



**MHHS
PROGRAMME**
Industry-led, Elexon facilitated

DIP Domain & Certificate Renewal Guide

PPC – Internal V1.0 Approved

MHHS-DEL3351

December 2024

1.0 Content and Control

Updates to DIP Certification & Domain Renewal Guidance

Date	Author	Version	Change Detail
11/12/2024	Piotr Penar	V1.0	

Key Terminology Explained

Term	Description
DIP	Data Integration Platform
DIP SP	Data Integration Platform Service Provider
PP	Programme Participant
DVC	Domain Verification Code
AKV	Azure Key Vault
MtLS	Mutual Transport Layer Security
GS	GlobalSign
SSL	Secure Sockets Layer

2.0 DIP Certification and Domain Renewal Guide

2.1 Introduction

During SIT Functional, the DIP Service Provider (DIP SP) supported programme participants with the following tasks:

- Domain Verification - a periodic activity, initially annual, required following GlobalSign vetting¹
- Renewal of DIP Certificates - an annual activity as each certificate generated by a PP expires 12 months from the creation date²

This pack sets out the steps that were covered by the DIP SP during the support sessions and are for programme participant (PP) reference, including:

- Steps for Domain Reverification
- Steps for Certificate creation/recreation using Azure Key Vault
- Advice for OpenSSL users
- Frequently Asked Questions

Please note: this pack is intended as a supplement to existing DIP materials, notably including the DIP Onboarding Guide.

1 *The frequency of domain reverification remains under review and further guidance will be provided once this has been confirmed*

2 *The DIP SP recommends renewal of a certificate in the two months before the expiration date to ensure uninterrupted access to DIP messaging*

2.2 Required Roles

To successfully reverify a domain and renew DIP certificates, the following roles are required:

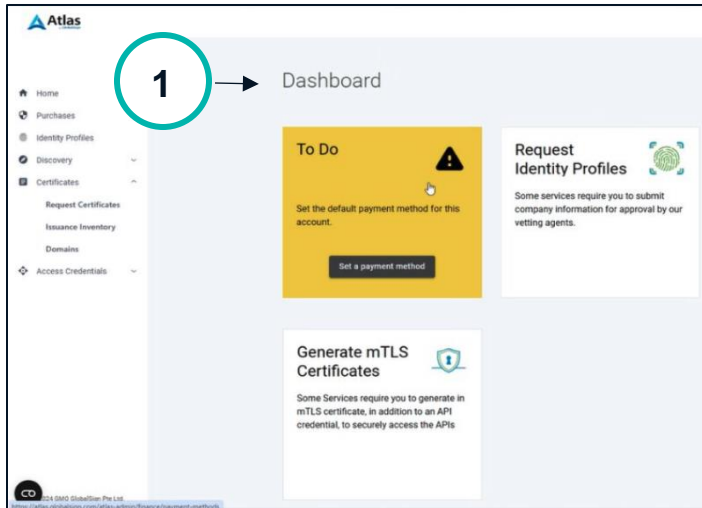
- A user previously registered in the GlobalSign Atlas Portal for the PP organization
- A Subject Matter Expert (SME) who can add a text record to the PP organization's own Domain Name System (DNS)
- A Certificate Administrator in the DIP Portal with ability to or supported by an SME who can generate a Private Key and Certificate Signing Request



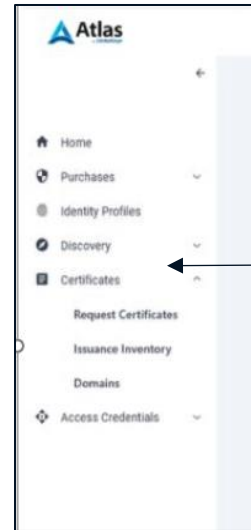
**MHHS
PROGRAMME**
Industry-led, Elexon facilitated

Domain Reverification

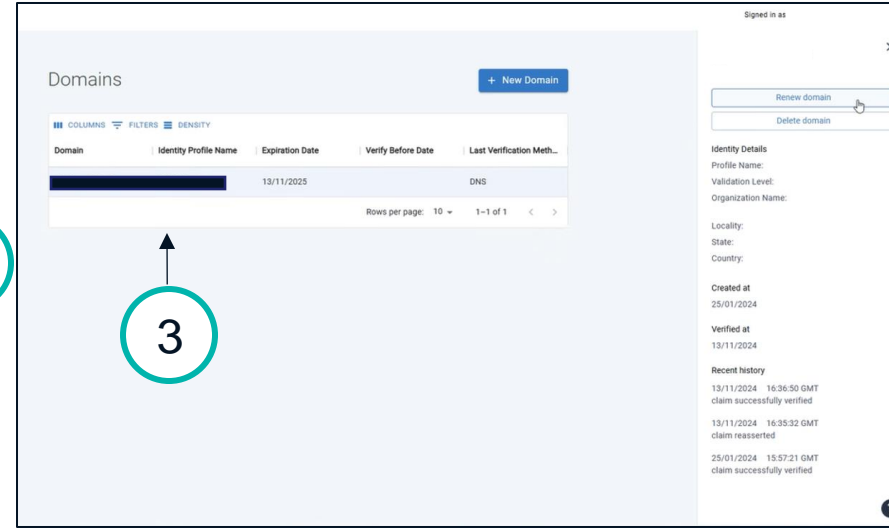
3.0 Domain Reverification



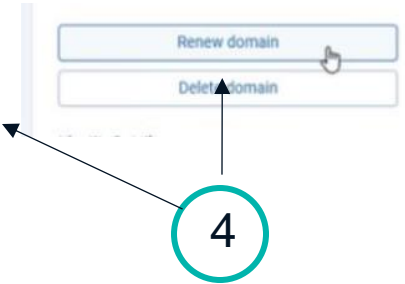
- 1) Registered user on GlobalSign Atlas Portal to sign in and navigate to the Dashboard:
<https://atlas.globalsign.com/>



- 2) On left hand menu click on 'Certificates' and then click on 'Domains'.



- 3) Select expiring or near expiring domain.



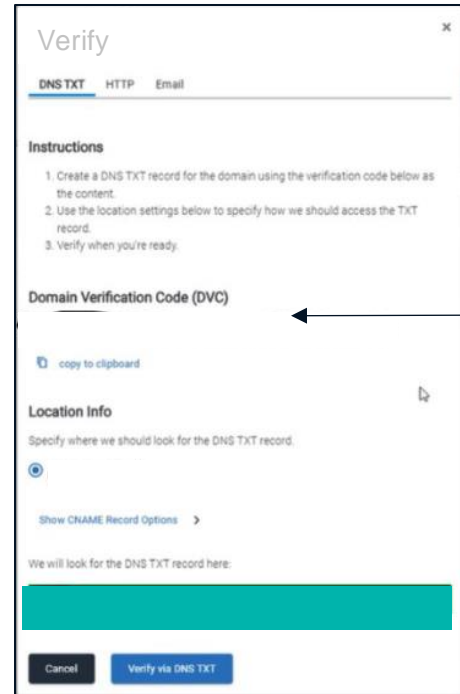
- 4) Click **Renew Domain** on the right-hand side.

3.0 Domain Reverification (continued)

5

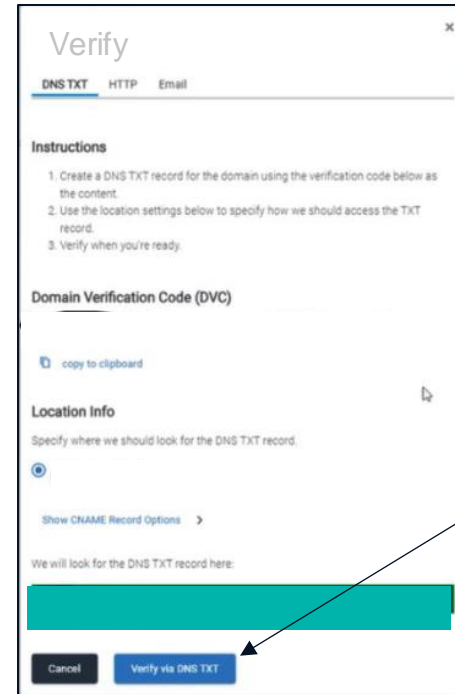


5) Then click again on the right-hand side on [Verify Domain](#).



6) This will give you [DVC string](#) that can be copied and added as a [DNS TXT record](#) for DNS.

6



7) Once the SME for DNS has made the appropriate configurations, click [Verify via DNS TXT](#). It can take time for Atlas to show the updated expiration date due to DNS propagation.

7

Verify via DNS TXT

Participants should note the new expiration date; domain verification needs to be completed before this expiry date.



**MHHS
PROGRAMME**
Industry-led, Elexon facilitated

Renewal of DIP Certificates

4.0 DIP Certification

4.1 Certificate Admin: Generate mTLS & Signing Cert within the DIP

The process for renewing DIP certificates follows a similar flow that was used for creation of certificates as part of DIP Onboarding.

1 Login to the DIP portal as a certificate Admin.

2 Select MP Menu

3 Click the 'Certificates' Tab, the 'Create Certificate'.

4 Enter the required Host Name & Domain.

5 Select 'Certificate Purpose' to choose a mTLS (for DCPs), "Signing" (for MPs) or mTLS & Signing certificates (both).

6 The SUBJECT NAME is pre-set – click 'COPY'.

Enter both fields: overall this should make up the address you want to receive messages on from the DIP (e.g. `sit-dipwebhook.testmp.co.uk`) where First part is Host Name and second is Domain Name.

Certificate Signing Request Form
This form is used to submit your certificate signing request (csr) to be signed by the DIP certificate authority (Global Sign). You will then be able to download the signed public key (csr) which you will then bind with private key you used to create your csr and thus creating your mTLS certificate, active for use when integrating with the DIP.
Before making a signing request, please ensure you have completed the necessary GlobalSign onboarding and domain verification process, more details can be found on the [GlobalSign website](#).
Please ensure that the details entered match those used during the organisation onboarding, setting and verification process.

Host Name: Domain:

Certificate Purpose:

Subject Name: Copy

4.0 DIP Certification

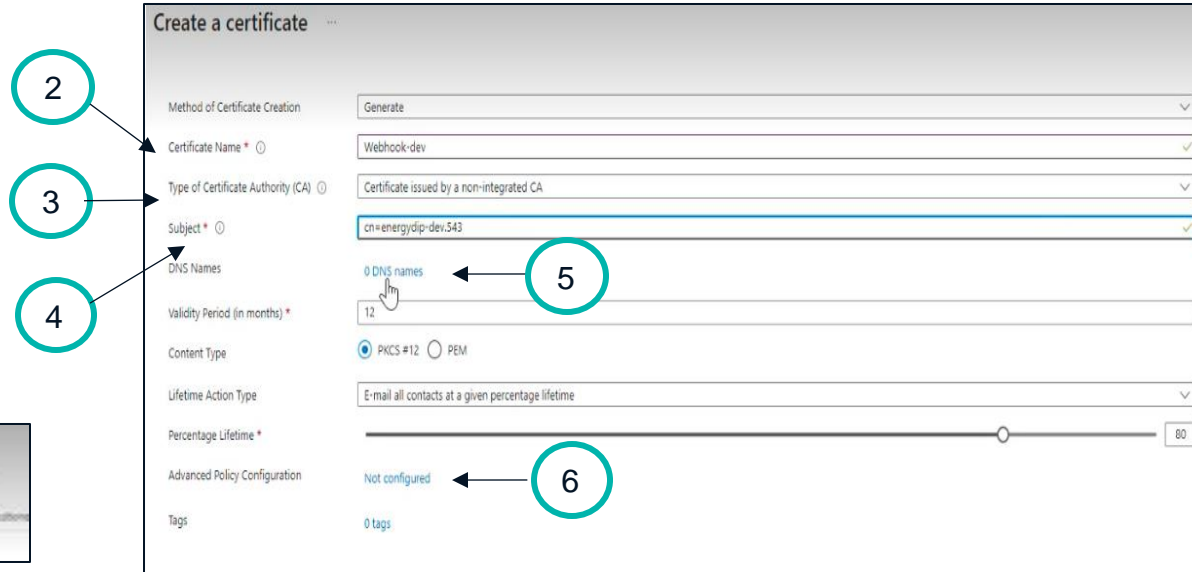
4.2 Certificate Admin: Generate mTLS & Signing Cert within the DIP (continued).

*It is critical a new CSR is generated using the details from the previous steps on the previous slide. To begin, open your chosen Certificate Creation Tool (this example uses Azure Key Vault)



1

1 Click 'Select' to generate a certificate (in AK click Generate/Import).



2

3

4

5

6

2

Certificate name: Give the certificate a name (no spaces).

3

Type of Certificate Authority, choose 'Certificate used by no-integrated CA' from the drop down.

4

Subject: Enter 'cn=' then paste the SUBJECT NAME copy from 4.1 (previous slide) step 6.

5

IMPORTANT – click 'DNS Names' which will open a pop up and complete the 2 entries.

6

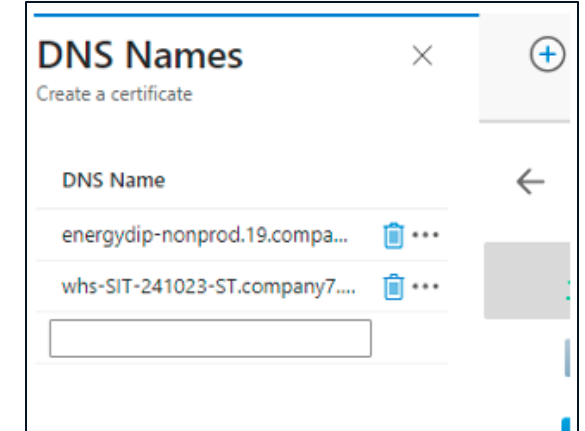
Click **Not configured** and ensure Key Size is 4096.

7

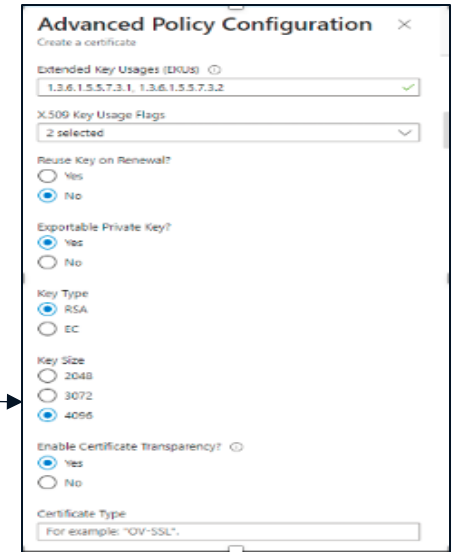
To complete the certificate creation, click 'create' button.

5

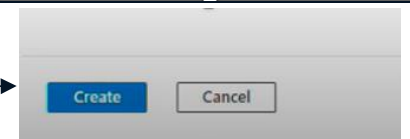
Enter the Host Name & Domain copy from 4.1(previous slide) step 4 & 6.



6

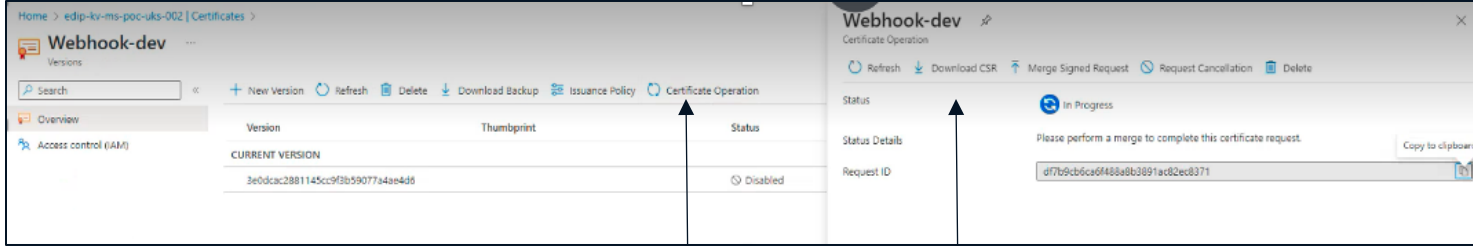


7

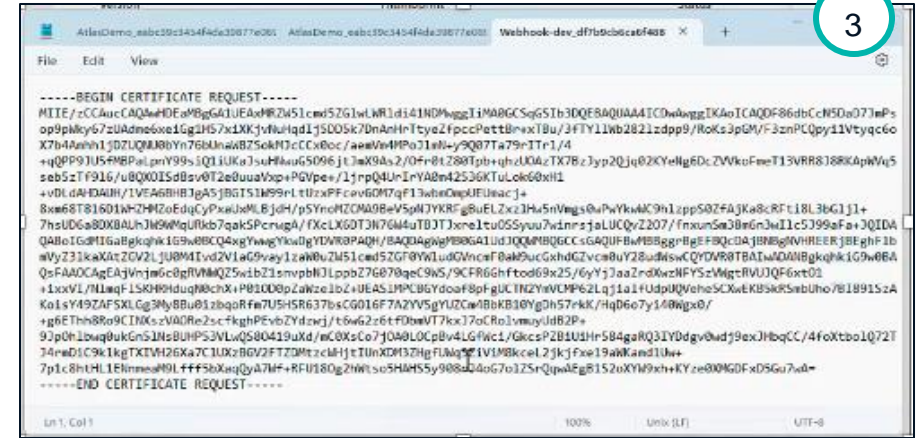


4.0 DIP Certification

4.3 Certificate Admin: Generate mTLS & Signing Cert within the DIP



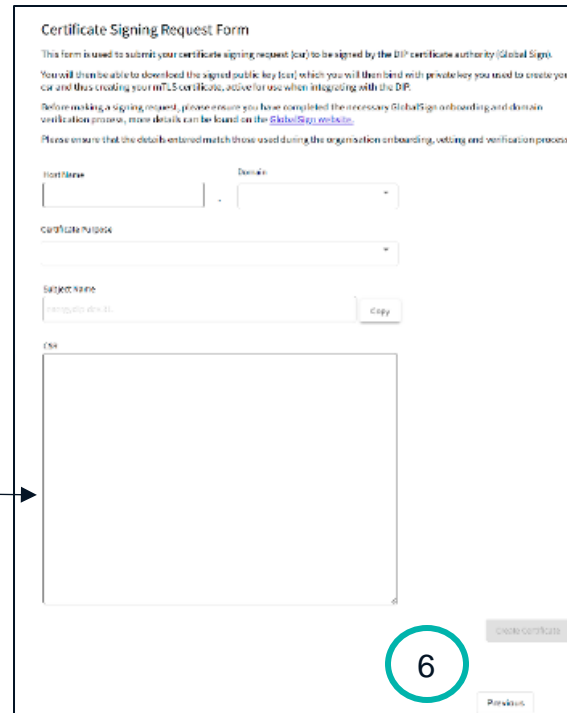
- 1) Select 'Certificate Operations'.
- 2) Select 'Download CSR'.



- 3) Open the downloaded file in a test editor



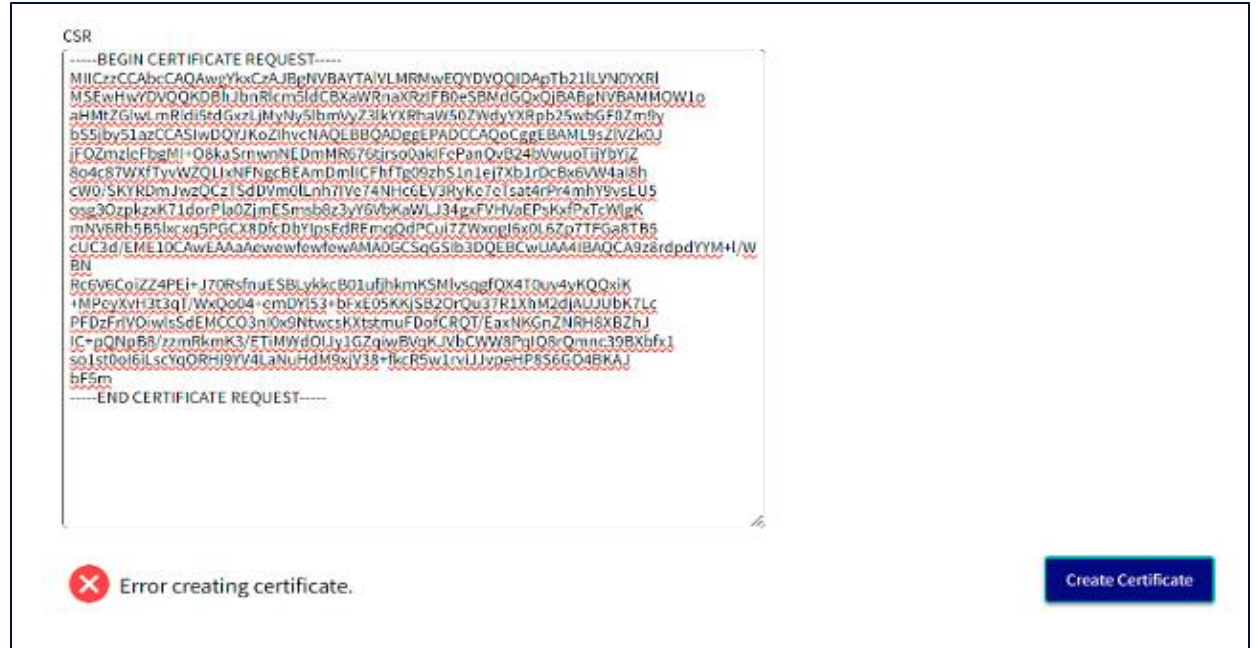
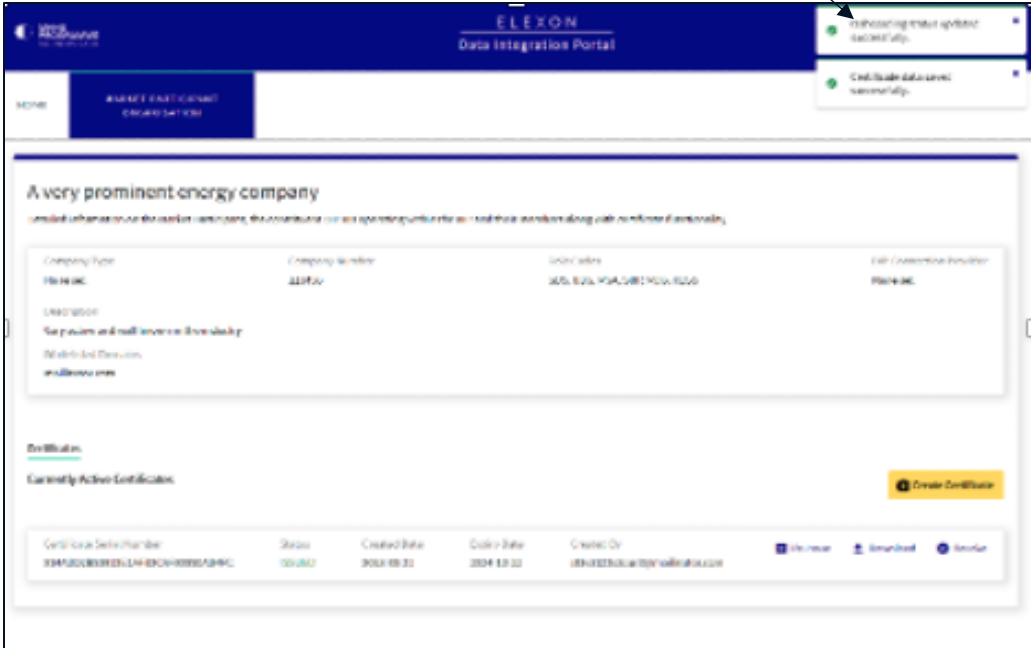
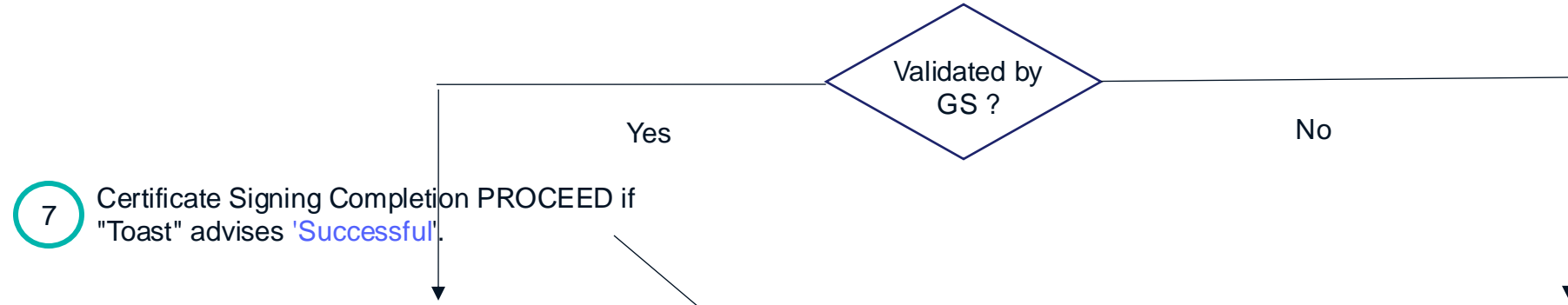
- 4) Select the Certificate Text



- 5) PASTE the Certificate Text into the CSR field in DIP

- 6) Click 'Create Certificate'

4.4 Certificate Admin: Generate mTLS & Signing Cert within the DIP (continued)



8 If an **ERROR** appears please repeat steps from slide 4.2,4.2 and 4.3 (previous 3 slides).

4.0 DIP Certification

4.5 Certificate Admin will check certificate is now ACTIVE within the DIP

The Certificate Admin will be presented with a list of certificates associated with the organisation and can DOWNLOAD the ACTIVE certificate

1) The list of your available certificates are displayed within Market Participant menu.

The screenshot shows the ELEXON Data Integration Portal interface. The 'Market Participant' menu is highlighted. Below it, the 'Certificates' tab is selected, displaying a table of certificates. A yellow warning banner indicates that the currently active certificate is expiring in 11 days. The table lists the following certificates:

Certificate Serial Number	Status	Created	Expiry Date	Created By	Actions
7348000010	Active	2022-11-15T15:12:00.147Z	2023-11-15T15:12:00.147Z	Peter Macintosh	Download
7348000009	Active	2022-10-15T12:12:00.147Z	2023-10-15T12:12:00.147Z	Rodrigues M. Washinton	Download
7348000008	Expired	2021-11-20T10:12:00.147Z	2022-11-20T10:12:00.147Z	Peter Macintosh	Download

- 2) Click 'Certificates' tab.
- 3) Check certificate is ACTIVE.

4) Click **Download** to utilise the new ACTIVE certificate.

The screenshot shows a Windows Certificate dialog box with the 'Details' tab selected. The 'Certificate Information' section displays the following details:

- Issued to: GLOBALSIGN TEST CERTIFICATE PURPOSES ONLY
- Issued by: GlobalSign Non-Public HVCA Demo
- Valid from: 07/09/2023 to 06/12/2023

The 'Details' section shows the following fields and values:

Field	Value
Serial number	0191bbfc28504de8036f8116...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	GlobalSign Non-Public HVCA D...
Valid from	07 September 2023 12:53:58
Valid to	06 December 2023 12:53:58
Subject	GLOBALSIGN TEST CERTIFICA...
Public-key	RSA (2048 Bits)

5) Open the downloaded Certificate file and Click 'Details' Tab.

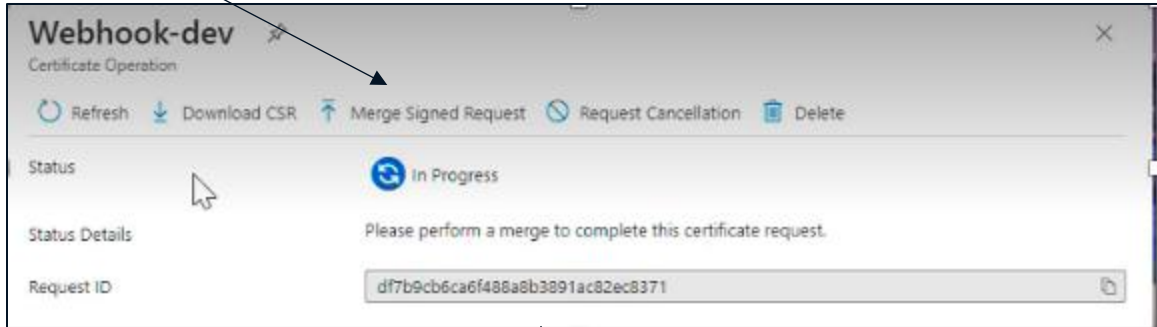
6) Check validity by checking **Serial Number** matches and **Subject** is as expected.

4.0 DIP Certification

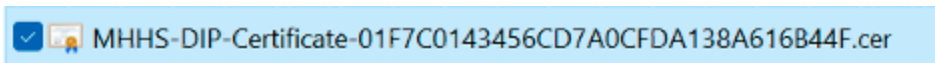
4.6 Merge the signed certificate

Final stage of the process must be conducted within the Certificate Generation tool chosen earlier (e.g. Azure Key Vault)

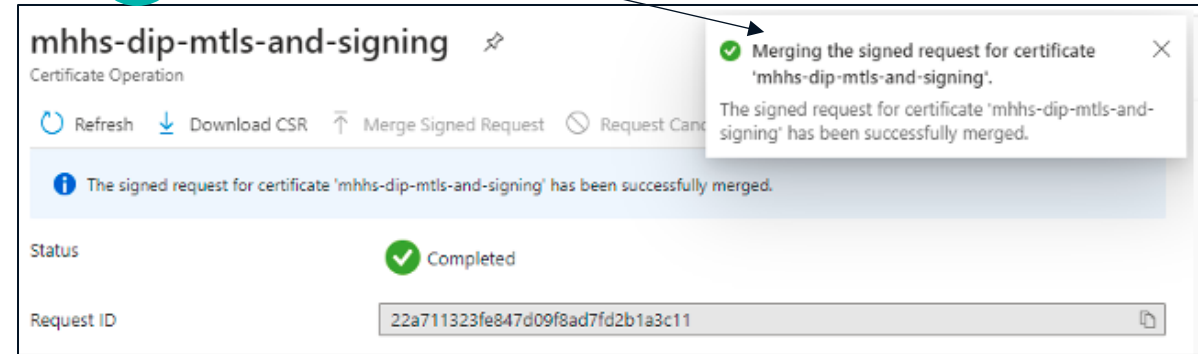
- 1 Select menu option 'Merge Signing Request' (or similar option).



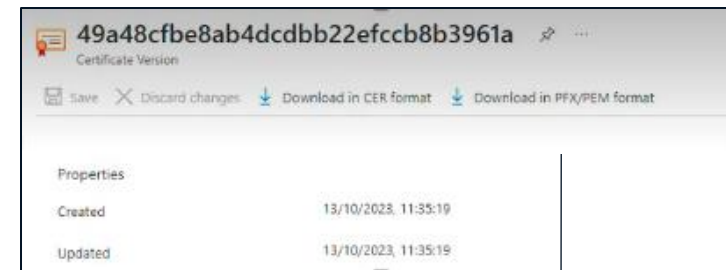
- 2 Select the file downloaded from the DIP Portal (a .cer file – example shown below)



- 3 A 'toast' pop up will confirm the merge was successful.

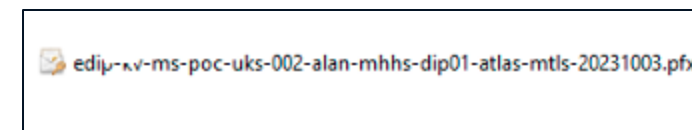


- 4 The certificate must now be downloaded as a PFX WITHOUT Password. Select the certificate and choose 'Download in PFX/PEM Format'.



- 5

This certificate is now available to be used mTLS and signing when sending messages to the DIP.



If you are using a DCP you MUST arrange for your DCP to have this certificate to send messages to DIP



**MHHS
PROGRAMME**
Industry-led, Elexon facilitated

Advice for Open SSL users

5.0 Open SSL Commands required during onboarding

API Credential Certificate

To generate the CSR and Private Key:

```
openssl req -new -newkey rsa:4096 -nodes -keyout apicert.key -out apicert.csr -subj "/CN=<enter API credential Subject Name Here>"
```

To merge the Private Key and Certificate into a PFX:

```
openssl pkcs12 -export -out apicert.pfx -inkey apicert.key -in apicert.cer -password pass:
```

mTLS/Signing Certificate

To generate the CSR and Private Key:

```
openssl req -new -newkey rsa:4096 -nodes -keyout mtls-cert.key -out mtls-cert.csr -subj "/CN=<enter Subject Name here>" -addext "subjectAltName = DNS:<enter Subject Name here>, DNS:<enter Hostname plus Domain here>"
```

To merge the Private Key and Certificate into a PFX:

```
openssl pkcs12 -export -out mtls-cert.pfx -inkey mtls-cert.key -in mtls-cert.cer -password pass:
```



**MHHS
PROGRAMME**
Industry-led, Elexon facilitated

Frequently Asked Questions

Can I generate a new certificate if my domain verification has expired?	No, GlobalSign does not allow you to do this.
Do I need to maintain my domain verification to send and receive messages from DIP?	No, domain verification is only checked when interacting with GlobalSign, such as when creating or renewing certificate. Your certificates remain valid until their expiration date or until they are revoked.
Does creating a new certificate invalidate the previous one?	No, your certificates are valid until their expiration date or until they are revoked. You can use both new and old certificates simultaneously. This allows you to replace your certificate within your desired maintenance window.
Can I have more than one GlobalSign Atlas portal administrator?	Yes, it is recommended to have more than one administrator. Please refer to https://support.globalsign.com/atlas/general-category-faqs/account-related-faqs for additional details.
What is Certificate reissue in DIP?	The certificate reissue feature in DIP allows you to create a new instance of your existing certificate with a new serial number. Please note that this feature does not extend the validity period of your certificates.
Do I need to renew each expiring Certificate?	Yes, you must repeat the renewal steps for each expiring certificate and domain if you are using more than one certificate.
Is the hostname mandatory when creating a Certificate?	Yes, a hostname is mandatory in DIP, even for signing certificates. However, please note that DIP does not verify the hostname for signing certificates when checking the signature.
How can I get more support?	For issues related to domain verification or accessing the Atlas portal, please contact Atlas Support at support-atlas@globalsign.com For issues relating to use of the DIP Portal, please contact DIP Support at support@energydataintegrationplatform.co.uk .