



MyCodeSigner Thales Integration

Code Signing Solution Integration Guide



All information herein is either public information or is the property of and owned solely by Encryption Consulting and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any publicly accessible network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

Document Number: MyCodesigner-Integration-Guide-v1 Release Date: February 2020



Contents

1. Preface	5
1.1 Scope	5
1.2 Gemalto Rebranding	5
1.3 Support Contacts	5
2. THALES – ELAB SETUP	6
3. HSM CLIENT SETUP AND CONFIGURATION	7
3.1 Download and Install the Luna HSM 10.1 Client (i.e. SDK)	7
3.2 SSH into the eLab HSM appliance	8
3.3 Establish a connection between the Luna Client and the Luna appliance HSM pathe tool "lunacm"	artition using 12
3.4 Verify Network Trust Link Service (i.e. NTLS) – Port 1792	
4. Windows (Microsoft Authenticode) signing	
4.1 Configuration	
4.1.1 SignTool installation on Windows 2016 server	
3.2 Signing Windows executable on Windows server 2016	
3.3 Signing windows executable using MyCodeSigner application	
3.3.1 Login	
3.3.2 Create build server	20
3.3.3 Create Certificate	21
3.3.4 Create Policy	
3.3.5 Register Job approver	
3.3.6 Manage Workflow	
3.3.7 Register Job submitter	24
3.3.8 Manage Job submitter	
3.3.9 Create a signing job	25
3.3.10 Action on job (Approve, Reject and more info)	25
3.3.11 Verify windows executable after signing	
4. Signing windows executable using REST API with postman	
4.1 Login	
4.2 Verify authentication code to complete two factor authentications	
4.3 Create Certificate	33
4.4 Sign the Windows Application	
4.5 Verify the Windows signed application	
5. SafeNet Luna HSM integration with Oracle JDK 8	
5.1 Prerequisite	



	5.2	Installation and configuration of Java	39
6	Signin	g JAR files using MyCodesigner application	40
	6.1 Lo	gin	40
	6.2 Cr	eate build server	41
	6.3 Cr	eate Certificate	42
	6.4 Cr	eate Policy	43
	6.4 Re	gister Job approver	44
	6.5 Ma	nage Workflow	44
	6.6 Re	gister Job submitter	45
	6.7 Ma	nage Job submitter	45
	6.8 Cr	eate a signing job	46
	6.9 Ac	tion on job (Approve, Reject and more info)	47
	6.10 V	erify JAR file after signing	48
7	. Signin	g JAR files with REST API using postman	48
	7.1 Lo	gin	48
	7.2	Verify authentication code to complete two factor authentications	50
	7.3 Ge	nerate Key	53
	7.4 Sig	ning Jar application	55
	7.5 Ve	rify JAR file after signing	. 56



1. Preface

This document is intended to customers for MyCodesigner application integration with SafeNet Network HSM, and also covers the necessary information to install Luna Client, configure and integrate MyCodesigner application with SafeNet Network HSM.

1.1 Scope

This document outlines the steps to integrate MyCodesigner application with SafeNet HSM. SafeNet HSM is used to secure the keys for code signing.

1.2 Gemalto Rebranding

In early 2015, Gemalto completed its acquisition of SafeNet, Inc. As part of the process of rationalizing the product portfolios between the two organizations, the Luna name has been removed from the SafeNet HSM product line, with the SafeNet name being retained. As a result, the product names for SafeNet HSMs have changed as follows:

New product name
SafeNet Network HSM
SafeNet PCI-E HSM
SafeNet USB HSM
SafeNet HSM Client

NOTE: These branding changes apply to the documentation only. The SafeNet HSM software and utilities continue to use the old names.

1.3 Support Contacts

Ø

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information
Address	Gemalto
	4690 Millennium Drive



	Belcamp, Maryland 21017, USA		
Phone	US	1-800-545-6608	
	International	1-410-931-7520	
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.		
Encryption Consulting Support Contact Details	 Fazel Ahsan, Cyber Security Consultant, Encryption Consulting LLC, email: fazelahsan@encryptionconsulting.com, Tel: +1 469 815 4136, 130 N Preston Rd, Prosper TX 75078. Puneet Singh, President, Encryption Consulting LLC, email: puneetsingh@encryptionconsulting.com, Tel: +1 469 815 4136, Cell: +1 469 400 7592, 130 N Preston Rd, Prosper TX 75078. Prabal Kanti Sarkar, Software Engineer, Encryption Consulting LLC, email: Prabal@encryptionconsulting.com, Tel: +1 469 815 4136, 130 N Preston Rd, 		

2. THALES – ELAB SETUP

- The SafeNet eLab environment is provided for the use of Thales customers and partners so that you can become familiar with the operation and functionality of SafeNet Luna Network HSM, with respect to testing application connectivity, development and integration. Since the eLab is a shared environment, you will not be able to experience the complete HSM appliance administration and management interface and capabilities, as this is being managed by the Thales eLab team, hence you have limited access to the roles described below, and you won't be allowed to run certain commands like 'tamper/decommission the HSM'.
- Feel free to test the your assigned HSM partition as you like, however, please be aware that at any time there may be more than one customer evaluating the appliance via the eLab units.
- The eLab email address is not for technical support. If you have any questions regarding the operation or capabilities of the network HSM product please contact your local Thales Systems/Sales Engineer.
- Questions specific to eLab status or feedback on the eLab program can be sent to eLab.request@gemalto.com.
- The purpose of this document is to setup and configure an HSM client to establish a secure connection with the HSM server running in the eLab environment.



3. HSM CLIENT SETUP AND CONFIGURATION

3.1 Download and Install the Luna HSM 10.1 Client (i.e. SDK)

• Navigate to the folder where the Luna HSM 10.1 client was downloaded, extract and right click the LunaHSMClient.exe application and select Run as administrator.



When you see the following on your screen, the installation is complete.





3.2 SSH into the eLab HSM appliance

- Check status of the HSM
- Check the state of the HSM partition assigned to you.

6.9



Microsoft Visual C + 2009 Padistributable v64.0.0.20720.4149

73 programs installed

Currently installed programs Total size: 4.44 GB

Microcoft Corporation

0

- - × 🕞 💭 🖉 🕨 🕨 Computer 🔸 Local Disk (C:) 🔸 Program Files 🔸 SafeNet 🔸 LunaClient 🔸 👻 🍫 🛛 Search Lu Q <u>File Edit View Tools H</u>elp Organize 🕶 🖬 Open 🛛 Burn New folder (?) Name Date modified Size Туре ☆ Favorites CSP E Desktop 2/22/2019 7:19 AM File folder 📃 Recent Places 🌗 data 2/22/2019 7:19 AM File folder 鷆 Downloads G5Driver 2/22/2019 7:19 AM File folder JCProv 2/22/2019 7:19 AM File folder 📄 Libraries JSP 2/22/2019 7:19 AM File folder Documents KSP 2/22/2019 7:19 AM File folder J Music PedClient service 2/22/2019 7:19 AM File folder Pictures 2/22/2019 7:19 AM RemotePEDDriver File folder 😸 Videos 鷆 snmp 2/22/2019 7:19 AM File folder softtoken 2/22/2019 7:19 AM File folder 💻 Computer win32 2/22/2019 7:19 AM File folder 🏭 Local Disk (C:) © 008-010068-001_EULA_HSM7_SW_revA 6/8/2018 4:08 PM Chrome HTML Do... 147 KB 👝 New Volume (E:) 💷 ckdemo 8/24/2018 5:14 PM Application 361 KB 🚳 cklog201.dll 8/24/2018 5:14 PM Application extens... 627 KB No previe available 👊 Network Cmu 8/24/2018 5:14 PM Application 1.359 KB 🚳 cryptoki.dll 8/24/2018 5:14 PM Application extens... 3,601 KB 👔 crystoki 2/22/2019 7:20 AM Configuration sett... 2 KB Iunacm 8/24/2018 5:14 PM Application 3,261 KB Application 💷 lunadiag 8/24/2018 5:14 PM 3,348 KB 26 KB Iunareset 8/24/2018 5:14 PM Application multitoken 8/24/2018 5:14 PM 371 KB Application 12/16/2016 8:29 AM CNF File 7 KB openssl.cnf PedClient 8/24/2018 5:14 PM 3,397 KB Application 2,365 KB PedServer 8/24/2018 5:14 PM Application 🐑 pedServer 🗬 PLINK 2/22/2019 7:20 AM Configuration sett... 1 KB 6/8/2018 4:08 PM 441 KB Application
 File description: SSH, Teinet and Rlogin Client
 Application

 Company: Simon Tatham
 File description: SSH, Teinet and Rlogin Client
 PM
 Application

 Date modified:
 Date created: 6/8/2018 4:08 PM
 PM
 Application

 Size:
 Size:
 SIZE
 SIZE
 PSCP 6/8/2018 4:08 PM Application 448 KB 625 KB 668 KB 2.710 KB 3 384 KR PUTTY ₽ Application Date created: 6/8/2018 4:08 PM
- Browse to the Luna client install directory

• Launch 'Putty'. Enter the IP or Hostname of the Luna appliance, click 'open'

🕵 PuTTY Configuration	2 ×
Category:	
- Session	Basic options for your PuTTY session
Logging ⊡ Terminal Keyboard	Specify the destination you want to connect to Host Name (or IP address) Port
Bell Features Window	IP or Hostname of Luna appliance 22 Connection type:
 Appearance Behaviour Translation Selection Colours Connection Data Proxy Teinet Rlogin BSH Senal 	Load, save or delete a stored session Saved Sessions
	Default Settings
	Close window on exit: Always Never
About <u>H</u> elp	<u>Open</u> <u>C</u> ancel

• Accept the server key, select 'Yes'





- Login using the appliance credentials given in the email
- Use Appliance username and Appliance password for this step.
- Example shown below:



• Run the 'hsm show' command. Verify your assigned partition is on this HSM appliance



R lunahsm1.thaleselab.com - PuTTY			J
Luna Network HSM Command Line Shell v7	2.0-220. Copyright (c) 2018 SafeNet. All rights rese		2
rvea.			
[local_host] lunash:>hsm sh			
and the second second second			
Appliance Details:			
Software Version: 7.2	2.0-220		
HSM Details:			
HSM Label:	elablunahsml		
Serial #:	597025		
Firmware:	7.0.3		
HSM Model:	Luna K/		
Authentication Method:	Password		
HSM Admin login status:	Not Logged In		
HSM Admin login attempts left:	3 before HSM zeroization!		
RPV Initialized:	No		
Audit Role Initialized:	No		
Remote Login Initialized:	No		
Manually Zeroized:	No		
Secure Transport Mode:	No tamper(s)		
HSM Tamper State.	NO Camper(S)		
Partitions created on HSM:			
Partition: 1390056889670 Nat	a elahlunaheminari		
Partition: 1390056889671, Na	me: elablunahsmlpar2		-
Partition: 1390056889672, Nam	ne: elablunahsmlpar3		
Number of partitions allowed:	35		
Number of partitions created:	3		
FIPS 140-2 Operation:			
The HSM is NOT in FIPS 140-2 approve	ed operation mode.		
HSM Storage Information:			
Maximum HSM Storage Space (Bytes):	33554432	-	
Space In Use (Bytes):	2876094	-	
Free Space Left (Bytes):	30678338		
Environmental Information on HSM:			
Battery Woltage	2 002 17		
Battery Warning Threshold Voltage:	2.750 V		
System Temp:	29 deg. C		
System Temp Warning Threshold:	75 deg. C		
Command Regult + 0 (Success)			
[local host] lunash:>		*	-

- Enter the following command to view the information about your assigned partition 'partition show -partition ration name> '
- Example below of viewing an assigned partition with the name 'elabhsm1par1'



Punahsm1.thaleselab.com - PuTTY		
[local_host] lunash:>par sh		•
Protition North	- 1 - 1-1 1 1	
Partition Name: Partition SN:	1390056889670	
Partition Label:		
Partition SO is not initialized. Crypto Officer is not initialized		
Crypto User is not initialized.		
Legacy Domain Has Been Set:	no	
Partition Object Count:	0	
Partition Name:	elabhsm1par2	
Partition SN:	1390056889671	
Partition Label: Partition SO is not initialized.		
Crypto Officer is not initialized.		
Crypto User is not initialized. Legacy Domain Has Been Set:	no	
Partition Storage Information (Bytes):	Total=949050, Used=0, Free=949050	
Partition Object Count:	0	
Partition Name: Partition SN:	elabhsmlpar3 1390056889672	
Partition Label:		
Partition SO is not initialized.		
Crypto User is not initialized.		
Legacy Domain Has Been Set:	no	
Partition Storage Information (Bytes): Partition Object Count:	0	
Command Result : 0 (Success)		=
[local_host] lunash:>		+

3.3 Establish a connection between the Luna Client and the

Luna appliance HSM partition using the tool "lunacm"

a) Use the client name as suggested below for registering your Luna Client workstation/server.

(Warning: You'll be able to do this step successfully only after sending your public IP from which you'll be accessing the HSM to your sales engineer as mentioned in introduction of this eLab setup)

When registering your client name please use the same exact username provided in the email.

Example: elabhsm1par1usr

b) Establish a connection between the Luna Client and the Luna appliance

Open a command prompt, use 'run as administrator' option. cdto the LunaClient install directory. C:\Program Files\SafeNet\LunaClient>



Administrator: Command Prompt		x
Microsoft Windows [Version 6.1.7601] Copyright <c> 2009 Microsoft Corporation. All rights reserved.</c>		-
C:\Windows\system32>cd "\Program Files\SafeNet\LunaClient"		
C:\Program Files\SafeNet\LunaClient>dir Uolume in drive C has no label. Volume Serial Number is ØC26-4E8D		=
Directory of C:\Program Files\SafeNet\LunaClient		
02/22/2019 07:20 AM (DIR)		
02/22/2019 07:20 HH (DIR) 06/08/2018 03:08 PM 149,836 008-010068-001_EULA_HSM7_SW_F	evA.pdf	
02/22/2019 07:19 HM (D1R) CePt 08/24/2018 04:14 PM 369,544 ckdemo.exe		
08/24/2018 04:14 PM 641,416 cklog201.dll 08/24/2018 04:14 PM 1,391,496 Cmu.exe		
02/22/2019 07:19 AM <dir> config 08/24/2018 04:14 PM 3.686.792 cryptoki.dll</dir>		
02/22/2019 07:20 AM 1,899 crystoki.ini 02/22/2019 07:19 AM (DIR) CSP		
$02/22/2019$ 07:19 AM $\langle DIR \rangle$ data		
02/22/2019 07:19 HM <dir> GSDriver 02/22/2019 07:19 AM <dir> JCProv</dir></dir>		
02/22/2019 07:19 AM <dir> JSP 02/22/2019 07:19 AM <dir> KSP</dir></dir>		
08/24/2018 04:14 PM 3,339,144 lunacm.exe		
08/24/2018 04:14 PM 3,428,232 lunadiag.exe 08/24/2018 04:14 PM 25,992 lunareset.exe		
08/24/2018 04:14 PM 379,784 multitoken.exe		
08/24/2018 04:14 PM 3,478,408 PedClient.exe		
02/22/2019 07:19 AM <dir> PedClient_service 08/24/2018 04:14 PM 2 421 640 PedServer eve</dir>		
02/22/2019 07:20 AM 698 pedServer.ini		
06/08/2018 03:08 PM 451,072 PLINK.EXE		
06/08/2018 03:08 PM 640,000 PUTTY.EXE		
06/08/2018 03:08 PM 683,594 PUTTY.HLP		
08/24/2018 04:14 PM 3,465,096 rbs_processor2.dll		
02/22/2019 07:19 AM (DIR) RemotePEDDriver		
08/24/2018 04:14 PM 235,912 shim.dll		
02/22/2019 07:19 AM (DIR) snmp 02/22/2019 07:19 AM (DIR) softskop		
08/24/2018 04:14 PM 1,909,640 softtoken.dll		
08/24/2018 04:14 PM 3,518,856 UTL.exe		
22/22/2019 07:19 HM (DIR) win32 24 File(s) 33.742.372 butes		
15 Dir(s) 16,219,332,608 bytes free		
C:\Program Files\SafeNet\LunaClient>_		
		- T

• Run 'lunacm' command



Now, run the following command **Syntax:**

lunacm:>clientconfig deploy -server <IP or Hostname of Luna appliance> –user <appliance username provided in email> -password <Luna appliance PW provided in email> -client <Client name as suggested in step 3.a> -partition cpartition name provided in email>



lunacm:> clientconfig deploy -server lunahsm1.thaleselab.com -username elabhsm1par2usr -password J0inThal#\$ -c lient elabhsm1par2usr -partition elabhsm1par2 Error: unknown parameter 'username'.				
Register the client with the appliance. The following options are available:				
Options	Short	Description		
-server -client -partition -user -hsmPassword -regen -force -verbose Syntax: clientcont r <string>] [-hsmPat</string>	-n -c -par -pw -ur -rg -f -v fig deploy -s ssword <strin< td=""><td>Server hostname or IP address (mandatory) Client hostname or IP address (mandatory) Partition name to assign to the client (mandatory) Appliance admin role user's password Appliance admin role user's name. default is admin HSM SO role password, only needed if HSM SO login enforcement is enabled Regenerate new and replace existing client's certificate Force Action Show verbose logs erver <string> -client <string> -partition <string> [-password <string>] [-use g>] [-regen] [-force] [-verbose]</string></string></string></string></td></strin<>	Server hostname or IP address (mandatory) Client hostname or IP address (mandatory) Partition name to assign to the client (mandatory) Appliance admin role user's password Appliance admin role user's name. default is admin HSM SO role password, only needed if HSM SO login enforcement is enabled Regenerate new and replace existing client's certificate Force Action Show verbose logs erver <string> -client <string> -partition <string> [-password <string>] [-use g>] [-regen] [-force] [-verbose]</string></string></string></string>		
Command Result : 0x ⁴	4 (Invalid ar	guments)		
lunacm:> clientconf: elabhsm1par2usr -pa	ig deploy -se rtition elabh	rver lunahsm1.thaleselab.com -ur elabhsm1par2usr -password J0inThal#\$ -client sm1par2		
Please wait while we	e set up the	connection to the HSM. This may take several minutes		
Please enter applia	nce admin rol	e user's password:		

Example:

lunacm:>clientconfig deploy -server lunahsm1.thaleselab.com -ur elabhsm1par1usr1 password J0inThal3\$ -client elabhsm1par1usr1 -partition elabhsm1par1

🖦 Administrator: Command Prompt - Iunacm.e	xe	
lunacm:> clientconfig deploy -so 1 -password J0inThal3\$ -client o	erver lunahsm1.thaleselab.com -ur elab elabhsm1par1usr101 -partition elabhsm1p	nsm1par1usr ar1
Please wait while we set up the utes	connection to the HSM. This may take s	everal min
Command Result : No Error		
lunacm.exe (64-bit) v10.1.0-32.	Copyright (c) 2019 SafeNet. All rights	reserved.
Available HSMs:		
Slot Id -> Label -> Serial Number -> Model -> Firmware Version -> Configuration -> Cloning Mode Slot Description -> FM HW Status ->	0 elabhsm1par1 1390056889670 LunaSA 7.4.0 7.3.3 Luna User Partition With SO (PW) Key E Net Token Slot FM Ready	Export With
Current Slot Id: 0		
lunacm:>		~

Back to the putty session verify client is registered on the Luna appliance. run 'client list' command





Show the details of the client registered.

Run 'client show -client <client name or IP>

Example:

P lunahsm1.thale	selab.com - PuTTY		_	X
[local_host]	lunash:>client show -	-client elabhsm1par1usr1		•
ClientID: Hostname: Partitions:	elabhsmlparlusrl elabhsmlparlusrl "elabhsmlparl"			
Command Resu [local_host]	lt : 0 (Success) lunash:>[]			

Back to the Luna client cmd window [C:\Program Files\SafeNet\LunaClient>] to verify Luna appliance registration on the client side

Run 'vtl listservers' command

Run 'vtl verify' command



3.4 Verify Network Trust Link Service (i.e. NTLS) – Port 1792

The Luna Network HSM is accessed by the HSM Client (i.e. app server) and other network appliances via an encrypted IP protocol called NTLs listening on TCP port 1792. Network Trust Links (NTL) is secure, authenticated network connections between the HSM and Clients. NTLs use SSL with client authentication to protect all communications between HSM server and its Clients. The Communication is secured through the exchange of certificates between the HSM Client and the HSM server. After the certificates have been exchanged, the SafeNet HSM module registers the app server as a client and assigns a partition. The HSM client then registers the SafeNet HSM and partition as a server.

a. Launch "lunacm" (i.e. application) to initialize a connection with the HSM





b. Open a new CMD prompt, verify NTLS is established

Run >**netstat -an | find "1792"** (or Run >netstat –an) Example shown below:



Con. Comman	nd Prompt			
C:\Users	\jjesudos>netstat -an	find "1792"		
TCP	192.168.2.103:65166	72.138.111.35:1792	ESTABLISHED	=
C:\Users	∖jjesudos>netstat -an	find "22"		
TCP	0.0.0.0:52230	0.0.0.0:0	LISTENING	
TCP	192.168.2.103:57925	(2.138.111.35:22	ESTABLISHED	
C. Mears	\ijocudoc\potetat -ap			
0. (03ei 3	(jjesudos/netstat an			
Active C	onnections			
Proto	Local Address	Foreign Address	State	
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:2701	0.0.0.0:0	LISTENING	
ТСР	0.0.0.0:6000	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:16386	0.0.0.0:0	LISTENING	
ТСР	0.0.0.0:49152	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:49161	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:49167	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:49494	0.0.0.0:0	LISTENING	
	0.0.0.0.52230	0.0.0.0:0	LISTENING	
TCP		0.0.0.0:0	LISTENING	
TCP	127.0.0.1:1501	127 0 0 1 65529	ELISTENING	
TCP	127 0 0 1.6000	127 0 0 1.65520		
TCP	127 0 0 1.6000	127 0 0 1 65531	ESTABLISHED	
TCP	127 A A 1.7778	A A A A A	LISTENING	
TCP	127.0.0.1:7778	127.0.0.1.49190	ESTABLISHED	
TCP	127.0.0.1:16388	0.0.0.0:0	LISTENING	
TCP	127.0.0.1:49155	127.0.0.1:49156	ESTABLISHED	
TCP	127.0.0.1:49156	127.0.0.1:49155	ESTABLISHED	
TCP	127.0.0.1:49162	127.0.0.1:49163	ESTABLISHED	
TCP	127.0.0.1:49163	127.0.0.1:49162	ESTABLISHED	
TCP	127.0.0.1:49164	127.0.0.1:49165	ESTABLISHED	
TCP	127.0.0.1:49165	127.0.0.1:49164	ESTABLISHED	
TCP	127.0.0.1:49188	127.0.0.1:49189	ESTABLISHED	
ТСР	127.0.0.1:49189	127.0.0.1:49188	ESTABLISHED	
TCP	127.0.0.1:49190	127.0.0.1:7778	ESTABLISHED	
TCP	127.0.0.1:49191	127.0.0.1:49192	ESTABLISHED	
TCP	127.0.0.1:49192	127.0.0.1:49191	ESTABLISHED	
TCP	127.0.0.1:49234	127.0.0.1:49235	E214BF12HED	
TCP			E21HBL12HED	
TCP	127 0 0 1 49236	127.0.0.1.49231	ESTABLISHED	
TCP				
ТСР	127 0 0 1.49242	127 0 0 1.49241	ESTABLISHED	
TCP	127 0 0 1 54182	127 0 0 1 54183	ESTABLISHED	
TCP	127.0.0.1:54183	127.0.0.1:54182	ESTABLISHED	*



TCP 127.0.0.1:54183 127.0.0.1:54182 ESTABLISHED TCP 127.0.0.1:54557 127.0.0.1:54558 ESTABLISHED	^
TCP 127.0.0.1:54557 127.0.0.1:54558 ESTABLISHED	
TCP 127.0.0.1:54558 127.0.0.1:54557 ESTABLISHED	
TCP 127.0.0.1:65395 0.0.0.0:0 LISTENING	
TCP 127.0.0.1:65529 127.0.0.1:6000 ESTABLISHED	
TCP 127.0.0.1:65530 127.0.0.1:6000 ESTABLISHED	
TCP 127.0.0.1:65531 127.0.0.1:6000 ESTABLISHED	
TCP 192.168.2.103:139 0.0.0.0:0 LISTENING	
TCP 192.168.2.103:57874 40.100.162.2:443 ESTABLISHED	
TCP 192.168.2.103:57879 13.107.42.11:443 ESTABLISHED	
TCP 192.168.2.103:57889 52.162.166.27:443 ESTABLISHED	
TCP 192.168.2.103:57891 40.83.21.197:443 ESTABLISHED	
TCP 192.168.2.103:57901 91.241.42.175:443 ESTABLISHED	
TCP 192.168.2.103:57925 72.138.111.35:22 ESTABLISHED	
TCP 192.168.2.103:57926 40.100.162.194:443 ESTABLISHED	
TCP 192.168.2.103:65073 54.218.80.178:443 ESTABLISHED	
TCP 192.168.2.103:65129 52.96.51.98:443 ESTABLISHED	
TCP 192.168.2.103:65142 40.100.162.2:443 ESTABLISHED	
TCP 192.168.2.103:65158 35.166.89.106:443 TIME WAIT	
TCP 192.168.2.103:65163 40.100.162.18:443 ESTABLISHED	
TCP 192 168 2 103 65166 72 138 111 35 1792 ESTABLISHED	
TCP [::]:135 [::]:0 LISTENING	
TCP [::]:445 [::]:0 LISTENING	
UDD 192.168.2.103.1900 *:*	
	-

4. Windows (Microsoft Authenticode) signing

4.1 Configuration

4.1.1 SignTool installation on Windows 2016 server

Microsoft SignTool is a command line tool that signs, verifies, and timestamps files to simplify the code signing process. The tool is installed in the \bin folder of the Microsoft Windows Software Development Kit (SDK) installation path.

- SignTool is available as part of the Windows SDK, which you can download from https://go.microsoft.com/fwlink/?LinkID=698771
- Install the SignTool application and it will be located in the C:\Program Files (x86)\Windows Kits\10\bin\x64



• Once installation completes, add SignTool application path in the environment variable to access from everywhere.

3.2 Signing Windows executable on Windows server 2016

Backend configuration of the Signing Windows Executable

- Install **Nodejs** version minimum 10.0.1 (If you have already installed, please ignore this step)
- Install pm2 globally using bellow command (Run command prompt as administrator):
 pm2 install -g
- Create a Directory called **gemaltoBackendServer** in **C:\Users\gemaltoBackendServer**.
- Copy gemaltoBackendServer.zip in the C:\Users\gemaltoBackendServer Directory.
- Unzip gemaltoBackendServer.zip in same Directory.
- Go to C:\Users\ gemaltoBackendServer Directory and run server.js as a pm2.
 >pm2 start server.js

3.3 Signing windows executable using MyCodesigner application

3.3.1 Login

- Go to MyCodesigner virtual machine, open browser and type localhost in the URL. It will take into the login screen.
- Enter CO Admin credentials and do 2-factor-authentication.
- Screenshot of login and 2-factor authentication

Secure Authorship, Publication date and Content	Email
Building trust between Users	Eorgot your password? Sign In



	Composition Code is sent to your email. Your Authentication code is valid for only 3 minute.
 Secure Authorship, Publication date and Content Maintains software integrity 	Authentication code
Building trust between Users	Resend Authentication code in 0.7

3.3.2 Create build server

- After login into CO Admin, it will take you to the dashboard and click on Configuration option to create build server.
- On Build server configuration tab, click on Create new button to create new build server.
- Enter build server name, choose platform as Gemalto Windows from drop-down, choose HSM as Gemalto HSM from drop-down, enter the other required details and click submit button to create a new build server.
- To view build server configuration, click view button on the table to view particular build server.
- To update build server configuration, update the details except Build server name and Platform, fill the other changes want to update and click Update button to update the Build server details.

Wycodesi	gner		prac	makamp ro@outlook.com (
3 Deckered	Configuration			
	Build server Configuration	Virus Scan Configuration		
Import Certificate	Create New +			
Policy				
Register Approver	Build Servers			
Manage Workflows	Build server	Platforme	Submitted on	View
Register Job Submitter	Gemalto Windows Server-1	GEMALTO_WINDOWS	February 8, 2020 8:56 PM	View
Audit Report	Complite IAP convert 1	GEMALTO JAR	Eebruary 14, 2020 2:09 DM	View
🖉 Job Report	Genalo JAK server-1	GEMALIO_JAR	rebruary 14, 2020 2.09 PM	VIEW
) User Manual				

• Screenshots of the build server

	Configuration		
reate Certificate	Build server Configuration	Virus Scan Configuration	
nport Certificate	Build Server Name *	Build cerver name	
licy			
gister Approver	Choose Platform *	Gemalto Windows 🗸	
nage Workflows	Choose HSM *	Gemalto HSM V	
gister Job Submitter dit Report	IP address / Server name *	Server IP address/Server name.	
Report	Server Username *	Server username.	
er Manual	Password *	0	
	Source file Path *	C/documents/applications/Unsigned/	
	Signed File(s) Path *	C:/documents/applications/signed/	
@ MyCodeS	igner		
	.9		prabhakarmp18@outlook.co
shhoand	Gemalto Windows S	erver-1 Build server details	prabhakarmp18@outlook.cc
shboard eate Certificate	Gemalto Windows S Build Server Name	erver-1 Build server details Gemalto Windows Server-1	prabhakarmp18@outlook.cc
shboard eate Certificate port Certificate	Gemalto Windows S Build Server Name Platform	Gemalto Windows Server-1	prabhakarmp18@outlook.cc
shboard eate Certificate port Certificate licy	Gemalto Windows S Build Server Name Platform IP address / Server name *	erver-1 Build server details Gemalto Windows Server-1 GEMALTO_WINDOWS * 192.168.124.157	prabhakarmp18@outlook.cc
shboard eate Certificate port Certificate licy gister Approver	Gemalto Windows S Build Server Name Platform IP address / Server name * Server Username *	erver-1 Build server details Gemalto Windows Server-1 GEMALTO_WINDOWS	prabhakarmp18@outlook.cc
shboard eate Certificate port Certificate licy gister Approver mage Workflows gister Job Submitter	Gemalto Windows S Build Server Name Platform IP address / Server name * Server Username * Password *	erver-1 Build server details Gemalto Windows Server-1 GEMALTO_WINDOWS 192.168.124.157 Administrator	prabhakarmp18@outlook.cc
shboard eate Certificate port Certificate licy gister Approver anage Workflows gister Job Submitter dilt Report	Gemalto Windows S Build Server Name Platform IP address / Server name * Server Username * Password *	erver-1 Build server details Gemalto Windows Server-1 GEMALTO_WINDOWS 192.168.124.157 Administrator	prabhakarmp18@outlook.cc
shboard eate Certificate port Certificate lley gister Approver anage Workflows gister Job Submitter ddt Report b Report	Gemalto Windows S Build Server Name Platform IP address / Server name * Server Username * Password * Source file Path *	erver-1 Build server details Gemalto Windows Server-1 GEMALTO_WINDOWS 192.168.124.157 Administrator © C\Users\hp\Documents\Unsigned_Windows_files\	prabhakarmp18@outlook.cc
asbboard eate Certificate uport Certificate ulcy gister Approver anage Workflows gister Job Submitter uldt Report b Report er Manual	Gemalto Windows S Build Server Name Platform IP address / Server name * Server Username * Password * Source file Path * Signed File(s) Path *	erver-1 Build server details Gemalto Windows Server-1 GEMALTO_WINDOWS	prabhakarmp18@outlook.cc

3.3.3 Create Certificate

- Create certificate is a self-signed certificate to sign the windows artifact types like exe, dll, msi, etc.
- Click on Create certificate in Dashboard.
- Choose Platform as Gemalto windows and fill the all other details.
- Click Create button to create a certificate.
- Screenshots of the create certificate for windows

C MyCodeSi	gner		prabhakarmp18@outlook.com
Dashboard	Create Certificate This is required when a new key-pain	to be generated for code signing.	
🚍 Create Certificate			
import Certificate	Choose Platform *	Gemalto Windows V	
Policy	Choose build server *	Select build server	
O Register Approver			
Manage Workflows	Certificate Name *	eg: Certificate1	
😰 Register Job Submitter	Common Name (CN) *	eg: www.example.com	
Audit Report			
Job Report	Organization (O) *	eg: Oracle Pvt. Ltd.	
(?) User Manual	Organizational Unit (OU) *	Security	
	Country *	Eg: For USA, country code is US	
	State (S) *	Eg: Texas	
	Locality (L) *	Eg: Dallas	
	Container Name *	Container Name	

3.3.4 Create Policy

- Policies define the high level parameters like the certificate, platform and the signing method which can be associated with a code signing workflow.
- To create a policy, click on Create policy menu in dashboard.
- Enter the required details to create policy and click on Create policy button.
- Screenshots of the create certificate for windows

@MyCodeSig	gner			prabhakarmp18@outlook.com 🔍 🗸
Dashboard Create Certificate Import Certificate Policy	Create Policy Policies define the high le code signing workflow. Note: If you don't have al generate key pair for Linu Create Policy +	vel parameters like the certificate, platj ny keys or certificates, click on Create (x based OS.	form and the signing method wh Certificate. There you can create o	ich can be associated with a certificate for Windows or
🖉 Register Approver	Policy name	Platform	Certificate name	Build server name
Manage Workflows	Gemalto_wind-1	GEMALTO_WINDOWS	gemalto_test.spc	Gemalto Windows Server-1
8] Audit Report	Gemalto JAR Policy-1	GEMALTO_JAR	myfeb14key	Gemalto JAR server-1
کی Job Report ۲) User Manual				



	Create Policy		
Dashboard	Policies define the high le code signing workflow.	evel parameters like the certificate, platform and the	e signing method which can be associated with a
Create Certificate	Note: If you don't have a	ny keys or certificates, click on Create Certificate. Ti	here you can create certificate for Windows or
mport Certificate	generate key pair for Land	M DUSEU (CS.	
Policy	Policy Name *	ex: dll policy sign for development	
🖉 Register Approver	Signing Platform *	Gemalto Windows	×
Manage Workflows	Choose build server *	Select build server	v
😰 Register Job Submitter			
Audit Report	Certificate *	Select Certificate	Y
D Job Report	Signing Tool *	Select a signing tool for windows	×

3.3.5 Register Job approver

- Click on Register approver menu in the dashboard.
- Enter Approver email and approver name.
- Click on Submit button to register job approver.
- Screenshot of register job approver

MyCodeSi	gner		prabhakarmalipatil@gmail.com 🔬 🗸
Dashboard	Approver Registr	ation	
🚍 Create Certificate	Approver Email *	Approver Email	
👔 Import Certificate	Approver Name *	Approver Name	
P Create Policy		Submit	
🔗 Register Approver			
Manage Workflows			
Register Job Submitter			
(B) Audit Report			
 User Manual 			

3.3.6 Manage Workflow

- Click on Manage workflow menu in the dashboard.
- Choose policy from the drop-down, select no. of approver, workflow description and each level approver and their designation.
- Click Create button to create new workflow
- Screenshot of the manage workflow



MyCodeSign	er			prabhakarmalipatil@gmail.com 🕦
Dashboard	Manage Workflow You can configure approv maximum of 5 approval : If you have already config there are no pending Job	s al workflows for each artifact type. You can have teps per workflow. ured workflows, then you can modify only if requests.		
Import Certificate	Policy *	Select Policy	¥.	
Register Approver	No. of Approvers *	1	×	
Manage Workflows	Level-1 Approver *	Select level-1 Approver V Approver Design		
Audit Report	If you did not find the ap	rover in the above dropdown, then you can create new appro	ver. It will appear in the dropdown list.	
🖉 Job Report	+ Create New Appro	ver		
?) User Manual	Description *	Workflow description		
		Create	ii	

3.3.7 Register Job submitter

- Click on the Register Job submitter menu from the dashboard.
- Enter the job submitter email, name and select policy from the drop-down.
- Click on Submit button to register new Job submitter.
- Screenshot of Register job submitter

MyCodeSig	ner		prabhakarmalipatil@gmail.com 🔍 🗸
🔁 Dashboard	Job Submitte	er Registration	
Create Certificate	Email *	Job Submitter Email	
👔 Import Certificate	Name *	Job Submitter Name	
Create Policy	Policy *	Select Policy	
🖉 Register Approver		Street rong	
Manage Workflows		Submit	
🕎 Register Job Submitter			
Diagonal Audit Report			
Job Report			
? User Manual			

3.3.8 Manage Job submitter

- Click on the Manage Job submitter menu from the dashboard.
- Choose Job submitter from the drop-down and select policy from the drop-down.
- Click on Submit button to assign new policy to the existing job submitter.
- Screenshot of Register job submitter



	er				prabhakarmalipatil@gmail.com 🕥
🖥 Dashboard	Assign Policy to exi	sting Job Submitter			
🚍 Create Certificate	Choose Job Submitter *	Select Job Submitter		\sim	
import Certificate	Choose Policy *	Select Policy		~	
Create Policy					
🖉 Register Approver			Submit		
Manage Workflows					
🔮 Register Job Submitter					
3 Audit Report					
Job Report					
🤊 User Manual					

3.3.9 Create a signing job

- Login as a job submitter and click on Create signing job menu in the dashboard.
- Enter the job name, description, choose policy from the drop-down, and select the build server from the drop-down.
- Enter the file name to sign the relative path.
- Click on Create Job button to create a job.
- Screenshot of Create a signing job

	iner		p	rabalkantisarkarwork@outlook.com 🕡 🗸
🔁 Dashboard	Create Signing Job			
Create Signing Job	Job Name *	eg: windows job1		
(?) User Manual	Description *	Description.	li,	
	Choose Policy *	Select Policy	v	
	Choose build server *	Select build server OR switch to Upload file	v	
		Create Job		

3.3.10 Action on job (Approve, Reject and more info)

- Login as a job approver and click on Action button in the Signing requests waiting for your approval table of particular job.
- You can add notes to the particular job.



- To approve a job, click on Approve button in the approval workflow table, once the job is approved it will go for signing.
- To reject a job, click on Reject button in the approval workflow table.
- To request more information about a job, click on more info requested button in the approval workflow table.
- Screenshot of Action on job

	Details					
	Job ID	1008		Status	PENDING	
ashboard	Submitted by	Kanti Sar	kar	Virus Scan	Clear	
ser Manual	Submitted on	January 3	i0, 2020 2:09 PM	Malware Scan	Clear	
	Description					
	Windows executable artifact s	igning job-1				
	Add Note					
	Add notes here.					
	Add					
	Approval Workflow					
	Approver Name	Date	Action	More Info Requested	N	otes

3.3.11 Verify windows executable after signing

- Go to your windows vm station and go to signed folder/directory and see the digital signature in the main tab.
- Screenshot of verifying windows executable.



👘 testMSI Pro	operties ×
General Comp	atibility Security Custom Details Previous Versions
18	testMSI
Type of file:	Windows Installer Package (.msi)
Opens with:	Windows® installer Change
Location:	C:\Users\nCipher\Documents\backend\unsigned_wir
Size:	3.72 MB (3,907,584 bytes)
Size on disk:	3.72 MB (3,907,584 bytes)
Created:	Tuesday, January 21, 2020, 5:29:58 PM
Modified:	Monday, September 30, 2019, 6:50:03 PM
Accessed:	Tuesday, January 21, 2020, 5:29:58 PM
Attributes:	Read-only Hidden Advanced
	ОК Сансы Арріу
157961551	4943testMSI Properties ×
Custom	Details Previous Versions
General	Compatibility Digital Signatures Security
1	1579615514943testMSI
Type of file:	Windows Installer Package (.msi)
Opens with:	Windows® installer Change
Location:	C:\Users\nCipher\Desktop\signed
Size:	3.73 MB (3.915.776 bytes)
Size on disk:	3.73 MB (3.915 776 bytes)
Created:	Friday, January 17, 2020, 6:54:34 PM
Modified:	Tuesday, January 21, 2020, 7:35:20 PM
Accessed:	Friday, January 17, 2020, 6:54:34 PM
Attributes:	Read-only Hidden Advanced
	OK Cancel Apply



4. Signing windows executable using REST API with postman

4.1 Login

- Here the Customer Organization admin will enter the login credentials like user email address and password to login. On successful verification of login credentials, one token will be generated and assigned to the user. Concurrently, the user will also get one email containing authentication code. User will use the token and authentication code to complete 2 factor authentications for successful login.
- Enter login URL and Choose Method POST Screenshot

ntitled Req	uest	1			📮 Co		
POST	*	http://localhost:8000/login/log	in_user	Send	•	Save	٣
² arams	Authoria	ation Headers Body	Pre-request Script Tests Settings		C	okies	Code
Query Paran	ns			B T C C C C C C C C C C C C C C C C C C		1 2012	-
Кеу			Value	Description		Bulk	Edit
esponse							

• Choose the Body option. Once Body option is chosen, click the raw radio button and choose JSON from the drop down.



POST http:	//localhos	t:8000/lo	gin/log• + •	••					No Environment	*
Untitled R	equest									Q C
POST	•	http://	/localhost:8000/logi	n/login_us	er					Send 💌
Params	Author	ization	Headers (1)	Body	Pre-requ	est Script	Tests	Settings		c
none	forr	n-data	x-www-form-u	rlencoded	🖲 raw	binary	Gra	phQL BETA	Text 🔺	
1									Text	
									JavaScript	
									JSON	
				5					HTML	
									XML	

• Inside the body, enter the Customer organization login credentials as per shared screenshot format. Then Click Send Button

equest							Comment	
Ŧ	http://localhost:8000/le	gin/login_user				Send	Save	٣
Author	ization Headers (2)	Body Pre-r	equest Script	Tests Setting	S		Cookies	Code
I forr	n-data 🌘 x-www-forn	-urlencoded 🧕 raw	binary	GraphQL BETA	JSON 🔻		Bea	utify
user_emai user_pass	il":"prabal@encryptionco sword":"Test@12345"	nsulting.com",						
	Author of forr user_emai user_pass	equest thttp://localhost:8000//c Authorization Headers (2) form-data x-www-form user_email":"prabal@encryptionco user_password":"Test@12345"	equest http://localhost:8000/login/login_user Authorization Headers (2) Body Pre-r form-data x-www-form-urlencoded raw user_email": "prabal@encryptionconsulting.com", user_password": "Test@12345" 	equest http://localhost:8000/login/login_user Authorization Headers (2) Body Pre-request Script form-data X-www-form-urlencoded raw binary user_email":"prabal@encryptionconsulting.com", user_password":"Test@12345"	equest http://localhost:8000/login/login_user Authorization Headers (2) Body Pre-request Script Tests Setting form-data x-www-form-urlencoded raw binary GraphQL BETA user_email":"prabal@encryptionconsulting.com",	equest Ittp://localhost:8000/login/login_user Authorization Headers (2) Body • Pre-request Script Tests Settings • form-data x-www-form-urlencoded • raw • binary • GraphQL BETA JSON * user_email*:*prabal@encryptionconsulting.com*, user_password*:*Test@12345** • • •	equest <pre>equest <pre> ttp://localhost:8000/login/login_user Authorization Headers (2) Body Pre-request Script Tests Settings form-data x-www-form-urlencoded raw binary GraphQLBETA JSON user_enail":"prabal@encryptionconsulting.con", user_password":"Test@12345"</pre></pre>	equest Comment http://localhost:8000/login/login_user Authorization Headers (2) Body Pre-request Script Tests Settings form-data x-www-form-urlencoded raw binary GraphQL BETA JSON Beauser_email": "prabal@encryptionconsulting.con", user_password": "Test@12345"

• On Successful login, token is generated.



POST ht	tp://loca	lhost:800	0/login/log	• + ••						No Environ	ment	•	0	1
POST		* ht	tp://localho	st:8000/login	/login_user						Send	•	Save	٣
1 • { 2 3 4 }	"user_ "user_	email": passwor	'prabal@enci I":"Test@12	ryptionconsu 345"	lting.com",									
												1 2000		
ody Co	ookies	Heade	rs (12) T	est Results				Sta	tus: 200 OK	Time: 842ms	Size: 777 B	Save	Respon	se 🔹
ody Co Pretty	ookles Rav	Heade w P	rs (12) T review	est Results Visualize ^{BET}	A JSON		fl I	Sta	tus: 200 OK	Time: 842ms	Size: 777 B	Save	Respon	se 🔹
ody Co Pretty 1	ookies Rav	Heade w P	rs (12) T review	est Results Visualize ^{BET}	A JSON	1 💌	n.	Sta	tus: 200 OK	Time: 842ms	Size: 777 B	Save	Respon	se 🔹
ody Co Pretty 1 2	ookles Rav	Heade w P	rs (12) T review *: 200,	est Results Visualize ^{BET}	a json	1 •	IP	Sta	tus: 200 OK	Time: 842ms	Size: 777 B	Save	Respon	se 🔹
Pretty 1 2 3	ookles Rav	Heade w P "Status "Msg" :	rs (12) T review ": 200, "Please o	est Results Visualize ^{BET} Io Authenti	A JSON	I ▼	⇒	Sta	tus: 200 OK e the log:	Time: 842ms	Size: 777 B	Save	Respon	se v
Pretty 1 2 3 4	ookies Rav	Heade W P "Status "Msg" : "token" "ey UxN opz	rs(12) T review "Please c JJhbGci0iJ LLVVTRVIth H0ElGpc30	est Results Viscolize BET lo Authenti IIUzIINIISJ I2M2Y2QwNjj IIYKJ_avEy(A JSON cation Co nR5cCI6II tNDE5NS0; 7RhpeT021	i ♥ ode-ver kpXVCJ9 xMWVhLT ISSleJ5	rification 0.eyJleHAiO TLIZWMt0GQ3 if6tj1k"	Sta to complete jE2MTE5MjA Y2ZmYzNiZW	tus: 200 OK e the log 3MzUsImRh QSIn0sImli	Time: 842ms in process", IGEiOnsiYWX: IdCI6MTU4MD/	Size: 777 B sX3VzZXJfdW 44NDczNX0.	Save (5pcXV1)	Respon	se Q

4.2 Verify authentication code to complete two factor authentications

• Enter verify authentication code URL and Choose Method POST

POST htt	p://localhos	t:8000/login/log <mark>(</mark>	POST http://	ocalhost:8000/master/v	+	No Environmen	t v	0	4
Untitled I	Request						Ş (
POST	v	http://localhos	t:8000/master/v	erify_otp			Send 🔻	Save	v
Params	Author	ization Hea	ders Body	Pre-request Script	Tests	Settings		Cookies	Code
Query Pa	arams								
KEY				VALUE		DESCRIPTION	•	• Bul	lk Edit
Кеу				Value		Description			
Respons	e								
1									

• Choose Headers option and Enter token in key data. Use the token value (generated on successful login)



		00		145						
Intitled Re	equest							Ģ		
POST	•	http://localhos	t:8000/mas	ster/verify_ot	p			Send 🔻	Save	٣
Params	Author	ization Hea	ders (1)	Body	Pre-request Script	Tests Settings			Cookies	Code
▼ Heade	rs (1)									
KEY				VAL	UE		DESCRIPTION	••• Bulk Ed	it Presel	ts 💌
V toker	n			eyJ	hbGciOiJIUzI1NiIsInR5	cCl6lkpXVCJ9.eyJleHAiO				
Key				dW	5pcXVIX2lkljoiQUxML	VVTRVItN2M2Y2QwNjAt	Description			
				ND 5In	E5NS0xMWVhLTIIZWI 0sImihdCl6MTU4MDI	MtOGQ3Y2ZmYzNiZWQ M4NDczNX0.opzH0ElGp				

• Choose the Body option. Once Body option is chosen, click the raw radio button and choose JSON from the drop down.

POST http:	//localhos	t:8000/login/log●	POST http://lo	calhost:8000/mas	ter/v	- •••		No Environmer	nt	*	C
Untitled Re	equest									Coi	
POST	٣	http://localhost:	8000/master/ver	ify_otp					Send	•	Save
Params	Author	ization Heade	rs (1) Bod	y Pre-reque	est Script	Tests	Settings			Co	ookies
none	forr	m-data 🕚 x-ww	w-form-urlencoo	led 🔎 raw	binary	I Grap	hQL ^{BETA} Tex	(t 🔺			
1							Te	ext			
							Jav	vaScript			
							JSC	ON			
							Н	ГML			
							XN	ЛL			

• Sample of email received with Authentication Code



Authe	ntication code-verification to complete login process i	n My	Cod	e Sig	Ining	
M	MyCodeSigner <iwishbids@gmail.com> Thu 1/30/2020 11:52 AM Prabal ⊗</iwishbids@gmail.com>	3	5	(5)	\rightarrow	111
	Dear prabal@encryptionconsulting.com,					
	Your authentication code for two-factor authentication is 6727					
	Your authentication code is valid for 3 minutes					
	Best Regards,					
	MyCodeSigner Team					
	<u>MyCodeSigner</u>					
	Note : This is an auto generated email.					

• Inside the body, enter the Authentication Code as per shared screenshot format. Then Click Send Button.

POST http://localho	st:8000/login/log	• POST http://	/localhost:8000/n	naster/v• +			No Environ	ment	٣	o	\$
POST *	http://localho	st:8000/master/\	verify_otp					Send	-	Save	*
<pre>none tor 1 * { 2 "user_otp 3 }</pre>	rm-data 🛛 🛡 x-v	www-torm-urlend	coded 🧶 raw	v 🌐 binary	GraphQL *****	J2ON 🔺				Deau	uny
4											
3ody Cookles H	leaders (12) T	est Results			51	atus: 200 OK	Time: 86ms	Size: 720 B	Save I	Response	e 💌
3ody Cookies H Pretty Raw	leaders (12) T Preview	est Results Visualize ^{BETA}	json 🔻	S	St	atus: 200 OK	Time: 86ms	Size: 720 B	Save I	Response	e 🔹



4.3 Create Certificate

• Enter creation of certificate URL and Choose Method POST

POST	٣	localho	st:8000/master/pos	itman_gema	to_create_certificate	Send	۲
Params	Authoria	zation	Headers (10)	Body 🌒	Pre-request Script Tests Settings		
none	6 form	-data	• x-www-form-ur	lencoded	● raw ● binary ● GraphQL <mark>JSON</mark> ▼		

• Choose Headers option and Enter token in key data. Use the token value (generated on successful login)

POST	♥ localho	st:8000/master/pos	stman_gemal	to_create_certifi	cate		Send 🔻
Params	Authorization	Headers (10)	Body •	Pre-request	Script Tests Settings		
▼ Head	lers (2)						
KEY					VALUE	DESCRIPTION	••• Bulk Edit
🗸 tok	en				eyjhbGciOijlUzI1NilsInR5cCl6lkpXVCJ9.eyjleHAiOjE2MTI4NjYyOTQsIm		
Cor	ntent-Type				YTAINGEANSUX/WWhLTROOTAINWI3NDU5MGFkMGVIn0simIhdCl6M		
Key					eLKDXo	Description	
• Temp	oorary Headers (8)	0					

• Choose the Body option. Once Body option is chosen, click the raw radio button and choose JSON from the drop down.

POST ¥	localhost:8000/master/postman_gemalto_create_certificate	+
Params Authoriz	ation Headers Body Pre-request Script Tests Settings	
none form-	data 🔍 x-www-form-urlencoded 🖲 raw 🔘 binary 🔘 GraphQL Text 🔺	
1	Text JavaScript JSON HTML XML	

• Inside the body, enter the mandatory data to create certificate as per shared screenshot format. Then Click Send Button.



POST v localhost:8000/master/postman_gemalto_create_certificate	Send 👻 Save
Params Authorization Headers (10) Body • Pre-request Script Tests Settings	Cookies
● none ● form-data ● x-www-form-urlencoded ● raw ● binary ● GraphQL J5ON ▼	Be
<pre>1" { "province": "Texas", "locality": "Dallas", "organisation": "Encryptio_Consulting_LLC", "organisation_unit": "Security", "dnsccommon_name": "MovimyCodesigner.com", "certificate_name": "postnam/indowSign", "continer_name": "postnam/indowSign", "server_inde_port": "34980", "country_code": "US" " </pre>	

• On successful certificate creation, user will get the Status Response 200 like given in the screenshot.



4.4 Sign the Windows Application

• Enter signing of windows application URL and Choose Method POST



Untitled F	Request			Ę
POST	٣	localhost:8000/master/postman_gemalto_sign_window	ıs_file	Send 🔻
Params	Author	ization Headers (10) Body • Pre-request	Script Tests Settings	
KEY	ii di lis		VALUE	DESCRIPTION
Кеу			Value	Description
Rody Co	okios Ur	adare (12) Toct Posulte		Status: 200 OK Time: Size: 547 B Save

• Choose Headers option and Enter token in key data. Use the token value (generated on successful login)

arams	Authorization	Headers (10)	Body 🌒	Pre-request S	cript Tests Settings		
• Head	lers (2)						
KEY					VALUE	DESCRIPTION	••• Bulk Edi
🖌 tok	en				eylhbGciOiJIUz11NiisInR5cCl6lkpXVCJ9.eylleHAiOjE2MTI4NjVyOTQsIm RhdGciOnc/WWxcY2Vz7VifdW5ncYVV2VillaiOLIVMLVVCRVIANTUNDM5		
Cor	ntent-Type				YTATNGEANSOX/WWhLTKOOTATNWI3NDU5/MGFk/MGVIIn0simlhdCi6/M		
Key	í.				точитиіzмызино.сттый і zsvтыушанаграночодто оzzooven in eLKDXd	Description	

• Choose the Body option. Once Body option is chosen, click the raw radio button and choose JSON from the drop down.

POST v localhost:8000/master/postman_g	emalto_sign_windows_file	Send 🔻
Params Authorization Headers (1) Body	Pre-request Script Tests Settings	
none form-data x-www-form-urlencode	d 🖲 raw 🌑 binary 🔘 GraphQL JSON 🔺	
1	Text JavaScript JSON HTML XML	

• Check Digital Signature of Application. Right Click on the application and choose properties option. In the tab, there should not be any Digital Signature tab.



ieneral Secu	Ity Details Previous Versions	
	testDLL.dll	
Type of file:	Application extension (.dll)	
Opens with:	Unknown application Change	.
Location:	C:\Users\hp\Documents\Unsigned_Window	s_files
Size:	92.0 KB (94,208 bytes)	
Size on disk:	92.0 KB (94,208 bytes)	
Created:	Tuesday, February 18, 2020, 3:52:58 AM	
Modified:	Friday, January 17, 2020, 6:46:32 AM	
Accessed:	Tuesday, February 18, 2020, 3:53:12 AM	
Attributes:	Read-only Hidden Adva	nced

• Inside the body, enter the mandatory data to digitally sign the application as per shared screenshot format. Then Click Send Button.

POST	¥	localh	ost:8000/ma	ster/postman	gemalto_sig	n_windows_f	le								Send	•
Params	Author	ization n data	Header	(10) Bo	dy • Pre	e-request Scr	ipt Tests y O Grap	Setting	es N ¥	,						
1 • { 2 3 4 5 6 7 8	<pre>"node_se "server_ "cert_na "contain "source_ "signed_"</pre>	rver_po ip":"19 me":"po er_name path":" path":"	rt":"34980 2.168.124. stmanWindo ":"postman C:\\Users\ C:\\Users\	, IS7", container", hp\\Documen hp\\Documen	ts\\Unsigne ts\\Signed_	d_Windows_fil Windows_fil	iles\\testD es\\"	LL.d11",								

• On Successful signing, the response status will be 200.



POST	٣	localho	ost:8000/master/pc	istman_gemalt	to_sign_windows	file							Send	v
Params	Author	rization	Headers (10)	Body 🌒	Pre-request S	cript Tests	Settings							
• none 1 • { 2 3 4 5 6 7	forr "node_se "server_ "cert_na "contain "source_ "signed_	n·data rver_po ip":"19 me":"po er_name path":" path":"	<pre>x-www-form-u rt":"34980", 2.168.124.157", stmanWindowsSign ":"postman_conta C:\\Users\\hp\\D C:\\Users\\hp\\D</pre>	rlencoded .spc", iner", ocuments\\Un ocuments\\Si;	raw bin signed_Windows_f: gned_Windows_f:	ary GraphQ files\\testDLL lles\\"	L JSON	¥						
8 } ody Co	okies He	eaders (1	2) Test Results								Status: 200 Ol	(Time:	Size: 547 B	Sa
Pretty 1 2 3 4 5	Raw "Staf "Msg "sign }	Previ tus": 20 ": "Winc ned_file	ew Visualize 20, dows file is sign e_name": "1582019	JSON 💌 Ned successfu 1013963te	ully.", estDLL.dll"									

4.5 Verify the Windows signed application

• Verify whether application is signed. Right click on the properties of the application. One Digital Signature tab is appeared.



	1582202826264testDLL.dll	
Type of file:	Application extension (.dll)	
Location:	C:\Users\hp\Documents\Signed_Windows_files	
Size: Size on disk:	97.4 KB (99,776 bytes) 100 KB (102,400 bytes)	
Created: Modified:	Tuesday, February 18, 2020, 3:52:58 AM Today, February 20, 2020, 6:47:28 AM	
Accessed:	Tuesday, February 18, 2020, 3:53:12 AM	51
Attributes:	Read-only Hidden Advanced	

5. SafeNet Luna HSM integration with Oracle

JDK 8

Java code signing is used for signing Java applications for desktops, digitally signing .jar files and Netscape Object signing recognized by Java Runtime Environment (JRE).

The integration guide supports all the versions of Luna Client notably Luna 10.1 Universal Client, Luna 7.5 Client and Luna 7.2 Client with Windows Server 2016 Operating system.

5.1 Prerequisite

Please make sure the Luna Client is installed and configured successfully. To verify the successful installation and configuration, please follow the below steps.

- 1. Open Command prompt as administrator.
- 2. Go to the folder where lunacm is located using cd command.(Example of lunacm file path is C:\Program Files\SafeNet\LunaClient)
- 3. Run the command lunacm.exe (for Windows).



4. Output should look like the below screenshot. If not, please do Luna client configuration first.

5.2 Installation and configuration of Java

- Only supported version for using Luna SafeNet HSM is Java 8.Download Java 8 from the official website <u>https://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html</u> as per your operating system (Windows Server 2016)
- Add "C:\Program Files\Java\jdk1.8.0_241\bin" in PATH variable (Environment).
- Update the Luna Provider in the java.security file in the folder C:\Program Files\Java\jdk1.8.0_241\jre\lib\security\java.security file using notepad. Add com.safenetinc.luna.provider.LunaProvider at the last of security.provider list. Output might be look like

security.provider.1=sun.security.provider.Sun security.provider.2=sun.security.rsa.SunRsaSign security.provider.3=sun.security.ec.SunEC security.provider.4=com.sun.net.ssl.internal.ssl.Provider security.provider.5=com.sun.crypto.provider.SunJCE security.provider.6=sun.security.jgss.SunProvider security.provider.7=com.sun.security.sasl.Provider security.provider.8=org.jcp.xml.dsig.internal.dom.XMLDSigRI security.provider.9=sun.security.smartcardio.SunPCSC security.provider.10=sun.security.mscapi.SunMSCAPI security.provider.11=com.safenetinc.luna.provider.LunaProvider

- Save the changed to the java.security file.
- Copy the LunaAPI.dll (Windows) and the LunaProvider.jar files from the C:\Program Files\SafeNet\LunaClient\JSP\lib\jsp\lib to the Java extension folder located atC:\Program Files\Java\jdk1.8.0_241\jre\lib\ext.
- Create a file called lunastore where the **project(**C:\Users\hp\Documents\backend**)** is running and add the following line:

tokenlabel:<service_label>

(Please replace the <service_label> with the partition name like elabhsm1par9.Example: tokenlabel:elabhsm1par9)

Installation and Configuration of JDK is completed.



6. Signing JAR files using MyCodesigner application

6.1 Login

- Go to MyCodesigner virtual machine, open browser and type localhost in the URL. It will take into the login screen.
- Enter CO Admin credentials and do 2-factor-authentication.
- Screenshot of login and 2-factor authentication

 Description Secure Authorship, Publication date and Content Maintains software integrity Building trust between Users 	Email Password © Eorgot your password? Sign In
 Secure Authorship, Publication date and Content Maintains software integrity Building trust between Users 	Content of the sent to your email. Your Authentication code is valid for only 3 minute.



6.2 Create build server

- After login into CO Admin, it will take you to the dashboard and click on Configuration option to create build server.
- On Build server configuration tab, click on Create new button to create new build server.
- Enter build server name, choose platform as GEMALTO JAR from drop-down, choose HSM as GEMALTO HSM from drop-down, enter the other required details and click submit button to create a new build server.
- To view build server configuration, click view button on the table to view particular build server.
- To update build server configuration, update the details except Build server name and Platform, fill the other changes want to update and click Update button to update the Build server details.
- Screenshots of the build server

MyCodeSig	iner			prabhakarmp18@outlook.com 🕡 🗸
Dashboard	Configuration Build server Configuration	Ø Virus Scan Configuration		
續 Import Certificate ፪ Policy	Create New +			
🕢 Register Approver	Build Servers			
Manage Workflows	Build server	Platforme	Submitted on	View
🕎 Register Job Submitter	Gemalto Windows Server-1	GEMALTO_WINDOWS	February 8, 2020 8:56 PM	View
🛐 Audit Report 💱 Job Report	Gemalto JAR server-1	GEMALTO_JAR	February 14, 2020 2:09 PM	View
(?) User Manual				



MyCodeSign	er		prabhakarmp18@outlook.co
	Configuration		
Dashboard	Build server Configuration	Virus Scan Configuration	
Create Certificate			
mport Certificate	Build Server Name *	Build server name	
olicy	Choose Platform *	x 8.00	
egister Approver	choose hardonn	Gemalto JAR	
anage Workflows	Choose HSM *	Gemalto HSM	
egister Job Submitter	IP address / Server name *	Server IP address/Server name.	
idit Report			
b Report	Server Username *	Server username.	
ser Manual	Password *		٥
	Source file Path *	C/documents/applications/Unsigned/	
	Signed File(s) Path *		
		C/documents/applications/signed/ Submit Cancel	
@MyCodeSig	gner	C/documents/applications/signed/ Submit Cancel	prabhakarmp18@outlook.cor
@MyCodeSig	gner Gemalto JAR server-1	Cydocuments/applications/signed/ Submit Cancel Build server details	prabhakarmp18@outlook.cor
CMyCodeSig	gner Gemalto JAR server-1 Build Server Name	Cydocuments/applications/signed/ Submit Cancel Build server details Gemalto JAR server-1	prabhakarmp18@outlook.cor
CMyCodeSig	gner Gemalto JAR server-1 Build Server Name Platform	Cydocuments/applications/signed/ Submit Cancel Build server details Gemalto JAR server-1	prabhakarmp18@outlook.com
CMyCodeSig	gner Gemalto JAR server-1 Build Server Name Platform	Cydocuments/applications/signed/ Submit Cancel Build server details Gemalto JAR server-1 GEMALTO_JAR	prabhakarmp18@outlook.cor
Comparison of the second secon	gner Gemalto JAR server-1 Build Server Name Platform IP address / Server name *	Cydocuments/applications/signed/ Submit Cancel Build server details Gemalto JAR server-1 GEMALTO_JAR 192.168.124.157	prabhakarmp18@outlook.cor
CCMyCodeSig asbboard reate Certificate mport Certificate olicy egister Approver tanage Workflows	gner Gemalto JAR server-1 Build Server Name Platform IP address / Server name * Server Username *	Cydocuments/applications/signed/ Submit Cancel Build server details Gemalto JAR server-1 GEMALTO_JAR 192.168.124.157 Administrator	prabhakarmp18@outlook.com
MyCodeSig ashboard reate Certificate olicy egister Approver aaaage Workflows egister Job Submitter	gner Gemalto JAR server-1 Build Server Name Platform IP address / Server name * Server Username *	Cydocuments/applications/signed/ Submit Cancel Build server details Gemalto JAR server-1 GEMALTO_JAR 192.168.124.157 Administrator	prabhakarmp18@outlook.com
CCMyCodeSig asbboard reate Certificate mport Certificate olicy egister Approver tanage Workflows egister Job Submitter udit Report	gner Gemalto JAR server-1 Build Server Name Platform IP address / Server name * Server Username * Password *	Cydocuments/applications/signed/ Submit Cancel Build server details Gemalto JAR server-1 GEMALTO_JAR 192.168.124.157 Administrator	prabhakarmp18@outlook.cor
Ashboard Ashboard Areate Certificate olicy atagister Approver tanage Workflows atagister Job Submitter udit Report ob Report	gner Gemalto JAR server-1 Build Server Name Platform IP address / Server name * Server Username * Password * Source file Path *	Cyldeenents/applications/signed/ Submit Cancel Build server details Gemalto JAR server-1 GEMALTO_JAR 192.168.124.157 Administrator	prabhakarmp18@outlook.com

6.3 Create Certificate

- Create certificate is a self-signed certificate to sign the jar file type. •
- Click on Create certificate in Dashboard. •
- Choose Platform as GEMALTO JAR and fill the all other details. •
- Click Create button to create a certificate. •
- Screenshots of the create certificate for JAR •

C:\Users\hp\Documents\Siged_JAR_files\

Update

Back

🔁 Dashboard	Create Certificate This is required when a ne	w key-pair to be generated for code signing.		
Create Certificate	Choose Platform *	Gemalto JAR	~	
Market Import Certificate	Choose build server *	Select build server	V	
Policy	Common Name (CN) *	eg: www.example.com		
) Register Approver	Organization (O) *	eg: Oracle Pvt. Ltd.		
Manage Workflows	Organizational Unit (OU) *	Security		
Register Job Submitter	Country *	Eg: For USA, country code is US		
	State (S) *	Eg: Texas		
Audit Report	Locality (L) *	Eg: Dallas		
💱 Job Report	Key Name *	Key name		
?) User Manual	Key Password *	Password		
	Key size (bits) *	Select a Key size	v	

6.4 Create Policy

- Policies define the high level parameters like the certificate, platform and the signing method which can be associated with a code signing workflow.
- To create a policy, click on Create policy menu in dashboard.
- Enter the required details to create policy and click on Create policy button.
- Screenshots of the create policy

MyCodeSig	gner			prabhakarmp18@outlook.com 🔬 🗸
Dashboard Create Certificate Import Certificate Policy	Create Policy Policies define the high let code signing workflow. Note: If you don't have an generate key pair for Linu	vel parameters like the certificate, plat ny keys or certificates, click on Create C x based OS.	orm and the signing method whic ertificate. There you can create co	ch can be associated with a ertificate for Windows or
🖉 Register Approver	Policy name	Platform	Certificate name	Build server name
Manage Workflows	Gemalto_wind-1	GEMALTO_WINDOWS	gemalto_test.spc	Gemalto Windows Server-1
Audit Report	Gemalto JAR Policy-1	GEMALTO_JAR	myfeb14key	Gemalto JAR server-1
Job Report				



	Create Policy			
ashboard Dashboard	Policies define the high le code signing workflow.	evel parameters like the certificate, platform and t	ne signing method which can be a	ssociated with a
Create Certificate	Note: If you don't have a	ny keys or certificates, click on Create Certificate. av based OS	There you can create certificate fo	Windows or
Import Certificate				
Policy	Policy Name *	ex dll policy sign for development		
Register Approver	Signing Platform *	Gemalto Windows	×	
Manage Workflows	Choose build server *	Select build server	~	
Register Job Submitter				
Audit Report	Certificate *	Select Certificate	×	
🖓 Job Report	Signing Tool *	Select a signing tool for windows	~	

6.4 Register Job approver

- Click on Register approver menu in the dashboard.
- Enter Approver email and approver name.
- Click on Submit button to register job approver.
- Screenshot of register job approver

C MyCodeSi	gner		prabhakarmalipatil@gmail.com ()) ~
🖬 Dashboard	Approver Registr	ation	
Create Certificate	Approver Email *	Approver Email	
import Certificate	Approver Name *	Approver Name	
P Create Policy		Submit	
🖉 Register Approver			
Manage Workflows			
🖹 Register Job Submitter			
Audit Report			
🛒 Job Keport			

6.5 Manage Workflow

- Click on Manage workflow menu in the dashboard.
- Choose policy from the drop-down, select no. of approver, workflow description and each level approver and their designation.
- Click Create button to create new workflow
- Screenshot of Manage Workflow



	ner				prabhakarmalipatil@gmail.com 🜘
Dashboard	Manage Workflow You can configure appro maximum of 5 approval If you have already confi there are no pending Job	S val workflows for each artifact type. You steps per workflow. gured workflows, then you can modify o requests.	ı can have only if		
Timport Certificate	Policy *	Select Policy		Y	
🖉 Register Approver	No. of Approvers *	1		~	
Manage Workflows	Level-1 Approver *	Select level-1 Approver	 Approver Designation 		
Audit Report	If you did not find the ap	prover in the above dropdown, then you	u can create new approver. It wil	l appear in the dropdown list	
💱 Job Report	+ Create New Appro	wer			
?) User Manual	Description *	Workflow description.			
			Create	10	

6.6 Register Job submitter

- Click on the Register Job submitter menu from the dashboard.
- Enter the job submitter email, name and select policy from the drop-down.
- Click on Submit button to register new Job submitter.
- Screenshot of Register Job submitter

	iner		prabhakarmalipatil@gmail.com () v
🛱 Dashboard	Job Submitte	er Registration	
Create Certificate	Email *	Job Submitter Email	
import Certificate	Name *	Job Submitter Name	
P Create Policy	Policy *	Select Policy	
🖉 Register Approver			
Pa Manage Workflows		Submit	
Register Job Submitter			
Job Report			
(?) User Manual			

6.7 Manage Job submitter

- Click on the Manage Job submitter menu from the dashboard.
- Choose Job submitter from the drop-down and select policy from the drop-down.



- Click on Submit button to assign new policy to the existing job submitter.
- Screenshot of Manage Job submitter

	ner		prabhakarmalipatil@gmail.com v
🔁 Dashboard	Assign Policy to exi	sting Job Submitter	
🚍 Create Certificate	Choose Job Submitter *	Select Job Submitter V	
👔 Import Certificate	Choose Policy *	Select Policy V	
P Create Policy			
🖉 Register Approver		Submit	
Manage Workflows			
Register Job Submitter			
Audit Report			
Job Report			
⑦ User Manual			

6.8 Create a signing job

- Login as a job submitter and click on Create signing job menu in the dashboard.
- Enter the job name, description, choose policy from the drop-down, and select the build server from the drop-down.
- Enter the file name to sign the relative path.
- Click on Create Job button to create a job.
- Screenshot of Create a signing job

MyCodeSi	gner			prabalkantisarkarwork@outlook.com ()) v
🖬 Dashboard	Create Signing Job			
Create Signing Job	Job Name *	eg: windows job1		
(?) User Manual	Description *	Description		
			li	
	Choose Policy *	Select Policy	V	
	Choose build server *	Select build server	V	
		OR switch to Upload file		
		Create Job		



6.9 Action on job (Approve, Reject and more info)

- Login as a job approver and click on Action button in the Signing requests waiting for your approval table of particular job.
- You can add notes to the particular job.
- To approve a job, click on Approve button in the approval workflow table, once the job is approved it will go for signing.
- To reject a job, click on Reject button in the approval workflow table.
- To request more information about a job, click on more info requested button in the approval workflow table.
- Screenshot of Approver

MyCodeSi	gner					viratavarva@gmail.com (
	Details					
E publication	Job ID	1025		Status	APPROVED	
E Dasuboard	Submitted by	Prabhakar M	aliPatil	Virus Scan	Clear	
? User Manual	Submitted on	February 24,	2020 2:48 PM	Malware Scan	Clear	
	Description					
	JAR file signing					
	Approval Workflo	ow				
	Approver Name	Date	Action	More Info Requested	Notes	
	Ashok Kumar	February 14, 2020 5:22 PM	PENDING			
						< Back



6.10 Verify JAR file after signing

01.	Administrator: Command Prompt	8 <u>.22</u>		×
C:\U⊴	ers\hp\Desktop\signedFolder>jarsigner -verbose -verify 1581589665933test.jar			
2	1131 Tue Feb 84 16:08:06 CST 2020 MFTA-INF/MANTEFST.MF			
1	1235 Tue Feb 04 16:08:08 CST 2020 META-INF/LUNAKEY.SF			
	4526 Tue Feb 04 16:08:08 CST 2020 META-INF/LUNAKEY.RSA			
	0 Man Nov 05 16:06:18 CST 2007 META-INF/			
	0 Mon Nov 05 16:06:18 CST 2007 META-INF/maven/			
	0 Mon Nov 05 16:06:18 CST 2007 META-INF/maven/org.objectweb.think.minus.test/			
	0 Mon Nov 05 16:06:18 CST 2007 META-INF/maven/org.objectweb.think.minus.test/java/			
sm	1161 Wed Oct 24 14:01:04 CST 2007 META-INF/maven/org.objectweb.think.minus.test/java/pom.xml			
sm	117 Mon Nov 05 16:06:16 CST 2007 META-INF/maven/org.objectweb.think.minus.test/java/pom.properties			
sm	379 Wed Oct 24 14:07:14 CST 2007 PlatformHelper.class			
SIT	1970 Wed Oct 24 14:07:14 CST 2007 Stm8010Helper.class			
sm	1759 Wed Oct 24 14:07:14 CST 2007 PosixXHelper.class			
sm	1870 Wed Oct 24 14:07:14 CST 2007 LxsimenvHelper.class			
sm	1882 Wed Oct 24 14:07:14 CST 2007 IntegratorHelper.class			
Sm	1/2/ Wed Oct 24 14:07:14 CS1 2007 POSIXHEIDER CIASS			
sm	1134 Wed Oct 24 14:07:14 CS1 2007 lestutilsprinterinread.class			
Sm	0017 Wed Uct 24 14.07,14 C31 2007 TestUtil.class			
	signature was verified			
	entry is listed in manifest			
k -	at least one certificate was found in keystore			
i -	at least one certificate was found in identity scope			
- Sig	ned by "CN=prabal, OU=ec, O=ec, L=Bangalore, ST=Karnataka, C=IN"			
0	ligest algorithm: SHA-256			
5	ignature algorithm: SHA256withRSA, 2048-bit key			
Tin	estamped by "CN-GlobalSign TSA for Standard - G2, O-GMO GlobalSign Pte Ltd, C-SG" on Tue Feb 04 10:38:09 UTC 2020			
	Timestamp digest algorithm: SHA-256			
	imestamp signature algorithm: SHAlwithRSA, 2048-bit key			
iar y	serified.			
Warni	ing:			
This	jar contains entries whose certificate chain is invalid. Reason: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException	unable	to find y	alid
cert	ification path to requested target			
This	jar contains entries whose signer certificate is self-signed.			

7. Signing JAR files with REST API using postman

7.1 Login

Here the Customer Organization admin will enter the login credentials like user email address and password to login. On successful verification of login credentials, one token will be generated and assigned to the user. Concurrently, the user will also get one email containing authentication code. User will use the token and authentication code to complete 2 factor authentications for successful login.

• Enter the login URL and Choose Method POST



POST ht	tp://localhos	:t:8000/login/log• +			No Environment	w	O	\$
Untitled	Request					📮 Cor		
POST	v	http://localhost:8000/lo	gin/login_user		Send	•	Save	v
Params	Author	ization Headers	Body Pre-request Script	Tests Settings		Со	okies	Code
Query P	arams							
KEY			VALUE		DESCRIPTION	***	Bull	k Edit
Ke	у		Value		Description			
Respons	se							

• Choose the Body option. Once Body option is chosen, click the raw radio button and choose JSON from the drop down.

POST http:/	//localhos	it:8000/lo	gin/log• + •	••					No Environ	ment	•
Untitled Re	equest										Co
POST	•	http://	/localhost:8000/logi	n/login_use	r					Send	
Params	Author	ization	Headers (1)	Body	Pre-requ	est Script	Tests	Settings			C
none	forr	n-data	x-www-form-u	rlencoded	🖲 raw	linary	I Gra	ohQL BETA	Text 🔺		
1									Text		
									JavaScript		
									JSON		
									HTML		
									XML		

• Inside the body, enter the Customer organization login credentials as per shared screenshot format. Then Click Send Button.



Untitled R	equest											Ę	Commen	ts (0)
POST	Ŧ	http://	localhost:8000/log	in/login_user							Send	•	Save	v
Params	Author	ization	Headers (2)	Body 🔵	Pre-re	quest Script	Tests	Setting	zs				Cookies	Code
none	I forr	n-data	x-www-form-u	urlencoded	🖲 raw	binary	Graph	IQL BETA	JSON	v			Bea	utify
1 • { 2 " 3 "	user_emai user_pass	ll":"prat sword":"1	pal@encryptioncon: Fest@12345"	sulting.com"										

• On Successful login, token is generated.

POST http://localhost:8000/lo	ogin/log• + •••		No Environment	• •	*
POST v http:/	/localhost:8000/login/login_user		Send	▼ Save ▼	۳.
1 * {{ 2 "user_email":"pra 3 "user_password":" 4 }	bal@encryptionconsulting.com", Test@12345"				
Body Cookies Headers (Pretty Raw Previ	12) Test Results iew Visualize ^{BETA} JSON •	Status: 200 OK	Time: 842ms Size: 777 B	Save Response	•
1 { 2 "Status": 3 "Msg": "P' 4 "token": "eyJhl UxMLV' opzH01 5 }	200, lease do Authentication Code- bGci0iJIUzI1NiIsInR5cCI6IkpXV VTRVItN2M2Y2QwNjAtNDE5NS0xMWV ElGpc3dIYKJ_avEy07RhpeT0zI5S1	verification to complete the log /CJ9.eyJleHAi0jE2MTE5MjA3MzUsImRh /hLTllZWMt0GQ3Y2ZmYzNiZWQ5In0sIml .eJ5f6tj1k"	in process", dGEiOnsiYWxsX3VzZXJfdW5 hdCI6MTU4MDM4NDczNX0.	ipcXVlX2lkIjoiQ	I

7.2 Verify authentication code to complete two factor authentications

• Enter the verify authentication code URL and Choose Method POST

Untitled R	equest				📮 Comments (0)
POST	v	http://localhost:8000/master	r/verify_otp	Send	▼ Save ▼
Params Query Par	Author ams	ization Headers Bod	y Pre-request Script Tests Settings		Cookies Code
KEY			VALUE	DESCRIPTION	••• Bulk Edit
Key			Value	Description	

• Choose Headers option and Enter token in key data. Use the token value (generated on successful login)

POS	T http://l	ocalhos	t:8000/login/l	og	POST ht	tp://loca	alhost:8000/master/v●	+	•••		No Environm	ient	,	-	•	\$
Untit	led Req	uest											P			
PO	ST	v	http://loca	lhost:800	00/mast	er/verif	y_otp					Sen	d 🔻	Sav	e	v
Para	ms	Author	ization	Headers	(1)	Body	Pre-request Script		Tests	Settings				Cookie	es C	ode
*	leaders	(1)														
	KEY						VALUE				DESCRIPTION	•••	Bulk Edit	Pres	sets	¥
\checkmark	token						eyJhbGciOiJIUzI1NilsIr	R5cCl	6lkpX\	/CJ9.eyJleHAiO						
	Key						dW5pcXVIX2lkljoiQUx	MLVV	TRVItN	2M2Y2QwNjAt	Description					
Resp	onse						NDE5NS0xMWVhL1112 5In0sImIhdCl6MTU4N c3dIYkJ_avEy07RhpeT	(WMtC 1DM41 Ozl5SI	DGQ3Y NDczN leJ5f6tj	22mYzNi2WQ X0.opzH0ElGp 1k						

• Choose the Body option. Once Body option is chosen, click the raw radio button and choose JSON from the drop down.

POST http:	//localhos	t:8000/login/log●	POST http://loca	lhost:8000/master/v●	+		No Environment		• •	>
Untitled Re	equest							Ę		
POST	•	http://localhost	8000/master/verif	y_otp			Send	•	Save	3
Params	Author	ization Head	ers (1) Body	Pre-request Scrip	t Tests	Settings			Cookies	s C
none	forr	n-data 🌑 x-ww	/w-form-urlencode	d 🖲 raw 🌑 bin	ary 🌘 Gra	iphQL ^{BETA} Text	rt 🔺			
						Jav	aScript			
						JSC	N			
						HT	ML			
						XM	L			

• Sample of email received with Authentication Code

Authe	Authentication code-verification to complete login process in My Code Signing													
м	MyCodeSigner <iwishbids@gmail.com> Thu 1/30/2020 11:52 AM Prabal ⊗</iwishbids@gmail.com>	3	5	(5)	\rightarrow	2112								
	Dear prabal@encryptionconsulting.com,													
	Your authentication code for two-factor authentication is 6727													
	Your authentication code is valid for 3 minutes													
	Best Regards,													
	MyCodeSigner Team													
	MyCodeSigner													
	Note : This is an auto generated email.													

• Inside the body, enter the Authentication Code as per shared screenshot format. Then Click Send Button.



POST http://localho	st:8000/login/log● Post http:	//localhost:8000/master/v	• + …	No Environment	• • •
POST 🔻	http://localhost:8000/master/	verify_otp		Send	▼ Save ▼
none	m-data 🛛 🛡 x-www-form-urlen	coded 👅 raw 🔵 b	inary 🔵 GraphQL 🚟 JSON 🔻		Deautity
1 * { 2 "user_otp 3 }	":"6727"				
Body Cookies H	eaders (12) Test Results		Status: 200 OK	Time: 86ms Size: 720 B	Save Response 👻
Pretty Raw	Preview Visualize BETA	JSON 🔹 🚍			ē Q
1 { 2 "St 3 "Ms 4 "da 5 6 7 8	atus": 200, g": "Two factor authentic ta": { "user_master_id": "USER- "customer_organisation_i "role_name": "CO_ADMIN", "user_email": "prabal@er	ation is successful MASTER-7c6cd061-419 d": "ORGANISATION-c cryptionconsulting.	lly done for the user", 95-11ea-9eec-8d7cffc3bed9", wYM2MrLC", .com"		

7.3 Generate Key

• Enter the key generation for signing jar application URL and Choose Method POST.

POST http:	://localhos	t:8000/master/× + •						No Environment	1	, (0	\$
Untitled Re	equest								Ę	Com		
POST	٣	http://localhost:8000/mas	ter/postman_	gemalto_add_jar_key				Send	•	Sav	e	v
Params	Author	ization Headers (10)	Body 🌒	Pre-request Script Te	sts	Settings				Cookie	es C	ode

• Choose Headers option and Enter token in key data. Use the token value (generated on successful login).

POST	¥	http://localhost:8000/master/postma	an_gemalto_add_ja	ır_key		Send
Params	Author	rization Headers (10) Body ●	Pre-request	Script Tests Settings		
▼ Head	ers (2)					
KEY				VALUE	DESCRIPTION	••• Bulk Edit
V toke	en			eyJhbGciOiJIUzI1NiIsInR5cCl6lkpXVCJ9.eyJleHAiOjE1ODIxMDc4NzMsI		
✔ Cor	ntent-Type			mRhdGEiOnsiYWxsX3VzZXJfdW5pcXVIX2lkljoiQUxMLWTRVItOTg5Mz NhYjAtNDk2ZC0xMWVhLWJkY2ltMmlzMmVIMGJINzZhIn0simlhdCl6M		
Key				TU4MjAyMTQ3M30.q7QyBQ-tmx77aTDw16TGj1DapX- MrITMdoO_robH95Y	Description	
▶ Temp	oorary Hea	aders (8) 🕕				

• Choose the Body option. Once Body option is chosen, click the raw radio button and choose JSON from the drop down.

POST	http://localhost:8000/master/postman_gemalto_add_jar_key		Send	•	S
Params	Authorization Headers Body Pre-request Script Tests Settings				Coc
none	● form-data ● x-www-form-urlencoded ● raw ● binary ● GraphQL	Text 🔺			
1		Text			
		JavaScript			
		JSON			
		HTML			
		XML			

• Inside the body, enter the mandatory data to generate key as per shared screenshot format. Then Click Send Button.



POST http://localhost.8000/master/postman_gemalto_add_jar_key 	Send Save *
Params Authonization Headers (10) Body Pre-request Script Tests Settings	Cookies Code
● none ● form-data ● x-www-form-urlencoded ● raw ● binary ● GraphQL JSON ▼	Beautify
<pre>server_ip':'192.168.137.133', "server_node_port':'34080', "website_name":'Incryption_Consulting_LLC', "organization_name":'Encryption_Consulting_LLC', "organization_unit_name":'Security', "tily_name":'Dills', "state_name":'Tens', "country_cude":'US', "country_cude":'US', "key_mame':'genalto_postman_one", "key_mame':'2456', "key_size":'2048' }</pre>	

• On Successful key generation, the response status will be 200.

POST	• http://	localhost:8000/ma	ster/postman_p	gemalto_add_jar_ke	у						Send	×
Params	Authorization	Headers (10)	Body 🌒	Pre-request Scrip	ot Tests	Settings						
none	form-data	🔵 x-www-form-u	irlencoded	🖲 raw 🏾 🔘 binary	GraphQL	JSON	٣					
2 3 4 5 6 7 8 9 10	"server_ip":"1 "server_node_p "website_name" "organization_ "organization" "ilty_name":"1 "state_name":"2 "key_name":"ge	92.168.137.133", ort":"34980", :"www.mycodesign name":"Encryptic unit_name":"Secu allas", Texas", :"US", malto_postman_on -Manarce	er.com", n_Consulting rity", e",	μις,								
Body Coo	kies Headers (2) Test Results							Status: 200 O	K Time: 219ms	Size: 511 B	Save
Pretty	Raw Previ	ew Visualize	JSON ¥	Ð								
1 7 3 4	"Status": 2 "Msg": "Key	10, for signing jar	file is gene	rated successful	ly."							

7.4 Signing Jar application

Г

• Enter signing jar application URL and Choose Method POST. Choose Headers option and Enter token in key data. Use the token value (generated on successful login).



POST	ST • http://localhost:8000/master/postman_gemalto_sign_jar_file							
Paran	is Authoi	rization Headers (10)	Body Pre-reque	st Script Tests Settings				
▼ H	eaders (2)							
	KEY			VALUE	DESCRIPTION	••• Bulk Edit		
✔ token .			¥.,	eylhbGciOijlUzl1NilsInR5cCl6lkpXVCJ9.eylleHAiOjE1ODixMDc4NzMsI				
Content-Type			mknadelonsirtwxsAsv22AjrawspCAviA2ikijoiQOXimLVvTkvitOTgSm2 NhYjAtNDk2ZC0xMWVhLWjkY2ltMmizMmVlMGJINzZhin0simlhdCl6M					
	Key			MrITMdoO_robH95Y	Description			
▶ Te	mporary Hea	aders (8) 🚺						

• Inside the body, enter the mandatory data to sign jar application as per shared screenshot format. Then Click Send Button. On Successful signing, the response status will be 200 along with the signed file name.

POST	http://localhost:8000/master/postman_gemalto_sign_jar_file	Send	v
Params	ithorization Headers (10) Body ● Pre-request Script Tests Settings		
none	form-data 🔍 x-www-form-urlencoded 🔎 raw 🔍 binary 🜑 GraphQL JSON 🔻		
2 3 4 5 6 7	ned_file_path":"C:\\Users\\hp\\Desktop\\signedFolder\\", igned_file_path":"C:\\Users\\hp\\Desktop\\UnsignedFolder\\test.jar", name":"gemalto_postman_one", ver_ip"."192.168.137.133", e_server_port":"34980"		
lody Co	Headers (12) Test Results Status: 200 OK Time: 96ms Siz	ze: 540 B	Sa
lody Co Pretty	Headers (12) Test Results Status: 200 OK Time: 96ms Siz	ze: 540 B	Sa

7.5 Verify JAR file after signing

• Check whether jar application is signed. For unsigned jar application, output of the command will have message "jar is unsigned". The command to check digital signature of jar is "jarsigner –verify test.jar"





• Verify the digital signature of the signed jar application. The command to check digital signature of jar is "jarsigner –verbose –verify 1581589665933-.-.test.jar"

0:1.	Administrator: Command Prompt	_		Х
C:\U	sers/hp/Desktop/signedFolder>jarsigner -verbose -verify 1581589665933test.jar			
	1131 Tuw Feb 04 16:88:86 CST 2020 META-TNF/MANTEFST.MF 1235 Tue Feb 04 16:88:86 CST 2020 META-TNF/LUNAKEY.SF 4526 Tue Feb 04 16:88:08 CST 2020 META-INF/LUNAKEY.RSA 0 Mon Nov 05 16:66:18 CST 2020 TETA-INF/maven/org.objectweb.think.minus.test/ 0 Mon Nov 05 16:66:18 CST 2007 META-INF/maven/org.objectweb.think.minus.test/ 0 Mon Nov 05 16:66:18 CST 2007 META-INF/maven/org.objectweb.think.minus.test/			
sm sm sm sm sm	161 Hod Do 20 Jobola CSI 2007 HL Ha Har Jameer (vg too jecked chain Halles test java) 161 Hod Do 2 4 14:01:14 CSI 2007 HLA INF, haven/org.objectkeb.think.minus.test/java/pom.properties 379 Wed Oct 24 14:07:14 CSI 2007 PlatformHelper.class 1970 Wed Oct 24 14:07:14 CSI 2007 Stm8010Helper.class 1970 Wed Oct 24 14:07:14 CSI 2007 Stm8010Helper.class 1970 Wed Oct 24 14:07:14 CSI 2007 Stm8010Helper.class 1970 Wed Oct 24 14:07:14 CSI 2007 LisimenvWelper.class			
500 500 500 500	1082 Wed Oct 24 14:07:14 CST 2007 Integratoriklper.class 1777 Wed Oct 24 14:07:14 CST 2007 Positiklper.class 134 Wed Oct 24 14:07:14 CST 2007 TestUltilsPrinterThread.class 8019 Wed Oct 24 14:07:14 CST 2007 TestUltil.class			
s m k i Si	= signature was verified = entry is listed in manifest = at least one certificate was found in keystore = at least one certificate was found in identity scope gned by "CN-prabal, OU-ec, O-ec, L-Bangalore, SI-Karnataka, C-IN" Digest algorithm: SHA256 Signature algorithm: SHA256withRSA, 2048-bit key			
Ti	mestamped by "CN-GlobalSign TSA for Standard - C2, O-GMO GlobalSign Pte Ltd, C-SG" on Tue Feb 04 10:38:09 UTC 2020 Timestamp digest algorithm: SNA-256 Timestamp signature algorithm: SNAiwithRSA, 2048-bit key			
Jar	tied.			
Warn This cer This	ing: jar contains entries whose certificate chain is invalid. Reason: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: tification path to requested tanget jar contains entries whose signer certificate is self-signed.	unable '	to find	valid



