

WebSphere software

The leading software platform for on demand business

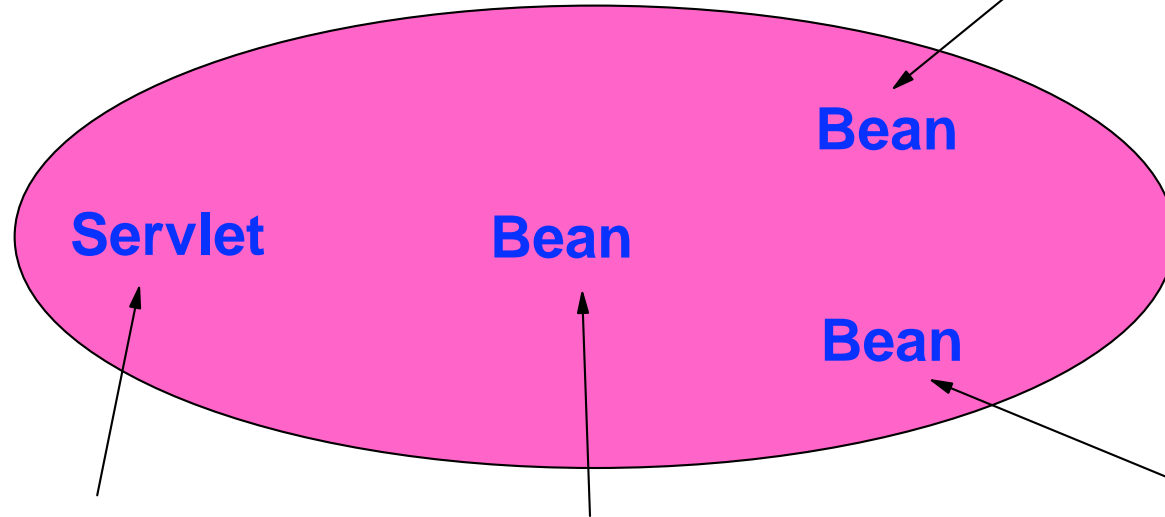


WebSphere for z/OS Security Advantage

IBM Americas Advanced Technical Support -- Washington Systems Center
Gaithersburg, MD, USA

- **Overview of WebSphere's security environment.**
- **Compare remote versus local environments.**
- **Discuss options for propagating an identity.**

J2EE Application Security Environment



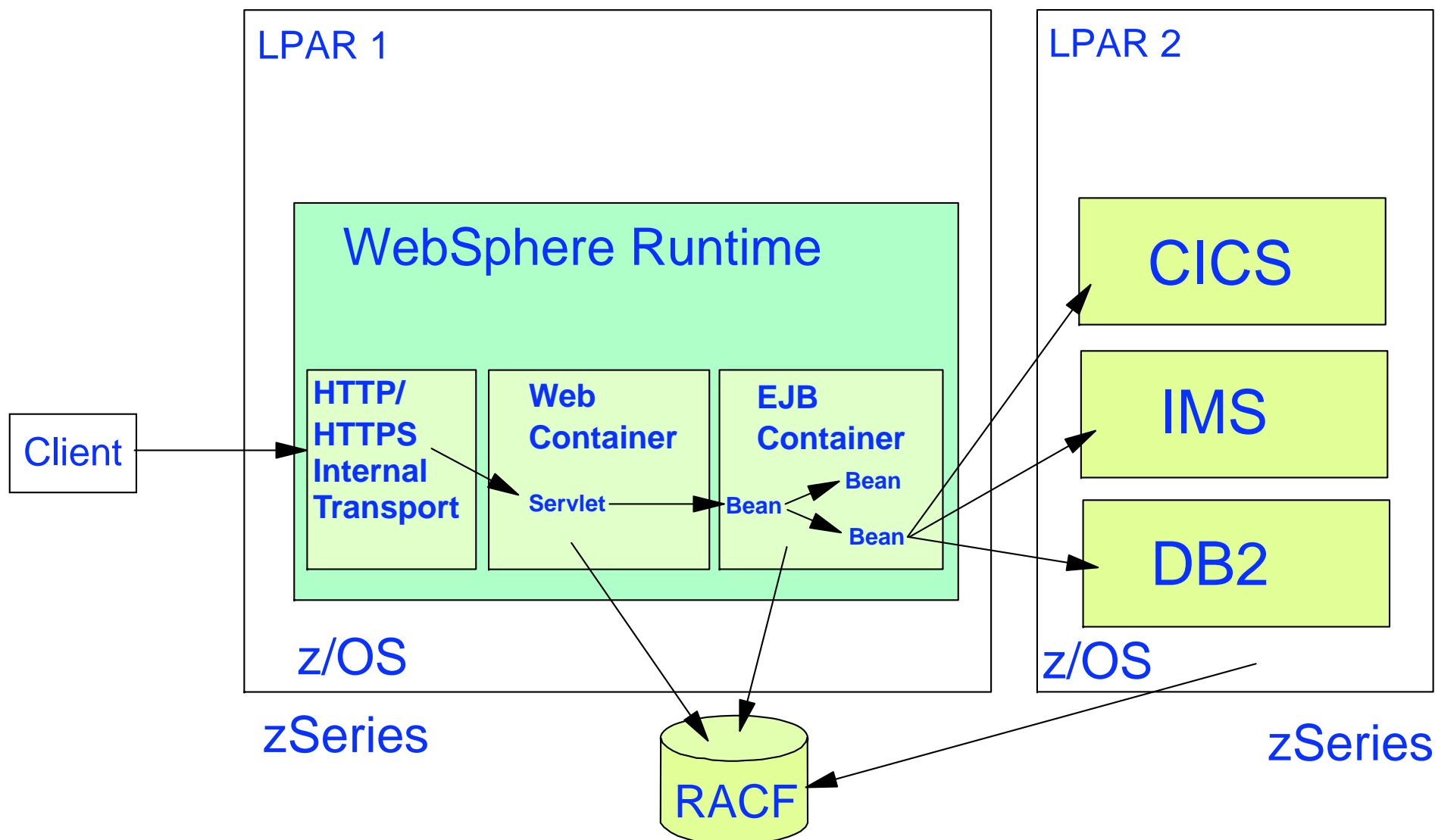
★ When an EJB method calls another method, a check is made to see if the method identity has the required role.

- ★ In most business applications, authentication of the client is required.
- ★ In order to run the application, the client must have the required role.
- ★ A Servlet typically runs with the identity of the client.

- ★ When a Servlet calls an EJB method, a check is made to see if the Servlet identity has the required role.
- ★ EJB methods can run with the identity of the Caller, the Servant's identity or an identity associated with a role.

- ★ Connectors provide a standard way to communicate with existing information systems like DB2, CICS and IMS.
- ★ When an EJB method uses a connector, an identity is provided.
- ★ The identity depends on the type of connector being used.

WebSphere V5/V6 'Remote' Environment

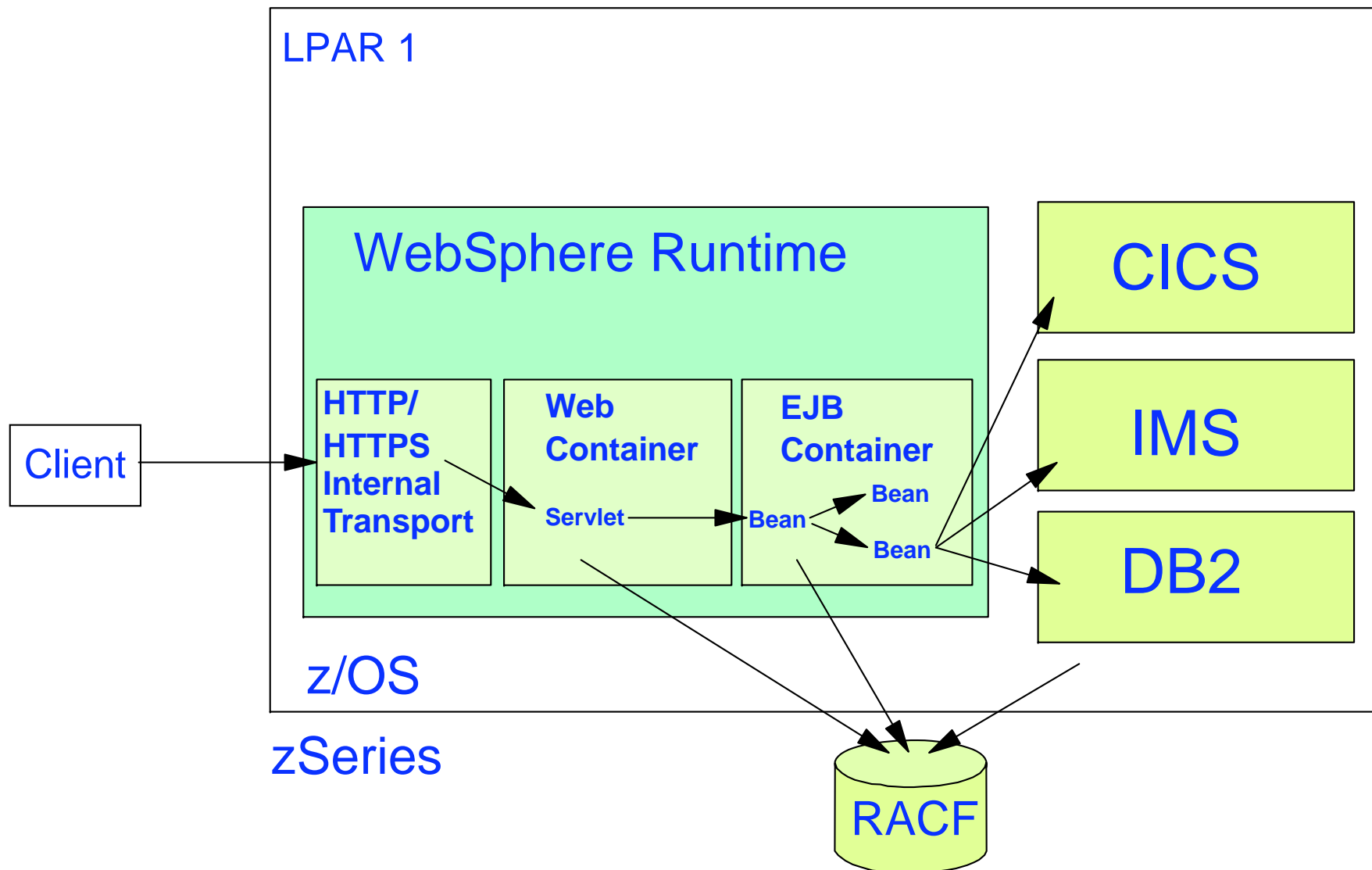


Propagating Identities using Connectors



- **If WebSphere is remote to CICS, IMS or DB2, you can**
 - ▶ Define a Userid and Password in an Authentication Alias.
 - Frowned upon by mainframe security auditors.
 - 1 userid/password per Alias = no security granularity.
 - ▶ Develop applications that perform Client authentication, saving the userid/password and passing it with connection requests.
 - Really frowned upon by mainframe security auditors.
 - Applications shouldn't be handling user passwords.

WebSphere V5/V6 'Local' Environment



Propagating Identities using Connectors

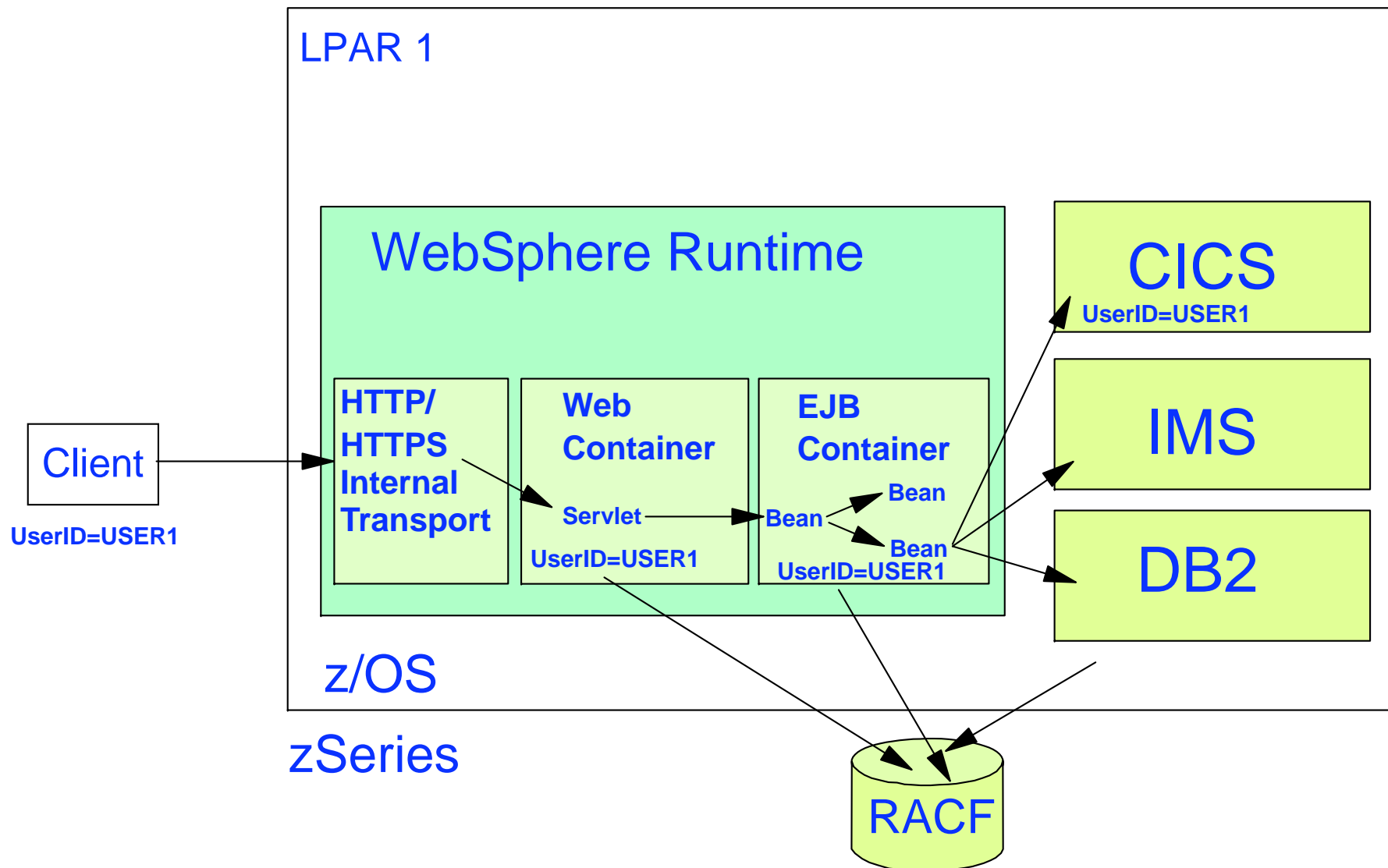


- **If WebSphere is local to CICS, IMS or DB2, you can**
 - ▶ Define a Userid and Password in an Authentication Alias.
 - Again, frowned upon by mainframe security auditors.
 - ▶ WebSphere can pass the identity of the Client, the Servant Region, or an identity associated with a role.
 - No password required.
 - Enables passing the client's identity to CICS, DB2 or IMS for downstream security checks.
 - Leverages legacy security protection.
 - e.g. WebSphere to CICS utilizes MRO security.
 - Connector request is cross memory, versus cross network.

WebSphere V5/V6 'Local' Environment



Example:



Summary

- **Putting WebSphere in the same LPAR as CICS, IMS or DB2 provides more options for passing a user identity to the backend server.**
- **This is due to the specialized function found in Type 2 connectors.**
- **Benefits include:**
 - ▶ More Granular Security.
 - ▶ Better Auditing.
 - ▶ Fewer passwords exposed.