ESTRATEGIA TRANSFORMACIÓN DIGITAL

IDENTIDAD DIGITAL

MANUAL DE INTEGRACIÓN

GUÍA TÉCNICA

ClaveÚnica

Tu acceso al Estado Digital

Versión 3.2 | Octubre 2020

gob digital CHILE

Ministerio Secretaría General de la Presidencia

Gobierno de Chile

ÍNDICE

Este documento está siempre en construcción

Ayúdanos a mejorarlo en este link

Suscríbete a nuestro newsletter o incluye contactos importantes de tu institución

Haz clic aquí

Nuestro newsletter usa mailchimp, por lo necesitas asegurarte de que tu casilla pueda recibir los mensajes

Control de versiones

Versión	Fecha	Descripción
3.3	14/12/2020	Se agrega diagrama de secuencia OpenID Connect
3.2	20/11/2020	Se agrega más información en procedimiento de certificación
3.1	25/09/2020	Se agrega actualización de seguridad del logout
3.0	10/09/2020	Se actualiza procedimiento de solicitud de credenciales en nuevo portal
2.0	01/05/2020	Se agrega información de mesa de ayuda
1.0	23/03/2020	Versión inicial

I. Información General

I.I. ¿Qué es ClaveÚnica?

ClaveÚnica es un mecanismo de identificación digital que permite a los ciudadanos acceder a todos los servicios del Estado a través de una sola contraseña y es la base para construir el Modelo de Identidad Digital en Chile.

I.2. ¿Quienes pueden integrar ClaveÚnica?

Actualmente ClaveÚnica está disponible **sólo para ser integrado en plataformas y aplicaciones de instituciones públicas**, según el mandato del Instructivo Presidencial de Transformación Digital. Además, podrán integrarse las empresas Proveedoras de Servicios de Certificación para el otorgamiento de certificados de Firma Electrónica Avanzada.

I.3. ¿Se puede usar dos formas de autenticación en paralelo?

Sí, se pueden mantener ambos sistemas en paralelo siempre y cuando la institución cumpla con lo indicado en el Instructivo Presidencial de Transformación Digital. En este caso es importante gestionar el cambio y comunicar oportunamente a los usuarios, clarificando las etapas y plazos en la migración al sistema de identificación exclusivo con ClaveÚnica.

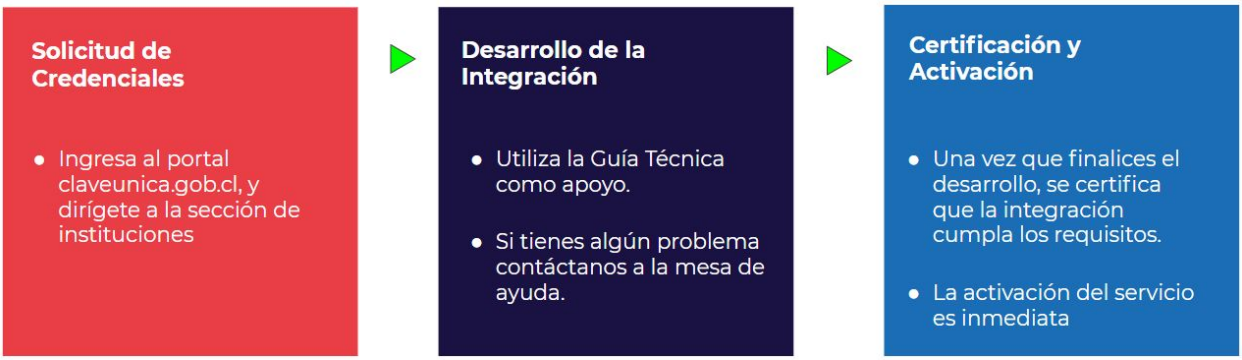
I.4. ¿Se puede integrar ClaveÚnica en trámites institucionales internos?

El Instructivo Presidencial indica que todos los trámites con autenticación dirigidos a personas naturales deben integrar ClaveÚnica, esto rige especialmente para los trámites listados en el Registro Nacional de Trámites que requieren o incorporan un mecanismo de autenticación, sin embargo esto no es una restricción en el caso que una institución requiera integrar ClaveÚnica como mecanismo de autenticación para sus funcionarios.

2. Integrar ClaveÚnica

2.1. ¿Cómo se integra ClaveÚnica a mis aplicaciones?

El proceso es el siguiente:

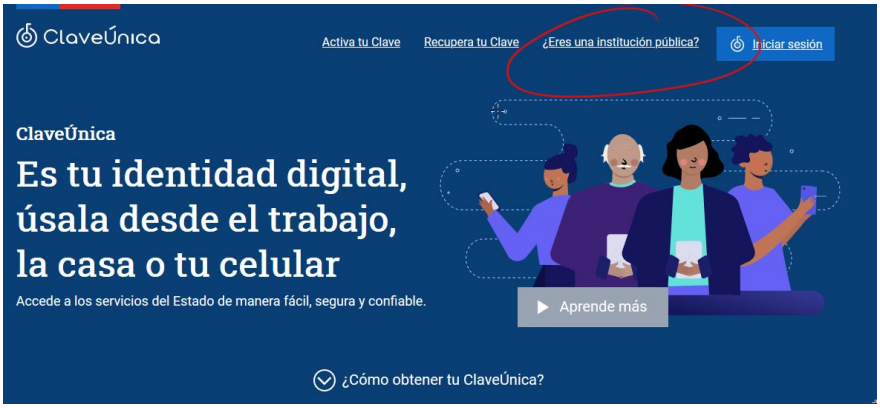


La complejidad de la implementación dependerá del lenguaje que ocupe en su plataforma o sistema.

Existen ejemplos de código fuente en los lenguajes de programación o frameworks más utilizados por integradores.

2.2. Solicitar credenciales para la Integración

Para solicitar credenciales de integración, debe dirigirse a la sección "¿Eres una institución pública?" de nuestro portal web ubicada en la parte superior derecha del sitio.



Luego, hacer clic en el botón “Enviar solicitud”

También puede ingresar directamente en este link.

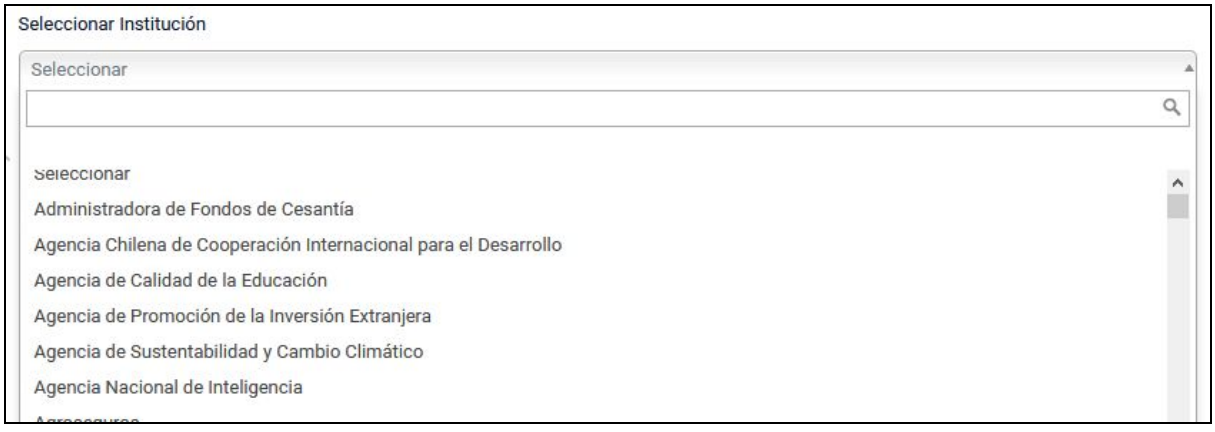
Al ingresar al sitio deberá autenticarse con su ClaveÚnica. Luego aparecerá el trámite “Solicitud de Integración a ClaveÚnica” en el cual ingresará pinchando en “Iniciar”.

A continuación se desplegará el formulario de solicitud de credenciales que deberá completar poniendo atención a cada campo solicitado.

Los campos solicitados son los siguientes:

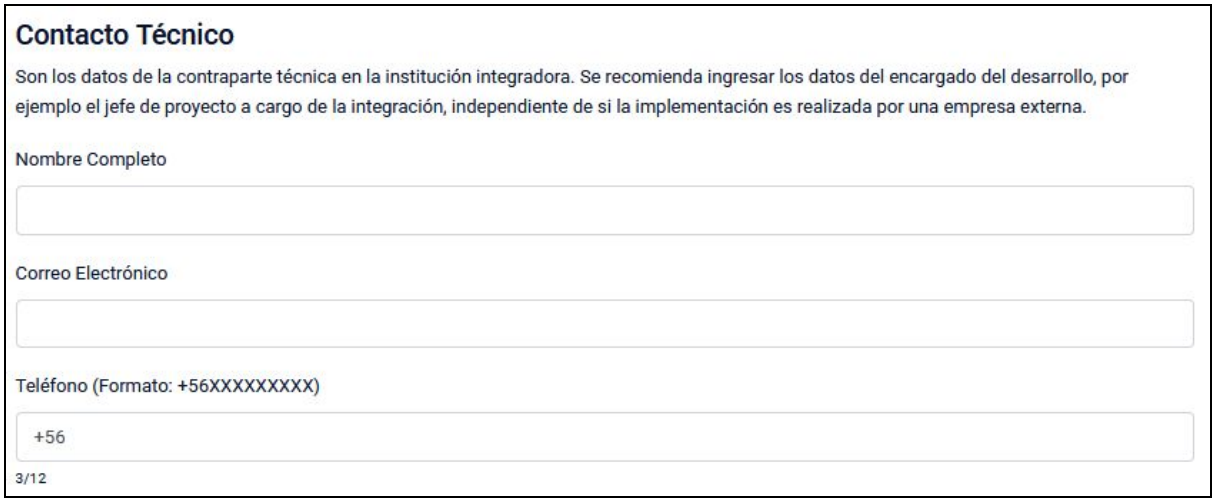
Seleccionar Institución

Es el nombre de la institución pública que requiere incorporar ClaveÚnica. Seleccione el nombre de la institución entre las opciones otorgadas.



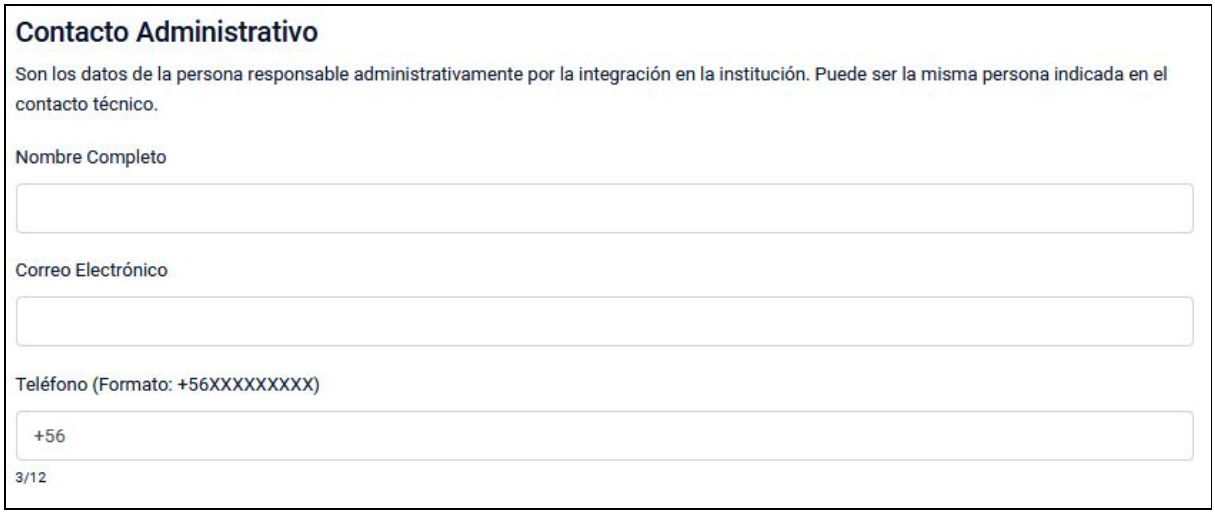
Contacto Técnico

Son los datos de la contraparte técnica en la institución integradora. Se recomienda ingresar los datos del encargado del desarrollo, por ejemplo el jefe de proyecto a cargo de la integración, independiente de si la implementación es realizada por una empresa externa.



Contacto Administrativo

Son los datos de la persona responsable administrativamente por la integración en la institución. Puede ser la misma persona indicada en el contacto técnico.



Nombre de la aplicación

Este campo es importante, el *nombre de la aplicación* es lo que aparecerá en la ventana de login.

Puede indicar el nombre de la institución solamente o complementar con el nombre del sistema si la institución tiene más de una integración. El largo máximo del nombre es de 30 caracteres.

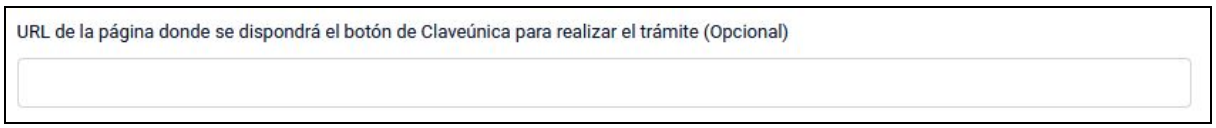
Si lo necesita, puede solicitar el cambio del nombre de la aplicación a través de la mesa de ayuda.

Descripción

Debe indicar una breve descripción del contexto y los fines de la integración, así como también cualquier información relevante, por ejemplo acá puede indicar si el desarrollo está a cargo de una empresa externa. La descripción debe ser concisa.

URL de la página donde se dispondrá el botón de Claveúnica para realizar el trámite

Este campo es opcional, pero también importante. Indica la dirección de la página donde los usuarios encontrarán el botón de autenticación.

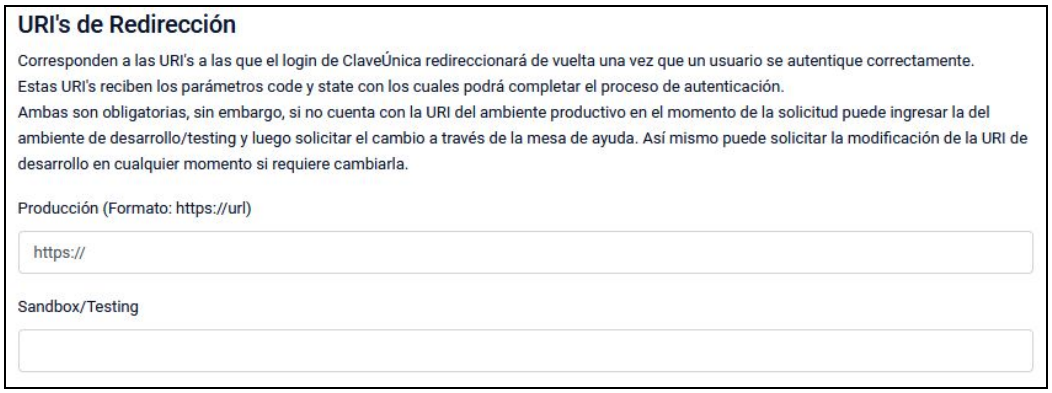


URI's de redirección

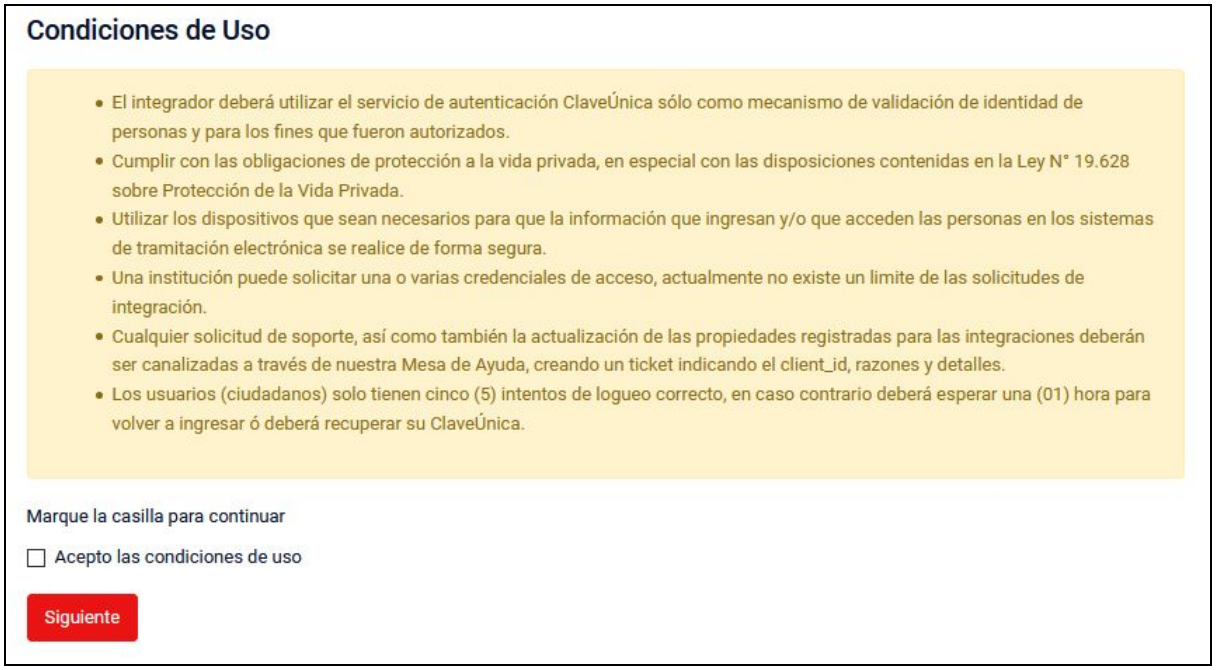
Corresponden a las URI's a las que el login de ClaveÚnica redireccionará de vuelta una vez que un usuario se autentique correctamente.

Estas URI's reciben los parámetros *code* y *state* con los cuales podrá completar el proceso de autenticación.

Ambas son obligatorias, sin embargo, si no cuenta con la URI del ambiente productivo en el momento de la solicitud puede ingresar la del ambiente de desarrollo/testing y luego solicitar el cambio a través de la mesa de ayuda. Así mismo puede solicitar la modificación de la URI de desarrollo en cualquier momento si requiere cambiarla.



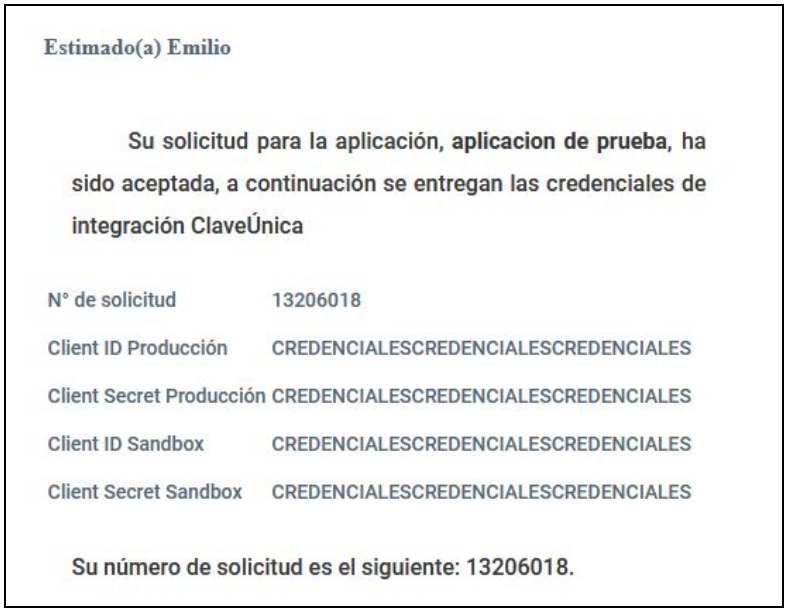
Luego de llenar los campos requeridos, ponga atención a las instrucciones para preparar el paso a producción y **acepte los Términos y Condiciones del Servicio**.



IMPORTANTE: Cuando solicite la habilitación de las credenciales de producción la DGD procederá a **certificar** la integración y podrá solicitar más información acerca de ella y los trámites que están relacionados.

Para finalizar el proceso de solicitud de credenciales

Luego de enviar la solicitud se notificará el recibo de este y se evaluará si es correcta. De ser así se le enviará un email a la casilla descrita en la solicitud con 2 pares de credenciales (client_id y client_secret) , unas vinculadas a ***Sandbox/Testing*** y otras a **Producción**.



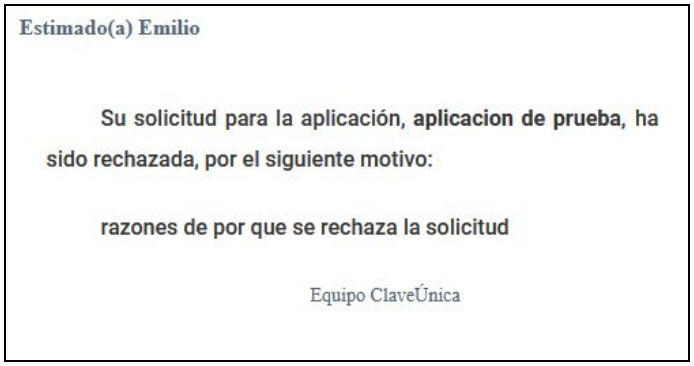
Estimado(a) Emilio

Su solicitud para la aplicación, **aplicacion de prueba**, ha sido aceptada, a continuación se entregan las credenciales de integración ClaveÚnica

N° de solicitud	13206018
Client ID Producción	CREDENCIALESCREDENCIALESCREDENCIALES
Client Secret Producción	CREDENCIALESCREDENCIALESCREDENCIALES
Client ID Sandbox	CREDENCIALESCREDENCIALESCREDENCIALES
Client Secret Sandbox	CREDENCIALESCREDENCIALESCREDENCIALES

Su número de solicitud es el siguiente: 13206018.

En caso que la solicitud sea rechazada se le enviará un correo indicando el motivo.



Estimado(a) Emilio

Su solicitud para la aplicación, **aplicacion de prueba**, ha sido rechazada, por el siguiente motivo:

razones de por que se rechaza la solicitud

Equipo ClaveÚnica

Las credenciales de Sandbox/Testing están operativas inmediatamente mientras que las de producción estarán bloqueadas.

Guarde todas las credenciales ya que, además de servirle para el desarrollo de su integración, le serán solicitadas para cualquier solicitud posterior.

IMPORTANTE: Todas las solicitudes relacionadas con la integración deben ser canalizadas abriendo un ticket de atención en nuestra mesa de ayuda.

2.3. ¿Qué son las credenciales de sandbox y de producción?

Una vez aprobada la solicitud de credenciales para integrar ClaveÚnica, se envían dos pares de credenciales, compuestas con un client_id y un client_secret. Éstas credenciales se usan en una integración para interoperar con la API del servicio de autenticación.

⚠ **IMPORTANTE:** El parámetro client_secret no debe ser expuesto por su aplicación.

Credenciales de sandbox

Al configurar el client_id y client_secret de sandbox en su aplicación podrá acceder a un ambiente limitado del servicio de autenticación dentro del cual tendrá la posibilidad de probar su integración.

Este ambiente solo permite utilizar un conjunto de RUN's de prueba indicados en el punto 3.2.

Credenciales de producción

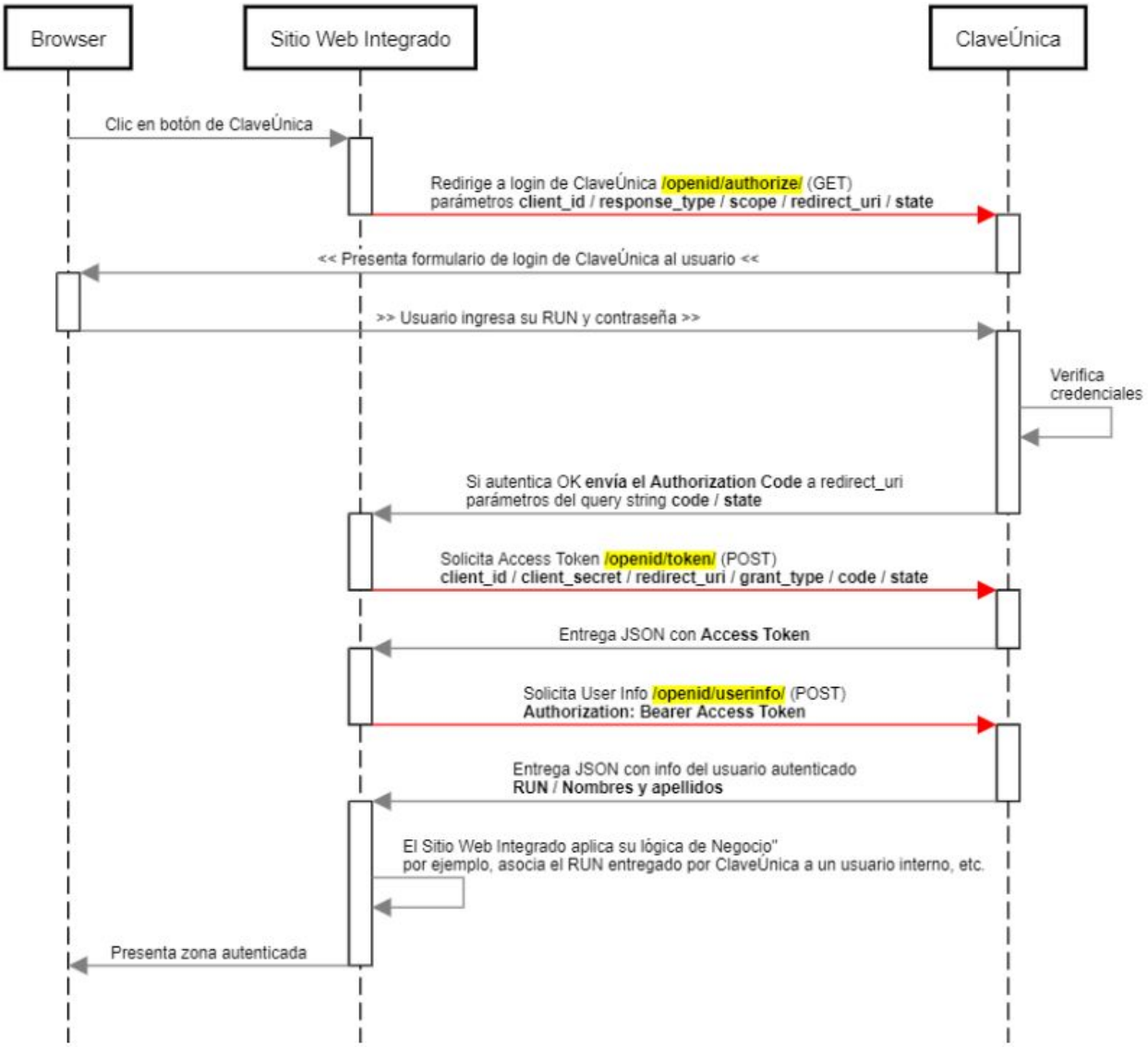
A diferencia del ambiente sandbox, las credenciales de producción permite autenticarse utilizando cuentas de ClaveÚnica de ciudadanos reales.

Para acceder a este ambiente, la aplicación integrada debe cumplir los requisitos de marca y seguridad solicitados y aprobar el proceso de certificación.

3. Implementación de la Integración

ClaveÚnica utiliza el estándar OpenID Connect, que a su vez está basado protocolo OAuth2.0 y que permite implementar el proceso de autenticación de manera segura. El proceso se lleva a cabo a través del intercambio de tokens entre el servicio ClaveÚnica y la aplicación integradora. En la especificación de OAuth2.0 este intercambio se denomina "Authorization Code Flow"

El siguiente diagrama de secuencia muestra de manera simplificada cómo se implementa la autenticación de ClaveÚnica.



3.1. Paso 1: Crear Token de estado anti-falsificación

El integrador debe proteger la seguridad de sus ciudadanos mediante la prevención de ataques de falsificación de petición, para ello el primer paso es crear un token de sesión único, que mantenga el estado entre el ciudadano y la aplicación integrada.

Posteriormente debe hacer coincidir este token de sesión único con la respuesta de autenticación devuelto por el servicio de ClaveÚnica. Así, tanto ClaveÚnica como el servicio integrado, pueden

asegurar que es el usuario quien está haciendo la solicitud y no se trata de un atacante malicioso. Este tipo de ataque se denomina como Cross-Site Request Forgery (CSRF).

Una buena opción para implementar este token de sesión único es generar una cadena aleatoria de 30 o más caracteres a través de alguna librería o generar un hash por medio de un secreto.

3.2. Paso 2: Enviar una solicitud de autenticación al servicio de ClaveÚnica

El siguiente paso es formar una solicitud **GET** vía **HTTPS** con los parámetros adecuados en la **URI**.

El protocolo **HTTP** no está permitido para ambientes productivos debido a que la información viaja en texto plano, por lo tanto debe usar el protocolo **HTTPS** en todo momento.

La **URI** donde debe ser enviada la solicitud **GET** es:

https://accounts.claveunica.gob.cl/openid/authorize/

Los parámetros que deben ser enviados en la **URI** son:

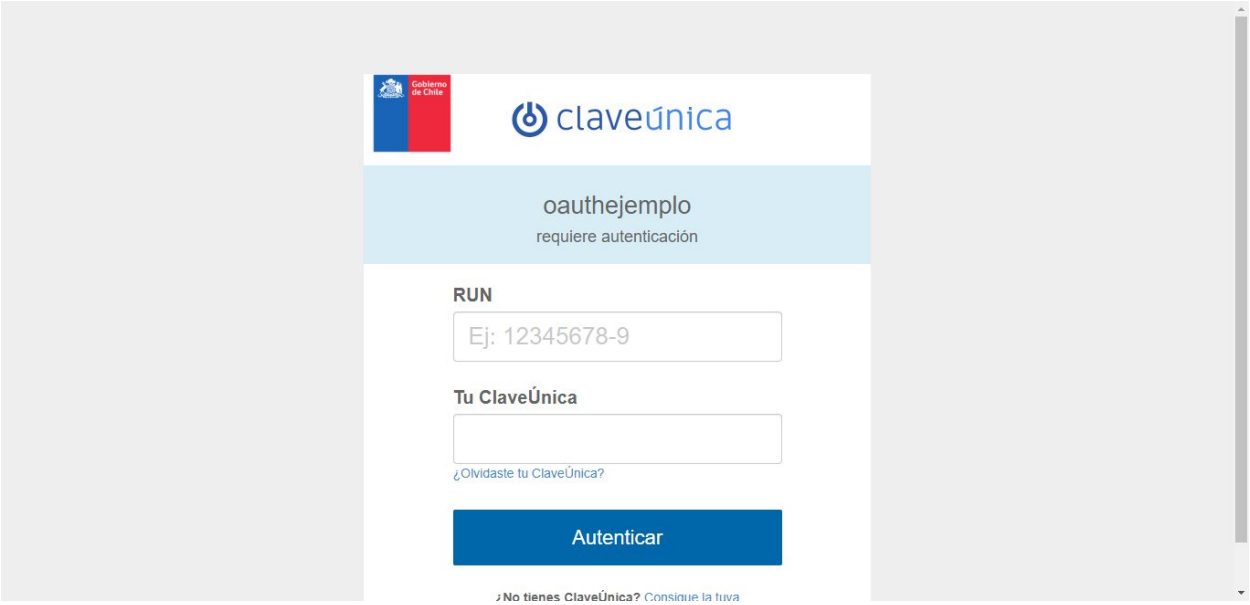
- **client_id:** Es el identificador de la integración, se obtiene al solicitar credenciales para la Institución.
- **response_type:** Este parámetro es parte de la lógica utilizada por OpenID Connect y siempre debe ser **code**.
- **scope:** Este parámetro permite obtener la información del ciudadano (run y nombre completo) y debe ser **openid run name**.
- **redirect_uri:** En este parámetro debe ir la URI (**codificada en formato URL**) de la aplicación que se integrará con ClaveÚnica. Esta URI es la que recibe la respuesta por parte de ClaveÚnica.
- **state:** En este parámetro debe ir el mismo Token único de sesión que fue indicado en el ***Paso 1***.

Ejemplo:

- **client_id:** Wbgx7HkjoeU6uarez3uYnn41VmGkd600
- **response_type:** code
- **scope:** openid run name
- **redirect_uri:** https://integrador.cl/callback (https%3A%2F%2Fintegrador.cl%2Fcallback)
- **state:** abcdefgh

- **URI final compuesta:**
  https://accounts.claveunica.gob.cl/openid/authorize/?**client_id**=Wbgx7HkjoeU6uarez3uYnn41VmGkd600&**response_type**=code&**scope**=openid run name&**redirect_uri**=https%3A%2F%2Fintegrador.cl%2Fcallback&state=abcdefgh

Cuando la aplicación integradora invoca a la URI compuesta por GET se levanta el formulario de inicio de sesión de ClaveÚnica



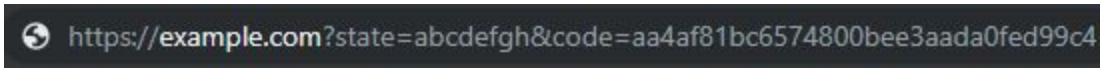
Al trabajar con las credenciales de Sandbox, puede probar la integración utilizando los siguientes RUN:

- RUN: 44.444.444-4 contraseña: testing
- RUN: 55.555.555-5 contraseña: testing
- RUN: 88.888.888-8 contraseña: testing
- RUN: 99.999.999-9 contraseña: testing

3.3. Paso 3: Confirmar el Token de estado de anti-falsificación

La respuesta que se obtiene del **Paso 2** (luego de ingresar rut y contraseña en formulario de ClaveÚnica) es enviada a la URI de Redirección indicada como **redirect_uri**. Continuando con el ejemplo, lo obtenido sería algo así

https://example.com?state=abcdefgh&code=aa4af81bc6574800bee3aada0fed99c4



En su aplicación, debe corroborar que el **state** que se recibió de Claveúnica coincide con el **token** de sesión creado en el **Paso 1**.

Esta verificación de *ida y vuelta* ayuda a garantizar que es un ciudadano y no un atacante que está haciendo la solicitud.

3.4. Paso 4: Cambiar el código de activación por los token de acceso y autorización

La respuesta incluye un parámetro llamado **code**. Este es un código de acceso único que tiene un tiempo de expiración de 5 minutos. Con este código su aplicación puede solicitar un **Token de acceso**.

NOTA: Si el parámetro code expira, debe enviar la solicitud de autenticación nuevamente (Paso 2) y así obtener uno nuevo.

Para solicitar este **Token de acceso** debe enviar una solicitud **POST via HTTPS**.

La **URI** donde debe ser enviada la solicitud POST es:

https://accounts.claveunica.gob.cl/openid/token/

Los parámetros que deben ser enviados en el cuerpo del mensaje POST son:

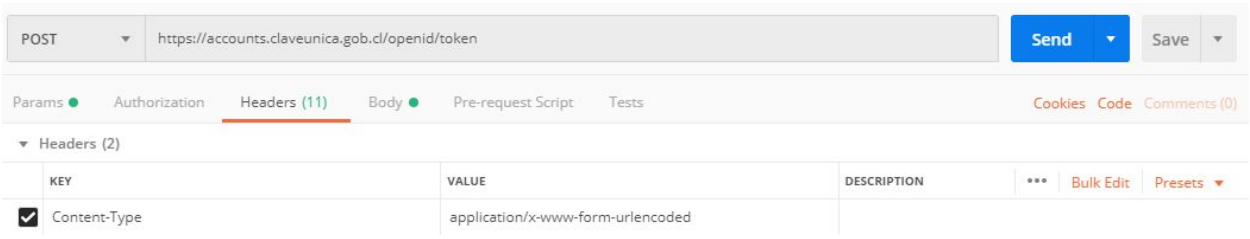
client_id	Es el identificador de la integración, se obtiene al solicitar credenciales para la Institución.

client_secret	Es el secreto asociado a la integración, se obtiene al solicitar credenciales para la Institución. Es importante que este dato sea protegido y jamás expuesto a terceros.
redirect_uri	En este parámetro debe ir la URI de su aplicación (la misma uri encodeada del Paso
grant_type	Este parámetro es parte de la lógica utilizada por OpenID Connect y siempre debe ser **authorization_code**.
code	En este parámetro debe ir el código de acceso obtenido en el Paso 3.
state	En este parámetro debe ir el mismo Token único de sesión que fue indicado en el ***Paso 1***.

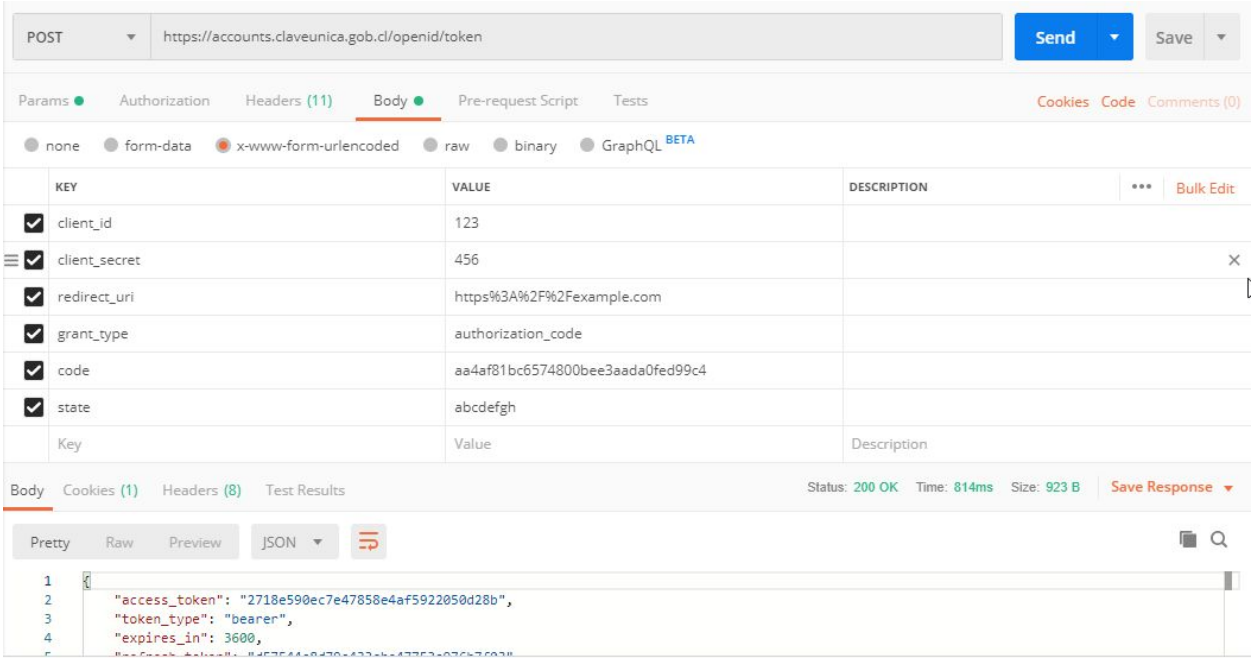
Continuando con el ejemplo iniciado en el **Paso 2**, la llamada que se debe hacer vía **POST** seria:

Ejemplo Postman

Configurar en "Headers" valor Content-Type como "application/x-www-form-urlencoded".



Ingresar parámetros en "Body" y seleccionar "x-www-form-urlencoded"



Ejemplo CURL

curl -i https://accounts.claveunica.gob.cl/openid/token/ -H "content-type: application/x-www-form-urlencoded; charset=UTF-8" --data "client_id=123&client_secret=456&redirect_uri=https%3A%2F%2Fexample.com&grant_type=authorization_code&code=aa4af81bc6574800bee3aada0fed99c4&state=abcdefgh"

3.5. Paso 5: Autenticar usuario

La respuesta obtenida en el paso anterior es un arreglo en formato **JSON**, del cual se utilizará el parámetro llamado **access_token**.

Ejemplo del JSON retornado

```
{
    "access_token": "95104ab471534af08683aefa7d0935a3",
    "token_type": "bearer",
    "expires_in": 3600,
    "id_token": “eyJhbGciOiJSUzI1NiIsIm6Ijg1ZGVjMDU1MjZmNjUwZlMTI4NTc3NGM3In0"
}
```

3.6. Paso 6: Obtener información de ciudadano por medio del Token de autorización

En este paso le explicaremos cómo puede obtener información del ciudadano basándose en el **scope**.

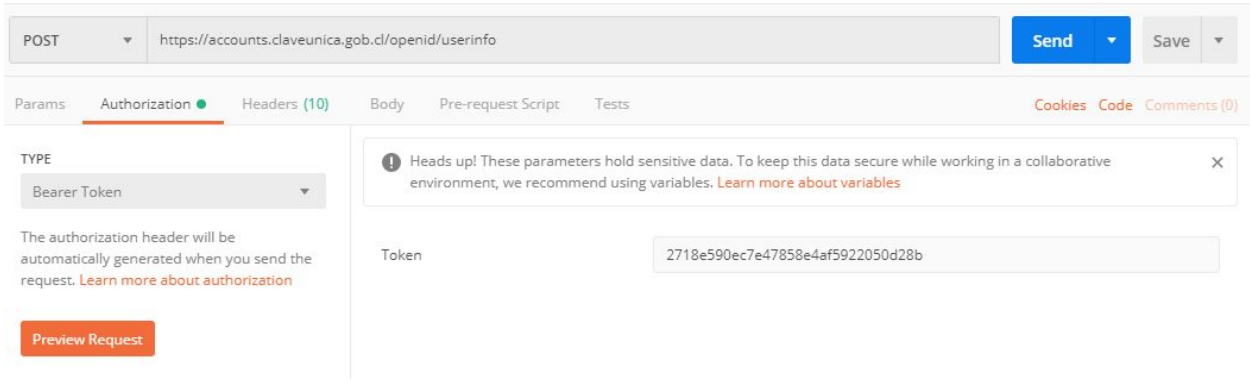
En el **Paso 5** el ciudadano ya está autenticado, pero posteriormente su aplicación puede obtener información adicional sobre el ciudadano, como por ejemplo su **nombre** y/o **RUN**.

Para lograr esto se debe enviar una solicitud POST con el **Token de acceso** obtenido anteriormente.

La solicitud POST se envía a **https://accounts.claveunica.gob.cl/openid/userinfo/** de la siguiente forma:

Ejemplo Postman

En "Authorization", seleccionar como "TYPE" valor "Bearer Token" y agregar token rescatado anteriormente.



Ejemplo CURL

curl -i **https://accounts.claveunica.gob.cl/openid/userinfo/** -X POST -H "authorization: Bearer 2718e590ec7e47858e4af5922050d28b"
JavaScript

Con esta solicitud su aplicación recibirá un JSON similar al de la imagen:

```
{
    "sub": "1234567",
    "RolUnico": {
        "DV": "9",
        "numero": 12345678,
        "tipo": "RUN"
    },
    "name": {
        "apellidos": [
            "Del Río",
            "Gonzalez"
        ],
        "nombres": [
            "María",
            "Carmen"
        ]
    }
}
```

En caso de que su aplicación intercambie el Token de autorización a otros componentes fuera del flujo de su aplicación, es recomendable que este componente valide dicho Token. La mayor parte de las API combinan la validación con el trabajo de descifrar el **base64** y parsear el **JSON**, por lo que probablemente terminará por validar el token.

3.7. Paso 7: Cierre de sesión

El último paso es implementar un correcto cierre de sesión de ClaveÚnica.

⚠ **IMPORTANTE:** Se ha reportado que la última actualización del navegador Chrome (80+) provoca que la sesión no se cierre correctamente al llamar al endpoint a través de Javascript.

Para solucionar este problema de compatibilidad / seguridad, **se debe implementar el cierre de sesión en su integración** de la siguiente forma:

En el botón de cierre de sesión de la aplicación integradora, dirigir al endpoint logout de ClaveÚnica, incluyendo como parámetro la URL encodeada de la página donde se cierra la sesión en el sitio integrador, por ejemplo:

https://accounts.claveunica.gob.cl/api/v1/accounts/app/logout?redirect=url_encodeada_página_donde_se_cierra_la_sesión_de_la_aplicación_integrada

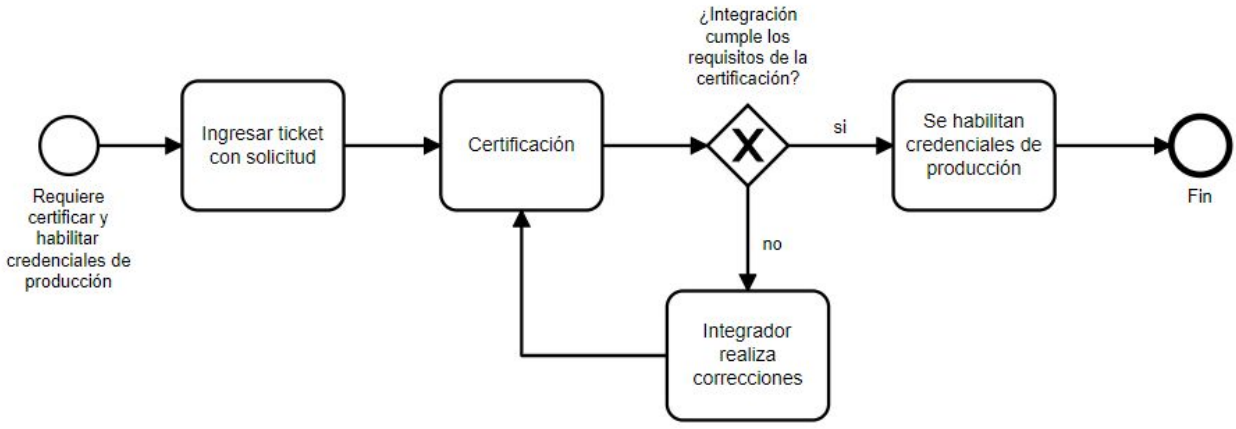
La URL que va en el parámetro "redirect" normalmente debería corresponder a la página que ya se utiliza para finalizar la sesión local en su aplicación. Cuando el endpoint de logout de ClaveÚnica es invocado, este se encargará de cerrar cualquier sesión de ClaveÚnica que se encuentre abierta y luego redireccionará para cerrar la sesión en la aplicación integradora, asegurándose de cerrar sesión en ambas partes.

4. Certificación y Habilitación de Credenciales de Producción

4.1. Procedimiento

Una vez que se ha desarrollado la integración según lo indicado en esta Guía Técnica, la institución debe certificar su aplicación para verificar si ésta cumple con los requisitos establecidos.

En caso de cumplir, se activarán sus credenciales de producción, con lo cual su aplicación podrá autenticar a cualquier ciudadano que posea ClaveÚnica activa.



4.2. Requisitos para la activación de credenciales en producción

Los requisitos para habilitar las credenciales de producción son:

✔️ Uso del botón oficial de ClaveÚnica

El botón de ClaveÚnica tiene como objetivo dejar en conocimiento al ciudadano que el trámite asociado a la integración debe o puede realizarse con ClaveÚnica, por eso es parte de la certificación de integraciones validar que exista el botón oficial implementado.

Para una correcta implementación del botón utilice los lineamientos oficiales. Además, en el siguiente enlace podrá descargar una plantilla con los estilos y gráficos para facilitar el desarrollo.

✔️ Uso de protocolo HTTPS en la aplicación integradora

El ambiente de producción debe utilizar protocolo **HTTPS**.

✔️ Llamada correcta al formulario de ClaveÚnica

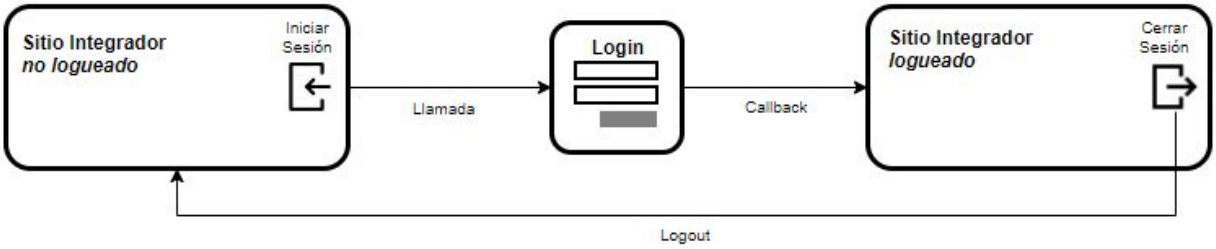
El botón de ClaveÚnica debe llamar al login a pantalla completa y seguir un flujo lineal, esto quiere decir que el formulario no debe estar por ejemplo incrustado dentro de un IFRAME, un popup u otro elemento similar.

✔️ Que la aplicación esté apuntando a los endpoints correctos

El flujo OpenID Connect que ClaveÚnica utiliza para el proceso de autenticación debe apuntar a los endpoints que están descritos en esta guía, que empiezan por **accounts.claveunica.gob.cl**.

✔️ Cierre de sesión explícito

Verificaremos que cierre de sesión se ejecuten correctamente. Esto quiere decir que el sitio integrador debe contar con un link o un botón claramente identificado para cerrar la sesión. Se revisará que se llame al endpoint tal como se especifica en esta guía y que luego de cerrar la sesión se pueda volver a iniciar sesión normalmente.



4.3. Solicitud de Certificación / Activación de Credenciales de Producción

Una vez que su integración esté desarrollada en el ambiente productivo, cumpla con los requisitos y esté lista para ser activada, debe solicitar la habilitación de las credenciales de producción.

Para hacerlo, debe enviar la solicitud desde nuestra Mesa de Ayuda DGD, teniendo en cuenta nuestras consideraciones generales sobre el envío de requerimientos.

Una vez que se identifique e indique cuál es su institución, en la lista de plataformas seleccione "ClaveÚnica" y luego en el listado de roles elija "Integrador Público"

En los antecedentes del ticket ingrese:

- **Solicitud específica:** Indique que desea realizar la certificación / activación de las credenciales de producción para su aplicación integrada.
- **CLIENT_ID de producción** entregado .
- **URL** del sitio a certificar y donde se encuentra visible el botón de ClaveÚnica (ver notas a continuación).

Nota

Para realizar el proceso de certificación, el integrador deberá contar con su ambiente de producción publicado y accesible desde Internet, para que pueda ser revisado por el equipo de ClaveÚnica.

Si el sitio integrado no está publicado aún, el integrador deberá proveer un acceso al ambiente Pre-Productivo o de QA, debido a que estos ambientes son idénticos al de producción. No se aceptará la revisión de integraciones en ambientes de desarrollo o en sitios incompletos.

Cuando no sea posible acceder desde el exterior a ninguno de los ambientes anteriormente descritos, el integrador deberá indicarlo en el ticket de solicitud para coordinar una certificación mediante una videollamada.

4.4. Tiempos estimados del procedimiento de certificación

El tiempo estimado para que el equipo de ClaveÚnica realice la certificación de una integración es de 3 días hábiles a partir de la fecha y hora de ingreso del ticket de solicitud en la mesa de ayuda. Es importante que considere este tiempo dentro de su planificación.

Este tiempo podría variar en caso que la integración no cumpla de manera cabal con los requisitos, que hubiera alguna dificultad en el acceso al sitio donde se realizará la certificación o en caso de que la certificación sea a través de videollamada.

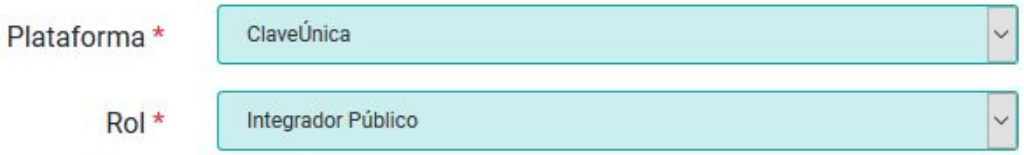
En caso que el equipo de ClaveÚnica encuentre observaciones o problemas en la integración, solicitará al integrador las correcciones respectivas, siendo este último el responsable de subsanarlas en el menor tiempo.

4.5. ¿Cómo actualizar el REDIRECT_URI u otro dato de la integración?

Es probable que mientras desarrolle su integración y antes de pasar a producción necesite actualizar algunos parámetros como: la URI de redireccionamiento, el nombre de la aplicación, entre otros datos.

Para hacerlo debe enviar la solicitud desde nuestra Mesa de Ayuda DGD, teniendo en cuenta nuestras consideraciones generales sobre el envío de requerimientos.

Una vez que se identifique e indique cuál es su institución, en la lista de plataformas seleccione "ClaveÚnica" y luego en el listado de roles elija "Integrador Público"



En los antecedentes del ticket ingrese:

- **Solicitud específica,** por ejemplo:
  - Actualización de nombre de la aplicación
  - Actualizar Redirect_uri en Sandbox
  - Actualizar Redirect_uri en Producción

- **Motivo** por el cual desea realizar el cambio. Sea específico y concreto.

- **Client_id** asociado a la integración a la cual desea aplicar el cambio.

- **Si ese client_id es de sandbox o de producción**

4.6. Consideraciones generales sobre el envío de requerimientos

Creación de tickets de atención

El ticket debe ser creado por la persona responsable en la institución del proyecto, utilizando su cuenta de correo institucional. No se aceptarán tickets ingresados con cuentas de correo genéricas (Gmail, Yahoo, etc.)

La Mesa de Ayuda institucional DGD es el medio oficial para solicitudes sobre integraciones

No se considerarán solicitudes fuera de este medio. En caso de que - en primera instancia - la solicitud haya sido realizada mediante email directamente a algún funcionario de ClaveÚnica, el integrador debe crear el ticket correspondiente con el fin de respaldar su solicitud.

5. Anexos

5.1. ¿Cómo puedo probar mi integración en CURL?

En el proceso de integración se harán llamadas a 3 endpoints: Uno en la carga del formulario de ClaveÚnica, otro para obtener el token de acceso y un último para obtener datos del usuario que inició sesión.

Existe otro endpoint para cerrar sesión, pero este no devuelve información.

En la herramienta cURL, se puede hacer pruebas de llamadas a los endpoints de la siguiente manera:

Endpoint para Token de Acceso

curl -i https://accounts.claveunica.gob.cl/openid/token/ -H "content-type: application/x-www-form-urlencoded; charset=UTF-8" --data "client_id=client_id&client_secret=client_secret&redirect_uri=redirect_uri&grant_type=authorization_code&code=code&state=state"

Ejemplo:

curl -i https://accounts.claveunica.gob.cl/openid/token/ -H "content-type: application/x-www-form-urlencoded; charset=UTF-8" --data "client_id=2177fdbd81d54ebab895ed86b5f7d1b4&client_secret=1ec2a3c429ac4763b2665d57d2379b81&redirect_uri=https%3A%2F%2Flocalhost%2Fcallback&grant_type=authorization_code&code=5050299f54064a708ac17420d02417e8&state=1e5bdc760608dc3cfcd0e7ae4"
Generic

Endpoint para Datos de Usuario

curl -i https://accounts.claveunica.gob.cl/openid/userinfo/ -X POST -H "authorization: Bearer access_token

Ejemplo:

curl -i https://accounts.claveunica.gob.cl/openid/userinfo/ -X POST -H "authorization: Bearer 10a169a98eb143c18a732ed2e1df32fb"

Generic

Para el endpoint del formulario de ClaveÚnica no es necesario usar cURL, ya que requiere autenticarse en un navegador para continuar el proceso de integración. Un ejemplo de URL para llamar al login de ClaveÚnica es:

Ejemplo:

https://accounts.claveunica.gob.cl/openid/authorize/?client_id=2177fdbd81d54ebab895ed86b5f7d1&response_type=code&scope=openid run name&redirect_uri=https%3A%2F%2Flocalhost%2Fcallback&state=1e5bdc760608dc3cfcd0e7ae4
Generic

5.2. ¿Cómo puedo probar mi integración en Postman?

En el proceso de integración se harán llamadas a 3 endpoints: Uno en la carga del formulario de ClaveÚnica, otro para obtener el token de acceso y un último para obtener datos del usuario que inició sesión.

Existe otro endpoint para cerrar sesión, pero este no devuelve información.

La explicación y funcionamiento de los endpoints indicados lo puede encontrar en la guía técnica de desarrollo de ClaveÚnica.

En la herramienta Postman, se puede hacer pruebas de llamadas a los endpoints de la siguiente manera:

Endpoint para Token de Acceso

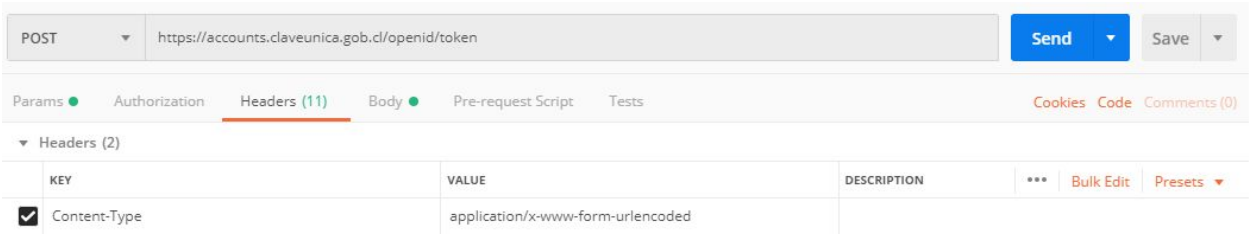
Sección: Headers

URL: **https://accounts.claveunica.gob.cl/openid/token/**

Llamada: POST

Key: Content-Type

Value: application/x-www-form-urlencoded



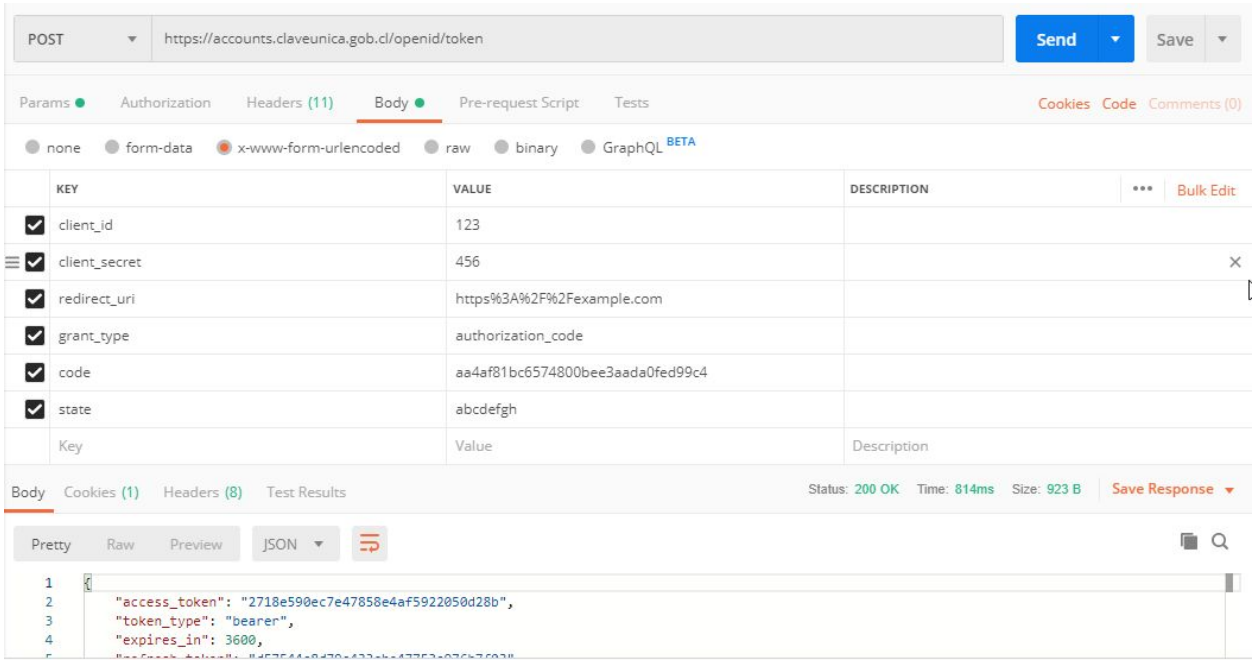
Sección: Body

URL: **https://accounts.claveunica.gob.cl/openid/token/**

Llamada: POST

Content Type: x-www-form-urlencoded

Key	Value
client_id	client_id de la integración
client_secret	client_secret de la integración
redirect_uri	redirect_uri de la integración
grant_type	authorization_code
code	code obtenido en login
state	state usado en login



Endpoint para Datos de Usuario

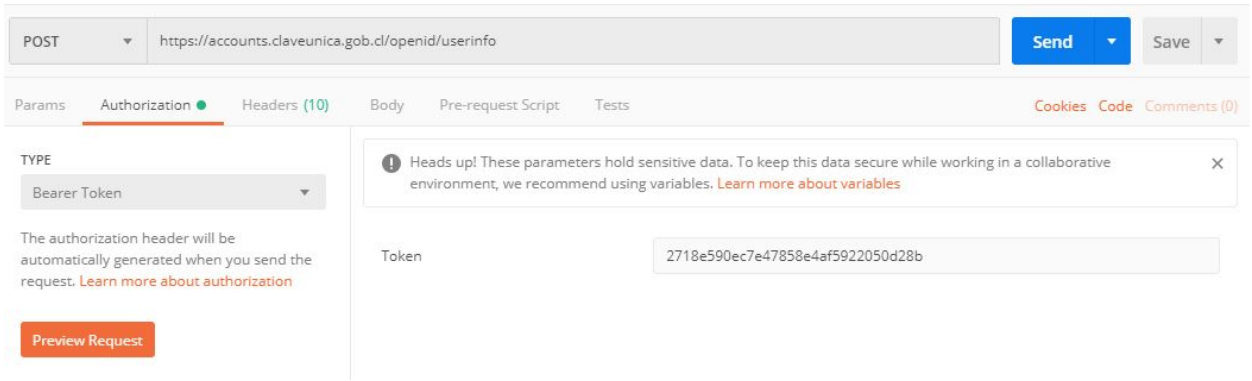
Sección: Authorization

URL: **https://accounts.claveunica.gob.cl/openid/userinfo/**

Llamada: POST

Type: Bearer Token

Token: access_token



Para el endpoint del formulario de ClaveÚnica no es necesario usar Postman, ya que requiere autenticarse en un navegador para continuar el proceso de integración. Un ejemplo de URL para llamar al login de ClaveÚnica es:

Ejemplo:

https://accounts.claveunica.gob.cl/openid/authorize/?client_id=2177fdbd81d54ebab895ed86b5f7d1&response_type=code&scope=openid run name&redirect_uri=https%3A%2F%2Flocalhost%2Fcallback&state=1e5bdc760608dc3cfcd0e7ae4

5.3. Código fuente de ejemplo

Contamos con piezas de código fuente de ejemplo que muestran la implementación de ClaveÚnica en distintos lenguajes y frameworks de programación. Actualmente contamos con:

- Python
- PHP
- DotNET
- Java

En esta carpeta puede acceder a los ejemplos de integraciones de ClaveÚnica

En la misma carpeta también está disponible un ejemplo de la integración realizado en POSTMAN

Bajo un espíritu de colaboración les dejamos la invitación a enviarnos sus sugerencias y si lo desean colaborar con otros ejemplos de implementaciones de ClaveÚnica utilizando lenguajes, frameworks y tecnologías, y así facilitar la integración a otras instituciones que lo necesiten.