Servicio de Identificación Telefónica
Profesionales Nube
Manual de Integración

Histórico de versiones

Versión	Fecha	Resumen de los cambios producidos
1.0	13/04/2026	Primera versión

Contenido

1 Introducción

1.1 Objeto del documento

El objetivo de este documento es detallar los elementos necesarios para integrar, en una aplicación, los servicios de identificación telefónica ofrecidos por Izenpe vinculados a la posesión de un certificado de profesional en la nube con segundo factor de autenticación basado en el envío de OTP por SMS.

El documento describe el funcionamiento interno del servicio REST creado para este fin. Detalla los mecanismos que proprocionan estos servicios para identificar las personas usuarias que disponen de un certificado profesional nube activo (estados en vigor o bloqueado).

A este efecto se detallan:

- Peticiones y respuestas para realizar la identificación telefónica de usuarios que disponen de un certificado profesional nube.

2 Integración

En este apartado se describen los mecanismos de registro de la aplicación invocante y los mecanismos de integración disponibles para el servicio que consta de 2 llamadas a diferentes endpoints:

- Comprobar los datos del usuario y generar el código OTP
- Verificar el código OTP recibido por el usuario en su teléfono móvil

2.1 Registro de una nueva aplicación

Antes de comenzar la integración de una nueva aplicación con el sistema, es necesario que la aplicación tenga a su disposición un certificado electrónico para poder realizar la autenticación de cliente contra la instancia segura mutua con el servidor que ofrece los servicios del sistema.

Además, la aplicación deberá estar dada de alta en el sistema como entidad solicitante. Para ello, se facilitará a Izenpe el valor del Asunto (Subject) del certificado electrónico que se utilizará en las peticiones a los servicios del sistema.

2.2 Generar código otp (solo DNI)

NOTA: En el caso en el que el poseedor de claves solo disponga de un certificado de profesional nube para una unica entidad es posible hacer uso de este método.
En el caso de que disponga de más de un certificado de profesional nube se producira un error. En este caso sera necesario hacer uso del metodo de genreración de código OTP descrito en la sección *2.3 Generar código otp (DNI y CIF)*.

El endpoint del servicio es:

POST https://servicios1.izenpe.com/profesional/rest/profesionalidtel/generarOtp/{dni}/{idioma}

Mediante esta invocación se válida que el usuario proporcionado en la invocación disponde de un certificado de profesional en la nube vivo (estados en vigor o bloqueado) y, is es asi, se genera un OTP y se envia mediante el canal de cominicación adecuado.

2.2.1 Petición

Para la generación del código OTP, la aplicación deberá mandar una petición POST al endpoint defindo:

```
POST /profesional/rest/profesionalidtel/generarOtp/{dni}/{idioma} HTTP/1.1
Host: servicios1.izenpe.com
```

Los parámetros de la petición son los siguientes:

Nombre	Valor	Presencia	Descripción
dni	Un DNI o NIE válido	Obligatorio	Valor del DNI (con letra) de la persona solicitante de la identificación.
lang	Valor discreto [ES|EU]	Obligatorio	Valor del idioma en el que se enviará, al solicitante de la identificación, el mensaje SMS con el OTP

2.2.2 Respuesta

[HTTP 400 – BAD REQUEST] Dependiendo de los datos proprocionado en la petición se puede obtener distintas respuestas. En el caso de que los datos proporcionados no sean validos se obtendrá una respuesta **HTTP 400 – BAD REQUEST**.

```
HTTP/1.1 400 BAD REQUEST
{
    "status": 400
    , "status": "Error validando datos de entrada"
    , "errorCode": <Código de error>
    , "details": <Descripción de error>
}
```

Dependiendo del error encontrado en los datos de entrada se pueden producir distintos código y descripciones de error. La siguiente tabla muestra los posibles códigos de error que se pueden producir y detalla su significado.

Código/Detalle	Descripción
INVALID_DNI ***El DNI/NIE <dni> no cumple con el formato***	El DNI proprocionado en la invocación no cumple con el patrón de DNI o NIE válido.
INVALID_LANG ***El idioma <idioma> no es valido***	El lenguaje proporcionado en la invocación no cumple con los valores permitidos

[HTTP 409 – CONFLICT] Una vez validados los datos entrada el proceso busca los datos del certificado de proporcional en la nube asociado a la persona usuaria cuyos datos se han proporcionado en la invocación. Si por algun motivo no se puede encontrar este certificado se devolverá un error **HTTP 409 – CONFLICT**.

```
HTTP/1.1 409 CONFLICT
<Código de error>
```

Dependiendo de la causa por la que no se puede determinar el certfiicado de profesional en la nube de los datos de la persona usuaria proporcionada se pueden producir distintos código de error. La siguiente tabla muestra los posibles códigos de error que se pueden producir y detalla su significado.

Código	Descripción
Sin usuario	El DNI proprocionado en la invocación no identifica a ningún poseedor de claves en el sistema.
Sin certificados	Aunque el DNI proporcinado en la invocación identifica a un poseedor de claves del sistema, este poseedor no tiene ningun certificado de profesional en la nube vivo (en vigor o bloqueado).
Multiples certificados	Aunque el DNI proporcinado en la invocación identifica a un poseedor de claves del sistema, este poseedor tiene más de un certificado de profesional en la nube vivo (en vigor o bloqueado). Como es necesario identificar un único certificado para poder continuar no se puede hacer uso de este método. Hacer uso del método definido en el apartado *2.3 Generar código otp (DNI y CIF)*.

[HTTP 200 – OK] Si se consigue obtener el certificado de profesional en la nube de la persona usuaria cuyos datos se han proporcionado en la invocación, el servicio generará y enviará un OTP a dicho usuario por el canal de comunicación establecido para las comunicaciones de dicho certificado. Este OTP quedará registrado en el sistema a la espera de verificación mediante el método definido en la sección *2.4 Comprobar código otp*. Se devolvera una respuesta **HTTP 200 -OK** en la que se muestran los datos del certificado y canal de comunicación usado para confirmar que el proceso ha terminado correctamente.

```
HTTP/1.1 200 OK
{
    "resultado": "OK"
    , "dni": <dni de la persona usuaria>
    , "cif": <cif de la entidad del certificado>,
    , "canal": <canal de comunicación usado en el OTP>
}
```

La siguiente tabla detalle el significado de los parametros obtenidos en la respuesta

Código	Descripción
dni	El DNI de la persona usuaria proporcionada en la invocación
cif	El CIF del certificado de profesional en la nube encontrado para la persona usuaria
canal	El canal de comunicación usado para enviar el OTP de la petición. Es un valor discreto que puede ser SMS, MAIL o NIK.

2.3 Generar código otp (DNI y CIF)

El endpoint del servicio es:

POST https://servicios1.izenpe.com/profesional/rest/profesionalidtel/generarOtp/{dni}/{cif}/{idioma}

Mediante esta invocación se válida que el usuario proporcionado en la invocación disponde de un certificado de profesional en la nube vivo (estados en vigor o bloqueado) y, is es asi, se genera un OTP y se envia mediante el canal de cominicación adecuado.

2.3.1 Petición

Para la generación del código OTP, la aplicación deberá mandar una petición POST al endpoint definido:

```
POST /profesional/rest/profesionalidtel/generarOtp/{dni}/{cif}/{idioma} HTTP/1.1
Host: servicios1.izenpe.com
```

Los parámetros de la petición son los siguientes:

Nombre	Valor	Presencia	Descripción
dni	Un DNI o NIE válido	Obligatorio	Valor del DNI (con letra) de la persona solicitante de la identificación.
cif	Un CIF válido	Obligatorio	Valor del CIF de la entidad cuyo certificado de profesional se esta buscando para la persona usuarioa
lang	Valor discreto [ES|EU]	Obligatorio	Valor del idioma en el que se enviará, al solicitante de la identificación, el mensaje SMS con el OTP

2.3.2 Respuesta

[HTTP 400 – BAD REQUEST] Dependiendo de los datos proprocionado en la petición se puede obtener distintas respuestas. En el caso de que los datos proporcionados no sean validos se obtendrá una respuesta **HTTP 400 – BAD REQUEST**.

```
HTTP/1.1 400 BAD REQUEST
{
    "status": 400
    , "status": "Error validando datos de entrada"
    , "errorCode": <Código de error>
    , "details": <Descripción de error>
}
```

Dependiendo del error encontrado en los datos de entrada se pueden producir distintos código y descripciones de error. La siguiente tabla muestra los posibles códigos de error que se pueden producir y detalla su significado.

Código/Detalle	Descripción
INVALID_DNI ***El DNI/NIE <dni> no cumple con el formato***	El DNI proprocionado en la invocación no cumple con el patrón de DNI o NIE válido.
INVALID_CIF ***El CIF <cif> no cumple con el formato***	El CIF proporcionado en la invocación no cumple con el patrón de CIF válido
INVALID_LANG ***El idioma <idioma> no es valido***	El lenguaje proporcionado en la invocación no cumple con los valores permitidos

[HTTP 409 – CONFLICT] Una vez validados los datos entrada el proceso busca los datos del certificado de proporcional en la nube asociado a la persona usuaria cuyos datos se han proporcionado en la invocación. Si por algun motivo no se puede encontrar este certificado se devolverá un error **HTTP 409 – CONFLICT**.

```
HTTP/1.1 409 CONFLICT
<Código de error>
```

Dependiendo de la causa por la que no se puede determinar el certfiicado de profesional en la nube de los datos de la persona usuaria proporcionada se pueden producir distintos código de error. La siguiente tabla muestra los posibles códigos de error que se pueden producir y detalla su significado.

Código	Descripción
Sin usuario	El DNI proprocionado en la invocación no identifica a ningún poseedor de claves en el sistema.
Sin certificados	Aunque el DNI proporcinado en la invocación identifica a un poseedor de claves del sistema, este poseedor no tiene ningun certificado de profesional en la nube vivo (en vigor o bloqueado).

[HTTP 200 – OK] Si se consigue obtener el certificado de profesional en la nube de la persona usuaria cuyos datos se han proporcionado en la invocación, el servicio generará y enviará un OTP a dicho usuario por el canal de comunicación establecido para las comunicaciones de dicho certificado. Este OTP quedará registrado en el sistema a la espera de verificación mediante el método definido en la sección *2.4 Comprobar código otp*. Se devolvera una respuesta **HTTP 200 -OK** en la que se muestran los datos del certificado y canal de comunicación usado para confirmar que el proceso ha terminado correctamente.

```
HTTP/1.1 200 OK
{
    "resultado": "OK"
    , "dni": <dni de la persona usuaria>
    , "cif": <cif de la entidad del certificado>,
    , "canal": <canal de comunicación usado en el OTP>
}
```

La siguiente tabla detalle el significado de los parametros obtenidos en la respuesta

Código	Descripción
dni	El DNI de la persona usuaria proporcionada en la invocación
cif	El CIF del certificado de profesional en la nube encontrado para la persona usuaria
canal	El canal de comunicación usado para enviar el OTP de la petición. Es un valor discreto que puede ser SMS, MAIL o NIK.

2.4 Comprobar código otp

El endpoint del servicio es:

GET https://servicios1.izenpe.com/profesional/rest/profesionalidtel/comprobarOtp/{dni}/{cif}/{otp}

Mediante esta invocación se comprueba si el OTP proporcionado por la persona usuaria concuerda con el último OTP generado para el certifiado de que se esta consultando.

2.4.1 Petición

Para la comprobación del código OTP, la aplicación deberá mandar una petición GET al endpoint definido:

```
POST /profesional/rest/profesionalidtel/comprobarOtp/{dni}/{cif}/{otp} HTTP/1.1
Host: servicios1.izenpe.com
```

Los parámetros de la petición son los siguientes:

Nombre	Valor	Presencia	Descripción
dni	Un DNI o NIE válido	Obligatorio	Valor del DNI (con letra) del usuario solicitante.
cif	Un CIF válido	Obligatorio	Valor con el CIF del certificado usado para la comprobación
otp	Valor numérico	Obligatorio	Valor del código OTP recibido por el usuario mediante el canal de comunicación pro defecto establecido para el certificado. **Por defecto, consta de 4 números.**

2.4.2 Respuesta

[HTTP 400 – BAD REQUEST] Dependiendo de los datos proprocionado en la petición se puede obtener distintas respuestas. En el caso de que los datos proporcionados no sean validos se obtendrá una respuesta **HTTP 400 – BAD REQUEST**.

```
HTTP/1.1 400 BAD REQUEST
{
    "status": 400
    , "status": "Error validando datos de entrada"
    , "errorCode": <Código de error>
    , "details": <Descripción de error>
}
```

Dependiendo del error encontrado en los datos de entrada se pueden producir distintos código y descripciones de error. La siguiente tabla muestra los posibles códigos de error que se pueden producir y detalla su significado.

Código/Detalle	Descripción
INVALID_DNI ***El DNI/NIE <dni> no cumple con el formato***	El DNI proprocionado en la invocación no cumple con el patrón de DNI o NIE válido.
INVALID_CIF ***El CIF <cif> no cumple con el formato***	El CIF proporcionado en la invocación no cumple con el patrón de CIF válido
El OTP <otp> no cumple con el formato	El OTP proprocionado no cuple con el formato de un OTP válido

[HTTP 409 – CONFLICT] Si los datos proporcionado en la invocación son validos, el servicio buscará un registro de OTP generado para el DNI y CIF proporcionados. Si por algun motivo no se puede encontrar este registro se proporcionará una respuesta **HTTP 409 – CONFLICT**.

```
HTTP/1.1 409 CONFLICT
<Código de error>
```

La siguiente tabla muestra los posibles códigos de error que se pueden producir y detalla su significado.

Código	Descripción
No se han encontrado registros para el DNI <dni> y CIF <cif>	No existe ningún registro de OTP para el DNI y CFI proporcionados

[HTTP 200 – OK] Si se encuentra un registro de OTP asociado al DNI y CIF proporcionados en la invocación se obtendra una respuesrta **HTTP 200 – OK**. Dependiendio del estado de este registro y de la validación del OTP del registro contra el OTP proprocionado en la invocación se pueden obtener distintos cuerpos en la respuesta.

[EXPIRED] En caso en el que haya pasado el tiempo máximo establecido desde la generación del OTP hasta su comprobación se obtendrá una **RESPUESTA DE OTP EXPIRADO**.

```
HTTP/1.1 200 OK
{
    "intentos": 0
    , "mensaje": "EXPIRED_OTP"
    , "resultado": "ERROR"
}
```

[INCORRECT] En el caso en el que el OTP proporcionado en la petición no coincida con el OTP del registro almacenado en la genración del OTP obtendrá una **RESPUESTA DE OTP INCORRECTO**.

```
HTTP/1.1 200 OK
{
    "intentos": 1
    , "mensaje": "INCORRECT_OTP"
    , "resultado": "ERROR"
}
```

[MAX ATTEMPTS EXCEEDED] En caso en el se haya realizado tantas comprobaciones incorrectas que se haya excedido el número máximo de intentos permitos, se invalidará el registro de OTP del sistema. A partir de este momento se obtendrán **RESPUESTAS DE NÚMERO DE INTENTOS MÁXIMOS EXCEDIDO**.

```
HTTP/1.1 200 OK
{
    "intentos": 3
    , "mensaje": "MAX_ATTEMPTS_EXCEEDED"
    , "resultado": "ERROR"
}
```

[OK] En caso en el que El OTP proporcionado en la invocación coincida con el OTP registrado en el sistema se obtendrá una **RESPUESTA DE OTP VÁLIDO**.

```
HTTP/1.1 200 OK
{
    "resultado": "OK"
    , "datosUsuario": {
        "dni": <dni de la persona usuaria>
        , "cif": <cif de la entidad>
        , "entidad": <razón social de la emtidad>
        , "nombre": <nombre de la persona usuaria>
        , "apellido1": <primer apellido de la persona usuaria>
        , "apellido2": <segundo apellido de la persona
      usuaria>
    }
}
```

La siguiente tabla detalle el significado de los parametros obtenidos en la respuesta

Código	Descripción
dni	El DNI de la persona usuaria proporcionada en la invocación
cif	El CIF del certificado de profesional en la nube encontrado para la persona usuaria
entidad	La razón social de la entidad
nombre	El nombre de la persona usuaria
apellido1	El primer apellido de la persona usuaria
apellido2	El segundo apellido de la persona usuaria