Dealing with Token Expiration, Reference Tokens and Token Revocation

Kevin Dockx
Architect

@KevinDockx https://www.kevindockx.com

Coming Up

Token lifetimes and expiration

Gaining long-lived access with refresh tokens

Reference tokens and token revocation

Validation procedures

Token Lifetimes and Expiration

Tokens have a limited lifetime

If a token has expired, validation will fail

Token Lifetimes and Expiration

Identity token

Very short lifetime (default: 5 minutes)

Used right after delivery

Applications often implement their own expiration policies

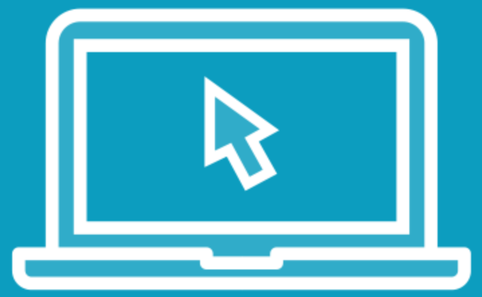
Access token

Longer lifetime (default: 1 hour)

Must be renewed to regain access to resources

The IDP controls the expiration policy

Demo



Token lifetimes and expiration

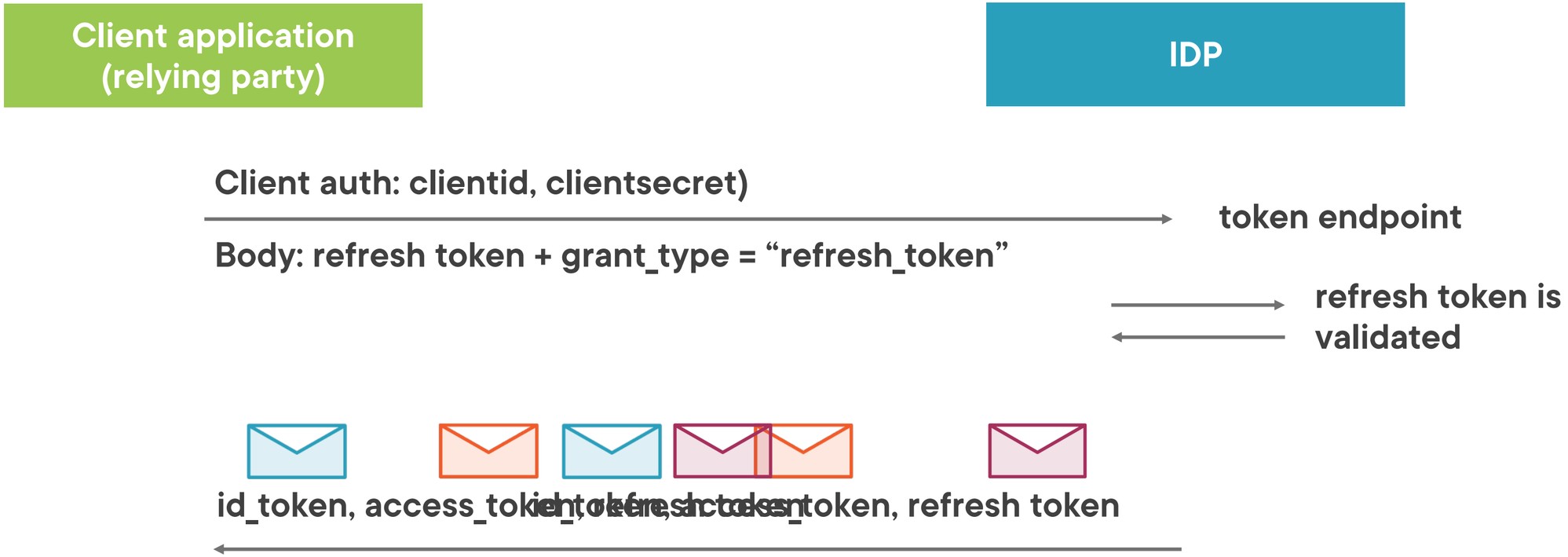
Gaining Long-Lived Access With Refresh Tokens

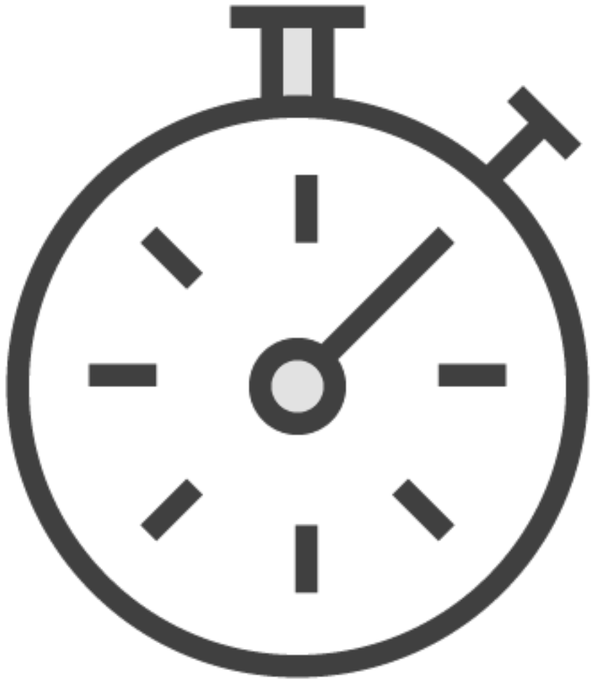
When a token expires, the flow can be triggered again to get a new one

Confidential clients can use refresh tokens to get new tokens via the back channel

- A refresh token is a credential to get new tokens

Refresh Token Flow

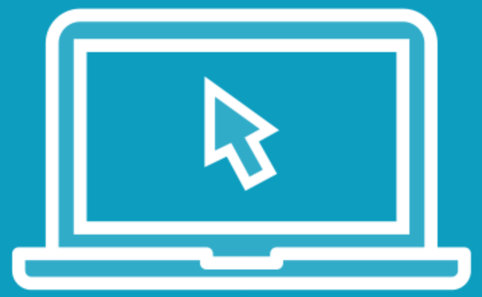




Scope: “offline_access”

- "Access to your applications and resources, even when you are offline“
- Offline in this context means the user is not logged in to the IDP

Demo



Gaining long-lived access

Working With Reference Tokens

Self-contained tokens (like JWT) can be validated without communicating with the IDP on each call

… but they don’t offer direct lifetime control

Reference token (aka opaque token)

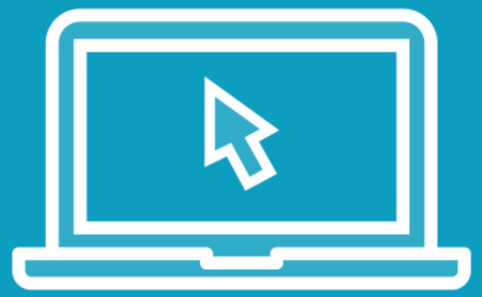
An identifier linked to a grant result / a set of permissions that would normally be in the JWT, stored at level of the IDP

Working With Reference Tokens

Token introspection endpoint

More direct lifetime control, but also more communication with the IDP

Demo



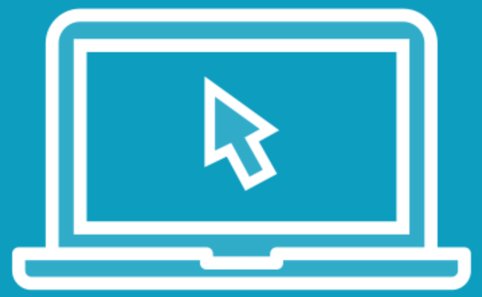
Working with reference tokens

Token Revocation

Tokens can be revoked through an administration tool

Clients can programmatically revoke tokens via the token revocation endpoint

Demo



Revoking tokens

Token Validation

Middleware takes care of validation

Validation procedures can differ between flows

Not every client or IDP uses the same validation procedures

Validation Procedures

Identity token (client level)

Access token (API level)

Identity Token Validation

Signature

Nonce

Issuer

Audience

Expiration

Access token hash is calculated from the access token

Must match at_hash in identity token: this links the access token to the identity token

“The methods used by the resource server to validate the access token are beyond the scope of this specification but generally involve an interaction or coordination between the resource server and the authorization server.”

OAuth2 specification

Access Token Validation

Signature

Issuer

Expiration

Audience

Summary

Tokens have a limited lifetime

Refresh tokens can be used to gain long-lived access for confidential clients

Summary

Reference tokens are identifiers linked to a token at level of the IDP

- Better control over lifetime
- More communication with the IDP

Tokens can be revoked by calling the token revocation endpoint

Up Next:

Storing Users and Credentials in a Local Database