Control de versiones			
Versión	**Descripción**	**Fecha**	**Modificado por**
2.0	Envió de OTP por correo electrónico	09/07/2020	Camilo Molina
2.1	Servicio de estampado de pdf	26/08/2020	Camilo Molina

Tabla de Contenido

1. Objetivo

Este documento pretende describir de manera técnica y detallada el consumo del servicio web para firma digital centralizada.

2. Operaciones del servicio

A continuación, se detallan las operaciones disponibles expuestas en un servicio en el servicio de firma centralizada.

2.1 Autenticación

Operación POST para realizar la autenticación y obtener un token para el consumo de las operaciones de firma.

URL Pruebas:
https://8uw10ruhfj.execute-api.us-east-2.amazonaws.com/qa/authentication/api/Login

URL Producción:
https://hdko60xft2.execute-api.us-east-2.amazonaws.com/pro/authentication/api/Login

2.1.1 Parámetros

Objeto JSON que debe cumplir con los siguientes atributos

Nombre	Tipo	Tamaño	Obligatorio	Descripción
Usuario	Cadena	30	Si	Usuario para autenticación
Clave	Cadena	30	Si	Clave del usuario

2.1.2 Ejemplo JSON de entrada

```
{
    "Usuario" : "xxxxxx",
    "Clave" : "yyyyyyyyy"
}
```

2.1.3 Respuesta

Como respuesta de la operación de autenticación se obtiene un JSON con la siguiente estructura:

Nombre	Tipo	Tamaño	Obligatorio	Descripción
codigoRespuesta	Alfanumérico	3	Si	Código del resultado de la transacción
httpStatus	Numérico		Si	Código http del estado de la transacción
descripcionRespuesta	Alfanumérico	max	Si	Descripción del código de la transacción
detalleRespuesta	Listado Alfanumérico		No	Especificación de inconsistencias en los parámetros
token	Alfanumérico	max	No	Token para autenticación

2.1.4 Ejemplo JSON de salida


```
{
    "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJVc3VhcmlvIjoiZ3N",
    "httpStatus": 201,
    "codigoRespuesta": "R1",
    "descripcionRespuesta": "Transacción exitosa, usuario autenticado.",
    "detalleRespuesta": null
}
```

2.1.5 Valores para el atributo de codigoRespuesta

Código	Descripción
RS1	Transacción exitosa, usuario autenticado.
RS2	La estructura de la petición no corresponde con la requerida.
RS3	Las credenciales son invalidas.
RS4	El cliente se encuentra inactivo.
RS5	Lo sentimos, ha ocurrido un error interno y no pudimos completar tu solicitud.

2.2 Firma digital

Operación POST que permite realizar la firma digital de un documento pdf con el envío de un objeto JSON. Como resultado del firmado se obtendrá un objeto en formato JSON con la respuesta de la transacción.
El método de acceso se realiza mediante Bearer Authentication el cual es un esquema de autenticación http que involucra tokens de seguridad (Bearer Token), generado por el servicio de autenticación.

URL Pruebas:
https://8uw10ruhfj.execute-api.us-east-2.amazonaws.com/qa/signature/api/sign/pades

URL Producción:
https://hdko60xft2.execute-api.us-east-2.amazonaws.com/pro/signature/api/sign/pades

2.2.1 Parámetros de entrada

Objeto JSON que debe cumplir con los siguientes atributos

Nombre	Tipo	Tamaño	Obligatorio	Descripción
numeroDocumento	Alfanumérico	20	Si	Identificador del certificado digital
clave	Alfanumérico	15	Si	Clave del certificado

base64	Alfanumérico	5 MB	Si	Documento pdf a firmar codificado en base64
usuarioTSA	Alfanumérico	20	No	Usuario de la tsa, es obligatorio cuando se desea agregar marca de tiempo en la firma
claveTSA	Alfanumérico	20	No	Clave de la tsa, es obligatorio cuando se desea agregar marca de tiempo en la firma
razon	Alfanumérico	30	No	Campo razón del detalle de la firma
ubicacion	Alfanumérico	30		Campo Ubicación del detalle de la firma
conLTV	boolean		Si	Indica si de desea marcar la firma como LTV
conEstampa	boolean		Si	Indica se coloca una marca de tiempo en el documento
firmaVisible	boolean		Si	Indica si de desea colocar la firma visible en el documento pdf
imagenFirma	ImagenFirma		Si	Especifica las propiedades de la firma visible

Objeto de entrada **ImagenFirma**

Nombre	Tipo	Tamaño	Obligatorio	Descripción
x	float		Si	Posicionamiento en el eje Y de la imagen.
y	float		Si	Posicionamiento en el eje Y de la imagen.
ancho	float		Si	Ancho de la imagen
alto	float		Si	Alto de la imagen
imagen	Alfanumérico	MAX	Si	Imagen codificada en base64
pagina	int		Si	Página en la que se va a posicionar la imagen de la firma

2.2.2 Ejemplo JSON de entrada


```
{
    "numeroDocumento": "xxxxxxx",
    "base64": "JVBERi0xLjcNCiW1tbW1DQoxIDAgb2JqDQo8PC9UeXBlLONhdGFsb2cvU=",
    "clave": "yyyyyyy",
    "usuarioTSA": "xxxxxxx",
    "claveTSA": "yyyyyyyy",
    "ubicacion": "",
    "razon": "",
    "conLTV": true,
    "conEstampa": false,
    "firmaVisible": true,
    "imagenFirma": {
        "x": "100",
        "y": "100",
        "ancho": "70",
        "alto": "100",
        "imagen": "/9j/4AAQSkZJRgABAQAAAQABAAD/2wCEAAgGBgcG",
        "pagina": "1"
    }
}
```


2.2.3 Respuesta

Como respuesta de la operación firma digital se va a devolver un JSON con la siguiente estructura:

Nombre	Tipo	Tamaño	Obligatorio	Descripción
codigoRespuesta	Alfanumérico	5	Si	Código de respuesta obtenido del proceso de firma
mensaje	Alfanumérico		Si	Descripción de la respuesta
httpStatus	Numérico		Si	Código http del estado de la transacción
documentoFirmado	Alfanumérico	MAX	No	Documento firmado y codificado en base64

2.2.4 Ejemplo JSON de respuesta

El siguiente es un ejemplo JSON con el response de la petición


```
{
    "mensaje": "Documento firmado exitosamente",
    "documentoFirmado": "FxggGC4nHR8gHhgaICspLCQlKCgoGxOtMSwmMCInKCYBC",
    "codigoRespuesta": "RS1",
    "httpStatus": 200
}
```


2.3 Firma electrónica

Operación POST que permite realizar la firma electrónica de un documento pdf con el envío de un objeto JSON. Como resultado del firmado se obtendrá un objeto en formato JSON con la respuesta de la transacción.

El método de acceso se realiza mediante Bearer Authentication el cual es un esquema de autenticación http que involucra tokens de seguridad (Bearer Token), generado por el servicio de autenticación.

URL Pruebas:
https://8uw10ruhfj.execute-api.us-east-2.amazonaws.com/qa/signature/api/sign/firmaelectronica

URL Producción:
https://hdko60xft2.execute-api.us-east-2.amazonaws.com/pro/signature/api/sign/firmaelectronica

2.3.1 Parámetros de entrada

Objeto JSON que debe cumplir con los siguientes atributos

Nombre	Tipo	Tamaño	Obligatorio	Descripción
base64	Alfanumérico	5MB	Si	Documento pdf a firmar codificado en base64
usuarioTSA	Alfanumérico	20	No	Usuario de la tsa, es obligatorio cuando se desea agregar marca de tiempo en la firma
claveTSA	Alfanumérico	20	No	Clave de la tsa, es obligatorio cuando se desea agregar marca de tiempo en la firma
razon	Alfanumérico	30	No	Campo razón del detalle de la firma
ubicacion	Alfanumérico	30		Campo Ubicación del detalle de la firma
conEstampa	boolean		Si	Indica se coloca una marca de tiempo en el documento
firmaVisible	boolean		Si	Indica si de desea colocar la firma visible en el documento pdf
firmante	Firmante		Si	Datos del firmante
imagenFirma	ImagenFirma		Si	Especifica las propiedades de la firma visible

Objeto de entrada **ImagenFirma**

Nombre	Tipo	Tamaño	Obligatorio	Descripción
x	float		Si	Posicionamiento en el eje Y de la imagen.
y	float		Si	Posicionamiento en el eje Y de la imagen.
ancho	float		Si	Ancho de la imagen
alto	float		Si	Alto de la imagen
imagen	Alfanumérico	MAX	Si	Imagen codificada en base64
pagina	int		Si	Página en la que se va a posicionar la imagen de la firma

Objeto de entrada **Firmante**

Nombre	Tipo	Tamaño	Obligatorio	Descripción
numeroDocumento	Alfanumérico	20	Si	Identificador del firmante
tipoDocumento	Numérico		Si	Código del tipo documento
nombres	Alfanumérico	50	Si	Nombres del firmante
apellidos	Alfanumérico	50	Si	Apellidos del firmante
email	Alfanumérico	40	No	Correo electrónico del firmante

2.3.2 Ejemplo JSON de entrada


```
{
    "base64": "JVBERi0xLjcNCiW1tbW1DQoxIDAgb2JqDQo8PC=",
    "usuarioTSA": "gse",
    "claveTSA": "123456789",
    "ubicacion": "Bogota",
    "razon": "",
    "conEstampa": false,
    "OTP": "1234567",
    "firmaVisible": false,
    "imagenFirma": {
        "x": "100",
        "y": "100",
        "ancho": "70",
        "alto": "100",
        "imagen": "/9j/4AAQSkZJRgABAQAAAQABAAD/2wCEAAgGBgcGEQgHB",
        "pagina": "1"
    },
    "firmante": {
        "numeroDocumento": "1051954972",
        "tipoDocumento": 2,
        "nombres": "Jose Camilo",
        "apellidos": "Molina piratova",
        "email": "jose.molina@grupodigital.co"
    }
}
```


2.3.3 Respuesta

Como respuesta de la operación firma digital se va a devolver un JSON con la siguiente estructura:

Nombre	Tipo	Tamaño	Obligatorio	Descripción
codigoRespuesta	Alfanumérico	5	Si	Código de respuesta obtenido del proceso de firma
mensaje	Alfanumérico		Si	Descripción de la respuesta
httpStatus	Numérico		Si	Código http del estado de la transacción
documentoFirmado	Alfanumérico	MAX	No	Documento firmado y codificado en base64

2.3.4 Ejemplo JSON de respuesta

El siguiente es un ejemplo JSON con el response de la petición


```
{
    "mensaje": "Documento firmado exitosamente",
    "documentoFirmado": "FxggGC4nHR8gHhgaICspLCQlKCgoGxOtMSwmMCInKCYBC",
    "codigoRespuesta": "RS1",
    "httpStatus": 200
}
```


2.4 Firma hash

Operación POST que permite realizar la firma digital de un hash con el envío de un objeto JSON. Como resultado del firmado se obtendrá un objeto en formato JSON con la respuesta de la transacción.

El método de acceso se realiza mediante Bearer Authentication el cual es un esquema de autenticación http que involucra tokens de seguridad (Bearer Token), generado por el servicio de autenticación.

URL Pruebas:
https://8uw10ruhfj.execute-api.us-east-2.amazonaws.com/qa/signature/api/sign/hash

URL Producción:
https://hdko60xft2.execute-api.us-east-2.amazonaws.com/pro/signature/api/sign/hash

2.4.1 Parámetros de entrada

Objeto JSON que debe cumplir con los siguientes atributos

Nombre	Tipo	Tamaño	Obligatorio	Descripción
numeroDocumento	Alfanumérico	20	Si	Identificador del certificado digital
clave	Alfanumérico	15	Si	Clave del certificado
hash	Alfanumérico	MAX	Si	Hash del documento a firmar en base64

2.4.2 Ejemplo JSON de entrada

```
{
    "numeroDocumento": "xxxxxxxxxxx",
    "hash": "IHsRqEzgnRy47ToWs+WKSg+Zr1orreUX4mkqdc+mHIQ=",
    "clave": "yyyyyyyyy"
}
```

2.4.3 Respuesta

Como respuesta de la operación firma hash se va a devolver un JSON con la siguiente estructura:

Nombre	Tipo	Tamaño	Obligatorio	Descripción
codigoRespuesta	Alfanumérico	5	Si	Código de respuesta obtenido del proceso de firma
mensaje	Alfanumérico		Si	Descripción de la respuesta
httpStatus	Numérico		Si	Código http del estado de la transacción

hashFirmado	Alfanumérico	MAX	No	hash firmado y codificado en base64

2.4.4 Ejemplo JSON de respuesta


```
{
    "mensaje": "Hash firmado exitosamente",
    "hashFirmado": "MIIVjAYJKoZIhvcNAQcCoIIVfT",
    "codigoRespuesta": "RS1",
    "httpStatus": 200
}
```


2.5 Obtener Certificado

Operación POST que permite obtener el certificado en formato X509 junto con la cadena de certificación.

El método de acceso se realiza mediante Bearer Authentication el cual es un esquema de autenticación http que involucra tokens de seguridad (Bearer Token), generado por el servicio de autenticación.

URL Pruebas:
https://8uw10ruhfj.execute-api.us-east-2.amazonaws.com/qa/signature/api/sign/getcertificate

URL Producción:
https://hdko60xft2.execute-api.us-east-2.amazonaws.com/pro/signature/api/sign/getcertificate

2.5.1 Parámetros de entrada

Objeto JSON que debe cumplir con los siguientes atributos

Nombre	Tipo	Tamaño	Obligatorio	Descripción
numeroDocumento	Alfanumérico	20	Si	Identificador del certificado digital
clave	Alfanumérico	15	Si	Clave del certificado

2.5.2 Ejemplo JSON de entrada

```
{
    "numeroDocumento": "XXXX",
    "clave": "YYYYY"
}
```

2.5.3 Respuesta

Como respuesta de la operación se va a devolver un JSON con la siguiente estructura:

Nombre	Tipo	Tamaño	Obligatorio	Descripción
codigoRespuesta	Alfanumérico	5	Si	Código de respuesta obtenido del proceso de firma
mensaje	Alfanumérico		Si	Descripción de la respuesta
httpStatus	Numérico		Si	Código http del estado de la transacción
rootca	Alfanumérico	MAX	No	Certificado de la root en base64
subca	Alfanumérico	MAX	No	Certificado de la subordinada en base64

certificados	Listado de certificados		No	Certificados disponibles

Objeto Certificado

Nombre	Tipo	Tamaño	Obligatorio	Descripción
keyStoreUuid	Alfanumérico		Si	Identificador del certificado
validFrom	Alfanumérico		Si	Fecha de inicio de validez del certificado
validTo	Alfanumérico		Si	Fecha de fin de validez del certificado
x509Certificate	Alfanumérico	MAX	Si	Certificado en base64

2.5.4 Ejemplo JSON de respuesta


```
{
    "httpStatus": 200,
    "codigoRespuesta": "RS1",
    "mensaje": "Certificado consultado exitosamente",
    "rootca": "MIIF+jCCA+KgAwICjFkYA==",
    "subca": "MIIGdzCOGBg",
    "certificados": [
        {
            "keyStoreUuid": "1583948708693456",
            "validFrom": "1583948640000",
            "validTo": "1615484640000",
            "x509Certificate": "MIIGkzCCBHZYU/ERiKw=="
        }
    ]
}
```

2.6 Generar OTP

Operación POST que permite enviar un código y enviarlo vía mensaje de texto y correo electrónico.

El método de acceso se realiza mediante Bearer Authentication el cual es un esquema de autenticación http que involucra tokens de seguridad (Bearer Token), generado por el servicio de autenticación.

URL Pruebas:
https://8uw10ruhfj.execute-api.us-east-2.amazonaws.com/qa/otp/api/otpclient/generate

URL Producción:
https://hdko60xft2.execute-api.us-east-2.amazonaws.com/pro/otp/api/otpclient/generate

2.6.1 Parámetros de entrada

Objeto JSON que debe cumplir con los siguientes atributos

Nombre	Tipo	Tamaño	Obligatorio	Descripción
celular	Alfanumérico	10	Si	Número de celular al cual es enviado el mensaje
mensaje	Alfanumérico	160	Si	Contenido del mensaje
email	Alfanumérico	30	No	Correo electrónico al que se envía el mensaje

2.6.2 Ejemplo JSON de entrada

```
{
    "celular": "xxxxxxx",
    "mensaje": "yyyyyyyyyy",
    "email": "xxxxxxxx@gmail.com"
}
```

2.6.3 Respuesta

Como respuesta de la operación se va a devolver un JSON con la siguiente estructura:

Nombre	Tipo	Tamaño	Obligatorio	Descripción
httpStatus	Numérico		Si	Código http del estado de la transacción
codigo	Numérico		Si	Resultado de la transacción
descripcion	Alfanumérico	MAX	Si	Detalle de la transacción

2.6.4 Ejemplo JSON de respuesta

```
{
    "httpStatus": 200,
    "codigo": 0,
    "descripcion": "Mensaje enviado correctamente"
}
```

2.7 Validar OTP

Operación POST que permite validar un código OTP enviado.

El método de acceso se realiza mediante Bearer Authentication el cual es un esquema de autenticación http que involucra tokens de seguridad (Bearer Token), generado por el servicio de autenticación.

URL Pruebas:
https://8uw10ruhfj.execute-api.us-east-2.amazonaws.com/qa/otp/api/otpclient/validate

URL Producción:
https://hdko60xft2.execute-api.us-east-2.amazonaws.com/pro/otp/api/otpclient/validate

2.7.1 Parámetros de entrada

Objeto JSON que debe cumplir con los siguientes atributos

Nombre	Tipo	Tamaño	Obligatorio	Descripción
celular	Alfanumérico	10	Si	Número de celular al cual es envió el mensaje
codigo	Alfanumérico	160	Si	Código OTP enviado

2.7.2 Ejemplo JSON de entrada

```
{
    "celular" : "xxxxxx",
    "codigo" : "yyyyyy"
}
```

2.7.3 Respuesta

Como respuesta de la operación se va a devolver un JSON con la siguiente estructura:

Nombre	Tipo	Tamaño	Obligatorio	Descripción
httpStatus	Numérico		Si	Código http del estado de la transacción
codigo	Numérico		Si	Resultado de la transacción
descripcion	Alfanumérico	MAX	Si	Detalle de la transacción

2.7.4 Ejemplo JSON de respuesta


```
{
    "httpStatus": 200,
    "codigo": 0,
    "descripcion": "El codigo se valido y es correcto."
}
```


2.8 Estampar documento

Operación POST que permite realizar la estampa de un documento pdf con el envío de un objeto JSON. Como resultado del estampado se obtendrá un objeto en formato JSON con la respuesta de la transacción.
El método de acceso se realiza mediante Bearer Authentication el cual es un esquema de autenticación http que involucra tokens de seguridad (Bearer Token), generado por el servicio de autenticación.

URL Pruebas:
https://8uw10ruhfj.execute-api.us-east-2.amazonaws.com/qa/signature/api/sign/stamp

URL Producción:
https://hdko60xft2.execute-api.us-east-2.amazonaws.com/pro/signature/api/sign/stamp

2.8.1 Parámetros de entrada

Objeto JSON que debe cumplir con los siguientes atributos

Nombre	Tipo	Tamaño	Obligatorio	Descripción
usuario	Alfanumérico	50	Si	Usuario de la tsa
clave	Alfanumérico	100	Si	Clave de la tsa
base64	Alfanumérico	5 MB	SI	Documento pdf en formato base64

2.8.2 Ejemplo JSON de entrada

```
{
    "usuario": "xxxxx",
    "clave": "yyyyyy",
    "base64": "JVBERiOxLjcNCiW1tbW1DQoxIDAgb2JqDQo"
}
```

2.8.3 Respuesta

Como respuesta de la operación estampado de documento se va a devolver un JSON con la siguiente estructura:

Nombre	Tipo	Tamaño	Obligatorio	Descripción
codigoRespuesta	Alfanumérico	5	Si	Código de respuesta obtenido del proceso de firma
mensaje	Alfanumérico		Si	Descripción de la respuesta
httpStatus	Numérico		Si	Código http del estado de la transacción
base64	Alfanumérico	MAX	No	Documento estampado y codificado en base64

2.8.4 Ejemplo JSON de respuesta

El siguiente es un ejemplo JSON con el response de la petición

```
{
    "mensaje": "Transacción exitosa.",
    "base64": "JVBERiOxLjcNCiW1tbW1DQoxIDAgb2JqDQo8PC9UeXB",
    "httpStatus": 200,
    "codigoRespuesta": "RS1"
}
```

3. Tabla de tipos de documento

Código	Descripción
1	Tarjeta de identidad
2	Cédula de ciudadanía
3	Cédula de extranjería
4	Pasaporte
5	Número de Identificación Tributaria

4. Valores de respuesta para atributo codigoRespuesta

Código	Descripción
RS1	Transacción exitosa.
RS2	El paquete no tiene cupo para la operación
RS3	Firmante no registrado
RS4	Es necesario el usuario y la clave de la tsa
RS5	Es necesario el objeto ImagenFirma para la firma
RS6	Es necesario especificar el Alto y el Ancho para la firma
RS7	Es necesario especificar la posición de la imagen
RS8	Es necesario especificar la imagen para la firma
RS9	Es necesario especificar la página para la firma
RS10	Error al validar los datos
RS11	Ocurrió un error al firmar el documento
RS12	Clave incorrecta
RS13	Documento invalido
RS14	Usuario o clave de tsa inválidos
RS15	Código OPT invalido
RS16	Es necesario el campo base64

RS17	No tiene certificados disponibles
RS18	Tipo de documento invalido
RS19	Es necesario el hash