

CMA – HSBC API Implementation

4th July, 2016



Agenda

1. Recap of our response to the PDR on APIs
2. Issues around technical implementation
 - a) Whitelists and PSD2
 - b) Permissions management and PSD2
 - c) Experience from other regulatory projects
3. Brief discussion of work of Payments UK on selection of IE and IT
4. Implementation risks specific to the Ring Fenced Bank

Recap of our response to the PDR on APIs

We strongly support the CMA's adoption of APIs as one of its foundation remedies. We think APIs have the potential to change the nature of competition in the retail banking market.

The main issue is around timeframes: large scale IT projects are very unpredictable. The development of a project's scope can generate significant amounts of unanticipated work streams. It is nobody's interests for things to go wrong.

There are four key, inter-related issues which need to be addressed for all customer data:

- a) Authorisation and Authentication
- b) White lists / Third Party Provider (TPP) registration
- c) Permissions management
- d) Customer redress mechanisms

We identify issues and options around white lists and permissions in the next section.

The IE and IT will need to integrate the CMA remedies work with work on PSD2. It is not yet clear (i) how far PCWs will fall within the scope of PSD2, and (ii) the extent to which it is possible for the CMA remedies work to run ahead of PSD2 implementation.

Given the range of uncertainties at this stage, the CMA should provide the IT with considerable discretion to set time frames for each aspect of the API implementation programme.

Whitelists – necessary for the Midata data sets

- “Read only” midata data sets present a data security risk to customers (in particular identity theft).
- A whitelist/TPP registration process is required.
- This will ultimately need to be set up on an industry wide, centrally managed basis.

Integration with PSD2:

- The European Banking Authority (EBA) is working on the Regulatory Technical Standards (RTS) which will likely include the processes and standards to be adopted in respect of Whitelists.
- The RTS Whitelists may not be approved until late in 2018
- The RTS Whitelists will relate to AISPs and PISPs: it is not clear whether PCWs will fall into either of these categories.

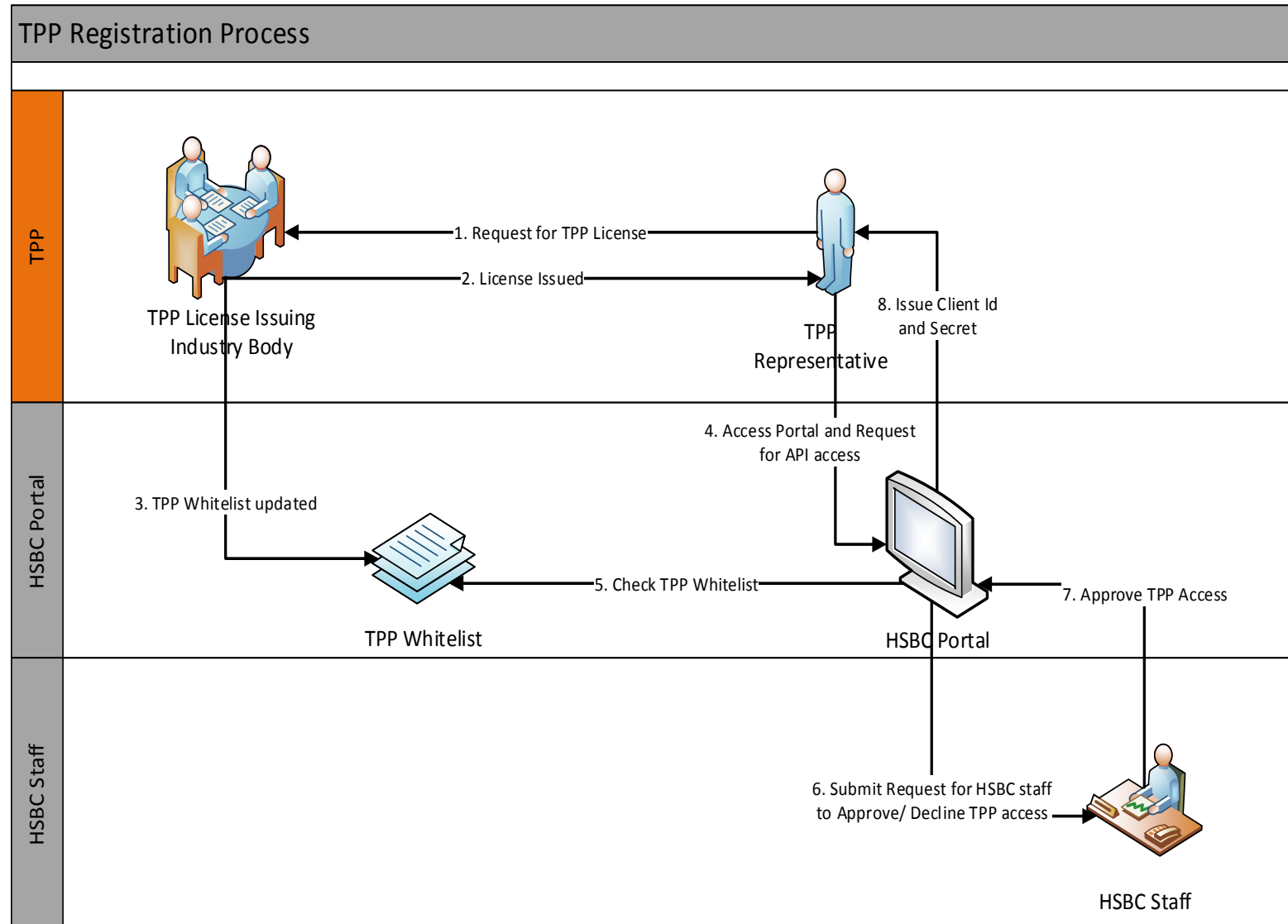
Centrally managed Whitelists

Requires a separate licensing body to assess and approve applications by TPPs for a license.

TPPs may need to submit to data security audits (equivalent to those conducted in the payment card industry – PCI DSS).

This can take time to agree and set up

In recent work on Lending Referrals, the process of due diligence and accreditation of the platforms (i.e. who banks will pass customer details to) took over 12 months:.



[See annex for more detail]

Short term alternative – HSBC manages TPP registration and verification

- The TPP applies to HSBC directly for permission to access HSBC customer data.
- HSBC applies objective and non discriminatory criteria to assess whether to supply the TPP with access to customer data.
- **Advantages:** this process does not require a third party data security certification authority to be set up. It may expedite the sharing of Midata data.
- **However:** it is not a replacement for the development of industry wide whitelists – TPPs will need to verify their security credentials with each bank individually.

The CMA should leave it open to the IE and IT to decide on how to tackle this issue

Permissions management

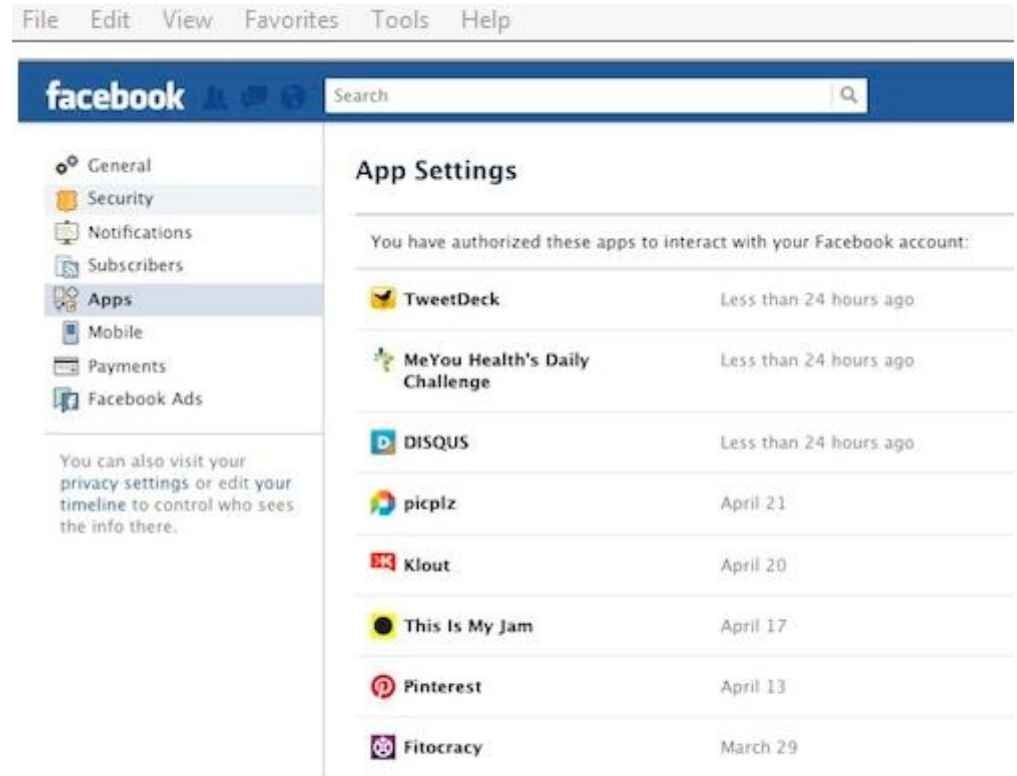
Development of a full permissions management regime will take time

Customers will need to be able to manage which TPPs can access their banking data, on what basis (eg read/write) and for what time period

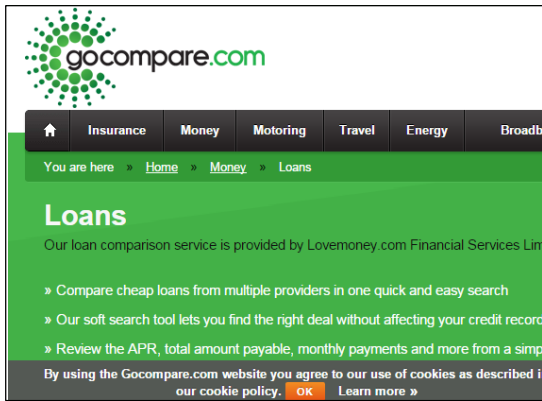
This will need to be developed as part of RTS for PSD2 – it may be difficult to front run PSD2 requirements

It may not be necessary for the sharing of read only Midata data (see next slide)

CMA should provide the IE and IT with discretion over how to implement permissions management

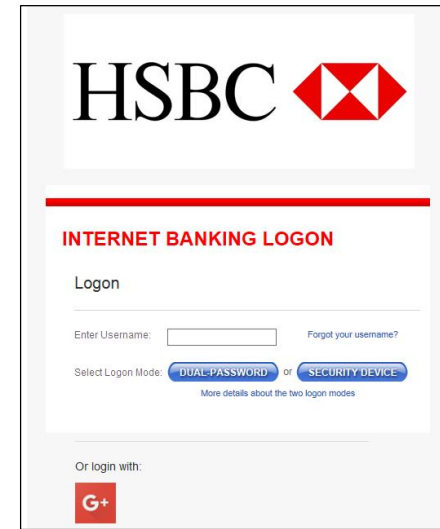


One off permission for Midata data possible

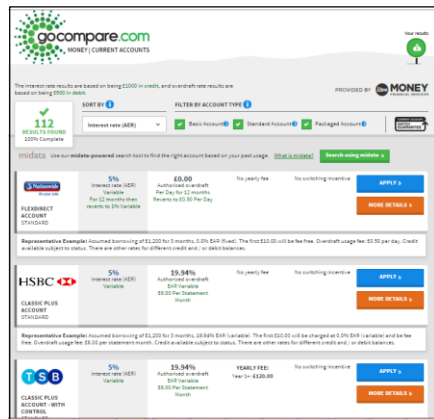


Customer accesses PCW

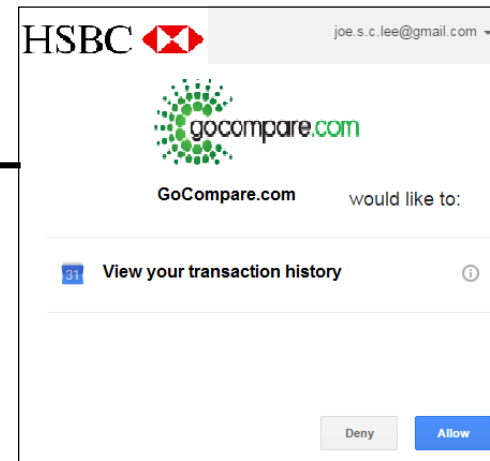
Customer gets redirected to HSBC site for authentication, while PCW requests for customer data (closed data)



HSBC asks for customer consent



HSBC serves PCW with the Customer data (Time bound – OAuth Token)



RESTRICTED

Recent experience of other IT projects

The original Midata data project commenced in March 2014, and completed in Q1 2015:

- A Midata file standard was agreed which covered: the period the data would cover, the format of the file, how balances should be displayed and which elements of the merchant transactional description should be redacted.
- The original deadline was December 2014, however a late change in specification delayed implementation to the end of Q1 2015.
- This did not require any consideration of the data security standards at issue in respect of the use of APIs for Midata data sets.

CASS: commenced in Mid 2011, delivered in Q3 2013.


- All banks needed to agree diverse elements of the service including, data definitions, liabilities, timings, customer verification and messaging standards.

Implementation Entity and Trustee

- Payments UK is helping the nine banks identified by the CMA to work on this.
- HSBC is happy with the progress made to date.
- Objective is to propose an Implementation Trustee by early August.
- Does the CMA have any views on the progress of Payments UK to date?

HSBC: contention with the Ring Fenced Bank (RFB) work

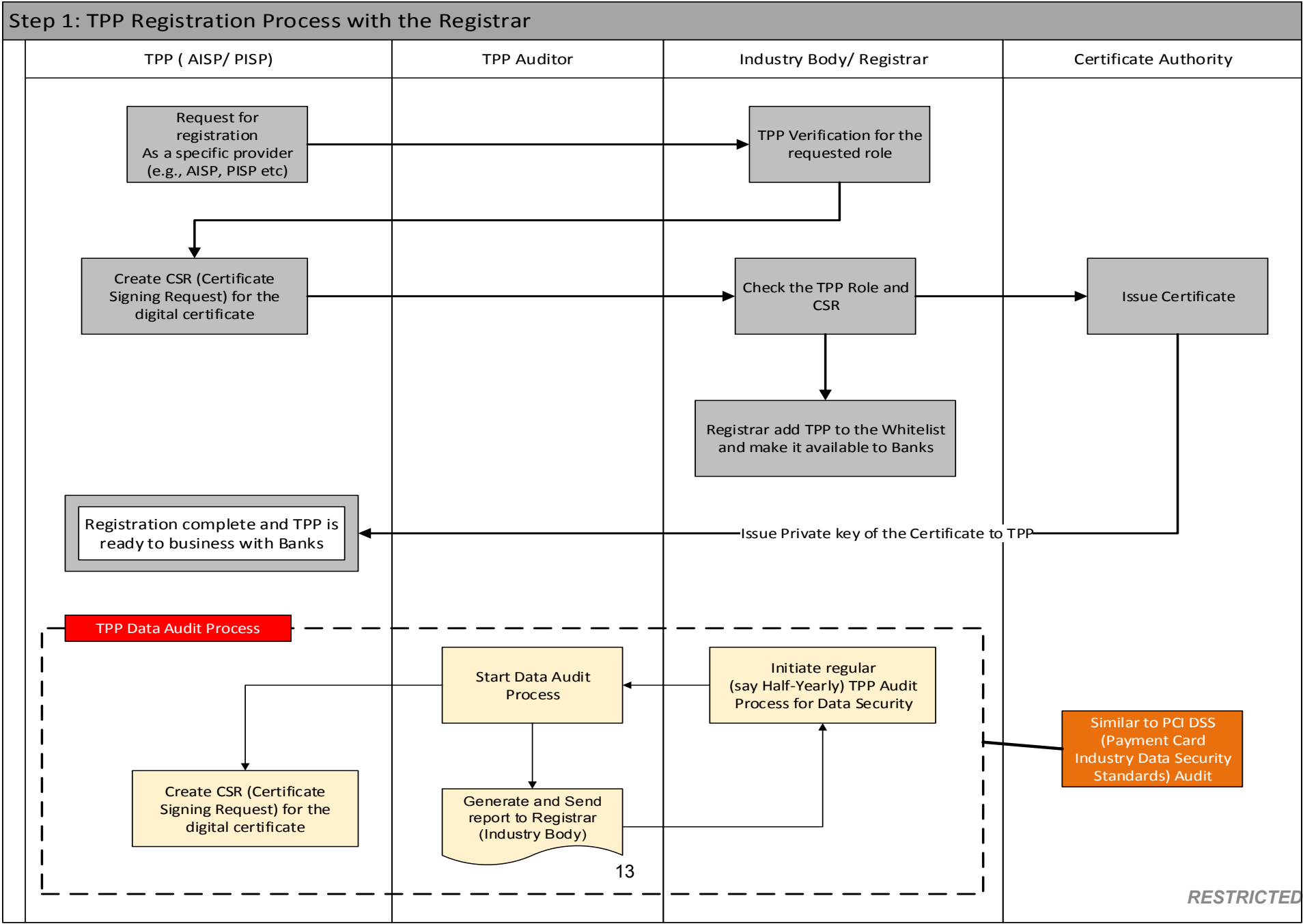
[CONFIDENTIAL]



Annex:

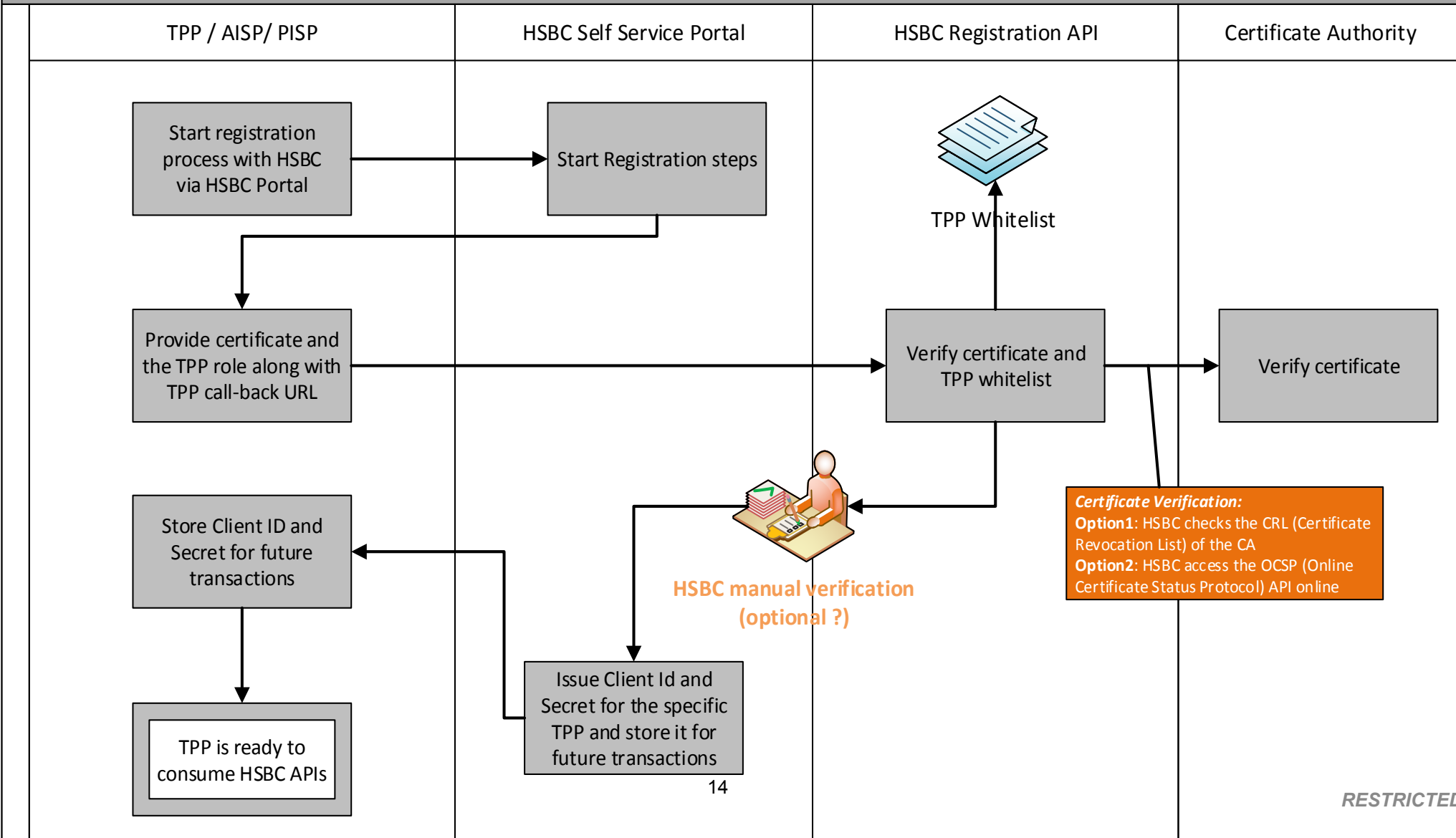
The Whitelist/TPP registration process

Step 1: TPP Registration with Registrar



Step2: TPP Registration with HSBC

Step 2: TPP Registration with HSBC



Step3: TPP – API Consumption

Step3 : TPP Request for HSBC API Consumption

