This is a Simple, Straight Forward way to Manage Secure Boot for z/OS

"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

1.	TABLE	OF CONTENT	2	
2. AN INTRODUCTION TO VALIDATED BOOT				
	1.1.	VALBOOT THE APPLICATION	5	
	1.1.1.	VALBOOT APPLICATION ACCESS AND LICENSING	6	
	1.2.	RELATED VALIDATED/SECURE BOOT REFERENCES	6	
	1.2.1.	DETAILED RACF Explanation	6	
	1.2.2.	https://ibm.biz/zosValidatedBoot	6	
	1.2.3.	IRR.PROGRAM.V2.SIGNING PROFILES	6	
	1.2.4.	RACF STEPS TO THE VALBOOT SIGNING OF RESOURCES	6	
	1.3.	SIGNING WITH VALBOOT – USING IEWSIGN	6	
	1.3.1.	SIGNING ACCOUNTABILITY AND RESPONSIBILITY	6	
	1.4.	VALBOOT APPLICATION - USER ROLES	7	
	1.4.1.	NEZ.VALBOOT.ADMIN UACC(NONE)	7	
	1.4.2.	NEZ.VALBOOT.ISIGN UACC(NONE)	7	
	1.4.3.	NEZ.VALBOOT.AUDIT UACC(NONE)	7	
	1.5.	VALBOOT APPLICATION - ADMINISTRATOR	7	
	1.5.1.	Assigning ValBoot User Roles	7	
3.	VALBO	DT - QUICK START	9	
	1.1.	THE FIRST KEY RING	9	
	1.2.	Your First Certificate Set	11	
	1.3.	TESTING A SIGNING STRUCTURE WORKS	13	
	1.4.	Your First Library Signing	15	
	1.5.	WHEN A SIGNING FAILS	17	
	1.5.1.	RETURN AND REASON CODES	17	
	1.5.1.	Possible Problem Resolutions	18	
	1.6.	WHEN A SIGNING IS SUCCESSFUL	18	
	1.6.1.	Posting to the Control Journal	19	
	1.6.2.	Showing Signing Findings Details	19	
	1.6.3.	Exporting the Signing Certificate	21	
	1.6.4.	Posting Signing Findings to the Control Journal	24	
4.	BUILDI	NG SIGNING STRUCTURES	25	
	1.1.	SETTING UP A SIGNING GROUP	25	
	1.2.	SETTING UP INDIVIDUAL SIGNERS – A RECOMMENDED BEST PRACTICE	28	
	1.3.	SETTING UP AN ADMIN/PERSONAL SIGNER – AN ADHOC GROUP	30	
5.	MANAG	EMENT TOOLS	32	

This is a Simple, Straight Forward way to Manage Secure Boot for z/OS

1.1.	Keyrings – Show the Key Ring Worksheet	
1.1.1.	Worksheet Columns	
1.1.2.	Worksheet Row Selection Operators	
1.2.	RDATALIB – Show Profile/Permits Worksheet	
1.2.1.	Worksheet Columns	
1.2.2.	Worksheet Row Selection Operators	
1.3.	FACILITY – Show Profile/Permits Worksheet	
1.3.1.	Worksheet Columns	
1.3.2.	Worksheet Row Selection Operators	
1.4.	CrtLabel – Show Certificate Worksheet	
1.4.1.	Worksheet Columns	
1.4.2.	Worksheet Row Selection Operators	
1.5.	CEXPORTS – SHOW EXPORT REGISTRY WORKSHEET	
1.5.1.	Worksheet Columns	
1.5.2.	Worksheet Row Selection Operators	
1.6.	Renewals – Show Renewal Registry Worksheet	
1.6.1.	Worksheet Columns	
1.6.2.	Worksheet Row Selection Operators	
1.7.	ICSFPKDS – Show ICSF/PKDS DATA STORE VBOBJECTS	
1.7.1.	Worksheet Columns	
1.7.2.	Worksheet Row Selection Operators	
1.8.	ICSFTKDS – Show ICSF/TKDS DATA STORE VBOBJECTS	
1.8.1.	Worksheet Columns	
1.8.2.	Worksheet Row Selection Operators	
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	
6. ADMI	IN ONLY OPTIONS	
1.1.	Assigning Roles	
1.2.	Accessing ValBoot History	
1.3.	SETTING UP THE LIBRARY SCANNER	
1.3.1.	Real-Time Audit	
1.3.2.	Scheduling an Audit	
1.4.	VB SIGNING STRUCTURES	
7. FACII	LITATED SIGNING USERS INTERFACE - ISIGN	

This is a Simple, Straight Forward way to Manage Secure Boot for z/OS

	1.1.	SIGNING A LIBRARY	51
	1.2.	UNSIGNING A LIBRARY	51
	1.3.	Present Findings	51
8	. FACILIT	ATED AUDIT USERS INTERFACE – AUDIT	52
	1.1.	Show Audit Journal	53
	1.2.	SIGN SELECTION	54
	1.3.	Show the Last Signing	56
9	. TECHNI	CAL SUPPORT CONTACT INFORMATION	58

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.

NSIMVUE - Contact NewEra Support, IFO SUPPLMENTAL License Required

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. <u>https://ibm.biz/zosValidatedBoot</u>
- 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.



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.

NSIMVUE:0601	VUE 18.0	- VB Role Ba	ised Assignme	nts <u>V</u> B	3 Structures
		Update VB Ad	ministrators		
/. PROFILE PERMITTED ACCESS	- REFINE FACI - /. PROBI1 - /. ALTER	LITY NEZ.VAL /. JLAUT1 /. ALTER	BOOT.ADMIN U /. PROBI2 /. ALTER	ACC(NONE) /. CMILL1 /. ALTER	
		Update V	/B Signers		
/. PROFILE PERMITTED ACCESS	- REFINE FACI - /. PROBI1 - /. ALTER	LITY NEZ.VAL /. PROBI2 /. READ	BOOT.ISIGN U /. JLAUT1 /. READ	ACC(NONE)	
PERMITTED ACCESS	:				
		<u>Update V</u>	'B Auditors -		
/. PROFILE PERMITTED	- RDEFINE FAC - /. PROBI1	ILITY NEZ.VA	LBOOT.AUDIT /. JLAUT1	UACC(NONE)	
ACCESS	- /. ALTER	/ . READ	/. READ	••	• •

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.

NSIMVUE:0621	VUE 18.0 - VB Signing	g - Structures	VB Management	
New Key Ring /.	VALIDATED.BOOT.SIGNI Key Ring OwnerId	Key Rings NG.KEYRING. JLAUT1 or /. LLG	PROBI2 Did Query Ring	0wner
APPLDATA Set /.	Id	APPLDATA('SHA512	RACFADM.VBTOK	EN
Alt Key Ring	Group Id UsrId	RACFADM	EP11 Card Ina	ctive
	ValBoot (Certificates		
CertAuthCert /.	VALIDATED.BOOT.CA	/.		5YR
	SignWith Cert VBCERTAUTH	Suffix	Common Name	Exp US
	Subject Title	Orga	anization	Cny
Signing Cert /.	VALIDATED.BOOT.SG	/		<u>1YR</u>
	Personal Cert	Suttix	Common Name	Exp
	Subject Title	Orga	anization	Cny
Select/Click	Create/Update/Profile	e Ring Create/	(Update/Connect	Cert

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.

NSIMVUE:0601 VUE 18.0 - Generated Key Ring Commands
You MUST Confirm Each UserId by Check /.
/. RACDCERT ID(JLAUT1) ADDRING(VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1)
RDATALIB Class Profile
/. RDEF RDATALIB (JLAUT1.VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1.LST) UACC(NONE
RDATALIB Permit Access Command
/. PERMIT JLAUT1.VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1.LST CLASS(RDATALIB)
<u>JLAUT1</u> ACCESS(<u>READ</u>)
<pre>/. RDEF FACILITY (IRR.PROGRAM.V2.SIGNING.JLAUT1) UACC(NONE) /. APPLDATA('SHA512 JLAUT1/VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1') FACILITY Permit Access Command /. PERMIT IRR.PROGRAM.V2.SIGNING.JLAUT1 CLASS(FACILITY) JLAUT1 ACCESS(READ)</pre>
/. Trace <u>Add/Profile/Permit the Key Ring</u>

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:

	VUE 18.0 - ICE Viewer - ValBoot Key Rings	Row 1 to 3 of 3
NSIMVUE 0621	2024/06/21 09:29:44	Target List
Row Selection: L S NumOwner	Validated Boot Key Ring Worksheet - 1 - Rec ist_Ring_Details Rdatalib_Profile Facility_ Key Ring Label	<mark>cord Profile Delete_Rings</mark> Rda Fac Cert War Row
_ 001 JLAUT1 CA Cert SG Cert	VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1 NONENONE	Yes Yes None 001 002 003
******	**************************************	****

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.



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.

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
Row Selection: List_Ring_Details Rdatalib_Profile Facility_Pro	ofile Delete_Rings Fac Cert War Row
001 JLAUT1 VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1 Yes CA Cert VALIDATED.BOOT.CA.CEC0JL DEFAULT:YES SG Cert VALIDATED.BOOT.SG.CEC0JL DEFAULT:YES ************************************	Yes02 001 002 003 *********

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.

V	<pre>UE 18.0 - ValBoot - Certificate Operat:</pre>	ions Row 1 to 2 of 2
NSIMVUE 0621	2024/06/21 09:29:44	Target List
Row Selection: Lis S Row -Owners	DATED.BOOT.SIGNING.KEYRING.JLAUT1 - 2 t_Certificates Export_Cert Renew_Cert I Certificate LabelsUs	- Records Delete_Cert Common_Name sages- Dfl EndDates War
- 001 CERTAUTH VAL 002 PROBI2 VAL ********************	IDATED.BOOT.CA.CEC0JL CEI IDATED.BOOT.SG.CEC0JL PEI ************************************	RTAUTH NO_ 29/06/21 RSONAL YES 25/06/21 ************************************

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 <u>IEWSIGNS</u> .. - Validate <u>JLAUT1</u> 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.

NSIMVUE:0621 VUE 18.0 -	ValBo	oot -	IEWSIGN A	Action:ADMIN
/. Signing User <u>JLAUT1</u>	Con	GrpId		Session Owner PROBI2
Source Libraries	•••	Sign	-in-Place	Signed Libraries
/. SYS1.SVCLIB	PDSU	4	PROBI2	.VBSIGNED.SYS1.SVCLIB
SYS1.LPALIB	PDSU	1795		
SYS1.NUCLEUS	PDSU	655		
SYS1.LINKLIB	PDSU	4487		
••				
• •				
••				
••				
••				
••				
/. Trace SIGNI	NG	U	NSIGNS	FINDING

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:

Line 000000000 Col 001 080
REGION=200M SPRINT
'S1.SVCLIB Ita ************************************
nter/Return or PFK3

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

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.)

Table 2. SIGINIT specific return and reason codes

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:

Invocatior Execution	n parameters: ACTION=SIGN Parameters: ACTION=SIGN,STAT	E=ALL,VERBOSE=	NO,RC4LIM=21474	483647,RC8LIM
DD INFILE OUTFILE	Data Set Name SYS1.SVCLIB PROBI1.VBSIGNED.SYS1.SVCLIB		Volume C5RES1 ZWORK5	Block Size 6144 32760
INFILE sur	nmary: Unsigned primary members Unsigned aliases Signed primary members Signed aliases Non-LM members Overlay LM Zero-Text LM	4 0 0 0 0 0 0 0		
SIGN resul IGG019PX IGG019PY	lts: Successful 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.

JLAUT1 Successful, Show Findings, Return/Enter or PFK3

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.

19

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 -----
                                                         Usage
                   Label
                                           Owner
                                                                   Default
                                       CERTAUTH
         VALIDATED.BOOT.CA.CEC006
                                                       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
             SYMCPACEWRAP: YES
             SYMCPACFRET: YES
                Permitted: PROBI1 ALTER
                Permitted: JLAUT READ
```

This is a Simple, Straight Forward way to Manage Secure Boot for z/OS

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

VUE 18.0 - ValBoot Certificate Export
EXPORT(LABEL
Exporting Label Owner Expiration Key Ring Owner JLAUT1 VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1 JLAUT1
You Must Confirm the Export Dataset
Export Dataset /. PERSONAL.EXPORT.DATASET Registry Version /. D240607 Time /. T171925 List0 Versions
You Must Select the EXPORT Files Format
Format OptionsCERTDERPKCS7D34PKCS12DER/. CERTB64PKCS7B64PKCS12B64For PKCS12 OnlyPKCS12 PASSWORD
/. Trace Select to Export Certificate

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 <u>Select to Export Certificate</u> 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:

PROBI1.PERSONAL.EXPORT.DATASET BROWSE Line 0000000 ----BEGIN CERTIFICATE-----MIIEOzCCAiOgAwIBAgIBATANBgkqhkiG9w0BAQsFADBEMQswCQYDVQQGEwJVUzEP MA0GA1UEChMGSkxPUkdOMRMwEQYDVQQMEwpWQkNFU1RBVVRIMQ8wDQYDVQQDEwZK TE5BTUUwHhcNMjQwNjA1MDcwMDAwWhcNMjUwNjA2MDY10TU5WjBDMQswCQYDVQQG EwJVUzEPMA0GA1UEChMGSkxPUk5HMRIwEAYDV00MEw1W01NJR05JTkcxDzANBgNV BAMTBkpMTkFNRTCBmzAQBgcqhkjOPQIBBgUrgQQAIwOBhgAEAChrDC1vIpP0Ubvu 7sNDQo/j/jVzr/G2HLcKFdlVFNxkvrAeti2/UF+sPCskL8vbA72I+PE9pi5wPy1q kkGQ40y2AYk9rIX5HtJnAQt3Uqy9xdCCFRdHv1G9leenGLDrdf2Q85hG9AW8/pOz vARGciovOn4mZfajVm030x5kARr1t1R9o4HAMIG9MD8GCWCGSAGG+EIBDQQyFjBH ZW51cmF0ZWQgYnkgdGh1IFN1Y3VyaXR5IFN1cnZ1ciBmb3Igei9PUyAoUkFDRikw FAYDVR0RBA0wC4IJV1dXRE9NQU10MA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQU vXfkHdvBD0kXW3mcurm1nYAJX0MwHwYDVR0jBBgwFoAUcHFJFaOsYxpkkpN7TJsq wotSlmYwFAYDVR0SBA0wC4IJV1dXRE9NQUl0MA0GCSqGSIb3DQEBCwUAA4ICAQAa LpbgG3gbyU05L9Q0Z40oQZe5h/2xtzWyBnPWIdrB7mIK6xh59AwQVV22hfhP0bAs mvGch5ZhKS2l9xe8KWkaHWrOMlBKTilKb48zCUIif9c59EdfgtMIx/XVpRzmaAu0 /5ZReZZ0xlMsnCqdEkEMwuT4/8IBuyy3EOMOnP5vpGEAb09qipauKIQMvajh2rj6 rbpAlXbz9KWbF1JfRI9QBygdo/n/9KQLiaEfwYohboFqU0oaFbP2P1JTIdbkN1IS KSdKdrUeI7tPqr+bkZ3hOQCPV5azAMU1rEeCV+9TkaOGXGdQTcHwWmV8L5PM2XBG rIbuyTymzyjWUtokQVhemQTbBJevSZApC551/bGxBXCE6ifbDb/41NeF4UY4oShK f02xgPwkbcb50pktUFg7AxF6Ff2Tn1Bj5g9P0H57tft9hP70MGnlf91f8jn30oXf A0zbG/kHqrNFp4wL+a0YzJzRT1WbUrgZ/WLfFTeHL5P0zBHASQejbfxr0K4PDaT7 L6xZNRm/P/7bC4spzgrHVLtWl22KVjHEPEfS5gGmliHs6TUEJdp8PfOMDY3c2K4u /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----MIIEOzCCAiOgAwIBAgIBATANBgkghkiG9w0BAOsFADBEMOswCOYDVOOGEwJVUzEP MA0GA1UEChMGSkxPUkdOMRMwEQYDVQQMEwpWQkNFUlRBVVRIMQ8wDQYDVQQDEwZK TE5BTUUwHhcNMjQwNjA1MDcwMDAwWhcNMjUwNjA2MDY1OTU5WjBDMQswCQYDVQQG EwJVUzEPMA0GA1UEChMGSkxPUk5HMRIwEAYDVQQMEw1WQ1NJR05JTkcxDzANBgNV BAMTBkpMTkFNRTCBmzAQBqcqhkjOPQIBBqUrqQQAIwOBhqAEAChrDC1vIpP0Ubvu 7sNDQo/j/jVzr/G2HLcKFdlVFNxkvrAeti2/UF+sPCskL8vbA72I+PE9pi5wPy1q kkGQ40y2AYk9rIX5HtJnAQt3Uqy9xdCCFRdHv1G9leenGLDrdf2Q85hG9AW8/poz vARGciovOn4mZfajVm030x5kARr1t1R9o4HAMIG9MD8GCWCGSAGG+EIBDQQyFjBH ZW51cmF0ZWQgYnkgdGhlIFNlY3VyaXR5IFNlcnZlciBmb3Igei9PUyAoUkFDRikw FAYDVR0RBA0wC4IJV1dXRE9NQU1OMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQU vXfkHdvBD0kXW3mcurm1nYAJX0MwHwYDVR0jBBgwFoAUcHFJFaQsYxpkkpN7TJsq wotSlmYwFAYDVR0SBA0wC4IJV1dXRE9NQU10MA0GCSqGSIb3DQEBCwUAA4ICAQAa LpbgG3gbyU05L9Q0Z40oQZe5h/2xtzWyBnPWIdrB7mIK6xh59AwQVV22hfhP0bAs mvGch5ZhKS219xe8KWkaHWrOM1BKTi1Kb48zCUIif9c59EdfgtMIx/XVpRzmaAu0 /5ZReZZ0xlMsnCqdEkEMwuT4/8IBuyy3EOMOnP5vpGEAb09qipauKIQMvajh2rj6 rbpAlXbz9KWbFlJfRI9QBygdo/n/9KQLiaEfwYohboFqUOoaFbP2P1JTIdbkN1IS KSdKdrUeI7tPqr+bkZ3hOQCPV5azAMU1rEeCV+9TkaOGXGdQTcHwWmV8L5PM2XBG rIbuyTymzyjWUtokQVhemQTbBJevSZApC551/bGxBXCE6ifbDb/41NeF4UY4oShK f02xgPwkbcb50pktUFg7AxF6Ff2Tn1Bj5g9P0H57tft9hP70MGnlf91f8jn30oXf A0zbG/kHgrNFp4wL+a0YzJzRT1WbUrgZ/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.

Post Summary to Control Journal, Return/Enter or PEK3 —
/**************************************
/*
/* Export Date:2024/06/07 Report Time:16:39:55 */
/* Registry DS:PROBI1.PERSONAL.EXPREGDS.D240607.T171925 */
/* EXPORT DS:PROBIL.PERSONAL.EXPORT.DATASET // /* */
/**************************************
Source Library:SYS1.SVCLIB, Target Library:PROBI1.VBSIGNED.SYS1.SVCLIB
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
MIIEOZCCA1OgAwIBAgIBATANBgkqhk1G9w0BAQsFADBEMQswCQYDVQQGEwJVUZEP MAQGA1UEChMGSkxPUkdOMRMwEOYDVOOMEwpW0kNFUIBBVVRIMO8wDOYDVOODEwZK
TE5BTUUwHhcNMjQwNjA1MDcwMDAwWhcNMjUwNjA2MDY10TU5WjBDMQswCQYDVQQG
EwJVUZEPMAOGA1UEChMGSkxPUk5HMRIwEAYDVQQMEwlWQlNJR05JTkcxDzANBgNV
BAMIBKPMIKENKICBMZAQBGCQNKJOPQIBBGUIGQQAIWOBNGAEACHIDCIVIPPUDDVU 7sNDOo/j/jVzr/G2HLcKFdlVFNxkvrAeti2/UF+sPCskL8vbA72I+PE9pi5wPv1q
kkGQ40y2AYk9rIX5HtJnAQt3Uqy9xdCCFRdHv1G91eenGLDrdf2Q85hG9AW8/pOz
vARGciovOn4mZfajVm030x5kARr1tlR9o4HAMIG9MD8GCWCGSAGG+EIBDQQyFjBH ZW51cmF0ZW0cYnkcdGblIFNlY3VyaXR5TFNlcnZlciBmb3Tcei9PUy4cUkEDRiky
FAYDVR0RBA0wC4IJV1dXRE9NQU1OMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQU
vXfkHdvBD0kXW3mcurm1nYAJX0MwHwYDVR0jBBgwFoAUcHFJFaQsYxpkkpN7TJsq
wotsimiwFAIDvR0SBAUwC415v1axRE9nQU10MAUGCSqGS1b3DQEBCW0AA41CAQAa LpbqG3qbyU05L900Z40o0Ze5h/2xtzWyBnPWIdrB7mIK6xh59AwQVV22hfhP0bAs
mvGch5ZhKS219xe8KWkaHWrOM1BKTi1Kb48zCUIif9c59EdfgtMIx/XVpRzmaAu0
/5ZReZZ0xlMsnCqdEkEMwuT4/8IBuyy3EOMOnP5vpGEAb09qipauKIQMvajh2rj6 rbpal%bp5llfRI9OBvqdo/n/9K0LiaEfwYobboEqUOaEbP2P1.TTIdbkW1TS
KSdKdrUeI7tPqr+bkZ3hOQCPV5azAMU1rEeCV+9TkaOGXGdQTcHwWmV8L5PM2XBG
rIbuyTymzyjWUtokQVhemQTbBJevSZApC551/bGxBXCE6ifbDb/41NeF4UY4oShK
LUZXGFWKBCDDUPKTUFG/AXF6FIZTNIBJDG9FUHD/TIT9NF/UMGNII91I8JN3U0XI A0zbG/kHgrNFp4wL+a0YzJzRTlWbUrgZ/WLfFTeHL5P0zBHASOejbfxr0K4PDaT7
L6xZNRm/P/7bC4spzqrHVLtW122KVjHEPEfS5qGmliHs6TUEJdp8PfOMDY3c2K4u
/eQ/R08bnzmDQQi/8x5M4JXRwM6F7GJdzRN1Go3Q0zBpOnfx/hlGLmtD2gUhnoQn g7ugu8v4c6Z0e0n+ZacZhasVy50Cidzwk3d4Bz9s1A==
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 <u>Setting up Individual Signers</u>. 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 <u>Key Ring OwnerId</u> but DO NOT check <u>LLQId</u>. This action will make SYS1ID the owner of the key ring.

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

NSIMVUE:0601	VUE 18.0 - VB S	igning - Structures	VB Management
New Key Ring /.	VALIDATED.BOOT. Key Ring OwnerI	lBoot Key Rings SIGNING.KEYRING. SYS1 d /. SYS1ID or LLQI	PROBI2 d Query Ring Owner
APPLDATA Set /.	SYS1 Id	APPLDATA('SHA512 UsrId RACFADM	RACFADM.VBTOKEN EP11 Card Inactive
Alt Key Ring		Alternate APPLDATA Key R	ling

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

USER(S)=	ACCESS=	ACCESS COU	NT=	UNIVERSAL	ACCESS=
IBMUSER	JOIN	003963		READ	
CONNECT	ATTRIBUTES=NON	IE			
REVOKE	DATE=NONE		RESUME	DATE=NONE	
OPEN1	USE	000013		NONE	
CONNECT	ATTRIBUTES=NON	IE			
REVOKE	DATE=NONE		RESUME	DATE=NONE	
OPEN2	USE	000002		NONE	
CONNECT	ATTRIBUTES=NON	IE			
REVOKE	DATE=NONE		RESUME	DATE=NONE	
OPEN3	USE	000000		NONE	
CONNECT	ATTRIBUTES=NON	IE			
REVOKE	DATE=NONE		RESUME	DATE=NONE	
SYSADM	USE	000009		NONE	
CONNECT	ATTRIBUTES=NON	IE			
REVOKE	DATE=NONE		RESUME	DATE=NONE	
SYSOPR	USE	000001		NONE	
CONNECT	ATTRIBUTES=NON	IE			
REVOKE	DATE=NONE		RESUME	DATE=NONE	

When satisfied with the entries, simply cursor under <u>Create/Update/Profile Ring</u> 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 <u>Add/Profile/Permit the Key Ring</u> 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) UNT	IL
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.

	VUE 18.0 - ICE Viewer - ValBoot Key Rings		Row	1 to	3 01	F 3
NSIMVUE 0621	2024/06/21 12:48:36		Ta	arget	List	t
Validated Boot Key Ring Worksheet - 1 - Reg Row Selection: List_Ring_Details Rdatalib_Profile Facility S NumOwner Key Ring Label				Delet Cert	te_R War	ings Row
_ 001 SYS1ID CA Cert_ SG Cert_	VALIDATED.BOOT.SIGNING.KEYRING.SYS1 NONENONE	Yes	Yes	None		001 002 003

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

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.

NSIMVUE:0601	UE 18.0 - VB Signing - Structures VB Management	
New Key Ring /.	ALIDATED.BOOT.SIGNING.KEYRING. JLAUT1 PROBI2 ey Ring OwnerId or /. LLQId Query Ring Owne	er
APPLDATA Set /.	Id APPLDATA('SHA512 RACFADM.VBTOKEN	
Alt Key Ring	Alternate APPLDATA Kev Ring	

When satisfied with the entries, simply cursor under <u>Create/Update/Profile Ring</u> 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:

NSIMVUE:0601 VUE 18.0 - Generated Key Ring Commands
You MUST Confirm Each UserId by Check /.
/. RACDCERT ID(JLAUT1) ADDRING(VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1)
<pre> RDATALIB Class Profile</pre>
·· JLAUT1 ·· ·· ·· ACCESS(UPDATE)
/. RDEF FACILITY (IRR.PROGRAM.V2.SIGNING.JLAUT1) UACC(NONE) /. APPLDATA('SHA512 JLAUT1/VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1') FACILITY Permit Access Command
/. PERMIT IRR.PROGRAM.V2.SIGNING.JLAUT1 CLASS(FACILITY) JLAUT1 ACCESS(<u>READ</u>)
/. Trace Add/Profile/Permit the Key Ring

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 <u>Add/Profile/Permit the Key Ring</u> 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) UNT	ΊL
PERMIT JLAUT1.VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1.LST CLASS(RDATALIB) ID(JLA ICH06011I RACLISTED PROFILES FOR RDATALIB WILL NOT REFLECT THE UPDATE(S) UNTIL	UT 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 01	F 6
NSIMVUE 0621	2024/06/21 12:48:36		Ta	arget	List	t
Row Selection: L S NumOwner	Validated Boot Key Ring Worksheet - 2 - Rec ist_Ring_Details Rdatalib_Profile Facility_ Key Ring Label	<mark>Pro</mark> Rda	<mark>s file</mark> Fac	Dele Cert	te_Ri War	ings Row
_ 001 JLAUT1 CA Cert SG Cert	VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1 _NONE NONE	Yes	Yes	None		001 002 003
_ 002 SYS1ID CA Cert SG Cert	VALIDATED.BOOT.SIGNING.KEYRING.SYS1 NONE NONE	Yes	Yes	None		004 005 006
******	**************************************	***	****	*****	****	****

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.

NSIMVUE:0601	VUE 18.0 - VB Signing	g - Structures	VB Management
	ValBoot	Key Rings	
New Key Ring /.	VALIDATED.BOOT.SIGNIN	G.KEYRING.	PROBI2
	Key Ring Ownerld	or LLQ	d Query Ring Owner
APPIDATA Set /.	ЪТ	ΔΡΡΙ ΠΑΤΑ(' SHA512	RACEADM, VRTOKEN
	. Group Id . UsrId	RACFADM	EP11 Card Inactive
Alt Key Ring			
	Altern	ate APPLDATA Key F	Ring

This process requires no entries. Simply cursor under <u>Create/Update/Profile Ring</u> 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:

NSIMVUE:0621 VUE 18.0 - Generated Key Ring Commands
You MUST Confirm Each UserId by Check /.
/. RACDCERT ID(PROBI2) ADDRING(VALIDATED.BOOT.SIGNING.KEYRING)
<pre>/. RDEF RDATALIB (PROBI2.VALIDATED.BOOT.SIGNING.KEYRING.LST) UACC(NONE)</pre>
<pre>/. RDEF FACILITY (IRR.PROGRAM.V2.SIGNING) UACC(NONE) /. APPLDATA('SHA512 PROBI2/VALIDATED.BOOT.SIGNING.KEYRING') FACILITY Permit Access Command /. PERMIT IRR.PROGRAM.V2.SIGNING CLASS(FACILITY)</pre>
··· ·· ·· ·· ACCESS(<u>READ</u>)
/. Trace Add/Profile/Permit the Key Ring

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 <u>Add/Profile/Permit the Key Ring</u> and press Eenter.

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



	VUE 18.0 - ICE Viewer - ValBoot Key Rings		Row	1 to	9 of	- 9
NSIMVUE 0621	2024/06/21 12:48:36		Ta	arget	List	
Row Selection: L	Validated Boot Key Ring Worksheet - 3 - Rec ist_Ring_Details Rdatalib_Profile Facility_	ords Prot	s file	Delet	:e_Ri	ings
S NumOwner	Key Ring Label	Rda	Fac	Cert	War	Row
_ 001 JLAUT1CA Cert	VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1 NONE	Yes	Yes	None		001 002
SG_Cert 002 PROBI2 CA_Cert_	_NONE	Yes	Yes	None		003 004 005
SG Cert 003 SYS1ID	NONE VALIDATED.BOOT.SIGNING.KEYRING.SYS1	Yes	Yes	None		006 007 008
SG Cert ****************	_NONE	***	****	*****	****	009 ****

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

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.

NSIM	WUE:0624	VUE 18.0 - VB Signing - Management Tools	VB Structures
ĸ	Keyrings	 Show the Key Ring Worksheet 	Userid - PROBI1
R	RDATALIB	Show Profile/Permits Worksheet	Sysplex - ADCDPL System - SOW1
F	FACILITY	Show Profile/Permits Worksheet	IFOhlq - MTGY
С	<u>CrtLabel</u>	Show the Certificate Worksheet	Assign Roles
Х	CExports	Show Exports Registry Worksheet	
Ν	Renewals	Show Renewal Registry Worksheet	VBHISTORY 10
•	тестрире	Charle TCCT (DVDC Data Charle VDObiosta	Library Scan
Р	ICSPPKDS	Show ICSF/PRDS Data Store VBODJects	VB Structure
Т	ICSFTKDS	Show ICSF/TKDS Data Store VBObjects	
S	VBSigner	••• • Validate PROBI1 as a Virtual VB Sig	ner
I	IEWSIGNS	Validate PROBI1 as a Real World Sig	ner

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.

	VUE 18.0 - ICE Viewer - ValBoot Key Rings		Row	1 to	9 01	F 9
NSIMVUE 0601	2024/06/15 15:55:11		Ta	arget	List	t
Row Selection: Li	alidated Boot Key Ring Worksheet - 3 - Rec st Ring Details Rdatalib Profile Facility	ord: Pro	s file	Delet	te_R:	ings
S NumOwner	Key Ring Label	Rda	Fac	Cert	War	Row
- 001 JLAUT1 V	ALIDATED.BOOT.SIGNING.KEYRING.JLAUT1 VALIDATED.BOOT.CA.CEC006	Yes	Yes	02		001 002
SG Cert 002 PROBI1V	VALIDATED.BOOT.SG.CEC006 DEFAULT:YES ALIDATED.BOOT.SIGNING.KEYRING.PROBI1	Yes	Yes	02		003 004
CA Cert SG Cert	VALIDATED.BOOT.CA.CEC002					005 006
_ 003 SYS1ID V CA Cert	ALIDATED.BOOT.SIGNING.KEYRING.SYS1	Yes	Yes	None		007 008
	NONE_ ************************************	***	****	*****	****	009 ****

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 worksheet 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'.

	<pre>VUE 18.0 - ValBoot - RDATALIB Profiles</pre>	Row 1 to 3 of 3
NSIMVUE 0601-	- 2024/06/15 15:55:11	Target List
Row Selection: S RowOwner	Validated Boot RDATALIB Profiles - 3 - Reco bhow_the_Profile Remove_Permit Permit_Additi RDATALIB Profile Label	rds onal Delete_Profile Pmt
001 JLAUT1	VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1.LST	002
_ 002 PROBI1	VALIDATED.BOOT.SIGNING.KEYRING.PROBI1.LST	004
_ 003 SYS1ID	VALIDATED.BOOT.SIGNING.KEYRING.SYS1.LST	002
*****	**************************************	******

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 <u>R_PgmSignVer</u>. 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.

VUE 18.0	- ValBoot - FACILITY Profiles	Row 1 to 6 of 6
NSIMVUE 0601	2024/06/17 11:41:35	Target List
Row Selection: List_the_Det S NumOwner	Goot FACILITY Profiles - 3 - Re ails Remove_Permits Permit_Add FACILITY Profile Label	cords itional Delete_Profile Pmt Row
001 PROBI2 IRR.PROGRAM	I.V2.SIGNING.JLAUT1	002 001
APPLDATA _JLAUT1/VAL	IDATED.BOOT.SIGNING.KEYRING.JL	AUT1 002
_ 002 PROBI2 IRR.PROGRAM	I.V2.SIGNING.PROBI1	002 003
APPLDATAPROBI1/VAL	IDATED.BOOT.SIGNING.KEYRING.PR	OBI1 004
_ 003 PROBI2 IRR.PROGRAM	I.V2.SIGNING.SYS1	002 005
APPLDATA SYS1ID/VAL	IDATED.BOOT.SIGNING.KEYRING.SY	S1 006
******	***** Bottom of data *********	******

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.
- $\circ~$ 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 Certi	ficate Row 1 to 12 of 12
NSIMVUE 0601	2024/06/15 15:55:11	Target List
Validated Boot	Centificate Worksheet - 1	2 - Records
Row Selection: List_Crt Conn	ect_Crt Export_Crt Renew_(Crt Delete_Crt Switch_Labl
S RowOwner Ce	rtificate Label	Rng Key ICSF EndDates War
001 PROBI2 VALIDATED.BO	OT.SG.CEC001	NOP ECC PKDS 24/07/15 030
- 002 PROBI2 VALIDATED.BO 003 PROBI2 VALIDATED.BO	OT.SG.CEC002 OT.SG.CEC009	YES ECC PKDS 25/06/14 NOP ECC PKDS 25/06/14
004 PROBI2 VALIDATED.BO	OT.SG.CEC010	NOP ECC PKDS 25/06/14
005 PROBI2 VALIDATED.BO	OT.SG.CEC00H OT.SG.CEC006	NOP ECC PKDS 24/08/15 060 YES ECC PKDS 25/06/14
007 CERTAUTH VALIDATED.BO	OT.CA.CEC001	NOP RSA PKDS 29/06/14
_ 009 CERTAUTH_ VALIDATED.BO	OT.CA.CEC002	NOP RSA PKDS 29/06/14
010 CERTAUTH_ VALIDATED.BO 011 CERTAUTH_ VALIDATED BO		NOP RSA PKDS 29/06/14
012 CERTAUTH_ VALIDATED.BO	OT.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

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

1.5. CExports – Show Export Registry Worksheet

VUE	<pre>18.0 - Certificate Export Regi</pre>	stry Row 1 to 5 of 5
NSIMVUE 0601	2024/06/15 15:55:11	Target List-
Row Selection: Show_Re	SONAL/CERTAUTH.EXPREGDS- Regis gistry_Detail Delete_Registry_	<pre>try - 5 Entries Record Renews_a_Certificate Exported EndDates War</pre>
001 PROBI2 VALIDA 002 PROBI2 VALIDA	TED.BOOT.SG.CEC002 TED.BOOT.SG.CEC002	24/06/12 25/06/14 24/06/12 25/06/14
- 003 PROBI1 VALIDA 004 JLAUT1 VALIDA 005 PROBI2 VALIDA	TED.B00T.SG.CEC001 TED.B00T.SG.CEC002 TED.B00T_SG_CEC002	24/05/30 *Deleted 24/05/22 *Deleted 24/03/13 25/06/14
*****	********* Bottom of data *****	****

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

VUE 1	18.0 - Certificate Renewal Reg	gistry Row 1 to 6 of 6
NSIMVUE 0601	2024/06/15 15:55:11	Target List-
Row Selection: List_Reg S RowOwner	SONAL/CERTAUTH.RENEWAL - Regis gistry_Detail Delete_Registry_ Certificate Label	<pre>ktry - 6 Entries Record Export_a_Certificate yy/mm/dd hh:mm:ss War</pre>
_ 001 PROBI2 VALIDA _ 002 PROBI2 VALIDA	<pre>FED.BOOT.SG.CEC00H FED.BOOT.SG.CEC001</pre>	24/06/11 16:01:11 060 24/06/11 16:00:44 030
_ 003 PROBI1 VALIDA 004 PROBI1 VALIDA	<pre>FED.BOOT.SG.CEC001 FED.BOOT.SG.CEC001</pre>	24/01/23 10:44:14 Del 24/01/23 10:36:22 Del
005 PROBI1 VALIDA 006 PROBI1 VALIDA	<pre>FED.BOOT.SG.CEC001 FED.BOOT.SG.CEC001</pre>	24/01/23 10:25:22 Del 24/01/23 10:23:11 Del
******	********* Bottom of data *****	*****

1.6.1. Worksheet Columns

• Row The worksheet row number.	0	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

VUE 18.0 -	ValBoot - ICSFPKDS	Resources	Row 1	to 12 of	12
NSIMVUE 0601	2024/06/15 15:55:11		Ta	arget Lis	st
Validated Boo	t ICSF/PKDS Resource	s - 12 - I	Records		
Row Selection: List_PKDS_Lab	el Shows_CSFKEYS_Wor	ksheet Di	splays_the	_Certifi	.cate
S Row Certifica	te Labels	- CSFKEYS	yy/mm/dd	hh:mm:ss	; Act
- 001 VALIDATED.BOOT.CA.CECO	он	PmtUser	24/06/14	16:07:04	Yes
002 VALIDATED.BOOT.CA.CEC0	01	PmtUser	24/06/14	13:47:09	Yes
003 VALIDATED.BOOT.CA.CEC0	02	PmtUser	24/06/14	13:55:47	Yes
004 VALIDATED.BOOT.CA.CEC0	06	PmtUser	24/06/14	17:04:01	Yes
005 VALIDATED.BOOT.CA.CEC0	09	PmtUser	24/06/14	14:39:53	Yes
006 VALIDATED.BOOT.CA.CEC0	10	PmtUser	24/06/14	14:55:26	yes
007 VALIDATED.BOOT.SG.CEC0	0Н	PmtUser	24/06/14	16:07:05	Yes
008 VALIDATED.BOOT.SG.CEC0	01	PmtUser	24/06/14	13:47:09	Yes
009 VALIDATED.BOOT.SG.CEC0	02	PmtUser	24/06/14	13:55:48	Yes
010 VALIDATED.BOOT.SG.CEC0	06	PmtUser	24/06/14	17:04:02	Yes
011 VALIDATED.BOOT.SG.CEC0	09	PmtUser	24/06/14	14:39:53	yes
012 VALIDATED.BOOT.SG.CEC0	10	PmtUser	24/06/14	14:55:27	Yes
*****	*** Bottom of data *	*******	********	*******	****

1.7.1. Worksheet Columns

- o Owner
- o Label
- Profile
- o 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

VUE 18.0 -	ValBoot - ICSFTKDS Resources	Row 1 to 3 of 3
NSIMVUE 0601	2024/06/15 15:55:11	Target List
Row Selection: TOKEN_Details S Row ICSFTKDS	t ICSF/TKDS Resources - 3 - Re RLIST_CRYPTOZ.SOUSER_PROFIL Resource Labels	ecords ES Bind_a_Certificate yy/mm/dd hh:mm:ss Obj
001 NEWERAS.VBTOKEN 002 RACFADM.VBTOKEN 003 RACFJIM.VBTOKEN ************************************	*** Bottom of data *********	24/02/13 14:33:22 000 24/02/14 16:31:30 003 24/02/17 10:49:50 000 ************************************

1.8.1. Worksheet Columns

- ICSFTKDS Resource Label
- o yy/mm/dd
- o hh:mm:ss
- o 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 Userld as a Virtual Signer

		VUE 18.0 - VB Signing Audit - PROBI2 Row 1	to 13 of	36
NSIM	IVUE 0601	2024/06/15 15:55:11Ta	rget List	t
Row Se S Num	election: Lis	Validated Boot Signing Resources - 3	ete_Prof:	iles Row
- 001	FACILITY	PROBI2/IRR.PROGRAM.V2.SIGNING.JLAUT1		001
	Access	FACILITY: PROBI2, JLAUT1	ALTER	002
	APPLDATA	JLAUT1/VALIDATÉD.BOOT.SIGNING.KEYRING.JLAUT1		003
	Access	RDATALIB:PROBI2,JLAUT1	ALTER	004
	CA Cert	VALIDATED.BOOT.CA.CEC006/1824/PKDS/TRUST/RSA		005
	Access	CSFKEYS:PROBI2,JLAUT1	ALTER	006
	SG Cert	VALIDATED.BOOT.SG.CEC006/0364/PKDS/TRUST/ECC		007
	Access	CSFKEYS:PROBI2,JLAUT1	ALTER	008
+	Results	PROBI2 Should be a Valid Signer	-	009
	FingerPrint_	0E:0C:15:20:6C:21:67:C9:61:E8:17:3F:83:6F:	62:30:	010
		4E:20:8F:A7:88:05:10:86:5E:3C:0A:54:D5:F9:0	69:9B	011
002	FACILITY	PROBI2/IRR.PROGRAM.V2.SIGNING.PROBI1		012 013

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.

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

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.

NSIMVUE:0621 VUE 18.0 -	ValBoot -	IEWSIGN Act	ion:ADMIN	
/. Signing User PROBI2	ConGrpId	BUILD	Session Owner	PROBI2
Source Libraries	Sign-	in-Place	Signed Libraries	
/. SYS1.SVCLIB	PDSU 4			
··· SYS1.NUCLEUS	PDSU 655 PDSU 4487			
··				
···				
•••				
/. Trace SIGNIM	NG UN	ISIGNS	FINDING	

See section 1.4, <u>How Library Signing Works</u>, 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, <u>When a Signing is Successful</u> 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.

NSIMVUE:0601 VUE 18.0 - Library Scanner - Actio	n:Au	dit		PROBI	L
Library Registry - IFO.MTGY.\$VB.IEWSI	GNS.	Scanni	ER		
Rt Target Libraries	Val	Fmat	Sign	Unsg	Sa
PROBI1.VBSIGNED.SYS1.LINKLIB	Err	PDSU	4487	Ø	/.
PROBI1.VBSIGNED.SYS1.LPALIB	Err	PDSU	1795	0	/.
PROBI1.VBSIGNED.SYS1.SVCLIB	Yes	PDSU	0	0	/.
/. PROBI1.VBSIGNED.SYS1.NUCLEUS	Err	PDSU	654	0	/.
••					•••
PROBI1.SYS1.SVCLIB.TESTING	Nop		654	0	/.
•••					••
••					••
•••					••
•••					••
•••					••
					•••
••					• •
<u>Real-Time Audit</u> <u>Schedule</u>	d Au	dit			

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.

This is a Simple, Straight Forward way to Manage Secure Boot for z/OS

SIGNIN PRO	BI1.VBSIGNED.SYS1.NUCLEUS	ZWORK5	32760
Modules Inclu <none></none>	ded:		
Modules Exclu <none></none>	ded:		
Algorithm ID 0202	Hash algorithm SHA2-512	Sign algorithm ECDSA-P521	
Certificate s Cert-Index: Subject KeyID Cert Fingerpr RACF Fingerpr Certificate: Signing Keyri	ummary: INDEX001 Modules:09 19090F3C D259BDA7 F int: AE55C57E B3A101DA 1 int: AE:55:C5:7E:B3:A1:0 C3:6B:72:43:0B:4B:F Corresponding certing ng: Unable to Identify	567 First Signature:2024-05 F48E4169 5EFF9259 666E793A 15BCD656 B7E8F4B3 C36B7243 01:DA:15:BC:D6:56:B7:E8:F4 B0:FF:EC:58:BA:EA:0E:2F:B0 ificate not found Key Ring	5-28 16:28:07 0B4BB0FF EC58BA B3: 9D

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.

TCE 18 A - Libnary Scannon - Audit Schodulo
ice 18.0 - Library Scaliner - Audit Schedule
Last Report Date: 2024/06/06 Time: 11:31:56
/ Day - Set Time 03 : 30 and Interval 2 (Specify One Interval)
nn: mm Values 1:2:3:4:6:8:12
/. Wks - Set Time 04 : 40 and Interval SUN.MON
bb mm Values SUN MON THE WED THE EPT SAT
/. Mth - Set Time 05 : 50 and Interval 1,2,3
hh : mm Values 1.2.3.10.15.20.25.EOM
(ENATURERORT Cubicate V/R Company Cabadula Audit
/. EMAILREPORT Subject: VB_Signing_Schedule_Audit
/. 1-To PRR@NEWERA.COM
2-TO PATONEWERA COM
3-10 GHB@NEWERA.COM
4-To ahr@newera.com
5-To jiml@newera.com
7. From SUPPORTENEWERA.COM
Update Audit Schedule

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:

Sample of a Successful Audit:

03) PROBI1.VBSIGNED. VBS0000I SIGNIN	SYS1.SVCLIB G STRUCTURE APPEARS	SIGNED:0004 UNSIGNED:0000 TO REMAIN VALID	
DD Data Set SIGNIN PROBI1.VB	Name SIGNED.SYS1.SVCLIB	Volume ZWORK5	Block Size 32760
Modules Included: <none></none>			
Modules Excluded: <none></none>			
Algorithm ID 0202	Hash algorithm SHA2-512	Sign algorithm ECDSA-P521	
Certificate summarv	:		
Cert-Index:	INDEX001 Modules:0	004 First Signature:2024-05-2	5 10:39:00
Subject KeyID:	A93CB27B EC3B1815	2A825765 625A6FE9 4BBC9FEB	
Cert Fingerprint:	53DC2C65 1429839B . 44b2136F 9793DF14	EDU514UD /5A19241 287E189B C956C34D	
HMC Fingerprint:	53:DC:2C:65:14:29:	83:9B:FD:05:14:0D:75:A1:92:41	:
	44:B2:13:6E:97:93:1	DF:A4:2B:7E:18:9B:C9:56:C3:4D	
RACF Certificate:	ID(JLAUT1) VALIDAT	ED.BOOT.SG.CEC006	
Expires: Signing Kowring:	2025/06/03 Days:36	4 OOT SIGNING KEVDING IINUT1	
Samula of a Failed Au	1:		
Sample of a Falled Au	dit:		
04) PROBI1.VBSIGNED. VBS0000E ONE/MO	SYS1.NUCLEUS RE ELEMENTS OF STRU	SIGNED:0654 UNSIGNED:0000 CTURE NOT VALID	
DD Data Set	Name	Volume	Block Size
SIGNIN PROBI1.VB	SIGNED.SYS1.NUCLEUS	ZWORK5	32760
Modules Included:			
Modules Excluded: <none></none>			
Algorithm ID 0202	Hash algorithm SHA2-512	Sign algorithm ECDSA-P521	
Certificate summarv	:		
Cert-Index:	INDEX001 Modules:0	567 First Signature:2024-05-2	5 10:39:00
Subject KeyID: Cert Fingerprint:	19090F3C D259BDA7 : AE55C57E B3A101DA	F48E4169 5EFF9259 666E793A 15BCD656 B7E8F4B3	

CorrespondingC36B7243 0B4BB0FF EC58BAEA 0E2FB09DHMC 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:B0:9DRACF Certificate:Corresponding certificate not foundSigning 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:00	521 VUE 18.0 - VB Signing Structures - 03
Key Ring: RDATALIB:	PROBI1/VALIDATED.BOOT.SIGNING.KEYRING PROBI1.VALIDATED.BOOT.SIGNING.KEYRING.LST
	ALTER READ UDDATE UDDATE
USI ACCESS	
Key Ring:	BUILDID/VALIDATED.BOOT.SIGNING.KEYRING.BUILD
RDATALIB:	BUILDID.VALIDATED.BOOT.SIGNING.KEYRING.BUILD.LST
Permitted	PROBI1 BUILD
UsrAccess	ALTER UPDATE
Key Ring: RDATALIB:	JLAUT1/VALIDATED.BOOT.SIGNING.KEYRING.JLAUT1 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.PAN ********	ELS(VALBOOT) ***** Top of	Data ** [;]	Line 000	00000000 Co	ol 001 080 ******
INFORMATIO SUPERI INSTAL	N FOR GR DR GROUP LATION D	OUP BUILD =SYS1 ATA=VALIDA1 SFT	OWNER=JLA TED BOOT GROU	UT1 P	CREATED=24	4.171	
TERMUA NO SUB	GROUPS						
USER(S PHAR)= L2	ACCESS= USE	ACCESS COU 000000	NT=	UNIVERSAL NONE	ACCESS=	
C R	DNNECT A	TTRIBUTES=NTE=NONE	IONE	RESUME	DATE=NONE		
	LI DNNECT A	USE TTRIBUTES=N	000000 None	DECIME			
JLAU	T1 ΣΝΝΕCT Δ		000000	RESUME	NONE		
R	EVOKE DA	TE=NONE USE	000000	RESUME	DATE=NONE NONE		
C R	ONNECT A	TTRIBUTES=N TE=NONE	IONE	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.

e SIGN	ING a	ccess to VALBOOT, see Your Admir
- ValBo	oot - 1	IEWSIGN Action:ISIGN
Acting	as Się	gner PROBI1
ies		Signed Libraries
PDSU PDSU	7 4487	
	<pre> • ValB • V</pre>	e SIGNING and ValBoot - : Acting as Signing ies PDSU 7 PDSU 7 PDSU 7 PDSU 7 PDSU 7

- 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:

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

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
Kou Direc DDATALTD Duckiles and Downite
Key Rings, RDATALIB Protiles 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.

NSIMVUE:0621 VUE 18.	.0 - ValBo	pot - IE	WSIGN Act	ion:AUDIT
PROBI2 is Auditor,	, Signing	for Use	rId PHARL	2 in ConGrpId SYS1
Source Libra	ries			Signed Libraries
/. SYS1.SVCLIB	PDSU	4		
••				
••				
••				
···				
••				
••				
••				
••				
••				
••				
10 Show Audit Jou	urnals	Sign Se	election	Show the Last Signing

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.

ICE 18. NSIMJLY 0314	0 - Journaled	Event Selection	Row 1 to 10 of 10 -Journal Entries-							
Selection Options: Show Event_Details Browse Event_Registry View Event_Versions										
- LineCategory	Event	Identification	Date and Time Post							
S NumbName 0001 TCE.DET.VALBOOT	JF Flag1 Fla MG OTHER AUD	g2 -Events- EventId IT SIGNED PROBI	s yy/mm/dd hh:mm:ss Rslt 1 24/06/21 07:26:06 PASS							
0002 TCE.DET.VALBOOT 0003 TCE.DET.VALBOOT	MG OTHER AUD MG OTHER AUD	IT SIGNED PROBI IT SIGNED PROBI	1 24/06/21 07:21:21 PASS 1 24/06/21 07:17:40 PASS							
0004 TCE.DET.VALBOOT 0005 TCE.DET.VALBOOT	MG OTHER AUD	IT SIGNED PROBI IT SIGNED PROBI	1 24/06/21 07:09:47 PASS 1 24/06/21 07:08:51 PASS							
0006 TCE.DET.VALBOOT 0007 TCE.DET.VALBOOT	MG OTHER AUD	IT SIGNED PROBI IT SIGNED PROBI	1 24/06/21 07:07:34 PASS 1 24/06/21 06:29:58 PASS							
0008 TCE.DET.VALBOOT	MG OTHER AUD	IT SIGNED PROBI IT SIGNED PROBI	1 24/06/21 06:27:57 PASS 1 24/06/20 18:05:54 PASS							
**************************************	MG OTHER AUD ********* Bott	om of data *******	1 24/06/20 17:41:40 PASS ********							

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.

BROWSE	PROBI2.\$ICEV	JE.VALBOOT(SIGNI	NG)	Line	0000000000	Col	001 (080
*******	*****	********* Top o	f Data *****	*****	**********	*****	****	****
//VALBOOT	JOB REGION=12	20M, USER=PHARL2,	GROUP=SYS1					
//SIGNS EX	EC PGM=IEWSIG	, PARM= 'ACTION=S	IGN', REGION=	=200M				
//SYSPRINT	DD DISP=SHR,	OSN=PROBI2.IEWSI	GN.SYSPRINT					
//INFILE	DD DISP=SHR,	DSN=SYS1.SVCLIB						
//OUTFILE	DD DISP=SHR,	OSN=PROBI2.VBSIG	NED.SYS1.SVC	CLIB				
******	******	******** Bottom	of Data ***	******	*********	*****	****	****

SYS1.SVCLIB Last Signed by PROBI2 2024-06-22 13:45:38 -

```
/*
         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: 2QbX2dbCyfLlwdPJxMHjxcRLwtbW40vix0vDxcPi60JA
         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
                                      Owner Usage Defaul
CERTAUTH CERTAUTH NO
ID(PROBI2) PERSONAL YES
        VALIDATED.BOOT.CA.CECSYS
        VALIDATED.BOOT.SG.CECSYS
                                                                  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
```

This is a Simple, Straight Forward way to Manage Secure Boot for z/OS

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:

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

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



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 <u>support@newera.com</u>



58