Autenticación SII - Método RUT/Clave

Aprende a autenticarte en el SII usando RUT y contraseña para realizar consultas tributarias

Anonymous · 11/09/2026

Autenticación SII - Método RUT/Clave

Muchas consultas al SII exigen **iniciar sesión**; el método más directo es enviar **RUT y clave tributaria** en el **cuerpo** de la petición (JSON). **API Gateway** actúa de intermediario: usa esas credenciales, obtiene los datos y te responde (casi siempre en **JSON**).

Respecto a Tu primera petición, allí solo usaste el **token de conexión** en la cabecera; aquí además envías el bloque **`auth`** con datos del SII en el cuerpo.

¿Por qué POST si “solo consulto”?

Aunque sea una consulta, muchas operaciones usan **POST** porque las credenciales van en el **cuerpo** (body), no en la URL visible: no quedan en el historial del navegador ni en logs de proxy como query string, y es más seguro que poner claves en parámetros `?clave=...` de un GET.

Caché de sesión (aprox. 2 horas)

API Gateway puede **reutilizar la sesión del SII** alrededor de **dos horas** para responder más rápido en consultas seguidas, reducir inicios de sesión repetidos y usar mejor los recursos. Si algo falla con la sesión, existe el parámetro **`auth_cache`** en la URL; más abajo lo explicamos en **Control de caché de sesión**.

Cabecera obligatoria: token de conexión

Además del JSON con `auth`, **toda** petición lleva el token de tu conexión:

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

Estructura del objeto `auth.pass`

Para autenticar en el SII usando RUT y clave, debes enviar el siguiente JSON:

```
{
  "auth": {
    "pass": {
      "rut": "11111111-1",
      "clave": "mi_clave_sii"
    }
  }
}
```

Los componentes del objeto `auth.pass` son:

Campo	Formato	Ejemplo	Descripción
`rut`	Texto	`"76192083-9"`	Sin puntos, con guión
`clave`	Texto	`"miClave123"`	Clave tributaria del SII

Paso a paso en la documentación interactiva

Lista de boletas de honorarios **emitidas** por un emisor en un período. Sirve para comprobar que RUT/clave y token funcionan y que entiendes ruta + cuerpo.

Los datos `emisor` y `periodo` van en la **ruta** (path), no en la query:

```
POST /api/v2/sii/bhe/emitidas/documentos/{emisor}/{periodo}
```

1. Localizar el endpoint

1. Abre **www.apigateway.cl/docs/api**.
2. Busca la sección **API BHE** (Boletas de Honorarios Emitidas) o similar.
3. Localiza el **POST** de documentos emitidos con `emisor` y `periodo` en la ruta.
4. Expande la operación.

2. Revisar la documentación

Lee qué significa cada parámetro de ruta, si hay query opcionales (`pagina`, `formato`, etc.) y el esquema del body.

3. Autorización

Configura **Authorize** con tu **token de conexión** (`Authorization: Token …`), igual que en Navegando Swagger UI.

4. Activar “Try it out”

Habilita la edición de campos.

5. Configurar parámetros

Parámetros de ruta (ejemplo)

```
emisor:   11111111-1
periodo:  202401
```

`periodo` suele ser mes calendario `YYYYMM`; algunos listados permiten día `YYYYMMDD`. Confirma en la descripción del endpoint.

Cuerpo (request body)

```
{
  "auth": {
    "pass": {
      "rut": "11111111-1",
      "clave": "tu_clave_sii"
    }
  }
}
```

Nota

`emisor` en la ruta es el RUT cuyas boletas consultas. El **`rut` dentro de `auth.pass`** es quien **inicia sesión** en el SII. A menudo son el mismo contribuyente; en escenarios con representación pueden diferir según permisos en el SII.

6. Ejecutar

Pulsa **Execute** y revisa código, cabeceras y cuerpo. Las cabeceras de créditos y límites se explican en Tu primera petición.

Interpretando la respuesta

Respuesta exitosa (200 OK)

Ejemplo ilustrativo:

```
{
  "data": {
    "n_boletas": 9,
    "n_paginas": 1,
    "boletas": [
      {
        "numero": 133,
        "rut": 76111111,
```

```
        "dv": "9",
        "nombre": "TESTING SPA",
        "fecha": "2025-07-14",
        "total_honorarios": 1000,
        "retencion_emisor": 0,
        "retencion_receptor": 145,
        "total_liquido": 855,
        "sociedad_profesional": "NO",
        "estado": "S",
        "anulada": "2025-07-14",
        "codigo": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
        "fecha_emision": "2025-07-14",
        "usuario_emisor": "TESTING USER",
        "email_envio": ""
      }
    ]
  }
}
```


Campos importantes (orientativo)

Campo	Descripción
`numero`	Número de la boleta
`rut` / `dv`	RUT del receptor
`nombre`	Nombre o razón social del receptor
`fecha`	Fecha de la boleta
`total_honorarios`	Total de honorarios
`retencion_emisor` / `retencion_receptor`	Retenciones
`total_liquido`	Monto líquido
`estado`	Estado según glosa del SII en la documentación del endpoint

Manejo de errores

Posibles errores que puedes obtener al autenticar en el SII usando RUT y clave:

Error 401: credenciales incorrectas

```
{
  "code": 401,
  "detail": "..."
}
```

Causas habituales: RUT o clave mal escritos, formato de RUT incorrecto.

Qué hacer: probar en www.sii.cl; usar RUT con guión y sin puntos.

Error 401: sesión SII / volver a autenticar

```
{
  "code": 401,
  "detail": "Se debe volver a autenticar al usuario en la sesión del SII."
}
```

Cabecera de ayuda: puede aparecer `X-Auth-Session-Problem: 1`.

Qué hacer: revisa la sección **Control de caché de sesión** más abajo y la guía Manejo de errores.

Control de caché de sesión

Comportamiento por defecto

Tras un inicio de sesión exitoso en el SII, la sesión puede **reutilizarse** un tiempo (del orden de **2 horas**): **acelera** las siguientes consultas, **reduce** logins repetidos y es el comportamiento recomendado para uso normal.

Forzar una nueva sesión (`auth_cache`)

Si la sesión queda en mal estado (por ejemplo mensajes de reautenticación o cabecera `X-Auth-Session-Problem`), la documentación del endpoint puede indicar que agregues a la URL un parámetro de consulta **`auth_cache`**.

Ejemplo de forma (ajusta la ruta al endpoint real):

```
POST
https://app.apigateway.cl/api/v2/sii/bhe/emitidas/documentos/11111111-1/202401?auth_cache=0
```

Cuándo tiene sentido usarlo: después de **cambiar la clave** del SII; cuando el error indica explícitamente problema de sesión y las repeticiones fallan; o durante **pruebas puntuales** de integración.

Advertencia

No añadas `auth_cache=0` en **cada** petición de producción. Forzar un login nuevo una y otra vez puede provocar bloqueos por demasiados accesos al SII y empeorar el rendimiento.

Los valores exactos aceptados (`0`, `1`) y su efecto están descritos en la **documentación interactiva** de cada operación: revísalos ahí antes de automatizar.

Mejores prácticas

1. **Seguridad**

- **No** escribas la clave del SII fija en código que subas a Git.
- **Usa** variables de entorno o un almacén de secretos.
- **Regenera** el token de API si sospechas filtración.

2. **Rendimiento**

- **Aprovecha** la reutilización de sesión cuando todo funciona bien, **agrupa** consultas cuando sea posible y **observa** `X-RateLimit-Remaining` y créditos en las cabeceras.

3. **Ejemplo de uso seguro (idea general)**

```
// ❌ Evitar: clave en el código fuente
const auth = { pass: { rut: "76192083-9", clave: "miClave123" } };

// ✅ Mejor: leer desde entorno seguro
const auth = {
  pass: {
    rut: process.env.SII_RUT,
    clave: process.env.SII_CLAVE
  }
};
```

Tu aplicación debe además enviar la cabecera `Authorization: Token …` con el token de conexión.

Última actualización el 11/09/2026