

# Formulaire OpenID Connect - Démarrage

## OBJECTIFS DU DOCUMENT

Support d'échange entre Cocoom et son client, qui regroupe des informations techniques nécessaires à la mise en place d'une liaison OpenID Connect.

## PREAMBULE

Afin de faciliter l'accès à la plateforme Cocoom aux utilisateurs finaux Cocoom recommande, lorsque cela est possible, d'interconnecter la plateforme déployée avec la fédération d'identité du client.

Cette interconnexion permet de mettre en place un mécanisme SSO (Single Sign-On) qui offre plusieurs avantages:

- **Pour l'utilisateur final, plus de fluidité** : son identifiant et son mot de passe habituel lui servent d'identifiant de connexion pour Cocoom. Par ailleurs, s'il est déjà connecté à une application web de l'entreprise, alors il est également déjà identifié par Cocoom et aucun mot de passe ne lui sera demandé.
- **Pour la direction informatique du client, plus de sécurité** : les identifiants et mots de passe des utilisateurs ne sont jamais échangés avec Cocoom. Si une faille de sécurité devait survenir sur l'infrastructure Cocoom, elle n'aurait aucune répercussion chez le client.

L'interconnexion entre la fédération d'identité du client et la plateforme Cocoom est réalisée au moyen de la couche OpenID Connect 1.0 du protocole OAuth 2.0.

Ce document centralise, dans les tableaux de la page suivante, les informations techniques que les deux parties doivent partager pour que cette liaison OpenID Connect puisse être mise en oeuvre.

Ce document doit être complété par le client et transmis par e-mail aux équipes techniques Cocoom à l'adresse [support@cocom.com](mailto:support@cocom.com).

Informations Générales		
Partenaire		Nom du client ou du projet
Contact partenaire		E-mail du contact technique chez le client
Nom technique du partenaire		Sous-domaine <code>cocom.com</code> du client
Technologie du partenaire		Nom ou fournisseur de la fédération d'identité du client
Calendrier du projet	Recette SSO: __/__/__ Lancement POC: __/__/__ Lancement Cocoom: __/__/__	Dates cibles pour les différents jalons

Données relative à la Relying Party (RP) Cocoom		
Mode d'autorisation	<code>Authorization code flow</code>	Type de flow OpenID Connect
Champs d'identification de l'utilisateur final	<code>sub</code>	Champs de l'ID Token contenant l'identifiant unique de l'utilisateur
scope	<code>openid, profile, email</code>	
Domaine à autoriser	<code>cocom.com</code>	Domaine qui doit être autorisé sur la fédération d'identité du client
Redirect URI	Exemple: <code>https://&lt;YOUR_DOMAIN&gt;.cocom.com/oidc</code>	URL de redirection à référencer dans la fédération d'identité du client

**Commenté [1]:**  
 (à remplir par le client ou par Cocoom)  
 exemple:  
`https://<YOUR_DOMAIN>.cocom.com/oidc`

Données relative à l'OpenID Provider (OP) du client		
Client ID		Identifiant de l'application Cocoom dans l'OP
Client Secret		Clé secrète pour l'application Cocoom
Discovery document location		L'URI du document regroupant les informations de configuration de l'OP
Compte test		Une adresse e-mail d'un utilisateur final, destiné à tester la liaison OpenID Connect

**Commenté [2]:**  
 (à remplir par le client)

**Commenté [3]:**  
 (à remplir par le client)

**Commenté [5]:**  
 Pour Azure AD:  
`https://login.microsoftonline.com/<YOUR_TENANT>/well-known/openid-configuration`

**Commenté [4]:**  
 (à remplir par le client)

**Commenté [6]:**  
 (à remplir par le client)