
E2E Onboarding Guide

Document owner
MHHS/DIP Manager

Document number

Version
V4.0

Status:
For Review

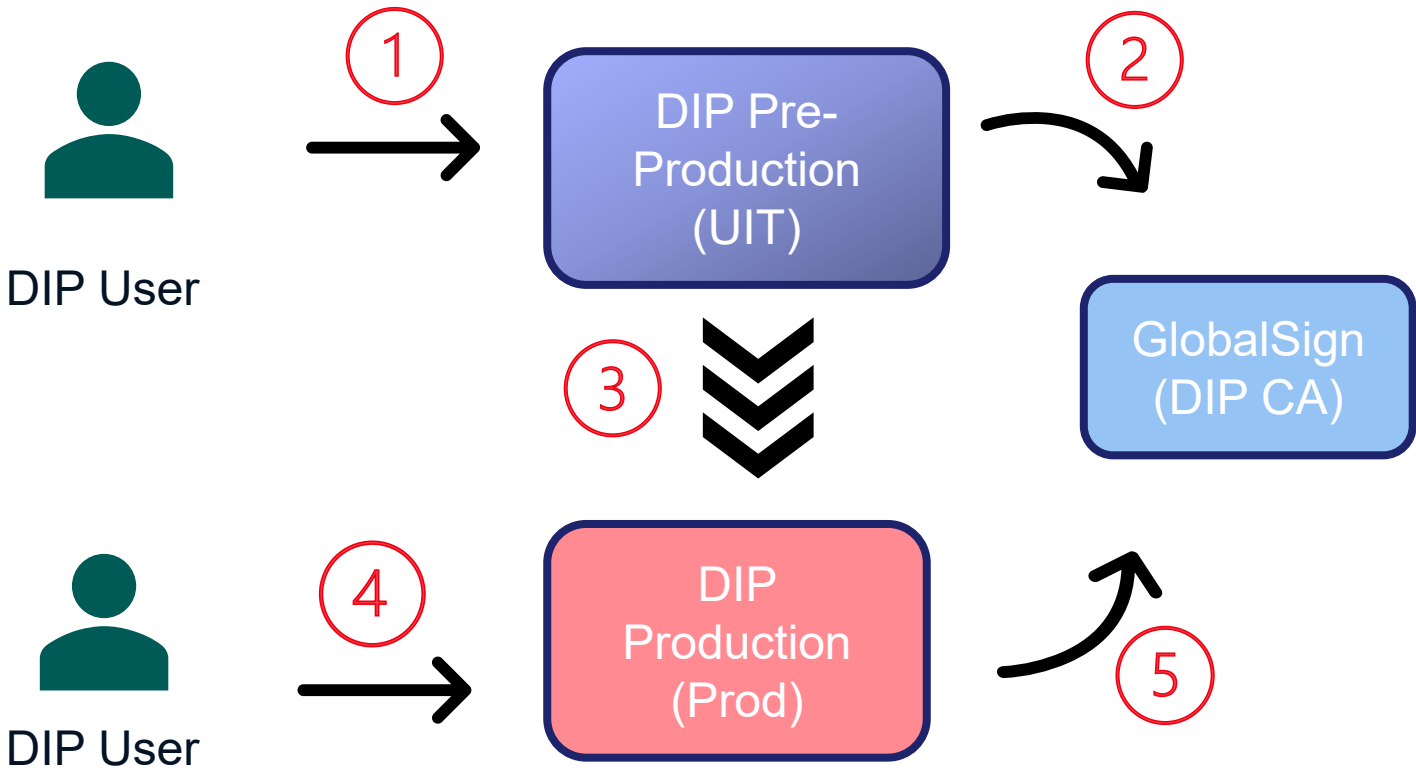
Date
17/06/2025

Data Integration Platform

The MHHS Data Integration Platform (DIP) is provided by Elexon and developed by Avanade to allow the different Market Participants in the electricity market to exchange messages.

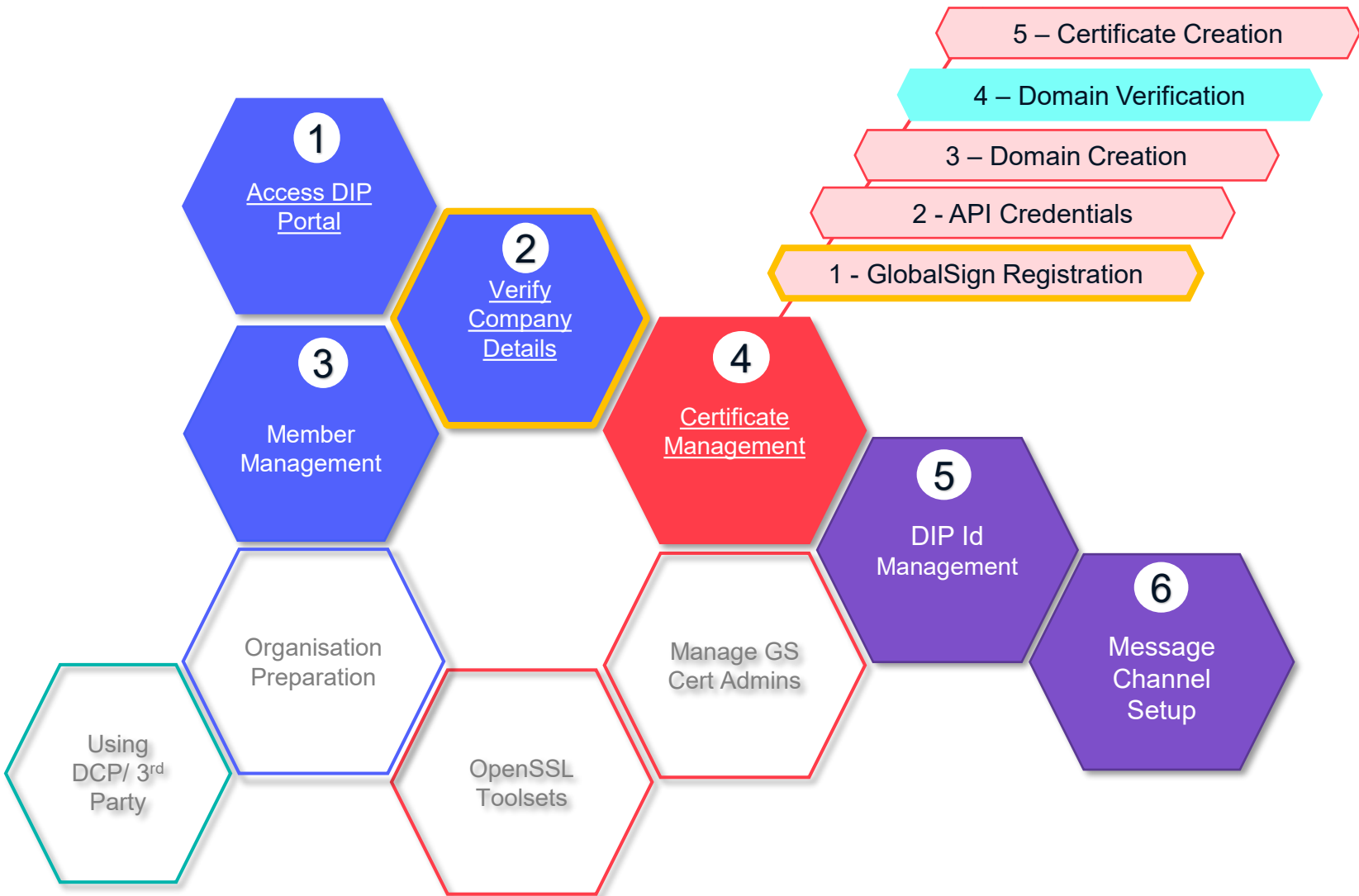
The onboarding guide provides a step-by-step instructions to enable a Market Participant (MP) to complete all tasks required to successfully onboard to the DIP and will be available for when Parties need to on-board.

DIP Onboarding Overview – Full Journey




- 1 DIP User receives an invitation to on-board to the Pre-Production DIP where they will carry out their qualification testing
- 2 As part of this initial on-boarding the organisation will need to undertake the following:
 - Setup organisation including Users in DIP
 - Onboard to GlobalSign the DIP CA
 - Generate GlobalSign cert & API key
 - Set-up DIP Ids & Message Channels
- 3 Once an Organisation has successfully passed qualification testing their Organisational set-up is moved to Production by the DIP Manager Team. This does not include their User base as this could be a different set of people.
- 4 DIP User will receive an invitation to the Production DIP environment with a new set of Users
- 5 New API keys & PFX certificate is required for communication with Production DIP


DIP Onboarding Overview – Pre-Production Environments





MP Organisation

 **Primary Admin**


DIP Roles


 **User Admin**

 **Message Admin**

 **Certificate Admin**

non-DIP Role

 **DNS Admin**

 **DIP Manager**

Support and Assistance

The process to on-board to the DIP has many intricate steps. We fully believe that if prepared correctly, these steps should complete successfully and allow a smooth on-boarding, however, we understand that sometimes things do not go as you expect, and a helping hand is needed.

If this situation arises, please send an email to DIPManager@elexon.co.uk with your contact details, description of the step/stage you have reached, a short description of the problem you have encountered and someone will respond as soon as possible.

Preparation Reminder

Before on-boarding please complete the following actions:

1. Have ready the assigned Primary & Certificate Admin details
2. Have your registered Company Name, the associated Company Number and a brief company description
3. Have your DNS admin prepared and ready for the DNS activity
4. Have your Certificate Admin, with the ability to manage through the conversion of certificates, on hand to assist (Section 4 and 5)
5. For non-BSCCo/RECCo qualified parties, i.e. DCPs and MDRs, a signed DIP access agreement.
6. Familiarisation with the [DIP Rules](#)

Post On-boarding

Ensure you have set up to optimise your DIP experience:

1. Read the DIP User Guides to understand the functions and features in detail
2. Ensure at least 2 each of User Admin, Certificate Admin and Message Admin are invited and joined the DIP to allow cover during holiday or absence situations
3. Remember that members can have multiple roles – use according to your needs
4. Non-Prod & Production - different users, different certificates but only one GlobalSign registration



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

Preparation Activities #1

Organisational Set-up

Organisation Prep Activities : Identifying individuals/Teams for DIP User Roles

When you receive your on-boarding proforma you will be asked for details about your organisation, this information is essential when you start to onboard.

Within the DIP there are four Market Participant member roles which can be assigned. Any organisation member invited to the DIP can have either a single role or be assigned multiple roles (allowing all four assigned to one person).

The individuals appointed in the Pre-Production do not carry over to Production as responsibilities within companies can vary between Production and non-Production environments.

Role	Description
User Admin	The User Admin is the person who will receive the invitation from the DIP Team to join the DIP. The User Admin role, when assigned to any member, provides the functions to add other DIP Members and manage DIPIDs.
Certificate Admin	The Cert Admin is responsible for all certificate management, including registration, GlobalSign verification, completion of the certificate upload, and ongoing certificate maintenance. Given the scope of the role this may be multiple people at different parts of the process.
Message Admin	Will have the control and ownership of all activities relating to message processing, replay and management.
Analytics Reader	Will only have access to review the DIP Dashboard feature.
DNS Admin	Not a DIP login. Needs access to organisation DNS to create TXT record for certificate validation

The table below outlines the DIP Portal tabs accessible to users based on their roles

<div><div>Roles</div><div>DIP Portal Tabs</div></div>	Market Participant Org	Message Channels	Messages	Performance
MP User Admin	Manage Users <i>(Create/Edit/Extend/Offboard)</i>			
MP Certificate Admin	Manage Certificates <i>(Create/Reissue/Download/Revoke)</i> View/ Generate API Keys			
MP Message Admin	Manage DIP Ids <i>(Request/Edit/Delete)</i>	Manage URLs <i>(Configure Status Message & Publication URLs, Replay/Requeue received messages)</i>	View sent messages	View performance reports for their Org(s)
MP Analytics Admin	View Org details			View performance reports for their Org(s)

Use of DIP Connection Providers

DIP Connection Providers (DCPs) are third-parties that provide IT services to Market Participants, the range of services can vary from providing hosted solutions to fully managed platforms. It is possible to delegate responsibility of some of the on-boarding tasks and ongoing DIP management functions to a DCP.

There are two options by which Market Participants can integrate DCPs within their DIP organisation:

1. **Full Company/DCP Integration** – where the DCP organisation is fully integrated in the Market Participant's company and are effectively a single organisation. The access for individuals within both companies is controlled by the roles and DIP Ids assigned to them.
2. **DIP Id Management** - where the DCP organisation has visibility of their clients DIP Id once the link between DIP Id & DCP ID is made by the client Market Participant.

DCPs that have multiple clients using the DIP can effectively be on-boarded multiple times. DCPs have the ability to switch 'context' i.e. organisations from within their portal.

Some of the initial key on-boarding steps **must** be undertaken by a full-time employee of the Parent MP, i.e. Initial DIP invitation to validate company details and the Global verification process.



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

Preparation Activities #2

OpenSSL

Choice of OpenSSL Toolset

PKCS certificates have a dual role in securing communication channels between DIP Users and the DIP, firstly for signing messages and secondly for securing mTLS connections. PKCS certificates will need to be generated by DIP Users once provided with API keys and secrets provided by both GlobalSign and the DIP

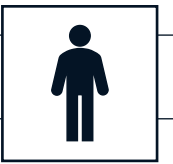
An internet search of SSL Toolsets will produce a plethora of results. Avanade uses Azure Key Vault to produce and manage PKCS certificates, whilst the DIP manager has used OpenSSL from a bash script on Windows. Both are acceptable and work, please consult your relevant IT teams for assistance on this topic.

Examples for both Azure Key Vault and OpenSSL (bash) are provided in the on-boarding guidance documentation.



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

Section 1 – Accessing the DIP Portal



The Invitation to Join the DIP

The process for on-boarding will commence with the Market Participant's (MP) nominated **Primary Admin** receiving an email from the Programme **DIP Manager/Team** (portal@Energydataintegrationplatform.co.uk) inviting them to join the DIP: The DIP Manager/Qualification Team will contact your organisation prior to your on-boarding to receive the name of the MP User Admin.

The email sent to the Primary Admin will contain a link to the DIP 'Sign in' home page which is shown in the forthcoming pages.

Multi-Factor Authentication (MFA) is a mandatory set up for all users who will be accessing the DIP. The MFA set up will initiate during the first sign in of each invited user and an MFA request will occur each time any user signs in thereafter.

Once the MP Admin has been set-up, they then have the control of sending out invites to other people within their organisation who will undertake the different activities within the DIP (described on the previous page). The steps are the same for all DIP Users after they have received the Invitation e-mail. All logins are via DIP Users company e-mail address names.

Preparation

1. Have MS Authenticator available on your phone to enable MFA
2. Complete and return your **DIP Onboarding Preparation Pro-Forma** to MHHSQualification@elexon.co.uk

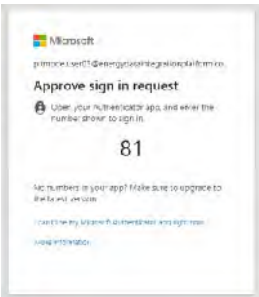
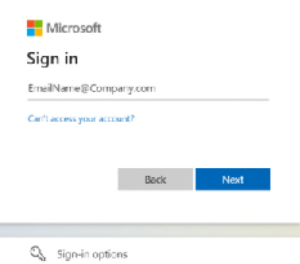
If you do not receive the invite, once you are advised it has been sent, please use this link to get started:
[Https://portal.uit.energydataintegrationplatform.co.uk](https://portal.uit.energydataintegrationplatform.co.uk)

You should ensure this is WHITE listed and is not subject to quarantine or a suspected phishing delay.



Access via the DIP Portal is via e-mail & password with MFA

- 1
- Click SIGN IN
-
- 2
- Sign in with email/password
-
- 3
- Complete MFA
-
- 4
- Read & Accept Term of Use (first time only)



Portal Area	Description
1	Identity of the logged in user
2	ELEXON Header Bar
3	Navigation/Menu options
4	Welcome Area
5	Common tools and Quicklinks

In the UIT environment the portal will have Yellow banners/menus



Section 2 – Verify Company Details

This is a one-off task undertaken by the Primary Admin for the organisation. The User Admin must enter/check the company details and has the option to create additional users (this can also be achieved at a later stage)

Optional

5

6

7

8

9

The screenshot shows the 'DIP Market Participant Organisation onboarding form' with the following sections and steps:

- Step 1:** Form title and instructions.
- Step 2:** 'Market Participant Organisation' section with a note to ensure company information is correct.
- Step 3:** 'Company Name' field with 'Example Company' as placeholder text.
- Step 4:** 'Company Description' text area with 'All the information supporting this example' as placeholder text.
- Step 5:** 'Company Number' field with '123456' as placeholder text.
- Step 6:** A checkbox labeled 'Please check this box to request your organisation to be DIP Connection Provider'.
- Step 7:** 'Users' section with a note to add additional users.
- Step 8:** A red '+' icon in the 'Users' section, with a red arrow pointing to the 'Create New User Profile' modal.
- Step 9:** 'Market Participants' section with a note to add market participants.
- Step 9:** A red '+' icon in the 'Market Participants' section.
- Buttons:** 'Cancel' and 'Submit' buttons at the bottom left.

The 'Create New User Profile' modal contains the following fields and options:

- First Name:** Text field with a red error message 'First Name is required'.
- Last Name:** Text field.
- Email Address:** Text field with a red '@' symbol.
- Member of All DIP IDs:** A radio button option.
- Select Organisation Role:** A dropdown menu.
- Select DIP IDs:** A dropdown menu.
- Note:** 'Note: If you require a domain which isn't listed, please contact the DIP Admin for it to be whitelisted.'
- Buttons:** 'Cancel' and 'Confirm' buttons at the bottom right.

Callouts and annotations:

- Callout 1:** A red box with the text 'Enter full name and email of the user' pointing to the 'First Name' and 'Email Address' fields.
- Callout 2:** A red box with the text 'Select the user role from the drop down (a user can have multiple roles)' pointing to the 'Select Organisation Role' dropdown.
- Callout 3:** A red box with the text 'Select the pertinent DIP IDs the user has access to. Defaults to All DIP IDs' pointing to the 'Select DIP IDs' dropdown.



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

Section 3 – Member Management



Member management is accessible from the Members sub-tab from the main Market Participant Organisation page

MHHS PROGRAMME

Member Data Network

ELEXON

Data Integration Portal

PL

HOME

MARKET PARTICIPANT ORGANISATION

MESSAGE CHANNELS

Super Energy Co

Detailed information on the Market Participant, the constituent DIP IDs operating within the DIP and their members along with certificate functionality.

Nominate DIP Connection Provider

Company Type	Company Number	Role Codes	DIP Connection Provider
Supplier, Distributor	1234567	SUP1, SDS, MDR, ADS, EES, SUP	None set
Description			
Our company is...			
Whitelisted Domains			
superenergy.co.uk, energydataintegrationplatform.co.uk, mailinator.com, accenture.com, energydataintegrationplatform.co.uk, accenture.com, evnade.com, pldipportslonmicrosoft.com			

DIP IDsMembersCertificates

Create MemberFilterSearch

A Cert Admin and a Message Admin need to be added as a first task to enable the on-boarding process

MHHS PROGRAMME

Member Data Network

ELEXON

Data Integration Portal

PL

HOME

MARKET PARTICIPANT ORGANISATION

Energy Demo Ltd

Detailed information on the Market Participant, the constituent DIP IDs operating within the DIP and their members along with certificate functionality.

Nominate DIP Connection Provider

Company Type	Company Number	Role Codes	DIP Connection Provider
Supplier, Distributor	1234567	None Set	None set
Description			
Our company			

DIP IDsMembers

Create MemberFilterSearch

First Name	Last Name	Email ID	Role	Role Codes	Actions
David	Gardiner	plmpdcsusr002@energydataintegrationplatform.co.uk	MP User Admin		<input checked="" type="checkbox"/> Edit <input checked="" type="checkbox"/> Onboard
David	Gardiner	plmpdcsusr002@energydataintegrationplatform.co.uk	MP Certificate Admin		<input checked="" type="checkbox"/> Edit <input checked="" type="checkbox"/> Onboard


Showing items 1 - 2 of 2Show 10All



Inviting users from outside your organisation

You are only able to add members to your organisation who have e-mail addresses featuring whitelisted domains, assuming you checked the ‘Whitelist DCP’s domains’ option when nominating a DCP, you should see that organisations domains listed. If not, or you need additional domains whitelisted, please contact the DIP Manager.

Once verifying the desired domain is present, navigate to the member tab

MHHS
PROGRAMME
PROGRESSIVE LEADERSHIP NETWORK

ELEXON
Data Integration Portal

EB

HOME

MARKET PARTICIPANT
ORGANISATION

MESSAGE CHANNELS

MESSAGES

PERFORMANCE

AUDIT

MPAN

USERS

Market Participants > Smart Energy

Smart Energy

You can view your organisation details below. Please ensure that you keep this information accurate and up-to-date.

Company Number	Role Codes	DCP Status
232424	MSA	Disabled

Description

New company

Whitelisted Domains

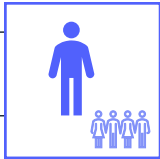
maillinator.com, pit.testmp.co.uk, dcporganisation.co.uk

+ Whitelist Domain

Webhook URL Configurations

+ Remove All Webhook URL Configurations

+ Add New Child Organisation



Adding New Users / Editing Existing Users

The User Admin should sign in, access the Members tab in Market Participants, and create the **Message Admin** using 'Create Member':

1 Click 'Create Member' in the Members tab

3 Click 'Confirm' to send the invitation

DIP IDs **Members** Certificates

You can view the details of your members and roles below. Please ensure that you keep this information accurate and up-to-date.

[Create Member](#) [Filter](#)

First Name	Last Name	Email ID	Role	Expiry Date	Actions
Ayl	Edet	ayl.edet@eleon-flex.com	MP User Admin MP Message Admin MP Certificate Admin MP Analytics Reader MP User Admin MP Message Admin	2026-07-23	Edit Extend Offboard
Egidio	Zindato	Egidio.Zindato@eleon-flex.com	MP User Admin MP Message Admin MP Certificate Admin	2025-07-24	Edit Extend Offboard

Select Organisation Role

This field is required

[Cancel](#) [Confirm](#)

2 Add **First Name**, **LAST Name** and a valid **Email Address**

Click @ to view list of whitelisted domains

Click **drop-down** to see available roles and select the appropriate **organisational roles** required for the user

4 **Recommended Action:**

It is advised that each Market Participant has at least 2 User Admin, 2 Certificate Admin and 2 Message Admin's to ensure cover is provided during potential situations of absence.

It is also acceptable for one person to hold multiple roles.

Please ensure you have cover for all potential access needs.

To **Edit** a members role, click the Edit button against that members name.

Create New User Profile

First Name is required.

☒ Member of All DIP IDs

Select Organisation Role

Note: If you require a domain which isn't listed, please contact the DIP Admin for it to be whitelisted.

[Cancel](#) [Confirm](#)



Extending Users

It is worthwhile noting all Users within a organisation having an expiry date, this is under the control of the Users Admins within the home organisation. It is down to the discretion of each company’s User Admin how these end dates are managed:

- 1
- Click ‘Extend’ in the Members tab for the specific User being extended

DIP IDsMembersCertificates

Create MemberFilterSearch

You can view the details of your members and roles below. Please ensure that you keep this information accurate and up-to-date.

First Name	Last Name	Email ID	Role	Expiry Date	Actions
Ayi	Edet	ayi.edet@elexon-flex.com	MP User Admin MP Message Admin MP Certificate Admin MP Analytics Reader	2026-07-23	EditExtendOffboard
Egidio	Zindato	Egidio.Zindato@elexon-flex.com	MP User Admin MP Message Admin MP Certificate Admin	2025-07-24	EditExtendOffboard

- 2
- Click ‘Yes’ in the pop-up window to confirm the extension of the User (at present all User extensions are on a six-monthly basis and they are additive)

Extend Market Participant User

Are you sure you want to extend Ayi Edet's access for 6 months?

CancelYes

Create MemberFilter

Please ensure that you keep this information accurate and up-to-date.

Email ID	Role	Expiry Date
ayi.edet@elexon-flex.com	MP User Admin MP Message Admin MP Certificate Admin	2026-07-23



Section 4 – GlobalSign Registration & API Key Generation

Interface Code of Connection

OFGEM have programme requirements around security and non-repudiation. This means:

1. All messages passing through the DIP must be digitally signed with a PKI certificate and authenticated by API keys
2. Connections between MPs, or their agents, to the DIP must be secured via an mTLS connection.

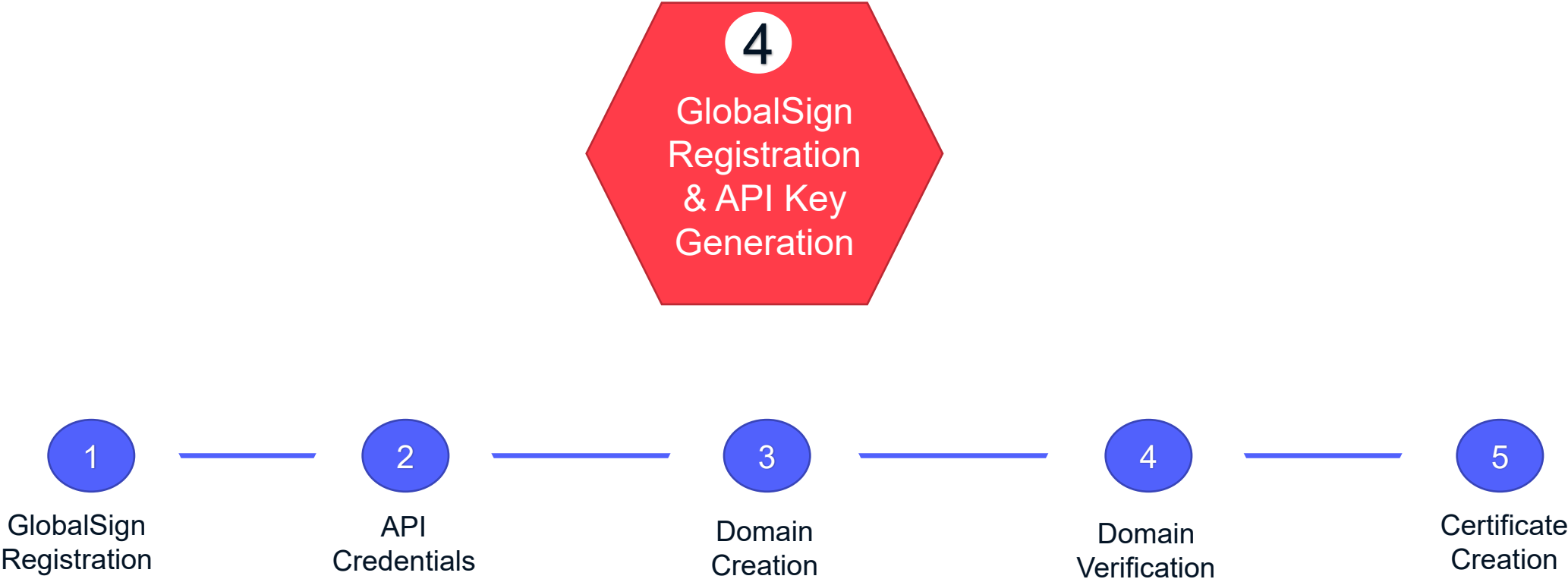
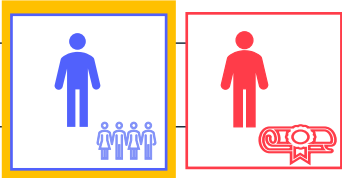
The Interface Code of Connection provides a description of how parties need to interact with the DIP.

The DIP Certificate Authority (DCA) is managed by GlobalSign.

- Each Market Participant is responsible for their own message signing, therefore, whether you are using a DCP or not, the Market Participant must complete the DNS and Certificate process for message signing.
- The DNS is validated by GlobalSign and therefore must belong to the Market Participant. The DNS can be the Market Participant's web domain or any other domain associated with the organisation.
- If using a DIP Connection Provider (DCP), the DCP should use their own mTLS certificate, and then use the MPs certificates for signing messages. The respective Market Participant's Signing certificate **must** be used to sign their messages.

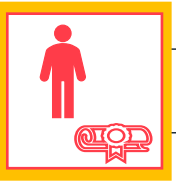
Two API & Certificate pairs are required:

- The first is used to authenticate against the GlobalSign API used for Signing Message Certificates
- Message Certificates signed above are then used for communication between the DIP and the MP or their agent





Step 4.1 – GlobalSign Registration



The Certificate Admin must follow the following steps to initiate the GlobalSign Registration process:

- 1 Select 'Market Participant' from the navigation menu
- 2 Check details of MP Company Details are correct
- 3 Select 'Certificates' tab to show 5-stage GlobalSign Registration and onboarding screen
- 4 Click the 'link' to GlobalSign MHHS Services registration page

The screenshot displays the Elexon Data Integration Portal interface. At the top, there is a yellow header with the MHHS PROGRAMME logo and the ELEXON Data Integration Portal title. Below the header, a navigation menu includes 'HOME', 'MARKET PARTICIPANT ORGANISATION', 'MESSAGE CHANNELS', and 'MESSAGES'. The 'MARKET PARTICIPANT ORGANISATION' section is active, showing details for 'Elexon Flex Limited'. The details include Company Number (12076975), Role Codes (None Set), DC-Status (Disabled), Description (Home of the DIP Manager and test harnesses), and Whitelisted Domains (elexon-flex.com). Below this, there are tabs for 'DIP IDs', 'Members', and 'Certificates'. The 'Certificates' tab is selected, showing a 5-stage GlobalSign Registration process: 1. GLOBALSIGN REGISTRATION, 2. API CREDENTIALS, 3. DOMAIN CREATION, 4. DOMAIN VERIFICATION, and 5. CERTIFICATE CREATION. The first stage, 'GlobalSign Registration', is expanded, showing instructions to visit the GlobalSign registration page at <https://www.globalsign.com/en/tp/global-sign-services/mhhs-programme> and complete the information requested to register. It also mentions that GlobalSign will carry out verification and may contact the head office to verify the Nominating Officer. Once verified, the user will be notified via e-mail and access to the GlobalSign portal will be provisioned. In the GlobalSign portal, the user should create API credentials and authentication certificate. Once created, they should press 'Next' to upload them into the DIP. A 'Next' button is visible at the bottom right of the registration instructions.

IMPORTANT

DO NOT CLICK 'NEXT'
until you complete
GlobalSign Registration.



The GlobalSign Registration and Verification

After clicking the link to the GlobalSign Services for MHHS home page, the Primary Certificate Admin must complete the following steps.



Read the GlobalSign MHHS introduction and scroll down screen



GENERAL NOTES

- 1. Ensure you follow the GlobalSign steps as outlined in the Onboarding Guide. DO NOT skip any steps / follow steps out of sequence.
- 2. Always check your spam when you're stuck or expecting an email from GS.
- 3. Wait for confirmation that account binding is done from GS and API credential ready to use before using your credentials. Otherwise, your certificate will be created before the API Keys gets bound to your account, and you will run into problems with your certificate down the line.

Complete the form in the lower half of the GlobalSign MHHS screen

Get Started with Atlas

About You

Tell us a bit about yourself

First Name *	Last Name *
Job Title *	Contact Phone Number
Email *	

Your Organisation

Please provide the official registration details of your organisation

Company Name *	Website *
Address Line One *	Address Line Two
City *	Postal Code *
Country *	

☐ I'm not a robot

View our Privacy Policy to understand how we collect and use your personal data.

Submit

INSTRUCTIONS

- 1. The details entered in fields FIRST NAME, LAST NAME, JOB TITLE in the 'About You' section should be the person dealing with the certificate request (Cert Admin) and GlobalSign vetting. Global Sign will contact the named individual and verify they are a current full-time employee and authorised to create a signing certificate.
- 2. The EMAIL ADDRESS provided is where all Global Sign communications will be sent for vetting only.

This should be the **Certificate Admin's** email address.

It is also acceptable to have a 'generic' email which is available to multiple people to monitor but must be accessible by the Cert Admin.

- 3. Please enter a direct contact number of the Cert Admin into 'Contact Phone Number': utilised to help in case the primary verification is unsuccessful
- 4. Click 'I am not a robot' then SUBMIT to conclude
- 5. You will receive a "Thank you for your interest in GlobalSign" message



The GlobalSign Registration and Verification

The email from GlobalSign will include their 12-step guide in the way of an itemised checklist – please follow as instructed.

After completing and submitting the GlobalSign Online Form an email will be received (as below) with a 12-step guide

- Thank you for starting your GlobalSign onboarding process as part of your onboarding to the Market wide Half Hourly Settlement (MHS) programme's Data Integration Platform (DIP).
- To continue your journey, we have listed each of the GlobalSign Atlas Portal steps in the order they will need to be followed in. Please take a moment to read through all of the steps before starting.
- Please note, you will not be able to continue your DIP registration until you have completed the GlobalSign onboarding process.
- 1 You will receive an email titled "New User Registration" from noreply@atlas.globalsign.com inviting you to join a GlobalSign Atlas Portal Account. Please follow the instructions in the email to proceed.
 - 2 You will receive a email titled "Password Reset Code - GlobalSign Atlas". Please use this code to create a new password. You can now login using your email and new password.
 - 3 You will be notified within 24 business hours by email from noreply-atlas@globalsign.com that your service quotation is ready for your approval. You will also receive an email from a representative of GlobalSign from firstname.lastname@globalsign.com with instructions.
 - 4 Log in to your Atlas Account and Approve the quotation.
 - 5 Select 'Identity Profile' tab and create a new Identity Profile for your IntranetSSL DV service.
 - 6 At this stage, your Organization Identity Profile will undergo Vetting. You will be notified once this process is complete, and you will be instructed to continue to the next step.
 - 7 Once the vetting process has been completed, and only when instructed to do so, please login to your Atlas Account.
 - 8 In the left menu, under the 'Access Credentials' tab, select 'API Credentials' and then click the 'Generate API Credentials' button in the top right corner.
 - 9 Select 'View and Copy' generation method.
 - 10 Select the service IntranetSSL (OV) to link your credentials to your vetted Atlas Organization profile.
 - 11 Input a familiar name - something to help you easily identify the service.
 - 12 GlobalSign will now configure your Atlas service to connect to the MHS Programme PKI hierarchy.
 - 13 Please wait for confirmation email from a representative of GlobalSign that the service can now be used.
 - 14 Once completed, continue to the next step of the DIP Onboarding Guide.

The following pages will provide guidance on the key steps of the GlobalSign ATLAS requirements. Steps 1-3 are self explanatory: note the 24hr window for Step 3.

- 1 You will receive an email titled "New User Registration" from noreply@atlas.globalsign.com inviting you to join a GlobalSign Atlas Portal Account. Please follow the instructions in the email to proceed.
 - 2 You will receive a email titled "Password Reset Code - GlobalSign Atlas". Please use this code to create a new password. You can now login using your email and new password.
 - 3 You will be notified within 24 business hours by email from noreply-atlas@globalsign.com that your service quotation is ready for your approval. You will also receive an email from a representative of GlobalSign from firstname.lastname@globalsign.com with instructions.
- Log in to your Atlas Account and Approve the quotation

Email arrival time:

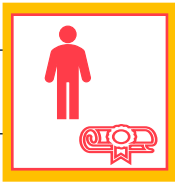
within 30 minutes of completing the online form and receiving the 12-step email

Within 1 minute of clicking the 'New User Reg' link

Up to 24hrs

May arrive within 1hr of step 2 completion

See next 2 pages for screens expected to complete your quotation in the Atlas account



GS Step 1 & 2 – Accept your invitation to the Atlas Portal

2 Follow the guidance in the email and complete the selections shown

1 On receiving the email from Globalsign you will receive an invitation to access the Atlas Portal

3

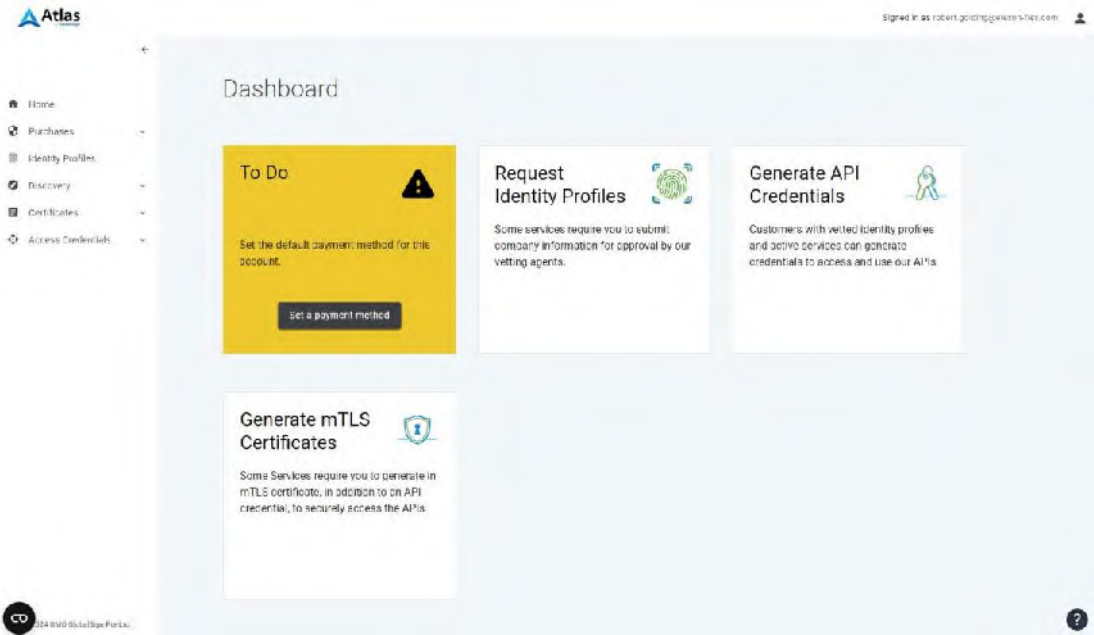
Review the Master Service Agreement and continue..



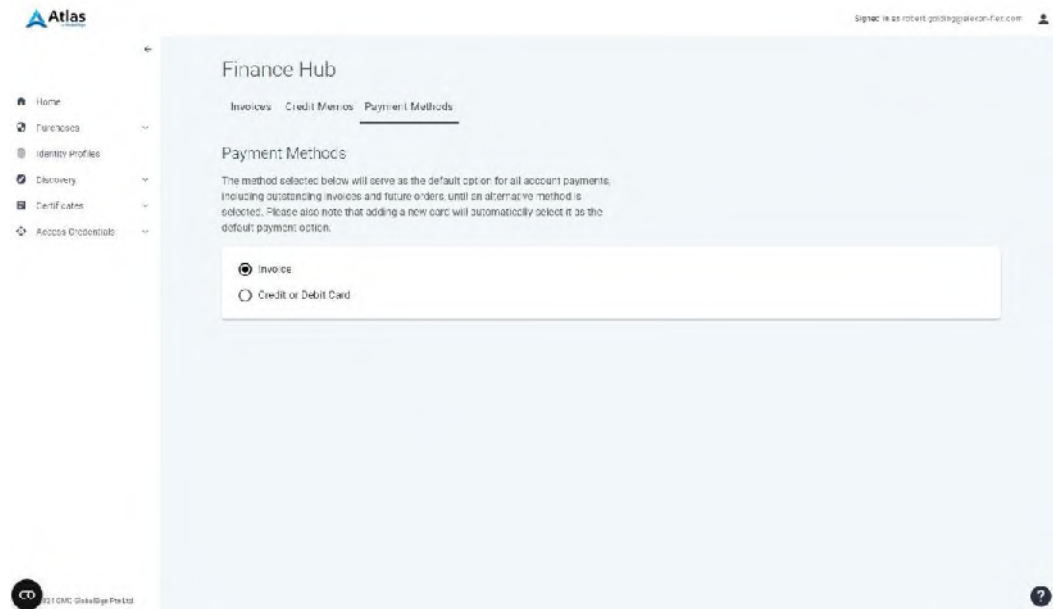
GS Step 3 – Approve Quotation - Set-up Payment Method (1 of 2)

A mustard tile will appear requesting the Payment Method is set-up. Choose invoice. This is only required for the GlobalSign system to function, **NO ACTUAL PAYMENT** is required.

- 1 LOGIN to Atlas and click the ‘To Do – Set a Payment Method’ tile



- 2 Choose Invoice

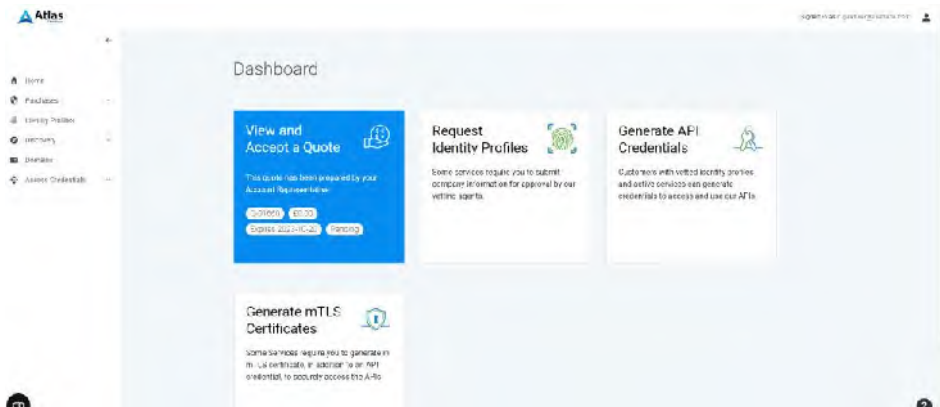




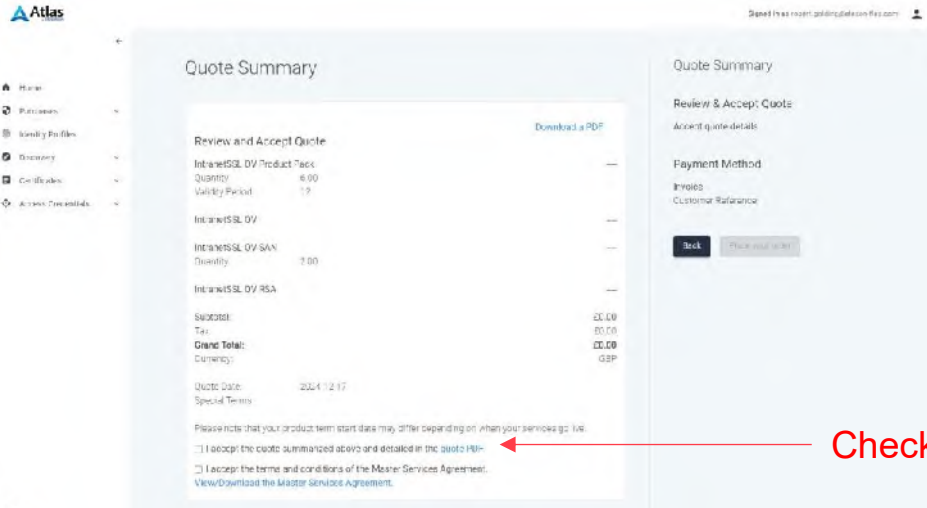
GS Step 3 - Approve the quotation (2 of 2)

NOTICE: Your quotation is ready', a BLUE TILE will appear in your dashboard. Click this to continue through the onboarding process.

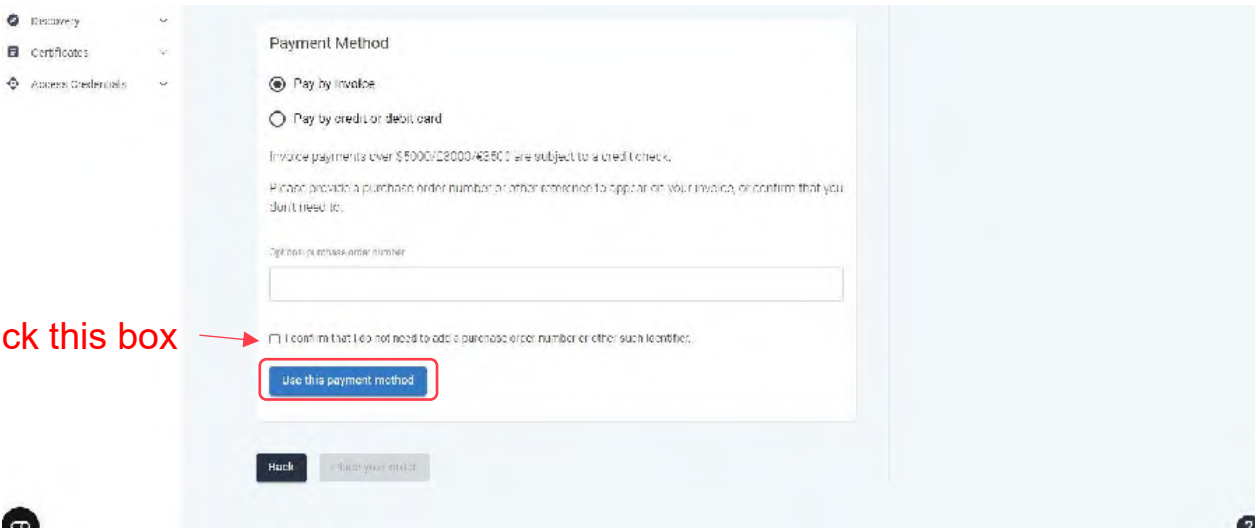
- 1 On receiving the email advising you're your quotation is ready, LOGIN to Atlas and click the 'View and Accept Quote' tile



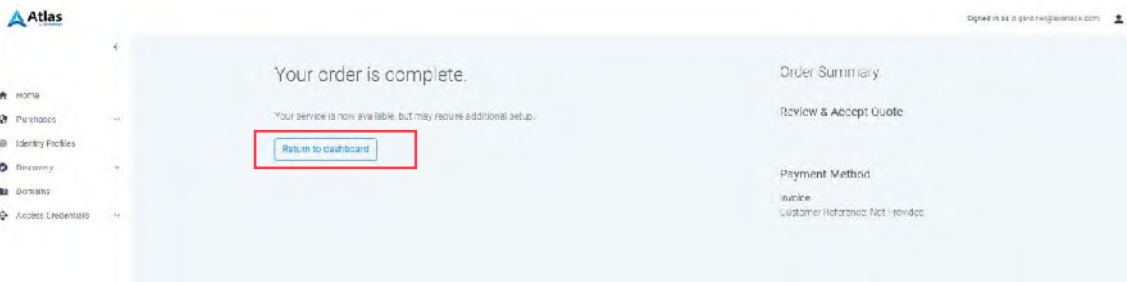
- 2 The £0 quotation will appear. Scroll down the page to complete the quotation acceptance see step 3



- 3 Follow the guidance in the email and complete the tick box selections shown



- 4 Complete quotation acceptance by clicking 'Use this payment method' button, this will return you to the dashboard



Check both boxes



GS Step 4 – Request Identity Profile

- 1

You will receive an email titled “New User Registration” from noreply@atlas.globalsign.com inviting you to join a GlobalSign Atlas Portal Account. Please follow the instructions in the email to proceed.
- 2

You will receive a email titled “Password Reset Code - GlobalSign Atlas”. Please use this code to create a new password. You can now login using your email and new password.
- 3

You will be notified within 24 business hours by email from noreply-atlas@globalsign.com that your service quotation is ready for your approval. You will also receive an email from a representative of GlobalSign from firstname.lastname@globalsign.com with instructions
- 4

Log in to your Atlas Account and Approve the quotation

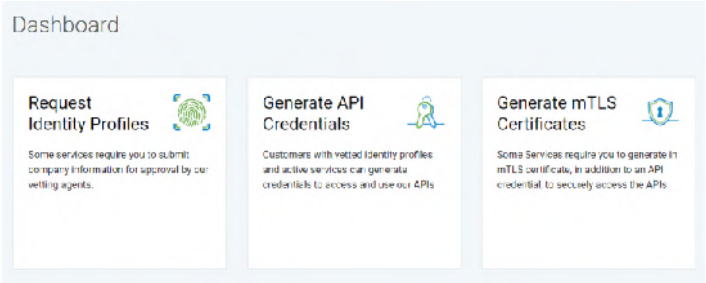
Select 'Identity Profile' tab and create a new Identity Profile for your IntranetSSL OV service

- 5

The DASHBOARD will default to the below 3 tiles – please await the **MUSTARD TILE** in Step

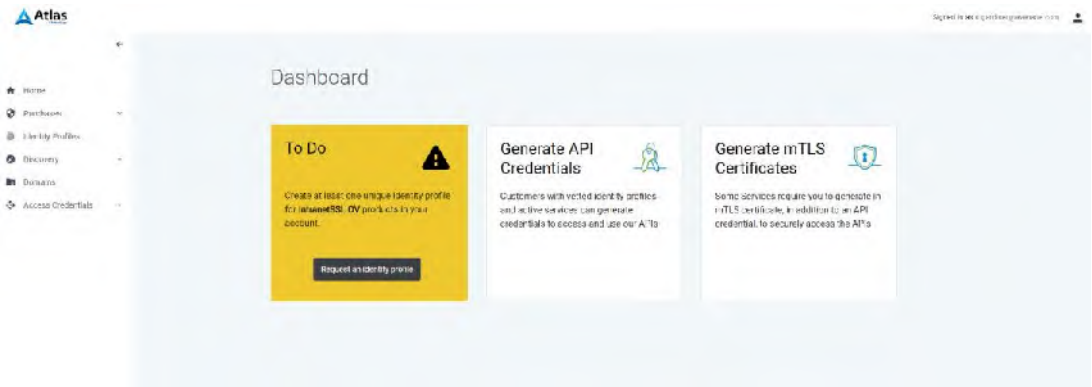
6

 before proceeding (up to 20-30 minutes)



- 6

Start STEP 4 (of the 12-step guide on slide 19) by clicking the new mustard coloured tile.





GS Step - 4 Create the Identity Profile

This requires accuracy in completion of the Identity Profile.

Each field will be used to verify the name provided is a known full-time employee of the company ORGANISATION NAME (O).

ADVICE – let your receptionist know an anonymous call may be received to avoid issue

The screenshot shows the 'New IntranetSSL OV Identity Profile' form. The form includes the following fields and annotations:

- Create a profile name:** Points to the 'Profile Name' field, which contains 'GerdnerProfile'.
- Enter the COUNTY here:** Points to the 'Country' dropdown menu, which is set to 'United Kingdom'.
- Enter the TOWN here:** Points to the 'Locality (L)' field, which contains 'Livingston'.
- This must be the ACCURATE Registered Company Name and is used to locate and call the company HQ.** A red box highlights the 'Organisation Name (O)' field, which contains 'Avanade UK Limited'.
- Click to start verification:** A blue arrow points to the 'Request this identity profile' button.

The form also includes a 'Cancel' button and a 'Request this identity profile' button. The 'Request this identity profile' button is highlighted with a red box.



GS Step 5 - GlobalSign Verification

Step 5 is the pause in the middle of the process where GlobalSign, through their own mechanisms, will conclude the vetting.

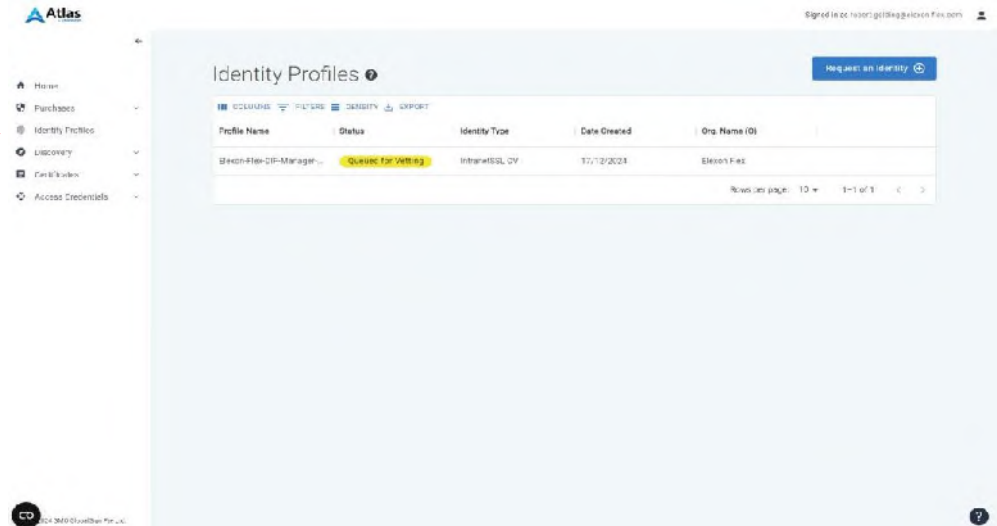
As shown below, there is a 72hr window for verification before you can proceed with steps 6-12.

Step 5 involves the original submitted name (Cert Admin) being vetted by telephone call, against the 'Organisation Name' entered in the Identity Profile

- 1 You will receive an email titled "New User Registration" from noreply@atlas.globalsign.com inviting you to join a GlobalSign Atlas Portal Account. Please follow the instructions in the email to proceed.
- 2 You will receive a email titled "Password Reset Code - GlobalSign Atlas". Please use this code to create a new password. You can now login using your email and new password.
- 3 You will be notified within 24 business hours by email from noreply-atlas@globalsign.com that your service quotation is ready for your approval. You will also receive an email from a representative of GlobalSign from firstname.lastname@globalsign.com with instructions
Log in to your Atlas Account and Approve the quotation
- 4 Select 'Identity Profile' tab and create a new Identity Profile for your IntranetSSL OV service
- 5 At this stage, your Organization Identity Profile will undergo Vetting. You will be notified once this process is complete, and you will be instructed to continue to the next step.

The completion of the IDENTITY PROFILE starts the 72hr verification process

The time taken for verification may take only a few hours however it should not exceed 72hrs after completing step 6



What happens during GlobalSign (GS) vetting?

GS will call the HQ number that they have uncovered from their secure vetting process. It doesn't matter if the contact is located at the HQ, or not; what they seek is that the HQ either

- i) transfers their call to the contact so they can speak with them; or
- ii) gives them the contact's phone number (can be landline or mobile) or email address so they can contact them.

If neither of the above happens, GS they will send a postal challenge letter for that contact, to the registered business address so that they (GS) can be contacted directly.

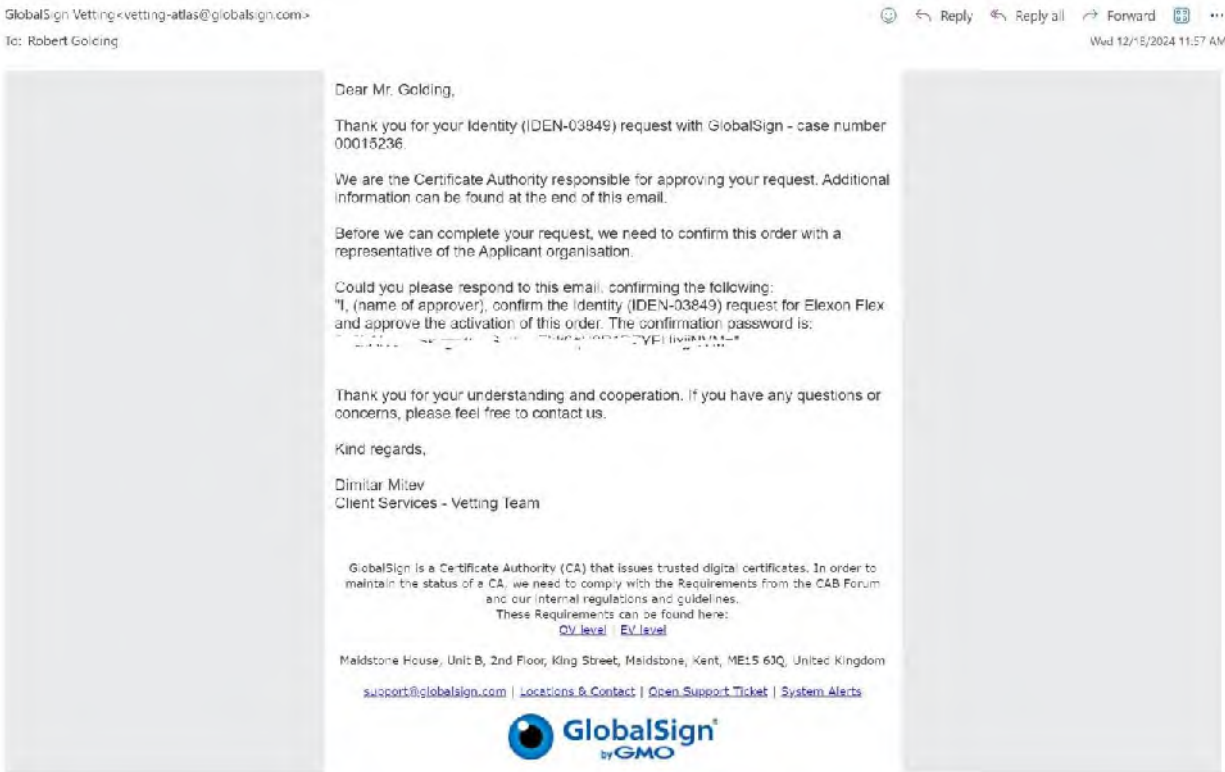


GS Step 5 - GlobalSign Verification

Step 5 is the pause in the middle of the process where GlobalSign, through their own mechanisms, will conclude the vetting. As shown below, there is a 72hr window for verification before you can proceed with steps 6-12.

A verification e-mail will be sent

DO NOT PROCEED UNTIL A VERIFICATION EMAIL HAS BEEN RECEIVED





Step 4.2 – Generate GlobalSign API Credentials

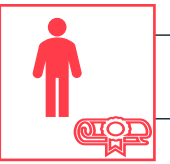


Generate API Credentials, PFX Signing Certificate and DIP Upload Overview (GS Steps 6-10)

1	2.	3.	4.	5.	6.	7.
Create API Credentials (Secret & API key)	Generate CSR & KEY file	Load CSR file into GlobalSign Portal	Generate CER file	Download CER file from Global Sign Portal	Merge CER & KEY file to generate PFX certificate	Upload the GS API Key & Secret, with the PFX Certificate, to the DIP

A certificate generation capability/tool is required to undertake steps 2 & 6.
Example usings Azure Key Vault and native OpenSSL commands are provided below

The end result is a PFX file loaded into the DIP



GS Steps 6-10 - Generating API credentials

The Certificate Admin must complete the API Certificate generation within the Global Sign Atlas system once 'Identity Validation' has been confirmed.

6

Once the vetting process has been completed, and only when instructed to do so, please login to your Atlas Account.

In the left menu, under the 'Access Credentials' tab, select 'API Credentials' and then click the 'Generate an API Credential' button in the top right corner

7

Select 'View and Copy' generation method

8

Select the service IntranetSSL (OV) to link your credentials to your vetted Atlas Organization profile

9

Input a familiar name - something to help you easily identify the service

10

GlobalSign will now configure your Atlas service to connect to the MHHS Programme PKI hierarchy.

11

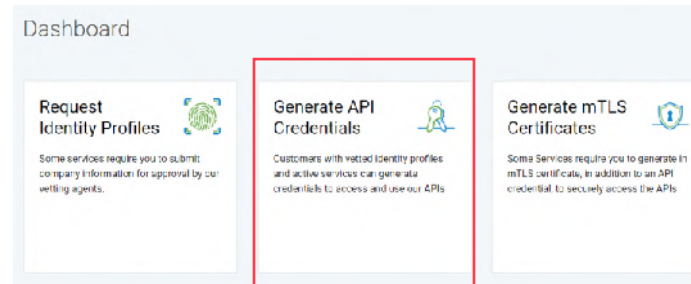
Please wait for confirmation email from a representative of GlobalSign that the service can now be used

12

Once completed, continue to the next step of the DIP Onboarding Guide.

6

Login to GlobalSign Atlas.
Select 'Generate API Credentials' option





Generating API credentials

The Certificate Admin must complete the API Certificate generation within the Global Sign Atlas system once ‘Identity Validation’ has been confirmed.

7 You must select ‘View and Copy’ in the ‘How would you like to receive your API credentials’ page, then Click **CONTINUE**

How would you like to receive your API credential?
You can optionally encrypt your key and secret.

View and Copy
We provide the key and secret in your web browser for you to copy to your clipboard. You can also download them in .env format.

Encrypted File
For additional security you can also provide a public key that we'll use to create an encrypted (.enc) file you can download.

Relevant customers should follow their Service Provider's instructions for generating and using public keys.

General help is available on the topic of [obtaining GlobalSign credentials](#).

Which method do you want to use?

View and Copy
View in browser, copy to clipboard.
Downloadable as a .env file.

Encrypted File
Insert an RSA public key.
Download key and secret as .enc file.

API CREDENTIAL SUMMARY

ENCRYPTED/KEY SELECTED:
No

SERVICE:
IDENTITY:
PROXY NAME:

BACK **CONTINUE**

8 Select **ACTIVE** certificate to assign Internet SSL to your credentials, then Click **CONTINUE**

Atlas

Signed in as user1.globalsign.com

Select Encryption Option: Link a Service Link an Identity Transfer Name

Link to a Service
This API credential must be linked to an active service.

intranetsslovrsa
ID: 544-0021933
Key Type: RSA
Start Date: 18 December 2024

ACTIVE

BACK **CONTINUE**

API CREDENTIAL SUMMARY

ENCRYPTED/KEY SELECTED:
No

SERVICE:
ID: 544-0021933
intranetsslovrsa - 1
IDENTITY:
PROXY NAME:



Generating API credentials with GlobalSign

Continued.....

- 9 Give the credential a familiar name (any text you wish) and record this safely and click 'CONTINUE'



- 10 Click 'Download key and secret as .csv' button and save file. Alternatively (and) click both the API Key and API Secret 'Copy Key to clipboard' and store in a .txt file for the next stage.

Add a Familiar Name

Create a label to distinguish this from similar credentials.

FAMILIAR NAME

xxxxxxxxxx key

BACK CONTINUE

API CREDENTIAL SUMMARY

1 KEYPAIR (CORE) IS ISSUED

NO

SERVICE

ID: A, SRV-0001036

Test Certificate-50

FAMILIAR NAME

xxxxxxxxxx key

Enter and take a note of your 'familiar name' then click CONTINUE

Success! Now Securely Save your API Key & Secret

If you lose this API secret, you'll need to generate a new API credential.

API KEY

186610baff175cae

COPY KEY TO CLIPBOARD

API SECRET

.....

COPY SECRET TO CLIPBOARD

DOWNLOAD KEY & SECRET AS .CSV

API DOCUMENTATION

VIEW & MANAGE API CREDENTIALS

RETURN TO DASHBOARD

PLEASE NOTE!

You must DOWNLOAD the .CSV.

Once you navigate away from this page you cannot return to access this content.



Generating CSR & Key File

GlobalSign provided the API Key and Secret. The DIP requires a validated certificate in PFX format together with these API credentials. The following will be conducted outside of the DIP **by someone with technical understanding of generating a certificate**.

Select a CSR(Certificate Signing Request) generation tool and create a CSR. Two methods tried and tested are **Azure Key Vault & OpenSSL**

Azure Key Vault

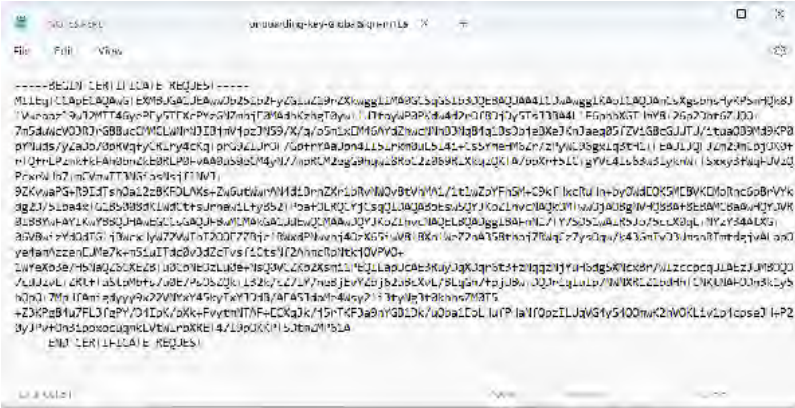
1

Create a CSR with any subject name.
YOU MUST select Key Size 4096 in Advanced Policy Config.
Click **DOWNLOAD CSR** to save your CSR file.

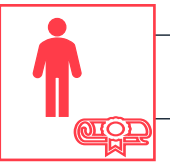
Please ensure you select Key Size 4096

2

Open the CSR to check structure is correct.



Please click 'YES' to Enable Cert Transparency
Certificate Type must be blank – no entry!



Openssl version:

openssl req -new -newkey rsa:4096 -nodes -keyout apicert.key -out apicert.csr -subj "/CN=onboarding_key"

Generates two files:

Certificate Signing Request (.csr)

```
-----BEGIN CERTIFICATE REQUEST-----
MIIEYjCCAKYCAQAwGTEXMBUGA1UEAwOb25ib2FyZGluZ19rZXkwggliMA0GCSqG
S1b3DQEBQUAA4ICDwAwggIKAoICAQCicss8+dKyWTFkG3+F3iJJK9D011k7yCqC
KGDjERKgtTpKaMHB0kpAkg6E+MlsP68LtWCp6UljhDjccFRKD5lx3EyvGAivFOO4
wMPwU7duED13VI0nFag7dAcQtCFdkzZ1N6dfoYqu9yCsUWj6Pp/3Fdolu8brjvX8
fq6lpXOCAKnH0Pdpj8hkeMFIqD1wU3PLLyX1ftabmlwBOKBhOGQbsbjAMgqAjlz
ZYh3i8QISqI6K5TKFcIcxUWtfpS2vVgQMoQ1DfSTwewRY8mKYMPBq371N7in4oBp
z29HlcZ0UTlt/pfvtnK9atY4APZtQLROsm7YI+eloGvldSYC/1y4pUcKeRmFodD
ZiuhCKspOyKugmmvyq3wwwY7TuUwPb8Zh28stOnw4ituAheeM5mgoEcHCbwolG9zs
RtXOW66w9iLb84r6jIdf+9Xf6p6Dj+dezTesD8N2QPqslnpsmR2027xicCWycUmk
---
---
---
ihY+qETHejO8x4iP4AtslUyilQxflr9MAEopuWS07OtWGPav8SPBpqyT/9hq2WHW
LRK5lt6C/N+wyO/RrJhLmfWQKQtpOvpWwpBH4QITaovvsEMFB2/P7gKibMCYNVer
3IRPIVpeldFmMX0WNmIpXJUyRRgM2OSjh4CCL68EgYTZ7eXzcgNRNwhu/ERb9OIR
CyRc1aYJUy+F5vv+4j6R/UlnjGFzZmluWmnKDw58aESAdtQwom9OMlmikliiYJZ
4Wo2yLHeonS7pirc48c5aJ7ytDxygsI7GXAireU1X8ChbnB0BTGCXw9yzhyZDcxV
MBNBSYDG/VMNuOBP8NDffwjZLJCYQw2lt9qKyns/A6apE2bNNOecc+tXJOldU01Z
Ezll8Y6Zf8hWKoj3oQatNCKI4ZcnoKxuxAy7KR+RRXhohXHSTk2C2WL15mOgi4k4
BaLB3Jmkce3h1QmdFrJswkee06652jk8KVMwL3mtf9EkDvUHng+nD09jfiAf3Tx5
1VX9Mi/y1Zr0iWtRBMcU32fE
-----END CERTIFICATE REQUEST-----
```

Private Key (.key)

```
-----BEGIN PRIVATE KEY-----
MIIEQwIBADANBgkqhkiG9w0BAQEFAASCCS0wggkpbAgEAAoICAQCicss8+dKyWTFk
G3+F3iJJK9D011k7yCqCKGDjERKgtTpKaMHB0kpAkg6E+MlsP68LtWCp6UljhDjcc
FRKD5lx3EyvGAivFOO4wMPwU7duED13VI0nFag7dAcQtCFdkzZ1N6dfoYqu9yCs
UWj6Pp/3Fdolu8brjvX8fq6lpXOCAKnH0Pdpj8hkeMFIqD1wU3PLLyX1ftabmlw
BOKBhOGQbsbjAMgqAjlzZYh3i8QISqI6K5TKFcIcxUWtfpS2vVgQMoQ1DfSTwewR
Y8mKYMPBq371N7in4oBpz29HlcZ0UTlt/pfvtnK9atY4APZtQLROsm7YI+eloGvld
SYC/1y4pUcKeRmFodDyVn+sCYpt23aM3TAQIVqmDB668y/hOBOFeECNEdpP0RB
ig0AgjVdeltXIVRHjJC+/e61WA2PIRoSVbTP6EXWuha4q75JGTK9YUBKW4jdctRM
r2YcM4K3n9CPkHhc7p7b7IVjS31Tm7860ZTwzX5yqM2av7thjmWnMWpE0RbcpAOw
---
---
---
ZqKSRdu92gboflCx1/ERHcz4ftW94otonWjhkbM58mFH8NvKHsyrYcPo3WU6Qml
JDduUjbtX1Y3ekyuB2id9LeMn7po+4PacZN6L6nWFGtKlgOCrrzzLAbVpgupWwWdD
SFz6763+pwQutY3+1Q4euvOcFDDOQIDAQABAoICABYVGitsZWP+WLQMtBkyaQXv
FehWk8nqKL3Xr/VKa8Z0CoustqDM+S31t5OBK44ykrhiNORw+X3X8NflpW6IDG
2FCfzeEbEMRIORF5xQS0tYm6V9l6ulebEeVm2STLW+sgNEAnLkhP1UsvvU0OKKCN
G+TM7e6gAgse75QX0T6yUqJ8jV/u3pU0GN5MSX5raL/T4LjydLwldnF32Mty7li
ESYCaplnVdMFxvAYK0it/hzCjrRgbgw+YG06owJ275HMyF5KDOjB5cCTVqwbT3ZT
RBielkW6XCqSveZXPzZXCoJ3kilGCqWtiMY5OF+uqTe9vUH6w4bRFvzlAb5eDjpb
OXEQcYzmlBNBNEf81f7hqV4A7qcxXzg=
-----END PRIVATE KEY-----
```



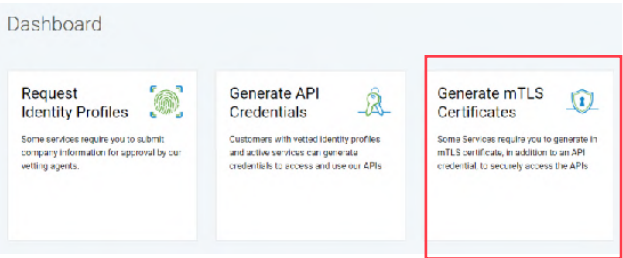
Generating the correct key format for upload to the DIP

The Certificate Admin must return to the GlobalSign Atlas system to complete the next stage of certificate preparation for the DIP.

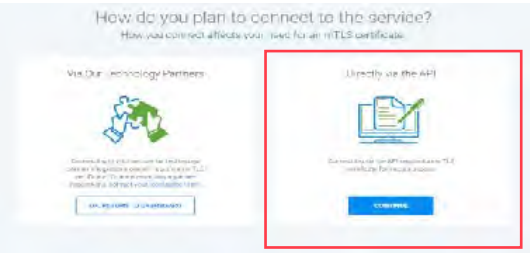
NOTE: If you have appointed a new Cert Admin into the Atlas account, they can complete the following steps.



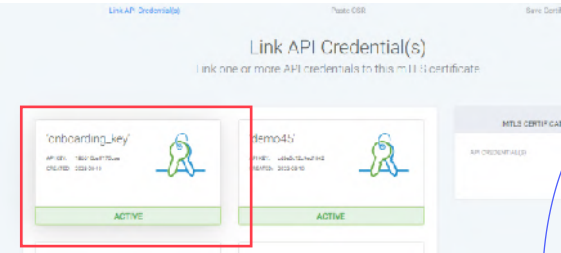
1
Sign in to the Atlas system.
Open your Dashboard.
Select 'Generate mTLS Certificates'.



2
On the subsequent screen, select the option
'Directly via the API'



3
Select the API Credentials just made
using the 'Familiar Name'



4
Paste the CSR generated into the
space provide then
click CONTINUE



N.B. Even though the GlobalSign screen states 'Paste in a 2048 CSR, this is incorrect, it should be a 4096 CSR



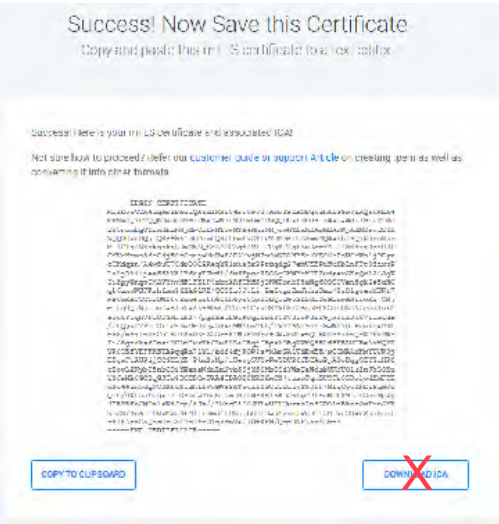
Create a PFX Certificate for Upload to the DIP

The output from the GlobalSign system requires the key to be converted to PFX format. This is completed using OpenSSL

This section is OUTSIDE DIP and GlobalSign (Example shown is Azure Key Vault)

5

If successful the following screen appears.
You must now Copy to Clipboard (or Cut-n-paste) the certificate into a **Notepad** file.
Save the Notepad file as a **.cer**
e.g. 'certname.cer'



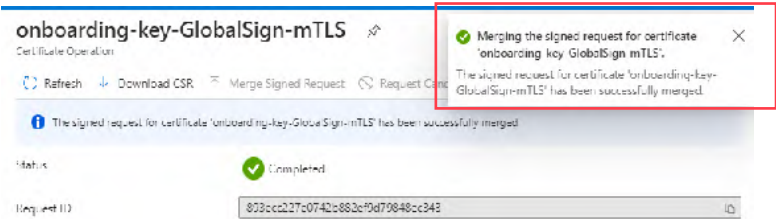
6

Re-open the certificate generation tool
Select 'Merge Signing Request', from the menu to **merge the private key and public key**



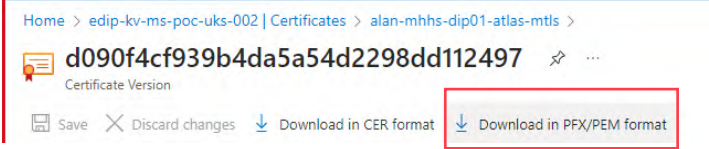
Select the file created in Step 5, e.g. certname.cer

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

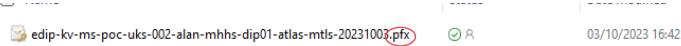


7

Download the certificate as a PFX file, **ensuring no password is specified.**



The resulting PFX format file will be listed in a download area ready for the next step





Return to the DIP to upload API credentials

The Certificate Admin will return to the ‘Certificates’ tab as below and click the **NEXT** button to proceed:

1

MARKET PARTICIPANT ORGANISATION

MARKET PARTICIPANT ORGANISATION

MESSAGE CHANNELS

MARKET PARTICIPANTS

Another test company

Another test company

Detailed information on the Market Participant, the constituent DIP IDs operating within the DIP and their members along with certificate functionality.

Company Type
None set

Company ID
123456

Role Codes
None set

Dip Connection Provider
None set

DIP IDs

Members

2

Certificates

1

2

3

4

5

GLOBALSIGN REGISTRATION

API CREDENTIALS

DOMAIN CREATION

DOMAIN VERIFICATION

CERTIFICATE CREATION

GlobalSign Registration

Please visit the GlobalSign registration page at <https://www.globalsign.com/en> and complete information requested to register. GlobalSign will then carry out verification and may contact your head office to verify the Nominating Officer. Once verified, the user will be notified via e-mail and access to GlobalSign portal provisioned.

In the GlobalSign portal please create API credentials and authentication certificate. Once created press Next to upload them into the DIP.

3

Next

Click ‘NEXT’ to move to on to ‘API Credentials’ entry

Step 2 – API Credentials



Upload API Credentials

The Certificate Admin must now upload the GlobalSign API Key & Secret, together with the PFX Certificate, to the DIP.

1


2

3

4

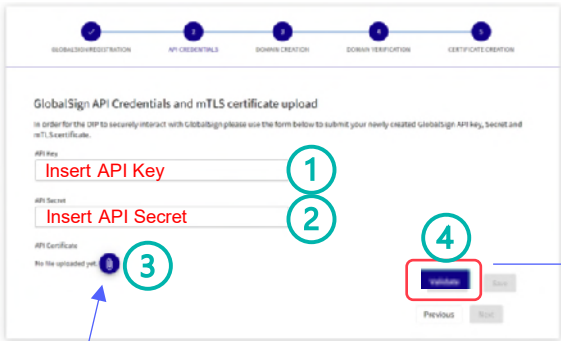
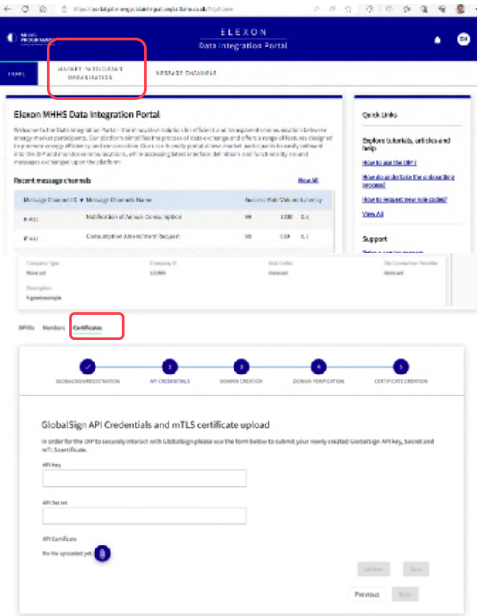
Certificate Admin will Sign In to DIP and click the 'Market Participant' and select 'Certificates' tab to display the process page

The process will have moved to STEP 2 'API Credentials' Add the Global Sign generated information:

- 1. Insert the API Key (1)
- 2. Insert the API Secret (2)
- 3. Click  to upload the PFX Certificate (3)
- 4. Click 'Validate' button (4)

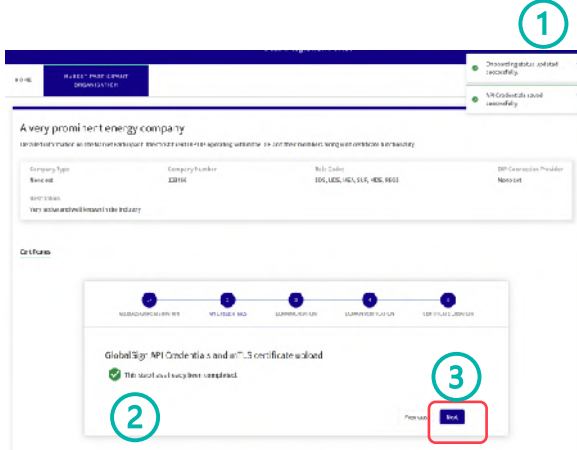
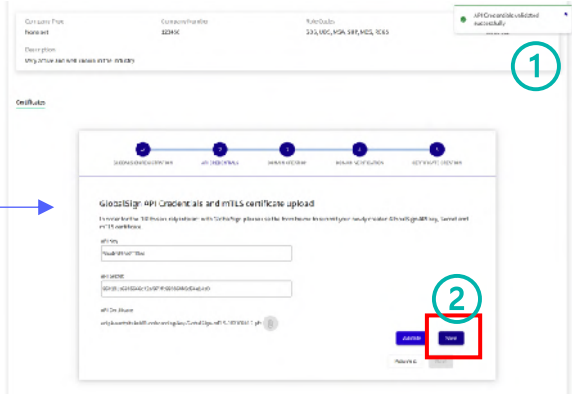
If the API entries are confirmed, A pop-up 'Added successfully' appears (1) click 'Save' to continue (2)

The following screen will appear 'Onboarding status updated successfully'.
1. Confirmation with 'Toast' Pop-up (1)
2. Confirmation onscreen message (2)
3. Click 'Next' to progress to Domain Registration & Verification (3)



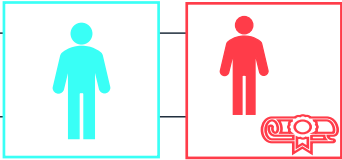
Click  and select your PFX version of the API Certificate

Y





Step 4.3 & 4.4 – Domain Registration & Verification



Register and Validate the Company Domain in the DIP

The Certificate Admin will work with a DNS Admin to complete the Domain registration in DNS.

Follow steps 1-3 to enter the MP's **Domain Name being used for GlobalSign verification** into the GlobalSign Domain Creation field **DOMAIN**, then click '**SUBMIT**' (4)

Once you have clicked next, you will be asked to **reselect the DOMAIN Name from the dropdown** and a **TXT Record** will appear (6)
NOTE that a '.' may appear after the Domain Name – this is not an issue and you should proceed

DNS Admin should add the record details into the DNS (6) with the values specified = '@' and the txt into VALUE

Certificate Admin, on confirmation DNS Record has been added (can be up to 1Hr), will click the Check box (5) and then click the **SUBMIT** button (7)

Certificate Admin can check **SUCCESS** or **FAIL** of verification: If Successful click '**Next**'

Domain Validation Successful
The DNS entry should not be removed as it is used for renewals

Please take a note of the '**Name**' = '@' and the **VALUE** is a '**txt**', and pass both to **DNS Admin** for insertion into the DNS **BEFORE** clicking (5).

Y

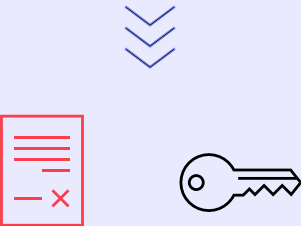
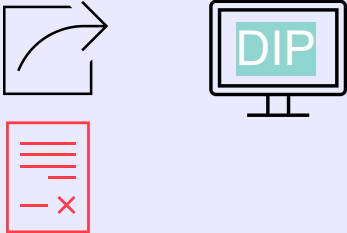

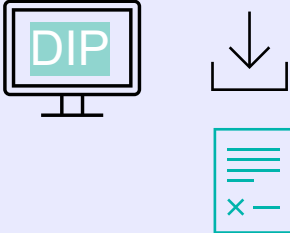
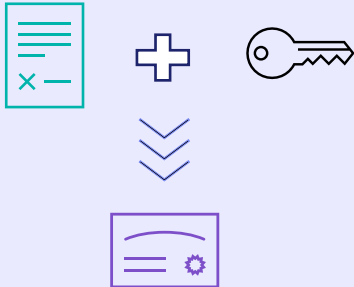


Step 4.5 – DIP Certificate Creation



Generate mTLS & Signing Certificate Overview

To generate a mTLS or a signing or a combined mTLS/signing certificate follow the steps below:

1.	2.	3.	4.	5.
Generate CSR & KEY file	Load CSR file into DIP	Generate CER file	Download CER file from the DIP	Merge CER & KEY file to generate PFX certificate
				

A certificate generation capability/tool is required to undertake steps 1 & 5.
Example usings Azure Key Vault and native OpenSSL commands are provided below

The end result is a PFX file



Step 1. Generate CSR & KEY file

1 Login to the DIP as Certificate Admin

- 1. From the Market Participant menu select the Certificates tab
- 2. Select the Create Certificate option

HOME

MARKET PARTICIPANT ORGANISATION

MESSAGE CHANNELS

MESSAGES

PERFORMANCE

Elexon Flex Limited

You can view your organisation details below. Please ensure that you keep this information accurate and up to date.

Company Number
16079976

Role Codes
SUP, REGS, SCS, ACS, MSS

DCP Status
Disabled

CD Request DIP Connection Provider Status

Description
Home of the DIP Manager and Test harnesses

Whitelisted Domains
elexon-flex.com

DIP IDs

Members

Certificates

Currently Active Certificates

You can view the status of your current active certificates below. Please ensure that you keep this information accurate and up to date.

Update API Credentials

Create Certificate

Certificate Serial Number	Status	Created Date	Expiry Date	Created By	Common Name	Type	Revoke	Download	Revoke
013F74952A3EB53D3A2F6DDAF2EC663	SEUED	2025-03-18	2026-03-25	robert.golding@elexon-flex.com	energypip-nonprod.2059.elexon-flex.com	mTLS & Signing			

Certificates History

Filter

Search

Certificate Serial Number	Status	Created Date	Expiry Date	Created By	Common Name	Type
012EF367B5230AD2F832F67BFD1C588F	REVOKED	2025-03-13	2026-03-20	robert.golding@elexon-flex.com	energypip-nonprod.2069.elexon-flex.com	mTLS & Signing

Showing items 1 - 1 of 1 | Show 10 | All

- 1. From the Create Certificate pop-up
- 2. Enter the required Host Name & Domain Name. Domain name is taken from a drop down populated by the list of domains registered against the organisation.
- 3. Select 'Certificate Purpose' to choose a "mTLS" (for DCPs), "Signing" (for MPs) or "mTLS & Signing" certificates (both)
- 4. Subject name is generated from values provided
- 5. Select Copy - this will copy the Subject Name - SN
- 6. You will also need to copy the Domain Name & Host - DN&H

Create Certificate

Host Name
my host

Domain Name
elexon-flex.com

Certificate Purpose
mTLS & Signing

Subject Name
energypip-nonprod.2059.elexon-flex.com

Copy

CSR

DN&H

SN

Step 5 – Certificate Creation

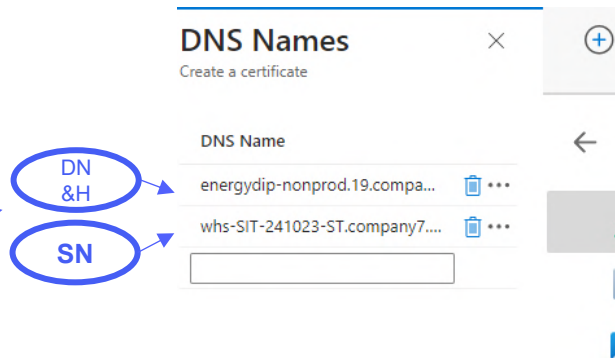
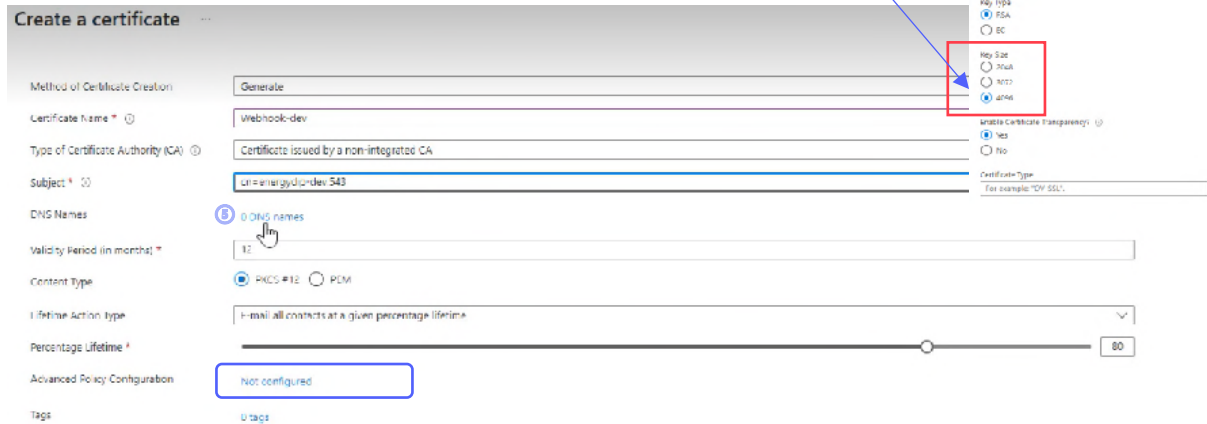
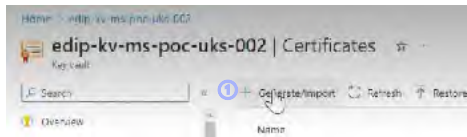


Step 1 (cont). Generate CSR & KEY file (Azure Key Vault version)

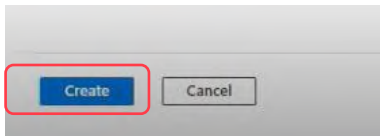
Using the details from the previous step

Open the Certificate Creation Tool (e.g. Azure Key Vault)

- 1. Click (select) to generate a certificate (in AKV click [Generate/Import](#))
- 2. Give the certificate a name (no spaces)
- 3. Choose ‘[Certificate used by non-integrated CA](#)’ from drop down
- 4. Enter ‘[cn=](#)’ then paste the [SUBJECT NAME \(SN\)](#) copied from previous step
- 5. IMPORTANT – click ‘[DNS Names](#)’ and complete the 2 entries – [SN](#) & [DN&H](#) copied from previous step
- 6. Click ‘[Not configured](#)’ next and ensure Key Size is [4096](#)

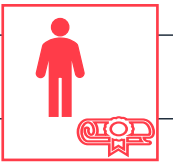


- 7. Click ‘[Create](#)’ button to create CSR & KEY files



- 8. Open the generated CSR
- 9. Download CSR





Step 1 (cont). Generate CSR & KEY file (OpenSSL version)

1. Using the Subject Name (SN) and the Host & Domain Name (H&DN) copied from previous step:
2. Enter the command OpenSSL command:

```
openssl req -new -newkey rsa:4096 -nodes -keyout mtlscert.key -out mtlscert.csr -  
subj "/CN=<SN>" -addext "subjectAltName = DNS<H&DN>, DNS:<SN>"
```

3. This will generate two files: CSR & KEY files

Step 5 – Certificate Creation



2. Load CSR file into DIP

3. Open the downloaded CSR file into a text editor



4. Select the Certificate Text



3. Generate CER File

5. PASTE the Certificate Text into the CSR field in DIP

Certificate Signing Request Form

The form is used to submit your certificate signing request (csr) to be signed by the DIP Certificate Authority (CA). The form is available on the DIP website and is a key part of the process of generating your certificate and thus creating your mTLS-certificates, which are used when interacting with the GPC.

Before making a signing request, please ensure you have considered the necessary digital signature and domain verification on account, once details can be found in the [DIP User Guide](#).

Please ensure that the details entered on this form are used during the organisation onboarding, testing and verification process.

new name:

cert type:

subject name:

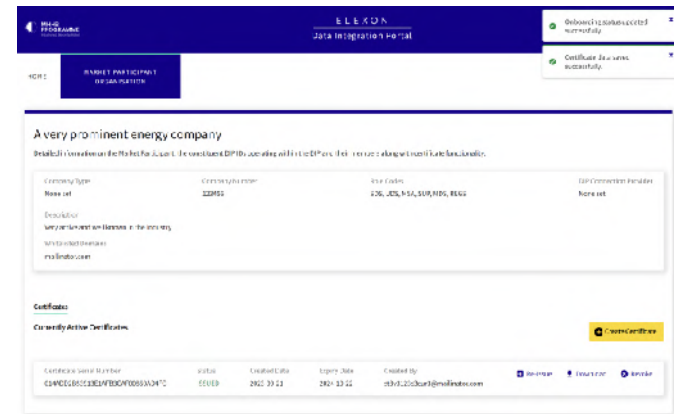
CSR

Create Certificate

Previous

6. Click ‘Create Certificate’

7. ‘Toast’ advises successful certificate generation

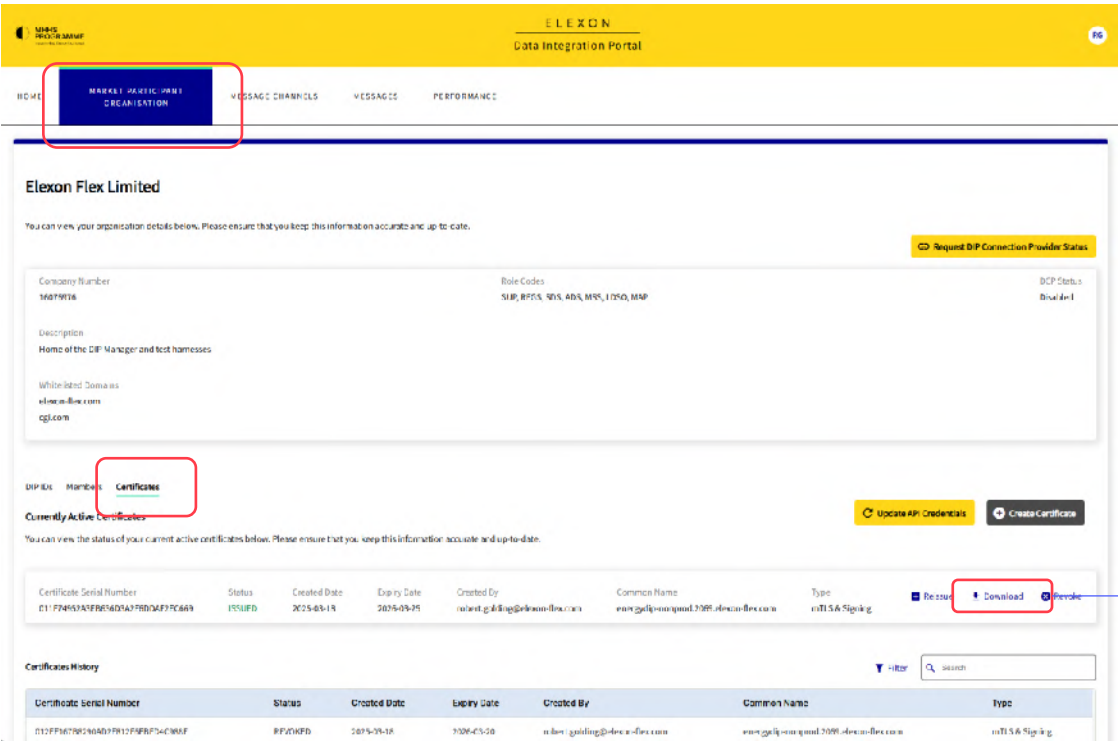




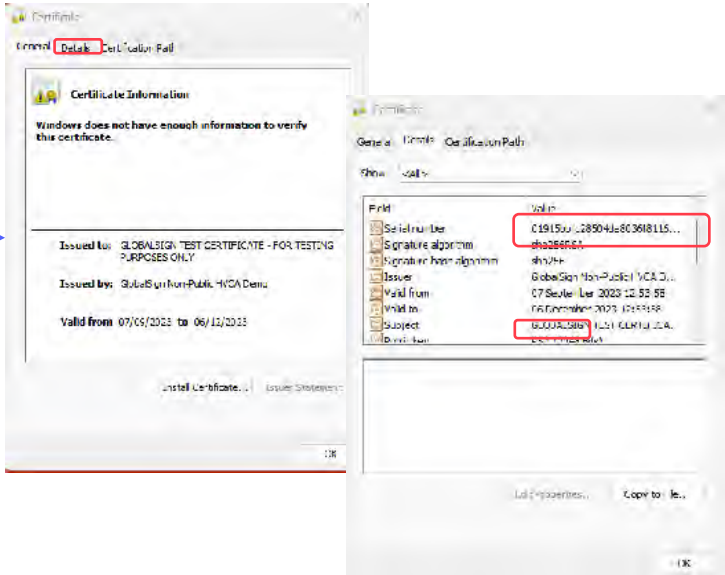
4. Download CER file from DIP

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
- 2. Click 'Certificates' tab and check certificate is ISSUED
- 3. Click [Download](#) to utilise the new ISSUED certificate.



3



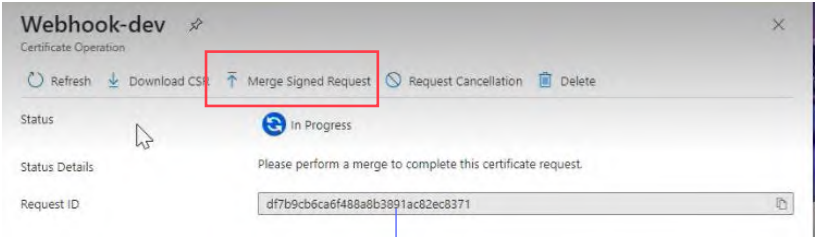
Open the downloaded Certificate file and Click 'Details' Tab.
Check validity by comparing **Serial Number** matches.
Check **Subject** is as expected.



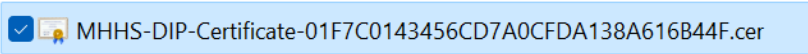
5. Merge CER & KEY file to generate PFX certificate (AKV version)

Final stage of the process must be conducted within the Certificate Generation tool chosen earlier

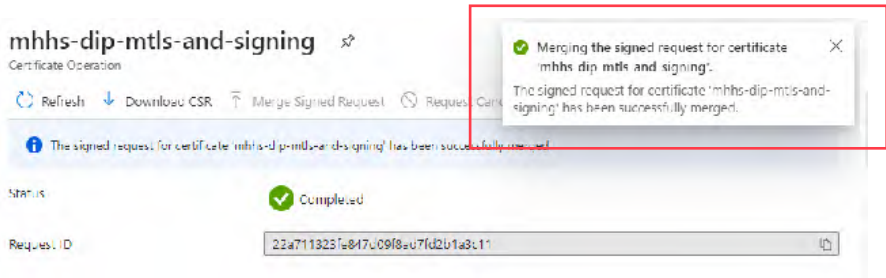
- 1. Select menu option ‘Merge Signed Request’



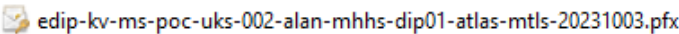
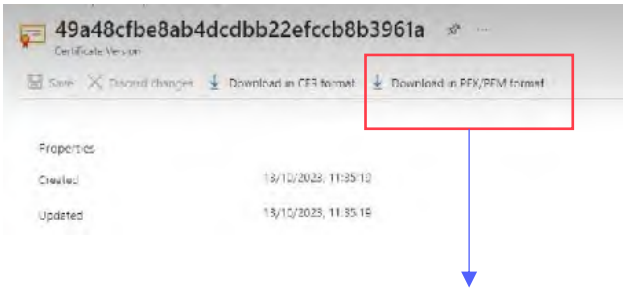
Select the FILE downloaded from the DIP Portal
(a .cer file – example shown below)

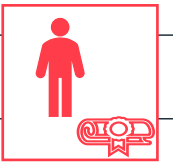


- 2. A ‘toast’ pop-up will confirm the merge was successful



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





5. Merge CER & KEY file to generate PFX certificate (OpenSSL version)

To generate the PFX file :

1. Enter the command OpenSSL command:

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

2. This will merge the CER and KEY generate a PFX file

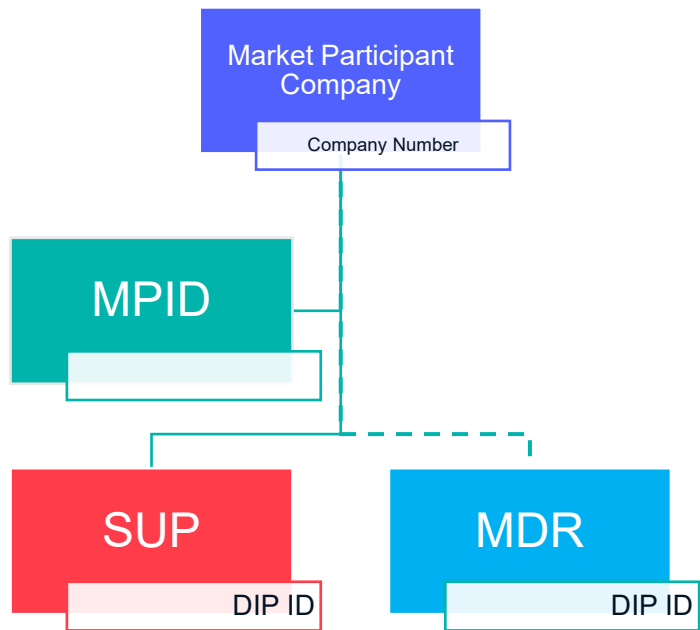


Step 5- Setting up DIP IDs

Background – DIP Roles

Role ID	DIP Active	Requestable role	Service Name	Market Segment/Role	Market Participant Role
MSA	*	✓	Metering Service (Advanced)	Advanced Market Segment	T
ADS	*	✓	Advanced Data Service		O
MSS	*	✓	Metering Service (Smart)	Smart and Traditional (non-Smart) Market Segments	S
MRS			Metering Reading Service		6
SDS	*	✓	Smart Data Service		N
SMSO	¥	✓	Smart Meter System Operator		
MDR	\$	✓	Meter Data Retrieval Service		
UMSO	*	✓	Unmetered Supplies Operator Service	Unmetered Supplies Market Segment	3
UMSDS	*	✓	Unmetered Supplies Data Service		Q
MDS	*		Market-wide Data Service	BSC Central Settlement (CS)	n/a
LSS	*		Load Shaping Service		n/a
ISD	*		Industry Standing Data		n/a
VAS	*		Volume Allocation Service		n/a
REGS	*	✓	Registration Service	Registration	P
SUP	*	✓	Supplier	Supplier	X
MAP	¥	✓	Meter Asset Provider		8
LDSO	*	✓	Licensed Distribution System Operator (IDNOs & DNOs)	Distribution Network Operator	R
EES	*		Electricity Enquiry Service	RECCo	L
\$ - MDR has the option to use the DIP for message exchange					
¥ - MAP & SMSO roles do not participate in message exchange in the DIP					

Market Participant Data Setup - Supplier



All the data required for each Market Participant on-boarding onto the UIT environment has been set up in advance.

Each Supplier requires a DIP Id for each of the MPIDs they are qualifying

Optionally each Supplier will need to understand their MDR status.

Suppliers and Smart Data Services Participants have choices about how to operate the MDR function within the MHHS Design.

Depending on how Suppliers and Smart Data Services intend to use the MDR function, this may involve some additional DIP Onboarding steps for how to set up the MDR Market Role.

Note - *the DIP has separate DIP IDs that need to be set up and configured to support the use of the MDR function*

The 'MDR' Market Role Participant details are used for two (2) purposes within the MHHS design

1. Registration Process (Mandatory)

- MDR identity details are used for populating data items within Registration DIP messages to ensure that every MPAN has a registered MDR Participant with the Registration systems for external party validation purposes (e.g. DCC).

2. Sending / Receiving DIP messages (Optional)

- MDR Participants using the MDR DIP Market Role wish to 'opt-in' and use the optional DIP messages introduced under CR-023 – Standardisation of Interfaces within the SDS

For example,

- *Where the Supplier intends to appoint themselves as an MDR for each MPAN and continue to collect consumption and generation data via the DCC using their existing Supplier User Roles then an additional separate DIP ID will be required to be set of for the DIP Market Role of 'MDR'*
- *If the Supplier, using its MDR function, also wishes to use the optional DIP messages introduced under CR-023 – Standardisation of Interfaces within the SDS to send / receive DIP messages (IF-061 to IF-065 messages) then this is an extra configuration required within the DIP to create a SDS to MDR Pairing.*



Create a new DIP ID:

HOME

MARKET PARTICIPANT ORGANISATION

MESSAGE CHANNELS

MESSAGES

PERFORMANCE

Elxon Flex Limited

You can view your organisation details below. Please ensure that you keep this information accurate and up-to-date.

Request DIP Connection Provider Status

Company Number

16076976

Role Codes

SUP, REGS, SDS, ADS, MSS, LDSO, MAP

DCP Status

Disabled

Description

Home of the DIP Manager and test harnesses

Whitelisted Domains

elxon-flex.com

cgi.com

DIP IDs

Members

Certificates

Create New DIP ID

Filter


Search

You can view the status of your DIP IDs below. Please ensure that you keep this information accurate and up-to-date.

DIP ID	DIP Role Code	MPID	MP Role Code	DCP Organisation	DCP ID	Effective From Date (MPR)	Effective To Date (MPR)	Actions
1191000001	ADS	DMXX	O	Unassigned	N/A	2025-01-30	2030-01-01	Edit Delete



Select DIP ID to administer:



ELEXON

Data Integration Portal

UU

HOME

MARKET PARTICIPANT ORGANISATION

MESSAGE CHANNELS

MESSAGES

PERFORMANCE

Big Energy Company

You can view your organisation details below. Please ensure that you keep this information accurate and up-to-date.

Company Number

2242424

Role Codes

SUP, VAS

DCP Status

Active

Description

new one

Whitelisted Domains

sit.testmp.co.uk, live.co.uk, esgglobal.com

DIP IDs

Members

Certificates

+ Create New DIP ID

Filter

Search

You can view the status of your DIP IDs below. Please ensure that you keep this information accurate and up-to-date.

DIP ID	DIP Role Code	MPID	MP Role Code	Effective From Date (MPR)	Effective To Date (MPR)	Actions
1086576131	VAS	ABCD	n/a	2024-07-15	2025-07-15	Edit Delete
1494431682	SUP	RDG1	X	2024-07-04	2025-07-04	Edit Delete


Showing items 1 - 2 of 2

Show 10 All

<

1

>



MHHS
PROGRAMME

Industry-led, Elexon facilitated

63

Step 5 – Nominate a DCP for a DIP ID



DIP ID	DIP Role Code	MPID	MP Role Code	Effective From Date (MPR)	Effective To Date (MPR)	Actions
1252210018	MSA	QAWD	T	2024-06-24	2025-06-24	Edit Delete

MARKET PARTICIPANT
ORGANISATION

MESSAGE CHANNELSMESSAGESPERFORMANCEAUDITMPANUSERS

Market Participant > Recent Entries > DIP ID 1252210018

DIP ID: 1252210018

Nominate DIP Connection Provider

Details

Company Number	MPID	Market Participant Role Code	DIP Role Code	DIP ID	Effective From Date (MPR)	Effective To Date (MPR)
252424	QAWD	T	MSA	1252210018	2024-06-24	2025-06-24

Interface Configuration

Please select an interface to configure for this DIP ID

Interface

Members

Add Member

Filter

Search

First Name	Last Name	Email	Role	Actions
Cert	Admin	certadm@mail.mhhs.com	MP Certificate Admin	Offboard
User	Admin	useradmin@mail.mhhs.com	MP User Admin	Offboard

Showing items 1 - 2 of 2. [Show All](#)

- 1
- Identify the DIP ID you wish to nominate a DCP for and click it
This will take you to the DIP ID details view.
Click the ‘Nominate DIP Connection Provider’ button.

2

Nominate DIP Connection Provider for DIP ID 1252210018

Market Participant

DIP ID

Whitelist DCP's domains?

This will allow you to invite members of the DCP organisation into yours and assign them roles

Cancel

Nominate

→

3

Nominate DIP Connection Provider for DIP ID 1252210018

Market Participant

DIP ID

Whitelist DCP's domains?

This will allow you to invite members of the DCP organisation into yours and assign them roles

Cancel

Nominate

Your desired DCP should have already created a DCP ID in the portal and shared it with you. Select you desired DCP from the Market Participant field and then the DCP ID they have shared with you.

You must also tick the ‘Whitelist DCP’s domains’ if you intend to add DCP users as members of your organisation to allow them to perform administration tasks, for example create certificates or generate API Keys. Please note, if you do not see your desired DCP listed, please ask them to create a new DCP ID for you.

Once happy with the nomination details, click the nominate button.



Section 6- Message Channel Set-up



MHHS PROGRAMME

Industry-led, Elexon facilitated

ELEXON

Data Integration Portal

UU

HOME

MARKET PARTICIPANT ORGANISATION

MESSAGE CHANNELS

MESSAGES

PERFORMANCE

Market Participants > Big Energy Company > DIP ID 1494431682

DIP ID: 1494431682

Nominate DIP Connection Provider

Details

Company Number	MP ID	Market Participant Role Code	DIP Role Code	DIP ID	Effective From Date (MPR)	Effective To Date (MPR)
2242424	RDG1	X	SLP	1494431682	2024-07-04	2025-07-04

API Keys

Primary Key

e6801728e13647190ba523d09c56731

Show

Copy

Regenerate

Secondary Key

428e7b74c0234c9d107d04nc5b04e50c

Show

Copy

Regenerate

Interface Configuration

Please select an interface to configure for this DIP ID

Interface

IF-001 - Not configured

IF-002 - Not configured

IF-003 - Not configured

IF-004 - Not configured

IF-006 - Not configured

Add Member

Filter

Search

Email	Role	Actions
edwardkbowyer@live.co.uk	MP User Admin MP Message Admin MP Certificate Admin MP Analytics Reader	Offboard
User	Eleven user11@sit.testmp.co.uk MP User Admin MP Message Admin MP Certificate Admin MP Analytics Reader	Offboard

Showing items 1 - 2 of 2 | Show 10 | All

<

1

>

MHHS PROGRAMME

Industry-led, Elexon facilitated

Section 6 – Message Channel Setup



MHHS PROGRAMME

ELEXON

Data Integration Portal

HOME

MARKET PARTICIPANT REGISTRATION

MESSAGE CHANNELS

MESSAGES

PERFORMANCE

Market Participants > Big Energy Company > DIP ID 149431682

DIP ID: 149431682

Navigate DIP Connection Provider

Details

Company Number	MPID	Market Participant Role Code	DIP Role Code	DIP ID	Effective From Date (MPR)	Effective To Date (MPR)
2242424	RDG1	X	SUP	149431682	2024-07-04	2025-07-04

API Keys

Primary Key

Secondary Key

Show Copy Regenerate

Show Copy Regenerate

Interface Configuration

Please select an interface to configure for this DIP ID

Interface

IT-001 - Configured

Publication Configuration

The Publication endpoint is where you receive messages sent to you from the DIP and is configured specific to each DIP ID

Publication URL

Subscription URL

Subscription Key

Subscription Secret

Subscription Token

Opt Out Preferences

Providing the ability to selectively Opt-Out of receiving messages for specific Grant Codes on Interface IT-001 for this DIP ID

Select Grant Code

Grant Code

Preference

Time Range

Description

It is not currently possible to Opt Out of publishing data on Interface IT-001 for this DIP ID.

MHHS PROGRAMME

Industry-led, Elexon facilitated

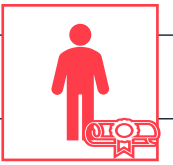


You have successfully onboarded to the DIP



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

Adding GlobalSign Admins



Guidance for Certificate Admin

Up to this point in the process, the Certificate Admin has been responsible for the vetting process and completion.

At this point of the process you may wish to assign additional Cert Admins to complete the upcoming sections as more technical knowledge is required to complete the next onboarding steps. Please note, this could be someone from the DCP or a 3rd Party technical Person.

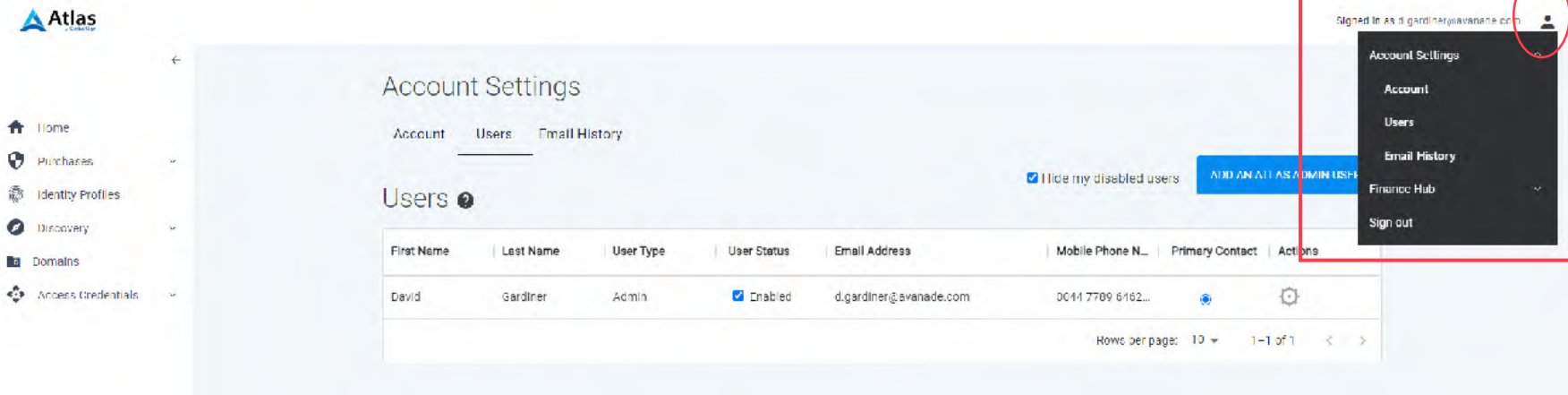
As well as adding the Cert Admin to the DIP they should also be added as a new User Admin within GlobalSign. See next page for details.

Please Note:

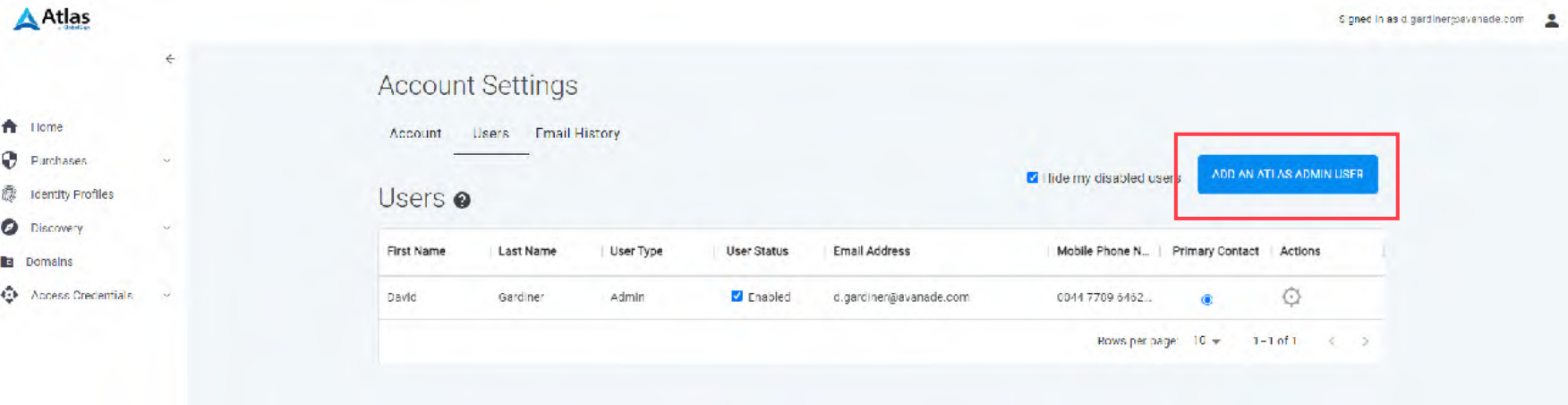
Additional Cert Admins are not mandatory at this point – you can continue through the process should you wish. If you decide to not add a new Cert Admin please ignore the next slide.



Assigning a new Cert Admin to GlobalSign Atlas account



Click the profile icon in the top-right corner. Select 'Account Settings' and then 'Users' to obtain the new user ADD screen



Select 'Add an Atlas Admin User' and add your new Cert Admin to the account.

This will result in a 'New User Registration' email being sent to that person.

Other resources

A full interactive demo of the on-boarding process can be found:

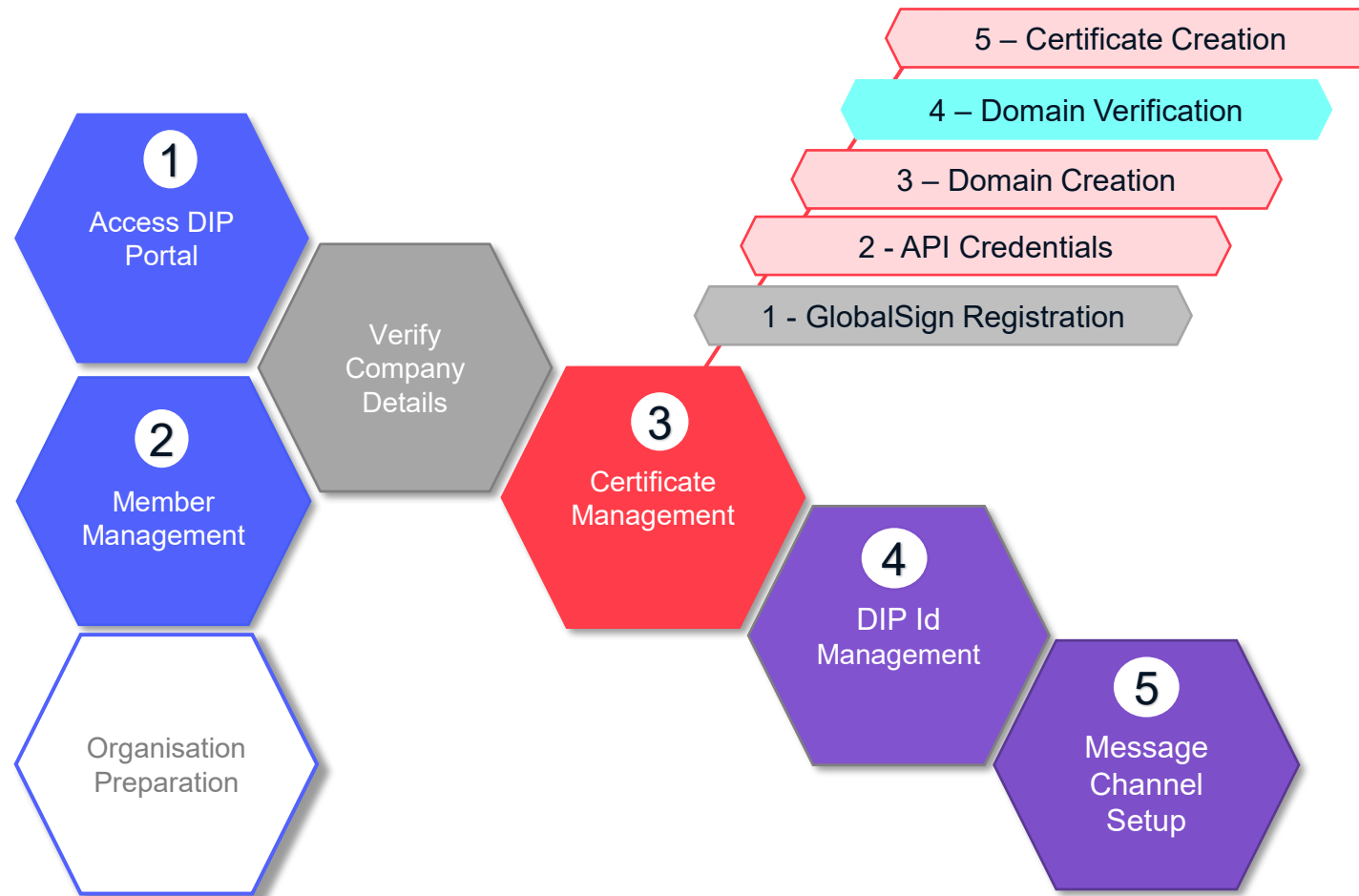
<https://www.youtube.com/watch?v=8K3fWSJFv0k>



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

Promotion to Production

DIP Onboarding Overview – Promotion to Production



Promotion to Production phase of DIP on-boarding involves transferring parties from the DIP UIT environment to the DIP production environment once they receive their PAB qualification.

The set of activities that need to be undertaken is a reduced set of instructions when compared to the initial UIT on-boarding tasks. All of the 'heavy lifting' has already been done.

Promotion to Production – Summary of Tasks

1. Access DIP Portal

- DIP Manager will send out the invite to on-board to the Production once they receive confirmation of PAB approval

2. Member Management

- The user base from each organisation is NOT copied from UIT. It is recognized that many companies will have different user bases between Production and non-Production

3. Certificate Management

- No requirement to on-board to GlobalSign
- New Globalsign signing certs and DIP MTLS/Signing certs are required

4. DIP Id Management

- MPIDs/DIP Ids/DCP Ids are copied over from UIT by DIP Manager
- DIP Manager updates the effective from time for each DIP Id according to the PAB guidance
- Qualified Party needs to download the pertinent API keys for each production DIP Id

5. Message Channel Setup

- Updated webhook configuration is required as the transfer of data from UIT to Production does NOT include the webhook config

1. Access DIP Portal

- DIP Manager will send out the invite to on-board to the Production once they receive confirmation of PAB approval

2. Member Management

- The user base from each organisation is NOT copied from UIT. It is recognised that many companies will have different user bases between Production and non-Production
- Set up Users as per earlier advice (slides 17-21)


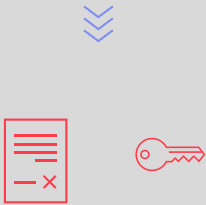
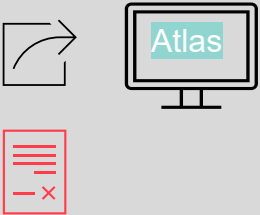
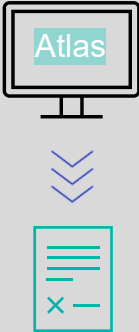

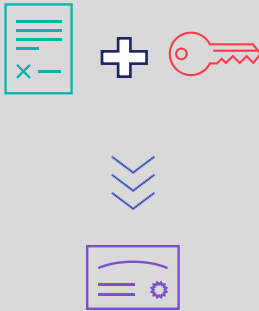
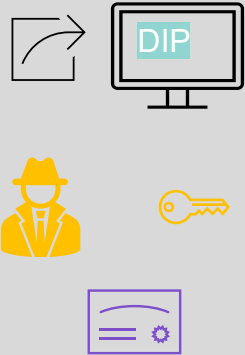
3. Certificate Management

- No requirement to on-board to GlobalSign
- New Globalsign signing certs and DIP MTLS/Signing certs are required

Promotion to Production – Certificate Management



For each Company promoted into Production a new set of API Credentials and PFX mTLS/Signing Certificate need to be produced for upload into the DIP

1	2.	3.	4.	5.	6.	7.
Create API Credentials (Secret & API key)	Generate CSR & KEY file	Load CSR file into GlobalSign Portal	Generate CER file	Download CER file from Global Sign Portal	Merge CER & KEY file to generate PFX certificate	Upload the GS API Key & Secret, with the PFX Certificate, to the DIP
						

The steps taken are exactly the same as those provided earlier – see slides 37-57

The end result is a PFX file loaded into the DIP

Promotion to Production – Certificate Management

4. DIP Id Management

- MPIDs/DIP Ids/DCP Ids are copied over from UIT by DIP Manager
- DIP Manager updates the effective from time for each DIP Id according to the PAB guidance
- Qualified Party needs to download the pertinent API keys for each production DIP Id

The steps taken to generate the API keys are exactly the same as those provided earlier – see slide 64

The screenshot displays the ELEXON Data Integration Portal interface. The top navigation bar includes the MHHS PROGRAMME logo, the ELEXON Data Integration Portal title, and a user icon (UU). The main navigation menu has tabs for HOME, MARKET PARTICIPANT ORGANISATION (selected), MESSAGE CHANNELS, MESSAGES, and PERFORMANCE.

The main content area shows the path: Market Participants > Big Energy Company > DIP ID 1494431682. Below this, the DIP ID 1494431682 is displayed, along with a yellow button labeled "Nominate DIP Connection Provider".

The "Details" section contains a table with the following data:

Company Number	MPID	Market Participant Role Code	DIP Role Code	DIP ID	Effective From Date (MPR)	Effective To Date (MPR)
2242424	RDG1	X	SUP	1494431682	2024-07-04	2025-07-04

The "API Keys" section is highlighted with a red box. It shows the Primary Key and Secondary Key, each with a "Show", "Copy", and "Regenerate" button.

The "Interface Configuration" section prompts the user to select an interface to configure for this DIP ID. A dropdown menu is visible.

The "Members" section displays a table with the following data:

First Name	Last Name	Email	Role	Actions
Edward	Bowyer	edwardkbowyer@live.co.uk	MP User Admin MP Message Admin MP Certificate Admin MP Analytics Reader	Offboard
User	Eleven	user11@scflesimp.co.uk	MP User Admin MP Message Admin MP Certificate Admin MP Analytics Reader	Offboard

At the bottom, there is a pagination bar showing "Showing items 1 - 2 of 2" and a "Show 10 All" link.

Promotion to Production – Certificate Management

5. Message Channel Set-up DIP Id

- MPIDs/DIP Ids/DCP Ids are copied over from UIT whilst the webhook links are not as Production URLs need to be defined
- It is recommended that the API to set the webhook URLs is used instead of the DIP Portal
- API to use is:
<https://app.swaggerhub.com/apis/MHHS/PROGRAMME/SubmitEvents/1.8.3#/DIP%20Channel%20Publication%20Configuration/configurePublication>
- Using the API means that Production PKCS (generated and uploaded in the previous steps) can be tested before any actual message exchange has been initiated.

Thank you