Documento de Seguridad y Guía de Integración

Servicio: `A122RServicios`

Este servicio expone APIs protegidas mediante **OAuth 2.0/OpenID Connect (OIDC)**.
Para acceder, los clientes deben **obtener un access token** desde nuestro *Authorization Server* y enviarlo en cada petición a la API.

---

1. Flujo soportado

Actualmente se soporta el flujo **Resource Owner Password Credentials (ROPC)**, con `grant_type password`.

Descripción del flujo

- El cliente envía al token_endpoint :
  - client_id -> Enviar los valores espeficados mas abajo segun ambiente client_secret ->
  - Enviar los valores espeficados mas abajo segun ambiente username -> Enviar el cuit de la
  - empresa password -> Clave de Identificación Tributaria (CIT) grant_type=password
  - scope=openid
- El servidor retorna un access_token (y, opcionalmente, un refresh_token).
- En cada request al servicio, el cliente debe enviar el access_token en el header: Authorization: Bearer Si el token expira o es inválido, debe solicitarse uno nuevo.

---

2. Endpoints y credenciales

Ambiente Testing

- **Método:** `POST`
- **URL:** `https://idp-test.arba.gov.ar/realms/ARBA/protocol/openid-connect/token`
- **client_id:** `A122RServicios`
- **client_secret:** `44cqahkhERKtkkDGmcqrPApCMtez3XxT`

Ambiente Producción

- **Método:** `POST`
- **URL:** `https://idp.arba.gov.ar/realms/ARBA/protocol/openid-connect/token`
- **client_id:** `A122RServicios`
- **client_secret:** `k1pwZG4GdRrK88KpMfK6ACqav1SNDiCa`

---

3. Ejemplo de request (obtener token)

```
curl --location 'https://idp.test.arba.gov.ar/realms/ARBA/protocol/openid-connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=A122RServicios' \
--data-urlencode 'client_secret=44cqahkhERKtkkDGmcqrPApCMtez3XxT' \
--data-urlencode 'username=30700888505' \
--data-urlencode 'password=xxxxxx' \
--data-urlencode 'grant_type=password' \
--data-urlencode 'scope=openid'
```

4. Ejemplo de respuesta:

```
{
    "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJyaUhLNmwxZXZtYjBVeF9GaFMxM3JSQUdSNWozemE5V2dRX1
    "expires_in": 300,
    "refresh_expires_in": 1800,
    "refresh_token": "eyJhbGciOiJIUzUxMiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJjODJlZDJlNy05Yzg4LTRhYjUtODlhNS02YWVjNDlhMzQwN
    "token_type": "Bearer",
    "not-before-policy": 0,
    "session_state": "6682bdc3-6953-46b2-88d7-351c18a19576",
```

```
    "scope": "arba-roles"
}
```


5. Ejemplo de payload del access token


```
{
  "exp": 1758627000,
  "iat": 1758626700,
  "jti": "8a797c2e-e268-4241-9ff4-0cfc53b60389",
  "iss": "https://idp.test.arba.gov.ar/realms/ARBA",
  "sub": "f:6fc04c49-4702-47dc-aee1-6764ed79e6d1:30700888505",
  "typ": "Bearer",
  "azp": "A122RServicios",
  "sid": "6682bdc3-6953-46b2-88d7-351c18a19576",
  "acr": "1",
  "allowed-origins": [
    "/*"
  ],
  "scope": "arba-roles",
  "identifier": "{cuit}",
  "permissions": [
    "A122RServicios|A122RServicios_Operacion|A122RServicios_Operacion"
  ],
  "fullname": "{nombre_empresa}",
  "login": "{cuit}",
  "type": "EXTERNO"
}
```


6. Consideraciones de seguridad

- Los **client_id** y **client_secret** son confidenciales y no deben compartirse.
- Los **tokens tienen vencimiento** (`expires_in`). Se recomienda implementar lógica de renovación automática.
- Todo el tráfico debe realizarse bajo **HTTPS**.

Comments

Contacto por consultas: servicioA122R@arba.gov.ar