MHHS Webinar: DIP Onboarding Webinar

MHHS-DEL1618

1 SPECIFIC QUESTIONS RELATING TO THE DIP ONBOARDING DEMONSTRATION 1
2 ADMINISTRATIVE QUESTIONS 4

Change Record

Date	Author	Version	Change Detail
08/09/23	Annabel Atkins	0.1	Initial draft

Reviewers

Reviewer	Role
PPC Team	Comms & Engagement

1 Specific questions relating to the Data Integration Platform (DIP) Onboarding Demonstration

Q1. Is there any mandate on the Multi-Factor Authentication (MFA) set up? Does this have to be mobile or are other options available?

MFA is required within seven days of logging into the DIP. Participants can choose from three options to verify their identity:

1. One-time PIN number via SMS
2. Verification phone call
3. Microsoft Authenticator App

There are other authenticator applications available, however, participants should note that the process is often not as seamless as Microsoft.

Q2. Can only one user per participant have access to the DIP (based on the MFA requirement?)

Participants can (and should) have multiple users for each role with the DIP to ensure that there is always someone available who has the right level of access. The User Admin role assigns and manages the roles to each member of their organisation who will access the DIP. Participants should follow the link in the invitation email and sign in with their existing credentials. They will be prompted to set up their own MFA when they first log in.

Q3. Is User Admin 'NO' or 'ADO' and what role is Cert Admin?

The User Admin does not have to be the Nominating Officer. The User Admin is the person assigned to receive the invitation from the DIP Manager to join the DIP and will generally be the administrator of the other User roles and assign control of responsibilities to each member.

In the Interface Code of Connection document, we identify the Senior Responsible Owner (SRO), the Technical Contact (TC) and the Appointed Responsible Owner (ARO) as individuals who can be assigned as the Cert Admin.

Q4. Please could you provide more detail on sending and receiving IF/PUB/REP messages?

Sending and receiving IF/PUB/REP messages is all operational and will form part of a future webinar.

Q5. How does this help me send a message to the DIP Simulator?

The DIP simulator and the DIP are two separate entities. The DIP Simulator has been developed by the Sims & Ems team. Please contact them for more information by emailing Sims.Ems@mhhsprogramme.co.uk and contact should be via the Sims and Ems team.

Q6. Where in this process do you specify the SRO, ARO and TC?

Certificate Admin will take on those roles in the DIP. The updated Interface Code of Connection document which will be available after the next SDWG, will describe the relationship between the ARO, SRO and TC and the Cert Admin role in the DIP.

Q7. Can multiple associates get access for a particular role?

Yes. The assignment of the user roles that were demonstrated can be assigned to as many people as needed within the organisation to make sure there is sufficient coverage and enough people in the different roles. One individual can have multiple roles.

Q8. Could you please provide a link to the DNS set-up process document?

The Domain Name System (DNS) set-up is internal to each participant's organisation. We will be issuing the DIP Onboarding User Guide which will take participants through the step-by-step process for full onboarding to the DIP. Most organisations will have a Change Advisory Board (CAB) or change process that will need to be talked through. We recommend participants find out who the right technical people are within their organisation to update the DNS records.

Q9. Is the API Key used when sending messages?

Yes.

Q10. Can you please elaborate on how GlobalSign determine a contact method of the company you work for to verify the identity of the user?

When participants register with GlobalSign they will need to provide the details of the company they work for. GlobalSign will then use a government database to find out the contact number for the company and will use that to verify that the individual signing up works for the company.

Q11. I presume this demo is for CIT/SIT? Will there be a separate DIP onboarding process for Qualification testing?

There may be a slightly evolved version of the onboarding process in the future, however, this webinar covers the bulk of the onboarding process, and this is not expected to change significantly. The Qualification process will be similar if not the same.

Q12. For a third-party adaptor to connect to the DIP, is the Cert Admin someone in the DIP adaptor vendor? Are the vendor cert admin employee details used in GlobalSign?

The correct terminology to use here is 'DIP Connection Provider' (DCP) rather than 'Adaptor'. This is where a third-party acts on a participant's behalf to provide the messages. The DCP and the participant will need to onboard separately onto the DIP. Within the DIP portal there is a yellow button that reads 'assign DIP connection provider'. This will link the two organisations together. For the DIP to connect these organisations, they both need to be registered and have their certificates.

Q13. Can you specifically set out what steps you are expecting a Nominating Officer to Execute?

The Nominating Officer is the person that will be vetted by GlobalSign to ensure they work for the organisation. The vetting and registration stage can also be completed by the Certificate Admin on behalf of the Nominating Officer, provided it is the Nominating Officer's details that are submitted. Although the Nominating Officer's details are entered, the email address that is provided below should be that of the Certificate Admin, as this is where GlobalSign will send their response.

The process is described in more detail in the DIP Onboarding User Guide which is due to be published.

Q14. Do market participants using a DIP adapter use a unique domain name or can they share the same domain name as other participants using the same adapter?

They will both need their own unique domain names. The DIP connection provider will need to register a domain name that they will use for the certs they require, while the individual participants will need to use their own domain name. Sign-ins from the participant but Mutual Transport Layer Security (mTLS) from the DIP provider instead. The DIP Connection Provider can use the same domain name for different Programme participants they are representing.

Q15. How will this process work for DIP Connection Providers? As a DIP Connection Provider, we will need to request an mTLS cert in our own name and then Message Signing Certs only?

DIP Connection Providers will be able to request an mTLS certificate on behalf of their own company. The sign-in certificates will need to be provided by the participant.

Q16. Can the Cert User be an employee of a service provider, or does it have to be an employee of the market participant?

The Cert Admin can be from another organisation.

Q17. In the demonstration you downloaded a CER file but you requested an MTLS and signing cert. Would you expect a private key as well which would potentially be a PFX file?

Yes. This part couldn't be showed during the demonstration. After the GlobalSign stage there is further activity which allows the file that is received to be converted to PFX. The process then comes back to the portal where the Cert Admin can upload the PFX file.

Q18. If either SRO, ARO or TC can be the Certificate Admin, do we need to appoint all of those roles or just one?

Not all of those roles are mandatory - it can be one person. There will be an updated version of the Code of Connection document coming out following the Security Design Working Group (SDWG) on 20 September, which will include updates on the relationships between SRO, ARO, TC and the Certificate Admin concept.

Q19. Will there be a future webinar for obtaining your private and public keys for digitally signing messages?

This is certainly possible and will be taken into consideration in the planning of future webinars. The process of creating a private key will depend on the Programme participant or the DIP Connection Provider, however we can provide a demonstration of how we do it.

Q20. Can two organisations share the same MTLS certificate?

No.

Q21. Will the market participant need to get a certificate themselves even though only the DIP connection provider certificate will be used to connect to the DIP?

Participants will need to create a certificate for signing purposes only. DIP connection providers will use their own MTLS certificate for connections. It is important to note that where participants are using a third-party DIP connection provider, they will still need to go through the onboarding process.

Q22. Does an organisation providing a DIP adaptor need to be onboarded or can all the necessary tasks be performed by the market participants using the DIP adaptor?

The correct terminology to use here is 'DIP Connection Provider' (DCP) rather than 'Adaptor'. This is where a third-party acts on a participant's behalf to provide the messages. The DCP and the participant will need to onboard separately onto the DIP. For the DIP to connect these organisations, they both need to be registered and have their certificates.

Q23. How reliable is GlobalSign with data reliability, as it does not work too well with passport organisation?

There are many options assessed but GlobalSIgn was regarded as optimum for this application. Details of the Atlas application can be found here: GlobalSign Unveils Next Generation PKI Platform, 'Atlas,' to Ease Complicated PKI Management from Overburdened Enterprise IT and Security Teams

Q24. Is there any kind of physical device needed for logging into the DIP?

Yes, for Multi-Factor Authentication (MFA).

Q25. The approach for MPs using a software / DIP provider is not clear. Please could you provide a worked example including who can / should be appointed in roles?

The correct terminology to use here is 'DIP Connection Provider' (DCP) rather than 'Adaptor'. This is where a third-party acts on a participant's behalf to provide the messages. The DCP and the participant will need to

onboard separately onto the DIP. For the DIP to connect these organisations, they both need to be registered and have their certificates. Please refer to the DIP Onboarding User Guide for more details (when published).

Q26. Is FIDO2 possible for the MFA e.g., YubiKey?

This is still under confirmation and will be advised at a later date.

2 Administrative questions

Q27. Will these slides be shared?

We will not be sharing the slides from this webinar; however, we have shared the recording on the MHHS website and the Collaboration Base.

There will be a DIP Onboarding User Guide that will be published on the Collaboration Base, the MHHS website and in the Clock that will provide detailed information on the onboarding process in its entirety, including the red bits outside of the DIP. In order to complete the successful delivery of the certificate to the DIP, participants should follow the sequencing of stages as they appear in the guide.

Q28. When will the guidance be published?

Both the DIP Onboarding User Guide and the updated Code of Connection document will be published by the end of September 2023

Q29. Will the Code of Connection be updated to reflect what has been described in the webinar?

Yes. Both the DIP Onboarding User Guide and the updated Code of Connection document will be published by the end of September 2023.

Q30. When will the future webinar around sending and receiving messages take place?

This will be confirmed in due course and confirmed via The Clock, Collaboration Base and MHHS website.