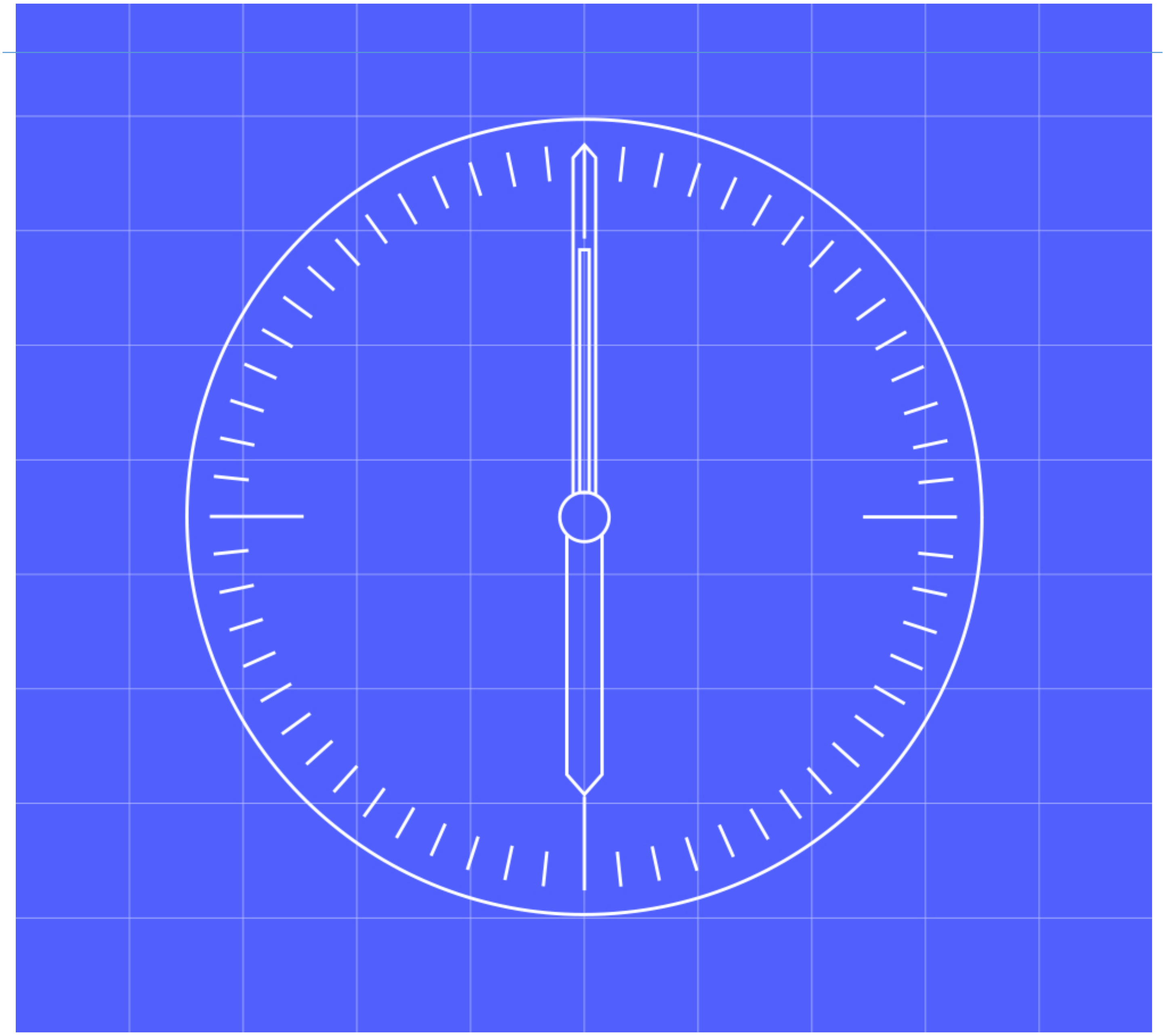
MHHS PROGRAMME
Industry-led, Elexon facilitated

DIP Onboarding FAQs



Document owner	Document number	Version	Status:	Date
DIP Team	**MHHS-DEL2066**	**Version 1.2**	**Approved**	**28/02/2024**

1. Contents

1.1 Change Record

Date	Author	Version	Change Detail
05/12/2023	Dolapo Adeyemi	0.1	For Review
05/12/2023	Dolapo Adeyemi	0.2	Added six more questions
08/12/2023	Dolapo Adeyemi	1.0	Approved Baseline
21/12/2023	Dolapo Adeyemi	1.1	Added six more questions
05/02/2024	Dolapo Adeyemi	1.2	Addressing Participant Feedback on v1.1

1.2 Terminology

Term	Description
DIP	Data Integration Platform
DCP	DIP Connection Provider
MP	Market Participant
URL	Uniform Resource Locator
GS	GlobalSign

2 Introduction

2.1 Background

This document is an addendum to the previously provided Onboarding Guide and the Webhook URL Configuration Guide and should not be viewed on its own.

2.2 Objective

The objective of this document is to compile the questions and answers received so far from the Market Participants throughout the onboarding process to enable participants to troubleshoot any issues they may encounter in the process of onboarding to the DIP. This document does not replace any other guides that have been previously published,

2.3 Document Scope

The scope of the document includes:

- Onboarding for CIT

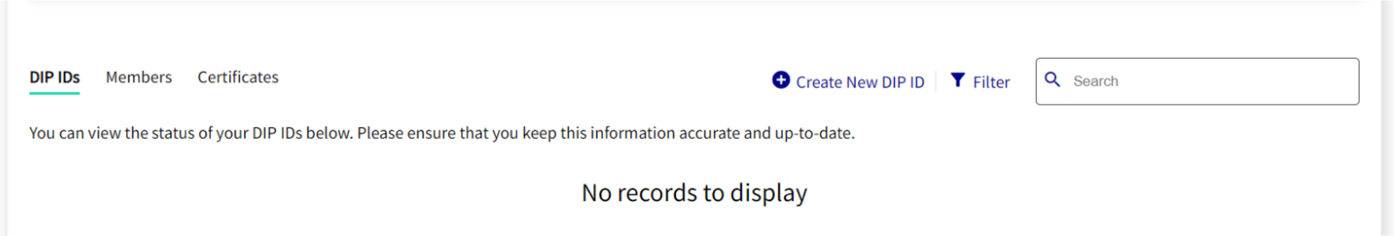
3 DIP Registration and General Portal

3.1 Q: Why haven’t I received my invitation link yet despite my interval environment availability?

- A: It was possibly blocked by spam, if invited you can login at https://portal.sit.energydataintegrationplatform.co.uk with the invited account to the same effect.

3.2 I am a Market Participant and I don’t see any DIP IDs listed; how do I assign my roles?

- A: All DIP IDs must correspond with those in the Industry Standing Data (ISD) and will be uploaded around the same time a participant onboards by the DIP Team. The enduring process for DIP ID allocation is still being discussed with the programme and this information will be updated once a final decision has been made. Please contact DIP support if your expected role(s) is not displayed so that it can be loaded in from the ISD. If you have created a new DIP ID, this will need to be corrected, so contact the DIP support team.



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

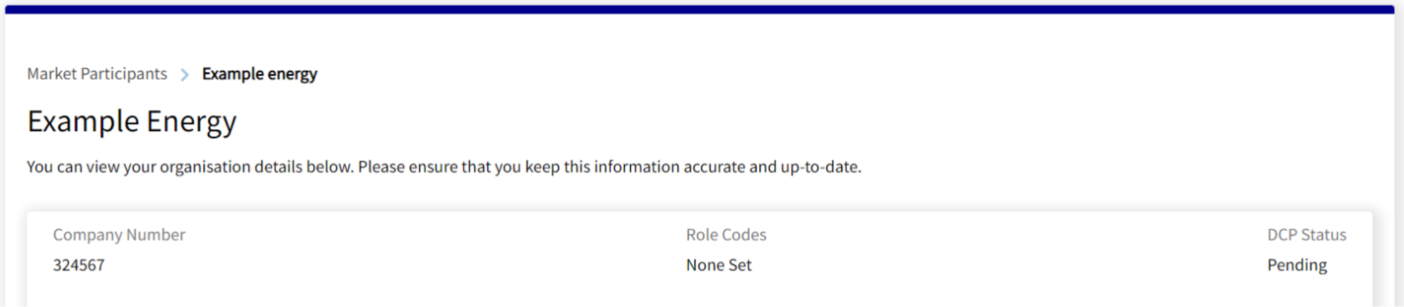
No records to display

3.3 Q: As a Market Participant, how do I nominate my DCP, I don’t see mine in the list?

- A: Only DCPs who have created DCP IDs, and whose DCP DIP IDs are yet to be allocated to a Market Participant are listed, please ask your DCP to create a new DCP DIP ID. These have a one-2-one mapping and once they’ve been nominated, cannot be reused. See sections 8 and 9 of the MHHS DEL1671 DIP Onboarding Guide.

3.4 Q: My DCP status is stuck in Pending, what should I do?

- A: Please contact support as a DIP Admin will need to approve your application.



Example 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
324567	None Set	Pending

3.5 Q: I am a DCP and want to Administer the Market Participant I provide for; how do I do this?

- A: Multi-organisation assignments are not currently supported, but you will be able to see all details of DIP ID that DCP was nominated for (From MP Org)

3.6 Q: As a MP User Admin, I have assigned myself additional roles, yet cannot see them reflected in the portal?

- A: You must logout and clear local storage in the browser to force a refreshed token with your new roles assigned.

3.7 How soon after onboarding would MPs receive their DIP IDs since their ability to nominate a DCP is dependent on this?

- A: Ideally as soon as they have been invited to onboard as they will be uploaded to the portal by the DIP team. Contact the DIP Support Team if this is not the case.

3.8 Some Participants have gone on to create DIP IDs – some before completing the cert process, some after completing the cert process. What’s the implication of DIP IDs deviating from ISD data?

- DIP IDs should match ISD data, as distributor mappings are created based on it. This is the only way all MPs in SIT can exchange messages predictably.

4 Certificate Admin Registration and Vetting

4.1 Q: I have not received a vetting call from GlobalSign

- The primary contact is made to a number GS have from a government database. The call will be made to your registered HQ. If this fails, they will contact the number entered into the first form on the GlobalSign registration to progress vetting. If this also fails a letter will be sent by 1st class post with instructions and the DIP Team will be informed.

4.2 Q: My cert upload to GlobalSign keeps failing

- A: Check you have pasted your API/Cert info without extra characters (e.g. space or '-'). It is possible the CSR may need regenerated.

4.3 Q: What is the significance of GS Domain Name creation?

- A: GS Domain Name creation is a process that involves registering a domain name with the country-code top-level domain name (ccTLD). It is used to verify the identity of the domain owner and to ensure that the domain name is unique.

4.4 Q: Does GS Domain Name creation have anything to do with the Signing or mTLS?

- A: Yes. For mTLS, the certificate is used for both ingress into DIP and egress to the webhook. When creating a certificate, you will be asked for a Host Name and Domain Name (the domain name that was vetted). It is relevant for the egress. The Host Name and Domain Name should be the URL of your egress webhook, otherwise, it won't bind to the certificate.

5 Certificates and Webhooks

5.1 Q: I am using OpenSSL but examples are Azure for Certs

a. Please see the instructions in the Addendum section for OpenSSL in the MHHS DEL1671 DIP Onboarding Guide. There is a short but sizable video available – please contact the DIP Team.

5.2 Q: What are the steps to raise a certificate for a DCP with a wildcard URL?

- A: Wildcard URLs are not permitted as they are avoidable in 95% of circumstances (use paths to differentiate between MPs) and allowing them also adds considerable cost and risk.

5.3 Q: How many roles, DIP IDs and certificates can a company have?

- A: A company can have as many roles as in the ISD data, which defines the market participants and their relationships. A company can also have multiple DIP IDs, which are allocated as in the ISD. A single mTLS certificate can be used for all DIP IDs, and multiple signing certificates are allowed but not required for CIT.

5.4 Q: What should I do if I have not received my onboarding email for User Admin?

- A: If you have not received your onboarding email for User Admin, please check your spam folder and make sure that you have provided the correct email address. If you still have not received it, please contact the DIP support team and they will resend it to you.

5.5 Q: Do I need to use different mTLS and signing certificates for different DIP IDs?

- A: No, you do not need to use different mTLS and signing certificates for different DIP IDs. You can use the same certificate for all DIP IDs, which simplifies the process and reduces the risk of errors. However, if you prefer to use different certificates, it should still work as long as they are valid and registered in the DIP portal.

5.6 Q: Why do I get a “Domain creation failed” message when I try to register my domain in the DIP portal?

- A: This could be due to a known defect in the DIP portal, which is being fixed and tested in PIT. The defect causes the domain validation to fail for some domains, even if they are correctly configured in DNS. The DIP support team is aware of this issue and will notify you when it is resolved. In the meantime, please do not attempt to register your domain again until you receive further instructions.

5.7 Q: MP has 3rd party organisation performing the DCP role, which party should be generating the certificate?

- A: DCP to create their own mTLS certificate within the DIP Portal, and MP to create own Signing Certificate and can either use that to sign a certificate and send on to their DCP or share their Signing Certificate with their DCP (subject to agreement between DCP and MP on how to safely transfer Certificates). This is based on the non-repudiation requirement – every message to be signed by the originating MP.

5.8 Q: What happens if any part of the DIP Onboarding process experiences a delay during end-to-end onboarding?

- **A:** In the event of delays during the DIP Onboarding process, the program plans to manage lost time by addressing the specific delays and adjusting the timeline accordingly. Contingency plans may be put in place to mitigate any impact on the overall schedule.

5.9 Q: User Admin connected their MP’s portal profile to their first DCP and discovered they had access to all the DCP’s setup, including Certs, members, and DIP IDs of their other customers. Is this intentional?

- **A:** No, this is not intentional. The situation where a user from another organisation has access to all DCP setups is currently being addressed, and a Change Request is in place to rectify this unintended access. Defect fixed in release from 04/12/2023

5.10 Q: Users haven't been prompted for Multi-Factor Authentication (MFA) in a long time. Is the current 7-day interval secure enough?

- **A:** MPs suggest that the 7-day interval for MFA prompts is not secure enough. Instead, they recommend being prompted for MFA every 24 hours to enhance security. Avanade to work on this.

5.11 Q: PFX files cannot be password protected when uploaded into the portal. Is this a security weakness?

- **A:** PFX files are used for Avanade to communicate with GS (GlobalSign) on behalf of the MP. Since the purpose is message signing, the decision to password protect PFX files lies with the MP. They can choose whether to password protect the files based on their specific security requirements.

5.12 Q: Can one only have one active certificate? Is it necessary to revoke a certificate before creating another one?

- **A:** Please read the Code of Connections document before creating certificates so as not to create an invalid one.
- **A:** Also, read the Code of Connections document before revoking certificates. Conditions for revocation of certificates can be found in Section 3.5.2.2 of the MHHS-DEL1197 - Interface Code of Connection v1.3. If none of the reasons stated apply, then do not revoke your certificate.
- **A:** Each user has a quota of **2 certificates per year**, and these certificates can be rotated. All issued certificates remain active until explicitly revoked. Revoking a certificate does not give you one back on your quota. If you require additional certificates, please contact the programme office as this will incur additional costs.

5.13 Q: A DCP, who is also an MP Organisation has a Common user who will be an admin for intervals 3, 4, and 5. Is this permitted?

- **A:** Yes, a role can be associated with multiple intervals. However, this participant has also encountered an issue where they were locked out of prior intervals. A Change Request has been raised to address this, and efforts are underway to resolve it promptly. Kraken should reach out to the DIP to request the restoration of interval 3 access for their User Admin.

5.14 Q: When will the RBAC (Role-Based Access Control) issue be fixed in order to guarantee one-to-many scenarios?

- **A:** The fix for the RBAC issue is currently being worked on. Specific timelines for implementation will be communicated once available.

5.15 Q: Can the domain used for vetting be different from the domain used for certificates during the certificate and vetting process?

- **A:** Yes, the domains can be different as long as you can create the necessary DNS records. if you're intending to do this, please contact the DIP mailbox for support.

5.16 Q: Participant initially had separate mTLS and signing certificates. Now they have a combined certificate in their Azure Key Vault, but the certificate chain is invalid. What should they do?

- **A:** To resolve the issue, use the issuing and root CA (Certificate Authority) along with the intermediate certificate. Installing these certificates should allow you to send messages successfully. Additionally, install the intermediate CA. Avanade is investigating why the full chain is not coming back from the API Address. In the meantime, installing the issuing and root CA serves as a workaround. Mark Chivers should email the details, and Alan will provide the C# code to trust the certificate chain.

5.17 Q: How will API keys be sent?

- **A:** Currently, API keys are sent via encrypted email. However, in the future, the Cert admin will be able to generate their own API keys.

5.18 Q: What are the constraints and requirements for choosing a domain name?

i) **A:** The only constraints are that the domain needs to be owned by the MP and the MP has the ability to update DNS for the domain.
ii) The format of the domain doesn't typically include the www. prefix, as this is typically a host within the domain (i.e. web host/web site www.customera.com in the customera.com domain).
iii) The domain is the same domain on which the webhook is going to be hosted.

5.19 Q: We received a Domain name failure error message. Should we use the Atlas portal to create and validate a domain?

- **A:** There is no harm in using the Atlas portal to create and validate a domain. Once added, the domain will be available in the portal, allowing you to create a certificate.

5.20 Q: Can we use our own certificate on our webhook?

- **A:** No, the certificate needs to be issued via the DIP Portal and issued by the DIP intermediate Certificate Authority (CA): "MHHS DIP Message Security Issuing CA 2023"

5.21 Q: How do I bind the mTLS certificate to our webhook?

- **A**: When creating a certificate in the DIP Portal you specify the hostname and select the domain, these combined should be the URL of the webhook. The Subject Alternative Name (SAN) of a DIP certificate specifies two entries the URL of the webhook and the common name as devised by the DIP Portal, the certificate can be bound to either entry.
- See attachment titled "mTLS certificates and Market Participant Webhooks" for further details (Appendix 2)

5.22 Q: What are the different certificates I need?

- A: There are two types of certificates:
  - GlobalSign connection certificate - the DIP portal requires a market participant to get a signed certificate in the GlobalSign portal. This cert is used in conjunction with an API Key and Secret to allow the DIP portal to communicate with the GlobalSign API to get DIP certificates signed:
  - DIP Message Security certificate - used for message security when communicating with the DIP, certificates can have one of three purposes:
    - mTLS - used to secure the channel when sending or receiving to/from the DIP. Created and used by a DCP, can be used for all connections to the DIP
    - Signing - where the private key is used to sign messages prior to them being sent to/from the DIP. Messages are sent with the certificate, which is used to verify the signature. Created and used by an indirect DCP, single signing cert required for the MP. Can be shared by the MP to their DCP, however, this would involve sharing the Private Key and is between the MP and their DCP.
    - mTLS & Signing - used for both purposes above. Created and used for both purposes by a direct MP
- See attachment titled "Certificates Required" for further details (Appendix 1)

5.23 What else do I need to know about mTLS certificates and Market Participant Webhooks?

- See attachment titled "mTLS certificates and Market Participant Webhooks" (Appendix 2)

5.24 How do I install certificates on a Webhook (Azure Function)?

1. Register Custom Domain in the Azure Function
2. Create entries in DNS
3. Bind the mTLS certificate to the Custom Domain
4. See attachment titled "Installing certificates on a Webhook (Azure Function)" for further details (Appendix 3)

5.25 Q: Can I get a wildcard certificate?

- A: No, you are allowed 2 certificates per year with an option of adding more upon request in very exceptional cases. Wildcard certificates cost 10X more than regular certificates and are not required in most cases.

5.26 Q: Partial chain errors

- A: We are looking into the issue around the chain not being supplied with our leaf certificate, but as a workaround, the certificate chain certs can be downloaded from:

- http://secure.p.globalsign.com/cacert/mhhsdipmessagesecurityica2023.crt (Opens in new window or tab)
- http://secure.p.globalsign.com/cacert/mhhsdiprootca2023.crt (Opens in new window or tab)

- Code examples can be provided on how you validate a certificate with this chain.

5.27 Q: Which domain name do I use?

- A: For signing certificates (or mTLS and Signing) the domain chosen by the Market Participant for vetting should be used. For mTLS (only) certificates the DCP's domain should be used.

5.28 Q: Does this mean every webhook we create / ask customers to create will have to use the domain that was used for the GS domain creation?

- A: Yes. If you have one webhook across all your MPs, then you can put that hostname into that cert. You don't need more than one webhook / URL. At the moment, you're capped at 2 certificates. This is not enforced now but will be enforced in production. GS can give more certs, but more certs cost more money.

5.29 Q: New MP for which we are acting as a DCP is going through GS verification and has used our (DCP's) domain name. Is this right?

- A: No. It should be the MP's domain. Whilst the MP can still use the DCPs domain, it's not ideal. However, signing certs must contain the originating MP's organisation's domain name. See FAQs 5.18 and 5.27

5.30 Q: As an MP, if I mistakenly enter the wrong domain name during the GlobalSign process, e.g. my DCP's domain name, instead of my organisation's what should I do?

- A: Go back to the page prior to that and enter the correct domain name

5.31 Q: Are the DCP IDs environment specific? Will DCPs get a different set of IDs when they get to SIT B etc or will they remain the same for every environment for each MPID/Role Code?

- A: DCP Ids are environment specific and are not part of the ISD feed, so in each environment will be different. has context menu.

5.32 Q: Certificate Status should be Active as per the Onboarding document, but status is "ISSUED"

- A: Onboarding Guide Screenshots were taken from an earlier version of the DIP. Any certificate that shows up under "Currently Active Certificates" are active.

5.33 Q: while attempting to "Merge Signed Request" into KeyVault as part of section 4 of the onboarding guide we are getting the following Key Vault error when uploading the file presented via "Download ICA"; "Unable to parse X5c certificate chain and locate leaf certificate"

- A: Download ICA is the GlobalSign portal, any CSR generated and signed using the DIP portal will not have that subject name. The error itself is that the cer file doesn't match the CSR.

5.34 Q: CoCo v1.3 states that the API Keys are available via the APIM Portal. I can access the APIM Portal via the DIP Portal but cannot find the User Profile page (with Keys) as illustrated in the CoCo

- A: The API Keys will be sent to you via encrypted email. The feature for generating them via the portal is currently not available.

5.35 Q: What are the parameters to consider while registering a webhook for inbound.

- A: It's entirely up to you, but it's important to remember that the DIP certificate has to be bound to the webhook URL. URLs should be all lower case when set up in DIP.

5.36 Q: Can we have a single webhook for all inbound messages.

- A: Yes, this is a valid scenario.

5.37 Q: How do we provide authentication for the webhooks.

- A: Your webhooks, should use DIP generated certificate, and check message signature.

5.38 Q: If a market participant has multiple DIP Participant IDs, will they need to have multiple signing certificates or will all DIP IDs use the same certificate for signing?

- A: The same signing certificate can be used

6 Smoke Testing

6.1 Q: How do we know if a message we sent has passed all the validations(L1, L2.. etc) and if it is stuck at any stage.

- A: L1 validation is usually received synchronously, so you should receive an error message if anything is wrong (HTTP 400) or HTTP 201, followed by a separate standard response sent to your error/status URL with L2 errors.

6.2 Q: What IP address will the DIP be calling MPs from?

- A: Find DIP IP addresses as follows:
  - Inbound: 20.254.70.171
  - Outbound: 20.90.209.207