imc
part of Scheer

SSO OIDC

Service-Beschreibung

imc Learning Suite

08. Oktober 2024

im-c.com

Vorwort

Eine Servicebeschreibung sorgt für Klarheit und Kommunikation, indem sie eindeutig definiert, worum es sich bei dem Service handelt, welchen Umfang er hat und wo seine Grenzen liegen, so dass ein gemeinsames Verständnis aller Beteiligten gewährleistet ist. Sie spezifiziert die Service-Levels und Qualitätsmetriken und legt die Erwartungen an Leistung und Zuverlässigkeit fest. Außerdem werden die Abhängigkeiten und Interaktionen mit anderen Diensten detailliert beschrieben und die notwendigen Integrationen aufgezeigt. Die Rollen und Zuständigkeiten sowohl des Dienstanbieters als auch des Kunden werden klar definiert, um die Verantwortlichkeit sicherzustellen.

Kontext

imc Learning Suite unterstützt verschiedene Protokolle, um eine Anmeldung am LMS über Single Sign-on (SSO) zu ermöglichen. Diese Servicebeschreibung behandelt den Prozess der Aktivierung von SSO über das OpenID Connect Protokoll (OIDC). OpenID Connect (OIDC) ist ein Authentifizierungsprotokoll, das auf OAuth 2.0 aufbaut und es Clients ermöglicht, die Identität eines Benutzers auf der Grundlage der von einem Autorisierungsserver durchgeführten Authentifizierung zu überprüfen. Es stellt ein ID-Token zusammen mit Zugriffstokens zur Verfügung und ermöglicht so ein sicheres und unkompliziertes Single Sign-On (SSO) über mehrere Anwendungen hinweg. OIDC wird wegen seiner Einfachheit, Sicherheit und der Fähigkeit zur Integration mit verschiedenen Identitätsanbietern weit verbreitet.

In den folgenden Kapiteln werden die notwendigen Schritte beschrieben, um SSO über OIDC einzurichten. Auf der imc-Seite wird der Prozess von einem Business Consultant geleitet, der bei Bedarf von einem Technical Consultant unterstützt wird. Auf Kundenseite sollte ein Ansprechpartner aus der Fachabteilung eingebunden werden, der das LMS managt und verantwortet. Außerdem ist ein technischer Ansprechpartner erforderlich, der Zugriff auf den zu verwendenden Identity-Provider hat und in der Lage ist, die erforderliche Konfiguration auf der Seite des Identity-Providers durchzuführen.

Beschreibung des Service

Voraussetzungen und Planungsphase

Die Implementierung eines SSO kann sich auf das Systemverhalten auswirken, da eine zusätzliche Methode bereitgestellt wird, wie sich Benutzer beim System anmelden können. Gemeinsam mit dem Business Consultant klärt der Kunde:

- Ist das SSO die einzige Methode, **wie sich Benutzer am System anmelden** können oder sollte es möglich sein, sich per Benutzername und Passwort parallel anzumelden, z.B. für separate Admin-Accounts?
- Falls der Kunde ein System mit **mehreren Mandanten** verwendet, soll das SSO für alle Mandanten oder nur für bestimmte Mandanten verfügbar sein?
- Soll das System über einen **öffentlichen Bereich** verfügen, in dem der SSO-Anmeldevorgang explizit vom Benutzer ausgelöst werden muss, oder soll der Anmeldevorgang sofort gestartet werden, sobald auf das System zugegriffen wird?
- Welcher **Claim** kann zur Identifizierung eines Benutzers verwendet werden und welchem Nutzerattribut in der ILS kann dieser Claim zugeordnet werden?

Wenn kein identifizierender Claim ermittelt werden kann, der sowohl auf der IdP- als auch auf der ILS-Seite verfügbar ist, stehen folgende Optionen zur Verfügung:

a) Erweiterung der vom IdP unterstützten Claims um ein Attribut, das zur Identifizierung eines Benutzers verwendet werden kann und das bereits in den ILS-Benutzerstammdaten vorhanden ist. Dies kann allein durch den Kunden erfolgen.

b) Erweiterung der Benutzerstammdaten im ILS um ein Attribut zur Aufnahme des identifizierenden Claims, z.B. durch eine entsprechende Erweiterung des CSV- oder SCIM-Benutzerimports. Dies erfordert Änderungen an der Nuzterimport-Schnittstelle, die sowohl auf Kundenseite als auch im LMS abgestimmt werden müssen.

Darüber hinaus benötigt imc einige **technische Parameter,** die der Kunde für die OIDC-Konfiguration angeben muss. Auf der Seite des Identitätsanbieters (IdP) muss der Kunde einen Client oder eine Anwendung erstellen. Folgende Informationen zu diesem Client / dieser Anwendung müssen imc zur Verfügung gestellt werden:

- Die Client ID / Anwendungs ID
- Das Client Secret / Anwendungs Secret
- URL zu dem Discovery Endpoint des Client / der Anwendung

Außerdem muss der Kunde einen zulässigen **Redirect URI** und einen **Post Logout Redirect URI** für den Client / die Anwendung im Identitätsanbieter konfigurieren. Diese URIs folgen den folgenden Schemata:

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

lms.customer.com muss durch den tatsächlichen Hostnamen der ILS-Installation des Kunden ersetzt werden.

Um die technische Umsetzung und das Testen so effizient wie möglich zu gestalten, wird dringend empfohlen, dass der Kunde imc einen **Testaccount** im Identity Provider zur Verfügung stellt. Durch die Verwendung eines Test-Accounts kann imc die SSO-Implementierung End-to-End unabhängig vom Kunden testen. Probleme und Fehlkonfigurationen können so frühzeitig im Prozess identifiziert und behoben werden.

Technische Umsetzung und Test

Wenn die technischen und fachlichen Themen geklärt sind und alle Voraussetzungen erfüllt sind, übernimmt ein imc Consultant die Systemkonfiguration. Dazu gehören:

- Konfiguration der OIDC-Schnittstelle im ILS-Konfigurationsmanager basierend auf den vom Kunden angegebenen Informationen (Discovery-URL, Client-ID, Client Secret)
- Konfiguration der ILS-Mandanten (Aktivieren von OIDC als Anmeldemethode, optional Deaktivieren aller anderen aktivierten Anmeldemethoden)
- (optional) Konfiguration der ILS-Navigation, um die automatische SSO-Auslösung zu aktivieren
- (optional) Erweiterung des Benutzerimports (CSV oder SCIM), um die Verfügbarkeit eines identifizierenden Attributs sicherzustellen

Nachdem die Konfiguration abgeschlossen ist, wird das neue Setup durchgängig getestet. Wenn der Kunde einen Test-Account zur Verfügung gestellt hat, führt der imc Consultant einen End-to-End-Test unter Berücksichtigung aller zuvor besprochenen Anforderungen durch.

Sollten während des Tests Probleme festgestellt werden, werden diese gemeinsam mit dem Technischen Service von imc analysiert. Wenn imc nicht in der Lage ist, die Probleme selbst zu lösen, müssen die Probleme gemeinsam mit dem technischen Ansprechpartner des Kunden besprochen und gelöst werden.

Wenn alle Probleme behoben sind, wird der Kunde darüber informiert, dass die Einrichtung abgeschlossen ist. Es wird dem Kunden dringend empfohlen, alle Szenarien mit verschiedenen Benutzerkonten und Rollen durchgängig zu testen. Nachdem der Kunde die Testphase erfolgreich abgeschlossen hat, ist das Projekt abgeschlossen.

ENDE DES DOKUMENTS