

# DIGICERT

Integration Guide

Applicable Devices: KMES Series 3

THIS DOCUMENT CONTAINS CONFIDENTIAL INFORMATION PROPRIETARY TO FUTUREX, LP. ANY UNAUTHORIZED USE, DISCLOSURE, OR DUPLICATION OF THIS DOCUMENT OR ANY OF ITS CONTENTS IS EXPRESSLY PROHIBITED.



#### TABLE OF CONTENTS

[1] OVERVIEW OF THE KMES SERIES 3 / DIGICERT INTEGRATION	3
[2] CONFIGURATION ON DIGICERT	4
[3] CONFIGURATION ON THE KMES SERIES 3	7
APPENDIX A: XCEPTIONAL SUPPORT	13



# [1] OVERVIEW OF THE KMES SERIES 3 / DIGICERT INTEGRATION

## [1.1] ABOUT DIGICERT

DigiCert is one of the world's leading providers of scalable TLS/SSL, IoT and PKI solutions for identity and encryption. Many of the most innovative companies, including 89% of the Fortune 500 and 97 of the 100 top global banks, choose DigiCert for its expertise in identity and encryption for web servers and Internet of Things devices. DigiCert supports TLS and other digital certificates for PKI deployments at any scale through its certificate lifecycle management solution, CertCentral<sup>®</sup>.

#### [1.2] PURPOSE OF THE INTEGRATION

This integration gives users the ability to orchestrate the issuing of certificates, signed by the DigiCert CA, using the KMES Series 3. Another way to put that is it incorporates DigiCert signing of keys into the Futurex Registration Authority process.

#### What is a Registration Authority (RA)?

Registration Authorities (RAs) approve and deny requests for certificates, also known as certificate signing requests (CSRs). The RA presides over and assists the Certificate Authorities (CAs) by informing them of which certificates can be issued (**NOTE**: DigiCert acts as an external CA for this use-case). Upon approving a CSR, the RA has validated the identity and registration information of the user, and permitted the CA to issue a certificate.

#### [1.3] KEY BENEFITS OF THE INTEGRATION

The KMES Series 3 / DigiCert integration gives you the ability to:

- Automatically download successfully signed requests submitted by the RA
- Utilize Futurex approval requirements
- Revoke signed requests from the RA
- Resign requests from the RA
- Cancel pending orders
- Utilize rate limiting mechanisms



# [2] CONFIGURATION ON DIGICERT

For DigiCert to authenticate the KMES Series 3 device that will be sending CSRs to the DigiCert CA, it is necessary to first generate an API Key in the DigiCert dashboard (CertCentral®), which will be imported into the KMES Series 3 in the next section.

#### [2.1] GENERATE A NEW API KEY

While logged in to the DigiCert dashboard (CertCentral<sup>®</sup>) hover over *Automation* on the left-hand menu, then click *API Keys*.





Adialaant®   CERTOR				Esturau Consective D	
		Key		×	enteria 🗸 🦕 🎰 🥐
REQUEST A CERTIFICATE	Add ATT	NC y			
	Description				
CERTIFICATES	User				
Q DISCOVERY	Select When you assign an	API key to a user, you link the us	er's permissions to the ke		
🔌 AUTOMATION	API key restriction Orders, Domains,	s (optional) Organizations		•	
API Keys	Further restrict the	PI key permissions to a defined	set of actions.		
ACME Directory URLs New		2			
S FINANCES		- 0	Cancel	Add API Key	🛱 Revoke
	Ben_Test (i)	Samantha Renteria	Active	07 Jul 2020	Î Revoke
ACCOUNT	test_key (j)	Samantha Renteria	Active	01 Jun 2020	1 Revoke
► SETTINGS	TestAPIkey (j)	Samantha Renteria	Active	29 May 2020	Î Revoke
r tools	Test (j)	Samantha Renteria	Revoked	28 May 2020	
	QA Key (j)	Samantha Renteria	Active	18 May 2020	1 Revoke
	Support Test Key	Samantha Renteria	Revoked	06 May 2020	0-
	Remotekey Order	Samantha Renteria	Revoked	06 May 2020	Ū

Click the Add API Key button and fill in the required fields.

**NOTE:** When adding an API Key in the DigiCert dashboard it must have the "Orders, Domains, Organizations" permissions.

Once you click *Add API Key* it will create and show you the clear API Key/Token that was generated. Click the text to copy the API Key to your clipboard, then acknowledge that the DigiCert dashboard will not show you the API Key again.





## [2.2] CREATE A NEW FILE WITH THE .CSV EXTENSION THAT CONTAINS YOUR API KEY/TOKEN

In a text editor, create a new file and type "api token" in the first line of the file, then hit *Enter* to go to the next line, and paste in the API Key. It should look similar to this:

api token

BTIMAQBS2XZAVTIF7BKJDJ6DON5AHWFU4DV3WJWWJCWSREE5UAUFY5QUZ4SIR7MDHTJBCVX5ANRTPENUO

Save the file with an extension of .csv. This is necessary in order to import it into the KMES Series 3.



# [3] CONFIGURATION ON THE KMES SERIES 3

In this section, we will create a CA group container on the KMES Series 3 that will hold a representation of the issuing CA housed at DigiCert. This is done by performing the following actions:

- Creating a CA group container and defining it as "External DigiCert X.509"
- Specifying which DigiCert signing/issuing CA that you want to use to issue certificates
- Defining an Issuance Policy for the CA group container

#### [3.1] SETTING CLOUD CREDENTIALS

Cloud Credentials are used to allow the KMES Series 3 device to interface with 3rd party services, such as DigiCert. The *Cloud Credentials* menu is where the API Key generated in section 3.1 will be imported. The full list of steps for importing the API Key are provided below:

1. Log into the key management device and select *Cloud Credentials* from the menu on the left.



2. At the bottom right of the window, click the *Add Cloud Credential* button. This will open a *Cloud Credential* window.





- 3. Fill in the following information:
  - Name: This is what will be used to identify the credentials on the KMES Series 3. DigiCert does not use this; this is used to identify the cloud credential on the KMES Series 3.
  - Service: Select DigiCert CertCentral API.
  - Secret Key: Click the Import button, then select the CSV file that was created in section 3.2.
- 4. Click **OK** to save the cloud credential.

If necessary, you can select a credential and click the Edit button, or right click on it and select *Edit*, thus allowing you to change its settings as required. You can also delete a credential via right clicking and selecting *Delete*, or by using the *Delete* button.

In addition, you can view and change the credential's permissions on the device by right clicking it and selecting *Permissions*.

### [3.2] MANAGING CERTIFICATE AUTHORITIES

Certificate Authorities are managed through the *Certificate Authorities* screen.

FLITUREX.COM	CERTIFICATE AUTHOR	RITIES	1 X509 shown, 1 to	tal	
Keve	Name	Notes A	Status	Owner Group	Archived
0 keys, 0 configuration settings	- DemoCa	External DigiCert X.509 Certificate Con		Admin Group	
Cloud Credentials	DiglCert ECC Secure Server CA	No Private Key	Valid	Admin Group	No
Certificate Authorities 1 X509 shown, 1 total					
S X.509 DN Profiles					
Contemporary Stress St					
Signing Approval 2 certificate requests, 0 signab					
PKI Keys 1 PKI Key Pair shown, 1 total					
WCCE Templates     33 WCCE templates shown					
Remote LDAP Servers 0 remote LDAP directories tota					
0 token generation Profile					
0 KMIP Objects shown, 0 total					
Hosts/Networks 0 hosts total					
Encryption Devices 1 group, 1 device, 0 clients					
Peers 0 peers					
Configuration MFK: 8071, PMK: 3B5E					
1 group, 2 users					
Logs 1000 logs shown					
Reports 3 reports					
0 templates	•				( )
Databases 0 databases				Add C	A Archive Restore Filter
Hardware				Gi	oup: Admin Group Users: Admin1,Admin



#### Adding a CA Group Container

- 1. Navigate to the *Certificate Authorities* tab by selecting the menu item on the left.
- 2. Right-click on the window and select Add CA... to create a new CA group container.
  - The CA group container holds all certificates in the certificate tree.

•		Certi	ficate Authority $ imes$
	(		
Name:	DemoCA		
Host:	None	-	
Туре:	External DigiCert X.509	-	
Owner group:	Admin Group	•	Permissions
API Credential:	DemoCredential	-	
Can be used Device Certifica	l for PKI authentication		Add
			Remove
		<u> </u>	Cancel

- 3. Specify the following information in the Certificate Authority window:
  - Name: a short text description of the CA group object, used for referencing on the device.
  - Host: Specification of a key encryption key to securely transport sensitive data, such as RSA private keys, to an external system; this is optional.
  - Type: This specifies the CA type; in this case, you must select External DigiCert X.509.
  - **Owner Group**: (optional) designation of the KMES Series 3 user group that will have full ownership permissions to this CA container object.
  - **API Credential**: Choose one of the DigiCert cloud credentials created. This will allow the CA to connect to DigiCert.
- 4. Click OK to create the CA group container.



#### Adding External Certificates

1. Right click on a CA group container, and select *Import -> External Certificate(s)*.

Search:					
Search.			l		<b></b>
	Common Name	Organization	Valid To	Private	Root
BA91527E6027CDC	DigiCert EV Code Signing CA (SHA2)	DigiCert Inc	2027-04-18 12:00:00	No	No
3FF28BD4075C8D9A	DigiCert SHA2 Secure Server CA	DigiCert Inc	2023-03-08 12:00:00	No	No
3D8532387C974F65	DigiCert ECC Secure Server CA	DigiCert Inc	2023-03-08 12:00:00	No	No
6D78BDE63787CB69	DigiCert SHA2 Assured ID Code Signing CA	DigiCert Inc	2028-10-22 12:00:00	No	No
570ADFB8EBCE94B8	DigiCert SHA2 Extended Validation Server CA	DigiCert Inc	2028-10-22 12:00:00	No	No
DB2E6314F8E71309	DigiCert SHA2 High Assurance Code Signing CA	DigiCert Inc	2028-10-22 12:00:00	No	No
00E00CAD821F2504	DigiCert Document Signing CA	DigiCert Inc	2028-11-05 12:00:00	No	No
DEB164E203C3D242	DigiCert ECC Extended Validation Server CA	DigiCert Inc	2031-06-21 12:54:27	No	No

- 2. The *Select An Intermediate* window will populate with a list of intermediate certificates pulled from DigiCert. Highlight the intermediate you wish to use, then click OK to add it.
  - If necessary, it is possible to quickly locate a intermediate certificate via the Search bar at the top of the window.

/erified: 0 certificates				
Subject	$\nabla$	File	Key Usage	
Jnverified: 1 certificate				
Cubicet	~	File	Error	
Subject		Intermediate	Error	
Digicert Loc Secure Server CA		Internetiate		
	-			
Major Key: PMK 👻 Load Folder:				



FUTUREX

- 3. An Import Certificates window will open. Verified certificates will appear in the Verified panel, and unverified will appear in the Unverified panel.
  - Choose the major key that will be used to verify the certificate.
  - Once chosen, click the Verify button at the bottom of the window to verify the certificate. If verified, it will appear in the Verified panel.
- 4. Click OK to add the certificate.

#### Adding an Issuance Policy

An Issuance Policy allows users to define the workflow of how certificates are deployed, who can deploy them, and what type of certificates can be deployed.

- 1. Expand the CA group container, right click on a certificate, and select Issuance Policy -> Add.
- 2. In the *Issuance Policy* window, select the *DigiCert* tab.

								, ,	
asic Info )	(.509 D	ligiCert	LDAP CRL	LDAP Bin	ding Info	Restrictio	ns		 
Organization:		Futures	K LP		•				
Product:		Standa	rd SSL		•				
Payment meth	od:	Default	•		-				
Domain Contr	ol Validation	Default							
Domain Contr	or vandation	Default							
Code Signing	Provisioning	g: Default	[		<b>T</b>				
Automatic Rer	newal:								
Use order revi	ocation:								
Potential Appr	overs								 
User ID /	Na	Name Title Telephone				Email			
1703923	Samanth	a Renteria	Client Services Specialist 8		830-980-97	30-980-9782 x1380 sr		teria@futurex.com	
, [	Ad	d EV Conta	act				Ren	nove Contact	
l									
								OK	Canacl





- 3. Fill in the following information as required:
  - Organization: Select the correct organization name from the list.
  - **Product**: Select the correct SSL certificate type (e.g. Standard, Multi-Domain, WildCard, EV, Code Signing, etc.). (**NOTE**: This field must match the type of certificate that was imported. If it does not match it will create an "Invalid" certificate.)
  - **Payment method**: The three payment methods are Default, Account Balance, and Profile.
  - Domain Control Validation: The Domain Control Validation field may or may not be editable, depending on the Product type that was selected. Essentially, this setting determines whether the CA verifies that the person making the request is in fact authorized to use the domain related to that request, before issuing an SSL.
  - Code Signing Provisioning: If the Product type is Code Signing this field will be editable. If the Product type is Standard SSL, for example, the Code Signing Provisioning field will be grayed out.
  - **Potential Approvers**: If using an extended validation (EV) certificate, an approver is required. Select Add EV Contact to add an approver to the list.
- 4. Click OK to save the settings.

**NOTE**: Currently it is not possible to change the **Organization** or **Product** fields without deleting and recreating the Issuance Policy. All of the other fields can be changed.

**NOTE**: If any type of Extended Validation (EV) certificate is selected for the Product type, then an EV contact must be added. Right now only "Approver" users can be added as an EV contact.

**NOTE**: If you want to associate additional domain names with a certificate, there must be an *X.509 Extension Profile* attached to the certificate that supports Subject Alternate Names. For more information about how to configure an X.509 Extension Profile that supports Subject Alternate Names, please see the relevant Administrative guide.

#### APPENDIX A: XCEPTIONAL SUPPORT



In today's high-paced environment, we know you are looking for timely and effective resolutions for your mission-critical needs. That is why our Xceptional Support Team will help do whatever it takes to ensure you have the best experience and support possible. Every time. Guaranteed.

- 24x7x365 mission critical support
- Level 1 to level 3 support
- Extremely knowledgeable subject matter experts

At Futurex, we strive to supply you with the latest data encryption innovations as well as our best-in-class support services. Our Xceptional Support Team goes above and beyond to meet your needs and provide you with exclusive services that cannot be found anywhere else in the industry.

- Technical Services
- Onsite Training
- Virtual Training
- Customized Consulting
- Customized Software Solutions
- Secure Key Generation, Printing, and Mailing
- Remote Key Injection
- Certificate Authority Services

Toll-Free: 1-800-251-5112

E-mail: <a href="mailto:support@futurex.com">support@futurex.com</a>



#### ENGINEERING CAMPUS

864 Old Boerne Road Bulverde, Texas, USA 78163 Phone: +1 830-980-9782 +1 830-438-8782 E-mail: info@futurex.com XCEPTIONAL SUPPORT 24x7x365 Toll-Free: 1-800-251-5112 E-mail: support@futurex.com SOLUTIONS ARCHITECT E-mail: solutions@futurex.com