

# Power Week 2025

18 - 19 - 20 novembre 2025

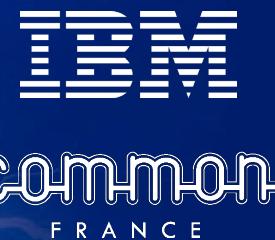
IBM Innovation Studio Paris

## S71 – APIs RSE pour gérer les certificats TLS

20 novembre 11:15 - 12:15

Damien Trijasson  
Gaia-Volubis  
[damien.trijasson@gaiavolubis.com](mailto:damien.trijasson@gaiavolubis.com)

Nathanaël Bonnet  
Gaia-Volubis  
[nathanael.bonnet@gaiavolubis.com](mailto:nathanael.bonnet@gaiavolubis.com)



# Présentation

## Nathanaël BONNET

IBM i depuis 1999  
Expert IBM i



## Damien Trijasson

IBM i depuis 1999  
Expert IBM i



## GAIA / VOLUBIS

Formation (débutant, perfectionnement)  
Expertise IBM i  
Centre de Services



Power Week

18 -19 - 20 novembre  
2025

# API RSE - Rappel

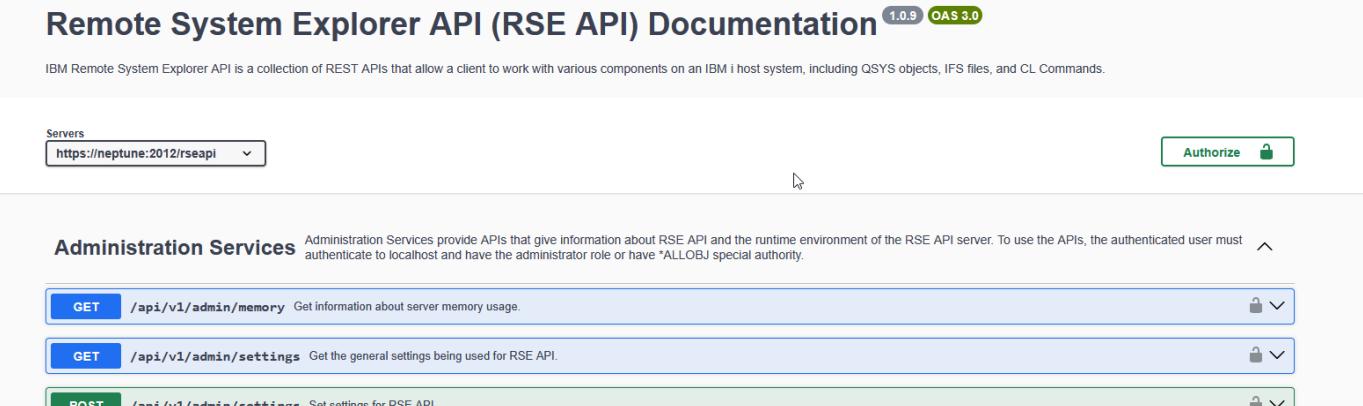
**IBM**  
common  
FRANCE

IBM

# Où ?

- Depuis un navigateur :
  - En consultation sur le port 2011 : <http://host:2011/rseapi/>
  - En gestion sur le port 2012 : <https://host:2012/rseapi/> Ou plus direct <https://neptune:2012/openapi/ui/>

- Interface Open liberty de type swaggerUI



Remote System Explorer API (RSE API) Documentation 1.0.0 OAS 3.0

IBM Remote System Explorer API is a collection of REST APIs that allow a client to work with various components on an IBM i host system, including QSYS objects, IFS files, and CL Commands.

Servers  Authorize

**Administration Services** Administration Services provide APIs that give information about RSE API and the runtime environment of the RSE API server. To use the APIs, the authenticated user must authenticate to localhost and have the administrator role or have \*ALLOBJ special authority.

**GET /api/v1/admin/memory** Get information about server memory usage. (locked)

**GET /api/v1/admin/settings** Get the general settings being used for RSE API. (locked)

**POST /api/v1/admin/settings** Set settings for RSE API. (locked)

# Comment ?

- Serveur admin5 démarré

ADMIN4	QWEBADMIN	BCI	0,2	JVM-/QIBM/Prod	THDW
ADMIN5	QLWISVR	BCI	0,0	JVM-/QIBM/Prod	THDW
CGIDEV2APA	QTMHHTTP	BCH	0,0	PGM-QZHBMAIN	SIGW

- Activer TLS sur le serveur admin5

Server: Admin5 - V8.5 (int app svr)

Admin5 > Properties

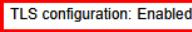
**Properties**

Display and manage the properties of the application server.

**Application Server**

Property information for the integrated Web application server 

Version: 8.5  
Subsystem: QHTTPSVR  
Job name: 194790/QLWISVR/ADMIN5  
User ID: QLWISVR  
Instance path: /qibm/usr/.../admin5/wlp/usr/servers/admin5  
Disable server:  

TLS configuration:  

 Admin5	V8.5 (int app svr)	 Running	10188
			*:2011
			*:2012

# Quoi ?

- 8 services

Servers  ▾

**Administration Services** Administration Services provide APIs that give information about RSE API and the runtime environment. To use these APIs, you must authenticate to localhost and have the administrator role or have \*ALLOBJ special authority.

**CL Command Services** CL Command Services provide APIs for running CL commands.

**IFS Services** Integrated File System (IFS) Services provide APIs for accessing objects in a way that is like personal computer and UNIX commands. You can read from files, write to files, and copy files.

**QSYS Services** QSYS Services provide APIs for accessing QSYS objects.

**SQL Services** SQL Services provide APIs associated with performing SQL operations.

**Security Services** Security Services provide APIs relating to security, such as the management of digital certificates and the retrieval of session keys. All the digital certificate management APIs require the Digital Certificate Manager, option 34 of the IBM i licensed program. You must have the \*ALLOBJ and \*SECADM special authorities.

**Server Information Services** Server Information Services provide APIs about RSE API.

**Session Services** Session Services provide APIs for authenticating a user and managing sessions that are tied to an authenticated user. Once authenticated, a bearer token is returned and must be submitted on requests when invoking protected APIs.

# Quoi ?

- Récupération d'un token

**Session Services** Session Services provide APIs for authenticating a user and managing sessions that are triggered. Once authenticated, a bearer token is returned and must be submitted on requests.

GET	/api/v1/session	Get information about the session.
PUT	/api/v1/session	Refresh session settings.
POST	/api/v1/session	Authenticate with user credentials and return an embedded token.
DELETE	/api/v1/session	Logout, releasing resources tied to the session.

- Limitation des accès - paramétrage

**Administration Services** Administration Services provide APIs that give information about RSE API access. Only users that are authenticated to localhost and have the administrator role or have \*ALLOE

GET	/api/v1/admin/memory	Get information about server memory usage.
GET	/api/v1/admin/settings	Get the general settings being used for RSE API.
POST	/api/v1/admin/settings	Set settings for RSE API.
DELETE	/api/v1/admin/settings	Reset settings for RSE API.

- Gestion des certificats

Security Services

All the certificates must have

Power Week

18 -19 - 20 novembre  
2025

# Gestion des certificats TLS

**IBM**  
common  
FRANCE

IBM

# Description de l'API

- <https://itest10.gaia.lan:2012/openapi/ui/>

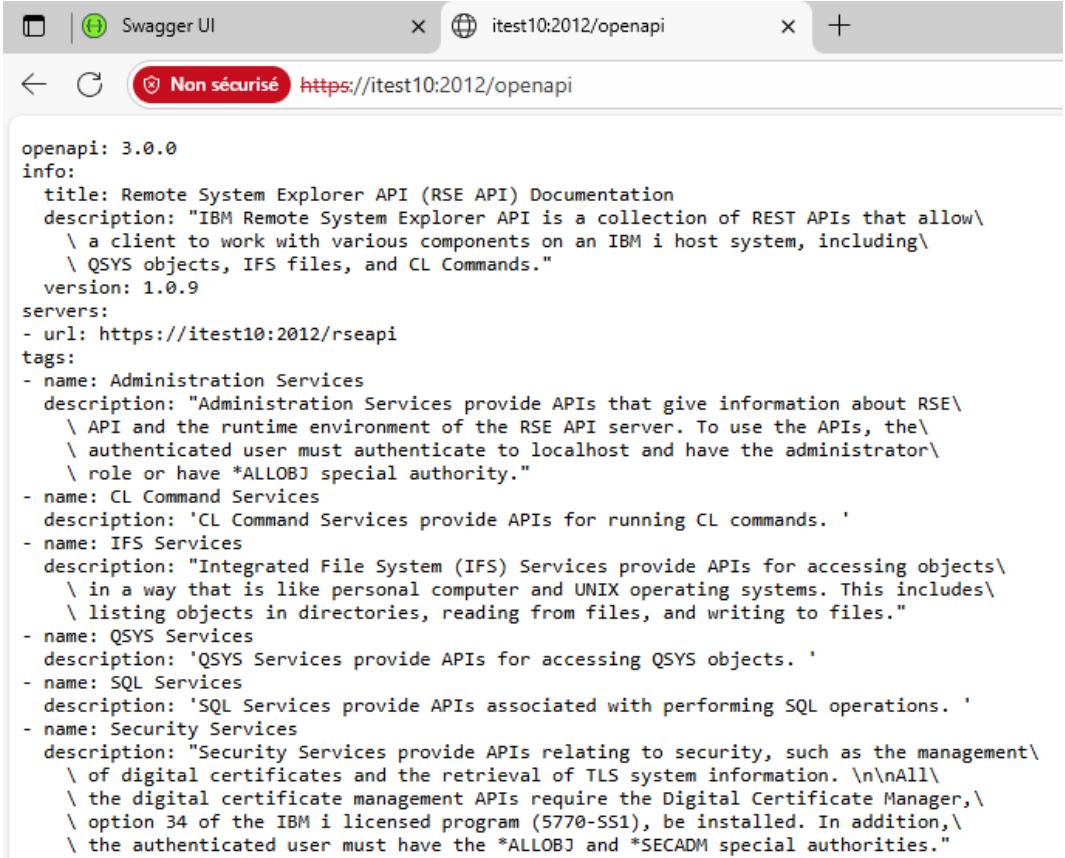
Security Services provide APIs relating to security, such as the management of digital certificates and the retrieval of TLS system information.

All the digital certificate management APIs require the Digital Certificate Manager, option 34 of the IBM i licensed program (5770-SS1), be installed. In addition, the authenticated user must have the \*ALLOBJ and \*SECADM special authorities.

<b>POST</b>	<code>/api/v1/security/dcm/cert/delete</code>	Delete a digital certificate.		
<b>GET</b>	<code>/api/v1/security/tls</code>	Retrieve system transport layer security (TLS) attributes.		
<b>POST</b>	<code>/api/v1/security/dcm/cert/export</code>	Export a digital certificate.		
<b>POST</b>	<code>/api/v1/security/dcm/cert/info</code>	Get detailed certificate information.		
<b>POST</b>	<code>/api/v1/security/dcm/appdef/associate</code>	Associate digital certificates to an application definition.		
<b>GET</b>	<code>/api/v1/security/dcm/appdef/list</code>	List application definitions.		
<b>POST</b>	<code>/api/v1/security/dcm/appdef/untrust</code>	Remove a certificate authority (CA) digital certificate from the application definition CA trust list.		
<b>POST</b>	<code>/api/v1/security/dcm/appdef/disassociate</code>	Disassociate digital certificates from an application definition.		
<b>POST</b>	<code>/api/v1/security/dcm/cert/list</code>	Retrieve a list of certificates in a certificate store.		
<b>POST</b>	<code>/api/v1/security/dcm/certstore/changepassword</code>	Change digital certificate store password.		
<b>POST</b>	<code>/api/v1/security/dcm/appdef/trust</code>	Add certificate authority (CA) digital certificate to the application definition CA trust list.		
<b>POST</b>	<code>/api/v1/security/dcm/cert/import</code>	Import a digital certificate.		
<b>GET</b>	<code>/api/v1/security/tls/stats</code>	Retrieve system transport layer security (TLS) statistics.		

# Importation dans Postman

- itest10:2012/openapi



```
openapi: 3.0.0
info:
  title: Remote System Explorer API (RSE API) Documentation
  description: "IBM Remote System Explorer API is a collection of REST APIs that allow\
    \ a client to work with various components on an IBM i host system, including\
    \ QSYS objects, IFS files, and CL Commands."
  version: 1.0.9
servers:
- url: https://itest10:2012/rseapi
tags:
- name: Administration Services
  description: "Administration Services provide APIs that give information about RSE\
    \ API and the runtime environment of the RSE API server. To use the APIs, the\
    \ authenticated user must authenticate to localhost and have the administrator\
    \ role or have *ALLOBJ special authority."
- name: CL Command Services
  description: 'CL Command Services provide APIs for running CL commands. '
- name: IFS Services
  description: "Integrated File System (IFS) Services provide APIs for accessing objects\
    \ in a way that is like personal computer and UNIX operating systems. This includes\
    \ listing objects in directories, reading from files, and writing to files."
- name: QSYS Services
  description: 'QSYS Services provide APIs for accessing QSYS objects. '
- name: SQL Services
  description: 'SQL Services provide APIs associated with performing SQL operations. '
- name: Security Services
  description: "Security Services provide APIs relating to security, such as the management\
    \ of digital certificates and the retrieval of TLS system information. \n\nAll\
    \ the digital certificate management APIs require the Digital Certificate Manager, \
    \ option 34 of the IBM i licensed program (5770-SS1), be installed. In addition, \
    \ the authenticated user must have the *ALLOBJ and *SECADM special authorities."
```

# Prérequis

- Pour les APIs « Security Service »
  - L'utilisateur doit être
    - \*ALLOBJ + \*SECADM
  - Le mot de passe des magasins de certificat

# Scénario 1

- On a une instance HTTP Apache existante et sécurisée
  - Importer un certificat
  - L'associer à l'instance
  - Redémarrer

# Scénario 1

## ■ Instance

### Display Configuration File

HTTP server: PW25RSE  
Selected file: /www/pw25rse/conf/htpd.conf

```
1 # Configuration originally created by Create HTTP Server wizard on Thu Nov 13 16:48:21 CET 2025
2 LoadModule ibm_ssl_module /QSYS.LIB/QHTTPSVR.LIB/QZSRVSSL.SRVM
3 Listen *:10700
4 Listen *:10701
5 DocumentRoot /www/pw25rse/htdocs
6 TraceEnable Off
7 Options -FollowSymLinks
8 LogFormat "%h %T %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" combined"
9 LogFormat "%{Cookie}n \"%r\" %t" cookie
10 LogFormat "%{User-agent}i" agent
11 LogFormat "%{Referer}i -%{User-Agent}i" referer
12 LogFormat "%h %l %u %t \"%r\" %>s %b" common
13 CustomLog logs/access_log combined
14 LogMaint logs/access_log 7 0
15 LogMaint logs/error_log 7 0
16 SetEnvIf "User-Agent" "Mozilla/2" nokeepalive
17 SetEnvIf "User-Agent" "JDK/1.0" force-response-1.0
18 SetEnvIf "User-Agent" "Java/1.0" force-response-1.0
19 SetEnvIf "User-Agent" "RealPlayer 4.0" force-response-1.0
20 SetEnvIf "User-Agent" "MSIE 4.0b2;" nokeepalive
21 SetEnvIf "User-Agent" "MSIE 4.0b2;" force-response-1.0
22 SetEnv HTTPS_PORT 10701
23 <Directory />
24   Require all denied
25 </Directory>
26 <Directory /www/pw25rse/htdocs>
27   Require all granted
28 </Directory>
29 <VirtualHost *:10701>
30   SSLEngine On
31   SSLAppName QIBM_HTTP_SERVER_PW25RSE
32   SSLProtocolDisable SSLv3 TLSv1 TLSv1.1
33 </VirtualHost>
```

Sample page for the server <https://itest10:10701>

Non sécurisé

## This is th

information on changing this page or serving additional pages using PW25RSE.

ation available on the [HTTP server](#)

Visionneuse de certificats : pw25rse

Général Détails

Émis pour

Nom commun (CN)	pw25rse
Organisation (O)	Gaia
Unité d'organisation (UO)	PW25

Émis par

Nom commun (CN)	itest10.gaia.lan_CERTIFICATE_AUTHORITY
Organisation (O)	IBM Web Administration for i
Unité d'organisation (UO)	<Ne fait pas partie du certificat>

QIBM\_HTTP\_SERVER\_PW25RSE  
Server

Assigned Certificates

- PW25 origine

Trusted Certificate Authorities

- LOCAL\_CERTIFICATE\_AUTHORITY\_78780E12(11)

/20 novembre 2025

# Scénario 1

- Authentification

The screenshot shows a POST request to `/{{baseUrl}}/api/v1/session`. The request body is a JSON object with fields: host, userid, and password. The response status is 201 Created, with a response time of 83 ms and a response size of 263 B. The Authorization header is highlighted with a red box and contains the value `Bearer 3530996e-df1f-4e70-83cd-f471fff33531-6915fd09-3137322e33302e362e323431`.

Key	Value
Authorization	Bearer 3530996e-df1f-4e70-83cd-f471fff33531-6915fd09-3137322e33302e362e323431

# Scénario 1

- Importer un certificat
  - Formats supportés :
    - PKCS12 si contient la clé privée (SERVER/CLIENT)
    - PEM (CRT) ou DER sinon (CA)
  - Dans notre cas, les CA existent, on peut importer directement le certificat

# Scénario 1

POST <https://{{baseUrl}}/api/v1/security/dcm/cert/import>

Docs Params Authorization (1) Headers (11) **Body** Scripts Settings

none  form-data  x-www-form-urlencoded  raw  binary  GraphQL **JSON**

```
1 {  
2   "certStoreType": "CMS",  
3   "certStorePath": "*SYSTEM",  
4   "certStorePassword": "PW25 v2",  
5   "certType": "SERVER_CLIENT",  
6   "certFormat": "PKCS12",  
7   "certAlias": "PW25 v2",  
8   "certDataPassword": "iTest10",  
9   "certData":  
10    "MIIJiwIBAzCCC...  
11    AQMwDQQIqZb2BtAURW...  
12    bfpbX6ohS62GCAF6Hxy...  
13    Hc5v5ojRVee35DN6FVY...  
14    9G39Q9gXWu7D/
```

DCM magasin \*SYSTEM

Alias dans DCM

Mot de passe du certificat

Certificat au format base64

Body Cookies Headers (4) Test Results  204 No Content • 156 ms •

# Scénario 1

- L'associer à l'instance
  - Correspondance avec DCM

POST <https://{{baseUrl}}/api/v1/security/dcm/appdef/associate>

Docs Params Authorization Headers (11) Body Script

none  form-data  x-www-form-urlencoded  raw  binary

```
1 {  
2   "appDefinitionID": "QIBM_HTTP_SERVER_PW25RSE",  
3   "certAliases": ["PW25 v2"]  
4 }
```

View Application Definition

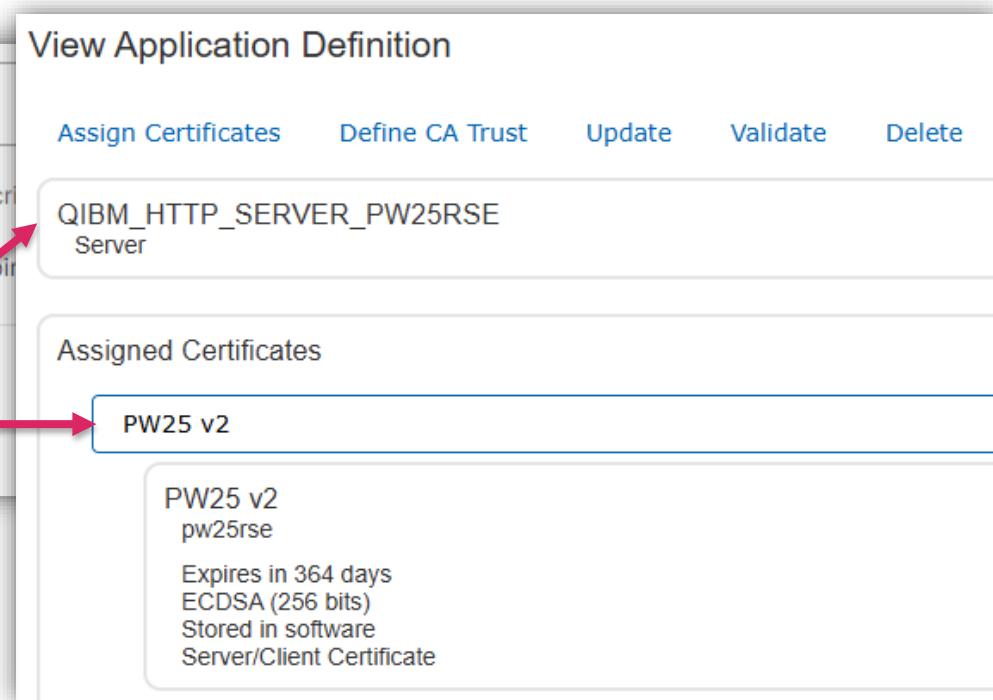
Assign Certificates Define CA Trust Update Validate Delete

QIBM\_HTTP\_SERVER\_PW25RSE  
Server

Assigned Certificates

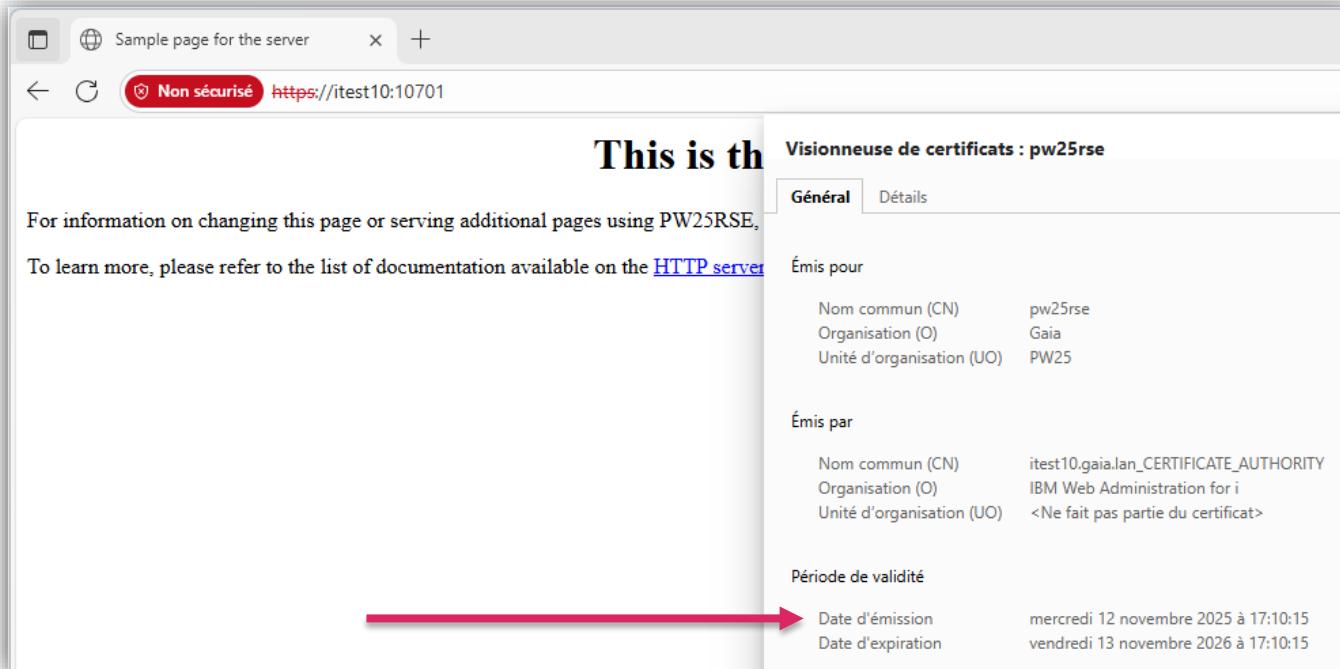
PW25 v2

PW25 v2  
pw25rse  
Expires in 364 days  
ECDSA (256 bits)  
Stored in software  
Server/Client Certificate



# Scénario 1

- Redémarrer
  - Nouveau certificat pris en compte

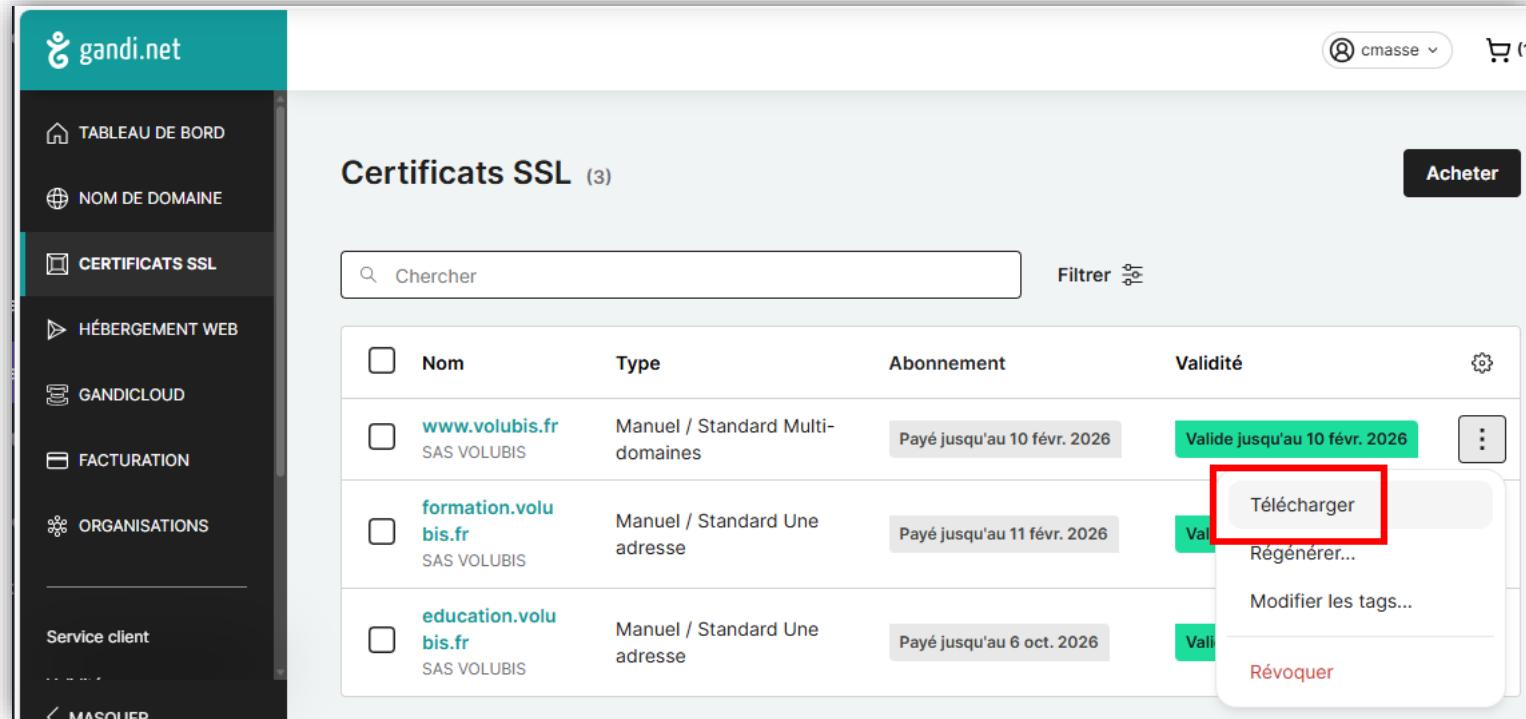


# Scénario 2

- Importer un certificat d'une autorité publique
  - Importer le CA / certificat
  - Dissocier le certificat actuel
  - Associer le certificat importé

# Scénario 2

- Récupérer le certificat + chaîne de certification (CAs)



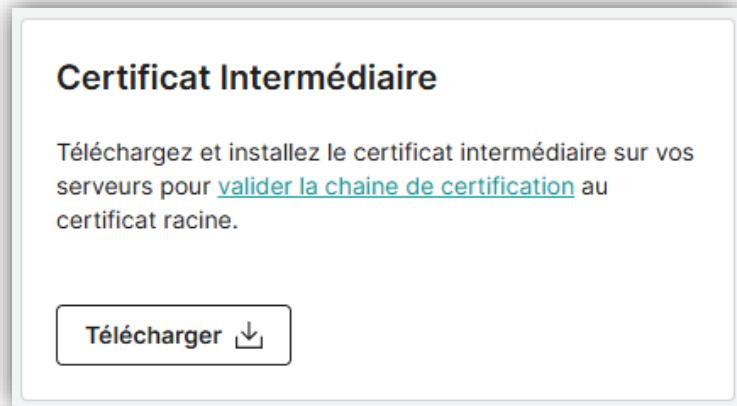
The screenshot shows the gandi.net control panel. The left sidebar includes links for TABLEAU DE BORD, NOM DE DOMAINE, CERTIFICATS SSL (selected), HÉBERGEMENT WEB, GANDICLOUD, FACTURATION, and ORGANISATIONS. The main area is titled "Certificats SSL (3)" and lists three certificates:

Nom	Type	Abonnement	Validité
www.volubis.fr SAS VOLUBIS	Manuel / Standard Multi-domaines	Payé jusqu'au 10 févr. 2026	Validé jusqu'au 10 févr. 2026
formation.volubis.fr SAS VOLUBIS	Manuel / Standard Une adresse	Payé jusqu'au 11 févr. 2026	Validé jusqu'au 11 févr. 2026
education.volubis.fr SAS VOLUBIS	Manuel / Standard Une adresse	Payé jusqu'au 6 oct. 2026	Validé jusqu'au 6 oct. 2026

A context menu is open over the "Validé jusqu'au 10 févr. 2026" button for the "education.volubis.fr" certificate. The menu options are: Télécharger (highlighted with a red box), Régénérer..., Modifier les tags..., and Révoquer.

# Scénario 2

- Récupérer le certificat + chaîne de certification (CAs)
  - Souvent une option pour récupérer les autorités (ici en PEM)



- Il faut pouvoir télécharger avec la clé privée (PKCS12, pfx)
  - Protégé par un mot de passe
  - Contient les CA
  - Peut être considéré comme un magasin

## Scénario 2

- Encoder le certificat en base 64

- On a utilisé

<https://www.base64encode.org/fr/>,  
<https://www.base64encode.net/> ou  
[https://emn178.github.io/online-tools/base64\\_encode.html](https://emn178.github.io/online-tools/base64_encode.html)

- Mais aussi

Filename	<a href="#">volubis.fr.pfx</a>
File size	<b>6368 bytes</b>
Mime type	<b>text/plain</b>
Link	<a href="#">Download output</a>

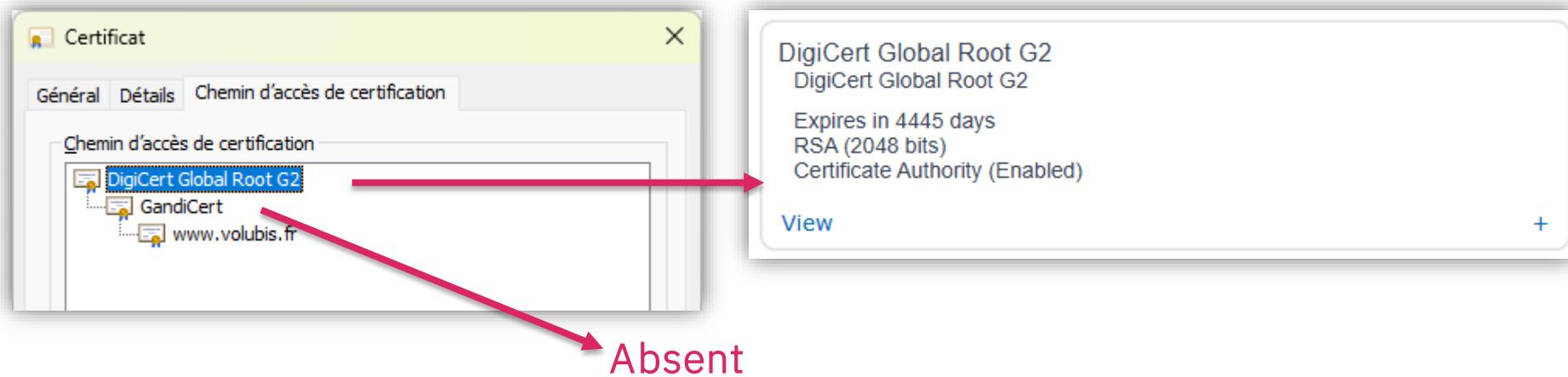
```
SELECT qsys2.base64_encode(line) FROM TABLE(QSYS2.IFS_READ_BINARY(PATH_NAME => '/home/NB/volubis.fr.pfx'));
```

00001

MIISowIBAzCCEmEGCSqGSIB3DOEHAaCCE1IEghJOMIISSjCCEkYGCSqGSIB3DOEHBaCCEjcwghIzAgEAMIISLAYJKoZIhvcNA...  
-----

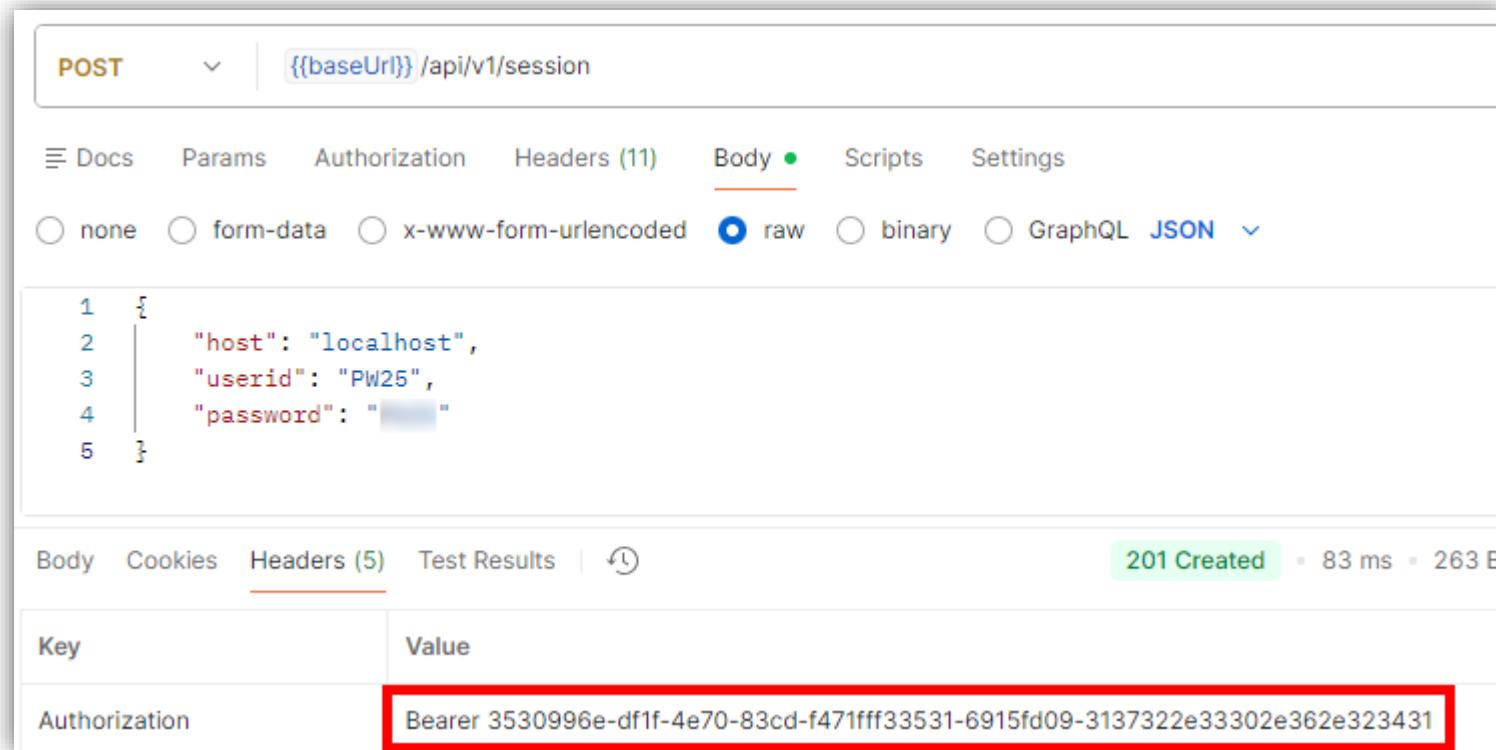
# Scénario 2

- Cas dans DCM



# Scénario 2

## ■ Authentification



POST <https://{{baseUrl}}/api/v1/session>

Body  raw  binary  GraphQL  JSON

```
1 {  
2     "host": "localhost",  
3     "userid": "PW25",  
4     "password": "████████"  
5 }
```

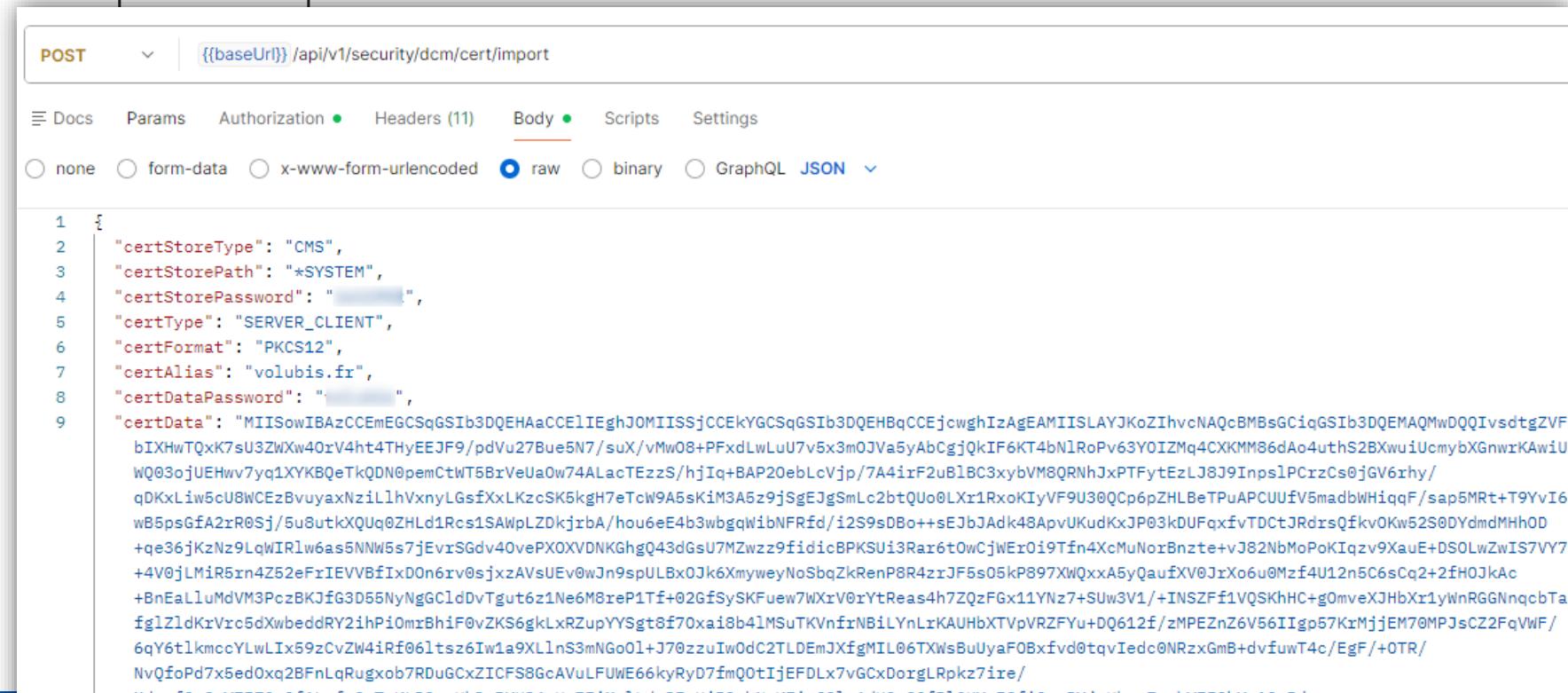
Headers (5)  Body  Cookies  Test Results  ⌚

201 Created 83 ms 263 B

Key	Value
Authorization	Bearer 3530996e-df1f-4e70-83cd-f471fff33531-6915fd09-3137322e33302e362e323431

# Scénario 2

## ■ Importer le pfx



POST [{{baseUrl}}/api/v1/security/dcm/cert/import](#)

Docs Params Authorization Headers (11) Body Scripts Settings

none  form-data  x-www-form-urlencoded  raw  binary  GraphQL **JSON**

```
1 {  
2     "certStoreType": "CMS",  
3     "certStorePath": "*SYSTEM",  
4     "certStorePassword": "*****",  
5     "certType": "SERVER_CLIENT",  
6     "certFormat": "PKCS12",  
7     "certAlias": "volubis.fr",  
8     "certDataPassword": "*****",  
9     "certData": "MIISowIBAzCCEmEGCSqGSIB3DQEHAaCCE1IEghJ0MIISSjCCEkYGCSqGSIB3DQEHBqCCEjcwghIzAgEAMIISLAYJKoZIhvcNAQcBMBsGCiqGSIB3DQEEMAQMwDQQIvsdtgZVFbIXHwTQxK7sU3ZwXw40rV4ht4ThyEEJF9/pdVu27Bue5N7/suX/vMw08+PFxdLwLuU7v5x3m0JVa5yAbCgjQkIF6KT4bNlRoPv63Y0IZMq4CXKMM86dAo4uthS2BXwuiUcmybXGnwrKAwiU,WQ03oj1UEHwv7yq1XYKBQeTkQDN0pemCtWt5BrVeUa0w74ALacTEzzS/hjIq+BAP20ebLcVjp/7A4irF2uBlBC3xybVM8QRNhJxPTFytEzLJ8J9InpslPCrzCs0jGV6rhy/qDKxLiw5cU8WCEzBvuyaxNziL1hVxnyLGsfXxLkzcSK5kgH7eTcW9A5sKiM3A5z9jSgEJgSmLc2btQuo0LXr1RxoKIyVF9U30Qcp6pZHLBeTPuAPCUUfV5madbWHiqqF/sap5Mrt+T9YvI6wb5psGfA2r0Sj/5u8utkXQuq0ZHld1Rcs1SAwplZDkjrB/hou6eE4b3wbgqWibNFRfd/i2S9sDBo++sEJbJAdk48ApvUKudKxJP03kDUFqxfvTDCtJRdrqfkv0Kw52S0DYdmdMHh0D+qe36jKzNz9LqWIRlw6as5NNW5s7jEvxSGdv40vePX0XVDNKGhgQ43dGsU7MzWzz9fidicBPKSU13Rai6t0wCjWEr0i9Tfn4XcMuNorBnzte+vJ82NbMoPoKIqzv9XauE+DS0LwZwIS7VY7,+4V0+jLMiR5in4Z52eFrIEVVBFixD0n6rv0sjxzAVsUEv0wJn9spULBx0Jk6XmyweyNoSbqZkRenP8R4zrJF6s05kP897XWQxxA5yQaufXV0JrXo6u0Mzf4U12n5C6sCq2+2fH0JkAc+BnEalluMdVm3PczBKJf6G3D55NyNgGClDvTgut6z1Ne6M8reP1Tf+02GfSySKFuew7Wxv0rYtReas4h7ZQzFGx11YNz7+Suw3V1/+INSZFF1VQSKhHC+g0mveXJHbXr1yWnRGGNnqcbTaefglZldKrVrc5dXwbeddRY2ihPi0mrBhiF0vZKS6gkLxRZupYYsgt8f0xa18b41MSuTKVnfrNBiLYnLrKAUhXTVpVRZFYu+DQ612f/zMPEZnZ6V56IIgp57KrmjjEM70MPJscZ2FqVWF/6qY6tlkmccYlwLIX59zCvZW4iRf06ltsz6IwLa9XLlnS3mNg0l+J70zuIw0dC2TLDEmJXfgML06TXwsBuuyaFOBxfvd0tqvIedc0NRzxGmB+dvfuwT4c/Eg/+OTR/NvQfpd7x5ed0xq2BFnLqRugxb07RDUgcxZICFS8GcAvuLFUWE66kyRyD7fmQ0tIjEFDLx7vGcxDorgLRpkz7ire/
```

# Scénario 2

- Après importation

Showing 1 of 35 certificates

The screenshot shows a certificate management interface with the following details:

- Certificate Hierarchy:**
  - DigiCert Global Root G2
  - GandiCer
  - volubis.fr
- volubis.fr (Left Certificate):**
  - volubis.fr
  - www.volubis.fr
  - Expires in 88 days
  - ECDSA (256 bits)
  - Stored in software
  - Server/Client Certificate
- volubis.fr (Right Certificate):**
  - volubis.fr
  - www.volubis.fr
  - Expires in 88 days
  - ECDSA (256 bits)
  - Stored in software
  - Server/Client Certificate
- GandiCer (Root Certificate):**
  - GandiCer
  - GandiCert
  - Expires in 3076 days
  - RSA (4096 bits)
  - Certificate Authority (Enabled)

View

+

IBM

Power W

26

# Scénario 2

- Dissocier le certificat

View Application Definition

Assign Certificates Define CA Trust

QIBM\_HTTP\_SERVER\_PW25RSE Server

Assigned Certificates

PW25 v2

Trusted Certificate Authorities

LOCAL\_CERTIFICATE\_AUTHORITY\_78780E12(11)

POST [\({{baseUrl}}/api/v1/security/dcm/appdef/disassociate\)]({{baseUrl}}/api/v1/security/dcm/appdef/disassociate)

Docs Params Authorization Headers (11) Body Scripts Settings

none  form-data  x-www-form-urlencoded  raw  binary  GraphQL **JSON**

```
1  {
2  |  "appDefinitionID": "QIBM_HTTP_SERVER_PW25RSE"
3  }
```

Server

Assigned Certificates

None assigned

Trusted Certificate Authorities

LOCAL\_CERTIFICATE\_AUTHORITY\_78780E12(11)

# Scénario 2

- Associer le certificat

The screenshot shows a REST API client interface with the following details:

- Method:** POST
- URL:** {{baseUrl}} /api/v1/security/dcm/appdef/associate
- Body:** raw (selected)
- Body Content:**

```
1  {
2    "appDefinitionID": "QIBM_HTTP_SERVER_PW25RSE",
3    "certAliases": ["volubis.fr"]
4 }
```

- View Application Definition:** A modal window showing the application definition details.
- Actions:** Assign Certificates, Define CA Trust, Update, Validate, Delete.
- Server Details:** QIBM\_HTTP\_SERVER\_PW25RSE Server
- Assigned Certificates:** volubis.fr (highlighted with a red arrow from the API body content).
- Trusted Certificate Authorities:** LOCAL\_CERTIFICATE\_AUTHORITY\_78780E12(11)

# Scénario 3

- Pour automatiser, du code
  - SQL

-- Variables pour intégration

```
create or replace variable nb.pw          varchar(10) ;
create or replace variable nb.pwstore     varchar(10) ;
create or replace variable nb.body        clob(1M)    ccsid 1208 ;
create or replace variable nb.bearer      varchar(200) ccsid 1208 ;

set nb.pw = ? ;
set nb.pwstore = ? ;
```

-- 1. Authentification

```
set nb.body = '{"host": "localhost", "userid": "PW25", "password": "' concat nb.pw concat '"}' ;

set nb.bearer = (
  select JSON_VALUE(response_http_header, '$.Authorization' RETURNING varchar(200)) as bearer
  from table(qsys2.http_post_verbose(URL => 'https://itest10.gaia.lan:2012/rseapi/api/v1/session',
                                         REQUEST_MESSAGE => nb.body,
                                         OPTIONS => '{"headers":{"Content-Type":"application/json","Accept":"*/*"}})) );
```

# Scénario 3

- Pour automatiser, du code
  - SQL

```
-- 2. Import
set nb.body = json_object( 'certStoreType' value 'CMS',
                           'certStorePath' value '*SYSTEM',
                           'certStorePassword': nb.pwstore, ←
                           'certType': 'SERVER_CLIENT',
                           'certFormat': 'PKCS12',
                           'certAlias': 'volubis.fr',
                           'certDataPassword': 'volubis',
                           'certData' : (select qsys2.base64_encode(line)
                                         from table(qsys2.ifs_read_binary(PATH_NAME => '/home/NB/volubis.fr.pfx'))) ) ;

select *
from table(qsys2.http_post_verbose(URL => 'https://itest10.gaia.lan:2012/rseapi/api/v1/security/dcm/cert/import',
                                     REQUEST_MESSAGE => nb.body,
                                     OPTIONS => '{"headers":{"Content-Type":"application/json",
                                         "Accept":"*/*",
                                         "Authorization":"' concat nb.bearer concat '"}})) ;
```

# Scénario 3

- Pour automatiser, du code

- curl

```
PATH=/QOpenSys/pkgs/bin:$PATH
export PATH PASE_PATH

# 1. Authentication
curl -v -k \
      --header 'Content-Type: application/json' \
      --header 'Accept: */*' \
      --data '{"host": "localhost", "userid": "PW25", "password": "████████"}' \
      --location --request POST 'https://itest10.gaia.lan:2012/rseapi/api/v1/session' \
      > /dev/null 2>curl.log

BEARER=$(grep -i '< Authorization:' curl.log | sed 's/< Authorization://g')
echo $BEARER
```

```
-bash-5.2$ ./changecert.sh
Bearer 7a0726a8-04ab-451d-b557-d2ae425340e6-69170057-3137322e33302e31342e3137
```

# Remarques

- Pas (encore ?) toutes les fonctions de DCM
  - Impossible de créer un nouveau certificat
    - « Même pas un renew »
- Via SQL

```
15 select *
16   from table (
17     qsys2.certificate_info(certificate_store_password => '*NOPWD')
18   )
19   where validity_end < current date + 1 month
20   order by validity_end;
```

CERTIFICATE_LABEL	SERIAL_NUMBER	VALIDITY_START	VALIDITY_END
LOCAL_CERTIFICATE_AUTHORITY_78780E12(5)	6785139B	2025-01-12 14:22:35	2025-01-15 14:22:35
LOCAL_CERTIFICATE_AUTHORITY_78780E12(6)	67BC422F	2025-02-23 10:55:59	2025-02-26 10:55:59
itest10-services-2024	66E012CA06E120	2024-09-09 11:35:06	2025-09-10 11:35:06

# Remarques

- <https://github.com/ThePrez/DCM-tools>

## dcmimport

Used to import certificates into DCM.

It can be used to import files of type:

- Binary DER-encoded certificate files
- Binary DER-encoded certificate bundles
- Human-readable DER-encoded certificate files
- Human-readable DER-encoded certificate bundles
- JKS trust stores
- JCEKS trust stores
- PKCS#12 or PFX bundles
- A directory containing any of the above
- A `.zip` file containing any of the above

It can also be used to fetch certificates from a remote host and import to DCM.

## dcmexport

Used to export the entire DCM keystore to file

MErci