Australian Government
Services Australia

Provider Digital Access

(PRODA)

B2B High Level Introduction

Version 1.4 27/02/2020

servicesaustralia.gov.au

Contents

Table of Figures

REMOVE THIS PAGE BEFORE PUBLISHING (also regenerate index!!)

Change Log

Version	Author	Description
1.5	Anton Chertok	

1 Introduction

1.1 Purpose

This document describes at a high level the interactions between software providers and Services Australia for B2G (aka B2B) unattended web service access. This document provides a high level overview of the interactions that are required by the 3rd Party Vendor software and should provide enough information to assist the vendors in determining the impact on their software. PRODA's design is intended to facilitate any organisation's software authenticating via PRODA to any system via web services. There is one restriction, that both entities are appropriately registered with PRODA. Detailed interface specifications will be provided in separate documentation.

The following diagram illustrates at a high level the major entities of the 3rd Party Vendor software and Services Australia solution, and provides the necessary concepts to understand the PRODA authentication pattern. Implementation of the provider's ICT network and management of the PRODA credentials is the responsibility of the provider and the 3rd Party Vendor software. Possible variations of the implementation are described later in this document, however sections 1.2 through to 5 provide the readers with the PRODA concepts which are required irrespective of the implementation strategy.

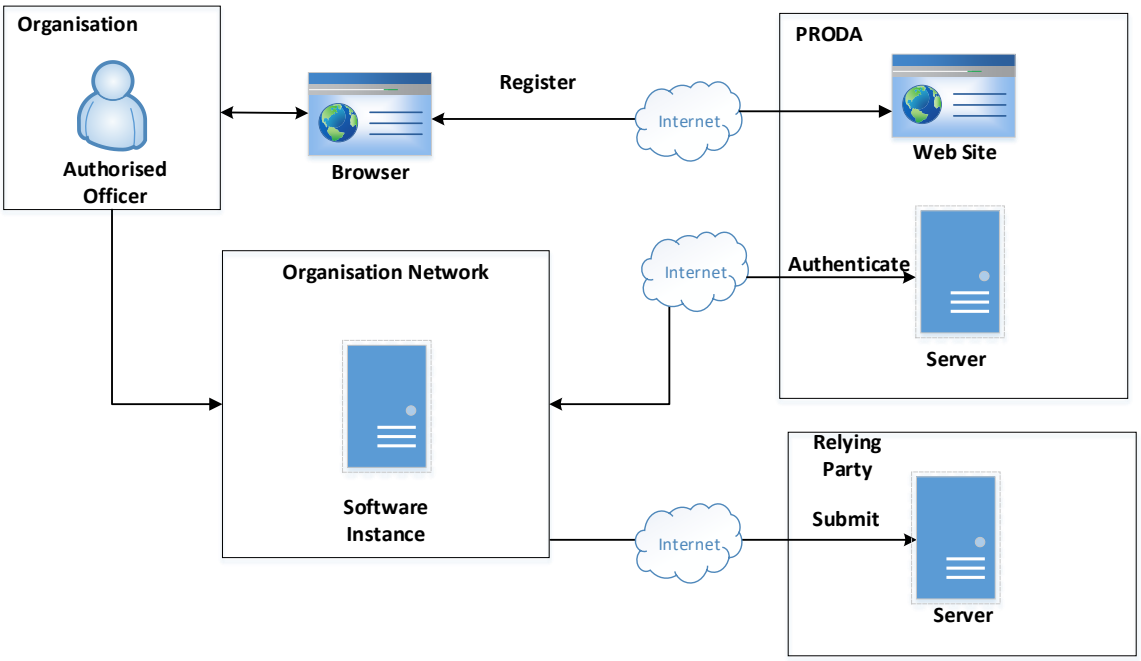

Figure 1: High Level Components

The PRODA B2B Unattended pattern provides an authentication framework for organisations to submit authenticated unattended web service transactions to Services Australia. This framework supports a self-service approach and provides the organisations with the ability to register and utilise the authentication mechanisms defined by PRODA and the OAuth2/JSON standards.

1.2 Glossary

The following acronyms and terms are in this document:

Acronym/Term	Description
API	Application Programming Interface
Authorised Officer	A person who has successfully registered, and is associated with an organisation within PRODA, through a director/associated role with the Australian Business Register (ABR).
B2B	Business to Business
OTSC	One Time Security Code
Device	A device is term to describe a physical server, a virtual server or even a desk top. It is being used interchangeably with software instance as the software resides on the device.
Device Name	The name of device used during software registration. It uniquely identifies a device associated with an organisation.
JSON	JavaScript Object Notation is a language-independent data format that contains human-readable data objects consisting of attribute-value pairs and array data types.
JWK	JSON Web Key
JWS	JSON Web Signature
JWT	JSON Web Token
TTL	Time To Live. A term to describe a time value in which an action needs to be completed by.
OAuth 2.0	The OAuth Open standard grants websites or applications access to their information without giving them passwords, therefore enabling a third-party application to obtain access to authorised services.
PRODA	Provider Digital Access application
REST	Representational state transfer (or REST) web services allows requesting systems to access and manipulate textual representations through stateless operations.
Relying Party	This is an entity that provides services, utilising PRODA to authenticate and authorise users.
RSA	A security (or authentication) token.
Software Instance	After the vendors software has been installed on a device, a term to collectively describe the combination.
Software Vendor	A Third party entity that owns the software used to communicate to Services Australia
Vendor Software	Software developed by a third-party to transact with the Agency and Relying Parties

2 Overview

PRODA B2B uses the JSON Web Keys and the OAuth2 standards to authenticate a provider that is using an approved 3rd Party Vendor software. Authentication of the provider's software is accomplished by the provider's instance of the 3rd Party Vendor software (i.e. a SI) digitally signing a JSON Web Token with their JSON private key and PRODA verifying this token with the private key's corresponding public key. This private / public key pair also allows PRODA to identify the provider and through the signature handshake be assured that the request is from the provider.

The process involves three major steps for the software instance:

1) Setup and Registration.
2) Activation.
3) Authentication.

An additional security feature that has been implemented is the requirement for the software instance to refresh the key pair at regular intervals. The interval time frame will be provided later. This refresh step ensures that a compromised software instance is identified as early as possible and steps can be taken to prevent any further web service submissions.

3 PRODA set up

Before providers and their software vendor can submit web service requests to Services Australia, the provider (or an authorised officer) must register with PRODA. Once registered, PRODA and Services Australia need to know about the provider's software that they wish to use to submit Services Australia web service requests. This software in PRODA is called a software instance (SI) and this software instance links the installed 3rd Party Vendor software to the provider. The link is accomplished via the use of a One Time Security Code (OTSC). This OTSC is generated by the PRODA web site for an authorised officer who is logged onto PRODA and who then registers their software instance.

The following diagram illustrates the relationships between the provider, the SI, and PRODA.

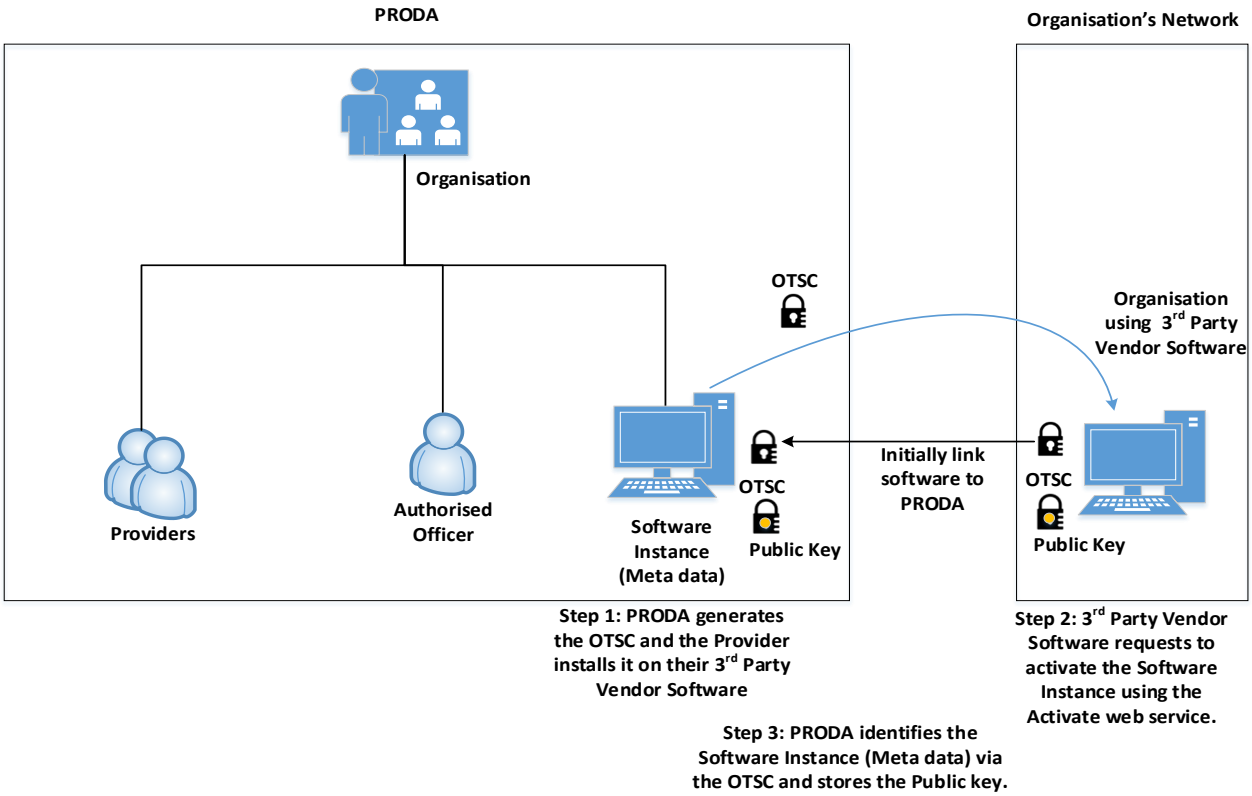

Figure 2: PRODA Setup

4 Software Instance activation

Once the software instance has been registered in PRODA it must then be activated. Activation involves the 3rd Party Vendors software generating a JSON Web Key private and public key pair and then using the OTSC generated at registration time and the public key submitting a PRODA activation web service request. This activation process provides PRODA with the public key to use for authentication requests for that provider's SI.

The following diagram illustrates the activation process that a provider and a 3rd Party Vendor software must perform. This process need only occur when a software instance is registered or re-registered in PRODA after becoming invalid or locked. The setup process described earlier is also illustrated below to provide a full end to end description of the process.

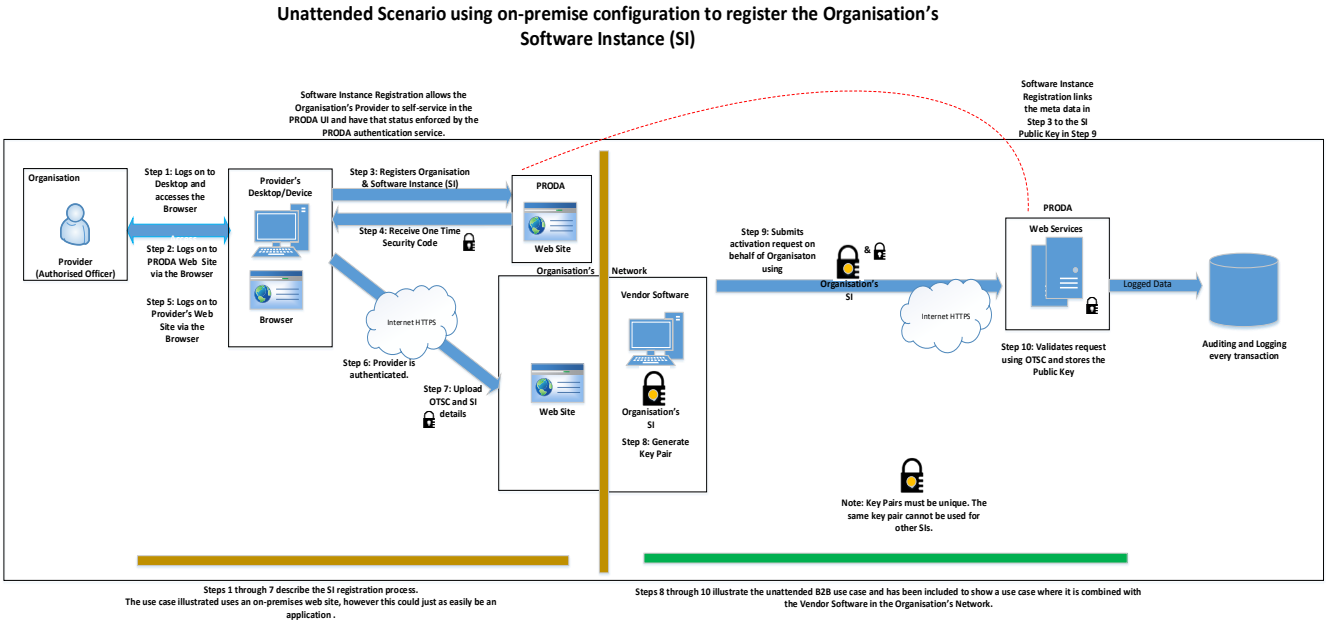

Figure 3: PRODA Activation

5 Software Instance authentication

Once the software instance has been registered and activated in PRODA it is now ready to authenticate to PRODA and use that authentication to submit web services to Services Australia. Authentication involves the 3rd Party Vendors software generating a digital signature using the appropriate private key and attaching that signature to an authentication web service request to PRODA. PRODA will verify this signature and if successful return an OAuth2 JSON Web Token in the form of an Access Token. This Access Token can then be used as authorisation to Services Australia web services.

The following diagram illustrates the authentication process that the provider and the 3rd Party Vendor software must perform. This process need only occur when a software instance is about to submit web service requests to Services Australia. The Access Token will be valid for a short period of time (e.g. 10 minutes) in which it can submit multiple web service requests until it expires at which time the SI can request a new Access Token. The Access Token validity period will be provided at a later date.

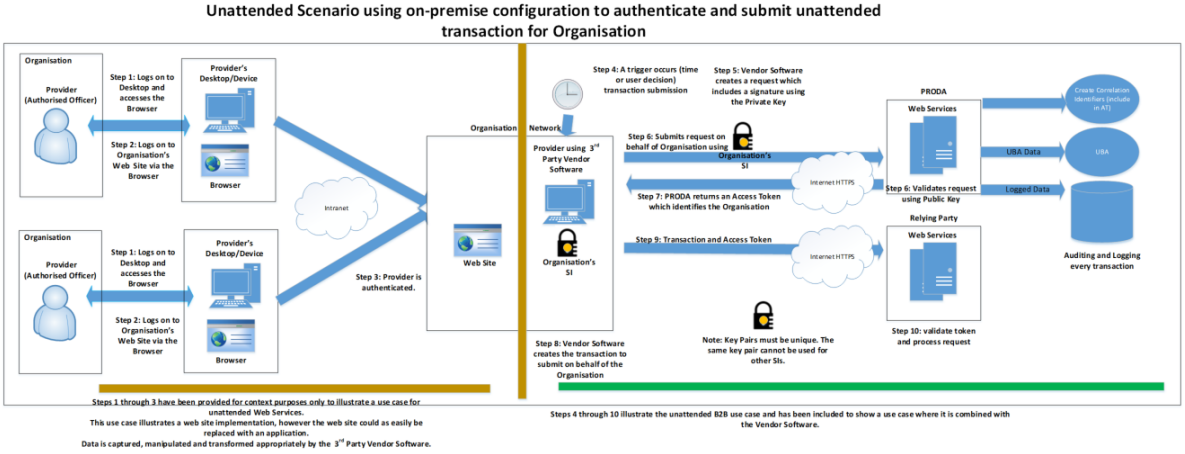

Figure 4: PRODA Authentication

The use of a web site by the provider to enter data to populate the 3rd Party Vendor software is only used as an example. How the data is entered into the 3rd Party Vendor software is a matter for the provider and the 3rd Party Vendor software to design and implement.

6 Services Australia to external entities

This section describes the high level processes required for external entities (e.g. a Health Fund) to receive authenticated web service transactions from Services Australia. This process follows the standard PRODA B2B pattern described earlier in the document. For this use case the roles in the PRODA B2B process have been reversed with DHS becoming the source of the transaction. It must be noted that whilst the roles have been reversed for this process, this process only describes the authentication pattern. Any business logic relating specifically to the use case is not effected by the PRODA pattern. Step 1 described below depicts only those elements that are relevant to this document. The process will involve further on-boarding with PRODA business.

In this use case Services Australia will act as an organisation and will be required to follow the standard PRODA processes for organisations (e.g. Register the SI, Activate the SI etc) as described earlier in this document. External entities (e.g. Health Funds) will act as relying parties of PRODA just like Services Australia does when receiving web service transactions from organisations.

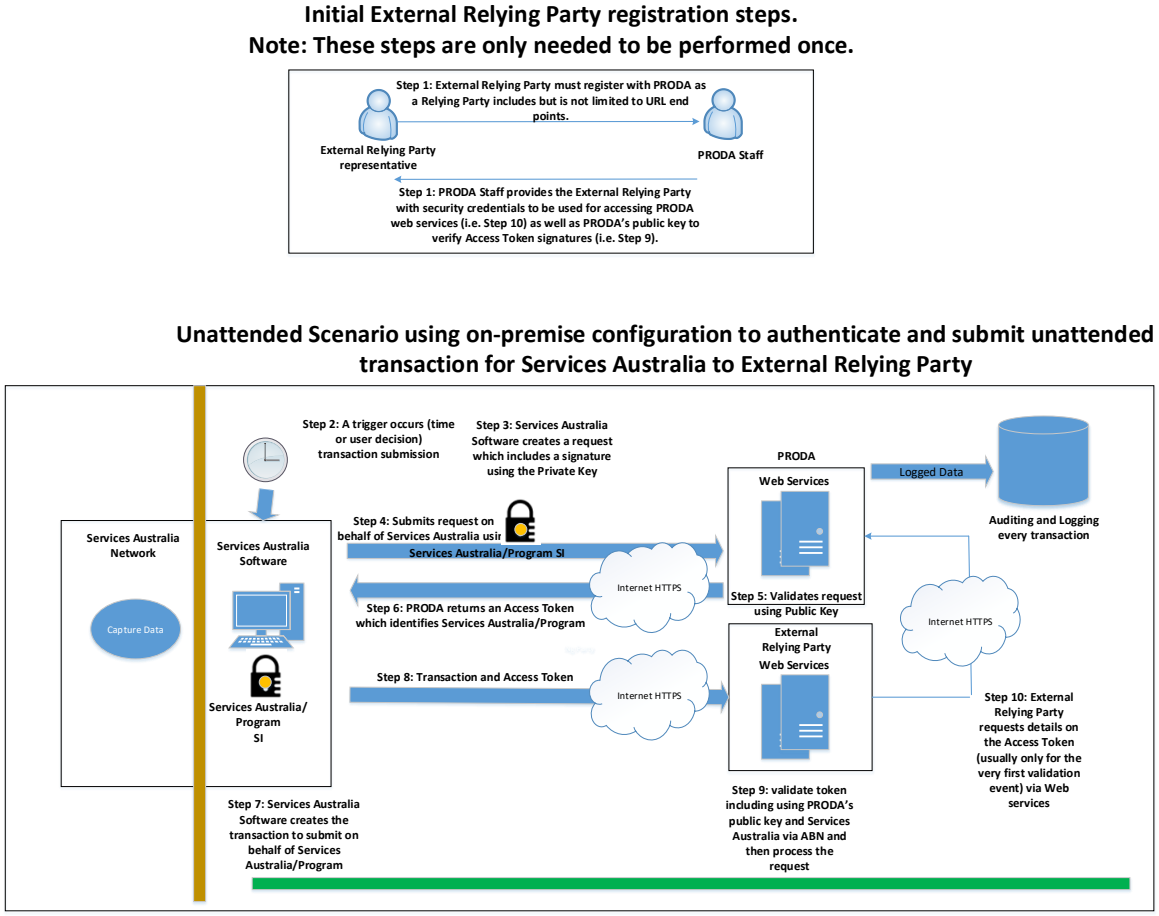

Figure 5: Services Australia to Health Fund Example

7 Alternative implementations

The following sections describe possible alternative implementations of the 3rd Party Vendor software. These alternatives are suggestions only and do not in any way dictate how the 3rd Party Vendor software is implemented.

7.1 On-Premise

The baseline implementation described earlier focuses on a single software instance and the associated registered PRODA credentials. This focus describes the implementation of a single software instance on a single device. This device could be a physical server, a virtual server or even a desk top. For providers that have the ICT capability that utilises many servers, the use of a single software instance implemented on every device may be impracticable. This section describes three possible alternatives to the single software instance on every device scenario and of course a combination of any of the three may also be possible. A very important point to remember is that a software instance and associated key pair securely represents an organisation and the key pair must be treated like any other credential, securely.

7.1.1 Multiple SI's accessing a single data source

The following diagram illustrates multiple SI's accessing a single data source whether that is a secure database, or a secure file system to service the SI's. Note: These SI's would be the same software performing the same functions, managed separately for scalability, performance etc. The management of the SI's is not described in this document.

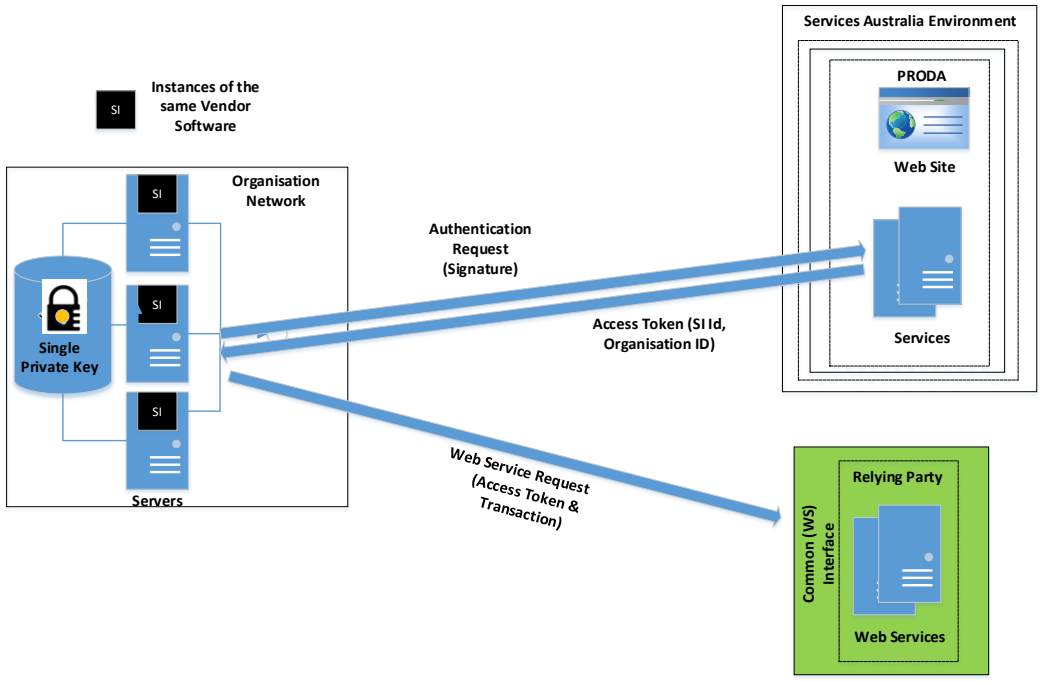

Figure 6: SI Single Data Source Example

7.1.2 Multiple SI's accessing a single proxy

The following diagram illustrates multiple SI's accessing a single proxy which manages and controls the SI's credentials. The term proxy does not represent a technical proxy, but a logical proxy which could be implemented by any software that can serve this purpose. Note: These SI's would be the same software performing the same functions, managed separately for scalability, performance etc. The management of the SI's is not described in this document.

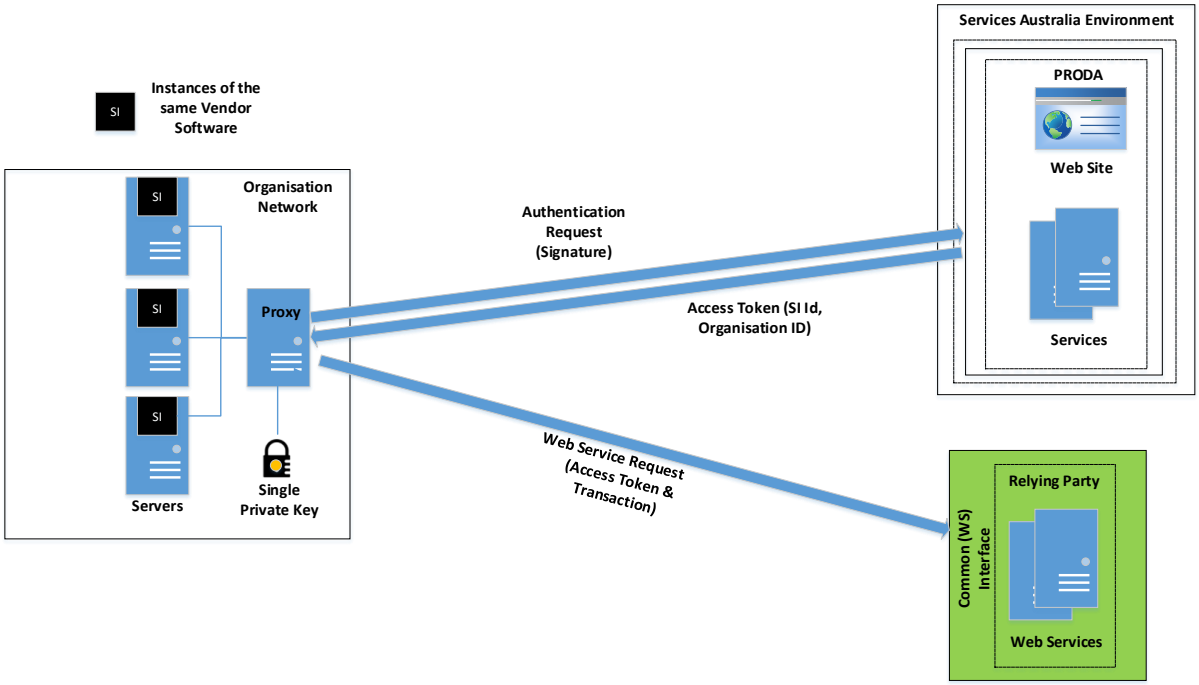

Figure 7: SI Proxy Example

7.1.3 SI's accessing a multiple users via Web browser

The following diagram illustrates an SI which captures data from multiple users via a Web Browser.

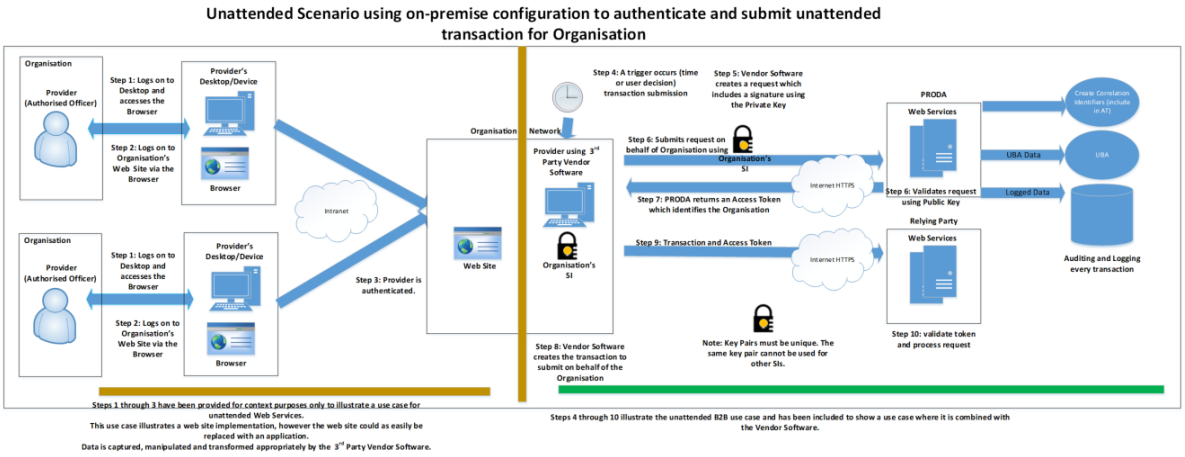

Figure 8: Web Based Example