imc
part of Scheer

SSO OIDC

Service Description

imc Learning Suite

October 08, 2024

Preface

A service description provides clarity and communication by clearly defining what the service is, its scope, and boundaries, ensuring a common understanding among all stakeholders. It specifies the service levels and quality metrics, setting expectations for performance and reliability. Additionally, it details the dependencies and interactions with other services, outlining necessary integrations. The roles and responsibilities of both the service provider and the customer are clearly defined, ensuring accountability.

Context

imc Learning Suite supports several protocols to be used to enable a login to the LMS via Single Sign-on (SSO). This Service Description covers the process of enabling SSO via the OpenID Connect protocol (OIDC). OpenID Connect (OIDC) is an authentication protocol built on top of OAuth 2.0, allowing clients to verify a user's identity based on the authentication performed by an authorization server. It provides an ID token alongside access tokens, enabling secure and straightforward Single Sign-On (SSO) across multiple applications. OIDC is widely used for its simplicity, security, and ability to integrate with various identity providers.

The following chapters describe the necessary steps to get SSO via OIDC up and running. On the imc side, the process is managed by a Business Consultant, who is supported by a Technical Consultant, if necessary. On the customer side, a contact person from the specialist department should be involved who manages and is responsible for the LMS. A technical contact is also required who has access to the identity provider to be used and has the ability to perform the necessary configuration on the identity provider side.

Description of the Service

Prerequisites and planning phase

Implementing an SSO can have in impact on the system behaviour as an additional method for how users can log in to the system is provided. Together with the Business Consultant, the customer clarifies:

- Is the SSO the only method **how users can log in** to the system or should it be possible to log in via username and password in parallel, e.g. for separate admin accounts?
- In case the customer uses a **multi-client system**, should the SSO be available for all clients or only for specific clients?
- Should the system have a **public space** where the SSO login process will have to be triggered explicitly by the user, or should the login process be initiated immediately as soon as the system is accessed?
- Which **claim** can be used to identify a user and to which personal attribute in ILS this claim can be mapped

If no identifying claim can be determined that is available on both the IdP and ILS side, the options are:

a) Extend the claims supported by the IdP with an attribute which can be used to identify a user, and which is already present in the ILS user master data. This can be done by the customer alone.

b) Extend the user master data in ILS with an attribute to hold the identifying claim, e.g. by extending the CSV or SCIM user import accordingly. This requires changes to the user import interface which need to be aligned on both the customer side and in the LMS.

In addition, imc requires some **technical parameters** which the customer must provide for the OIDC configuration. On the Identity Provider (IdP) side, the customer must create a client or application. The following information to this client / application must be provided to imc:

- The client ID / application ID
- The client secret / application secret
- URL to the Discovery endpoint of the client / application

Also, the customer must configure an allowed **Redirect URI** and **Post Logout Redirect URI** for the client / application in the Identity Provider. These URIs follow the following schemes:

Redirect URI: https://lms.customer.com**/idm/oidc/login**
Post Logout Redirect URI: https://lms.customer.com**/idm/logoff**

lms.customer.com must be replaced with the actual hostname of the customer's ILS installation.

To make the technical implementation and testing as efficient as possible, it is highly recommended that the customer provides imc with a **test account** in the Identity Provider. By using a test account, imc can test the SSO implementation end-to-end independently from the customer. Issues and misconfigurations can so be identified and resolved early in the process.

Technical implementation and testing

When the technical and functional topics are clarified and all prerequisites are met, an imc Consultant will perform the system configuration. This includes:

- Configuration of the OIDC interface in the ILS configuration manager based on the information given by the customer (Discovery URL, client ID, client secret)
- Configuration of the ILS clients (enabling OIDC as log in method, optionally disabling any other enabled log in methods)
- (optional) Configuration of the ILS navigation to enable automatic SSO triggering
- (optional) Extension of the user import (CSV or SCIM) to ensure the availability of an identifying attribute

After the configuration is done, the new setup is tested end-to-end. If the customer provided a test account, the imc Consultant will perform an end-to-end test considering all the requirements discussed before.

If any issues are identified during testing, the issues will be analysed together with imc Technical Services. If imc is not able to solve the issues on their own, the issues must be discussed and solved together with the technical contact of the customer.

When all issues are resolved, the customer is informed that the setup is completed. It is highly recommended for the customer to end-to-end test all the scenarios with various user accounts and roles. After the customer completed the testing phase successfully, the project is completed.

END OF DOCUMENT