Transport for London

Single Sign-on

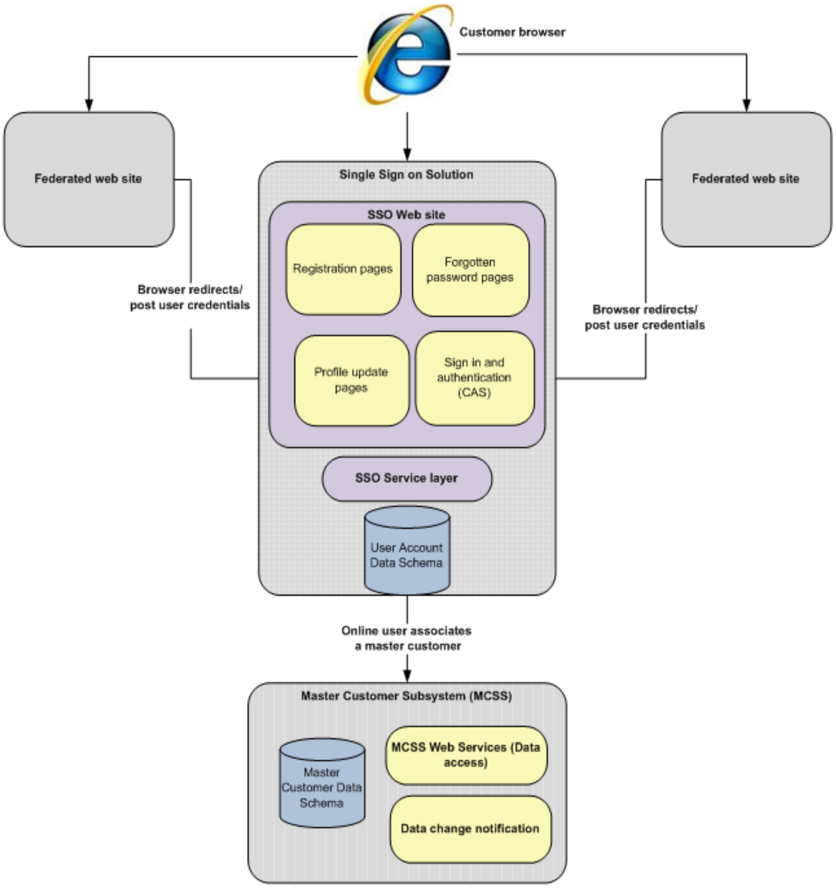
Single Sign-on (SSO) enables us to centralize the end to end management of online user accounts and provide transparent and integrated sign-in across our federated web sites. This document outlines the requirements for single sign-on where there is a need for user authentication.

Audience

- Solution Architects
- Technical Architects
- Developers
- Project Managers

Outline

The following diagram summarises our SSO solution at a conceptual level.


Customer browser
Federated web site
Federated web site
Single Sign on Solution
SSO Web site
Registration pages
Forgotten password pages
Profile update pages
Sign in and authentication (CAS)
Browser redirects/ post user credentials
Browser redirects/ post user credentials
SSO Service layer
User Account Data Schema
Online user associates a master customer
Master Customer Subsystem (MCSS)
Master Customer Data Schema
MCSS Web Services (Data access)
Data change notification

Single sign-on benefits

We have adopted SSO to enable a number of benefits:

- We can enforce uniform authentication and/or authorisation policies across the enterprise
- We can implement end to end user audit sessions to improve security reporting and auditing
- Removes the need for application developers to understand and implement identity security in their applications
- Inactivity time-out and attempt thresholds are applied uniformly closer to user points of entry
- It improves the effectiveness/timeliness of disabling all network/computer accounts for terminated users
- It reduces the administrative overhead in resetting forgotten passwords over multiple platforms and applications
- It provides users with the convenience of having to remember only a single set of credentials. This also improves security as users find it easier to remember their credentials and do not have to write them down, allowing for a more efficient user log on process
- It reduces the time taken by users to log into multiple applications and platform

Requirements

When integrating services with our SSO solution, you must comply with the following;

Responsibilities of our SSO solution

- Our SSO solution is responsible for user Authentication
- Our SSO solution is responsible for validating a user's login credentials (username and password)
- Our SSO solution provides services to allow a user to manage and update SSO credentials (change password)
- Our SSO service is responsible for redirecting the user back to the originating application once a user is successfully logged in via the SSO service

- Our SSO service provides a service for global log out

Responsibilities for integrating services

- Integrating services **must** implement their own Authorisation
- Each integrating service **must** maintain and secure user data that is specific to their own applications and **must** validate users are authorised to perform actions upon that data or view that data
- Each integrating service **must** define which pages within that application require the user to be identified (logged in) and **must** hand the end user off to the SSO service to log in when required
- Each integrating service **must** keep the "SSO session" alive so as to retain a logged in session for as long as possible
- Each integrating service **must** provide a call-back for SSO to use to co-ordinate a global log-out. This call back should clear any "sessions" that are local to that service

Why we do this

We have a SSO solution to enable us to centralize the end to end management of online user accounts and provide transparent/integrated sign-in across our federated web sites.

Further reading

- Site integration standard

Glossary

Authentication - Authentication is any process by which you verify that someone is who they claim they are.

Authorisation - Authorisation is any process by which someone is allowed to be where they want to go, or to have information that they want to have.

User Account Data Schema - Database for the storage of the SSO account, connected system configuration and the tracking of certain events relating to online usage (e.g. Forgot password, account locked, signed in etc). Each user account has an optional association to a master customer record.

Type:	Guidelines
Owner:	TfL Online Compliance
Department:	TfL Online

Version History

Version	Date	Summary of changes
1.0	14/01/2014	First issue

Review History

Name	Title	Date	Comments