MHHS Webinar: Data Integration Platform (DIP) – Code of Connections and Public Key Infrastructure Policy

MHHS-DEL1230

Change Record

Date	Author	Version	Change Detail
16/05/23	Alice Chudley	0.1	Initial Draft
16/05/23	Richard Gwatkin	0.2	Second Draft

Reviewers

Reviewer	Role
PPC Team	Comms & Engagement

1 Certificate

Q1. Does 'placing reliance' as a general principle extend to parties being able to delegate certificate requests to their software provider?

Parties are responsible for delegating any nominating officers, senior responsible officers, appointed responsible officers and technical contacts. The organisation is fully responsible rather than Market-wide Half-Hourly Settlement (MHHS) or DIP Manager.

Q2. Regarding managing DIP certificates, for suppliers with third-party managed services can certificates be sent directly to them, or will they be directed to the supplier first?

Where a Programme participant actively makes a certificate signing request, they will need to provide their chosen DIP Connection provider with the key materials using a secure mechanism. See Code of Connections (CoCo) Section 6.2 “Private Keys” for further details.

Q3. CoCo mentions the use of a Portal to request and access certificates. Will this be in place in time for Component Integration Testing (CIT) commencement?

Yes, the DIP User Portal will be in-place for CIT.

Q4. Has the Programme allowed appropriate time to undertake the Public Key Infrastructure (PKI) activities before starting testing that requires certificate usage?

Yes, Avanade have integrated GlobalSign into the DIP User Portal for both vetting / registration and certificate management. This is scheduled to be ready for all parties on-boarding into CIT. The MHHS Design team are working on how the process will work for Pre-Integration Testing (PIT).

Q5. When certifications expire and a new one is requested, will the old one work until its end date to allow seamless transfer?

This is correct.

Q6. Where a company has >1 Programme Participant ID (MPID) interacting with the DIP, but is not using a third-party Dip Connection Providers (DCP), would one set of certificates be used for both MPIDs or one set per MPID?

One set of certificates for all MPIDs; one for non-production, one for production.

Q7. Is there a process for developing and testing certificates?

There are production and non-production certificates. The process is the same for both. Non-production certificates are accessed via the non-production portal, and production certificates via the production portal.

Q8. What was the reason for sending the public key as a header, rather than sending a key ID and allowing the recipient to download the key from global sign?

The public key certificate is sent in the header because if the key was retrieved from GlobalSign, we would need up-to-date GlobalSign credentials for each Programme participant. Man-in-the-middle (MITM) attacks are negated, as the public key certificate will only be accepted if it has been issued by the correct Certificate Authority.

Q9. What about the fourth scenario for connecting to DIP? Party uses a DIP Connection provider, but that provider uses a separate connection for each party.

The design can be flexed so that the DCP will create multiple DCP IDs if they wish and assign a different DCP ID to each of their clients, however this is not really required. The separate connections can use the same Mutual Transport Layer Security (mTLS) certificate.

Q10. Where a company has multiple market roles, will a separate certificate be required for each market role, even where all roles use the same DIP connection?

A single certificate suffices.

Q11. What will be the maximum certificate age?

397 days will be the maximum certificate age. Please see CoCo section 6.1.1 Certificate Issuance for further details.

Q12. When will applications to Avanade for certificates need to start?

The recommendation is to start at least one month before being onboarded to the DIP.

Q13. What is the Certificate rotation policy?

397 days – please see CoCo for the certificate rotation policy. See section 6.1.1 Certificate Issuance for further details.

Q14. If placing reliance on a software provider in SIT or Qualification Testing, and they are testing with another customer's data, whose certificates do they use?

Messages must be signed with the correct Programme participants certificate (separation of customer environments need to be key within their design).

Q15. Third Connection Scenario - how does that work if the connection provider is not a BSC Party and cannot request their own connection certification?

DIP Connection Providers don't have to be BSC Parties.

Q16. Is the same certificate used for mTLS and for JavaScript Object Notation (JSON) signing?

Yes, for active participants, not for inactive participants using DCPs. This is clearly explained in the CoCo.

Q17. The document suggests that the certificate is being sent at the same time as the message. We would expect the recipient to retrieve the certificate from the Certificate Authority (CA)?

The certificates will come originally from the CA and is a dual-purpose certificate which is authorised to do JSON signing and MTLS signing. They are separate but can use the same certificate for two different purposes.

Q18. For DIP High Availability/Disaster Recovery (HA/DR) will we need to provide additional certificates for JSON signing & endpoint [Technical Layer Security (TLS)] security or will the certs be duplicate deployed [re-use]?

No additional certificates will be required for HA/DR purposes.

Q19. In Functional Specification (FS) a service provider has their own certificate, this seems more complex, what is the reason for the difference?

The requirement from Ofgem was for all Programme participants to digitally sign their own messages.

Q20. Can you confirm how much of the certificate signing request process will require manual activity vs being available via Application Programme Interfaces (APIs)/possible to automate?

We automate as much as possible in the DIP portal, however, generation of the Certificate Signing Request (CSR) must be undertaken by the Programme participant from the system requesting the CSR.

Q21. Can you expand on the decision to use the same certificate for mTLS and digital signing. Good practice would typically be for these to be separate.

This was based on advice from Avanade and GlobalSign.

2 Connectivity

Q22. Section 5.2 does not appear to include connectivity testing of the Live / Prod with Adapters. Nothing in the Programme Project Plan, which could be a significant risk of connectivity failure.

Through the PIT, CIT, and Systems Integration Testing (SIT) phases the connectivity will be tested. When we look to move into a productionised state, the same processes will be followed as the previous non-production environments, but more specific connectivity testing must be understood from the testing / transition / migration plans.

Q23. The CoCo is part of the connectivity piece, which relates to the requirement of Balancing Settlement Code (BSC) acceptance. Is work complete to allow Non BSC parties to connect to the DIP?

Programme participant and DIP Connection providers will register in the DIP. There is no longer a requirement for DIP Connection Providers to register with the BSC to access the DIP. However, Programme participants will be required to complete the qualification process.

3 DIP IDs

Q24. How do non-active participants nominate their active participants (technology service providers)?

Non-active participants will need to create DIP IDs for all the services they are registered for, and then they will need to assign the DIP IDs over to the technology service providers (the Programme uses the term DIP Connection Providers), by assigning the corresponding DCP ID to the DIP ID.

Q25. Where a Technical Contact (TC) supports multiple Programme participants, will they need multiple user accounts for the user portal?

No. Once a Programme participant has been given stewardship of their DIP IDs to a DCP, the DCP can view the DIP IDs within the portal.

4 Issue 101 Forum

Q26. Is the Code of Connections & PKI Policy documentation being progressed through the MHHS Programme Security Working Group as well as the Issue 101 forum?

Yes, the CoCo and PKI Policy will be taken to the Security Design Working Group (SDWG) before the Design Advisory Group (DAG).

The Issue 101 forum deals with the issue of enduring DIP governance. Issue 101 embraces the need for the CoCo and the PKI Policy and will ensure that these documents are included in the future governance plans.

Q27. Please could you confirm the enduring governance of the CoCo? Will the obligations on users be captured in the Programme BSC drafting?

This will be addressed in the Issue 101 forum.

5 Document Management

Q28. Please confirm how parties can submit more formal comments back to the Programme on the document?

The CoCo and PKI Policy are both currently out for industry consultation. To submit your feedback, please download the PKI Policy Comments Log and Interface CoCo Comments Log documents, on the DIP page on the MHHS website and save with a file name that includes the short name of your organisation. Once completed, please email the spreadsheet to PPC@mhhsprogramme.co.uk by **17:00** on **25 May 2023**.

Once the consultation period is closed, the Programme will review the comments submitted and publish comment responses and updated documents for industry assurance review. More information will be shared on this in due course.

Q29. Please confirm release (v0.5) is an early draft, the document does not appear to have been reviewed ahead of its release (errors displayed within the document).

At the time of publishing this Q&A version 0.5 was an early draft of the Interface Code of Connection document.

Q30. Has the Programme used lessons learnt from Switching? The document does not account for business requirements (E.g., only 1 TC solely responsible per Market role).

Yes, this was discussed at SDWG, and the consensus was to align with Faster Switching, In the DIP, a party can nominate as many TCs (Technical Contact) as they feel is necessary to support their business. A TC can either be an employee of the Programme participant organisation or an employee of a third-party organisation such as a DIP Connection Provider.

Q31. Has the Programme recognised that the CoCo NC0077 was not complete by end of the Switching Programme. It still had several unresolved issues?

Yes, we expect the CoCo to be a living document through to production.

Q32. Where do we find the early release documents or where can we subscribe to this type of information?

Information on the consultations have been emailed to the Programme participant principal contacts.

Q33. Can we confirm the versions and location of the documents being reviewed?

The documents are available on the Data Integration Platform pages of the MHHS Website and Collaboration Base. As of the publishing of this Q&A, the PKI Certificate Policy is version 0.2 and the Interface Code of Connection document is version 0.5.

6 Miscellaneous

Q34. How are we defining a Supplier given that larger suppliers may be set up with Settlement and Forecasting functions within a (separate) Trading business?

This is covered in the DIP Design. Large Suppliers can operate as an 'umbrella' organisation where they control multiple Programme participants from a single organisation account.

Q35. We understand that only a Supplier role has access to the DIP and unless you are a Supplier then you cannot access the DIP directly. Is this true?

No, all Programme participants and DIP Connection Providers can access the DIP. Please contact the PPC Team at PPC@mhhsprogramme.co.uk if you would like to gain access to the DIP.

Q36. Can you confirm the location of the Swagger files (API definitions)

https://app.swaggerhub.com/apis/MHHSPROGRAMME/SubmitEvents/1.2

This location will be moved once Avanade stand-up the Production DIP environment. The version number is currently 1.2, this will change as new releases get rolled out. Version 1.2 is "work in progress" but it does give participants early visibility of forthcoming changes.

Q37. Will messages be re-signed by the DIP before being sent to recipients, or will they retain the originator's signature?

Yes, the DIP will re-sign messages before they send it on to the recipient.

Q38. Do the Senior Responsible Officer (SRO) and Appointed Responsible Officer (ARO) need BS7858 checks?

No, the Programme participant / DIP Connection Provider Organisation will be vetted as part of the registration process and not individuals. Programme participant / DIP Connection Provider organisations are responsible for vetting their own employees who they authoriae to act as an SRO/ARO/TC.

Q39. Section 8.1.4 Verifying Signature - The logic seems incorrect as we are not verifying our own hash of the message to the hash in the signature. Do you agree?

The hash can be verified against either the X-DIP-Content-Hash, the recipients calculated hash or both. We could update section 8.1.4 to say:
The Content Hash matches X-DIP-Content-Hash and/or your own hash of the body content using SHA256.

Q40. Is it proposed that individual parties appoint a DIP manager role, or is this central?

This is a Central Role. This role is currently undertaken by Chris Wood at Elexon.

Q41. How are you going to manage the access to different APIs for different participants? Or are all the APIs accessible by everyone who can sign in?

All APIs are accessible to all participants once they have completed the DIP on-boarding process. If a participant attempts to send/pull data from a channel for which they do not hold the correct authorisation (i.e. role) they will receive a '401'/'403' response.

Q42. Could you confirm what payload compression/content encoding will be supported?

There is not a payload compression/content currently.