

# Laboratoire 3

## Configuration de l'authentification unique de Google pour une application Web dans Microsoft Azure

Université du Québec en Outaouais  
Titre du cours : CYB1123 - Sécurité de l'infonuagique et des services Web

Date de remise : Avant lundi 4 Novembre 2024, 23 :59

Nom et Prénom : Sankara Kabem Abdoul Charif

Code permanent : Sank90300007

# I Introduction

Ce laboratoire vise à mettre en pratique les compétences acquises dans le cours de sécurité en infonuagique en explorant l'intégration de l'authentification unique via Google Identity Platform dans une application Web. En configurant un fournisseur d'identité externe dans notre cas avec Google, Nous pourrions expérimenter l'utilisation des API d'authentification de Google et constater les avantages de la délégation de l'authentification à un tiers sécurisé et éprouvé. Les tâches incluent la création et la configuration de l'API, la mise en place de Google comme fournisseur d'identité dans l'application, et la validation de la fonctionnalité d'authentification unique, avec des captures d'écran à l'appui pour illustrer chaque étape.

## 1) Listons au moins 3 avantages d'utiliser un fournisseur d'identité externe

Voici trois avantages d'utiliser un fournisseur d'identité externe, tel que Google Identity Platform, pour la gestion de l'authentification d'une application Web :

1. **Sécurité renforcée** : Les fournisseurs d'identité comme Google utilisent des normes de sécurité avancées, telles que l'authentification multifactorielle (MFA) et la détection des activités suspectes, pour protéger les informations d'identification des utilisateurs. Ils offrent également des mises à jour de sécurité régulières, réduisant les risques d'intrusion ou de vol de données.
2. **Simplicité d'utilisation pour les utilisateurs** : Les utilisateurs peuvent se connecter en utilisant leurs identifiants Google existants, ce qui simplifie l'expérience de connexion. Cela réduit également le besoin pour les utilisateurs de créer un compte spécifique, diminuant ainsi les risques de perte de mot de passe ou de compte inactif.
3. **Économie de temps et de coûts pour les développeurs** : Intégrer un fournisseur d'identité externe permet de déléguer la gestion des processus d'authentification (création de comptes, gestion de mots de passe, etc.). Cela réduit le besoin de développement et de maintenance d'un système d'authentification personnalisé, permettant aux développeurs de se concentrer sur d'autres aspects de l'application.

## 2) Exemple d'application Web où un fournisseur d'identité externe est contre-indiqué

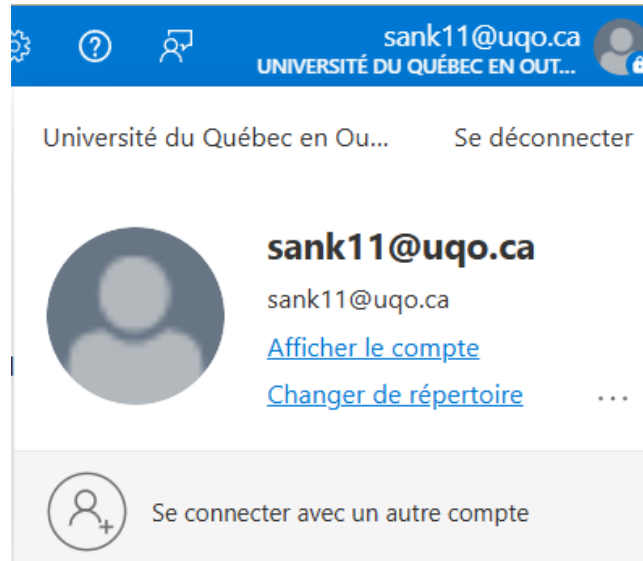
La gestion des informations de santé d'un hôpital ou d'une clinique.

### Explication :

Dans le domaine de la santé, les données sont extrêmement sensibles et sont soumises à des réglementations strictes de protection de la vie privée. L'utilisation d'un fournisseur d'identité externe, tel que Google Identity Platform, pourrait poser des problèmes de conformité, car il impliquerait de partager certaines informations avec une tierce partie. En outre, les hôpitaux préfèrent souvent utiliser des systèmes d'authentification internes pour garder un contrôle total sur la gestion des accès et assurer une sécurité maximale. Ils peuvent ainsi garantir que toutes les données d'authentification et d'accès restent dans leur propre infrastructure, sans dépendre d'un service externe qui pourrait être vulnérable à des violations de données ou des politiques de confidentialité différentes.

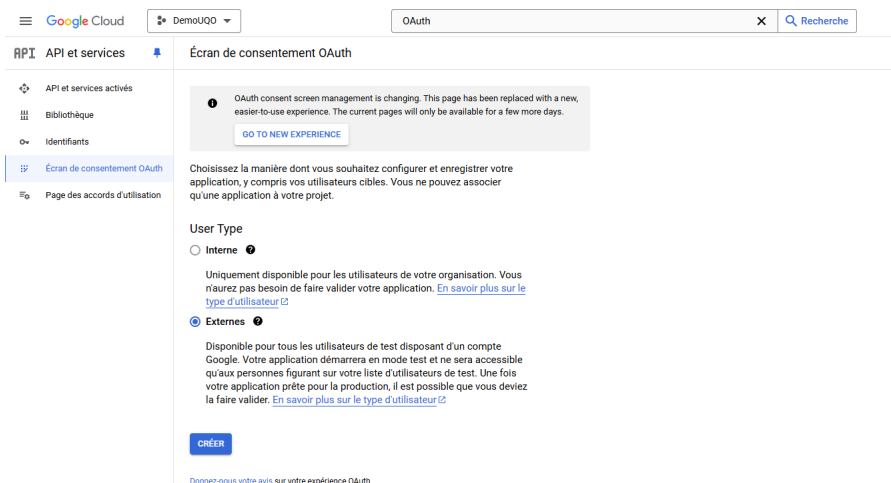
### 3) Captures d'écran requises et explications sur les différentes étapes du laboratoire

Les captures d'écran suivantes expliquent les grand point pour la configurations des API et dans l'autorisation dans Azure :



#### a) L'information sur votre application (App information, Partie 1 – Étape 7)

Après avoir créé un compte Google (si ce n'est pas déjà fait), nous accédons à la console développeur de Google. Nous y créons un nouveau projet, puis spécifions que nous souhaitons configurer un utilisateur de type externe. Ensuite, nous définissons le nom de l'application ainsi que l'adresse courriel qui permettra d'y accéder.



Google Cloud | DemouQO | OAuth

RPI API et services | Modifier l'enregistrement de l'application

API et services activés

Bibliothèque

Identifiants

Écran de consentement OAuth

Page des accords d'utilisation

### Informations sur l'application

Ces informations apparaissent dans l'écran de consentement, et permettent aux utilisateurs finaux de vous identifier et de vous contacter.

Nom de l'application \*

DemouQO

Adresse e-mail d'assistance utilisateur \*

sankara.hiem@gmail.com

Permet aux utilisateurs de vous contacter s'ils ont des questions concernant leur consentement. [En savoir plus](#)

### Logo de l'application

Ceci est votre logo. Il permet aux utilisateurs de reconnaître votre application et figure sur l'écran de consentement OAuth. Après avoir importé un logo, vous devrez faire valider votre application, sauf si celle-ci est configurée uniquement pour une utilisation interne ou si son état de publication est "Test". [En savoir plus](#)

Aperçu du logo de l'application

Fichier de logo à importer

peFvB8g\_400x400.jpg

PARCOURIR

Pour aider les utilisateurs à reconnaître votre application, importez une image ne dépassant pas 1 Mo et affichée sur l'écran de consentement. Les formats d'image autorisés sont JPG, PNG et BMP. Pour des résultats optimaux, les logos doivent être au format carré et d'une dimension de 120 px par 120 px.

### Domaine de l'application

Pour garantir votre protection et celle de vos utilisateurs, Google limite l'utilisation de domaines autorisés aux applications qui utilisent OAuth. Les informations suivantes seront présentées à vos utilisateurs dans l'écran de consentement.

Page d'accueil de l'application

Fournissez un lien vers votre page d'accueil aux utilisateurs

Lien vers les règles de confidentialité de l'application

Fournissez un lien vers vos règles de confidentialité publiques aux utilisateurs

Lien vers les conditions d'utilisation de l'application

Fournissez un lien vers vos conditions d'utilisation publiques aux utilisateurs

### Domaines autorisés

Lorsqu'un domaine est utilisé sur l'écran de consentement OAuth, il doit être pré-enregistré ici. Si votre application doit être validée, accédez à [Google Search Console](#) pour valifier si vos domaines sont autorisés. [En savoir plus](#)

Apprendre

### Comment ces informations sont-elles présentées aux utilisateurs ?

Voici l'écran de consentement que voient les utilisateurs

1. Logo et nom de votre application

Un logo est recommandé, mais pas obligatoire

2. L'adresse e-mail que les utilisateurs peuvent utiliser pour vous contacter, ainsi qu'une liste des champs d'application

Les champs d'application correspondent aux demandes spécifiques de votre application concernant l'accès au compte Google d'un utilisateur et aux données qui seront partagées.

Vous allez ajouter des champs d'application à l'étape suivante.

3. Liens vers les règles de confidentialité et les conditions d'utilisation de votre application

Cette section comprend également les éléments suivants :

- Une phrase qui décrit comment un

## b) Votre domaine applicatif (App domain, dernière capture d'écran de la Partie 1 – Étape 8)

Après avoir saisi les informations liées à notre application, nous passons à la configuration des informations de domaine. Dans notre cas, l'application a été déployée sur Azure, donc nous avons ajouté le lien du domaine autorisé.

Google Cloud | DemouQO | OAuth

RPI API et services | Modifier l'enregistrement de l'application

API et services activés

Bibliothèque

Identifiants

Écran de consentement OAuth

Page des accords d'utilisation

### Informations sur l'application

sur l'écran de consentement OAuth. Après avoir importé un logo, vous devrez faire valider votre application, sauf si celle-ci est configurée uniquement pour une utilisation interne ou si son état de publication est "Test". [En savoir plus](#)

uqo

Aperçu du logo de l'application

Fichier de logo à importer

peFvB8g\_400x400.jpg

PARCOURIR

Pour aider les utilisateurs à reconnaître votre application, importez une image ne dépassant pas 1 Mo et affichée sur l'écran de consentement. Les formats d'image autorisés sont JPG, PNG et BMP. Pour des résultats optimaux, les logos doivent être au format carré et d'une dimension de 120 px par 120 px.

### Domaine de l'application

Pour garantir votre protection et celle de vos utilisateurs, Google limite l'utilisation de domaines autorisés aux applications qui utilisent OAuth. Les informations suivantes seront présentées à vos utilisateurs dans l'écran de consentement.

Page d'accueil de l'application

<https://sankaraqo.azurewebsites.net>

Fournissez un lien vers votre page d'accueil aux utilisateurs

Lien vers les règles de confidentialité de l'application

Fournissez un lien vers vos règles de confidentialité publiques aux utilisateurs

Lien vers les conditions d'utilisation de l'application

Fournissez un lien vers vos conditions d'utilisation publiques aux utilisateurs

### Domaines autorisés

Lorsqu'un domaine est utilisé sur l'écran de consentement ou dans la configuration d'un client OAuth, il doit être pré-enregistré ici. Si votre application doit être validée, accédez à [Google Search Console](#) pour valifier si vos domaines sont autorisés. [En savoir plus](#)

Domaine autorisé \*

sankaraqo.azurewebsites.net

+ AJOUTER UN DOMAINE

### Coordonnées du développeur

Adresses e-mail \*

Ces adresses e-mail sont utilisées par Google pour vous informer de toute modification apportée à votre projet.

ENREGISTRER ET CONTINUER

ANNULER

Apprendre

### Comment ces informations sont-elles présentées aux utilisateurs ?

Voici l'écran de consentement que voient les utilisateurs

1. Logo et nom de votre application

Un logo est recommandé, mais pas obligatoire

2. L'adresse e-mail que les utilisateurs peuvent utiliser pour vous contacter, ainsi qu'une liste des champs d'application

Les champs d'application correspondent aux demandes spécifiques de votre application concernant l'accès au compte Google d'un utilisateur et aux données qui seront partagées.

Vous allez ajouter des champs d'application à l'étape suivante.

3. Liens vers les règles de confidentialité et les conditions d'utilisation de votre application

Cette section comprend également les éléments suivants :

- Une phrase qui décrit comment un

Google Cloud

Demo400

OAuth

RPI API et services

Modifier l'enregistrement de l'application

API et services activés

Identifiants

Écran de consentement OAuth

Page des accords d'utilisation

Écran de consentement OAuth

Niveaux d'accès

Utilisateurs tests

Résumé

OAuth consent screen management is changing. This page has been replaced with a new, easier-to-use experience. The current pages will only be available for a few more days.

GO TO NEW EXPERIENCE

Les champs d'application représentent les autorisations que vous demandez aux utilisateurs d'accorder à votre application. Ils permettent à votre projet d'accéder à certains types de données utilisateur privées à partir de leur compte Google. En savoir plus

AJOUTER OU SUPPRIMER DES CHAMPS D'APPLICATION

Vos niveaux d'accès non sensibles

API

Champs d'application

Description visible par l'utilisateur

Aucune ligne à afficher

Vos champs d'application sensibles

Les niveaux d'accès sensibles sont des niveaux d'accès demandant l'accès à des données utilisateur sensibles.

API

Champs d'application

Description visible par l'utilisateur

Aucune ligne à afficher

Vos champs d'application restreints

Les niveaux d'accès restreints sont des niveaux d'accès demandant l'accès à des données utilisateur très sensibles.

API

Champs d'application

Description visible par l'utilisateur

Aucune ligne à afficher

ENREGISTRER ET CONTINUER

ANNULER

Seuls les niveaux d'accès associés aux API activées sont répertoriés ci-dessous. Pour ajouter un niveau d'accès manquant à cet écran, localisez et activez l'API dans la Bibliothèque des API Google ou utilisez la zone de texte "Niveaux d'accès collés" ci-dessous. Actualisez la page pour afficher toutes les nouvelles API activées depuis la bibliothèque.

Filtrer

Saisissez le nom ou la valeur de la propriété

API	Champs d'application	Description visible par l'utilisateur
<input checked="" type="checkbox"/>	.../auth/userinfo.email	Afficher l'adresse e-mail principale associée à votre compte Google
<input checked="" type="checkbox"/>	.../auth/userinfo.profile	Consulter vos informations personnelles, y compris celles que vous avez choisies de rendre disponibles publiquement
<input type="checkbox"/>	openid	Créer une relation entre vous et vos informations personnelles sur Google
<input type="checkbox"/>	Analytics Hub API	View and manage your data in Google BigQuery and see the email address for your Google Account
<input type="checkbox"/>	Analytics Hub API	Vous, modifier, configurer et supprimer vos données Google Cloud, et voir l'adresse e-mail de votre compte Google
<input type="checkbox"/>	BigQuery API	Afficher vos données dans Google BigQuery
<input type="checkbox"/>	BigQuery API	Consulter vos données dans les services Google Cloud et voir l'adresse e-mail de votre compte Google
<input type="checkbox"/>	BigQuery API	Manage your data and permissions in Cloud Storage and see the email address for your Google Account
<input type="checkbox"/>	BigQuery API	Afficher vos données dans Google Cloud Storage
<input type="checkbox"/>	BigQuery API	Gérer vos données dans Cloud Storage et voir l'adresse e-mail de votre compte Google

Lignes par page: 10 1 - 10 sur 24

Ajouter manuellement des niveaux d'accès

Si les niveaux d'accès que vous souhaitez ajouter n'apparaissent pas dans le tableau ci-dessus, vous pouvez les saisir ici. Les niveaux d'accès doivent être saisis séparément sur plusieurs lignes ou séparés par des virgules. Veuillez indiquer la chaîne complète du niveau d'accès (en commençant par "https://"). Lorsque vous avez terminé, cliquez sur "Ajouter au tableau".

AJOUTER À LA TABLE

METTRE À JOUR

## c) L'adresse de retour (Partie 1 – Étape 16)

Pour créer notre adresse de retour, nous avons ajouté le suffixe `/.auth/login/google/callback` à l'adresse générée automatiquement sur Microsoft Azure. L'adresse de retour obtenue est donc : `'sankarauqo.azurewebsites.net/.auth/login/google/callback'`.

## URI de redirection autorisés

À utiliser avec les requêtes provenant d'un serveur Web

URI 1 \*

https://sankarauqo.azurewebsites.net/.auth/login/google/callback

+ AJOUTER UN URI

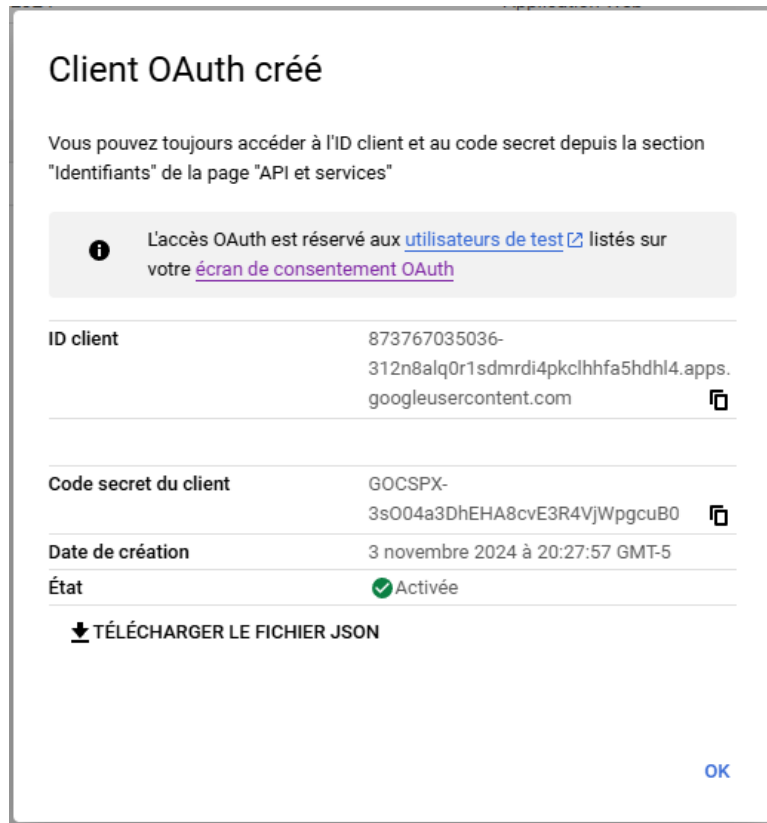
Remarque : L'application des paramètres peut prendre de cinq minutes à quelques heures

CRÉER

ANNULER

## d) Les valeurs du Client ID et du Client secret (Partie 1 – Étape 17)

- **Client ID** : 873767035036-312n8alq0r1sdmr4pkclhhfa5hdhl4.apps.googleusercontent.com
- **Client secret** : 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



## e) Configuration du fournisseur d'identités (Partie 2 – Étape 5)

Après avoir configuré notre application dans l'espace développeur de Google, nous accédons au portail de Microsoft Azure et allons dans notre section *App Services* pour démarrer notre application. Ensuite, nous ajoutons le fournisseur d'identité Google en sélectionnant *Identity Provider*. À ce stade, nous configurons l'application en entrant l'ID client généré ainsi que le code secret du client. Désormais, en tentant de se connecter à l'adresse de notre domaine, nous constatons qu'un accès au compte Google est requis en premier lieu.

The screenshot displays the Azure portal interface for configuring a Google Identity Provider. The left sidebar contains navigation links such as 'Créer une ressource', 'Accueil', 'Tableau de bord', and 'Tous les services'. The main content area is titled 'Ajouter un fournisseur d'identité' and includes the following sections:

- Informations de base**: Shows the 'Fournisseur d'identité' set to 'Google'.
- Inscription d'application**: Provides instructions on how to register an application and shows the 'ID client' and 'Secret client' fields.
- Paramètres d'authentification App Service**: Allows configuring authentication requirements, such as 'Demander une authentification' or 'Autoriser un accès non authentifié'.

Below the configuration page, a preview of the application is shown, displaying a welcome message in French: 'Bienvenue sur ma première application Web Azure'.

## II Conclusion

Ce laboratoire nous a permis de nous familiariser avec les concepts pratiques de sécurité infonuagique en mettant en œuvre une solution d'authentification unique basée sur un fournisseur d'identité externe. À travers la configuration de Google Identity Platform et son intégration dans l'application, la simplicité et la sécurité qu'apporte un fournisseur d'identité de grande envergure. Les connaissances acquises dans ce laboratoire soulignent l'importance de la sécurité dans les applications Web, tout en mettant en évidence les avantages, les limites et les particularités des solutions d'authentification infonuagique dans un environnement applicatif réel.