Token y certificado

Generación del token de la conexión y obtención del certificado digital en formato PEM.

Anonymous · 11/09/2026

Token y certificado

Token de la conexión

Es la credencial con que tu sistema se identifica ante API Gateway. Se genera en Gestionar conexión → Token y va en la cabecera de **todas** las consultas:

```
Authorization: Token <tu_token>
```

Tres cosas que conviene tener claras:

El token está asociado a la conexión, no a los productos. No cambia al activar o desactivar un producto y **no hay que regenerarlo** tras un cambio de configuración.

La pestaña Token no muestra qué servicios incluye. Los productos activos se ven en la pestaña *Productos*, que es también donde se configuran. El token por sí solo no “lleva” servicios: la autorización se resuelve al consultar, según los productos activos de la conexión.

Regenerar el token invalida el anterior de inmediato. Actualiza tu integración al hacerlo.

Trátalo como una contraseña: no lo publiques en repositorios ni en código que compartas. Si sospechas que se filtró, regenéralo.

No es la API Key de tu usuario

La API Key de Mi perfil es otra credencial, para operar sobre tu cuenta y tus conexiones. Para consumir recursos del SII necesitas el **token de la conexión**.

Formato de la cabecera

La única forma admitida es el esquema `Token`. La API **no acepta** `Bearer`, ni `X-Api-Key`, ni el token como parámetro en la URL.

```
Authorization: Token 0123456789abcdef0123456789abcdef01234567   ← correcto
```

```
Authorization: Bearer 0123456789abcdef0123456789abcdef01234567  ← incorrecto
Authorization: 0123456789abcdef0123456789abcdef01234567         ← incorrecto
```

Enviar la clave sin la palabra `Token` produce `Las credenciales de autenticación no se proveyeron.`

Certificado digital en formato PEM

Algunos recursos requieren autenticación con **certificado digital**, y la API lo espera en formato **PEM**. Tu certificado normalmente viene en un archivo `.p12` o `.pfx`.

La pestaña Gestionar conexión → Certificado convierte tu certificado al formato requerido. También puedes usar la utilidad pública de tools.libredte.cl, o seguir el tutorial para extraer el PEM.

Esa sección no almacena tu certificado

Es solo una herramienta de conversión. El certificado **no queda cargado** en API Gateway ni en la conexión: debes enviarlo en el cuerpo de cada consulta que lo requiera.

Una vez que tienes el PEM:

```
{
  "auth": {
    "cert": {
      "cert-data": "-----BEGIN CERTIFICATE-----..-----END CERTIFICATE-----",
      "pkey-data": "-----BEGIN PRIVATE KEY-----..-----END PRIVATE KEY-----"
    }
  }
}
```

También se acepta el archivo PFX en base64, según el recurso:

```
{
  "auth": {
    "cert": {
      "file-data": "<pfx en base64>",
      "file-pass": "<clave del certificado>"
    }
  }
}
```

Qué método de autenticación usar

Lo define cada recurso, y su documentación lo indica. Usar el método equivocado no siempre da un

error claro: puede aparecer como un `409` de indisponibilidad del SII o como un `401` intermitente. Revisa Errores de autenticación en la API.

Caché de sesión del SII

Cuando envías credenciales en el cuerpo, API Gateway inicia sesión en el SII y **reutiliza esa sesión unas dos horas**. Es intencional: acelera las consultas siguientes y reduce el riesgo de bloqueos por exceso de logins.

Si la sesión queda en mal estado, la API responde `Se debe volver a autenticar al usuario en la sesión del SII.` y puede acompañarlo con la cabecera `X-Auth-Session-Problem: 1`. En ese caso puedes forzar una sesión nueva agregando `auth_cache=0` a la URL.

No uses `auth_cache=0` en todas tus peticiones

Cada forzado equivale a un login nuevo en el SII. Usarlo permanentemente en producción aumenta el riesgo de que el SII bloquee tus accesos.

Última actualización el 11/09/2026