

324

Sistema cl@ve

ViCoTAE



Sistemas similares en el sector privado. Ser:

- **Cliente**
- **Suscriptor**
- **Abonado**
- **Militante**
- **Afiliado**
- **Colaborador**
- **Socio**



Nos censan y emiten una credenciales sólo válidas para sus servicios así como claves de un solo uso (OTP), en cada actuación

Definición

Sistema horizontal para la identificación y autenticación de ciudadanos y el registro de la voluntad de realizar actos, basado en un sistema distinto del certificado electrónico y que cuente con las garantías de seguridad y usabilidad suficientes.

No es firma, permite la traza de actuación y custodia de evidencias.
En la Firma en la nube es el habilitador (llave) para utilizar el certificado personal allí custodiado

Definición

Sistema horizontal para la identificación y autenticación de ciudadanos y el registro de la voluntad de realizar actos, basado en un sistema distinto del certificado electrónico y que cuente con las garantías de seguridad y usabilidad suficientes.

Registro. Censo Único de ciudadanos que les permita relacionarse electrónicamente con las Administraciones Públicas. Este Censo se apoya en una aplicación de Registro que podrá ser utilizada por los organismos para registrar ciudadanos. Para cumplir este objetivo:

- El Censo debe recoger el teléfono móvil que facilitará el ciudadano, así como otros datos de contraste necesarios para gestionar los sistemas de Autenticación y Firma. Correo
- El Censo debe identificar la calidad del registro para que los organismos puedan decidir qué requisitos exigen para acceder a sus requisitos.



Punto de partida



Ideas	Notas
La Administración tiene muchos datos nuestros	DNI, fecha de caducidad, equipo expedidor, Domicilio, IBAN de cuentas declaradas, ...
Le falta el número de móvil y el correo electrónico	Debe conseguirlos en acto de registro 'laxo' o estricto de manera que estén asociados a los datos anteriores porque sean de la misma persona
Es accesible multi canal	Las AAPP son accesibles multicanal (por Sede, página Web, desde PC, desde Tablet, desde móvil, por telefonía de datos por telefonía, por datos por fibra/ADSL, por Wifi)
Puede poner en práctica la autenticación de dos fases	Operamos por un canal y las AAPP nos hacen llegar una clave de un solo uso (OTP o One time password) que se re introduce en la transacción de curso

Simplificando



Se crea Cl@ve que permite determinar la identidad y acceso a la firma

Se dosifica la seguridad entre escalones

Se concibe la firma por evidencias o 'registro de voluntad'

Es habilitador de la firma en la nube denominado 'Cl@ve firma'

Se hace uso de la autenticación en dos pasos

Simplicidad y uso en todo tipo de dispositivos sin requerir ni instalación ni lector

Dependiendo de la forma de alta en el servicio y comunicación de datos relativos a número de teléfono y correo electrónico

Dejar traza de que se ha realizado una acción que presupone aceptar lo que se ha presentado previamente en 'navegación por la sede'

Permite utilizar el certificado almacenado en las AAPP a nuestro nombre y utilizarlo para firmar de forma centralizada

La Directiva PSD2 para la Banca ha institucionalizado la identificación en dos pasos (OTP), como muy segura. Recibida por SMS



Normativa



BOLETÍN OFICIAL DEL ESTADO

- **Ley 39/2015**, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Artículo 10. [Ver](#)
- **Orden PRE/1838/2014**, de 8 de octubre, por la que se publica el **Acuerdo de Consejo de Ministros**, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas. [Ver](#)
- **Orden HAP/2142/2014**, de 14 de noviembre, por la que se crea el fichero de datos de carácter personal Cl@ve. [Ver](#)
- **Resolución de 14 de diciembre de 2015**, de la Dirección de Tecnologías de la Información y las Comunicaciones, por la que se establecen las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve. [Ver](#)
- **Resolución de 28 de septiembre de 2015** de la dirección de tecnologías de la información y las comunicaciones, por la que se establecen las condiciones para actuar como oficina de registro presencial del sistema Cl@ve. [Ver](#)
- **Ley 40/2015**, de 1 de octubre, de Régimen Jurídico del Sector Público. Convenios CAPÍTULO VI. [Ver](#)
- **Stork Secure identity across borders linked**. Identidad segura y coordinada sin fronteras (UE) [Ver](#)



Conocer **cl@ve** [Ver](#)

Procesos de alta. Una sola vez

1

Nivel
avanzado

Con certificado SW,
eDNI o certificado en
tarjeta criptográfica

Ya tenemos personalidad digital y deseamos tener otro medio para identificarnos. Aportamos el número de móvil y el correo electrónico

2

Nivel
básico

Sin comparecencia en
oficina de Registro ni
certificado

Solicitamos vía Web dando datos que sólo conoce la AP
Se nos remite a la dirección postal
Aportamos datos y completamos registro con el CSV recibido

3

Nivel
avanzado

Con comparecencia
en oficina de registro

Solicitamos de forma presencial

Activación: En cualquiera de los escenarios se comprueba que somos 'dueños' del número de móvil y/o de la cuenta de correo electrónico que hemos aportado, completando el registro con una respuesta a lo recibido. Se elige PIN de protección

Procesos de alta. Con certificado

Nivel
avanzado

Confirmación de alta

Acceso identificado a la
solicitud de registro

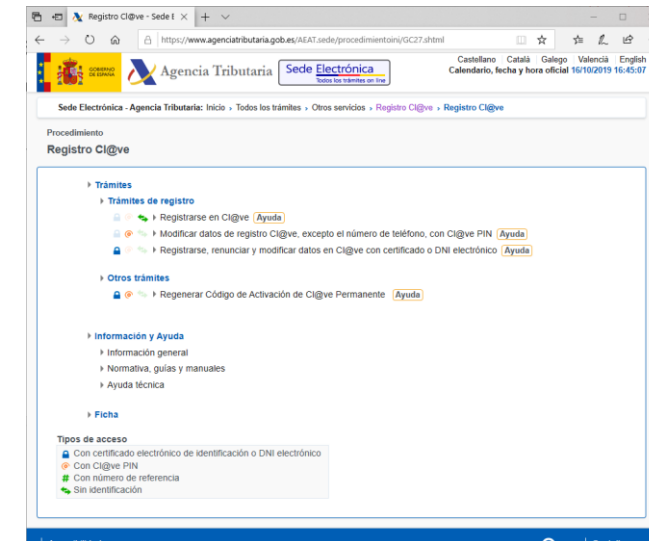
1

Con certificado

Aceptación de condiciones

Se nos presentan los datos
que la Administración tiene de
nosotros

Se aportan los datos de teléfono móvil y
correo electrónico



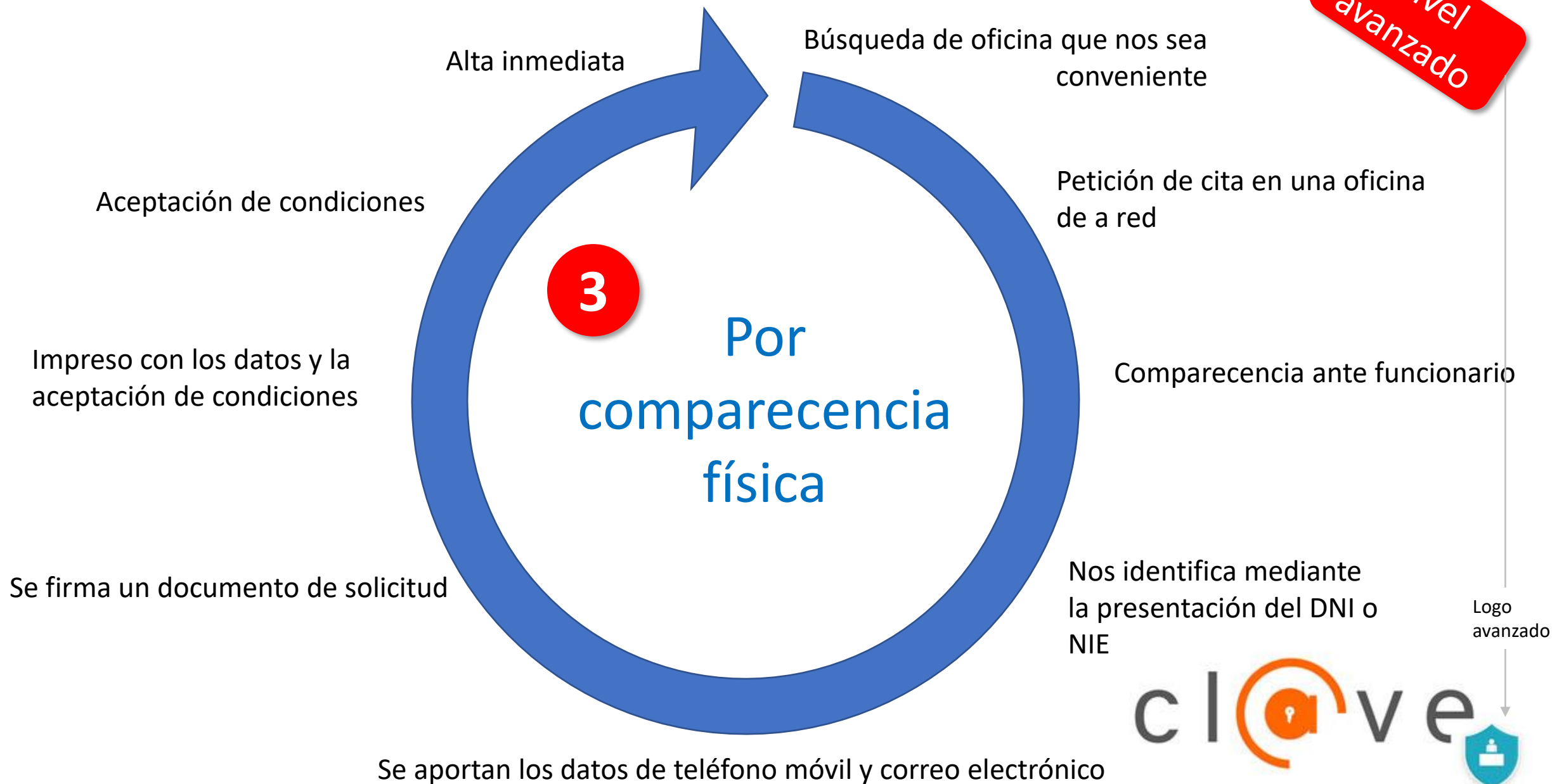
Procesos de alta. Sin certificado ni comparecencia

Nivel
básico



Procesos de alta. Por comparecencia

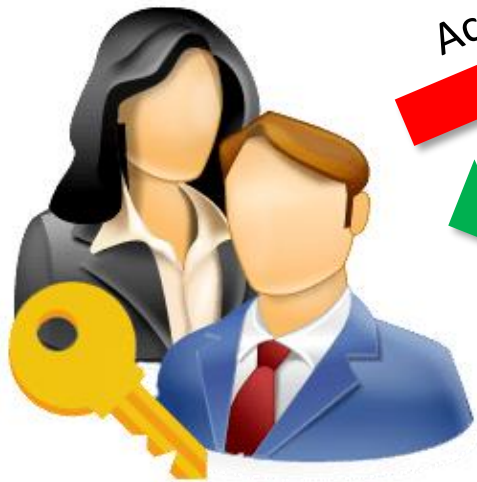
Nivel
avanzado



Proceso de uso



Usuarios



Acceso

Navegación
identificada

Proveedores de servicios de administración
electrónica (SP)
Sede de la Administración Pública

Generación de clave
de un sólo uso

Proveedores de servicios de identificación y
autenticación (IdP)
AEAT / GISS-TGSS / M.Interior / Stork

SP Proveedores de servicios de
administración electrónica
IdP Proveedores de servicios de
identificación y autenticación
OTP One time password



Cl@ve



Plataforma de Autenticación - Cl@ve Permanente

¿Qué es?

Es un sistema de autenticación diseñado para personas que necesitan acceder frecuentemente a los servicios electrónicos de la Administración. Se basa en el uso de un código de usuario, su DNI o NIE, y de una contraseña que se establece en el proceso de activación y que sólo debe ser consultada por ti. Para acceder al proceso de activación es necesario que previamente lo hayas registrado en el sistema.

Para los servicios de administración electrónica que requieren un nivel de seguridad elevado, el sistema refuerza la autenticación con la solicitud de introducción de un código numérico de un solo uso (One Time Password, OTP) que se envía previamente por mensaje SMS a tu teléfono móvil.

Teclee el código de un sólo uso
enviado a su teléfono móvil

Código

Autenticar >

Cancelar >

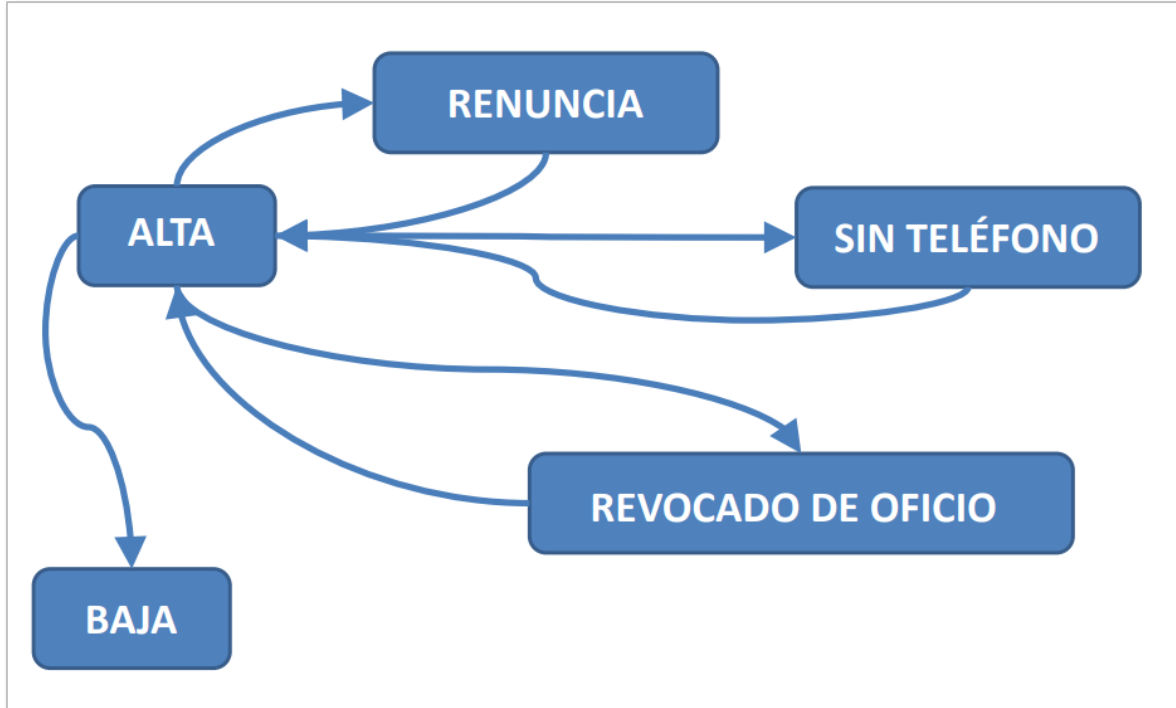
cl@ve

© 2015 Cl@ve - Identidad Electrónica para las Administraciones - Gobierno de España



Notas

Estados en el sistema Cl@ve



1. Un NIF (DNI o NIE) sólo puede estar asociado a un número de línea móvil ya que es el dispositivo y elemento esencial que garantiza la posesión en exclusiva del segundo factor de autenticación utilizado en el proceso de obtención de códigos de acceso al sistema
2. Pueden registrarse menores de edad según el procedimiento establecido. Se requiere móvil a asignar.
3. Estando de alta en el servicio, puede cambiarse de número de móvil o la dirección de correo electrónico, tanto de forma presencial como por formulario web. Se genera un nuevo código de activación.
4. Se puede promover la renuncia (baja) del sistema



Acceder al HSM (Hardware Security Module) o depósito seguro de certificados o 'dispositivo seguro de creación de firma', no es firmar. Eso permite Cl@ve firma y sólo eso.

Una vez se ha accedido, se firma con el certificado digital expedido a nombre del titular y custodiado de forma centralizada o en la nube.





PSD2 (Payment Services Directive) es la segunda Directiva Europea que regula los servicios de pago (por ejemplo transferencias, domiciliaciones, pagos con tarjetas...)



Sector privado. EEFF.

Equivalentes



Sector público

Identificación robusta y registro de voluntades
como sucedáneo de la firma adecuada a demostrar autoría o aceptación

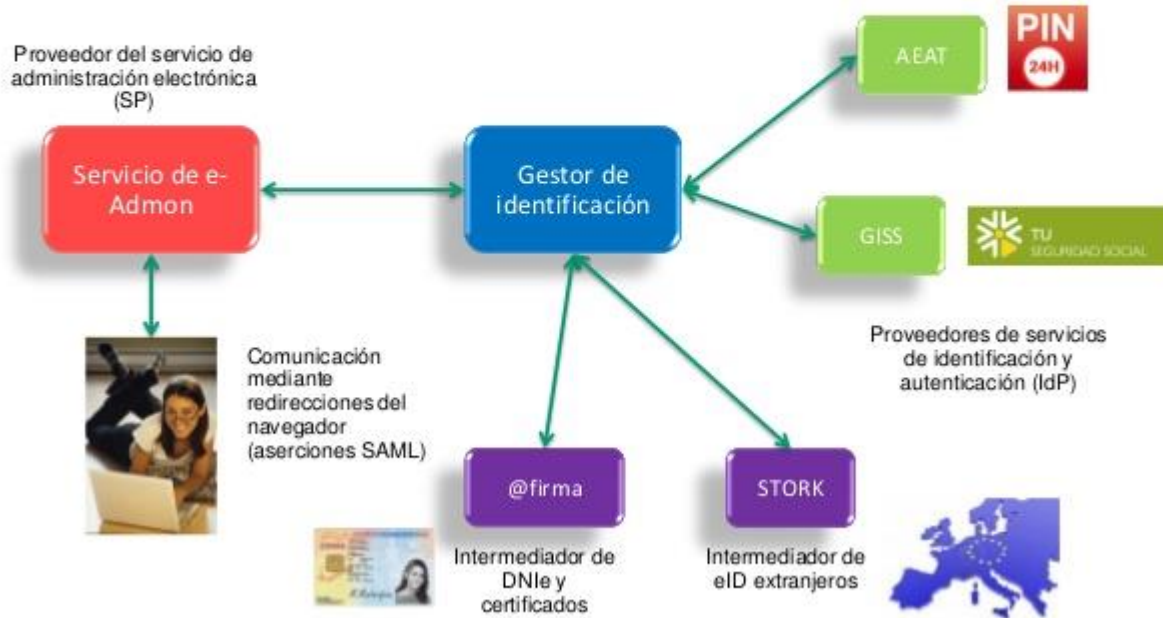
Federación de identidades,
SAML, SP, IdP, Stork, ...



Sistema de federación de identidades



Técnicamente **se apoya en los resultados del proyecto europeo STORK**



- Proveedores de servicios de administración electrónica (SP)
- Proveedores de servicios de identificación y autenticación (IdP)
- Pasarela / Gestor de Identificación primario y @firma y Stork

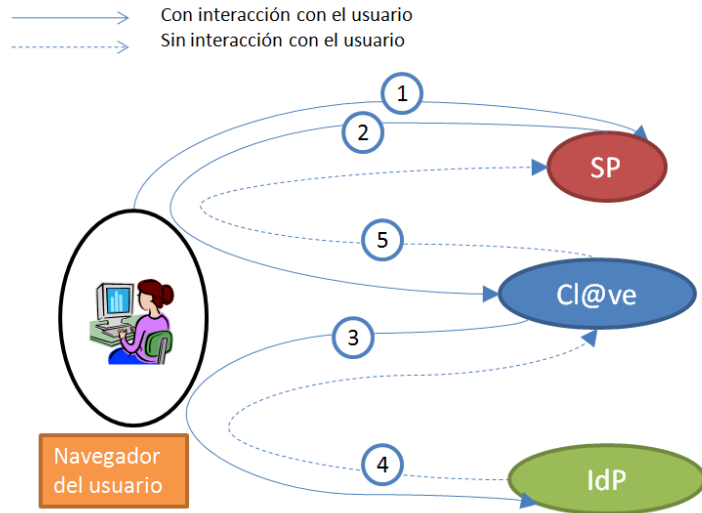
Los pasos de la interacción son los siguientes

- El ciudadano accede a un servicio de administración electrónica integrado con Cl@ve que requiere que se identifique
- El ciudadano es redirigido a Cl@ve, que le presenta una pantalla en la que debe seleccionar el método de identificación que quiere utilizar. – Las opciones activas en la pantalla vienen condicionadas por los parámetros que el SP ha indicado en el mensaje que ha enviado a Cl@ve relativos a los IdP y niveles QAA permitidos.
- El ciudadano selecciona el método de identificación y es redirigido al IdP correspondiente. – El ciudadano se autentica en el IdP seleccionado y es redirigido de nuevo a Cl@ve
- De forma transparente, sin que sea necesario interacción, el ciudadano es redirigido de nuevo al SP.

<https://administracionelectronica.gob.es/ctt/clave/infoadicional>

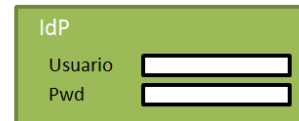
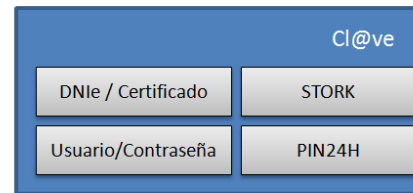
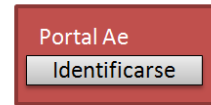


GOBIERNO
DE ESPAÑA



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



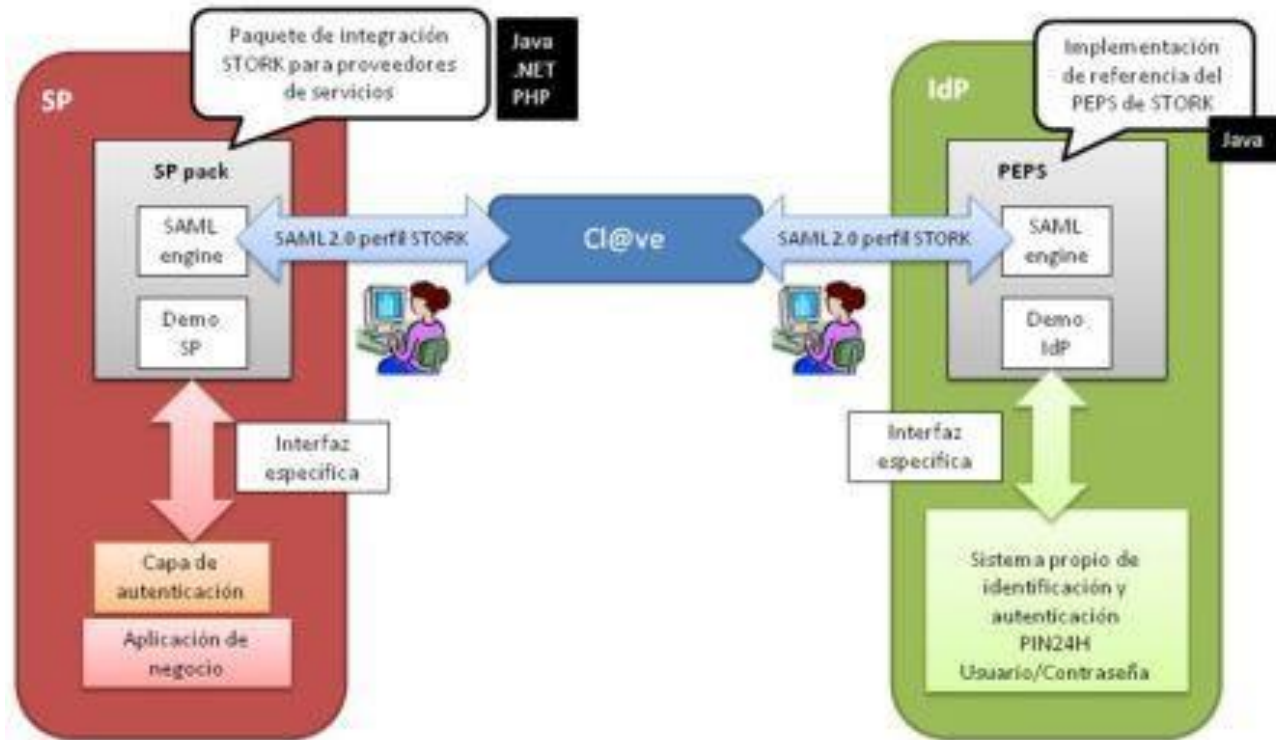
Flujo de interacción

Toda la comunicación con un componente de la plataforma Cl@ve se realiza a través del intercambio de tokens que pasan previamente por el navegador del ciudadano. De esta manera cada proveedor de servicios de identificación sólo responde al ciudadano desde el que ha recibido una petición de autenticación.

Los pasos de la interacción son los siguientes:

- El ciudadano accede a un servicio de administración electrónica integrado con Cl@ve que requiere que se identifique.
- El ciudadano es redirigido a Cl@ve, que le presenta una pantalla en la que debe seleccionar el método de identificación que quiere utilizar. Las opciones activas en la pantalla vienen condicionadas por los parámetros que el SP ha indicado en el mensaje que ha enviado a Cl@ve relativos a los IdP y niveles QAA permitidos.
- El ciudadano selecciona el método de identificación y es redirigido al IdP correspondiente. El ciudadano se autentica en el IdP seleccionado y es redirigido de nuevo a Cl@ve
- De forma transparente, sin que sea necesario interacción, el ciudadano es redirigido de nuevo al SP.

Proveedor de identidad

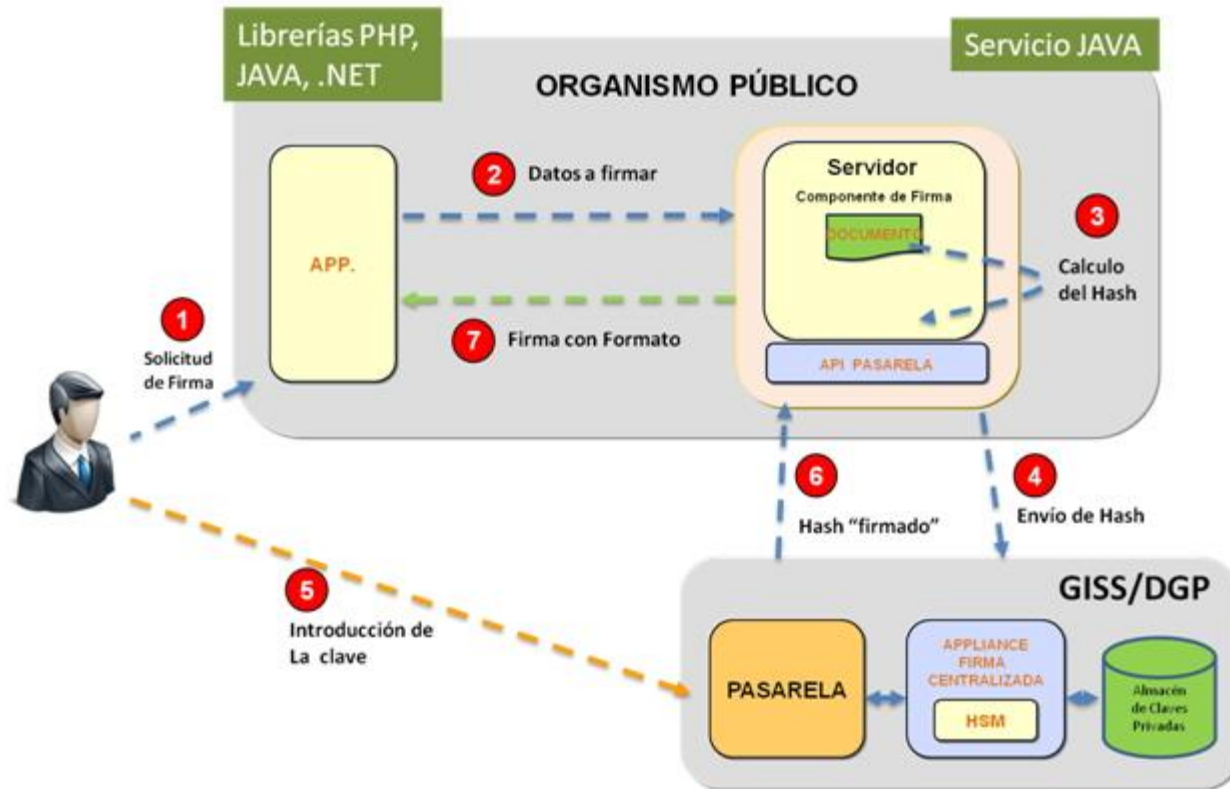


Para la identificación del ciudadano, el modelo de federación de identidades de Cl@ve se basa en el estándar SAML. Por tanto el modo de conexión al servicio de clave no es mediante servicios Web, sino mediante aserciones SAML de navegador.

En concreto, Cl@ve se basa en la utilización del perfil SAML 2.0 definido por STORK. Este perfil se utilizará tanto para la integración entre Cl@ve y el proveedor de servicios, como para la integración entre Cl@ve y el proveedor de identidad



Proceso de uso



- El usuario se identifica ante el sistema y solicita la firma de algún formulario/documento (1). Se consulta a la plataforma de firma de la GISS/DGP para saber si el ciudadano identificado con ese NIF posee certificados en la nube.
- Se prepara la prefirma (primera parte de la firma trifásica, anterior al cifrado de los datos con la clave privada), con los documentos y el hash que debe ser cifrado (2) y (3).
- Se solicita a la plataforma de firma de la GISS/DGP el uso de la clave privada, devolviendo al usuario una URL en la que debe introducir su contraseña y la clave OTP para el uso del certificado (4).
- El usuario introduce los datos requeridos para autorizar el proceso de firma (5).
- La plataforma de firma de la GISS/DGP realiza el cifrado de la huella digital con la clave privada del ciudadano (segunda parte de la firma trifásica) (6).
- Se redirige al ciudadano a la página en la que se finalizará el proceso de firma (7).

Convenios

Orden PRE/1838/2014, de 8 de octubre, por la que se publica el **Acuerdo de Consejo de Ministros**, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del **Sector Público Administrativo Estatal** para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas

Cuarto. Aplicación del sistema

2. Asimismo, con el fin de facilitar el acceso electrónico de los ciudadanos a la Administración y en desarrollo del principio de eficiencia, **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. Su incorporación al sistema Cl@ve será publicada en el Portal www.060.gob.es y en las sedes electrónicas que sean de aplicación.

Ley 40/2015, de 1 de octubre, de
Régimen Jurídico del Sector Público.
CAPÍTULO VI. De los convenios



Múltiples formas de identificación Reglamento (UE) nº 910/2014

En uso

Usuario y contraseña

Usuario, contraseña y token

324

Sistema Cl@ve de las AAPP

Nivel
básico

Nivel
avanzado

Certificado digital SW o HW

Basada en biometría

Personalidad soberana



eIDAS

Identidad multifactor con OTP
MFA Multi factor Autentication
SCA Strong Customer Autentication

OTP es One Time Password o clave de un solo uso
SCA Autenticación usuario robusta

310

Servicios de confianza UE

Identificación

Firma y sello

Sello de tiempo

Notificación

Terceros de confianza

Autoridad Registro

Emisión CRL
Revocación

OCSP
Comprueba

Gestión Estado

Autenticidad
Integridad
Confidencialidad
No repudio
Trazabilidad
Disponibilidad
Conservación



Persona física
Representante
Sello de PJ
De Sitio Web
De código

Seguridad probatoria

Tecnología

Soporte

Básica

Avanzada

Calificada

Login/Pass
Doble factor

PKI

Biométrica

Software

Criptográfico

HSM
Centralizado

324

324

ViCoTAE Canal YouTube
de difusión de la
Administración Electrónica
para todos los públicos



Miguel Solano Gadea

Videos sobre **Conceptos** y **Términos** de la **AE**



Gracias

Contenidos y realización del autor.
Licencia Creative Commons citando la fuente.



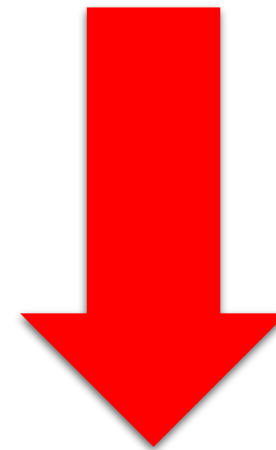
Temario general

- ☐ 000 Planteamiento general global
- ☐ 100 El enfoque funcional
- ☐ 200 Documento – Expediente - Archivo
- ☐ **300 Servicios de confianza**
- ☐ 400 Interoperabilidad
- ☐ 500 Normativa
- ☐ 600 Implantación
- ☐ 700 **Blog** Comentarios, opiniones, casos, anécdotas

miguel@solanogadea.es

@solanogadea

www.solanogadea.es



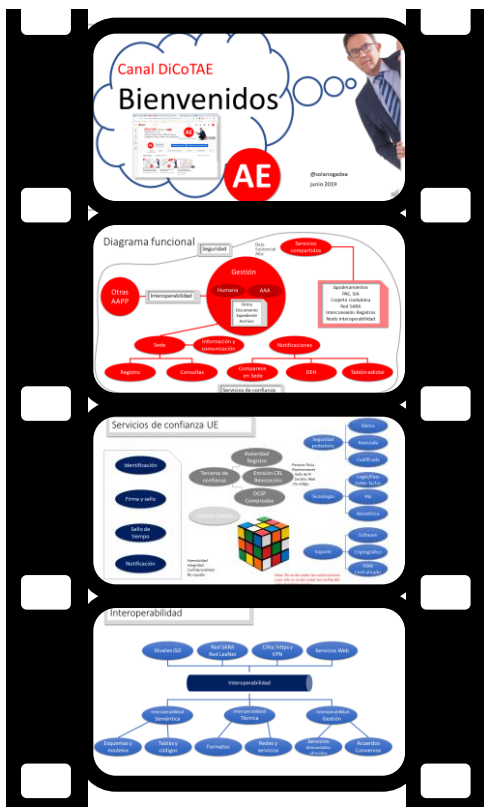
ViCoTAE

Vídeos sobre **C**onceptos y **T**érminos de la **AE**

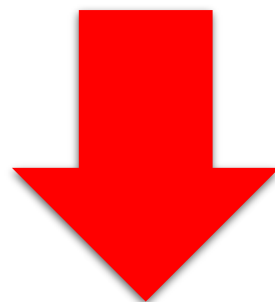


<https://www.youtube.com/c/ViCoTAE>

Acerca de



Contenidos y realización del autor.
Licencia Creative Commons citando la fuente.
Leer ficha y 'Mostrar más'



miguel@solanogadea.es
[@solanogadea](https://www.solanogadea.es)
www.solanogadea.es

Suscribirse

Compartir

Valorar 👍 👎

Comentar