# Vorlage - Anbindung OIDC Applikation

## Einführung

Beim Anbinden einer OpenID Connect Applikation an das IAM System müssen diverse Daten erhoben und diverse Prozesse bestimmt werden. Dieses Dokument soll als Leitfaden dienen und sämtliche zu erhebenden Daten für alle beteiligten zu dokumentieren.

## Anzubindende Applikation

Die folgende Tabelle gibt Auskunft über die IST-Situation vor der Anbindung an das IAM System:

| **Parameter** | **Wert** |
|---|---|
| Name der Applikation | |
| Version / Release | |
| Hersteller | |
| Applikationsverantwortlicher | |
| Umgebungen | PROD / INT / DEV |
| Hostname / IP-Adresse | |
| Benutzerverwaltung<br><br>Wo führt die Applikation heute ihren Benutzer stamm, innerhalb der Applikation, in einem externen System, im Active Directory oder bezieht es die Benutzer bereits heute aus einem IAM System? | IAM / AD / eigene Benutzerverwaltung / andere |
| Benutzermapping<br><br>Wie können wir bestehende Benutzer mappen? Haben wir ein eindeutiges Merkmal das wir verwenden können um die bestehenden Benutzer zu identifizieren? | |
| 2FA / MFA vorhanden<br><br>Hat das System heute einen zweiten Faktor? | |
| Benutzertypen<br><br>Unterscheidet das System zwischen unterschiedlichen Benutzertypen? | Intern / Extern / Bürger / Kunden / etc. |
| Anzahl Benutzer | |
| Föderation mit anderen IDPs | |
| Berechtigungsmodell<br><br>Führt die Applikation ein internes Berechtigungsmodell? Falls ja, wie sieht dieses aus? | |

# Prozesse

## On-Boarding / Registration

**Wie registrieren sich Benutzer heute an der Applikation und benötigen wir ggf. einen Registrationsprozess?**

TBD

**Welche Daten werden erhoben über die Personen?**

TBD

**Wie sieht der neue On-Boarding Prozess über das IAM-System aus?**

TBD

**Führt die Applikation Organisationen / Unternehmen?**

TBD

## Off-Boarding

**Können Benutzer heute ihren Account selbständig Löschen?**

TBD

**Wie sieht der neue Off-Boarding Prozess über das IAM-System aus (falls vorhanden)?**

TBD

## Mutationen

**Können Benutzer ihre eigenen Daten heute mutieren?**

TBD

**Sollen Benutzer ihre Daten im IAM-System mutieren können? Wenn ja, welche?**

TBD

## Benutzer Migration

**Müssen existierende Benutzer Daten von der Applikation ins IAM System migriert werden?**

TBD

## Berechtigungsvergabe

**Wie sieht der heutige Prozess zur Berechtigungsvergabe aus?**

TBD

**Wie soll der neue Prozess zur Berechtigungsvergabe aussehen?**

TBD

# Identity Provider

Folgende allgemeinen Daten werden für die OpenID Connect Konfiguration benötigt. Zusätzlich werden clientspezifische Daten benötigt die im nächsten Kapitel beschrieben sind.

| Parameter | Wert |
| --- | --- |
| Well Known Configuration<br><br>Beinhaltet in aller Regel sämtliche benötigten Daten. | https://idp.coreone.ch/.well-known/openid-configuration |
| JWKS URI | https://idp.coreone.ch/.well-known/openid-configuration/jwks |
| Authorization Endpoint | https://idp.coreone.ch/connect/authorize |
| Token Endpoint | https://idp.coreone.ch/connect/token |
| User Info Endpoint | https://idp.coreone.ch/connect/userinfo |

# Applikations- und Clientkonfiguration

## Verbindungsdaten

Folgende clientspezifischen Daten werden benötigt um die Applikation zu konfigurieren.

| Parameter | Wert |
| --- | --- |
| Application Name<br><br>Wird in aller Regel nur IAM intern benötigt | Application Name |
| Client ID | client_name |
| Client Secret | ******** |
| Flow<br><br>Wo immer möglich soll der Authorization Code Flow with PKCE verwendet werden. | Authorization Code Flow with PKCE |

## Sicherheitsdaten

| Parameter | Wert |
| --- | --- |
| Redirect URI<br><br>An welche URI darf das IAM den Benutzer nach der Anmeldung weiterleiten? Regex Pattern oder fixe URI Liste. | https://meine.applikation.ch/sign-in |
| Post Logout Redirect URIs<br><br>An welche URI darf das IAM den Benutzer nach der Abmeldung weiterleiten? Regex Pattern oder fixe URI Liste. | https://meine.applikation.ch/logout |

## Claims

Welche Benutzerinformationen / Claims müssen an die Applikation ausgeliefert werden?

### Standard Claims

| Claim | Beispiel | Ursprung |
|---|---|---|
| sub<br>OpenID Connect Standard claim, wird immer ausgeliefert. | idp:12345 | Wird automatisch generiert |
| email<br>OpenID Connect Standard claim, wird immer ausgeliefert. | max@muster.ch | Wird bei der Registration erhoben. |
| family_name | Muster | Wird bei der Registration erhoben. |
| given_name | Max | Wird bei der Registration erhoben. |
| display_name | Max Muster | Mapping aus Vor- und Nachname. |

### Spezifische Claims

| Claim | Scope Zuweisung | Beispiel | Ursprung |
|---|---|---|---|
| ? | ? | ? | ? |

## Sicherheitsaspekte

### Signatur Check

Die vom Identity Provider ausgestellten Tokens werden signiert. Es muss sichergestellt werden dass die Applikation, bzw. die eingesetzte Library oder das eingesetzte Modul diese Signatur über das über die JWKS URI publizierte öffentliche Zertifikat validiert.

- [ ] Bestätigt durch Applikationsverantwortlicher

### Single Page Applikation

Ist die Applikation als Single Page Applikation implementiert gilt es ein paar Sicherheitsaspekte zu diskutieren / dokumentieren.

#### Token im Frontend

Single Page Applikationen haben in der Regeln keine Backend Componenten sondern greifen direkt auf Web-APIs zu. Der Zugriff auf diese Web-APIs benötigt Authorisierung weshalb hier oft direkt der Access Token im Request mitgesendet wird. Das bedeuted aber auch, dass der Token somit im Browser gespeichert ist. Dies birgt Risiken, da er dort ungeschützt ist. Es empfiehlt sich daher den Einsatz eines BFFs oder einer anderen geeigneten Massnahme.

- [ ] Bestätigung durch den Applikationsverwantwortlicher dass **keine** Token im Frontend gehalten werden

**Public client**

Eine Single Page Applikation wird im Browser ausgeführt. Für die OIDC Prozesse bedeutet dass, dass Client Id und Client Secret im Browser liegen würden und somit Public sind.

- [ ] Bestätigung das der client als public und somit **ohne** client secret konfiguriert wurde