



**INFORMATICS
INSTITUTE OF
TECHNOLOGY**

INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

**Secret Vault – A secure secret storage mechanism for web
browsers**

An interim progress report by

Mr. Anthony Jerad Dilip Mahesh Rutnam

Supervised by

Mr. Saman Hettiarachchi

Submitted in partial fulfilment of the requirements for the MSc in Advanced Software
Engineering degree at the University of Westminster.

August 2022

Abstract

Single-Page Applications (SPA) has been popular among these day on web application development because of it's nature of high performance and better user experience. And almost all the companies are transforming their existing traditional web applications to SPAs. Said that, this also comes with some security challenges to the developers. As when it becomes a pure public client that runs on the client browser without server-side support. These apps should have a secure mechanism to keep sensitive data like Access Tokens that will be obtain through an OpenID Connect (OIDC) authorization, which will be used for secure API calls. However, existing HTML5 browser storages are not secure enough for this purpose.

This research proposes a native secure vault supporting for web browsers, and a Proof of Concept (PoC) will be implemented as a browser extension. Which can be embedded natively in the browsers in the future. This will allow applications to make a connection to an Identity Provider and obtain an Access Token through OIDC authorization code flow. And store it securely and use it when a secure API invocation is required to the Identity Provider.

And the concept solution proves that the stored access token in the browser extension in-memory is not accessible through application main thread. And the during the evaluation it has found out that this addresses the research problem and this can be further improve by generalising and support it natively from the browsers.

Keywords – Single-Page Application, OpenID Connect, Access Token, Secure Vault, Web Browser Storage, Authorization Code.