

Plataforma de Identificación, Autenticación y Firma

- **Sistema Cl@ve**
- **Portal Informativo**
- **Soporte al usuario**

- **Sistema Cl@ve**
- **Portal Informativo**
- **Soporte al usuario**

El Proyecto Cl@ve

- **Proyecto colaborativo** promovido por la DTIC y alineado con las medidas CORA
- Gobernanza
  - Grupo de trabajo reducido: Entidades responsables del sistema: SGAD, AEAT, GISS, DG Policía + DG Tráfico
  - Grupo de trabajo extendido
- Formalizado por el **Acuerdo de Consejo de Ministros del 19 de septiembre de 2014**
  - Cl@ve es la plataforma común del Sector Público Administrativo Estatal para la **identificación, autenticación y firma electrónica** mediante el uso de claves concertadas, abierta a su utilización por parte de todas las Administraciones Públicas.
  - Uso obligatorio para el Sector Público Administrativo Estatal a finales de 2015
- Integra dos sistemas de identificación previamente existentes
  - PIN 24H de la AEAT
  - Usuario y contraseña de la Seguridad Social
- Técnicamente se apoya en los resultados del proyecto europeo STORK
  - Especificaciones: perfil SAML 2.0 STORK
  - Implementación del SW (PEPS, paquetes de integración)
- Empezó a operar el 17 de noviembre de 2014

El Sistema Cl@ve

- Sistema orientado a **unificar y simplificar el acceso electrónico** de los ciudadanos a los servicios públicos
  - Principal objetivo: un ciudadano puede identificarse y autenticarse frente a una entidad pública usando claves concertadas, sin tener que recordar claves diferentes para acceder a servicios distintos
- **Complementa los sistemas actuales** basados en DNI-e y certificados electrónicos
- Requiere **registro previo**
  - Presencial
  - Online: Certificado electrónico / datos conocidos por ambas partes (información tributaria)
- **Dos modalidades** de identificación electrónica basada en claves concertadas
  - **Cl@ve PIN**: Usuario (NIF) + contraseña formada por dos partes, una de ellas elegida por el ciudadano, la otra un código enviado a su teléfono móvil por SMS con validez limitada en el tiempo. Destinado a usuarios que acceden a los servicios de forma esporádica.
  - **Cl@ve permanente**: Usuario (NIF) + contraseña definida y custodiada por el ciudadano, reforzada (si se requiere) por un código enviado por SMS al móvil.
- Ofrece la posibilidad de **firmar en la nube** con certificados personales custodiados en servidores remotos: Cl@ve Firma.

Base Legal

Formalizado por el **Acuerdo del Consejo de Ministros del 19 de septiembre de 2014**

- "Se aprueba el sistema Cl@ve, un **sistema de identificación, autenticación y firma electrónica** común para todo el Sector Público Administrativo Estatal …"

- "… podrán **adherirse al sistema mediante convenio otras Administraciones Públicas** en las condiciones técnicas, económicas y organizativas que se determinen en las prescripciones técnicas de desarrollo a las que se refiere el apartado Quinto de este Acuerdo."

- "… La Dirección de Tecnologías de la Información y las Comunicaciones de la Administración General del Estado podrá acordar **ampliar la red de Oficinas de Registro con aquellos organismos públicos** que dispongan de despliegue territorial y cumplan los requisitos técnicos necesarios establecidos por resolución de esta Dirección".

Pasarela Cl@ve de autenticación

Proveedor del servicio de administración electrónica (SP)

Servicio de e-Admon

Gestor de identificación

AEAT

PIN 24H

GISS

TU SEGURIDAD SOCIAL

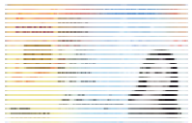


Comunicación mediante redirecciones del navegador (aserciones SAML)

Proveedores de servicios de identificación y autenticación (IdP)

@firma

STORK

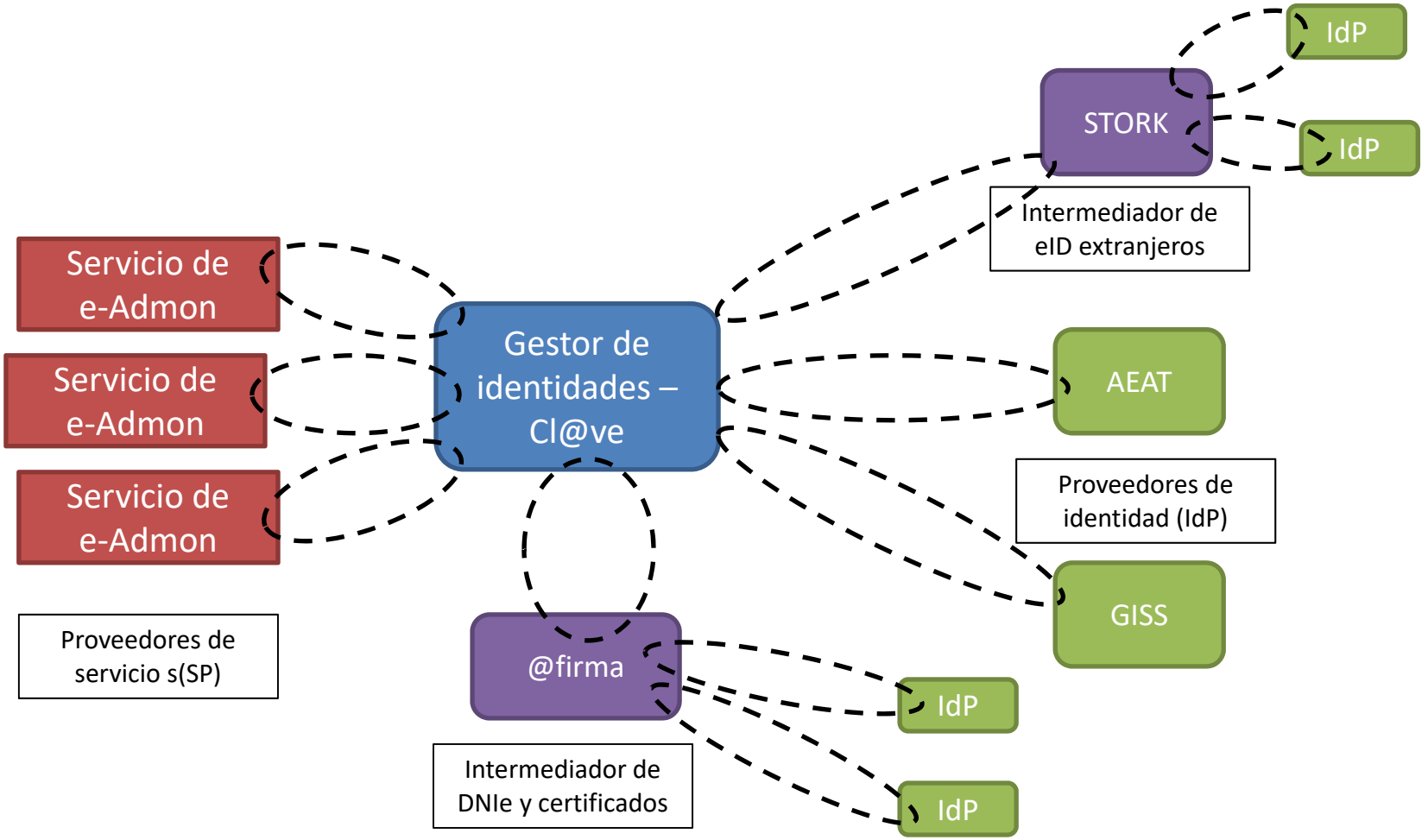


Intermediador de DNIe y certificados

Intermediador de eID extranjeros



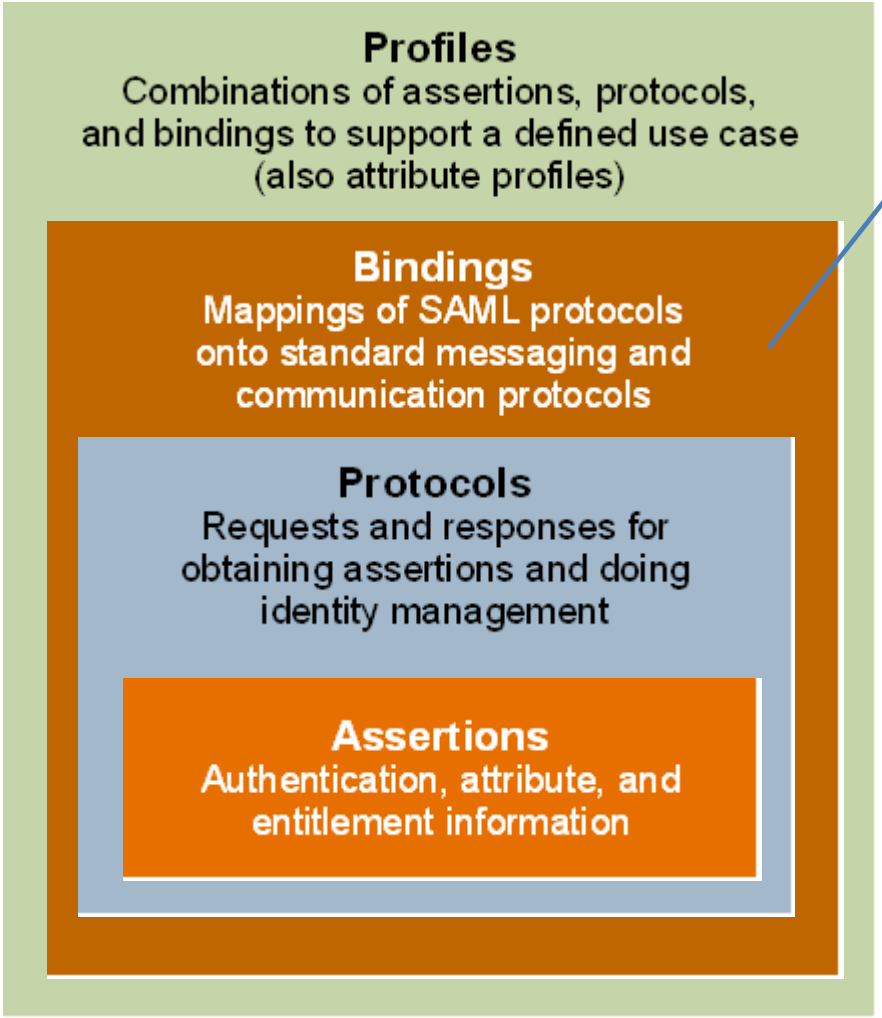
Círculos de Confianza



SAML – Protocolo de Intercambio de Tokens

- **Usado en sistemas de federación de identidades**
- **Framework basado en XML para reunir y organizar información de seguridad e identidad e intercambiarla entre diferentes dominios**
  - Integra tecnologías de seguridad ya existentes en lugar de inventar nuevas tecnologías
  - Sus perfiles ofrecen interoperabilidad para una variedad de casos de uso, pero se pueden ser extendidos para casos adicionales
- **Base de SAML: aserciones acerca de sujetos**
  - Autenticación
  - Atributos
  - Derechos de acceso
- **SAML 2.0 (OASIS): Integra SAML 1.0 y 1.1, Liberty Alliance, y Shibboleth 5**

Conceptos SAML



- SAML SOAP Binding (based on SOAP 1.1)
- Reverse SOAP (PAOS) Binding
- **HTTP Redirect (GET) Binding**
- **HTTP POST Binding**
- **HTTP Artifact Binding**
- SAML URI Binding

Authentication Context
Detailed data on types and strengths of authentication

Metadata
Configuration data for identity and service providers

Datos personales manejados por la interfaz STORK

Interfaz STORK

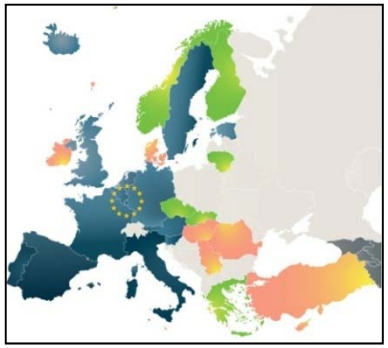
Atributo personal	Valores y comentario
eIdentifier	Identificador nacional de otros países.
givenName	Nombre del ciudadano
surname	inheritedFamilyName / adoptedFamilyName (cada país tendrá en el surname uno de estos casos como el apellido comúnmente usado)
inheritedFamilyName	Apellido de nacimiento
adoptedFamilyName	Apellido adoptado (para casos en que el apellido cambia al contraer matrimonio, por ejemplo)
gender	Género
nationalityCode	Código del país de nacionalidad
maritalStatus	Estado civil
dateOfBirth	Fecha de nacimiento
countryCodeOfBirth	Código del país de nacimiento
age	Edad
isAgeOver	¿La edad es mayor de X años?
textResidenceAddress	Dirección en varias líneas de texto de la dirección postal.
canonicalResidenceAddress	Dirección en formato canónico
residencePermit	Permiso de residencia
eMail	Correo electrónico
title	Título
pseudonym	Seudónimo
citizenQAAlevel	Nivel con el que se autenticó el usuario.
fiscalNumber	Número fiscal

Datos de registro

Nombre	Descripción / Observaciones
Tipo de Documento Identificativo	Valor inicial: DNI/NIE En este modelo de datos se debe contemplar que en el futuro se puedan tener identificaciones distintas del DNI/NIE. Por ejemplo, ciudadanos de otros países.
NIF/NIE	La identificación del ciudadano debe ser los que figura en la DGP, responsable de emitir los DNI/NIE. Para cumplir este requisito, se utilizará el servicio SVDI de la DGP desde la aplicación de Registro.
Nombre	
Apellido1	
Apellido2	
Fecha de validez del DNI/NIE	
Indicador de Permanente	
Teléfono	Aunque actualmente sólo se permiten teléfonos españoles (9 posiciones), el modelo contemplará números de otros países (15 posiciones)
Email	
Tipo de Registro	• Telemático a partir de una carta de invitación • Con certificado electrónico, equivalente al presencial • Presencial
Identificación del Organismo	Identificador del Organismo que realiza el Registro. Se utiliza el identificador asignado en el Directorio de Organismos DIR3
Identificación del Funcionario	NIF del funcionario que realiza el Registro en su modalidad Presencial.
Estado	• Alta • Renuncia • Revocado • Baja-Fallecido
TimeStamp	TimeStamp del momento en el que se realiza el último movimiento
Código de Activación	El código de referencia será un código de 8 posiciones numéricas. En la base de datos se almacenará el HASH del código.

Niveles de Identificación

- **Niveles** de aseguramiento de la calidad de la autenticación, en base a:
  - Como se **verifica la identidad** de la persona antes de darle el mecanismo de identificación. Requiere **registro** fiable.
  - Aspectos técnicos de los **medios** de autenticación…
- El **proveedor del servicio define el nivel de calidad** en la autenticación que requiere para su servicio
- Recogidos en el Reglamento Europeo eIDAS:
  - Básico
  - Sustancial
  - Alto
- Obligatoriedad de **reconocimiento** de credenciales extranjeras con nivel mayor o igual al requerido para las nacionales



Niveles de Identificación y Calidad de Registro

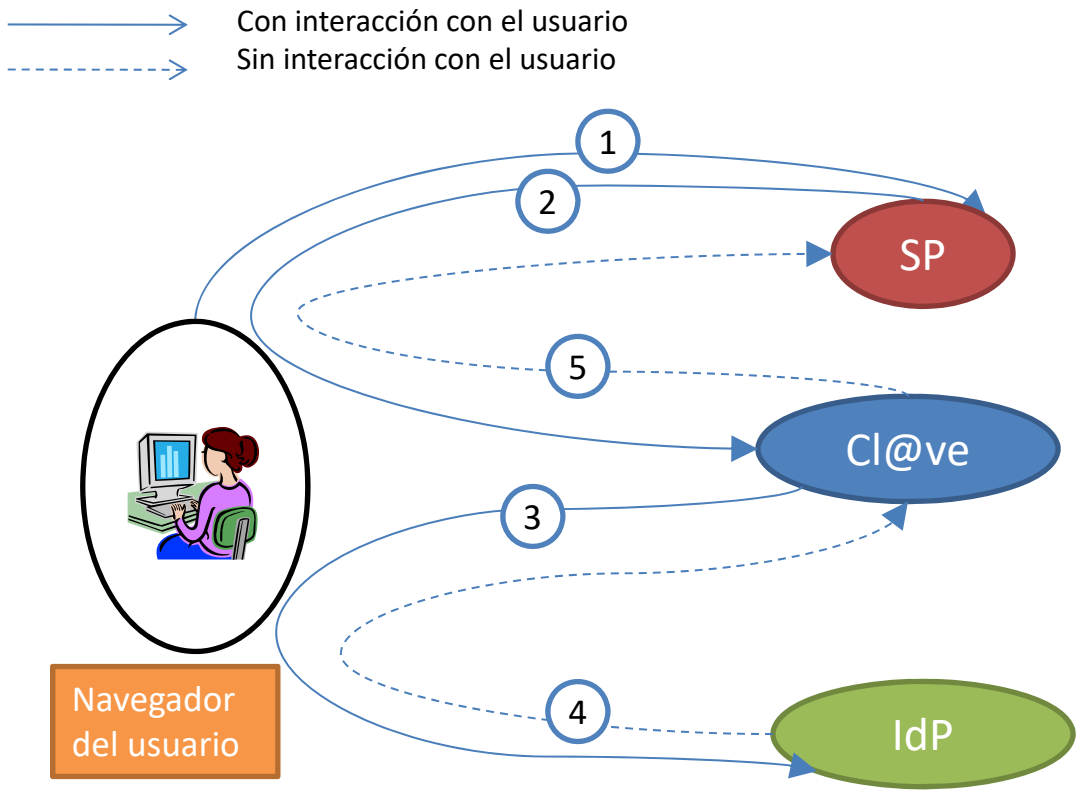
- Niveles influidos por el proceso de registro:
  - Presencial
  - Con certificado reconocido
  - No presencial
- Ejemplos basados en el QAA de STORK
  - Alto: Certificados electrónicos (contienen los datos de identidad). Nivel alto
  - Sustancial: Usuario/contraseña + doble factor (clave de un solo uso/tarjeta coordenadas)
  - Básico: Usuario/contraseña
- Básico
  - Registro telemático o
  - Registro Presencial



Información Intercambiada

- El proveedor del servicio define
  - Qué proveedores de identidad deben ser intermediados por Cl@ve
  - El nivel de calidad de la credencial (QAA) que se debe usar para autenticarse en su servicio
  - Opcional en nivel básico: Requerir el registro presencial.
- El proveedor de servicio recibe como respuesta
  - Resultado del proceso de autenticación (OK, KO)
  - Datos de identidad: identificador (DNI), nombre y apellidos
  - Datos del proceso de autenticación: QAA, proveedor de identidad
- El proveedor de identidad recibe datos de identificación del proveedor del servicio
  - País, sector, proveedor de servicio, aplicación del proveedor

Navegación





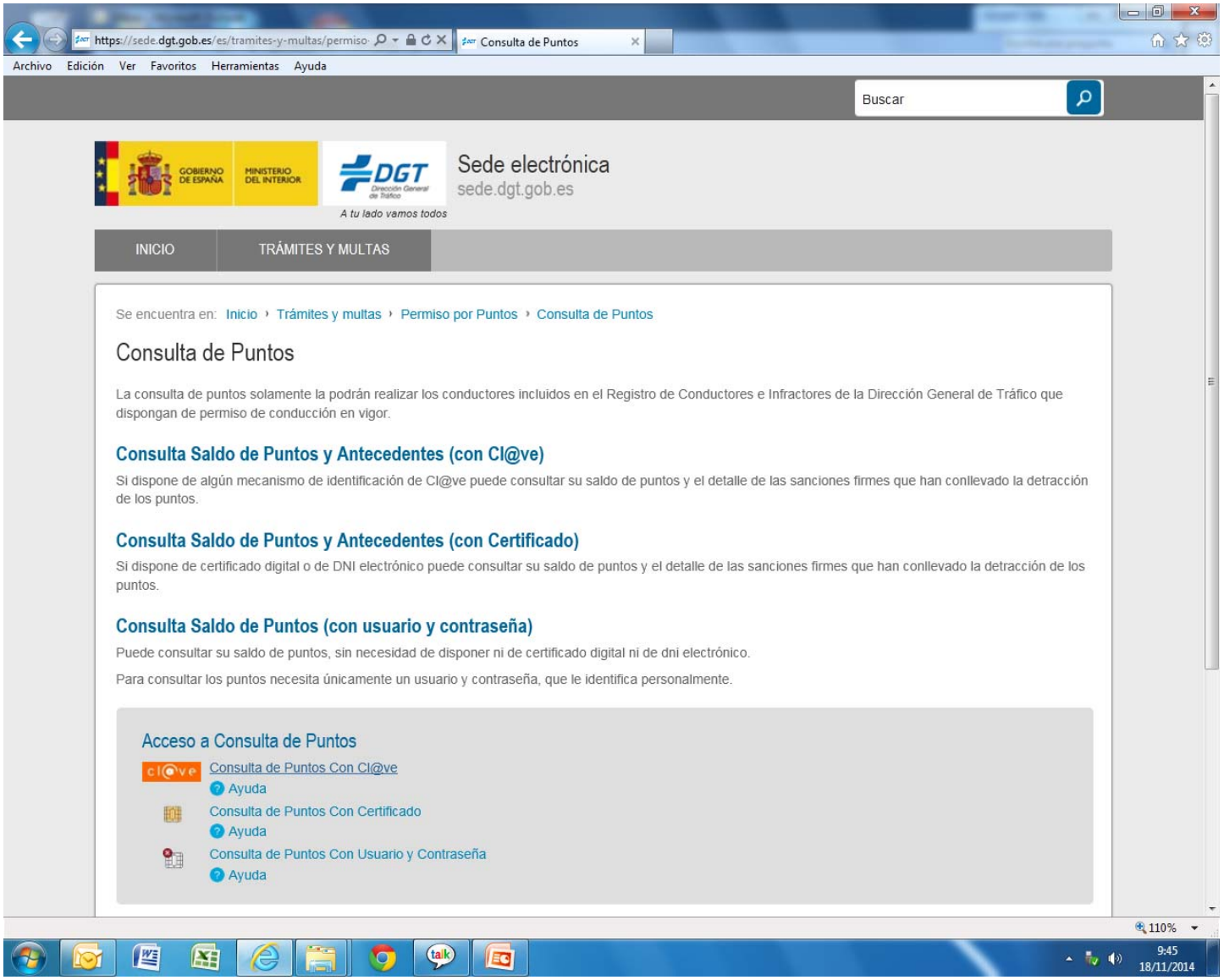




Mensajes SAML

2 - Servicio que invoca (SP), nivel de calidad de eID exigido, firmado por SP
3 - Servicio que invoca (SP), nivel de calidad de eID, firmado por Cl@ve
4 – Respuesta de la identificación, firmada por IdP
5 – Respuesta de la identificación, firmada por Cl@ve

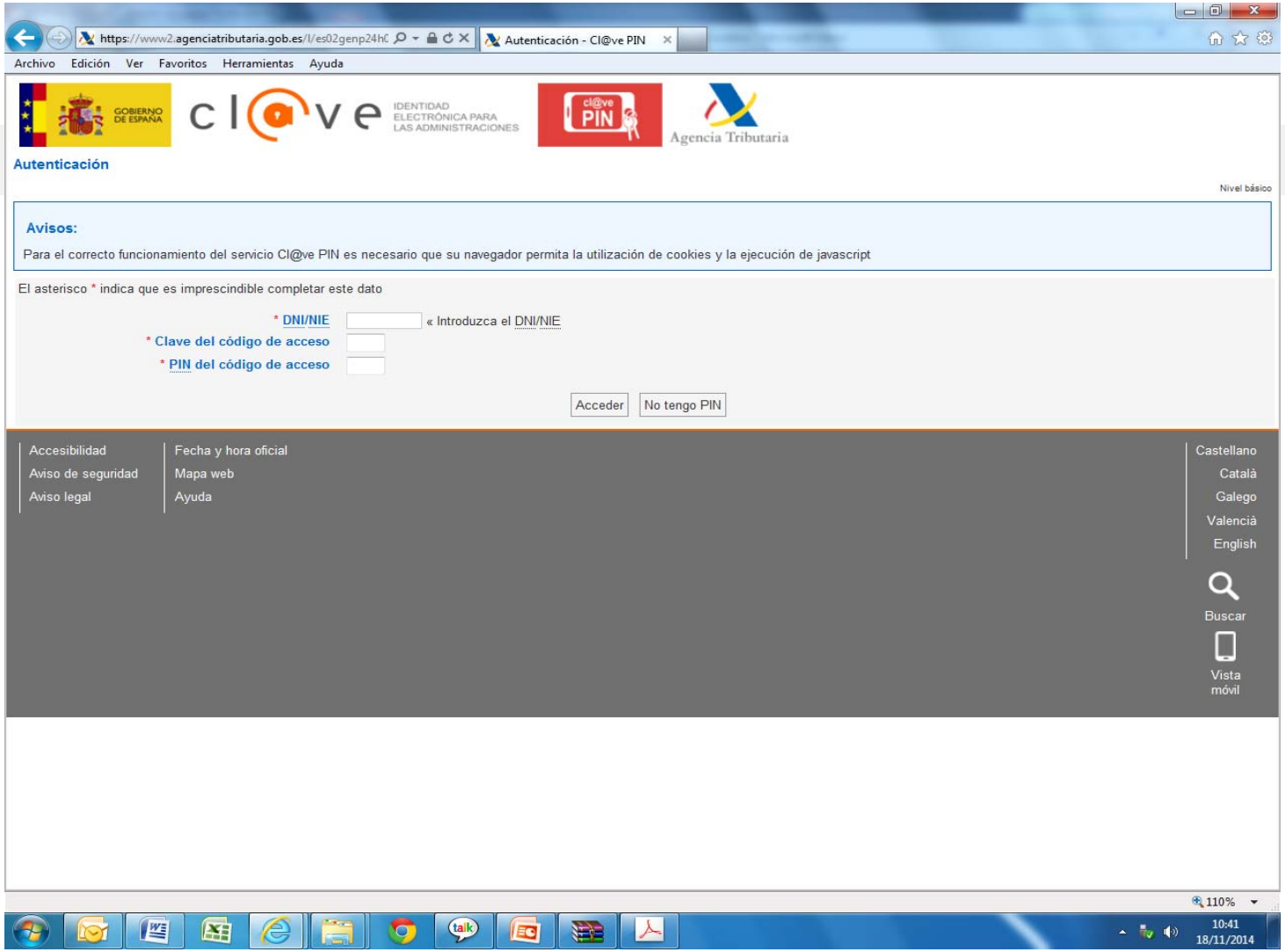
Integración de Cl@ve - Ejemplo



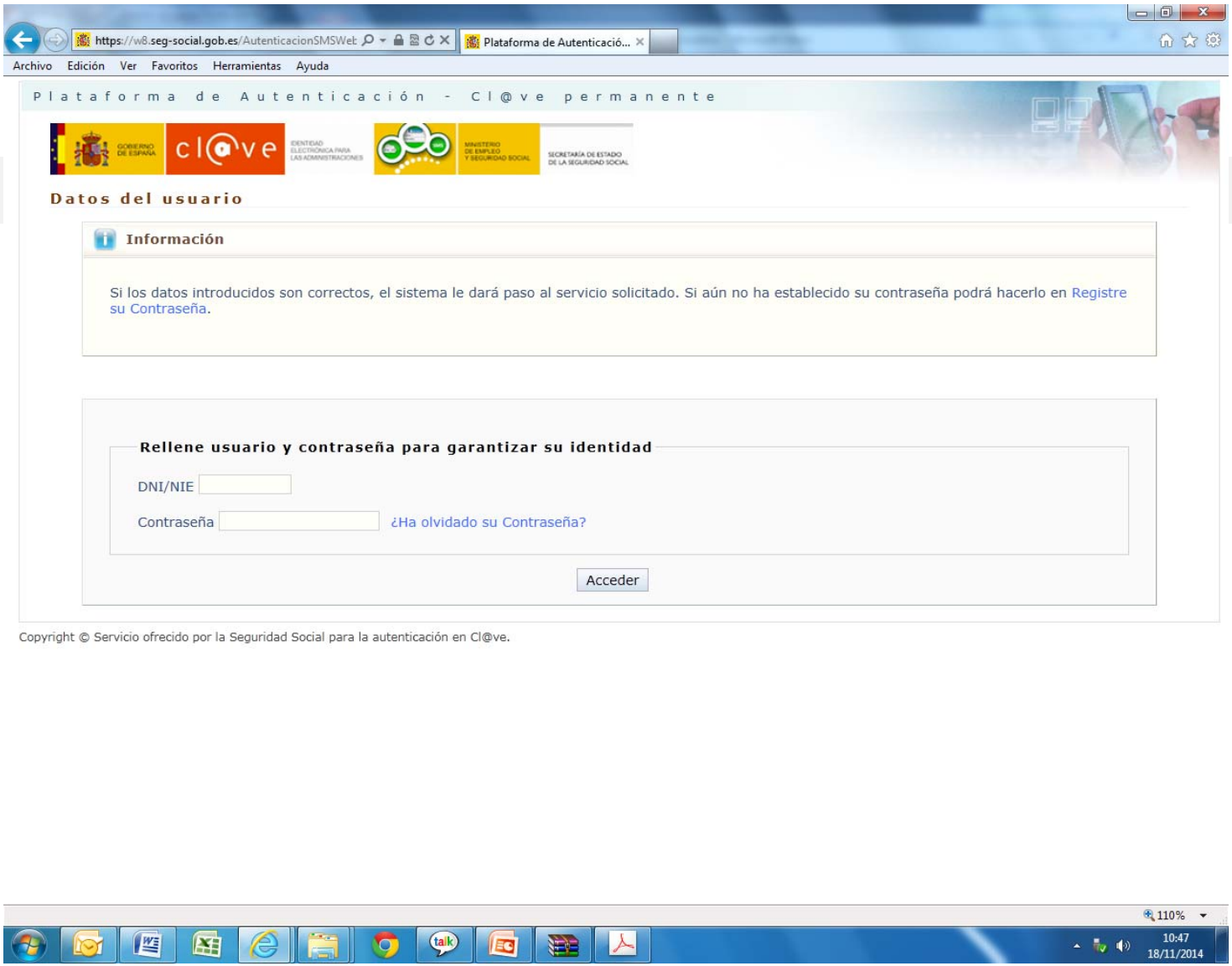
Pasarela Cl@ve



Cl@ve PIN de la AEAT



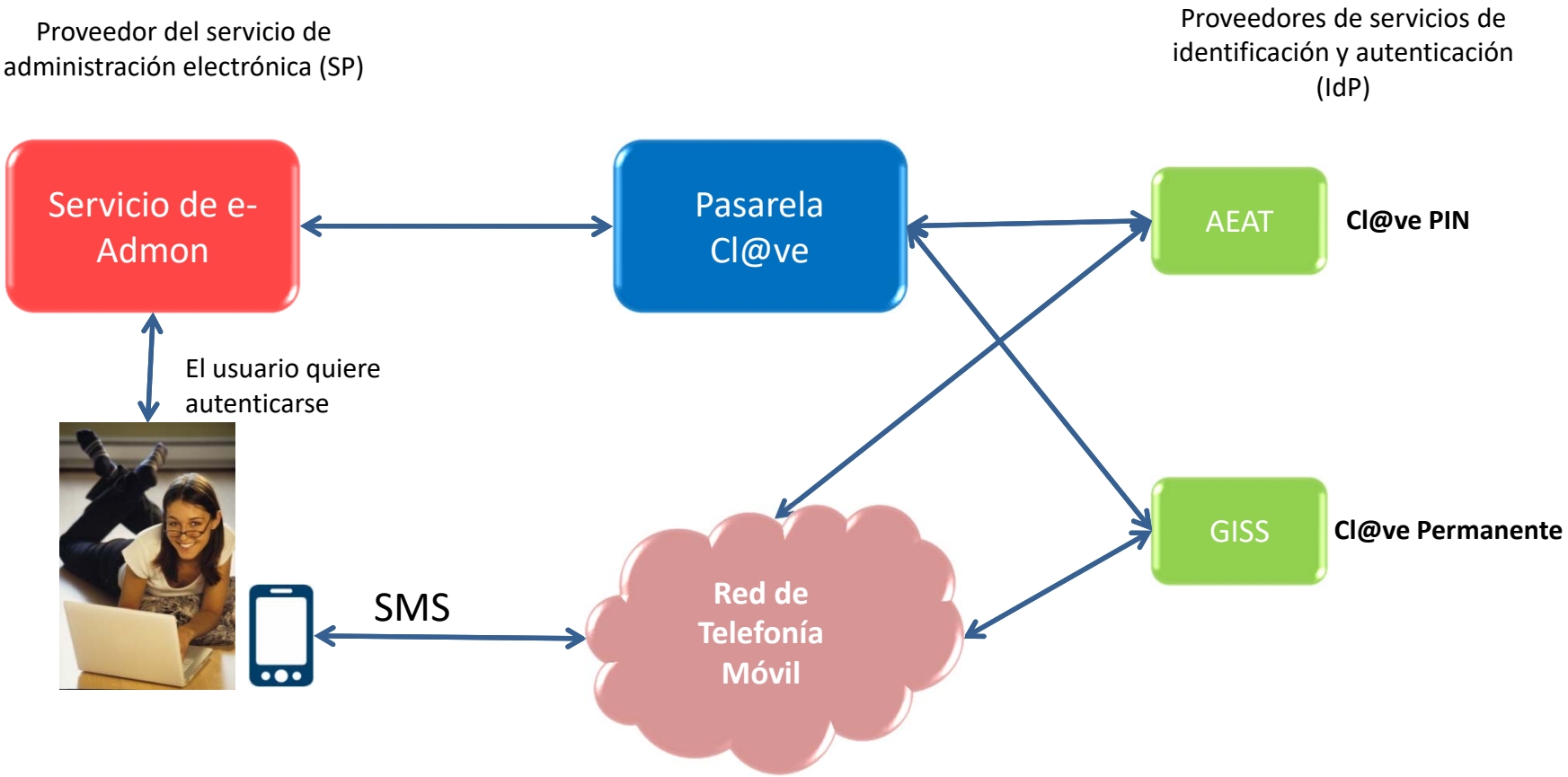
Cl@ve Permanente de la GISS



Envío de SMS

- **El SMS es el segundo factor de autenticación usado en:**
  - Cl@ve PIN
  - Autenticación de nivel 3 en Cl@ve Permanente
  - Cl@ve Firma

Necesidad de SMS

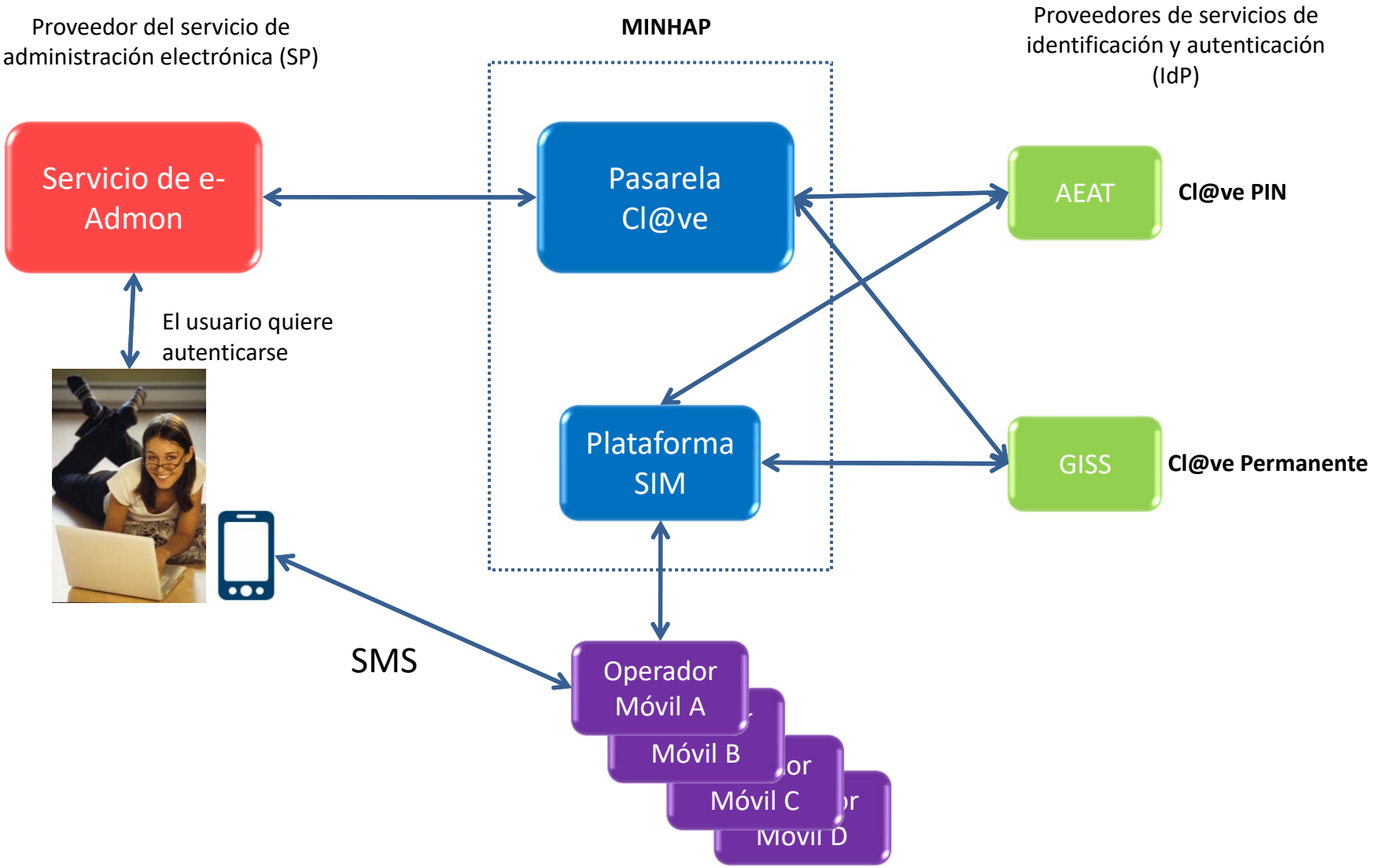


Coste de los SMS

- **El coste de los SMS los asumirá el organismo que origina la petición de autenticación.**

- **Mecanismo:**
  - El SMS se envía a través del operador con el que el organismo tiene contrato.
  - El operador factura directamente al organismo con cargo a ese contrato.

Arquitectura Técnica



- Sistema Cl@ve
- **Portal Informativo**
- Soporte al usuario

Portal Cl@ve

- http://clave.gob.es

- Información al ciudadano sobre el sistema Cl@ve
- Resolución de dudas, problemas y acceso a Soporte

GOBIERNO DE ESPAÑA

clave.gob.es

cl@ve IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

Castellano | Català | Euskera | Gallego | Valencià | English

cl@ve IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

Cl@ve | Registro | Cl@ve PIN | Cl@ve Permane... | Cl@ve Firma

Conoce Cl@ve

Identidad Electrónica para las Administraciones



¿Qué es?

Un sistema para identificarte electrónicamente en las relaciones con las Administraciones Públicas

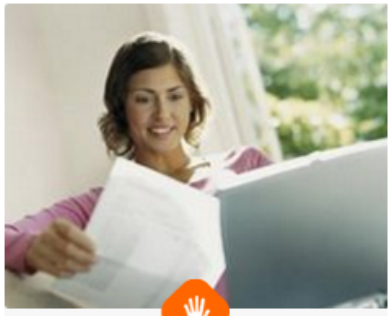
Leer más >



¿Dónde puedo usarlo?

Cl@ve está pensado para usarlo con tu ayuntamiento, pedir cita médica, presentar tu declaración de impuestos...

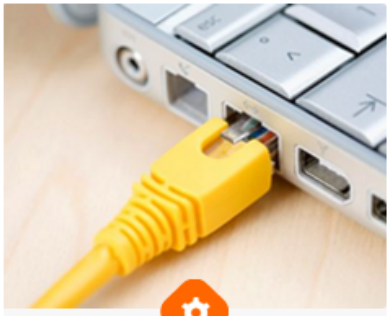
Leer más >



¿Qué necesito para empezar?

Solamente tienes que registrarte en el sistema para obtener tus datos de acceso

Leer más >



¿Cómo funciona?

Rápido y sencillo, tu eliges cómo identificarte en cada momento

Leer más >

Cl@ve

¿Qué es?

¿Dónde puedo usarlo?

¿Qué necesito para empezar?

¿Cómo funciona?

Preguntas frecuentes (FAQs)

¿Qué es Cl@ve?

Cl@ve es un sistema orientado a unificar y simplificar el acceso electrónico de los ciudadanos a los servicios públicos. Su objetivo principal es que el ciudadano pueda identificarse ante la Administración mediante claves concertadas (usuario más contraseña), sin tener que recordar claves diferentes para acceder a los distintos servicios.

Cl@ve complementa los actuales sistemas de acceso mediante DNI-e y certificado electrónico, y ofrece la posibilidad de realizar firma en la nube con certificados personales custodiados en servidores remotos.

Se trata de una plataforma común para la identificación, autenticación y firma electrónica, un sistema interoperable y horizontal que evita a las Administraciones Públicas tener que implementar y gestionar sus propios sistemas de identificación y firma, y a los ciudadanos tener que utilizar métodos de identificación diferentes para relacionarse electrónicamente con la Administración.

Cl@ve permite que las aplicaciones de administración electrónica puedan definir el nivel de aseguramiento en la calidad de la autenticación que desean, en base a los datos que tratan y a la clasificación de seguridad siguiendo las recomendaciones del Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica). El ciudadano usuario de los servicios de administración electrónica puede entonces escoger el identificador que desea usar entre los disponibles para el nivel de aseguramiento requerido por la aplicación.

El sistema Cl@ve fue aprobado por Acuerdo del Consejo de Ministros, en su reunión del 19 de septiembre de 2014, y sus condiciones de utilización son determinadas por la Dirección de Tecnologías de la Información y las Comunicaciones.

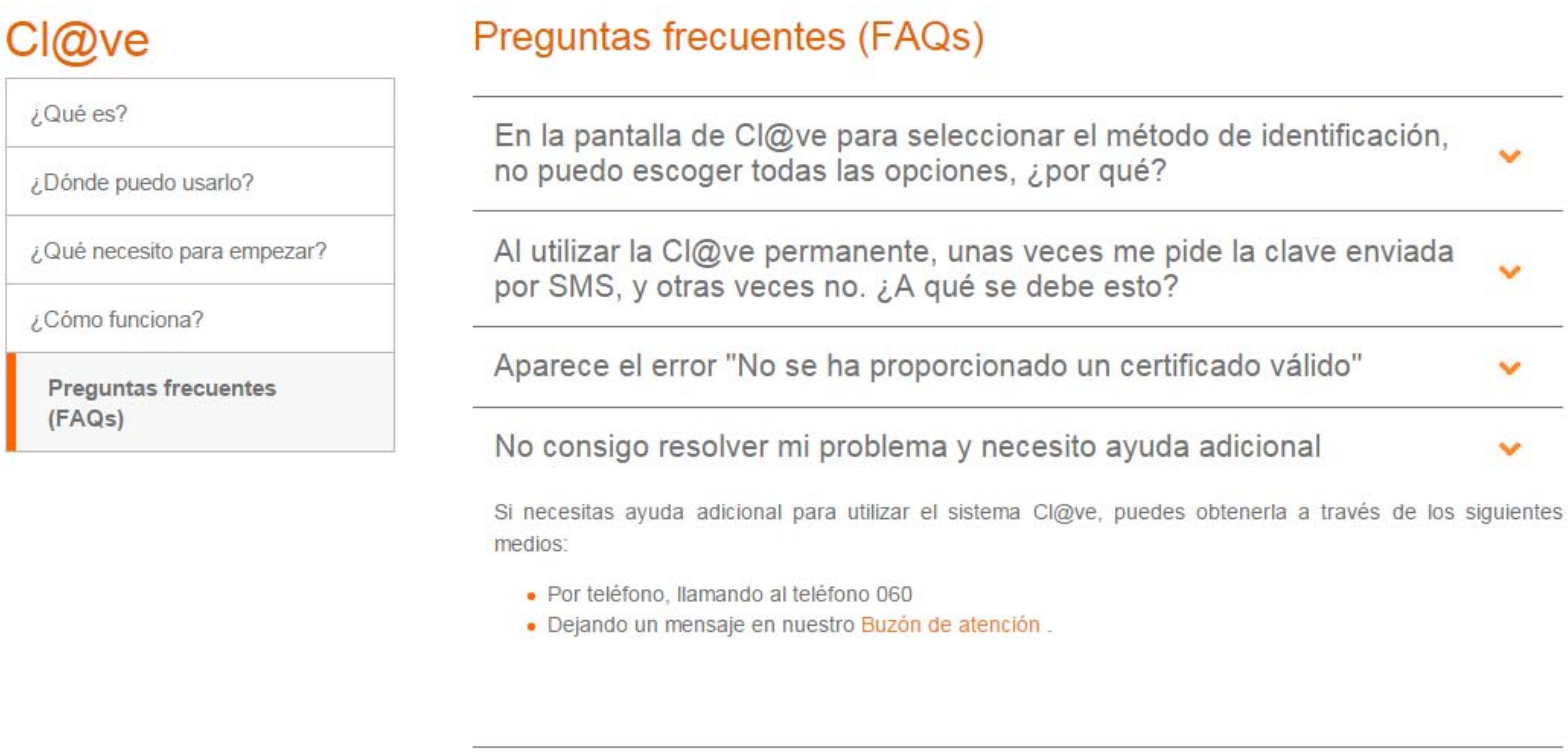
GOBIERNO DE ESPAÑA

cl@ve IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

Preguntas Frecuentes (FAQs)



Acceso del ciudadano al soporte



GOBIERNO DE ESPAÑA

clave.gob.es

cl@ve IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

cl@ve IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

Cl@ve | **Registro** | Cl@ve PIN | Cl@ve Permane... | Cl@ve Firma

Registro Cl@ve

Cómo darse de alta en Cl@ve



¿Cómo puedo registrarme?

Puedes regístrate por Internet o de forma presencial. Revisa el proceso y escoge el que más se adapte a tus necesidades.

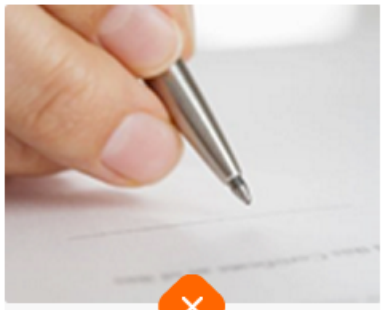
Leer más >



Modificación de datos

Puedes modificar tus datos con Cl@ve PIN, DNIe, certificado electrónico o en una de nuestras oficinas.

Leer más >



Renuncia

Puedes renunciar a Cl@ve en el momento que lo necesites tanto con certificado electrónico como de forma presencial.

Leer más >



Preguntas frecuentes · FAQs

Consulta tus dudas para darte de alta en Cl@ve

Leer más >



Registro

¿Cómo puedo registrarme?

Modificación de datos

Renuncia

Preguntas frecuentes (FAQs)

¿Cómo puedo registrarme?

Cl@ve es una plataforma de verificación de identidades electrónicas para la identificación y autenticación de los ciudadanos. Nos permite identificarnos ante las Administraciones Públicas con plenas garantías de seguridad. Para ello tenemos que registrarnos y puede hacerse por 3 vías:

- A través de Internet sin certificado electrónico
- A través de Internet con certificado electrónico o DNIe
- Presencialmente en una Oficina de Registro

Debe tenerse en cuenta que el registro a través de Internet sin certificado electrónico no permitirá acceder a determinados servicios ni utilizar Cl@ve Firma.

Registro

¿Cómo puedo registrarme?

Modificación de datos

Renuncia

Preguntas frecuentes (FAQs)

¿Cómo puedo registrarme?

Cl@ve es una plataforma de verificación de identidades electrónicas para la identificación y autenticación de los ciudadanos. Nos permite identificarnos ante las Administraciones Públicas con plenas garantías de seguridad. Para ello tenemos que registrarnos y puede hacerse por 3 vías:

A través de Internet sin certificado electrónico

Registro Nivel Básico.

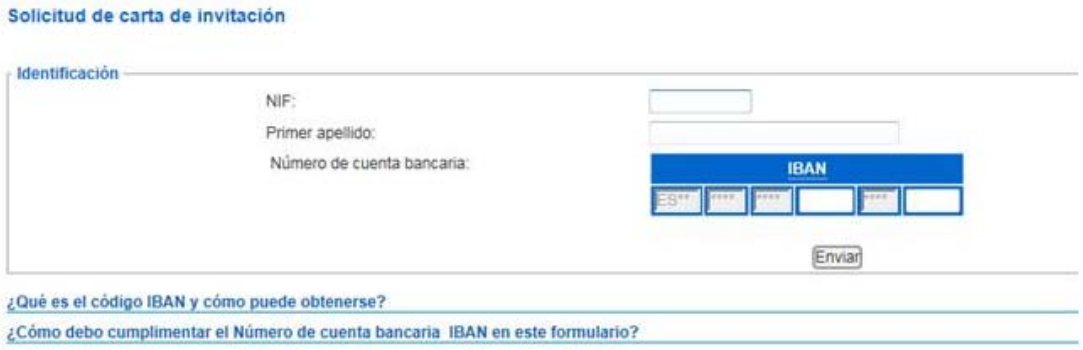
El proceso de alta en el Registro Cl@ve consiste en dos pasos:

Primero, tiene que acceder a la opción de Solicitud de Carta de Invitación, donde se le pedirán unos datos básicos de identificación necesarios para que reciba la carta invitación en su domicilio fiscal. En esta carta se incluirá un Código Seguro de Verificación (CSV), que le permitirá seguir con el paso 2.

Segundo, una vez que ha recibido la carta de invitación tendrá que acceder a la opción de alta en Cl@ve para completar el registro, aportando los datos necesarios que le permitirá utilizar Cl@ve.

A continuación se describen detalladamente estos dos pasos.

1. Solicitar una carta invitación para el alta en el Sistema Cl@ve.



GOBIERNO DE ESPAÑA

clave.gob.es

cl@ve IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

cl@ve IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

Cl@ve | Registro | **Cl@ve PIN** | Cl@ve Permane... | Cl@ve Firma

Bienvenido a Cl@ve PIN

Aprende a usarlo



¿Qué es?

Es un sistema de identificación y autenticación, que nos permite acceder a servicios de las Administraciones Públicas

Leer más >



Obtención de Cl@ve PIN

Con tu DNI/NIE y su fecha de caducidad, eliges una clave y recibes un PIN en un SMS ...

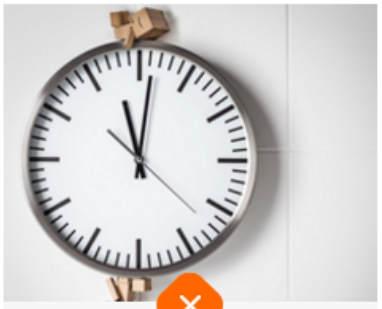
Leer más >



¿Cómo usarlo?

Introduces tu clave y el PIN que has recibido vía SMS ...

Leer más >



¿Cuándo caduca?

La validez será muy limitada en el tiempo

Leer más >

GOBIERNO DE ESPAÑA

clave.gob.es

cl@ve IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

cl@ve IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

Cl@ve | Registro | Cl@ve PIN | Cl@ve Permane... | Cl@ve Firma

Cl@ve Permanente



¿Qué es?

Sistema de autenticación que utiliza el usuario y la contraseña como parámetros para verificar la identidad de una persona.

Leer más >



¿Cómo funciona?

¿Qué hay que hacer para acceder a un servicio electrónico de una Administración Pública utilizando Cl@ve Permanente?

Leer más >



Procedimientos

Procedimientos relacionados con la gestión de Cl@ve Permanente: activación, olvido o cambio de contraseña.

Leer más >



Seguridad

Características que debe tener la contraseña para ser suficientemente segura.

Leer más >

Activación de Cl@ve Permanente

Cl@ve | Registro | Cl@ve PIN | Cl@ve Permane... | Cl@ve Firma

Cl@ve Permanente > **Procedimientos**

Cl@ve Permanente

- ¿Qué es?
- ¿Cómo funciona?
- **Procedimientos**
- Seguridad
- Preguntas frecuentes (FAQs)

Procedimientos

Describimos a continuación los procedimientos relacionados con la activación, uso y gestión personal de Cl@ve Permanente

Activación de usuario

Mediante este servicio puedes activar tu usuario de Cl@ve Permanente y crear tu propia contraseña de acceso.

Para la activación de tu usuario de Cl@ve Permanente debes acceder al servicio de activación donde se te pedirá que introduzcas tu usuario (tu DNI o NIE), tu dirección de correo electrónico (como dato adicional de contraste) y el código de activación que te suministraron en el acto de registro.

Accede al servicio clave.gob.es/activar

Si son correctos, el sistema te enviará un SMS con un código numérico de un solo uso (One Time Password, OTP) que deberás teclear en el campo del formulario correspondiente. Si es correcto, el sistema te permitirá establecer la contraseña que prefieras, siempre que cumpla con unas características mínimas de seguridad. Esta contraseña será la que deberás utilizar de ahora en adelante cada vez que un servicio de administración electrónica te la solicite.

Si introduces erróneamente el código de activación más de 5 veces, el sistema te informará y acto seguido bloqueará el código de activación. En este caso será necesario generar un nuevo código de activación, para lo cual deberás realizar de nuevo el acto de registro en Cl@ve.

Gestión de la contraseña

Si has olvidado tu contraseña o simplemente deseas cambiarla, puedes volver a establecerla de nuevo en cualquier momento con uno de los siguientes procedimientos:

- Cambio de Contraseña

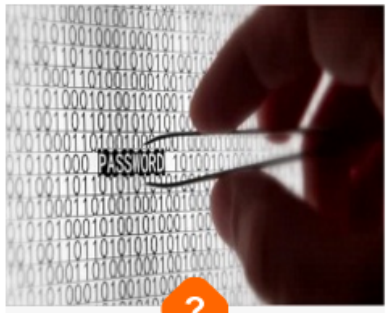
  Por motivos de caducidad o seguridad, puedes desear cambiar la contraseña. Para ello accede al servicio de cambio de contraseña y sigue los pasos que allí se describen.

GOBIERNO DE ESPAÑA

clave.gob.es

cl@ve IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

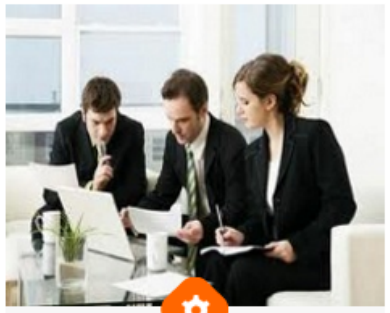




¿Que es?

Cl@ve es un sistema de Identificación, Autenticación y Firma Electrónica común para todo el Sector Público Administrati

Leer más >



Emisión y uso del dni

La entidad encargada de realizar las funciones de emisión y custodia de certificados electrónicos centralizados

Leer más >



Realizando la firma

Para la utilización del DNI electrónico es necesario contar con determinados elementos hardware y software que nos va...

Leer más >



Definiciones

En este apartado encontraremos las definiciones de la terminología empleada en la web de Cl@ve.

Leer más >

- Sistema Cl@ve
- Portal Informativo
- **Soporte al usuario**
  - **Soporte al Integrador**
  - Soporte al Ciudadano

Integración de Aplicaciones

Formas de Integración:

1. Implementación propia del motor de generación e intercambio de tokens SAML 2.0 definido por Stork.

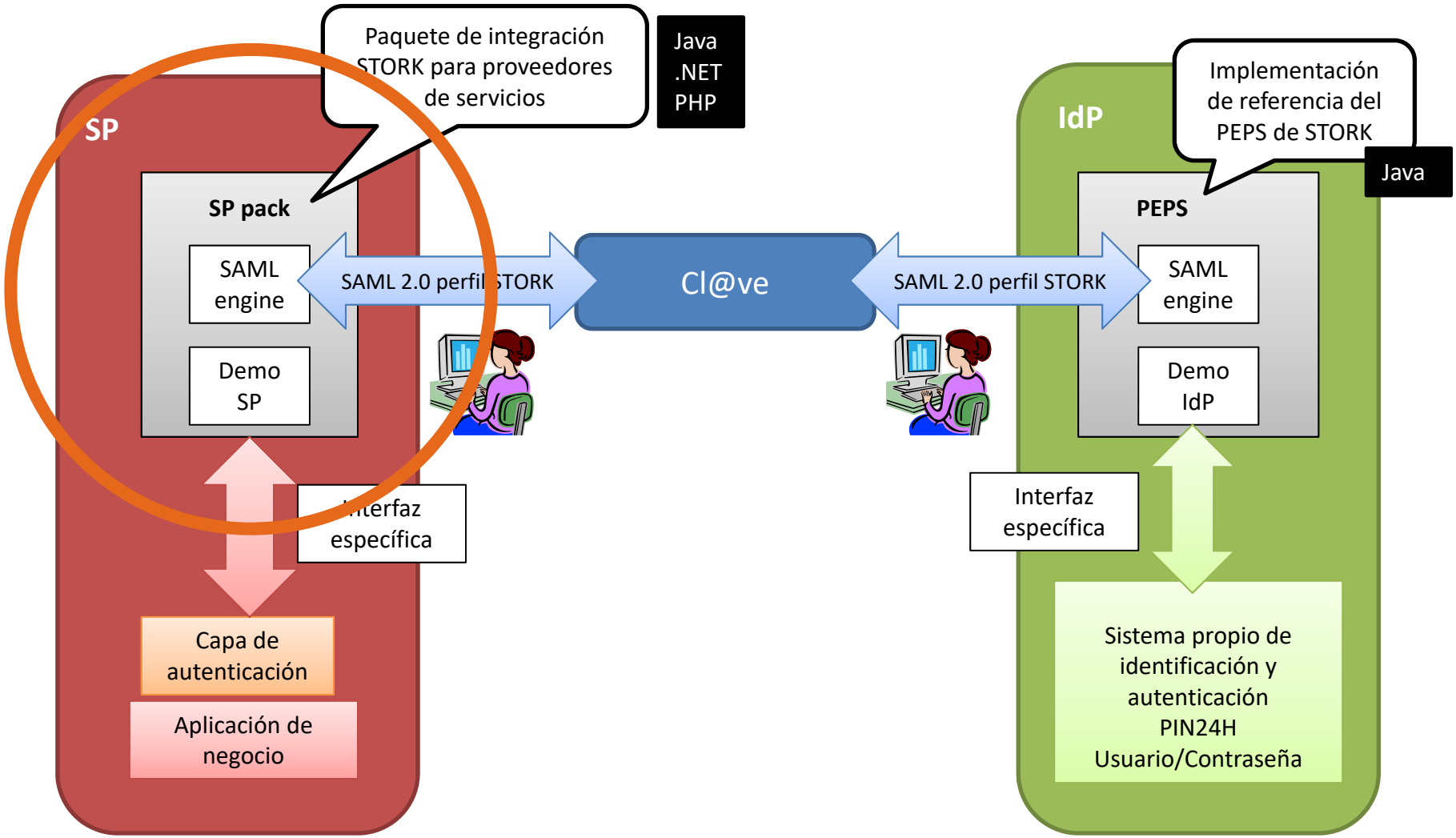
2. Utilización del Kit de Integración proporcionado por el proyecto Cl@ve.

Integración de Aplicaciones

- Información en el Portal de Administración Electrónica
  - Documento de integración
  - Kits de integración Java, .Net y PHP
  - ACL: Datos del Organismo y Aplicación. Parte pública de certificado electrónico.

http://administracionelectronica.gob.es/ctt/clave

Kit de integración



Soporte al Integrador

- CAID – Centro de Ayuda a Integradores y Desarrollares

  https://ssweb.seap.minhap.es/ayuda/consulta/CLAVE

  – Datos de contacto del integrador
  – Seleccionar “Integración de aplicaciones”

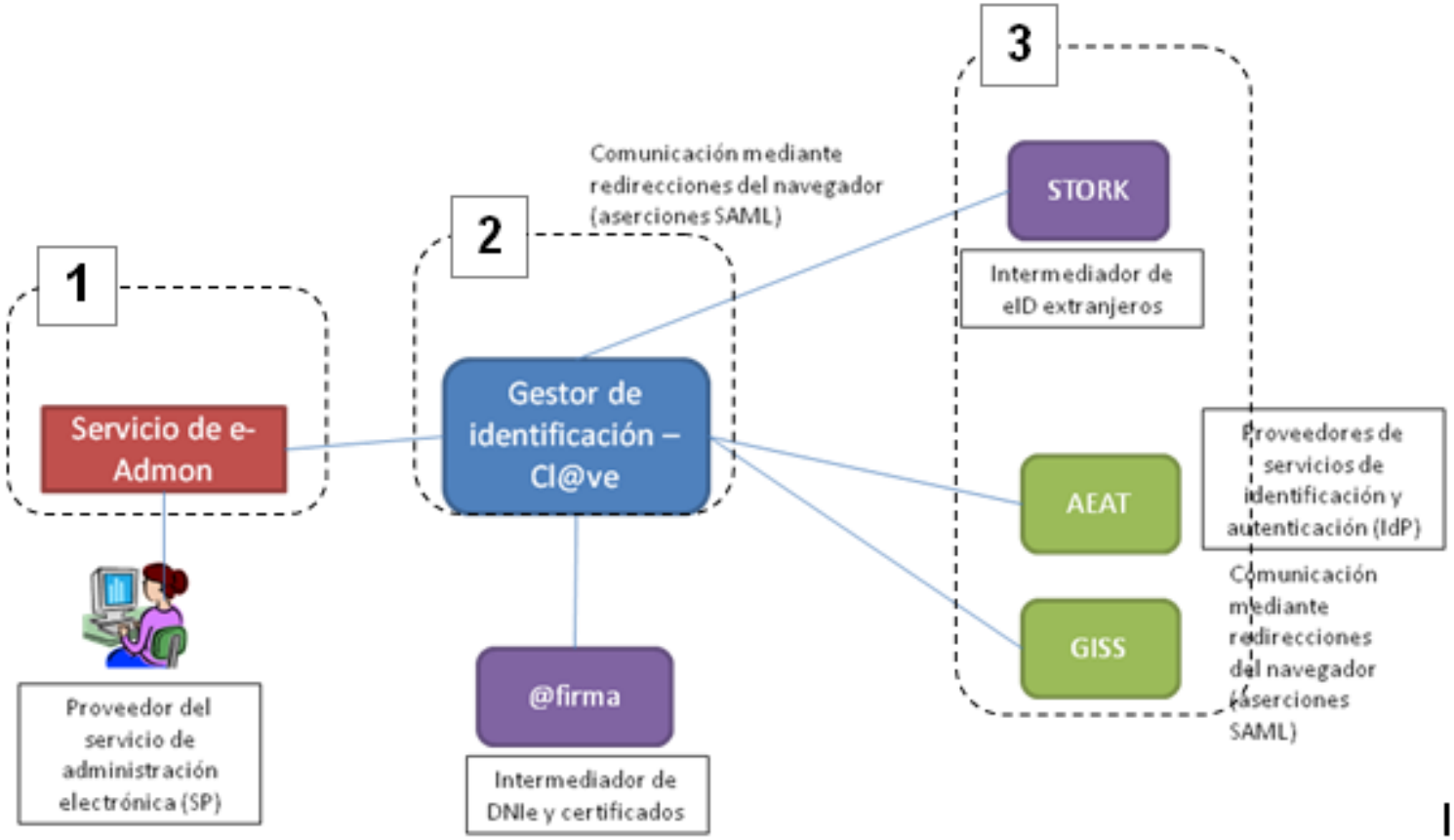
Soporte al Integrador



- Pasarela de Autenticación
- Portal Informativo
- **Soporte al usuario**
  - Soporte al Integrador
  - **Soporte al Ciudadano**

Atención a Ciudadanos

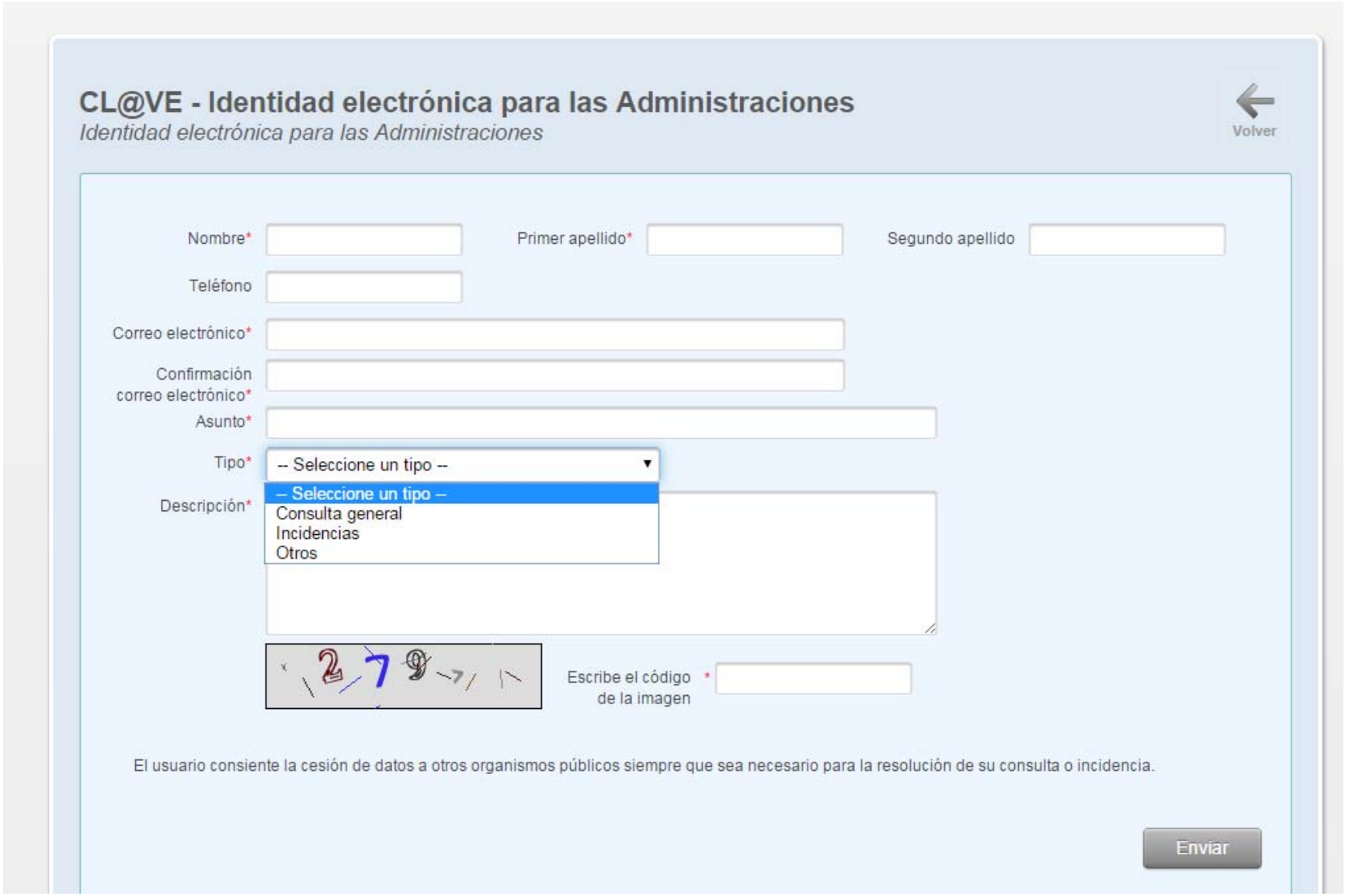
- El ciudadano “puede” contactar con diferentes organismos o actores en función de la página en que se encuentre.



Atención a Ciudadanos

- Servicio centralizado a través del 060
  - Las páginas de Cl@ve y Proveedores de Identificación apuntan a las FAQs correspondientes del Portal informativo
  - La última FAQ contiene los datos de contacto del 060
  - Teléfono y formulario. También canales disponibles en el portal administracion.gob.es

Formulario de contacto 060



Atención a Ciudadanos

- El 060 transferirá la incidencia al organismo responsable de su resolución: CAID o Proveedor de Identificación
- El 060 realizará un “Cross Channeling” hacia los soportes de 2º nivel
  - El 060 escala la incidencia al 2º nivel a través de un formulario
    (En el caso del Cl@vePIN/AEAT se puede transferir la llamada telefónica)
- El CAID centraliza y coordina las incidencias que involucran a varios actores o en el que interviene un SP

Gracias por su atención