IDLAC Broker Modelo Regional

DOCUMENTACIÓN TÉCNICA
Parte II b: Especificaciones técnicas y Seguridad

Versión	Modificación	Fecha	Modificado por:
1.0	Versión inicial	2025-09-04	Mariana Silvera
1.1	Incluye URL well-known de Testing y logout uri. Mapeo de Claims	2025-10-06	Mariana Silvera
1.2	Incluye documentación final Fase 1	2025-12-04	Mariana Silvera
1.3	Separa documentación técnica del broker del Modelo	2025-12-10	JP García

Documento en permanente evolución elaborado por el Grupo de trabajo de Red Gealc con apoyo del Consorcio Ciudadano Digital Regional (BID, Banco Mundial, CoDevelop y OEA)

9. Especificaciones técnicas

9.1. Especificaciones y versionado general de la solución (ID Broker):

Información para tener en cuenta:	
OpenID Connect	Versión 2.0
Flujos OIDC soportados	Authorization Code (con PKCE)
Response_mode	form_post
TLS	1.2 o superior
Algoritmo firmas JWT	HMAC con SHA-256
JWT	En cumplimiento con RFC 7519
Scopes	openid | email | profile
Tokens emitidos	Id token | Access token

9.2. Especificación del intercambio de datos – IDPs

El detalle de los datos de identificación de cada persona se encuentra en el documento del Modelo IdLAC.

Si bien cada IdP puede darle a su información un formato distinto, los datos fundamentales que se deben proveer del usuario son:

- Nombre y apellidos completos
- Identificador (código país según la norma ISO 3166-1 código alfa-2, tipo de documento y número)
- Email
- Número de teléfono celular
- Nivel de seguridad compuesto de 3 variables (ver estandarización de niveles):
    - RID: registro;
    - AE: autenticación;
    - NID: menor entre RID y AE.

El broker procesa estos datos y los envía al SP. La respuesta se estructura en distintas categorías denominadas "scopes", las cuales contienen distintos datos denominados "claims". Esta estructura es siempre igual y no depende del IDP utilizado

Scope	**Claims**
Información personal	Nombre completo, primer nombre, segundo nombre, primer apellido, segundo apellido
Documento	país, tipo de documento, número de documento
Email	email
Celular	Número completo de celular (incluyendo el código del país)
Nivel	nivel de registro, nivel de autenticación, nivel de seguridad

9.3. Especificación del intercambio de datos – SPs

Descripción del Token JWT entregado por ID Broker

La siguiente tabla describe el contenido del token JWT proporcionado, incluyendo sus claims estándar y personalizados.

Claim	Descripción / Valores posibles	Obligatoriedad	Formato	Ejemplo
sub	Identificador del sujeto global.	SI	código país – código documento – número documento	UY-CI-42907981-
ae	Nivel de autenticación. Los valores posibles son: 0, 1, 2, 3	SI	Integer	0
document_country	Código de país que emitió el documento del usuario según la norma ISO 3166 alfa-2	SI	String	UY
document_id	Número de documento sin incluir barras, separadores o puntos	SI	String	42907981
document_type	Código de documento	SI	String	CI
iss	Issuer (emisor del token)	SI	String	
nid	Nivel de Seguridad: 0, 1, 2 o 3	SI	Integer	1
rid	Nivel de Registro: 0, 1, 2 o 3	SI	Integer	1
given_name	Primer nombre del usuario autenticado	SI	String	Juan
middle_name	Segundo nombre del usuario autenticado	NO	String	Martín
sid	ID de sesión	SI	String	OOtZNDRTPpLR... 2-SA0wg
aud	Propósito de uso del token	SI	String	email

auth_time	Hora de autenticación	SI	Integer	
name	Nombre completo	NO	String	Juan Martín Perez
phone_number	Número de celular (incluyendo código del país)	NO	String	+506-223100
exp	Fecha de expiración del token	SI	Integer	1755611155
iat	Fecha de emisión del token	SI	Integer	1755609355
family_name	Primer apellido del usuario	SI	String	Perez
second_family_name	Segundo apellido del usuario	NO	String	Gómez
jti	JWT ID	SI	String	0b700e02-f1ac-4ccb-addb-3f51197ec0bc
email	Correo electrónico del usuario	SI	String	Juan.gomez@agesic.gub.uy

Ejemplo de token


```
{
  "sub": " UY-CI-42907981-",
  "ae": 3,
  "document": {
    "document_country": "UY",
    "document_id": "42907981",
    "document_type": " CI"
  },
  "iss": "http://localhost:8080",
  "nid": 1,
  "rid": 1,
  "given_name": "Juan",
  "middle_name": "Martín",
  "sid": "OOtZNDRTPpLR5D07bsdQ0Mj3LIqYoj4_LdvE2-SA0wg",
```

```
  "aud": "sp-client",
  "auth_time": 1755609343,
  "name": "Juan Martín Pérez Gómez ",
  "phone_number": "+506-223100",
  "exp": 1755611155,
  "iat": 1755609355,
  "family_name": "Perez",
  "second_family_name": "Gómez",
  "jti": "0b700e02-f1ac-4ccb-addb-3f51197ec0bc",
  "email": "juan.gomez@agesic.gub.uy"
}
```


9.4. ID Broker – Intercambio de información y mensajes

Como se mencionó al inicio de la guía, el Service Provider se dará de alta en ID Broker, a través del protocolo OIDC v2.0. A continuación se muestran los mensajes esperados que se intercambiarán en una integración exitosa.

EJEMPLO de:

mensajes intercambiados

Id_token

Access_token

Well-known URL