BPAY ID Investigation – Findings

Introduction

There was a requirement to assess the capability of BPay Digital ID and this document presents the findings around that investigation.

The System

The BPay Digital ID system is developed and maintained by BPay and they can involve other organisations such as banks and other qualifying organisations as Identity Providers (IDP) in their system. The users of the system are Relying Parties (RP) and Illion would also act as one.

It is a mainly browser UI based system which prompts the user at various points and gets the them to click buttons and to fill out forms. There are also web services based requests and responses that occur in the background that are not visible to the user and are used to exchange sensitive information between the various actors in the system such as IDPs and RPs.

BPay has specified at other actors would also be involved in the future named Service Providers or Credential Providers that can provide other information beyond the basic identifying personal information provided by IDPs. This information would include educational qualification information, working with children background checks, etc. BPay has stated that Illion could be a Service Provider and could provide information such as credit reports as a part of this information.

Example Use

An example use would be if a RP such as Illion had an user at a web based form that required additional information such as their personal details. A button would be presented at the top of the form prompting the user to connect to the BPay Digital ID system.

Rather than filling the form with their full name, date of birth, email address, phone number and residential address, the user would elect to press the button at the top of the form to connect them to the BPay Digital ID system. Once this button is pressed the user is presented with a list of IDPs that they can select from to retrieve their personal information. From this list, which would include all the IDPs that are on the BPay system, the user would select their bank.

Once they make this selection, without filling the form, they are re-directed on their browser to the IDP (e.g. their bank) website where they are presented with form, asking the user to login using the IDP or their bank credentials. Once they login they are presented with another form asking the user to provide authorisation to share their personal information with the RP (e.g. Illion).

The user is actually directed to the page hosted on the IDP's / bank's side. The user logs into the bank system using their everyday login details and once authenticated, they are re-directed back to the RPs page which is again hosted on the RPs side. BPay does not have access to the user's bank credentials and also is not aware of the contents of the information that is sent from the IDP to the RP. BPay knows only the type of information that was sent for billing purposes.

This form presents to the user exactly what information held at the IDP would be shared with the RP such as their full name, date of birth, etc. along with a check box control they must click on to authorise access and a button to confirm the authorisation.

Once the user provides the authorisation, the user is re-directed back to the RP's form where they started from and the form gets populated automatically with the data from the IDP, which they authorised earlier to share with the RP. This information is transmitted to the RP via web services based responses.

The advantage is that the user does not need to manually fill in the form at the RP and their data is automatically populated for them from the data they initially provided to the IDP, which they consented to share with the RP. In addition to saving the user time, it can also minimise errors in the form data.

If the user were to select an IDP that they are not registered with, then once they go to this IDP's page, they would not be able to proceed any further and they would need to return to the starting form at the RP to select the correct IDP.

In the BPay demos there has also been a sign-up form for the user at the IDP side, but BPay has stated that the user would never see this sign-up form in a production environment. This is because the user would already be configured to use BPay Digital ID on the bank side prior to using the system. There may however be a one off acceptance of terms of services form the user would have to click and accept.

Available Data

Currently the only available data from IDPs that are banks, is in the form of user data such as the user's full name, date of birth, email address, phone number and residential address. Organisations other than banks may also become IDPs as long as they qualify for it.

It is expected that state government departments, Australia Post, etc. would be the initial Service or Credit Providers with more to be added later on.

More data would be available later on such as BSB and bank account numbers as well as other information such as the user's educational qualifications, background checks such as working with children checks, etc., with the bulk of this information being available from Service or Credit Provers. BPay has stated that Illion could be a Service Provider and could provide information such as credit reports as a part of this information.

At this stage BPay do not have any documentation in relation to exactly what data would be available beyond the basic identifying information available about users from IDPs. However, they have stated that Illion would be able to provide them with information on any required data.

Meeting Recordings

This document is based on meetings conducted between BPay and Illion. The recordings of these meetings are available at this network location:

xxx

The first meeting was on the 26th of May 2022 and the recording for this is in the folder titled "2022-05-26 BPay Digital ID Technical Meeting" at the above network location. In addition to general information that would be useful for everyone, this recording has extra information on how to configure and run their sample applications, which is expected to be valuable for system implementers.

The second meeting was on the 30th of May 2022 and the recording for this is in the folder titled "2022-05-30 BPay Digital ID Billing Information Meeting" at the above network location. This meeting was mainly focused around the billing aspects of the BPay Digital ID system but also has general information about the system.