OAuth 2.0 Best Practices

KU LEUVEN DistriNet

BEST PRACTICE

BEST PRACTICE

BEST PRACTICE

Use the Client Credentials grant for machine-to-machine authorization

BEST PRACTICE
BEST PRACTICE
BEST PRACTICE

Use the Authorization Code grant + PKCE when a user is involved

BEST PRACTICE
BEST PRACTICE
BEST PRACTICE

Do not use the Password grant

Do not use the Implicit grant

Use Cases – Grant Types

BEST PRACTICE
ANNO
2021

Web-server apps

authorization code + PKCE

Browser-based apps

~~implicit~~ authorization code + PKCE

Mobile apps

~~implicit~~ authorization code + PKCE

~~**Username/Password access**~~

~~password~~

Application access

client credentials

BEST PRACTICE

BEST PRACTICE

BEST PRACTICE

Always exactly match Redirect URIs with the registered values

BEST PRACTICE

BEST PRACTICE

BEST PRACTICE

Use the HTTP Authorization header to pass access tokens to an API

BEST PRACTICE

BEST PRACTICE

BEST PRACTICE

Use Mutual TLS to authenticate clients and to enable sender-constrained access tokens

BEST PRACTICE

BEST PRACTICE

BEST PRACTICE

Refresh tokens must either be sender-constrained or one-time use