2 令牌的配置（有效期 & 格式）

文章目录

令牌的配置

有效期

令牌格式

自包含（JWT）

引用（Opaque）

令牌的配置

在实际配置中，令牌的配置是以客户端的粒度区分的，也就是不同客户端可以指定不同的令牌有效期和令牌格式。

令牌的配置实际上就是客户端的属性：RegisteredClient.tokenSettings，其类型为 TokenSettings。

上篇文章有写到设置客户端信息的代码，如下：

@Bean

public RegisteredClientRepository registeredClientRepository() {

RegisteredClient registeredClient = RegisteredClient.withId(UUID.randomUUID().toString())

.clientId("messaging-client")

.clientSecret("{noop}secret")

.clientAuthenticationMethod(ClientAuthenticationMethod.CLIENT\_SECRET\_BASIC)

.authorizationGrantType(AuthorizationGrantType.AUTHORIZATION\_CODE)

.authorizationGrantType(AuthorizationGrantType.REFRESH\_TOKEN)

.authorizationGrantType(AuthorizationGrantType.CLIENT\_CREDENTIALS)

.redirectUri("http://127.0.0.1:8080/login/oauth2/code/messaging-client-oidc")

.redirectUri("http://127.0.0.1:8080/authorized")

// 便于调试授权码流程

.redirectUri("https://cn.bing.com")

.scope(OidcScopes.OPENID)

.scope("message.read")

.scope("message.write")

.clientSettings(ClientSettings.builder().requireAuthorizationConsent(true).build())

.build();

return new InMemoryRegisteredClientRepository(registeredClient);

}

代码中并没有直接设置 tokenSettings 属性，通过查看源码发现，实际上该属性的默认值为 TokenSettings.builder().build();，查看其源码：

public static Builder builder() {

return new Builder()

.accessTokenTimeToLive(Duration.ofMinutes(5))

.accessTokenFormat(OAuth2TokenFormat.SELF\_CONTAINED)

.reuseRefreshTokens(true)

.refreshTokenTimeToLive(Duration.ofMinutes(60))

.idTokenSignatureAlgorithm(SignatureAlgorithm.RS256);

}

通过字面意思不难知道，令牌有效期默认是5分钟。令牌格式默认是自包含格式。

有效期

令牌有效期可以通过 TokenSettings 进行设置：

RegisteredClient registeredClient = RegisteredClient.withId(UUID.randomUUID().toString())

...（省略）

// 令牌有效期设置为 30 分钟

.tokenSettings(TokenSettings.builder().accessTokenTimeToLive(Duration.ofMinutes(30)).build())

.build();

令牌格式

从官方文档中的功能列表可以知道，令牌支持两种格式：自包含（JWT）和引用（Opaque）。



自包含（JWT）

自包含令牌使用受保护的、有时间限制的数据结构，其中包含令牌元数据和用户和/或客户端的声明。 JSON Web Token (JWT) 是一种广泛使用的格式。

RegisteredClient registeredClient = RegisteredClient.withId(UUID.randomUUID().toString())

...（省略）

// 令牌格式指定为 自包含（JWT）

.tokenSettings(TokenSettings.builder().accessTokenFormat(OAuth2TokenFormat.SELF\_CONTAINED).build())

.build();

引用（Opaque）

引用令牌是唯一标识符，用作对令牌元数据和用户和/或客户端声明的引用，存储在提供者处。

RegisteredClient client1 = RegisteredClient.withId(UUID.randomUUID().toString())

...（省略）

// 令牌格式指定为 引用（Opaque）

.tokenSettings(TokenSettings.builder().accessTokenFormat(OAuth2TokenFormat.REFERENCE).build())

.build();

end