

KeyTalk ACME server

Last updated: 2 April 2026

Contents

1. Purpose	2
2. Prerequisites	2
3. KeyTalk configuration	3
4. Enrolling standalone certificate with certbot on Ubuntu Linux	6
4.1 Configuration	6
4.2 Certificate enrollment	7
5. Enrolling Apache certificate with certbot on Ubuntu Linux	9
6. Enrolling certificate for Nginx on Rocky Linux using certbot	10
6.1. Configure Nginx	10
6.2 Install certbot.	10
6.3 Enroll certificate.	10
7. Enrolling certificate for Apache on RHEL 9 using certbot	12
7.1. Configure Apache	12
7.2. Install certbot and enable SSL on Apache	13
7.3. Enroll certificate	13
7.4. Configure Apache and certbot for offline use	14
8. Enrolling certificate using win-acme.	17
9. Enrolling DigiCert DV certificates	18
10. Troubleshooting	19

1. Purpose

This manual outlines the steps to configure KeyTalk to function as ACME server to enroll SSL certificates.

2. Prerequisites

- KeyTalk server v7.6.9 and higher
- certbot or WinACME ACME agent

3. KeyTalk configuration

- Navigate to *Templates > CSR Matching Rules* and or set subject CSR matching rule to “none”. Alternatively, you can set default certificate TEMPLATE subject attributes to empty values.
- Uncheck “use seat name as initial default for certificate CN” and check “use the first entry of SAN DNS as initial default for certificate CN”. Reason: ACME agents often submits CSR with empty CN, which cannot be used as KeyTalk seat name.

Signer:	KeyTalk - Primary Signing CA
Key Size (bits):	2048
Match OUs of CSR and imported certificate: ⓘ	☒
Require email in SAN: ⓘ	☐
Add CN to SAN DNS: ⓘ	☐
Subject CN:	Certificate subject CN is filled from: - bound Registration Authority overwrite, when defined - otherwise from seat CN, when not empty - otherwise from seat name, when the below checkbox is selected - otherwise from the first entry of SAN DNS, when defined and the below checkbox is selected - otherwise CN stays empty ☐ use seat name as initial default for certificate CN ☒ use the first entry of SAN DNS as initial default for certificate CN
Subject Country:	
Subject State:	State
Subject City/Locality:	City or locality
Subject Organization:	Organization name
Subject Organizational Unit:	Organization unit name
Subject Email:	user@example.com

Enable ACME for the above configured TEMPLATE:

**keytalk**

ACME

≡

Templates

Configure

Tenants

Mobile Device Management

Email Disclaimers

Generic SCEP

Intune SCEP

ACME

Configure certificate enrollment using ACME

Select Template: acme-service

Enable certificate enrollment via ACME: ☒

URL for ACME Agent: ⓘ <https://demo.keytalkdemo.com/acme/directory?keytalk-template-name=acme-service>

Ok

Make sure your SSL domain is resolvable by KeyTalk.

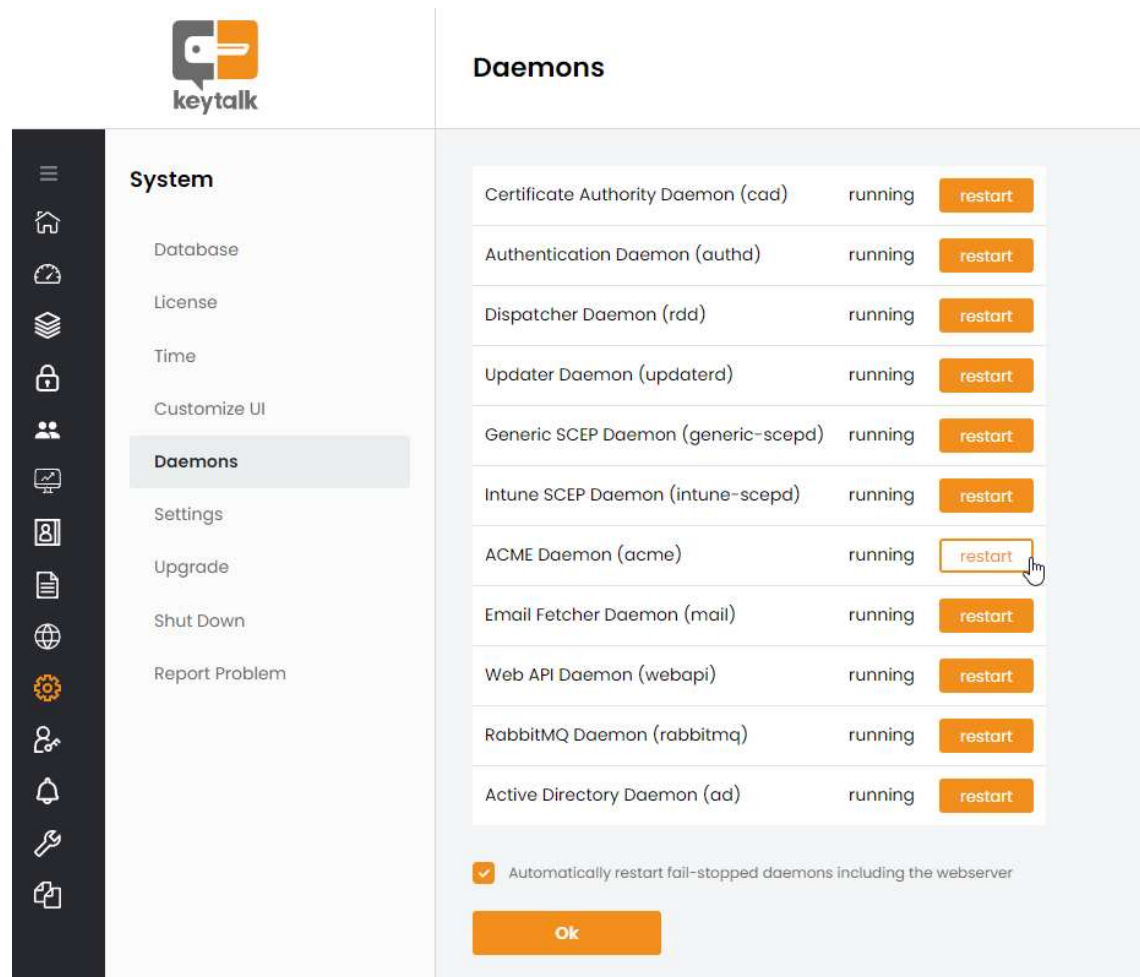
The screenshot shows the 'Configure Local DNS Lookup Database' dialog in the KeyTalk Network configuration interface. The dialog contains a table with columns for IP address, Host name, Aliases, and a Ping button. The entry for 'acmetest.keytalk.com' is highlighted with a red circle and labeled 'REACHABLE'.

IP address	Host name	Aliases	Ping
127.0.0.1	localhost		Ping
127.0.1.1	keytalk		Ping
::1	ip6-localhost	ip6-loopback	Ping
fe00::0	ip6-localnet		Ping
ff00::0	ip6-mcastprefix		Ping
ff02::1	ip6-allnodes		Ping
ff02::2	ip6-allrouters		Ping
10.100.0.209	keytalk-docker.test	kt-docker	Ping
10.100.0.5	dc01-dev.keytalkdemo.io		Ping
10.100.0.6	dc02-dev.keytalkdemo.io		Ping
192.168.70.134	acmetest.keytalk.com		Ping REACHABLE

For each host, a single line should be present with the following information:
IP address, host name and optional one or more aliases.

Buttons: Add, Ok

Should you have made any changes to KeyTalk DNS configuration, you must restart ACME daemon:



keytalk

Daemons

Certificate Authority Daemon (cad)	running	restart
Authentication Daemon (authd)	running	restart
Dispatcher Daemon (rdd)	running	restart
Updater Daemon (updaterd)	running	restart
Generic SCEP Daemon (generic-scep)	running	restart
Intune SCEP Daemon (intune-scep)	running	restart
ACME Daemon (acme)	running	restart
Email Fetcher Daemon (mail)	running	restart
Web API Daemon (webapi)	running	restart
RabbitMQ Daemon (rabbitmq)	running	restart
Active Directory Daemon (ad)	running	restart

☒ Automatically restart fail-stopped daemons including the webserver

Ok

Furthermore, for the sake of simplicity, we also assume that:

- the configured TEMPLATE is bound to the Internal RA;
- the configured TEMPLATE allows registering new seats;
- there is initially no seat and no RA entry for *acmetest.keytalk.com*

4. Enrolling standalone certificate with certbot on Ubuntu Linux using certbot

4.1 Configuration

Install certbot:

```
sudo snap install --classic certbot
```

In order to prove to the ACME server that you have full control over the host requesting the SSL certificate, make sure the host's inbound port 80 is accessible from KeyTalk server (i.e. routable and is not firewalled) and is not occupied by any software (webserver). Stop any webserver using port 80 if applicable, e.g.:

```
sudo systemctl stop apache2
```

Optionally check KeyTalk ACME server is accessible and is running by requesting the directory.

```
curl --silent http://<keytalk-server>/acme/directory | python -m json.tool  
curl --silent https://<keytalk-server>/acme/directory | python -m json.tool
```

Notice that you can use either HTTPS or plain HTTP connection to access KeyTalk ACME server. The former should only be used for test purposes.

You should get back something like:

```
{  
  "newAuthz": "https://<keytalk-server>/acme/new-authz",  
  "newNonce": "https://<keytalk-server>/acme/newnonce",  
  "newAccount": "https://<keytalk-server>/acme/newaccount",  
  "newOrder": "https://<keytalk-server>/acme/neworders",  
  "revokeCert": "https://<keytalk-server>/acme/revokecert",  
  "keyChange": "https://<keytalk-server>/acme/key-change",  
  "renewalInfo": "https://<keytalk-server>/acme/renewal-info",  
  "1324316c8d5d4aa088c1a7b145ee8310":  
    "https://community.letsencrypt.org/t/adding-random-entries-to-the-directory/33417"  
}
```

4.2 Certificate enrollment

Go to the system with the configured certbot.

```
sudo certbot certonly -d acmetest.keytalk.com --server http://<keytalk-server>/acme/directory?keytalk-template-name=<keytalk-acme-template-name>
```

- Specify the name of the TEMPLATE you enabled ACME for on KeyTalk server. You can omit the `keytalk-template-name` parameter in the URL when the only one TEMPLATE is configured for ACME on the server.
- The use of plain `http://` for KeyTalk ACME server URL is for testing purposes only. Make sure to use `https://` in production after setting up SSL trust between the agent and the server.

Choose “*run local HTTP server*” (option 1) to authenticate against ACME server followed by your email address.

If everything goes well, you should receive an SSL certificate back:

```
...
Requesting a certificate for acmetest.keytalk.com

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/acmetest.keytalk.com/fullchain.pem
Key is saved at:        /etc/letsencrypt/live/acmetest.keytalk.com/privkey.pem
This certificate expires on 2023-10-03.
...
```

Feel free to check the received certificate:

```
sudo openssl x509 -noout -text -in
/etc/letsencrypt/live/acmetest.keytalk.com/fullchain.pem
```

```
keytalk@keytalk:~$ sudo openssl x509 -noout -text -in /etc/letsencrypt/live/acmetest.keytalk.com/fullchain.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            56:30:7b:a1:88:e0:49:c3:84:e3:71:84:f8:34:ac:53
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: emailAddress = info@keytalk.com, C = NL, O = KeyTalk IT Security, OU = Factory Default, CN = KeyTalk Demo Signing CA
        Validity
            Not Before: Sep 18 07:23:52 2023 GMT
            Not After : Oct  3 08:23:52 2023 GMT
        Subject:
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
            Public-Key: (256 bit)
            pub:
                04:bb:ea:8b:ce:fa:eb:df:b7:25:a8:0b:26:06:d0:
                a2:02:6c:93:91:6d:23:36:54:f1:43:c1:21:3e:0d:
                d3:f8:8b:cd:7c:81:1a:82:98:e2:b7:81:df:5c:7a:
                de:87:01:ee:15:ed:47:e3:e8:a2:8b:d2:ea:bl:17:
                ed:a3:ec:cb:f0
            ASN1 OID: prime256v1
            NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                60:DB:42:1B:63:93:27:60:C1:3F:9F:6E:97:FE:A3:7D:EF:7C:A7:DF:0B:BF:01:BE:EC:01:54:FB:D8:92:00:B8
            X509v3 Authority Key Identifier:
                0.
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
```


5. Enrolling Apache certificate with certbot on Ubuntu Linux

The process is similar to enrolling a standalone certificate. Below we outline the major points only, please refer to the above section for details.

Install and configure Apache:

```
sudo apt install -y apache2

if ! sudo a2query -m ssl; then \
    sudo a2enmod ssl; \
    sudo a2ensite default-ssl; \
    sudo service apache2 restart; \
fi
```

Install certbot:

```
sudo snap install --classic certbot
```

or when using apt:

```
sudo apt -y install certbot python3-certbot-apache
```

Enroll SSL certificate for Apache:

```
sudo certbot --apache -d acmetest.keytalk.com --server http://<keytalk-  
server>/acme/directory?keytalk-template-name=<keytalk-acme-template-name>
```

Point your browser to <https://acmetest.keytalk.com> to test the certificate has been successfully installed.

6. Enrolling certificate for Nginx on Rocky Linux using certbot.

This section outlines the steps to enroll SSL certificate for Nginx with certbot on Rocky Linux 9.

6.1. Configure Nginx

Install and configure NGINX. Choose to skip this section if you already have a configured Nginx installation.

```
sudo dnf install -y nginx
```

Create `/etc/nginx/conf.d/acmetest.keytalk.com.conf` to contain at least the following:

```
server {  
    server_name  acmetest.keytalk.com;  
}
```

Start Nginx:

```
sudo systemctl enable nginx  
sudo systemctl start nginx
```

Adjust firewall:

```
sudo firewall-cmd --permanent --add-service=http  
sudo firewall-cmd -reload
```

6.2 Install certbot.

```
sudo dnf install -y epel-release  
sudo dnf install -y certbot python3-certbot-nginx
```

6.3 Enroll certificate.

Configure KeyTalk ACME server as described in [Section 3](#).

Make sure your server (`acmetest.keytalk.com`) is resolvable to the same IP for KeyTalk server and for the server itself.

Check KeyTalk ACME server is accessible and is running by requesting the directory.

```
curl --silent http://<keytalk-server>/acme/directory | python -m json.tool
curl --silent https://<keytalk-server>/acme/directory | python -m json.tool
```

You can use either HTTPS or plain HTTP connection to access KeyTalk ACME server. The former should only be used for test purposes.

Enroll Nginx SSL certificate:

```
sudo certbot --nginx -d acmetest.keytalk.com --server http://<keytalk-  
server>/acme/directory?keytalk-template-name=<keytalk-acme-template-name>
```

- Specify the name of the TEMPLATE you enabled ACME for on KeyTalk server. You can omit the `keytalk-template-name` parameter in the URL when the only one TEMPLATE is configured for ACME on the server.
- The use of plain `http://` for KeyTalk ACME server URL is for testing purposes only. Make sure to use `https://` in production after setting up SSL trust between the agent and the server.

Choose option 1 “Nginx Web Server plugin (nginx)”

If everything goes well, an SSL certificate should be received and Nginx should be configured with it:

```
...
Requesting a certificate for acmetest.keytalk.com

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/acmetest.keytalk.com/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/acmetest.keytalk.com/privkey.pem
This certificate expires on 2024-05-15.
These files will be updated when the certificate renews.
...

Deploying certificate
Successfully deployed certificate for acmetest.keytalk.com to
/etc/nginx/conf.d/acmetest.keytalk.com.conf
Your existing certificate has been successfully renewed, and the new certificate
has been installed....
```

Point your browser to <https://acmetest.keytalk.com> to test the certificate has been successfully installed.

7. Enrolling certificate for Apache on RHEL 9 using certbot.

This section outlines the steps to enroll SSL certificate for Apache with certbot on Red Hat Enterprise Linux 9.5.

7.1. Configure Apache

Install and configure Apache to serve plain HTTP first. Choose to skip this section if you already have configured Apache installation.

```
sudo dnf install -y httpd
```

Open TCP port 80 on firewall:

```
sudo firewall-cmd --permanent --add-port=80/tcp
sudo firewall-cmd --reload
```

Create `/etc/httpd/conf.d/acmetest.keytalk.com.conf` to contain at least the following:

```
<VirtualHost *:80>
    DocumentRoot "/var/www/acmetest.keytalk.com/"
    ServerName acmetest.keytalk.com
    # ServerAlias www.acmetest.keytalk.com
    CustomLog /var/log/httpd/acmetest.keytalk.com.conf_access.log combined
    ErrorLog /var/log/httpd/acmetest.keytalk.com.conf_error.log
</VirtualHost>
```

Create test page

```
sudo mkdir /var/www/acmetest.keytalk.com/
sudo chown -R $USER:$USER /var/www/acmetest.keytalk.com/
echo "Hello from ACME test!" > /var/www/acmetest.keytalk.com/index.html
```

Start *httpd*:

```
sudo systemctl restart httpd
```

Point your browser to <http://acmetest.keytalk.com> to test Apache is up and running on port 80.

7.2. Install certbot and enable SSL on Apache

Certbot is available from EPEL repository, enable it first

```
sudo subscription-manager repos --enable codeready-builder-for-rhel-9-$(arch)-rpms
sudo dnf install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
sudo dnf install -y mod_ssl certbot python3-certbot-apache
```

Open TCP port 443 on firewall:

```
sudo firewall-cmd --permanent --add-port=443/tcp
sudo firewall-cmd --reload
```

Restart *httpd* service and enable auto-start:

```
sudo systemctl restart httpd
sudo systemctl enable --now httpd
```

7.3. Enroll certificate

Configure KeyTalk ACME server as described in the [Section 3](#).

Make sure your server (acmetest.keytalk.com) is resolvable to the same IP for KeyTalk server and for the server itself.

Check KeyTalk ACME server is accessible and is running by requesting the directory.

```
curl --silent http://<keytalk-server>/acme/directory | python -m json.tool
curl --silent https://<keytalk-server>/acme/directory | python -m json.tool
```

Enroll Apache SSL certificate:

```
sudo certbot --apache -d acmetest.keytalk.com --server http://<keytalk-server>/acme/directory?keytalk-template-name=<keytalk-acme-template-name>
```

- Specify the name of the TEMPLATE you enabled ACME for on KeyTalk server. You can omit the `keytalk-template-name` parameter in the URL when the only one TEMPLATE is configured for ACME on the server.

- The use of plain `http://` for KeyTalk ACME server URL is for testing purposes only. Make sure to use `https://` in production after setting up SSL trust between the agent and the server.

If everything goes well, an SSL certificate should be received and certbot should automatically install it to Apache:

```
keytalk@localhost ~]$ sudo certbot --apache --key-type rsa -d acmetest.keytalk.com --server http://192.168.206.128/acme/directory
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
(Enter 'c' to cancel): a.korostelev@keytalk.com

-----
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
-----
(Y)es/(N)o: N
Account registered.
Requesting a certificate for acmetest.keytalk.com

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/acmetest.keytalk.com/fullchain.pem
Key is saved at: /etc/letsencrypt/live/acmetest.keytalk.com/privkey.pem
This certificate expires on 2025-02-12.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

Deploying certificate
Successfully deployed certificate for acmetest.keytalk.com to /etc/httpd/conf.d/acmetest.keytalk.com-le-ssl.conf

Congratulations! You have successfully enabled HTTPS on https://acmetest.keytalk.com

-----
If you like Certbot, please consider supporting our work by:
* Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
* Donating to EFF: https://eff.org/donate-le
-----
```

Point your browser to <https://acmetest.keytalk.com> to test the certificate has been successfully installed.

7.4. Configure Apache and certbot for offline use

This section outlines the above steps of configuring Apache and certbot on RHEL 9.5 having no internet connection to the outside (offline).

Download the following packages from

https://access.redhat.com/downloads/content/479/ver=/rhel---9/9.5/x86_64/packages :

- [httpd](#)
- [httpd-core](#)
- [httpd-filesystem](#)
- [httpd-tools](#)
- [mailcap](#)
- [apr](#)
- [apr-util](#)
- [apr-util-bdb](#)
- [redhat-logos-httpd](#)

Transfer the downloaded packages to your RHEL server and install:

```
sudo dnf install -y ~/packages/*.rpm
```

Perform basic configuration of Apache as described in this [section](#)

Install Apache mod_ssl module. Download the following packages from https://access.redhat.com/downloads/content/479/ver=/rhel---9/9.5/x86_64/packages :

- [mod_ssl](#)
- [sscg](#)

Transfer the downloaded packages to your RHEL server and install:

```
sudo dnf install -y ~/packages/*.rpm
```

Open TCP port 443 on firewall:

```
sudo firewall-cmd --permanent --add-port=443/tcp  
sudo firewall-cmd --reload
```

Install certbot with Apache bindings.

Download the following packages from

https://dl.fedoraproject.org/pub/epel/9/Everything/x86_64/Packages :

- [certbot](#)
- [python3-certbot](#)
- [python3-acme](#)
- [python3-certbot-apache](#)
- [python3-josepy](#)
- [python3-pyrfc3339](#)
- [python3-configargparse](#)
- [python3-parsedatetime](#)

Download the following packages from

https://access.redhat.com/downloads/content/479/ver=/rhel---9/9.5/x86_64/packages :

- [augeas-libs](#)
- [python3-augeas](#)
- [fontawesome-fonts](#)
- [python3-cryptography](#)
- [python3-pyOpenSSL](#)
- [python3-pytz](#)
- [python3-configobj](#)

- [python3-importlib-metadata](#)
- [python3-pycparser](#)
- [python3-cffi](#)
- [python3-zipp](#)
- [python3-ply](#)

Transfer the downloaded packages to your RHEL server and install:

```
sudo dnf install -y ~/packages/*.rpm
```

Restart *httpd* service and enable auto-start:

```
sudo systemctl restart httpd  
sudo systemctl enable --now httpd
```

Enroll SSL certificate using certbot as described in the [the section above](#)

8. Enrolling certificate using win-acme.

Download Win-ACME from <https://www.win-acme.com/>. Make sure port 80 is available for inbound TCP connections and is not occupied by any application.

Create a directory where the resulted certificates in PEM format will be stored. E.g. C:\FetchedCerts.

Enroll certificate:

```
> wacs.exe --baseuri http://<keytalk-server>/acme/directory?keytalk-template-name=<keytalk-acme-template-name> --source manual --host acmetest.keytalk.com --store pemfiles --pemfilespace C:\FetchedCerts
```

- Specify the name of the TEMPLATE you enabled ACME for on KeyTalk server. You can omit the `keytalk-template-name` parameter in the URL when the only one TEMPLATE is configured for ACME on the server.
- The use of plain `http://` for KeyTalk ACME server URL is for testing purposes only. Make sure to use `https://` in production after setting up SSL trust between the agent and the server.

The output:

```
...
Connecting to https://keytalk.keytalk.com/acme/directory...
...
[windowsapachedemo.keytalk.com] Authorizing using http-01 validation (SelfHosting)
[windowsapachedemo.keytalk.com] Authorization result: valid
Downloading certificate [Manual] acmetest.keytalk.com
Store with PemFiles...
Exporting .pem files to C:\FetchedCerts
...
Certificate [Manual] acmetest.keytalk.com created
```

9. Enrolling DigiCert DV certificates

KeyTalk ACME server can also be used to enroll certificates which are issued immediately as well as DigiCert DV certificates which require an additional step to approve domain. KeyTalk ACME server supports automated approval of DigiCert DV certificates configured with email domain validation.

The only extra configuration to enable enrolling DV certificates will be mailbox settings. Please refer to the dedicated document [KeyTalkEnrollDigiCertDvCerts.pdf](#) for more detail.

10.Troubleshooting

Check KeyTalk logs in the following order:

- ACME logs
- RDD logs
- CAD logs
- AUTHD logs