

SSO User workflow

Overview

Description: This workflow describes how the IL will provide a mechanism to allow single-sign-on (SSO) to be enables for the user of the management application for the HIE registries (Note: This does not include user from the PoS applications, these application will be responsible for managing their users locally).

Sponsor: [Ryan Crichton](#), with the IL community

Status: proposed

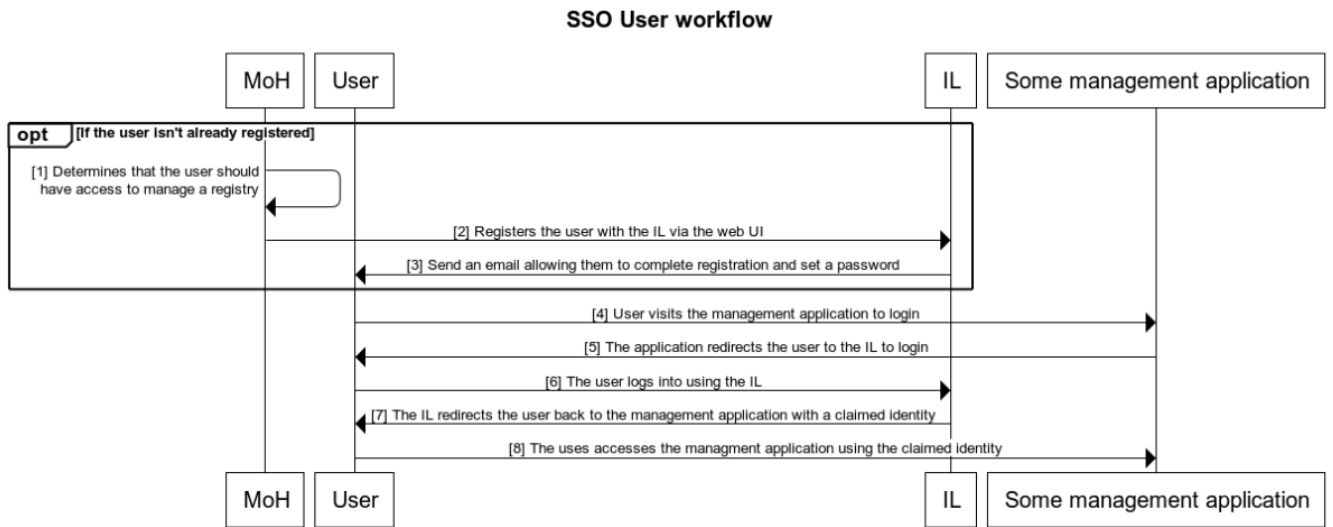
Last Modified: 19/02/2014

Referenced Standards and APIs:

- [OpenID](#)

Actors

- MoH - This actor represents the authority that controls access to the HIE. This is likely a Ministry of Health or a Department of Health.
- User - a user of the management application in question
- Some management application - an application that manages one of the registries that make up the HIE
- IL - the interoperability layer that provides the SSO service



www.websequencediagrams.com

Open Questions

- Do the management applications control their own user authorisation lists or should this be something that the IL does?

Technical details

Ref	Interaction	Endpoint	Data	Transaction Specification
1	Determines that the user should have access to manage a registry		policy	
2	Registers the user with the IL via the web UI		The users details (email, name, department, job title)	Via the Web UI
3	Send an email allowing them to complete registration and set a password		A registration link	email

4	User visits the management application to login			OpenID authentication request
5	The application redirects the user to the IL to login			OpenID authentication request
6	The user logs into using the IL			OpenID authentication response
7	The IL redirects the user back to the management application with a claimed identity			OpenID authentication response
8	The user accesses the management application using the claimed identity			OpenID verifying assertions