GlobalSign PKIaaS connector for Service Now

User guideline

Version 1.2.1

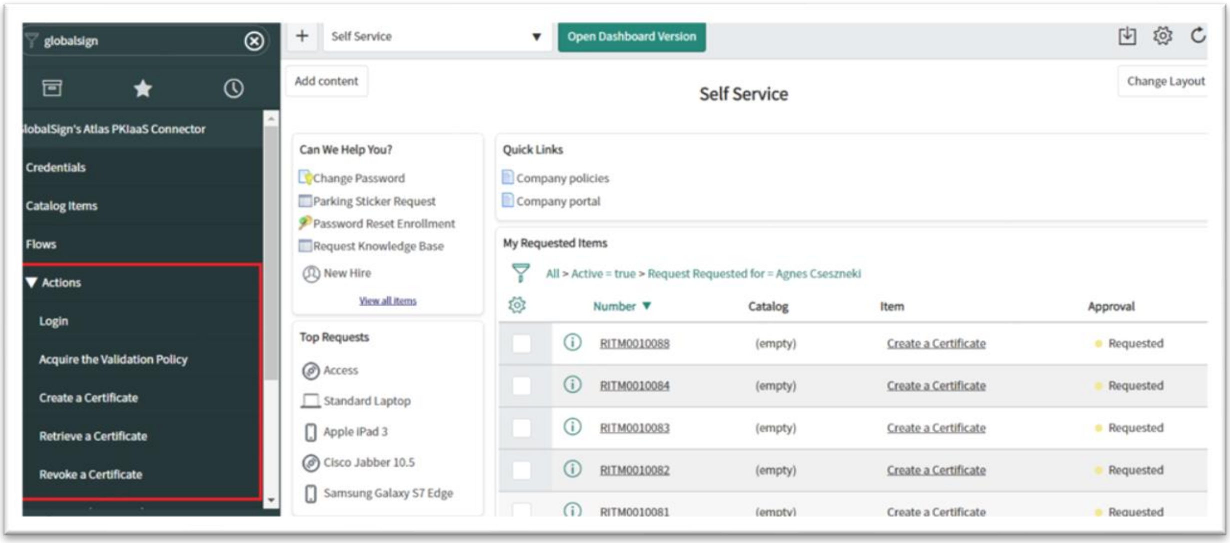
Table of Contents

Introduction

The Atlas PKIaaS Connector scoped application is a toolbox that allows the customer to communicate with the Atlas API using ServiceNow and Flow Designer. This article provides step-by-step instructions for install and set up GlobalSign PKIaaS connector via Service Now ITSM instance.

Using GlobalSign PKIaaS connector actions

Note: To use the connector you need to set up all the connections configuration. Please follow the "Set up connection for GlobalSign PKIaaS" for further information.



My Requested Items

All > Active = true > Request Requested for = Agnes Csesznek

Number ▼	Catalog	Item	Approval
RITM0010088	(empty)	Create a Certificate	Requested
RITM0010084	(empty)	Create a Certificate	Requested
RITM0010083	(empty)	Create a Certificate	Requested
RITM0010082	(empty)	Create a Certificate	Requested
RITM0010081	(empty)	Create a Certificate	Requested

The action items in GlobalSign PKIaaS connector are using Atlas HVCA APIs. For further information, please visit globalsign.com for the latest API documentation.

The GlobalSign PKIaaS connector contains the following GlobalSign PKIaaS connector specific active actions:

- Acquire validation policy
- Certificates issued
- Certificates revoked
- Create certificate
- Find certificate
- Get System property
- Login
- Payload Helper – Create certificate
- Payload Helper – Revoke certificate
- Retrieve Certificate
- Retrieve Trust Chain
- Revoke certificate – PATCH
- Create a certificate record
- Update a certificate record - create
- Update a certificate record – revoke
- Get a certificate record by certificate number

- Get certificate record

Using this actions, the administrators can create new flows or customize the existing ones.

Note: The detailed information for this actions is available in the “Developer Guide”.

Using GlobalSign PKIaaS connector flow

Note: Combining a Flow and Actions we can produce the desired outcome based on the supplied information from the end user (catalog item). GlobalSign PKIaaS connector provide the “TLS Certificate” and “Revoke certificate” flows as an example. More information about the pre-defined actions, what you can use to build further flows, please see above “Using GlobalSign PKIaaS connector actions” section.

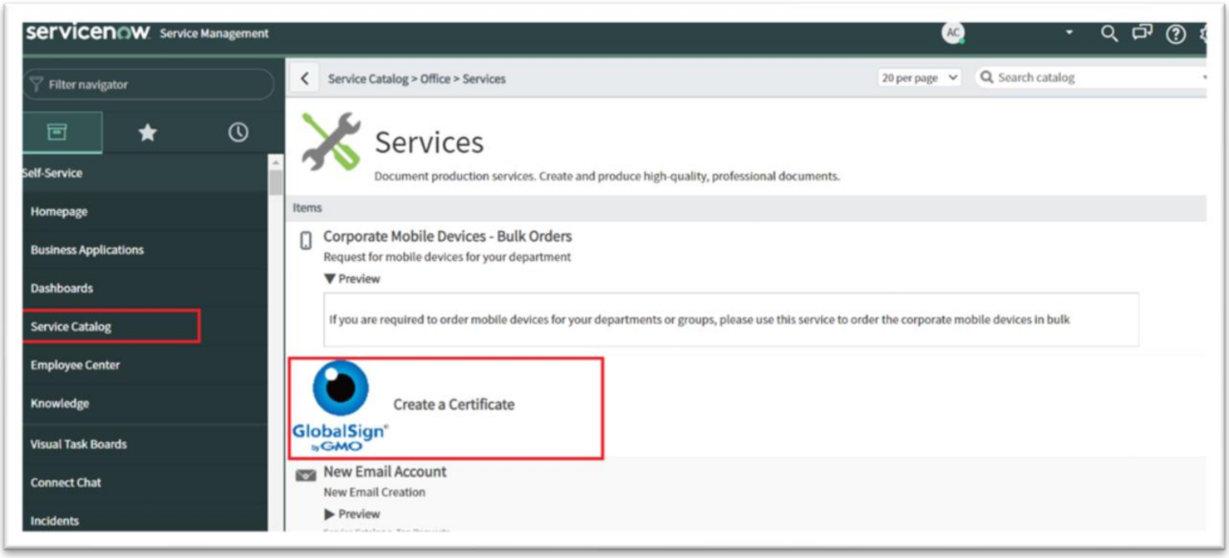
The GlobalSign PKIaaS connector contains the following GlobalSign PKIaaS connector specific active flows:

- TLS certificate
- Revoke certificate

Note: The detailed information about the flows is available in the “Developer Guide”.

Using GlobalSign PKIaaS connector catalog item

Packaged with the scoped application is two example catalog items: “TLS Certificate” and “Revoke Certificate”. With the action items, you can create as many as you would like flows and catalog items and add them to your business flow and catalogs.



Services

Document production services. Create and produce high-quality, professional documents.

Corporate Mobile Devices - Bulk Orders

Request for mobile devices for your department

If you are required to order mobile devices for your departments or groups, please use this service to order the corporate mobile devices in bulk

New Email Account

New Email Creation

The GlobalSign PKIaaS connector contains the following GlobalSign PKIaaS connector specific active catalog items:

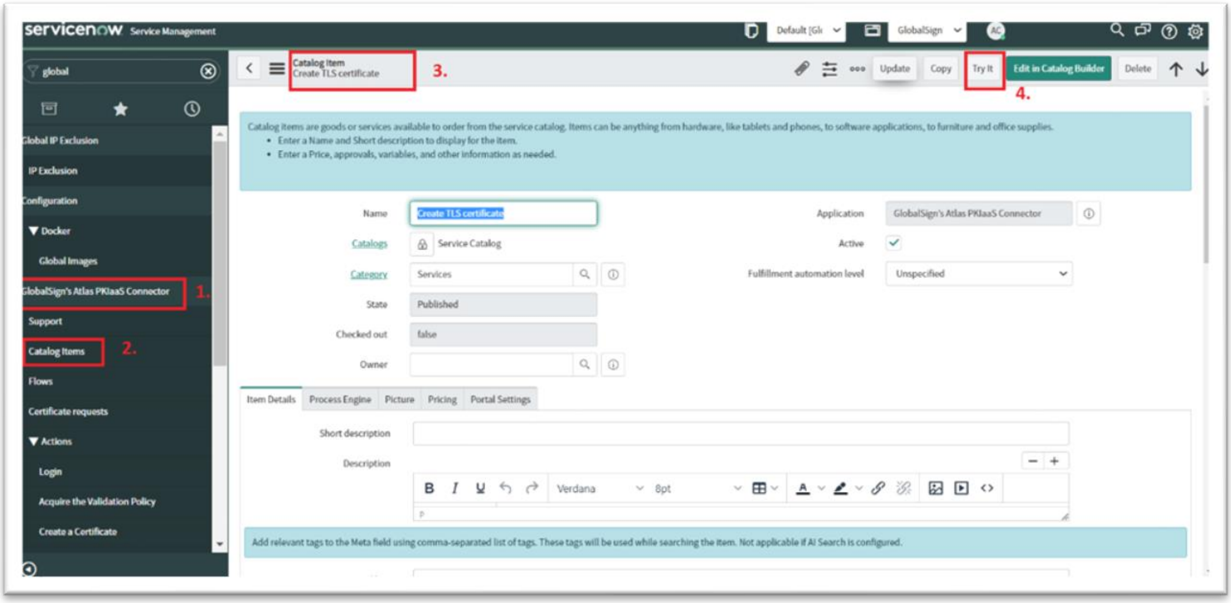
- TLS certificate
- Revoke certificate

This catalog items are available from the application menu or from the selected catalogs. The catalog items are already added to GlobalSign certificate catalog.

Catalog items

TLS certificate

To issue certificate via catalog item, follow the following steps:



Catalog items are goods or services available to order from the service catalog. Items can be anything from hardware, like tablets and phones, to software applications, to furniture and office supplies.

- Enter a Name and Short description to display for the item.
- Enter a Price, approvals, variables, and other information as needed.

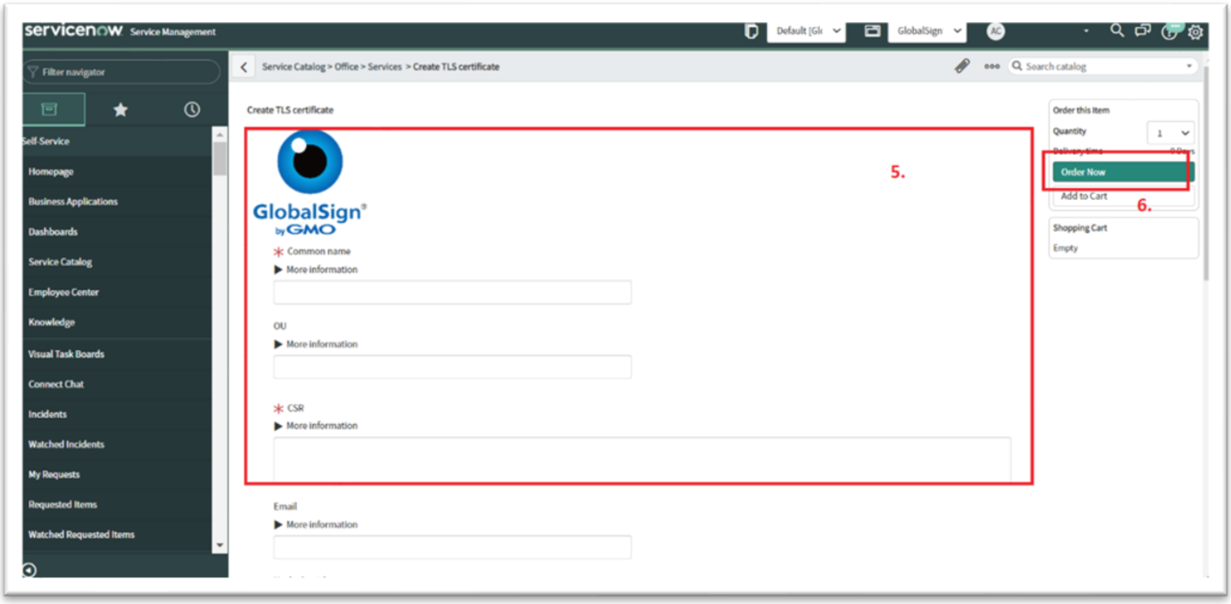
Name	Create TLS certificate	Application	GlobalSign's Atlas PKIaaS Connector
Catalogs	Service Catalog	Active	✓
Category	Services	Fulfillment automation level	Unspecified
State	Published		
Checked out	false		
Owner			

Short description

Description

Add relevant tags to the Meta field using comma-separated list of tags. These tags will be used while searching the item. Not applicable if AI Search is configured.

1. Type into the search box on the left top: “GlobalSign”
2. You can see now in the list the “Catalog Items”.
3. Click on the “Catalog Items” and you can see in the list “TLS Certificate”
4. Click on the link and you can see the form to issue a certificate, please click on the “Try it”.



Create TLS certificate

* Common name
▶ More information

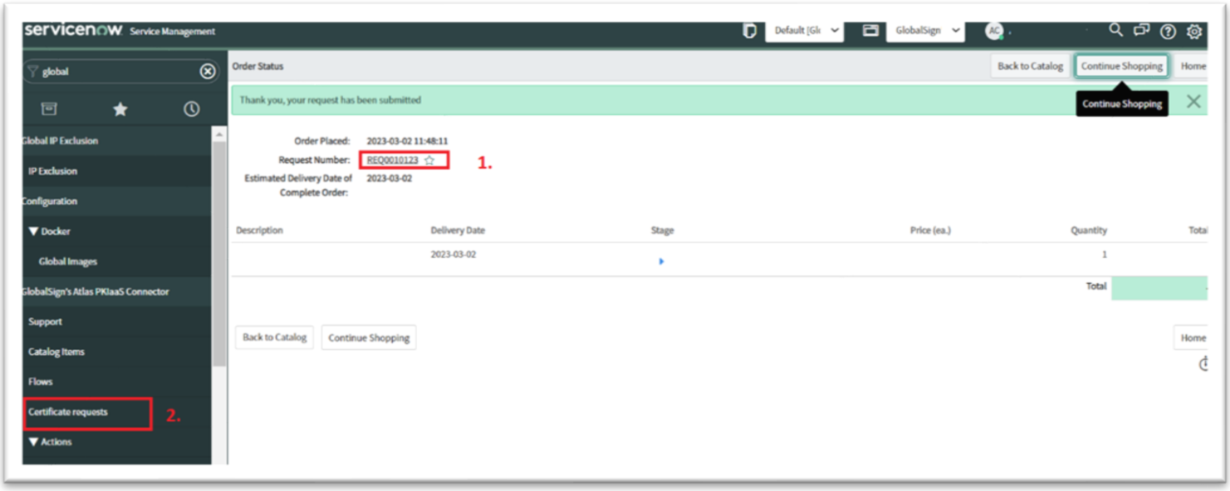
OU
▶ More information

* CSR
▶ More information

Email
▶ More information

5. The request based on your validation policy. Please note some field what not marked, can be mandatory based on your validation policy. Fill out the following fields:
    - Common name: Fully qualified name of your server. The expected value of the common name is depends on the validation policy and the type of the certificate. For DV products is for example: www.globalsign.com, for OV certificates: GlobalSign Ltd. Common name for TLS DV have to be one of the SAN DNS names.
    - OU: Organizational Unit (OU). From 1st September public certificates OU field is deprecated, only available for private certificates. To issue public certificates, keep it empty.
    - CSR: The Certificate Signing Request (CSR) begins with the line "—-BEGIN CERTIFICATE REQUEST—– " and ends with the line "—–END CERTIFICATE REQUEST—–"
    - Email: Public email address of the certificate. Example: john.doe@demo.hvca.globalsign.com
    - Hash algorithm: Value and the needs are depends on the product configuration. Hash Algorithm is not specified, certificates will be issued based on the hash algorithm of the certificate being reissued. One of SHA-256, SHA-384, SHA-512
    - Validity information -> Valid not before.
    - Validity information -> Valid not after, if not specified or 0, than automatically set the maximum allowed value from the validation policy
    - SAN information -> DNS names: List of domain names, need to match or subdomain of validated domain. Example format: test.demo.hvca.globalsign.com, test2.demo.hvca.globalsign.com
    - SAN information -> IP addresses: List of public IP addresses, needs to match with the IPs in the domain claim. Example: 198.41.214.154, 118.41.214.152
    - SAN information -> Emails: List of Email addresses, needs to match with the domain claim.: Example: test@globalsign.com, test2@globalsign.com
    - SAN information -> Other names -> Type: Use these SAN Other Name "Type" field for objects such as OIDs, UPNs etc. or leave them blank. Note: When using them, you must to provide both a "type" and a "value" in the provided fields below.
    - SAN information -> Other names-> Value: Use these SAN Other Name "Value" fields for objects such as OIDs, UPNs etc. or leave them blank. Note: When using them, you must to provide both a "type" and a "value" in the provided fields below.
6. On the top right side, click on the "Order now" button.

Get your certificate



Thank you, your request has been submitted

Order Placed: 2023-03-02 11:48:11
Request Number: REQ0010123 ☆
Estimated Delivery Date of Complete Order: 2023-03-02

Description	Delivery Date	Stage	Price (ea.)	Quantity	Total
	2023-03-02			1	
				Total	

1. After to using catalog item, you can click on the request and find the request item at the bottom of the page where you can find the certificate details. Please note, may you need to wait a couple of seconds to finish the background processes and make it visible.

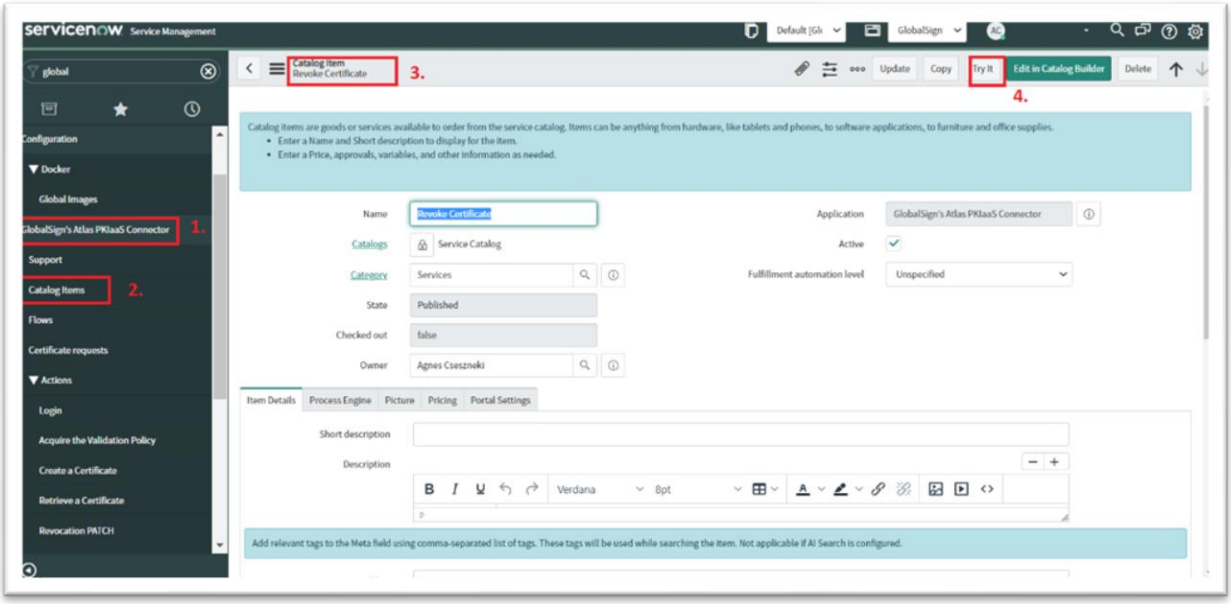
2. You can see also all of your certificate request under the GlobalSign Atlas PKIaaS connector application menu “Certificate requests” menu item. For more information please check the “Using Certificate requests module” below.

Note: If there was a failure, instead of creating work notes, we will see a Catalog Task created. Once the task has been resolved (and the API / connection has been restored), the user can resubmit their request.

Note: Using the certificate number you can also get your certificate details via the “Retrieve certificate” action.

Revoke Certificate

To revoke a certificate via catalog item, please follow the steps below:



Catalog items are goods or services available to order from the service catalog. Items can be anything from hardware, like tablets and phones, to software applications, to furniture and office supplies.

- Enter a Name and Short description to display for the item.
- Enter a Price, approvals, variables, and other information as needed.

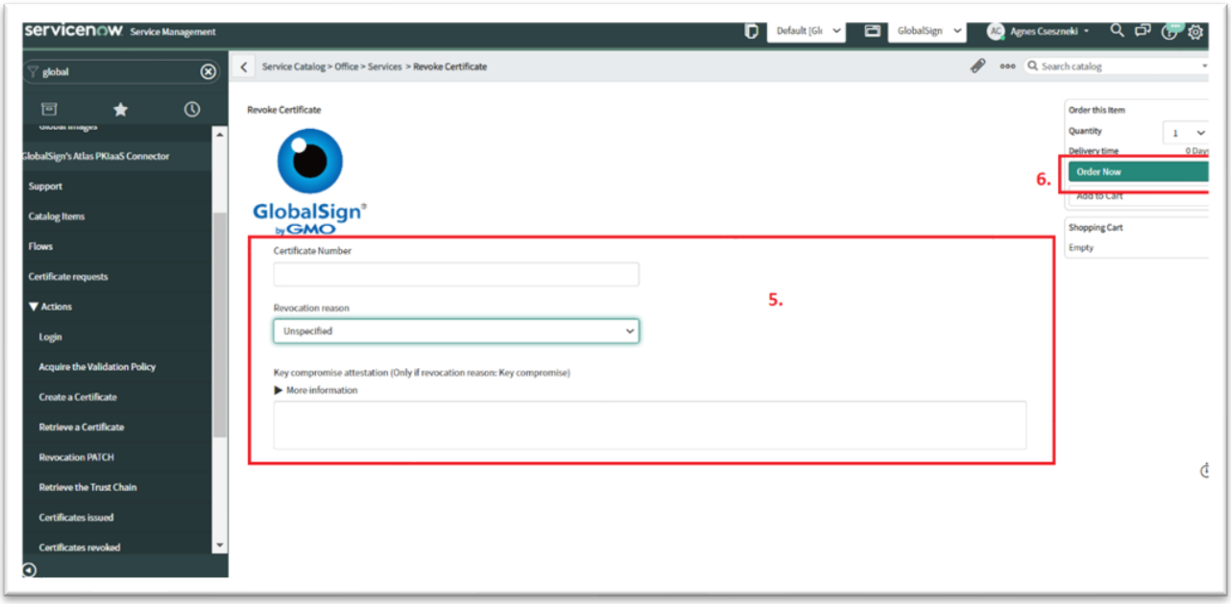
Name	Revoke Certificate	Application	GlobalSign's Atlas PKIaaS Connector
Catalogs	Service Catalog	Active	✓
Category	Services	Fulfillment automation level	Unspecified
State	Published		
Checked out	false		
Owner	Agnes Cseszneki		

Short description

Description

Add relevant tags to the Meta field using comma-separated list of tags. These tags will be used while searching the item. Not applicable if AI Search is configured.

1. Type into the search box on the left top: “GlobalSign”
2. You can see now in the list the “Catalog Items”.
3. Click on the “Catalog Items” and you can see in the list “Revoke Certificate”
4. Click on the link and you can see the form to issue a certificate, please click on the “Try it”.



Revoke Certificate

Certificate Number

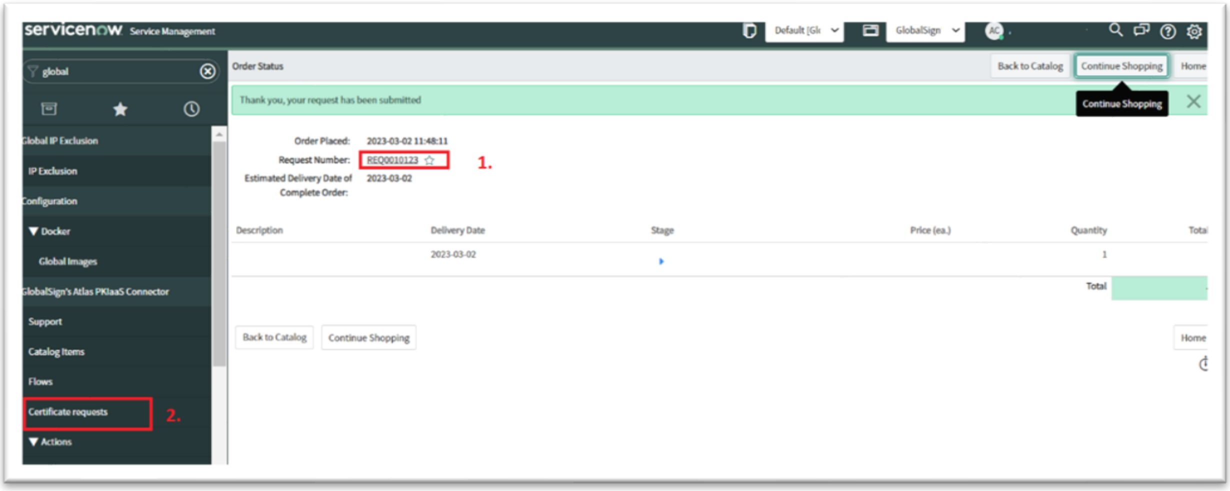
Revocation reason: Unspecified

Key compromise attestation (Only if revocation reason: Key compromise)

▶ More information

5. Fill out the form. Please note the “Key compromise attestation” field just need to fill out in the case if the selected revocation reason is “Key compromise”.
6. Click on the “Order” button.

Get your certificate



Thank you, your request has been submitted

Order Placed: 2023-03-02 11:48:11

Request Number: REQ0010123

Estimated Delivery Date of Complete Order: 2023-03-02

Description	Delivery Date	Stage	Price (ea.)	Quantity	Total
	2023-03-02			1	
				Total	

1. After to using catalog item, you can click on the request and find the request item at the bottom of the page where you can find the certificate details. Please note, may you need to wait a couple of seconds to finish the background processes and make it visible.

2. You can see also all of your certificate request under the GlobalSign Atlas PKIaaS connector application menu “Certificate requests” menu item, where you can find the revocation reason, revocation RITM item and the user who did the revocation for each certificate. For more information please check the “Using Certificate requests module” below.

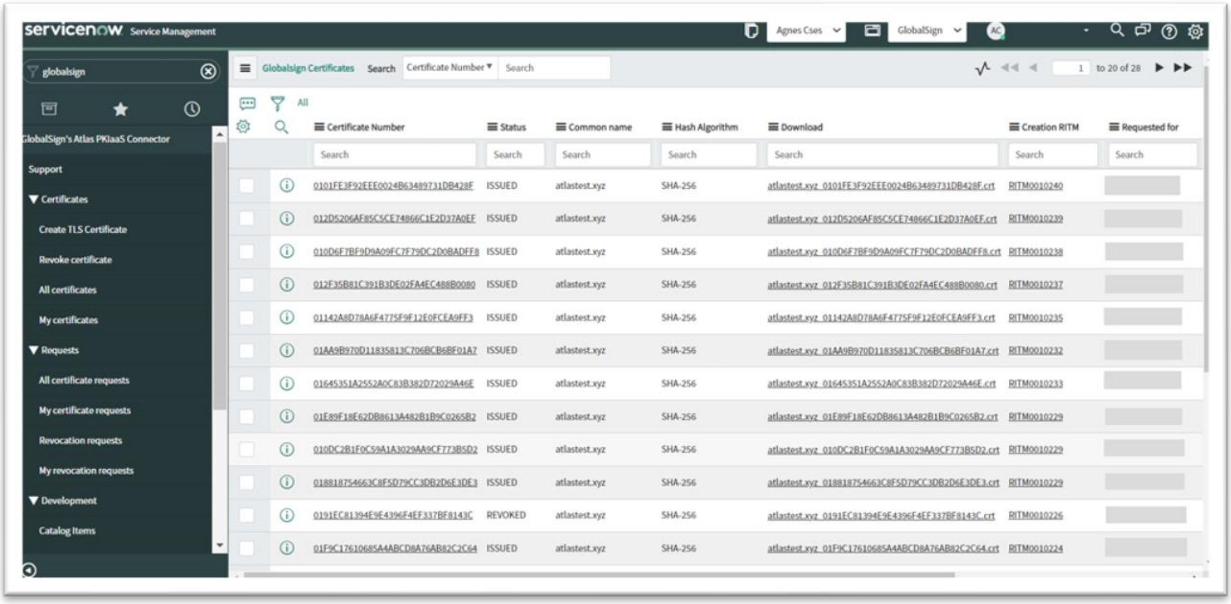
Note: If there was a failure, instead of creating work notes, we will see a Catalog Task created. Once the task has been resolved (and the API / connection has been restored), the user can resubmit their request.

Note: Using the certificate number you can also get your certificate details via the “Retrieve certificate” action.

Certificates

All certificates

All certificate what was requested via the “TLS certificate” catalog item are visible in the All certificates module. To click on the certificate number all details and activities will be available about the certificate. This menu item is available only for the administrator users.



Certificate Number	Status	Common name	Hash Algorithm	Download	Creation RITM	Requested for
Search	Search	Search	Search	Search	Search	Search
0101FE3F92EEE0024B63489731DB428F	ISSUED	atlastest.xyz	SHA-256	atlastest.xyz_0101FE3F92EEE0024B63489731DB428F.crt	RITM0010240	[redacted]
012D5206AF85C5CE74866C1E2D37A0EF	ISSUED	atlastest.xyz	SHA-256	atlastest.xyz_012D5206AF85C5CE74866C1E2D37A0EF.crt	RITM0010239	[redacted]
010D6F7BF9D9A09FC7F79DC2D0BADFF8	ISSUED	atlastest.xyz	SHA-256	atlastest.xyz_010D6F7BF9D9A09FC7F79DC2D0BADFF8.crt	RITM0010238	[redacted]
012F35B81C391B3DE02FA4EC488B0080	ISSUED	atlastest.xyz	SHA-256	atlastest.xyz_012F35B81C391B3DE02FA4EC488B0080.crt	RITM0010237	[redacted]
01142A8D78A6F4775F9F12E0FCEA9FF3	ISSUED	atlastest.xyz	SHA-256	atlastest.xyz_01142A8D78A6F4775F9F12E0FCEA9FF3.crt	RITM0010235	[redacted]
01AA9B970D11835813C706BCB6BF01A7	ISSUED	atlastest.xyz	SHA-256	atlastest.xyz_01AA9B970D11835813C706BCB6BF01A7.crt	RITM0010232	[redacted]
01645351A2552A0C83B382D72029A46E	ISSUED	atlastest.xyz	SHA-256	atlastest.xyz_01645351A2552A0C83B382D72029A46E.crt	RITM0010233	[redacted]
01E89F18E62DB8613A482B1B9C0265B2	ISSUED	atlastest.xyz	SHA-256	atlastest.xyz_01E89F18E62DB8613A482B1B9C0265B2.crt	RITM0010229	[redacted]
010DC2B1F0C59A1A3029AA9CF773B5D2	ISSUED	atlastest.xyz	SHA-256	atlastest.xyz_010DC2B1F0C59A1A3029AA9CF773B5D2.crt	RITM0010229	[redacted]
01881875466 3C8F5D79CC3DB2D6E3DE3	ISSUED	atlastest.xyz	SHA-256	atlastest.xyz_018818754663C8F5D79CC3DB2D6E3DE3.crt	RITM0010229	[redacted]
0191EC81394E9E4396F4EF337BF8143C	REVOKED	atlastest.xyz	SHA-256	atlastest.xyz_0191EC81394E9E4396F4EF337BF8143C.crt	RITM0010226	[redacted]
01F9C17610685A4ABCD8A76AB82C2C64	ISSUED	atlastest.xyz	SHA-256	atlastest.xyz_01F9C17610685A4ABCD8A76AB82C2C64.crt	RITM0010224	[redacted]

In the GlobalSign Atlas PKIaaS connection "All certificate" module you can find the following information about your certificate requests:

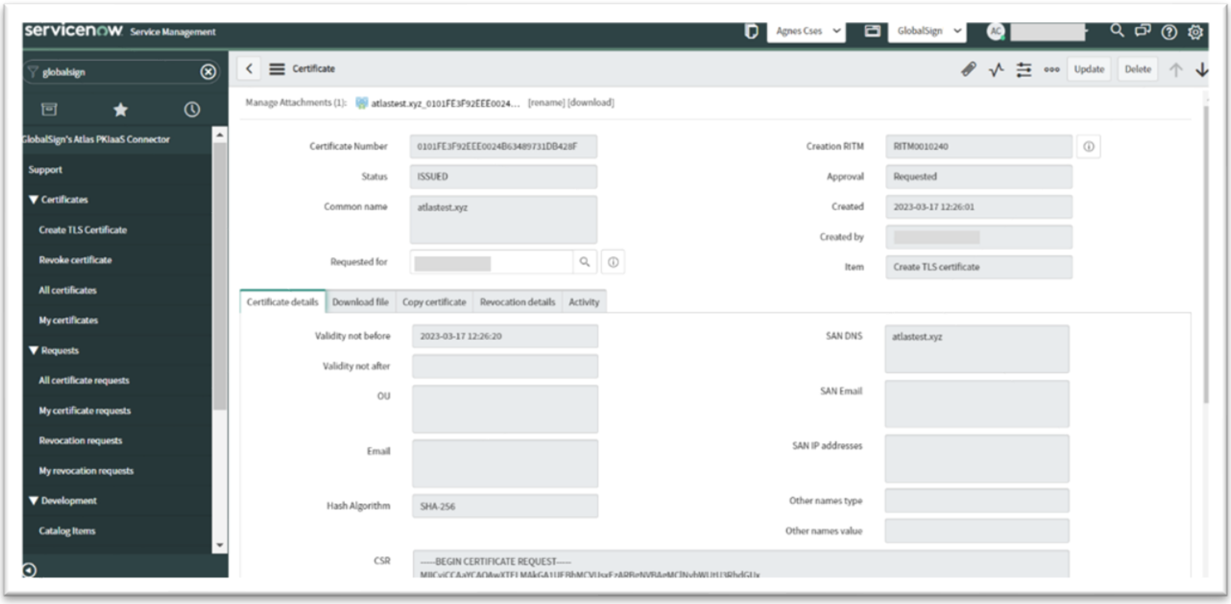
- Certificate number
- Create certificate request item
- Certificate status
- Certificate common name
- Hash Algorithm
- Requested for
- Certificate in the selected downloadable format (.pem or .crt or .txt based on Administration -> Application settings what can be managed by the administrator user role)
- Revocation reason
- Revocation request item
- Revoked by
- Revocation time

My certificates

All the details under the my certificates are same as for the all certificates but this module are filtered to the active users requested certificates.

Certificate details

After click on the certificate number on the "All certificate" or "My certificate" module, you can get all the certificate details.



Manage Attachments (1): atlastest.xyz_0101FE3F92EEE0024... [rename] [download]

Certificate Number: 0101FE3F92EEE0024B63489731DB428F

Status: ISSUED

Common name: atlastest.xyz

Requested for: [redacted]

Creation RITM: RITM0010240

Approval: Requested

Created: 2023-03-17 12:26:01

Created by: [redacted]

Item: Create TLS certificate

Validity not before: 2023-03-17 12:26:20

Validity not after:

OU:

Email:

Hash Algorithm: SHA-256

SAN DNS: atlastest.xyz

SAN Email:

SAN IP addresses:

Other names type:

Other names value:

CSR:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICyjCCAaYCAQAwXTELMAkGA1UEBhMCVUsxEzARBgNVBAgMClNvbWUtU3RhdGUx
```

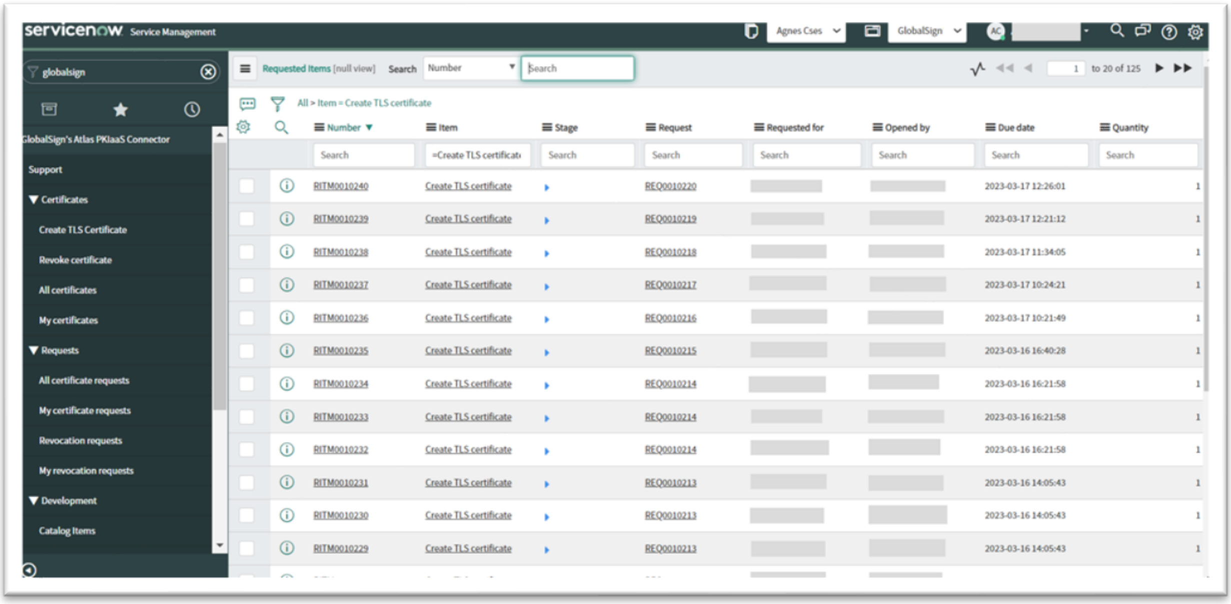
Under the certificate details are the following data available:

- Certificate creation details
- Certificate
- Downloadable file
- Revocation details
- Activity

Requests

All certificate requests

In the Requests menu you can find all the certificate requests, what contains all the default view information about the request items. In the details view you can see also the activities what was performed for the certificate request e.g. retrieve the certificate or revoke the certificate. This menu item is only available for administrator users.



All > Item = Create TLS certificate

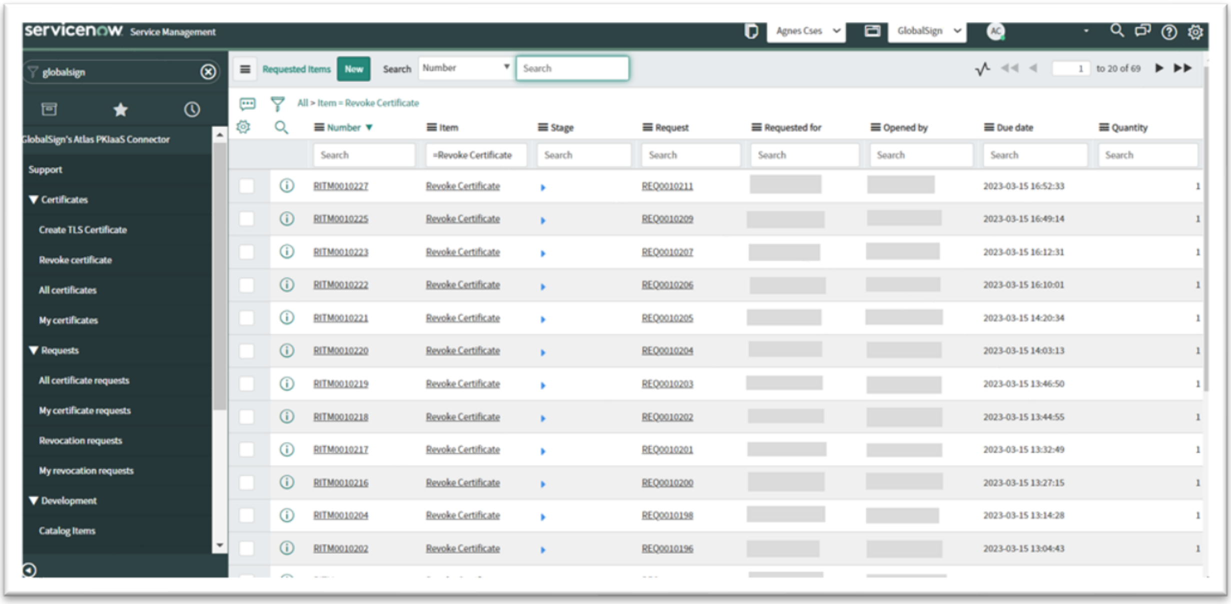
Number ▼	Item	Stage	Request	Requested for	Opened by	Due date	Quantity
Search	=Create TLS certificat	Search	Search	Search	Search	Search	Search
RITM0010240	Create TLS certificate	▸	REQ0010220	[redacted]	[redacted]	2023-03-17 12:26:01	1
RITM0010239	Create TLS certificate	▸	REQ0010219	[redacted]	[redacted]	2023-03-17 12:21:12	1
RITM0010238	Create TLS certificate	▸	REQ0010218	[redacted]	[redacted]	2023-03-17 11:34:05	1
RITM0010237	Create TLS certificate	▸	REQ0010217	[redacted]	[redacted]	2023-03-17 10:24:21	1
RITM0010236	Create TLS certificate	▸	REQ0010216	[redacted]	[redacted]	2023-03-17 10:21:49	1
RITM0010235	Create TLS certificate	▸	REQ0010215	[redacted]	[redacted]	2023-03-16 16:40:28	1
RITM0010234	Create TLS certificate	▸	REQ0010214	[redacted]	[redacted]	2023-03-16 16:21:58	1
RITM0010233	Create TLS certificate	▸	REQ0010214	[redacted]	[redacted]	2023-03-16 16:21:58	1
RITM0010232	Create TLS certificate	▸	REQ0010214	[redacted]	[redacted]	2023-03-16 16:21:58	1
RITM0010231	Create TLS certificate	▸	REQ0010213	[redacted]	[redacted]	2023-03-16 14:05:43	1
RITM0010230	Create TLS certificate	▸	REQ0010213	[redacted]	[redacted]	2023-03-16 14:05:43	1
RITM0010229	Create TLS certificate	▸	REQ0010213	[redacted]	[redacted]	2023-03-16 14:05:43	1

My certificate requests

All the details under the my certificate requests are same as for the all certificate requests but this module are filtered to the active users requested certificates.

Revocation requests

Under the revocation requests menu you can find all the revocation request for certificates.



Number	Item	Stage	Request	Requested for	Opened by	Due date	Quantity
Search	=Revoke Certificate	Search	Search	Search	Search	Search	Search
RITM0010227	Revoke Certificate	▸	REQ0010211	[redacted]	[redacted]	2023-03-15 16:52:33	1
RITM0010225	Revoke Certificate	▸	REQ0010209	[redacted]	[redacted]	2023-03-15 16:49:14	1
RITM0010223	Revoke Certificate	▸	REQ0010207	[redacted]	[redacted]	2023-03-15 16:12:31	1
RITM0010222	Revoke Certificate	▸	REQ0010206	[redacted]	[redacted]	2023-03-15 16:10:01	1
RITM0010221	Revoke Certificate	▸	REQ0010205	[redacted]	[redacted]	2023-03-15 14:20:34	1
RITM0010220	Revoke Certificate	▸	REQ0010204	[redacted]	[redacted]	2023-03-15 14:03:13	1
RITM0010219	Revoke Certificate	▸	REQ0010203	[redacted]	[redacted]	2023-03-15 13:46:50	1
RITM0010218	Revoke Certificate	▸	REQ0010202	[redacted]	[redacted]	2023-03-15 13:44:55	1
RITM0010217	Revoke Certificate	▸	REQ0010201	[redacted]	[redacted]	2023-03-15 13:32:49	1
RITM0010216	Revoke Certificate	▸	REQ0010200	[redacted]	[redacted]	2023-03-15 13:27:15	1
RITM0010204	Revoke Certificate	▸	REQ0010198	[redacted]	[redacted]	2023-03-15 13:14:28	1
RITM0010202	Revoke Certificate	▸	REQ0010196	[redacted]	[redacted]	2023-03-15 13:04:43	1

My revocation requests

All the details under the my revocations requests are same as for the all certificates but this module are filtered to the active users requested to revoke certificate.