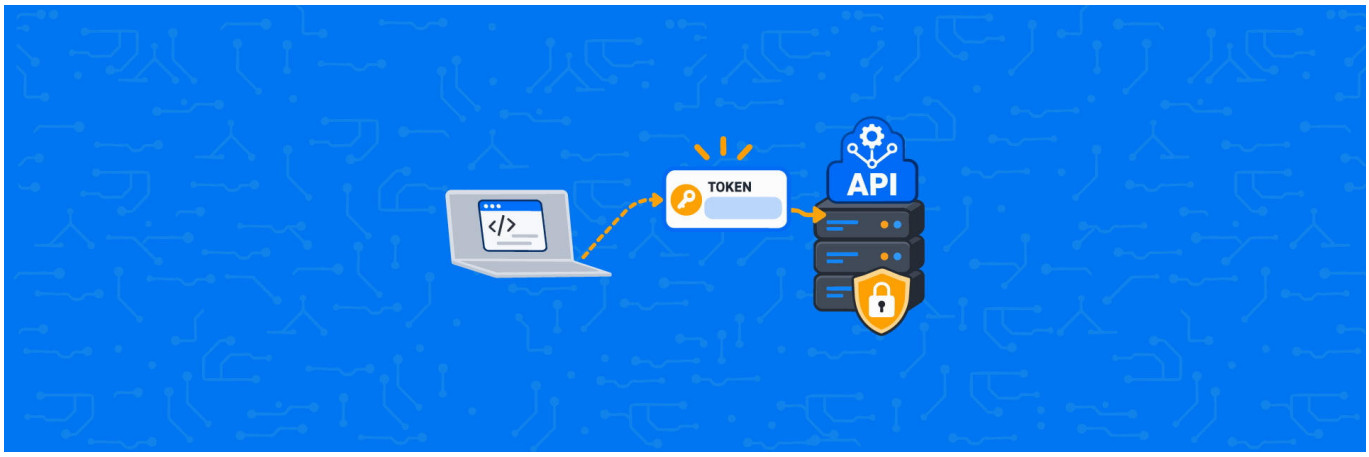
Tokens de autenticación en APIs: ¿qué son y cómo funcionan?

Aprende qué son los tokens de autenticación, cómo funcionan y por qué son importantes para proteger el acceso a una API.



API Gateway · 28/09/2026

Tokens de autenticación en APIs: ¿qué son y cómo funcionan?

Las APIs permiten que diferentes aplicaciones se comuniquen entre sí. Cuando una API entrega información privada o permite realizar operaciones específicas, necesita comprobar quién está realizando la solicitud.

Para controlar este acceso existen diferentes mecanismos de autenticación. Uno de los más utilizados es el **token de autenticación**.

¿Qué es un token de autenticación?

Un **token de autenticación** es una cadena de caracteres que funciona como una **credencial digital** para demostrar que una aplicación o usuario puede realizar solicitudes a una API.

Por ejemplo:

```
Authorization: Token abc123xyz
```

La API valida este token antes de procesar la solicitud. El formato y la forma de enviarlo dependen del

sistema de autenticación utilizado.

¿Para qué sirve un token?

Su principal objetivo es **controlar quién puede utilizar determinados recursos de una API**.

El proceso puede resumirse así:

```
Aplicación
    ↓
Solicitud + token
    ↓
API
    ↓
Validación
    ↓
Respuesta
```

Si el token es válido, la API procesa la solicitud. Si es incorrecto, ha expirado o no se incluye cuando es obligatorio, puede rechazarla.

Autenticación vs. autorización

Aunque están relacionadas, no significan lo mismo:

- **Autenticación:** comprueba quién está realizando la solicitud.
- **Autorización:** determina qué puede hacer esa aplicación o usuario.

En términos simples:

```
Autenticación → ¿Quién eres?
```

```
Autorización  → ¿Qué puedes hacer?
```

Un token puede participar en ambos procesos, dependiendo de cómo esté diseñada la API.

¿Cómo funciona un token de autenticación?

El funcionamiento general puede resumirse en cuatro pasos:

1. **La aplicación obtiene sus credenciales.**
2. **Realiza una solicitud** al endpoint correspondiente e incluye el token.
3. **La API valida el token**, comprobando aspectos como su vigencia y permisos.
4. **La API procesa o rechaza la solicitud.**

Una solicitud podría verse así:

```
GET https://api.example.com/users

Authorization: Token abc123xyz
```

Cuando la autenticación no es válida, la API normalmente responderá algo como `401 Unauthorized`.

¿Dónde se envía el token?

La forma habitual es mediante una **cabecera HTTP**:

```
Authorization: Token abc123xyz
```

El nombre de la cabecera y el formato dependen de cada API, por lo que siempre es importante revisar su documentación.

¿Un token es lo mismo que una contraseña?

No. Ambos pueden funcionar como credenciales, pero los tokens pueden tener características específicas como:

- Fecha de expiración.
- Permisos determinados.
- Alcance limitado.
- Posibilidad de revocación.

Por eso, un token debe tratarse como una **credencial privada** y nunca publicarse en repositorios, código compartido o documentos públicos.

Buenas prácticas para utilizar tokens

Al trabajar con APIs, es recomendable:

- **Mantener los tokens privados.**
- **Evitar incluirlos directamente en el código.**
- **Utilizar HTTPS** para proteger la comunicación.
- **Renovar o revocar tokens** cuando corresponda.
- **Limitar los permisos** de cada credencial.

Estas medidas ayudan a reducir los riesgos asociados a credenciales expuestas o comprometidas.

¿Qué tipos de tokens existen?

No todas las APIs utilizan el mismo mecanismo. Algunos conceptos habituales son:

- API Keys.
- Bearer Tokens.
- OAuth 2.0.
- JSON Web Tokens (JWT).
- Tokens de acceso.
- Tokens de actualización.

La documentación de cada servicio debe indicar qué mecanismo utiliza y cómo realizar la autenticación.

¿Qué relación tienen los tokens con los endpoints?

El **endpoint** define dónde se realiza una determinada operación, mientras que el **token** permite demostrar que la aplicación tiene las credenciales necesarias para utilizar ese recurso.

```
Aplicación
    ↓
Token de autenticación
    ↓
Endpoint
    ↓
Validación
    ↓
Respuesta
```

Por lo tanto, conocer un endpoint no significa que cualquier persona pueda utilizarlo. Si el recurso está protegido, la API puede exigir autenticación.

Tokens de autenticación en API Gateway

API Gateway utiliza autenticación para controlar el acceso a sus servicios y recursos.

De forma conceptual, una integración funciona así:

```
Tu aplicación
    ↓
Token de autenticación
    ↓
Endpoint de API Gateway
    ↓
Validación
    ↓
Servicio correspondiente
    ↓
Respuesta
```

Para conocer el formato exacto de autenticación y los requisitos para realizar solicitudes, es importante consultar la documentación oficial de API Gateway.

¿Por qué es importante la autenticación al integrar servicios del SII?

Cuando un software necesita comunicarse con servicios tributarios, la autenticación permite controlar el acceso a los recursos disponibles.

La integración puede representarse así:

```
Software
    ↓
Autenticación
    ↓
API Gateway
    ↓
Servicios del SII
    ↓
Respuesta
```

De esta manera, las aplicaciones pueden comunicarse con los servicios disponibles mediante una API y procesar la información dentro de sus propios sistemas.

Conclusión

Los **tokens de autenticación son credenciales que permiten a una aplicación demostrar que puede realizar determinadas solicitudes a una API**.

Comprender cómo funcionan y cómo protegerlos es fundamental al desarrollar integraciones con servicios externos. Además, como no todas las APIs utilizan el mismo mecanismo, siempre es importante revisar la documentación del servicio.

¿Tu software necesita comunicarse con servicios del SII?

Accede a datos del SII y Previred que no están disponibles a través de servicios web oficiales.

Conoce los productos

Última actualización el 26/10/2026