

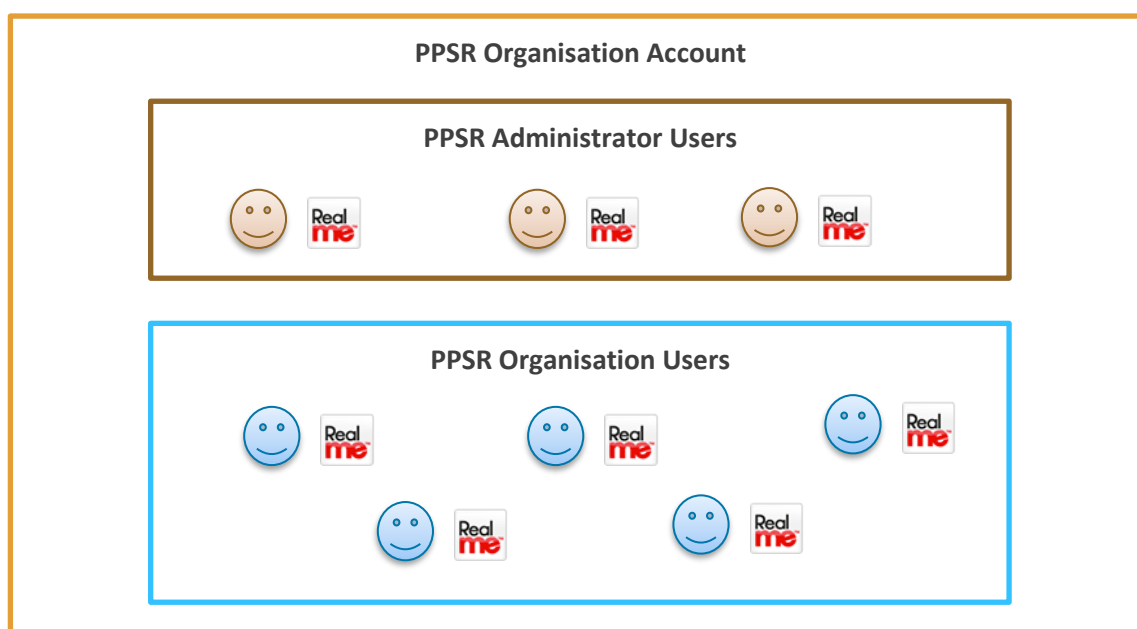


PPSR API Authentication Options & User Scenarios

The purpose of the user scenarios is to help PPSR software providers choose the most appropriate PPSR API authentication and authorisation model to use for software products.

PPSR Organisations

A PPSR organisation account can be set up in the PPSR website to define a group of PPSR users who can all transact on behalf of a single organisation. Users access the PPSR system with their RealMe login¹.



Creating a PPSR organisation account

When a user first registers on the PPSR website, logging in with a RealMe login, they have four available options:

- Set up as a new PPSR individual user
- Set up as administrator of a new PPSR organisation account
- Become a PPSR organisation user (in response to an invitation email)
- Retrieve legacy PPSR account details

Administrators

¹ The RealMe login can be the same as the user uses for other government services, e.g. Companies Office, and doesn't have to be RealMe verified.

A PPSR administrator user has elevated privileges that allow them to add new PPSR organisation users and to delete users that are no longer with the organisation.

It is strongly recommended that a PPSR organisation account always has at least two administrators to ensure that access and ability to maintain the PPSR organisation account is not compromised if one administrator is unavailable or has left.

Adding a user to a PPSR organisation account

New PPSR organisation users can be added to a PPSR organisation account by an administrator using the website or via an API call.

An email invitation will be sent to a staff member with a link for them to follow to become a PPSR organisation user. The email will include an activation code to enter once the user registers on the PPSR website with a RealMe login.

Deleting a user from a PPSR organisation account

PPSR organisation users can be deleted from the PPSR organisation account by an administrator using the website or via an API call. When the user is deleted any API tokens associated with the user are automatically revoked.

A deleted user is able to register in the PPSR system again using their same RealMe login, to become a new individual user or member of a different PPSR organisation account.

E.g. if a staff member changes jobs to work at a different finance company they will be able to carry on using their own RealMe login under their new employer's PPSR organisation account.

Transacting in the PPSR

Any PPSR organisation user can conduct PPSR transactions on the PPSR website on behalf of their organisation using the payment options available to the organisation, or separately as an individual.

PPSR will record the organisation and user details of who conducted each transaction.

API Access

Subscription key and Three-Legged OAuth

The preferred method for accessing PPSR by API is the use of three-legged OAuth tokens that identify the PPSR user that is making the transaction.

The provider of a product that uses the PPSR subscribes to the API and generates a subscription key to be used by the product. Users of the product do not need to subscribe to the API.

Each user that will access the PPSR API through the product goes through a one-off consent process². At the end of the process a three-legged OAuth bearer token and refresh token associated with their PPSR user are generated. Transactions that they make via the software will authenticate to the PPSR API using the subscription key and the three-legged token.

Advantages

- An end user of PPSR software only has to register in one place, the PPSR website, and doesn't need to go through separate processes to get access to the PPSR API. There's no delay for new users of PPSR software to get started.
- Simplified user management, any user that exists in the PPSR system can transact via PPSR API without any further set-up required.
- PPSR has more detailed information about which user in the organisation has made a transaction.

Disadvantages

- More complex integration for software providers as they must support the generation of three-legged bearer and refresh tokens.

Subscription key only, or subscription key with Two-Legged OAuth

The alternative method for accessing PPSR via API is for end-users of a product to subscribe to the PPSR API themselves and generate their own access details that are then entered into the product.

One user in a PPSR organisation account goes through a subscription process² to request access to the PPSR API and generates a non-expiring subscription key that is used for all transactions by their organisation's PPSR software product. In some cases the product may require a further level of security through the use of short-life OAuth tokens. In that case the user will also need to generate the credentials necessary for token creation.

Multiple users in the PPSR organisation could create API subscriptions and have their own API subscription keys for use in transactions, but in that situation it should be considered whether the three-legged model with its just-in-time token provisioning is more appropriate.

Advantages

- Simpler technical integration for software providers.

² See Appendix A

Disadvantages

- More complex set up for customers as they must go through an API subscription process on a website separate to the PPSR website, and must wait for access requests to be approved.
- More difficult to manage PPSR access. If the user that set up the API subscription leaves the organisation then another user must go through the subscription process to ensure continuation of access.
- No audit trail in the PPSR system of who made a PPSR transaction, all transactions will show as from the same PPSR organisation account.

User Scenarios

It is up to the software provider and their business customer to decide which method of access is most suitable for their needs, some common scenarios and situations where these are applicable are described here.

Multiple end users, individual PPSR logins

I'm a business that has multiple staff, each with their own login to the software I use for connecting to the PPSR. My software uses three-legged OAuth authentication to connect to the PPSR APIs.

Applies to

- Users of commercial off the shelf (COTS) products that connect to the PPSR, e.g. small-medium finance companies, motor vehicle traders etc.
- Direct API consumers that have developed their own products to connect to the PPSR.

PPSR organisation account management

All the staff in my business that need to use PPSR have a login to the PPSR website. At least two of these staff are PPSR administrator users.

Software and API set up

I don't need to add any authentication details to the configuration of the software I use to access PPSR.

When a new user is added to my PPSR software they are automatically sent an invitation by email to register as a member of my PPSR organisation account. The software does this with an API call when the user is created.

After a user has been created in my software and has registered on the PPSR website as a user of my PPSR organisation account, the PPSR software asks them to log in to PPSR as a one-off process. This gets the details needed to make PPSR API transactions on that users behalf.

When a staff member leaves my business their login to my PPSR software is disabled.

Software has end users without their own PPSR logins

I'm a business that has multiple end users of the software I use to connect to the PPSR, but they do not have their own logins to the PPSR system. My software uses subscription key authentication to connect to the PPSR APIs.

Applies to

- Users of COTS products that connect to the PPSR, e.g. small-medium finance companies, motor vehicle traders etc., where staff have shared logins to the product.
- Direct API consumers that have developed their own products to connect to the PPSR, where the software operates in batch processes, is used by staff with shared logins, or is used by staff without needing a login.
- Commercial intermediaries that process PPSR transactions for customers and on-charge fees to them.

PPSR organisation account management

I have at least two staff in my business that have registered on the PPSR website and are administrators of my PPSR organisation account.

If one of the administrators leaves my business, another is available to delete them from my PPSR organisation account and add their replacement as a new PPSR user. When they are deleted from my PPSR organisation any API token associated with them are revoked.

Software and API set up

Before I can start using my PPSR software I need to add an OAuth token to the software's configuration so that it can authenticate PPSR API calls.

To get the OAuth token one of the users in my PPSR organisation account must go through the registration and PPSR subscription process³ at portal.api.business.govt.nz.

If the user that set up the PPSR API subscription leaves my business I need another staff member in my PPSR organisation account to go through the same registration and subscription process, then add the new subscription key to my software configuration.

³ Appendix A – Subscription key process

Software provider with product that accesses PPSR

I am a software provider about to build a product that will use the PPSR system via the PPSR API.

Applies to

- Providers of COTS products whose customers need to use the PPSR.
- In-house development teams of businesses that use the PPSR, e.g. banks, large finance companies, commercial intermediaries.
- Software providers that have been contracted by a business to produce custom software for PPSR access.

Software and API set up

Whether or not I choose to use a subscription key or three-legged integration, someone in my business must subscribe to the PPSR API so I can proceed with development.

Any products I build that provide three-legged OAuth integration will use my API subscription details (consumer ID and consumer secret) when generating end users' OAuth tokens, as my customers will grant consent for my software product to transact with the PPSR system on their behalf.

Any products I build that provide subscription key integration will require my customers to subscribe to the PPSR API and add their subscription key details to the product configuration. In this situation my subscription details are only needed for development in the PPSR API sandbox environment, and I do not use them for any purpose in production.

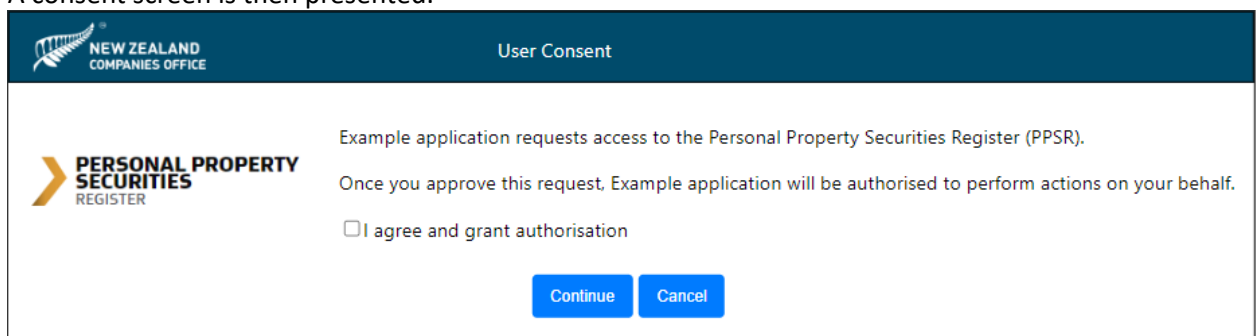
Appendix A: Token Provisioning

Three-Legged token process

Providing user consent

When a new staff member is set up in their organisation's PPSR software product they must go through a one-off process to link their software login with their PPSR RealMe login using these steps⁴:

1. User logs in to their software product (could be cloud-based or an installed product)
2. The software asks the user if it can transact in the PPSR system on their behalf
3. If the user agrees then the software takes them to a RealMe login page
4. The user logs in with the RealMe login that they use in the PPSR system
5. A consent screen is then presented:



6. User approves consent
7. Upon approval the software product receives a code that is used to generate three-legged bearer and refresh tokens that are associated with the PPSR user
8. Software stores the bearer and refresh tokens against the user's profile. (Bearer token has a one-hour life, refresh tokens are 14 days)

Calling the PPSR API

When a user of the software conducts a PPSR transaction, e.g. a search or registering a financing statement, the software uses the user's refresh token to generate a new bearer and refresh token.

The new tokens are stored against the user's profile in the software product. The new bearer token has one hour expiry and the new refresh token has 14 day expiry.

The software then calls the PPSR API with the bearer token as authorisation for the PPSR user.

The PPSR system processes the transaction and is aware of who the PPSR organisation account and PPSR user are.

⁴ See <https://support.api.business.govt.nz/s/article/cloud-authentication-oauth-3-legged> for more detail

Two-legged token process

To set up PPSR software for two-legged token access a member of the PPSR organisation account needs to follow the separate process of subscribing to the PPSR API as documented at

<https://support.api.business.govt.nz/s/article/cloud-subscriptions>

Setting up a new user

When the organisation first gets the PPSR software product they must go through a process to create a subscription key and add that into their software's configuration.

1. One of the organisation's PPSR users must register at portal.api.business.govt.nz, using the same RealMe login that they use in PPSR
2. The user subscribes to the PPSR API by browsing to the API product page and clicking the subscribe button
3. The subscription request must be approved by MBIE
4. The user generates a non-expiring subscription key, and optionally a client ID and client secret to be used for short-life OAuth token creation
5. The user copies the API credentials into their software's configuration.

Calling the PPSR API

When any user of the software conducts a PPSR transaction, e.g. a search or registering a financing statement, the software uses the non-expiring subscription key, and optionally a short-life OAuth token, as authentication in the call.

The PPSR system processes the transaction and is aware of who the PPSR organisation account and the PPSR user associated with the API subscription are. All transactions from the organisation are identified as coming from the same PPSR user.

Subscribed user leaves organisation

If the subscriber to the PPSR API is removed from the PPSR organisation then the access credentials used in their software configuration will become invalid and the organisation will be unable to connect to the PPSR.

To prevent this happening, another PPSR user in the organisation will need to subscribe to the PPSR API, wait for approval, then generate and add their API credentials token into the software configuration.