

Enrolling DigiCert DV certificates

Last updated: 17 January 2024

1. Purpose

This manual outlines the steps to configure KeyTalk to enroll DigiCert DV SSL certificates with automated approval of the domains to be set on the certificates.

2. Prerequisites

- KeyTalk server v7.4.0 and higher
- DigiCert Central account with DV (domain validation) product(s)
- Azure company account
- Optionally, certbot or Win-ACME for fully automated certificate enrollment

3. Email fetch configuration

In order to approve (validate) placed DigiCert DV orders, KeyTalk needs to access the mailbox (specified on DigiCert Central account) where DigiCert will send the order confirmation email. KeyTalk supports Office 365 mailboxes accessed via Microsoft Graph (for Exchange Online mail accounts) or via IMAP (for On-Premises MS Exchange mail accounts).

3.1. Configure fetching email from Exchange Online using MS Graph API

1. Login to [MS Azure portal \(App registrations\)](#)
2. Register the app with account type **Accounts in this organizational directory only**
3. Set the redirect uri (Web) to:
`https://login.microsoftonline.com/common/oauth2/nativeclient`
4. Under **Certificates & secrets**, generate a new client secret. Write down the value of the client secret created now. It will be hidden later on.
5. Select **Add permission**, select **Microsoft Graph** then **application permissions** and select the following permissions: **Mail.Read**, **User.Read** and **offline_access**.
6. Depending on the permissions of the user account configuring the email application, it should be necessary for an Admin to login and give his consent for the above permissions.

The screenshot shows the 'API permissions' page in the Microsoft Azure portal. The left sidebar contains navigation links for Overview, Quickstart, Integration assistant, Manage (Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest), and Support + Troubleshooting (Troubleshooting, New support request). The main content area shows the 'msgraph-email-fetcher-app | API permissions' page. It includes a search bar, a refresh button, and a feedback link. A warning message states: 'Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. Add MPN ID to verify publisher.' Below this, an information message explains the 'Admin consent required' column. The 'Configured permissions' section lists three permissions under the 'Microsoft Graph' scope: Mail.Read (Application, Read mail in all mailboxes, Admin consent required: Yes, Status: Granted for KeyTalk 1 BV), User.Read (Delegated, Sign in and read user profile, Admin consent required: No, Status: Granted for KeyTalk 1 BV), and User.Read.All (Application, Read all users' full profiles, Admin consent required: Yes, Status: Granted for KeyTalk 1 BV). A note at the bottom states: 'To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.'

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Mail.Read	Application	Read mail in all mailboxes	Yes	Granted for KeyTalk 1 BV ***
User.Read	Delegated	Sign in and read user profile	No	Granted for KeyTalk 1 BV ***
User.Read.All	Application	Read all users' full profiles	Yes	Granted for KeyTalk 1 BV ***

3.2. Configure fetching email from On-Premises MS Exchange using IMAP

1. Login to [MS Azure portal \(App registrations\)](#)
2. Register the app with account type **Accounts in this organizational directory only**
3. Set the redirect uri (Web) to:
`https://login.microsoftonline.com/common/oauth2/nativeclient`
4. Under **Certificates & secrets**, generate a new client secret. Write down the value of the client secret created now. It will be hidden later on.
5. Select **Add permission**.

Select the **APIs my organization uses** tab and search for "Office 365 Exchange Online".

Request API permissions

Select an API

Microsoft APIs **APIs my organization uses** My APIs

Apps in your directory that expose APIs are shown below

Name	Application (client) ID
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000

Click **Application permissions** and choose the **IMAP.AccessAsApp** and **Mail.Read** permissions.

Request API permissions



Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Permission	Admin consent required
Other permissions	
☐ full_access_as_app ⓘ Use Exchange Web Services with full access to all mailboxes	Yes
Calendars	
Contacts	
Exchange	
IMAP (1)	
☒ IMAP.AccessAsApp ⓘ IMAP.AccessAsApp	Yes
Mailbox	
MailboxSettings	
Mail (1)	
☒ Mail.Read ⓘ Read mail in all mailboxes	Yes

- Depending on the permissions of the user account configuring the email application, it should be necessary for an Admin to login and give his consent for the above permissions.
- Make sure IMAP is enabled and enable if necessary. See <https://learn.microsoft.com/en-us/exchange/clients/pop3-and-imap4/configure-mailbox-access?view=exchserver-2019#enable-or-disable-pop3-or-imap4-access-to-a-single-mailbox> for the instructions.
- KeyTalk Azure admin should register service principals in Exchange and give it IMAP access to the specific mailbox. To do this, open PowerShell, preferably in admin mode, and execute the following:

```
Set-ExecutionPolicy RemoteSigned
Install-Module -Name ExchangeOnlineManagement
```

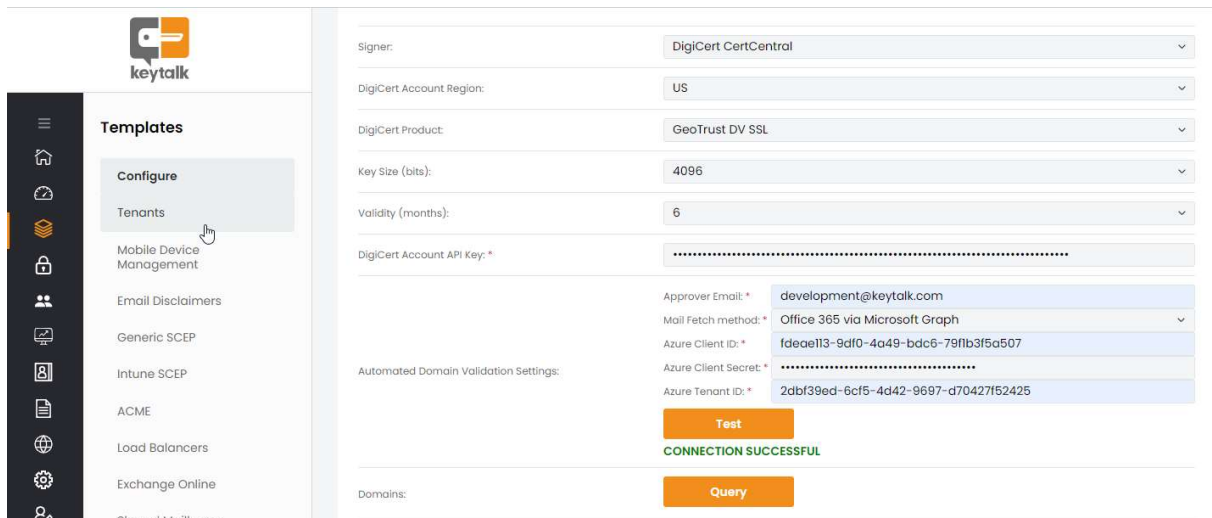
```
Import-Module ExchangeOnlineManagement
Connect-ExchangeOnline -UserPrincipalName "<admin-upn-email>"
New-ServicePrincipal -AppID <AppId> -ServiceId <ServiceId> -Organization
<OrganizationId>
Add-MailboxPermission -Identity "<mailbox>" -User -AccessRights FullAccess
```

The **AppID** and **OrganizationId** are taken from the "App registrations/App name/Overview/Application ID" and "App registrations/App name/Overview/Directory (Tenant) ID" while the **ServiceId** is taken from "Enterprise applications/App name/Overview/Object ID"

See <https://learn.microsoft.com/en-us/exchange/client-developer/legacy-protocols/how-to-authenticate-an-imap-pop-smtp-application-by-using-oauth> for more detail

4. Configure KeyTalk

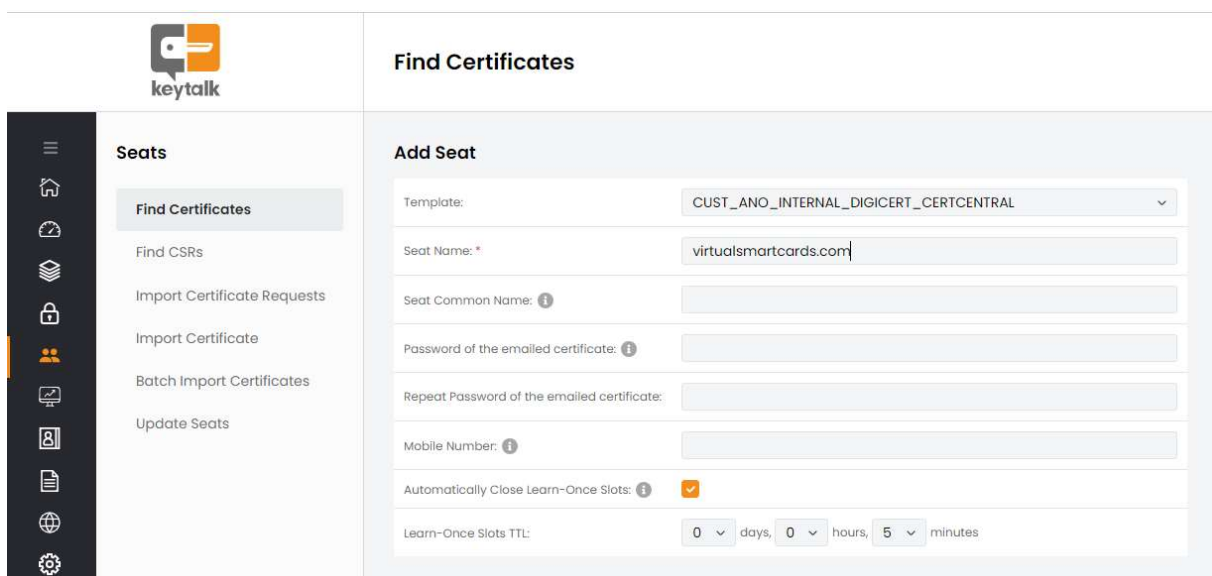
Configure KeyTalk TEMPLATE with one of DigiCert DV products and fill in Azure mail approval application configuration which should already be setup as per section 3.



The screenshot shows the KeyTalk web interface. On the left is a sidebar with a 'Templates' menu. The 'Configure' option is selected, showing a list of templates: Mobile Device Management, Email Disclaimers, Generic SCEP, Intune SCEP, ACME, Load Balancers, Exchange Online, and Shared Mailboxes. The main area displays the configuration for a DigiCert CertCentral template. Fields include: Signer (DigiCert CertCentral), DigiCert Account Region (US), DigiCert Product (GeoTrust DV SSL), Key Size (4096), Validity (6 months), and DigiCert Account API Key (masked). Below these are fields for Automated Domain Validation Settings: Approver Email (development@keytalk.com), Mail Fetch method (Office 365 via Microsoft Graph), Azure Client ID (fdae113-9df0-4a49-bdc6-79fb3f5a507), Azure Client Secret (masked), and Azure Tenant ID (2dbf39ed-6cf5-4d42-9697-d70427f52425). A 'Test' button is present, with a green message 'CONNECTION SUCCESSFUL' below it. At the bottom, there is a 'Domains' section with a 'Query' button.

Check your mail configuration by clicking the **Test** button.

Add new a seat under the configured TEMPLATE. The simplest way would be to name the new seat under the SSL domain name and leave the rest of the fields empty provided the **use seat name as initial default for certificate CN** is enabled on the TEMPLATE. Another, more production-oriented option would be to choose the domain name to come from CN and/or SAN DNS of the Registration Authority bound to this TEMPLATE or from the seat CN.



The screenshot shows the KeyTalk web interface. On the left is a sidebar with a 'Seats' menu. The 'Find Certificates' option is selected, showing a list of actions: Find CSRs, Import Certificate Requests, Import Certificate, Batch Import Certificates, and Update Seats. The main area displays the 'Find Certificates' section, which includes an 'Add Seat' form. The form fields are: Template (CUST_ANO_INTERNAL_DIGICERT_CERTCENTRAL), Seat Name (virtualsmartcards.com), Seat Common Name (empty), Password of the emailed certificate (empty), Repeat Password of the emailed certificate (empty), Mobile Number (empty), Automatically Close Learn-Once Slots (checked), and Learn-Once Slots TTL (0 days, 0 hours, 5 minutes).

5. Enroll certificate.

5.1. Enroll certificate via KeyTalk Admin Web interface.

Locate the seat you just created and click **Enroll** to place the certificate order.

The screenshot displays the KeyTalk Admin Web interface. On the left is a dark sidebar with a 'keytalk' logo and a vertical menu of icons. The main content area is titled 'Seats' and contains a table of seat information. The table has columns for 'Seat Name', 'Seat Common Name', 'Seat Emailed Certificate password', 'Seat Mobile Number', 'Seat Archived', 'ROCA key detected', and 'Automatically Close Learn-Once Slots'. Each row has an 'Edit' button. Below the table are two orange buttons: 'Refresh' and 'Remove Seat'. Further down are two expandable sections: 'Certificate & Key Meta Information' and 'Card Verifiable Certificate (CVC) Information'. Below these is a section for 'Configure the associated Internal Registration Authority Db user.' with a 'Configure' button. At the bottom, there is a 'Certificate actions' section with four buttons: 'Enroll', 'Revoke', 'Revoke and enroll', and 'Remove historical'. A mouse cursor is pointing at the 'Enroll' button.

Seat Name	Seat Common Name	Seat Emailed Certificate password	Seat Mobile Number	Seat Archived	ROCA key detected	Automatically Close Learn-Once Slots	Action
virtualsemarts.com				No	No	Disabled	Edit

Refresh **Remove Seat**

Certificate & Key Meta Information

Card Verifiable Certificate (CVC) Information

Configure the associated Internal Registration Authority Db user.

Configure

Certificate actions

Enroll **Revoke** **Revoke and enroll** **Remove historical**

After clicking the **Enroll**, you will be shown the order status tracking screen. The screen will automatically update once the order gets approved by KeyTalk by accessing the confirmation email and finally once the certificate gets issued by DigiCert. The entire cycle normally takes about less than a minute.

Find Certificates

DigiCert Central DV Certificate Order Status

Order ID:	620268800
Product:	GeoTrust DV SSL
Order Status:	pending
Order Status Changed:	17-01-2024 09:02:11
Order Approved:	yes
Order Approval Date:	17-01-2024 09:02:25
Domains:	virtualsmartcards.com
Approver Email:	development@keytalk.com

The order status is updated automatically.

After the order is automatically approved by KeyTalk and the certificate is issued by DigiCert, the certificate will become available under the seat page of KeyTalk.

Ok

Alternatively, you can track the status of all placed seat orders by clicking on **View Orders** on the seat configuration page.

DigiCert Central DV certificate orders

Order ID	Product	Order Status	Order Status Changed	Order Approved	Order Approval Date	Domains	Approver Email
620268800	GeoTrust DV SSL	issued	17-01-2024 09:02:51	yes	17-01-2024 09:02:25	virtualsmartcards.com	development@keytalk.com

The orders are updated automatically

Ok

Once the certificate gets issued, it will become available for download under the seat page.



Seats

Find Certificates

Find CSRs

Import Certificate Requests

Import Certificate

Batch Import Certificates

Update Seats

Current Certificate details

Subject:	CN=virtualsmartcards.com
Issuer:	C=US/CN=GeoTrust TLS RSA CA G1/O=DigiCert Inc/OU=www.digicert.com
Serial Number:	03f87e9c:a6:7d:8a:a0:69:f9:9c:42:66:3c:82:6b
Subject Alternative Names:	DNS:virtualsmartcards.com
Valid From:	17-01-2024 00:00 (17-01-2024 00:00 GMT)
Valid To:	15-04-2024 23:59 (15-04-2024 23:59 GMT)
Signature Algorithm:	sha256WithRSAEncryption
Subject Key Identifier:	ae3c75a37ab532c4a7a9dd00f9cdcfcc183e1797
Authority Key Identifier:	KeyID: 944fd45d8be4a4e2a680fefdd8f900efa3be0257
Authority Information Access:	Issuer CA URL: http://cacerts.geotrust.com/GeoTrustTLRSACAG1.crt OCSP URL: http://status.geotrust.com/
Public Key:	RSA (4096 bits)
SHA1 Fingerprint:	28247c519f43267be839e3af88485883d14f1887
CRL Distribution Point:	http://cdp.geotrust.com/GeoTrustTLRSACAG1.crl
Revoked:	no
TPM Attested:	no
DigiCert CertCentral Order ID:	620268800

CA trust chain of the Current Certificate

Subject:	C=US/CN=GeoTrust TLS RSA CA G1/O=DigiCert Inc/OU=www.digicert.com
Issuer:	C=US/CN=DigiCert Global Root G2/O=DigiCert Inc/OU=www.digicert.com
Serial Number:	0d07782a133fc6f9a57296e131ffdl:79
Subject Alternative Names:	
Valid From:	02-11-2017 12:23 (02-11-2017 12:23 GMT)
Valid To:	02-11-2027 12:23 (02-11-2027 12:23 GMT)

5.2. Enroll certificate via KeyTalk ACME agent.

You can choose to enroll DigiCert DV domain certificate using one of ACME agents like certbot or Win-ACME. Please refer to *KeyTalkAcmeServer.pdf* for the details.