WASPlugin_http.so
- ➤could be used for expired PW support (with protection setup and basic auth only)



© Copyright IBM Corp. 2003. All rights reserved.

Client Certificates with Transport Handler



- Client Certificate returned from SSL Handshake
- Client Certificate info passed to Server Region via private header with request
  - Certificate not passed unless running in TrustedProxy=true. The Plug-in will pass any needed certificate info via HTTP headers

ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

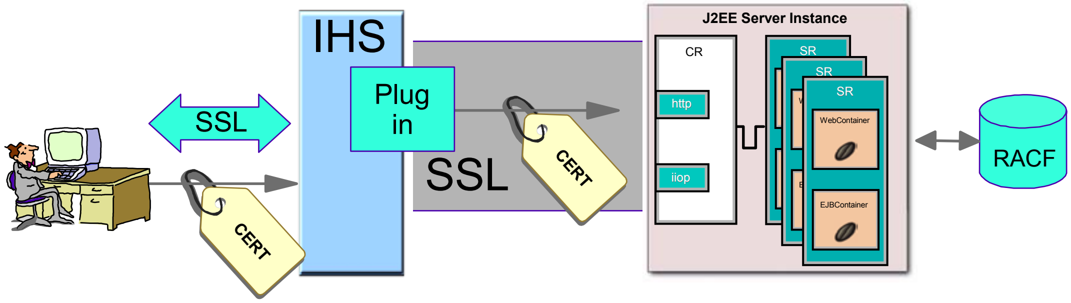
Authentication variation according TrustedProxy property

Configuration	TrustedProxy=false	TrustedProxy=true
direct to HTTP transport handler	Basic auth. enabled	Basic auth. enabled
	Form based auth. enabled	Form based auth. enabled
	Certificate auth. enabled web container has an HTTPS transport.	Certificate auth. disabled
HTTP plug-in -> TH	Basic auth. enabled	Basic auth. enabled
	Form based auth. enabled	Form based auth. enabled
	Certificate auth. enabled. HTTP server certificate is used to authenticate if web container has an HTTPS transport.	direct user certificate auth. disabled. certs flow in a private header

ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

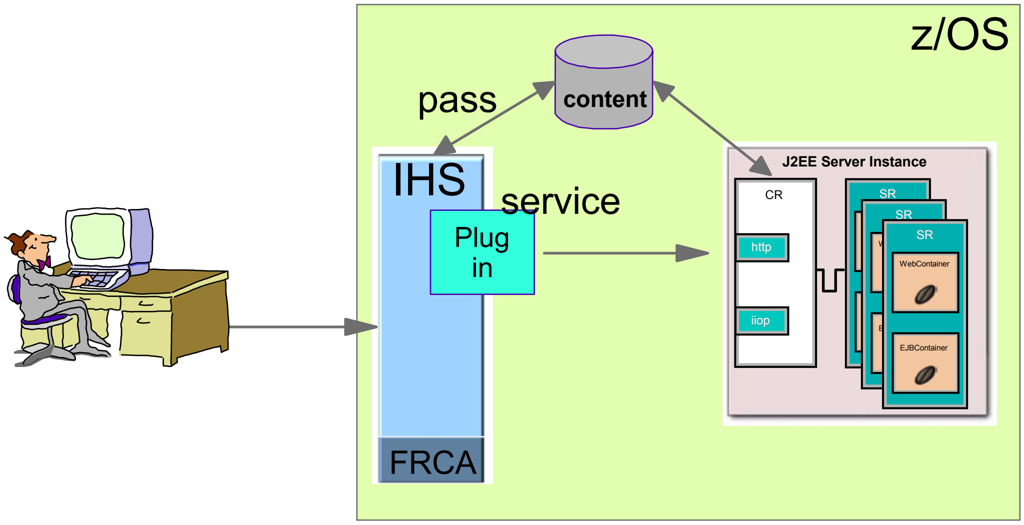
encrypting traffic between WAS and PI



- ➤To encrypt all traffic between the plugin and the web container remove all non-SSL transport ports from the web container, update the plugin-cfg.xml file. Following the regular InfoCenter instructions for configuring SSL for the plugin to web container connection would only encrypt https requests.
- ➤Use ~~BBOC_HTTP_SSL_CBIND=ON~~ protocol_https_mutual_auth_cbind_check to enforce mutual handshake and also restrict the clients that can connect to TH
- ➤CB.BIND provides addition level of security/verification on HTTP SSL Transport connections
  - ➤WebServers Cert must be mapped to an user which has access(CONTROL) to CBIND CB.BIND.webcontainerID
  - ➤PERMIT CB.BIND.servername CLASS(CBIND) ID(clientCertUserid) ACCESS(CONTROL)

© Copyright IBM Corp. 2003. All rights reserved.

IHS/plug-in for static content acceleration



- ➤don't use security for the static content
- ➤or use basic auth and sync the values for the
  - ➤ServerID in the protection setup in the httpd.conf
  - ➤and the <realm-name> in the web.xml

© Copyright IBM Corp. 2003. All rights reserved.

authc combinations

HTTP server with plug-in protection	Web container login setting	Result
None	Basic	web container prompts realm thru the plugin
	Form based	web container redirects request to the form login page thru the plugin
	Certificate	depends on HTTPS transport availability and TrustedProxy custom variable. See next pages
Basic	Basic	web container reuses HTTP server authentication if realm is the same
	Form based	web container ignores HTTP server authentication and redirects request to the form login page thru the plugin
	Certificate	depends on HTTPS transport availability and TrustedProxy custom variable.
SSL	Basic	web container ignores certificate authentication and prompts realm thru the plugin
	Form based	web container ignores certificate authentication and redirects request to the form login page thru the plugin
	Certificate	depends on HTTPS transport availability and TrustedProxy custom variable.

© Copyright IBM Corp. 2003. All rights reserved.

top secret!
inside the private headers

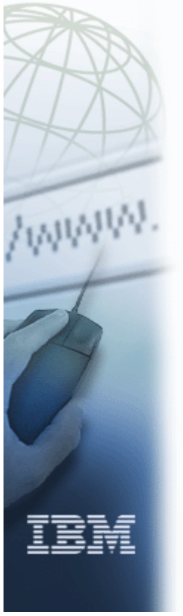
```
PrintWriter server = new PrintWriter(s.getOutputStream());

String line;
System.out.println("Connected... Type your manual HTTP request");
System.out.println("----------------------------------------");

  server.print("GET /IBMClientSSL/secure/sslEjbCaller HTTP/1.1\n");
  server.print("Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,  application/msword\n");
  server.print("Accept-Encoding: gzip, deflate\n");
  server.print("Cookie: msp=2\n");
  server.print("User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)\n");
  server.print("Host: wtsc59.itso.ibm.com\n");
  server.print("Connection: Keep-Alive\n");
  server.print("Accept-Language: en-us\n");
  server.print("$WSCC: MIICYzCCAcygAwIBAgIBDjANBgkqhkiG9w0BAQUFADAkMQswCQYDVQQGEwJVUzEVMBMGA1UEAx...
  server.print("$WSIS: true\n");
  server.print("$WSSC: https\n");
  server.print("$WSPR: HTTP/1.1\n");
  server.print("$WSRA: 9.12.6.175\n");
  server.print("$WSSN: wtsc59.itso.ibm.com\n");
  server.print("$WSSP: 4469\n");
  server.print("$WSSI: BQACzgkMBq8IRAAAAAAAAAAAAAAAAAAAPyrtnQAAAAY=\n");
  server.print("Surrogate-Capabilities: WS-ESI=\"ESI/1.0+\"\n\r\n");  // HTTP lines end with \r\n
  server.flush();
```

client cert

© Copyright IBM Corp. 2003. All rights reserved.

ibm.com

e-business



EJB Container

Redbooks

International Technical Support Organization

© Copyright IBM Corp. 2003. All rights reserved.

Authc/Authz

Authentication

- LOCAL OS only
- delegation from WC (run-as)
- zSAS and/or CSIv2

Authorization

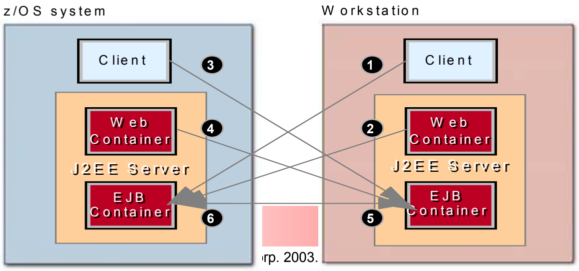
- SAF based or
- bindings

© Copyright IBM Corp. 2003. All rights reserved.

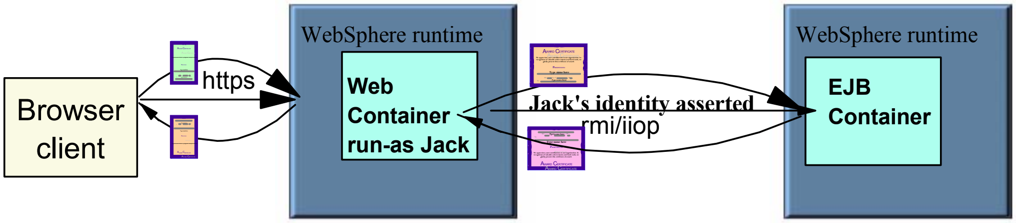
cross platform Authentication

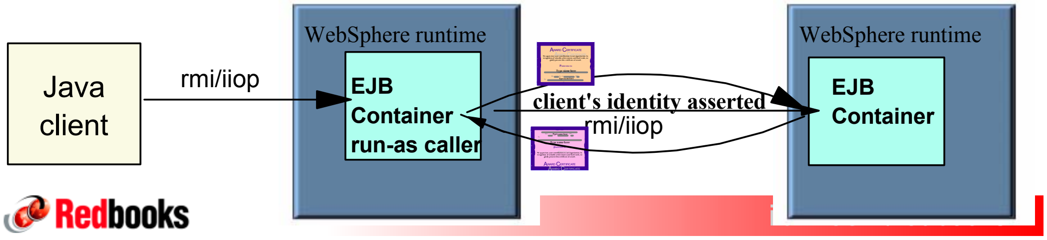
- **z/SAS Features**
  - IBM z/OS specific
  - Userid/Password over wire
  - SSL choice can be independent of security mechanism
  - requires zOS SAF credentials
- **CSIv2 Features**
  - SSL/TLS or TCPIP Choice per configuration
  - Accepts asserted Distinguished Names and Digital Certs from ND
  - requires zOS SAF credentials
  - Stateful/Stateless Choice

1) Userid/password over SSL, SSL mutual authentication
2) Server's userid/password over SSL
3) SSL mutual authentication
4) SSL mutual authentication
5) Server's userid/password over SSL
6) SSL mutual authentication
+
Supplemental Client Authentication asserted identities



CSIv2 identity assertion

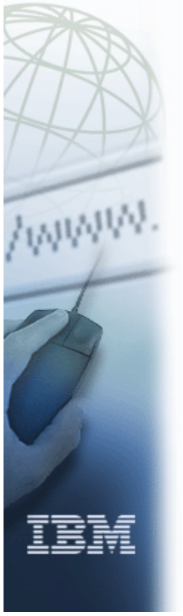




© Copyright IBM Corp. 2003. All rights reserved.

ibm.com

e-business



EIS security

Redbooks

International Technical Support Organization

© Copyright IBM Corp. 2003. All rights reserved.

JCA Authentication Options

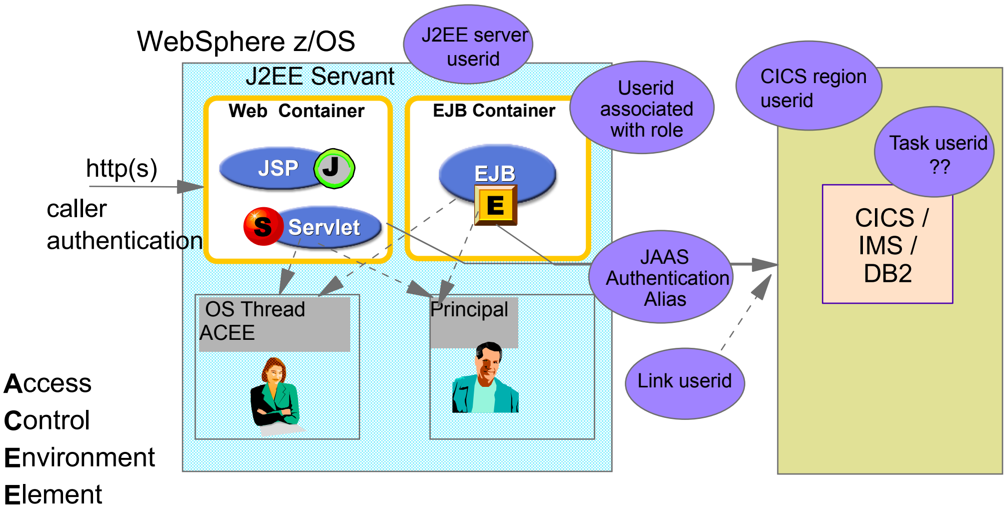
Defined by J2EE resource reference descriptor <res-auth>

- Container - Container Managed Sign-on
  - EIS sign-on managed by WebSphere Application Server
- Application - Component Managed Sign-on
  - Application component provides explicit security information

New in WAS V5! J2C Connection Factories can use JAAS Authentication Alias for Component and/or Container authentication

© Copyright IBM Corp. 2003. All rights reserved.

Lots of Userids/Principals/Identities!


WebSphere z/OS

J2EE server userid

J2EE Servant

Web Container

EJB Container

Userid associated with role

CICS region userid

Task userid ??

http(s)

caller authentication

JSP

J

S

Servlet

EJB

E

JAAS Authentication Alias

CICS / IMS / DB2

OS Thread ACEE

Principal

Link userid

Access

Control

Environment

Element

which userid do you want to flow to the EIS ?

© Copyright IBM Corp. 2003. All rights reserved.

z/OS Thread Identity

Thread Identity: z/OS exclusive option that allows the identity of the current thread to be assigned to a connection.

Applicable only to JCA resource adapters and JDBC providers that support the use of thread identity and only when:

- res-auth=Container in J2EE Resource Reference
- no Container-managed JAAS alias specified for J2C Connection Factory

You do not need to specify anything to declare the level of support. The Resource Adapter's ConnectionFactory or DataSource states its level of support to the container.

- Thread identity support (Allowed, Not Allowed, Required)

Thread Identity support applies to local mode JCA only.

© Copyright IBM Corp. 2003. All rights reserved.

Thread Security (SynchtoOSThread)

Thread Security: z/OS exclusive option that allows the identity of the current thread to be pushed onto the OS thread.

(Also known as SynchtoOSThread).

You do not need to specify anything to declare the level of support. The Resource Adapter's ConnectionFactory or DataSource states its level of support to the container.

- OS Thread Security support (Yes, Not Supported)

To enable Thread Security :

- Enable for the server using Administration Console Security->Global Security->Additonal Properties, z/OS Security Options. Then enter a check mark in the box titled,"Sync To OS Thread Allowed" (**Available only for AdminConsole W500103**)
- res-auth=Container in J2EE Resource Reference
- no Container-managed JAAS alias specified for J2C Connection Factory (DB2 z/OS Only)

© Copyright IBM Corp. 2003. All rights reserved.

Thread Identity and Thread Security Support

Connectors	Thread Identity Support	Thread Security Support
IMS Connector local mode configuration	ALLOWED	Not supported
IMS Connector remote mode configuration	NOTALLOWED	Not supported
CTG Connector local mode configuration	ALLOWED	Not supported
CTG Connector remote mode configuration	NOTALLOWED	Not supported
IMS JDBC Connector	REQUIRED	True
RRA DB2 z/OS Local JDBC Provider	ALLOWED	True

- IMS Connector for Java ThreadIdentity support requires APAR PQ76633

© Copyright IBM Corp. 2003. All rights reserved.

z/OS Thread Identity Connectors Support

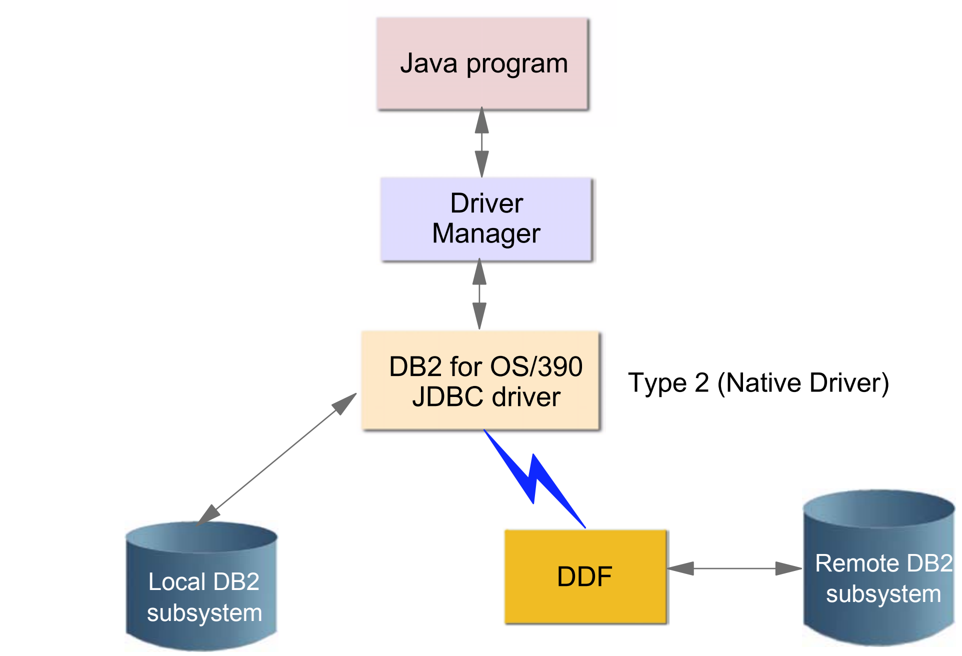
<table>
<tr><td colspan="8">Container-managed JAAS Authentication Alias specified?</td></tr>
<tr><td colspan="4">NO</td><td colspan="4">YES</td></tr>
<tr><td colspan="4">Connector Allows or Requires Thread Identity?</td><td colspan="4">Connector Requires Thread Identity?</td></tr>
<tr><td>NO</td><td colspan="3">YES</td><td>NO</td><td colspan="3">YES</td></tr>
<tr><td rowspan="5">Proceeing is dependent on connector:
• may throw exception
• may default to connector user/pswd custom properties</td><td colspan="3">Connector Requires OS Thread Security?</td><td rowspan="5">Use specified JAAS alias</td><td colspan="3">Connector Requires OS Thread Security?</td></tr>
<tr><td>NO</td><td colspan="2">YES</td><td>NO</td><td colspan="2">YES</td></tr>
<tr><td rowspan="3">Use RunAs user identity associated with current thread</td><td colspan="2">Server Sync-To-Thread enabled?</td><td rowspan="3">Use RunAs user identity associated with current thread</td><td colspan="2">Server Sync-To-Thread enabled?</td></tr>
<tr><td>NO</td><td>YES</td><td>NO</td><td>YES</td></tr>
<tr><td>Use Server identity</td><td>Use RunAs user identity associated with current thread</td><td>Use Server identity</td><td>Use RunAs user identity associated with current thread</td></tr>
</table>

© Copyright IBM Corp. 2003. All rights reserved.

DB2 z/OS

© Copyright IBM Corp. 2003. All rights reserved.

Java Application Flow with JDBC for OS/390

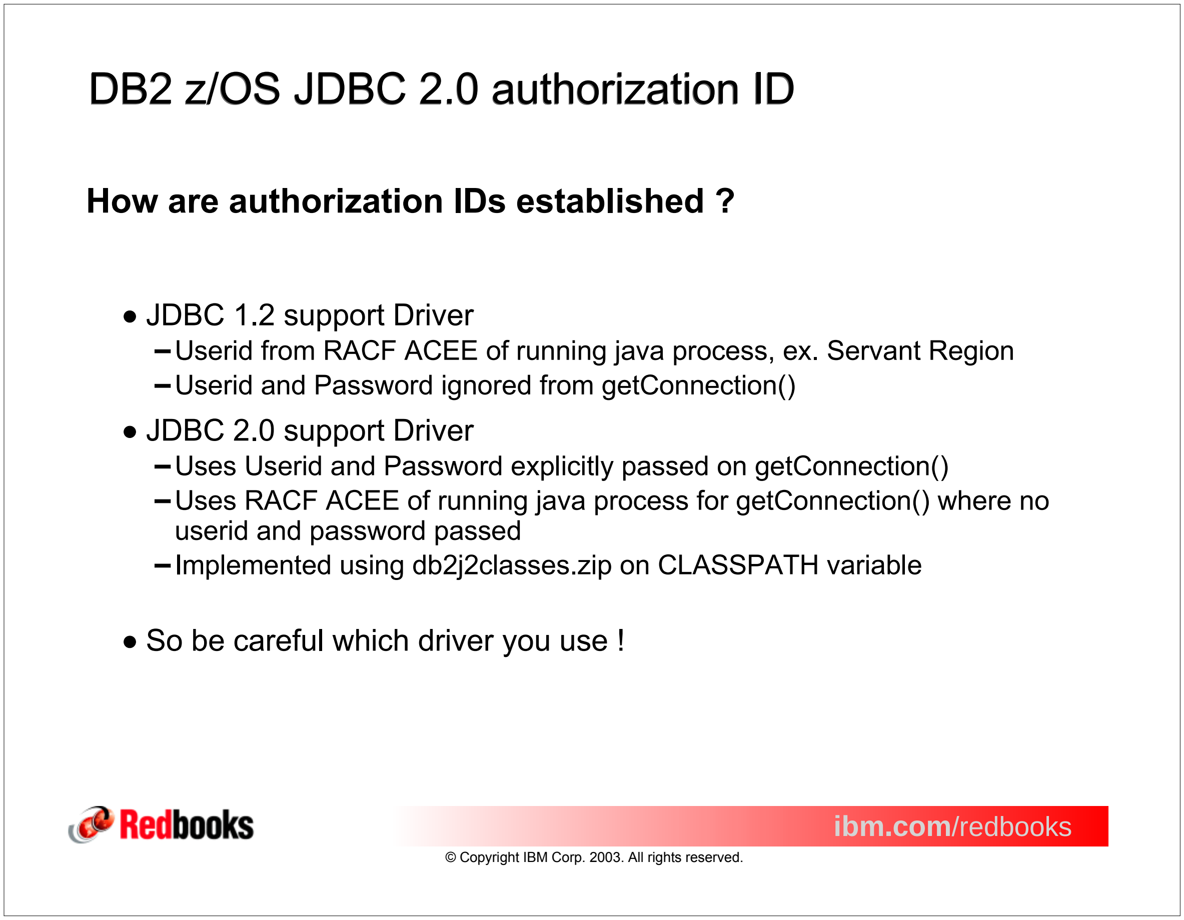


© Copyright IBM Corp. 2003. All rights reserved.

Implicit and explicit userid in JDBC

```
Hashtable parms = new Hashtable();
parms.put(Context.INITIAL_CONTEXT_FACTORY,cx_factory);
Context ctx = new InitialContext(parms);
jndisource = "java:comp/env/jdbc/DbSecurity");   (1)
ds = (javax.sql.DataSource) ctx.lookup(jndisource);

// Are we trying to supply our own USERID and PASSWORD?
if (userid == null) {
      System.out.println("Use implicit Userid & Password");
      conn = ds.getConnection();   (2a)
}
else {
      System.out.println("Use explicit <" + userid + "> &
Password");
      conn = ds.getConnection(userid, password);   (2b)
}
```

© Copyright IBM Corp. 2003. All rights reserved.

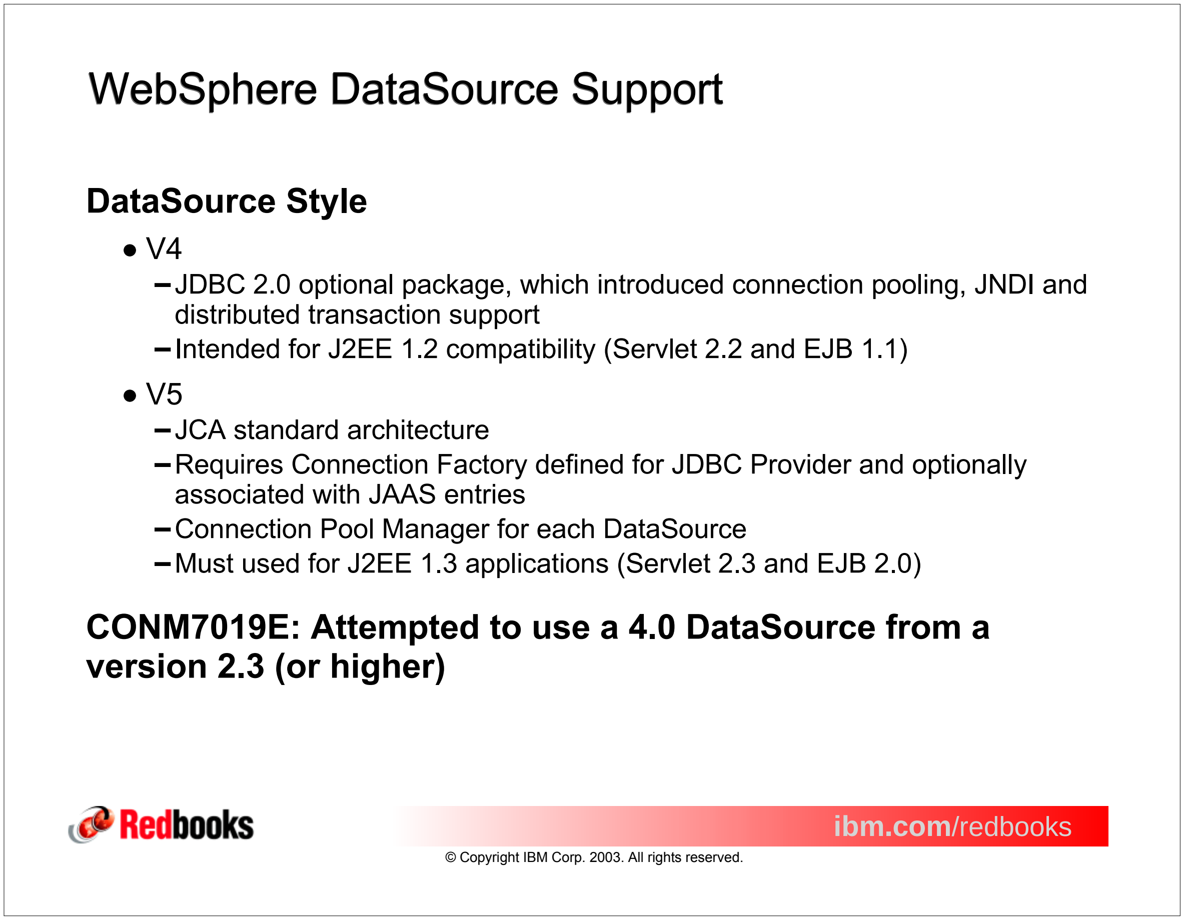


DB2 z/OS JDBC 2.0 authorization ID

How are authorization IDs established ?

- JDBC 1.2 support Driver
  - Userid from RACF ACEE of running java process, ex. Servant Region
  - Userid and Password ignored from getConnection()
- JDBC 2.0 support Driver
  - Uses Userid and Password explicitly passed on getConnection()
  - Uses RACF ACEE of running java process for getConnection() where no userid and password passed
  - Implemented using db2j2classes.zip on CLASSPATH variable
- So be careful which driver you use !

© Copyright IBM Corp. 2003. All rights reserved.



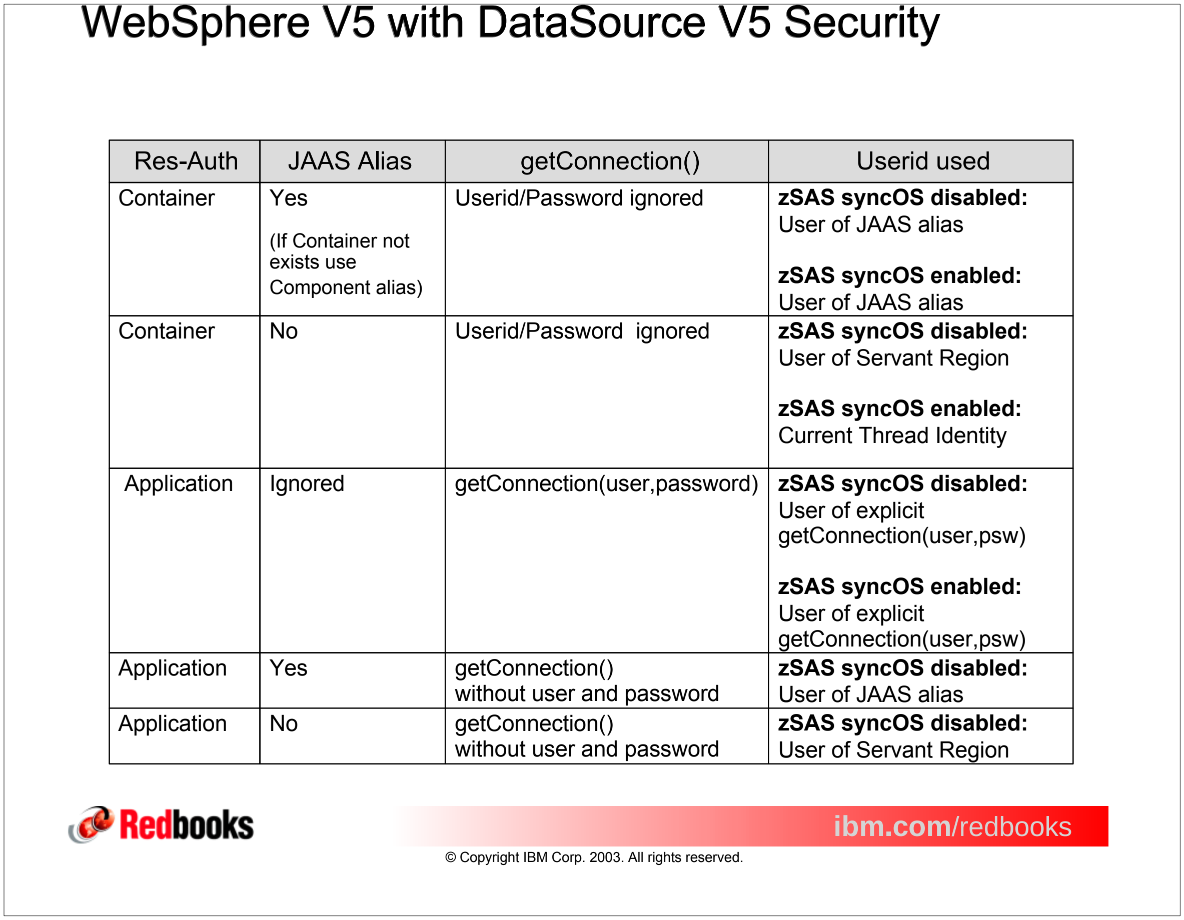
WebSphere DataSource Support

DataSource Style

- V4
  - JDBC 2.0 optional package, which introduced connection pooling, JNDI and distributed transaction support
  - Intended for J2EE 1.2 compatibility (Servlet 2.2 and EJB 1.1)
- V5
  - JCA standard architecture
  - Requires Connection Factory defined for JDBC Provider and optionally associated with JAAS entries
  - Connection Pool Manager for each DataSource
  - Must used for J2EE 1.3 applications (Servlet 2.3 and EJB 2.0)

CONM7019E: Attempted to use a 4.0 DataSource from a version 2.3 (or higher)

© Copyright IBM Corp. 2003. All rights reserved.

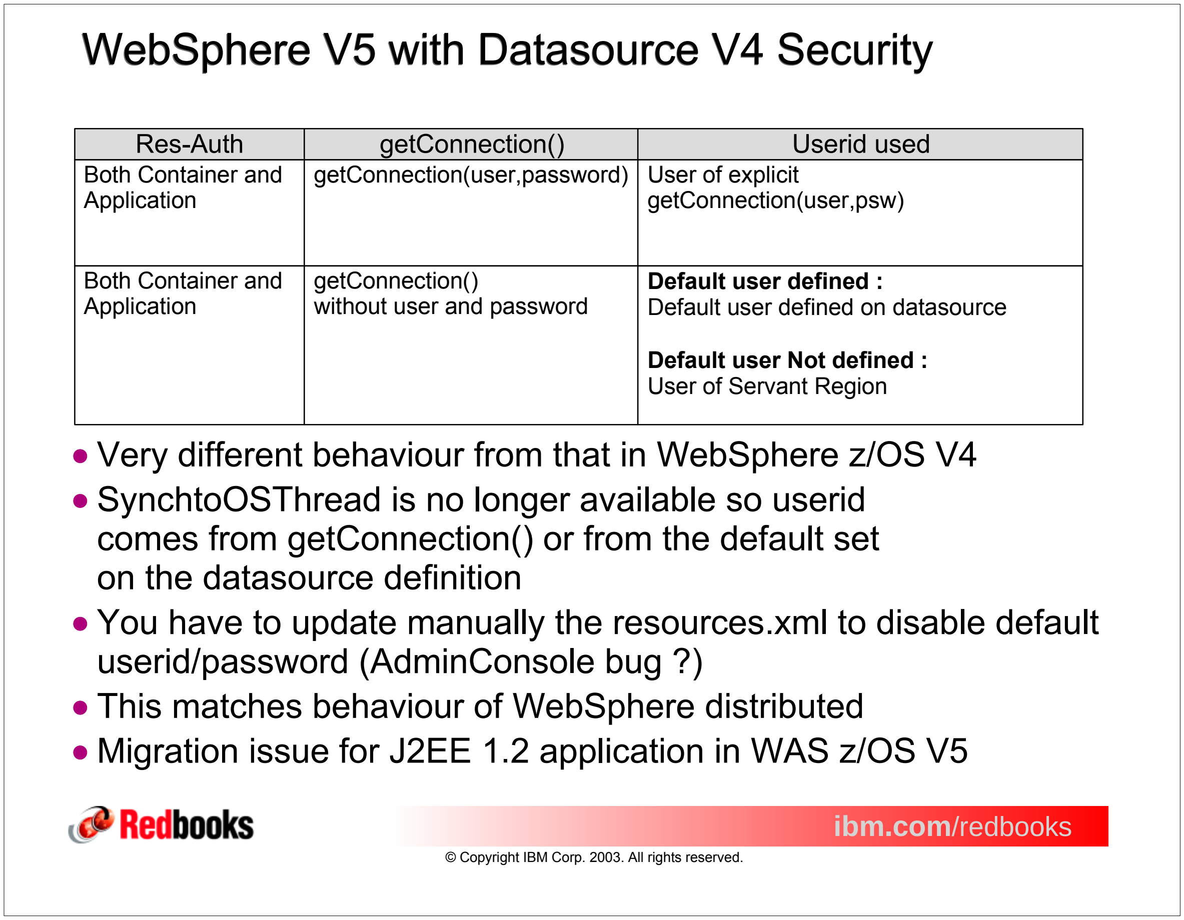


WebSphere V5 with DataSource V5 Security

Res-Auth	JAAS Alias	getConnection()	Userid used
Container	Yes (If Container not exists use Component alias)	Userid/Password ignored	**zSAS syncOS disabled:** User of JAAS alias **zSAS syncOS enabled:** User of JAAS alias
Container	No	Userid/Password ignored	**zSAS syncOS disabled:** User of Servant Region **zSAS syncOS enabled:** Current Thread Identity
Application	Ignored	getConnection(user,password)	**zSAS syncOS disabled:** User of explicit getConnection(user,psw) **zSAS syncOS enabled:** User of explicit getConnection(user,psw)
Application	Yes	getConnection() without user and password	**zSAS syncOS disabled:** User of JAAS alias
Application	No	getConnection() without user and password	**zSAS syncOS disabled:** User of Servant Region

Redbooks ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.



WebSphere V5 with Datasource V4 Security

Res-Auth	getConnection()	Userid used
Both Container and Application	getConnection(user,password)	User of explicit getConnection(user,psw)
Both Container and Application	getConnection() without user and password	**Default user defined :** Default user defined on datasource **Default user Not defined :** User of Servant Region

- Very different behaviour from that in WebSphere z/OS V4
- SynchtoOSThread is no longer available so userid comes from getConnection() or from the default set on the datasource definition
- You have to update manually the resources.xml to disable default userid/password (AdminConsole bug ?)
- This matches behaviour of WebSphere distributed
- Migration issue for J2EE 1.2 application in WAS z/OS V5

Redbooks ibm.com/redbooks

© Copyright IBM Corp. 2003. All rights reserved.

Notes

© Copyright IBM Corp. 2003. All rights reserved.

The difference is WebSphere.

IBM eserver zSeries