"ValBoot enables Secure Boot for z/OS. A feature of many modern computer systems, Secure Boot helps to ensure that only trusted software can be executed on the system. When Secure Boot is enabled for z/OS it will verify the digital signature of defined executables in signed libraries before allowing them to run."

Getting Started with ValBoot

An Image FOCUS Supplemental Application

ICE 18.0

See Also YouTube for ValBoot Training

NewEra Software Technical Support
800-421-5035 or 408-520-7100
support@newera.com

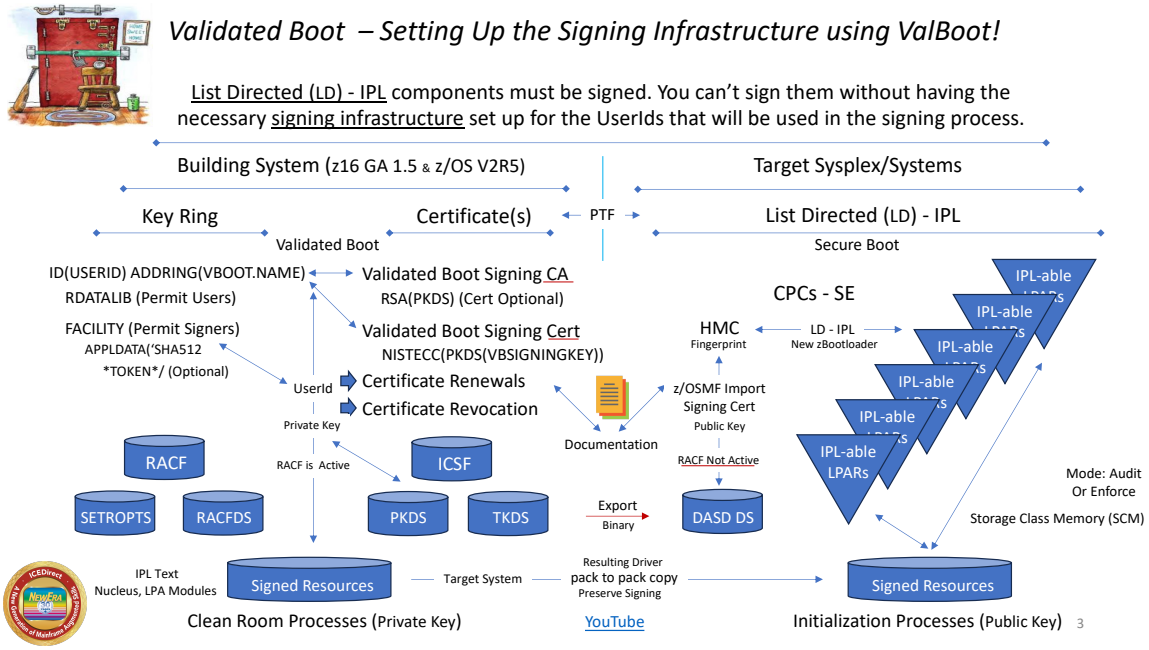
Rev: 2024-06-28

1. Table of Content

2.An Introduction to Validated Boot

Validated Boot is used in a Mainframe 'Clean Room' for the signing of z/OS resource objects including IPL text and various system datasets. The resulting signed objects are then copied to LPAR targets where they are used in the initialization of a List-Directed IPL (LD-IPL) also called 'Secure Boot'. The LD-IPL performs a verification process that helps to prevent viruses and other malicious software from running on the LPAR, making it more difficult for attackers to take over system level control. It is often used in conjunction with other security features of z/OS such as the External Security Manager (ESM), data encryption (ICSF), intrusion detection (PAGENT), Zero-Trust (ICE), and others to implement a multi-layered approach to overall z/OS security.

The diagram shown below outlines the major elements of the overall process necessary to achieve an LD-IPL: building and applying the Validated Boot RACF infrastructure on the left, and application of the signed resources to one or more LPARs via the HMC on the right.



1.1. ValBoot The Application

ValBoot is a full-screen 3270 application, executing either under TSO or ICE, that provides a straight forward way of interactively building key rings, certificates, profiles and access lists while also providing an interface for testing and deploying the resulting certificate resources. In addition, ValBoot will maintain and renew the created infrastructures, audit and monitor these infrastructures, and report potential problems, i.e. pending certificate expiration.

1.1.1. ValBoot Application Access and Licensing

Access is controlled via a valid Image FOCUS Supplemental Inspectors License Key. If the License Key is not present or has expired, the following message will be displayed.

1.2. Related Validated/Secure Boot References

Validated/Secure Boot is a unique process initially introduced in z/OS 2.5. Its intended purpose is to strengthen overall z/OS system integrity. This is a complex process and many questions may arise as to not only its purpose but also its internal details and constructs. The following references will address these issues and are recommended for review:

1.2.1. Detailed RACF Explanation

1.2.2. https://ibm.biz/zosValidatedBoot

1.2.3. IRR.PROGRAM.V2.SIGNING profiles

1.2.4. RACF Steps to the ValBoot Signing of Resources

1.3. Signing With ValBoot – Using IEWSIGN

When signings are attempted, the IBM provided signing application, IEWSIGN, with the PARM='ACTION=SIGN', will be called. This action will check for FACILITY class profiles, selecting the one that best matches the access profile of the signing UserId.

1.3.1. Signing Accountability and Responsibility

As shown in the diagram on the next page, there are several possible formats of the FACILITY class profile that may match the potential signer. Confusion can be minimized with designated signing structures if the following 'Best Practices' ValBoot recommended format is used:

IRR.PROGRAM.V2.SIGNING.UserId

This is specific to an individual user and is believed to be a best fit to establishing responsibility and accountability for signing actions.

Validated Boot – Setting Up the Signing Infrastructure using ValBoot!

1.4. ValBoot Application - User Roles

ValBoot supports three user roles – ADMIN, SIGNER, AUDITOR. Access is controlled via one of three Facility class profiles.

1.4.1. NEZ.VALBOOT.ADMIN UACC(NONE)

1.4.2. NEZ.VALBOOT.ISIGN UACC(NONE)

1.4.3. NEZ.VALBOOT.AUDIT UACC(NONE)

1.5. ValBoot Application - Administrator

The ValBoot Administrator (there can be more than one) MUST have RACF SPECIAL authority in order to execute the RACF and ICSF commands necessary to build the signing structure and assign appropriate roles and permits to ValBoot users.

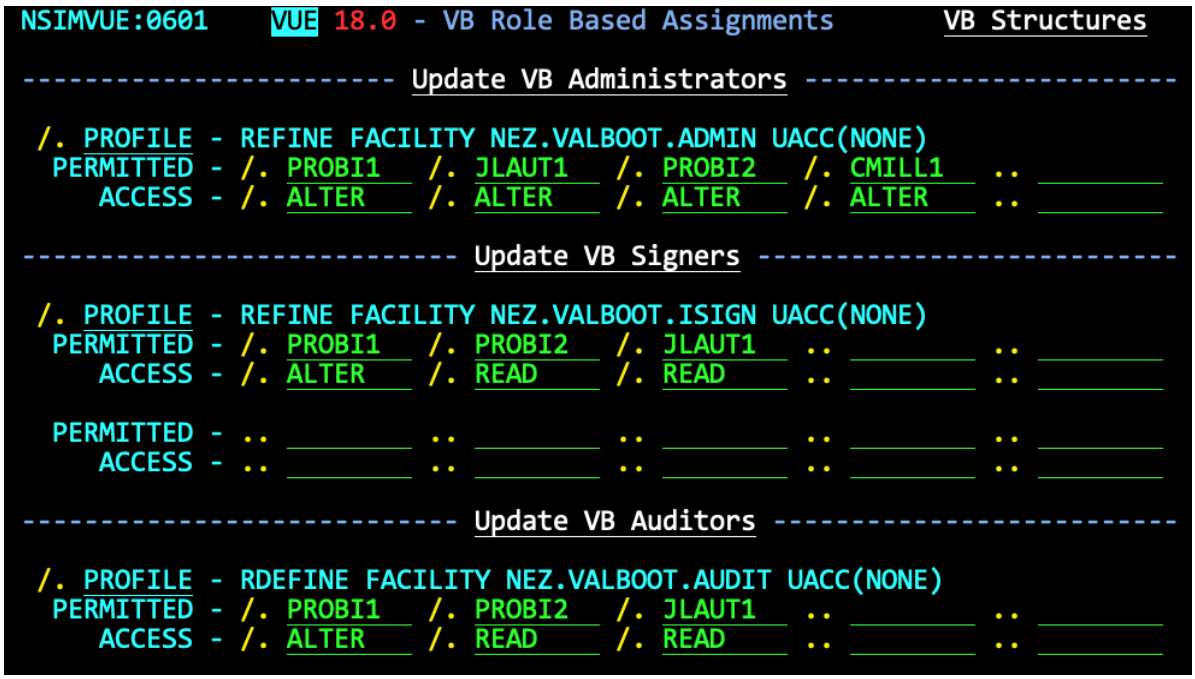
The first user to logon from the TSO/ISPF command line with:

TSO $CLI,*VB,ADMIN

that has SPECIAL authority will cause the ADMIN profile to be defined and also permit the user to the profile with ALTER access.

1.5.1. Assigning ValBoot User Roles

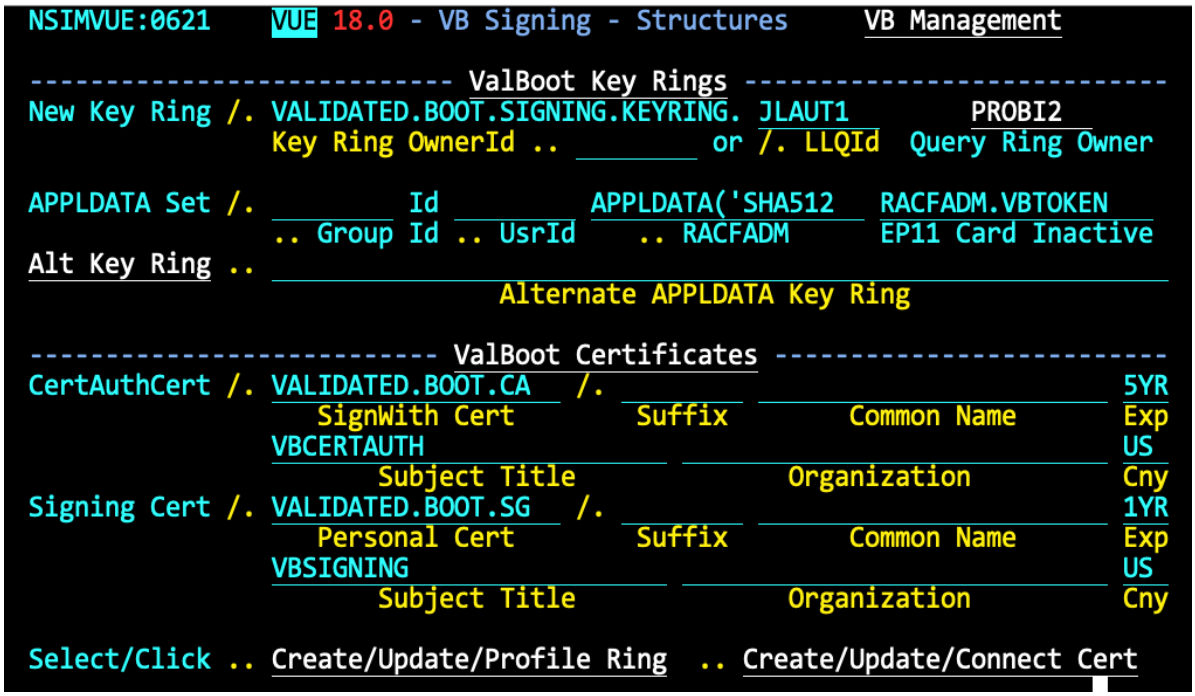
Once logged in as the ADMIN, the user may assign the signing and auditing roles by navigating to the ValBoot Management Options panel and selecting Assign Roles and following the Help instruction, PFK1.



3. ValBoot - Quick Start

The panel shown below is always presented to the ValBoot Administrators when they login. It offers not only the necessary interface for building key rings and certificates but it also provides access to the existing inventory contained RACF. To display the current inventory and its status, cursor under either of the major headings – ValBoot Key Rings or ValBoot Certificates - and press Enter.

Note that if a problem is detected with certificate expiration a warning will be displayed.



1.1. The First Key Ring

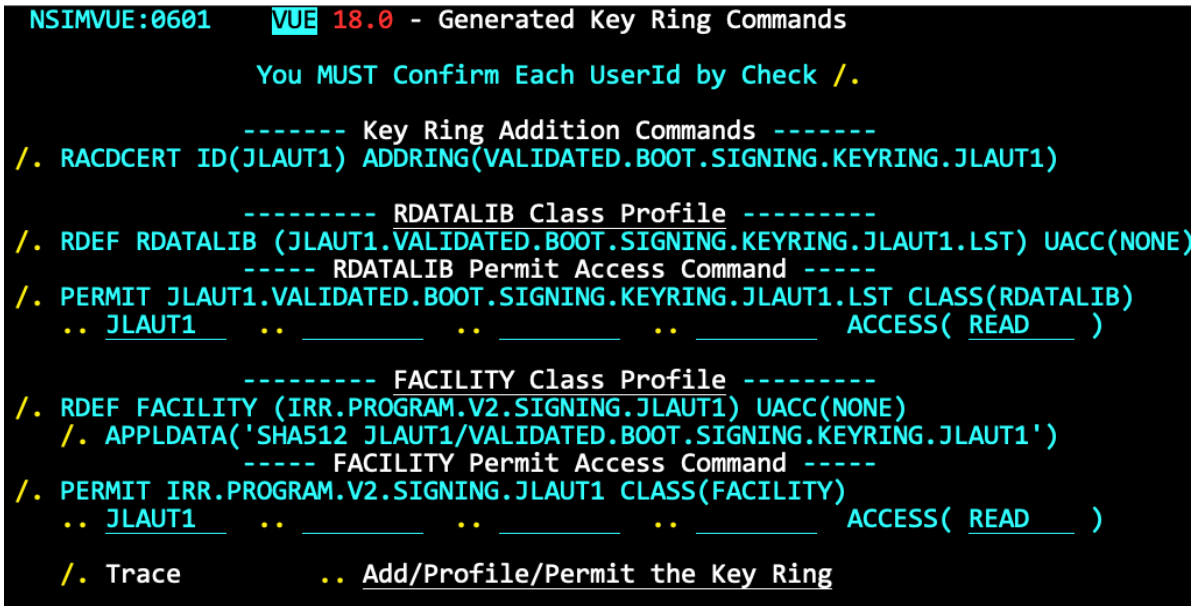
As the Structures Panel infers there are several different formats that can be used to define a signing key ring. Best practice is to construct one for each individual signing user. To do this, enter a valid userid in LLQId (in this example JLAUT1), check below and then cursor down under Create/Update/Profile Ring and press Enter. These actions will validate the panel input, report problems and, if all is proper, generate the RACF/RACDCERT commands necessary to generate:

- Key ring with LLQId as owner
- FACILITY class profile with APPLDATA entry permitting owner
- RDATALIB class profile permitting owner

These generated commands will be shown in a panel that follows and should be checked carefully before continuing. If problems are discovered, PFK3 to backup, make the required correction(s) and resubmit to continue.

A sample Generated Key Ring Commands panel follows.

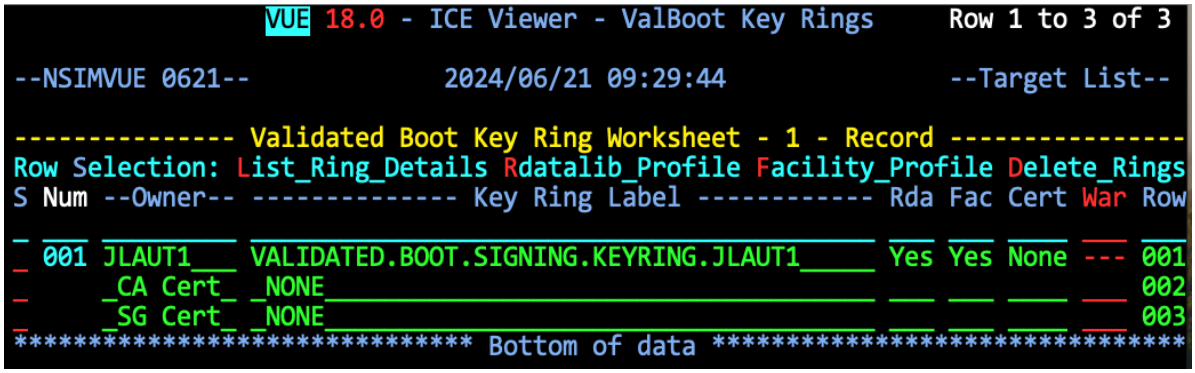
Note that JLAUT1 is named in both the Key Ring extension and is the owner of the Key Ring and is included in the RDATALIB and FACILITY profiles and permits.



Permit additional users as needed and then cursor under Add/Profile/Permit the Key Ring and press Enter. This will result in the issuance of the displayed commands and the display of the Trace Report.

Examine the report for any possible problems or errors encountered as reported by RACF during actual command execution.

To continue, press PFK3. This action will display the Key Ring Worksheet as shown below:



If problems were reported in the TRACE, delete the key ring, troubleshoot the cause of the problem (NewEra Technical Support can help), and repeatkey ring build.

The next step is to generate the Certificate Authority (CA) and Signing Certificates (SG). To do this, PFK3 back to the Primary/Structures Panel.

1.2. Your First Certificate Set

ValBoot certificates come in pairs - first is the Certificate Authority (CA) certificate and the second, which is signed by the CA certificate, is the Personal/Signing certificate (SG). It will appear as the DEFAULT certificate when connected to the target key ring.

Because the certificates are paired, it is imperative that the suffix values assigned to each match. This ensures that should a signing certificate need to be renewed, the pair will be rematched correctly. One practice would be to assign the name of the CEC (Central Electronic Complex) that will ultimately perform the LD-IPL of its LPARs. By using this method in a multi-CEC environment, it should be become clear which certificate pair is used with which CEC and therefore which certificate fingerprint should be referenced in the receiving HMC.

Common Name and Organization are required to differentiate certificate “Subject Names” from existing certificates. Take care to not reuse values in future certificate pairs. Certificate expirations are set by default to ‘5YR’ and ‘1YR’. To change defaults, overtype the numeric value leaving ‘YR’ in place. By default, country is ‘US’, overtype to change.

Next, cursor under Create/Update/Connect Cert and press Enter. These actions will validate the panel input, report problems and generate the RACF/RACDCERT/ICSF commands necessary to:

- Generate the CA and Signing Certificate
- Connect the CA and Signing Certificate to the key ring
- Store the CA and Signing Certificate Key Pairs in ICSF/PKDS

A sample Generated Certificate Commands panel follows.

```
NSIMVUE:0601    VUE 18.0 - Generated Certificate Commands

   /. Change the Key Ring: JLAUT1/VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1

   /. Confirm      ---- RACDCERT GENCERT CERTAUTH ----

      WITHLABEL('VALIDATED.BOOT.CA.CEC006') SUBJECTSDN(CN('JLNAME')
      T('VBCERTAUTH') O('JLORGN') C('US'))
      ALTNAME(DOMAIN('WWWDOMAIN')) KEYUSAGE(CERTSIGN)
      NOTAFTER(DATE(2029/06/05)) TIME(23:59:59))
      RSA(PKDS(VALIDATED.BOOT.CA.CEC006)) SIZE(4096)

   /. Confirm      ---- RACDCERT GENCERT ID(JLAUT1) ----

      SIGNWITH(CERTAUTH LABEL('VALIDATED.BOOT.CA.CEC006'))
      WITHLABEL('VALIDATED.BOOT.SG.CEC006') SUBJECTSDN(CN('JLNAME')
      T('VBSIGNING') O('JLORNG') C('US'))
      ALTNAME(DOMAIN('WWWDOMAIN')) KEYUSAGE(HANDSHAKE DOCSIGN)
      NOTAFTER(DATE(2025/06/05)) TIME(23:59:59))
      NISTECC(PKDS(VALIDATED.BOOT.SG.CEC006)) SIZE(521)

   /. Trace        .. Generate/Sign/Connect Certificates
```

Review the commands shown in the panel carefully taking special note of the key king shown at the top. If problems are noted, use PFK3 to back up, make necessary corrections and resubmit.

Continue by placing the cursor under Generate/Sign/Connect Certificates and press Enter. This will result in the issuance of the displayed commands and the display of the Trace Report.

```
/*****************************************************************************/
/*                                                                           */
/*        ICE Viewer - NSIMVUE - Validated Boot Trace Records - PROBI2       */
/*                Report Date:2024/06/21 Report Time:09:29:44                */
/*                     TRACEDS:PROBI2.$VALBOOT.$CTRACE                       */
/*                                                                           */
/*****************************************************************************/

--- Generate Certificates, Connections & Replies ---

RACDCERT GENCERT CERTAUTH WITHLABEL('VALIDATED.BOOT.CA.CEC0JL') SUBJECTSDN(CN('J
IRRD175I The new profile for DIGTCERT will not be in effect until a SETROPTS REF

RACDCERT ID(JLAUT1) CONNECT(CERTAUTH LABEL('VALIDATED.BOOT.CA.CEC0JL') RING(VALI
NO REPLY RECEIVED

ICH10006I RACLISTED PROFILES FOR CSFKEYS WILL NOT REFLECT THE ADDITION(S) UNTIL

PERMIT VALIDATED.BOOT.CA.CEC0JL CLASS(CSFKEYS) ID(JLAUT1) ACCESS(READ)
```

Examine the report for any possible problems or errors encountered and reported by RACF and/or ICSF during actual command execution. Press PFK3 to display the Key Ring

Worksheet which now shows the newly generated certificates as connected to the targeted Key Ring.

```
                VUE 18.0 - ICE Viewer - ValBoot Key Rings     Row 1 to 3 of 3

--NSIMVUE 0621--              2024/06/21 09:29:44              --Target List--

--------------- Validated Boot Key Ring Worksheet - 1 - Record ---------------
Row Selection: List_Ring_Details Rdatalib_Profile Facility_Profile Delete_Rings
S Num --Owner-- -------------- Key Ring Label ------------ Rda Fac Cert War Row
_ ___ ________ ____________________________________ ___ ___ ____ ___ ___
_ 001 JLAUT1___ VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1_____ Yes Yes __02 --- 001
_     _CA Cert_ _VALIDATED.BOOT.CA.CEC0JL_________________ ___ ___ ____ ___ 002
_     _SG Cert_ _VALIDATED.BOOT.SG.CEC0JL      DEFAULT:YES ___ ___ ____ ___ 003
******************************** Bottom of data ********************************
```

Select List_Ring_Details to display the Certificate Operations worksheet as shown below. From the worksheet you can export the Signing Certificate to a targeted HMC and/or renew it and the CA Certificate as necessary.

```
                VUE 18.0 - ValBoot - Certificate Operations   Row 1 to 2 of 2

--NSIMVUE 0621--              2024/06/21 09:29:44              --Target List--

------------ VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1 - 2 - Records ------------
Row Selection: List_Certificates Export_Cert Renew_Cert Delete_Cert Common_Name
S Row -Owners- --------- Certificate Labels --------- -Usages- Dfl EndDates War
_ ___ ________ ____________________________________ ________ ___ ________ ___
_ 001 CERTAUTH VALIDATED.BOOT.CA.CEC0JL_____________ CERTAUTH NO_ 29/06/21 ---
_ 002 PROBI2__ VALIDATED.BOOT.SG.CEC0JL_____________ PERSONAL YES 25/06/21 ---
******************************** Bottom of data ********************************
```

Select each certificate with List Certificates and review their contents. If a problem is noted, use Delete_Cert to delete each certificate and PFK3 back to the Primary/Structure Panel and try again.

If things are valid, it's time to test the structure and attempt an actual library signing.

1.3. Testing a Signing Structure Works

To attempt a library signing, PFK3 back to the Primary/Structure Panel and from the upper right, select VB Management. This action will display the Management Tools Panel. Note at the bottom of the panel the IEWSIGN option as shown below:

I IEWSIGNS .. - Validate UserId as a Real World Signer

```
I   IEWSIGNS  ..  - Validate JLAUT1   as a Real World Signer
```

Enter the UserId, in this case JLAUT1, of the signing user whose signing structure is to be tested and press Enter. This action will display the IEWSIGN Action:ADMIN Panel.

In order to submit the IEWSIGN job used in validation, the session owner, if different from the specified signing userId, will need submit authority in order to act on behalf of the signing user.

If the session owner does not have the necessary permissions to submit for the signer the following message is displayed.

For the session owner to act as the signer, these RACF steps must be performed:

Under TSO option 6 issue the following to determine if the signer has a profile.
RLIST SURROGAT signerId.SUBMIT AUTHUSER

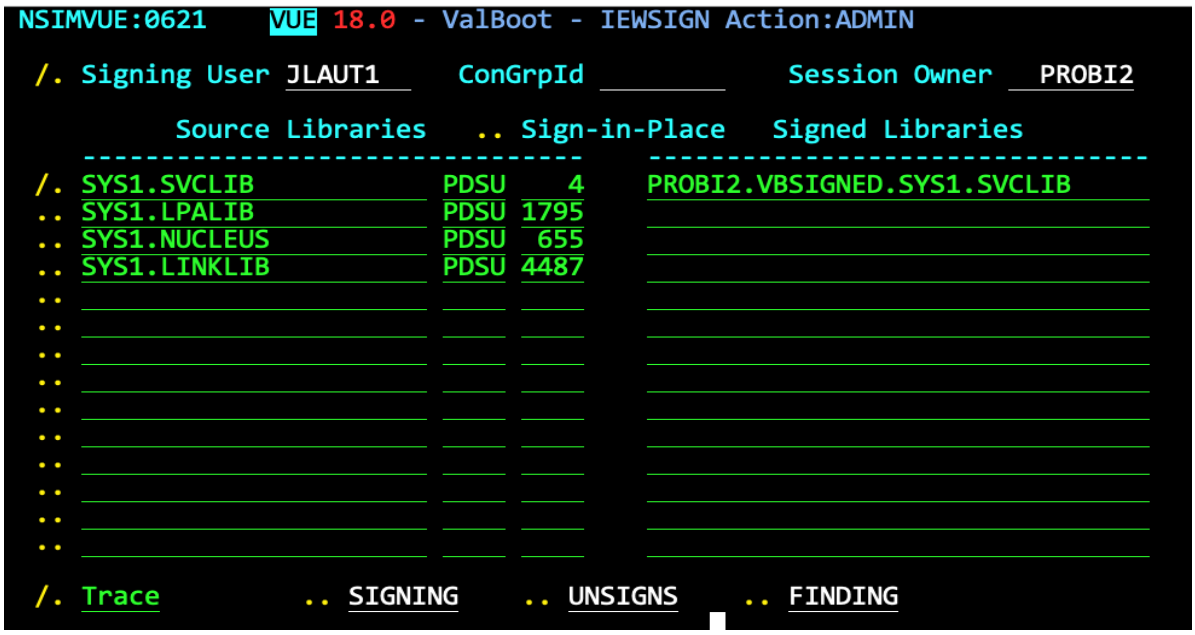
If a SURROGAT class profile for the signing userId does not exist, do the following:

RDEFINE SURROGAT signerId.SUBMIT UACC(NONE)

Finally, issue the following to permit the session owner to the profile
PERMIT signerid.SUBMIT CLASS(SURROGAT) ID(session_owner) ACCESS(READ)

This is a sensitive action and should be reviewed by the security department before proceeding.

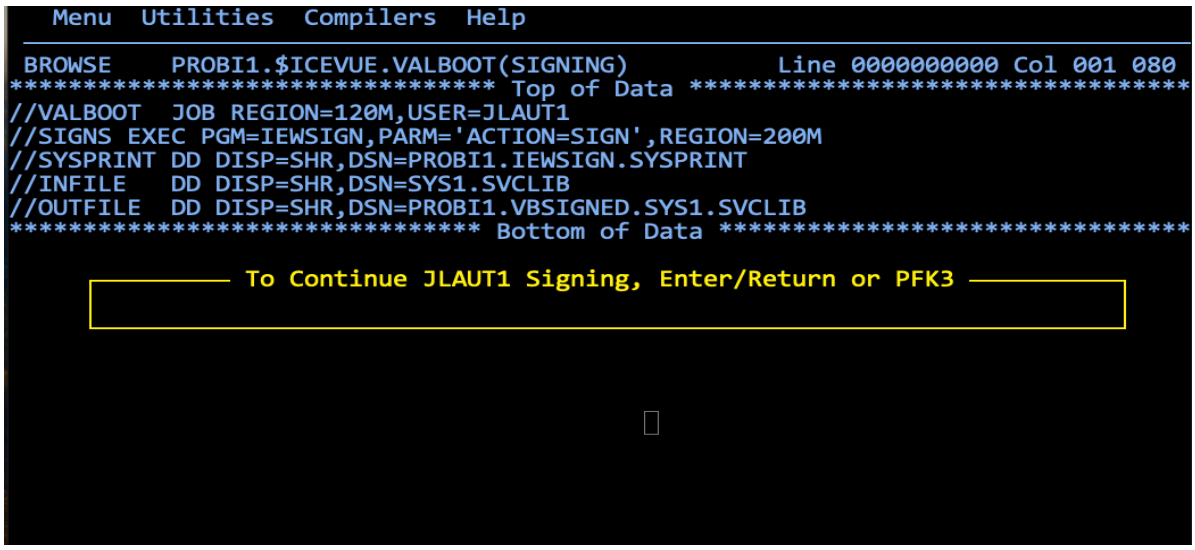
Note that the signing user is the UserId from the prior panel. The Session Owner is the ValBoot Admin who is performing the signing test using IEWSIGN on behalf of the Signing User.



The Source Libraries column is specific to and maintained for each Session Owner and intended to contain only libraries that have undefined record formats, i.e. LPALIB, NUCLEUS. ConGrp is used in a case where users in a specified connect group are being tested. This use-case is explained later in this document. Review PFK1 Help.

1.4. Your First Library Signing

With prerequisites in place, Admins can test for a signer. A good test selection would be a small library i.e. SYS1.SVCLIB. Enter the test selection, cursor under Signing and press enter. These actions will generate and display the IEWSIGN JCL, a sample of which is shown below:



Note the user named on the Job Card is the signing user while the SYSPRINT and OUTFILE DDs are prefixed with the owner's UserId. It is necessary to permit the signing user with update access to DD/datasets highlighted below.

```
//VALBOOT  JOB REGION=120M,USER=JLAUT1,GROUP=SYS1
//SIGNS EXEC PGM=IEWSIGN,PARM='ACTION=SIGN',REGION=200M
//SYSPRINT DD DISP=SHR,DSN=PROBI2.IEWSIGN.SYSPRINT
//INFILE   DD DISP=SHR,DSN=SYS1.SVCLIB
//OUTFILE  DD DISP=SHR,DSN=PROBI2.VBSIGNED.SYS1.SVCLIB
```

To submit the job, press Enter. This action will call IEWSIGN to sign the library named on the INFILE DD and display the Signing Report.

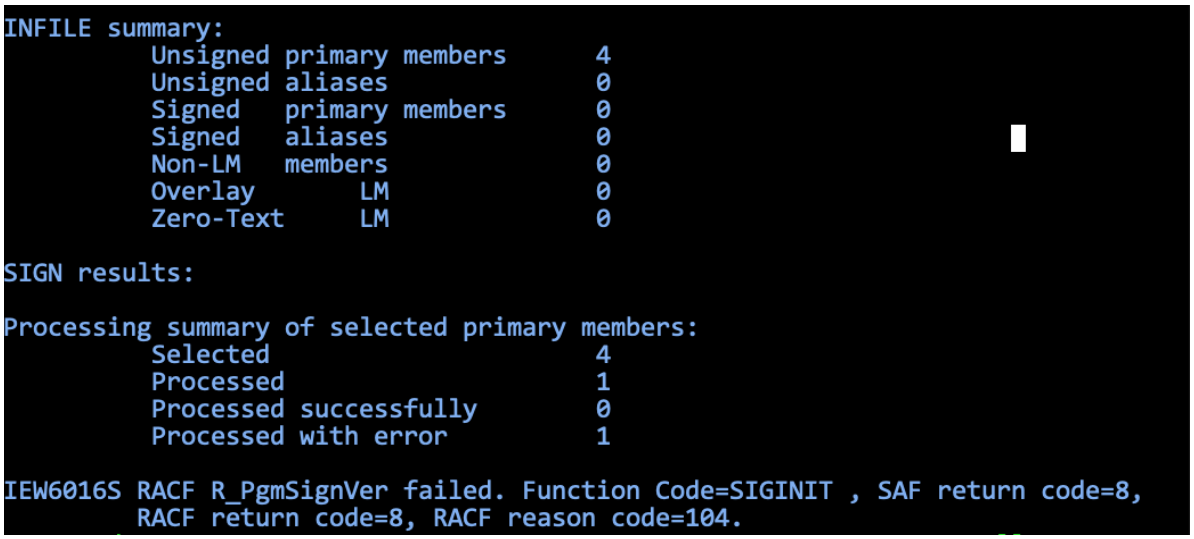
1.5. When a Signing Fails

Should the signing user not be able to write to the DD/datasets the following message will be displayed:

Should the signing process continue but fail for other reasons, a message similar to the following will be displayed:

1.5.1. Return and Reason Codes

When a signing fails, the Signing Report will provide Return and Reason Codes that point to issues preventing a successful signing as shown at the bottom of the image below:



A partial list of Return and Reason Codes is shown below. See Full List

Table 2. SIGINIT specific return and reason codes

SAF return code	RACF return code	RACF reason code	Explanation
8	8	100	Signature operation is already in progress for the specified program name.
8	8	104	Security Manager is unable to determine the key ring to use.
8	8	108	Syntax error in supplied key ring name, or in the key ring name contained within the APPLDATA of the RACF FACILITY class profile.
8	8	112	Key ring does not exist or does not contain a default certificate.
8	8	116	Caller not authorized to use R_datalib to access the key ring.
8	8	120	Certificate chain in the key ring is incomplete.
8	8	124	Certificate chain contains more than 10 certificates, or key ring contains more than 50 certificates. (Some of these might not constitute part of the trust chain. However, you should not connect any certificates that do not.)
8	8	128	CA certificate in the key ring does not have certificate signing capability. (KeyUsage extension present but keyCertSign flag is off or BasicConstraints extension is present but cA flag is off.)
8	8	132	Default certificate in key ring does not have a private key.
8	8	136	Default certificate in key ring does not have code signing capability. (KeyUsage extension present but digitalSignature or nonRepudiation flag is off.)

1.5.1. Possible Problem Resolutions

Reason 104 – Check FACILITY APPLDATA for conflicts
Reason 112 – Check key king for valid certificates
Reason 116 – Check RDATALIB if UserId permitted
Reason 120 – Check that both CA and SG are on the key ring

1.6. When a Signing is Successful

When a signing is successful, the IEWSIGN Signing Report will provide that indication module by moduleMODULE. A sample report is shown below:

```
Invocation parameters: ACTION=SIGN
Execution  Parameters: ACTION=SIGN,STATE=ALL,VERBOSE=NO,RC4LIM=2147483647,RC8LIM

DD        Data Set Name                              Volume       Block Size
INFILE    SYS1.SVCLIB                                C5RES1       6144
OUTFILE   PROBI1.VBSIGNED.SYS1.SVCLIB                ZWORK5       32760

INFILE summary:
          Unsigned primary members      4
          Unsigned aliases              0
          Signed   primary members      0
          Signed   aliases              0
          Non-LM   members              0
          Overlay       LM              0
          Zero-Text     LM              0

SIGN results:
IGG019PX  Successful
IGG019PY  Successful
```

1.6.1. *Posting to the Control Journal*

To record and document the signing event, a condensed version of the report may be posted to the Control Journal. Press Enter for that action, otherwise press PFK3 to return.

1.6.2. *Showing Signing Findings Details*

If continuing, the next option is to show the ValBoot Detail Signing Report, press Enter. If not PFK3 to return.

If continuing, the next step is to run IEWSIGN once more with ACTION=REPORT. A sample of the JCL is shown below, PFK3 to submit.

```
//VALBOOT  JOB REGION=120M,USER=PROBI1
//SIGNS EXEC PGM=IEWSIGN,PARM='ACTION=REPORT,VERBOSE=YES,REPORTLEVEL=3'
//SYSPRINT DD DISP=SHR,DSN=PROBI1.IEWSIGN.REPORTS
//INFILE   DD DISP=SHR,DSN=PROBI1.VBSIGNED.SYS1.SVCLIB
```

When the report is complete, the following options will be displayed press Enter to display the report or PFK3 to return. A sample report is shown on the next page.

Show SYS1.SVCLIB Signing Details, Return/Enter, or PFK3

```
/*******************************************************************************
/*         ICE Viewer - NSIMVUE - ValBoot Certificate Detail - PROBI1
/*               Report Date:2024/06/07 Report Time:16:39:55
/*                    Dataset:PROBI1.$VALBOOT.$DETAIL
/*   Source Library:SYS1.SVCLIB, Target Library:PROBI1.VBSIGNED.SYS1.SVCLIB
/*                          Signing UserId:JLAUT1
/*******************************************************************************

          Digital certificate information for user JLAUT1:

          Label: VALIDATED.BOOT.SG.CEC006
          Certificate ID: 2QbR08Hk4/HlwdPJxMHjxcRLwtbW40vix0vDxcPw8PZA
          Status: TRUST
          Start Date: 2024/06/05 00:00:00
          End Date:   2025/06/05 23:59:59
          Serial Number:
          >01<
          Issuer's Name:
          >CN=JLNAME.T=VBCERTAUTH.O=JLORGN.C=US<
          Subject's Name:
          >CN=JLNAME.T=VBSIGNING.O=JLORNG.C=US<
          Subject's AltNames:
          Domain: WWWDOMAIN
          Signing Algorithm: sha256RSA
          Key Usage: HANDSHAKE, DOCSIGN
          Key Type: NIST ECC
          Key Size: 521
          Private Key: YES
          PKDS Label: VALIDATED.BOOT.SG.CEC006
          Certificate Fingerprint (SHA256):
          70:11:B6:ED:C1:6D:6B:19:EE:E7:85:C4:04:3E:6D:49:
          07:D5:5C:46:89:B8:59:CE:82:07:61:FB:FA:4E:B4:9C
          Ring Associations:
          Ring Owner: JLAUT1
          >VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1<
         ---- Connected Certificates -----
                     Label                    Owner            Usage    Default
          VALIDATED.BOOT.CA.CEC006          CERTAUTH         CERTAUTH     NO
          VALIDATED.BOOT.SG.CEC006          ID(JLAUT1)       PERSONAL     YES

        -------- PKDS Label Meta --------
            PKDS Key Label: VALIDATED.BOOT.SG.CEC006
               Create Date: 24/06/05
               Create Time: 12:38:16
               Update Date: n/a
               Update Time: n/a
          Callable Service: CSFDSG
                Start Date: n/a
                 Stop Date: n/a
                Last Usage: 24/06/07
              Archive Date: n/a
             Archive State: OFF
          Archive Prohibit: OFF
            Archive Recall: n/a
         PrivateKey Status: Active
         --------- Key Attributes ---------
                 Key Usage: KEYM SIGN NO-XLATE
          Key Format/Curve: PRIME
            Curve P (bits): 521
           Curve Q (bytes): 133
            Modulus (bits): n/a
                  Sections: PRIVATE PUBLIC
          Private Key Name: n/a
         -------- Security Profile --------
           CSFKEYS Profile: PROBI1/VALIDATED.BOOT.SG.CEC006/NONE
             SYMEXPORTABLE: BYLIST
                 ASYMUSAGE: HANDSHAKE SECUREEXPORT
              SYMCPACFWRAP: YES
               SYMCPACFRET: YES
                 Permitted: PROBI1 ALTER
                 Permitted: JLAUT READ
```

1.6.3. *Exporting the Signing Certificate*

To continue, PFK3. This action will present the Certificate Export option.

Press Enter to show Export panel or PFK3 to return. Once in the panel, use PFK1 for Help

Review the panel content carefully. Note that ValBoot maintains an Export Registry, by version, as defined in the panel. By default the version number is the current date and time. These values may be overtyped as needed to customize the versioning to fit a particular need.

When satisfied with the entries in the panel, cursor under Select to Export Certificate and press Enter. These actions will record the panel values in the ValBoot Export Registry and in the Control Journal. In addition, ValBoot will allocate the Export Dataset, formulate and submit the RACDCERT EXPORT commands necessary to write the SG (signing) certificate into the dataset and finally display the content as shown on the following page:

```
 BROWSE    PROBI1.PERSONAL.EXPORT.DATASET          Line 00000000
******************************** Top of Data ********************
-----BEGIN CERTIFICATE-----
MIIEOzCCAiOgAwIBAgIBATANBgkqhkiG9w0BAQsFADBEMQswCQYDVQQGEwJVUzEP
MA0GA1UEChMGSkxPUkdOMRMwEQYDVQQMEwpWQkNFUlRBVVRIMQ8wDQYDVQQDEwZK
TE5BTUUwHhcNMjQwNjA1MDcwMDAwWhcNMjUwNjA2MDY1OTU5WjBDMQswCQYDVQQG
EwJVUzEPMA0GA1UEChMGSkxPUk5HMRIwEAYDVQQMEwlWQlNJR05JTkcxDzANBgNV
BAMTBkpMTkFNRTCBmzAQBgcqhkjOPQIBBgUrgQQAIwOBhgAEAChrDC1vIpP0Ubvu
7sNDQo/j/jVzr/G2HLcKFdlVFNxkvrAeti2/UF+sPCskL8vbA72I+PE9pi5wPy1q
kkGQ40y2AYk9rIX5HtJnAQt3Uqy9xdCCFRdHv1G9leenGLDrdf2Q85hG9AW8/pOz
vARGciovOn4mZfajVm030x5kARr1tlR9o4HAMIG9MD8GCWCGSAGG+EIBDQQyFjBH
ZW5lcmF0ZWQgYnkgdGhlIFNlY3VyaXR5IFNlcnZlciBmb3Igei9PUyAoUkFDRikw
FAYDVR0RBA0wC4IJV1dXRE9NQUlOMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQU
vXfkHdvBD0kXW3mcurm1nYAJX0MwHwYDVR0jBBgwFoAUcHFJFaQsYxpkkpN7TJsq
wotSlmYwFAYDVR0SBA0wC4IJV1dXRE9NQUlOMA0GCSqGSIb3DQEBCwUAA4ICAQAa
LpbgG3gbyUO5L9QOZ40oQZe5h/2xtzWyBnPWIdrB7mIK6xh59AwQVV22hfhPObAs
mvGch5ZhKS2l9xe8KWkaHWrOMlBKTilKb48zCUIif9c59EdfgtMIx/XVpRzmaAu0
/5ZReZZ0xlMsnCqdEkEMwuT4/8IBuyy3EOMOnP5vpGEAb09qipauKIQMvajh2rj6
rbpAlXbz9KWbFlJfRI9QBygdo/n/9KQLiaEfwYohboFqUOoaFbP2P1JTIdbkN1IS
KSdKdrUeI7tPqr+bkZ3hOQCPV5azAMU1rEeCV+9TkaOGXGdQTcHwWmV8L5PM2XBG
rIbuyTymzyjWUtokQVhemQTbBJevSZApC55l/bGxBXCE6ifbDb/41NeF4UY4oShK
f02xgPwkbcb5OpktUFg7AxF6Ff2Tn1Bj5g9P0H57tft9hP7OMGnlf91f8jn30oXf
A0zbG/kHqrNFp4wL+a0YzJzRTlWbUrgZ/WLfFTeHL5P0zBHASQejbfxr0K4PDaT7
L6xZNRm/P/7bC4spzqrHVLtWl22KVjHEPEfS5qGmliHs6TUEJdp8PfOMDY3c2K4u
/eQ7R08bnzmDQQi/8x5M4JXRwM6F7GJdzRN1Go3Q0zBpOnfx/hlGLmtD2gUhnoQn
q7uqv8v4c6ZQeQp+ZacZhasVy5QCjdzwk3d4Rz9s1A==
-----END CERTIFICATE-----
```

A sample of an Export Registry entry, as shown on the following page, should be considered as an alternative or an addition to sending along just the export dataset to its HMC destination as it documents the complete set of export actions.

```
/*******************************************************************************/
/*        ICE Viewer - NSIMVUE - Certificate Export Registry - PROBI1          */
/*             Export Create Date:2024/06/07 Report Time:16:39:55              */
/*            Registry DS:PROBI1.PERSONAL.EXPREGDS.D240607.T171925             */
/*                  Export DS:PROBI1.PERSONAL.EXPORT.DATASET                   */
/*******************************************************************************/

Source Library:SYS1.SVCLIB, Target Library:PROBI1.VBSIGNED.SYS1.SVCLIB
Signing UserId:JLAUT1
---Certificate:JLAUT1/VALIDATED.BOOT.SG.CEC006
----Export DSN:PROBI1.PERSONAL.EXPORT.DATASET

---Private Key:YES, Trust:Is Trusted
-End Date/Time:2025/06/05 23:59:59
-----Algorithm:(SHA256):
--Finger Print:70:11:B6:ED:C1:6D:6B:19:EE:E7:85:C4:04:3E:6D:49:
--------------:07:D5:5C:46:89:B8:59:CE:82:07:61:FB:FA:4E:B4:9C

-----Export Command Syntex:
-----RACDCERT EXPORT(LABEL('VALIDATED.BOOT.SG.CEC006'))
-----ID(JLAUT1)
-----DSN(PROBI1.PERSONAL.EXPORT.DATASET)
-----FORMAT(CERTB64)

-----BEGIN CERTIFICATE-----
MIIEOzCCAiOgAwIBAgIBATANBgkqhkiG9w0BAQsFADBEMQswCQYDVQQGEwJVUzEP
MA0GA1UEChMGSkxPUkdOMRMwEQYDVQQMEwpWQkNFUlRBVVRIMQ8wDQYDVQQDEwZK
TE5BTUUwHhcNMjQwNjA1MDcwMDAwWhcNMjUwNjA2MDY1OTU5WjBDMQswCQYDVQQG
EwJVUzEPMA0GA1UEChMGSkxPUk5HMRIwEAYDVQQMEwlWQlNJR05JTkcxDzANBgNV
BAMTBkpMTkFNRTCBmzAQBgcqhkjOPQIBBgUrgQQAIwOBhgAEAChrDC1vIpP0Ubvu
7sNDQo/j/jVzr/G2HLcKFdlVFNxkvrAeti2/UF+sPCskL8vbA72I+PE9pi5wPy1q
kkGQ40y2AYk9rIX5HtJnAQt3Uqy9xdCCFRdHv1G9leenGLDrdf2Q85hG9AW8/pOz
vARGciovOn4mZfajVm030x5kARr1tlR9o4HAMIG9MD8GCWCGSAGG+EIBDQQyFjBH
ZW5lcmF0ZWQgYnkgdGhlIFNlY3VyaXR5IFNlcnZlciBmb3Igei9PUyAoUkFDRikw
FAYDVR0RBA0wC4IJV1dXRE9NQUlOMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQU
vXfkHdvBD0kXW3mcurm1nYAJX0MwHwYDVR0jBBgwFoAUcHFJFaQsYxpkkpN7TJsq
wotSlmYwFAYDVR0SBA0wC4IJV1dXRE9NQUlOMA0GCSqGSIb3DQEBCwUAA4ICAQAa
LpbgG3gbyUO5L9QOZ40oQZe5h/2xtzWyBnPWIdrB7mIK6xh59AwQVV22hfhPObAs
mvGch5ZhKS2l9xe8KWkaHWrOM1BKTilKb48zCUIif9c59EdfgtMIx/XVpRzmaAu0
/5ZReZZ0xlMsnCqdEkEMwuT4/8IBuyy3EOMOnP5vpGEAb09qipauKIQMvajh2rj6
rbpAlXbz9KWbFlJfRI9QBygdo/n/9KQLiaEfwYohboFqUOoaFbP2P1JTIdbkN1IS
KSdKdrUeI7tPqr+bkZ3hOQCPV5azAMU1rEeCV+9TkaOGXGdQTcHwWmV8L5PM2XBG
rIbuyTymzyjWUtokQVhemQTbBJevSZApC55l/bGxBXCE6ifbDb/41NeF4UY4oShK
f02xgPwkbcb5OpktUFg7AxF6Ff2Tn1Bj5g9P0H57tft9hP7OMGnlf91f8jn30oXf
A0zbG/kHqrNFp4wL+a0YzJzRTlWbUrgZ/WLfFTeHL5P0zBHASQejbfxr0K4PDaT7
L6xZNRm/P/7bC4spzqrHVLtWl22KVjHEPEfS5qGmliHs6TUEJdp8PfOMDY3c2K4u
/eQ7R08bnzmDQQi/8x5M4JXRwM6F7GJdzRN1Go3Q0zBpOnfx/hlGLmtD2gUhnoQn
q7uqv8v4c6ZQeQp+ZacZhasVy5QCjdzwk3d4Rz9s1A==
-----END CERTIFICATE-----

Digital certificate information for user JLAUT1:
Certificate ID: 2QbR08Hk4/HlwdPJxMHjxcRLwtbW40vix0vDxcPw8PZA
Status: TRUST
Start Date: 2024/06/05 00:00:00
End Date:   2025/06/05 23:59:59
Serial Number:
>01<
Issuer's Name:
>CN=JLNAME.T=VBCERTAUTH.O=JLORGN.C=US<
Subject's Name:
>CN=JLNAME.T=VBSIGNING.O=JLORNG.C=US<
Subject's AltNames:
Domain: WWWDOMAIN
Signing Algorithm: sha256RSA
Key Usage: HANDSHAKE, DOCSIGN
Key Type: NIST ECC
Key Size: 521
Private Key: YES
PKDS Label: VALIDATED.BOOT.SG.CEC006
Certificate Fingerprint (SHA256):
Label: VALIDATED.BOOT.SG.CEC00670:11:B6:ED:C1:6D:6B:19:EE:E7:85:C4:04:3E:6D:49:
07:D5:5C:46:89:B8:59:CE:82:07:61:FB:FA:4E:B4:9C
Ring Associations:
Ring Owner: JLAUT1
Ring:
>VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1<
```

Following a review of the Export Registry entry, press PFK3 to show the optional Control Journal Posting.

1.6.4. Posting Signing Findings to the Control Journal

To post the Export Summary to the Control Journal, press Enter or PFK3 to return. A sample Pop-Up dialog and Summary are shown below.


```
/*******************************************************************************/
/*                                                                             */
/*         ICE Viewer - NSIMVUE - Certificate Export Summary - PROBI1          */
/*               Export Date:2024/06/07 Report Time:16:39:55                   */
/*            Registry DS:PROBI1.PERSONAL.EXPREGDS.D240607.T171925             */
/*                  Export DS:PROBI1.PERSONAL.EXPORT.DATASET                   */
/*                                                                             */
/*******************************************************************************/

Source Library:SYS1.SVCLIB, Target Library:PROBI1.VBSIGNED.SYS1.SVCLIB
Signing UserId:JLAUT1
---Certificate:JLAUT1/VALIDATED.BOOT.SG.CEC006
----Export DSN:PROBI1.PERSONAL.EXPORT.DATASET

---Private Key:YES, Trust:Is Trusted
-End Date/Time:2025/06/05 23:59:59
-----Algorithm:(SHA256):
--Finger Print:70:11:B6:ED:C1:6D:6B:19:EE:E7:85:C4:04:3E:6D:49:
--------------:07:D5:5C:46:89:B8:59:CE:82:07:61:FB:FA:4E:B4:9C

-----BEGIN CERTIFICATE-----
MIIEOzCCAiOgAwIBAgIBATANBgkqhkiG9w0BAQsFADBEMQswCQYDVQQGEwJVUzEP
MA0GA1UEChMGSkxPUkdOMRMwEQYDVQQMEwpWQkNFUlRBVVRIMQ8wDQYDVQQDEwZK
TE5BTUUwHhcNMjQwNjA1MDcwMDAwWhcNMjUwNjA2MDY1OTU5WjBDMQswCQYDVQQG
EwJVUzEPMA0GA1UEChMGSkxPUk5HMRIwEAYDVQQMEwlWQlNJR05JTkcxDzANBgNV
BAMTBkpMTkFNRTCBmzAQBgcqhkjOPQIBBgUrgQQAIwOBhgAEAChrDC1vIpP0Ubvu
7sNDQo/j/jVzr/G2HLcKFdlVFNxkvrAeti2/UF+sPCskL8vbA72I+PE9pi5wPy1q
kkGQ40y2AYk9rIX5HtJnAQt3Uqy9xdCCFRdHv1G9leenGLDrdf2Q85hG9AW8/pOz
vARGciovOn4mZfajVm030x5kARr1tlR9o4HAMIG9MD8GCWCGSAGG+EIBDQQyFjBH
ZW5lcmF0ZWQgYnkgdGhlIFNlY3VyaXR5IFNlcnZlciBmb3Igei9PUyAoUkFDRikw
FAYDVR0RBA0wC4IJV1dXRE9NQUlOMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQU
vXfkHdvBD0kXW3mcurm1nYAJX0MwHwYDVR0jBBgwFoAUcHFJFaQsYxpkkpN7TJsq
wotSlmYwFAYDVR0SBA0wC4IJV1dXRE9NQUlOMA0GCSqGSIb3DQEBCwUAA4ICAQAa
LpbgG3gbyUO5L9QOZ40oQZe5h/2xtzWyBnPWIdrB7mIK6xh59AwQVV22hfhPObAs
mvGch5ZhKS2l9xe8KWkaHWrOMlBKTilKb48zCUIif9c59EdfgtMIx/XVpRzmaAu0
/5ZReZZ0xlMsnCqdEkEMwuT4/8IBuyy3EOMOnP5vpGEAb09qipauKIQMvajh2rj6
rbpAlXbz9KWbFlJfRI9QBygdo/n/9KQLiaEfwYohboFqUOoaFbP2P1JTIdbkN1IS
KSdKdrUeI7tPqr+bkZ3hOQCPV5azAMU1rEeCV+9TkaOGXGdQTcHwWmV8L5PM2XBG
rIbuyTymzyjWUtokQVhemQTbBJevSZApC55l/bGxBXCE6ifbDb/41NeF4UY4oShK
f02xgPwkbcb5OpktUFg7AxF6Ff2Tn1Bj5g9P0H57tft9hP7OMGnlf91f8jn30oXf
A0zbG/kHqrNFp4wL+a0YzJzRTlWbUrgZ/WLfFTeHL5P0zBHASQejbfxr0K4PDaT7
L6xZNRm/P/7bC4spzqrHVLtWl22KVjHEPEfS5qGmliHs6TUEJdp8PfOMDY3c2K4u
/eQ7R08bnzmDQQi/8x5M4JXRwM6F7GJdzRN1Go3Q0zBpOnfx/hlGLmtD2gUhnoQn
q7uqv8v4c6ZQeQp+ZacZhasVy5QCjdzwk3d4Rz9s1A==
-----END CERTIFICATE-----
```

The Posting is attributed to the signing session owner.

To return to the originating IEWSIGN Action:ADMIN Panel, press PFK3.

4.Building Signing Structures

A Signing Structure is built by using a composition of RACF and ICSF control elements – key kings, certificates, RDATALIB, FACILITY, CSFKEYS class profiles and access lists, and the PKDS Data Store for securing the Certificate Public/Private key pairs. This is a complex task or certainly time consuming.

The three examples presented below will demonstrate how ValBoot shields this complexity by automatically generating what is necessary to build the structures but to also back them off when results are unsatisfactory and a redo is necessary.

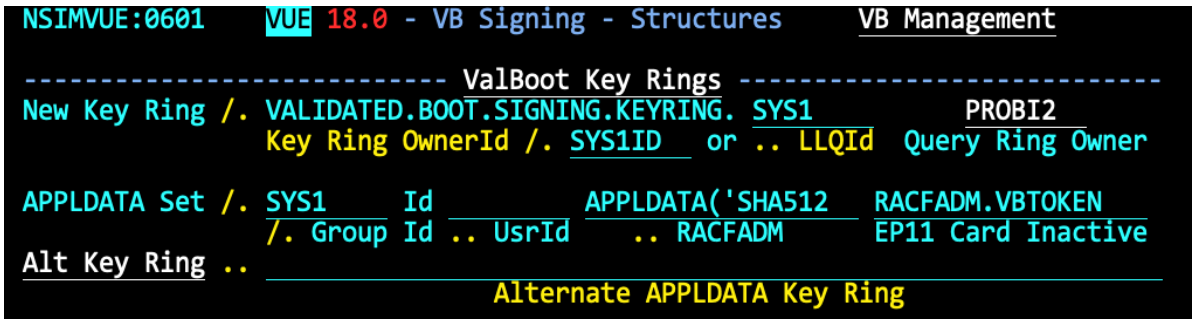
Note that while ValBoot supports each example equally well, it is considered a "Best Practice" to focus attention on Setting up Individual Signers. This method will assure accuracy for each signer's action and prevent any possible confusion as to which structure was used to perform the signing that might arise when Signing Groups overlap with Individual Signers.

1.1. Setting Up a Signing Group

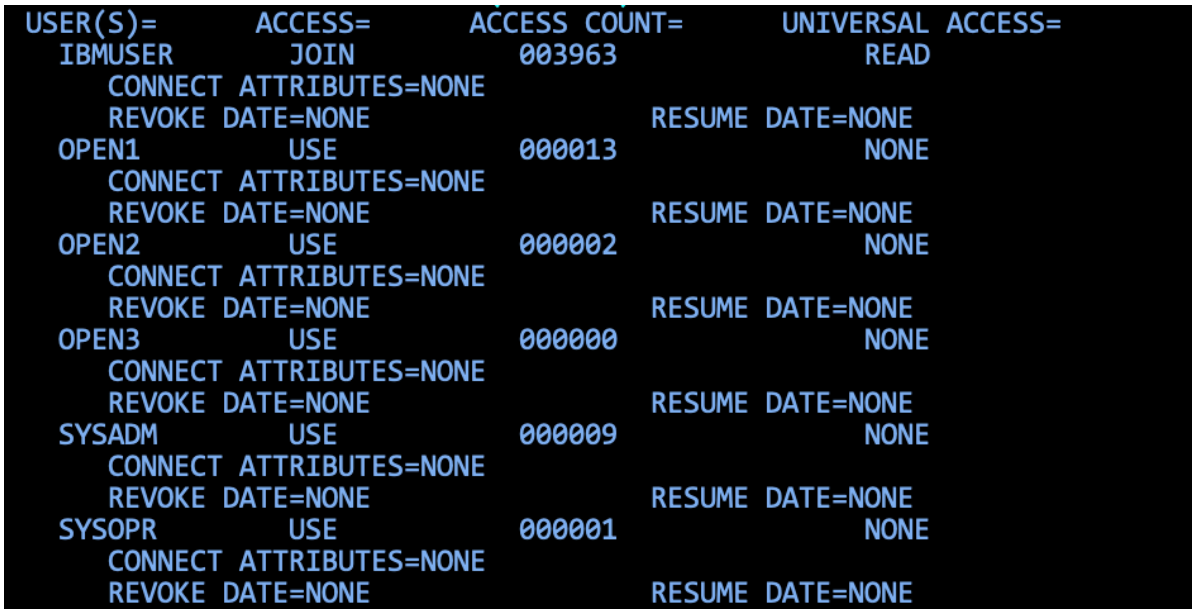
The first step in setting up a Group Signing Structure is to define to RACF a group affiliated "UserId" that can own the key ring – a group cannot own a key ring. For example, if the group name is SYS1, as used below, its id must be the group name plus the suffix value of "ID", i.e. SYS1ID in this example.

Once the GroupId is defined, the GroupId and the Group name are entered in the panel as shown below.
Check Key Ring OwnerId but DO NOT check LLQId. This action will make SYS1ID the owner of the key ring.

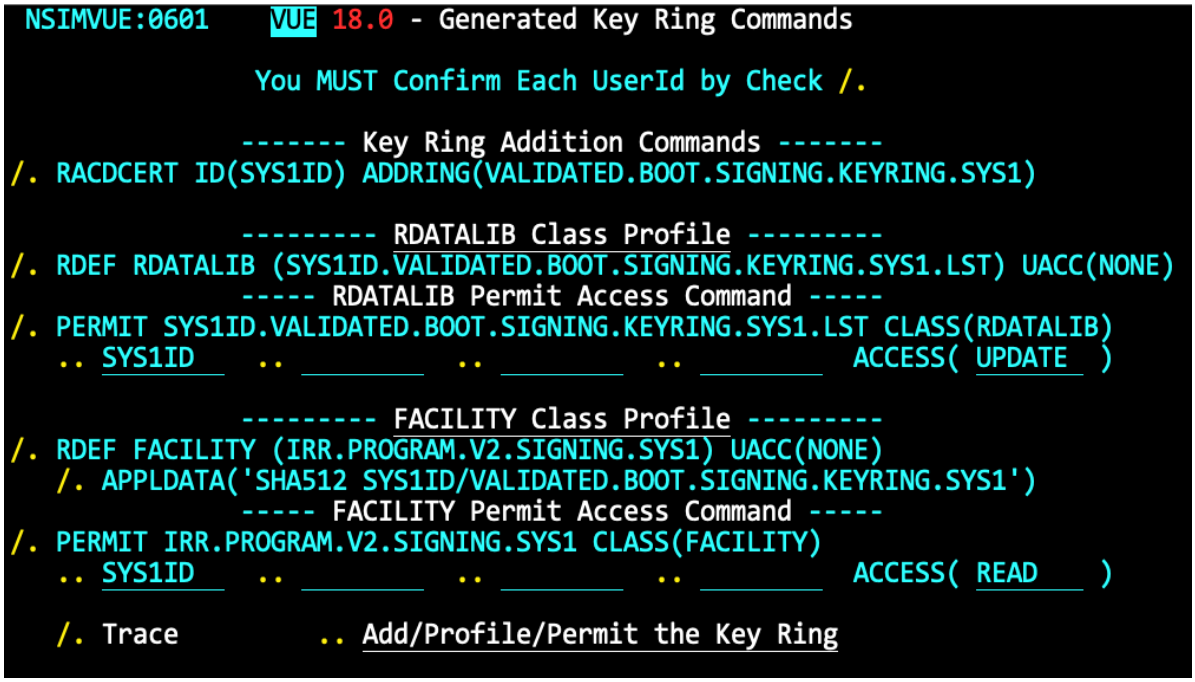
Next, in the APPLDATA Set section enter SYS1 and check Group. This action will create the appropriate FACILITY classs IRR profile name and APPLDATA attribute automatically adding "ID" to the group name value as necessary.



To review the members of the group specified, cursor under it and press Enter.



When satisfied with the entries, simply cursor under Create/Update/Profile Ring at the bottom of the panel and press Enter. This action will Generate the RACDCERT key ring, RDATALIB and FACILITY class commands shown below.



Multiple users can be empowered to sign using this structure so it is a best practice to limit connections to those entrusted with the responsibility of signing system resources.

Examine the commands carefully. Note that the UserId has been inserted in the RDATALIB and FACILITY Permit fields with a UACC of UPDATE and READ respectively. If a change to the Permits is considered necessary, overtype them as needed. When satisfied with the generated command, cursor under Add/Profile/Permit the Key Ring and press Enter.

Trace is on by default so it will follow as shown below.

```
/*****************************************************************************/
/*                                                                           */
/*        ICE Viewer - NSIMVUE - Validated Boot Trace Records - PROBI2       */
/*               Report Date:2024/06/21 Report Time:09:29:44                 */
/*                     TRACEDS:PROBI2.$VALBOOT.$RTRACE                       */
/*                                                                           */
/*****************************************************************************/

--- Generate Key Ring Command and Replies ---

RACDCERT ID(SYS1ID) ADDRING(VALIDATED.BOOT.SIGNING.KEYRING.SYS1)
NO REPLY RECEIVED

RDEF RDATALIB (SYS1ID.VALIDATED.BOOT.SIGNING.KEYRING.SYS1.LST) UACC(NONE)
ICH10006I RACLISTED PROFILES FOR RDATALIB WILL NOT REFLECT THE ADDITION(S) UNTIL

PERMIT SYS1ID.VALIDATED.BOOT.SIGNING.KEYRING.SYS1.LST CLASS(RDATALIB) ID(SYS1) A
ICH06011I RACLISTED PROFILES FOR RDATALIB WILL NOT REFLECT THE UPDATE(S) UNTIL A
```

Examine the output carefully for any problems as reported by RACF.

PFK3 to continue and display the Key Ring Worksheet shown below.

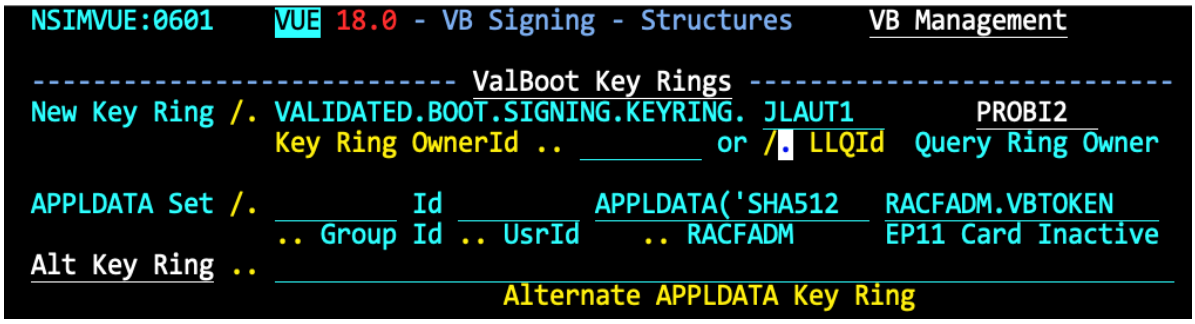
```
                VUE 18.0 - ICE Viewer - ValBoot Key Rings     Row 1 to 3 of 3

 --NSIMVUE 0621--             2024/06/21 12:48:36              --Target List--

 --------------- Validated Boot Key Ring Worksheet - 1 - Record ----------------
 Row Selection: List_Ring_Details Rdatalib_Profile Facility_Profile Delete_Rings
 S Num --Owner-- ------------- Key Ring Label ------------ Rda Fac Cert War Row
 _ ___ ________ _____________________________________ ___ ___ ____ ___ ___
 _ 001 SYS1ID___ VALIDATED.BOOT.SIGNING.KEYRING.SYS1_____ Yes Yes None --- 001
 _     _CA Cert_ _NONE_____________________________________ ___ ___ ____ ___ 002
 _     _SG Cert_ _NONE_____________________________________ ___ ___ ____ ___ 003
 ******************************* Bottom of data ********************************
```

Note that there may be more than one ValBoot key ring. The one just created, owned by SYS1ID, is shown without CA and SG Certs. They will need to be added to make the key ring operational.

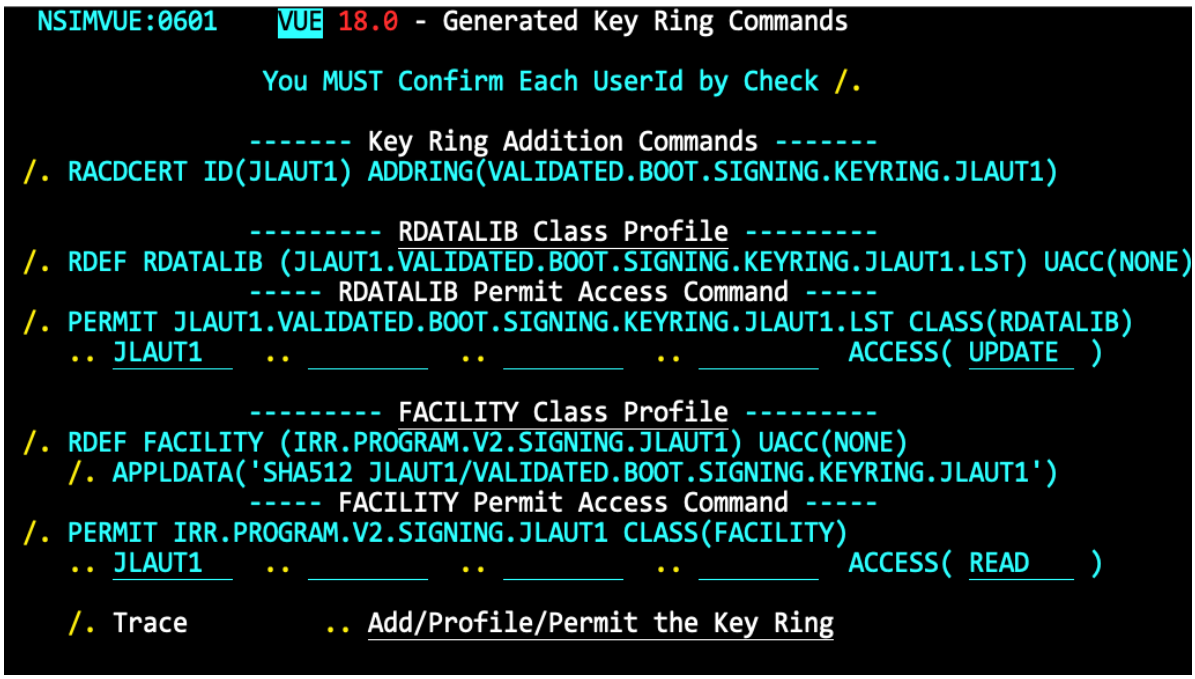
Use the Row Selection options to examine the Ring Details and the RDATALIB and FACILITY profiles. If unsatisfied with the newly generated key ring, delete it. PFK3 back to the Primary/Structure Menu and begin again to build a new key ring or continue and generate CA and SG certificates and connect them to the newly created key ring.

1.2. Setting up Individual Signers – a Recommended Best Practice

When an Admin wants to create a signing structure for a specific UserId they do the following: Enter the UserId (ValBoot will check its validity) in the LLQId field and check "/". When the key ring commands are generated, this will tell ValBoot that the UserId is to be added to the name of the key rRing and that the UserId is also to be the owner of the Key Ring.



When satisfied with the entries, simply cursor under Create/Update/Profile Ring at the bottom of the panel and press Enter. This action will generate the RACDCERT key ring and the RDATALIB and FACILITY class commands shown on the following panel:



Examine the commands carefully. Note that the UserId has been inserted in the RDATALIB and FACILITY Permit fields with the UACC of UPDATE and READ respectively. If a change to the Permits is considered necessary overtype them as needed. If satisfied cursor under Add/Profile/Permit the Key Ring and press Enter.

Trace is on by default so it will follow' Examine it carefully. PFK3 to continue and display the Key Ring Worksheet shown below.

```
/*******************************************************************************/
/*                                                                             */
/*        ICE Viewer - NSIMVUE - Validated Boot Trace Records - PROBI2         */
/*                Report Date:2024/06/21 Report Time:12:48:36                  */
/*                      TRACEDS:PROBI2.$VALBOOT.$RTRACE                        */
/*                                                                             */
/*******************************************************************************/

--- Generate Key Ring Command and Replies ---

RACDCERT ID(JLAUT1) ADDRING(VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1)
NO REPLY RECEIVED

RDEF RDATALIB (JLAUT1.VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1.LST) UACC(NONE)
ICH10006I RACLISTED PROFILES FOR RDATALIB WILL NOT REFLECT THE ADDITION(S) UNTIL

PERMIT JLAUT1.VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1.LST CLASS(RDATALIB) ID(JLAUT
ICH06011I RACLISTED PROFILES FOR RDATALIB WILL NOT REFLECT THE UPDATE(S) UNTIL A
```

When the review is complete, having taken note of any problems indicated by RACF, press PFK3 to continue and display the Key Ring worksheet.

```
                VUE 18.0 - ICE Viewer - ValBoot Key Rings     Row 1 to 6 of 6

 --NSIMVUE 0621--             2024/06/21 12:48:36              --Target List--

 --------------- Validated Boot Key Ring Worksheet - 2 - Records ---------------
 Row Selection: List_Ring_Details Rdatalib_Profile Facility_Profile Delete_Rings
 S Num --Owner-- ------------- Key Ring Label ------------ Rda Fac Cert War Row
 _ ___ ________ ____________________________________________ ___ ___ ____ ___ ___
 _ 001 JLAUT1___ VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1_____ Yes Yes None --- 001
 _     _CA Cert_ _NONE_____________________________________ ___ ___ ____ ___ 002
 _     _SG Cert_ _NONE_____________________________________ ___ ___ ____ ___ 003
 _ 002 SYS1ID___ VALIDATED.BOOT.SIGNING.KEYRING.SYS1_______ Yes Yes None --- 004
 _     _CA Cert_ _NONE_____________________________________ ___ ___ ____ ___ 005
 _     _SG Cert_ _NONE_____________________________________ ___ ___ ____ ___ 006
 ******************************* Bottom of data ********************************
```

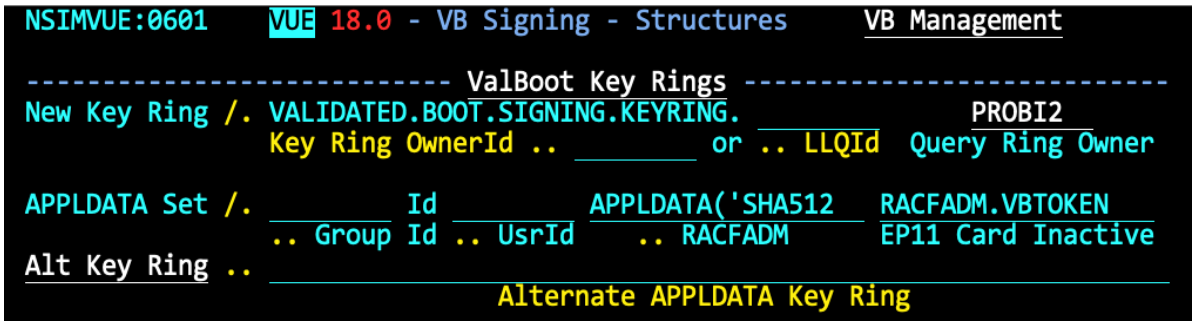
There may be more than one ValBoot Key Ring. The one just created, owned by JLAUT1, is shown without CA and SG certificates. They will need to be added to make the key ring operational.

Examine the Ring Details, RDATALIB and FACILITY profiles. If unsatisfied with the newly generated key ring, delete it. PFK3 back to the Primary/Structure Menu and begin again to create a new key ring or continue and generate CA and SG certificates and connect them to the newly generated key ring.

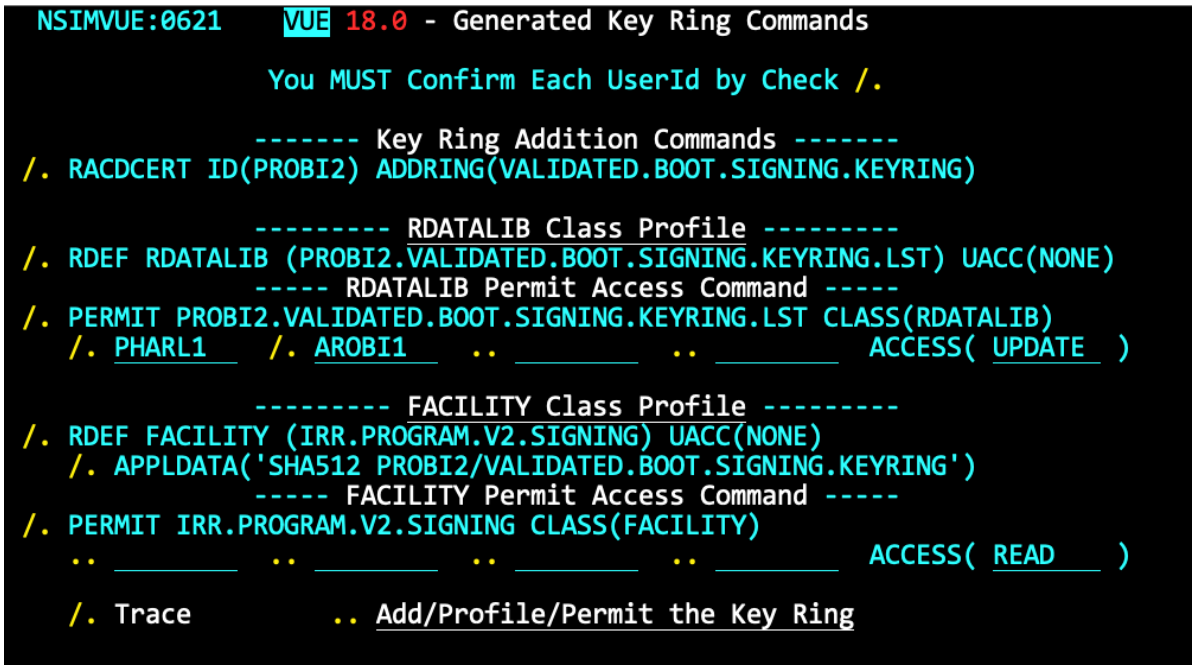
It is possible that the UserId, in this case JLAUT1, could also be in the connect group that has its own group signing structure. This Individual Signers Structure for JLAUT1 would take precedence over JLAUT1's group association.

1.3. Setting up an Admin/Personal Signer – An AdHoc Group

When the Logged on Admin wants to create a signing structure and personally control its use, permitting individual UserIds as desired without regard for their possible group associations, the following will generate the necessary key ring and related profiles.



This process requires no entries. Simply cursor under Create/Update/Profile Ring at the bottom of the panel and press Enter. This action will generate the RACDCERT key ring and the RDATALIB and FACILITY class commands shown on the following panel:



In addition to the generated commands, the panel also supports Permitting Users (PHARL1 and AROBI1 for example) by UserId, access to the RDATALIB profile that will be used to protect the Key Ring. Naming and Checking users here will create an "AdHoc Signing Group" granted UPDATE access. This "Group" is controlled directly by the Admin.

Examine the commands and permit entries, be sure to check them carefully. When satisfied, cursor under Add/Profile/Permit the Key Ring and press Eenter.

Trace is on by default so it will follow. Examine it carefully.

```
/*****************************************************************************/
/*                                                                           */
/*        ICE Viewer - NSIMVUE - Validated Boot Trace Records - PROBI2       */
/*                Report Date:2024/06/21 Report Time:12:48:36                */
/*                      TRACEDS:PROBI2.$VALBOOT.$RTRACE                      */
/*                                                                           */
/*****************************************************************************/

--- Generate Key Ring Command and Replies ---

RACDCERT ID(PROBI2) ADDRING(VALIDATED.BOOT.SIGNING.KEYRING)
NO REPLY RECEIVED

RDEF RDATALIB (PROBI2.VALIDATED.BOOT.SIGNING.KEYRING.LST) UACC(NONE)
ICH10006I RACLISTED PROFILES FOR RDATALIB WILL NOT REFLECT THE ADDITION(S) UNTIL

RDEF FACILITY (IRR.PROGRAM.V2.SIGNING) UACC(NONE) APPLDATA('SHA512 PROBI2/VALIDA
ICH10006I RACLISTED PROFILES FOR FACILITY WILL NOT REFLECT THE ADDITION(S) UNTIL
```

PFK3 to continue and display the Key Ring Worksheet shown below.

```
                VUE 18.0 - ICE Viewer - ValBoot Key Rings     Row 1 to 9 of 9

--NSIMVUE 0621--              2024/06/21 12:48:36              --Target List--

--------------- Validated Boot Key Ring Worksheet - 3 - Records ---------------
Row Selection: List_Ring_Details Rdatalib_Profile Facility_Profile Delete_Rings
S Num --Owner-- -------------- Key Ring Label ------------ Rda Fac Cert War Row
_ ___ ________ ____________________________________________ ___ ___ ____ ___ ___
_ 001 JLAUT1___ VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1_____ Yes Yes None --- 001
_     _CA Cert_ _NONE_____________________________________ ___ ___ ____ ___ 002
_     _SG Cert_ _NONE_____________________________________ ___ ___ ____ ___ 003
_ 002 PROBI2___ VALIDATED.BOOT.SIGNING.KEYRING_____________ Yes Yes None --- 004
_     _CA Cert_ _NONE_____________________________________ ___ ___ ____ ___ 005
_     _SG Cert_ _NONE_____________________________________ ___ ___ ____ ___ 006
_ 003 SYS1ID___ VALIDATED.BOOT.SIGNING.KEYRING.SYS1_______ Yes Yes None --- 007
_     _CA Cert_ _NONE_____________________________________ ___ ___ ____ ___ 008
_     _SG Cert_ _NONE_____________________________________ ___ ___ ____ ___ 009
******************************** Bottom of data ********************************
```

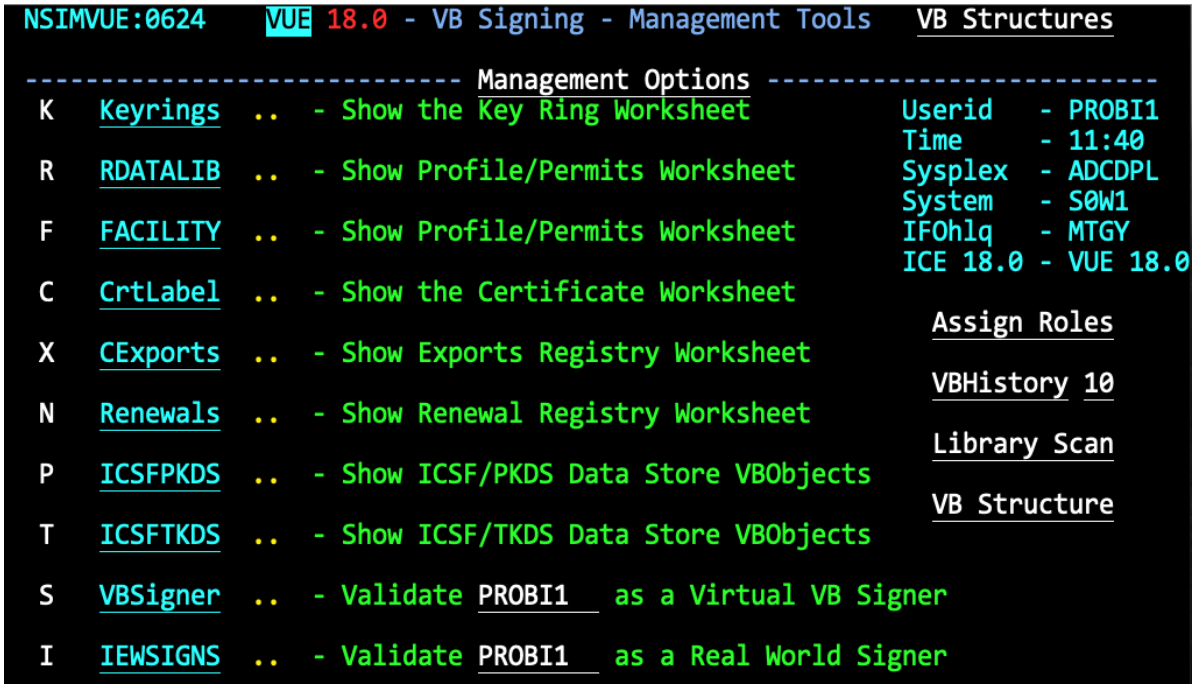
Note that there may be more than one ValBoot Key Ring. The one just created, owned by PROBI1, is shown without CA and SG certificates. The certificates will need to be added to make the key ring operational.

Examine the Ring Details, RDATALIB and FACILITY profiles. If unsatisfied with the newly generated key ring, delete it. PFK3 back to the Primary/Structure Menu and begin again to create a new key ring or continue and generate CA and SG certificates and connect them to the newly generated key ring.

It is possible that the UserId, in this case JLAUT1, could also be in the connect group that has its own group signing structure or have its Individual Signers Structure. These would take precedence over JLAUT1's permit to the described "AdHoc Group".

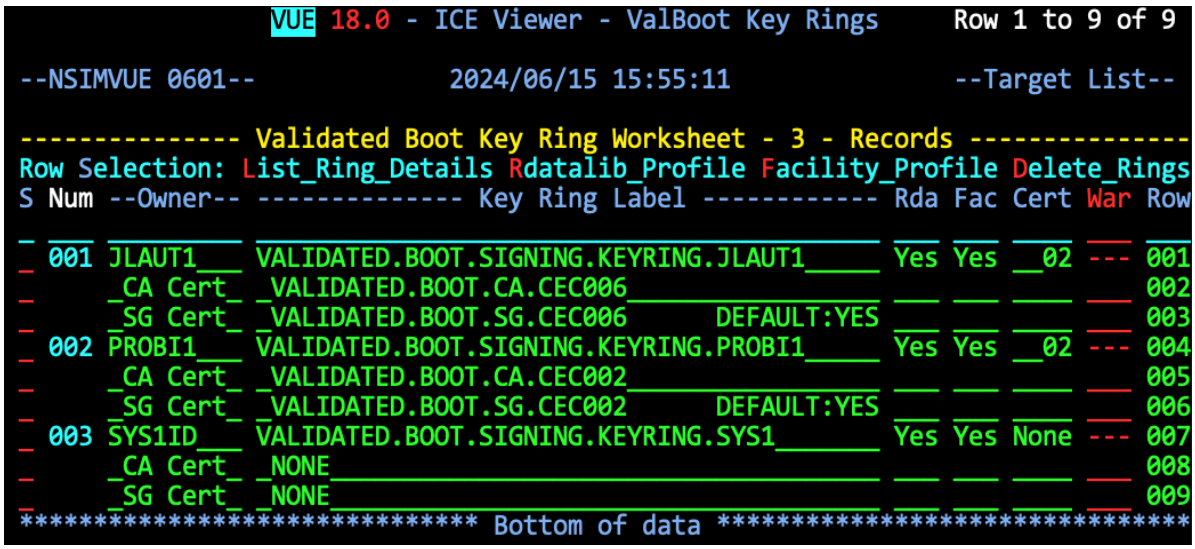
5.Management Tools

Management Tools are designed to assist the ValBoot Administrator, in exploring, updating, renewing, monitoring and testing Validated Boot Signing Structures.



1.1. Keyrings – Show the Key Ring Worksheet

This Worksheet shows only RACF defined key rings that match the key ring naming standard – VALIDATED.BOOT.SIGNING.KEYRING.LLQId. Access a key ring with a specific operator by entering its single prefix character in the 'S' column adjacent to the target and then press enter.



1.1.1. Worksheet Columns

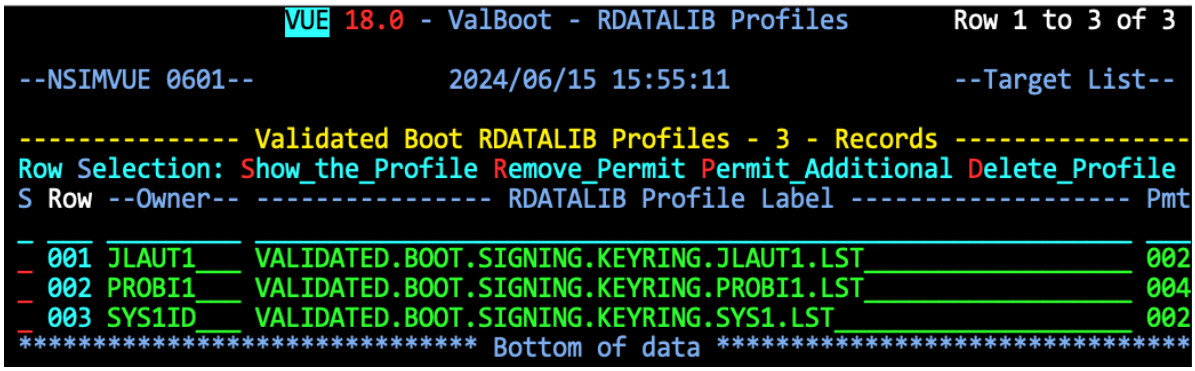
- Owner Key Ring Owner
- Label Key Ring Label
- Rda If Yes, this indicates that a RDATALIB class profile exists. To display Profile Class and Worksheet select with R.
- Fac If Yes, this indicates that a FACILITY class profile exists and contains an APPLDATA attribute with references to the Key Ring's RDATALIB class profile. .
- Cert Key Rings can be expanded into a display of connected Certificates. From there, attributes of each are shown.
- War Indicates if the certificates connected to the key ring are within 99 days of expiration.

1.1.2. Worksheet Row Selection Operators

- L List Key Ring's Certificate Detail in a work-sheet that, in turn, supports displaying of the certificates.
- R Detail of Key Ring's RDATALIB class profile displayed.
- F Detail of Key Ring's FACILITY class profile displayed.
- D Will delete the key ring. Will not delete certificates, RDATALIB or the FACILITY profiles or permits. Delete confirmation is required.

1.2. RDATALIB – Show Profile/Permits Worksheet

The RDATALIB profile controls access to the key ring. Its actual labeling follows the name of the Key Ring prefixed with the OwnerId and suffixed with '.LST'.



1.2.1. Worksheet Columns

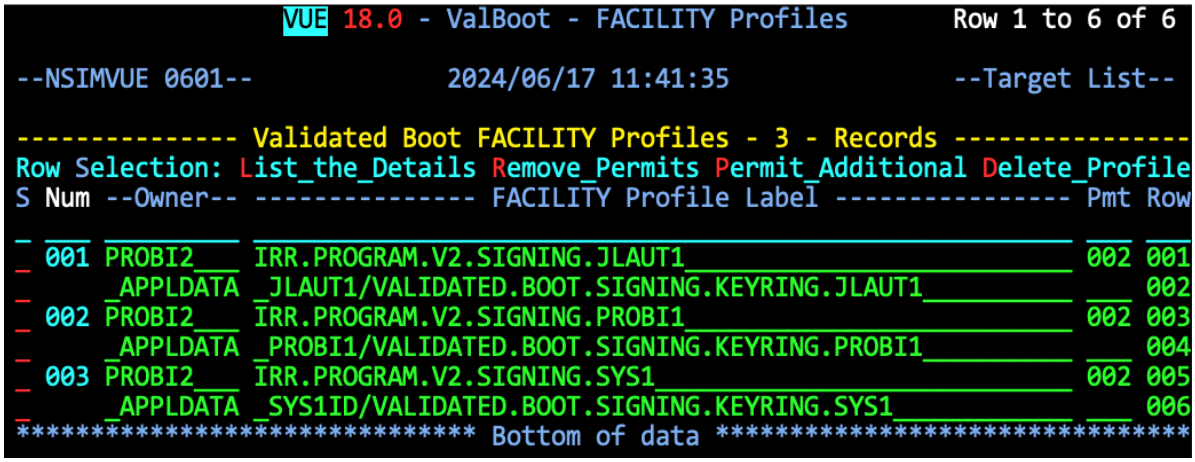
- Owner Owner of the Profile
- Label Profile label was automatically assigned at the time the key ring was originally defined to RACF by ValBoot/RACDCERT.
- Permits The current number of UserIds that are permitted access to the profile.

1.2.2. Worksheet Row Selection Operators

- S Show the Profile Details as would be shown by RLIST.
- R Remove Permits
- P Permit Additional
- D Delete the Profile

1.3. FACILITY – Show Profile/Permits Worksheet

The FACILITY class profile acts as a 'Traffic Cop' for IEWSIGN and its use of the RACF callable service R_PgmSignVer. This function will examine profiles that match the naming convention – IRR.PROGRAM.V2.SIGNING in order to determine which best fits the calling UserId. If a match is not found, signing is denied. If a profile match is found, the APPLDATA contained in the profile provides further integration for RDATALIB access rights to the named key ring. If a permitted match is found, the UserId is a valid signer.



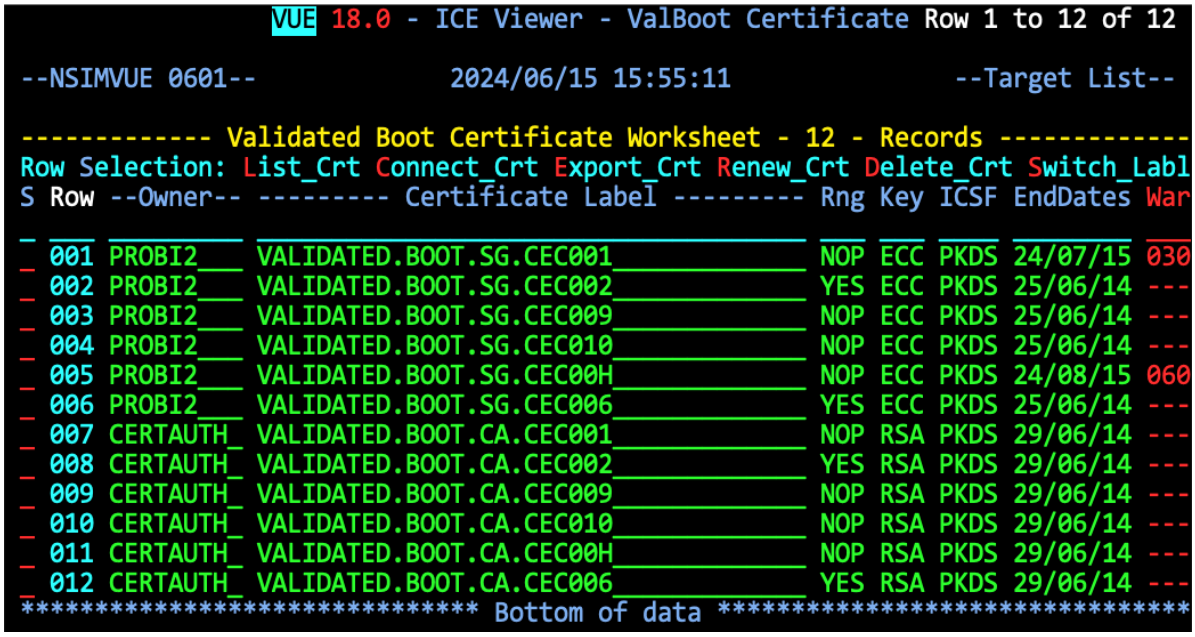
1.3.1. Worksheet Columns

- Owner Owner of the profile
- Label Profile label was automatically assigned at the time the Key Ring was originally defined to RACF by ValBoot/RACDCERT. APPLDATA indicates the name of the key ring that must be accessed/matched.
- Permits The current number of UserIds that are permitted access to the profile.

1.3.2. Worksheet Row Selection Operators

- S List the profile details as would be shown by RLIST.
- R Remove Permits
- P Permit Additional
- D Delete the Profile

1.4. CrtLabel – Show Certificate Worksheet



```
                VUE 18.0 - ICE Viewer - ValBoot Certificate Row 1 to 12 of 12

--NSIMVUE 0601--              2024/06/15 15:55:11                --Target List--

------------ Validated Boot Certificate Worksheet - 12 - Records -------------
Row Selection: List_Crt Connect_Crt Export_Crt Renew_Crt Delete_Crt Switch_Labl
S Row --Owner-- --------- Certificate Label --------- Rng Key ICSF EndDates War
_ ___ ________ ____________________________________ ___ ___ ____ ________ ___
_ 001 PROBI2___ VALIDATED.BOOT.SG.CEC001___________ NOP ECC PKDS 24/07/15 030
_ 002 PROBI2___ VALIDATED.BOOT.SG.CEC002___________ YES ECC PKDS 25/06/14 ---
_ 003 PROBI2___ VALIDATED.BOOT.SG.CEC009___________ NOP ECC PKDS 25/06/14 ---
_ 004 PROBI2___ VALIDATED.BOOT.SG.CEC010___________ NOP ECC PKDS 25/06/14 ---
_ 005 PROBI2___ VALIDATED.BOOT.SG.CEC00H___________ NOP ECC PKDS 24/08/15 060
_ 006 PROBI2___ VALIDATED.BOOT.SG.CEC006___________ YES ECC PKDS 25/06/14 ---
_ 007 CERTAUTH_ VALIDATED.BOOT.CA.CEC001___________ NOP RSA PKDS 29/06/14 ---
_ 008 CERTAUTH_ VALIDATED.BOOT.CA.CEC002___________ YES RSA PKDS 29/06/14 ---
_ 009 CERTAUTH_ VALIDATED.BOOT.CA.CEC009___________ NOP RSA PKDS 29/06/14 ---
_ 010 CERTAUTH_ VALIDATED.BOOT.CA.CEC010___________ NOP RSA PKDS 29/06/14 ---
_ 011 CERTAUTH_ VALIDATED.BOOT.CA.CEC00H___________ NOP RSA PKDS 29/06/14 ---
_ 012 CERTAUTH_ VALIDATED.BOOT.CA.CEC006___________ YES RSA PKDS 29/06/14 ---
******************************* Bottom of data ********************************
```

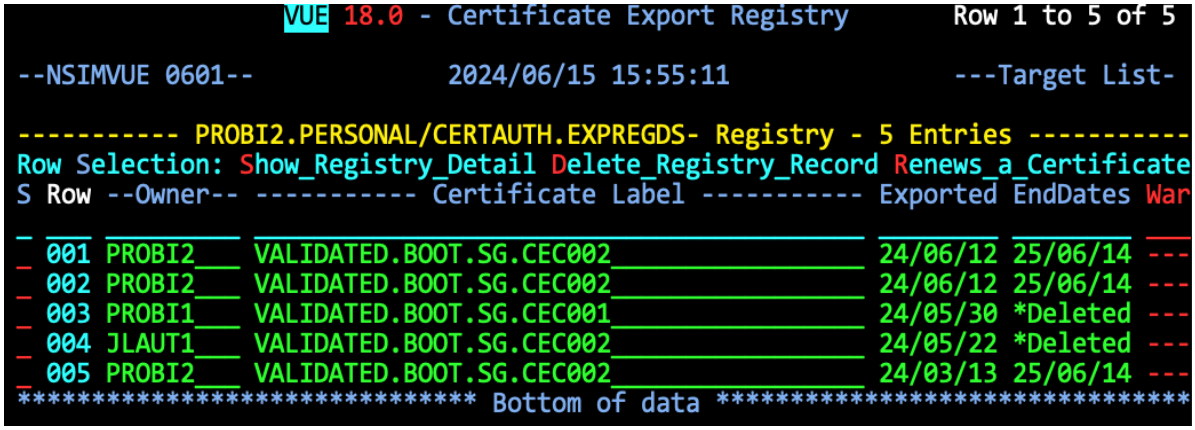
1.4.1. Worksheet Columns

- Row The worksheet row number.
- Owner When owned as End-Entity, UserId or CERTAUTH if CA certificate. The actual signing certificate is always an End-Entity
- Label The full certificate label or Subject Common Name.
- Key RSA(PKDS size (4096) or NISTECC(PKDS size (512).
- ICSF PKDS or TKDS, depending on use of which key pair storage.
- EndDate Date when the certificate is scheduled to expire.
- War This flag will begin to appear when the number of days to The certificate's expiration is less than 99.

1.4.2. Worksheet Row Selection Operators

- L Shows full decoded content of selected certificate in the form of a dated and timestamped report.
- C Select a certificate to display the available key rings. Next, Select Target Key Ring to connect the certificate to.
- E To complete the Validated Boot Cycle, certificates must exported. This option assists in exporting and tracking.
- R As End-Entity certificates reach maturity they can be easily renewed and tracked using this option.
- D Select to delete a certificate from the RACF data store.
- S Will switch certificate label to Subject Common Name and back.

1.5. CExports – Show Export Registry Worksheet



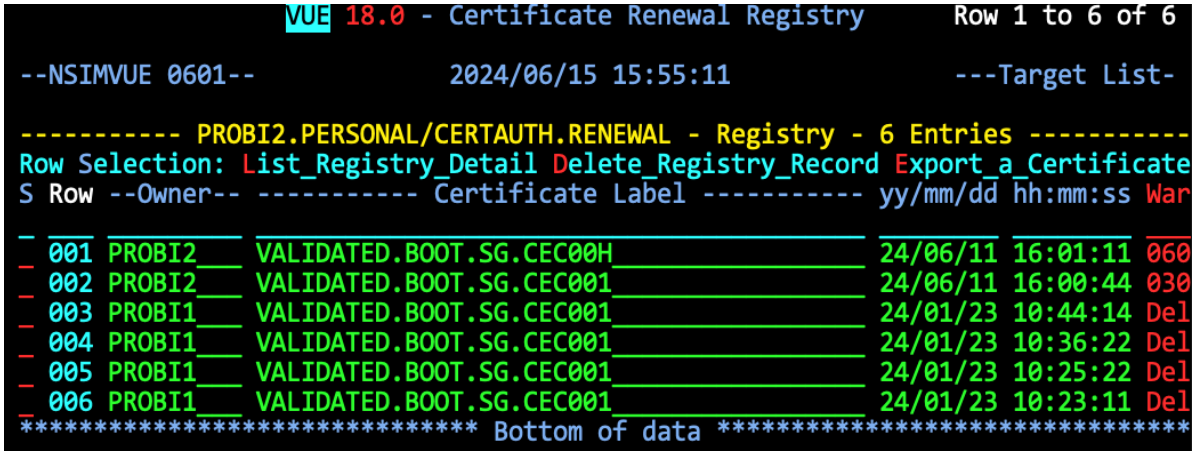
1.5.1. Worksheet Columns

- Owner Validated Boot certificates owned as End-Entity by users or CERTAUTH certificates. The actual signing certificate is always an End-Entity certificate whose public/private key pair will be used to both sign and decode z/system configuration resources: IPLTEXT, Nucleus/LPA Modules.
- Label The full certificate label.
- Request Show the date when the Export Request was formulated and submitted to RACF via RACDCERT commands
- EndDate Date when the certificate will expire. If the certificate is no longer available, the word 'Deleted'.
- Warning This flag will begin to appear when the number of days until the certificate's expiration is 99 days or less.

1.5.2. Worksheet Row Selection Operators

- S Shows Registry Detail - Each registry contains detail information about the export the selection will show.
- D Delete the Registry Record - Selection will immediately delete the entry. Confirmation is required.
- R Renew a Certificate - Action will load owner and certificate into the Certificate Renewal panel.

1.6. Renewals – Show Renewal Registry Worksheet



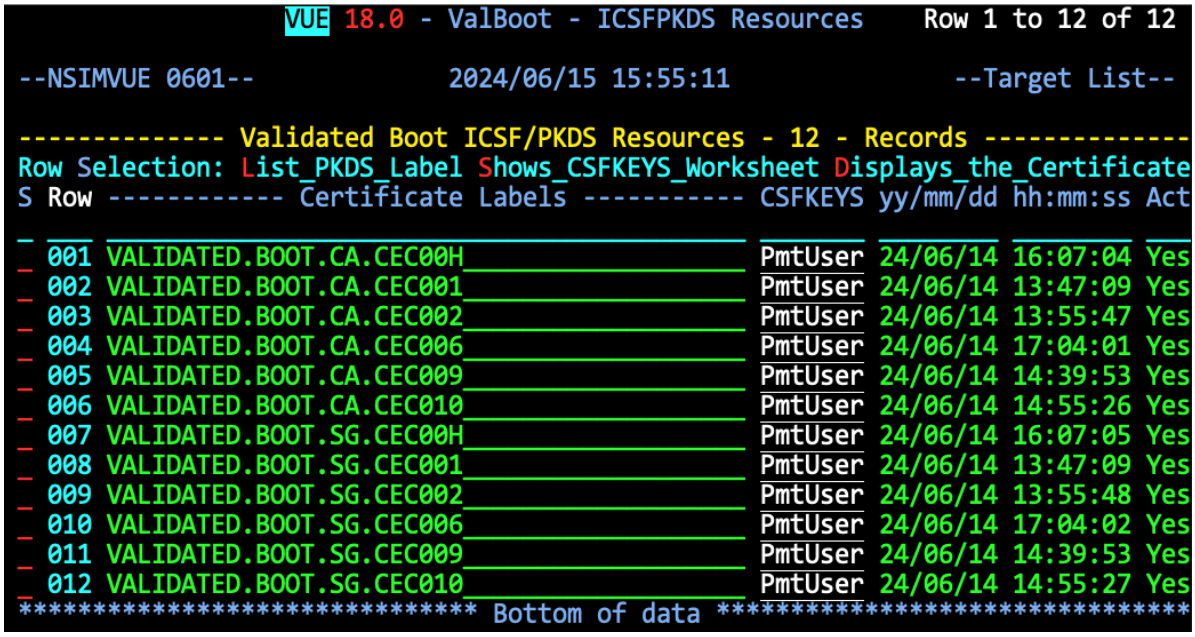
1.6.1. Worksheet Columns

- Row — The worksheet row number.
- Owner — Validated Boot Certificates owned as End-Entity by users or CERTAUTH certificates. The actual signing certificate is always an End-Entity certificate whose public/private key pair will be used to both sign and decode z/system configuration resources: IPLTEXT, Nucleus/LPA Modules.
- Label — The full certificate label.
- yy/mm/dd — Request Show the date when the Renewal Request was formulated and submitted to RACF via RACDCERT commands
- hh:mm::ss — Date when the certificate will expire. If the certificate is no longer available, the word 'Deleted'.
- War — This flag will begin to appear when the number of days until the certificate's expiration is 99 days or less.

1.6.2. Worksheet Row Selection Operators

- S — Shows Registry Detail - Each registry contains detail information about the renewal the selection will show.
- D — Delete the Registry Record - Selection will immediately delete the entry. Confirmation is required.
- E — Export a Certificate - Action will load owner and certificate into the Certificate Export panel.

1.7. ICSFPKDS – Show ICSF/PKDS Data Store VBObjects



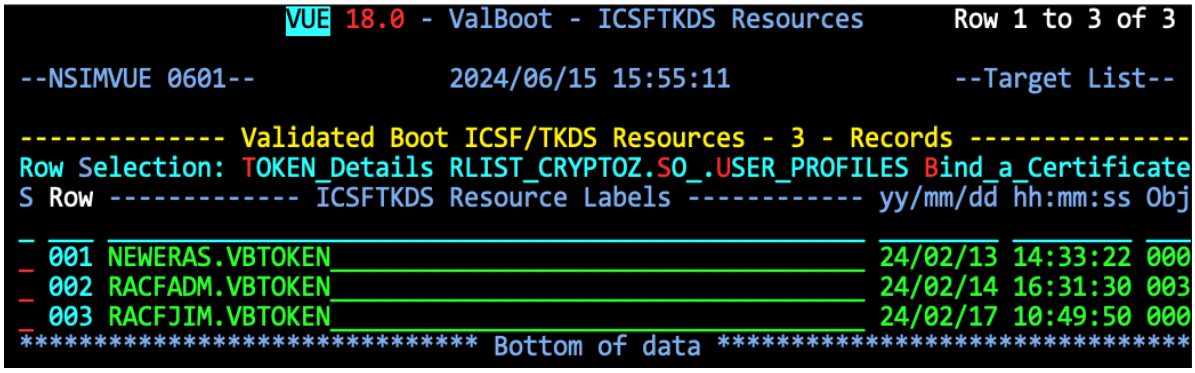
1.7.1. Worksheet Columns

- Owner
- Label
- Profile
- PmtUser

1.7.2. Worksheet Row Selection Operators

- L List PKDS Label
- S Show CSFKEYS Worksheet
- D Display the Source Certificate

1.8. ICSFTKDS – Show ICSF/TKDS Data Store VBObjects



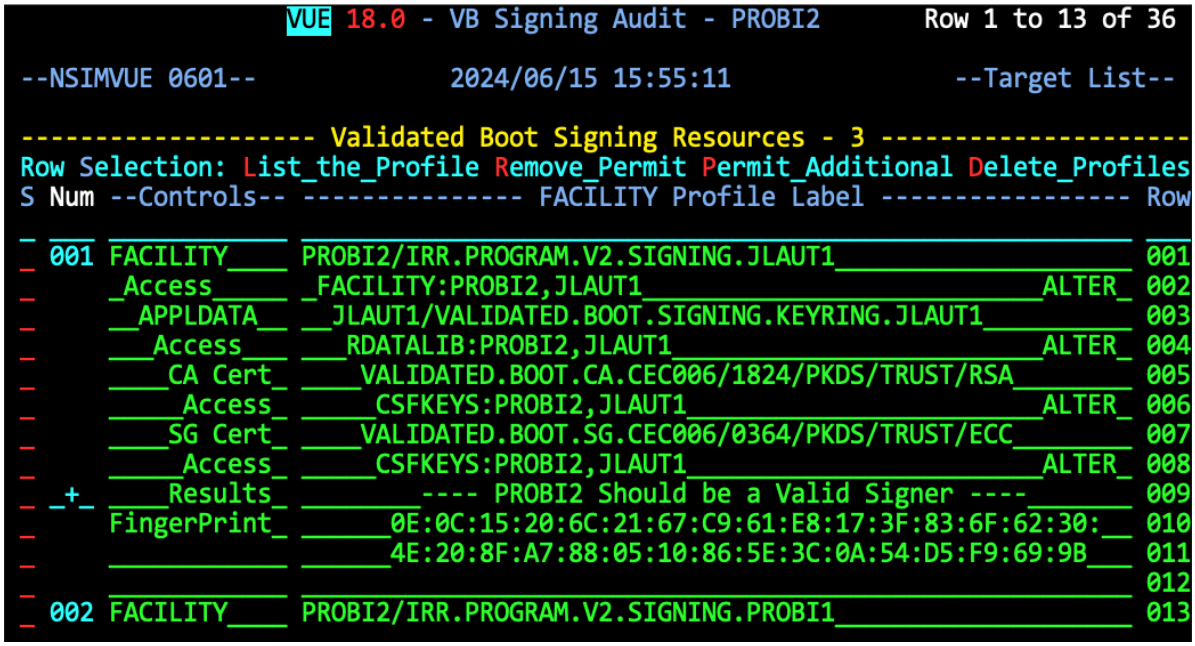
1.8.1. Worksheet Columns

- ICSFTKDS Resource Label
- yy/mm/dd
- hh:mm:ss
- Objects

1.8.2. Worksheet Row Selection Operators

- T TOKEN Details
- S RLIST_CRYPTOZ.SO Profile
- U RLIST_CRYPTOZ.USER Profile
- B Bind a Certificate to a Token

1.9. VBSigner – Validate UserId as a Virtual Signer



1.9.1. Worksheet Columns

1.9.2. Worksheet Row Selection Operators

1.10. IEWSIGNS – Validate UserId as a Real World Signer

To validate a single user's signing ability, enter a UserId, not a GroupId, into the panel adjacent to the option name. Cursor under it and press Enter.

To submit the IEWSIGN JOB that will be used in validation, the session owner, if different from the specified UserId, will need submit authority in order to act for the signer.

If the session owner does not have the necessary permissions to submit for the signer the following message is displayed.

For the session owner to act as the signer, these RACF steps must be performed:

Under TSO option 6 issue the following to determine if the signer has a profile.
RLIST SURROGAT signerId.SUBMIT AUTHUSER

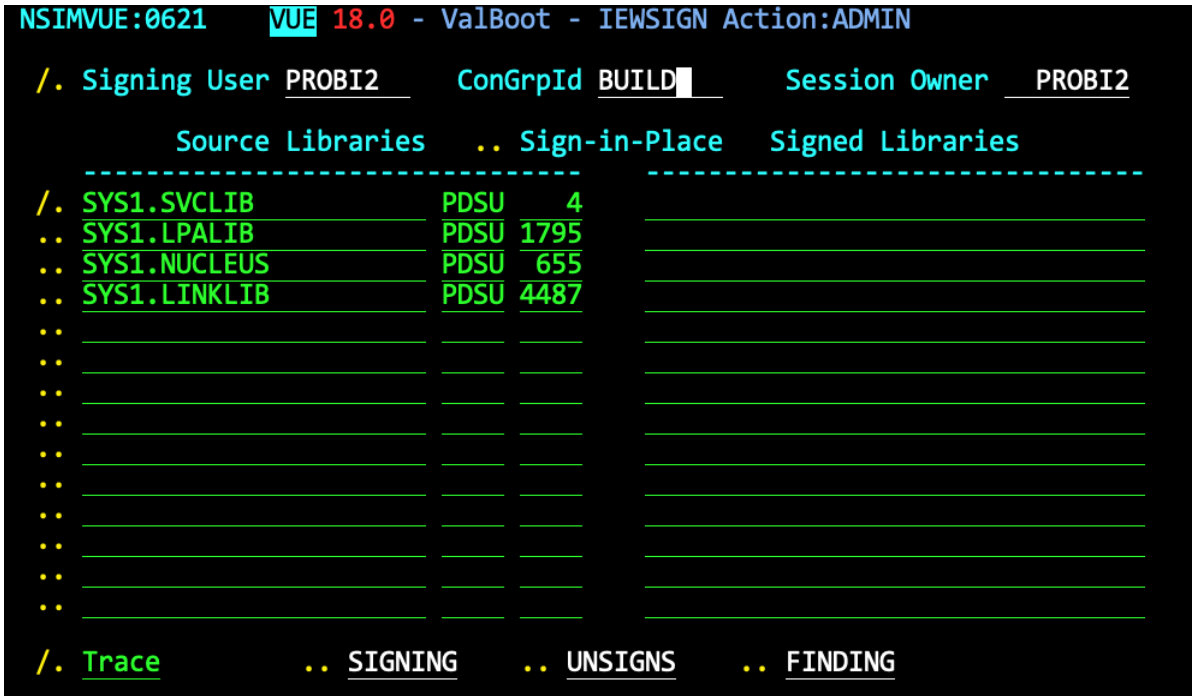
If a SURROGAT class profile does not exist for the signer, do the following:
RDEFINE SURROGAT signerId.SUBMIT UACC(NONE)

Finally, issue the following to permit the session owner to the profile
PERMIT signerid.SUBMIT CLASS(SURROGAT) ID(session_owner) ACCESS(READ)

This is a sensitive action and should be reviewed by the security department before proceeding.

The panel below shows two UserIds, one is for the Signing User (the UserId being tested) the other for the Session Owner (the UserId conducting the test). The value of ConGrpId is relevant when the Signing User is being tested as a member of a specific connect group.

While IEWSIGN is capable of signing any PDS with an undefined record format (PDSU) for testing, for speed, it is best to select a library with few modules such as SYS1.SVCLIB as shown below.



See section 1.4, How Library Signing Works, for a detailed explanation of the ValBoot signing process and why the Session Owner needs access to the Signers SURROGAT SUBMIT Profile. In addition, see section 1.7, When a Signing is Successful for a detailed explanation of the report journal post and export options that accompany a successful signing.

```
//VALBOOT  JOB REGION=120M,USER=PROBI2,GROUP=BUILD
//SIGNS EXEC PGM=IEWSIGN,PARM='ACTION=SIGN',REGION=200M
//SYSPRINT DD DISP=SHR,DSN=PROBI2.IEWSIGN.SYSPRINT
//INFILE   DD DISP=SHR,DSN=SYS1.SVCLIB
//OUTFILE  DD DISP=SHR,DSN=PROBI2.VBSIGNED.SYS1.SVCLIB
```

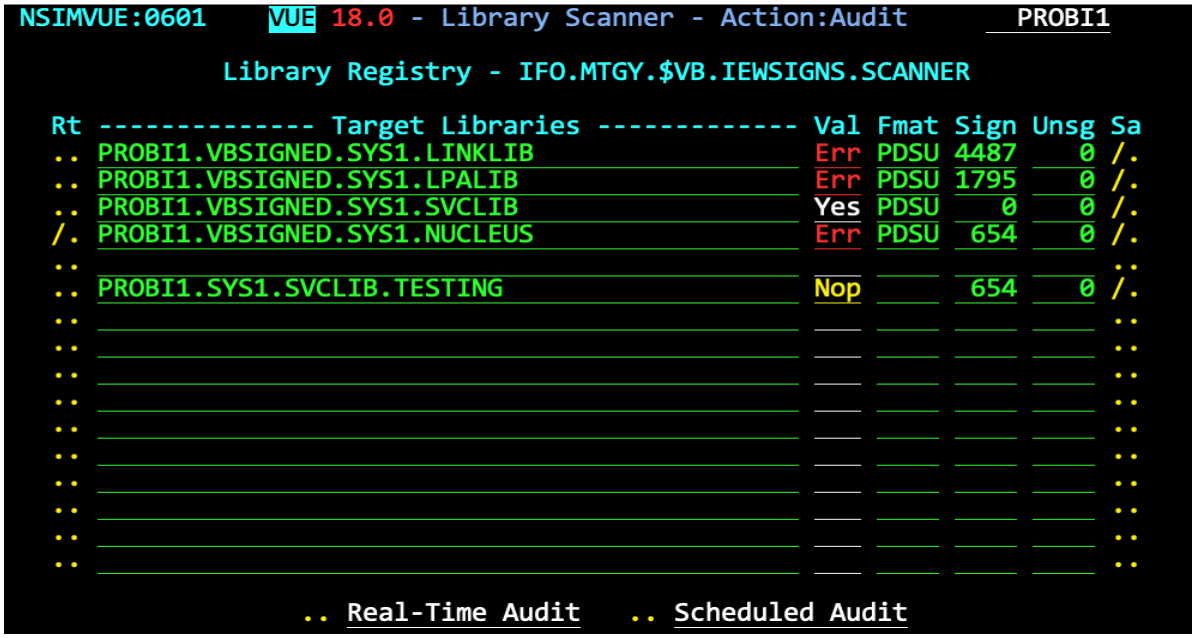
6.Admin Only Options

1.1. Assigning Roles

1.2. Accessing ValBoot History

1.3. Setting Up the Library Scanner

The Library Scanner interface presents a summary of libraries that may qualify for an Audit. Those noted with 'Err' have signing issues, those denoted with 'Nop' were not found via a catalog lookup, those denoted with 'Yes' were found and appear to be valid for signing.



1.3.1. Real-Time Audit

To kick-off a Real Time Audit 'Check' in the 'Rt' column adjacent to the target library, cursor under Real_Time and press Enter. The sample below highlights a potential error.

```
SIGNIN    PROBI1.VBSIGNED.SYS1.NUCLEUS                ZWORK5        32760

Modules Included:
<NONE>

Modules Excluded:
<NONE>


Algorithm ID        Hash algorithm              Sign algorithm
0202                SHA2-512                    ECDSA-P521

Certificate summary:
Cert-Index:         INDEX001 Modules:0567 First Signature:2024-05-28 16:28:07
Subject KeyID:      19090F3C D259BDA7 F48E4169 5EFF9259 666E793A
Cert Fingerprint:   AE55C57E B3A101DA 15BCD656 B7E8F4B3 C36B7243 0B4BB0FF EC58BA
RACF Fingerprint:   AE:55:C5:7E:B3:A1:01:DA:15:BC:D6:56:B7:E8:F4:B3:
                    C3:6B:72:43:0B:4B:B0:FF:EC:58:BA:EA:0E:2F:B0:9D
Certificate:        Corresponding certificate not found
Signing Keyring:    Unable to Identify Key Ring
```

1.3.2. Scheduling an Audit

Scheduled audits can be performed by entering target libraries and by checking them in the 'Sa' column, ValBoot can create and send an audit report focused on libraries named and selected from the Library Scanner Primary Menu and sent Daily, Weekly, and/or Monthly. To schedule a report to be sent, Check ('/') one or more intervals. To suspend sending, enter either blank or 'X' for interval selection. Using the 'X' will save the interval detail for future use. To reactivate an existing interval or to setup new intervals, Check ('/') to update the detail.

An interval's time is maintained using a 24 hour clock where both hours 'hh' and minutes 'mm' must be 2 digits. The actual interval definition will vary depending on selection.

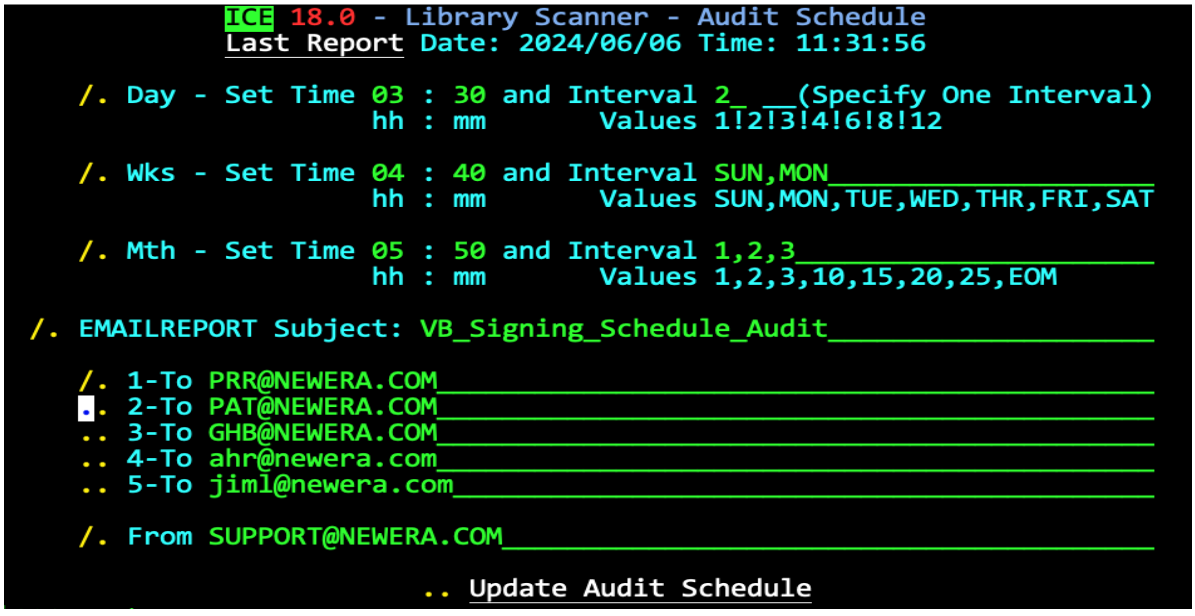
For Day the interval can range from once a day to once an hour. For once daily, specify a 'BLANK'. Valid hour intervals are 1, 2, 3, 4, 6, 8, and 12.

For Weekly, specify one or more days of the week. Use commas to separate multiple day indicators.

For Monthly, specify numerically one or more days separating multiple days with a comma. EOM will schedule a scan/audit report for the End-of-Month.

Email Subject should be a representative text string. Limit 26 characters.

The Address To and From (required). The Email Addresses will be retained on update. They must be checked '/' to become valid for processing.



To activate the Audit, cursor under Update Audit Schedule and press Enter. Note that all three intervals (Day, Wks, Mth) can be active at the same time if they are 'checked' at the time of the update. Sample report elements are shown below:

```
/*******************************************************************************
/*                                                                             *
/*        VALBOOT - Library Signing Audit - Summary - Structure Fails          *
/*         Date:06/04/24 - Time:07:31:56 - System:S0W1 - XIVBSCN:0518          *
/*            Summary Records:IFO.MTGY.IEWSIGN.@S0W1.AUDIT.SUMMARY             *
/*                                                                             *
/*******************************************************************************
```

Sample of a Successful Audit:

```
03) PROBI1.VBSIGNED.SYS1.SVCLIB         SIGNED:0004 UNSIGNED:0000
     VBS0000I SIGNING STRUCTURE APPEARS TO REMAIN VALID

 DD        Data Set Name                                  Volume        Block Size
 SIGNIN    PROBI1.VBSIGNED.SYS1.SVCLIB                    ZWORK5        32760

 Modules Included:
 <NONE>
 Modules Excluded:
 <NONE>

 Algorithm ID        Hash algorithm               Sign algorithm
 0202                SHA2-512                     ECDSA-P521

 Certificate summary:
 Cert-Index:         INDEX001 Modules:0004 First Signature:2024-05-25 10:39:00
 Subject KeyID:      A93CB27B EC3B1815 2A825765 625A6FE9 4BBC9FEB
 Cert Fingerprint:   53DC2C65 1429839B FD05140D 75A19241
                     44B2136E 9793DFA4 2B7E189B C956C34D
 HMC Fingerprint:    53:DC:2C:65:14:29:83:9B:FD:05:14:0D:75:A1:92:41:
                     44:B2:13:6E:97:93:DF:A4:2B:7E:18:9B:C9:56:C3:4D
 RACF Certificate:   ID(JLAUT1) VALIDATED.BOOT.SG.CEC006
 Expires:            2025/06/03 Days:364
 Signing Keyring:    JLAUT1/VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1
```

Sample of a Failed Audit:

```
04) PROBI1.VBSIGNED.SYS1.NUCLEUS        SIGNED:0654 UNSIGNED:0000
     VBS0000E ONE/MORE ELEMENTS OF STRUCTURE NOT VALID

 DD        Data Set Name                                  Volume        Block Size
 SIGNIN    PROBI1.VBSIGNED.SYS1.NUCLEUS                   ZWORK5        32760

 Modules Included:
 <NONE>
 Modules Excluded:
 <NONE>

 Algorithm ID        Hash algorithm               Sign algorithm
 0202                SHA2-512                     ECDSA-P521

 Certificate summary:
 Cert-Index:         INDEX001 Modules:0567 First Signature:2024-05-25 10:39:00
 Subject KeyID:      19090F3C D259BDA7 F48E4169 5EFF9259 666E793A
 Cert Fingerprint:   AE55C57E B3A101DA 15BCD656 B7E8F4B3
                     C36B7243 0B4BB0FF EC58BAEA 0E2FB09D
 HMC Fingerprint:    AE:55:C5:7E:B3:A1:01:DA:15:BC:D6:56:B7:E8:F4:B3:
                     C3:6B:72:43:0B:4B:B0:FF:EC:58:BA:EA:0E:2F:B0:9D
 RACF Certificate:   Corresponding certificate not found
 Signing Keyring:    Unable to Identify Key Ring
```

1.4. VB Signing Structures

The path to signing begins with a search for an available FACILITY class profile that fits the signing naming convention. The search order is:

- IRR.PROGRAM.V2.SIGNING.connect_group.userid
- IRR.PROGRAM.V2.SIGNING.userid
- IRR.PROGRAM.V2.SIGNING.connect_group
- IRR.PROGRAM.V2.SIGNING

The content of the profile definition determines which key ring, if any, best fits a given user or connect group. The key ring selected is dependent on the value contained in the APPLDATA attribute of the profile definition. Once a key ring candidate is determined, a check is made of the related RDATALIB class profile. Possible signers or their connect group must have at least UPDATE access. The first UserId shown on the UsrAccess row is the owner of the RDATALIB profile and is the controller of access to the signing structure.

The panel below shows Signing Key Rings, related RDATALIB profiles, and the status of users or connect groups with defined access to the profile.

```
NSIMVUE:0621     VUE 18.0 - VB Signing Structures - 03

--------------- Key Rings, RDATALIB Profiles and Permits ---------------
Key Ring: PROBI1/VALIDATED.BOOT.SIGNING.KEYRING
RDATALIB: PROBI1.VALIDATED.BOOT.SIGNING.KEYRING.LST
Permitted PROBI1   JLAUT1   GBAGS1   PHARL2
UsrAccess ALTER    READ     UPDATE   UPDATE

Key Ring: BUILDID/VALIDATED.BOOT.SIGNING.KEYRING.BUILD
RDATALIB: BUILDID.VALIDATED.BOOT.SIGNING.KEYRING.BUILD.LST
Permitted PROBI1   BUILD
UsrAccess ALTER    UPDATE

Key Ring: JLAUT1/VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1
RDATALIB: JLAUT1.VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1.LST
Permitted PROBI1   JLAUT1
UsrAccess ALTER    UPDATE

Key Ring:
RDATALIB:
Permitted
UsrAccess
```

Cursoring under a Permitted cell that contains a connect group name and pressing Enter will cause the following message to be displayed:

```
 NSIMVUE - Group Can't Sign, Overtype Group with a Member UserId
```

Since a connect group cannot own a key ring, a further selection is needed. Press Enter and the connect group profile is displayed. All named UserIds in the profile are eligible signers.

```
 BROWSE    PROBI1.$ICEVUE.PANELS(VALBOOT)          Line 0000000000 Col 001 080
******************************** Top of Data ********************************
INFORMATION FOR GROUP BUILD
    SUPERIOR GROUP=SYS1         OWNER=JLAUT1      CREATED=24.171
    INSTALLATION DATA=VALIDATED BOOT GROUP
    NO MODEL DATA SET
    TERMUACC
    NO SUBGROUPS
    USER(S)=      ACCESS=      ACCESS COUNT=      UNIVERSAL ACCESS=
      PHARL2        USE           000000              NONE
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                 RESUME DATE=NONE
      PROBI1        USE           000000              NONE
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                 RESUME DATE=NONE
      JLAUT1        USE           000000              NONE
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                 RESUME DATE=NONE
      AROBI1        USE           000000              NONE
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                 RESUME DATE=NONE
```

To proceed, select a UserId and enter it in the panel adjacent to the connect group, cursor under it and press Enter.

To submit the IEWSIGN job the session owner, if different from the selected eligible signer, will need submit authority in order to act as the signer. If the session owner does not have the necessary permissions to submit for the signer, the following message is displayed:

```
 NSIMVUE - Signing UserId Does NOT Have a SURROGAT/SUBMIT PROFILE
```

In order for the session owner to act for the signer these RACF steps must be performed:

Under TSO option 6 issue the following to determine if the signer has a profile.
RLIST SURROGAT signerId.SUBMIT AUTHUSER

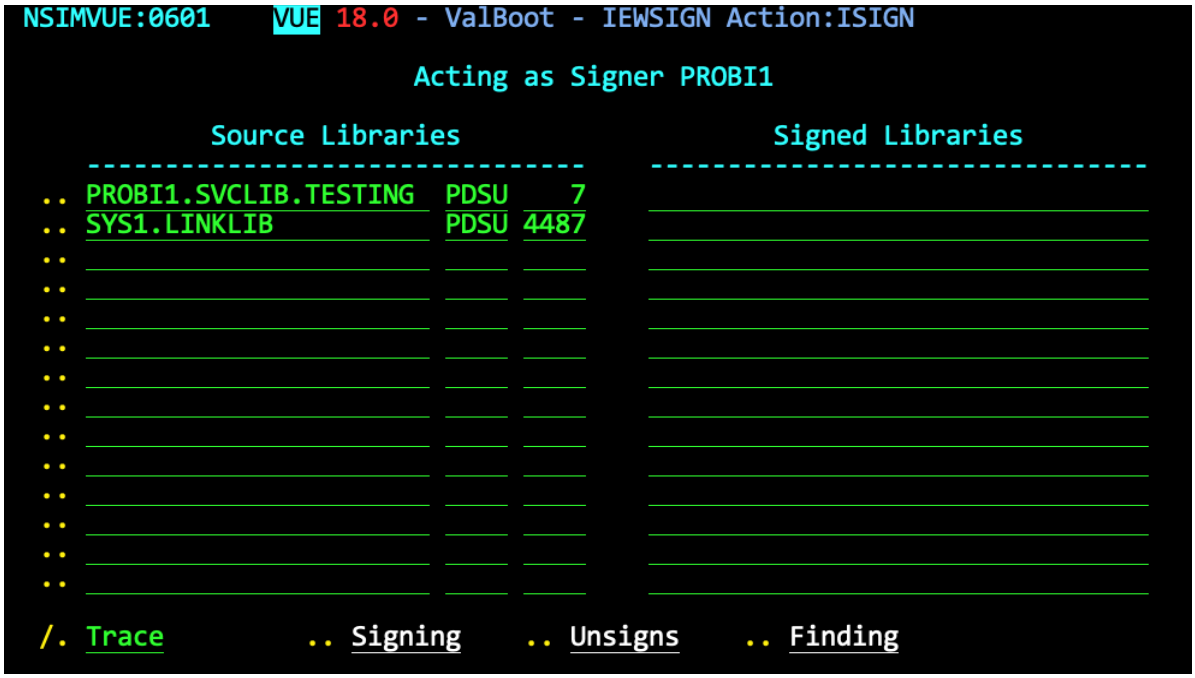
If a SURROGAT Class profile does not exist for the signer do the following:
RDEFINE SURROGAT signerId.SUBMIT UACC(NONE)

Finally, issue the following to permit the session owner to the profile
PERMIT signerid.SUBMIT CLASS(SURROGAT) ID(session_owner) ACCESS(READ)

This is a sensitive action and should be reviewed by the security department before proceeding.

7.Facilitated Signing Users Interface - ISIGN

Facilitated Signers must sign in to ValBoot by entering TSO $CLI,*VB,ISIGN.



1.1. *Signing a Library*

1.2. *Unsigning a Library*

1.3. *Present Findings*

8.Facilitated Audit Users Interface – AUDIT

Facilitated Auditors must sign in to ValBoot by entering TSO $CLI,*VB,ISIGN.

If the following message appears, the Admin has not setup the FACILITY class profile necessary for granting access to the Audit Interface:

```
NSIMVUE - FACILITY Class Profile NEZ.VALBOOT.AUDIT is Required
```

If the following message appears the Admin has not granted you access to the FACILITY class profile controlling access to the Audit Interface:

```
NSIMVUE - You don't have AUDITOR access to VALBOOT, see Your Admin
```

If the following message appears, it indicates that no viable structures exist for signing:

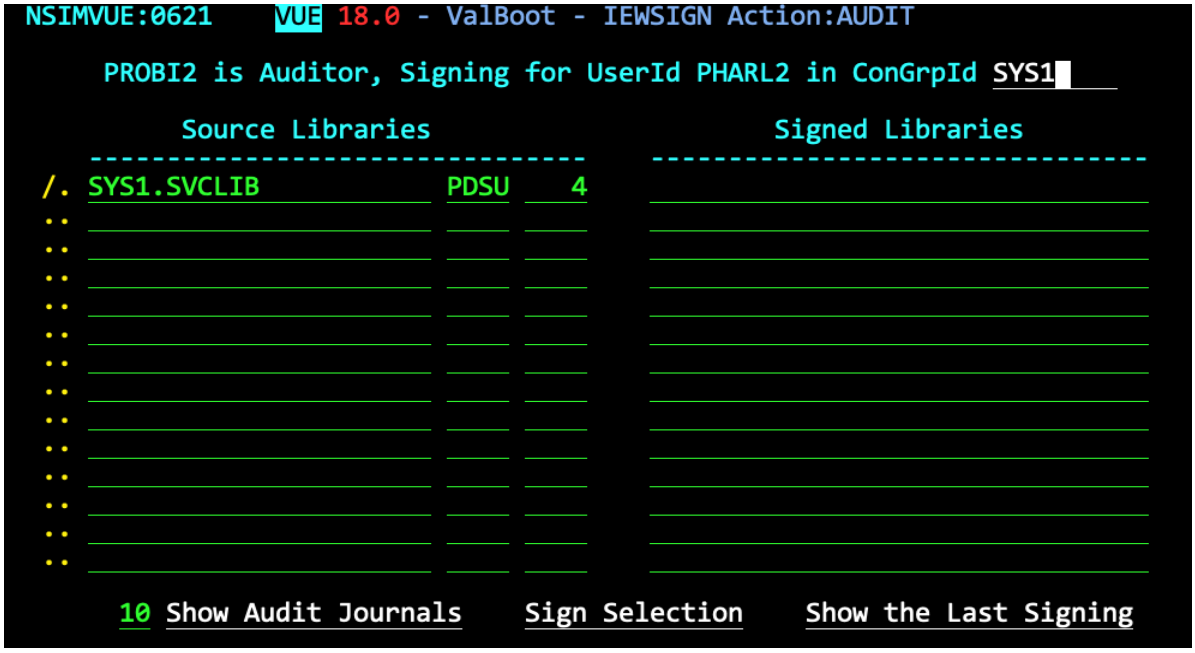
```
NSIMVUE - No Validated Boot Certificate Records Found
```

If certificates and signing structures are detected, the following panel is displayed:

```
NSIMVUE:0621     VUE 18.0 - VB Signing Structures - 03

--------------- Key Rings, RDATALIB Profiles and Permits ---------------
Key Ring: PROBI2/VALIDATED.BOOT.SIGNING.KEYRING
RDATALIB: PROBI2.VALIDATED.BOOT.SIGNING.KEYRING.LST
Permitted PROBI2    GBAGS1    AROBI1    PHARL2
UsrAccess ALTER     UPDATE    UPDATE    NONE

Key Ring: JLAUT1/VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1
RDATALIB: JLAUT1.VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1.LST
Permitted PROBI2    JLAUT1
UsrAccess ALTER     UPDATE

Key Ring: SYS1ID/VALIDATED.BOOT.SIGNING.KEYRING.SYS1
RDATALIB: SYS1ID.VALIDATED.BOOT.SIGNING.KEYRING.SYS1.LST
Permitted PROBI2    SYS1
UsrAccess ALTER     UPDATE

Key Ring:
RDATALIB:
Permitted
UsrAccess
```

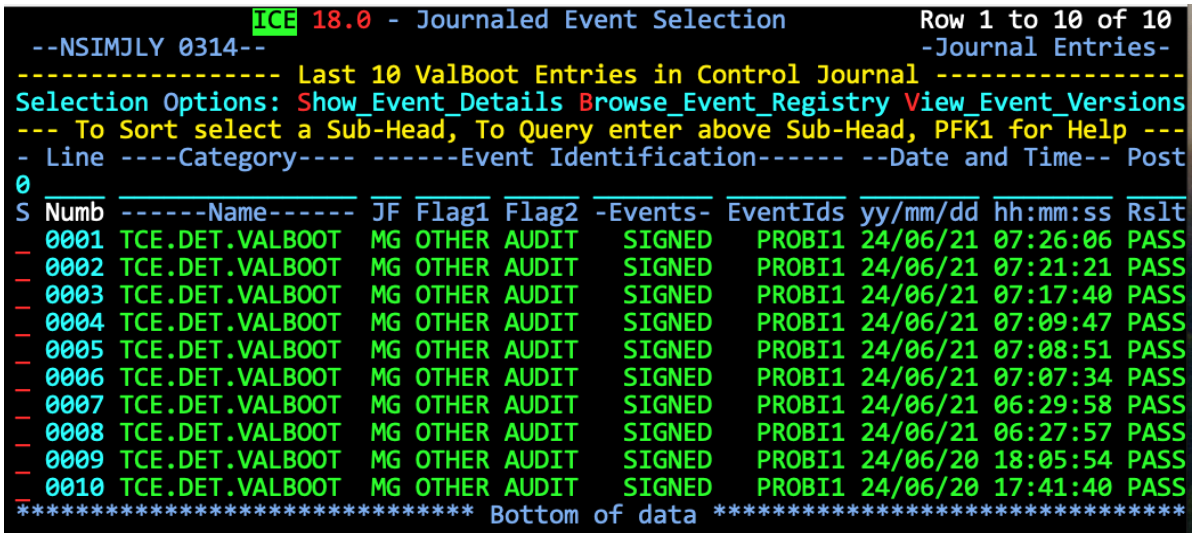
If the following message is displayed when Return is selected, the "List" of Group Members will be shown. Select a member from the "List". Enter the member UserId to the right.

Cursor under a UserId and press Enter to display the IEWSIGN Action:AUDIT panel.



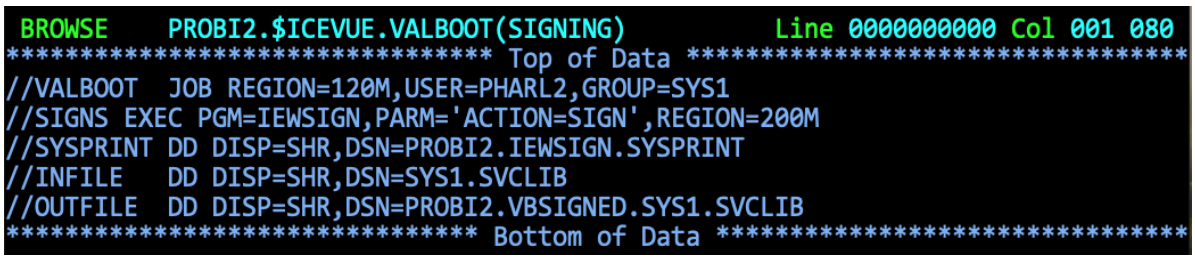
1.1. Show Audit Journal

Signing, Export and Renew Events are recorded in the ICE Control Journal. This panel shows 10 such events as determined by the numeric entered in the prior panel.



1.2. Sign Selection

If the UserId being audited is a group member, the Connect Group Id (ConGrpId) is required. In this example, it is SYS1.



```
/*******************************************************************************/
/*         ICE Viewer - NSIMVUE - ValBoot Certificate Detail - PROBI2          */
/*                Report Date:2024/06/22 Report Time:13:40:24                  */
/*                      Dataset:PROBI2.$VALBOOT.$DETAIL                        */
/*   Source Library:SYS1.SVCLIB, Target Library:PROBI2.VBSIGNED.SYS1.SVCLIB    */
/*                           Signing UserId:PHARL2                             */
/*******************************************************************************/

          Digital certificate information for user PROBI2:

          Label: VALIDATED.BOOT.SG.CECSYS
          Certificate ID: 2QbX2dbCyfLlwdPJxMHjxcRLwtbW40vix0vDxcPi6OJA
          Status: TRUST
          Start Date: 2024/06/22 00:00:00
          End Date:   2025/06/22 23:59:59
          Serial Number:
          >01<
          Issuer's Name:
          >CN=SYSNAME.T=VBCERTAUTH.O=SYSORGN.C=US<
          Subject's Name:
          >CN=SYSNAME.T=VBSIGNING.O=SYSORGN.C=US<
          Subject's AltNames:
          Domain: WWWDOMAIN
          Signing Algorithm: sha256RSA
          Key Usage: HANDSHAKE, DOCSIGN
          Key Type: NIST ECC
          Key Size: 521
          Private Key: YES
          PKDS Label: VALIDATED.BOOT.SG.CECSYS
          Certificate Fingerprint (SHA256):
          F7:25:2E:F3:13:D2:11:7F:9F:F8:78:1A:03:07:48:97:
          7C:8B:EA:1D:96:4D:45:CF:35:F5:BC:50:E9:5E:5B:6A
          Ring Associations:
          Ring Owner: SYS1ID
          Ring:
          >VALIDATED.BOOT.SIGNING.KEYRING.SYS1<
         ---- Connected Certificates -----
                    Label                     Owner         Usage    Default
        VALIDATED.BOOT.CA.CECSYS           CERTAUTH       CERTAUTH     NO
        VALIDATED.BOOT.SG.CECSYS           ID(PROBI2)     PERSONAL     YES
        -------- PKDS Label Meta --------
           PKDS Key Label: VALIDATED.BOOT.SG.CECSYS
              Create Date: 24/06/22
              Create Time: 13:25:22
              Update Date: n/a
              Update Time: n/a
         Callable Service: CSFDSG
               Start Date: n/a
                Stop Date: n/a
               Last Usage: 24/06/22
             Archive Date: n/a
            Archive State: OFF
         Archive Prohibit: OFF
           Archive Recall: n/a
        PrivateKey Status: Active
         --------- Key Attributes ---------
                 Key Usage: KEYM SIGN NO-XLATE
          Key Format/Curve: PRIME
            Curve P (bits): 521
           Curve Q (bytes): 133
            Modulus (bits): n/a
                  Sections: PRIVATE PUBLIC
          Private Key Name: n/a
         -------- Security Profile --------
           CSFKEYS Profile: PROBI2/VALIDATED.BOOT.SG.CECSYS/NONE
             SYMEXPORTABLE: BYLIST
                 ASYMUSAGE: HANDSHAKE SECUREEXPORT
              SYMCPACFWRAP: YES
               SYMCPACFRET: YES
                 Permitted: PROBI2 ALTER
                 Permitted: SYS1 READ
```

1.3. Show the Last Signing

The selected library is passed to the IEWSIGN ACTION=REPORT JCL as shown below:

```
//VALBOOT  JOB REGION=120M,USER=PROBI1
//SIGNS EXEC PGM=IEWSIGN,PARM='ACTION=REPORT,VERBOSE=YES,REPORTLEVEL=3'
//SYSPRINT DD DISP=SHR,DSN=PROBI1.IEWSIGN.REPORTS
//INFILE   DD DISP=SHR,DSN=PROBI1.VBSIGNED.PROBI1.SVCLIB.TESTING
```

Note that the USER= UserId is the Auditors Id and not the Original Signer Id.

```
NSIMVUE - Finding SYS1.SVCLIB, Return/Enter or PFK3
```

If the library has not yet been signed, the following message will be shown:

```
NSIMVUE - Library SYS1.LPALIB2, not Signed by ValBoot
```

If the library has been signed by IEWSIGN, the following message will be shown:

```
PROBI1.SVCLIB.TESTING Last Signed by PROBI1 2024-05-28 16:37:28
```

If the Fingerprint used in the Last Signing cannot be matched to a Signing Certificate, the following message will be shown:

```
NSIMVUE - Unable to Match Fingerprint to any Signing Certificate
```

For nornal signing completion conditions, the following message will be displayed:

```
Show SYS1.SVCLIB Signing Details, Return/Enter, or PFK3
```

Press Enter to display the Certificate Detail Audit Report.

```
/*******************************************************************************/
/*                                                                             */
/*         ICE Viewer - NSIMVUE - ValBoot Certificate Detail - PROBI1          */
/*               Report Date:2024/06/06 Report Time:15:48:28                   */
/*                     Dataset:PROBI1.$VALBOOT.$DETAIL                         */
/*   Source Library:SYS1.SVCLIB, Target Library:PROBI1.VBSIGNED.SYS1.SVCLIB    */
/*                          Signing UserId:PROBI1                              */
/*                                                                             */
/*******************************************************************************/

         Digital certificate information for user JLAUT1:

         Label: VALIDATED.BOOT.SG.CEC006
         Certificate ID: 2QbR08Hk4/HlwdPJxMHjxcRLwtbW40vix0vDxcPw8PZA
         Status: TRUST
         Start Date: 2024/06/05 00:00:00
         End Date:   2025/06/05 23:59:59
```

9. Technical Support Contact Information

NewEra Software, Inc.
8070 Santa Teresa Blvd., Ste. 240
Gilroy, CA 95020

Mailing Address:

PO Box 2726
Gilroy, CA 95020

Phone:

(408) 520-7100
(800) 421-5035

FAX:

(888) 939-7099

Email Address:

support@newera.com

Web Site:

https://www.newera.com

Technical Support:

24 hours a day, 7 days a week
1-800-421-5035
support@newera.com