

Documento de integración entre un sistema de información web y la Plataforma FIRMA PERÚ para la creación de firmas digitales

Guía para el uso e integración de la Plataforma Nacional de Firma Digital en la Administración Pública

Resolución de Secretaría de Gobierno y Transformación Digital
N° 002-2022-PCM/SGTD

**PERÚ**Presidencia
del Consejo de MinistrosSecretaría de Gobierno
y Transformación Digital

CONTROL DE VERSIONES

Versión	Fecha	Título	Elaborado por
1.0.0	2022/08	Documento de integración entre un sistema de información y la Plataforma FIRMA PERÚ para la creación de firmas digitales	Secretaría de Gobierno y Transformación Digital
2.0.0	2023/03	Documento de integración entre un sistema de información y la Plataforma FIRMA PERÚ para la creación de firmas digitales	Secretaría de Gobierno y Transformación Digital
3.0.0	2023/07	Documento de integración entre un sistema de información web y la Plataforma FIRMA PERÚ para la creación de firmas digitales	Secretaría de Gobierno y Transformación Digital



CONTENIDO

1. DOCUMENTACIÓN DE CONFIGURACIÓN	3
1.1. Alcance.....	3
1.2. Configuración para Sistema Operativo Windows	3
1.3. Configuración para Sistema Operativo Linux.....	4
1.4. Configuración para Sistema Operativo macOS.....	5
2. DOCUMENTACIÓN DE INTEGRACIÓN.....	5
2.1. Alcance.....	5
2.2. Indicaciones de integración	5



GUÍA PARA EL USO E INTEGRACIÓN DE LA PLATAFORMA NACIONAL DE FIRMA DIGITAL EN LA ADMINISTRACIÓN PÚBLICA

Documento de integración entre un sistema de información web y la Plataforma FIRMA PERÚ para la creación de firmas digitales

1. DOCUMENTACIÓN DE CONFIGURACIÓN

1.1. Alcance

El presente documento está dirigido al personal de desarrollo y de soporte de las entidades de la Administración Pública que se integren a la Plataforma Nacional de Firma Digital (Plataforma FIRMA PERÚ).

1.2. Configuración para Sistema Operativo Windows

Para sistema operativo Windows 10 y superior, funciona con DNle¹ y certificados digitales instalados en el sistema operativo, la instalación se realiza automáticamente en la primera ejecución.

Para la instalación, debes contar mínimo con .NET Framework 4.8 (incluido por defecto en Windows 10 y Windows 11). Si tienes problemas al instalar, deberás aplicar las últimas actualizaciones al sistema operativo desde Windows Update.

Configuración de los navegadores web

Para que la aplicación de Firma Perú en aplicaciones web funcione desde la integración realizada por los desarrolladores de las entidades, es importante tener instalado en el navegador el plugin de ClickOnce.

Si un plugin de ClickOnce correspondiente al navegador está instalado se iniciará automáticamente el servicio, caso contrario instale un Plugin de las opciones a continuación:

Plugin para el navegador Firefox (Instalar solo uno de los listados)

- <https://addons.mozilla.org/es/firefox/addon/logalty-clickonce/>
- <https://addons.mozilla.org/es/firefox/addon/breez-clickonce/>

Plugin para el navegador Google Chrome (Instalar solo uno de los listados)

- <https://chrome.google.com/webstore/detail/windows-remix-clickonce-h/dgpgholdldjibcmpeckiephijgdpikan>
- <https://chrome.google.com/webstore/detail/clickonce-for-google-chro/kekahkplibinaibelipdcikofmedafmb>

Para el navegador Microsoft Edge basado en Chromium, las últimas versiones trabajan de manera nativa, en caso no se realice la ejecución, puede instalar uno de los plugin de Google Chrome, para esto tendrá que aceptar el mensaje de instalación de componentes desde las tiendas de terceros que aparece al momento de la instalación.

¹ DNle: Documento Nacional de Identidad Electrónico.

Al instalar un plugin se descargará un archivo .exe, es importante que este archivo .exe se ejecute para que la instalación del plugin sea correcta. En caso sea necesario, habilitar la ejecución de este .exe en caso el antivirus muestre un mensaje.

Si luego de tener un plugin instalado y no se ejecuta el servicio, asegúrese que la PC tiene acceso al puerto que el desarrollador estableció para la ejecución del servicio local y que la URL "http://localhost:+port+/firmaperu/sign" no esté bloqueada por algún programa local como antivirus o firewall.

Puede revisar el log de ejecución en:

- USER_HOME/PCM/FirmadorClienteWeb/FirmadorClienteWeb.log

1.3. Configuración para Sistema Operativo Linux

Para sistema operativo Ubuntu 20.04 LTS y superior, solo funciona con DNLe, es necesario realizar las siguientes instalaciones y configuraciones:

Con super usuario:

1. Ejecutar `sudo apt install pcscd openjdk-8-jre icedtea-netx`
2. Ejecutar `sudo update-alternatives --config java`
3. Digitar el número que corresponde a la alternativa `/usr/lib/jvm/java-8-openjdk-amd64/jre/bin/java`
4. Ejecutar `sudo systemctl status pcscd.socket`, verificar que esté activo -> Active: active (running)
Nota: En caso `systemctl` no esté activo:
 1. Ejecutar `sudo systemctl start pcscd.socket`
 2. Ejecutar `sudo systemctl enable pcscd.socket`
 3. Ejecutar `sudo reboot`

Con usuario normal:

1. Ejecutar `itweb-settings`
2. Ir a JVM Settings -> Browse for JVM for IcedTea-Web
3. Ingresar: `/usr/lib/jvm/java-8-openjdk-amd64/jre`
4. Seleccionar "Ok"

Después de realizar estas configuraciones, ya se podrá ejecutar el firmador.

NOTA: Solo funciona con Navegador Mozilla Firefox.

Esta configuración funciona para Sistema Operativo Ubuntu (Ubuntu 20.04 LTS y superior) y algunos de sus derivados.

Puede revisar el log de ejecución en:

- USER_HOME/PCM/FirmadorClienteWeb/FirmadorClienteWeb.log

1.4. Configuración para Sistema Operativo macOS

Para sistema operativo macOS Big Sur y superior, solo funciona con DNle, es necesario realizar las siguientes instalaciones y configuraciones:

Instalar JRE:

1. Ir a <https://adoptium.net/es/temurin/releases/>
2. Seleccionar el Sistema Operativo "macOS", arquitectura "X64", tipo de paquete "JRE" y versión "8".
3. Descargar el paquete ".PKG"
4. Instalar el paquete descargado
5. Abrir un terminal y ejecutar "java -version" y verificar que esté instalado el JRE

Instalar OpenWebStart:

1. Ir a <https://openwebstart.com/download/>
2. Descargar el paquete X64 ".dmg" para macOS
3. Instalar el paquete descargado
4. Abrir "Launchpad" y ejecutar "OpenWebStart Settings", se abrirá un diálogo principal.
5. Ir a "JVM Manager" y seleccionar la opción "Find local" con lo cual se agregará automáticamente el JRE instalado, luego seleccionar "Settings" y en el diálogo que aparece seleccionar en Update strategy "Do not download any version" y luego "ok".
6. Ir a "Proxy Setting" y seleccionar "No Proxy".
7. Ir a "Desktop Integration" y seleccionar en Shortcut Handling "Ask if hinted" y en Shortcuts Overwrite Strategy "Overwrite existing shortcuts".
8. Finalmente, en la parte inferior del diálogo principal seleccionar "Apply" y luego en "Ok".

Después de realizar estas configuraciones, ya se podrá ejecutar el firmador.

NOTA: Funciona con navegadores Safari, Google Chrome y Mozilla Firefox.

Puede revisar el log de ejecución en:

- USER_HOME/PCM/FirmadorClienteWeb/FirmadorClienteWeb.log

2. DOCUMENTACIÓN DE INTEGRACIÓN

2.1. Alcance

Este documento está dirigido a los desarrolladores que se encarguen de integrar aplicaciones web a la Plataforma Nacional de Firma Digital (Plataforma FIRMA PERU).

2.2. Indicaciones de integración

Para que un desarrollador realice la integración con la Plataforma FIRMA PERÚ, tiene que realizar la siguiente implementación en HTML con JavaScript:

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title>Firma Peru Web</title>
5     <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
6     <meta name="description" content="" />
7     <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1"/>
8     <meta http-equiv="content-type" content="text/html; charset=UTF-8"/>
9     <link href="https://getbootstrap.com/docs/4.6/dist/css/bootstrap.min.css" rel="stylesheet">
10    <script src="https://code.jquery.com/jquery-3.5.1.min.js"></script>
11    <script src="https://getbootstrap.com/docs/4.6/dist/js/bootstrap.bundle.min.js"></script>
12    <script type="text/javascript">
13      //
14      console.log("jQuery de la web demo: " + $.fn.jquery);
15      //]]&gt;
16    &lt;/script&gt;
17  &lt;/head&gt;
18  &lt;body&gt;
19    &lt;script src="https://code.jquery.com/jquery-3.6.0.min.js"&gt;&lt;/script&gt;
20    &lt;script type="text/javascript"&gt;
21      //<![CDATA[
22      //Variables y funciones necesarias para el funcionamiento de Firma Perú:
23      var jqFirmaPeru = jQuery.noConflict(true);
24
25      function signatureInit() {
26        //Aquí se puede poner un preload
27        alert('PROCESO INICIADO');
28      }
29
30      function signatureOk() {
31        //Cancelar el preload
32        alert('DOCUMENTO FIRMADO');
33      }
34
35      function signatureCancel() {
36        //Cancelar el preload
37        alert('OPERACIÓN CANCELADA');
38      }
39
40
41
42      //Funciones del integrador:
43      function sendParam() {
44        var param = "ew0KIC=..."; //Base 64
45        var port = "48596";
46        //FUNCIÓN DE INICIO DE FIRMA DIGITAL
47        startSignature(port, param);
48        //+++++
49      }
50      //]]&gt;
51    &lt;/script&gt;
52    &lt;!-- Poner la URL del servicio firmaperu.min.js --&gt;
53    &lt;script src="https://xyz.gob.pe/cliente/firmaperu.min.js"&gt;&lt;/script&gt;
54    &lt;div id="addComponent" style="display:none;"&gt;&lt;/div&gt;
55
56    &lt;button type="button" class="btn btn-lg btn-primary" onclick="sendParam();"&gt;INICIAR FIRMA&lt;/button&gt;
57  &lt;/body&gt;
58 &lt;/html&gt;</pre></div><div data-bbox="173 628 370 644" data-label="Text"><p>La URL del servicio es:</p></div><div data-bbox="173 644 688 659" data-label="Text"><p><a href="https://apps.firmaperu.gob.pe/web/clienteweb/firmaperu.min.js">https://apps.firmaperu.gob.pe/web/clienteweb/firmaperu.min.js</a></p></div><div data-bbox="173 688 862 719" data-label="Text"><p>Es obligatorio la implementación de la variable y las funciones que se señalan a continuación:</p></div><div data-bbox="173 734 862 829" data-label="List-Group"><ul><li>• <b>Variable jqFirmaPeru</b>, especifica el uso de JQuery en <b>firmaperu.min.js</b> y se requiere jQuery v3.6.0</li><li>• <b>Función signatureInit()</b>, se invoca al iniciar la firma digital.</li><li>• <b>Función signatureOk()</b>, se invoca al finalizar la firma digital de manera satisfactoria.</li><li>• <b>Función signatureCancel()</b>, se invoca al cancelar la firma digital.</li></ul></div><div data-bbox="173 841 748 859" data-label="Text"><p>Asimismo, se tiene que poner la URL del servicio <b>"firmaperu.min.js"</b>.</p></div><div data-bbox="173 871 860 904" data-label="Text"><p>También es obligatorio agregar <b>&lt;div id="addComponent" style="display:none;"&gt;&lt;/div&gt;</b> dentro de la etiqueta <b>&lt;body&gt;</b>.</p></div><div data-bbox="137 928 862 956" data-label="Page-Footer"><p>PCM | Documento de integración entre un sistema de información web y la Plataforma FIRMA PERÚ para la creación de firmas digitales. Versión 3.0.0</p></div><div data-bbox="749 940 862 956" data-label="Page-Footer"><p>Página 6 de 12</p></div>
```

Para la ejecución del servicio, se tiene que llamar a la función **startSignature (port, param)** y pasar los valores correspondientes:

port	Número de puerto para levantar un servidor local en <code>http://localhost:port</code> , donde port es el número de puerto, se recomienda siempre utilizar el puerto 48596 y solo cambiarlo cuando ese puerto este en uso en la PC donde se realizará la firma digital.
param	<p>Parámetros para obtención de información para iniciar la firma digital, es un objeto JSON codificado en Base64, el objeto tiene la siguiente estructura:</p> <pre>{ "param_url": " http://localhost:8080/ruta/api/param", "param_token": "1626476967", "document_extension": "pdf" }</pre> <p>Donde: param_url, ruta de donde se obtendrá el objeto JSON con los parámetros de firma. param_token, tiene que ser un token de un único uso. document_extension, la extensión del documento a firmar.</p>

Especificación de la URL que va en param_url, recibe parámetro de tipo x-www-form-urlencoded:

POST	http://localhost:8080/ruta/api/param	
KEY	TYPE	DESCRIPTION
param_token	String	Token de un único uso enviado por el integrador.
Response	<p>Debe de retornar un objeto JSON codificado en Base64 con los parámetros de firma.</p> <p>Objeto JSON para PAdES:</p> <pre>{ "signatureFormat": "PAdES", "signatureLevel": "B", "signaturePackaging": "enveloped", "documentToSign": "http://localhost:8080/web/doc/demo.pdf", "certificateFilter": ".*", "webTsa": "", "userTsa": "", "passwordTsa": "", "theme": "claro", "visiblePosition": true, "contactInfo": "", "signatureReason": "Soy el autor de este documento", "batchOperation": false, }</pre>	


```
"oneByOne": true,  
"signatureStyle": 1,  
"imageToStamp":  
"http://localhost:8080/web/doc/stamp.png",  
"stampTextSize": 14,  
"stampWordWrap": 37,  
"role": " Analista de servicios",  
"stampPage": 1,  
"positionx": 20,  
"positiony": 20,  
"uploadDocumentSigned": "http://localhost:8080/web/api/upl  
oad/162",  
"certificationSignature": false,  
"token":  
"eyJhbGciOiJIJFZlbnR5cCI6IkpXVCIsImtpZCI6IjE2MiJ9.eyJ1bmlkLWp1b3R5cCI6IjE2MiJ9.eyJ1bmlkLWp1b3R5cCI6IjE2MiJ9"
```

```
}
```

Objeto JSON para XAdES:

```
{  
  "signatureFormat": "XAdES",  
  "signatureLevel": "B",  
  "signaturePackaging": "enveloped",  
  "documentToSign": "http://localhost:8080/web/doc/001",  
  "certificateFilter": ".*",  
  "webTsa": "",  
  "userTsa": "",  
  "passwordTsa": "",  
  "theme": "claro",  
  "batchOperation": false,  
  "uploadDocumentSigned": "http://localhost:8080/web/api/upl  
oad/162",  
  "token":  
  "eyJhbGciOiJIJFZlbnR5cCI6IkpXVCIsImtpZCI6IjE2MiJ9.eyJ1bmlkLWp1b3R5cCI6IjE2MiJ9.eyJ1bmlkLWp1b3R5cCI6IjE2MiJ9"
```

```
}
```

Objeto JSON para CAdES:

```
{  
  "signatureFormat": "CAdES",  
  "signatureLevel": "B",  
  "signaturePackaging": "detached",  
  "documentToSign": "http://localhost:8080/web/doc?id=001",  
  "certificateFilter": ".*",  
  "webTsa": "",  
  "userTsa": "",  
  "passwordTsa": "",  
  "theme": "claro",  
  "batchOperation": false,  
  "uploadDocumentSigned": "http://localhost:8080/web/upload  
?id=162",  
  "token":  
  "eyJhbGciOiJIJFZlbnR5cCI6IkpXVCIsImtpZCI6IjE2MiJ9.eyJ1bmlkLWp1b3R5cCI6IjE2MiJ9.eyJ1bmlkLWp1b3R5cCI6IjE2MiJ9"
```

```
}
```

Especificación del objeto JSON de los parámetros de firma:

signatureFormat	PAdES: Para documentos PDF. XAdES: Para documentos XML. CAAdES: Para cualquier tipo de documento (Firma desacoplada).
signatureLevel	B: Firma básica. T: Firma con sello de tiempo. LTA: Firma con datos de validación a largo plazo (Long Term Archival).
signaturePackaging	PAdES: Por defecto es enveloped, se puede enviar en blanco. XAdES: Por defecto es enveloped, se puede enviar otros valores como: enveloping detached internallydetached CAAdES: Por defecto es detached, se puede enviar otro valor como: enveloping.
documentToSign	URL del documento que se descargará en la PC para firmar. Si la respuesta es un array de bytes se tiene que indicar en la cabecera de la respuesta el tipo de documento. Para firmar en lote se tiene que enviar un 7z con los documentos a firmar. En la URL debe de enviar un ID como parte de la URL o una variable de URL, esto para identificar en su servicio que archivo se va a descargar.
certificateFilter	Expresión regular al CN del certificado. ".*": Todos los certificados digitales. ".*FIR.* .FAU.*": Solo certificados de Firma y/o Autenticación. ".*FIR.*44587589.*": Que sea de firma y contenga el DNI ingresado.
webTsa	URL del servicio de sello de tiempo TSA.
userTsa	Usuario de la TSA. Si no tiene poner ""

passwordTsa	Password de la TSA. Si no tiene poner ""
theme	Estilo de la interfaz gráfica de usuario: claro, oscuro, claro 2, oscuro 2, claro 3, oscuro 3.
visiblePosition	true: Muestra el visor para el posicionamiento visual de la representación gráfica de la firma. false: No muestra el visor.
contactInfo	Opcional, poner "". Permite definir un tipo de ID para identificar la firma en el documento al obtener la información de las firmas desde código fuente.
signatureReason	Texto que indica la Razón de la firma.
batchOperation	false: Para realizar una firma simple. true: Para realizar una firma en lote.
oneByOne	Funciona cuando batchOperation es true. true: El usuario posiciona uno por uno la representación gráfica de la firma. false: EL usuario posiciona solo una vez la representación gráfica de la firma, tomara esa referencia para las demás.
signatureStyle	0: Firma invisible. 1: Firma con estampado y descripción horizontal. 2: Firma con estampado y descripción vertical. 3: Solo firma con estampado. 4: Solo firma con descripción.
imageToStamp	URL la imagen de estampado que se descargará en la PC para la firma. Si la respuesta es un array de bytes se tiene que indicar en la cabecera de la respuesta el tipo de documento. La imagen tiene que ser solamente del tipo PNG. En la URL puede enviar un ID como parte de la URL o una variable de URL, esto para identificar en su servicio que imagen se va a descargar.
stampTextSize	Tamaño del texto en el estampado de la firma, valor recomendado 14.
stampWordWrap	Longitud del texto en el estampado, valor recomendado 37.
role	

	Rol del firmante, es opcional, en caso de no usar enviar ""
stampPage	Página en la que se pondrá el estampado de la firma. Inicia en 1 (solo si visiblePosition es false).
positionx	Posición X en la página donde se pondrá el estampado de la firma (solo si visiblePosition es false).
positiony	Posición Y en la página donde se pondrá el estampado de la firma (solo si visiblePosition es false).
uploadDocumentSigned	<p>URL al cual se realizará POST del documento firmado en la PC del usuario. Se envía el objeto de formulario con nombre "signed_file". Si son varios documentos firmados retorna un 7z.</p> <p>En la URL se debe de enviar un ID como parte de la URL o una variable de URL, esto para identificar en su servicio que documento está recibiendo.</p>
certificationSignature	Único firmante del documento PDF. (CertificationPermission.MINIMAL_CHANGES_PERMITTED). Nadie más podrá agregar una firma digital después. Por defecto es false.
token	Token de acceso al servicio, este debe ser generado por el integrador en su mismo servidor. (*)

(*) Para que una entidad se integre al servicio deberá contar con la credencial correspondiente, esta credencial se encuentra en el archivo **fwAuthorization.json**, este archivo tiene la siguiente información:

```
{"client_id":"GSMYFqZiNTlwMTY4OTk5OTI23INyQ5F-NQ","client_secret":"JIQDQiu_C3K5m0xD3UECAwCNUvvdCC2KByk","token_url":"https://algunauri.gob.pe/adm/generate-token"}
```

Para la obtención del token deberá realizar un POST (desde el servidor) con esta información según la siguiente especificación:

Recibe parámetro de tipo x-www-form-urlencoded:

POST	https://algunauri.gob.pe/adm/generate-token La URL se obtiene del archivo fwAuthorization.json (token_url)	
KEY	TYPE	DESCRIPTION
client_id	String	El valor se obtiene del archivo fwAuthorization.json
client_secret	String	El valor se obtiene del archivo fwAuthorization.json



Se recomienda definir una ruta en disco para almacenar el archivo **fwAuthorization.json**, de esta manera cuando existan algún cambio de la credencial, bastará con reemplazar el archivo.

El token obtenido se envía como parámetro de firma, el token es un *JSON Web Token* y tiene una vigencia de duración establecido.

El desarrollador puede obtener del token la vigencia y determinar si aún el token no expiró, de esta manera puede reutilizar el token y solo solicitar uno nuevo cuando este expire. La implementación de esta lógica es recomendada para que no se esté solicitando un token nuevo por cada firma a generar.

Es indispensable tener conexión a internet para la verificación de certificados antes de firmar, ya que se accede a información de consulta de estado de revocación de los certificados, así como a la URL de la TSL y a la ruta <https://www.google-analytics.com> (Para estadísticas de uso).

Durante la ejecución del firmador, en el navegador se imprimen mensajes con `console.log`