

# 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@gaia.fr

Nathanaël Bonnet  
Gaia-Volubis  
nathanael.bonnet@gaia.fr

The IBM logo, consisting of the letters "IBM" in a stylized, horizontally-striped font.The logo for "common FRANCE", with "common" in a stylized, rounded font and "FRANCE" in a smaller, sans-serif font below it.

# 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



# 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** 1.0.9 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  
https://neptune:2012/rseapi 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. lock
- GET** /api/v1/admin/settings Get the general settings being used for RSE API. lock
- POST** /api/v1/admin/settings Set settings for RSE API. lock

# Comment ?

- Serveur admin5 démarré

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

- Activer TLS sur le serveur admin5

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/userdata/os/admininst/admin5/wlp/usr/servers/admin5  
Disable server: False  
**TLS configuration: Enabled**

				10188
Admin5	V8.5 (int app svr)	Running	*:2011	*:2012
			*:2013	*:2014

# Quoi ?

- 8 services

Servers  
https://itest10:2012/rseapi ▼

---

**Administration Services** Administration Services provide APIs that give information about RSE API and the runtime environment. They require authentication 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, such as reading from files, and writing to 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 digital certificates. All the digital certificate management APIs require the Digital Certificate Manager, option 34 of the IBM i licensed program. The user 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 then accessed. 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 AF authentication 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.

- Gestion des certificats

**Security Services** All the c must ha

Power Week

18 -19 - 20 novembre  
2025



# Gestion des certificats TLS



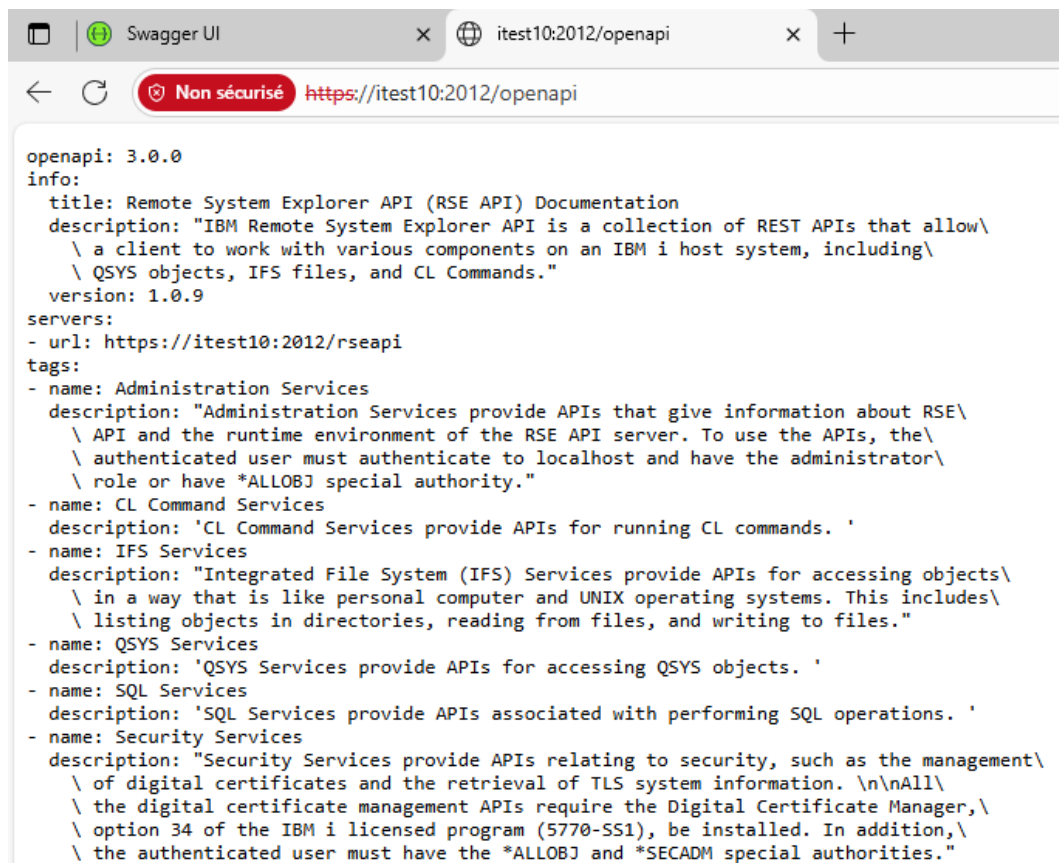
# Description de l'API

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

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

# Importation dans Postman

- [itest10:2012/openapi](https://itest10:2012/openapi)



# 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

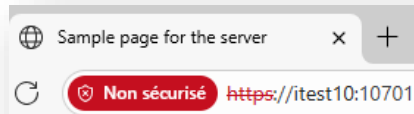
## ■ Instance

### Display Configuration File

HTTP server: PW25RSE

Selected file: /www/pw25rse/conf/httpd.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.SRVPGM
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 -> %U" 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>
```



This is the

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.gaiia.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)

# Scénario 1

- Authentication

The screenshot shows a REST client interface for a POST request to `{{baseUrl}}/api/v1/session`. The request body is a JSON object with the following fields:

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

The response status is **201 Created** with a response time of 83 ms and a body size of 263 B. The response headers are displayed in a table:

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 ▼ `{{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": "PW25 v2",
8   "certDataPassword": "iTest10",
9   "certData":
      "MIIJiwIBAzCCUkGCSqGSIb3DQEHAaCCCToEggk2MIIJmJCCCS4GCSqGSIb3DQEHBqCCCR8wggkbAgEAMIIJF
      AQMwDQIQZb2BtAURWsCAQWAggJowHPK0Kb0cm7Mp1JtZ/ioVYrDVwLsqeeQAegVTBJl/AU9aAnJZgiLqMABbK
      bfpbX6ohS62GCAF6HxyWoBsDmJoMV1eZJMNJc2QK1EMKCIWftVsWcM9kSae7N+yxjrf8CiSbL/I5Ttc0S1Z4Q2
      Hc5v5ojRVee35DN6FVYmzYFERc6ndGtLNNN0JpTZRKuN3i8khHAV4q9G39Q9gXWu7D/
```

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

The image shows a REST client interface on the left and a 'View Application Definition' dialog on the right. The REST client displays a POST request to `{{baseUrl}}/api/v1/security/dcm/appdef/associate` with a raw body containing a JSON object. The JSON object has two fields: `"appDefinitionID": "QIBM_HTTP_SERVER_PW25RSE"` and `"certAliases": ["PW25 v2"]`. Red arrows point from these fields to the corresponding elements in the dialog. The dialog has tabs for 'Assign Certificates', 'Define CA Trust', 'Update', 'Validate', and 'Delete'. The 'Assign Certificates' tab is active, showing a list with 'QIBM\_HTTP\_SERVER\_PW25RSE Server' and 'Assigned Certificates' containing 'PW25 v2'. A detailed view of 'PW25 v2' is shown below, including its name 'pw25rse', expiration 'Expires in 364 days', signature 'ECDSA (256 bits)', storage 'Stored in software', and type 'Server/Client Certificate'.

```
POST {{baseUrl}}/api/v1/security/dcm/appdef/associate
```

Docs Params Authorization Headers (11) Body raw

```
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

Sample page for the server x +

← ↻ Non sécurisé https://itest10:10701

**This is th**

For information on changing this page or serving additional pages using PW25RSE,

To learn more, please refer to the list of documentation available on the [HTTP server](#)

**Visionneuse de certificats : pw25rse**

Général Détails

Émis pour

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

Émis par

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

Période de validité

Date d'émission	mercredi 12 novembre 2025 à 17:10:15
Date d'expiration	vendredi 13 novembre 2026 à 17:10:15

# Scénario 2

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

# Scénario 2

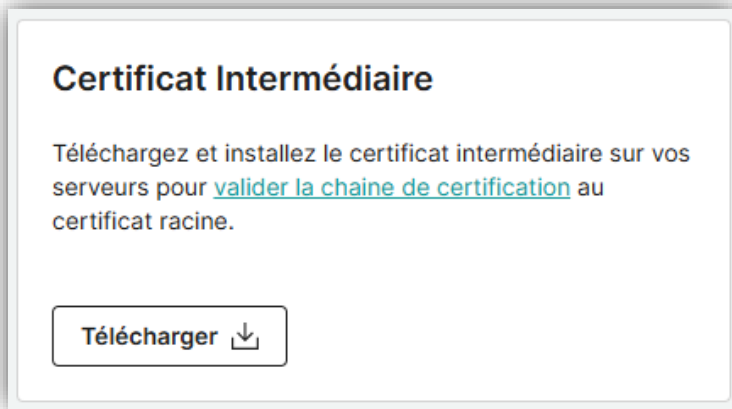
- Récupérer le certificat + chaîne de certification (CAs)

The screenshot shows the Gandi.net user interface for managing SSL certificates. The left sidebar contains navigation links: TABLEAU DE BORD, NOM DE DOMAINE, CERTIFICATS SSL (selected), HÉBERGEMENT WEB, GANDICLOUD, FACTURATION, and ORGANISATIONS. The main content area is titled 'Certificats SSL (3)' and features a search bar and a 'Filtrer' button. Below this is a table with three columns: Nom, Type, Abonnement, and Validité. The table lists three certificates for the domain 'volubis.fr'. A dropdown menu is open for the first certificate, showing options: Télécharger (highlighted with a red box), Régénérer..., Modifier les tags..., and Révoquer.

<input type="checkbox"/>	Nom	Type	Abonnement	Validité	
<input type="checkbox"/>	www.volubis.fr SAS VOLUBIS	Manuel / Standard Multi-domaines	Payé jusqu'au 10 févr. 2026	Valide jusqu'au 10 févr. 2026	<div><div>Télécharger</div><div>Régénérer...</div><div>Modifier les tags...</div><div>Révoquer</div></div>
<input type="checkbox"/>	formation.volubis.fr SAS VOLUBIS	Manuel / Standard Une adresse	Payé jusqu'au 11 févr. 2026	Val	
<input type="checkbox"/>	education.volubis.fr SAS VOLUBIS	Manuel / Standard Une adresse	Payé jusqu'au 6 oct. 2026	Vali	

# 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	volubis.fr.pfx
File size	6368 bytes
Mime type	text/plain
Link	Download output

MIIISowIBAzCCEmEGCSqGSib3DQEHAaCCElIEghJOMIISsjCCEkYGCSqGSib3DQEHBqCCEjcwghIzAgEAMIISLAYJKoZiHvcNAQcBMBsGCiqGSib3DQEMAQMwDQQLvsdtgZVFKFcCAQWAgHIA4ZNoqsgSuZcA  
DjdA/bIXHwTQxK7sU3ZWXw4OrV4ht4THyEEJF9/pdVu27Bue5N7/suX/vMwO8+PFxdLwLuU7v5x3m  
OJVasYAbCgQkIF6KT4bNIrOPv63YOIZmq4CXKMM86dAo4uthS2BXwuiUcmybXGnwrKAwiU/WQ03oj  
UEHwv7yq1XYKBQeTkQDN0pemCtWT5BrVeUaOw74ALacTEzzS/hjlq+BAP2OebLcVjp/7A4irF2uBIBC3  
xybVM8QRNhJxPTFytEzLJ8J9InpsIPCzCs0jGV6rhy/qDKxLiW5cU8WCEzBvuyaxNziLhVxnyLGSfXxLK  
zcSK5kgH7eTcW9A5sKiM3A5z9jSgEJgSmLc2btQUo0LXr1RxoKlyVF9U30QCp6pZHLBeTPuAPCUUfV  
5madbWHiqqF/sap5MRt+T9Yvl6DvgQ7NEy0lqfqMvVPXqol2m6fFj/wB5psGfA2rR0Sj/5u8utkXQUq0ZH  
Ld1Rcs1SAWpLZDkjrba/hou6eE4b3wbqqWibNFRfd/i2S9sDBo++sEJbJAdk48ApvUKudKxJP03kDUFq  
xfvTDctJRdrsQfkvOKW52S0DYdmdMHhOD+qe36jKzNz9LqWIRlw6as5NNW5s7jEvrSGdv4OvePXOXV  
DNKGhgQ43dGsU7MZwzz9fidicBPKSUi3Rar6tOwCjWErOi9Tfn4XcMuNorBnzte+vJ82NbMoPoKlqzv9  
XauE+DSOLwZWIS7VY7/SVJmDds89uJ+4V0jLMiR5rn4Z52eFrlEVVBfIxDON6rv0sjxzAVsUEv0wJn9sp  
ULBxOJk6XmyweyNoSbqZkRenP8R4zrJF5sO5kP897XWQxxA5yQaufXV0JrXo6u0Mzf4U12n5C6sCq2

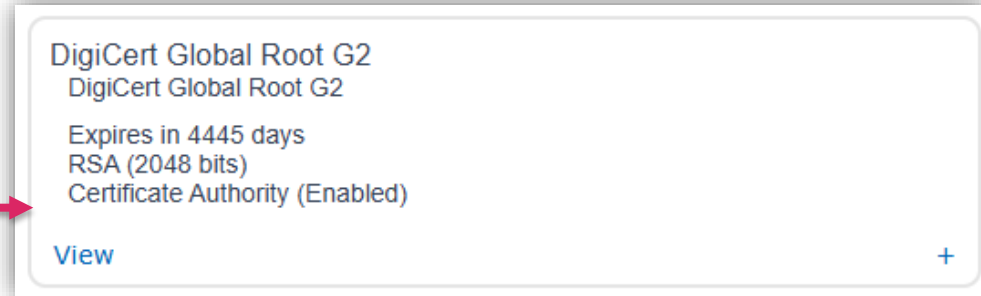
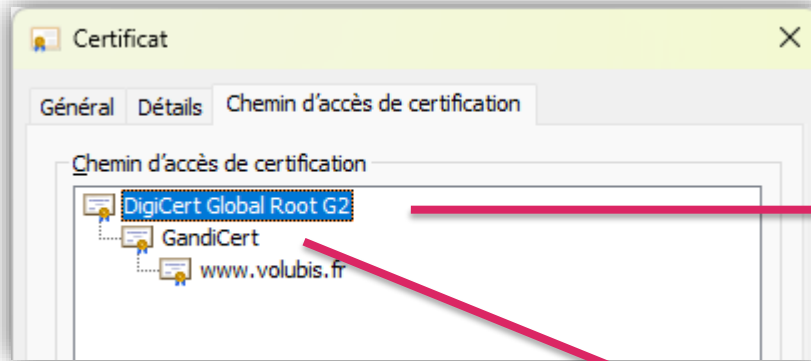
```
SELECT qsys2.base64_encode(line) FROM TABLE(QSYS2.IFS_READ_BINARY(PATH_NAME => '/home/NB/volubis.fr.pfx'));
```

00001

MIIISowIBAzCCEmEGCSqGSib3DQEHAaCCElIEghJOMIISsjCCEkYGCSqGSib3DQEHBqCCEjcwghIzAgEAMIISLAYJKoZiHvcNA...

# Scénario 2

- Cas dans DCM



Absent

# Scénario 2

- Authentication

The screenshot shows a REST client interface for a POST request to `{{baseUrl}}/api/v1/session`. The request body is a JSON object with the following fields:

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

The response status is **201 Created** with a response time of 83 ms and a size of 263 B. The response headers are displayed in a table:

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



# Scénario 2

## ■ Importer le pfx

POST `{{baseUri}}/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": "MIISowIBAzCCEmEGCSqGSIb3DQEHAaCCElIEghJOMIISsjCCEkYGCsqGSIb3DQEHBqCCEjcwghIzAgEAMIISLAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIvsdtgZVFH
bIXHwTQxK7sU3ZWxw40rV4ht4THyEEJF9/pdVu27Bue5N7/suX/vMw08+PFxdLwLU7v5x3m0JVa5yAbCgjqKIF6KT4bNlRoPv63Y0IZMq4CXKMM86dAo4uthS2BXwuiUcmbyXGnwrKAwiU,
WQ03ojuUEHv7yq1XYKBQeTkQDN0pemCtWT5BrVeUa0w74ALacTEzzS/hjIq+BAP20ebLcVjp/7A4irF2uB1BC3xybVM8QRNhJxPTFytEzLJ8J9InpslPCrzCs0jGV6rhy/
qDKxLiW5cU8WCEzBvuyaxNziLlhVxnyLGsfXxLKzC5K5kgH7eTcW9A5sKiM3A5z9jSgEJgSmLc2btQUo@LXr1RxoKIyVF9U30QCp6pZHLBeTPuAPCUUfV5madbWHiqqF/sap5MRt+T9YvI6U
wB5psGfA2rR0Sj/5u8utkXQUQ0ZHLd1Rcs1SAWpLZDkjrBA/hou6eE4b3wbqgqwbNFRfd/i2S9sDBo++sEJbJAdk48ApvUKudKxJP03kDUFqxfrvTDCTJRdrsQfkw0Kw52S0DYdmdMHhOD
+qe36jKzNz9LqWIRLw6as5NNW5s7jEvrSGdv40vePXOXVDNKGhGQ43dGsU7M2wzz9fidicBPKSUi3Rar6tOwCjWEr0i9Tfn4XcMuNorBnzte+vJ82NbMoPoKIqzv9XauE+DSOLwZwIS7VY7,
+4V0jLMiR5rn4Z52eFrIEVVBfIXD0n6rv0sjxzAVsUEv@wJn9spULBx0Jk6XmyweyNoSbQZkRenP8R4zrJF5s05kP897XWQxxA5yQaufXV0JrXo6u0Mzf4U12n5C6sCq2+2fH0JkAc
+BnEaLlUmdVM3PczBKJfG3D55NyNgGCldDvTgut6z1Ne6M8reP1Tf+02GfSySKFuew7WxRv0rYtReas4h7ZQzFGx11YNz7+SUw3V1/+INSZFf1VQSKhHC+gOmveXJHbXr1yWnRGGNqcbTae
fglZldKrVrc5dXwbeddRY2ihPi0mrBhIF0vZKS6gkLxRZupYYSgt8f70xai8b4lMSuTKVnfrNBiLYnLrKAUHbXTVpVRZFYu+DQ612f/zMPEZnZ6V56Ilgp57KzrMjjEM70MPJsCZ2FqVWF/
6qY6tlkmccYLwLIx59zCvZW4iRf06ltsz6Iw1a9XLlnS3mNGo0l+J70zzuIw0dC2TLDemJXfgMIL06TXWsBuYuaF0Bxfvd0tqvIedc0NRzxGmB+dvfuwT4c/EgF/+0TR/
NvQfoPd7x5ed0xq2BFnLqRugxob7RDuGCxZICFS8GcAvULFUWE66kyRyD7fmQ0tIjEFDLx7vGCxGdorgLRpkz7ire/
"
```

Body Cookies Headers (4) Test Results 204 No Content 270 ms

# Scénario 2

- Après importation

Showing 1 of 35 certificates

volubis.fr

www.volubis.fr

! Expires in 88 days  
ECDSA (256 bits)  
Stored in software  
Server/Client Certificate

[View](#)

## Certificate Hierarchy

DigiCert Global Root G2

GandiCer

volubis.fr

volubis.fr

www.volubis.fr

! Expires in 88 days  
ECDSA (256 bits)  
Stored in software  
Server/Client Certificate

GandiCer

GandiCert

Expires in 3076 days  
RSA (4096 bits)  
Certificate Authority (Enabled)

[View](#)

+

# Scénario 2

- Dissocier le certificat

### View Application Definition

[Assign Certificates](#) [Define CA Trust](#) [Up](#)

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`

☰ 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 displays a REST client interface. The top section shows a POST request to the endpoint `{{baseUrl}}/api/v1/security/dcm/appdef/associate`. The request body is set to 'raw' and contains the following JSON:

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

A red arrow points from the `"certAliases": ["volubis.fr"]` line in the request body to the 'Assigned Certificates' section of the response. The response, titled 'View Application Definition', shows the application definition 'QIBM\_HTTP\_SERVER\_PW25RSE Server' with the certificate alias 'volubis.fr' assigned. The 'Trusted Certificate Authorities' section lists 'LOCAL\_CERTIFICATE\_AUTHORITY\_78780E12(11)'.

**POST** `{{baseUrl}}/api/v1/security/dcm/appdef/associate`

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

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

1 {  
2 "appDefinitionID": "QIBM\_HTTP\_SERVER\_PW25RSE",  
3 "certAliases": ["volubis.fr"]  
4 }

**View Application Definition**

Assign Certificates Define CA Trust Update Validate Delete

QIBM\_HTTP\_SERVER\_PW25RSE  
Server

Assigned Certificates

volubis.fr

Trusted Certificate Authorities

LOCAL\_CERTIFICATE\_AUTHORITY\_78780E12(11)

# Scénario 3

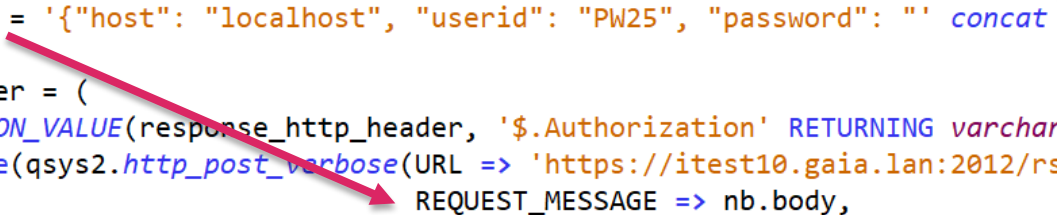
- Pour automatiser, du code
  - SQL

```
-- 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/pkgsrc/bin:$PATH
export PATH PASE_PATH

# 1. Authentification
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

MERC

