IBM Education Assistance for z/OS V2R1

Item: Database Unload of Certificate DNs
Element/Component: RACF

Material is current as of April 2013

Agenda

- Trademarks
- Overview
- Usage & Invocation
- Appendix

Trademarks

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

Overview

- Problem Statement / Need Addressed
  - The RACF database unload utility (IRRDBU00) allows installations to create a sequential file from a RACF database which can be used in several ways, including upload to a database manager, such as DB2, to process complex inquiries and create installation-tailored reports
  - Prior to z/OS V2.1, IRRDBU00 did not unload information from the encoded digital certificate when writing the General resource certificate data record (0560)
  - Customers requested more information, such as the subject's distinguished name (DN), in order to monitor and check the use of digital certificates
- Solution
  - IRRDBU00 will parse the certificate and write a General resource certificate information record (1560) containing the subject's DN, the issuer's DN, and the hashing algorithm used for signing (e.g. SHA-256)
- Benefit / Value
  - This aids audit compliance by allowing searches against critical fields from a digital certificate

Usage & Invocation

- A new type of IRRDBU00 record will be provided
  - Today, record type values are formatted as PPSF, where PP = 01-05, for Group records, User records, etc. (0100 = Group Basic Data)
  - A record type prefix (PP) of 1n will now be used to identify extended field processing records (1560, for example)

Usage & Invocation

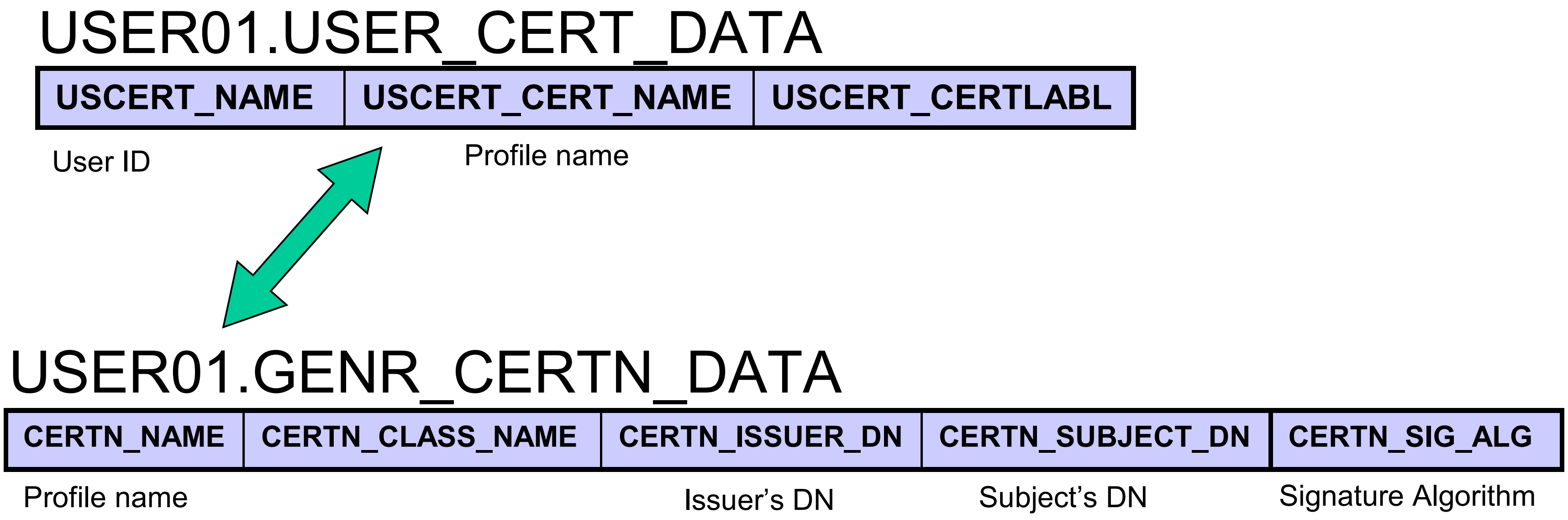
- Additional certificate values will be unloaded using type 1560 General Resource Certificate Information records, described in the following table

		Position		
Field Name	**Type**	**Start**	**End**	**Comments**
CERTN_RECORD_TYPE	Int	1	4	Record type of the certificate information record (1560).
CERTN_NAME	Char	6	251	General resource name as taken from the profile name.
CERTN_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs.
CERTN_ISSUER_DN	Char	262	1285	Issuer’s distinguished name. (1024 characters)
CERTN_SUBJECT_DN	Char	1287	2310	Subject’s distinguished name. (1024 characters)
CERTN_SIG_ALG	Char	2312	2327	Certificate signature algorithm. Valid values are md2RSA, md5RSA, sha1RSA, sha1DSA, sha256RSA, sha224RSA, sha384RSA, sha512RSA, sha1ECDSA, sha256ECDSA, sha224ECDSA, sha384ECDSA, sha512ECDSA, and UNKNOWN.

- See z/OS Security Server RACF Security Administrator's Guide for a description of IRRDBU00 and instructions on how to run it

Usage & Invocation

- Once loaded into DB2 tables, SQL queries can be used to join information, as shown in the following graphic



USER01.USER_CERT_DATA

USCERT_NAME	USCERT_CERT_NAME	USCERT_CERTLABL
User ID	Profile name	

USER01.GENR_CERTN_DATA

CERTN_NAME	CERTN_CLASS_NAME	CERTN_ISSUER_DN	CERTN_SUBJECT_DN	CERTN_SIG_ALG
Profile name		Issuer's DN	Subject's DN	Signature Algorithm

Appendix

- z/OS Security Server RACF Macros and Interfaces (SA23-2288)
- z/OS Security Server RACF Security Administrator's Guide (SA23-2289)