Renewal of EU Hub Public Certificates & Alert endpoints

Q&A Session: Questions and Answers – Version 4

Document history:	
Date of publication:	19th May 2022
Supersedes:	Version 3
Changes compared to superseded version:	New Q&As: N/A Revised Q&As: 3.2

Important disclaimer: The answers may include recommendations or advice. You are solely and exclusively responsible for deciding any particular course of action or omission and for implementing any actions or taking any decision on this basis. EMVO disclaims all liability with regard to such actions or decisions and their consequences.

This document sets out the main questions raised during the Q&A sessions regarding the renewal of the EU Hub public certificates & endpoints. The document will be updated following each Q&A session. The recordings of the *Q&A session 1* can be consulted here, the *Q&A session 2* here, the *Q&A session 3* here and the *Q&A session 4* here. Further information can also be found in the enhanced version of the slide deck which is available here.

Regularly consult EMVO's website and Knowledge Database (here) to follow up on the latest communication.

Contents

1. General 2
2. Connection Providers, EMVO Gateway & Direct connection 3
3. Timeline of certificates & endpoints renewal 5

1. General

1.1 What is the purpose and the frequency of renewing the EU Hub Public certificates & alert endpoints?

Answer: To ensure technical security, the EU Hub uses certificates with a validity period of 5 years. This period is now expiring, and an update is required. The certificates and endpoints will require a new update in 5 years.

1.2 Where can we download the EU Hub certificates from?

Answer: The certificates can be downloaded from the OBP Portal in 'Step 4 – Technical On-Boarding'.

1.3 Will this change require a new Session Token and EU conformance test?

Answer: No, this will not require a new session token and/or test status metrics to be redone.

1.4 Should we change the certificate if we downloaded one in the previous year?

Answer: Yes, you need the new certificates.

1.5 Where do we get the new endpoint information from?

Answer: On 'Step 4 – Technical On-boarding' of the OBP Portal, you can click on Step 4.1 "Technical Info Pack" wherein the document EMVS0714-EMVS SDK for OBPs v16.0 can be found.

1.6 Do we need to start with the CSR step?

Answer: No, you do not need to perform the CSR step. Please consult the recordings and/or the slide deck for further information (*refer to page 1 of this document*).

1.7 When will the new certificates be available on the OBP Portal?

Answer: They are already available in the OBP Portal in 'Step 4 – Technical On-boarding'.

1.8 Will there be any downtime(s) during the renewal of the certificates/alert endpoints?

Answer: Currently, no downtime is foreseen.

1.9 Which time zone are the times expressed in?

Answer: The times are expressed in CEST – Central European Summer Time.

2. Connection Providers, EMVO Gateway & Direct connection

2.1 What is a registered Connection Provider (Gateway Provider)?

Answer: This is a third-party contractor engaged by the OBP, who assists in whole or part of with the development, implementation, provision, use and/or operation of the OBP interface to the EU Hub via a Gateway Connection. OBPs can choose to connect to the EU Hub via a *direct connection* (data send from OBPs system straight to EU Hub) or a *Gateway Connection* (data sent first to a Gateway Provider. The Gateway Provider sends it through to the EU Hub).

2.2 What is the EMVO Gateway?

Answer: This is an alternative means of connecting to the European Hub (alternate to developing a direct connection, or other Gateway Provider solutions). The EMVO Gateway provides an easier way to connect to the EU Hub using typically understood techniques and is aimed at the OBPs who want to participate in pilot programs but do not yet have a direct connection established or smaller OBPs who have no need for the direct connection because their volumes of batches are much lower.

2.3 How can I check which Connection Provider(s) my company is using?

Answer: An OBP can have up to two (2) connections. You can check the type of connection and connection details in your OBP Portal account in Steps 4.2.1 and 4.3.1.

2.4 Is there any detailed guidance on how specifically to handle this change using common systems, like SAP or Tracelink?

Answer: No, EMVO has no detailed guidance on how SAP, Tracelink or other Connection Providers should perform the change as each system is unique and only their respective teams would be knowledgeable on the topic.

For SAP users: all SAP ICH customers do not need to perform any actions - SAP will take care of it. The OBPs will be contacted to get the certificates and the update will be executed for all customers.

For Tracelink users: all Tracelink users will be informed before the actions are executed and following the completion of the renewal process.

2.5 Do we have to do something as a developer? Is there a new SDK or is this just about endpoints and certificates that would have to be replaced by 18th July, at the latest? At the moment we have the 2018 endpoints. Is it enough to replace them with the new ones, or has something changed in the database structure or WSDL?

Answer: There is no new SDK – the API is exactly the same. All OBPs have to update the certificates and endpoints.

2.6 If we use a connection provider, what are my responsibilities as an OBP?

Answer: You have the responsibility to ensure that your provider updates the certificates, and you remain connected to the EU Hub.

2.7 If we use Tracelink, do we need to send the certificate to Tracelink because it is a personal certificate, or can I relax because it is a common certificate for all users, and someone already sent it to Tracelink?

Answer: The certificate that changes is the PUBLIC certificate and NOT your personal one. Therefore, the public certificate should be provided to Tracelink (or at least one Tracelink client has to provide the certificate to the connection provider). *This also applies for any other connection provider and not only Tracelink.*

2.8 Are there any actions needed from OBPs? Should our Simple Network Management System (SNMS) implement these certificates at their infrastructure?

Answer: The OBPs should provide all the needed materials to their connection provider or technical team (in case they have a direct connection). The connection provider and/or technical team should perform the renewal.

2.9 If we use EMVO Gateway, are we affected by this change at all?

Answer: Yes, you are affected. However, EMVO Gateway users should not perform any actions, as the EMVO technical team will take care of the certificate renewal.

2.10 What to do if I do not have a Connection Provider or do not use EMVO Gateway?

Answer: If no Connection Provider (or EMVO Gateway) is used then it can be assumed that your organisation has created a direct connection. In that case, the knowledge on how to perform the implementation should be with the team that developed the direct connection. To ensure your team has all the needed information at hand, make sure you are forwarding all the communication distributed from EMVO.

2.11 Where to install the new certificate if I am not using a connection provider?

Answer: The certificate should be installed within the system you are using. Please contact your technical team for more information.

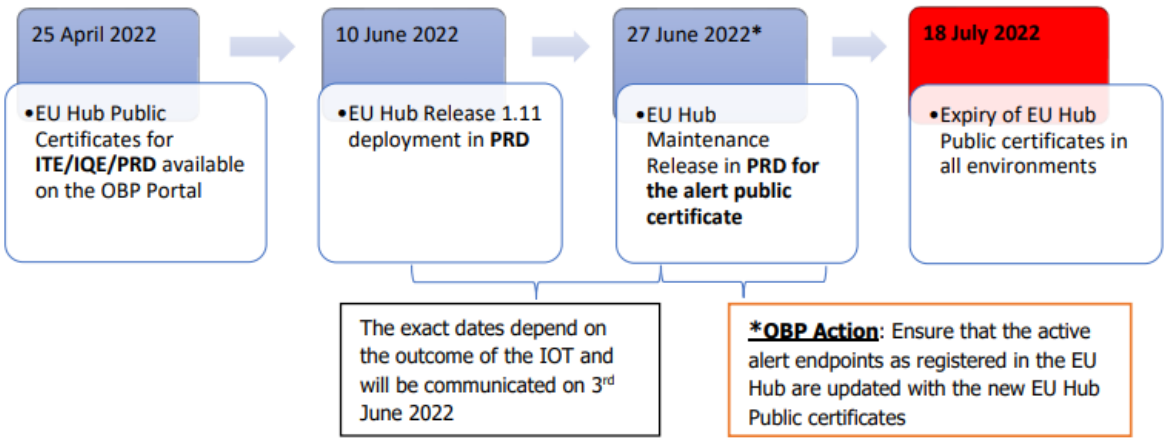
2.12 Do these certificates need to be installed in the testing environment as well (ITE/IQE) and should sanity tests be performed?

Answer: The certificates should be installed within each environment the OBP is active in. A sanity check can be performed.

3. Timeline of certificates & endpoints renewal

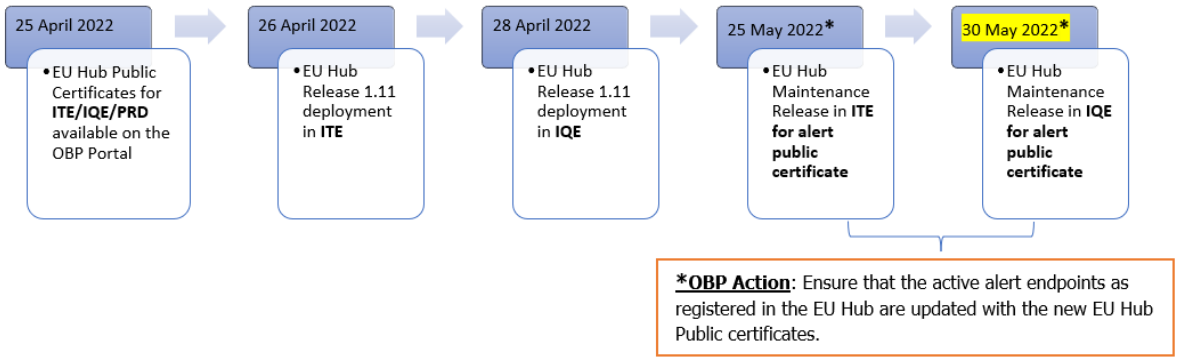
3.1 What is the timeline for the changes in the PRD Environment?

Answer: The timeline for the PRD Environment is as follows:



3.2 What is the timeline for the changes in the ITE & IQE Environments?

Answer: The timeline for ITE and IQE Environments is as follows:



Do not hesitate to consult the recordings (*refer to page 1 of this document*) and EMVO's website (Knowledge Database → Letter of Announcements) for the latest information on the timelines.

3.3 Why do we have to update the certificate for transactions until the 27th June? Wouldn't it be possible to update both the transactions and alert certificates at the same time?

Answer: Yes, you can update both at the same time if you want. EMVO is simply advising that you can sort the primary connection out sooner.