Cl@ve – Firma

Facilita a los ciudadanos la firma electrónica en los servicios que proporcionan las Administraciones Públicas.

El sistema Cl@ve es la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica. Nace con el objetivo de facilitar el acceso y la firma electrónica de los ciudadanos en los servicios públicos electrónicos de las Administraciones Públicas.

Esta plataforma se aprobó por Acuerdo de Consejo de Ministros de 19 de septiembre de 2014 y, empezó a funcionar, proporcionando el servicio de identificación electrónica, el 17 de noviembre de 2014.

Ya hay (a finales de septiembre de 2016) **más de 3 millones de usuarios registrados en el sistema** y se han realizado **más de 12 millones de identificaciones,** con los distintos mecanismos previstos en la plataforma.

Hay un total de **54 organismos adheridos de la AGE** recientemente han empezado a integrarse con el sistema otras Administraciones no incluidas en el ámbito del Acuerdo de Consejo de Ministros (Sector Público Administrativo Estatal), permitiéndose ya con el sistema Cl@ve, el acceso a la sede electrónica del Ayuntamiento de Zaragoza y a determinados servicios de la sede electrónica de la Junta de Comunidades de Castilla-La Mancha.

Firma Centralizada

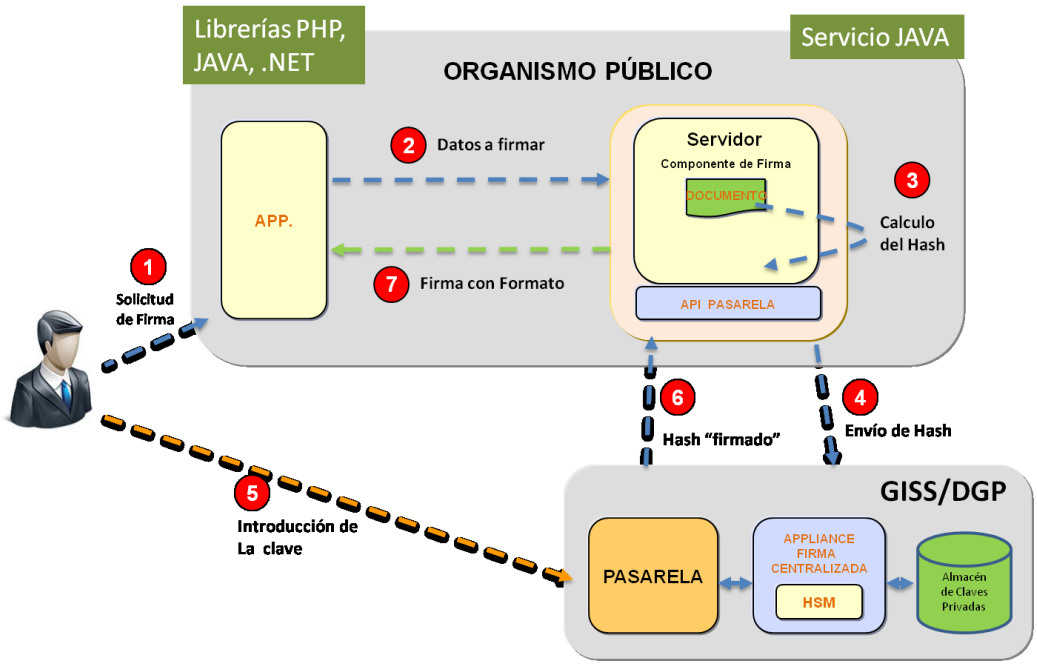
Pero el sistema Cl@ve también incluye la **firma centralizada, con certificados en la nube,** que pretende superar de manera definitiva los problemas de uso de los certificados electrónicos en los ordenadores de los usuarios. Los certificados de los ciudadanos se encuentran custodiados con fuertes medidas de seguridad en servidores centralizados de la Administración, en concreto de la Dirección General de la Policía (DGP) y respaldados en la Gerencia Informática de la Seguridad Social (GISS). Para acceder a ellos el titular necesita autenticarse con el usuario y contraseña de su Cl@ve Permanente e introducir un código de un solo uso enviado por teléfono (autenticación de doble factor). La firma se realiza en el servidor y no en el equipo del usuario, por lo que el ciudadano no tiene que preocuparse de la gestión de los certificados y puede, además, firmar desde cualquier dispositivo.

La firma se realiza siempre en el sistema HSM y "utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo", por lo que ésta podrá considerarse como firma electrónica reconocida o cualificada en términos del Reglamento eIDAS, equivalente por tanto a la firma manuscrita.

De esta manera, con Cl@ve – Firma se consigue reunir en una misma solución técnica la facilidad de uso que supone para el ciudadano el utilizar un usuario, contraseña y código enviado a su teléfono con el elevado nivel de

seguridad que proporcionan los certificados electrónicos. Además, el uso de certificados electrónicos garantiza que los documentos firmados son directamente interoperables, facilitando así su tratamiento posterior en los sistemas de administración electrónica.

Arquitectura de la solución cl@ve firma

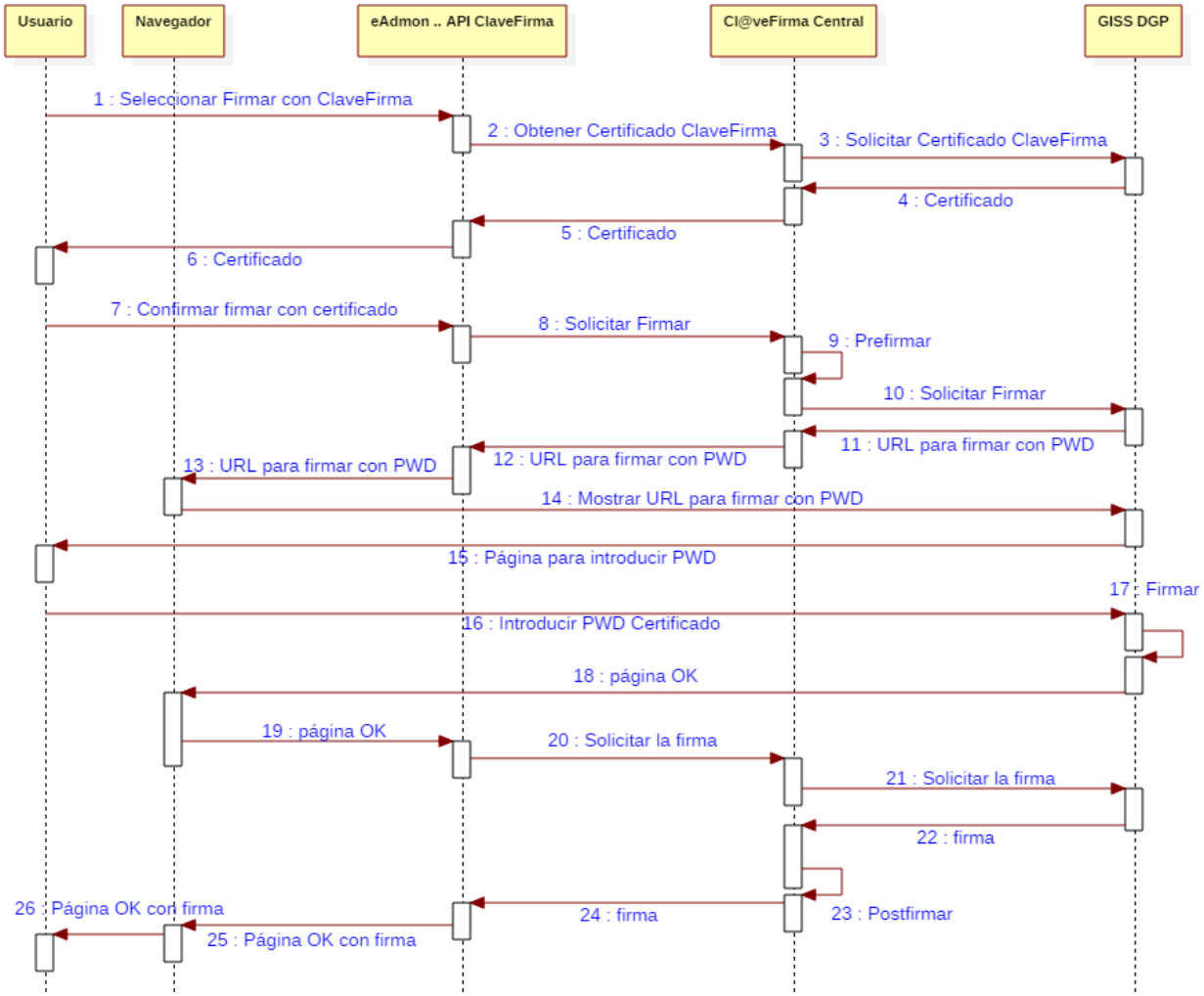


El proceso de la firma es el siguiente:

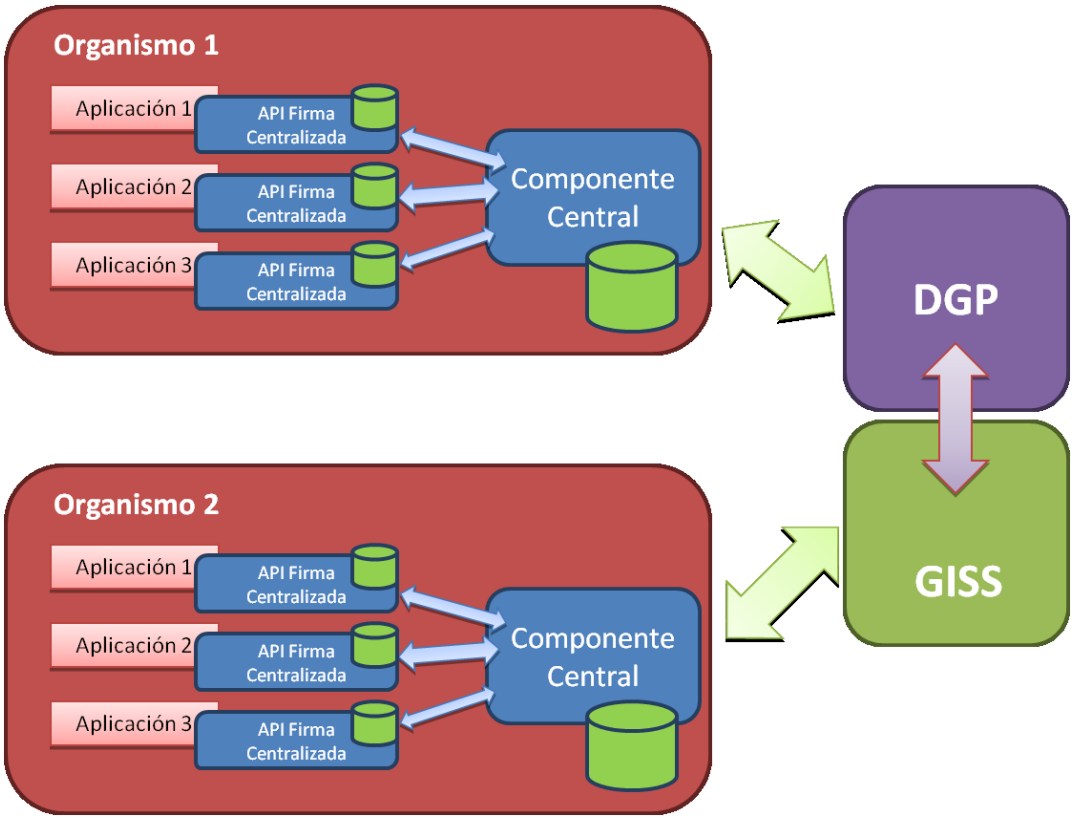
- El usuario se identifica ante el sistema y solicita la firma de algún formulario/documento (1). Se consulta a la plataforma de firma de la GISS/DGP para saber si el ciudadano identificado con ese NIF posee certificados en la nube.
- Se prepara la prefirma (primera parte de la firma trifásica, anterior 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).
- La API a través del componente central solicita el PKCS#1 generado a la plataforma de firma de la GISS/DGP.
- El Componente Central recupera el PKCS#1 y realiza la postfirma (tercera parte de la firma trifásica), componiendo la firma electrónica completa (AdES).
- La página de AE opera con la firma como se haya indicado.

Y en un diagrama de secuencia:



Para facilitar la integración de las aplicaciones con cl@ve la DTIC distribuye sendos kits de integración disponibles en http://administracionelectronica.gob.es/ctt/clave/descargas y en http://administracionelectronica.gob.es/ctt/clavefirma/descargas. Constan de una API de firma y de un componente central, a desplegar según este esquema:



Indicadores

La infraestructura de firma entró en producción el 19 de Enero de 2016, siendo el primer servicio de firma el de alta de beneficiario en la cartilla sanitaria. Posteriormente se han incorporado otros servicios de la Seguridad Social, del Servicio Público de Empleo Estatal y del MEySS, habiéndose realizado hasta el momento **más de 50.000 firmas con certificados centralizados**.

Está en proceso la integración de otros servicios de firma (DTIC, DGT,…)

Conclusiones

¿Qué se ha conseguido hasta ahora con la plataforma Cl@ve de identificación y firma electrónica?

- Un registro único de ciudadanos.
- Dos proveedores de servicios de autenticación distintos, con dos modos de autenticación, que complementan la autenticación tradicional mediante certificados electrónicos.
- Cada organismo puede elegir como se accede a sus servicios electrónicos en base a la calidad de Registro, nivel de seguridad y tipo de autenticación.
- Plena operatividad de la solución en todo tipo de dispositivos fijos y móviles.
- El ciudadano puede escoger en la pasarela Cl@ve el proveedor de identidad, en función del servicio electrónico con el que va a tramitar.
- Única identificación entre servicios de diferentes Organismos, mediante sesiones SSO (Single Sign-On).
- Ofrecer al ciudadano la posibilidad de realizar firma electrónica centralizada para la tramitación electrónica completa.

Autores:

Dirección de Tecnologías de la Información y las Comunicaciones

Dirección General de la Policía

Gerencia de Informática de la Seguridad Social