

Firma electrónica

“firma.gub.uy”

Manual técnico de integración firma.gub.uy con sistemas externos

Sumario

Introducción.....	3
Propósito.....	3
Audiencia.....	3
Integración.....	3
Descripción general.....	4
Descripción del proceso.....	6
Carga y envío de documentos.....	6
Redirección a “firma.gub.uy”	8
En la plataforma de “firma.gub.uy”	8
La plataforma detecta que se ha completado el proceso de firma.....	9
De regreso al sistema externo.....	9
Descarga de documentos.....	9
Descripción de APIS.....	11
Iniciar proceso de firma.....	11
Iniciar proceso de firma (solo metadatos).....	15
Iniciar proceso de firma.....	17
Consultar estado del proceso de firma.....	21
Obtener Archivos firmados (todos juntos).....	23
Obtener archivo firmado(forma individual).....	24
Obtener Información sobre las firmas de un archivo.....	25
Anexos.....	27
1. Se agrega anexo de colecciones de postman para cada una de las api de sistemas externos.....	27
Historial de cambios.....	27



Introducción

El presente documento detalla la integración de “firma.gub.uy” con los sistemas externos.

Los sistemas externos que se integren podrán enviar uno o mas documentos PDFs para firmar mediante el consumo de API tipo rest, después se hará una redirección a la url de la plataforma de “firma.gub.uy”, para firmar ahí los documentos y retornar nuevamente al sistema externo, recibiendo los documentos firmados.

Propósito

El presente documento tiene por propósito dar a conocer la descripción técnica del mecanismo de integración entre la plataforma de “firma.gub.uy” con sistemas externos.

Audiencia

Dirigido a técnicos, funcionales y desarrolladores.

Integración.

La **plataforma firma.gub.uy** permite firmar documentos PDF usando dispositivos locales (**cédula de identidad electrónica o e-tokens**) y servicios en la nube (actualmente **TuID de Antel** e **Identidad Mobile de Abitab**). La integración es independiente del medio de firma elegido por el usuario.

A efectos de ilustrar el procedimiento de integración de un sistema externo con la plataforma se mostrará las interacciones utilizando el aplicativo de firma y la firma en la nube.

Por **sistema externo** se entiende cualquier **aplicación web**, funcionando bajo cualquier plataforma, sistema operativo y arquitectura, y desarrollada en cualquier lenguaje de programación, que sea capaz de consumir **servicios web** de tipo rest y que pueda exponer un **recurso web** (una página, servlet u otro mecanismo) al cual la plataforma de firma electrónica pueda hacerle un **GET** a los efectos de notificarle(retornar) cuando el proceso de firma esté finalizado.



Estrictamente hablando, también pueden ser sistemas externos que se integren con “firma.gub.uy” cualquier otra aplicación, aunque no sea web, siempre que pueda consumir servicios web (rest). En este caso, como la aplicación no podrá exponer un recurso web donde la plataforma de firma electrónica pueda notificarle, será responsabilidad de la aplicación hacer un polling constante preguntando por el estado del proceso de firma, hasta obtener como respuesta el documento firmado. Esto no es aconsejable por la sobrecarga que produce sobre la red y sobre el servidor de la firma.gub.uy.

Descripción general

En la siguiente imagen se muestra la iteración completa entre los sistemas externos, plataforma firma.gub.uy, APIs para los sistemas externos, y aplicativo de firma o firma en la nube, estos 2 últimos según corresponda. describiendo de forma visual el flujo a seguir en cada etapa del proceso de firma, desde su inicio hasta su fin.

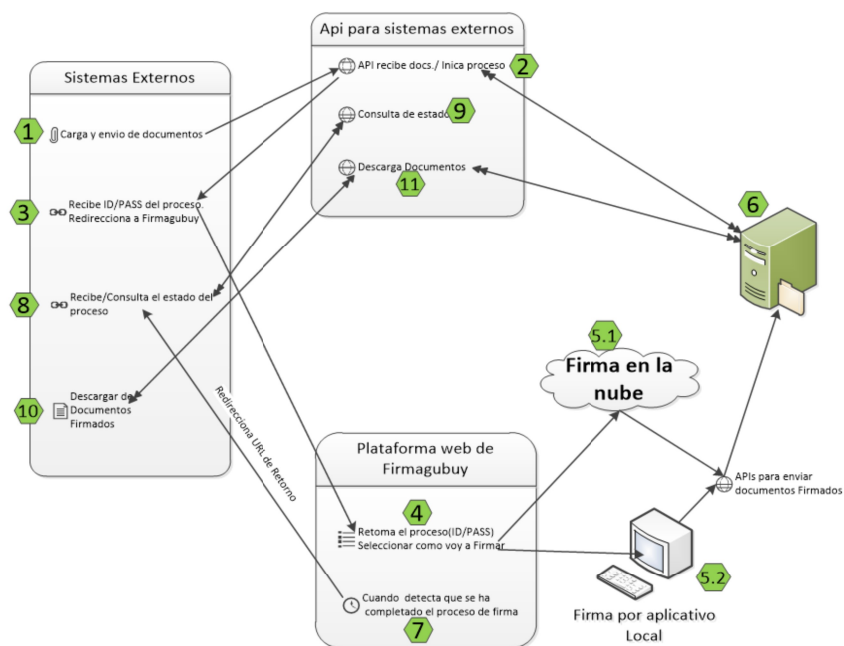


Figura 1: Flujo de “firma.gub.uy” con sistemas externos

Descripción del proceso

Carga y envío de documentos.

El sistema externo carga y envía uno o mas documentos PDF para firmar.

- El envío de documentos se puede hacer de dos formas:
 - a. Envío de documentos en base64 dentro de un json e invocando la api de tipo POST `"/api/v1/externos/proceso1"`, un ejemplo es:

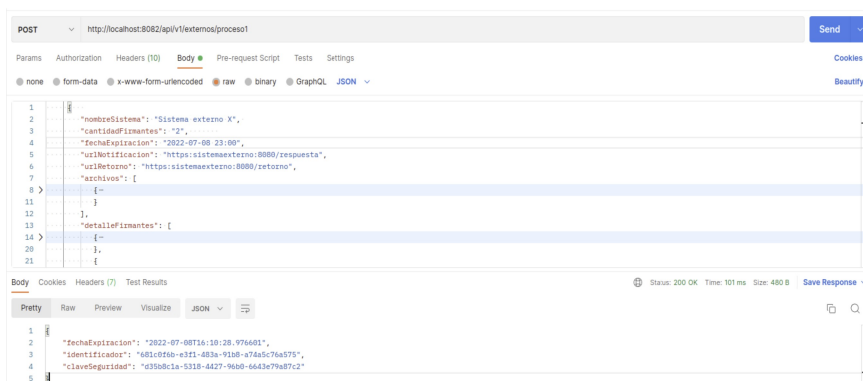


Figura 2: Ejemplo de iniciar proceso base64

- b. Envío de documentos utilizado 2 apis, la primera “carga de archivo” api `"/api/v1/externos/archivo"` envía cada documento y devuelve un identificador de documento que después se utilizará para iniciar el proceso de firma, los identificadores de archivos van dentro de un json y se envían a la api `"/api/v1/externos/proceso2"`, los ejemplos de lo anterior son:



Carga de archivo.

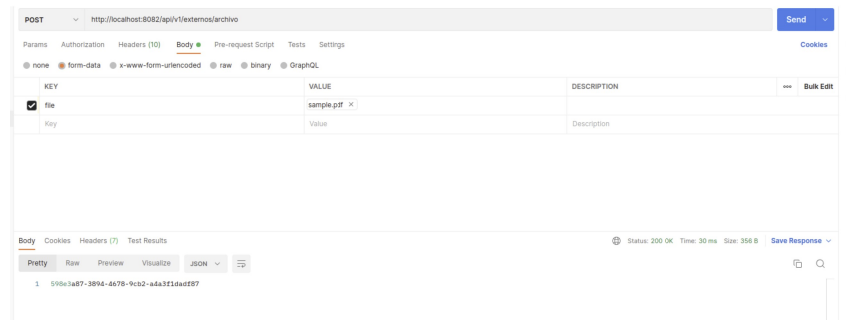


Figura 3: Ejemplo de carga de archivo (uno por uno)

Envío de Json con los identificadores de archivos, previamente cargados

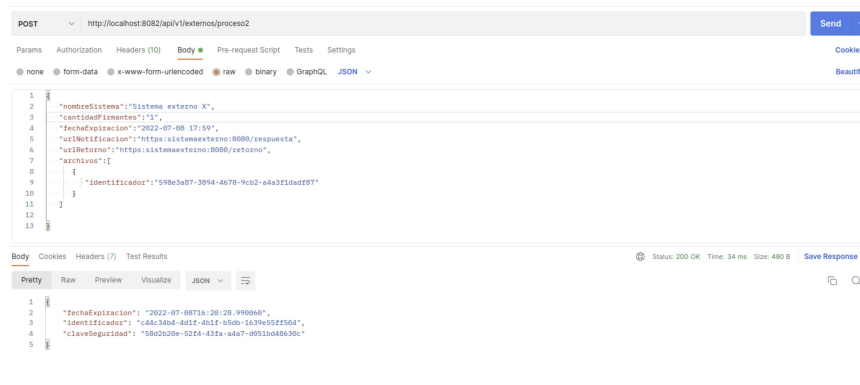


Figura 4: Ejemplo de iniciar proceso con los identificadores de archivos

- En el body en ambos procesos se debe de agregar algunas propiedades opcionales, nombreSistema, cantidadFirmantes, fechaExpiracion, urlNotificacion, urlRetorno. Se amplía esto más adelante en la documentación de cada api.
- Las apis de inicio de proceso devuelven un identificador, claveSeguridad y fechaExpiracion, siendo el identificador y claveSeguridad necesarios para identificar al proceso de firma.

Redirección a “firma.gub.uy”

Una vez que la aplicación externa comenzó un proceso de firma, obtiene como resultado un identificador y una clave de seguridad, el usuario del sistema externo debe ser redirigido a una página específica de la plataforma para que pueda realizar la firma del documento.

Esta página es identificada por la siguiente URL:

`https://<host>:<port>/es/pp/firmar?id=c44c34b4-4d1f-4b1f-b5db-1639e55ff504&pass=58d2b20e-52f4-43fa-a4a7-d051bd48630c`

Donde “c44c34b4-4d1f-4b1f-b5db-1639e55ff504” debe ser sustituido por el identificador del proceso y “58d2b20e-52f4-43fa-a4a7-d051bd48630c” es la clave de seguridad, asignado por la plataforma al proceso de firma.

En la plataforma de “firma.gub.uy”.

- La plataforma identifica el proceso de firma por medio de “id” y “pass” pasados como parametros.
- Dentro de la plataforma el usuario debe de elegir como quiere firmar, la plataforma guiará dependiendo su elección
- En el caso que seleccione firmar con Antel o Abitab la firma se completara en la plataforma de ellos, siguiendo los pasos que se indiquen, como punto final este proceso incluye el envío de los documentos firmados al servidor.
- Si selecciona firmar con dispositivo, tendrá las opciones de firmar con cédula, token abitab o token correo, en todos estos casos la firma se hará descargando un archivo con extensión “.firmagubuy” que la plataforma le guiara hasta llegar a la descarga. Luego se abrirá este archivo el cual a su vez abre al aplicativo de firma en donde se



completará la firma. Como punto final el aplicativo de firma enviara al servidor los archivos firmados mediante apis.

La plataforma detecta que se ha completado el proceso de firma

La plataforma de “firma.gub.uy”, se quedó esperando, cuando detecta que el proceso de firma ha sido completado, la plataforma hará una redirección hacia la url de retorno proporcionada al inicio del proceso de firma, agregando como parámetro el estado del proceso de firma.

De regreso al sistema externo

El sistema externo, podra consultar el estado del proceso de firma (si lo estima conveniente) haciendo esto por medio del api “{URL}/api/v1/externos/estado/681c0f6b-e3f1-483a-91b8-a74a5c76a575”, se detalla un ejemplo en la siguiente imagen.

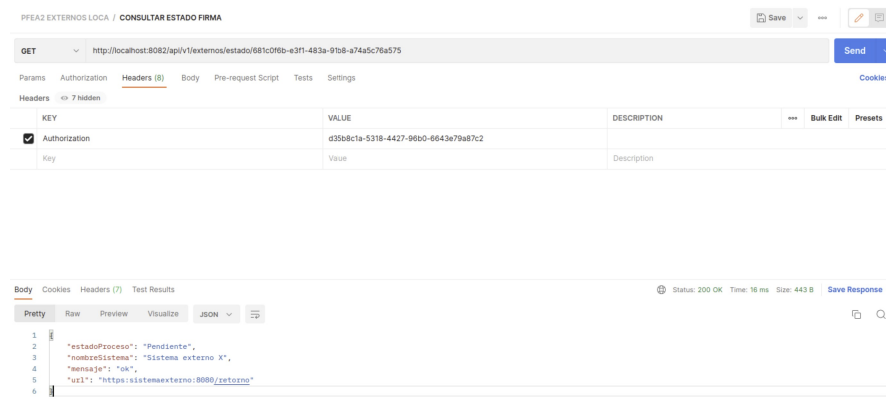


Figura 5: Ejemplo de consulta de estado de proceso de firma

Descarga de documentos

El sistema externo invoca el api para descargar los documentos, aquí tiene 2 opciones.

- Descargar documento uno a uno, invocando la api “{URL}/api/v1/externos/archivo/598e3a87-3894-4678-9cb2-a4a3f1dadf87”, siendo en este caso “598e3a87-3894-4678-9cb2-



a4a3f1dadf87” el identificador de archivo que deseamos descargar . Para usar esta opción se debe de iniciar el proceso de firma desde el api “/api/v1/externos/proceso2” y el sistema externo debe de guardar los identificadores de archivos asociados al proceso, para pedir los archivos individualmente por medio de estos. (ver documentación de api)

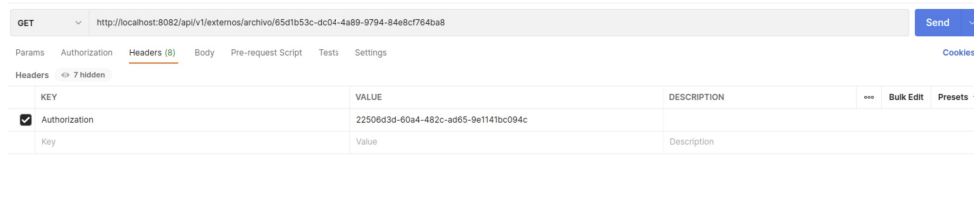


Figura 6: Ejemplo de descarga de archivo (individual)

- Descargar de documentos todos juntos, se utilizara el api “{URL}/api/v1/externos/archivos/681c0f6b-e3f1-483a-91b8-a74a5c76a575” siendo “681c0f6b-e3f1-483a-91b8-a74a5c76a575” el identificador del proceso de firma. Esta api nos devolverá en un json el listado de archivos en base64. Ejemplo:

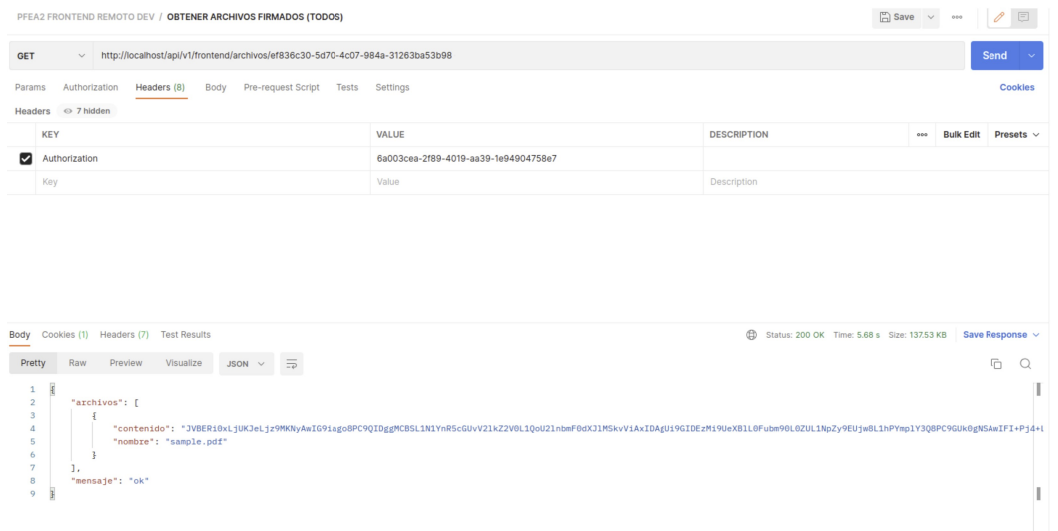


Figura 7: Ejemplo de obtener documentos firmados (todos)



Descripción de APIS

Iniciar proceso de firma

Datos generales				
Descripción	Permite a los sistemas externos generar un proceso de firma a partir de uno o más archivos y otros datos.			
Método HTTP	POST			
Path	/api/externos/proceso1			
Entrada	application/json			
Salida	application/json			
Parámetros de entrada				
archivos	Lista de archivos	Obligatorio; debe contener al menos un archivo.		
		nombre	Texto	Obligatorio; nombre del archivo.
		contenido	Bytes	Obligatorio; contenido del archivo, en formato Base64.
nombre_sistema	Texto	Obligatorio; nombre del sistema que inicia el proceso, para mos-		



		trar al usuario y para auditoría.		
firma_longeva	Sí/No	Opcional; indicador de si se requiere utilizar firma longeva o no. Si no se es especifica se asume que no se utiliza firma longeva.		
cantidad_firmantes	Entero	Opcional; cantidad de firmas que deben efectuarse sobre el archivo. Si no se proporciona, se asume "1". Si se proporciona el valor "0", no se limita la cantidade firmantes.		
detalles_firmantes	Lista de firmantes	Opcional; detalles sobre los firmantes, para mostrar antes de proceder a la firma de cada uno de los usuarios. Si el largo de la lista es menor a la cantidad de firmantes, los firmantes en exceso serán tratados como anónimos, con los valores asumidos para todas las variables. Si el largo de la lista es mayor a la cantidad de firmantes, se ignoran los firmantes en exceso. Para cada firmante se debe especificar:		
		documento_numero	Texto	Opcional; número de documento de la persona que debe firmar. Si se proporciona, el API debe validar que la persona que firma el archivo pueda ser identificada con el mismo número en el certificado digital que usa para firmar.
		documento_pais	Texto	Opcional; código ISO2 del país emisor del documento de la persona que debe firmar. Si se pro-



				porciona el parámetro documento_numero pero no se proporciona este parámetro, se asume "UY" (Uruguay).
		documento_tipo	Texto	Opcional; tipo de documento, según el catálogo de tipos de documentos que determine AGESIC. Si se proporciona el parámetro documento_numero pero no se proporciona este parámetro, se asume el valor que corresponda a la cédula de identidad.
		forzar_cedula	Sí/No	Opcional; indicador de si se debe forzar que la firma de los archivos sea realizada utilizando una cédula de identidad electrónica o no. Si se omite, se asume "No".
		validar_firmante	Sí/No	Opcional; indicador de si se debe validar que la persona que firma puede identificarse mediante el certificado digital. Si se omite, se asume "No".
fecha_limite	Fecha y hora	Opcional; fecha y hora límites para que el proceso de firma sea completado. Si se proporciona, el API puede limitarlo a un período menor, según configuración. Si no se proporciona, el API		



		debe asignarle un valor, según configuración.
url_notificación	URL	<p>Opcional; URL a donde la plataforma de firma debe notificar que el proceso de firma fue completado. El recurso detrás de esta URL debe aceptar el método POST, incluyendo en el cuerpo (body) del mensaje los siguientes parámetros en formato JSON:</p> <p>identificador: identificador del proceso de firma finalizado (UUID).</p> <p>estado: estado del proceso de firma ('FINALIZADO', 'RECHAZADO').</p> <p>Si se omite, el sistema externo no podrá ser notificado cuando el proceso de firma se complete, debiendo hacer polling constante utilizando el método de consulta de estado.</p>
url_retorno	URL	<p>Opcional; URL a la cual la plataforma de firma debe redirigir al usuario luego de que éste complete la firma de los archivos. (se espera que el sistema externo pueda continuar con su proceso, ya sea incluyendo un identificador en la propia URL o tomando los datos de la sesión, o de otra manera, a su criterio). Si no se especifica, al finalizar el proceso de firma el usuario quedará viendo una pantalla de confirmación propia de la plataforma.</p>
Parámetros de salida		
	identificador	<p>UUID</p> <p>Identifica unívocamente a un proceso de firma.</p>



200	clave_seguridad	Texto	Clave de seguridad que deberá ser proporcionada para consultar el estado del proceso de firma y obtener los archivos firmados.
	fecha_expiracion	Fecha y hora	<p>Fecha y hora de expiración del proceso de firma. Esta fecha es calculada por la plataforma, de la siguiente manera:</p> <p>Si la invocación no incluye el parámetro “fecha_limite”, se calcula como (ahora + N minutos), donde N es un parámetro de configuración denominado “PLAZO_EXPIRACION”.</p> <p>Si la invocación incluye el parámetro “fecha_limite”, y el mismo es válido (la diferencia entre ahora y dicha fecha es menor o igual a un parámetro de configuración denominado “PLAZO_MAXIMO_EXPIRACION”), entonces es la misma fecha.</p> <p>Si la invocación incluye el parámetro “fecha_limite”, pero el no mismo es válido (la diferencia entre ahora y dicha fecha es mayor a un parámetro de configuración denominado “PLAZO_MAXIMO_EXPIRACION”), entonces se calcula como (ahora + N minutos), donde N es un parámetro de configuración denominado “PLAZO_MAXIMO_EXPIRACION”.</p>
400	mensaje	Texto	Mensaje explicativo en el caso de fallo.



Iniciar proceso de firma (solo metadatos)

Datos generales			
Descripción		Permite a un sistema externo cargar un único archivo, obteniendo un identificador para el mismo. Se debe tener en cuenta que aún no se generó un proceso de firma para este archivo, sino que se hará posteriormente cuando se hayan cargado todos los archivos correspondientes.	
Método HTTP		POST	
Path		/api/externos/archivo	
Entrada		application/octet-stream	
Salida		application/json	
Parámetros de entrada			
archivo	Archivo	Obligatorio; el archivo debe ser pasado en formato binario.	
nombre	Texto	Obligatorio; debe ser pasado usando el header "Content-Disposition".	
Parámetros de salida			
200	identificador	UUID	Identifica unívocamente a un archivo.
400	mensaje	Texto	Mensaje explicativo en el caso de fallo.



Iniciar proceso de firma

Datos generales		
Descripción	Permite a los sistemas externos generar un proceso de firma a partir de uno o más archivos cargados previamente utilizando el endpoint “Cargar archivo”.	
Método HTTP	POST	
Path	/api/externos/proceso2	
Entrada	application/json	
Salida	application/json	
Parámetros de entrada		
archivos	Lista de identificadores	Obligatorio; debe contener al menos un identificador, y todos ellos deben corresponderse a archivos cargados previamente utilizando el endpoint “Cargar archivo” y que no estén asociados aún a ningún proceso de firma.
nombre_sistema	Texto	Obligatorio; nombre del sistema que inicia el proceso, para mostrar al usuario y para auditoría.
firma_longeva	Sí/No	Opcional; indicador de si se requiere utilizar firma longeva o no. Si no se especifica se asume que no se utiliza firma longeva.



cantidad_firmantes	Entero	Opcional; cantidad de firmas que deben efectuarse sobre el archivo. Si no se proporciona, se asume "1". Si se proporciona el valor "0", no se limita la cantidad de firmantes.		
detalles_firmantes	Lista de firmantes	Opcional; detalles sobre los firmantes, para mostrar antes de proceder a la firma de cada uno de los usuarios. Si el largo de la lista es menor a la cantidad de firmantes, los firmantes en exceso serán tratados como anónimos, con los valores asumidos para todas las variables. Si el largo de la lista es mayor a la cantidad de firmantes, se ignoran los firmantes en exceso. Para cada firmante se debe especificar:		
		documento_numero	Texto	Opcional; número de documento de la persona que debe firmar. Si se proporciona, el API debe validar que la persona que firma el archivo pueda ser identificada con el mismo número en el certificado digital que usa para firmar.
		documento_pais	Texto	Opcional; código ISO2 del país emisor del documento de la persona que debe firmar. Si se proporciona el parámetro documento_numero pero no se proporciona este parámetro, se asume "UY" (Uruguay).



		documento_tipo	Texto	Opcional; tipo de documento, según el catálogo de tipos de documentos que determine AGESIC. Si se proporciona el parámetro documento_numero pero no se proporciona este parámetro, se asume el valor que corresponda a la cédula de identidad.
		forzar_cedula	Sí/No	Opcional; indicador de si se debe forzar que la firma de los archivos sea realizada utilizando una cédula de identidad electrónica o no. Si se omite, se asume "No".
		validar_firmante	Sí/No	Opcional; indicador de si se debe validar que la persona que firma puede identificarse mediante el certificado digital. Si se omite, se asume "No".
fecha_limite	Fecha y hora	Opcional; fecha y hora límites para que el proceso de firma sea completado. Si se proporciona, el API puede limitarlo a un período menor, según configuración. Si no se proporciona, el API debe asignarle un valor, según configuración.		
url_notificacion	URL	Opcional; URL a donde la plataforma de firma debe notificar que el proceso de firma fue completado. El recurso detrás de esta URL debe aceptar el método POST, incluyendo en el cuerpo		



			<p>(body) del mensaje los siguientes parámetros en formato JSON:</p> <ul style="list-style-type: none"> identificador: identificador del proceso de firma finalizado (UUID). estado: estado del proceso de firma ('FINALIZADO', 'RECHAZADO'). <p>Si se omite, el sistema externo no podrá ser notificado cuando el proceso de firma se complete, debiendo hacer polling constante utilizando el método de consulta de estado.</p>
url_retorno	URL		<p>Opcional; URL a la cual la plataforma de firma debe redirigir al usuario luego de que éste complete la firma de los archivos. (se espera que el sistema externo pueda continuar con su proceso, ya sea incluyendo un identificador en la propia URL o tomando los datos de la sesión, o de otra manera, a su criterio). Si no se especifica, al finalizar el proceso de firma el usuario quedará viendo una pantalla de confirmación propia de la plataforma.</p>
Parámetros de salida			
200	identificador	UUID	Identifica unívocamente a un proceso de firma.
	clave_seguridad	Texto	Clave de seguridad que deberá ser proporcionada para consultar el estado del proceso de firma y obtener los archivos firmados.
	fecha_expiracion	Fecha y hora	Fecha y hora de expiración del proceso de firma. Esta fecha es calculada por la plataforma, de la siguiente manera:



			<ul style="list-style-type: none"> • Si la invocación no incluye el parámetro “fecha_limite”, se calcula como (ahora + N minutos), donde N es un parámetro de configuración denominado “PLAZO_EXPIRACION”. • Si la invocación incluye el parámetro “fecha_limite”, y el mismo es válido (la diferencia entre ahora y dicha fecha es menor o igual a un parámetro de configuración denominado “PLAZO_MAXIMO_EXPIRACION”), entonces es la misma fecha. • Si la invocación incluye el parámetro “fecha_limite”, pero el no mismo es válido (la diferencia entre ahora y dicha fecha es mayor a un parámetro de configuración denominado “PLAZO_MAXIMO_EXPIRACION”), entonces se calcula como (ahora + N minutos), donde N es un parámetro de configuración denominado “PLAZO_MAXIMO_EXPIRACION”.
400	mensaje	Texto	Mensaje explicativo en el caso de fallo.

Consultar estado del proceso de firma.

Datos generales	
Descripción	Permite al módulo frontend o sistemas externos consultar el estado de un proceso de firma (pendiente, completado, obsoleto).
Método HTTP	HEAD



Path		/api/externos/estado/{identificador}	
Entrada		No tiene	
Salida		application/json	
Parámetros de entrada			
identificador		UUID	Obligatorio; identificador del proceso de firma que se desea consultar.
clave_seguridad		Texto	Obligatorio; clave de seguridad correspondiente al proceso de firma; debe ser pasado utilizando el encabezado “Authorization”.
Parámetros de salida			
200		json	Devuelve un json con la siguiente información: estadoProceso, nombreSistema, mensaje y url de retorno.
304	mensaje	Texto	Sin Mensaje
403	mensaje	Texto	Mensaje indicando que la clave de seguridad no es correcta.
404	mensaje	Texto	Mensaje indicando que el proceso de firma no existe o ya está expirado.



Obtener Archivos firmados (todos juntos)

Datos generales				
Descripción		Permite al módulo frontend obtener todos los archivos firmados correspondientes a un proceso de firma.		
Método HTTP		GET		
Path		/api/externos/archivos/{identificador}		
Entrada		No tiene		
Salida		application/json		
Parámetros de entrada				
identificador		UUID	Obligatorio; identificador del proceso de firma para el cual se desean obtener los archivos firmados.	
clave_seguridad		Texto	Obligatorio; clave de seguridad correspondiente al proceso de firma; debe ser pasado utilizando el encabezado “Authorization”.	
Parámetros de salida				
200	archivo	Lista de archivos	Lista de archivos firmados. Para cada archivo se proporcionan los siguientes datos:	
			nombre	Texto Nombre original del archivo.



			contenido	Bytes	Contenido del archivo, en formato Base64.
304	mensaje	Texto	Sin mensaje.		
403	mensaje	Texto	Mensaje indicando que la clave de seguridad no es correcta.		
404	mensaje	Texto	Mensaje indicando que el proceso de firma no existe o ya está expirado.		

Obtener archivo firmado(forma individual)

Datos generales	
Descripción	Permite al módulo frontend obtener un archivos firmados correspondiente a un proceso de firma.
Método HTTP	GET
Path	/api/externos/archivo/{identificador}
Entrada	No tiene
Salida	application/octet-stream
Parámetros de entrada	



identificador	UUID	Obligatorio; identificador del archivo para el cual se desea obtener su correspondiente archivo firmado.
clave_seguridad	Texto	Obligatorio; clave de seguridad correspondiente al proceso de firma al cual pertenece el archivo; debe ser pasado utilizando el encabezado "Authorization".
Parámetros de salida		
200	archivo	Archivo Archivo firmado. El contenido del archivo se devuelve en formato binario, mientras que el nombre del mismo se informa a través del header "Content-Disposition".
304	mensaje	Texto Sin Mensaje
403	mensaje	Texto Mensaje indicando que la clave de seguridad no es correcta.
404	mensaje	Texto Mensaje indicando que el proceso de firma no existe o ya está expirado.



Obtener Información sobre las firmas de un archivo.

Datos generales			
Descripción		Permite al módulo frontend obtener un archivos firmados co- rrespondiente a un proceso de firma.	
Método HTTP		GET	
Path		/api/externos/archivo/{identificador}	
Entrada		No tiene	
Salida		application/octet-stream	
Parámetros de entrada			
identificador		UUID	Obligatorio; identificador del archivo para el cual se desea obtener su correspondiente archivo fir- mado.
clave_seguridad		Texto	Obligatorio; clave de seguridad correspondiente al proceso de firma al cual pertenece el archivo; debe ser pasado utilizando el encabezado “Authoriza- tion”.
Parámetros de salida			
200	archivo	Archivo	Archivo firmado. El contenido del archivo se de- vuelve en formato binario, mientras que el nombre



			del mismo se informa a través del header “Content-Disposition”.
304	mensaje	Texto	Sin mensaje
403	mensaje	Texto	Mensaje indicando que la clave de seguridad no es correcta.
404	mensaje	Texto	Mensaje indicando que el proceso de firma no existe o ya está expirado.

Anexos

1. Se agrega anexo de colecciones de postman para cada una de las api de sistemas externos



Historial de cambios

Versión	Fecha	Autor	Detalle
1.0	08-jul-2022	Jorge Valenzuela.	Primera versión del documento.

