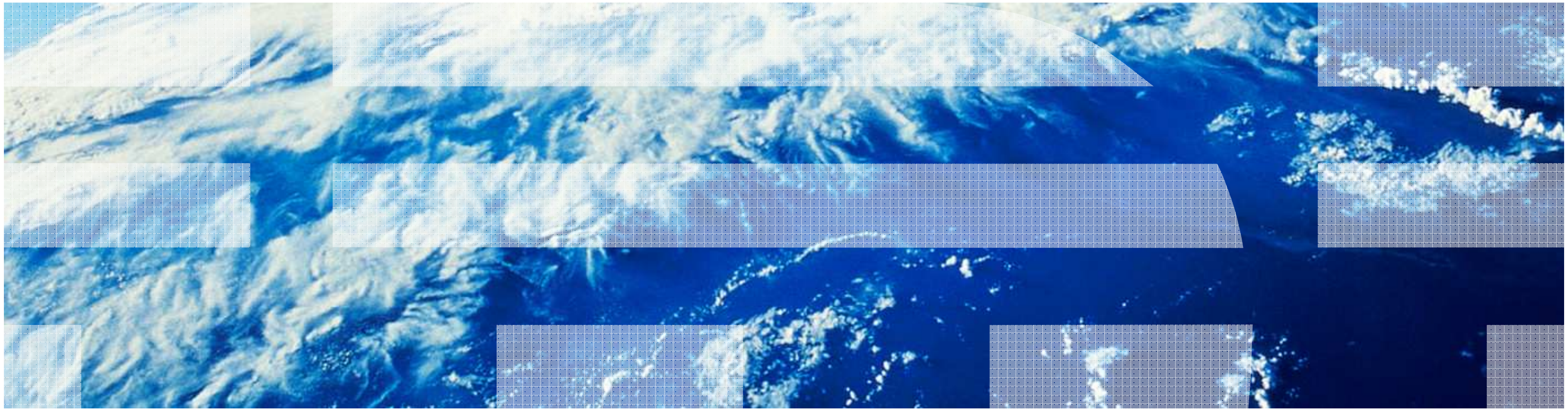
RACF® Identity Propagation on z/OS®
Who Are You?

Mark Nelson
SHARE Session 8352
z/OS Security Server (RACF) Design and Development. IBM Poughkeepsie
markan@us.ibm.com



© 2011 IBM Corporation

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Java and all Java-based trademarks are 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.

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

© 2011 IBM Corporation

Agenda

- **Identities on z/OS**
  - –Building and managing security environments (ACEEs)
    - Tokens, RACOs, etc.
    - DB2 Trusted Context
    - Digital Certificates to establish identities
- **z/OS V1.11 Identity Propagation**
  - –**New constructs:** IDID, ICRX
  - –**New command:** RACMAP
  - –**Updated APIs:** RACROUTE REQUEST=VERIFY, InitACEE, R_cacheserv
  - –**New functions:** ENF Signals
  - –**New logging:** SMF records

© 2011 IBM Corporation

Identity on z/OS

- **Every job, started task, or transaction on z/OS has associated with it an identity**
  - A 1 to 8 character string called the User ID
- **The Accessor Environment Element (ACEE) is the z/OS control block which represents a user’s identity.**
  - It contains the user ID and other related information used in establishing the identity of the user and the user’s credentials
- **ACEEs are created by the external security manager (RACF) on request by resource managers, such as UNIX System Services, JES, CICS, IMS, etc.**
  - Using z/OS SAF APIs such as RACROUTE REQUEST=VERIFY and InitACEE

© 2011 IBM Corporation

Identity on z/OS

- **ACEEs can exist in several places:**
  - –Associated with the address space (ASXBACEE)
  - –Associated with a task (TCBSENV)
  - –“Free floating” within an address space
- **When resource managers make access control checks they can:**
  - –Specify what ACEE is to be used in the check
  - –Use the “default” ACEEs, which checks
    - The task-level ACEE first. If there is none, then
    - The address-space level ACEE

© 2011 IBM Corporation

Identity on z/OS

- **There are other z/OS blocks which can be used to build an ACEE:**
  - **TOKEN**: The TOKEN is an 80-byte value which can be used to represent a user
    - Contains a user ID, default group ID, and some credential information
    - Can be used to build an ACEE (using APIs such as RACROUTE REQUEST=VERIFY) but:
      - Should be done on a system sharing the RACF database
      - Will require I/O
  - **RACF Environment Object ("RACO"):** A "flattened" ACEE which can be transported from one address space to another address space and reconstituted into an ACEE
    - Can be used across MVS images
    - Should have a shared RACF data base

© 2011 IBM Corporation

Identities from Outside z/OS

- **Not all parts of all applications are on z/OS**
  - –When connecting to z/OS, these applications often use an “application identity” using a “hard-coded” user ID (and sometimes a “hard-coded” password)
  - –These applications often perform identification and authentication
  - –The end user identity is not passed in to z/OS

© 2011 IBM Corporation

Identity Mapping on z/OS

- **z/OS has several mechanisms to with these client identities**
  - DB2 has the Trusted Context and roles
  - SSL has two-part authentication with digital certificates
  - Kerberos principal and realms
  - … and now with z/OS V1.11 we have identity propagation on z/OS

© 2011 IBM Corporation

DB2: Trusted Context and Roles

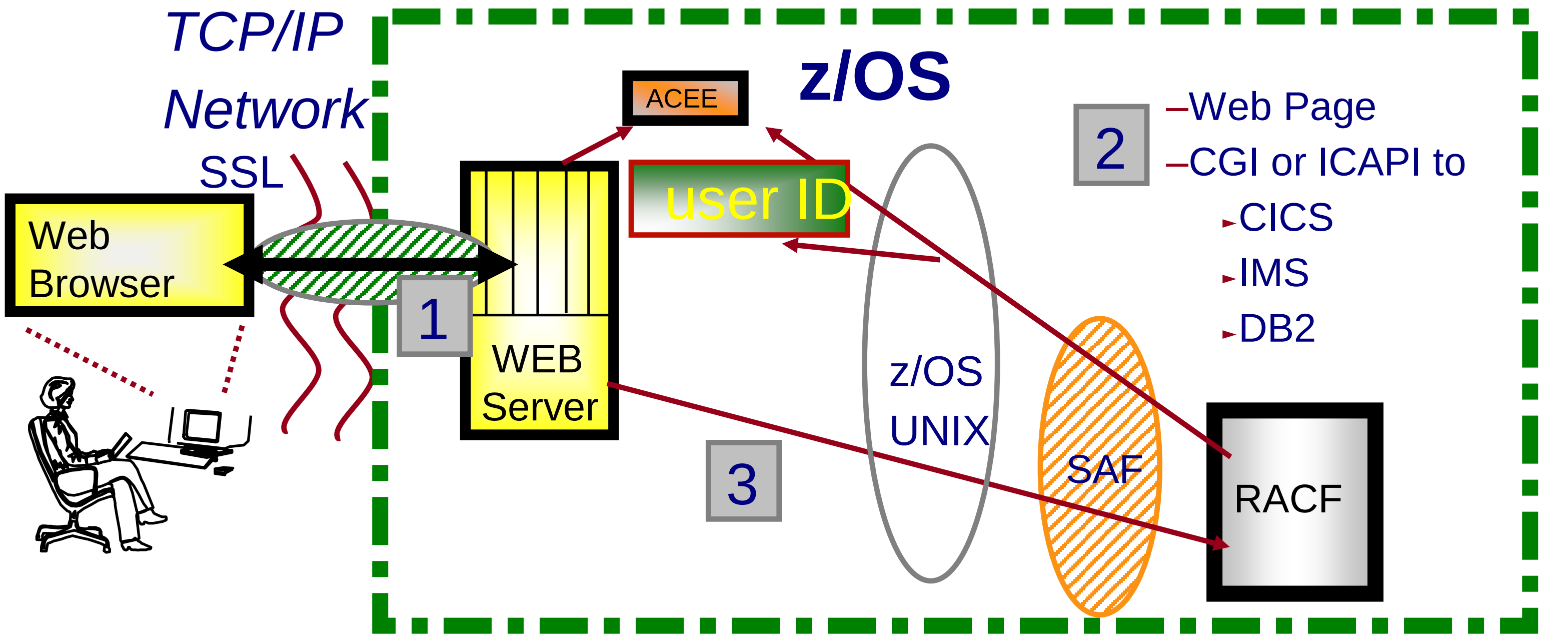
- **DB2 V9 introduces a new authorization mechanism: The ROLE**
  - 1 to 128 character identifier
  - Assigned to a connection using the DB2 TRUSTED CONTEXT
  - Assignment based on characteristics of the connection
    - Source user ID (with or without authentication)
    - Source of the connection (IP address, domain name, SERVAUTH)
    - Encryption level of the connection

- **ROLEs can be:**
  - Used for authorization
    - GRANT READ ON USER01.USER_BASIC_DATA TO ROLE TELLER
  - Owners of objects

- **Supported in RACF with:**
  - WHEN(CRITERIA(SQLROLE(….))
  - REQUEST=FASTAUTH, CRITERIA=, AUTHCHKS=

© 2011 IBM Corporation

Identification and Authentication Using Certificates



1- User authenticates to Secured Sockets Layer (SSL)

2- User requests OS/390 secured resource via browser

3- Web Server invokes RACF via z/OS UNIX System Services to build local security context (ACEE),

passing SSL validated certificate instead of prompting for user ID & password

© Copyright IBM Corporation, 1997, 2000

© 2011 IBM Corporation

Mapping Digital Certificates to User IDs

- **Digital certificates can be mapped to user IDs in one of two ways:**
  - One to one mapping, where the certificate has been loaded into the RACF data base and when that certificate is presented it is mapped to the specified user ID.
    - The certificates are mapped using the issuer's distinguished name, subject's distinguished name, and certificate serial number.
  - Many to one mapping, where the certificate is not in the RACF database, but the rules for mapping certificates to user IDs are.
    - The certificates are mapped based on the issuer's distinguished name and/or subject's distinguished name
- **The certificates are loaded into the RACF database and the mapping rules defined using the RACDCERT Command**
- **The issuer's distinguished name and subject's distinguished name appear in all of the RACF SMF records created. This provides end-user accountability.**

RACF Identity Propagation

- **With z/OS V1.11, RACF introduced a set of constructs and services which allow:**
  - The mapping of arbitrary user identities and realms/domains into RACF z/OS user IDs
    - Mapping based on user identity and domain name
    - Supports both one-to-one mapping and many-to-one
  - The recording of the distributed user's identity in RACF log records
  - Similar in concept to the digital certificate support, but not constrained to just digital certificates

© 2011 IBM Corporation

RACF Identity Propagation: New Constructs

- **z/OS V1.11 Identity Propagation introduces these new constructs:**
  - **IDID:** Distributed [user] Identity Data
    - A new control block which can contain:
      - Distinguished Name of user, UTF-8, maximum length 246 bytes
      - Registry Name, UTF-8, maximum length 255 bytes
      - Other security information
    - Created by RACF or caller of RACF
    - Pointed to from the ACEE (ACEEIDID)
    - If present in an ACEE, will be used to place end-user domain and user ID information in log records created by RACF

© 2011 IBM Corporation

RACF Identity Propagation: New Constructs

- **z/OS V1.11 Identity Propagation introduces these new constructs:**
  - **ICRX:** Identity Context Reference Extended.
    - An extended version of the Identity Context Reference (ICR).
      - The ICR may or may not be set.
    - Created by RACF or caller of RACF
    - Used to cache and retrieve an identity
      - Uses the R_cacheserv support from RACF in z/OS V1.8
    - Input for RACROUTE REQUEST=VERIFY/VERIFYX
  - **RACMAP**: New RACF command to create distributed identity mapping rules (more on RACMAP in a moment)

© 2011 IBM Corporation

RACF Identity Propagation: New Constructs

- **z/OS V1.11 Identity Propagation introduces these new constructs:**
  - **IDIDMAP:** New RACF General Resource Class
    - Contains the distributed identity to z/OS user ID mapping rules
    - Can be managed only using RACMAP commands
  - **ENF Signal:** New ENG signal (ENF Event Code 71) for certain profile changes
    - CONNECT
    - REMOVE
    - ALTUSER REVOKE

© 2011 IBM Corporation

RACF Identity Propagation: New APIs

- **z/OS V1.11 Identity Propagation introduces these new RACROUTE REQUEST=VERIFY/VERIFYX keywords**
  - –New parameters on RACROUTE REQUEST=VERIFY/VERIFYX
    - ICRX=icrx address
      - –The ICRX may or may not contain a reference to a cached user identity (ICR)
    - IDID=idid address
  - –When an ICRX contains an identity context reference (ICR) then RACF uses that reference to extract the RACO for the user ID for which the REQUEST=VERIFY is being done
    - If successful, an ACEE is inflated from the RACO. The IDID reference within the ICRX is ignored. The one to be used is in the RACO.
  - –If the ICRX does not contain an ICR or the ICR cannot be resolved RACF uses the IDID and the identity filters to find the correct user ID and create the ACEE
  - –The IDIDMAP class must be active and RACLISTEd.

© 2011 IBM Corporation

RACF Identity Propagation: New APIs…

- **z/OS V1.11 Identity Propagation introduces these new RACROUTE REQUEST=VERIFY/VERIFYX abend reason codes:**
  - Abend283 (RACROUTE REQUEST=VERIFY parameter list error) has two new reason codes:
    - 6C = ICRX block is not valid.
      - Either the eyecatcher value or length values were not valid, or the ICRX parameter was specified with the IDID, ICTX, NESTED=COPY, or NESTED=YES parameter.
    - 70 = IDID block is not valid.
      - Either the ID value, subpool or length values were not valid, or the IDID parameter was specified with the ICTX, NESTED=COPY, or NESTED=YES parameter

© 2011 IBM Corporation

RACF Identity Propagation: New APIs…

- **InitACEE:** A new parameter has been added to InitACEE. The IDID parameter points to an IDID data structure which contains information about the distributed user's identity.

```
CALL IRRSIA00 (Work_Area,
               ALET, SAF_Return_Code,
               ALET, RACF_Return_Code,
               ALET, RACF_Reason_Code,
               Function_Code, Attributes, RACF_UserID,
               ACEE_Ptr, APPL_ID, Password,
               Logstring, Certificate, ENVR_In, ENVR_Out,
               Output_Area, X500 name, Variable_List,
               Security_Label, SERVAUTH_Name,
               Password_Phrase,
               IDID_Area )
```

  - If the function code is "create an ACEE" and there is no user ID specified then the IDID_Area is used along with the IDIDMAP filters to find the correct user ID and create an ACEE (which will contain the specified IDID information)

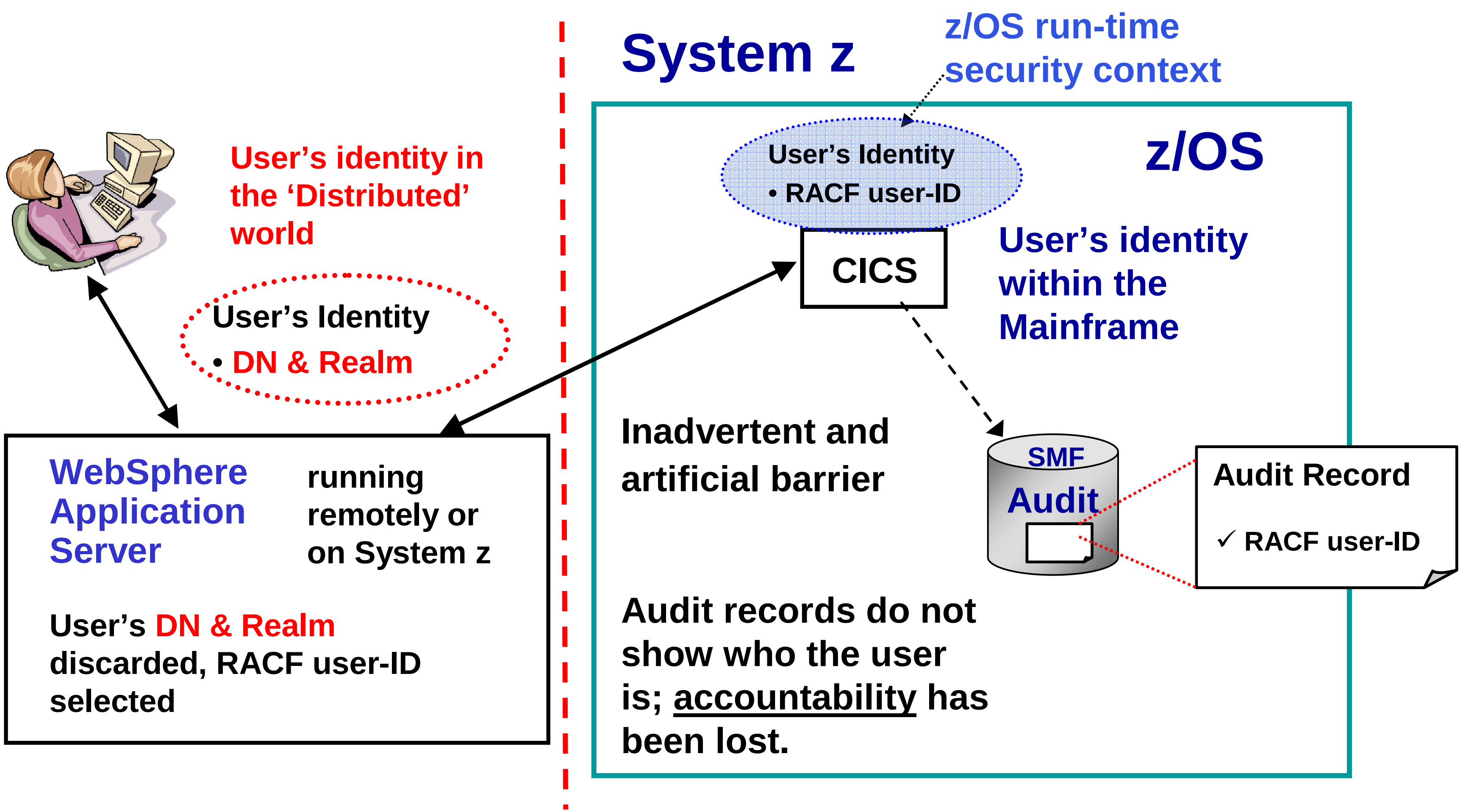
© 2011 IBM Corporation

RACF Identity Propagation: New APIs…

- **R_cacheserv:** R_cacheserv has been enhanced with new function code 7 (manage an extended read/write cache), which will have 3 options
  - ***Option 1*** (store data and return ICRX) will return an extended reference using a new ICRX parameter. It will use the ACEE as the source record and create a record name from the IDID pointed to by the ACEE. A cache reference will be created for the new record, and its ICR will be returned in an ICRX along with the IDID and RACF user ID.
  - ***Option 2*** (retrieve application data) will behave in a similar way to function code 6 option 4 (retrieve application data).
  - ***Option 3*** (remove record) will behave in a similar way to function code 6 option 5 (remove record) if an ICR is set in the ICRX. It will mark a data record as no longer valid if an IDID is provided in the ICRX with a non-set ICR.

© 2011 IBM Corporation

Identity Propagation Without Identity Propagation



User's identity in the 'Distributed' world

User's Identity
- DN & Realm

WebSphere Application Server

running remotely or on System z

User's DN & Realm discarded, RACF user-ID selected

System z

z/OS run-time security context

z/OS

User's Identity
- RACF user-ID

CICS

User's identity within the Mainframe

Inadvertent and artificial barrier

SMF Audit

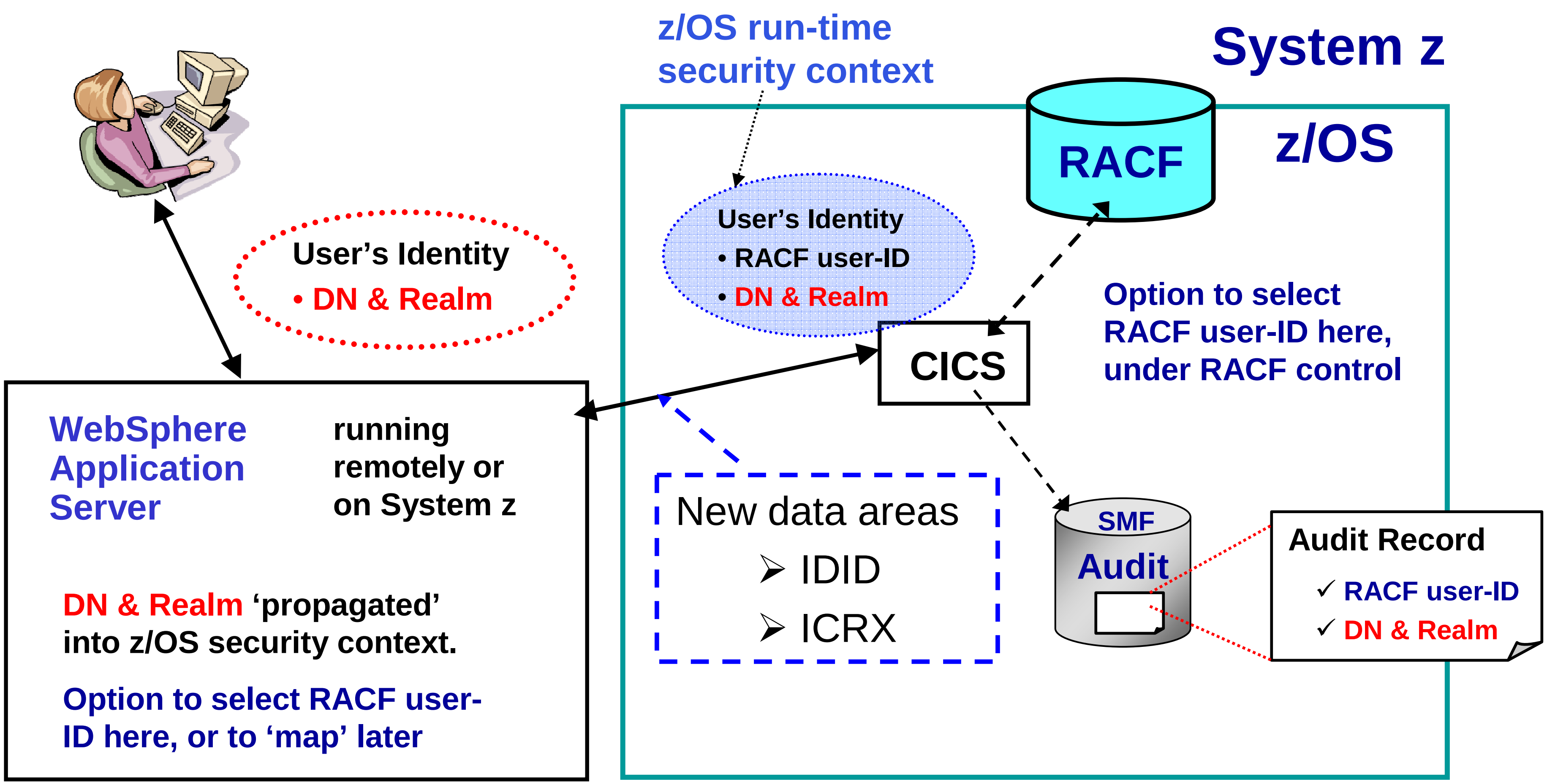
Audit Record

✓ RACF user-ID

Audit records do not show who the user is; <u>accountability</u> has been lost.

© 2011 IBM Corporation

Identity Propagation with z/OS Identity Propagation



z/OS run-time security context

System z

z/OS

RACF

User's Identity
- DN & Realm

User's Identity
- RACF user-ID
- DN & Realm

CICS

Option to select RACF user-ID here, under RACF control

WebSphere Application Server

running remotely or on System z

DN & Realm 'propagated' into z/OS security context.

Option to select RACF user-ID here, or to 'map' later

New data areas
- ➢ IDID
- ➢ ICRX

Audit Record
- ✓ RACF user-ID
- ✓ DN & Realm

© 2011 IBM Corporation

RACF Identity Propagation: Administrative Controls

- **RACMAP:** The RACMAP command is a new RACF command which:
  - Can be used to define, list and delete a distributed user identity mapping, also called a distributed identity name filter.
    - Creates profiles in the IDIDMAP class
    - Used to map the distributed identity to a user ID
    - Can create a one-to-one mapping or a many-to-one mapping
    - A user ID is found by comparing the user’s distributed name from the Distributed Identity Data structure (IDID) with the filter value used to create the IDIDMAP profile.

- **RACMAP Syntax:**

```
RACMAP  [ID(mapped-to-userID)]
         MAP
             USERDIDFILTER(NAME(’distributed-identity-username-filter’))
             REGISTRY(NAME(‘distributed-identity-registryname’))
             [WITHLABEL(’label-name’)]
       | DELMAP[(LABEL('label-name'))]
       | LISTMAP[(LABEL('label-name'))]
```

© 2011 IBM Corporation

RACMAP: Examples

```
RACMAP  MAP
    ID(MARKN)
    MAP
    USERDIDFILTER(NAME('UID=MNELSON,CN=Mark Nelson,O=BobsMart,C=US‘)
    REGISTRY(NAME('ldaps://us.bobsmarturl.com'))
    WITHLABEL('Map for Mark')

RACMAP  MAP
   ID(BOBDFLT)
   MAP
   USERDIDFILTER(NAME('O=BobsMart,C=US'))
   REGISTRY(NAME('ldaps://us.bobsmarturl.com'))
   WITHLABEL('BobMart Default')
```

- **These commands map ‘Mark Nelson’ from the us.bobsmarturl.com registry to the user ID MARKN and everyone else to the user ID BOBDFLT.**

© 2011 IBM Corporation

RACMAP LISTMAP

- **RACMAP LISTMAP shows the mapping for a user ID.**

```
RACMAP LISTMAP(LABEL('Map for Mark'))


Mapping information for user MARKN:


  Label: Map for Mark
  Distributed Identity User Name Filter:
    >UID=MNELSON,CN=Mark Nelson,O=BobsMart,C=US<
  Registry Name:
    >ldaps://us.bobsmarturl.com<


READY
```

© 2011 IBM Corporation

RACF Identity Propagation: Administrative Controls

- **RACMAP Authorization requires that the user have one of the following:**
  - SPECIAL authority
  - Have sufficient authority to the **IRR.IDIDMAP.*function*** resource in the FACILITY class, where *function* is MAP, DELMAP or LISTMAP.
    - To create, delete or list a mapping associated with your own RACF user ID, READ authority or higher is needed. To create, delete or list a mapping associated with another user's user ID requires UPDATE or higher authority.

© 2011 IBM Corporation

RACF Identity Propagation: Logging Enhancements

- **A new event code [87(x’57’)] has been introduced to audit the RACMAP command. The command will be audited based on UAUDIT, SETR SAUDIT, SETR AUDIT(USER), and SETR CMDVIOL**.

- **Existing event code 1 (RACINIT) and 67 (InitACEE) have a new qualifier to describe the failure that results when the distributed identity in the IDID cannot be mapped to a RACF user ID**.

- **The IDID information (domain and user ID) information has been added to the appropriate these SMF records**
  - RACF SMF type 80 records (all, except 68,71,79,81, and 82)
  - RACF SMF type 83 records subtytpe 2 and above records
  - IDID information is in UTF-8

- **The RACF SMF Unload (IRRADU00) and RACF Database Unload (IRRDBU00) utilities have been updated to support these new SMF and database records.**
  - IDID information is in EBCDIC

© 2011 IBM Corporation

RACF Identity Propagation: Cache Controls

- The RACF command processors **CONNECT**, **REMOVE**, and **ALTUSER** (when the **REVOKE** option has been specified), will issue a new ENF signal (71) to alert listeners to a possible change in a user’s group authorizations.
- Subsystems can also listen for this signal and use it to clean up cached data.

© 2011 IBM Corporation

New/Changed Messages

- Additional text for message **ICH408I**
  - **ICH408I** DISTRIBUTED IDENTITY IS NOT DEFINED: *distributed-identity-information*

- A new DELUSER message is issued if a related IDIDMAP profile is found when deleting a user
  - **ICH04018I** *userid* cannot be deleted. Distributed identity mapping profiles are associated with this user.

© 2011 IBM Corporation

New Messages - RACMAP command

- **IRRW201I** You are not authorized to issue the RACMAP command.
- **IRRW202I** The user ID specified is not defined to RACF.
- **IRRW203I** Unexpected ICHEINTY error encountered during command processing. ICHEINTY RC = x'*RetCode*', ICHEINTY RSN = x'*RsnCode*'.
- **IRRW204I** No information was found for user *User-Id*.
- **IRRW205I** Additional information is required to identify the identity mapping.
- **IRRW206I** No matching identity mapping found for this user.
- **IRRW207I** Unexpected RACROUTE REQUEST=Request-Type error encountered during command processing. SAF RC = x'*RetCode*', RACF RC = x'*RetCode*', RACF RSN = x'*RsnCode*'.
- **IRRW208I** The label *Label-Name* is already in use.
- **IRRW209I** The filter already exists. It cannot be added.
- **IRRW210I** RACLISTed profiles for the IDIDMAP class will not reflect changes until a SETROPTS RACLIST REFRESH is issued.
- **IRRW211I** Registry information is required.
- **IRRW212I** Distributed user identity information is required.
- **IRRW213I** Unexpected error occurred while converting from EBCDIC to UTF-8 the data for the *KeyWord-Name* keyword.

© 2011 IBM Corporation