# Public Clients

Theresa Henze - 2025-09-25 - Miscellaneous

# Public Clients – Usage and Security Considerations

A Bare.ID application can be created as a public OAuth2/OIDC client. Public clients are applications that cannot securely store credentials, such as browser-based applications (SPAs) or mobile apps. These clients do not use a client secret, since storing it in the frontend is insecure.

## When to Use Public Clients

- For **browser-based applications** (React, Angular, etc.)
- For **mobile apps** without a secure backend
- When **no backend** is available to protect a client secret

## Limitations of Public Clients

- Cannot prove their identity to the Keycloak server
- Vulnerable to token interception or manipulation if not configured properly
- Not suitable for highly sensitive operations without additional layers of security

## Security Considerations for Public Clients

To secure applications using public clients:

- **Use PKCE (Proof Key for Code Exchange)**
  - Mandatory for SPAs and mobile apps
  - Prevents authorization code interception
- **Set CORS and Redirect URIs Strictly**
  - Limit redirect URIs to known, trusted domains
  - Avoid wildcards
    - If you must use wildcards in any URLs for technical reasons, ensure that the domain and path prefixes are as strict as possible. Keep in mind that wildcards are omitted entirely from the OAuth 2.1 standard and should be avoided whenever possible.

- **Enable Content Security Policy (CSP)**
    - Helps prevent cross-site scripting (XSS) attacks in frontend apps
- **Access Token Lifespan**
    - Reduce token TTL to limit damage from token leakage
    - Use refresh tokens with care
- **Use Backend Services for Critical Operations**
    - Delegate sensitive logic to secure backend APIs
    - Public clients should not handle critical data or roles
- **Reduce Token Information**
    - Minimize the data contained in the token to reduce the risk in case of a potential token theft

**Note**: For more information about how to secure applications, see: https://datatracker.ietf.org/doc/html/rfc9700

## Configuring a Public Client

- Create the OAuth2/OIDC application as described in the Connect application page.
- Disable the "Confidential Client" switch in the "Settings" section.