

Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell EMC PowerEdge Servers

This Dell EMC technical white paper describes the process of enabling SEKM on iDRAC, PERC of PowerEdge servers. Key tips and troubleshooting techniques for using SEKM are also discussed.

On PowerEdge server

- Install iDRAC SEKM license
 Ensure iDRAC & PERC
- firmware version support SEKM

Key Management Server (KMS)

- Set up valid CA to sign
- iDRAC CSR • User account to

Prerequisites for setting up SEKM on PowerEdge servers

- represent iDRAC on
- KMSAuthentication setting
- on KMIP of KMS

Abstract

Keeping your business-critical operations and IT infrastructure safe and secure is key to providing seamless services. Dell EMC provides the OpenManage Secure Enterprise Key Manager (SEKM) that assists iDRAC (the Dell EMC PowerEdge server BMC) in locking and unlocking storage devices on a PowerEdge server. This technical white paper provides step-by-step procedure to set up SKEM on iDRAC by using GUI, RACADM and SCP. Also, a few important tips and troubleshooting steps are provided to help you effectively use this SEKM on your PowerEdge servers.

July 2019

Revisions

Date	Description
July 2019	Initial release

Acknowledgements

This technical white paper was produced by the following members of the Dell EMC Enterprise Server Solutions team:

Author—Sanjeev Dambal and Texas Romer

Support—Sheshadri PR Rao (InfoDev)

Other-N/A

The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

© July/23/2019 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Contents

Re	vision	S	2
Acl	knowle	edgements	3
Exe	ecutivo	e summary	6
Pre	erequi	sites	6
1	Set u	up the SEKM solution on PowerEdge servers	7
	1.1	Set up SEKM on external KMS	7
	1.2	Set up SEKM on iDRAC	8
	1.3	Configure SEKM on the iDRAC GUI	9
	1.3.1	Get the CSR file signed on Gemalto	12
	1.3.2	2 Download the server CA file from Gemalto and upload to iDRAC	16
	1.3.3	Configure the Key Management Server (KMS) settings on iDRAC	19
2	Enab	ble SEKM on the iDRAC PERC	21
	2.1	Ensure that SEKM is enabled on iDRAC PERC	23
3	Conf	igure the SEKM Solution by using iDRAC RACADM CLI	25
	3.1	Generate a CSR	26
	3.2	Get the CSR file signed on the Gemalto GUI	26
	3.3	Download the server CA file from Gemalto and upload to iDRAC	30
	3.4	Upload the Server CA file to the iDRAC	31
	3.5	Configure the Key Management Server settings on the iDRAC	31
4	Enab	ble SEKM on Storage Controllers	33
5	Conf	igure SEKM by using a Server Configuration Profile (SCP)	35
	5.1	An SCP file example for configuring iDRAC SEKM configuration	35
	5.2 PER	Example of SCP file that has been modified to only show RAID changes which will enable SEKM on the C and create a RAID locked volume	40
6	Trou	bleshoot issues while setting up SEKM on iDRAC	44
	6.1	I installed the SEKM license, but I cannot enable the SEKM on iDRAC?	44
	6.2 on iD	I set up the KMS information and uploaded the SEKM SSL certificates but I am still unable to enable SEK DRAC?	(M 44
	6.3	I am unable to switch PERC to SEKM mode?	44
	6.4 Faile	I set up SEKM on iDRAC and PERC and rebooted the host, but PERC shows the Encryption Mode as SE	ΞKM 44
	6.5	I checked the SEKM status on iDRAC and it shows "Unverified Changes Pending". What does that mean	? 45
	6.6 "Faile	I changed the KMIP authentication settings on the KMS and now iDRAC SEKM status has changed to ed"?	45
	6.7 my d	I moved a SED from one SEKM enabled PERC to another SEKM enabled PERC on another server and r Irive shows up as Locked and Foreign. How do I unlock the drive?	າow 45

	6.8 Faileo	I moved a SEKM enabled PERC to another server and now my PERC encryption mode shows as SEKM d. How do I enable SEKM on the PERC?	46
	6.9	What key size and algorithm is used to generate the key at the KMS?	46
	6.10	I had to replace my motherboard. How do I now enable SEKM on the new motherboard?	46
	6.11 None	I replaced a SEKM enabled PERC with another PERC and now I see that the new PERC encryption mode . Why is the new PERC encryption mode not SEKM?	is 46
	6.12 from t	I replaced a SEKM enabled PERC and now I see that iDRAC has generated a new key. Why was the key the original PERC not used?	46
	6.13	I am unable to rollback iDRAC firmware – what could be the reason for rollback to be blocked?	47
	6.14 state.	I rebooted the host and key exchange failed because of a network outage and the PERC is in SEKM failed The network outage has been resolved – what do I need to do to put PERC back in SEKM mode?	47
	6.15	I would like to change the keys on a PERC—is that possible?	47
	6.16	I did a system erase, but the PERC encryption mode continues to show as SEKM	47
	6.17	I cannot switch PERC to SEKM mode when it is in LKM mode	47
	6.18 Locke	I migrated an SED, locked by a PERC in LKM mode, to a PERC in SEKM mode. The drive is indicated as and Foreign. Why was it not unlocked?	47
	6.19	I cannot switch PERC to SEKM mode when it is in eHBA personality mode	48
	6.20 failure	Where can I get more information about any type of failures when setting up SEKM or for key exchange es, successful key exchanges or rekey operations?	48
Co	nclusic	איר	48
Α	Tech	nical support and resources	49

Executive summary



Figure 1 Advantages of SEKM over LKM in Dell EMC PowerEdge servers

The OpenManage SEKM enables you to use an external Key Management Server (KMS) to manage keys that can then be used by iDRAC to lock and unlock storage devices on a Dell EMC PowerEdge server. iDRAC requests the KMS to create a key for each storage controller, and then fetches and provides that key to the storage controller on every host boot so that the storage controller can then unlock the SED drives.

The advantages of using SEKM over Local Key Management (LKM) are:

- In addition to the LKM–supported "Theft of a SED drive" use case, SEKM protects from a "Theft of a server" use case. Because the keys used to lock and unlock the SED drives are not stored on the server, attackers cannot access data even if they steal a server.
- Centralized key management at the external Key Management Server.
- SEKM supports the industry standard OASIS KMIP protocol thus enabling use of any external third party KMIP server.

This white paper uses the Gemalto KeySecure as an example of a Key Management Interoperability Protocol (KMIP) Key Management Server, but the workflows described in this technical white paper are applicable for any KMIP compatible KMS, which has been validated for use with PowerEdge SEKM.

Prerequisites

Before you start setting up iDRAC SEKM support, you must first ensure that the following prerequisites are fulfilled. Else, you cannot successfully set up the SEKM.

PowerEdge Server Prerequisites

- iDRAC SEKM license installed
- iDRAC Enterprise license
- iDRAC updated to the firmware version which supports SEKM
- PERC updated to the firmware version which supports SEKM

Key Management Server (KMS) Prerequisites

- Set up a valid CA to sign iDRAC CSR
- A user account that represents the iDRAC on the KMS (For Gemalto, this means having the associated connector license)
- Authentication settings on the KMIP Service of the KMS

1 Set up the SEKM solution on PowerEdge servers

- Set up SEKM on external KMS
- Set up SEKM on iDRAC
- Enable SEKM on the PERC of iDRAC
- Enable SEKM on Storage Controllers
- Configure SEKM by using a Server Configuration Profile (SCP)

1.1 Set up SEKM on external KMS

This section describes the Gemalto KeySecure features that are supported by iDRAC. For information about all other KeySecure features, see the *KeySecure Appliace Administration Guide* available on the Gemalto support site: <u>https://safenet.gemalto.com/</u>.

Users and groups

It is recommended that you create a separate user account for each iDRAC on the KMS. This enables you to protect the keys created by an iDRAC from being accessed by another iDRAC. If the keys require to be shared between iDRACs then it is recommended to create a group and add all iDRAC user names that must share keys to that group.

Authentication

The authentication options supported by the KeySecure KMS are as shown in the sample screen shot:

Authentication Settings	
Password Authentication:	Required
Client Certificate Authentication:	Used for SSL session and username
Trusted CA List Profile:	Server CA
Username Field in Client Certificate:	CN (Common Name)
Require Client Certificate to Contain Source IP:	

(marked

Figure 2 Authentication settings on Gemalto

Password authentication

It is recommended that you set this setting to "Required (most secure)". When set to this option, the password for the user account that represents the iDRAC on the KMS must be provided to iDRAC as explained later in <u>Set up SEKM on iDRAC</u>.

Client certificate authentication

It is recommended that you set to "Used for SSL session and username (most secure)". When set to this option, the SSL certificates must be set up on iDRAC as explained later in <u>Set up SEKM on iDRAC</u>.

The Username field in client certificate It is recommended to set this option to one of the iDRAC supported values:

- CN (Common Name)
- UID (User ID)
- OU (Organizational Unit)

When set to one of these values, the iDRAC username on the KMS must be set up on the iDRAC as explained later in <u>Set up SEKM on iDRAC</u>.

Require client certificate to contain source IP

It is recommended that you enable this option only if the iDRAC IP address does not change frequently. If this option is enabled and the iDRAC IP address changes then the SEKM will stop functioning until the SSL certificates are set up again. If this option is enabled then ensure the same option is enabled on iDRAC also, as explained later in <u>Set up SEKM on iDRAC</u>.

1.2 Set up SEKM on iDRAC

Licensing and firmware update

SEKM is a licensed feature with the iDRAC Enterprise license as a pre-requisite. To avoid an additional iDRAC firmware update, it is recommended that the SEKM license is installed first and then the iDRAC firmware updated to a version that supports SEKM. This is because an iDRAC firmware update is always required after the SEKM license is installed irrespective of whether the existing firmware version supports SEKM or not. The existing interface methods for installing license and firmware update can be used for SEKM.

Set up SSL certificate

The SEKM solution mandates two-way authentication between the iDRAC and the KMS. iDRAC authentication requires generating a CSR on the iDRAC and then getting it signed by a CA on the KMS and uploading the signed certificate to iDRAC. For KMS authentication, the KMS CA certificate must be uploaded to iDRAC.

Generate iDRAC CSR

Though most of the CSR properties are standard and self-explanatory, here are a few important guidelines:

- If the "Username Field in Client Certificate" option on the KMS is enabled then ensure that the iDRAC account user name on the KMS is entered in the correct field (CN or OU or KMS User ID) that matches the value selected in the KMS.
- If the **Require Client Certificate to Contain Source IP** field is enabled on the KMS then enable the "iDRAC IP Address in CSR" field during the CSR generation.

1.3 Configure SEKM on the iDRAC GUI



Figure 3 Key processes in configuring SEKM on PowerEdge servers by using iDRAC GUI

For the Key Management Server, this workflow will be using Gemalto KeySecure as the Key Management Server.

- 1. Start iDRAC by using any supported browser.
- 2. Click iDRAC Settings \rightarrow Services.
- 3. Expand the SEKM Configuration menu and click Generate CSR.

Integrated Dell Remote Access Controller 9 Enterprise		
🐂 Dashboard 📲 System 🗸 🛢 Storage 🗸 🔟 Confi	guration V 🔤 Maintenance V	♦₀ iDRAC Settings ∨
iDRAC Settings		
Overview Connectivity Services Users Settings		
> Local Configuration		
> Web Server		
✓ SEKM Configuration		
KMS Information Set-up upstream communications with the Key Management Server.		
KMS (IP Address or FQDN)*		
Port Number*	5696	
Redundant KMS Information		
Port Number	5696 🔹	
Redundant KMS 1 (IP Address or FQDN)		
+ Add Redundant KMS		
IDRAC Account on KMS Setup your iDRAC account on the Key Management Server. Provide information about Ensure all details match the account details on the Key Management Server.	this iDRAC's account on the Key Management Server	×
User ID*		
Password Provide password if Password based authentication has been enabled on the Key Management Server.		
Rekey All devices in SEKM mode will be rekey-ed.	Rekey	
SEKM Certificate		
Generate and Sign CSR by the Key Management Server Certifyin	ig Authority	
STEP 1 Generate a Certificate Signing Request (CSR) Generate CSR		
STEP 2 Log into the Key Management Server, upload the C	SR and get the CSR signed from the Key M	Janagement Server Certifying Authority(CA).

Figure 4 Generate CSR on the iDRAC GUI

4. In the Generate Certificate Signing Request (CSR) dialog box, select or enter data.

5. Click Generate.

6. The CSR file is generated. Save it to your system.

Generate Certificate Signing I	Request (CSR)	U
Instructions: Generate a CSR that Certifying Authority. If you have alree	can then be signed by the Ke eady generated a CSR, this st	ey Management Server ep is not required.
Generating a new CSR prevents cer CSR from being uploaded to iDRAC	rtificates that are created with	h the previously generated
Common Name (CN)*	idracuserG1FWHQ2	
Country Code (CC)	United States	>
Locality (L)*	Round Rock	
Organization Name (O)*	Dell EMC	
Organization Unit (OU)*	Test	
State*	Texas	
Email*	tester@dell.com	
Subject Alternative Names		0
KMS User ID If username authentication for the SSL certificate is enabled on the Key Management Server using the User ID(UID) field, select this option.	Include	
iDRAC IP Address in CSR	Include	
		Cancel Generate

Figure 5 Enter or select data in the CSR dialog box of iDRAC

- 7. Get the full CSR file contents signed on Gemalto. See Get the CSR file signed on Gemalto.
- 8. Download the signed image file, and then upload it to iDRAC.

1.3.1 Get the CSR file signed on Gemalto

----BEGIN CERTIFICATE REQUEST----

MIIC/jCCAeYCAQAwgY8xCzAJBgNVBAYTAlVTMQ4wDAYDVQQIDAVUZXhhczETMBEG A1UEBwwKUm91bmQgUm9jazERMA8GA1UECgwIRGVsbCBFTUMxDTALBgNVBAsMBFR1 c3QxGTAXBgNVBAMMEG1kcmFjdXN1ckcxRldIUTIxHjAcBgkqhkiG9w0BCQEWD3R1 c3RlckBkZWxsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADqqEPADCCAQoCqqEBAKnj 7mgS3hzKz5rw9Guh5pEe5hnSR7jgI+MSmUgi45UtnXXGkU6a81KXKKE/cRIX9TOL JcBr4teq5kIF2dtXnAX6Eq+M18aVuz0EbRFeD1I70mgwjqMgmRhidnINI6Ya+1WV i/OyLyeJ7l1SKnu4UpUGF1jcpYubDSpT11ZZ5bw3LotBk1rbLq1HpY1c9kGqnjae LPXSqhw/kIc+EockUaN4kuWAVPXmr3xB5ptGugkKneP9ZY0boX4LL0CHMFAcqp0z 76vqTYAVn73oyinMW8p5hchyOThqWbXzocYPeX01k7c4zmb3/aNjXSTSGi/KR4Zg 5VWdVJ+m2ILLNyKC+9MCAwEAAaApMCcGCSqGSIb3DQEJDjEaMBgwCQYDVR0TBAIw ADALBgNVHQ8EBAMCBeAwDQYJKoZIhvcNAQELBQADggEBAD8K6LED0+uNioiBL7Na V3t5LGma/I3sPY14baDdOngNQ87NxOvv/qermZPiWn02Oc/Z1fkpvxw+bYY1dH3+ ewe4Zntba5fkvKxIPcCRKxO/fUadtM928+pKlmIF784OsVaJiyAXFhcaB33Sdtc4 Kt3m2JQUuv+eKDxG+xvugSiwuEftZ2FJZsHUeUcl6aH1cTuBhpm5XiP/IUmvgF1A EplLYX9uwLS7B16UomeRVtP1G2LwksFzaHVFDwGmzQY/AB216UP1CzpXxF02yA3y kjw+SxEOs6JnYpT9yxJSCj2RmddB56ZYUUGD02DL7iALsbkQtfovLpjo9pPBD21p 36A=

-----END CERTIFICATE REQUEST-----

- 1. Log in to Gemalto.
- 2. Click Security Tab \rightarrow Local CAs.
- 3. Click Sign Request.

gem	nalto [×]	Safe	Net Key	Secure M	anag	jem	ient Console		
Home	Security	Devic	e						
Managed Obj	jects	Security *	Local CAs						
🛃 Keys		Certificat	e and CA C	onfiguration	l.				
 Certificate 	s				_	-	_	-	
Certificate	Requests	Local Ce	rtificate Au	thority List					
Authorizat	tion Policies	CA Na	me	C	A Inform	ation			
Users & Grou	ips	Server	CA	C It E	Common: I ssuer: Del xpires: Fe	Dell C. I EMC eb 12 3	A 20:56:48 2029 GMT		
€ Local Auth	nentication	Edit Delete	Download P	roperties Sign Re	equest	Show S	Signed Certs		
E LDAP									
Device CAs 8 Certificates	i SSL icates		Certificate	cate Authorn Authority Name: Common Name:	су []	
	A LISUS		Org	anization Name:					
 Local CAS Known CA 	.s	-	Organizati	onal Unit Name:]	
Advanced Se	curity		State or	Province Name:				1	
 High Secu 	irity			Country Name:	US]	
SSL				Email Address:				1	
 FIPS Statu 	us Server			Key Size:	2048	•		1	
			Certificate	Authority Type:	Se C M O Int	elf-sigr A Cert laximu termec	ied Root CA ifficate Duration (days): m User Certificate Duration diate CA Request	<mark>(</mark> days):	3650 3650
		Create							

Figure 6 Enter or select data in the Select Request section of Gemalto

- 4. Select **Client** as the purpose of generating the certificate.
- 5. Paste the complete CSR content in the Certificate Request box.
- 6. Click Sign Request.

gem	alto [×]	SafeNet KeySecure Management Console
Home	Security	Device
lanaged Obje	cts	Security » Local CAs
🛃 Keys		Certificate and CA Configuration
 Certificates 		Sign Certificate Request
Certificate F	Requests	Sign with Certificate Authority: Server CA (maximum 3526 days) 🔻
Jsers & Group Local Authe	es ntication	Certificate Purpose:
E LDAP		Certificate Duration (days): 3526
Device CAs & S Certificates	SSL	Gi
 SSL Certific Trusted CA 	ates Lists	ZvGJa3AM4f9M9h0iQBQ4q2DBLB3Jz/SLd/GlrQI+2qjfJyNkxrvcqbV2NJGx5p B7 VX3opG6u4wFBKKBrqnHYhu5nD62qK6djosxm2i70imbp+kZ2Dt1Fo70kx1b/5E F4
Local CAs		BnTI+tyWDJoMx/lejMcirjEzUMKvGtvazam5vsHjCm/Q2WILbzaBd0lHWT2BXW
Known CAs		5K HwMPXyLN7UBFoWwZ5W1Z52DCPcKfU6syQIFHHPvrbpKHoST26LaCY3E2hCN9X1 d8
dvanced Secu	urity	DqjgVEURNQ/RwazKgvIW/2E9AZseVDdgOf9RGØVHaP1GEGtN2y9poKRTnC+ygP
High SecuriSSL	ty	q2QsPBjce6uIFg== END CERTIFICATE REQUEST
FIPS Status	Server	Sign Request Back

Figure 7 Request for certificate signing on Gemalto

7. After the request is signed, click **Download** to save the signed CSR file to your system.

Home Security	Device		
maged Objects	Security > Local CAs		
Keys	Certificate and CA Configuration	1	
Certificates	CA Certificate Information		
Certificate Requests			
	Key Size:	2048	2 2010 0117
Authorization Policies	Start Date:	Jun 18 17:31:1.	2 2019 GMT
	Expiration:	Feb 12 17.31.1	2 2029 GW1
sers a groups		C: ST	US
Local Authentication		31.	Round Rock
E LDAP	Issuer:	0:	Dell EMC
		OU:	Product Group Validation
evice CAs & SSL		CN:	Dell CA
ertificates		emailAddress:	texas_roemer@dell.com
SSL Certificates		C:	US
Tructed CA Lists		ST:	Texas
ITUSIEU CA LISIS	0.15-4	L:	Round Rock
Local CAs	Subject:	0:	Dell ENIC Product Test
Known CAs		CN:	idracuserG1FWHQ2
		emailAddress:	tester@dell.com
Ivanced Security			
High Security	BEGIN CERTIFICATE MIID4zCCAsugAwIBAgIDApb/MA0GCSgGSIb	3DOEBCwUAMIGa	MOswCOYDVOOGEwJV
- High Security	UzEOMAwGA1UECBMFVGV4YXMxEzARBgŇVBAc	TClJvdW5klFJv	Y2sxETAPBgNVBAoT
SSL	CERIDGWGRUIDMSEWHWYDVQQLExhQem9kdWN BgNVBAMTB0RlbGwgQ0ExJDAiBgkghkiG9w0	UIEdyb3VWIFZn BCQEWFXRleGFz	MGIRYXRpb24xEDAO X3JvZW11ckBkZWxs
FIPS Status Server	LmNvbTAeFw0x0TA2MTgxNzMxMTJaFw0y0TA	yMTIxNzMxMTJa	MIGXMQswCQYDVQQG
	EWJVUZEOMAWGAIUECAWFVGV41XMXEZARBGN BAoMCER1bGwgRU1DMRUwEwYDVQQLDAxQcm9	kdWN0IFR1c3Qx	GTAXEGNVEAMMEG1k
	cmFjdXN1ckcxR1dIUTIxHjAcBgkqhkiG9w0	BCQEWD3R1c3R1	ckBkZWxsLmNvbTCC
	ASIWDQYJKoZIhvcNAQEBBQADggEPADCCAQo gVUD1D0zdIGY4J7Bn2iJo/aVIpvmSgGwAkm	CggEBAMMNmGtB Bg1ShKvLK1pDH	KcbQI6CmvHuIdfUo Izhkox/+ze2i/TaZi
	zd2z/HHR/Da346MBSGEMuvitcgYVb58Pg9Y	KVVt7D9R£AFk2	/DkJeeTljRnXhB6D
	bgFwpga41EzJj2ICTskQcnAG40DUY+18nzu ogUGB1A0zGeN/rTXrUMTBZs9SBBZm1NM9TD	jXHZK/ABXcu+2 3nKEn668SPuMC	Azbxne0e16zJopWt JU/5Ic06g0HPW5y4
	QHjEyV6ChbSiT1CPUUhStKzvkVrmWpmHpVo	AFW/8JGL8HH19	IGDAdC+IB2Z0QmMC
	AwEAAaMtMCswCQYDVR0TBAIwADARBglghkg	BhvhCAQEEBAMC	B4AwCwYDVR0PBAQD
	f33ZwJxYGva8W8zTS0E8YivhKHUULPGKimD	9h/eFfggtrllf	glX6sjsIgBUGkDi2
	uPyjBt5U1iQL9dH1K1SZ105oMNs6UXrZVDK	X2mIJWPhU7Wj0	NkVky+aIaxBodK1V
	dxVCN7RAmeUYPknbsay8PLkqEZC8rBDvKAc	j/z94KA0s3Re3 R4bVpbMNeH9f7	gjzNBv5P/qt5NuV/ WZ5H1N94Sf2pTbb7
	suPyiJDNsCMHrOIyh+RX0bbxxL3U24yMXjQ	bym3RrrYQ8WXY	Y2DJ 💼
	END CERTIFICATE		Storeston, The second se
	Download Back		
	Download Dack		

Figure 8 Download and save the CSR file on Gemalto

8. On the iDRAC GUI, in the **SEKM Certificate** page, click **Upload Signed CSR** to upload the file you just got signed on Gemalto.

A message is displayed to indicate the successful upload.

Integrated Dell I	Remote Access Controller 9 En	terprise			
The Dashboard	System∨ Storage∨		🔤 Maintenance 🗸	IDRAC Settings ∨	
KMS Inform Set-up upstream o	ation mmunications with the Key Management Server				
KMS (IP Addre	ess or FQDN)*				
Port Number*		5696	+		
Redundant	KMS Information				
Port Number		5696	10		
Redundant KN	IS 1 (IP Address or FQDN)				
+ Add Red	undant KMS				
iDRAC Acco Setup your iDRAC i Ensure all details n	UNE ON KMS account on the Key Management Server. Provide hatch the account details on the Key Managemen	nformation about this iDRAC's acco t Server.	unt on the Key Management Server.		
User ID*					
Password Provide password it Management Serve	Password based authentication has been enabled r.	on the Key			
Rekey	and all be also a	Rek	ey -		
All devices in SERVI	mode will be rekey-ed.				
SEKM Certil	icate				
Generate and	Sign CSR by the Key Management S	erver Certifying Authority			
STEP 1	Generate a Certificate Signing Reque	st (CSR)			
STEP 2	Log into the Key Management Server	, upload the CSR and get the	CSR signed from the Key Ma	nagement Server Certifying Authority(CA	A).
STEP 3	Beturn to this Configuration screen a Upload Signed CSR	nd upload the signed CSR.			

Figure 9 Upload the signed CSR certificate on iDRAC GUI

1.3.2 Download the server CA file from Gemalto and upload to iDRAC

- 1. On the Gemalto GUI, click **Security Tab** \rightarrow **Local CA**.
- Select the Server CA you are using and click **Download**. The file is saved to your local system.

jen	allo	Safenet Ke	Secure M	anage	ement Cons	ole	
Home	Security	Device					
maged Object	ts	Security » Local CAs					
Keys		Certificate and CA	Configuration				
Certificates Certificate R	equests	Local Certificate A	uthority List				
Authorizatio	n Policies	CA Name	C	A Informat	tion		
ers & Group	5	Server CA	C Is E	ommon: De suer: Dell E xpires: Feb	ell CA EMC 12 20:56:48 2029 GMT		
Local Auther	ntication	Edit Delete Download	Properties Sign Re	equest Sh	ow Signed Certs		
LDAP							
		Create Local Certi	ficate Authori	ty			
rice CAs & S tificates	SL	Certificat	e Authority Name:	1		i -	
SSL Certifica	ites						
Trusted CA L	ists		Common Name:	-			
Local CAs		0	rganization Name:				
Known CAs		Organiza	ational Unit Name:				
KIIOWII CAS			Locality Name:				
ranced Secu	rity	State of	or Province Name:				
High Securit	У		Country Name	LLC.			
SSL			Country Name:	05			
FIPS Status	Server	·	Email Address:				
and <mark>and a state</mark>			Key Size:	2048 🔻			
				Self-	signed Root CA		
		0-10-		CA	Certificate Duration (day	ys):	3650
		Certifica	te Authority Type:	Max	kimum User Certificate [Duration (days):	3650

Figure 10 Download the server CA file from Gemalto

- 3. On the iDRAC GUI, in the KMS CA Certificate section, click Upload KMS CA Certificate.
- 4. Upload the Server CA you just downloaded from Gemalto.

A message is displayed to indicate the successful upload.

tegrated Del	Remote Acces	s Controller 9 Ent	erprise			
ashboard	📕 System 🗸	🛢 Storage 🗸	\blacksquare Configuration \lor	🖾 Maintenance 🗸	♥ iDRAC Settings ∨	
SEKM Cert	ificate					
Generate and	d Sign CSR by the	Key Management Se	rver Certifying Authority			
Serial Nur	nber				0296FF	
Subject	Information				Issuer Information	
Common	Name (CN)		idracuserG1FWHQ	2	Common Name (CN)	Dell C
Country C	ode (CC)		US		Country Code (CC)	US
Locality (L	-)		Round Rock		Locality (L)	Round
Organizat	ion Name (0)		Dell EMC		Organization Name (O)	Dell El
Organizat	ion Unit (OU)		Product Test		Organization Unit (OU)	Produ
State			Texas		State	Texas
Valid Fron	n		Jun 18 17:31:12 20	119 GMT	Valid To	Feb 1:
STEP 1 STEP 2 STEP 3	Generate a Cer Generate C Log into the Ke Return to this C	tificate Signing Request SR y Management Server, configuration screen al	upload the CSR and get the nd upload the signed CSR.	CSR signed from the Key Ma	nagement Server Certifying Authority(CA).	
KMS CA Ce	ertificate Upload	d ey Management Serv	ver and download the Key I	Management Server Certify	ing Authority(CA) Certificate. 0	

Figure 11 Upload the CA certificate to iDRAC

1.3.3 Configure the Key Management Server (KMS) settings on iDRAC

1. Enter or select data in the fields, and then click Apply.

IMPORTANT—Make sure you already have a user created on the KMS you will be using for key exchange with the iDRAC. For the user name, ensure it matches the exact value in the CSR certificate property you selected for the Gemalto KMIP **Username field in client certificate** Authentication Settings

For example, in the signed CSR Certificate on iDRAC used in this experiment, the Common Name property is set to "idracuserG1FWHQ2". On the Gemalto server, in the KMIP Authentication Settings, the "Username field in client certificate" field is set to "Common Name". For creating a user name on Gemalto, you must create a user with the name "idracuserG1FWHQ2". This is the user which iDRAC will be using for key exchange.

Integrated Dell Remote Access Controller 9 Enterprise	
🛉 Dashboard 🗏 System 🗸 🛢 Storage 🗸 💷 Configura	ation 🗸 🔤 Maintenance 🗸 🍬 iDRAC Settings 🗸
iDRAC Settings Overview Connectivity Services Users Settings	
> Local Configuration	
> Web Server	
✓ SEKM Configuration	
KMS Information Set-up upstream communications with the Key Management Server.	
KMS (IP Address or FQDN)*	100.64.25.206
Port Number*	5696
Redundant KMS Information	
Port Number	5696 -
Redundant KMS 1 (IP Address or FQDN)	
+ Add Redundant KMS	
IDRAC Account on KMS Setup your iDRAC account on the Key Management Server. Provide information about this i Ensure all details match the account details on the Key Management Server.	DRAC's account on the Key Management Server.
User ID*	idracuserG1FWHQ2
Password Provide password if Password based authentication has been enabled on the Key Management Server.	•••••
Rekey	Rekey
All devices in SEKM mode Will be rekey-eq.	
SEKM Certificate	

Figure 12 Configure the KMS properties on iDRAC GUI

A message is displayed stating a job ID has been created.

- 2. Go to the Job Queue page and ensure that the job ID is marked as successfully completed.
- 3. If you see any job status failures, view Lifecycle Logs for more information about the failure.



Figure 13 A job is created on iDRAC for configuring KMS on iDRAC

Integr	rated Dell Remote Access Controller 9 Er	nterprise	Search Everything
🕈 Dash	board 📱 System 🗸 🛢 Storage 🗸	Configuration V A Maintenance V So iDRAC Settings V	
Main	Itenance le Log Job Queue System Update	System Event Log Troubleshooting Diagnostics SupportAssist	
Job Que	eue		
🔟 Delet	te		
	ID 🗸	Job	Status
+ 0	ID ∽ JID_609661272293	Job SEKM Status Change	Status Completed (100%)
+ 0 + 0	ID → JID_609661272293 JID_608939592760	Job SEKM Status Change Configure: RAID Slot 3-1	Status Completed (100%) Completed (100%)
	ID ∽ JID_609661272293 JID_608939592760 JID_608922607190	Job SEKM Status Change Configure: RAID Slot 3-1 Configure: Import Server Configuration Profile	Status Completed (100%) Completed (100%) Completed (100%)
+ 0 + 0 + 0 + 0	ID ✓ JID_609661272293 JID_609939592760 JID_608922607190 JID_608922128163	Job SEKM Status Change Configure: RAID Slot 3-1 Configure: Import Server Configuration Profile Configure: Import Server Configuration Profile	Status Completed (100%) Completed (100%) Completed (100%) Completed (100%)
+ 0 + 0 + 0 + 0 + 0	ID ✓ JID_609661272293 JID_608339592760 JID_608922607190 JID_608922128163 JID_608918955216	Job SEKM Status Change Configure: RAID Slot.3-1 Configure: Import Server Configuration Profile Configure: Import Server Configuration Profile Configure: Import Server Configuration Profile	Status Completed (100%) Completed (100%) Completed (100%) Failed (100%)

iDRAC SEKM configuration is now complete.

ŀ

2 Enable SEKM on the iDRAC PERC

- 1. On the iDRAC GUI, click Configuration \rightarrow Storage Configuration.
- 2. Select your storage controller.
- 3. Expand Controller Configuration.
- 4. From the Security (Encryption) down-down menu, select Secure Enterprise Key Manager.
- 5. Click Add to Pending Operations.

Integrated Dell Remote Access Controller 9 Enterpris	e	
🕈 Dashboard 🗏 System 🗸 🛢 Storage 🗸 🔟	Configuration V 🛛 🖾 Maintenance V 🌼 iDRAC Setting	js∨
Use this page to configure your storage settings. Storage sett Pending Operations. You must Apply when you are ready to st	ings are confirmed per controller and only one job per controller or art or schedule the job. Pending Operations will persist until the jo	an be scheduled or running at a time. You can b b is created or they are discarded.
Controller PERC H740P Adapter V		
Y Controller Configuration		
Reset Configuration Discard Preserved Cache		
Configuration	Current Value	Pending Value
Controller Mode	RAID	
Patrol Read Mode	Auto 🖌	
Patrol Read Rate	30 👘	
Manual Patrol Mode Action	Action	
Patrol Read Unconfigured Areas	Enabled 🛩	
Check Consistency Mode	Normal v	
Copyback Mode	Off	
Load Balance Mode	Auto 🗸	
Check Consistency Rate	33 👘	
Rebuild Rate	11 80	
BGI Rate	22 👘 %	
Reconstruct Rate	44 160 %	
Enhanced Auto Import Foreign Config	Enabled 👒	
Security (Encryption Status)	None	
Security (Encryption)	Secure Enterprise Key Manager	
	Add to Pending Operations Discard	

Figure 14 Enable SEKM on iDRAC PERC

6. Select At Next Reboot.

A message is displayed indicating that the job ID is created.

- 7. Go to the Job Queue page and ensure that this job ID is marked as Scheduled.
- 8. Restart the server to run the configuration job.

Integrated Dell Remote Access Controller 9 Enterprise		Search Everything
🕈 Dashboard 🔳 System 🗸 🛢 Storage 🗸 🔟 Conf	1 Information	
Manual Patrol Mode Action	RAC0609: The job JID_609663137404 has been successfully added to the job queue.	
Patrol Read Unconfigured Areas	The status of jobs can be viewed on the Job Queue page.	
Check Consistency Mode	Job Oueue Ok	
Copyback Mode		
Load Balance Mode	Auto 🗸	
Check Consistency Rate	33 * %	
Rebuild Rate	11 * %	
BGI Rate	22 * %	
Reconstruct Rate	44	
Enhanced Auto Import Foreign Config	Enabled 💌	
Security (Encryption Status)	None Secu	re Enterprise Key Manager Pending
Security (Encryption)	Action × Assig	ined
	Add to Pending Operations Discard	
Foreign Configuration		

Figure 15 A job is created to enable SEKM on IDRAC PERC

inte	egrated Dell Remote Access Controller 9 Ent	terprise	Search Everything Q
🛉 Das	shboard 📱 System 🗸 🛢 Storage 🗸	Configuration V Anintenance V So iDRAC Settings V	Enable Group
Mai	ntenance		
Lifecy	ycle Log Job Queue System Update	System Event Log Troubleshooting Diagnostics SupportAssist	
Job Q	ueue		
💼 Del	lete		
C		Job	Status
+ 0	JID_609663137404	Configure: RAID.Slot.3-1	Scheduled (0%)
+ c	JID_609663137404 JID_609661272293	Configure: RAID Slot 3-1 SEKM Status Change	Scheduled (0%) Completed (100%)
+ (+ (JID_609663137404 JID_609661272293 JID_608939592760	Configure: RAID Slot.3-1 SEKM Status Change Configure: RAID Slot.3-1	Scheduled (0%) Completed (100%) Completed (100%)
+ (+ (+ (JID_609663137404 JID_609661272293 JID_608939592760 JID_608922607190	Configure: RAID Slot 3-1 SEKM Status Change Configure: RAID Slot 3-1 Configure: Import Server Configuration Profile	Scheduled (0%) Completed (100%) Completed (100%) Completed (100%)
+ (+ (+ (+ (JID_609663137404 JID_609661272293 JID_608989592760 JID_608922607190 JID_608922128163	Configure: RAID Slot.3-1 SEKM Status Change Configure: RAID Slot.3-1 Configure: Import Server Configuration Profile Configure: Import Server Configuration Profile	Scheduled (0%) Completed (100%) Completed (100%) Completed (100%) Completed (100%)
+ (+ (+ (+ (+ (JID_609663137404 JID_609661272293 JID_608989592760 JID_608922607190 JID_608922128163 JID_608913760	Configure: RAID Slot.3-1 SEKM Status Change Configure: RAID Slot.3-1 Configure: Import Server Configuration Profile Configure: Import Server Configuration Profile Configure: Import Server Configuration Profile	Scheduled (0%) Completed (100%) Completed (100%) Completed (100%) Completed (100%) Failed (100%)

Figure 16 A job is scheduled to enable SEKM on iDRAC PERC

After restarting the server, the configuration job is run in the Automated Task Application to enable SEKM on the PERC.

The server is automatically restarted.

9. After the POST or Collecting Inventory operation is completed, ensure that the job ID has been marked as "Completed" on the Job Queue page.

	Integr	rated Dell Remote Access Controller 9 E		Search Everything Q
*	Dasht	board 🔳 System 🗸 🛢 Storage 🗸	■ Configuration ∨	Enable
M	ain	tenance		
Li	fecycl	e Log Job Queue System Update	System Event Log Troubleshooting Diagnostics SupportAssist	
Job	Que	eue		
Û	Delete	e		
	Π		Job	Status
	1000			otatao
+		JID_609663137404	Configure: RAID.Slot.3-1	Completed (100%)
++		JID_609663137404 JID_609661272293	Configure: RAID.Slot 3-1 SEKM Status Change	Completed (100%) Completed (100%)
+ + +		JID_609663137404 JID_609661272293 JID_608939592760	Configure: RAID Slot 3-1 SEKM Status Change Configure: RAID Slot 3-1	Completed (100%) Completed (100%) Completed (100%)
+ + +		JID_609663137404 JID_609661272293 JID_608939692760 JID_608922607190	Configure: RAID Slot 3-1 SEKM Status Change Configure: RAID Slot 3-1 Configure: Import Server Configuration Profile	Completed (100%) Completed (100%) Completed (100%) Completed (100%)
+ + + +		JID_609663137404 JID_609661272293 JID_609939592760 JID_608922607190 JID_608922128163	Configure: RAID Slot 3-1 SEKM Status Change Configure: RAID Slot 3-1 Configure: Import Server Configuration Profile Configure: Import Server Configuration Profile	Completed (100%) Completed (100%) Completed (100%) Completed (100%) Completed (100%)
+ + + + +		JID_609663137404 JID_609661272293 JID_6093939592760 JID_608922607190 JID_608922128163 JID_608918955216	Configure: RAID Slot 3-1 SEKM Status Change Configure: RAID Slot 3-1 Configure: Import Server Configuration Profile Configure: Import Server Configuration Profile Configure: Import Server Configuration Profile	Completed (100%) Completed (100%) Completed (100%) Completed (100%) Completed (100%) Failed (100%)

Figure 17 A job successfully run to enable SEKM on iDRAC PERC

2.1 Ensure that SEKM is enabled on iDRAC PERC

- 1. On the iDRAC GUI, click **Storage** \rightarrow **Overview**.
- 2. Expand your storage controller and ensure the following statuses:
 - Security Status = Security Key Assigned
 - Encryption Mode = Secure Enterprise Key Manager

	Integrated Dell Ren	note Access Controller 9 Er	nterprise				Search Everything
ħ	Dashboard 🔳 S	ystem∨ 🛢 Storage∨	🔟 Configuration 🗸 🖂 Main	tenance 🗸 🌼 iDI	AC Settings 🗸		Enable Group
St	orage						
0	verview						
		Summary	Controllers	Physical Disks	s Virtual C	iisks Enclo	osures
	Controllers						
	Rollup Status	Name	Device Description	PCI Slot	Firmware Version	Driver Version	Cache Memory Size
+		BOSS-S1	AHCI controller in slot 6	6	2.5.13.3016	Information Not Available	0 MB
_		PERC H740P Adapter	RAID Controller in Slot 3	3	50.9.0-2699	Information Not Available	8192 MB
	Advanced Pro	perties					
	Status				Rebuild Rate	11%	
	Controller Mode		RAID	_	BGI Rate	22%	
1	Security Status		Security Key Assigned		Reconstruct Rate	44%	
1	Encryption Mode		Secure Enterprise Key Manager		Max Capable Speed	12 Gbps	
	SAS Address		0x5D0946600B5E9F00		Persistent Hotspare	Disabled	
	PCI Vendor ID		0x1000		Load Balance Setting	Auto	
	PCI Subvendor II	0	0x1028		Preserved Cache	Not Present	
	PCI Device ID		0x16		Time Interval for Spin Down	30 minutes	
	PCI Subdevice IE	1	0x1fcb		Spindown Unconfigured Driv	es Disabled	
	PCI Bus		0x33		Spindown Hotspares	Disabled	
	PCI Device		0x0		Learn Mode	Not Supported	

Figure 18 Ensure that SEKM is enabled on your controller

- 3. On the Gemalto GUI, click the **Security** tab.
- 23 Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell EMC PowerEdge Servers

A Key ID is generated and displayed for the user you assigned to the iDRAC. This is the key ID that iDRAC uses for key exchange.

gemalto	SafeNet KeySecure Management Console								
Home Security	Device								
Managed Objects	Security » Keys » Key List								
Keys	Keys								
• Keys	Keys								
Query Keys		Query: [All] 🔻	Run Query						
Create Keys	Items per page: 10 V Submit	Page 1	of 113 Go						
 Import Keys 	Key Name	Owner	Object Type	Algorithm	State	Exportable	Deletable	Versioned Key	Certificate
 Key Options 	B6BDDC6AB94C2D5D696E30861ED1326DA0B5EEB2540A51AA991F8C6484EB1AF0	idracuserG1FWHQ2	Symmetric Key	AES-256	Active	Z	Ľ.		
 Schedule Key Rotation 	E28C646B9E7599B6BD64C1BF0486E07C9B7695A9E91562D69DB3776E186066D0	idracuser18R5QM2	Symmetric Key	AES-256	Active	×	Z		
I Certificates	D8F4B12FCF0760826056BDB9622F3F9940B5CEF12B3917C31F6992DAEBEF5C3F	idracuserG1FWHQ2	Symmetric Key	AES-256	Active	Z	Z		
Certificate Requests	7567369EE99C4DDA3C42420F6870675CAA3ACDC0E6E597A1A63D741A02F236E4	idracuser18R5QM2	Symmetric Key	AES-256	Active	Ø	1		
Authorization Policies	2FFD332B89EA1EBE9014278FA0EAF07834674B96BB33D16DE998A934165CD413	idracuser18R5QM2	Symmetric Key	AES-256	Active	Ø	Ø		
- Addition 2 delign Policies	FBEB715DCEE88D41825A67389E7559A39CC6D673B3E2D47CAD7593E96AA91C0F	idracuser18R5QM2	Symmetric Key	AES-256	Active	Ø	ø		
Users & Groups	7FF5FDCF8838D7043D94CE18E809A3D5EF012EA8A38BFDAA9371AAEAFA227113	idracuserR640112	Symmetric Key	AES-256	Active	Ø	Z		
Local Authentication	BEAB2C0AC07DA915E9EA0D9C6C11318E72F2A40750F1AC061AC84F5702A01D31	idracuser18R5QM2	Symmetric Key	AES-256	Active	Ø			
LDAP LDAP	9788E9ACD6C2AE9A2A401616276B928D99AAE2476FEF01F4F9F0CE2BA267CDB2	idracuser18R5QM2	Symmetric Key	AES-256	Active	Ø	₽ ′		
	52342A942B7D5DA6F177C28C83351BF165741F2C7815A683CCCF81D4EE86022F	idracuser18R5QM2	Symmetric Key	AES-256	Active	Ø	Ø		
Device CAs & SSL Certificates		1 - 10 of	f 1130						
SSL Certificates	Delete Properties								
Trusted CA Lists	Delete All Keys On Current Page								
Local CAs									
Known CAs	Create Key Import Key Create Query								
Advanced Security									

Figure 19 The iDRAC key ID is generated on Gemalto

The SEKM setup operation is completed. You can now start creating locked RAID volumes and perform key exchanges.

3 Configure the SEKM Solution by using iDRAC RACADM CLI

In this workflow example, an iDRAC RACDM (remote) is used to set up the complete SEKM solution for the iDRAC. For the Key Management Server (KMS), Gemalto KeySecure is used as the Key Management Server.

- 1. Configure the iDRAC SEKM certificate attributes. These must be configured first before you generate a CSR file.
- 2. To set each attribute, run the SET command. The examples here use the default iDRAC user name and password (root/calvin).
- 3. Replace it with an appropriate iDRAC user name and password set up on the PowerEdge server.

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn get idrac.sekmcert
[Key=idrac.Embedded.1#SEKMCert.1]
#CertificateStatus=NOT PENDING
CommonName=
CountryCode=US
EmailAddress=
LocalityName=
OrganizationName=
OrganizationUnit=
StateName=
SubjectAltName=
UserId=
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.sekmcert.CommonName
idracuserG1FWHQ2
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.sekmcert.CountryCode US
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.sekmcert.EmailAddress
tester@dell.com
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.sekmcert.LocalityName "Dell
EMC'
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.sekmcert.OrganizationName
"DELL EMC"
[Key=idrac.Embedded.1#SEKMCert.1]
Object value modified successfully
```

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.sekmcert.OrganizationUnit Test [Key=idrac.Embedded.1#SEKMCert.1] Object value modified successfully C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.sekmcert.StateName Texas [Key=idrac.Embedded.1#SEKMCert.1] Object value modified successfully

3.1 Generate a CSR

- 1. Get the CSR contents signed on the Gemalto server. See Get the CSR file signed on Gemalto.
- Download the signed file, and then upload it back to iDRAC. Run the following command at the RACADM CLI:

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sslcsrgen -g -t 3 -f sekm_csr

A CSR is successfully generated and downloaded.

3.2 Get the CSR file signed on the Gemalto GUI

----BEGIN CERTIFICATE REQUEST-----

MIIC/jCCAeYCAQAwgY8xCzAJBgNVBAYTA1VTMQ4wDAYDVQQIDAVUZXhhczETMBEG A1UEBwwKUm91bmQgUm9jazERMA8GA1UECgwIRGVsbCBFTUMxDTALBgNVBAsMBFR1 c3QxGTAXBgNVBAMMEGlkcmFjdXNlckcxRldIUTIxHjAcBgkqhkiG9w0BCQEWD3Rl c3RlckBkZWxsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKnj 7mgS3hzKz5rw9Guh5pEe5hnSR7jgI+MSmUgi45UtnXXGkU6a81KXKKE/cRIX9TOL JcBr4teq5kIF2dtXnAX6Eq+M18aVuz0EbRFeD1I70mgwjqMgmRhidnINI6Ya+1WV i/OyLyeJ711SKnu4UpUGF1jcpYubDSpT11ZZ5bw3LotBk1rbLq1HpY1c9kGgnjae LPXSqhw/kIc+EockUaN4kuWAVPXmr3xB5ptGugkKneP9ZY0boX4LL0CHMFAcqp0z 76vqTYAVn73oyinMW8p5hchyOThqWbXzocYPeX01k7c4zmb3/aNjXSTSGi/KR4Zq 5VWdVJ+m2ILLNyKC+9MCAwEAAaApMCcGCSqGSIb3DQEJDjEaMBgwCQYDVR0TBAIw ADALBgNVHQ8EBAMCBeAwDQYJKoZIhvcNAQELBQADggEBAD8K6LED0+uNioiBL7Na V3t5LGma/I3sPY14baDdOngNQ87NxOvv/qermZPiWn02Oc/Z1fkpvxw+bYY1dH3+ ewe4Zntba5fkvKxIPcCRKxO/fUadtM928+pKlmIF784OsVaJiyAXFhcaB33Sdtc4 Kt3m2JQUuv+eKDxG+xvugSiwuEftZ2FJZsHUeUcl6aH1cTuBhpm5XiP/IUmvgF1A EplLYX9uwLS7B16UomeRVtP1G2LwksFzaHVFDwGmzQY/AB216UP1CzpXxF02yA3y kjw+SxEOs6JnYpT9yxJSCj2RmddB56ZYUUGD02DL7iALsbkQtfovLpjo9pPBD21p 36A=

----END CERTIFICATE REQUEST-----

- 1. On the Gemalto GUI, click **Security Tab** \rightarrow **Local CAs**.
- 2. Click Sign Request.

gem	alto	Sat	feNet Ke	ySecure N	lana	gei	ment Console		
Home	Security	De	vice						
anaged Obje	acts	Security	» Local CAs						
] Keys		Certifi	cate and CA	Configuratio	n				
] Certificates			0		3	-			_
Certificate	Requests	LOCAL	Certificate i	AUTIONITY LIST	8				
Authorizati	on Policies	CA	Name		CA Inform	matic	on		
ers & Group	ps	• Ser	ver CA		Common Issuer: De Expires: F	: Dell ell EN Feb 1	CA MC 2 20:56:48 2029 GMT		
Local Auth	entication	Edit De	lete Download	Properties Sign	Request	Shov	v Signed Certs		
LDAP									_
evice CAs & ertificates	SSL		Certifica	te Authority Name					
SSL Certilit	ales			Common Name					
Trusted CA	LISTS	-	(Organization Name				- D	
Local CAs		-	Organia	zational Unit Name					
Known CAs	K	-	0.0100000	Locality Name					
vanced Sec	urity	-	Chata	Descripter Norma					
High Secur	ity		State	or Province Name			7		
SSL				Country Name	US		<u></u>		
FIPS Statu	s Server			Email Address					
	<u> </u>			Key Size	2048	•			
		-	Cartific	ste Authority Tune) ۱	Self-si CA C	igned Root CA ertificate Duration (days):		3650
			Certific	ate Automity Type	6	Maxir	mum User Certificate Durati	on (days):	3650
		1							

Figure 20 Get the CSR request signed on Gemalto GUI

- 3. Select **Client** as the purpose of generating a certificate.
- 4. Paste the complete CSR contents and click **Sign Request**.

gema	alto	SafeNet KeySecure Management Console
Home	Security	Device
lanaged Objec	ts	Security > Local CAs
		Sign Certificate Request
 Certificate Re Authorization 	equests n Policies	Sign with Certificate Authority: Server CA (maximum 3526 days) 🔻
Jsers & Groups	Nication	Certificate Purpose: Server
E LDAP		Certificate Duration (days): 3526
evice CAs & S ertificates	SL	BgNVHRMEAjAAMAsGA1UdDwQEAwIF4DANBgkqhkiG9w0BAQsFAAOCAQEAOVjLEX Gi
 SSL Certifica Trusted CA L 	ists	ZvGJa3AM4f9M9h0iQBQ4q2DBLB3Jz/SLd/GlrQI+2qjfJyNkxrvcqbV2NJGx5p B7 VX3opG6u4wFBKKBrqnHYhu5nD62qK6djosxm2i70imbp+kZ2Dt1Fo70kx1b/5E
Local CAs		BnTI+tyWDJoMx/lejMcirjEzUMKvGtvazam5vsHjCm/Q2WILbzaBd0lHWT2BXW
Known CAs		HWMPXyLN7UBFoWwZ5W1Z52DCPcKfU6syQIFHHPvrbpKHoST26LaCY3E2hCN9X1 d8
dvanced Secu	rity	DqjgVEURNQ/RwazKgvIW/2E9AZseVDdgOf9RG0VHaPlGEGtN2y9poKRTnC+ygP CT
High SecuritySSL	y	q2QsPBjce6uIFg== END CERTIFICATE REQUEST
FIPS Status	Server	Sinn Benuest Back

Figure 21 Submit a Sign Request job

5. After the CSR is successfully signed, click **Download**.

The signed CSR file is saved to your system.

Security > Local CAs s tificates tificates tificates tificates tificates tificates tificates tificates tificates al Authentication p tissuer: 0: US s ST. Texas al Authentication p Issuer: certificates ted CA Lists al CAs wn CAs ed Security 1 Security tes: cotting cotting tes: of Security tes: tes: <tr< th=""><th>e Security</th><th>Device</th><th></th><th></th></tr<>	e Security	Device		
eys Ecrtificate and CA Configuration eys Ertificate and CA Configuration CA Certificate Information CA Certificate Information Start Date: Jun 18 17/31:12 2019 GMT Expiration: Feb 12 17/31:12 2019 GMT Start Date: Jun 18 17/31:12 2019 GMT C: US Start Date: Jun 18 17/31:12 2019 GMT C: US scal Authentication ST: DAP Stude CA Lists scal CAs C: US scal CAs Studects: Exage nown CAs C: US scal CAs Studect: C: US start Date: Nound Rock St. C: US start Date: St. C: US St. start Scaling C: US St. start Date: St. Nound Rock OU: Product Test start Date: Nound Rock C: US start Date: St. Record Start Date: Nound Rock start Date: C: US St.	aged Objects	Security » Local CAs		
CA Certificate Information ertificates ertificate Requests uthorization Policies Start Date: Jun 18 17:31:12 2019 GMT Expiration: Feb 12 17:31:12 2029 GMT Expiration: Feb 12 17:31:12 2029 GMT CUS ST. Texas boal L: Round Rock DAP OU: Product Group Validation CN: Dell CA emailAddress: texas C: US St. Certificates C: US start Date: St. Trexas cold CAs Subject: O: Dell EMC nown CAs C: US St. Round Rock start Date: Subject: O: Dell EMC GO: Product Group Validation C: US St. Round Rock start Date: Subject: O: Dell EMC ocil CAs OU: Product Test C: N: kiracuserG1FWH02 gli Security II: 42CCAsugAwiEkg1DApD/kiROCSq0SID3DQEBCWUANIGWEWOYUVQQEWJVU D: Product Test start Date: Subject: O: Dell EMC D: Product Test start Date: Subject: O: Dell EMC D: Product Test start Date:	leys	Certificate and CA Configuration	í -	
ertificate Requests uthorization Policies & Groups ccal Authentication DAP DAP Issuer: C: US Start Date: Jun 18 17:31:12 2029 GMT C: US scal Authentication DAP Issuer: O: Dell EMC OU: Product Group Validation C: US States States States States C: US States C: US States States C: US States	Certificates	CA Certificate Information		
Key Size: 2048 uthorization Policies Start Date: Jun 18 17:31:12 2019 GMT Expiration: Feb 12 17:31:12 2029 GMT Expiration: Feb 12 17:31:12 2029 GMT C: US bocal Authentication ST: Texas DAP Issuer: O: Dell EMC OU: Product Group Validation SL: Criticates C: US susted CA Lists C: US ocal CAs Subject: O: Dell EMC nown CAs C: US reced Security St. It Round Rock SL: SUB C: US Ip5 Security St. Dell EMC OU: SL: St. Dell EMC OU: Product Test Ip5 Status Server MID42/CEAsugAx/EBg/TBApb/MAD0CS/GSG51bSD0EBCwUAMI GM06w0C0YDV00GEw/V UzeOMAw6A1UECCMFV04Y1MMxEARBg/NBAFC11_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V012MEXEARBg/NBAFC1_V04MEXEARBg/NBAFC1_V04MEXEARB	Certificate Requests			
alit Date: Juin Date: <td>A the institution</td> <td>Key Size:</td> <td>2048 Jun 19 17-24-41</td> <td>2010 CMT</td>	A the institution	Key Size:	2048 Jun 19 17-24-41	2010 CMT
i & Groups C: US scal Authentication ST: Texas DAP Usuardian issuer: O: Dell EMC OU: Product Group Validation OU: Product Group Validation St. Certificates C: US rusted CA Lists C: US scal CAs C: US nown CAs C: US inced Security Dell EMC igh Security Dell EMC SL OU: Product Test ISL RumalAddress: teste@dell.com Inced Security NITD42CC8.ugAMEBAgTIDApb/MAD0CSqGSIb3DDEBCwDAMIGqMQswCQTDVQQEBwJV SL USEOMacGlutCEMPTV04YIMKASARBgNVBACTCLJvdMSkFJVY2xxETAPBgNVBAct CERLBOAGRUTUMSEMWTVDQLExhQemBkdMN01EdybSWFF2hb51kYXpb24xEDb0 BgNVUSEOMacGlutCEMPCV4YIMALEAABgNVBACTCLJvdMSkFJVY2xxETAPBgNVBAct IpS Status Server DEMEMBY DUDUCAWYUNDQLExhQemBkdMN01ERJb24xEDb0 BedVUZEOMAWGAUECAWFUVVDQLEAACGgreBAMMMeCEKbcD1CEMVEGNVEGUEWORD Saturb2000000000000000000000000000000000000	Authorization Policies	Start Date:	Feb 12 17:31:12	2019 GMT
C. O.S. bocal Authentication DAP DAP C. S. B. C. C. S. B. C. C. S. B. C. C. S. S. Krates SL Certificates rusted CA Lists ocal CAs nown CAs C. US subject: O: Dell EMC OU: Product Test nown CAs CELLOW CERTIFICATE MITD42CCAsugAwIBAgIDApb/MA0CCSGSID3DQEBCWUMIGdM0swCQUDVQQEEwJV VizeDMMAGAUCENTWEX2ABABMURACTCLIveMSkIFJvV2sxETAPBgNVBACT SL Ipin Security SL SL IPS Status Server MID44CCRIbowg012kUDBaby/MA0CCSGSENDAUCEWXMIG4M03wCVDVQ02EwJV VuzEOMAGAUCENDAPUSV4XVMIXEARBgNVBACTCLIveMSkIFJvV2sxETAPBgNVBACT SL IPS Status Server MID44CCRIbowg012kUDApemSkdMN017kBAUG2wCVDVQ02EwJV VuzEOMAGAUCCAN/VSV4XVMIXEARBgNVBACTCLIveMSkIFJvV2sxETAPBgNV SAdvBAUCENDOWG012kAUG2wSQUDVQ02EwJV VBAAMCERLBOWG012kUDAWEARBAUG11vdMSkIFJvV2sxETAPBgNV BAAMCERLBOWG012kUDAWEARBAUG11vdMSkIFJvV2sxETAPBgNV BAAMCERLBOWG01110kWWVVVVVVV20BAUMECIL <t< td=""><td>are & Croune</td><td>Expiration.</td><td>1 60 12 17.31.1.</td><td>110</td></t<>	are & Croune	Expiration.	1 60 12 17.31.1.	110
ocal Authentication L: Round Rock DAP Issuer: O: Dell EMC OU: Product Group Validation C: Dell CA incates emailAddress: texas_roemer@dell.com SL Certificates ST: Texas rusted CA Lists L: Round Rock ocal CAs Subject: O: Dell EMC nown CAs C: US meed Security IID 420C3sugAvEBAg1DApb/VA00C3gGS1b3DQEBCWUAMIGpMgswCQVDVQQEwJV UzEOMAwGAUDECBMFV04YIMAExABgNVBAcTC1/vaMSLF1vV2 szETAPBgNVBAcT CERLIGAGRUIDECBMFV04YIMMExABgNVBAcTC1/vaMSLF1vV2 szETAPBgNVBAcT CERLIGAGRUIDECBMFV04YIMMExABgNVBAcTC1/vaMSLF1vV2 szETAPBgNVBAcT CERLIGAGRUIDECBMFV04YIMMExABgNVBAcTC1/vaMSLF1vV2 szETAPBgNVBACT CERLIGAGRUIDECBMFV04YIMMExABgNVBACTC1/vaMSLF1vV2 szETAPBgNVBACT UzEOMAwGAUDECBMFV04YIMMExABgNVBACTC1/vaMSLF1vV2 szETAPBgNV PS Status Server MANCERLIGAGNSCUDVQQEWVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV	a s a aroups		ST:	US Texas
DAP Issuer: O: Dell EMC OU: Product Group Validation CN: Dell CA emailAddress: texas_roemer@dell.com CN: Dell CA emailAddress: texas_roemer@dell.com CN: Dell CA CN: US ST: Texas C: US ST: Texas C: US ST: Texas C: US CR: Dell EMC OU: Product Test O: Dell EMC OU: Product Test D: Dell EMC OU: Product Test D: Dell EMC OU: Product Test D: Dell EMC OU: Product Test O: Dell EMC OU: Product Test D: Dell EMC D: D'	Local Authentication		L:	Round Rock
OU: Product Group Validation icrates Dell CA icrates emailAddress: susted CA Lists C: US ocal CAs Subject: O: Dell EMC ocal CAs OU: Product Test nown CAs C: US idp Security Subject: O: Dell EMC SL OU: Product Test igh Security SL Esclin CERTIFICATE MIID42CCAsugAxIBAgIDApb/MA0CSqGSID5DDEBcwUAMIGqM0swCQYDVQQEewJV SL DSS Status Server MIID42CCAsugAxIBAgIDApb/MA0CSQGSID5DDEBcwUAMIGgM0swCQYDVQQEewJV Vu2EOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTCIJvdWStFIFJvY2sxETAPBgNVBAcT CERIbOwgRUDMSUMTDQUExhQremSkdMNIEdbyWigewCQYDVQQEewJV BSNUSBMTEORIbOwgRUDMWEWDVQULAx/CmBkdMIJ JaFNOKMCJaWCMWDQCEWVVQQEBWVV Dewlot AckerskdWsEarDAQ BgNVBAMTEORIbOwgRUDMWEWDVQULAx/CmBkdMIJ JaFNOKMCJaWCMVDQCEWVVQQEWVVQQEWVVQQEWVVQQEWVVQQEWVVQQEWVVQQEWXVVDQQEWVVQQEWXVVD	LDAP	Issuer:	0:	Dell EMC
c CAs & SSL incates CN: Dell CA emailAddress: texas_roemer@dell.com SL Certificates rusted CA Lists C: US ST: Texas L: Round Rock ocal CAs OU: Product Test nown CAs OU: Product Test igh Security CREDENCEMENTION SL CREDENCEMENTION IPS Status Server MIID4zCCAsugAnitAbglDaph/MAD02GSGSIb3DQEBCwUAMIGyMQswQQYDVQQEBwJV Dawnord RAMERAND CREDENGENTIAL Section MUZEOMAwGA1UECBMFVQV4YXMxE2ARBgNVBAcTC1JvdW5kIFJvV2 sxETAPBgNVBAcT CREDENGWQ0DXJDA1Bgkghk1G9w0BCQENTXRLeGFzxX3vZWILck8kZMxs IPS Status Server MIID4zeCCAsugAnitAbgkgDub/WMVVQULDAxCom9xdWN01LdWb1DvdW5kIFJvV2 sxETAPBgNV BAMCER1bGwgRU1DMRUMEWTDVQULDAxCom9xdWN01LodW5kIFJvV2 sxETAPBgNV BAMCER1bGwgRU1DMRUMEWTDVQULDAxCom9xdWN01LodW5kIFJvV2 sxETAPBgNV BAMCER1bGwgRU1DMRUMEWTDVQULDAxCom9xdWN01LodW5kIFJvV2 sxETAPBgNV BAMCER1bGwgRU1DMRUMEWTDVQULDAxCom9xdWN01LodW5kIFJvV2 sxETAPBgNV BAMCER1bGwgRU1DMRUMEWTDVQULDAxCom9xdWN01LodW5kIFJvV2 sxETAPBgNV BAMCER1bGwgRU1DMRUMEWTDVQULDAxCom9xdWN01LodW5kIFJvV2 sxETAPBgNV BAMCER1bGWgRU1DWC0CQUVXCQUBSARDQEBUN3LICASLCBXZMSEQUFV2 DVU2D020d1QV2QV2VV2 DV202QV2VV2 DV202QUENQQUENQQUENQUENQUENQUENQUENQUENQUENQU			OU:	Product Group Validation
incates emailAddress: texas_roemer@dell.com SL Certificates C: US rusted CA Lists L: Round Rock ocal CAs OU Product Test nown CAs OU: Product Test igh Security SL SL SL SL MID42CSAugAria MID42CCAsugAwIBAgIDApb/MA0CSgGSIb3DQEBCwUAMIGgMQswCQYDVQQGEwJV UzEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTC1JvdM5kIFJvY2sxETAPBgNVBAcT CERLb@wgRUIDMSbeHwUDVQQLExhQcm3xdMVD1EdgbGVwLF2hbG1kYXRb24xBDAO ByNBAMTB0R1bGwgQ0ZxJDAiBgkphkiG9w0SCQDFWRAleGFX3JvZW1LckBzZMxs IPS Status Server MAWCRAIDECAWFUGV4YXMxEzARBgNVBAcMC1JvdM5kIFJvY2sxETAPBgNVBAMUCIC Astropy KoczintwinkQa1UECAWFUGV4YXMxEzARBgNVBAcMC1JvdM5kIFJvY2sxETAPBgNV BAMCCRID6WgQUZIDMIBgkghkiG9w0SCQDEWFRAIeGFX3JvZW1LckBzZMxs LmNvbTaFFw0x0TAZMTgwNatkMTJaFW0y0TAyMTIXMEMMJJAIKGDGwCQYDVQQG BwNDaMTSDLBWQQCZCLDAvQcm3kdMN0IFRLsQwC1JvdMskIFJV2sxETAPBgNV BAMCCRID6WgRUIDMRUMEWDVCUQLAkQcm3kdMN0IFRLsQwC1JvdMskImMTJaMIGMQswCQ2DVQQG BwNDutZeMAwGA1UECAWFUGV4YXMxEzARBgNVBAMCLJvdWsLakMMJaMIGAUCENkcQC2DVRQGGBWDGQBDMM0mC1AkbeRkbc2QC2DVRQG BwNDaMTSDLBWQQCCCAQCGGGBAMMIDECAWFUGV4YXMxEzARBgNVBAMECLJv2baNc0elkc0lk cm7jdN1ckcxRldTUTHHjAEgkqhkiG9w0SCQEDWDALcSRLckkbc20yt2sumMatClkclkcm2QVDVQQG cm7jdN1ck	vice CAs & SSL		CN:	Dell CA
SL Certificates rusted CA Lists bcal CAs nown CAs nown CAs nown CAs CERTIFICATE MILD4xCCAsugAwIBAgIDApb/MAGCSqGSIb3DQEBCwUAMIGdMQswCQYDVQQGEwJV UzEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTC1JvdM5kIFJvY2xxETAPBgNVBAcT CERLIBWgRUIDMSBwHwUTVQQLExhQcm3kdMN0IEdgbGswCQYDVQQGEwJV UzEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTC1JvdM5kIFJvY2xxETAPBgNVBAcT CERLIBWgRUIDMSBwHwUTVQQLExhQcm3kdMN0IEdgbGswCQYDVQQGEwJV UzEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTC1JvdM5kIFJvY2xxETAPBgNVBAcT CERLIBWgRUIDMSBwHwUTVQQLExhQcm3kdMN0IEdgbGswCQYDVQQGEwJV UzEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTC1JvdM5kIFJvY2xxETAPBgNVBAcT CERLIBWgRUIDMSBwHwUTVQQLExhQcm3kdMN0IEdgbGswCQYDVQQG bwJVJzEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcMC1JvdM5kIFJvY2xxETAPBgNVB bACCERLIbWgRUIDMSBwHwUTVQQLExhQcm3kdMN0IERL3QxGTAXBgNVBAMEG1k cm7jdM1ckcxRldIUTIHjAEBgkqhkiG9w0SCQEMDRL3RlckBzZMxsLmNbvTCC AkSLAWLKCHLOWgRUIDMRUWEWDVQQLDAxQcm3kdNN0IFRL3QxGTAXBgNVBAMEG1k cm7jdM1ckcxRldIUTIHjAEBgkqhkiG9wDSCQENDBRL3RlckBzZMxsLmNbvTCC AkSLAWLKCSWCVDV0TDFALWADARBg1ghkgBhvCAQEEBAMMm6kzAzbwncelf&JoPH bg7wga41EzJj2ICT3kcenAG40DUH14BraujXHZX/AbXcut2Azbwncelf&JoPH bg7wga41EzJj2ICT3EBDADgeFNLCCAQcCggEBAMMm6kzKzDg0EfcwHuIdfUo gVUD1D0zdIGY4J7Bn2jJo/aVIpymSgWAkmBg1ShKyLK1pDHzhkqx/±zejjTaZi zdzz/HHR/Da346MBSGEMuviccgYDS6BgPINCCAQcEgBEAMMCBUALAzbwncelf&JoPH bg7wga41EzJj2ICT3EBDADgeFNLCCAQcCggBAMMfMcHzAzbwncelf&JoPH bg7wga41EzJj2ICT3EBDADgeFNLCCAQcCgBEAMMfAkKUG4Fg2gcT7WLSTIVAFjYVW fi33ZwJYVQg8NeffSBBSDCWAALHBAQBGMWHABARg1ghkgFAWUCAQEEBAMCB4AcWUVDROPBAQD AkgAMAMKCSwCQYDVROTBAIwADARBg1ghkgEAMMfakWUG4Fg2gcT7WLSTIVAFjYVW fi33ZwJYVQg8NeffSBBSUNCHAULDFKKINDFAC/jz4KA03Re3gjz1BkvEP/qt5NuV/ PQEK5auS0v0+RakID58tcTRASUCam1158tD7W2jMHVF4G2jHv95K2DpT05 suPyibsU1iQL9dH1K1S2105MN164D5xcTABACCam1158tDV2M5K2yVYZDJDVPTkameUYFknbsaygPETkCCAFFDVK2jILWPhDWH9f0NkVKyzDJ	rtificates		emailAddress:	texas_roemer@dell.com
rusted CA Lists ST: Texas bcal CAs Subject: O: Dell EMC nown CAs OU: Product Test igh Security SI: Ester@dell.com SL MID142CCAsugAwIBAgIDApb/MA0CSgGSIb3D0EBCwUAMIGgM0swC0YDVQ0GEwJV VizEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTC1JvdM5k1FJvY2sxETAPBgNVBAcTC CCR1bGwgRUIDMSbwHwUDVQ0LExhQcm9xdMVD1Edgb0SwK0YDVQ0GEwJV VizEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTC1JvdM5k1FJvY2sxETAPBgNVBAcTC CCR1bGwgRUIDMSbwHwUDVQ0LExhQcm9xdMVD1Edgb0SwK1FJvY2sxETAPBgNVBAcTC SL IPS Status Server MANDELGAWQA1UECBMFVGV4YXMxEzARBgNVBAcMC1JvdM5k1FJvY2sxETAPBgNV BANCER1bGwg0ZiZDAiBigkghkiG9w0BCQDDVQ0G BANCER1bGwg0ZiZDAiBigkghkiG9w0BCQDDVQ0G CwrJdXIAeFW0X0TAZMTgwNaMxHTJaFW0y0TAyMTIXmAMxHTJAMIGM0swCQDVQQG BANCER1bGwg0ZiIDNEGAwFVGV4YXMxEzARBgNVBAcMC1JvdW5k1FJvY2sxETAPBgNV BANCER1bGwg0ZiIDNEGAwFVGV4YXMxEzARBgNVBACMC1JvcBkcb20GcmWb01cH ShuDQJKSCIHwchAcBBDADggEFADCCAQcGgBEBAMMmotEKkeD1C6wHuIdfUo gVUD1D0zdIGY4J7Bn2jJo/aVIpymSqWAkmBg1ShKyLK1pDHzhkgx/+ze2j/Ta2i zdzz/HHR/Da346MBSGEMuvitcqYVD588gPANCD4X/EXAbsne0e16zJpWt GVGB1A0z6sN/zTXxVVIRZ9SRB2m1MN9IP3nKEn668spuMC0U/SICQG0HWSv4 GVGB1A0z6sN/zTXxVVIRZ9SRB2m1MM9IP3nKEn668spuMc0U/SICQG0HWSv4 GVGB1A0z6sN/zTXxVVIRZ9SRB2m1MMF1AAKUG4pF2gstTNLSTIVAF5JYVW <td>SSL Certificates</td> <td></td> <td>C:</td> <td>US</td>	SSL Certificates		C:	US
Lists Li Round Rock socal CAs Subject: O: Dell EMC nown CAs OU: Product Test igh Security Itractors in the construction of the constructin of the construction			ST:	Texas
subject: O: Del EMC nown CAs OU: Product Test igh Security igh Security igh Security SL MID42CMaugAMIBAgIDApb/NAOGCSqGSIb3DQEBCWDAMIGgMQswCQYDVQQGEwJV UZEDMAwGALUECOMFVQV4YUMzaABAgBNVBAcTCLJvdM5kIFJvY2sxETAPBgNVBAcT CERLbGwgRUIDMSEwHwYDVQQLExhQcm9kdWN0IEdyb3VwIFZhbG1kYXRpb24xEDA0 BgNVBAMTB0R1bCBMFVQV4YUMzaABgNVBAcTCLJvdM5kIFJvY2sxETAPBgNVBAcT CERLbGwgRUIDMSEwHwYDVQQLExhQcm9kdWN0IEdyb3VwIFZhbG1kYXRpb24xEDA0 BgNVBAMTB0R1bGwgQ05xJDAiBgkqhkiG9w0SCQEWFXRLeGFxX3Jv2W11ckBkZWxs INVbTAFtovXoT2ATGMNtMtXJJFW0yOTAyMTIXM1XM1JAMIJAMIDAMIGKWCQYDVQQG ByNVBACKLbCWSVGY4YXMxEaRBgNVBAcMCLJvdW5kIFJvY2sxETAPBgNV BAAMCERLbCwgRUIDMREwYDVQULDAxQemskdMN0IFRLsQuGTAWGXXBgNVBAMEG1k ByNU2ZOMAwGA1UECAWFVGV4YXMxEaRBgNVBAcMCLJvdW5kIFJvY2sxETAPBgNV BAAMCERLbCwgRUIDMREwYDVQULDAxQemskdMN0IFRLsQuGTAWGXXBgNVBAMEG1k ByNU2ZOMAwGA1UECAWFVGV4YXMxEaRBgNVBAcMCLJvdW5kIFJvY2sxETAPBgNV BAAMCSCHDwgRUIDMRCWEWDVQULDAxQemskdMN0IFRLsQUGTAWGXXBgNVBAMEG1k ByNU2ZOMAwGA1UECAWFVGV4YXMxEaRBgNVBACMCLJvdW5kIFJvY2sxETAPBgNV BAAMCSCHDwgRUIDMRCWEWDVQULDAxQemskdMN0IFRLsQUGTAWGAX/H2GYDGQUEYDQQG ByNU2ZOMAwGA1UECAWFVGV4YXMxEaRBgNVBACMCLJvdW5kIFJvDVSALMBVDCC ASIWDQYJKoZIhveNAQEBBQADggEPADCCAQoCggBBMMMmGEBkcbQI6CmvHuIdfUo gVUDLD0adGYATMac1jao/xVDNSSggNVKVDVDSRAMEG1kkW2/VDVGQGBNE	Trusted CA Lists		Li	Round Rock
nown CAs OU: Product rest nced Security CN: idracuserG1FWHQ2 igh Security IID42CCAsugAwIBAgIDApb/NA0GCSqG3Ib3DQEBCwDAHIGgMQswCQYDVQQGEwJV SL MID42CCAsugAwIBAgIDApb/NA0GCSqG3Ib3DQEBCwDAHIGgMQswCQYDVQQGEwJV UzzOMAwGA1UBCOBNYQVQYLMxEzABBgNVBAcTCL7udH5k1FJvY2sxETAPBgNVBAcT CERIbGwgRU1DMSEwHwYDVQQLExhQcm9kdWN01Edyb3Vw1F2hbG1kYXRpb24xEDA0 BgNVBAMTB0R1bGwg005xJDA1BgkqhkiG9w08CQEWFXRLeGFxX3JvZW11ckBkzMxs IIVb5TheFvoxOT2AUTgxN1ktWf1JaFW0yOTAyMT1xM1ktM1JAHIGMQ0ewCQYDVQQG BwJVUzEOMAwGA1UECAwFVGV4YXMxEzARBgNVBAcMC1JvdW5k1FJvY2sxETAPBgNV BAcMCER1bGwgRU1DMRDwEwVDVQQLDAxQem3kdMN01FR1c3Qx5TANBgNVBAMEG1k ByJVJZEOMAwGA1UECAwFVGV4YXMxEzARBgNVBAcMC1JvdW5k1FJvY2sxETAPBgNV BAcMCER1bGwgRU1DMRDwEwVDVQULDAxQem3kdMN01FR1c3Qx5TANBgNVBAMEG1k ByJVJZEOMAwGA1UECAwFVGV4YXMxEzARBgNVBAcMC1JvdW5k1FJvY2sxETAPBgNV BAcMCER1bGwgRU1DMRDwEwVDVQULDAxQem3kdMN01FR1c3Qx5TANBgNVBAMEG1k ByJVJZZCMkwR1BJ1DMZEWVDVQULDAxQem3kdMN01FR1c3Qx5TANBgNVBAMEG1k ByJVZZCMAwGA1UECAWFVGV4YXMxEzARBgNVBACMC1JvdW5kVEJDV2sxETAPBgNV ByJVZZCMAwGA1UECAWFVGV4YXMxEzARBgNVBACMC1JvdW5kVEJDV52syZVAXV2D3 ByJVZZCMAwGA1UECAWFVGV4YXMxEzARBgNVBACMC1JvdW5kVEJDV5c0Q05CMDA4HAWFXWVUCQCQCg0HPM5A4 ByJVZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ	Local CAs	Subject:	0:	Dell EMC
Interfects Interfects Inced Security emailAddress: tester@dell.com igh Security IIID42CLaugAwIBAgIDApb/MA0GCSqGSIb3DQEBCwUAMIGqMQswCQUDVQQGEwJV SL MID42CMaugAwIBAgIDApb/MA0GCSqGSIb3DQEBCwUAMIGqMQswCQUDVQQGEwJV IPS Status Server MID42CMaugAwIBAgIDApb/MA0GCSqGSIb3DQEBCwUAMIGqMQswCQUDVQQGEwJV ByWDBAMTB0R1bGcwg00ExJDAiBgkqhkiG9w0BCQEWFXRLeGFzX3Jv2W11ckBkzMxs IPS Status Server ByWDaActClJvdM5kIFJvY2sxETAPBgNVBActClJvdW5kIFJvY2sxETAPBgNV BAMCER1bCwg20IDMRDwEwVDVQ0LDAxQemskdMN0IFRLsQxGxTANBgNVBAMEG1k EwJVuzEOMAwGA1UECAwFVGV4YXMxEzARBgNVBAcMClJvdW5kIFJvY2sxETAPBgNV BAMCER1bCwg20IDMRDwEwVDVQ0LDAxQemskdMN0IFRLsQxGTANBgNVBAMEG1k EwJVuzEOMAwGA1UECAwFVGV4YXMxEzARBgNVBAcMClJvdW5kIFJvY2sxETAPBgNV BAMCER1bCwg20IDMRDwEwVDVQ0LDAxQemskdMN0IFRLsQxGTANBgNVBAMEG1k EwJVUzEOMAwGA1UECAwFVGV4YXMxEzARBgNVBAcMClJvdW5kIFJvY2sxETAPBgNV BAMCZ2/HER/Da346M5SERUvitcgYVDV589g9YKVvTDSRAFK2/Db3e1GebxUMvx/T22 EwJVUzEOMAwGA1UECAwFVGV4YXMxEzARBgNVBAcMCLJvdW5kIFJvY2sxETAPBgNV BAMCZ2/HER/Da346M5SERUvitcgYVD5889g9YKWvTDSRAFK2/Db3680g9W5K4/Db3680g00000000000000000000000000000000000	Known CAc		OU: CN:	idracuserC1EWHO2
igh Security igh Security SL JID 42CCA.sugAwIBAgIDApb/NA.0GCSqGSID3DQEBCwUAMIGGMQswCQYDVQQGEwJV UzzOMAwGALUECOMFVQVYLVKLZA.RABGNVBAcTCLIvudM5kIFJvY2sxETAPBgNVBAcT CERLbGwgRU1DNSEwHwYDVQQLExhQcm9kdWN0IEdyb3VwIFZhbG1kYXRpb24xEDA0 BgNVBAMTBORLbGwgQOExJDAiBgkqhkiG9w0SCQEWFKLeGFzX3JvZW11ckBkZMxs IPS Status Server BdNVDZENboxOT2ZMTQxN1kWtJTAJFN0yOTAyMTIxM1xM1JAIDAMIGXMQswCQYDVQQG BwJVUzEOMAwGA1UECAwFVGV4YXMxEzARBgNVBAcMC1JvdW5kIFJvY2sxETAPBgNV BAcMCERLbGwgRU1DMRDwEwVDVQQLDAxQemskdMN0IFFLc3QxSTANBgNVBAMEG1k BacMCERLbGwgRU1DMRDwEwVDVQQLDAxQemskdMN0IFFLc3QxSTANBgNVBAMEG1k BAMUZZOMAwGA1UECAwFVGV4YXMxEzARBgNVBACMC1JvdW5kIFJvY2sxETAPBgNV BAcMCERLbGwgRU1DMRDwEwVDVQQLDAxQemskdMN0IFFLc3QxSTANBgNVBAMEG1k BACMCERLbGwgRU1DMRDwEwVDVQVDDAxQemskdMN0IFFLc3QxSTANBgNVBAMEG1k BACMCERLbGwgRU1DMRDwEwVDVQVDDAxQemskdMN0IFFLc3QxSTANBgNVBAMEG1k BACMCERLbGwgRU1DMRDwEwVDVQVDDAxQemskdMN0IFFLc3QxSTANBgNVBAMEG1k BACMCERLbGwgRU1DMRDwEwVDVQVDDAxQemskdMN0IFFLc3QxSTANBgNVBAMEG1k BACMCERLbGwgRU1DMRDwEwVDVQVDDAxQemskdMN0IFFLc3QxSTANBgNVBAMEG1k BACMCERLbGwgRU1DMRDwEwVDVQVDAxAGPskdMmag1ShkyLK1pDHahkqx/zze2jTaZi CyUDDDaalGY4JTBn2jJO'AVDSgPYVVYD5SFRZYDD5sQDAMMGCBKc0QIECQUVQGBHAMCGNVQVQQBQHWVQQG BACKSTICCUNUSKExvVVmWMPMBPVDAFWV3JVEXDBACG2QDWVTCBQBAPW BAGWSGSENTCUUVYVTNTKULSKzvVVmMpMBPVDAFW 3JS	KHOWIE CAS		emailAddress:	tester@dell.com
BEGIN CERTIFICATE MILD4zCC4zugAwIBAgTDApb/MAOCSgGSIb3DQEBCwUAMIGgMQswCQYDVQQEBwJV UzEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTC1JvdW5kIFJvY2sxETAPBgNVBAcT SL IPS Status Server BAVWBAMTBORIbGwgOGZJDAiBgdqhkiG8w0SCQBWFXRleGFX3JvZW1LcHStZMxs LmNvbTAeFw0xOTAZMTgxNatKxHTJaFw0y07AyMTIxNatKxHTJAMIGMQswCQYDVQQE BwJVUzEOMAwGA1UECAwFVGV4YXMxEzARBgNVBAcMC1JvdWskIFJvY2sxETAPBgNV BAOMCSR1bGwgOUIDMRUWEWYDVQQLDAxQcm9xdMN0IFR1c3Qx6TAXBgNVBAMMEG1k cm7jdN1ckcxRldTUTIxHjAeBgvqhkiG9w0SCQEWD3Rlc3RlcBXZWxsLmNvbTCC AstwQ7WSCIThvcHAcBBQADggEPADCCAcQcGgEBAMMmotEKcb0I6cwHuIdfUo gVUD1D0zdIGY4J7Bn2jJo/aVIpymSqGwAkmBg1ShKyLK1pDHzhkgx/+ze2j/Ta2i zdzz/HHR/Da34GMSGEMuvitcgYVD58g9VKVv7D9RAFFx2/DbJeT1jRAXhB6D bg7wga41EzJj2ICT5kcwAkJRSGEMuvitcgYVD58g9VKVv7D9RAFFx2/DbJeT1jRAXhB6D bg7wga41EzJj2ICT5kcwAkJRSGEMuvitcgYVD58g9VKVv7D9RAFFx2/DbJeT1jRAXhB6D bg7wga41EzJj2ICT5kcwAkJRSGEMuvitcgYVD58g9VKVv7D9RAFFx2/DbJeT1jRAXhB6D bg7wga41EzJj2ICT5kcwAkJRSGEMuvitcgYVD58g9VKVv7D9RAFFx2/DbJeT1jRAXhB6D bg7wga41ESJj2ICT5kcwAkJRBSGEMuvitcgYVD58g9KVV7D9RAFFx2/DbJeT1jRAXhB6D bg7wga41ESJj2ICT5kcwAkJRBSGEMuvitcgYD58g9KVV7D9RAFFx2/DbJeT1jRAXhB6D bg7wga41ESJj2ICT5kcwAkJARBg1ghkgFbNvCAQEEBAMCU/JSICQG0HWSv4 QHJEJV6chbS1T1CPUUhSKzvVvTmMPHD9AFW/F1ggtz11fG1X6sjz1gBUGbLj2 uyjEtSU11QL9dH1K1S21050M1s6UXr2VDKX2mIJWPhU7Wj0NkVxy4zIaxBodK1V dxVCN7RAmeUYPknbsaySPL4zC28HD0H15g1zM2f4403Rs3gjzNBv5P/qt5NuV/ PQ6K53uSJ00+Rx41D58ktTR8LC2mN158LVxJ2WJDNeHSFT2jHW3F2gHT9bD7 suPyiJDNsCHHcD1yh+RX0bbxxL3U24yMKjQWy3RrrYQ8WYY2DJ	anced Security			
UZEOMAWGA1UÉCBMFVGV4YXMxEzARBgNVBAcTCIJvdW5kIFJÝY2sxETAPBgNVBAoT SL UZEOMAWGA1UÉCBMFVGV4YXMxEzARBgNVBAcTCIJvdW5kIFJÝY2sxETAPBgNVBAoT CERIbØwgRUIDNSbwHwITVCQLExhCem3x4MN0IEdyb3VwIFZhbG1kYXRbb24xEDAO BgNVBAMTBORLb6wgOEXJDAIBgkqhkiG3w0SCCDWFXRleGFX3JvZW1LckBkZWxs ImNvbTAeFv0x0TAZMTgxNaMxMTJaFv0y0TAyMTIxNaMxHJJAHIGNMQswCQDVQQG EwJVUzEOMAwGA1UECAwFVGV4YXMxEzARBgNVBAcMCIJvdW5kIFJvY2sxETAPBgNV BACCERIb6WgRUIDNEDWAVDVQULDAxQcm3x4MN0IFR1c3Qx6TAXBgNVBAMMcG1k cm7jdN1ckcxRldIUTIxHjAeBgkqhkiG3w0SCQEND3RLc3RlckBkZ0xsLmNvbTCC ASITMQYJKSZIhvcNhCBBDADggEPADCCAQcCggEBAMMMorEKkcD16cmVHIdEUv gVUD1D0zdIGY4J7Bn2jJo/sVIpymSqGwAkmBq1ShKyLK1pDHzhkqx/+ze2j/Ta2i zdzz/HHR/Da346MSGEMuvicgYVD585g97KVvT0BFAFKz/DbJeFIjgRxNhB6D bgFwga41E2Jj2ICTskchaGeDUY+18nzujXHZK/ABXcutAzbxne0e16zJopWt oqVGB1L0zGSN/rTXrVHIRZ9SBEZm1NN9IP3nKEn6685puMCIU/SICQG0HPW5v4 QHJEJV6ChbSiTCPUUNSKzvKvrWmBmHpVoAFW/SJGL8HH19IGDACHEZQOMC AwEAAMtMCSwCQVDVROTBAIwADARBg1ghkgEfymCAZEBAMCB4AvGwVDNQDBAQD AgXgMA0CSGgGSIb3DQEBCwAA4IBAQBGHMMfAwKUG2F9E3gt7WLSTUArFjYVW f33ZwJxYGyaBWg2TS0ESYLvhKUULDGKImDBh/cFfggtr11fg1X6js1gBUGCh2 uPyjEtSU11QL9dH1K1S2105oMNs6UXrZVDKX2mIJWPhU7WjONkVky+aIaxBodKIV dxVCN7RAmeUYPkNbsaySPLZC3FBDVK2jhLWFf3dy21Bw5F/qt5NuV/ PQQK53u8J00+Rx41bf8tCTR8LCzmN15B4bVpbNMeH5PTZjHIN94Sf2pTbb7 suPyiJDNSCMH+2DTw5m2	High Security	BEGIN CERTIFICATE MIID4zCCAsugAwIBAgIDApb/MA0GCSgGSIb	3DOEBCWUAMIGo	MOSWCOYDVOOGEwJV
SL CERIOWGROUTESSWWWTUOQULEXRQCmSRWWTUODEWRIGESSWWTICHCBGIEXRUDAC BGWUBAMTBOLL6GwgOUTEXJDAIBgkqhkiGSw0BCQDEFKRIeGFX3JJ2WILcK8kZMxs LmWubTAEFw0xOTA2MTgxNatkxHTJaFw0yOTAyMTIXMatkHTJAHIGMQswCQDUQQG EwJUUZEOMAwGAIUECAwFUGV4YXMxEzRBgNVBAcMCIJvdWSkIFJvY2xETAPBgNV BACCRLH6WgRUIDMRUWEWTDVQULDAxQcmSkdNN0IFRIe3Qx6TAXBgNVBAMMEGIk cmFjdN1ckcxRldIUTIXHJAEGgkqhkiGSw0BCQEND3RLeSRLeSRZWxsLmNvbTCC ASIMOQIKcZIhveNhCBBDADggEPADCCAQcGgBEAMMMotEKkcDIGCwHuIdfUo gVUD1D0zdIGY4J7Bn2jJo/aVIpymSqGwAkmBqIShKyLKIpDHzhkqx/+ze2j/TaZi zdzz/HHR/Da346MBSGEMuvicgYV56S99VKVvTDSRAFKzZ/DbJeTIjRxNhB6D bgFwga41L2Jj2ICT5kceAkGBSGEMuvicgYV58S99VKVvTDSRAFKzZ/DbJeTIjRxNhB6D bgFwga41L2Jj2ICT5kceAkG4DUYH1BnzujXHZ/AkZetAzbxne0e16zJopWt oqVGBLA0zGsN/zTXrVHIRZ9SBEZmINHJPSnKEn66S9DMCJU/SICQGDHWSv4 QHjEyV6ChbSiTICPUUhSKzvkVrmWpmBpVoAFW/SJGLSHH19IGDAC+IB220QmMC AwSAAMtHCSwOQYDVROTBAIwADARBg1ghkgBhvCAQEEBAMCB4AcVDVR0PBAQD AggMA0GCSqGSI58DQEBCwAA4IBAQBGHMWfAwKUG2FSB3t7WLSTUArFjYVW f33ZwJxYGya8W82TS0BSYLvhKUULDGKImDBh/eFfggtz1Ifg1X6sja[BBUGF] uPyjEtSU11QL9dH1K1S2IO5oMNs6UXrZVDKX2mIJWPhU7WjONkVky+aIaxBodKIV dxVCN7RAmeUYPkNbsaySPLGZC8FB0VK2j/z54KA03R63gjzNBv5P/qtSNvV/ PQ6K53uSJ00+Rx41D58ktTR8LCzmN15B4bVpbNMeH5PZjHvgjHw57 suPyiJDNsCHH20JyhFRX0bbxxL3U24yMKjQWy3RrrYQ8WXY2DJ	righ becamey	UzEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAc	TClJvdW5kIFJv	Y2sxETAPBgNVBAoT
IPS Status Server IPS Status Server Lm ^{NubTAEFw0xOTA2MTgxNatkxdTjFv0yOTAyMTIxNatkxdTjAMIGMQswCQYDVQQG EwJVUzEOMAwGA1UECAwFVGV4YXMxE2ARBgNVBACMC1JvdWskIFJvY2xETAPBgNV BACMCSR1b0wgNU1DMRUWEWVDVQULDAxQcm9kdNN0IFR1c3Qx6TAXBgNVBAMEG1k cmFjdN1ckcxRldIUTIxHjAeBgkqhkiG9w0SQCDWD3Rlc3Rlc8RlcBAVEMstCC AstwDQJKscIhvcNh2BBQADggEPADCCAQcGgBEAMMmbtRkcD1C6wHu1dtUo gVUD1D0zdIGY4J7Bn2jJo/aVIpymSqCwAkmBq1ShKyLK1pDHzhkqx/+ze2j/Ta2i zdzz/HHR/Da346MBSGEMuvitcgYVDs8g9VKVv7D9RfFk2/DbJef1jRxNhB6D bgFwga41L2Jj2ICT5kchAC94C9SB2DUY18nzujKXK3KAC42bxne0e16zJopWt oqVGB1A0zGsN/xTXvVHRZ9SRBZn1NHJPSnKEn6685uMCJU/SICQG0HWSv4 QHjEyV6ChbSiT1CPUUhStKzvkVrmMpHBV0AFW/SJGL8HH19IGDAC+IB220QmMC AxGAMA0CGSGGSIb3DQEBcwAA4IBAQBG4hWfAwKUG4PpSgt7WLSTVArFjYVW f33ZwJxYGya8Wg2TS0ES1vhAKUULDFGKimD5h,Ffggt11fg1X6js1gBUGKD12 uPyjEtSU11Q19dH1K1S2105oM1s6UXr2VDKX2mIJWPhU7Wj0NkVky+aIaxBodK1V dxVCN7RAmeUYPknbsaySPLaZC8HD0xA15724KA03Re3gjzNBv5P/qt5NuV/ PQ6K53uS100+Rx41D58xtTRaXCarN1584b7bDNeH5frggt11Eg2HbF7 suPyiJDNsCHHz01yh+RX0bbxxL3U24yMKjQWy3RrrYQ8WXY2DJ}	SSL	CERIDGwgRUIDMSEwHwYDVQQLExhQcm9kdWN BgNVBAMTBOR1bGwgQ0ExJDAiBgkghkiG9w0	01Edyb3VW1F2n BCQEWFXR1eGFz	bGIRIXRpb24xEDAO X3JvZW11ckBkZWxs
BWJUGZONAWARI DECAW VEVY INMEZARSYN BACHCIJOWNSI I 712 SKILAPSYN BACKER I bewgRUIDHKUEWYDVQUDAxQem SkiMNOIFRI 23 XETAKBSYNSAMECI k emFjdXNI ekexRldIUTIXHjAEBgkqhkiG9w0BCQEWD3Rle3RlekBkZWxsLmNvbTCC ASIWDQYJKoZINvelAQEBGADggEPADCCAQCggEBAMMmetBKebGI6cmvHuIdfUo gVUD1D0zdIGY4JTBarjJol X JUpwBGGwAkmBqIShKyLKIDHahkgx/+ze2j/TzZi zd2z/HHR/Da346MBSGEMuvitegYVbS8Pg9YKVVTD9RfAFk2/DkJeeT1jRnXhB6D bgTwpga41EzJj2ICTskQenAG40DUY+18nzujXHZK/ASKut4Zazbwne0e16zJopWt ogVCBLA0263N/zTXYUNTZ39SHSZmINM9IP3nKK668SpuNCU/SICGG0HBW5v4 QHjEyV6ChbSiT1CPUUhStKzvkVrmMpmHpVoAFW/8JGL8HH19IGDAC+1B2ZOQMMC AwEAAAMtMCswCQVDVROTBATwADARSq1ghkgBhvhCAQEBBMCB4AwCWTDVR0PBRAD AgXgMA0GCSqGSIb3DQEBcwUAA4IBAQBGHAMMfAwKUG6YpE8gt7WzLS7IVAF5jYVW f33ZwUXYGya8W8zTSOESY1vhKHUUDFGKimDBh/Ffggtr1Ifq1X6sjsIgBUGKD12 uPyjBt5U1iQL9dHLK1S21050MIsGUXZDVKX2mJJWPhUTWjONKVky+sIaxBodKIV dxVCNTRAmeUYPknbssy8PLkq2Z67BDVKAcj/z94KA038R3gjzNBvSPqt5NuV/ PQ6K5Su8J0X0++Rx4IDH58ktTR8kDcmN15B4bYpbNNH9fTWZjHIN4Sf2pTbb7 suPyiDNsCMHz0Iyh+RX0bbxxL3UZ4yMKjQbym3RrrYQ8WXY22DJ	FIPS Status Server	LmNvbTAeFw0xOTA2MTgxNzMxMTJaFw0yOTA	yMTIxNzMxMTJa	MIGXMQswCQYDVQQG
<pre>emFjdXN1ckexRldIUTIxHjAeBgkqhkiG9w0BCQEWD3Rlc3RlckBkZŴxsLmNvbTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQCggEBAMMmcEEKcbQI6CmvHuIdfUo gVUD1D0zdIGY4JTBarJjoJ v/ JVypW3GGwAkmBqI5KkpLKIDHahkgx/+zc2j/TzZi zd2z/HHR/Da346MBSGEMuvitcgYVbS8Pg9YKVVt7D9RfAFk2/DkJeeT1jRnXhB6D bgTwpga41EzJj2ICTskQcnAG40DUY+18nzujXH2K/A8kcu+2Azbxne0e1czJopWt oqV0B1A0zGsN/TXYVMIRZ9SPSEZmINM9IP9nKKn6685PuMCUV/SICQ6g0HBW5v4 QHjEyV6Ch5S1T1CPUUNStKzvkVrmMpmHpVoAFW/SJGL8HH19IGDAC-HB2Z0QmMC AwEAAattMCswCQVDVROTBAFwADARBq1ghkgBhvhCAQEBBMCB4AwCWYDVR0PBAQD AgXgMA0GCSqGSIb3DQEBcwUAA4IBAQBGHAMMfAwKUG6YpE8gt7WzLS7IVAF5jYVW f33ZuV3xYGya8W8zTS0ESY1vhKHUUDFGKimDBh/eFfggtr1Ifq1X6sjsIqBUGKD12 uPyjBstU1iQL9dHLK1S21050MHsGUXrZVDKX2mJJWPhUTWj0NkVky+sIaxBodKIV dxVCN7RAmeUYPknbssySPLkq2Z67BDVKAcj/z94KA0s3Re3gjzNBvSPqt5NuV/ PQ6K55u8J0X0++Rx41Dh58xTR4RNcmN15B4bYpbNNeH9fTW2jHIN94Sf2pTbb7 suPyiDNsCMHz0Iyh+RX0bbxxL3UZ4yMKjQbym3RrrYQ8WXYY2DJ _ coPD7ETC4Freement</pre>		EMJVUZEOMAWGAIUECAWFVGV41XMXEZARBGN BAoMCER1bGwgRU1DMRUwEwYDVOOLDAxOcm9	kdWN0IFR1c30x	GTAXEGNVEANMEG1k
ASIWDUJJKoZIAUCHAQEBBQADggEPADCAQCCggEBAMMMotERcbQI6CmuHuidTUo gVUD1D0zdIGY4JTBarjjov/AUgymGgGwAkmBqI5KKyLKIDPHahkqx/+ze2j/TzZi zd2z/HHR/Da346MBSGEMuvitcgYVbS8Pg9YKVVt7D9RfAFk2/DkJeeT1jRnXhB6D bgTwpga41EzJj2ICTskQcnAG40DUY+18nzujXH2K/A8kcu+2Azbxne0e16zJopWt ogVGB1A0263W/ZTXYUHTZ959R5ZmlNM9IP3nKK6685PuNCUV/SICG9DHBW5v4 QHjEyV6ChbS1T1CPUUhStKzvkVrmMpmHpVoAFW/8JGL8HH19IGDAC+1B2ZOQmMC AwEAAathMCswCQYDVROTBATwADARBq1ghkgBhvhCAQEBBAMCB4AwCwYDVR0PBAQD AgXgMA0GCSqGSIb3DQEBcwUAA4IBAQBGHAMMfAwKUG6YpE8gt7WzLS7IVAF5jYYW f33ZuWJxYGya8W8zTSOE8Y1vhKNUUPGKimDBh/eFfggtr1Ifq1X6sjsIgBUGkDi2 uPyjBt8U1iQL9dHLK1S21050MBsGUXZDKX2mJWPhUTWjONkVky+sIaxBodKIV dxVCN7RAmeUYPknbssy8PLkq2Z67BDvKAcj/z94KA033Re3gjzNBvSPqt5NuV/ PQ6K53u8J0X0++Rx41bh5ktTR8zNCzmN15B4bYpbNNeH9fTW2jHIN94Sf2pTbb7 suPyiDNsCH+z01yh+RX0bbxxL3UZ4yMKjQbym3RrrYQ8WXY22DJ		cmFjdXNlckcxRldIUTIxHjAcBgkqhkiG9w0	BCQEWD3R1c3R1	ekBkZWxsLmNvbTCC
zd2z/HHR/Da346MBSGEMuvitcgYVb58Pg9YKVVt7D9RfAFk2/DkJeeT1jRnXhB6D bgFwpga41EzJj2ICTsKQcnAG40DUY+18nzujXH2K/A8Xcu+2Azbxne0e16zJopWt ogVOBLA0263M/zTXYVHTR29SHSEZmlNM9IP3nKK668SpUMCUV/5ICQ6UHW5v4 QHjEyV6ChbSiT1CPUUhStKzvKVrmMpmHpVoAFW/8JGL8HH19IGDAC+IB2ZOQmMC AwEAAaMtMCswCQVDVROTBAFwADARBq1ghkQBhvMcAQEEBAMCB4AwCwYDVR0PBAQD AgXgMA0GCSqGSIb3DQEBcwUAA4IBAQBGHAMMfAwKUG6YpE8gt7WzLS7IVAF5jYVW f33ZwVxYGyaSM8zTSOESY1vhKNUUJPGKimDBh/eFfggtr1Ifq1X6sjsIgBUGkD12 uPyjBt5U1iQL9dH1K1S21050MNsGUX2ZDKX2mJWPhUTWjONkVky+sIaxBodKIV dxVCN7RAmeUYPknbssy8PLkq2Z62BDVKAcj/z94KA0s3Re3gjzNBvSPqt5NuV/ PQ6K5Su8J0X0++Rx41bh58tTR8zNCzmN15B4bYpbNNeH9fTW2jHIN94Sf2pTbb7 suPyiDNsCMHz0Iyh+RX0bbxxL3UZ4yMKjQbym3RrrYQ8WXYY2DJ		ASIWDQYJKoZIhvcNAQEBBQADggEPADCCAQo gVUD1D0zdIGY4J7Bn2iJo/aVIpvmSgGwAkm	CggEBAMMNmGtB BalShKvLKlpDH	KcbQI6CmvHuIdfUo zhkox/+ze2j/TaZi
bgFwpga4LEzJj2ICTskQcnAG4ODUY+1BnzujXH2K/ASkcu+2AzbxneOe1&zJopWt oqVGBLA0zGsN/TXTWIRZs9SBZmlNM9IP3nKEn6&SSPuMCUV/SICQ6g0HBMSv4 QHjEyV6Ch5ST1CPUULStKzvkVrmMpmHpVoAFW/SJCL8HH19IGDAC-IB2Z0QmMC AwEAAMtMCswCQVDVROTBATwADARBq1qhkgBhvhCAQEEBAMCB4AwCwYDVR0PBAQD AgXgMA0GCSqGSIb3DQEBcwUAA4IBAQBGHAMMfAwKUG6YpE8gt7WzLS7IVArFjYYW f33ZwJxYGya8M8zTS0ESY1vhKHUULPGKimDBh/eFfggtr1Ifq1X6sjsIgBUGkDi2 uPyjBt5U1iQL9dH1K1S21050M1sGUXr2DUX2mJUWPhUTWj0NkVky+sIaxBodKIV dxVCN7RAmeUYPknbssy8PLkq2Z67BDvKAcj/z94KA0s3Re3gjzNBv5P/qt5NuV/ PQ6K55uSJ0X0+tRx41Dh58tTR8zNCzmN15B4bYpbNNeH9fTW2jHIN94Sf2pTbb7 suPyiDNsCMHz01yh+RX0bbxxL3U24yMXjQbym3RrrYQ8WXYY2DJ		zd2z/HHR/Da346MBSGEMuvitcgYVb58Pg9Y	KVVt7D9RfAFk2	/DkJeeTljRnXhB6D
QHjEyV6ChbSiTiCPUUhStKzvkVrmMpmHpVoAFW/8JGL8HH19IGDAGC+IB2ZOQmMC AwEAAMtMCswCQYDVROTBATwADARBq1qhKgBhvhCAQEEBAMCB4AwGwYDVR0PBAQD AgXgMA0GCSqGSIb3DQEBcwUAA4IBAQBGHAMMfAwKUG6YpE8gt7WzLS7IVArFjYYW f33ZwJxYGyaSM8zTSOESY1vhKHUULPGKimDBh/Ffggtr1Ifq1X6sjsIgBUGkDi2 uPyjBt6U1iQL9dHLK1S21050kNisGUX2Z0DK2mJJWPhUTWjONkVky+sIaxBodKIV dxVCN7RAmeUYPknbssy8PLkqEZC87BDvKAcj/z94KA0s3Re3gjzNBv5Pqt5NuV/ PQ6K55uSJ0X0+tRx41Dh58ktTR8zNCzmN15B4bYgbNNeH9fTW2jHLN94Sf2pTbb7 suPyiDNsCM+z01yh+RX0bbxxL3UZ4yMKjQbym3RrrYQ8WXYY2DJ		bgFwpga41EzJi2ICTskQenAG40DUY+18nzu	jXHZK/ABXcu+2	Azbxne0e16zJopWt JU/5Ic06g0HPW5y4
AwEAAAWtMCswCQYDUROTBATwADARBq1qhkQBhuhCAQEEBAMCB4AwCwYDUROPBAQD AgXgMA0GCSqGSIb3DQEBCwUAA4IBAQBGHAMMfAwKUG6YpE3gt7WzLS7IVArFjYYW f33ZwJxYGya8M8zTS0E8Y1uhKHUULPGKimDBh/Ffggtr1IfqlX6sjsIgBUGkD12 uPyjBt5U1iQL9dHLK1SZ1056NMs6UXrZDUKX2mJWFhU7Wj0NkVky+sIaxBodKIV dxVCN7RAmeUYPknbsay8PLkqZ2C8rBDvKAcj/z94KA0s3Re3gjzNBv5P/qt5NuV/ PQ6K55uSJ0X0+tRx41Dh58xtTR8zNCzmN15B4bYgbNNeH5fTWZjHIN94Sf2pTbb7 suPyiJDNsCMHz01yh+RX0bbxxL3UZ4yMKjQbym3RrrYQ8WXYY2DJ		ONUCRIA07CON/ TYTUMID709SDB7m1NM9TD	3nKEn668SDuMC	oc) oregegemences
f33ZwUxYEyga8M8zTS0E8YivhKHUUDFGKimDbh/FFfggtrllfqlX&sjfIgBUGkD12 uPyjBt5U1iQL9dHLK1S21056MNs6UXrZDUX2mJWPhU7Wj0NkVky+aIaxBodKlV dxVCN7RAmeUYPknbsay8PLkqZC8rBDvKAcj/z94KA0s3Re3gjzNBv5P/qt5NuV/ PQ6K55u8J0XO++Rx41bh58xtR8aNCzmN15B4bYpbNNeH9fTW2jHLN94Sf2pTbb7 suPyiJDNsCMHz01yh+RX0bbxxL3U24yMKjQbym3RrrYQ8WXYY2DJ		oqVGBIA0zGsN/rTXrVMIRZs9SRBZmlNM9IP QHjEyV6ChbSiT1CPUUhStKzvkVrmWpmHpVo	3nKEn668SPuMC AFW/8JGL8HH19	IGDAdC+IB2ZOQmMC
uPyjBt5U1iQL9dHLK1S2105obMseGUX2DUX2mIJWPhU7WjONkUky+aIaxBodK1V dxVCN7RAmeUYPknbsay9PLkqZCSrBDvKAcj/z94KA0s3Re3gjzNBv5P/qt5NuV/ PQSK53u8J0XO++Rx4lbh58ktTR8zNCzmN1584bYpbNNeH5fTNZjHLN94Sf2pTbb7 suPyiJDNsCMHz01yh+RX6bbxxL3U24yMKjQbym3RrrYQ8WXYY2DJ		ogVGBIAOzGsN/rTXrVMIRZs9SRBZm1NM9IP QHjEyV6ChbSiTiCPUUhStKzvVVrmMpmHpVo. AwEAAMMCCswCQYDVR0TBAWADARBg1ghkg baYwMAOCSaCGSTb3DoPEAJHADARBg1ghkg	3nKEn668SPuMC AFW/8JGL8HH19 BhvhCAQEEBAMC WfbwKUG6VpF8g	IGDAdC+IB2ZOQmMC B4AwCwYDVR0PBAQD +7W7IS7IVAxF4XVW
DAVON (ARDECIFATOSEYSFIAQLOCIDIONAL)/274AAUSARSSEJSUBVS/455000/ PQRKS3u8JOO+RA4IDA58ktTRSENCzmN1584b7050bNeH5TM2jHLN9452pTbb7 suPyiJDNsCMHz01yh+RX0bbxxL3U24yMKjQbym3RrrYQ8WXYY2DJ		oqVGBİAOzGSN/TXYVMİRZSSSRBZm1NM9IP OHJEYV6Ch551T1CPUDh5KZvkVrMMpmHpVo AwEAAaMtMCswCQYDVROTBAIwADARBq1ghkg AqXgMaCCSqGSTB3DQEBCWLAA4TBAQBGHAM f33ZwJxYGya8W8zTS0E8YivhKHUULPGKimD	3nKEn668SPuMC AFW/8JGL8HH19 BhvhCAQEEBAMC WfAwKUG6YpE8g 9h/eFfggtr1If	IGDAdC+IB2ZOQmMC B4AwCwYDVR0PBAQD t7WzLS7IVArFjYYW q1X6sjsIqBUGkD12
suPyiJDNsCMHrOIyh+RXObbxxL3U24yMXjQbym3RrrYQ8WXYY2DJ		oqVGBIA02GsN/rTXrVMIRZs9SRBZm1NM9IP OHjEyV6Chb51T1CPUDh5KzvkVrMMpmHpVo AwEAAmtMCswCQYDVROTBAIwADARBg1ghkg AgXgMA0CCSqGSTb30QEBCwUAA4IBAQBGHAM f33ZwJxYGya8W8zTS0E8YivhKHUULPGKimD uPyjBt5U1iQL9dH1K1S2105oMNs6UXrZVDK dwCWIBmeIVUPbac102Dt27205722	3nKEn668SPuMC AFW/8JGL8HH19 BhvhCAQEEBAMC WfAwKUG6YpE8g 9h/eFfggtr1If X2mIJWPhU7Wj0	IGDAdC+IB2ZOQmMC B4AwCwYDVR0PBAQD t7WzLS7IVArFjYYW qlX6sjsIqBUGkDi2 NkVky+aIaxBodK1V gi>NBvky+aIaxBodK1V
		oqVGBİA02GsN/rTXrVMİRZs9SRBZm1NM9IP QHjEyV6Chb5iT1CPUUh5KzvkVrmMpmBpVa AwEAAmtMCswCQYDVROTBAIwADARBg1ghkg AqXgMA0CCSqGSID3DQEBCwUAA4IBAQBGHAM f33ZwJxYGya8W8zTS0E8YivhKHUULPGKimD uPyjBt5U1iQL9dH1K1SZ105oMNs6UXrZUDK dxVCNTRAmeUVPknbsay8PLkgEZC8rBbvKkc PQ8K53u5JUXO++Rx41Dh58ktTR8zNCzmN15	3nKEn668SPuMC AFW/8JGL8HH19 BhvhCAQEEBAMC WfAwKUG6YpE8g 9h/eFfggtr1If X2mIJMPhU7Wj0 j/z94KA0s3Re3 B4bYpbMNeH9fT	IGDAC+IB220QmMC B4AwCwYDVR0PBAQD t7WzLS7IVArFjYYW q1X6sjsIqBUGkD12 NkVky+aIaxBodK1V gjzNBv5P/qtSNuV/ M2JH1N945f2pTbb7
		oqVGBIA02GsN/rTXrVMIR2s9SRBZm1NM9IP GHJEyV6Ch56ITICPUDh5KzvkVrmMpmBpVo AwEAAaMtMCswCQYDVROTBAIwADARBq1ghkg AgXgMA0CCSqGSIb3DQEBCwUAA4IBAQBGHAM f33ZwJxYCys8UW2TSOE9YivhKHUULPCKimD uPyjBt5U1iQL9dH1K1S2105oMNs6UXrZVDK dxVCNTRAmeUYPhrbssy8EL02CsrBDvKAc PQ8K53u8J0XO++Rx41Dh58ktTR8zNCzmN15 suPyiJDNsCHHrOIyh+RX6bbxxL3U24yMXjQ END CERTIFICATE	3nKEn668SPuNC AFW/8JGL8HH19 Bh/bCADEBBANC WfAwKUG6YpE8g Sh/eFfggtr11f X2mIJWPhU7Wj0 J/294KADs3Re3 B4bYpbNNeH9fT bym3RrrYQ8WXY	IGDAdC+IBZ20QmMC B4AwCwYDVR0PBAQD t7WzLS7IVArFyYW qlX6sjsIqBUGkDi2 N&Vky+aIaxBadk1V gjzBW59/qt5NuV/ WZjH1N94Sf2pTbb7 Y2DJ

Figure 22 Download the signed CSR file from Gemalto to your local system

6. Upload the CSR certificate to the iDRAC. Run the following the command at the RACADM CLI:

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sslcertupload -t 6 -f C:\Users\tester\Downloads\signed_cert.crt
```

Certificate is successfully uploaded to the RAC.

3.3 Download the server CA file from Gemalto and upload to iDRAC

- 1. On the Gemalto GUI, click **Security Tab** \rightarrow **Local CA**.
- 2. Select the Server CA you are using and click **Download**.

The file is locally saved to your system.

Homo	Cocurity	Davica							
nome	Security	County a local C	4-						
anaged Obje	ects	Security » Local C		2215					
Keys		Certificate and	CA Configuratio	n					
Certificates	s	Local Certificat	e Authority List						
Certificate	Requests			2					
Authorizati	on Policies	CA Name		CA Inform	ation				
		Server CA		Common: I Issuer: Del	Dell CA				
ers & Grou	ps		1	Expires: Fe	BD 12 20	0:56:48 202	29 GM I		
Local Auth	entication	Edit Delete Downlo	ad Properties Sign	Request	show Si	gned Certs			
LDAP		24							
		Create Local Ce	ertificate Autho	ity					
vice CAs & rtificates	SSL	Certit	icate Authority Name	-					
SSL Certifi	cates							_	
Trusted CA	Lists	a	Common Name						
Local CAs	0.000		Organization Name	: L					
Kasura Cha	1	Orga	nizational Unit Name	:					
Known CAs	5		Locality Name						
vanced Sec	urity		ata ar Dravinas Nama					_	
High Secur	ity		ate of Province Marine		1				
551			Country Name	US					
EIDE Statu	- Conjor		Email Address						
FIPS Statu	s Server		Key Size	2048	Ŧ				
		2		Se	elf-signe	d Root CA			
				0	A Certif	ficate Durat	ion (days):		3650
		Cert	ificate Authority Type		avina -	n Lloor Cord	ificata Dur-E-	on (daus)	2650
				IVI	aximun	n oser cen	nicate Duratio	on (days):	0000
				Int	ermedi	ate CA Red	uest		

Figure 23 Download the server CA file from Gemalto

3.4 Upload the Server CA file to the iDRAC

Run the following command at the RACADM CLI:

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sslcertupload -t 7 -f C:\Users\texas_roemer\Downloads\Server_CA.crt

The certificate is successfully uploaded to the RAC.

3.5 Configure the Key Management Server settings on the iDRAC

Note—Ensure you already have a user created on the Key Management Server (KMS) you will be using for key exchange with the iDRAC. For the user name, make sure it matches the same value in the CSR certificate property you selected for the Gemalto KMIP **Username field in client certificate** Authentication Settings.

For example, in the signed CSR Certificate on iDRAC used in this experiment, the Common Name property is set to "idracuserG1FWHQ2". On the Gemalto server, in the KMIP Authentication Settings, the "Username field in client certificate" field is set to "Common Name". For creating a user name on Gemalto, you must create a user with the name "idracuserG1FWHQ2". This is the user name which iDRAC will be using for key exchange.

1. Run the following command at the RACADM CLI:

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn get idrac.kms
[Key=idrac.Embedded.1#KMS.1]
!!iDRACPassword=******* (Write-Only)
iDRACUserName=
KMIPPortNumber=5696
PrimarvServerAddress=
RedundantKMIPPortNumber=5696
RedundantServerAddress1=
RedundantServerAddress2=
RedundantServerAddress3=
RedundantServerAddress4=
RedundantServerAddress5=
RedundantServerAddress6=
RedundantServerAddress7=
RedundantServerAddress8=
Timeout=10
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.kms.PrimaryServerAddress
100.64.25.206
[Key=idrac.Embedded.1#KMS.1]
Object value modified successfully
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.kms.iDRACUserName
idracuserG1FWHQ2
[Key=idrac.Embedded.1#KMS.1]
Object value modified successfully
```

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set idrac.kms.iDRACPassword P@ssw0rd
[Key=idrac.Embedded.1#KMS.1]
Object value modified successfully
```

- After configuring all the KMS attributes, enable the SEKM on the iDRAC. When you execute the command, job ID is returned.
- 4. Query the job ID to ensure that the job status is displayed as "Completed".
- 5. If you see a job failure, check Lifecycle logs for more information about the failure:

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sekm enable

SEKM0212—The SEKM Enable operation is successfully started. To view the status of a job, run the "racadm jobqueue view -i JID_580315196579" command at the Command Line Interface (CLI).

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sekm getstatus SEKM Status = Enabled

The iDRAC SEKM setup operation is complete.

4 Enable SEKM on Storage Controllers

1. Get the FQDD of the controller you are going to enable SEKM. In this workflow, the controller FQDD is "RAID.Slot.3-1". Run the following RACADM command at the CLI:

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn storage get controllers -o -p name
RAID.Slot.3-1
Name = PERC H740P Adapter (PCI Slot 3)
```

2. Use this controller FQDD and run the command to enable SEKM pending value:

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn storage setencryptionmode:RAID.Slot.3-1 - mode SEKM

RAC1040—Successfully accepted the storage configuration operation. To apply the configuration operation, create a configuration job, and then restart the server. To create the required commit and reboot jobs, run the jobqueue command. For more information about the jobqueue command, enter the RACADM command "racadm help jobqueue".

- 3. Create a job ID to apply the pending changes.
- 4. Use the same controller FQDD to create a config job.
- 5. Also, for the job to run, a server reboot is required. Use the -r option which will automatically create a reboot job ID and reboot the server:

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn jobqueue create RAID.Slot.3-1 -s TIME_NOW -r pwrcycle
```

RAC1024-Successfully scheduled a job. Verify the job status using "racadm jobqueue view -i JID_xxxxx" command.

```
Commit JID = JID 580317754984
```

```
Reboot JID = RID_580317755572
```

The server is automatically restarted.

6. Run the config job in Automated Task Application.

Server is restarted again. After the POST or Collecting Inventory operation is completed, the job status is indicated as **Completed**.

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn jobqueue view -i JID_580317754984

----- JOB -----

```
[Job ID=JID_580317754984]
Job Name=Configure: RAID.Slot.3-1
Status=Completed
Start Time=[Now]
Expiration Time=[Not Applicable]
Message=[PR19: Job completed successfully.]
Percent Complete=[100]
```

- 7. Check the storage controller.

It is now in the SEKM encryption mode. It will also report the Key ID assigned to controller which iDRAC uses for key exchanges:

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn storage get controllers:RAID.Slot.3-1 -p encryptionmode, keyid RAID.Slot.3-1

EncryptionMode

= Secure Enterprise Key Manager

KeyID = 4163A493F1B50C8E727E9474627DC9D19193B0FEB0F40CAA03FD42DC81447BED

gemalto	SafeNet KeySecure Management Console								
Home Security	Device								
Managed Objects	Security * Keys * Key List								
Keys	Keys								
• Keys	Keys								
Query Keys		Query: [All] 🔻	Run Query						
Create Keys	Items per page: 10 V Submit	Page 1	of 113 G0						
 Import Keys 	Key Name	Owner	Object Type	Algorithm	State	Exportable	Deletable	Versioned Key	Certificate
 Key Options 	B6BDDC6AB94C2D5D696E30861ED1326DA0B5EEB2540A51AA991F8C6484EB1AF0	idracuserG1FWHQ2	Symmetric Key	AES-256	Active	ď	₽ 1		
 Schedule Key Rotation 	E28C646B9E7599B6BD64C1BF0486E07C9B7695A9E91562D69DB3776E186066D0	idracuser18R5QM2	Symmetric Key	AES-256	Active	ĭ. ∎	ĭ. ∎		
Certificates	D8F4B12FCF0760826056BDB9622F3F9940B5CEF12B3917C31F6992DAEBEF5C3F	idracuserG1FWHQ2	Symmetric Key	AES-256	Active	₩.	₽ ′		
Certificate Requests	7567369EE99C4DDA3C42420F6870675CAA3ACDC0E6E597A1A63D741A02F236E4	idracuser18R5QM2	Symmetric Key	AES-256	Active	Ø	Ø		
Authorization Delicion	2FFD332B89EA1EBE9014278FA0EAF07834674B96BB33D16DE998A934165CD413	idracuser18R5QM2	Symmetric Key	AES-256	Active	Z	Z		
 Autronization Policies 	FBEB715DCEE88D41825A67389E7559A39CC6D673B3E2D47CAD7593E96AA91C0F	idracuser18R5QM2	Symmetric Key	AES-256	Active	Ø	Ø		
Users & Groups	7FF5FDCFB838D7043D94CE1BE809A3D5EF012EA8A3BBFDAA9371AAEAFA227113	idracuserR640112	Symmetric Key	AES-256	Active	R	Z		
Local Authentication	BEAB2C0AC07DA915E9EA0D9C6C11318E72F2A40750F1AC061AC84F5702A01D31	idracuser18R5QM2	Symmetric Key	AES-256	Active	Ø	Ø		
IDAP	9788E9ACD6C2AE9A2A401616276B928D99AAE2476FEF01F4F9F0CE2BA267CDB2	idracuser18R5QM2	Symmetric Key	AES-256	Active	Z	Z		
	52342A942B7D5DA6F177C28C83351BF165741F2C7815A683CCCF81D4EE86022F	idracuser18R5QM2	Symmetric Key	AES-256	Active	Ø	Ø		
Device CAs & SSL Certificates	1 - 10 of 1130								
SSL Certificates	Delete Properties								
Trusted CA Lists	Delete All Keys On Current Page								
Local CAr									
E Known Cós	Greate Key Import Key Greate Query								
- KIOWI CAS									
Advanced Security									
High Security									

The SEKM solution is now completely set up. You can now create locked RAID volumes and perform key exchanges.

5 Configure SEKM by using a Server Configuration Profile (SCP)

In this workflow example, the Server Configuration Profile (SCP) feature is used to set up the complete SEKM solution for the iDRAC. For the Key Management Server, Gemalto KeySecure is used as the Key Management Server.

- 1. Using SCP, import the signed SSL certificate, Server CA, iDRAC KMS attributes.
- 2. Enable SEKM on the iDRAC.

For the signed SSL certificate, a CSR is already generated, signed on Gemalto, and then downloaded. The Server CA is also downloaded from Gemalto.

 In the SCP, copy the complete contents of the signed SSL certificate and Server CA as shown in the example SCP file below.

5.1 An SCP file example for configuring iDRAC SEKM configuration

This SCP file has been edited to show you only the SEKM configuration changes required to enable the SEKM on the iDRAC.

<SystemConfiguration> <Component FQDD="iDRAC.Embedded.1"> <Attribute Name="SEKM.1#IPAddressInCertificate">Disabled</Attribute> <Attribute Name="SEKM.1#SEKMStatus">Enabled</Attribute> <Attribute Name="SEKM.1#KeyAlgorithm">AES-256</Attribute> <Attribute Name="SEKM.1#Rekey">False</Attribute> <Attribute Name="KMS.1#PrimaryServerAddress">100.64.25.206</Attribute> <Attribute Name="KMS.1#KMIPPortNumber">5696</Attribute> <Attribute Name="KMS.1#RedundantServerAddress1"/> <Attribute Name="KMS.1#RedundantServerAddress2"/> <Attribute Name="KMS.1#RedundantServerAddress3"/> <Attribute Name="KMS.1#RedundantServerAddress4"/> <Attribute Name="KMS.1#RedundantServerAddress5"/> <Attribute Name="KMS.1#RedundantServerAddress6"/> <Attribute Name="KMS.1#RedundantServerAddress7"/> <Attribute Name="KMS.1#RedundantServerAddress8"/> <Attribute Name="KMS.1#Timeout">10</Attribute> <Attribute Name="KMS.1#iDRACUserName">idracuserG1FWHQ2</Attribute> <Attribute Name="KMS.1#iDRACPassword">P@ssw0rd</Attribute> <Attribute Name="KMS.1#RedundantKMIPPortNumber">5696</Attribute> <Attribute Name="SEKMCert.1#CommonName">idracuserG1FWH02</Attribute> <Attribute Name="SEKMCert.1#OrganizationName">Dell EMC</Attribute> <Attribute Name="SEKMCert.1#OrganizationUnit">Test</Attribute> <Attribute Name="SEKMCert.1#LocalityName">Round Rock</Attribute> <Attribute Name="SEKMCert.1#StateName">Texas</Attribute> <Attribute Name="SEKMCert.1#CountryCode">US</Attribute> <Attribute Name="SEKMCert.1#EmailAddress">tester@dell.com</Attribute>

<Attribute Name="SEKMCert.1#SubjectAltName"/>

<Attribute Name="SEKMCert.1#UserId"/>

<Attribute Name="SecurityCertificate.1#CertData">----BEGIN CERTIFICATE-----MIIEvzCCA6egAwIBAgIBADANBgkqhkiG9w0BAQsFADCBoDELMAkGA1UEBhMCVVMx DjAMBqNVBAqTBVR1eGFzMRMwEQYDVQQHEwpSb3VuZCBSb2NrMREwDwYDVQQKEwhE ZWxsIEVNQzEhMB8GA1UECxMYUHJvZHVjdCBHcm91cCBWYWxpZGF0aW9uMRAwDqYD VQQDEwdEZWxsIENBMSQwIqYJKoZIhvcNAQkBFhV0ZXhhc19yb2VtZXJAZGVsbC5j b20wHhcNMTkwMjE0MjA1NjQ4WhcNMjkwMjEyMjA1NjQ4WjCBoDELMAkGA1UEBhMC VVMxDjAMBqNVBAqTBVRleGFzMRMwEQYDVQQHEwpSb3VuZCBSb2NrMREwDwYDVQQK EwhEZWxsIEVNQzEhMB8GA1UECxMYUHJvZHVjdCBHcm91cCBWYWxpZGF0aW9uMRAw DqYDVQQDEwdEZWxsIENBMSQwIqYJKoZIhvcNAQkBFhV0ZXhhc19yb2VtZXJAZGVs bC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQChyihz1suLIIz1 K+XxI9nh59J+yCNXsMpKzneX0CSr1Aiay1Yyd1Uy21cifJbmuocP2wLQUEWTnR19 K0zbRKTMNty0fr9NhnwiRFVfUzUPiEGPwTyqR7w2WmHqu5jCnOodC9n+6w8lGnV9 3LzKLaJYdJ9TPGn63ffVrDeprhQ376EK6QjR1x1rTG7kUH2Hu9D1thwxQCykS2eQ 50icshUAsy5sCo5quisNLZZmJefREPx1x7ih/NtMGe5lEiZGyHIf91Ucf5L2vP6J lYKLZL7AqvJioHSSxD8nvP7naxKmIL3dlzohV8V+8DMc1UabDLhqUek/UX+jqSQ3 cuCY6LhLAgMBAAGjggEAMIH9MB0GA1UdDgQWBBQEk+OPdA03pnzCGUBnUK5a2Z/v hzCBzQYDVR0jBIHFMIHCgBQEk+OPdA03pnzCGUBnUK5a2Z/vh6GBpqSBozCBoDEL MAkGA1UEBhMCVVMxDjAMBqNVBAqTBVR1eGFzMRMwEQYDVQQHEwpSb3VuZCBSb2Nr MREwDwYDVQQKEwhEZWxsIEVNQzEhMB8GA1UECxMYUHJvZHVjdCBHcm91cCBWYWxp ZGF0aW9uMRAwDgYDVQQDEwdEZWxsIENBMSQwIgYJKoZIhvcNAQkBFhV0ZXhhc19y b2VtZXJAZGVsbC5jb22CAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOC AQEAgumRcKE3+dbYgNRNeYbvKH29B1NI01/PIP2V6he4/rDLYgyBLqNmtvRCUvu9 DnZczchZoGIdWm0j/1qW2108nptDM+R3olMEwNGdl+ZQNLUdMKdzKJbji8IaSxun B4Y21uLvykGm0Ts+X2/R84RAFHgDrRrentaM2WyJ7GCT470CDdUIg7NApxm8WoSA EQrt6RGJYQ1RZTFTW12f9+2K7CifHvNnth0zLjaK+vK4bTwhaPhkbM/00/qE1vaH zgwN+ZaVbl+amGabZdMvQbtDRqNoS+hQ7T91kbJjPJfza4frrxDzZyhxEN2H99pt zIto472w7hLB56tRjHfA6Vnh4w==

----END CERTIFICATE----

</Attribute>

<Attribute Name="SecurityCertificate.1#CertType">KMS_SERVER_CA</Attribute>
<Attribute Name="SecurityCertificate.2#CertData">-----BEGIN CERTIFICATE----MIID2zCCAsOgAwIBAgIDAmNQMA0GCSqGSIb3DQEBCwUAMIGgMQswCQYDVQQGEwJV
UzEOMAwGA1UECBMFVGV4YXMxEzARBgNVBAcTClJvdW5kIFJvY2sxETAPBgNVBAoT
CERlbGwgRU1DMSEwHwYDVQQLExhQcm9kdWN0IEdyb3VwIFZhbGlkYXRpb24xEDA0
BgNVBAMTB0RlbGwgQ0ExJDAiBgkqhkiG9w0BCQEWFXRleGFzX3JvZW1lckBkZWxs
LmNvbTAeFw0xOTA1MTYxODMyMzlaFw0yOTAyMTIxODMyMzlaMIGPMQswCQYDVQQG
EwJVUzEOMAwGA1UECAwFVGV4YXMxEzARBgNVBAcMClJvdW5kIFJvY2sxETAPBgNV
BAoMCERlbGwgRU1DMQ0wCwYDVQQLDARUZXN0MRkwFwYDVQQDDBBpZHJhY3VzZXJH
MUZXSFEyMR4wHAYJKoZIhvcNAQkBFg90ZXN0ZXJAZGVsbC5jb20wggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCl2WXSI3N90EXmbCxwylhkk2g/OYyvupwg
nL5uEF4TF8+BKjc3hw1PryzK+vPMPsv7J9fX4Ropy5bjsLXL7ZUdKTYMrhSlZ/13
v7qdZkBInHJfpHTiXbKQwvaMryPedToLNTWdG0Mr+ni05Ebzx/eG+x3LJQsbkxwX

f5NQGVZNtZnYzdTCkQnwmfseBRfJSzbxTm8HpoT9KGchVsYZDpPSz54ZIRlbqRmz
wJBlcyEPq63CjFp4RxfmZW0IPOGbmmcnGy3Rd4YFBmiC75pR3Wx+J1Xzr3inyRJ2
/XWpgm4XYfGSbyQ2in6Kzwf8CA3hTdsdx20FGJ0j3EUnj1PpOOq1AgMBAAGjLTAr
MAkGA1UdEwQCMAAwEQYJYIZIAYb4QgEBBAQDAgeAMAsGA1UdDwQEAwIF4DANBgkq
hkiG9w0BAQsFAAOCAQEAVJdEgKMfmhjrRulC/f7SZjy6pDhLSGM5KwJjQm/8fSjm
lfEyVTbD/eedWo6U6cah2uZrY0jD6SN17CAGMU/J6r4jkhZMrmB/cr3HXiCDQd/x
ReqmjVWOCJDb/tSt0kWAS3VFuRZzXfk083Kp6Zzak4Ue3mwJywThklOsoyXx1XEs
esNFxcsAGL9ABcuGUShpdKtYYWW098og6P1w1aiWRnaZQ6HP4To3tfmnQ9QKUeZ1
i3QsZ5Q6186dBZjaaoKSWp5y1fph2ciV//SoOtPhNHXYP5H/3AUQoEqNw71SX2H/
w9TJtElsc2htmbp6bHudrVI1B80lehk6IE4UxAEO/w==
----END CERTIFICATE-----</Attribute>
</Component>
</Component>
</Component>
</Component>

- 1. Run the RACADM set command to import this SCP file which is located on a HTTP share.
- 2. Ensure the SCP import job is marked as completed.
- Check config results to see what changes got applied to the iDRAC.
 The examples here use the default iDRAC user name and password (root/calvin).
- 4. Replace it with the appropriate iDRAC user name and password set up on the PowerEdge server.

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set -f 2019-5-17_132647_export.xml -t xml -1 http://100.65.84.72/http_share_vm

RAC977—Import configuration XML file operation initiated. Use the "racadm jobqueue view -i JID_581182121065" command to view the status of the operation.

C:>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn jobqueue view -i JID 581182121065 ----- JOB -----[Job ID=JID 581182121065] Job Name=Configure: Import Server Configuration Profile Status=Completed Start Time=[Not Applicable] Expiration Time=[Not Applicable] Message=[SYS053: Successfully imported and applied Server Configuration Profile.] Percent Complete=[100] _____ C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn lclog viewconfigresult -j JID 581182121065 SeqNumber = 5966 FODD = iDRAC.Embedded.1 Job Name = Import Configuration DisplayValue = SEKM.1#SEKMStatus

Name = SEKM.1#SEKMStatus

OldValue = Disabled

Configure SEKM by using a Server Configuration Profile (SCP)

NewValue	=	Enabled
Status	=	Success
ErrCode	=	0
SeqNumber	=	5963
FQDD	=	iDRAC.Embedded.1
Job Name	=	Import Configuration
DisplayValue	=	Certificate Data
Name	=	SecurityCertificate.1#CertData
OldValue	=	* * * * *
NewValue	=	* * * * *
Status	=	Success
ErrCode	=	0
DisplayValue	=	Certificate Type
Name	=	SecurityCertificate.1#CertType
OldValue	=	""
NewValue	=	KMS_SERVER_CA
Status	=	Success
ErrCode	=	0
DisplayValue	=	Certificate Data
Name	=	SecurityCertificate.2#CertData
OldValue	=	* * * * *
NewValue	=	* * * * *
Status	=	Success
beacas		5466655
ErrCode	=	0
ErrCode DisplayValue	=	0 Certificate Type
ErrCode DisplayValue Name	=	0 Certificate Type SecurityCertificate.2#CertType
ErrCode DisplayValue Name OldValue	= = =	0 Certificate Type SecurityCertificate.2#CertType
ErrCode DisplayValue Name OldValue NewValue	 	0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT
ErrCode DisplayValue Name OldValue NewValue Status	= = =	0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT Success
ErrCode DisplayValue Name OldValue NewValue Status ErrCode		0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT Success 0
ErrCode DisplayValue Name OldValue NewValue Status ErrCode SeqNumber		0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT Success 0 5961
ErrCode DisplayValue Name OldValue NewValue Status ErrCode SeqNumber FQDD		0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT Success 0 5961 iDRAC.Embedded.1
ErrCode DisplayValue Name OldValue NewValue Status ErrCode SeqNumber FQDD Job Name		0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT Success 0 5961 iDRAC.Embedded.1 Import Configuration
ErrCode DisplayValue Name OldValue NewValue Status ErrCode SeqNumber FQDD Job Name DisplayValue		0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT Success 0 5961 iDRAC.Embedded.1 Import Configuration Primary Server Address
ErrCode DisplayValue Name OldValue NewValue Status ErrCode SeqNumber FQDD Job Name DisplayValue Name		0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT Success 0 5961 iDRAC.Embedded.1 Import Configuration Primary Server Address KMS.1#PrimaryServerAddress
ErrCode DisplayValue Name OldValue NewValue Status ErrCode SeqNumber FQDD Job Name DisplayValue Name OldValue		0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT Success 0 5961 iDRAC.Embedded.1 Import Configuration Primary Server Address KMS.1#PrimaryServerAddress ""
ErrCode DisplayValue Name OldValue NewValue Status ErrCode SeqNumber FQDD Job Name DisplayValue Name OldValue NewValue		0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT Success 0 5961 iDRAC.Embedded.1 Import Configuration Primary Server Address KMS.1#PrimaryServerAddress "" 100.64.25.206
ErrCode DisplayValue Name OldValue NewValue Status ErrCode SeqNumber FQDD Job Name DisplayValue Name OldValue NewValue Status		0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT Success 0 5961 iDRAC.Embedded.1 Import Configuration Primary Server Address KMS.1#PrimaryServerAddress "" 100.64.25.206 Success
ErrCode DisplayValue Name OldValue NewValue Status ErrCode SeqNumber FQDD Job Name DisplayValue Name OldValue NewValue Status ErrCode		0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT Success 0 5961 iDRAC.Embedded.1 Import Configuration Primary Server Address KMS.1#PrimaryServerAddress "" 100.64.25.206 Success 0
ErrCode DisplayValue Name OldValue NewValue Status ErrCode SeqNumber FQDD Job Name DisplayValue Name OldValue NewValue Status ErrCode DisplayValue		0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT Success 0 5961 iDRAC.Embedded.1 Import Configuration Primary Server Address KMS.1#PrimaryServerAddress "" 100.64.25.206 Success 0 iDRAC User Name
ErrCode DisplayValue Name OldValue NewValue Status ErrCode SeqNumber FQDD Job Name DisplayValue Name OldValue Name Status ErrCode DisplayValue Status		0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT Success 0 5961 iDRAC.Embedded.1 Import Configuration Primary Server Address KMS.1#PrimaryServerAddress "" 100.64.25.206 Success 0 iDRAC User Name KMS.1#iDRACUserName
ErrCode DisplayValue Name OldValue NewValue Status ErrCode SeqNumber FQDD Job Name DisplayValue Name OldValue NewValue Status ErrCode DisplayValue Name OldValue Name OldValue		0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT Success 0 5961 iDRAC.Embedded.1 Import Configuration Primary Server Address KMS.1#PrimaryServerAddress "" 100.64.25.206 Success 0 iDRAC User Name KMS.1#iDRACUserName ""
ErrCode DisplayValue Name OldValue NewValue Status ErrCode SeqNumber FQDD Job Name DisplayValue Name OldValue Status ErrCode DisplayValue Status ErrCode DisplayValue Name OldValue Name OldValue Name		0 Certificate Type SecurityCertificate.2#CertType "" SEKM_SSL_CERT Success 0 5961 iDRAC.Embedded.1 Import Configuration Primary Server Address KMS.1#PrimaryServerAddress "" 100.64.25.206 Success 0 iDRAC User Name KMS.1#iDRACUserName "" idracuserG1FWHQ2

Configure SEKM by using a Server Configuration Profile (SCP)

ErrCode	=	0
DisplayValue	=	iDRAC Password
Name	=	KMS.1#iDRACPassword
OldValue	=	* * * * *
NewValue	=	* * * * *
Status	=	Success
ErrCode	=	0

5. Check to validate iDRAC SEKM is enabled, and the SSL certificate and Server CA are installed.

```
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sekm getstatus
SEKM Status = Enabled
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sslcertview -t 6
Serial Number
               : 026350
Subject Information:
Country Code (CC) : US
State (S)
                      : Texas
Locality (L)
                     : Round Rock
Organization (O)
                     : Dell EMC
Organizational Unit (OU) : Test
Common Name (CN) : idracuserG1FWHQ2
Issuer Information:
Country Code (CC)
                    : US
State (S)
                      : Texas
Locality (L)
                     : Round Rock
Organization (O)
                      : Dell EMC
Organizational Unit (OU) : Product Group Validation
                     : Dell CA
Common Name (CN)
Valid From
                     : May 16 18:32:39 2019 GMT
Valid To
                      : Feb 12 18:32:39 2029 GMT
C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn sslcertview -t 7
Serial Number
                     : 00
Subject Information:
Country Code (CC)
                    : US
State (S)
                      : Texas
Locality (L)
                     : Round Rock
Organization (O) : Dell EMC
Organizational Unit (OU) : Product Group Validation
Common Name (CN) : Dell CA
```

Issuer Information:					
Country Code (CC)	:	US			
State (S)	:	Texas			
Locality (L)	:	Round Rock			
Organization (O)	:	Dell EMC			
Organizational Unit (OU)		Product Group Validation			
Common Name (CN)		Dell CA			
Valid From	:	Feb 14 20:56:48 2019 GMT			
Valid To	:	Feb 12 20:56:48 2029 GMT			

- 6. After setting up iDRAC SEKM, use SCP to enable SEKM on the PERC along with creating a locked RAID volume. SCP enable you to stack multiple RAID operations without the need of running multiple jobs or commands.
- 7. Run one import command to stack these RAID operations and apply them.

5.2 Example of SCP file that has been modified to only show RAID changes which will enable SEKM on the PERC and create a RAID locked volume

```
<SystemConfiguration>
<Component FQDD="RAID.Slot.3-1">
    <Attribute Name="RAIDresetConfig">True</Attribute>
    <Attribute Name="EncryptionMode">Secure Enterprise Key Manager</Attribute>
    <Component FQDD="Disk.Virtual.0:RAID.Slot.3-1">
        <Attribute Name="RAIDaction">Create</Attribute>
        <Attribute Name="LockStatus">Locked</Attribute>
        <Attribute Name="BootVD">True</Attribute>
        <Attribute Name="RAIDinitOperation">None</Attribute>
        <Attribute Name="DiskCachePolicy">Disabled</Attribute>
        <Attribute Name="RAIDdefaultWritePolicy">WriteBack</Attribute>
        <Attribute Name="RAIDdefaultReadPolicy">ReadAhead</Attribute>
        <Attribute Name="Name">SCP VD</Attribute>
        <Attribute Name="Size">0</Attribute>
        <Attribute Name="StripeSize">512</Attribute>
        <Attribute Name="SpanDepth">1</Attribute>
        <Attribute Name="SpanLength">2</Attribute>
        <Attribute Name="RAIDTypes">RAID 1</Attribute>
        <Attribute Name="IncludedPhysicalDiskID">Disk.Bay.0:Enclosure.Internal.0-1:RAID.Slot.3-
1</Attribute>
        <Attribute Name="IncludedPhysicalDiskID">Disk.Bay.1:Enclosure.Internal.0-1:RAID.Slot.3-
1</Attribute>
    </Component>
</Component>
```

</SystemConfiguration>

The SCP file is located on HTTP share and imported by using the RACADM set command to import it.

- 8. After the SCP import job is marked as completed, verify configuration results to see what changes are applied.
- 9. Check storage configuration now to ensure that the PERC is in SEKM mode along with locked volume created.

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn set -f 2019-5-17_135217_export.xml -t xml -1 http://100.65.84.72/http_share_vm

RAC977—Import configuration XML file operation initiated. Use the "racadm jobqueue view -i JID_581203847849" command to view the status of the operation.

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn lclog viewconfigresult -j JID 581203847849

SeqNumber	= 6094
FQDD	= RAID.Slot.3-1
DisplayValue	= PERC H740P Adapter
Name	= PERC H740P Adapter
Status	= Success
DisplayValue	= PERC H740P Adapter
Name	= PERC H740P Adapter
Status	= Success
DisplayValue	= SCP VD
Name	= SCP VD
NewValue	= RAID 1
NewValue	= Physical Disk 0:1:0
NewValue	= Physical Disk 0:1:1
NewValue	= Virtual Disk Size in Bytes : 899527213056
NewValue	= Virtual Disk Stripe Size : 256 Kb
NewValue	= Physical Disks per Span : 2
NewValue	= VirtualDisk Lock status: Locked
Status	= Success
DisplayValue	= RAIDbootVD
Name	= RAIDbootVD
OldValue	= None

Configure SEKM by using a Server Configuration Profile (SCP)

NewValue	= Disk.Virtual.0:RA	AID.Slot.3-1
Status	= Success	
SeqNumber	= 6091	
FQDD	= RAID.Slot.3-1	
DisplayValue	= PERC H740P Adapte	er
Name	= PERC H740P Adapte	er
Status	= Success	
DisplayValue	= PERC H740P Adapte	er
Name	= PERC H740P Adapte	er
Status	= Success	
C:\>racadm -r encryptionmode	100.65.99.179 -u root ,keyid	t -p calvinnocertwarn storage get controllers -o -p
RAID.Slot.3-1		
EncryptionM	ode	= Secure Enterprise Key Manager
KeyID B13FCCB4D926F0	AEA37A718856F366E78F7	= 7D4AB6D76B793FAACB01D05993D22E
AHCI.Embedded.	2-1	
EncryptionM	ode	= None
KeyID		= null
AHCI.Slot.6-1		
EncryptionM	ode	= None
KeyID		= null
AHCI.Embedded.	1-1	
EncryptionM	ode	= None
KeyID		= null

C:\>racadm -r 100.65.99.179 -u root -p calvin --nocertwarn storage get vdisks -o Disk.Virtual.0:RAID.Slot.3-1

Status	= Ok
DeviceDescription	= Virtual Disk 0 on RAID Controller in Slot 3
Name	= SCP VD
RollupStatus	= Ok
State	= Online
OperationalState	= Not applicable
Layout	= Raid-1
Size	= 837.750 GB
SpanDepth	= 1
AvailableProtocols	= SAS
MediaType	= HDD
ReadPolicy	= Read Ahead
WritePolicy	= Write Back
StripeSize	= 256K
DiskCachePolicy	= Disabled

Configure SEKM by using a Server Configuration Profile (SCP)

BadBlocksFound	= NO	
Secured	= YES	
RemainingRedundancy	= 1	
EnhancedCache	= Not Applicable	
T10PIStatus	= Disabled	
	BlockSizeInBytes	= 512
Secured RemainingRedundancy EnhancedCache T10PIStatus	<pre>= YES = 1 = Not Applicable = Disabled BlockSizeInBytes</pre>	= 51

6 Troubleshoot issues while setting up SEKM on iDRAC

This section addresses some of the common issues encountered when using SEKM.

6.1 I installed the SEKM license, but I cannot enable the SEKM on iDRAC?

Make sure you update the iDRAC firmware after you install the SEKM license. This is required even if you had a SEKM supported iDRAC firmware version prior to installing the SEKM license.

6.2 I set up the KMS information and uploaded the SEKM SSL certificates but I am still unable to enable SEKM on iDRAC?

There are many possible reasons why iDRAC is unable to enable SEKM. Check the SEKM enable job Config Results for information about the job failure. Also, check the Lifecycle Controller logs for possible reasons for failure to enable SEKM. Also, check the following SEKM settings:

- Ensure that the:
 - o Primary and Redundant KMS IP addresses are correct
 - Primary and Secondary KMIP port numbers are correct.
 - o KMS CA certificate is the same as the one used to sign the KMS Server certificate.
 - CA used to sign the iDRAC CSR is in the Trusted CA list on the KMS server.
 - SSL Timeout value is large enough to allow iDRAC to be able to establish the SSL connection to the KMS.
 - User name of the iDRAC account on the KMS is entered in the correct field—It should match the value chosen in the "Username field in the Client Certificate" authentication property on the KMS.
- If the "Require Client Certificate to contain Source IP" option is enabled on the KMS then ensure that the iDRAC CSR contains the IP address in the **Common Name** field.

6.3 I am unable to switch PERC to SEKM mode?

- Make sure the PERC firmware has been upgraded to a version that supports SEKM.
- Make sure the SEKM status on iDRAC is Enabled. You can use the "*racadm sekm getstatus*" command to see the current SEKM status.

6.4 I set up SEKM on iDRAC and PERC and rebooted the host, but PERC shows the Encryption Mode as SEKM Failed?

The primary reason for this is that the PERC could not get the key from the iDRAC. In this case the iDRAC SEKM status will change to Failed. Therefore, refer to the troubleshooting tips mentioned earlier and make sure iDRAC can communicate to the KMS.

6.5 I checked the SEKM status on iDRAC and it shows "Unverified Changes Pending". What does that mean?

This means that changes were made to the SEKM settings on iDRAC, but these changes were never validated. Use the racadm command "*racadm sekm enable*" to enable SEKM to ensure that iDRAC can validate the changes made and set the SEKM status back to either Enabled or Failed.

6.6 I changed the KMIP authentication settings on the KMS and now iDRAC SEKM status has changed to "Failed"?

- If you changed the user name or password of the iDRAC account on the KMS then make sure you change the corresponding properties on the iDRAC as well and enable SEKM.
- If you changed the value of the "Username field in the Client Certificate" option on the KMS, then you
 need to generate a new CSR from iDRAC by setting the appropriate CSR property to the username, get
 the CSR signed by the KMS CA and then upload it to iDRAC. For example, if you change the value of the
 "Username field in the Client Certificate" option on the KMS from "Common Name" to "Organizational
 Unit" then generate a new CSR by setting the OU property to the iDRAC KMS username, sign it using the
 KMS CA and then upload it to iDRAC.
- If you enabled the "Require Client Certificate to contain Source IP" property on the KMS then generate a new CSR by selecting the "Include iDRAC IP Address in CSR", sign it using the KMS CA and then upload it to iDRAC.

6.7 I moved a SED from one SEKM enabled PERC to another SEKM enabled PERC on another server and now my drive shows up as Locked and Foreign. How do I unlock the drive?

Because each iDRAC is represented on the KMS by a separate user account, the keys created by one iDRAC are by default not accessible to another iDRAC. To enable the other iDRAC to get the key generated by the first iDRAC and provide it to PERC to unlock the migrated SED, create a Group to include the two iDRAC usernames and then give the key group permissions so that the iDRACs in the group can share the key. The steps to do this for the Gemalto KeySecure are described below.

- Log in to the KeySecure Management Console and click Users and Groups → Local Users and Groups.
- 2. To create a new group, click Add in the Local groups section.
- 3. Select the newly created group and click **Properties**.
- 4. In the User List section, click Add, and then add both the iDRAC user names to this group.
- 5. After the group is created, click **Security** \rightarrow **Keys**.
- 6. Identify the key created by the first iDRAC using the iDRAC unique user name.
- 7. Select the key and click **Properties**.
- 8. Click the Permissions tab, and then click Add under Group Permissions.
- 9. Enter the name of the newly created Group in step 2 above.
- 10. Remove and insert the drive to initiate a key exchange.

Now the second iDRAC should be able to get the key and provide it to PERC to successfully unlock the drive. The SED should appear as Foreign and Unlocked, and now you can import or clear the foreign configuration on the drive.

6.8 I moved a SEKM enabled PERC to another server and now my PERC encryption mode shows as SEKM Failed. How do I enable SEKM on the PERC?

Follow the steps outlined in <u>I moved a SED from one SEKM enabled PERC to another SEKM enabled PERC</u> on another server and now my drive shows up as Locked and Foreign. How do I unlock the drive? and restart the host.

6.9 What key size and algorithm is used to generate the key at the KMS?

In this release, iDRAC uses the AES-256 to generate keys at the KMS.

6.10 I had to replace my motherboard. How do I now enable SEKM on the new motherboard?

After a mother board replacement, the Easy Restore feature will restore the SEKM license and all SEKM attributes to the newly replaced iDRAC. But it will not restore the SEKM certificates as these are iDRAC specific.

- 1. Update the iDRAC firmware to a version that supports SEKM. This is irrespective of the version that came with the new iDRAC.
- 2. Generate a CSR on the new iDRAC, get it signed by the KMS CA, and then upload it to the new iDRAC.
- 3. Upload the KMS CA certificate to iDRAC.
- 4. Enable SEKM on the new iDRAC.
- 5. Ensure that the job is successfully completed.

6.11 I replaced a SEKM enabled PERC with another PERC and now I see that the new PERC encryption mode is None. Why is the new PERC encryption mode not SEKM?

On a Part Replacement, iDRAC will set the encryption mode of the new PERC to SEKM only if the firmware version on the new PERC is SEKM capable. Make sure that the replacement PERC has a firmware version that supports SEKM. If not, then perform a firmware update of the PERC to a version that supports SEKM and then check the PERC encryption mode.

6.12 I replaced a SEKM enabled PERC and now I see that iDRAC has generated a new key. Why was the key from the original PERC not used?

Each PERC needs its own key for SEKM – so when a PERC is replaced the new PERC will request iDRAC to create a new key and it will use the old key to unlock the drives and then rekey them with its own new key. Hence you will see iDRAC creating a new key after PERC part replacement.

6.13 I am unable to rollback iDRAC firmware – what could be the reason for rollback to be blocked?

Make sure that there are no storage devices that are in SEKM mode. iDRAC will block a rollback to a version that does not support SEKM if there are any storage devices that are in the SEKM mode. This is to prevent data lockout since after rollback iDRAC will not be able to provide keys to the storage devices to be unlocked.

6.14 I rebooted the host and key exchange failed because of a network outage and the PERC is in SEKM failed state. The network outage has been resolved – what do I need to do to put PERC back in SEKM mode?

Ideally, you do not have do anything because iDRAC will periodically try to connect to the KMS. After the network is started, iDRAC should be able to connect to the KMS, get the keys and provide them to PERC, and put it back in the SEKM mode. After five minutes, if the PERC is still in SEKM Failed state then reboot the host and check if key exchange is successful.

6.15 I would like to change the keys on a PERC—is that possible?

Yes, iDRAC allows a rekey operation, with which, you can rekey all storage devices supported for SEKM or a specific storage device. These rekey operations are supported by using either iDRAC GUI, RACADM, or Server Configuration Profile (SCP).

6.16 I did a system erase, but the PERC encryption mode continues to show as SEKM

This is an expected behavior—system erase does not change the encryption mode of the storage controller. To delete security on the PERC, use any of the supported iDRAC interfaces and switch the PERC encryption mode to **None**.

6.17 I cannot switch PERC to SEKM mode when it is in LKM mode This is an expected behavior—switching from LKM to SEKM mode is currently not supported.

6.18 I migrated an SED, locked by a PERC in LKM mode, to a PERC in SEKM mode. The drive is indicated as Locked and Foreign. Why was it not unlocked?

This is an expected behavior. Because the SED was locked by a PERC in LKM mode, it must be unlocked manually by providing the LKM passphrase by using any of the IDRAC interfaces. After unlocking, the foreign configuration on the drive can be imported, and then the drive will be locked by the SEKM key.

6.19 I cannot switch PERC to SEKM mode when it is in eHBA personality mode

This is an expected behavior. In eHBA personality mode, the SEKM encryption mode is not supported.

6.20 Where can I get more information about any type of failures when setting up SEKM or for key exchange failures, successful key exchanges or rekey operations?

In all these cases, refer to the iDRAC Lifecycle logs for detailed log entries. Alongside checking iDRAC Lifecycle logs for detailed log entries, check logs on the key management server for any key exchange activity.

Conclusion

Security has always been the highest challenge in data management and server solutions applications. Dell EMC PowerEdge servers, along with iDRAC, have been ensuring that your business-critical data is secure. The Secure Key Enterprise Management (SEKM)—in partnership with Gemalto—is now strengthening such security features for the PowerEdge customers. In this technical white paper, the procedure to enable the SEKM on iDRAC, PERC, and Storage Controller—by using both iDRAC and RACAM interfaces—is discussed. At the end of this technical white paper, tips and resolutions to some commonly faced issues are also discussed.

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.