ESTRATEGIA TRANSFORMACIÓN DIGITAL

IDENTIDAD DIGITAL

MANUAL DE INTEGRACIÓN

PROTOCOLO DE CONEXIÓN A REPOSITORIO DE FIRMAS

firma.gob

Confianza y eficiencia en la gestión de documentos

Versión 13 | Noviembre 2021

gob digital CHILE

Ministerio Secretaría General de la Presidencia

Gobierno de Chile

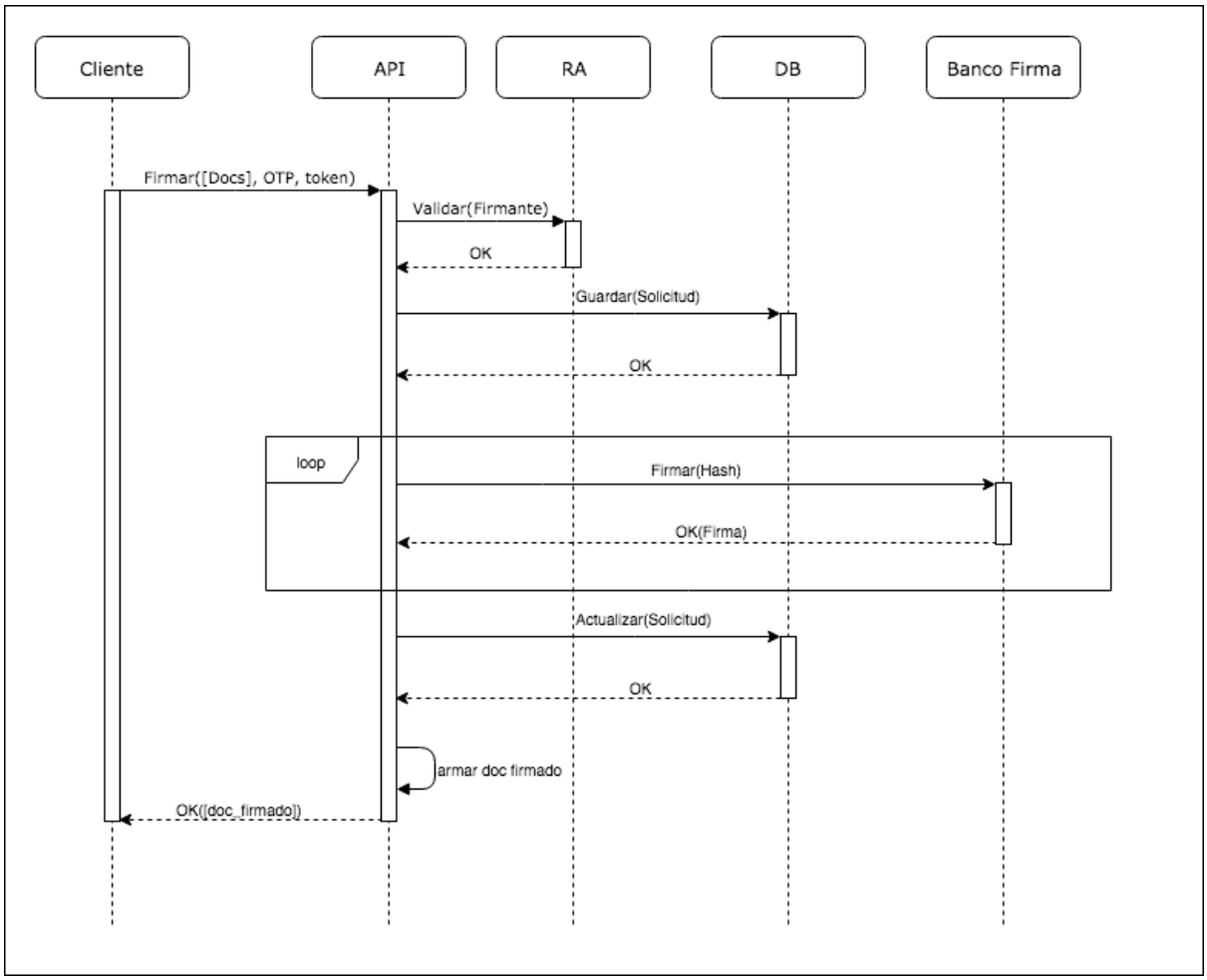
Índice

1. Introducción

Este documento contiene la documentación de los mecanismos para que aplicaciones desarrolladas por las instituciones puedan realizar procesos de firma de documentos utilizando las firmas electrónicas avanzadas de autoridades o funcionarios custodiadas en el Repositorio Centralizado de Firmas.

2. Diagrama de secuencia

A continuación se presenta el diagrama correspondiente a las acciones a realizar con el objetivo de obtener uno o más documentos firmados.



- **Cliente:** Aplicación cliente que requiere firmar uno o más documentos.
- **API Firma:** Interfaz entre las aplicaciones externas (clientes) y las operaciones asociadas a la firma de uno o más documentos.
- **RA (Autoridad de Registro):** Contiene el registro de las aplicaciones externas habilitadas para realizar operaciones de firma. Las aplicaciones deben estar previamente registradas y cumplir con un conjunto de restricciones asociadas a la identificación del certificado de firma electrónica avanzada a utilizar (***entidad***, ***propósito*** y ***run*** del titular de la firma).

- **Banco**: Repositorio donde se custodian los certificados de firma electrónica avanzada habilitados para realizar operaciones de firma. El banco recibe los documentos a firmar y realiza la operación de firma, nunca un certificado será expuesto.

Firmar Documento

Con esta llamada, se puede firmar documentos PDF, XML o hash, utilizando un certificado de firma electrónica avanzada de propósito general (atendido) o desatendido.

Para utilizar su firma desatendida, previamente tendrá que haber solicitado su certificado por el "Sistema de Solicitud de Firma Electrónica" y habilitado la aplicación correspondiente.

En el caso de firmar un PDF, el proceso tomará más tiempo ya que se requiere manipular el documento para incrustar la firma. La recomendación es firmar un hash, pero es necesario que la aplicación cliente reconstruya el documento. Si necesita ayuda con la firma de hash póngase en contacto con soporte.

Protocolo: HTTPS

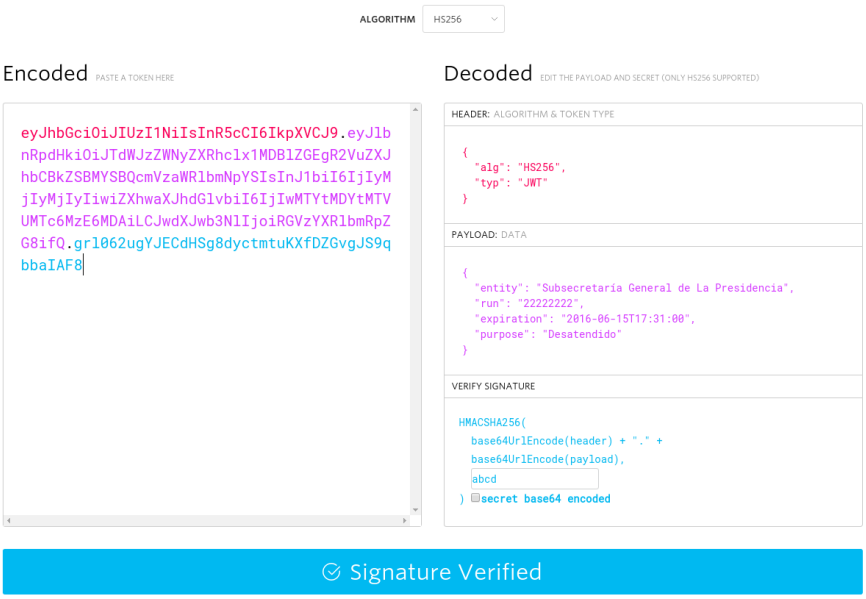
URL: https://api.firma.cert.digital.gob.cl/firma/v2/***files/tickets'***, *método* = *['POST']*

HTTP Headers

OTP: <Valor OTP> (Esta cabecera sólo es necesaria para la firma atendida, en caso de ser firma desatendida, no se debe enviar esta cabecera).

HTTP Parámetros

token	Campo encriptado y firmado en JWT con una clave simétrica, esta clave es obtenida a partir del registro de la aplicación. El campo JWT encriptado en algoritmo HS256 y firmado con clave simétrica contiene los siguientes campos: 1. **run:** run identificador del titular de firma, no debe contener puntos, guión ni tampoco el dígito verificador (string). 2. **entity:** código asociado a la institución a la cual pertenece el titular (string) 3. **purpose:** código asociado al tipo de certificado a utilizar (string) 4. **expiration:** fecha expiración del token en hora chilena formato ISODate (YYYY-MM-DDTHH:MM:SS). No puede ser mayor a 30

<table>
<tr><td></td><td>minutos del momento actual.
 
</td></tr>
<tr><td>api_token_key</td><td>Campo no encriptado de tipo string que contiene el código único generado a partir del registro de la aplicación.</td></tr>
<tr><td>files</td><td>Array no encriptado que contiene información de él o los documentos sobre los cuales se realizarán operaciones de firma.
Cada objeto del array según el formato de archivo a firmar debe contener:

<table>
<tr><th>JSON</th><th>PDF</th><th>XML</th></tr>
<tr><td>description</td><td>description</td><td>description</td></tr>
<tr><td>checksum</td><td>checksum</td><td>checksum</td></tr>
<tr><td>content</td><td>content</td><td>content</td></tr>
<tr><td>content-type</td><td>content-type</td><td>content-type</td></tr>
<tr><td></td><td>layout (opcional ver Anexo B)</td><td>references</td></tr>
<tr><td></td><td></td><td>xmlObjects</td></tr>
</table>

A continuación se describe el tipo de dato asociado al parámetro requerido:
1. description: string con la descripción del archivo
2. checksum: SHA256 del archivo
3. content: archivo en base64
4. content-type: dependiendo del archivo a firmar
i. application/pdf</td></tr>
</table>

	ii. application/xml iii. application/json 5. **layout**: string opcional en caso de desear incrustar elemento al archivo PDF 6. **references**: array de string con la identificación del nodo a firmar en caso de ser un archivo XML ejemplo: ["#nodo1", "#nodo2"] 7. **xmlObjects**: array de string con los pie de firma en un archivo XML ejemplo: ["<a>","<b/>"]

A continuación se presentan ejemplos de los parámetros:

token	***"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbnRpdHkiOiJTdWJzZWNyZXRhcsOtYSBHZW5lcmFsIGRlIGxhIFByZXNpZGVuY2lhIiwicnVuIjoiMjIyMjIyMjIiLCJleHBpcmF0aW9uIjoiMjAyMS0xMS0xNVQxNzozMTowMCIsInB1cnBvc2UiOiJEZXNhdGVuZGlkbyJ9.EqcNFArqasx_hlZSYTO2Tnuqa36dMn_qnmk90XEyhTA"*** ***Algoritmo: HS256, Secreto: 27a216342c744f89b7b82fa290519ba0*** ***{*** ***"entity": "Subsecretaría General de la Presidencia",*** ***"run": "22222222",*** ***"expiration": "2021-11-15T17:31:00",*** ***"purpose": "Desatendido"*** ***}***
api_token_key	***sandbox***
files	***[*** ***{*** ***"content-type": "application/pdf",*** ***"content": "archivo en base64",*** ***"description": "str",*** ***"checksum": "hash en sha256"*** ***}*** ***]***

Ejemplo del JSON BODY para firmar un documento PDF:

{

"api_token_key": "sandbox",

"token":

"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbnRpdHkiOiJTdWJzZWNyZXRhcsOtYSBHZW5lcmFsIGRlIGxhIFByZXNpZGVuY2lhIiwicnVuIjoiMjIyMjIyMjIiLCJleHBpcmF0aW9uIjoiMjAyMS0xMS0xNV

QxNzozMTowMCIsInB1cnBvc2UiOiJEZXNhdGVuZGlkbyJ9.EqcNFArqasx_hlZSYTO2Tnuqa36dMn_qnmk90XEyhTA",

```
 "files": [
   {
     "content-type": "application/pdf",
     "content": "archivo en base64",
     "description": "str",
     "checksum": "hash en sha256"
   }
 ]
}
```

Ejemplo del JSON BODY para el caso de hash

- Para obtener el content a firmar, se deben parsear el PDF según las indicaciones:
    - https://www.adobe.com/devnet-docs/etk_deprecated/tools/DigSig/Acrobat_DigitalSignatures_in_PDF.pdf
- Al firmar un hash, se debe tener en consideración que se debe agregar el content de respuesta (mensaje firmado en formato p7s) al diccionario de firma del PDF. Para hacer esto se recomienda el uso de la librería iText de Java o C#

[

"api_token_key": "sandbox",

"token":

"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbnRpdHkiOiJTdWJzZWNyZXRhcsOtYSBHZW5lcmFsIGRlIGxhIFByZXNpZGVuY2lhIiwicnVuIjoiMjIyMjIyMjIiLCJleHBpcmF0aW9uIjoiMjAyMS0xMS0xNVQxNzozMTowMCIsInB1cnBvc2UiOiJEZXNhdGVuZGlkbyJ9.EqcNFArqasx_hlZSYTO2Tnuqa36dMn_qnmk90XEyhTA",

```
 "hashes": [
          {
                    "content-type": "application/pdf",
                   "content": "hash_to_sign in base64"
          }
```

Ejemplo del JSON BODY para el caso de XML

- El content será el base64 del XML a firmar
- Se puede agregar información del firmante con el parámetro “xmlObject”. Quedará en el tag Object dentro de la firma con id “CustomObject_XXX”
- Se puede agregar las referencias a firmar con el parámetro “references” tipo Lista
- La respuesta será tendrá dentro del contant un XML firmado encodeado en base64

{

"api_token_key": "sandbox",

"token":

"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbnRpdHkiOiJTdWJzZWNyZXRhcsOtYSBHZW5lcmFsIGRlIGxhIFByZXNpZGVuY2lhIiwicnVuIjoiMjIyMjIyMjIiLCJleHBpcmF0aW9uIjoiMjAyMS0xMS0xNVQxNzozMTowMCIsInB1cnBvc2UiOiJEZXNhdGVuZGlkbyJ9.EqcNFArqasx_hlZSYTO2Tnuqa36dMn_qnmk90XEyhTA",

"files": [

{

"content-type": "application/xml",

"content":

"PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48P3htbC1zdHlsZXNoZWV0IHR5cGU9InRleHQveHNsIiBocmVmPSJodHRwOi8vbG9jYWxob3N0OjgwODAvdmFsaWRhZG9jL3hzbC92NC9yZXNfZGVjLnhzbHQiPz4NCjxEb2N1bWVudG8geG1sbnM9Imh0dHA6Ly93d3cuY29udHJhbG9yaWEuY2wvMjAwNS8wNS9DR1JEb2MiIHhtbG5zOnhzaT0iaHR0cDovL2xvY2FsaG9zdDo4MDgwL3ZhbGlkYWRvYy8iIHZlcnNpb249IjEuMCIgeHNpOnNjaGVtYUxvY2F0aW9uPSJodHRwOi8vd3d3LmNvbnRyYWxvcmlhLmNsLzIwMDUvMDUvQ0dSG9jIGh0dHA6Ly93d3cuY29udHJhbG9yaWEuY2wvZG9jcy9yZWN1cnNvcy9Fc3F1ZW1hQ0dSX3YyLjIuMS54c2QiPjxDb250ZW5pZG8gSUQ9IjE2MzExIiBjb2RpZ289IjQiPjxGb2xpbz48TnVtZXJvPjk1PC9OdW1lcm8+PEFnbm8+MjAyMDwvQWdubz48L0ZvbGlvPjxSZXNvbHVjaW9uIHZlcnNpb249IjEuMCI+PENoZWNrc3VtPjwvQ2hlY2tzdW0+PC9SZXNvbHVjaW9uPjxEb2pZXJubyBkZSBDaGlsZTwvR2xvc2FMaW5lYT48R2xvc2FMaW5lYT5NaW5pc3RlcmlvIGRlbCBJbnRlcmlvciBEZXBhcnRhbWVudG8gZGUgU2FsdWQ9IjE2MzExIiBjb2RpZ289IjQiPjxGb2xpbz48TnVtZXJvPjk1PC9OdW1lcm8+PEFnbm8+MjAyMDwvQWdubz48L0ZvbGlvPjxSZXNvbHVjaW9uIHZlcnNpb249IjEuMCI+PENoZWNrc3VtPjwvQ2hlY2tzdW0+PC9SZXNvbHVjaW9uPjxEb2pZXJubyBkZSBDaGlsZTwvR2xvc2FMaW5lYT48R2xvc2FMaW5lYT5NaW5pc3RlcmlvIGRlbCBJbnRlcmlvciBEZXBhcnRhbWVudG8gZGUgU2FsdWQ=

WNyZXRhcsOtYSBkZWwgSW50ZXJpb3I8L0dsb3NhTGluZWE+PEdsb3NhTGluZWE+RGl2aXNpw
7NuIGRlIFJlZGVzIHkgU2VndXJpZGFkIEluZm9ybcOhdGljYTwvR2xvc2FMaW5lYT48L05vbUluc3R
pdHVjaW9uPjwvRW1pc29yPjxMdWdhcj5TYW50aWFnbzwvTHVnYXI+PEZlY2hhPjIwMjAtMDUtMT
M8L0ZlY2hhPjxXaXN0bz48UGFycmFmbyBudW1lcm89IjEiLz48L1Zpc3RvPjxDb25zaWRlcmFuZ
G8+PFBhcnJhZm8gbnVtZXJvPSIxIi8+PC9Db25zaWRlcmFuZG8+PFRlbmllbmRvUHJlc2VudGU+P
FBhcnJhZm8gbnVtZXJvPSIxIi8+PC9UZW5pZW5kb1ByZXNlbnRlPjxzaWdlOkRvY3VtZW50byB4b
WxuczpzaWdlPSJodHRwOi8vd3d3LmludGVyaW9yLmdvYi5jbC8yMDEzLzA2L1NpZ2UiIHVybERv
Yz0iaHR0cDovL2xvY2FsaG9zdDo4MDgwL3ZhbGlkYWRvY y8iIHZlcnNpb249IjEuMCIgeHNpOnNj
aGVtYUxvY2F0aW9uPSJodHRwOi8vd3d3LmludGVyaW9yLmdvYi5jbC8yMDEzLzA2L1NpZ2Uga
HR0cDovL3ZhbGlkYWRvY y5pbnRlcmlvci5nb2luY2wveHNkL0VzcXVlbWFJTlRFUklPUl92MS4xLn
hzZCI+PHNpZ2U6Q29udGVuaWRvIElEPSIxNjMxMS1zaWdlIiBjb2RpZ289IjQiPjxzaWdlOlJlc29sd
WNpb24gdmVyc2lvbj0iMS4wIj48c2lnZTpDdGxQcmV2TGVnPkVYRU5UTzwvc2lnZTpDdGxQcmV2
TGVnPjxzaWdlOk5pdmVsQ29uZmlkPlBVQkxJQ088L3NpZ2U6Tml2ZWxDb25maWQ+PHNpZ2U
6RmVjaGE+MjAyMC0wNS0xMzwvc2lnZTpGZWNoYT48c2lnZTpWaXN0bz48IVtDREFUQVs8cD5
Mb3JlbSBpcHN1bSBkb2xvciBzaXQgYW1ldCwgY29uc2VjdGV0dWVyIGFkaXBpc2NpbmcgZWxp
dC4gQWVuZWFuIGNvbW1vZG8gbGlndWxhIGVnZXQgZG9sb3IuIEFlbmVhbiBtYXNzYS4gQ3VtIH
NvY2lpcyBuYXRvcXVlIHBlbmF0aWJ1cyBldCBtYWduaXMgZGlzIHBhcnR1cmllbnQgbW9udGVzL
CBuYXNjZXR1ciByaWRpY3VsdXMgbXVzLiBEb25lYyBxdWFtIGZlbGlzLCB1bHRyaWNpZXMgbmVj
LCBwZWxsZW50ZXNxdWUgZXUsIHByZXRpdW0gcXVpcywgc2VtLiBODWxsYSBjb25zZXF1YXQ
gbWFzc2EgcXVpcyBlbmltLiBEb25lYyBwZWRlIGp1c3RvLCBmcmluZ2lsbGEgdmVsLCBhbGxxdW
VoIG5lYywgdnVscHV0YXRlIGVnZXQsIGFyY3UuIEluIGVuaW0oganVzdG8sIHJob25jdXMgdXQsIGltc
GVyZGlldCBhLCB2ZW5lbmF0aXMgdml0YWUsIGp1c3RvLiBODWxsYW0gZGljdHVtIGZlbGlzIGV1I
HBlZGUgbW9sbGlzIHByZXRpdW0uIEludGVnZXIgdGluY2lkdW50LjwvcD5dXT48L3NpZ2U6Vmlz
dG8+PHNpZ2U6Q29uc2lkZXJhbmRvPjwhW0NEQVRBWzxwPkxvcmVtIGlwc3VtIGRvbG9yIHNpd
CBhbWV0LCBjb25zZWN0ZXR1ZXIgYWRpcGlzY2luZyBlbGl0LiBBZW5lYW4gY29tbW9kbyBsaWd
1bGEgZWdldCBkb2xvci4gQWVuZWFuIG1hc3NhLiBDdW0gc29jaWlzIG5hdG9xdWUgcGVuYXRp
YnVzIGV0IG1hZ25pcyBkaXMgcHVsdHJpY2llcyBuZWMsIHBlbGxlbnRlc3F1ZSBldSwgcHJld
Gl1bSBxdWlzLCBzZW0uIE51bGxhIGNvbnNlcXVhdCBtYXNzYSBxdWlzIGVuaW0uIERvbmVjIHBlZ
GUganVzdG8sIGZyaW5naWxsYSB2ZWwsIGFsaXF1ZXQgbmVjLCB2dWxwdXRhdGUgZWldldCwg
YXJjdS4gSW4gZW5pbSBqdXN0bywgcmhvbmN1cyB1dCwgaW1wZXJkaWV0IGEsIHZlbmVuYXR
pcyB2aXRhZSwganVzdG8uIE51bGxhbSBkaWN0dW0gZmVsaXMgZXUgcGVkZSBtb2xsaXMgcH

JldGl1bS4gSW50ZWdlciB0aW5jaWR1bnQuPC9wPl1dPjwvc2lnZTpDb25zaWRlcmFuZG8+PHNpZ
2U6VGVuaWVuZG9QcmVzZW50ZS8+PHNpZ2U6UmVzdWVsdm8+PCFbQ0RBVEFbPHA+TG9yZ
W0gaXBzdW0gZG9sb3Igc2l0IGFtZXQsIGNvbnNlY3RldHVlciBhZGlwaXNjaW5nIGVsaXQuIEFlbm
VhbiBjb21tb2RvIGxpZ3VsYSBlZ2V0IGRvbG9yLiBBZW5lYW4gbWFzc2EuIEN1bSBzb2NpaXMgbm
F0b3F1ZSBwZW5hdGlidXMgZXQgbWFnbmlzIGRpcyBwYXJ0dXJpZW50IG1vbnRlcywgbmFzY2V
0dXIgcmlkaWN1bHVzIG11cy4gRG9uZWMgcXVhbSBmZWxpcywgdWx0cmljaWVzIG5lYywgcGV
sbGVudGVzcXVlIGV1LCBwcmV0aXVtIHF1aXMsIHNlbS4gTnVsbGEgY29uc2VxdWF0IG1hc3NhIHF
1aXMgZW5pbS4gRG9uZWMgcGVkZSBqdXN0bywgZnJpbmdpbGxhIHZlbCwgYWxpcXVldCBuZ
WMsIHZ1bHB1dGF0ZSBlZ2V0LCBhcmN1LiBJbiBlbmltIGp1c3RvLCByaG9uY3VzIHV0LCBpbXBlc
mRpZXQgYSwgdmVuZW5hdGlzIHZpdGFlLCBqdXN0by4gTnVsbGFtIGRpY3R1bSBmZWxpcyBldS
BwZWRlIG1vbGxpcyBwcmV0aXVtLiBJbnRlZ2VyIHRpbmNpZHVudC48L3A+XV0+PC9zaWdlOlJlc
3VlbHZvPjxzaWdlOkluZGljYWNpb24+PCFbQ0RBVEFbPHAgc3R5bGU9InRleHQtYWxpZ246IGNl
bnRlcjsiPjxzdHJvbmc+RHVpcyBsZW8uIFNlZCBmcmluZ2lsbGEgbWF1cmlzIHNpdCBhbWV0IG5p
YmguPC9zdHJvbmc+PC9wPl1dPjwvc2lnZTpJbmRpY2FjaW9uPjxzaWdlOk51bWVyb0ludGVybm8
vPjwvc2lnZTpSZXNvbHVjaW9uPjxzaWdlOkRpc3RyaWJ1Y2lvbmVzPjxzaWdlOkRpc3RyaWJ1Y2lv
biBudW1lcm89IjEiPjxzaWdlOkRlc2NyaXBjaW9uPlV6aWVsIFJvZHJpZ28gUGVyZXogVmFyZ2FzIC
hNaW5pc3RlcmlvIGRlbCBJbnRlcmlvciB5IFNlZ3VyaWRhZCBQw7pibGljYS9TdWJzZWNyZXRhcs
OtYSBkZWwgSW50ZXJpb3IvRGl2aXNpw7NuIGRlIFJlZGVzIHkgU2VndXJpZGFkIEluZm9ybcOhd
GljYSk8L3NpZ2U6RGVzY3JpcGNpb24+PC9zaWdlOkRpc3RyaWJ1Y2lvbj48c2lnZTpEaXN0cmlid
WNpb24gbnVtZXJvPSIyIj48c2lnZTpEZXNjcmlwY2lvbj5NaW5pc3RlcmlvIGRlbCBJbnRlcmlvciB5IF
NlZ3VyaWRhZCBQw7pibGljYS9TdWJzZWNyZXRhcsOtYSBkZWwgSW50ZXJpb3IvT2ZpY2luYSBk
ZSBQYXJ0ZXMgeSBBcmNoaXZvIENlbnRyYWw8L3NpZ2U6RGVzY3JpcGNpb24+PC9zaWdlOkR
pc3RyaWJ1Y2lvbj48L3NpZ2U6RGlzdHJpYnVjaW9uZXM+PHNpZ2U6SW5pY2lhbGVzUmVzcG9uc
2FibGVzPnVwdjwvc2lnZTpJbmljaWFsZXNSZXNwb25zYWJsZXM+PHNpZ2U6RXN0YWRvRG9jLz
48L3NpZ2U6Q29udGVuaWRvPjwvc2lnZTpEb2N1bWVudG8+PC9SZXNvbHVjaW9uPjwvQ29udG
VuaWRvPjwvRG9jdW1lbnRvPg==",
"references": [
"#16311"
],
"xmlObjects": [
"<MINTObject
xmlns=\"http://www.interior.gob.cl/2013/06/Sige\"><DatosOperacion><Tipo>FIRMA</Tipo><Fi

rmante><Tipo>PERSONA</Tipo><NomPersona>Uziel Rodrigo Perez Vargas</NomPersona><RUT>14228849-4</RUT><Email>uperez@interior.gov.cl</Email><RutaImagen>202_20171018060143.jpeg</RutaImagen><Cargo>Asesor</Cargo></Firmante><RutaImagenLogo>t4_20150821041014.jpeg</RutaImagenLogo></DatosOperacion><CodigoVerificacion>1nbuwJfnoJLWo5xYYqQLfg==</CodigoVerificacion></MINTObject>"

]

}

]}

Ejemplo del JSON BODY para el caso de JSON

- El content será el base64 del json a firmar por ejemplo: eyJrZXkxIjogInZhbHVlMSIsImtleTIiOiAidmFsdWUyIno=
- La respuesta será tendrá dentro del contant un JWS encodeado en base64

```
{
 "api_token_key": "sandbox",
"token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbnRpdHkiOiJTdWJzZWNyZXRhcsOtYSBHZW5lcmFsIGRlIGxhIFByZXNpZGVuY2lhIiwicnVuIjoiMjIyMjIyMjIiLCJleHBpcmF0aW9uIjoiMjAyMS0xMS0xNVQxNzozMTowMCIsInB1cnBvc2UiOiJEZXNhdGVuZGlkbyJ9.EqcNFArqasx_hlZSYTO2Tnuqa36dMn_qnmk90XEyhTA",
 "files": [
        {
                "content-type": "application/json",
                "content": "eyJrZXkxIjogInZhbHVlMSIsImtleTIiOiAidmFsdWUyIno=",
                "checksum":
        "9971224dc8f574ec570ce9fa86f649e2fc26928f561d1649e16841432f9165ff"
        }
}
```

Response Json Schema Body

El resultado de este llamado corresponde a un JSON que contiene los documentos firmados.


```
[
 "$schema": "http://json-schema.org/draft-04/schema#",
 "description": "Recepción de documentos firmados",
 "type": "object",
 "required": [
  "session_token",
  "files"
 ],
 "additionalProperties": false,
 "properties": {
  "session_token": {
   "type": "string"
  },
  "metadata": {
   "type": "object",
   "properties": {
    "OTP_expired": {
     "type": "boolean"
    },
    "files_recived": {
     "type": "number"
    },
    "files_signed": {
     "type": "number"
    },
    "signed_failed": {
     "type": "number"
    }
   },
```

```
    "required": [
      "OTP_expired",
      "files_received",
      "files_signed",
      "signed_failed"
    ]
  },
  "files": [
    "type": "array",
    "minItems": 1,
    "items": [
      "type": "object",
      "required": [
        "checksum_original",
        "status"
      ],
      "additionalProperties": false,
      "properties": [
        "type": [
          "enum": [
            "PDF",
            "JSON",
            "XML"
          ]
        ],
        "content": [
          "type": "string"
        ],
        "checksum_original": [
          "type": "string"
        ],
        "checksum": [
```

```
          "type": "string"
        ],
        "description": [
          "type": "string"
        ],
        "status": [
          "type": "string"
        ]
      }
    }
  ]
}
```


Un ejemplo de respuesta es la siguiente:


```
[
  "files": [
    [
                                                    "checksum_original":
"447ac80f0d813be18d2ad59db26c4167198b656d356bd1b47ccd131d61716527",
      "status": "error"
    ],
    [
                                                    "checksum_original":
"453ac80f0d813be18d2ad59db26c4167198b656d356bd1b47ccd131d61716527",
      "Content": "YXNkYXNkc2FkYXNk"
      "status": "OK"
    ]
  ],
  "metadata": [
    "signed_failed": 1,
    "OTP_expired": false,
```

```
  "files_signed": 0,
  "files_received": 1
 ]
}
```

En el campo files se recibe una lista de objetos, este contiene lo siguiente:

checksum_original	SHA256 del archivo original.
status	error - no se concretó la firma
	OK - transacción correcta
content	base64 del archivo firmado

En el campo metadata se recibe un objeto que contiene lo siguiente:

signed_file	número de archivos firmados
OTP_expired	booleano que indica si el OTP se pudo usar de manera correcta con la totalidad de archivos
files_signed	Número de archivos que se pudieron firmar
files_recived	Número de archivos recibidos

3.Ambiente de TEST

Las firmas generadas en este ambiente no son válidas, es sólo para facilitar la integración.

URL: https://api.firma.cert.digital.gob.cl/firma/v2/***files/tickets'***, *método* = *['POST']*

Firma atendida

api_token_key	sandbox

JWT	{
	"entity": "Subsecretaría General de la Presidencia",
	"run": "11111111",
	"expiration": "2021-11-15T17:31:00",
	"purpose": "Propósito General"
	}

secreto	27a216342c744f89b7b82fa290519ba0

El código QR correspondiente a semilla para generar OTPs asociadas a este certificado es el siguiente:

En el Anexo A se detalla cómo realizar la instalación y configuración para la generación de OTPs.

Firma desatendida

api_token_key	sandbox

JWT	{
	"entity": "Subsecretaría General de la Presidencia",
	"run": "22222222",
	"expiration": "2021-11-15T17:31:00",
	"purpose": "Desatendido"
	}

secreto	27a216342c744f89b7b82fa290519ba0

En el caso de firma desatendida no debe enviarse el header OTP.

4.Códigos HTTP asociados a la API

Status code	Tipo	Response

200	Ok	{
		"files":[
		{
		"content":"ARCHIVO BASE64 FIRMADO",
		"status":"OK",
		"contentType":"application/pdf",
		"description":"DESCRIPCION DE DOCUMENTO",
		"checksum_original":"CHECKSUM ENVIADO",
		"checksum_signed":"CHECKSUM FIRMANDO"
		}
		],
		"metadata":{
		"otpExpired":false,
		"filesSigned":1,
		"signedFailed":0,
		"objectsReceived":1
		}
		}

400	Bad request	{
		"timestamp": "yyyy-MM-dd hh:mm:ss",
		"status": 400,
		"error": "Mensaje de Error*"
		}
		
		* Mensaje de Error, pueden ser los siguientes:
		● Aplicación no existe en la RA
		● Error al decodificar el token favor revisar el formato.
		● Favor revisar los campos del token, ya que contiene datos vacíos
		● Solicitud excede el tamaño máximo que son 5 MB.
		● token : xxxxxxx no valido, favor revise su secret.
		● Formato de campo expiration en token, esta mal emitido, el formato de ejemplo es el siguiente : 2020-01-29T13:28:00
		● Debe ingresar un código OTP Valido
		● Debe ingresar un código OTP

		• Fecha de expiración del token está vencida • Debe Adjuntar Documento/s, a Firmar • Tipo de documento no permitido • Cuerpo de la solicitud mal formada

401	Error no autorizado	{
		"timestamp": "yyyy-MM-dd hh:mm:ss",
		"status": 401,
		"error": "Error no autorizado"
		}

403	Error de Acceso	{
		"timestamp": "yyyy-MM-dd hh:mm:ss",
		"status": 403,
		"error": "Mensaje de Error*"
		}
		
		*Mensaje de Error, pueden ser los siguientes:
		• certificado del usuario : (run) se encuentra vencido.
		• Esta aplicación no tiene permisos para el recurso que desea acceder
		• Acceso a Banco de Firma no permitido, favor revise sus permisos

404	Error de Recurso no Encontrado	{
		"timestamp": "yyyy-MM-dd hh:mm:ss",
		"status": 404,
		"error": "Mensaje de Error*"
		}
		
		*Mensaje de Error, pueden ser los siguientes:
		• Error data servicio y/o propósito
		• Datos incompletos
		• Aplicación no existe en la RA
		• No existen certificados para el firmante
		• “run” no se puede obtener los datos del firmante

412	Error no autorizado	{
		"timestamp": "yyyy-MM-dd hh:mm:ss",
		"status": 401,
		"error": "Mensaje de Error*"
		}
		
		*Mensaje de Error, pueden ser los siguientes:
		• Aplicación no tiene permisos para esta operación
		• Verificaciòn de OTP fallido

500	Error interno de	{

	servidor	"timestamp": "yyyy-MM-dd hh:mm:ss", "status": 500, "error": "Internal Server Error" }

504	Error tiempo agotado de espera del Servidor	{
		"timestamp": "yyyy-MM-dd hh:mm:ss",
		"status": 504,
		"error": "Gateway timeout"
		}

Anexo A. Instalación aplicación móvil y configuración OTP

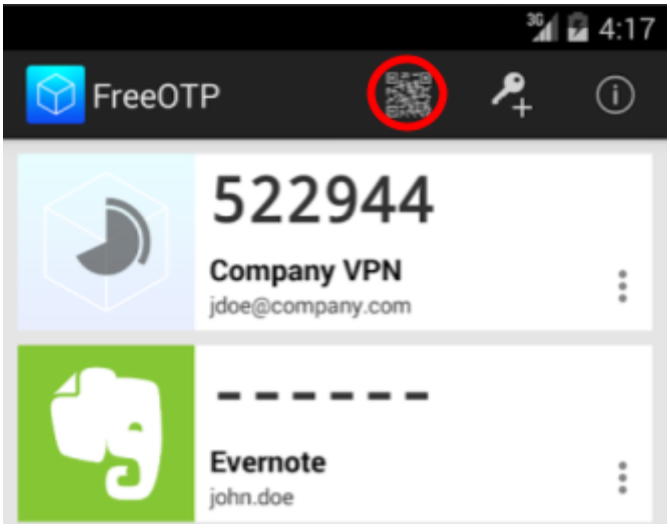
Es requisito habilitar una aplicación que permita generar un OTP válido al momento de realizar las pruebas al servicio. Por tal motivo, se ha habilitado una clave generadora de OTPs que permite utilizar un ambiente sandbox solo para la ejecución de pruebas.

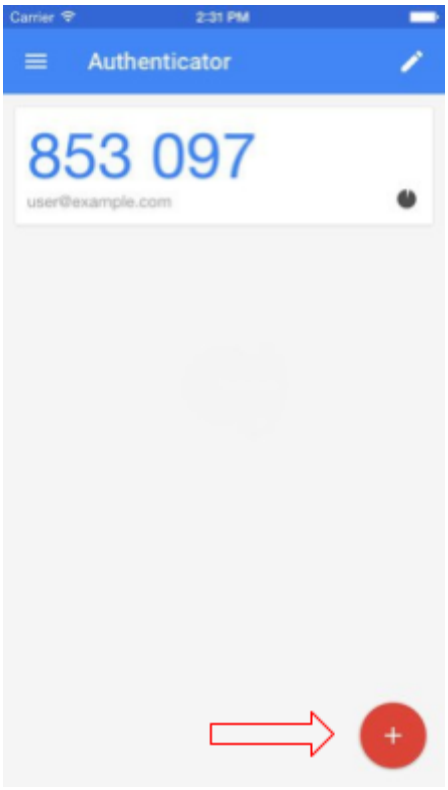
A continuación se detallan los pasos a seguir para habilitar un generador de OTP en un smartphone.

Aplicación OTP

Acceder a Google Play o App Store, descargar e instalar la aplicación Free OTP o Google Authenticator (para el ejemplo se ha utilizado un equipo con versión 5.1.1)

Abrir la aplicación ya instalada y habilitar la aplicación para la lectura de códigos QR.





Escanee el código QR.

Anexo B. Configuración para incrustar firma a PDF

Propiedad layout

La propiedad layout permite embeber una imagen asociada a la firma, análoga, de la persona que firma el documento electrónicamente. El siguiente XML muestra la estra la estructura del layout.

```
<AgileSignerConfig>
        <Application id=\"THIS-CONFIG\">
                <pdfPassword/>
                <Signature>
                        <Visible active=\"true\" layer2=\"false\" label=\"true\" pos=\"1\">
                                <llx></llx>
                                <lly></lly>
                                <urx></urx>
                                <ury></ury>
                                <page>LAST</page>
                                <image>BASE64</image>
                                <BASE64VALUE></BASE64VALUE>
                        </Visible>
                </Signature>
        </Application>
</AgileSignerConfig>
```

Variable	Descripción	Tipo Valor
llx	Coordenada x de la esquina inferior izquierda de la imagen.	Número entero
lly	Coordenada y de la esquina inferior izquierda de la imagen.	Número entero
urx	Coordenada x de la esquina superior derecha de la imagen.	Número entero
ury	Coordenada y de la esquina superior derecha de la imagen.	Número entero
page	Número de página donde se incluirá	Numero entero. También es posible

	la imagen con la firma.	usar la palabra LAST para hacer referencia a la última hoja del documento.
image	Tipo de encoding utilizado para embeber la imagen	Texto. Valor constante a utilizar BASE64
base64value	Contenido de la imagen con el formato y encoding definido anteriormente.	Texto. Contenido del archivo en base64

Ejemplo:

Por restricciones de tamaño de archivo, el siguiente ejemplo no considera el contenido de la imagen. El ejemplo completo se encuentra publicado en EjemploXmlLayout.xml

```
<AgileSignerConfig>
        <Application id=\"THIS-CONFIG\">
                <pdfPassword/>
                <Signature>
                        <Visible active=\"true\" layer2=\"false\" label=\"true\" pos=\"1\">
                                <llx>250</llx>
                                <lly>300</lly>
                                <urx>350</urx>
                                <ury>450</ury>
                                <page>LAST</page>
                                <image>BASE64</image>
                                <BASE64VALUE></BASE64VALUE>
                        </Visible>
                </Signature>
        </Application>
</AgileSignerConfig>
```

Anexo C. Definiciones y acrónimos

Acrónimo	Definición
API	Application Programming Interface
APP	Aplicación
JSON	JavaScript Object Notation
JWT	JSON Web Token
SHA256	hash criptográfico
OTP	One-Time Password
RA	Registration authority
XML	Extensible Markup Language

Término	Descripción
Firma atendida	Operación de firma en la cual se requiere la intervención del titular para la generación del OTP.
Firma desatendida	Operación de firma en la cual no se requiere la intervención del titular para la generación del OTP.

Anexo D. Historial de cambios

Versión	Fecha	Descripción
1	31/03/2016	Versión inicial
2	25/05/2016	Cambios menores de redacción e incorporación de códigos de error
3	15/09/2016	Cambios menores de redacción y ejemplos
4	15/11/2016	1. Cambio estructura del documento 2. Correcciones a parámetros en primera llamada 3. Incorporación parámetros para firma XML y JSON 4. Instalación y configuración aplicación iOS
5	31/01/2017	Cambio en código QR
6	24/03/2017	Cambios menores.
7	30/05/2017	Cambio en título de documento y corrección nombre de variables ejemplos firmas atendidas y desatendidas.
8	29/01/2020	Se modificó el documento de acuerdo a la nueva versión de API Se modificó el anexo A, configuración de OTP
9	13/04/2020	Se modificó sección 4. Códigos HTTP
10	04/02/2021	Se incorpora ejemplo hash
11	09/02/2021	Se incorpora ejemplo JSON
12	10/02/2021	Se incorpora ejemplo XML
13	15/11/2021	Se actualizan datos de prueba (sección 3) Se modifica ejemplo XML

Anexo E. Clasificación del documento

Este documento se encuentra clasificado bajo la categoría de ordinario, según el Instructivo de clasificación del Ministerio Secretaría General de la Presidencia.