MINISTERIO DE LA PRESIDENCIA
ESTADO PLURINACIONAL DE BOLIVIA

AGETIC
agencia de gobierno electrónico y tecnologías de información y comunicación

Ciudadanía Digital

Especificaciones técnicas para el servicio de Autenticación.

Versión 1.1.0

En este documento se describe todos los pasos que deben seguir los sistemas que utilizarán la plataforma de ciudadanía digital como medio de autenticación.

Las especificaciones del presente documento están basados en OpenID Connect la cual es una capa de identidad basada en las especificaciones del protocolo OAuth 2.0 que define mecanismos para obtener y usar los token de acceso, pero que no especifica métodos estándares para proporcionar información de identidad.

Es necesario señalar que el OpenID Connect implementa la autenticación como una extensión del proceso de autorización que especifica OAuth 2.0., realiza la comprobación de la identidad del usuario y proporciona información del mismo (claims).

DESCRIPCIÓN DE ACTORES

- Propietario del recurso (Resource Owner)
  Es el ciudadano que tiene acceso a un navegador web y es capaz de dar acceso a sus recursos protegidos.

- Cliente (Client)
  Es el Sistema Cliente que hace peticiones a recursos protegidos en nombre del propietario del recurso y con la autorización del mismo.

- Servidor de autorización (Authorization Server)
  Es el Sistema Proveedor de Identidad que es el responsable de validar las credenciales del ciudadano (Authorization endpoint) y generar tokens de acceso (Token endpoint).

- Recurso protegido (Protected Resource)
  Es la entidad que tiene los recursos protegidos. Es capaz de aceptar y responder peticiones usando el token de acceso.

REGISTRO DEL SISTEMA CLIENTE

Para el registro de un sistema cliente en el Sistema Proveedor, el encargado de la entidad solicitante solicitará el registro a la AGETIC, una vez registrado el Sistema Cliente en el Sistema Proveedor se generará un *id_client* de la aplicación y la misma quedará habilitada para que reciba tokens de acceso. El *id_client* y *tokens* generados se enviará al correo del encargado de la entidad (el *id_client* y *tokens* generados serán encriptados con GPG para el envío por correo).

Los parámetros que se deben remitir para la creación de la cuenta son los que se detallan a continuación:

Parámetro	Condición	Descripción

redirect_uris	requerido	Array de urls de redirección tras la autenticación.
post_logout_redirect_uris	requerido	Array de urls de redirección tras el logout del proveedor de identidad.
client_name	recomendado	Nombre del sistema cliente.
authorization_params	requerido	JSON con parámetros de autorización.
scope	requerido	Conjunto de objetos que identifican al ciudadano. Están definidos los siguientes objetos: ● *openid*: Especifica que la solicitud de autenticación del tipo OpenID y para retornar el ID token (requerido). ● nombre: Nombres y apellidos del ciudadano (opcional). ● *documento_identidad*: Número de documento de identidad del ciudadano (opcional). ● *fecha_nacimiento*: Fecha de nacimiento del ciudadano (opcional). ● *email*: Correo electrónico del ciudadano (opcional). ● *celular*: Números de teléfono celular del ciudadano (opcional). La solicitud de petición de estos datos debe ser justificada.
redirect_uris_signature	recomendado	Array de urls ([0] backend, [1] frontend) Urls que utiliza el servicio de certificación para notificar al sistema cliente sobre el resultado del proceso de aprobación de documentos. El primer elemento es la url del backend del sistema cliente al que hace la notificación para proseguir, el segundo elemento es la ruta del frontend para redireccionar al ciudadano a la página del sistema cliente donde puede ver resultados del

		proceso.
authorization_token	requerido si utiliza el servicio de certificación.	Token JWT para la notificación del servicio de certificación (el servicio de certificación adjuntará este token a la cabecera "Authorization" de la petición al backend del sistema cliente que le informa de la conclusión del proceso de aprobación por parte del propietario del recurso).
contacts	recomendado	Correo electrónico de contacto del sistema cliente.

La especificación de cómo el cliente y el proveedor de identidad interactúan es *authorization_code*.

El tipo de código definido para el intercambio del token de acceso es *code* y el tipo de aplicación es *web*.

Las urls de redirección deberán ser urls limpias (no deben contener caracteres especiales).

El sistema cliente de estar sobre https.

Una vez creado el cliente se enviará las credenciales al encargado de la entidad. Las credenciales contendrán el *id_client*, *secret y registration_access_token* los mismos deben ser conservados, ya que estos datos serán necesarios en la configuración del sistema cliente.

AUTENTICACIÓN Y AUTORIZACIÓN

Para el proceso de autenticación y autorización de ciudadanía digital, se deberá seguir con los siguientes pasos:

1. **Crear un token de estado**

Para proteger la seguridad de los ciudadanos mediante la prevención de ataques de falsificación de solicitudes, se debe crear un token de sesión única para mantener el estado entre el sistema cliente y el ciudadano. Este token de estado debe ser generada de manera aleatoria y debe ser conservada para validar más adelante (se sugiere generar una cadena de al menos 30 caracteres).

2. **Enviar solicitud de autenticación al Sistema Proveedor de Identidad**

En este paso se debe realizar una petición GET vía protocolo HTTPS con parámetros apropiados que se especifican a continuación:

La URL donde se debe enviar la solicitud GET es la siguiente:

```
https://<base-url-proveedor-identidad>/auth
```

Los parámetros necesarios que se deben enviar en la petición son:

Parámetro	Condición	Descripción
client_id	requerido	Es el identificador del Sistema Cliente, este identificador se obtiene cuando se registra el Sistema Cliente en el Sistema Proveedor de Identidad.
response_type	requerido	Parámetro utilizado en el flujo openID connect y siempre deberá ser *code*.
redirect_uri	requerido	Es la url que recibirá el código de acceso tras la autenticación en el proveedor de identidad. Debe estar codificado en formato url y debe ser la misma que se proporcionó en el registro del sistema cliente.
scope	requerido	El parámetro permite obtener información acerca del propietario del recurso. Los scopes a solicitar deben ser *openid*, *documento_identidad*, *etc* Los scopes enviados debe ser un subconjunto de los scopes solicitados en la creación del cliente.
state	requerido	Valor del token de estado y de sesión única creada en el paso anterior.
nonce	requerido	Valor aleatorio generado en el sistema cliente que habilita la protección de repetición. Debe ser conservada para más adelante.
prompt	opcional	El Cliente podrá utilizar el parámetro de solicitud para asegurarse de que el Usuario final aún esté presente en la sesión actual o para llamar la atención sobre la solicitud (si se envía este parámetro el proveedor de identidad siempre solicitará las credenciales al ciudadano en el inicio de sesión). El valor que se debe enviar es login (prompt=login)

Ejemplo de solicitud:

```
https://<base-url-proveedor-identidad>/auth?
response_type=code&client_id=s6JKYjjYU6869BhdRkqt3&state=509ccc2713049e6efea071a9c
34f6f45&nonce=231301a1afe20d88ca963ee84c3929c3&redirect_uri=https://example.com/
oauth&scope=openid%20documento_identidad
```

Es necesario recordar que en todo momento se debe hacer uso del protocolo HTTPS.

3. Validar el código de sesión única

Una vez que el ciudadano haya procedido a autenticarse en el Sistema Proveedor de Identidad el

mismo redirigirá al Sistema Cliente (a la url registrada como *redirect_uri*) con un código de acceso (*code)* y el código de estado (*state)* en caso de éxito, código de error en caso de que la autenticación no fuera exitosa, se detectará una petición malformada o se produjera un error.

En caso de retorno exitoso el sistema cliente debe verificar que el valor del parámetro *state* que recibe del Sistema Proveedor de identidad coincide con el generado en paso anterior.

Ejemplo de retorno con autenticación exitosa:

```
https://<SISTEMA-CLIENTE>/callback?
code=ausTUY67HyGTog78&state=509ccc2713049e6efea071a9c34f6f45
```

Ejemplo de retorno con autenticación no exitosa

```
https://<SISTEMA-CLIENTE>/callback?error=consent_required&error_description=client
%20not%20authorized%20for%20End-User%20session
%20yet&state=509ccc2713049e6efea071a9c34f6f45
```

4. Intercambiar el código de acceso por un token de acceso y token de identidad

Para intercambiar el código de acceso (*code*) por el token de acceso y el token de identidad se debe enviar una petición POST via HTTPS con los parámetros necesarios.

La url donde se debe enviar la solicitud POST es la siguiente:

```
https://<base-url-proveedor-identidad>/token
```

Los parámetros necesarios que se debe enviar en la cabecera son:

Parámetro		**Descripción**
Authorization	requerido	El *id_client* y *secret* (ambos obtenidos en el registro del sistema cliente) deben ser pasados en la cabecera mediante la autenticación básica (debe estar codificada en base64, el *secret* debe estar codificado con urlEncode antes de hacer la codificación con base64)

Los parámetros necesarios que se deben enviar en el cuerpo son:

Parámetro		**Descripción**
code	requerido	Es el código de acceso obtenido en el paso 3.
redirect_uri	requerido	Es la misma url utilizada en el paso 2.
grant_type	requerido	El valor deberá ser *authorization_code*.

Ejemplo de solicitud:

```
POST /token HTTP/1.1
Host: https://<base-url-proveedor-identidad>/token
Content-Type: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

grant_type=authorization_code
&code=SplxlOBeZQQYbYS6WxSbIA
&redirect_uri=https://<SISTEMA-CLIENTE>/callback
```

En caso de éxito el Sistema Proveedor de Identidad devolverá un objeto JSON con los siguientes parámetros:

Parámetro	**Descripción**
Id_token	Es un JWT que contiene información de la sesión.
access_token	Es un token que servirá acceder a los recurso protegidos.
token_type	Identifica el tipo de token devuelto.
expires_in	Tiempo de vida del token de acceso.

Ejemplo de respuesta:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
  "id_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjFlOWdkazcifQ.ewogImlzcyI6ICJo
dHRwOi8vceHAihdCI6IDEzMTEyODA5NzAKfQ.ggW8hZ1EuVkKU8NXNHq-rvKMzqg"
  "access_token": "SlAV32hkKG",
  "token_type": "Bearer",
  "expires_in": 3600,
}
```

5. **Obtener identidad del usuario.**

El Sistema Cliente debe realizar una petición al Proveedor de Identidad haciendo uso del token de acceso obtenido en el paso 4.

La url donde se debe enviar la solicitud GET es la siguiente:

```
https://<base-url-proveedor-identidad>/me
```

Los parámetros necesarios que se deben enviar en la cabecera son:

Parámetro		**Descripción**
Authorization	requerido	El *acces_token* mediante la autenticación tipo Bearer.

Ejemplo de solicitud:

```
curl -X GET \
  https://<base-url-proveedor-identidad>/me \
  -H 'authorization: Bearer bN8OXruRhvl8WD13haKyV62ba2n2c1uMRibYis7kUBytylA'
```

Esto retornará claims autorizados por el ciudadano, alguno de estos es el CI, nombre, etc.

El parámetro *CI* debe ser utilizado para identificar al ciudadano y a partir de ello se debe consultar en la base de datos del Sistema Cliente si el ciudadano está registrado o no. A partir de este punto se seguirá flujo correspondiente de autenticación e inicio de sesión propia en el Sistema Cliente incluyendo su propia gestión de roles.

6. Finalizar sesión

Para finalizar la sesión iniciada en el Sistema Proveedor de Identidad se debe realizar una petición GET.

La url donde se debe enviar la solicitud GET es la siguiente:

```
https://<base-url-proveedor-identidad>/session/end
```

Los parámetros necesarios que se deben enviar en la petición son:

Parámetro		**Descripción**
id_token_hint	requerido	id_token
post_logout_redirect_uri	requerido	Url de redirección

Una vez que se haya finalizado la sesión en el Sistema Proveedor de Identidad, la misma retornará a la url de redirección de deslogueo (*post_logout_redirect_uris*). Finalmente en el Sistema Cliente se deberá cerrar su propia sesión.

TIEMPO DE VIDA DE TOKENS (TTL)

El tiempo de vida definido para la sesión en el Sistema Proveedor de Identidad y los tokens son los siguientes:

	Tiempo de vida
session	4 horas
authorization_code	10 minutos
access_token	60 minutos
id_token	60 minutos

BASE-URL-PROVEEDOR-IDENTIDAD

Test: **https://account-idetest.agetic.gob.bo/**