KMIP for key management

- Follow the guide to install KMIP on a Synology NAS server and client

Certificates

1. The default, out-of-the-box self-signed Synology certificate will fail on DSM 7.4 and later, which hardened the certificate requirements. You will generate matching certificates from an official Synology script, which will be installed alongside the default certificates, and are valid for 10 years. These certificates also work for Synology clients connecting to a KMIP Server (PyKMIP) not hosted on a synology NAS.
2. Login to your NAS on the command line with SSH and elevate to root
3. Download Synology's official KMIP certificate script:

   ```
   wget
   supweb.synology.com/support_web/kc_tool/how_to_gen_cert_for_kmip_servic
   es/gen_kmip_certs.sh
   ```

4. Run the script as root:

   ```
   bash gen_kmip_certs.sh kmip_certs
   ```

   The second parameter *kmip_certs* is the name of a shared folder the script will create to store the certificates

5. Upload the generated scripts in `/volume1/kmip_certs` to your local computer you use to access your DSMs through your web browser, after which you can remove the shared folder and it's content
6. The script will generate the following certificates:

   ```
   ca-key.pem
   ca.pem
   client-fullchain.pem
   client-key.pem
   client.pem
   server-fullchain.pem
   server-key.pem
   server.pem
   ```

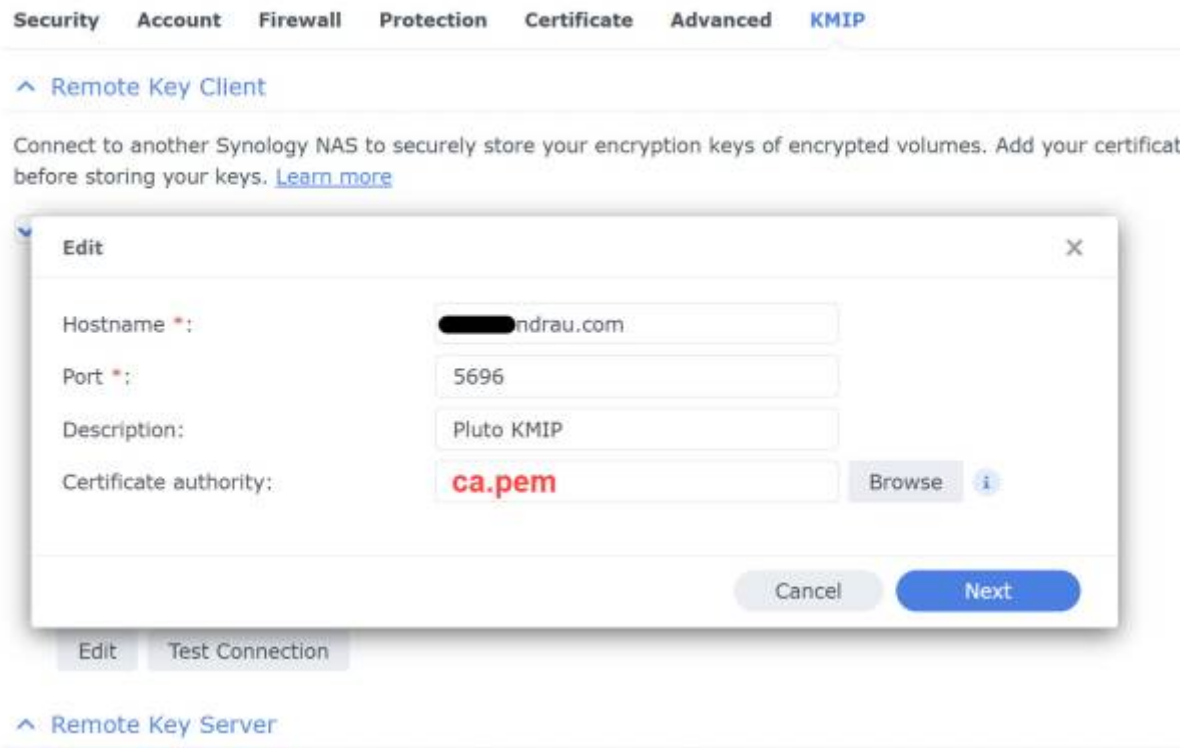
DSM as Server

1. go to *Control Panel > Security > Certificate*
2. Click *Add*, choose *Import Certificate*, and upload:
   - Private key: `server-key.pem`
   - Certificate: `server.pem`
   - Leave Intermediate certificate empty

3. Click Settings (in the Certificate tab), find the *KMIP dropdown menu*, select this new server certificate, and click OK
4. Go to *Control Panel > Security > KMIP* and select *Set as remote key server*
5. Under *Manage Client Connection*, click *Manage > Add*
6. Upload the client files you generated:
    - Client certificate: `client.pem`
    - Certificate authority: `ca.pem`
7. Add a port forward for port 5696 to your server NAS

DSM as Client

1. go to *Control Panel > Security > Certificate*
2. Click *Add*, choose *Import Certificate*, and upload:
    - Private key: `client-key.pem`
    - Certificate: `client.pem`
    - Leave Intermediate certificate empty
3. Click Settings (in the Certificate tab), find the *KMIP dropdown menu*, select this new client certificate, and click OK
4. Go to *Control Panel > Security > KMIP* and select *Set as remote key client*
5. Enter the server's IP address and port 5696
6. Upload the certificate authority file `ca.pem` and click **Next**. Wait until you see the connection is successful.
7. Now you need to go to **Storage Manager –> Storage** and click *Global Settings*. Scroll down to **Encryption Key Vault** and click *Reset* (important!) to make the switch to the KMIP Server permanent and move the encryption keys.
8. Go to **Control Panel –> Security –> KMIP**, check *Set as remote key client*, and make sure your KMIP Server with uploaded Synology certificates is running (either Synology DSM, or PyKMIP on Debian, or a commercial KMIP Server)
9. Enter the following credentials. Note that every time you edit the connection you need to upload the *Certificate Authority* file (**ca.pem**).



Rescue

- Read Rescue an encrypted volume to prepare the rescue if your KMIP Server get's unaccessible.

Links

- KMIP Protocol Explained: Key Management Interoperability in Practice
- Updated security and certificate guidelines for DSM 7.4
- Setting up a KMIP server with DSM 7.4
- Random Password Generator

From:
https://wiki.condrau.com/ - **Bernard's Wiki**

Permanent link:
https://wiki.condrau.com/syno:dsm7kmip

Last update: **2026/09/21 23:53**