z/OS 3.2 IBM Education Assistant

Solution Name: RACF RACDCERT Certificate Generation and List Support of Multiple Altnames

Solution Element(s): z/OS Security Server RACF

July 2025

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Objectives (slide 1 of 8)

The Task:	Securing internet entities with digital certificates generated by z/OS Security Server RACF.
The Challenge:	In-service versions of RACF limit the specification of Subject Alternative Name values to *one* of each of the four supported types of names in a digital certificate in most cases. This limitation often requires RACF administrators to generate *multiple* digital certificates to secure the *same* internet entity. This often results in increased effort for the RACF administrator to generate, manage, and distribute these certificates to clients, and increased effort for internet entities to manage their certificates. In-service versions of RACF permit administrators to import digital certificates that specify multiple Subject Alternative Names generated by external certificate issuing authorities, but RACF can only list *one* value for any of the supported types of names. RACF also will not list some characteristics for these certificates that can be used to uniquely identify these certificates. This requires administrators to expend additional effort and perform additional tasks to determine the identifies asserted by digital certificates under RACF's control.

Objectives (slide 2 of 8)

The Objective:	Reduce the security administrative overhead of securing internet entities with certificates generated using z/OS Security Server RACF.
The Solution:	Extend z/OS Security Server RACF digital certificate services to permit the specification and display of multiple Subject Alternative Name values of the same type in the same RACF-generated digital certificate. Extend these same services to list all Subject Alternative Name values asserted by a digital certificate, and to display Subject Key Identifier and Authority Key Identifier information to reduce the effort required to uniquely identify and track digital certificates under RACF's control.

Objectives (slide 3 of 8)

Background

Internet entities use X.509 digital certificates to assert and prove that entity's identity. In an X.509 certificate, identity is asserted through the subject distinguished name (a.k.a. SDN).

Typically, in cases where an entity is an internet-facing server, identity is further asserted through the inclusion of subject alternative names (a.k.a. subject alternate names, altnames, or SANs).

- The SDN asserts "who" or "what" the entity is. Examples:
  - Bob Gensler, IBM, Poughkeepsie, NY, US
  - Some Company, East Hungadunga, NY, US
- The SANs asserts the valid, supported methods for connecting to a server. Examples:
  - Hostname www.someco.com
  - IP address 104.94.71.173
  - Home page http://www.someco.com/home.html

Objectives (slide 4 of 8)

Internet-facing servers are often reachable by multiple addresses and URIs to provide redundancy in case of an outage on any one network. They also often support multiple access methods, such as HTTP, FTP, and LDAP. For this reason, the X.509 specification permits the specification of multiple SANs in a digital certificate, so that one certificate may be used to assert and prove the identity of the server regardless of the internet address, hostname, or protocol used to contact it.

All in-service versions of RACF support four SAN types:

- Domain Name www.someco.com, service.someco.com
- Email Address info@email.someco.com, feedback@someco.com?subject=Widget
- IP Address 9.115.185.96, 2001:0db8:85a3::8a2e:0370:7334
- URI Name http://www.someco.com, ftp://downloads.someco.com

RACF permits security administrators to generate certificates using:

- A PKCS#10 Certificate Signing Request (CSR) that specifies the public key and (optionally) certificate attributes, including the SDN and SANs.
- Command options or callable service parameters.
- A combination of the two.

Objectives (slide 5 of 8)

Administrators sometimes need to locate X.509 digital certificates using specific key values if those keys become compromised. To assist with this effort, X.509 digital certificates can contain additional information.

- The Subject Key Identifier (OID 2.5.29.14) is a certificate extension containing a value derived from the certificate's public key using a cryptographic hash function. This extension provides a means for identifying a certificate containing the specific public key used in an application.
- The Authority Key Identifier (OID 2.5.29.35) is a certificate extension containing a value derived in a similar fashion, except that the certificate signer's public key is used. This value can help the user to find the issuer's certificate especially in the case when the issuer's certificate has been renewed with a different key pair.

Objectives (slide 6 of 8)

z/OS Security Server RACF provides these interfaces to generate X.509 certificates:

- The RACDCERT GENCERT command.
- The R_PKIServ Callable Service GENCERT Function SAF Path programming interface.

z/OS Security Server RACF provides these interfaces to query digital certificate information:

- The RACDCERT CHECKCERT command for X.509 certificate packages stored in datasets.
- The RACDCERT LIST and RACDCERT LISTCHAIN commands for digital certificates under RACF's control.

Objectives (slide 7 of 8)

For in-service versions of RACF, if the command options or callable service parameters are used to specify SAN values, only one SAN value of each type can be specified. This limits a RACF generated certificate to one SDN and a maximum of four SANs, one of each type. For instance, the certificate cannot contain more than one IP address SAN if the command options or callable service parameters are used to specify any SAN values, regardless of the content of the CSR.

For internet-facing servers that are reachable through multiple addresses or host names, this requires the security administrator to generate, manage, and distribute separate RACF certificates *per address or host name*.

To meet the objective: remove this limitation, and reduce the administrative overhead of securing internet entities, by allowing more than one SAN of any one type to be specified through command options and callable service parameters.

Objectives (slide 8 of 8)

For in-service versions of RACF, RACDCERT LIST, RACDCERT LISTCHAIN and RACDCERT CHECKCERT commands can display only the first SAN value of each type for a digital certificate. These commands also do not display the Authority Key ID or Subject Key ID extensions of a digital certificate. This limits the ability to see important details about certificates in RACF.

To meet the objective: enhance RACDCERT to display these additional certificate details to help the security administrator better understand the RACF digital certificate environment.

Overview

- Who (Audience)
  - z/OS security administrators who issue and manage certificates
  - z/OS system administrators who employ certificates to secure system entry points
- What (Solution)
  - Permit multiple Subject Alternative Names (SANs) of the same type to be specified for a z/OS Security Server RACF generated certificate via command options and callable service parameters.
  - Enhance RACDCERT list commands to display of multiple Subject Alternative Names (SANs) of the same type and display the subject key ID and authority key ID extensions.
- Wow (Benefit / Value, Need Addressed)
  - Reduce number of certificates required to secure a server.
  - Reduce number of certificates administered by z/OS administrators and their clients.
  - Reduce effort required to locate digital certificates using specific keys.
  - Remain competitive with existing certificate generation utilities.

Usage & Invocation (slide 1 of 15)

```
RACDCERT GENCERT [ (request-data-set-name) ]
   [ ID(certificate-owner) | SITE | CERTAUTH ]
   [ SUBJECTSDN( [ CN('common-name') ] [ T('title') ]
    [ OU('organizational-unit-name-1','organizational-unit-name-2',...) ]
    [ O('organization-name') ] [ L('locality') ]
    [ SP('state-or-province') ] [ C('country') ]
    ) ]
   [ SIZE(key-size) ]
   [ NOTBEFORE( [ DATE(yyyy-mm-dd) ] [ TIME(hh:mm:ss) ] ) ]
   [ NOTAFTER( [ DATE(yyyy-mm-dd) ] [ TIME(hh:mm:ss) ] ) ]
   [ WITHLABEL('label-name') ]
   [ SIGNWITH( [ CERTAUTH | SITE ] LABEL('label-name')) ]
   [ { RSA [ (PKDS [ (pkds-label | * ) ] | TOKEN(token-name) ) ]
    | NISTECC [ (PKDS [ (pkds-label | * ) ] | TOKEN(token-name) ) ]
    | BPECC [ (PKDS [ (pkds-label | * ) ] | TOKEN(token-name) ) ]
    | DSA
    | FROMICSF(pkds-label)
    } ]
   [ SIGATTR [ (RSAPSS) ] ]
   [ KEYUSAGE(
    [ CERTSIGN ] [ DATAENCRYPT ] [ DOCSIGN ] [ HANDSHAKE ] [ KEYAGREE ]
    ) ]
   [ ALTNAME(
    [ IP(numeric-IP-address) ]
    AIP(numeric-IP-address-1,numeric-IP-address-2,...) ]
    [ DOMAIN('internet-domain-name') ]
    [ ADOMAIN('internet-domain-name-1','internet-domain-name-2',...) ]
    [ EMAIL('email-address') ]
    [ AEMAIL('email-address-1','email-address-2',...) ]
    [ URI('universal-resource-identifier') ]
    [ AURI('universal-resource-identifier-1','universal-resource-identifier-2',...) ]
    ) ]
```

RACDCERT GENCERT is extended.

The ALTNAME keyword of the RACDCERT GENCERT command is extended to support four new subkeywords that permit the command user to specify one or more subject alternate name values of that specific SAN type:

- AIP – specifies one or more IPV4 or IPV6 formatted numeric IP address values.
- ADOMAIN – specifies one or more Domain name values as single-quoted strings.
- AEMAIL – specifies one or more email address values as single-quoted strings.
- AUID – specifies one or more URI values as single-quoted strings.

These new subkeywords may be combined with the existing subkeywords. They pertain only to the ALTNAME keyword and are not applicable to any other RACDCERT command.

Usage & Invocation (slide 2 of 15)

Comparing the new RACDCERT GENCERT ALTNAME subkeywords to the originals:

Subkeyword	Type	# Values	Maximum Length	Notes
DOMAIN	Domain Name	1	255 chars	Meets MUST (63 chars) and SHOULD (255) directives in RFC-1123 for hostnames and email names.
ADOMAIN	Domain Name	1 or more	250 chars per value	Meets MUST (63 chars) directive in RFC-1123 for hostnames and email names. 250-char limit is imposed by underlying utility limitations.
EMAIL	Email Address	1	255 chars	Meets MUST (63 chars) and SHOULD (255) directives in RFC-1123 for hostnames and email names.
AEMAIL	Email Address	1 or more	250 chars per value	Meets MUST (63 chars) directive in RFC-1123 for hostnames and email names. 250-char limit is imposed by underlying utility limitations.
IP	IP Address	1	45 chars	
AIP	IP Address	1 or more	45 chars per value	
URI	URI Name	1	255 chars	Meets MUST (63 chars) and SHOULD (255) directives in RFC-1123 for hostnames and email names.
AURI	URI Name	1 or more	250 chars per value	Meets MUST (63 chars) directive in RFC-1123 for hostnames and email names. 250-char limit is imposed by underlying utility limitations.

Usage & Invocation (slide 3 of 15)

Example:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BobGens1')) WITHLABEL('BOBGENS1')
ALTNAME(DOMAIN('www.madeup.com') ADOMAIN('ww2.madeup.com','ww3.madeup.com')
EMAIL('bobgens@madeup.com') AEMAIL('bastila@madeup.com','keyleth@madeup.com')
IP(9.117.24.160) AIP(9.117.24.161,9.117.24.162,2001:db8:3333:4444:5555:6666:7777:8888)
AURI('http://www.madeup.com/main.html','ldap://www.madeup.com/ldap:user=client'))
KEYUSAGE(HANDSHAKE)
 READY
```

Notes:

- DOMAIN and ADOMAIN are used in combination to specify 3 Domain name subject alternate names.
- EMAIL and AEMAIL are used in combination to specify 3 email address subject alternate names.
- IP and AIP are used in combination to specify 3 IPv4 addresses and 1 IPv6 address as IP address subject alternate names.
- AURI is used to specify 2 URI subject alternates names, and is used by itself to demonstrate that the original URI subkeyword is not required if the newer subkeywords are specified.
- The X.509 RFC places no importance on the order of these values in the certificate's Subject Alternative Name extension, just that the values are included in that certificate extension.

Usage & Invocation (slide 4 of 15)

Results:

The subject alternative name values are included in the generated certificate. RACDCERT LIST (and LISTCHAIN and CHECKCERT) are extended to display these multiple names.

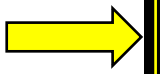
```
RACDCERT CERTAUTH LIST(LABEL('BOBGENS1'))

 Digital certificate information for CERTAUTH:

   Label: BOBGENS1
   Certificate ID: 2QiJmZmDhZmjgcLWwsfF1eLx
   Status: TRUST
   Start Date: 2024/10/24 00:00:00
   End Date:   2025/10/24 23:59:59
   Serial Number:
        >00<
   Issuer's Name:
        >CN=BobGens1<
   Subject's Name:
        >CN=BobGens1<
   Subject's AltNames:
     IP: 9.117.24.161
     IP: 9.117.24.162
     IP: 2001:0DB8:3333:4444:5555:6666:7777:8888
     IP: 9.117.24.160
     EMail: bastila at madeup.com
     EMail: keyleth at madeup.com
     EMail: bobgens at madeup.com
     Domain: ww2.madeup.com
     Domain: ww3.madeup.com
     Domain: www.madeup.com
     URI: http://www.madeup.com/main.html
     URI: ldap://www.madeup.com/ldap:user=client
   Subject Key ID:
        7B:7A:3E:87:10:C5:43:11:1F:53:06:78:F3:B1:F1:06:
        48:06:75:B5
   Signing Algorithm: sha256RSA
   Key Usage: HANDSHAKE, CERTSIGN
   Key Type: RSA
   Key Size: 2048
   Private Key: YES
   Certificate Fingerprint (SHA256):
        82:CA:A6:5C:E6:6C:D4:5F:2F:99:53:F2:F9:BE:B1:1C:
        CA:CC:84:3C:29:E4:7D:E9:70:ED:F4:F7:6C:05:2E:0E
   Ring Associations:
   *** No rings associated ***

 READY
```

Usage & Invocation (slide 5 of 15)

Results:

RACDCERT LIST, LISTCHAIN and CHECKCERT are also extended to display the Authority Key ID and Subject Key ID.

Note: This certificate is self-signed and does not have an Authority Key ID extension.



```
RACDCERT CERTAUTH LIST(LABEL('BOBGENS1'))

 Digital certificate information for CERTAUTH:

   Label: BOBGENS1
   Certificate ID: 2QiJmZmDhZmjgcLWwsfF1eLx
   Status: TRUST
   Start Date: 2024/10/24 00:00:00
   End Date:   2025/10/24 23:59:59
   Serial Number:
        >00<
   Issuer's Name:
        >CN=BobGens1<
   Subject's Name:
        >CN=BobGens1<
   Subject's AltNames:
     IP: 9.117.24.161
     IP: 9.117.24.162
     IP: 2001:0DB8:3333:4444:5555:6666:7777:8888
     IP: 9.117.24.160
     EMail: bastila at madeup.com
     EMail: keyleth at madeup.com
     EMail: bobgens at madeup.com
     Domain: ww2.madeup.com
     Domain: ww3.madeup.com
     Domain: www.madeup.com
     URI: http://www.madeup.com/main.html
     URI: ldap://www.madeup.com/ldap:user=client
   Subject Key ID:
        7B:7A:3E:87:10:C5:43:11:1F:53:06:78:F3:B1:F1:06:
        48:06:75:B5
   Signing Algorithm: sha256RSA
   Key Usage: HANDSHAKE, CERTSIGN
   Key Type: RSA
   Key Size: 2048
   Private Key: YES
   Certificate Fingerprint (SHA256):
        82:CA:A6:5C:E6:6C:D4:5F:2F:99:53:F2:F9:BE:B1:1C:
        CA:CC:84:3C:29:E4:7D:E9:70:ED:F4:F7:6C:05:2E:0E
   Ring Associations:
   *** No rings associated ***

 READY
```

Usage & Invocation (slide 6 of 15)

The contents of the certificate (decoded)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = BobGens1
        Validity
            Not Before: Oct 24 05:00:00 2024 GMT
            Not After : Oct 25 04:59:59 2025 GMT
        Subject: CN = BobGens1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e2:c4:88:07:72:25:4c:3b:b1:ab:f9:6c:0e:7b:
                    f4:99:4e:a9:12:e4:ca:45:2c:8f:8d:16:12:11:f3:
                    40:a3:7c:a3:16:b6:6f:ea:19:d8:96:2f:f4:59:6d:
                    cf:72:fc:20:43:a0:d8:0b:02:1c:59:68:25:0d:dc:
                    4e:e9:8a:42:b8:1b:af:1e:da:e6:60:64:74:e0:0c:
                    a5:fd:30:04:5e:bd:4a:1c:33:19:47:96:14:21:e6:
                    15:06:04:5f:81:e1:85:dd:36:a1:6c:49:7e:2a:b4:
                    32:d9:62:d4:3f:eb:07:fe:3b:1a:0f:48:65:31:9b:
                    a2:83:ab:5a:32:ca:3e:26:24:d8:ca:97:ff:21:43:
                    db:92:62:cd:d3:dd:31:37:f6:db:4c:f5:8d:44:08:
                    e4:67:5c:a3:b2:3b:e2:da:c6:3e:29:e7:a8:41:bb:
                    22:ee:b7:14:bb:42:79:f2:38:2a:3d:b3:b2:26:93:
                    fb:10:7b:c2:73:77:1e:e7:05:84:e1:e4:bc:a4:ec:
                    b3:48:25:34:bb:4c:f2:49:90:c6:7a:81:8c:a1:83:
                    c8:de:a6:c5:93:14:a7:a1:33:bc:53:ae:96:92:0b:
                    94:f9:8b:48:fa:d7:ad:d5:6e:13:38:4d:b3:58:dc:
                    46:0c:3a:fb:64:03:f8:dc:1c:86:e0:36:81:91:01:
                    f2:71
                Exponent: 65537 (0x10001)
            X509v3 extensions:
                Netscape Comment:
                    Generated by the Security Server for z/OS (RACF)
                X509v3 Subject Alternative Name:
                    email:bastila@madeup.com, email:keyleth@madeup.com,
    email:bobgens@madeup.com, DNS:ww2.madeup.com, DNS:ww3.madeup.com,
    DNS:www.madeup.com, URI:http://www.madeup.com/main.html,
    URI:ldap://www.madeup.com/ldap:user=client, IP Address:9.117.24.161, IP
    Address:9.117.24.162, IP Address:2001:DB8:3333:4444:5555:6666:7777:8888, IP
    Address:9.117.24.160
                X509v3 Key Usage: critical
                    Digital Signature, Key Encipherment, Certificate Sign, CRL Sign
                X509v3 Basic Constraints: critical
                    CA:TRUE
                X509v3 Subject Key Identifier:
                    7B:7A:3E:87:10:C5:43:11:1F:53:06:78:F3:B1:F1:06:48:06:75:B5
        Signature Algorithm: sha256WithRSAEncryption
        Signature Value:
            47:17:e1:99:0c:e0:e4:c6:43:60:4d:fc:05:b4:f0:85:6e:c0:
            a8:18:a1:a2:d9:73:8b:2a:4f:ff:57:76:21:46:4f:d2:bc:d8:
            ef:cb:24:5a:14:45:d4:61:b6:37:64:82:27:62:7a:0d:56:8b:
            69:3e:46:ce:66:ce:b4:22:b1:c5:2e:0a:cd:f9:7a:13:e5:7f:
            e5:43:78:b7:dd:a1:fa:81:22:66:80:7d:05:8b:81:84:37:2c:
            3b:e4:46:0d:b1:69:82:4c:4b:9f:7d:9a:8f:81:1d:d7:14:ab:
            9c:d8:4a:0b:d6:62:ef:e5:bc:85:16:2d:8f:11:2f:cd:83:db:
            52:78:1a:82:2e:29:45:36:30:2a:ea:9e:09:77:15:41:db:29:
            2f:15:d0:3d:a5:09:9a:ce:05:67:ea:97:4c:82:c7:f9:e9:4c:
            96:67:0a:7b:bc:5c:c3:98:36:de:60:42:41:26:18:2b:99:f0:
            ae:74:19:e3:9f:ec:51:d0:da:33:ab:a0:b8:94:fc:21:19:bc:
            54:37:65:4c:2a:09:4a:0e:6d:d1:a9:28:05:90:45:1e:00:7f:
            e0:c1:48:23:0a:f8:c9:21:b5:54:70:0b:b6:0e:6b:e2:af:2e:
            3d:ae:68:f3:18:43:24:29:8e:0f:f8:27:53:42:97:20:88:d0:
            a2:dc:a7:74
    -----BEGIN CERTIFICATE-----
    <Omitted for brevity>
    -----END CERTIFICATE-----
```

Note that all specified subject alternate name values are included in the certificate's Subject Alternative Name extension.

Usage & Invocation (slide 7 of 15)

The SMF Type 80 Event Code 66 entry that is recorded for the event:

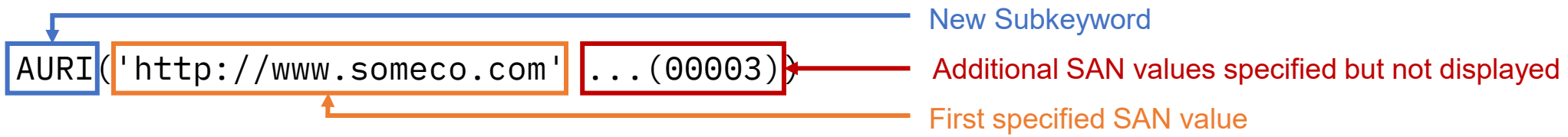
```
RECORD SEQUENCE NUMBER - 2
000000  1E500036 877C0124 298FC9D4 F1F32800   4200C9C2 D4E4E2C5 D940E2E8 E2F14040   *.&...@....IM13....IBMUSER SYS1  *
000020  4040005E 00034020 0000D3D6 C3C1D3C6   F1F0C9C2 D4E4E2C5 D9400030 77730124   *  .;.. ...LOCALF10IBMUSER .....*
000040  298F4040 40404040 40400800 F7F7C6F0   E2E8E2D4 E4D3E3C9 017B0010 000006B3   *..         ..77F0SYSMULTI.#.....*
000060  02002000 40404040 40404040 40404040   40404040 40404040 40404040 40404040   *....                                *
000080  40404040 40404040 40404040 40404040   40404040 40404040 40404040 40404040   *                                    *
0000A0  40404040 40404040 40404040 40404040   40404040 40404040 40404040 40404040   *                                    *
0000C0  C2D6C2C7 C5D5E2F1 40404040 40404040   40404040 40404040 40404040 40404040   *BOBGENS1                            *
0000E0  00000800 F2F0F2F4 61F1F061 F2F4F0F0   7AF0F07A F0F0F2F0 F2F561F1 F061F2F4   *....2024/10/2400:00:002025/10/24*
000100  F2F37AF5 F97AF5F9 01F80000 00000000   00000031 14FFFFFF FFFFFFFF FFFFFFFF   *23:59:59.8.....................*
000120  FFFFFFFF FFFFFFFF FF355050 01220600   01C000E2 E8E2D4E4 D3E3C900 00000000   *.........&&.....{.SYSMULTI.....*
000140  00000000 00000000 00000000 00000000   00000000 00000000 000000D3 D6C3C1D3   *............................LOCAL*
000160  C6F1F000 00000000 000000C9 C2D4E4E2   C5D940E2 E8E2F140 40404001 3E0002F0   *F10........IBMUSER SYS1    ....0*
000180  F0013F00 0BC3D57E C29682C7 8595A2F1   01470008 C29682C7 8595A2F1 01BE0020   *0....CN=B..G...1....B..G...1....*
0001A0  82CAA65C E66CD45F 2F9953F2 F9BEB11C   CACC843C 29E47DE9 70EDF4F7 6C052E0E   *...*W%M^...29........U'Z..47%...*
0001C0  0150000C F94BF1F1 F74BF2F4 4BF1F6F1   0150000C F94BF1F1 F74BF2F4 4BF1F6F2   *.&..9.117.24.161.&..9.117.24.162*
0001E0  01500026 F2F0F0F1 7AC4C2F8 7AF3F3F3   F37AF4F4 F4F47AF5 F5F5F57A F6F6F6F6   *.&..2001:DB8:3333:4444:5555:6666*
000200  7AF7F7F7 F77AF8F8 F8F80150 000CF94B   F1F1F74B F2F44BF1 F6F00151 00128281   *:7777:8888.&..9.117.24.160......*
000220  A2A38993 817C9481 8485A497 4B839694   01510012 9285A893 85A3887C 94818485   *.....@.....................@....*
000240  A4974B83 96940151 00128296 82878595   A27C9481 8485A497 4B839694 0152000E   *.................@..............*
000260  A6A6F24B 94818485 A4974B83 96940152   000EA6A6 F34B9481 8485A497 4B839694   *..2.................3..........*
000280  0152000E A6A6A64B 94818485 A4974B83   96940153 001F88A3 A3977A61 61A6A6A6   *...........................://...*
0002A0  4B948184 85A4974B 83969461 94818995   4B88A394 93015300 26938481 977A6161   *............/.................://*
0002C0  A6A6A64B 94818485 A4974B83 96946193   8481977A A4A28599 7E839389 8595A3     *............../....:....=...... *
```

This is a hexadecimal dump of the single SMF Type 80 Event Code 66 entry. IP Address SANs are stored as Extended Relocate 336s ('0150'X in this dump), Email Address SANs as Extended Relocate 337s ('0151'X), Domain Name SANs as Extended Relocate 338s ('0152'X), and URI name SANs as Extended Relocate 339s ('0153'X). This entry contains the 3 IP addresses, the 3 Email addresses, the 3 Domain names, and the 2 URI names specified in the RACDCERT GENCERT command shown earlier.

Usage & Invocation (slide 8 of 15)

Output from the RACF SMF Unload utility IRRADU00 is modified to use the new ALTNAME subkeywords in the RACD_SPECIFIED field in place of the original ALTNAME subkeywords, to provide correct information in cases where more than one SAN value of a supported SAN type were specified. Recall that the new subkeywords support the use of 1 or more values, so the new subkeywords can be used in place of the original – the original continue to be supported for compatibility.

In cases where more than one SAN value of a specific SAN type was specified, an abbreviation scheme is used to save space in the 1024-byte RACD_SPECIFIED output field. Example:



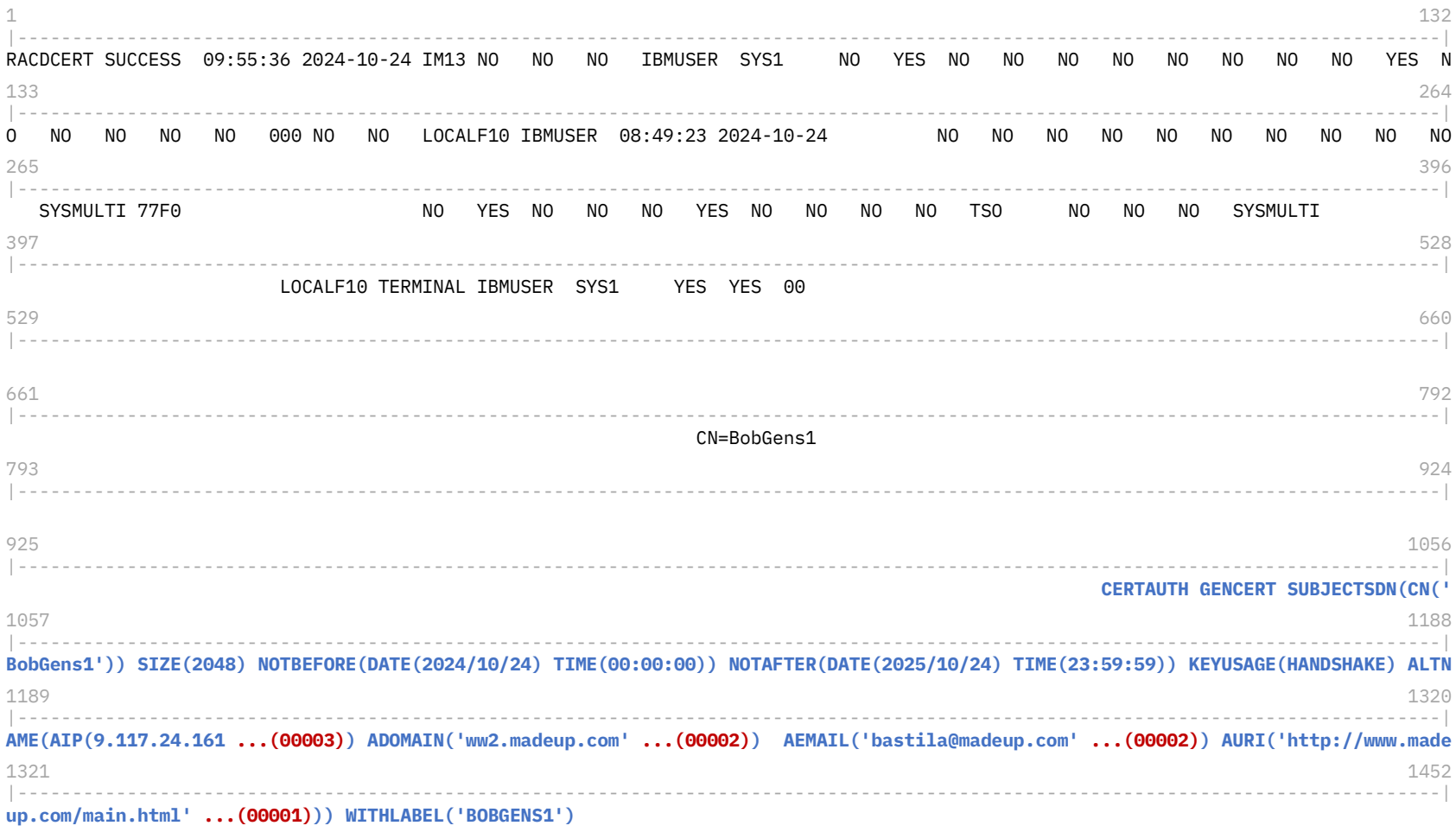
IRRADU00 is a *convenience utility* for viewing SMF entry data, and is not always capable of displaying all data recorded in an SMF entry because of output field size constrains. The SMF Type 80 Event Code 66 entry records all of the SAN values that were specified for the command. Clients that require complete, untruncated information about the event are encouraged to obtain these records directly from the SMF entry.

Usage & Invocation (slide 9 of 15)

The first 1452 columns of the output for the single SMF entry is displayed to the left – there is additional information in further columns.

The RACD_SPECIFIED field, which displays a *likely* RACDCERT command that could be issued to achieve the result achieved by the *actual* command, begins in column 1024.

Note the abbreviation scheme used to reduce the amount of space consumed by the SAN values in RACD_SPECIFIED.



Usage & Invocation (slide 10 of 15)

The R_PKIServ Callable Service is also extended.

The R_PKIServ Callable Service allows applications to request the generation, retrieval, and administration of X.509 certificates and certificate requests. Usually the interface to z/OS Cryptographic Services PKI Services, this callable service can be used to request the generation of certificates from z/OS Security Server RACF through the GENCERT function's SAF Path. Details on how this is done are provided in *z/OS Security Server RACF Callable Services*.

In prior releases, the last SAN value of any of the four supported SAN types detected in the parameter list provided to the GENCERT function was included in the generated certificate when using the SAF Path to generate the certificate; any earlier SANs specified in the parameter list were ignored.

This limitation is removed. Multiple SAN values for any of the four supported SAN types may now be specified in the parameter list provided through the callable service.

By the way, the GENCERT function PKI Services Path does not have this limitation in any of the releases currently in service.

Usage & Invocation (slide 11 of 15)

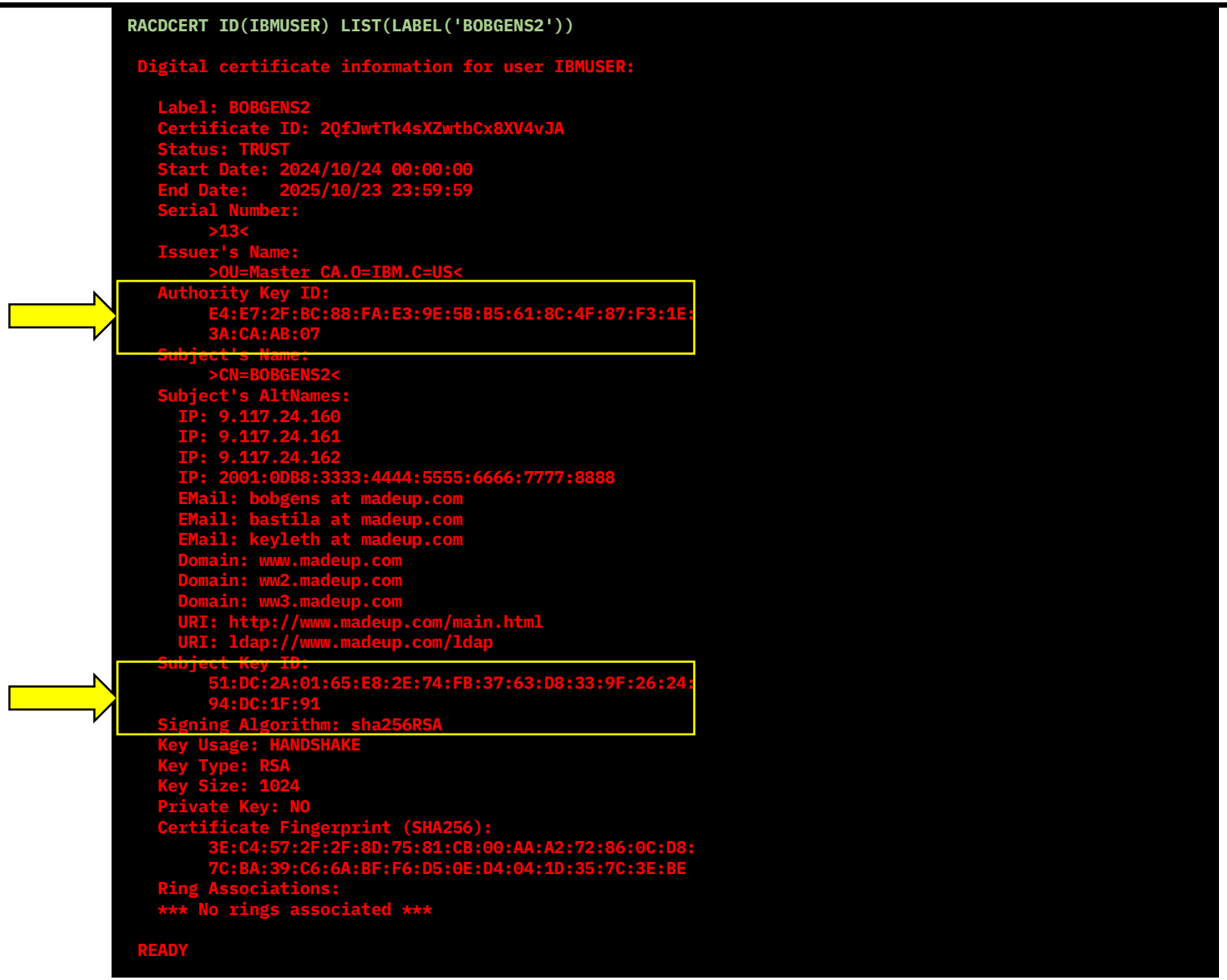
This certificate was generated using the R_PKIServ Callable Service GENCERT function SAF Path, using values similar to those used in the prior RACDCERT GENCERT example.

The subject alternative name values are included in the generated certificate. RACDCERT LIST (and LISTCHAIN and CHECKCERT) are extended to display these multiple names.

```
RACDCERT ID(IBMUSER) LIST(LABEL('BOBGENS2'))

 Digital certificate information for user IBMUSER:

   Label: BOBGENS2
   Certificate ID: 2QfJwtTk4sXZwtbCx8XV4vJA
   Status: TRUST
   Start Date: 2024/10/24 00:00:00
   End Date:   2025/10/23 23:59:59
   Serial Number:
        >13<
   Issuer's Name:
        >OU=Master CA.O=IBM.C=US<
   Authority Key ID:
        E4:E7:2F:BC:88:FA:E3:9E:5B:B5:61:8C:4F:87:F3:1E:
        3A:CA:AB:07
   Subject's Name:
        >CN=BOBGENS2<
   Subject's AltNames:
     IP: 9.117.24.160
     IP: 9.117.24.161
     IP: 9.117.24.162
     IP: 2001:0DB8:3333:4444:5555:6666:7777:8888
     EMail: bobgens at madeup.com
     EMail: bastila at madeup.com
     EMail: keyleth at madeup.com
     Domain: www.madeup.com
     Domain: ww2.madeup.com
     Domain: ww3.madeup.com
     URI: http://www.madeup.com/main.html
     URI: ldap://www.madeup.com/ldap
   Subject Key ID:
        51:DC:2A:01:65:E8:2E:74:FB:37:63:D8:33:9F:26:24:
        94:DC:1F:91
   Signing Algorithm: sha256RSA
   Key Usage: HANDSHAKE
   Key Type: RSA
   Key Size: 1024
   Private Key: NO
   Certificate Fingerprint (SHA256):
        3E:C4:57:2F:2F:8D:75:81:CB:00:AA:A2:72:86:0C:D8:
        7C:BA:39:C6:6A:BF:F6:D5:0E:D4:04:1D:35:7C:3E:BE
   Ring Associations:
   *** No rings associated ***

 READY
```

Usage & Invocation (slide 12 of 15)

Note: This certificate is signed by a certificate authority (CA) certificate. Therefore, this certificate has an Authority Key ID extension using the CA certificate as well as a Subject Key ID generated from its own public key. Both are displayed by this example RACDCERT LIST command, and are also displayed by the RACDCERT CHECKCERT and RACDCERT LISTCHAIN commands.



Usage & Invocation (slide 13 of 15)

The contents of the certificate (decoded)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 19 (0x13)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = IBM, OU = Master CA
        Validity
            Not Before: Oct 24 05:00:00 2024 GMT
            Not After : Oct 24 04:59:59 2025 GMT
        Subject: CN = BOBGENS2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:ca:fd:94:1e:ad:5d:7c:5e:f3:37:ba:c0:b4:3c:
                    32:ab:39:83:5a:ec:cf:a3:b8:c6:4f:d7:6c:62:6b:
                    c2:c9:c8:7a:a5:02:94:c7:cd:6b:af:d3:8b:58:e4:
                    5f:e5:6a:a6:af:28:4d:c1:ce:8a:10:b1:90:a5:60:
                    0f:0e:89:30:ca:e3:6b:da:63:0a:23:6f:ba:6f:d9:
                    22:65:bb:69:a7:53:a8:ad:82:2d:3f:24:76:12:01:
                    2e:ec:f0:91:5d:2c:89:85:4a:7c:75:a4:fa:7b:e7:
                    2e:9b:c3:61:b2:92:df:fc:64:d8:55:ba:e9:b1:fd:
                    70:ce:9c:c5:3a:4d:77:26:8d
                Exponent: 65537 (0x10001)
            X509v3 extensions:
                Netscape Comment:
                    Generated by the Security Server for z/OS (RACF)
                X509v3 Subject Alternative Name:
                    email:bobgens@madeup.com, email:bastila@madeup.com,
    email:keyleth@madeup.com, DNS:www.madeup.com, DNS:ww2.madeup.com,
    DNS:ww3.madeup.com, URI:http://www.madeup.com/main.html,
    URI:ldap://www.madeup.com/ldap, IP Address:9.117.24.160, IP Address:9.117.24.161,
    IP Address:9.117.24.162, IP Address:2001:DB8:3333:4444:5555:6666:7777:8888
                X509v3 Key Usage: critical
                    Digital Signature, Key Encipherment
                X509v3 Subject Key Identifier:
                    51:DC:2A:01:65:E8:2E:74:FB:37:63:D8:33:9F:26:24:94:DC:1F:91
                X509v3 Authority Key Identifier:
                    E4:E7:2F:BC:88:FA:E3:9E:5B:B5:61:8C:4F:87:F3:1E:3A:CA:AB:07
                X509v3 Issuer Alternative Name:
                    DNS:alps4077.pok.ibm.com, IP Address:9.57.1.78
        Signature Algorithm: sha256WithRSAEncryption
        Signature Value:
            8d:ac:e6:3c:ca:80:4a:ca:4c:8c:d1:f3:d8:a2:30:d5:58:c2:
            e8:eb:fb:0c:46:3b:a1:bd:e8:43:3a:13:c1:76:29:15:c8:aa:
            3e:ca:38:a4:6d:c6:a4:29:46:1a:f7:b9:e6:73:cb:21:a1:c0:
            6f:d9:82:50:68:94:da:b5:a7:02:62:f2:b5:67:ce:e4:f6:ff:
            1d:bc:a9:10:dd:a6:2b:de:84:bc:8f:b0:db:68:8d:80:68:8d:
            05:64:89:3f:91:6b:9f:6a:22:ef:33:a9:9b:9e:ec:05:da:db:
            b3:2d:81:44:d1:40:5e:6b:5a:df:6c:2f:dd:03:6e:d2:57:af:
            61:a7:60:79:0a:52:d7:e2:86:cf:13:59:77:84:ff:3d:51:7c:
            22:24:46:10:7e:94:81:b4:b7:04:1b:37:af:68:49:3e:6b:14:
            75:d6:c3:c6:80:4b:e0:f1:9e:8d:23:a7:cb:09:2b:30:b7:a6:
            e2:a4:c2:d8:74:13:f3:6e:b6:a2:8f:4a:9e:7d:c2:f5:50:f3:
            df:e0:e1:bc:5a:44:50:3c:4d:3a:3d:92:1b:2e:3b:25:68:ed:
            6a:0a:99:15:70:44:2c:d0:f9:47:a5:6a:05:cc:18:b5:50:db:
            46:86:68:b7:4f:7d:88:74:16:51:3a:d9:ba:c7:c2:73:d6:61:
            14:36:ad:92
-----BEGIN CERTIFICATE-----
<Omitted for brevity>
-----END CERTIFICATE-----
```

Note that all specified subject alternate name values are included in the certificate's Subject Alternative Name extension.

Usage & Invocation (slide 14 of 15)

The R_PKIServ Callable Service GENCERT function SAF Path records *one or more* SMF Type 80 Event Code 69 entries to record the event (not Event Code 66). When multiple SAN values of the same SAN type are specified in the GENCERT function parameter list, a linked series of SMF records is generated, all sharing a common link field. This is the same behavior that occurs when z/OS Cryptographic Services PKI Services is used to generate a certificate.

The linked record format is described in *z/OS Security Server RACF Macros and Interfaces.*

Usage & Invocation (slide 15 of 15)

The RACF SMF Unload utility IRRADU00 uses the same logic to process the linked record series as it does when the R_PKIServ Callable Service GENCERT PKI Services Path is used:

Excerpts from the four entries generated by the example request are shown to the right.

The common link value starting at column 10527 shows that these four records all pertain to the same R_PKIServ GENCERT request.

Note that these records repeat a lot of the same information, except for the different SAN values.

```
1                                                                                                                                      132
|------------------------------------------------------------------------------------------------------------------------------------|
RPKIGENC SUCCESS  14:24:45 2024-10-24 IM13 NO    NO    NO    IBMUSER  SYS1     NO    YES  NO    NO    NO    NO    NO    NO    NO    NO    YES   N
RPKIGENC SUCCESS  14:24:45 2024-10-24 IM13 NO    NO    NO    IBMUSER  SYS1     NO    YES  NO    NO    NO    NO    NO    NO    NO    NO    YES   N
RPKIGENC SUCCESS  14:24:45 2024-10-24 IM13 NO    NO    NO    IBMUSER  SYS1     NO    YES  NO    NO    NO    NO    NO    NO    NO    NO    YES   N
RPKIGENC SUCCESS  14:24:45 2024-10-24 IM13 NO    NO    NO    IBMUSER  SYS1     NO    YES  NO    NO    NO    NO    NO    NO    NO    NO    YES   N

2188                                                          2253                                                              2320
|-------------------------------------------------------------|-----------------------------------------------------------------|
9.117.24.160                                                  http://www.madeup.com/main.html
9.117.24.161                                                  ldap://www.madeup.com/ldap
9.117.24.162
2001:DB8:3333:4444:5555:6666:7777:8888

2509                                                                                                    2610                    2641
|-----------------------------------------------------------------------------------------------------|------------------------------|
bobgens@madeup.com                                                                                     www.madeup.com
bastila@madeup.com                                                                                     ww2.madeup.com
keyleth@madeup.com                                                                                     ww3.madeup.com

10527                                                                                                                            10659
|------------------------------------------------------------------------------------------------------------------------------------|
00DFE4E3D43344F0760000000B800001 3EC4572F2F8D7581CB00AAA272860CD87CBA39C66ABFF6D50ED4041D357C3EBE
00DFE4E3D43344F0760000000B800001 3EC4572F2F8D7581CB00AAA272860CD87CBA39C66ABFF6D50ED4041D357C3EBE
00DFE4E3D43344F0760000000B800001 3EC4572F2F8D7581CB00AAA272860CD87CBA39C66ABFF6D50ED4041D357C3EBE
00DFE4E3D43344F0760000000B800001 3EC4572F2F8D7581CB00AAA272860CD87CBA39C66ABFF6D50ED4041D357C3EBE
```

Interactions & Dependencies

- Software Dependencies
  - None.
- Hardware Dependencies
  - None.
- Exploiters
  - None (so far...).

Upgrade & Coexistence Considerations (1 of 2)

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No.
- Toleration/coexistence APARs/PTFs: None.
- List anything that doesn't work the same anymore. IRRADU00 processing of SMF Type 80 Event Code 66 Records, as described in the earlier slide.
- No upgrade actions are necessary – the original RACDCERT GENCERT options remain and operate as they always have.

Upgrade & Coexistence Considerations (2 of 2)

- No coexistence actions are necessary
  - Certificates generated using the extended RACDCERT GENERT command or the R_PKIServ Callable Service GENCERT SAF Path function on higher level systems can be utilized on lower level systems.
  - Certificates generated using the original RACDCERT GENERT command or the R_PKIServ Callable Service GENCERT SAF Path function on lower level systems can be utilized on higher level systems.
  - RACDCERT EXPORT will provide the same certificate in either environment.
  - RACF commands are not a programming interface, but there may be applications which parse the output of RACDCERT LIST / LISTCHAIN / CHECKCERT.
  - RACDCERT may start to display more details of an existing certificate in RACF.

Installation & Configuration

- Are any APARs or PTFs needed for enablement? No.
- What jobs need to be run? No new jobs are required.
- What hardware configuration is required? No special configuration is required.
- What PARMLIB statements or members are needed? No new members are needed.
- Are any other system programmer procedures required? No.
- Are there any planning considerations? No.
- Are any special web deliverables needed? No.
- Does installation change any system defaults? No.

Summary

- RACF certificate generation commands and callable services now permit the specification of multiple Subject Alternative Names (SANs) of the same data type to be included in the generated certificate.
  - Reduces the number of RACF generated certificates required to secure internet entities that can be identified by or reached through more than one name, address, or protocol.
  - Helps reduce the volume of RACF generated certificates in current and future releases.
  - Helps reduce the administrative overhead in distributing and managing RACF generated certificates.
- RACF certificate display commands now display multiple SANs of the same type and the Authority Key ID and Subject Key ID extensions.
  - These additional certificate details to help the security administrator better understand the RACF digital certificate environment.

Appendix (slide 1 of 3)

- IBM Publications – RACF RACDCERT Certificate Generation
- *z/OS Security Server RACF Security Administrator's Guide* (SA23-2289-xx), specifically the RACF and digital certificates chapter.
- *z/OS Security Server RACF Command Language Reference* (SA23-2292-xx), specifically the RACDCERT GENCERT (Generate Certificate) command.
- *z/OS Security Server RACF Callable Services Reference* (SA23-2293-xx), specifically the R_PKIServ (IRRSPX00 or IRRSPX64) chapter.
- *z/OS Security Server RACF Macros and Interfaces Guide* (SA23-2288-xx), specifically the Record Type 80: RACF processing record section.
- *z/OS Security Server RACF Auditor's Guide* (SA23-2290-xx), specifically The RACF SMF data unload utility chapter.
- IBM Publications – List Support of Multiple Altnames
- *z/OS Security Server RACF Command Language Reference* (SA23-2292-xx), specifically the RACDCERT LIST, LISTCHAIN and CHECKCERT commands.

Appendix (slide 2 of 3)

Terminology

- Certificate – A digital data object that proves the ownership of a private key, and in so doing, prove the identity of the owner of the public key. Also referred to as a X.509 certificate, public key certificate, digital certificate, or identity certificate.
- Subject Distinguished Name (SDN) – An assertion in an X.509 certificate as to the identity of the entity, the "to whom" or "to what" the certificate has been issued.
- Certificate Extension – Optional, additional information supported by an X.509 certificate to indicate intended use of the certificate. An extension can be used to indicate if the certificate is intended to be used to sign other certificates, whether it is a certificate issuing authority (CA) certificate, how the key associated with the certificate is intended to be used, and what identities in addition to the subject distinguished name are asserted by the certificate.
- Subject Alternative Name (SAN) – A specific X.509 Certificate Extension, indented to assert further identities for the entity to whom the certificate was issued. In practice, a SAN is used to identify an intended method by which a server may be contacted or used, as through a specific set of internet addresses, internet URIs, hostnames or domain names, and email addresses.
- Subject Key ID – A specific X.509 extension which contains a value which is derived from the certificate's public key using a cryptographic hash function. This extension provides a means for identifying a certificate containing the specific public key used in an application.
- Authority Key ID – A specific X.509 extension which contains a value which is derived in a similar way as that of the Subject Key ID, except that the certificate signer's public key is used. This value can help the user to find out the issuer's cert in the case when the issuer's certificate has been renewed with a different keypair.