

z/OS V1R8 Remote Services

Remote Auditing

Remote Authorization

RACF Identity Cache



Prepared by Patrick Kappeler
IBM Consulting IT Specialist
kappeler@fr.ibm.com

Redbooks
International Technical Support Organization

© 2007 IBM Corporation

z Security Update

Trademarks

See url <http://www.ibm.com/legal/copytrade.shtml> for a list of trademarks

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

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

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the 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.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- EIM ICTX LDAP backend
- Remote Authorization
- Remote Auditing
- z/OS Identity Cache

z/OS Remote Services

New set of functions at z/OS V1R8, and above, that address

Remote SAF auditing and authorization

- Consolidation of security authorization and auditing functions on the z/OS platform
 - Allow off-platform clients to query a z/OS system to check a users authority to a resource
 - Consolidate audit data across the enterprise by remotely writing audit records to the z/OS System Management Facility (SMF)

An infrastructure to ease implementing end-to-end identity propagation solutions


- A z/OS identity cache with a Java API
- Related SAF interface and audit enhancements

The services are provided to remote systems via the LDAP protocol, with

- The ITDS for z/OS LDAP server on the serving z/OS
- The new ICTX backend
- The LDAP client must support LDAP extended operations and DER encoding/decoding (Java, OpenLDAP, .. Clients)

These functions are documented in the z/OS EIM book:

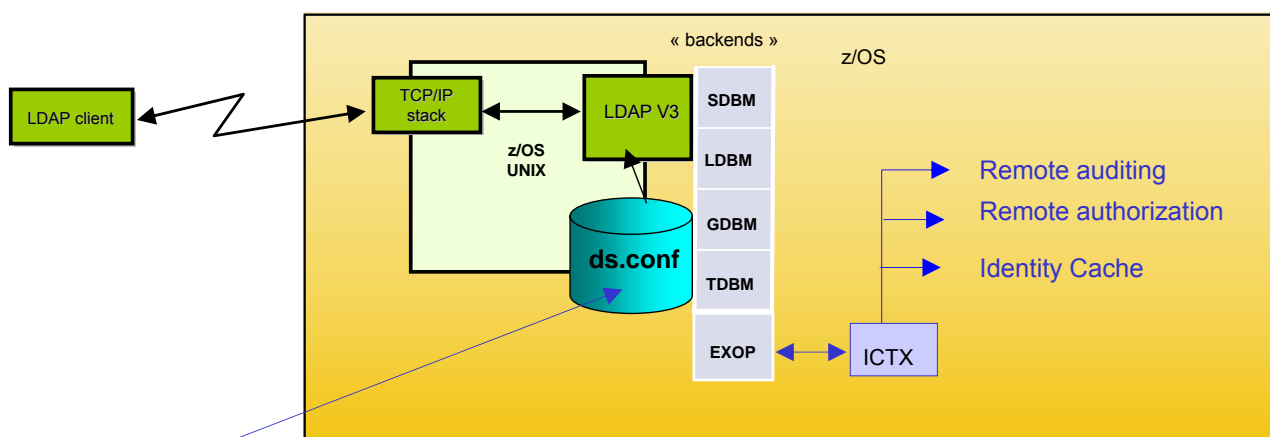
z/OS Integrated Security Services Enterprise Identity Mapping (EIM) Guide and Reference
 SA22-7875



The EIM ICTX LDAP Backend

The z/OS EIM ICTX Backend

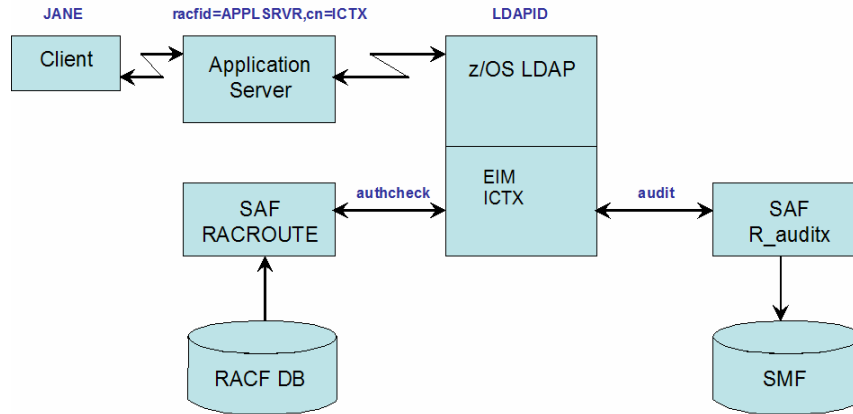
Extended operations (exop): extension mechanism to LDAP protocol that allows for new operations not already defined – A framework for any exops to be implemented in future



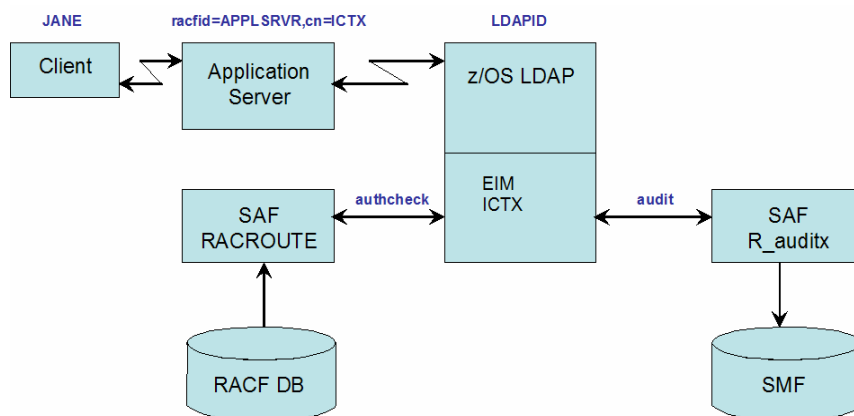
```
# ICTX extended operations support section
Database ictx ITYBIC31
suffix « cn=ictx »
```

Shipped in library SYS1.SIEALNKE

Clients perform an authenticated bind using their RACF userID
DN: racfid=<RACF userID>,cn=ictx with the RACF password



- JANE, APPLSRVR and LDAPID are users in the RACF Database
- The ICTX backend task is running under the LDAPID userID
- The remote auditing or authorization service is issued by userID APPLSRVR (that is the LDAP authenticated bind ID)
- APPLSRVR requests remote authorization test for subject user JANE, or remote creation of audit data

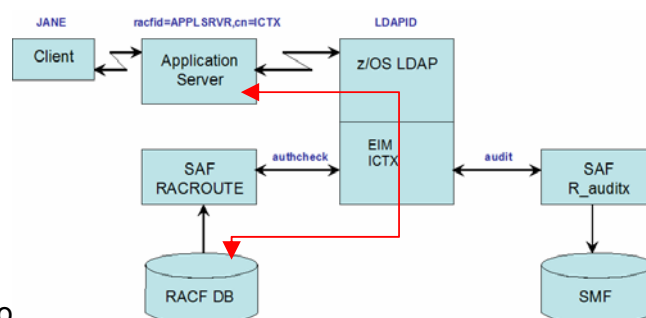


- Authorization check is performed by issuing the RACROUTE REQUEST=AUTH macro
- Remote auditing is done using the R_auditx (IRRSAX00) SAF callable service
Audit data are recorded in SMF records type 83 subtype 4

Remote Authorization and Auditing

Remote Authorization

Remote Authorization – Required Permissions



The issuing user (e.g. APPLSRVR) must be permitted to

IRR.LDAP.REMOTE.AUTH in the FACILITY class

ACCESS(**READ**)= the issuing user can request a check for its own authorizations

ACCESS(**UPDATE**) = the issuing user can request to check authorizations of another user

The issuing user is the user that was authenticated during the LDAP bind

Support for SECLABELS (see appendix)

Request's OID: 1.3.18.0.2.12.66

```

RequestValue ::= SEQUENCE {
  RequestVersion  INTEGER,
  ItemList       SEQUENCE OF
    Item          SEQUENCE {
      ItemVersion  INTEGER,
      ItemTag      INTEGER,
      User         IA5String,
      Resource     IA5String,
      Class        IA5String,
      Req. Access  INTEGER,
      LogString    IA5String
    }
}

```

Example

```

RequestVersion  1,
ItemVersion     1,
ItemTag         12,
User            BOB,
Resource        BANK.TELLER,
Class           EJBROLE,
Req. Access     0x01,
LogString       "Does Bob have
                READ access
                to EJBROLE
                BANK.TELLER"

```

RequestVersion: Overall version of the input data. The only allowable value is 1

ItemVersion: Version of data within the Item. The only allowable value is 1.

ItemTag: A number specified by the caller which will be returned untouched in the response. This can be used to match up which request items and their corresponding response items.

User: z/OS userid which is known to SAF. Any mapping of non-SAF userids to SAF userids must be performed prior to calling EIM ICTX.

Resource: SAF Resource

Class: SAF Class

Req. Access: What access is requested for the User to the Resource in the Class. Valid values are 0x01-Read, 02-Update, 0x03-Control, 0x04-Alter.

Logstring: Miscellaneous data which is added to the SAF authorization request which will appear in the log record for this Authorization request.

Response's OID: 1.3.18.0.2.12.67

```

Response ::= SEQUENCE {
  Version          INTEGER, - Version of Response
  ResponseCode     INTEGER, - Overall Return code of Response
  ItemList         SEQUENCE OF
    Item           SEQUENCE{
      ItemVersion  INTEGER, - Version of this Item
      ItemTag      INTEGER, - itemTag, copied from input
      MajorCode    INTEGER, - Main return code for item
      MinorCode1   INTEGER, - reason code
      MinorCode2   INTEGER, - reason code
      MinorCode3   INTEGER, - reason code
    }
}

```

Version – Version of this response structure. It is always 1

ResponseCode – Overall return code for the request. Usually, this will be the highest MajorCode from all of the items, unless there is a higher-severity error which prevents the Request from running.

Item – return code information corresponding to a single item in the request. There be a response item to match every item in the request.

itemTag – Copy of the itemTag of the corresponding request item.

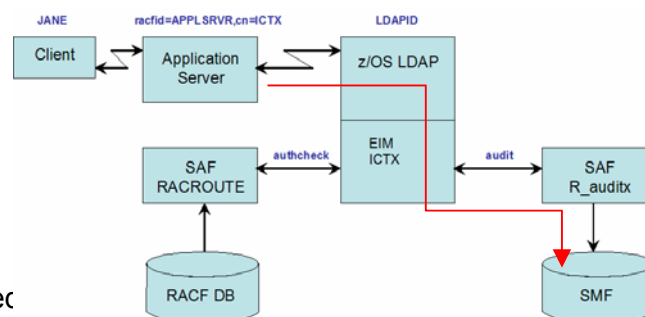
MajorCode – return code for this item (see appendix)

MinorCode1-3 – Additional reason codes (see appendix)

Remote Authorization and Auditing

Remote Auditing

Remote Auditing – Required Permissions



The issuing user (e.g. APPLSRVR) must be permitted

IRR.LDAP.REMOTE.AUDIT in the FACILITY class

ACCESS(**READ**)

The ITDS userID (e.g. LDAPID) must be permitted to

IRR.RAUDITX in the FACILITY class

ACCESS(**READ**)

The issuing user is the user that was authenticated during the LDAP bind

See the SMF unload data in the appendix

OIDs: request: 1.3.18.0.2.12.68, response: 1.3.18.0.2.12.69

```
RequestValue ::= SEQUENCE {
  RequestVersion INTEGER,
  ItemList       SEQUENCE OF
    Item         SEQUENCE {
      ItemVersion INTEGER,
      ItemTag     INTEGER,
      LinkValue   OctetString,
      Violation   Boolean,
      Event       INTEGER,
      Qualifier   INTEGER,
      Class       IA5String,
      Resource    IA5String,
      LogString   IA5String,
      DatafieldList SEQUENCE OF
        DataField SEQUENCE {
          TYPE   INTEGER,
          VALUE  IA5STRING
        }
      }
    }
}
```

example

```
RequestVersion 1,
ItemVersion 1,
ItemTag 15,
LinkValue 0x0102030405060708,
Violation TRUE,
Event 1,
Qualifier 0,
Class DATACLAS,
Resource BOB.DATA,
LogString "VIOLATION on BOB.DATA
TYPE 111,
VALUE "VALUE1"
TYPE 112,
VALUE "VALUE2"
```

RequestVersion: Overall version of the input data. The only allowable value is 1

ItemVersion: Version of data within the Item. The only allowable value is 1.

ItemTag: A number specified by the caller which will be returned untouched in the response. This can be used to match up which request items and their corresponding response items.

LinkValue: Binary data which will appear in audit record. Used to link together multiple audit records to a single transaction.

Violation: Is this event being recorded due to a Violation

Event: Event type

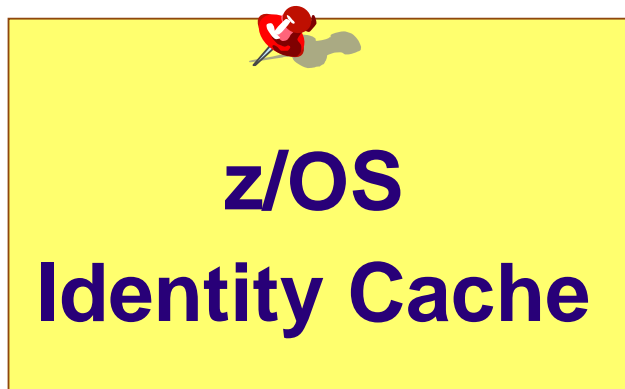
Qualifier: Event Qualifier

Class: SAF Class

Resource: SAF Resource

Logstring: Miscellaneous data which is added to the SAF audit request which will appear in the log record for this Audit request.

DataFields: Sequence of one or more data fields which add information to the audit record. Each data field has a numeric TYPE and some string VALUE.



An infrastructure put in place to ease solving the end-to-end user accountability and auditability problem

- ▶ z/OS is enhanced to provide an Identity Cache service
 - ▶ The Identity Cache infrastructure exploits SAF-RACF enhancements made to the R_cacheserv SAF callable service
 - ▶ The Identity Cache operational behavior can be specified in RACF profiles, including whether or not an identity mapping should occur

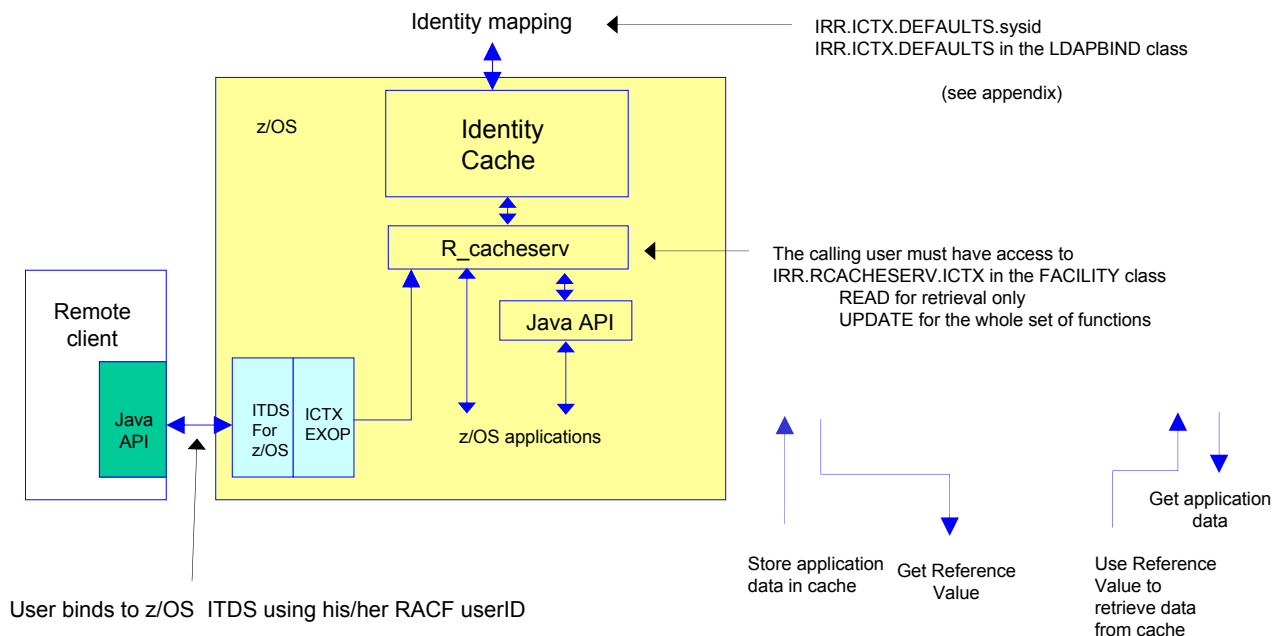
- ▶ A Java API is available for storing and retrieving identity information by local or remote applications
 - Primary API to access the cache - Alternatively R_cacheserv can be used
 - Operates remotely using the LDAP interface to the ITDS/ICTX backend
 - The API jar file is in the z/OS HFS: `/usr/lpp/eim/lib/ictx.jar`

Initially implemented at z/OS V1R3

- Roughly: a service which enables a task to create a cache of named data (in dataspace), readable by other tasks in the system, under RACF access control

Improved at z/OS V1R8

- Read/write cache, primarily intended now to cache user identity information (in a structured way)
- A reference value is returned on successful store operations
 - Used to later retrieve the data
 - One-time use only
 - With a specified life-time
- EIM, or another mapping mechanism, can be called to map identity data when stored in the cache

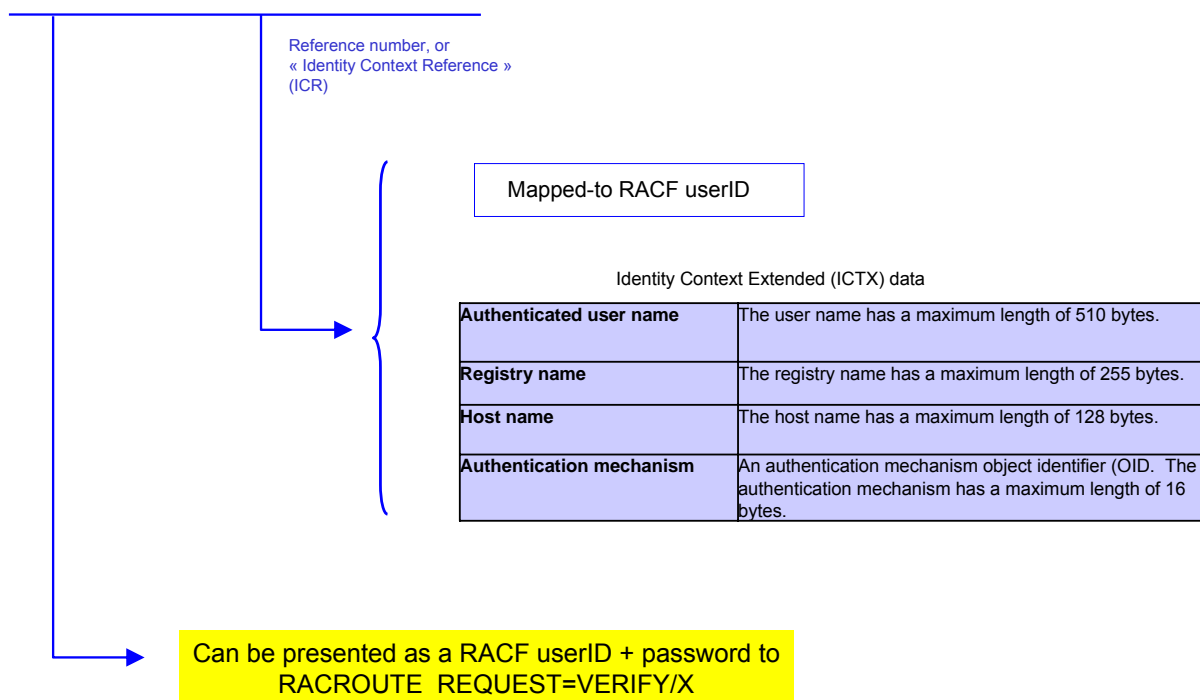


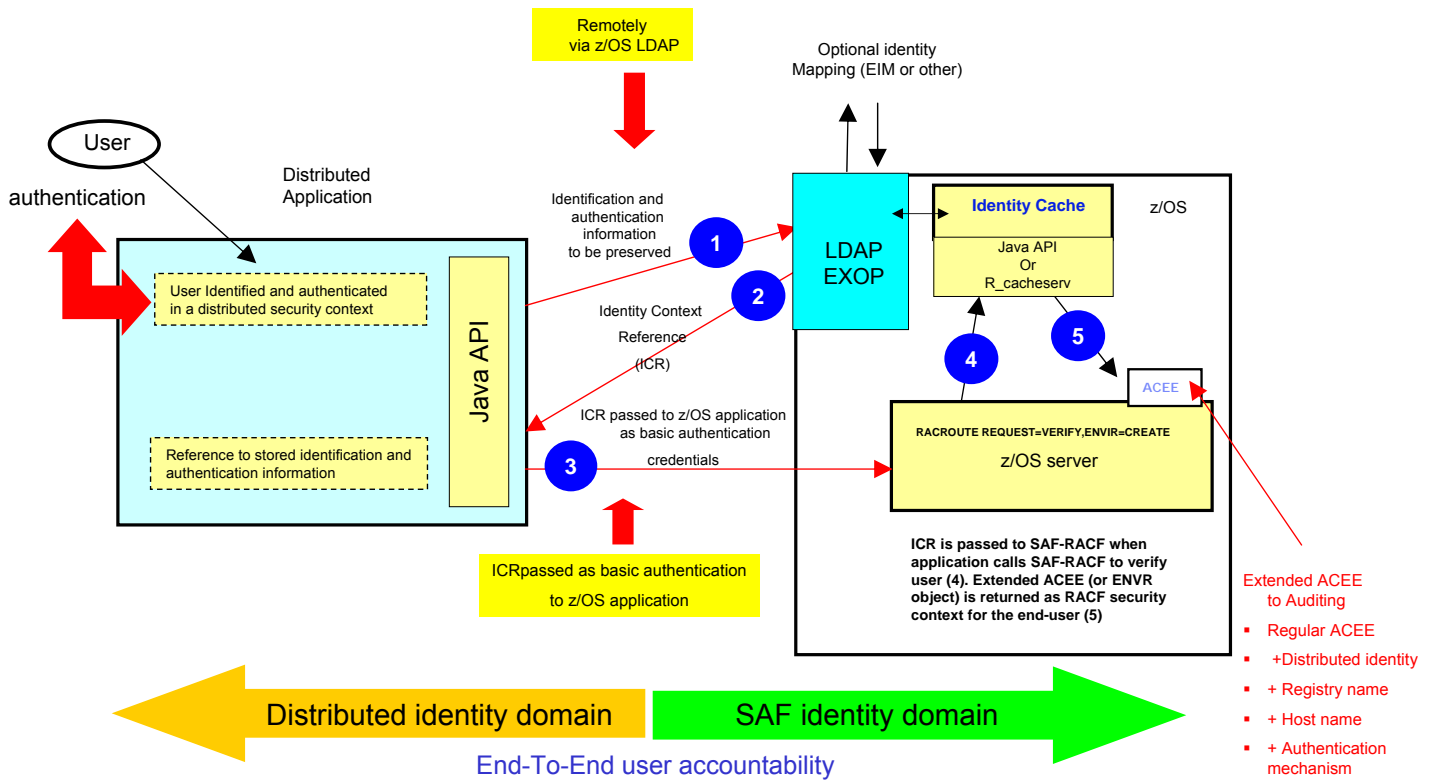
z/OS Security Server RACF Callable Services - SA22-7691

z/OS Integrated Security Services Enterprise Identity Mapping (EIM) Guide and Reference - SA22-7875

****nnXUSR + 8-byte random number**

(nn=system number in the Sysplex)

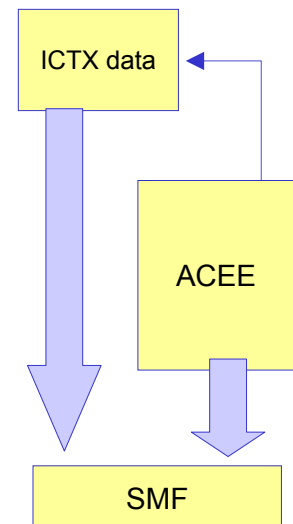




The RACROUTE REQUEST=VERIFY macro has been modified at z/OS V1R8

- Recognizes an 8-byte user ID with a prefix of "***" (X'5C5C') and an 8-byte password as an ICR
- RACF calls R_cacheserv to get the application data from the cache
RACF Sysplex communication is used if the cache is not local
- RACF builds an ACEE for the mapped-to userID, extended with the ICTX data (the "extended ACEE" points to an ICTX block)

When RACF builds an SMF record for any audit event (any, not just job initiation!) if the ACEE points to an ICTX block, the ICTX data are included in the SMF record



Thank You

Any Questions ?



Appendix

Affected Publications

- z/OS Integrated Security Services Enterprise Identity Mapping (EIM) Guide and Reference (SA22-7875)
- z/OS Security Server RACF Auditor's Guide (SA22-7684)

Remote Authorization – Security Labels Support

- The LDAP server can retrieve the SECLABEL which is assigned to the network connection with the client (parameter 'securityLabel=on' in ds.config)
- When RACROUTE REQUEST=AUTH is executed, this SECLABEL is used in the authorization decision
- Note: the SECLABEL is only used for the actual Remote Authorization request itself, it is not used to check whether the BIND user is authorized to use the remote services
This requires proper MLS profiles setup in RACF – Not addressed here

▪ Configuring the Identity Cache

▶ Identity Cache configuration (optional) is provided by RACF commands

```
-RDEFINE LDAPBIND IRR.ICTX.DEFAULTS
  ICTX( USEMAP | NOUSEMAP DOMAP | NODOMAP
        MAPREQUIRED | NOMAPREQUIRED
        MAPPINGTIMEOUT(0-3600))
```

▶ If USEMAP or DOMAP is used (or defaulted to), the EIM local registry needs to be defined

```
-RALTER LDAPBIND IRR.ICTX.DEFAULTS EIM(LOCALREGISTRY())
-SETROPS CLASSACT(LDAPBIND) RACLIST(LDAPBIND)
-Note: Same as IRR.EIM.DEFAULTS EIM(LOCALREGISTRY())
```

▶ If DOMAP is used, EIM needs to be configured

▶ If the Identity Cache will be accessed remotely

```
-z/OS V1R8 LDAP server required
-ds.conf defines ictx extended operations support
```

Remote Audit RACF SMF Unload Support

- Record type 83 subtype 4 for remote audit
- Both tabular and XML output formats
- Common type 83 subtype 2+ data
- Unique events and qualifiers

Event	Event String	Comments
1	*SAFAUTN	Authentication
2	*SAFAUTZ	Authorization
3	*SAFAUTM	Auhorization
4	*SAFKEYM	Mapping Key Management
5	*SAFPOLM	Policy Management
6	*SAFADMC	Administrator Configuration
7	*SAFADMA	Administrator Action

Qualifie r	Qualifier String	Comments
0	SUCCESS	Successful request / authorized
1	INFO	Information about an event
2	WARNING	Not a failure, but may warrant investigation.
3	FAILURE	Unsuccessful request / unauthorized

Remote Audit RACF SMF Unload Support (continued)

- Unique relocates 100 through 114

Relocate	DB2 Field Name	Type	Length	Start	End	Comments
100	SAF_LOCAL_USER	Char	8	3000	3007	SAF identifier for bind user
101	SAF_BIND_USER	Char	256	3010	3265	Requestor's bind user identifier
102	SAF_DOMAIN	Char	512	3268	3779	Originating security domain
103	SAF_REG_NAME	Char	256	3782	4037	Originating registry / realm
104	SAF_REG_USER	Char	256	4040	4295	Originating user name
105	SAF_MAP_DOMAIN	Char	512	4298	4809	Mapped security domain
106	SAF_MAP_REG_NAME	Char	256	4812	5067	Mapped registry / realm
107	SAF_MAP_REG_USER	Char	256	5070	5325	Mapped user name
108	SAF_ACTION	Char	64	5328	5391	Operation performed
109	SAF_OBJECT	Char	64	5394	5457	Mechanism / object name
110	SAF_METHOD	Char	64	5460	5523	Method / function used
111	SAF_KEY	Char	256	5526	5781	Key / certificate name
112	SAF_SUBJECT_NAME	Char	256	5784	6039	Caller subject initiating security event
113	SAF_DATE_TIME	Char	32	6042	6073	Date and time security event occurred
114	SAF_OTHER_DATA	Char	2048	6076	8123	Application specific data