ESTRATEGIA TRANSFORMACIÓN DIGITAL

IDENTIDAD DIGITAL

MANUAL DE INTEGRACIÓN

GUÍA TÉCNICA

ClaveÚnica

Tu acceso al Estado Digital

Versión 5.5 | Enero 2025

SECRETARÍA gob digital

ÍNDICE

Este documento está siempre en construcción

Ayúdanos a mejorarlo en este link

Control de versiones

Versión	Fecha	Descripción
5.5	06/01/2025	Se modifica nombre de Mesa de Ayuda a Mesa de Servicio
5.4	20/12/2024	Se incorpora ejemplos en HTML y CSS del nuevo Botón Oficial
5.3	16/12/2024	Se actualiza SLA de respuesta de las solicitudes
5.2	23/09/2024	Se agrega video tutorial de diseño de botón
5.1	02/09/2024	Se agrega nueva guía de diseño de botón
5.0	24/06/2024	Se agrega información de capacitaciones
4.9	17/04/2024	Se agregan ejemplos en requisitos de certificación
4.8	25/03/2024	Se agregan métodos de logout
4.7	13/03/2024	Se agrega nuevo item de certificación
4.6	28/02/2024	Se agrega prohibición de Localhost en los Redirect URI's
4.5	28/11/2023	Eliminación de requisito de puertos en las uris de redirección y de logout
4.4	24/08/2023	Se agregan canales de comunicación
4.3	11/08/2023	Se agrega información para la activación de credenciales en producción
4.2	26/07/2023	Se actualiza links a mesa de ayuda y portal Cerofilas, se corrige notificación de aprobación de credenciales

4.1	21/12/2022	Se agrega descripción de dato “Tipo de Público Objetivo”
4.0	19/10/2022	Se agrega obligación de uso de dominio “.gob.cl” en solicitud de credenciales
3.9	11/05/2022	Se actualiza proceso de certificación de integraciones
3.8	15/12/2021	Se actualiza información sobre implementación de logout
3.7	01/06/2021	Se actualiza proceso de solicitud e información sobre implementación logout
3.6	08/04/2021	Se agrega explicitar en userinfo/ que el identificador de la persona es el RUN
3.5	25/02/2021	Se actualiza descripción de la pregunta “quiénes pueden integrar ClaveÚnica”
3.4	29/12/2020	Se actualiza el link a la mesa de ayuda
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 proveedor de identidad digital (Identity Provider) que funciona como mecanismo de autenticación para que los ciudadanos puedan acceder a distintas plataformas y servicios del Estado utilizando una sola contraseña. ClaveÚnica es la base del Modelo de Identidad Digital en Chile.

I.2. ¿Quienes pueden integrar ClaveÚnica?

Actualmente ClaveÚnica está disponible para ser integrado sin costo en plataformas y aplicaciones web y mobile de los Organismos de la Administración del Estado.

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

De acuerdo a lo indicado en el Instructivo Presidencial de Transformación Digital, las instituciones del Estado mandatadas por el Instructivo deberán utilizar ClaveÚnica como único medio de autenticación para personas naturales.

En caso que la institución cuente con otros mecanismos es importante gestionar el cambio con los usuarios y establecer etapas y plazos en la migración a la identificación exclusiva con ClaveÚnica.

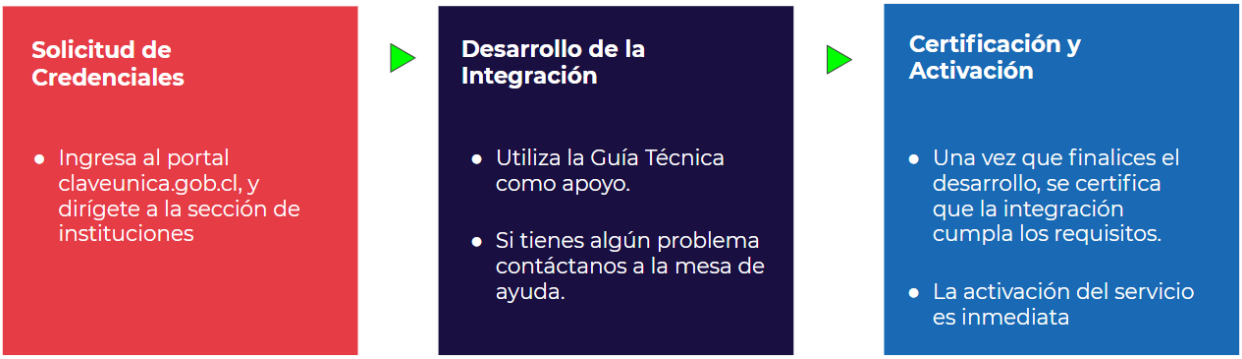
I.4. ¿Se puede integrar ClaveÚnica en trámites institucionales internos?

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 en sus plataformas internas.

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 “Instituciones Públicas” 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 Credenciales de Integración a ClaveÚnica” en el cual ingresará pinchando en “Iniciar trámite”.

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

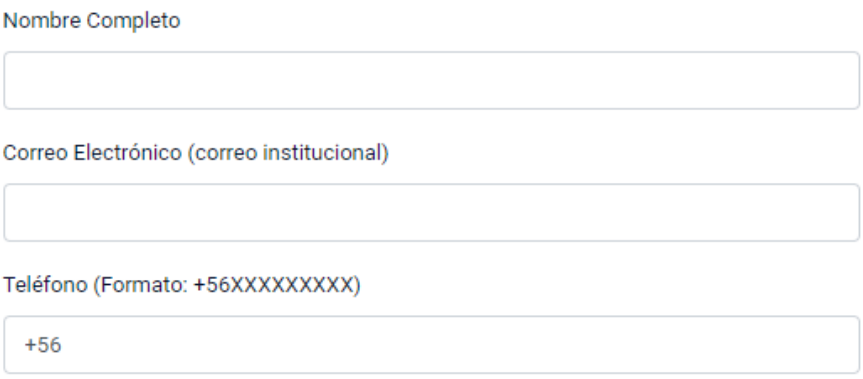
Los campos solicitados son los siguientes:

Seleccionar Institución

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

Contacto Administrativo

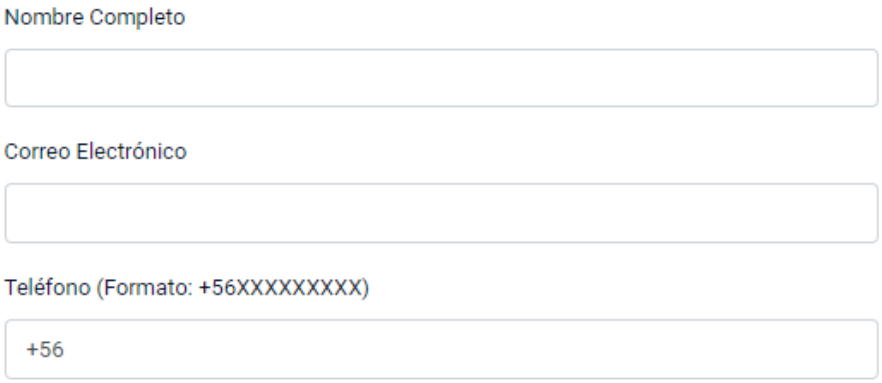
Corresponde al funcionario responsable en la institución de la plataforma que integrará ClaveÚnica, independiente si el desarrollo es ejecutado por un proveedor externo. Es obligatorio que el correo electrónico provisto sea institucional.



Contacto Técnico

Corresponde a la contraparte técnica de la plataforma que integrará ClaveÚnica. Si el desarrollo es realizado por un proveedor externo puede indicar al jefe de proyectos del proveedor, aunque debido a que el resguardo de las credenciales de integración son responsabilidad de la institución, se recomienda que el contacto técnico sea un funcionario.

El contacto puede ser la misma persona que se indicó como contacto administrativo. Es obligatorio que el correo electrónico provisto sea institucional o del dominio del proveedor si corresponde.



Nombre de la aplicación

Corresponde a lo que aparece en el formulario de login de ClaveÚnica y debe identificar claramente a la institución y a la plataforma integrada.

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

Descripción de la Aplicación

Indique el propósito de la integración, incluyendo cualquier información que considere relevante, por ejemplo si el desarrollo estará a cargo de un proveedor externo. La descripción debe ser concisa.

Tipo de Público Objetivo

Indica a quienes están orientados el uso de la aplicación. Existen dos opciones:

Público (ciudadanía): Indica que la aplicación brinda servicios a la ciudadanía en general.

Interno (Institución): Indica que la aplicación brinda servicios a los funcionarios y servicios internos de la institución integradora.

URL de la Aplicación

Indica la dirección pública con la que se accede al sitio integrado a ClaveÚnica.

En caso de que sea declarado este dato, **la URL debe tener como dominio ".gob.cl"**, según el decreto que aprueba la Norma Técnica sobre sistemas y sitios web de los órganos de la administración del estado, en su capítulo II, artículo 13

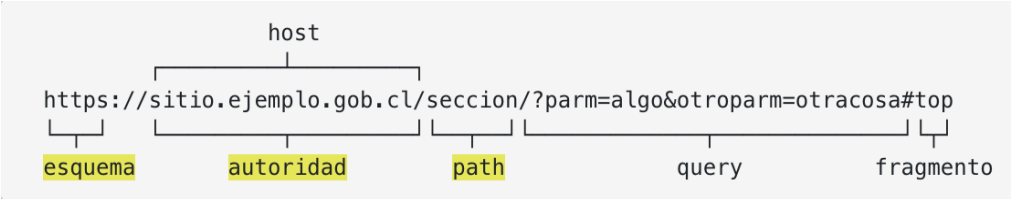
Redirect URI

También conocido como "callback", es la URL o endpoint perteneciente a la aplicación integradora a la cual ClaveÚnica redireccionará luego que un usuario se haya autenticado correctamente, recibiendo además los datos "code" y "state".

Debe ingresar un Redirect URI para su ambiente de testing, otro para su ambiente de QA y un último para su ambiente de producción obligatoriamente. Si no cuenta con la URI del ambiente productivo al momento de solicitar las credenciales puede repetir la URI del ambiente de testing y/o QA y luego solicitar el cambio a través de nuestro portal Cerofilas en el trámite 'Actualización de Redirect_URI de Credenciales de Integración ClaveÚnica'.

Cada Redirect URI debe estar compuesto solo por por los elementos esquema, autoridad y path de la dirección web. No se permite incluir elementos adicionales como la query.

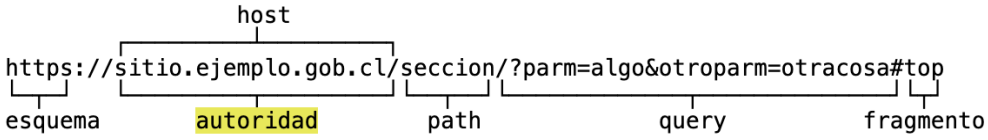
Por motivos de seguridad, no está permitido el uso de dominios LOCALHOST en los Redirect URI's.



Además, por decreto que aprueba la Norma Técnica sobre sistemas y sitios web de los órganos de la administración del estado, en su capítulo II, artículo 13, **la URI de redirección de producción debe tener como dominio ".gob.cl"**.

Logout URI

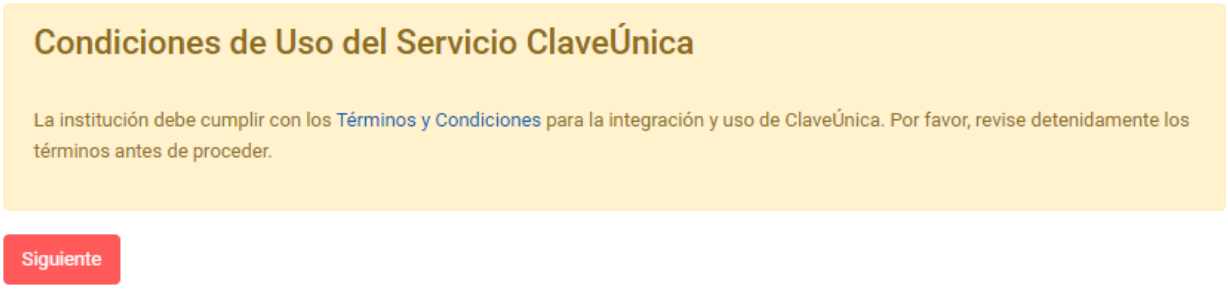
Complete este campo si su aplicación utilizará el parámetro "redirect" en el endpoint logout de ClaveÚnica. Debe indicar solamente la parte de la URI que corresponde a la autoridad. En caso que lo requiera, podrá solicitar el cambio del Logout URI a través de la Mesa de Servicio.



Este campo es opcional. Si su aplicación utiliza más de una URL utilice una coma como separador.

Términos y Condiciones

Luego de completar los campos requeridos, es obligatorio abrir y leer Términos y Condiciones para poder continuar con el proceso de solicitud.



Finalizando el proceso de Solicitud de Credenciales

Luego de enviar la solicitud se notificará el recibo de este al equipo de ClaveÚnica y se evaluará si es correcta. El tiempo de revisión es de 3 días hábiles.

Si la solicitud cumple con los requisitos, se le enviará un email a la casilla descrita en la solicitud con tres pares de credenciales compuestos por un **client_id** y un **client_secret**. Un par le servirá para su ambiente de **pruebas o sandbox**, otro par para su ambiente de **QA** y el otro para su ambiente de **producción**.

Nota: Le solicitamos por favor revisar que la casilla de notificaciones **no-reply@digital.gob.cl no se encuentre en su lista de correos no deseados.**

Estimado(a) Usuario(a)

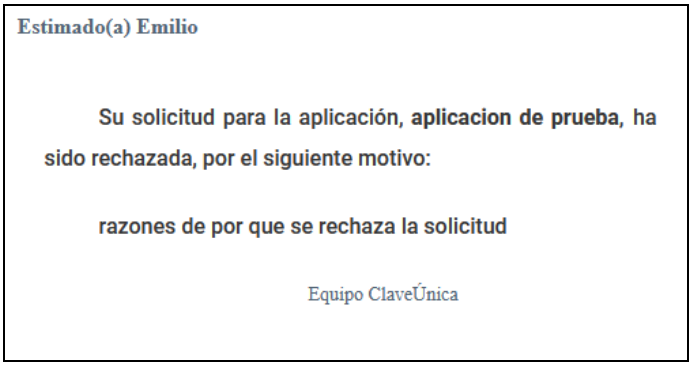
Su solicitud para la aplicación, **Nombre de Aplicación de Nombre de Institución**, ha sido aceptada. Se adjunta en un archivo comprimido las credenciales de integración a ClaveÚnica

Su número de solicitud es el siguiente: 99999999.

Para abrir el archivo comprimido y ver sus credenciales, debe ingresar una contraseña compuesta por su RUN y el número de solicitud.

Contraseña Archivo ZIP: 4444444499999999

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 hasta que su integración sea certificada.

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

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

El valor client_secret es confidencial, evite exponerlo.

El client_id es el identificador de su integración y le será solicitado para cualquier cambio o actualización que desee realizar en su integración.

Mantenga el debido control sobre las credenciales entregadas y permita su uso sólo a las personas autorizadas. El resguardo de las credenciales es responsabilidad de la institución.

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 QA

Su funcionamiento es idéntico al de las credenciales de sandbox. Configurando el client_id y client_secret de QA, accederá al mismo ambiente limitado descrito anteriormente para realizar pruebas en su integración..

Al igual que las credenciales de sandbox, solo es posible utilizar el conjunto de RUN's de prueba señalados en el punto 3.2.

Credenciales de producción

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

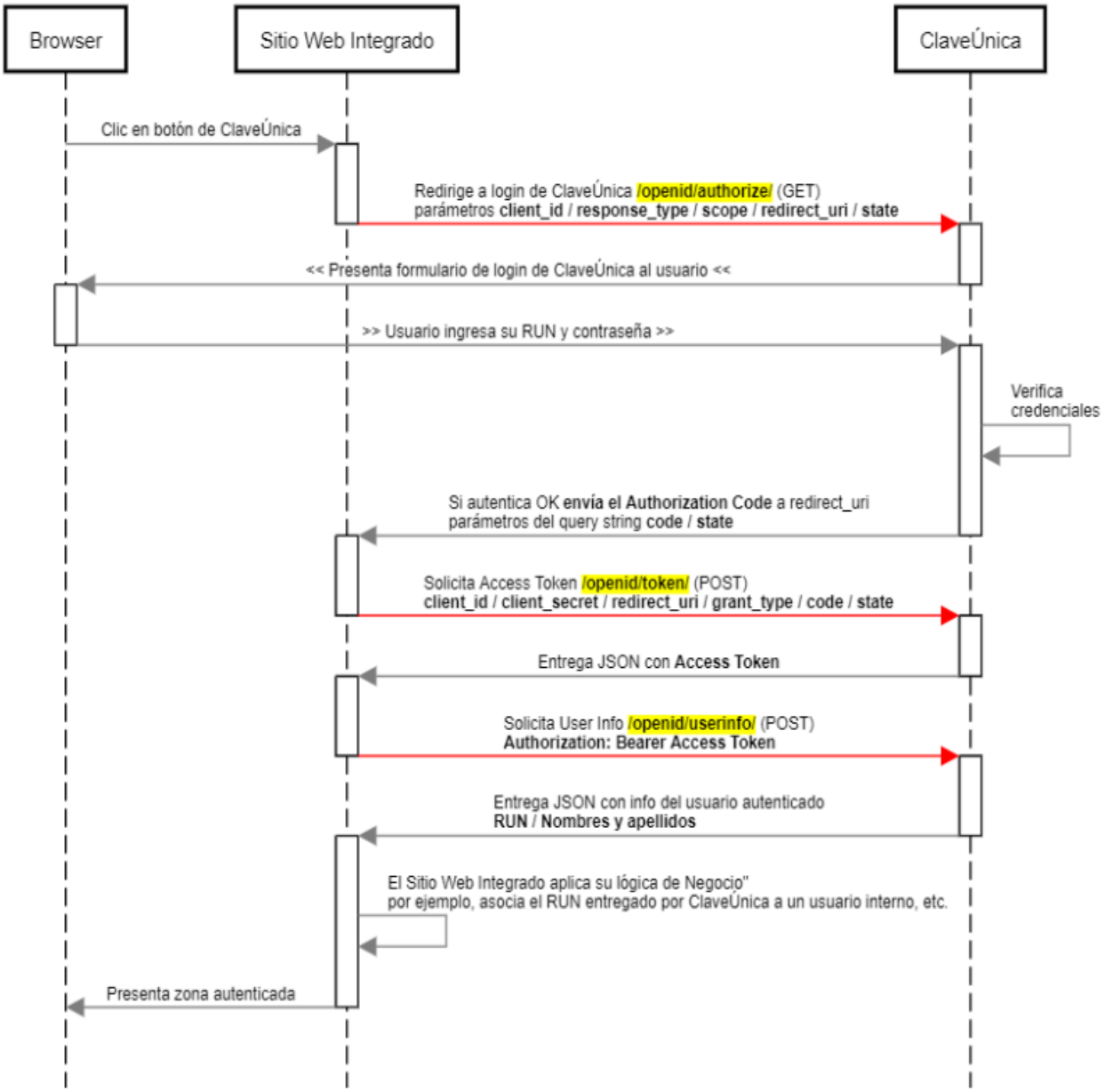
Estas credenciales están deshabilitadas por defecto. Para habilitarlas, la aplicación integrada debe cumplir los requisitos de marca y seguridad solicitados y aprobar el proceso de certificación.

3. Implementación de la Integración

ClaveÚnica utiliza el estándar OpenID Connect, que a su vez está basado en el protocolo OAuth2.0 y que permite implementar el proceso de autenticación de manera segura.

El proceso de autenticación 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 interopera ClaveÚnica como mecanismo de autenticación entre un sitio web integrado y sus usuarios.



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 se 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

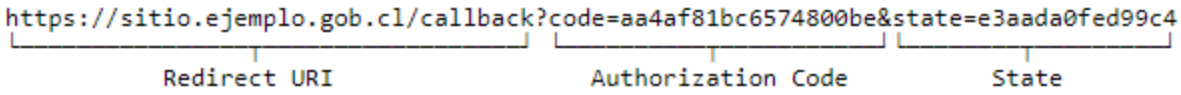
Cuando la aplicación integradora invoca a la URI compuesta por GET se levanta el formulario de inicio de sesión de ClaveÚnica

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 obtenida del paso anterior, luego de ingresar rut y contraseña en formulario de ClaveÚnica, es enviada a la dirección que se registró como **Redirect URI**, a la cual se le añaden los valores **code** y **state**.



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

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

La respuesta del paso anterior incluye el parámetro llamado **code** o código de autorización. Este es un código único de 32 caracteres que tiene un tiempo de expiración de 5 minutos y permite continuar con el proceso de autenticación solicitando el **Token de Acceso** (access token).

NOTA: Si el parámetro code expira el usuario deberá autenticarse nuevamente.

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/

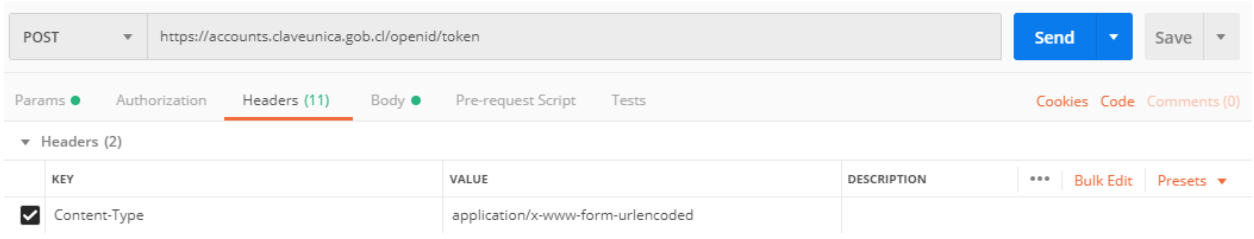
Los parámetros que deben ser enviados en el cuerpo del mensaje POST son:

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***.

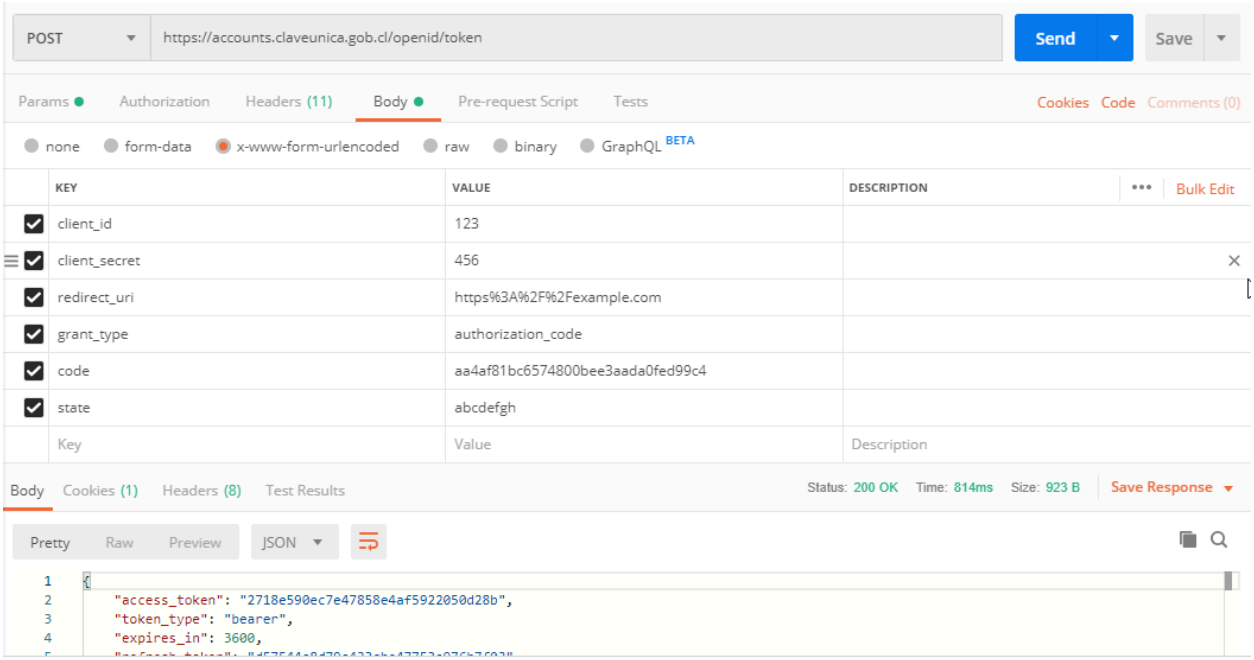
Es fundamental para la seguridad de las credenciales, que estas no se encuentren codificadas de manera fija dentro del código fuente.

Ejemplo de la llamada en Postman

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



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



Ejemplo en 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 **JSON** que contiene el **Token de Acceso** (access token) con el cual podrá obtener la información del usuario que se está autenticando.

Ejemplo del JSON retornado

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

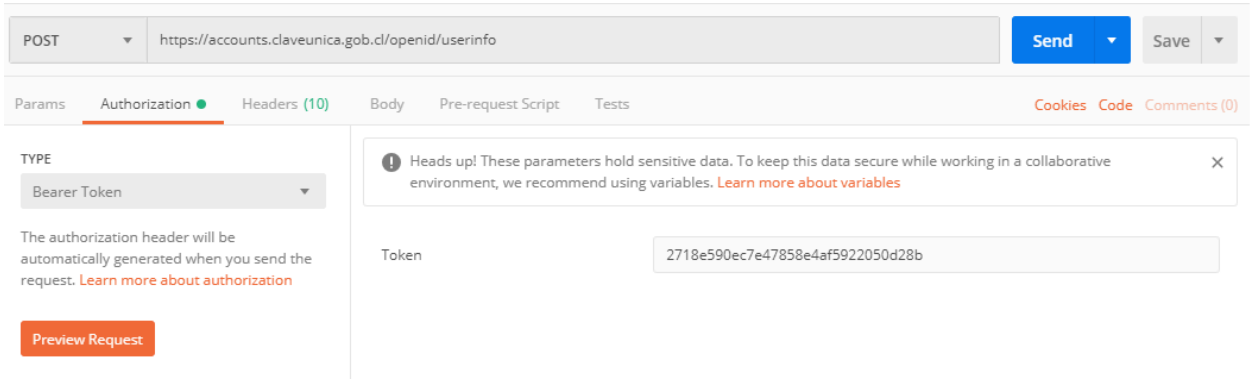
3.6. Paso 6: Obtener información de ciudadano por medio del Token de autorización

En el **Paso 5** el usuario ya se encuentra autenticado, pero su aplicación puede identificarlo solicitando su **nombre** y **RUN** con el **Token de Acceso** (access token) obtenido en el paso anterior.

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

Ejemplo en Postman

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



Ejemplo en 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"
        ]
    }
}
```

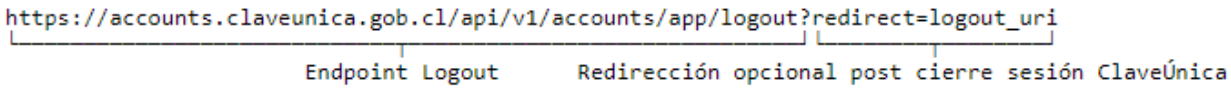

El campo sub se incluye por ser requerido dentro de la especificación OpenID Connect, sin embargo no debe utilizarse como llave del registro. El identificador de la persona que se autentica es el RUN (campo RolUnico.numero).

3.7. Paso 7: Cierre de sesión

Luego que el usuario se ha autenticado, ClaveÚnica crea su propia sesión que durará 60 segundos y en paralelo traspasa el control hacia la aplicación integradora que, a su vez, podrá crear su propia sesión y administrar su duración según sus definiciones de negocio.

Aun cuando la sesión de ClaveÚnica tiene una duración limitada para mantener su comportamiento *Single Sign On* y así facilitar la autenticación en algunos casos de uso, es necesario que la aplicación integradora siempre se encargue de cerrar la sesión de ClaveÚnica cada vez que cierre la propia, de manera preventiva.

Para cerrar la sesión de ClaveÚnica se debe utilizar el endpoint a continuación.



Casos de uso generales de cierre de sesión en ClaveÚnica: “explícito” e “implícito”.

Un cierre de sesión explícito se refiere al que se hace directamente desde el botón en la aplicación que ha sido destinado para ello, que normalmente es visible para el ciudadano cuando éste se encuentra en una zona privada del sitio.

El cierre de sesión implícito es cuando la aplicación cierra la sesión unilateralmente según sus reglas de negocio, por ejemplo luego de que el usuario se autentica y la aplicación integrada no lo reconoce como uno de sus usuarios.

Existe otro tipo de cierre de sesión implícito que se hace inmediatamente al finalizar el flujo OpenID Connect, luego de obtener los datos del usuario a través del endpoint UserInfo. Este caso de uso corresponde normalmente a procesos donde se utiliza ClaveÚnica como medio para firmar documentos electrónicos o procesos lineales, como encuestas, que por definición no tienen un botón de cierre de sesión disponible y solo requieren validar la identidad al principio.

La llamada al endpoint Logout es vía **GET** y se debe evitar el uso de llamadas por popups o iframes, ya que esto provoca un error de CORS, lo que conlleva a que la sesión de ClaveÚnica quede abierta.

La URI que va en el parámetro “redirect” es opcional pero se recomienda utilizarla, ya que complementa el proceso de cierre de sesión en general, redirigiendo a una página para cerrar la sesión de la aplicación integradora inmediatamente después de haber cerrado la sesión de ClaveÚnica, por ejemplo.

Las URI de logout pueden ser varias y deben registrarse al momento de solicitar las credenciales y pueden cambiarse ingresando una solicitud en la Mesa de Servicio.

Si se llama al endpoint utilizando una URI no registrada el redireccionamiento no se realizará.

Métodos de logout a utilizar:

Método 1:

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

Método 2:

```
function Logout() {
    // llamada al endpoint de logout
    window.location.href = "https://accounts.claveunica.gob.cl/api/v1/accounts/app/logout";
    // redireccion al cabo de 1 segundo a un handler de logout en la aplicación integradora
    setTimeout(function () {
      window.location.href = “logout_uri”;
    }, 1000);
  }
```

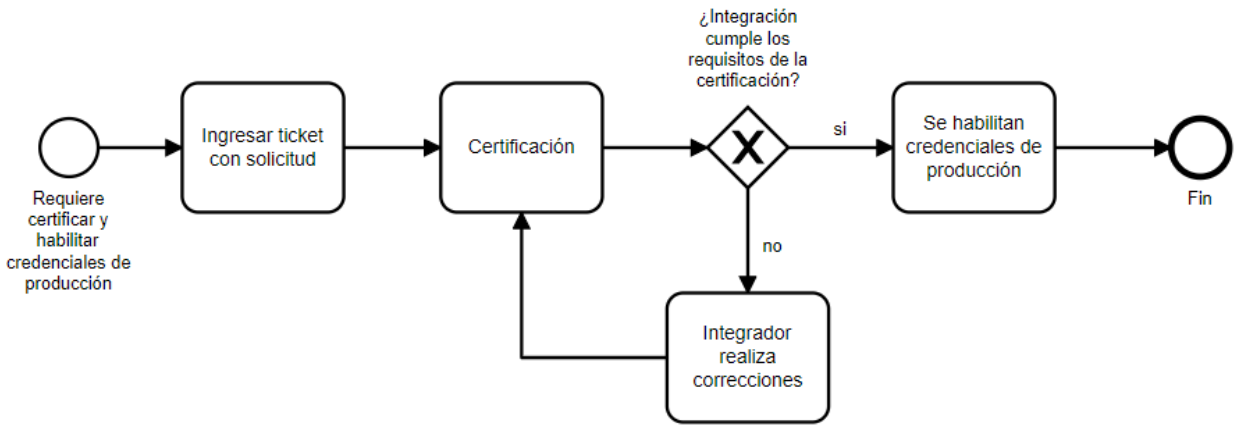
4. Certificación y Activación de Credenciales de Producción

Certificación y activación de credenciales de producción

Toda prueba y desarrollo que se realice para la implementación de ClaveÚnica se lleva a cabo utilizando las credenciales de sandbox y QA. Las credenciales de producción se encuentran desactivadas.
Una manera de corroborar que estas credenciales están desactivadas es un mensaje que se muestra en el login de ClaveÚnica cuando se intenta iniciar sesión.

El mensaje "**La institución no está habilitada en ClaveÚnica**" indica que las credenciales deben activarse para ser utilizadas, por lo que una vez que se ha desarrollado la integración según lo indicado en esta Guía Técnica, se 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.



4.1. Requisitos de la certificación

✅ **Uso del botón oficial de ClaveÚnica**

Utilizar el botón oficial garantiza que los ciudadanos puedan identificar de manera inequívoca cuándo un trámite se efectúa a través de ClaveÚnica. A continuación, se presentan los botones oficiales.

Para su correcta implementación, siga los lineamientos oficiales.

Desde Figma puede exportar los elementos.

También puede revisar nuestros ejemplos en código.

Para complementar la nueva guía técnica, les recomendamos visualizar el siguiente video.

✅ **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. Al llamar al formulario, la barra de direcciones no debe quedar oculta.

✅ State dinámico

Se verificará que el parámetro state sea generado dinámicamente según lo indicado en el paso 1 de la integración con el servicio.

✅ Que la aplicación realice la llamada al servicio correctamente

Para asegurar un buen funcionamiento, aplicación debe llamar al servicio correctamente, esto implica a) realizar la secuencia completa de autenticación según lo indicado en esta guía (OpenID Connect); b) utilizar el scope "openid run name" y c) que todos los endpoints que se utilizan para consumir el servicio empiecen con **accounts.claveunica.gob.cl**.

✅ Llamadas al servicio desde el backend

Se solicitará evidencia de las llamadas a los endpoints token/ y userinfo/ desde el backend de la aplicación, los cuales deberán llamar correctamente al servicio. La evidencia puede ser un print de pantalla que muestre el bloque de código donde está registrada la llamada. **La evidencia debe mostrar la URL que se está utilizando para llamar a ambos endpoints sea https://accounts.claveunica.gob.cl/openid/token/ y https://accounts.claveunica.gob.cl/openid/userinfo/, respectivamente.**

Ejemplo de evidencia endpoint token/

```php
$body = array(
    "client_id" => $client_id_sandbox,
    "client_secret" => $client_secret_sandbox,
    "redirect_uri" => urlencode($uri_de_retorno),
    "grant_type" => "authorization_code",
    "code" => $respuesta,
    "scope" => $_SESSION['token']
);

$response = wp_remote_post( 'https://accounts.claveunica.gob.cl/openid/token' , array(
    'headers'     => array('Content-Type' => 'application/x-www-form-urlencoded; charset=utf-8'),
    'body'        => http_build_query($body),
    'method'      => 'POST'
) );

$res = wp_remote_retrieve_body($response);

$res = json_decode($res);
$access = $res->access_token;



if ( is_wp_error( $response ) ) {
    $error_message = $response->get_error_message();
} else {
}
```

Ejemplo de evidencia endpoint userinfo/

```php
function endpoint_userinfo($token) {

    $response = wp_remote_post( 'https://accounts.claveunica.gob.cl/openid/userinfo/', array(
        'headers'     => array('Content-Type' => 'application/json; charset=utf-8', 'Authorization' => 'Bearer ' . $token),
        'method'      => 'POST'
    ) );

    $res = wp_remote_retrieve_body($response);
    $data = json_decode($res);



    if ( is_wp_error( $response ) ) {
        $result = 'false wp_error';
    } else {
        $result = $response;
    }
```

✅ Client_id y Client_secret ocultos

Para garantizar la seguridad de las credenciales de integración y evitar su exposición, es obligatorio no almacenar estas credenciales directamente en el código fuente. En su lugar, deben ser gestionadas a través de variables de entorno o mediante otros métodos de almacenamiento seguro recomendados.

Se requerirá que se proporcione evidencia visual que demuestre cómo se han implementado las variables de entorno y los métodos en los cuales se consumen dichas variables.

Ejemplo credenciales en variables de entorno

```
<add key="client_id" value="aBcDeF1234" />
<add key="client_secret" value="aBcDeF1234" />
```

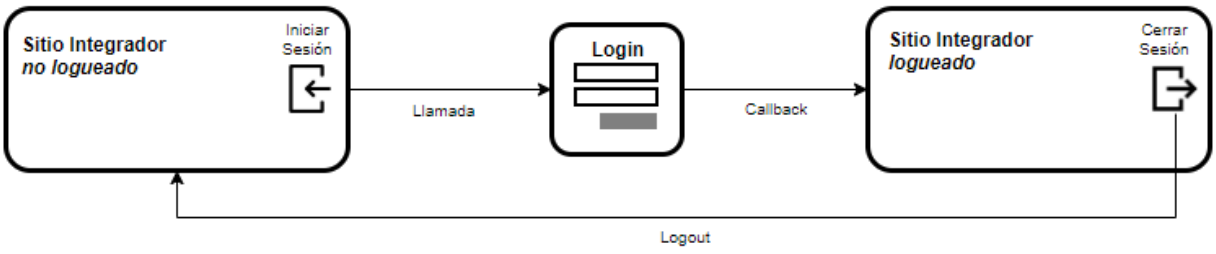
Ejemplo métodos donde se utiliza las variables de entorno

```
public string client_id = AppConfiguration.ClientID;
public string client_secret = AppConfiguration.ClientSecret;

public ActionResult SignInCallback(string code, string state)
{
    using (var client = new HttpClient())
    {
        var urlToken = AppConfiguration.TokenEndpoint;
        var request = System.Web.HttpContext.Current.Request;
        var appUrl = HttpRuntime.AppDomainAppVirtualPath;
        if (appUrl != "/") appUrl = "/" + appUrl;
        var returnUrl = System.Web.HttpContext.Current.Server.UrlEncode(redirect_uri);
        var content = new FormUrlEncodedContent(new[]
        {
            new KeyValuePair<string, string>("client_id", client_id),
            new KeyValuePair<string, string>("client_secret", client_secret),
            new KeyValuePair<string, string>("redirect_uri", returnUrl),
            new KeyValuePair<string, string>("grant_type", "authorization_code"),
            new KeyValuePair<string, string>("code", code),
            new KeyValuePair<string, string>("state", state),
        });

        HttpRequestMessage requestMessage = new HttpRequestMessage(HttpMethod.Post, urlToken)
        {
            Content = content
        };

        var tokenResponse = client.SendAsync(requestMessage);
```

✅ Cierre de sesión

Verificaremos que el cierre de sesión se ejecute correctamente. Esto quiere decir que el sitio integrador debe contar con un link o un botón claramente identificado para cerrar la sesión. Para manejar otros casos de uso también se debe llamar al endpoint, por ejemplo cuando un RUN autenticado no se encuentra en la base de datos del sitio integrador.

Se comprobará la llamada al endpoint cerrando e intentando iniciar la sesión nuevamente.

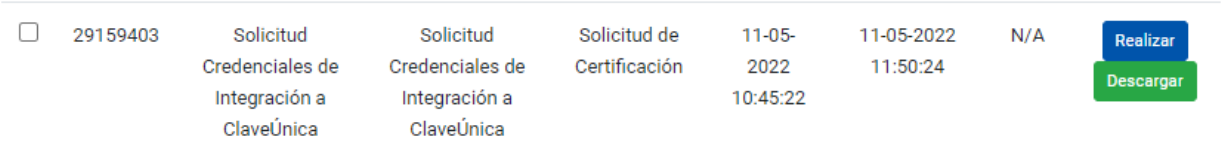


4.2. Solicitud de Certificación / Activación de Credenciales de Producción

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 el trámite de solicitud de credenciales creado con anterioridad en la plataforma Cerofilas, continuando el proceso posterior a la entrega de las credenciales de integración:

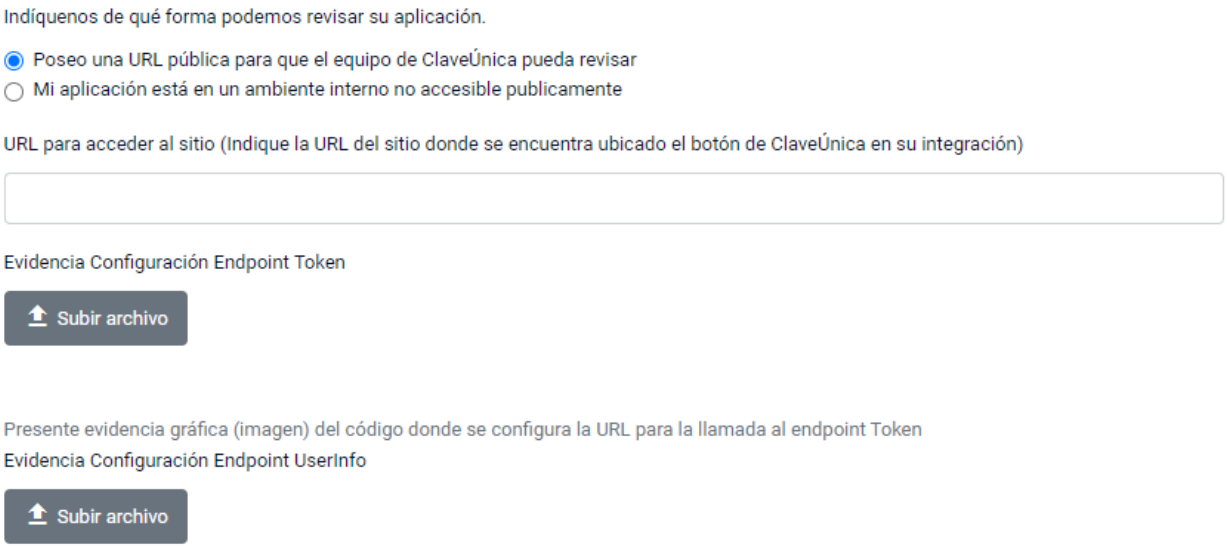
- Una vez evaluada la solicitud de credenciales y aceptada, la plataforma regresará la solicitud a la bandeja de entrada del usuario solicitante para realizar la solicitud de certificación.



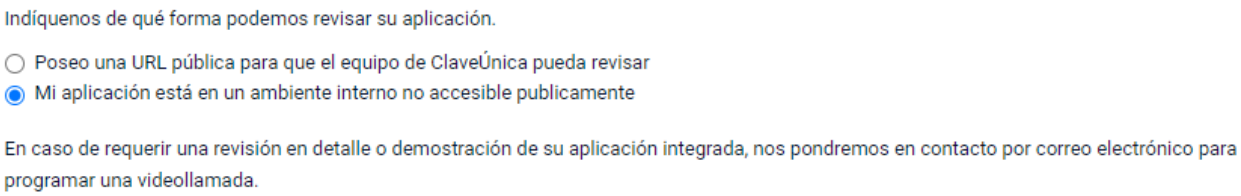
☐	29159403	Solicitud Credenciales de Integración a ClaveÚnica	Solicitud Credenciales de Integración a ClaveÚnica	Solicitud de Certificación	11-05-2022 10:45:22	11-05-2022 11:50:24	N/A	Realizar Descargar

- Ya ingresado en el formulario de solicitud de certificación, en la sección "Datos para la revisión práctica" debe verificar si el client_id indicado corresponde a las credenciales de producción generadas anteriormente.

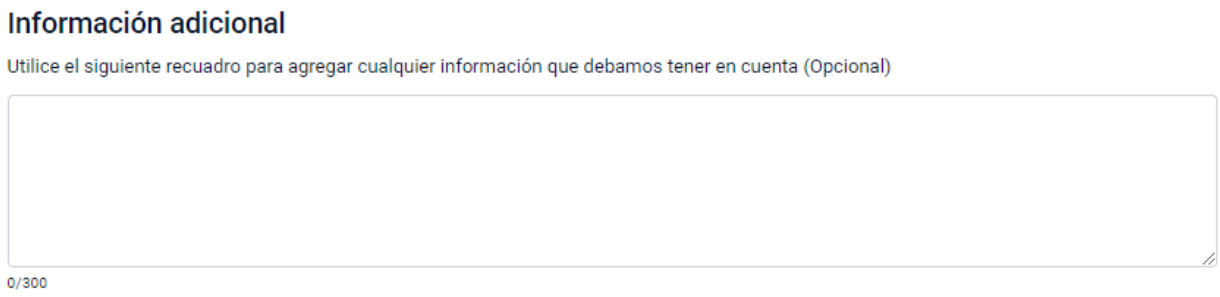
- También debe indicar el método de revisión de la integración. Existe dos opciones a seleccionar:
  - ☐ Indicando que cuenta con el sitio a certificar público en la internet y señalar la URL del sitio donde se encuentra el botón de ClaveÚnica. También adjuntando evidencia en imágenes de la configuración en código de las llamadas a los endpoint token y userinfo



- ☐ Indicando que la aplicación a certificar existe en un ambiente no accesible públicamente. Si esta opción es seleccionada, el equipo de ClaveÚnica se contactará vía email para agendar una videoconferencia para certificar dicha aplicación.



- Finalmente, puede agregar información adicional que considere útil para apoyar la certificación.



Notas sobre la revisión para certificar integraciones

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 ambiente productivo no está publicado aún, el integrador deberá proveer un acceso a un ambiente Pre-Productivo/QA publicado en la internet, 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 la solicitud para coordinar una certificación mediante una videollamada.

4.3. Tiempos estimados del procedimiento de certificación

El tiempo estimado para que el equipo de ClaveÚnica realice la certificación de una integración es de 6 días hábiles a partir de la fecha y hora de ingreso del ticket de solicitud en la Mesa de Servicio. 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 posible.

4.4. ¿Cómo actualizar el Redirect URI u otro dato de la integración?

Es probable que, durante el desarrollo de su integración y antes de pasar a producción, o incluso ya estando en producción, necesite actualizar algunos parámetros, como la Redirect URI, el nombre de la aplicación, entre otros.

Para Actualizar las URIs, debe ingresar a nuestro portal Cerofilas y hacer la solicitud en el trámite "Actualización de URIs de Credenciales de Integración ClaveÚnica".

En los antecedentes de la solicitud ingrese lo siguiente:

- **Datos del solicitante**:
  - Nombre y correo electrónico del solicitante
  - Client_id del ambiente de URI que desea actualizar

- **URI callback y/o logout** por el cual desea realizar el cambio.

Para actualizar el nombre de la aplicación, debe solicitarlo a través de un ticket en la Mesa de Servicio.

Es importante destacar que estos cambios sólo pueden ser solicitados por el contacto administrativo registrado en las credenciales.

El tiempo de respuesta de esta solicitud es de 3 días hábiles.

4.5. 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 Servicio institucional SGD y el portal de trámites Cerofilas de Gobierno Digital 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

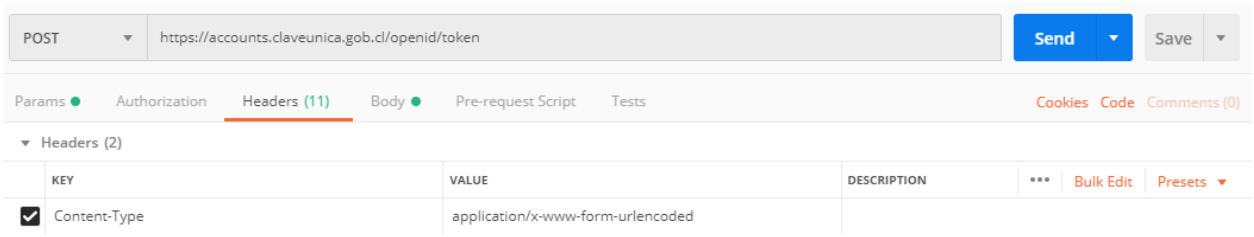
Sección: Headers

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

Llamada: POST

Key: Content-Type

Value: application/x-www-form-urlencoded



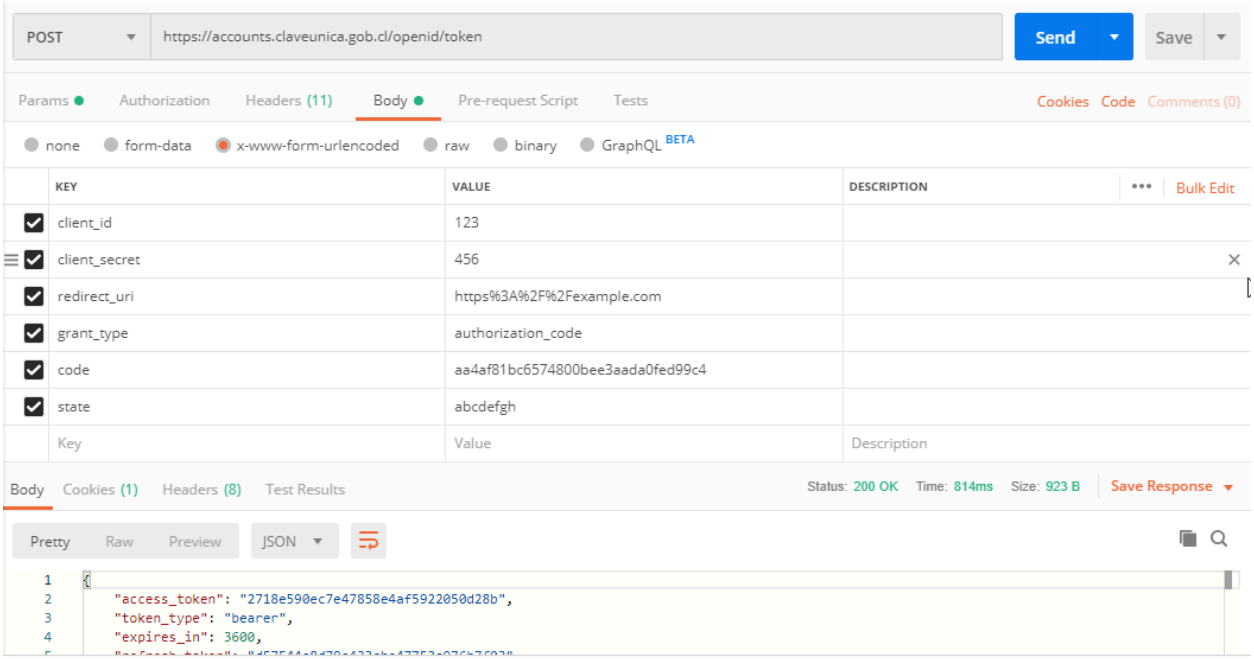
Sección: Body

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

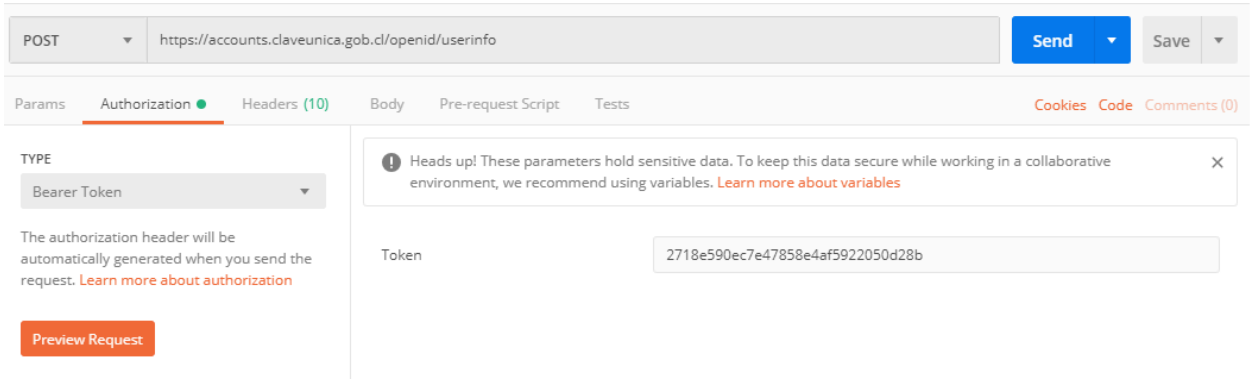


Endpoint para Datos de Usuario

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
- Postman
- HTML y CSS del Botón Oficial

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

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.

6. Canales de comunicación

Los canales de comunicación oficiales son Mesa de Servicio y el correo electrónico claveunica@digital.gob.cl.

7. Capacitaciones mensuales

En nuestro compromiso por facilitar la integración efectiva del servicio de ClaveÚnica, ofrecemos sesiones de capacitación mensuales. Estas capacitaciones están diseñadas para ayudar a las instituciones en el proceso de implementación.
Para inscribirte, debes acceder al portal Cerofilas en el trámite **'Inscripción a capacitaciones de productos de Gobierno Digital'.**