

Documento de integración entre un sistema de información y la Plataforma FIRMA PERÚ para la validación 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 validación 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 validación de firmas digitales	Secretaría de Gobierno y Transformación Digital
3.0.0	2023/11	Documento de integración entre un sistema de información y la Plataforma FIRMA PERÚ para la validación de firmas digitales	Secretaría de Gobierno y Transformación Digital



CONTENIDO

1. DOCUMENTACIÓN DE DESPLIEGUE.....	3
1.1. Alcance.....	3
1.2. Requerimientos para despliegue	3
1.3. Despliegue del Módulo de Validación de Firmas	4
1.4. Información General.....	4
2. DOCUMENTACIÓN DE CONFIGURACIÓN	4
2.1. Alcance.....	4
2.2. Configuración de credenciales para aplicaciones o sistemas.....	4
2.3. Autorización de uso del servicio de validación	5
2.4. Configuración de la autorización para uso del servicio	6
3. DOCUMENTACIÓN DE INTEGRACIÓN.....	6
3.1. Alcance.....	6
3.2. Especificación del API REST.....	6
3.2.1. info	6
3.2.2. validation.....	7
3.2.3. clean_temp	11
3.3. Información general.....	12



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 y la Plataforma FIRMA PERÚ para la validación de firmas digitales

1. DOCUMENTACIÓN DE DESPLIEGUE

1.1. Alcance

Esta guía está dirigida al personal técnico encargado del despliegue de aplicaciones en la infraestructura de la entidad.

1.2. Requerimientos para despliegue

El Módulo de Validación de Firmas debe ser publicado en un servidor propio de la entidad que requiera del servicio con las siguientes características mínimas (Según la carga la entidad deberá de proveer más recursos al servidor):

Tipo	Servidor Virtual o Dedicado
Sistema Operativo	Linux / Windows
Distribución	Red Hat o CentOS o Ubuntu / Windows Server 2019 o superior
RAM	5 GB / 6 GB
CPU	2
Disco	15 GB / 80 GB
Tráfico de datos	Ilimitado
Aplicaciones instaladas	OpenJDK 8, Tomcat 10.0.X (no funciona con 10.1.X)
Configuraciones	• Tener instalado lsb_release (solo en Linux). • Asignar 3 GB de RAM para la ejecución de Tomcat. • Configurar el "user.home" del usuario del tomcat, generalmente es en "/home/tomcat" para Linux, "C:\Users\tomcat" para Windows (crear un usuario tomcat y con este realizar la instalación)
Salida a internet	Requerido

El servidor debe de tener conexión a internet para la verificación de firmas, 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).



El acceso al servidor solo debe ser dado solamente personal encargado de realizar la publicación de aplicaciones, es responsabilidad del encargado de infraestructura a quienes da acceso al servidor y la gestión de este.

1.3. Despliegue del Módulo de Validación de Firmas

Se puede publicar el Módulo de Validación de Firmas mediante la consola de administración web de Tomcat o copiando el binario en el contenedor de aplicaciones directamente (carpeta webapps), este paso lo puede realizar el personal técnico encargado del despliegue de aplicaciones en la infraestructura de la entidad, ya que cuentan con ese conocimiento.

Una vez desplegado el Módulo de Validación de Firmas, acceder a la siguiente URL para validar la disponibilidad del servicio: <http://127.0.0.1:8080/validador> (Poner la IP que tenga asignado el servidor en 127.0.0.1). Cargará una página de bienvenida, con esto ya se tiene desplegado el servicio para realizar validación de firmas mediante API REST.

1.4. Información General

Para realizar pruebas, se recomienda primero ver la Documentación de Configuración y luego y la Documentación de Integración.

2. DOCUMENTACIÓN DE CONFIGURACIÓN

2.1. Alcance

Esta guía está orientada para el personal técnico encargado del despliegue de aplicaciones en la infraestructura de la entidad.

2.2. Configuración de credenciales para aplicaciones o sistemas

Luego de realizado el despliegue del módulo de validación de firmas se procederá a realizar la configuración para habilitar el acceso a las aplicaciones internas que comparten la misma red del módulo desplegado.

El archivo “credentials.json”, se tiene que copiar en la ruta “user.home”/PCM/Validador/credentials.json

“user.home” hace referencia a la ruta home que se le configuró al contenedor de aplicaciones Tomcat al momento de su instalación, revisar apartado 3.2.1.

Procedemos a editar el archivo “credentials.json” teniendo en cuenta la siguiente especificación:

```
[
  {
    "app": "Sistema 1",
    "credential": "9513d4e3d0df4fb62458c40263622d470eb473d3c5d1b823d6e530619d8787ff"
  },
  {
    "app": "Sistema 2",
    "credential": "f01c95ac9c007d2a4e06d3bf20d69b268fb46e12680ff44c8018a5d56752bbc9"
  },
  {
    "app": "Sistema X",
    "credential": "9f5084fb955276dc4ae126f1032b737c1c8464fc7cba62ed7707aafdf47680af"
  }
]
```

app: Hace referencia al nombre de la aplicación o sistema que va a usar el Módulo de Validación de Firmas, es un dato informativo que se imprime en los logs del servicio.

credential: Es la credencial asignada para que ese sistema haga uso del servicio, al momento de su definición esta tiene que ser compartida con los desarrolladores que realizan la integración al servicio. Si después de tener definida una credencial para una aplicación o sistema, esta se cambia en este archivo, se tiene que enviar la nueva credencial a los desarrolladores de la aplicación o sistema para que realicen la actualización correspondiente y puedan seguir usando el servicio. Este valor es definido a criterio y no tiene un formato en particular.

La cantidad de credenciales registradas va a depender de la cantidad de integraciones por aplicación o sistema que usen del servicio, debiendo generar una credencial por cada aplicación o sistema.

2.3. Autorización de uso del servicio de validación

La entidad deberá de solicitar a la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros la autorización correspondiente para el uso del servicio, para lo cual debe de remitir un correo a firmaperu@pcm.gob.pe con el asunto "Solicitud de credenciales Firma Perú" con la siguiente información:

- Número de RUC
- Nombre de la entidad
- Siglas de la entidad
- Dirección completa de la entidad (incluir departamento, provincia y distrito)
- Número de DNI del contacto técnico ⁽¹⁾
- Nombres y apellidos del contacto técnico ⁽¹⁾
- Correo institucional del contacto técnico ⁽¹⁾
- Número de celular del contacto técnico ⁽¹⁾
- Descripción del uso del servicio, ejemplo: Validación de documentos internos, Validación de documentos de la entidad, etc.
- IP del servidor (producción y/o pruebas y desarrollo separado por ";").

⁽¹⁾ Esta información es de la persona técnica a quien se enviará la autorización.

En la respuesta al correo recibirá un archivo "vAuthorization.json", el cual define los parámetros necesarios para que el servicio funcione. Sin este archivo no podrá realizar operaciones de validación.

2.4. Configuración de la autorización para uso del servicio

En la ruta “user.home”/PCM/Validador/ poner el archivo “vAuthorization.json”, este archivo es enviado por la SGTD cuando se solicita el uso del servicio por parte de una entidad. Sin este archivo el servicio no funcionará, revisar apartado 3.2.1.

3. DOCUMENTACIÓN DE INTEGRACIÓN

3.1. Alcance

Este documento está orientado para los desarrolladores que se encarguen de integrar aplicaciones o sistemas al Módulo de Validación de Firmas mediante su API REST.

3.2. Especificación del API REST

El Módulo de Validación de Firmas expone 03 API REST, reemplazar el IP local 127.0.0.1 y el puerto 8080 por el IP y puerto del servidor donde está desplegado el servicio.

3.2.1. info

Sirve para obtener la información de configuración del servicio, este no recibe parámetros y retorna la información al realizar un GET a:

<http://127.0.0.1:8080/validador/api/info>

El servicio responde un objeto JSON con la información de configuración del servicio.

RESPUESTA	
<pre>{ "vAuthorization.json": "C:\\Users\\user\\PCM\\Validador\\vAuthorization.json - true", "credentials.json": "C:\\Users\\user\\PCM\\Validador\\credentials.json - true", "temp": "C:\\Users\\user\\PCM\\Temp", "log": "C:\\Users\\user\\PCM\\Validador\\log", "user.home": "C:\\Users\\user", "home": "C:\\Users\\user\\PCM\\Validador" }</pre>	
vAuthorization.json	Ruta completa donde tiene que ir el archivo vAuthorization.json, al final true indica si existe en esa ruta, false en caso contrario.
credentials.json	Ruta completa donde tiene que ir el archivo credentials.json, al final true indica si existe en esa ruta, false en caso contrario.

temp	Ruta donde se almacenan los archivos temporales.
log	Ruta donde está el archivo Validador.log
user.home	Ruta configurada como user.home para el contenedor de aplicaciones.
home	Ruta donde tienen que estar los archivos de configuración del servicio.

3.2.2. validation

Sirve para realizar operaciones de validación de documentos, recibe parámetros de tipo form-data los cuales se detallan a continuación:

POST: http://127.0.0.1:8080/validador/api/validation		
KEY	TYPE	DESCRIPTION
param	String	{ "documentExtension": "pdf" }
credential	String	Credencial de uso del servicio registrado en "credentials.json"
signed	File	Documento firmado para validar como Array de Bytes
original	File	Documento sin firma como Array de Bytes (Cuando se envía un *.p7s en signed)

La entrada "param" representa a un objeto JSON que tiene como especificación:

PARÁMETROS PARA VALIDACIÓN		
VAR	TIPO	DESCRIPCIÓN
documentExtension	String	Extensión del documento a validar en minúsculas.

El servicio responde un objeto JSON con el resultado de la validación.

RESPUESTA PARA PADES
{ "result" : "RESULTADO VÁLIDO", "validationDate" : "23/08/2022 14:40:42-0500", "file" : "demo[FP].pdf", "signatures" : 1, "validSignatures" : 1, "integrity" : "La integridad del documento y de sus firmas se mantiene.",



```
"observations" : [ "Todas las firmas digitales del documento son válidas." ],
"listSignatures" : [ {
  "number" : 1,
  "signer" : "PORTUGAL VARGAS PAULO CESAR FIR 44627780 hard",
  "status" : "VÁLIDO",
  "date" : "21/08/2022 11:56:21-0500",
  "format" : "PAdES_BASELINE_LTA",
  "signatureAlgorithm" : "RSA with SHA256",
  "rootInTsl" : true,
  "serial" : "5047E928C39167844A0B7EB7060CD1A8C4DBC6CC",
  "notBeFore" : "21/01/2022 12:22:07-0500",
  "notAfter" : "10/08/2025 21:53:42-0500",
  "chain" : [ "PORTUGAL VARGAS PAULO CESAR FIR 44627780 hard",
    "ECEP-RENIEC CA Class 2", "ECEP-RENIEC", "ECERNEP PERU CA
    ROOT 3" ],
  "trustSigningTime" : true,
  "timestampType" : "SIGNATURE_TIMESTAMP",
  "tsaNotes" : "Se utilizó un servicio de sello de tiempo al momento de la
  generación de la firma, la firma fue extendida.",
  "tsaDate" : "21/08/2022 11:56:25-0500",
  "tsaSignatureAlgorithm" : "RSA with SHA256",
  "rootTsaInTsl" : true,
  "tsaSerial" : "5D0103AB96F8FD0",
  "tsaNotBeFore" : "28/01/2022 10:44:35-0500",
  "tsaNotAfter" : "10/08/2033 16:36:50-0500",
  "tsaChain" : [ "PSVA-TSA-XXX TSU-20XX-XX", "EC-PSVA", "ECERNEP
  PERU CA ROOT X" ],
  "indications" : [ ],
  "informations" : [ ],
  "warnings" : [ ],
  "errors" : [ ],
  "notes" : [ "Razón / Motivo: Soy el autor del documento", "Ubicación:
  Plataforma Firma Perú 1.0.0 | DSS 5.11.1 | Windows | E86F38765E53 |
  192.168.1.9 | pportugal | user", "Fecha y hora: La firma se generó el
  21/08/2022 11:56:25-0500 (servicio de sello de tiempo)" ],
  "issuerDN" : "CN=ECEP-RENIEC CA Class 2, O=Registro Nacional de
  Identificación y Estado Civil, C=PE",
  "subjectDN" : "CN=PORTUGAL VARGAS PAULO CESAR FIR 44627780
  hard, SERIALNUMBER=PNOPE-44627780, GIVENNAME=PAULO CESAR,
  SURNAME=PORTUGAL VARGAS, OU=EREP_PN_RENIEC_4418965,
  L=Chorrillos, ST=Lima-Lima, C=PE",
  "contactInfo" : ""
} ],
"detailedReport" : "",
"trustedSignatures" : true,
"errorMessage" : "",
"generatedBy" : "Plataforma Firma Perú 1.0.0 | DSS 5.11.1 | Linux |
A86D38065E23 | 10.10.127.43 | validador | user"
}
```

RESPUESTA PARA XAdES

```
{
  "result" : "RESULTADO VÁLIDO",
  "validationDate" : "23/08/2022 14:40:42-0500",
}
```

```
"file" : "demo[FP].xml",
"signatures" : 1,
"validSignatures" : 1,
"integrity" : "La integridad del documento y de sus firmas se mantiene.",
"observations" : [ "Todas las firmas digitales del documento son válidas." ],
"listSignatures" : [ {
  "number" : 1,
  "signer" : "PORTUGAL VARGAS PAULO CESAR FIR 44627780 hard",
  "status" : "VÁLIDO",
  "date" : "21/08/2022 11:56:21-0500",
  "format" : "XAdES_BASELINE_LTA",
  "signatureAlgorithm" : "RSA with SHA256",
  "rootInTsl" : true,
  "serial" : "5047E928C39167844A0B7EB7060CD1A8C4DBC6CC",
  "notBefore" : "21/01/2022 12:22:07-0500",
  "notAfter" : "10/08/2025 21:53:42-0500",
  "chain" : [ "PORTUGAL VARGAS PAULO CESAR FIR 44627780 hard",
"ECEP-RENIEC CA Class 2", "ECEP-RENIEC", "ECERNEP PERU CA
ROOT 3" ],
  "trustSigningTime" : true,
  "timestampType" : "SIGNATURE_TIMESTAMP",
  "tsaNotes" : "Se utilizó un servicio de sello de tiempo al momento de la
generación de la firma, la firma fue extendida.",
  "tsaDate" : "21/08/2022 11:56:25-0500",
  "tsaSignatureAlgorithm" : "RSA with SHA256",
  "rootTsaInTsl" : true,
  "tsaSerial" : "5D0103AB96F8FD0",
  "tsaNotBefore" : "28/01/2022 10:44:35-0500",
  "tsaNotAfter" : "10/08/2033 16:36:50-0500",
  "tsaChain" : [ "PSVA-TSA-XXX TSU-20XX-XX", "EC-PSVA", "ECERNEP
PERU CA ROOT X" ],
  "indications" : [ ],
  "informations" : [ ],
  "warnings" : [ ],
  "errors" : [ ],
  "notes" : ["Fecha y hora: La firma se generó el 21/08/2022 11:56:25-0500
(servicio de sello de tiempo)" ],
  "issuerDN" : "CN=ECEP-RENIEC CA Class 2, O=Registro Nacional de
Identificación y Estado Civil, C=PE",
  "subjectDN" : "CN=PORTUGAL VARGAS PAULO CESAR FIR 44627780
hard, SERIALNUMBER=PNOPE-44627780, GIVENNAME=PAULO CESAR,
SURNAME=PORTUGAL VARGAS, OU=EREP_PN_RENIEC_4418965,
L=Chorrillos, ST=Lima-Lima, C=PE",
  "contactInfo" : ""
} ],
"detailedReport" : "",
"trustedSignatures" : true,
"errorMessage" : "",
"generatedBy" : "Plataforma Firma Perú 1.0.0 | DSS 5.11.1 | Linux |
A86D38065E23 | 10.10.127.43 | validador | user"
}
```

RESPUESTA PARA CAdES

```
{
  "result" : "RESULTADO VÁLIDO",
  "validationDate" : "23/08/2022 14:40:42-0500",
  "file" : "demo-png-detached[FP].p7s",
  "signatures" : 1,
  "validSignatures" : 1,
  "integrity" : "La integridad del documento y de sus firmas se mantiene.",
  "observations" : [ "Todas las firmas digitales del documento son válidas." ],
  "listSignatures" : [ {
    "number" : 1,
    "signer" : "PORTUGAL VARGAS PAULO CESAR FIR 44627780 hard",
    "status" : "VÁLIDO",
    "date" : "21/08/2022 11:56:21-0500",
    "format" : "CAdES_BASELINE_LTA",
    "signatureAlgorithm" : "RSA with SHA256",
    "rootInTsl" : true,
    "serial" : "5047E928C39167844A0B7EB7060CD1A8C4DBC6CC",
    "notBefore" : "21/01/2022 12:22:07-0500",
    "notAfter" : "10/08/2025 21:53:42-0500",
    "chain" : [ "PORTUGAL VARGAS PAULO CESAR FIR 44627780 hard",
      "ECEP-RENEIC CA Class 2", "ECEP-RENEIC", "ECERNEP PERU CA
      ROOT 3" ],
    "trustSigningTime" : true,
    "timestampType" : "SIGNATURE_TIMESTAMP",
    "tsaNotes" : "Se utilizó un servicio de sello de tiempo al momento de la
    generación de la firma, la firma fue extendida.",
    "tsaDate" : "21/08/2022 11:56:25-0500",
    "tsaSignatureAlgorithm" : "RSA with SHA256",
    "rootTsaInTsl" : true,
    "tsaSerial" : "5D0103AB96F8FD0",
    "tsaNotBefore" : "28/01/2022 10:44:35-0500",
    "tsaNotAfter" : "10/08/2033 16:36:50-0500",
    "tsaChain" : [ "PSVA-TSA-XXX TSU-20XX-XX", "EC-PSVA", "ECERNEP
    PERU CA ROOT X" ],
    "indications" : [ ],
    "informations" : [ ],
    "warnings" : [ ],
    "errors" : [ ],
    "notes" : ["Fecha y hora: La firma se generó el 21/08/2022 11:56:25-0500
    (servicio de sello de tiempo)" ],
    "issuerDN" : "CN=ECEP-RENEIC CA Class 2, O=Registro Nacional de
    Identificación y Estado Civil, C=PE",
    "subjectDN" : "CN=PORTUGAL VARGAS PAULO CESAR FIR 44627780
    hard, SERIALNUMBER=PNOPE-44627780, GIVENNAME=PAULO CESAR,
    SURNAME=PORTUGAL VARGAS, OU=EREP_PN_RENEIC_4418965,
    L=Chorrillos, ST=Lima-Lima, C=PE",
    "contactInfo" : ""
  } ],
  "detailedReport" : "",
  "trustedSignatures" : true,
  "errorMessage" : "",
  "generatedBy" : "Plataforma Firma Perú 1.0.0 | DSS 5.11.1 | Linux |
  A86D38065E23 | 10.10.127.43 | validador | user"
}
```

INTERPRETACIÓN DE LA RESPUESTA JSON

El resultado del proceso de validación está definido en el valor contenido en "result" el cual puede tener como valores:

RESULTADO VÁLIDO	La integridad del documento y de sus firmas se mantiene. Todas las firmas digitales del documento son válidas.
RESULTADO INDETERMINADO	La integridad del documento y de sus firmas se mantiene. Revisar las indicaciones del proceso de validación, posibles causas: - Uno o más certificados han expirado. - Uno o más certificados raíz no están en la TSL. - No se puede obtener la información de verificación de uno o más certificados (TSL, CRL, OCSP).
RESULTADO NO VÁLIDO	La integridad del documento o de alguna firma está comprometida. Revisar las indicaciones del proceso de validación, posibles causas: - El documento fue modificado después de ser firmado. - Ha ocurrido un error al momento de generar alguna firma.
SIN FIRMAS DIGITALES	Documento sin firmas digitales.

3.2.3. clean_temp

Sirve para limpiar los temporales existentes en caso presente problemas al validar un documento, recibe un parámetro de tipo x-www-form-urlencoded el cual se detalla a continuación:

POST: http://127.0.0.1:8080/validador/api/clean_temp		
KEY	TYPE	DESCRIPTION
credential	String	Credencial de uso del servicio registrado en "credentials.json"

El servicio responde un objeto JSON con el resultado de la operación.

RESPUESTA OK
<pre>{ "status": "ok" }</pre>

**RESPUESTA ERROR**

```
{  
  "error_message": "No está autorizado para utilizar el servicio de validación.",  
  "status": "error"  
}
```

3.3. Información general

Archivos temporales están en “user.home”/PCM/Temp (CRL,TSL, Token).

El log está guardado en:

- “user.home”/PCM/Validador/log/Validador.log

EL servicio de validación de firmas debe ser desplegado únicamente en la red interna de servidores ya que su finalidad es consumir el servicio web que expone por las aplicaciones de la entidad, no se tiene que exponer el servicio mediante una URL.