AYI NEDJIMI Consultants

OAuth2 vs OpenID Connect vs SAML :

3 mai 2026 • Mis à jour le 17 mai 2026 • 49 min de lecture • 9949 mots •

> La gestion des identités et des accès constitue l'un des défis architecturau
> Trois protocoles dominent le paysage de l'authentification et de l'autorisat
> d'autorisation déléguée publiée en 2012 (RFC.

La gestion des identités et des accès constitue l'un des défis architecturaux les pl
protocoles dominent le paysage de l'authentification et de l'autorisation en 2026 :
publiée en 2012 (RFC 6749) et depuis enrichie de nombreuses extensions (PKCE,
d'identité construite sur OAuth 2.0 qui standardise l'authentification via des token
Markup Language), vénérable standard XML publié en 2005 et omniprésent dans
Federation Services et les solutions SSO legacy. Ces trois protocoles répondent à
de sécurité distinctes, et leur confusion — extrêmement courante même parmi les
vulnérabilités critiques. Ce guide compare en profondeur leurs mécanismes, leurs
optimaux, et détaille l'implémentation sécurisée avec Keycloak, Azure AD/Entra ID
OpenID Connect pour les organisations cherchant à moderniser leur infrastructure

Réponse sous 24h

Devis gratuit →

À RETENIR

Résumé en une phrase : OAuth 2.0 = autorisation (déléguer l'accès à des ress
(vérifier l'identité) ; SAML 2.0 = SSO d'entreprise (fédération d'identité XML/a
interchangeables et répondent à des besoins complémentaires.

1. OAuth 2.0 : délégation d'autorisation

OAuth 2.0 résout un problème précis : comment permettre à une application tierce
appartenant à un utilisateur (le *resource owner*), sans que l'utilisateur ait à partage

Les quatre rôles OAuth 2.0 :

Resource Owner : l'utilisateur final qui possède les ressources

Client : l'application qui demande l'accès (web app, mobile app, API)

Authorization Server : le serveur qui émet les tokens (Keycloak, Azure AD, Okt

Resource Server : l'API qui héberge les ressources protégées

2. Le flux Authorization Code : analyse détaillée

Le flux *Authorization Code* est le flux OAuth 2.0 recommandé pour les applications
sécurisé car le token n'est jamais exposé au navigateur.

```
Flux Authorization Code (sans PKCE) :

1. L'utilisateur clique "Se connecter avec
```

n projet cybersécurité ?
Réponse sous 24h
Devis gratuit →

Réponse sous 24h

Devis gratuit →