



TIC

▶ TALENTO
TECH

REGIÓN 3

CAUCA - NARIÑO

LECCIÓN 2-UNIDAD 2



UTP
Universidad Tecnológica
de Pereira

faceIT

¿Qué es OpenID Connect?



OpenID Connect es un protocolo de autenticación interoperable basado en el marco de especificaciones de OAuth 2.0 (IETF RFC 6749 y 6750). Simplifica la verificación de la identidad de los usuarios utilizando la autenticación realizada por un servidor de autorización y permite obtener información del perfil del usuario de una manera interoperable y similar a REST.

Con OpenID Connect, los desarrolladores de aplicaciones y sitios web pueden implementar flujos de inicio de sesión y recibir datos verificables sobre los usuarios en clientes web, móviles y de JavaScript. Además, la suite de especificaciones es extensible, lo que permite incluir características opcionales como el cifrado de datos de identidad, descubrimiento de Proveedores de OpenID (OP) y cierre de sesión en las sesiones activas.

Para los desarrolladores, ofrece una solución segura y verificable para responder a la pregunta: **“¿Quién es la persona que está usando actualmente el navegador o la aplicación móvil conectada?”**. Lo mejor de todo es que elimina la necesidad de gestionar contraseñas, lo cual es un factor común en las brechas de seguridad basadas en credenciales.

¿Cómo funciona OpenID Connect?

OpenID Connect crea un ecosistema de identidad en Internet que se basa en integración sencilla, configuración segura que preserva la privacidad, interoperabilidad, amplio soporte para clientes y dispositivos, y la capacidad de que cualquier entidad actúe como Proveedor de OpenID (OP).

De manera abstracta, el flujo de OpenID Connect sigue estos pasos:

El usuario accede a un sitio web o aplicación web mediante un navegador.

Por ejemplo, una persona entra a una tienda online desde su computadora

El usuario hace clic en "Iniciar sesión" e ingresa su nombre de usuario y contraseña.

Podría usar su cuenta de Google o Facebook para autenticarse.

El cliente (RP) envía una solicitud al Proveedor de OpenID (OP).

El sitio web envía esta solicitud al servidor de Google o Facebook.

El OP autentica al usuario y obtiene autorización.

Google verifica las credenciales del usuario y su consentimiento para compartir información con la tienda online.

El OP responde con un Token de Identidad y, generalmente, un Token de Acceso.

La tienda online recibe estos tokens que confirman quién es el usuario.

El cliente puede usar el Token de Acceso para solicitar información adicional del usuario.

Por ejemplo, la tienda puede solicitar el nombre y correo electrónico del usuario.



Conceptos Clave de OpenID Connect

1. Autenticación:

Es el proceso seguro de confirmar que la persona que usa una aplicación o navegador es quien dice ser. Por ejemplo, cuando un usuario se autentica en un sitio utilizando su cuenta de Google, el servidor verifica su identidad.

2. Cliente:

Es el software que solicita tokens, ya sea para autenticar a un usuario o para acceder a recursos. Puede ser una aplicación web, una aplicación móvil o una aplicación de escritorio. Ejemplo: Una aplicación bancaria móvil que solicita tokens para confirmar la identidad de un usuario.

3. Parte Dependiente (Relying Party - RP):

Es la aplicación o sitio web que delega la autenticación de usuarios a un Proveedor de Identidad (IDP).

Ejemplo: Un sitio web que utiliza Facebook como proveedor para el inicio de sesión.



4. Proveedor de OpenID (OP) o Proveedor de Identidad (IDP):

Es la entidad que implementa los protocolos de OpenID Connect y OAuth 2.0. Puede actuar como servidor de autorización o servicio de tokens de seguridad.

Ejemplo: Google, Facebook o Microsoft.

5. Token de Identidad:

Representa el resultado del proceso de autenticación. Contiene un identificador único para el usuario (llamado sub o subject claim) e información sobre cómo y cuándo se autenticó. También puede incluir datos adicionales de identidad.

Ejemplo: Un token que confirma que el usuario autenticado es "usuario123" y que lo hizo a las 10:30 AM del 3 de diciembre de 2024.

6. Usuario:

Es la persona que utiliza un cliente registrado para acceder a recursos.

Ejemplo: Un cliente que usa su cuenta de Google para iniciar sesión en una tienda en línea.

Ejemplo

Imagina que estás usando una aplicación para hacer compras en línea:

- Haces clic en "Iniciar sesión con Google".
- La aplicación envía una solicitud al servidor de Google para autenticarte.
- Ingresas tu correo y contraseña de Google.
- Google verifica tus datos y te pregunta si deseas compartir información con la aplicación.
- Si aceptas, Google envía un Token de Identidad y un Token de Acceso a la aplicación.
- La aplicación usa esos tokens para acceder a tu nombre y correo electrónico.
- Finalmente, la aplicación muestra un saludo personalizado: "¡Bienvenido!"
- Así, la identidad de usuario fue autenticada y compartida de manera segura gracias a OpenID Connect.

