ESPECIFICACIONES TÉCNICAS DE INTEROPERABILIDAD

v.1.2

Identificador del Documento:	GENERALIDADES
Nombre del documento:	ESPECIFICACIONES TÉCNICAS DE INTEROPERABILIDAD
Estado del documento:	

Versión	Creación	Descripción Cambio	Autor/es
1.0	04/03/2020	Especificaciones técnicas de interoperabilidad.	Ernesto Medina
1.1	10/03/2020	Seguridad del llamado de los servicios	Clímaco Llamas
1.2	15/03/2020	Confirmación de la recepción	Clímaco Llamas

Contenido

1. Introducción

1.1. Objetivo

Esta especificación describe los mecanismos, estándares y requerimientos para que un sistema externo (aplicación/solución) pueda consumir servicios de la DIAN.

Se presenta el esquema general de seguridad tecnológica que aplicará para el consumo de cualquier servicio desde el año 2017 en adelante como referencia para cualquier proceso de interoperabilidad con la DIAN.

1.2. Terminología

Para facilidad del entendimiento de este documento, se establece la siguiente terminología de uso común.

Término / Abreviatura	**Descripción**
TOKEN	También conocido como token de autenticación o token criptográfico es un elemento electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.
JWT	JSON Web Token es un estándar abierto (RFC-7519) basado en JSON para crear un token que sirva para enviar datos entre aplicaciones o servicios y garantizar que sean válidos y seguros. El caso más común de uso de los JWT es para manejar la autenticación en aplicaciones móviles o Web.
REST-Based Web Service	Representational State Transfer (REST por sus siglas en ingles), son una forma de proveer interoperabilidad entre sistemas. Los servicios que cumplen con los requerimientos REST permitir a sistemas acceder y manipular representaciones de Recursos Web usando una forma única y predefinida de operaciones sin estado.
JSON	JavaScript Object Notation, es un formato mínimo y legible para estructurar datos. Es utilizado para la transmisión de datos entre aplicaciones web como una alternativa al XML.
CLIENTE	Aplicación externa que quiere hacer interoperabilidad con los servicios de la entidad.
TOKEN ENDPOINT	Para el caso de la DIAN, el token endpoint es sinónimo del servicio de identidad de la organización, quien es el encargado de administrar el ciclo de vida del token.

2. Seguridad

2.1. Generalidades

Para el consumo por un actor externo de cualquier servicio ofrecido por la DIAN, se debe tener en cuenta que:

- Como estándar para el intercambio de mensajes para los servicios se debe utilizar HTTPS conforme al protocolo HTTPS (HTTP + TLS v1.2) con las siguientes características
    - Suites de cifrado: ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256.
    - Tipo de certificado: ECDSA
    - Tamaño mínimo de la llave del certificado de comunicación segura: 2048
    - Algoritmo de firma del certificado de comunicación: sha256WithRSAEncryption, ecdsa-with-SHA256, ecdsa-with-SHA384, ecdsa-with-SHA512

2.2. Autenticación basada en dirección IP.

La DIAN se reserva el derecho de definir cuando un servicio se asegurará por IP. De ser así, solo permitirá el acceso al servicio(s) para aquellas direcciones IP que se encuentren registradas, de tal manera que se garantice que el acceso al servicio sea privado. Sin embargo, esta condición no aplica para los servicios de autenticación, ya que estos son de uso general.

Si la autenticación por IP es requerida, el actor externo está obligado a entregar durante la configuración del servicio a consumir las direcciones IP públicas para poder habilitar el acceso.

2.3. REST-Based Web Service

La información de autenticación va ubicada en el header de la solicitud de cualquier servicio REST. A continuación, se presenta un ejemplo de este:

Authorization: Bearer {Token obtenido en la autenticación del sistema}
ClientId: {ClientId de la aplicación registrada}

Ejemplo:

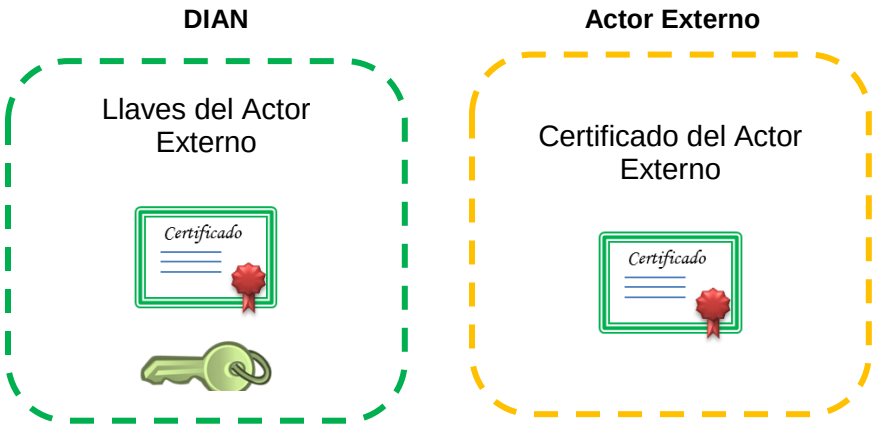
…

Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiI5MDAwMDAwMDA2MDAwNC0wLTg5MDkwMzkzOCIsImF1ZCI6WyJLVHNsTEg3UmhOeWxHOGZHQjlXM0FScjhmbEFhIl0sImlzcyI6Imh0dHBzOlwvXC9tdWlzY2EuZGlhbi5nb3YuY28iLCJleHAiOjE1MjIyNjEyNTIsImlhdCI6MTUyMjI1NzY1Miwicm9sIjoiaHR0cHM6XC9cL2dvb2dsZS5jb20uY28iLCJqdGkiOiIzZDMzOWFjZC1lMzM1LTRiMGUtYjFlYy01NTgzYzQxY2M5NTcifQ.IX1O_b5kpK_gX4He8JzX-NiYuhOB4sUdGvvH5r8rl2w
ClientId: KTslLH7RhNylG8fGB9W3ARr8flAa
…

2.4. Seguridad a nivel de canal con HTTPS.

El HTTPS garantiza la seguridad del canal entre los host o servidores relacionados, en comparación de la VPN que sólo llega hasta los equipos de borde. Sin embargo, en ocasiones se ponen servidores intermediarios que terminan la conexión TLS como balanceadores de carga, firewalls de aplicación, entre otros.

Para la implementación del HTTPS se requiere un certificado digital por parte de DIAN. Este certificado digital debe ser instalado en el servicio que se expone hacia el actor externo y también debe ser enviado al actor externo para poder autenticar al servidor (DIAN). Éste certificado sólo será recibido por el actor externo si se envía de la persona que acompaña el proceso de implementación.



Se utilizan certificados digitales vigentes, emitidos por entidades certificadoras reconocidas, cuyo propósito permita el cifrado de información. El certificado digital debería tener las siguientes características:

Característica	Valor
Tipo	X509v3
Algoritmo de firma	SHA2
Algoritmo de llave pública	RSA

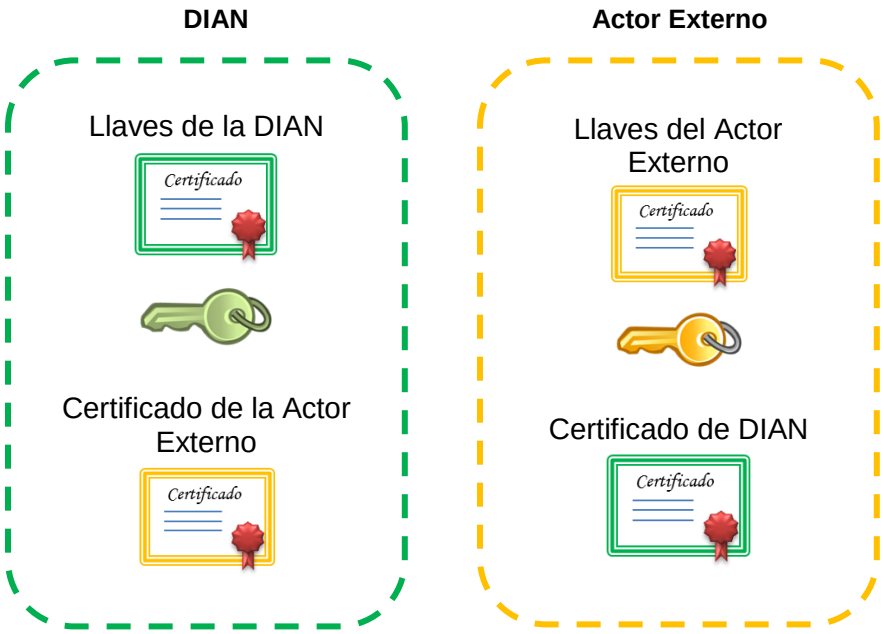
Característica	Valor
Tamaño mínimo de llave pública (bits)	2048
Vigencia	Mínimo un (1) año y máximo tres (3) años
Entidad certificadora	Reconocida a nivel internacional (Ej.: VeriSign)
Common Name del certificado (CN)	Razón social de la DIAN. En el actor externo se usa NOMBRE ACTOR.
Atributos	Cifrado (certificado Web)

2.5. Autenticación de cliente en HTTPS.

El TLS en el que se basa el HTTPS tiene una opción donde se puede definir que se requiera autenticación del cliente. Para esto el servidor le solicita al cliente su certificado digital, que es comparada con los certificados válidos y finalmente lo autentica mediante procesos criptográficos que garantizan que el cliente tenga la llave privada asociada.

Esto sólo se puede realizar cuando se tiene establecida la conexión HTTPS adicionalmente el cliente posee instalado un certificado digital para este propósito. El actor externo posee el certificado digital y está en la capacidad de utilizar esta característica.

Para poder usar esta característica, el actor externo debe enviar a la DIAN su certificado digital. Éste será enviado por personal que acompañará la implementación. Los certificados y el intercambio de llaves entre las entidades deben quedan de la siguiente manera para el completo funcionamiento del HTTPS con esta funcionalidad.



2.6. Trazabilidad de transacciones.

Todas las transacciones procesadas por la DIAN deben dejar registro en un log transaccional que permita la trazabilidad de la transacción, grabando la información necesaria para cumplir con la regulación pertinente.

2.7. Disponibilidad del servicio.

Para garantizar la disponibilidad de la solución por parte de la DIAN y actor externo se requiere que la plataforma ofrezca redundancia y sea lo suficientemente robusta para soportar las peticiones de todos los actores externos.

2.8. Acerca de los formatos de comunicación

- Protocolo de aplicación: REST-Based Web Service (Open API 3.0 o superior),
- Formato de intercambio de datos en el contenido del mensaje: JSON
- Formato de codificación en el contenido del mensaje: UTF-8.
- Formato de datos de tipo Datetime: Los datos de tipo datetime (fecha y hora) se deben enviar usando el estándar ISO 8601, en formato YYYY-MM-DDThh:mm:ss.sss (con precisión hasta milésimas de segundos), usando la hora local colombiana (para facilitar los procesos de comparación de fechas). Ejemplo, 2017-07-16T19:20:30.984.

3. Responsabilidades

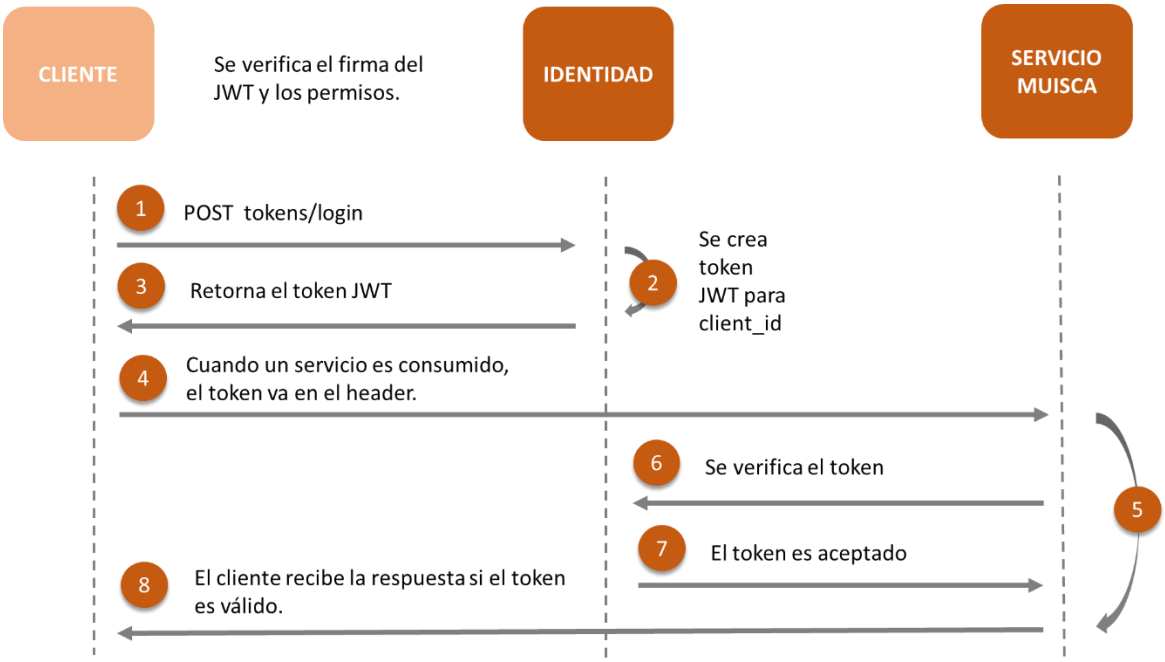
La integración entre los clientes y los servicios DIAN tiene los siguientes planteamientos base al respecto de los flujos de información y las responsabilidades sobre los mismos.

- El CLIENTE se autentica con el servicio de identidad y obtiene un token válido de la entidad.
- El CLIENTE consume servicios utilizando el token recibido.
- El CLIENTE revoca el certificado una vez termina con las transacciones.
- El CLIENTE puede refrescar el token si está próximo a vencer, usando el servicio de refrescar.
- El CLIENTE es responsable del uso adecuado del token.
- El CLIENTE es responsable de notificar el uso indebido de un token generado cuando pierda control de este o de las credenciales para su generación.
- El CLIENTE es responsable de revocar el token tan pronto no requiera consumir más servicios para evitar que siga vigente.
- La DIAN es responsable de garantizar la disponibilidad de los servicios conforme a los ANS generales de la organización para TI.

4. Registro de aplicaciones y flujos

4.1. Flujo general de consumo de un servicio.

A continuación, se presenta un diagrama de interacción para el consumo de un servicio Muisca:



Este modelo tiene las siguientes restricciones:

- Uso de Tokens basados en el estándar JWT (JSON Web Token) que brindará información sobre fechas de creación, uso y vencimiento de este, entre otros.
- La verificación de los Tokens deberá realizarse contra el Token Endpoint.
- Se limitarán las comunicaciones entrantes conforme a las políticas definidas por la entidad según el usuario mediante el registro de las direcciones IP origen autorizadas utilizando el Firewall disponible. Esto se dará a conocer para el caso de acuerdos específicos que la entidad realice.

4.2. Seguridad del llamado de los servicios

Se debe aclarar que todas las operaciones expuestas para ser consumidas por un cliente deben llevar en el encabezado la información del clientId y Authorization.

5.

Nombre del Campo (Path)	Descripción	Obligatorio	Longitud	Tipo
Header del request para cualquier método				
clientId	Entregado por la DIAN, identificador dado a la aplicación registrada.	S	50	Alfanumérico
Authorization	Es el token obtenido por medio del servicio de autenticación.	S	500	Alfanumérico

Ejemplo del header:
…
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiI5MDAwMDAwMDA2MDAwNC0wLTg5MDkwMzkzOCIsImF1ZCI6WyJLVHNsTEg3UmhOeWxHOGZHQjlXM0FScjhmbEFhIl0sImlzcyI6Imh0dHBzOlwvXC9tdWlzY2EuZGlhbi5nb3YuY28iLCJleHAiOjE1MjIyNjEyNTIsImlhdCI6MTUyMjI1NzY1Miwicm9sIjoiaHR0cHM6XC9cL2dvb2dsZS5jb20uY28iLCJqdGkiOiIzZDMzOWFjZC1lMzM1LTRiMGUtYjFlYy01NTgzYzQxY2M5NTcifQ.IX1O_b5kpK_gX4He8JzX-NiYuhOB4sUdGvvH5r8rl2w

clientId: KTslLH7RhNylG8fGB9W3ARr8flAa

4.3. Confirmación de la recepción

El servicio que recibe la petición envía una respuesta HTTP al cliente. Los posibles códigos de respuesta HTTP generalmente usados en los servicios de la DIAN son:

- 200 – Petición recibida exitosamente. Pendiente de procesamiento.
- 204 – Para cuando no hay contenido (específicamente para peticiones tipo GET)
- 400 – Petición invalida (ErrorResponse - especificación técnica Swagger - es el objeto estándar para especificar la causa del rechazo y deberá ser entregada en el cuerpo de la respuesta).
- 401 – Credencial de autenticación inválida. Autenticación Fallida. Unauthorized.
- 429 – Demasiadas peticiones. Por favor reintente más tarde.
- 500 – Error interno de servidor. ClientId no autorizado para utilizar este token
- 503 – Servicio no disponible. Reintente tarde. Autenticación no disponible

4.4. Registro de aplicaciones Cliente (Web y Móviles)

Para que una aplicación externa a la entidad pueda acceder al catálogo de servicios de la DIAN, es necesario registrar la aplicación previamente a través de los servicios de registro existente. Esto permite establecer una identificación a la aplicación y administrar sus características.

Cuando se registra una aplicación cliente, se recibe un **Client ID**. Este identificador es utilizado por la aplicación para identificarse tanto en los servicios a consumir como con los usuarios que deseen autorizar la aplicación. Igualmente, con cada aplicación se entrega un **Client Secret** que será solicitado al momento de la autenticación.

Desde esta función de autogestión también podrá cambiar o renovar el EncryptionKey utilizado para el proceso de cifrado AES-128.

Los pasos para registrar una aplicación son:

1. Ingrese a la plataforma de la DIAN con el usuario y clave del representante legal o autorizado.
2. Localice la opción de autogestión en el menú de servicios.
3. Seleccione “Administrador de Aplicaciones”.
4. Agregue la aplicación que desea registrar.