RACF ® Update for z/OS® 3.2

NY/Tampa/Dallas/Raleigh RACF Users Group
11 June, 2025

Bob Gensler, RACF Development
Mark Nelson, RACF Development, CISSP®, CSSLP®, markan@us.ibm.com
Andrew Rundall, RACF Development
Bruce Wells, RACF Development

1

RACF Update: What did we Cover Before?

15 May 2024
- SPECIAL user password revocation prompt suppression
- Support for AES as the password-based encryption algorithm for PKCS#12 packages in both RACF and PKI Services
- RVARY password protection
- https://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/nyrug_2024_05_15_racf_update.pdf

11 October, 2023
- z/OS 3.1 Only
  - APPLAUDIT Enhancements
  - Custom Field Information in ACEE
- z/OS 2.5 Continuous Delivery
  - Identity Token Enhancements
  - Passphrase Interval
  - Support for the IBM Z Security and Compliance Center
  - Center for Internet Security (CIS) IBM z/OS V2R5 with RACF Benchmark
  - Encrypted RACF VSAM data set as RACF database
  - Ability to Disable Additional logon attempts for a RACF SPECIAL user after exceeding the SETROPTS PASSWORD(REVOKE(nnn)) value
  - Sharing RACF data base with RACF on z/VM
  - https://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/nyrug_2023_10_11_RACF_Update_3.1.pdf

2

RACF Update: What's New Since our Last Update?

z/OS® 3.2 Only: https://www.ibm.com/docs/en/announcements/preview-zos-32-plan z17?region=US

- RACF Support for Digital Certificates with multiple subject alt names
- Granular data set encryption support for basic and large format data sets

z/OS 2.5 – Continuous Delivery

- Common Criteria Evaluation
- Validated Boot
- KEYSMSTR Class Enhancements
- Stronger Encryption for Enveloped for Passwords/Password Phrases
- Logging Supervisor State or Key 0 Opens of VSAM data sets

z/OS 3.2 items that were not in the announcement will be covered at the next NY/Tampa/Dallas/Raleigh (and others?) meeting tentatively scheduled for Wednesday, 22 October, 2025.

3

z/OS 3.2 Enhancements

4

RACDCERT subject alternate names support

- **Allow the generation of a digital certificate containing multiple subject altnames with the RACDCERT GENCERT command**
- **RACDCERT LIST to display the subject altnames contained within a certificate, whether it was imported or created with RACDCERT**
- **While we're at it, display the authority key ID and subject key**

5

RACDCERT GENCERT Multiple Subject Alt Names


```
RACDCERT GENCERT
        :
    [ALTNAME(
       IP(numeric-IP-address)
       AIP(numeric-IP-address1,numeric-IP-address2,...)

       DOMAIN('internet-domain-name')
       ADOMAIN('internet-domain-name1','internet-domain-name2',...)

       EMAIL('email-address')
       AEMAIL('email-address1','email-address2',...)

       URI('universal-resource-identifier')
       AURI('universal-resource-identifier1','universal-resource-identifier2',...)
    )
    ]
```


6

RACDCERT GENCERT Multiple Subject Alt Names

RACDCERT GENCERT generated multiple SAN certificate, viewed off-platform

```
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-----
```


7

RACDCERT GENCERT Multiple Subject Alt Names

SMF Unload IRRADU00 report for a RACDCERT GENCERT multiple SAN certificate

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.

```
1                                                                                                                                132
|------------------------------------------------------------------------------------------------------------------------------|
RACDCERT SUCCESS  09:55:36 2024-10-24 IM13 NO   NO   NO   IBMUSER  SYS1     NO   YES  NO   NO   NO   NO   NO   NO   NO   NO   YES  N
133                                                                                                                              264
|------------------------------------------------------------------------------------------------------------------------------|
O   NO   NO   NO   NO   000 NO   NO   LOCALF10 IBMUSER  08:49:23 2024-10-24          NO   NO   NO   NO   NO   NO   NO   NO   NO   NO
265                                                                                                                              396
|------------------------------------------------------------------------------------------------------------------------------|
   SYSMULTI 77F0                     NO   YES  NO   NO   NO   YES  NO   NO   NO   NO   TSO      NO   NO   NO   SYSMULTI
397                                                                                                                              528
|------------------------------------------------------------------------------------------------------------------------------|
                        LOCALF10 TERMINAL IBMUSER  SYS1     YES  YES  00
529                                                                                                                              660
|------------------------------------------------------------------------------------------------------------------------------|


661                                                                                                                              792
|------------------------------------------------------------------------------------------------------------------------------|
                                                    CN=BobGens1
793                                                                                                                              924
|------------------------------------------------------------------------------------------------------------------------------|


925                                                                                                                             1056
|------------------------------------------------------------------------------------------------------------------------------|
                                                                                                                 CERTAUTH GENCERT SUBJECTSDN(CN('
1057                                                                                                                            1188
|------------------------------------------------------------------------------------------------------------------------------|
BobGens1')) SIZE(2048) NOTBEFORE(DATE(2024/10/24) TIME(00:00:00)) NOTAFTER(DATE(2025/10/24) TIME(23:59:59)) KEYUSAGE(HANDSHAKE) ALTN
1189                                                                                                                            1320
|------------------------------------------------------------------------------------------------------------------------------|
AME(AIP(9.117.24.161 ...(00003)) ADOMAIN('ww2.madeup.com' ...(00002))  AEMAIL('bastila@madeup.com' ...(00002)) AURI('http://www.made
1321                                                                                                                            1452
|------------------------------------------------------------------------------------------------------------------------------|
up.com/main.html' ...(00001))) WITHLABEL('BOBGENS1')
```


8

RACDCERT GENCERT Multiple Subject Alt Names

SMF Unload IRRADU00 report for a R_PKIServ SAF GENCERT multiple SAN certificate

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
```


9

RACDCERT LIST Multiple Subject Alt Names

```
Subject's Name:
       >CN=samplecert.O=Test.SP=Poughkeepsie.C=US<
Subject's AltNames:
    IP: 127.0.0.5
    IP: 127.0.0.6
    IP: 127.0.0.7
    EMail: admin1 at us.ibm.com
    EMail: admin2 at us.ibm.com
    Domain: developer.ibm.com
    Domain: demo.ibm.com
    Domain: api.ibm.com
    Domain: tester.ibm.com
    URI: https://developer.ibm.com/welcome.html
    URI: https://tester.ibm.com/token
```

10

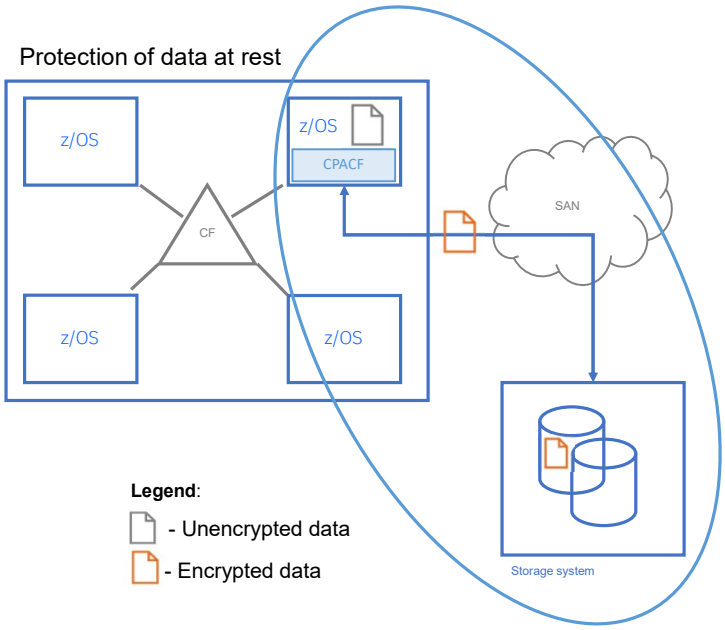
RACDCERT LIST: Authority Key and Subject Key


```
Start Date: 2023/02/01 00:00:00
End Date: 2024/02/01 23:59:59
Serial Number:
>05<
Issuer's Name:
>CN=sampleCA.O=Test.SP=Poughkeepsie.C=US<
Authority Key ID:
FC:C4:91:DF:D3:32:F3:08:9B:85:42:E9:46:53:C6:61:
97:FE:94:4E
Subject's Name:
>CN=samplecert.O=Test.SP=Poughkeepsie.C=US<
Subject's AltNames:
... ... ...
Subject Key ID:
D8:38:7A:E5:58:3E:79:74:83:66:53:C6:61:97:04:DA:
DC:98:96:2B
... ... ...
```


11

z/OS Data Set Encryption

- Application transparent & enabled by policy
- Host encryption via CPACF as data is written to or read from disk
- Supports seqential extended format, VSAM extended format, PDSE, JES2 spool, Db2, CICS, & IMS
- Includes HSM & DSS migration and backup of encrypted data sets
- Replicated data remains encrypted



12

Statements of Direction: Tape Encryption

- **Encryption of tape data sets**

  IBM intends to **enhance pervasive encryption** to perform **encryption within the access methods for tape data sets**. It is expected to be **transparent to the application** program **unless it uses EXCP**. This new data set encryption support is intended to be independent of any encryption that occurs in the tape subsystem.

  (*) See the disclaimer.

13

Granular Data Set Encryption

- **A new field in the DFP segment of the DATASET profile specifies encryption policy for *tape, PDSE, and sequential basic and large format* data sets covered by the profile**
  - *No change to current support of extended format data sets*
- **This policy is not bound to the encryption key label in the DFP DATAKEY field**
  - *That is, the key can be sourced elsewhere, like today*
- **For each type, you can choose to**
  - *INclude the type for encryption*
  - *EXclude the type from encryption*
  - *Defer to SMS for the decision (the default). SMS checks a FACILITY profile for system-wide default policy.*

14

ADDSD and ALTDSD

```
[ DFP(
      [RESOWNER(userid or group-name) | NORESOWNER]
      [DATAKEY(CKDS key label) | NODATAKEY]
      [ENCRYPTTYPES(
          [ALL |
          [INTAPE | EXTAPE | NOTAPE]
          [INPDSE | EXPDSE | NOPDSE]
          [INSEQ  | EXSEQ  | NOSEQ ]
          ]
                  ) | NOENCRYPTTYPES]
    ) | NODFP ]
```

- **ALL is mutually exclusive with EXxxxx and NOxxxx**
- **NOxxxx, INxxxx, and EXxxxx are mutually exclusive for the same type**

```
IRR52128I Mutually exclusive operands are specified for keyword
ENCRYPTTYPES. Processing terminated.
```


15

LISTDSD - examples

```
INFORMATION FOR DATASET BRUCE.* (G)

DFP INFORMATION
---------------
RESOWNER= NONE
DATAKEY= MYKEY
DATA SET TYPES ENCRYPTED= INTAPE EXSEQ

INFORMATION FOR DATASET BRUCE.* (G)

DFP INFORMATION
---------------
RESOWNER= NONE
DATAKEY= MYKEY
DATA SET TYPES ENCRYPTED= ALL INTAPE INPDSE INSEQ
```


16

Continuous Delivery Enhancements

17

z/OS Common Criteria

- **z/OS 2.5 has:**
  - Completed the Common Criteria evaluation for version 4.3 of the Operating System Protection Profile (OSPP)!

    https://www.commoncriteriaportal.org/products/index.cfm

  - **Been placed on the National Information Assurance Partnership (NIAP) Product Compliant List**

    https://www.niap-ccevs.org/products/international-product/2024.1282

Agenzia per la Cybersicurezza Nazionale

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) ve.3.1 rel. 5

Certificato n. *(Certificate No.)*	08/2024
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/ATS/05/2023/RC, v 1.0.
Decorrenza *(Date of 1st Issue)*	21 ottobre 2024
Nome e Versione del Prodotto *(Product Name and Version)*	IBM z/OS Version 2 Release 5
Sviluppatore *(Developer)*	IBM Corporation
Tipo di Prodotto *(Type of Product)*	Sistema Operativo
Conformità a PP *(PP Conformance)*	Protection Profile for General Purpose Operating Systems v.4.3
Funzionalità di sicurezza *(Conformance of Functionality)*	Funzionalità conformi a PP, CC Parte 2 estesa

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR *(CCRA recognition for components up to EAL2 and ALC_FLR only)*

Riconoscimento SOGIS MRA per componenti fino a EAL4 *(SOGIS MRA recognition for components up to EAL4)*

Roma, 21 ottobre 2024

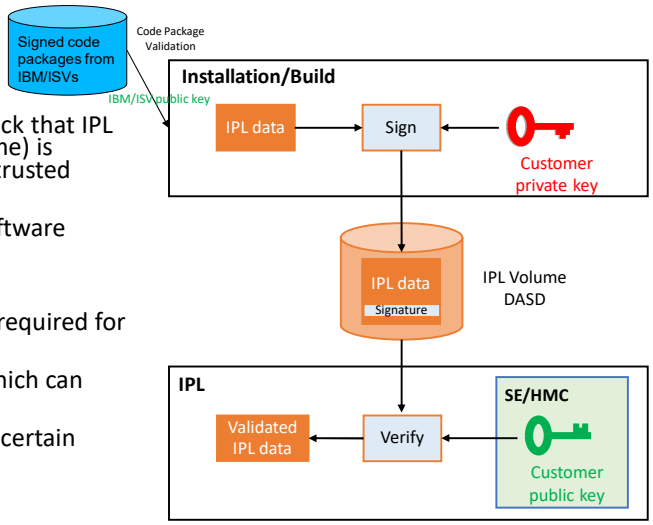
Il Capo Servizio Certificazione e Vigilanza (A. Billet)

18

z/OS Validated Boot

- **What is z/OS Validated Boot?**
- Uses digital signatures to provide an IPL-time check that IPL data (that is, executables residing on an IPL volume) is intact, un-tampered-with, and originates from a trusted source from the time it was built and signed
- Enables detection of unauthorized changes to software executables
- **What value does it provide?**
- Ability to meet regulatory compliance standards required for certain secure software deployment scenarios
- Early detection of *accidental* IPL data changes, which can reduce impact and scope of outages
- Detection of *malicious* IPL data changes can stop certain types of attacks

- Note:
  - "Validated Boot" = "Secure Boot" = "Boot Integrity Validation"
  - "Boot" = "IPL" **(NOT firmware IML)**
  - Note that Validated Boot is NOT the same thing as "Secure Execution"



19

Related Solutions…

- **GIMZIP package signing and verification in z/OS SMP/E and z/OSMF Software Management**
  - Ensures the integrity of signed code packages delivered to customers from IBM and other software vendors

- **Validated Boot for z/OS**
  - Ensures the integrity of built z/OS system executables (load modules), once the above code packages have been validated and "unpacked" and the contents have been used to build signed, IPLable z/OS systems

- **Secure Boot for ECKD Devices**
  - Provides firmware support for secure List-Directed IPL (LD-IPL) from ECKD storage devices in addition to SCSI devices, for both z/OS and Linux use

20

Design Approach: Load Module Signing and Validation

- Code Package Validation validates the incoming signed code package deliverables using software vendor's **public** key
- **Client's "secure build" process creates and signs the *z/OS IPL Text and system load modules* with the client's private key, and stores them on disk**
- Client's **public** keys for validation purposes are provided to and maintained in the platform firmware and made available to partitions for IPL-time validation use
- **At IPL time, platform firmware (Z Bootloader) validates the IPL Text using the client's public keys; the IPL Text contains validation support which z/OS** uses **in subsequent load module validation steps during the IPL**
- **As z/OS loads subsequent authorized load modules during IPL,** it **validates their signatures** using **the client's public keys**
- Validation failures during IPL may result in non-restartable wait state termination of the IPL, or not, depending on the requested IPL validation mode

➢ ***Build up a chain of trust through digital signature validation, at every step of this cascading process, anchored in the firmware validation of the IPL Text and the secure firmware repository for the validation certificates/keys***

21

NIAP Certification and Regulatory Compliance

- **We are targeting Z and z/OS NIAP Certification with OS Protection Profile (OSPP) 4.3, which now requires both code package signing/validation and Boot Integrity Validation for IPLed "kernel" software**
  - Requirements for code package signing/validation and for Validated Boot are relatively new and are now incorporated into the NIAP profile; earlier certifications of z/OS and Z hardware/firmware *do not implement this requirement*
  - This higher level of certification may be required in some client environments, based on industry regulations and/or other security requirements
  - Boot Integrity Validation is an important part of securing the "supply chain" for system software from the software vendors, through the build process, to time of use
- ***We** provided **the basic validation capabilities needed to achieve NIAP certification first, then potentially we will provide additional value-add validation capabilities in future stages of z/OS Validated Boot support…***

22

Support Requirements – Overall Solution

- **Hardware/Firmware Support**
  - CPACF digital signature support with Elliptic Curve ECDSA-P521 support and SHA-512 hashing support
  - Virtual Flash Memory (VFM), also known as Storage Class Memory (SCM), for use in z/OS paging for LPA pages
  - z16 GA1.5 firmware (5/2023) provides:
    - **Support for List-Directed IPL (LD-IPL) from ECKD DASD (in addition to SCSI DASD)**
      - Via SE/HMC and DPM new load panel/load profile options – SCSI vs ECKD, CCW-IPL vs LD-IPL, Enforce vs Audit security mode
        - **For Linux on Z** – supports Linux IPL from ECKD DASD, not just SCSI DASD like today
        - **For z/OS** – supports z/OS Validated Boot from ECKD DASD
      - Current CCW-IPL (non-validated IPL) capabilities are preserved for migration, compatibility, and fallback, from same IPL Volume
    - **Certificate Store for Validated Boot**
      - Via SE/HMC and DPM Certificate import and Certificate management, including mapping imported certificates to specific LPARs for IPL-time validation use
      - PR/SM provides support for the Certificate Store on a per-LPAR basis
        - **For Linux on Z** - provides value for key management of Linux distributor validation keys without needing to deliver those Linux distributor keys in IBM firmware as we do today, simplifying distributor key rotation etc.
        - **For z/OS** – provides the trusted validation keys for z/OS Validated Boot

- **z/OS Software Support**
  - z/OS 2.5 post-GA support, delivered via z/OS CD APARs (5/2023); also 3.1 base
  - ServerPac installation workflow support

23

Support Details – Overall Solution

- **z/OS APARs**
  - ICKDSF – PH45198
  - Binder – OA63323
  - Signing Utility – OA63377
  - Supervisor – OA62783/OA63507
  - ASM/VSM – OA63420
  - RACF – OA61878
  - SAF – OA61901
  - SADMP – OA63404
  - IOS/Loadwait – OA63392
  - BCPii – OA63488

- **ServerPac z/OS Installation Workflow Support**

- **FIXCATs**
  - FIXCAT for Validated Boot for z/OS (all support):
    - **IBM.Function.ValidatedBoot**
  - FIXCAT for Exploitation support for z16:
    - **IBM.Device.Server.z16-3931.Exploitation**
  - FIXCAT for "Clean Room" Driving System (front-end support only):
    - **IBM.DrivingSystem-RequiredService**

24

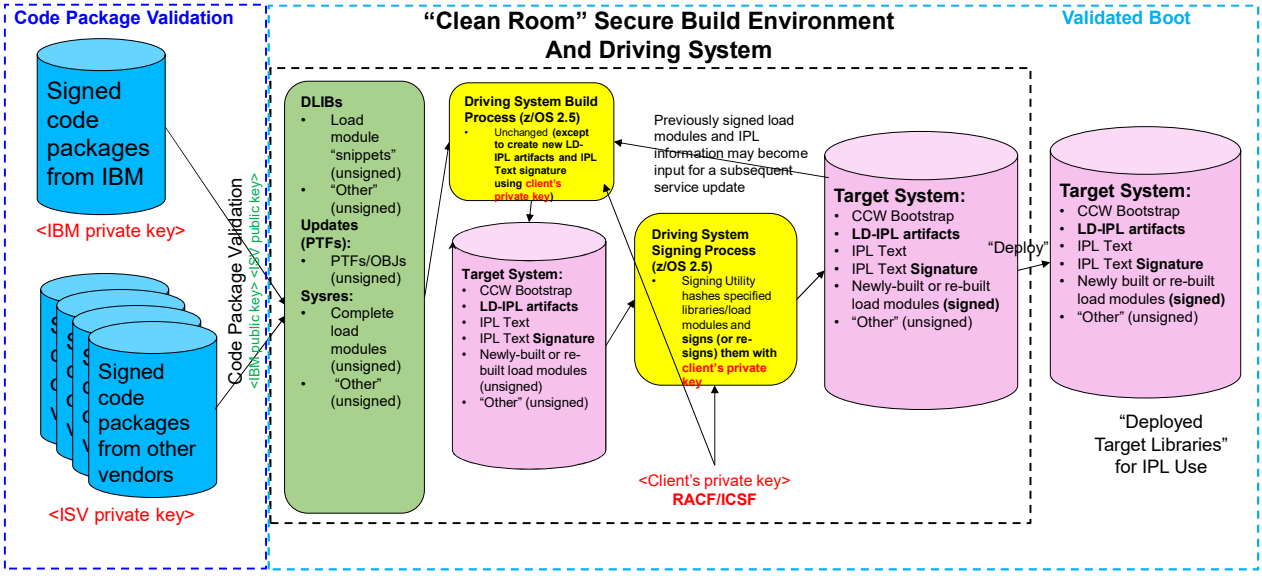
Support for z/OS Validated Boot is Optional

- **The use of z/OS Validated Boot is <u>entirely optional</u>**
  - **Clients may continue to build IPL Volumes in the "classic" way that does not support Validated Boot, and continue to perform unvalidated CCW IPLs, with no change**
  - **Clients may elect to build IPL volumes and sign load module executables in the new way to support Validated Boot, and then perform individual IPLs:**
    - In Validated Boot Enforce Mode (validation failure terminates IPL) using LD-IPL
    - In Validated Boot Audit Mode (validation failures are logged but do not terminate IPL) using LD-IPL
    - Unvalidated, using CCW-IPL
  - **Desired IPL mode is specified by authorized individuals via SE/HMC load panel/load profile UI or APIs**
  - **Software-initiated IPLs (AUTOIPL) *cannot* change the security mode of the IPL**

- *Use Audit Mode to discover signing and certificate setup issues, and correct them*
- ***Fallback capability** to performing unvalidated IPLs exists at all times*

25

Front-End Driving System Processing



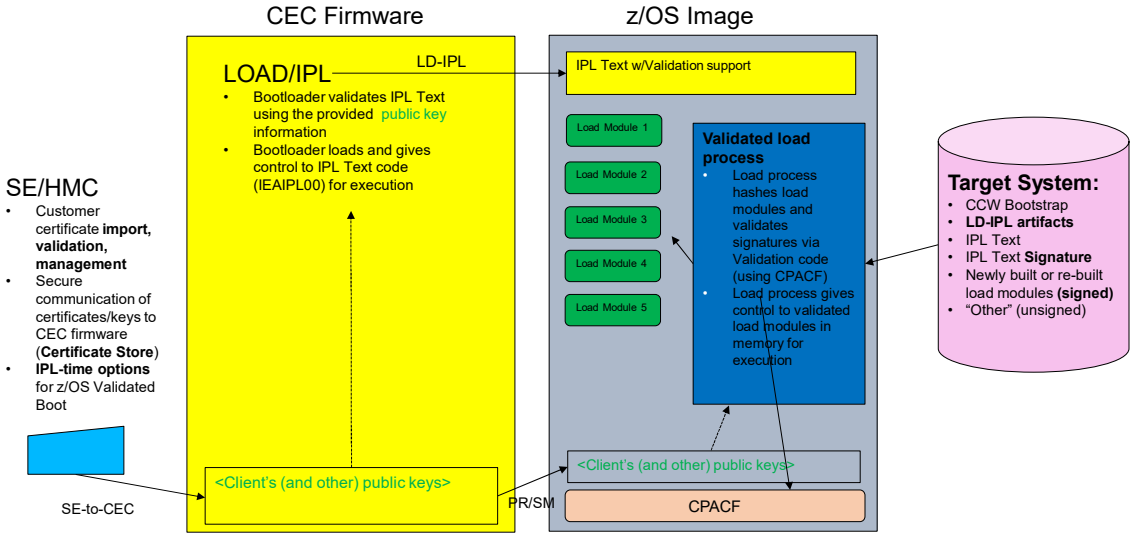
26

Support Requirements – Front-end Driving System (“Clean Room”)

- **No specific Hardware/Firmware requirements**
- **z/OS Software Support**
  - z/OS 2.5 post-GA support, delivered via z/OS CD APARs (5/2023); also 3.1 base
  - ServerPac installation workflow support
- **“One-time” setup**
  - RACF setup (including creation and assignment of signing certificates) needed for doing IPL Text signing and load module signing
  - Build Target System’s IPL Volume with LD-IPL artifacts needed to support Validated Boot
- **Recurring processes**
  - Build/re-build z/OS Target System
  - Sign/re-sign z/OS Target System IPL Text, Nucleus and LPA load modules
  - Rotate/delete/replace signing certificates as needed, and re-sign z/OS Target System

27

Back-End Target System z/OS Validated Boot Process (via LD-IPL)



28

Support Requirements – Back-end Target System ("IPLing System")

- **Hardware/Firmware Support**
  - z16 GA1.5 firmware
  - CPACF digital signature support with Elliptic Curve ECDSA-P521 support and SHA-512 hashing support
  - Virtual Flash Memory (VFM), aka Storage Class Memory (SCM), for use in z/OS paging for LPA pages
- **z/OS Software Support**
  - z/OS 2.5 post-GA support, delivered via z/OS CD APARs (5/2023); also 3.1 base
- **"One-time" setup**
  - Import public-key validation certificates to SE/HMC and assign to the set of LPARs where they will be needed for IPL-time validation
- **Recurring processes**
  - Rotate/delete/replace validation certificates via SE/HMC and reassign to LPARs as needed
  - Customize LOAD profiles and LOAD panel usage to request the desired IPL type for IPLs

29

KEYSMSTR Class Enhancements

- **Some applications have a need to connect to an external server such as LDAP. When connecting to an external server with a stored user ID and password, it's best to encrypt those credentials.**

- **KEYSMSTR Class:**
  - RACF/SAF provides functions for encrypting and decrypting passwords for external servers such as LDAP via the KEYSMSTR class.
  - Although the KEYSMSTR function is expressed in terms of the LDAP application (and DCE), any type of non-RACF-user password can be encrypted, saved in the RACF database, decrypted and returned to be used as a password to authenticate to the external server.
- **Encryption Algorithm:**
  - The existing KEYSMSTR class functions use the DES encryption algorithm.
  - Not NIST approved. Not quantum-safe.

30

KEYSMSTR Class – AES Support

•Starting with OA66458 (z/OS 2.5+) the RACF KEYSMSTR class functions provide an option for quantum-safe encryption with support for the AES encryption algorithm.

•Using an AES key with the KEYSMSTR class:

- With this support, the security administrator can now use the KEYLABEL field in the SSIGNON segment in the KEYSMSTR class profile to refer to an AES key in ICSF.
  - `RDEFINE KEYSMSTR LDAP.BINDPW.KEY SSIGNON(KEYLABEL(ICSF.KEY.LABEL))`
- The security administrator configures the application password in the application profile in the LDAPBIND class.
  - `RDEFINE LDAPBIND APPL01.PROFILE PROXY(BINDPW('PASSWORD'))`

•Other KEYSMSTR class usage (which now also support AES):

- R_dcekey functions that encrypt DCE passwords.
  - Uses the DCE.PASSWORD.KEY profile in the KEYSMSTR class.
- R_Proxyserv callable service can also use KEYSMSTR class profiles.
  - Uses the LDAP.BINDPW.KEY in the KEYSMSTR class.

31

Stronger Encryption for *Enveloped* Passwords/Password Phrases

- **OA66067 (z/OS 3.1) provides stronger, quantum-safe protection of RACF passwords and password phrases**
- **The RACF password enveloping symmetric encryption and signing algorithms are configured with the APPLDATA() keyword in profiles in the RACFEVNT class:**
  - Password Envelope Policy for passwords:
    `RDEFINE RACFEVNT PASSWORD.ENVELOPE APPLDATA('MD5/STRONG')`
  - Password Envelope Policy for password phrase:
    `RDEFINE RACFEVNT PASSPHRASE.ENVELOPE APPLDATA('MD5/STRONG')`

32

Logging of Supervisor State or Key 0 VSAM OPENs

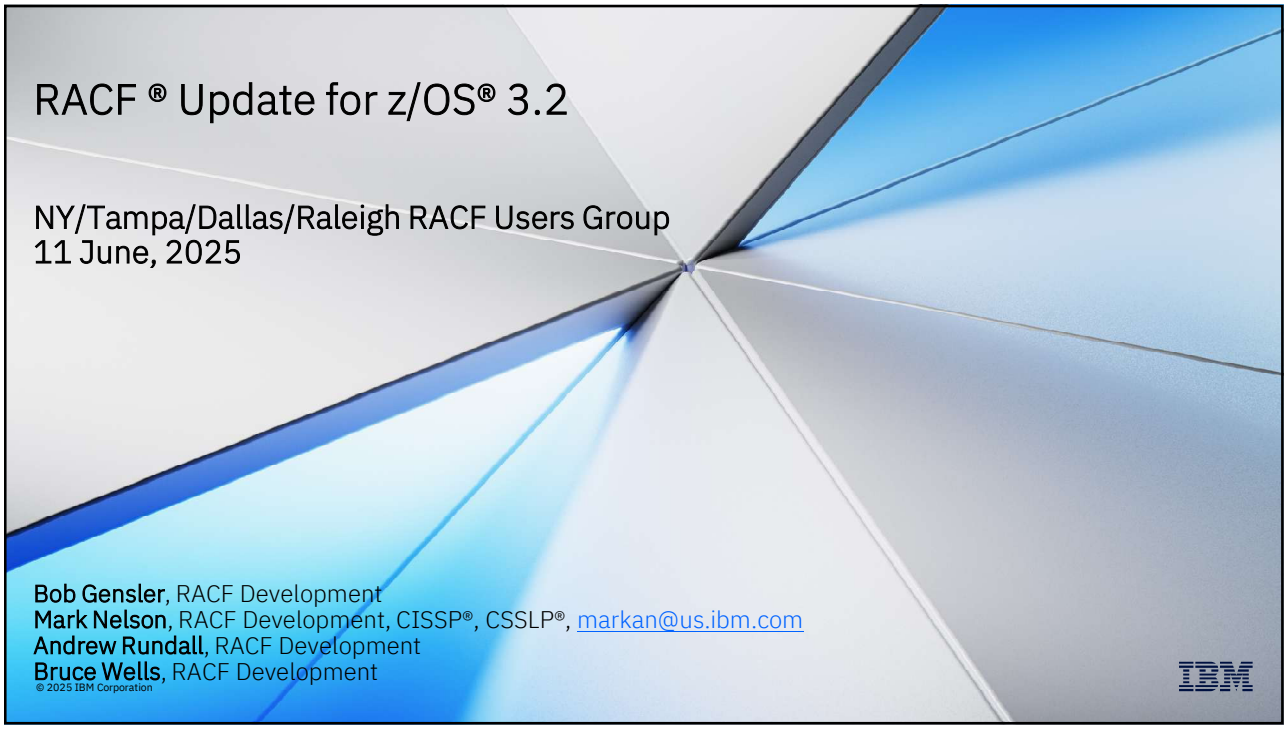
- **As documented in *z/OS DFSMS Using Data Sets:***
  - "VSAM OPEN routines bypass RACF security checking if the program issuing OPEN is in supervisor state or protection key 0".
    - No RACF call means access is allowed and no possibility for an SMF 80 record
- **APARs OA66738 and OA67032 allow you become aware of the places in which SAF check is being bypassed**
- **These APARs cause a REQUEST=AUTH to be performed against the resource STGADMIN.IGG.AUTO.BYPASS.LOG for READ authority in the FACILITY to write a log record**
  - Only successes are logged on authorization check (LOG=NOFAIL)
    - No log record is written if access is not allowed
  - The LOGSTR contains the data set name
    - `SAF CHECK BYPASSED FOR VSAM OPEN. PROGRAM NAME=<program name (8 char)>, JOB STEP=<job step name (8 char)>, DSN=<data set name (44 char)>`
  - Specifying AUDIT(SUCCESS) or AUDIT(ALL) causes the records to be written

33

Logging of Supervisor State or Key 0 VSAM OPENs…

- **The installation of APARs OA66738 and OA67032 and the definition of a profile covering the resource STGADMIN.IGG.AUTO.BYPASS.LOG in the FACILITY class will not affect the applications ability to OPEN the VSAM data set**

34


RACF ® Update for z/OS® 3.2
NY/Tampa/Dallas/Raleigh RACF Users Group
11 June, 2025
Bob Gensler, RACF Development
Mark Nelson, RACF Development, CISSP®, CSSLP®, markan@us.ibm.com
Andrew Rundall, RACF Development
Bruce Wells, RACF Development
© 2025 IBM Corporation
IBM

35