OAuth 2.0 y OpenID Connect: autorización delegada y protección de APIs

W. J. Carrillo Sandoval
Carnet: 7690-21-3740
wcarrillos1@miumg.edu.gt

Resumen
OAuth 2.0 permite a clientes obtener acceso limitado a recursos sin compartir credenciales del usuario. OpenID Connect (OIDC) añade identidad sobre OAuth. Se explican roles, flujos recomendados (Authorization Code + PKCE, Client Credentials, Device Code), buenas prácticas (TLS, scopes mínimos, state/nonce, rotación de refresh tokens) y validación de JWTs (aud/iss/exp) para proteger APIs modernas.
Palabras clave: oauth 2.0, oidc, pkce, scopes, jwt, autorización

1. Roles y componentes

Authorization Server (emite tokens), **Resource Server** (protege APIs), **Cliente** (app), **Propietario del recurso** (usuario). OIDC introduce ID Token y endpoint *userinfo* para autenticación.

2. Flujos recomendados

- **Authorization Code + PKCE**: estándar para SPAs y móviles; mitiga robo de código.
- **Client Credentials**: servicio-a-servicio sin usuario final.
- **Device Code**: dispositivos sin navegador cómodo.

3. Tokens y validación

Acceso (TTL corto) y **actualización** (rotación y detección de reuso). JWTs firmados (JWS) para validación local o tokens de referencia con *introspection*. Validar `iss`, `aud`, `exp`, firma y *key rotation* (JWKS).

4. Buenas prácticas de seguridad

TLS **siempre**; *redirect URIs* exactas; *state*/*nonce* contra CSRF y *replay*; *scopes* mínimos; límites de tasa, *token binding* y políticas de revocación.

5. OAuth vs OIDC

OAuth trata **autorización**; OIDC añade **identidad**. Separar roles simplifica arquitectura y reduce errores de interpretación.

6. Observaciones y comentarios

El mayor riesgo es una configuración permisiva (scopes amplios, redirecciones comodín). Plantillas seguras y pruebas de *redirect* evitan incidentes.

7. Conclusiones

1. Authorization Code + PKCE es el flujo por defecto para clientes públicos.
2. Separar OIDC (identidad) de OAuth (autorización) reduce complejidad y fallos.
3. Rotación de tokens y validaciones estrictas fortalecen la postura de seguridad.

Bibliografía

1. Hardt, D. (2012). *RFC 6749: The OAuth 2.0 Authorization Framework*. IETF. https://www.rfc-editor.org/rfc/rfc6749
2. Jones, M., Hardt, D., et al. (2012). *RFC 6750: Bearer Token Usage*. IETF. https://www.rfc-editor.org/rfc/rfc6750
3. OpenID Foundation. *OpenID Connect Core*. https://openid.net/specs/openid-connect-core-1_0.html