cl@ve
IDENTIDAD
ELECTRÓNICA PARA
LAS ADMINISTRACIONES

Cl@ve Firma

- Cl@ve Identificación

ESQUEMA GENERAL

GOBIERNO DE ESPAÑA

cl@ve IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

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



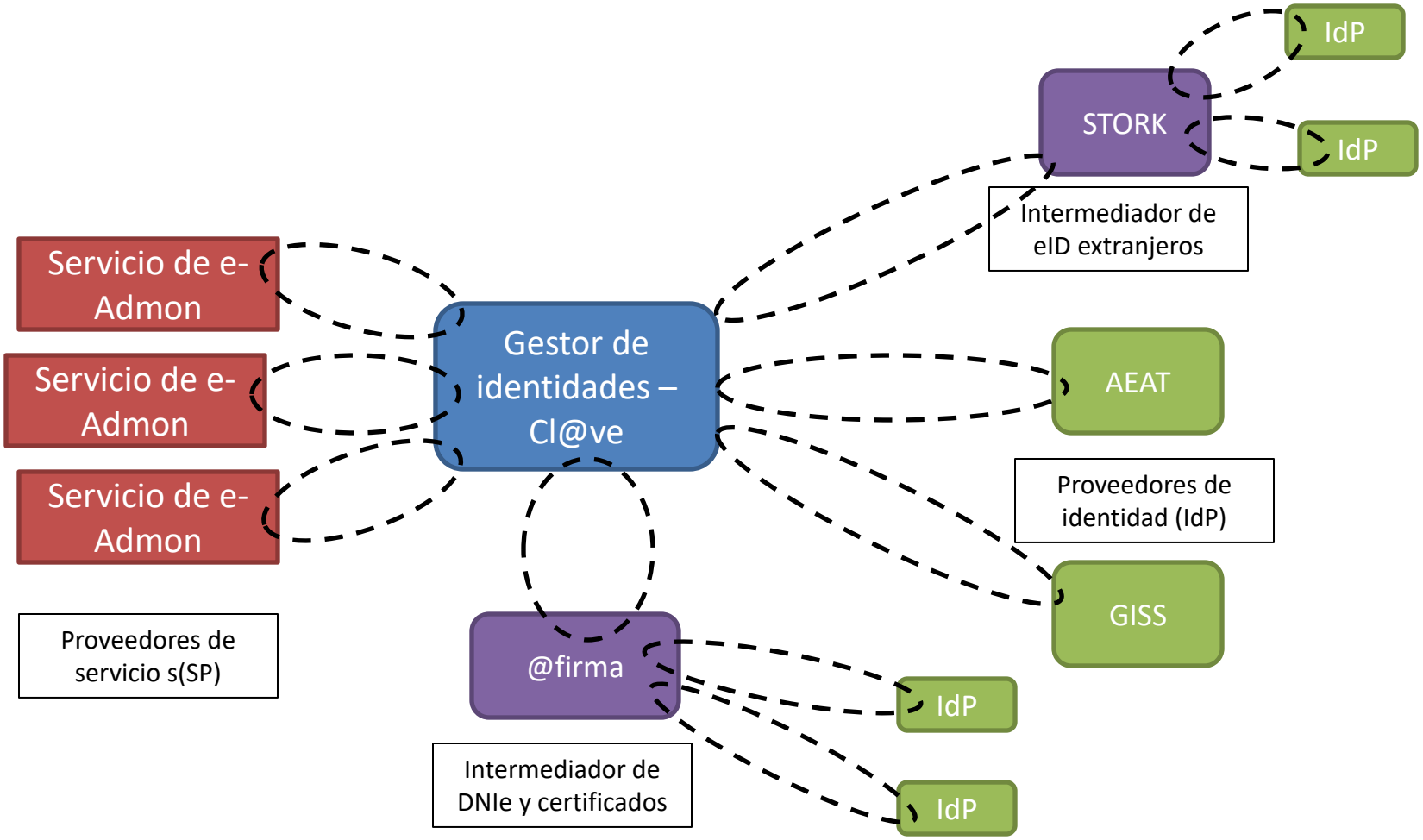
Intermediador de DNIe y certificados

STORK / eIDAS



Intermediador de eID extranjeros

Círculos de confianza



Intermediador de IdP



- Cl@ve Firma

Objetivos

Facilitarle la vida al Ciudadano

- ✓ No tiene que llevar el certificado encima
- ✓ Firma desde cualquier dispositivo
- ✓ Se olvida de problemas técnicos y de Java
- ✗ Reticencias a que un tercer custodie el certificado
- ✗ De momento **Firma Avanzada**
  - Falta pasar las auditorías correspondientes para que el sitema de la DGP y GISS pueda considerar Dispositivo Seguro de Creación de Firma

Base Legal

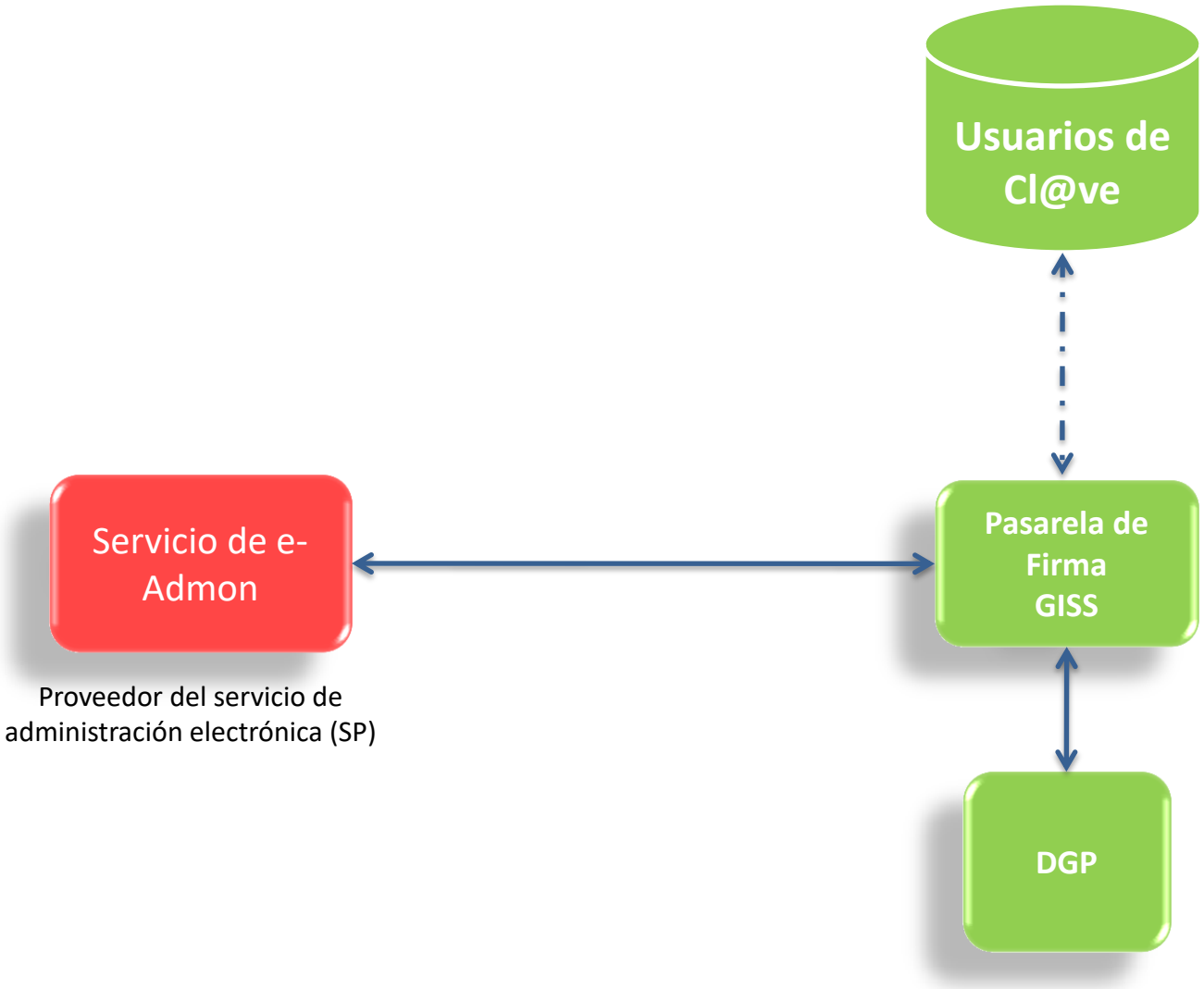
Formalizado por el **Acuerdo del Consejo de Ministros del 19 de septiembre de 2014**

- "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".

Plataforma Cl@veFirma



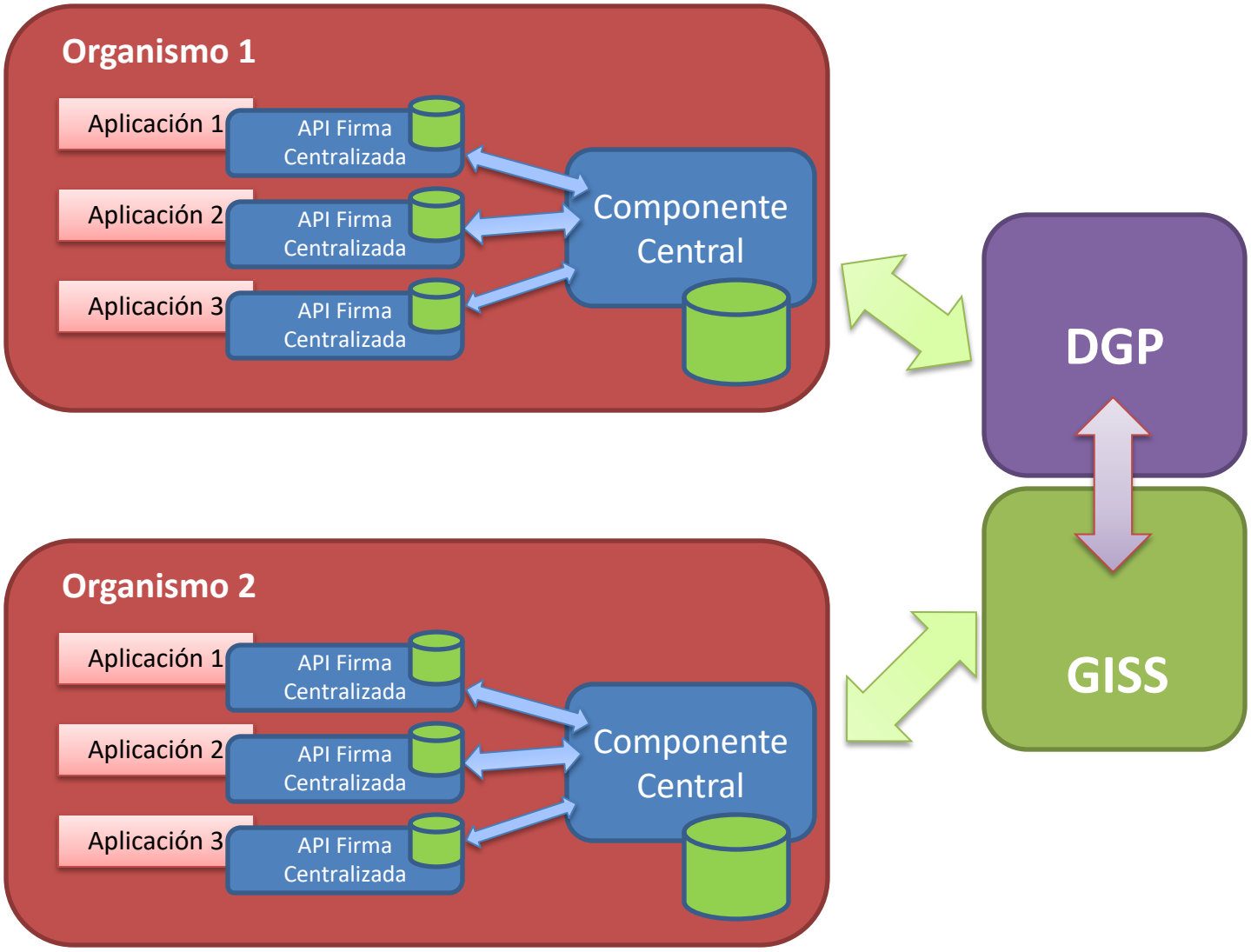
Proveedor del servicio de administración electrónica (SP)

Cl@ve Firma – Kit de Integración

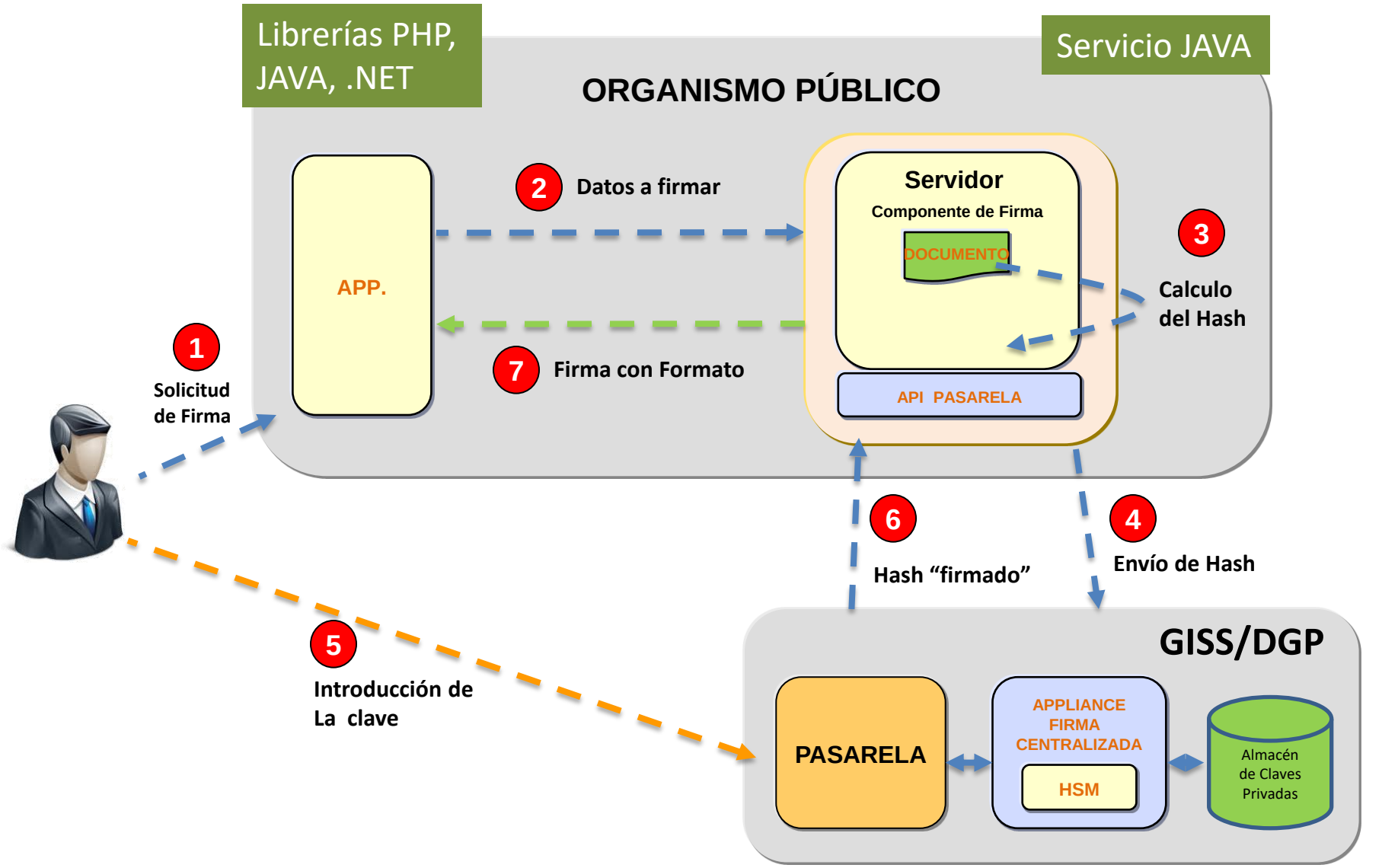
- **Componente Central**
  - Se instala uno en cada organismo. Tecnología Java
  - Funciones: Gestión de la firma trifásica y de las comunicaciones con los sistemas de la GISS/DGP.

- **Componente Distribuido - API cliente**
  - API a integrar en cada una de las aplicaciones de Administración Electrónica. Tecnología Java, PHP o .Net
  - Se encarga de la interacción con el ciudadano y la comunicación con el componente central.

Cl@ve Firma - Arquitectura



Cl@ve Firma - Arquitectura



Proceso de Firma Centralizada I

- Se consulta a la GISS/DGP para saber si el ciudadano identificado con ese NIF posee certificados en la nube.
- Se pide al ciudadano que seleccione el certificado de firma e indique el documento a firmar.
- Se prepara la prefirma (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.
- Se solicita a 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.
- El usuario introduce los datos requeridos para autorizar el proceso de firma.

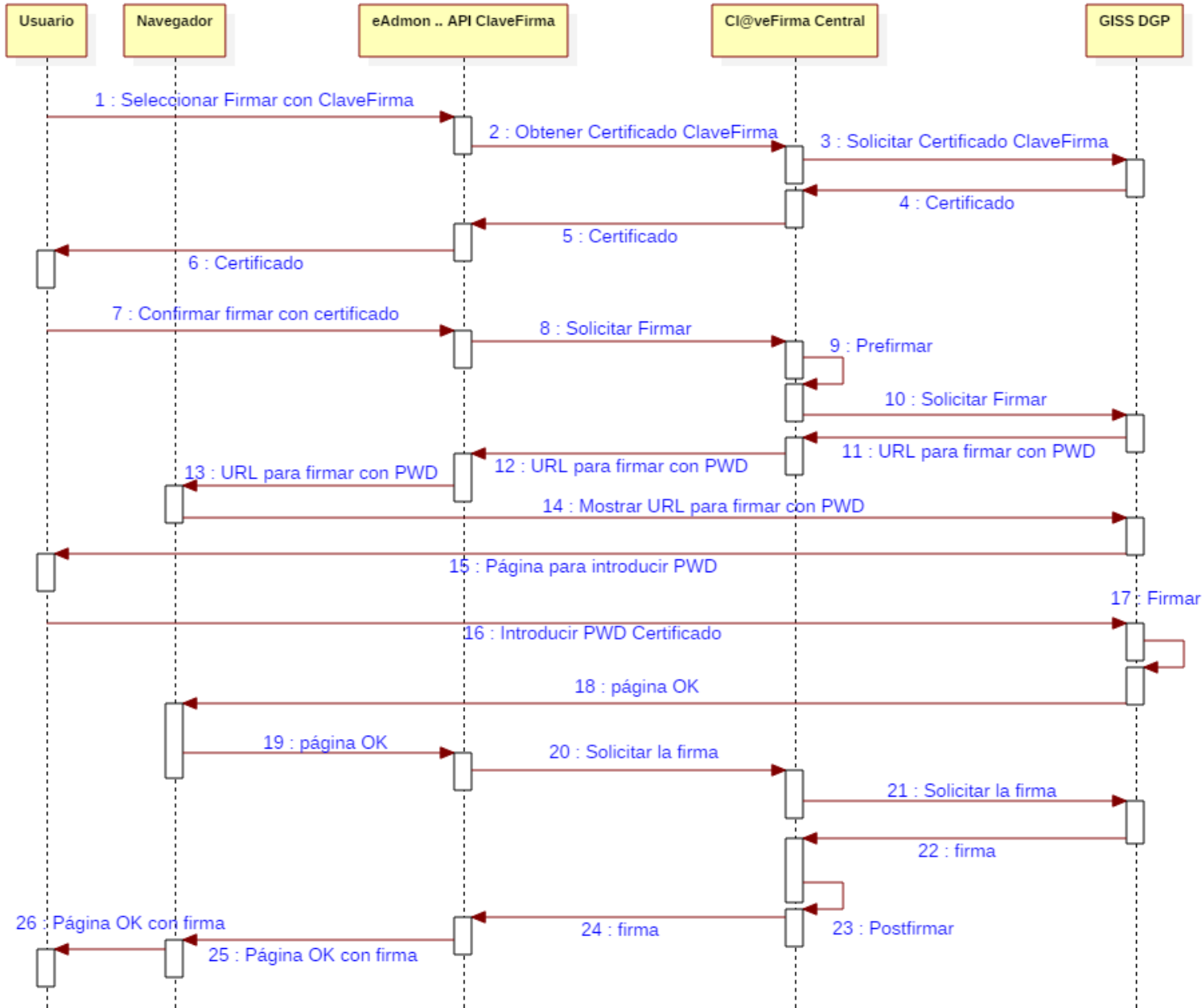
.....

Proceso de Firma Centralizada II

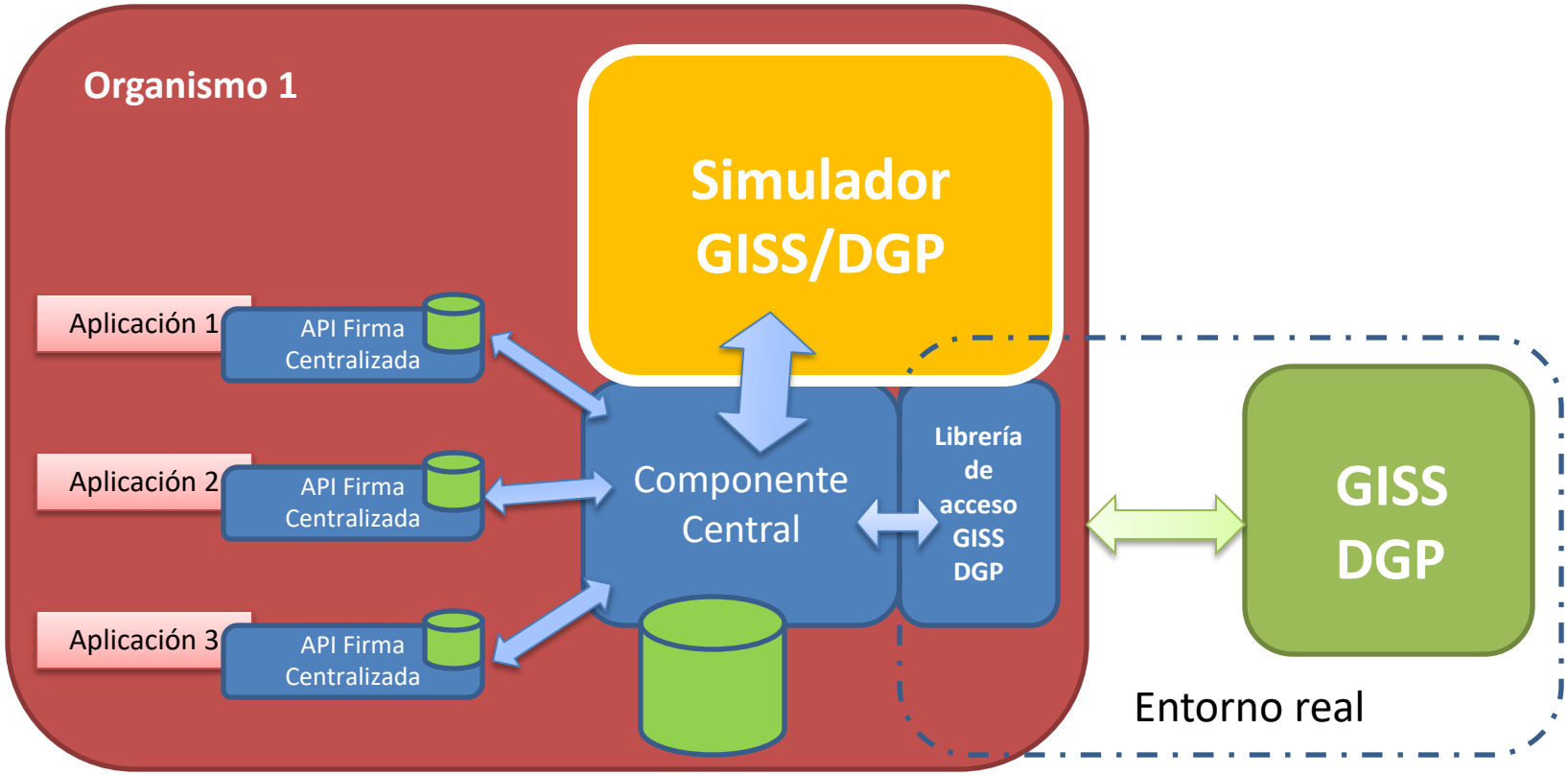
...

- La GISS/DGP realiza el cifrado de la huella digital con la clave privada del ciudadano (PKCS#1).
- Se redirige al ciudadano a la página en la que se finalizará el proceso de firma.
- El API a través del componente central solicita el PKCS#1 generado a 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.

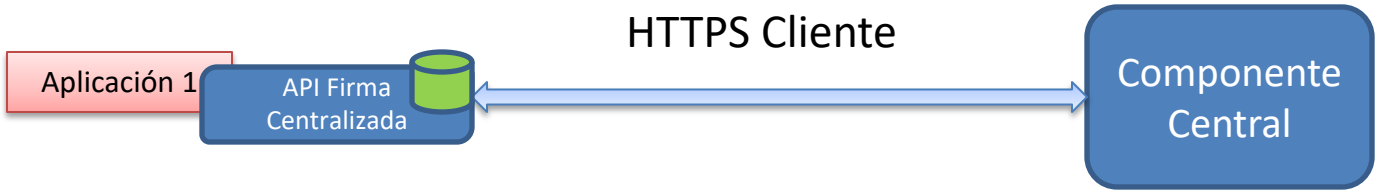
Proceso de Firma Centralizada



Simulador de Firma Centralizada
Librería java



Cl@ve Firma – Integración



Conexión con el Componente Central:

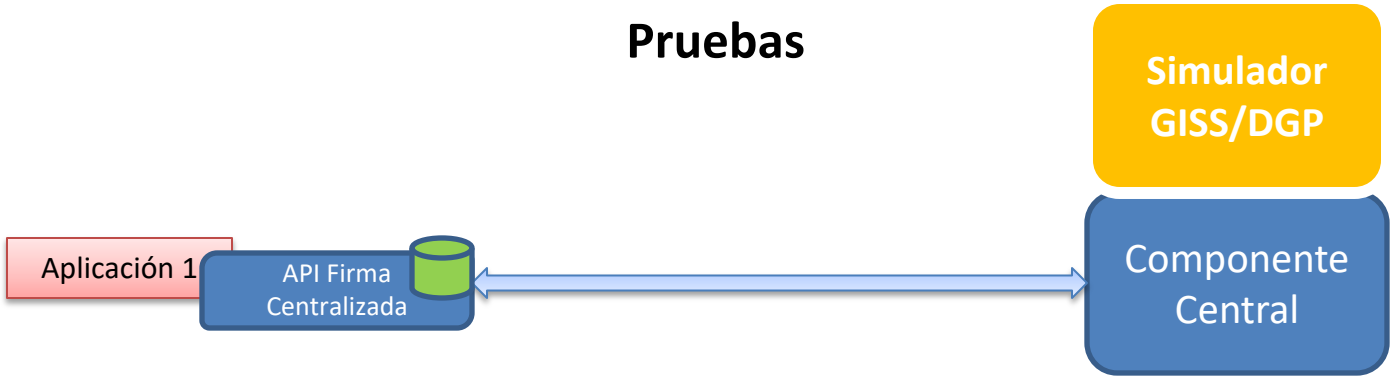
- **HTTPS Cliente**
- Enviar **Identificador** de aplicación
- Futuro: Enviar identificador de procedimiento

Alta de la aplicación en el Componente Central:

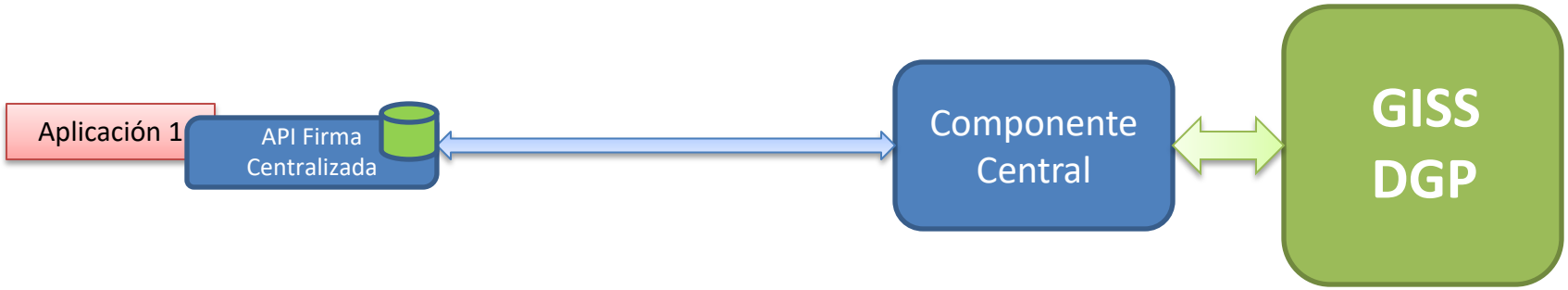
- Nombre de la aplicación
- Identificador
- Clave pública del certificado
- Datos del Responsable

Entornos

Pruebas



Producción



Cl@ve Identificación y Cl@ve Firma

Integración:

- Kit y documentos de integración en: http://administracionelectronica.gob.es/ctt/fire/descargas

Pruebas:

- Pruebas del organismo en local

Alta:

- El alta del Componente Central en la pasarela de la GISS
  - Enviar ACL de Cl@veFirma al CAID: alta de SP y aplicaciones

Necesidad 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

Proveedor del servicio de administración electrónica (SP)

Proveedores de servicios de identificación y autenticación (IdP)

Servicio de e-Admon

Pasarela Cl@ve

AEAT

Cl@ve PIN

El usuario quiere autenticarse



SMS

Red de Telefonía Móvil

GISS

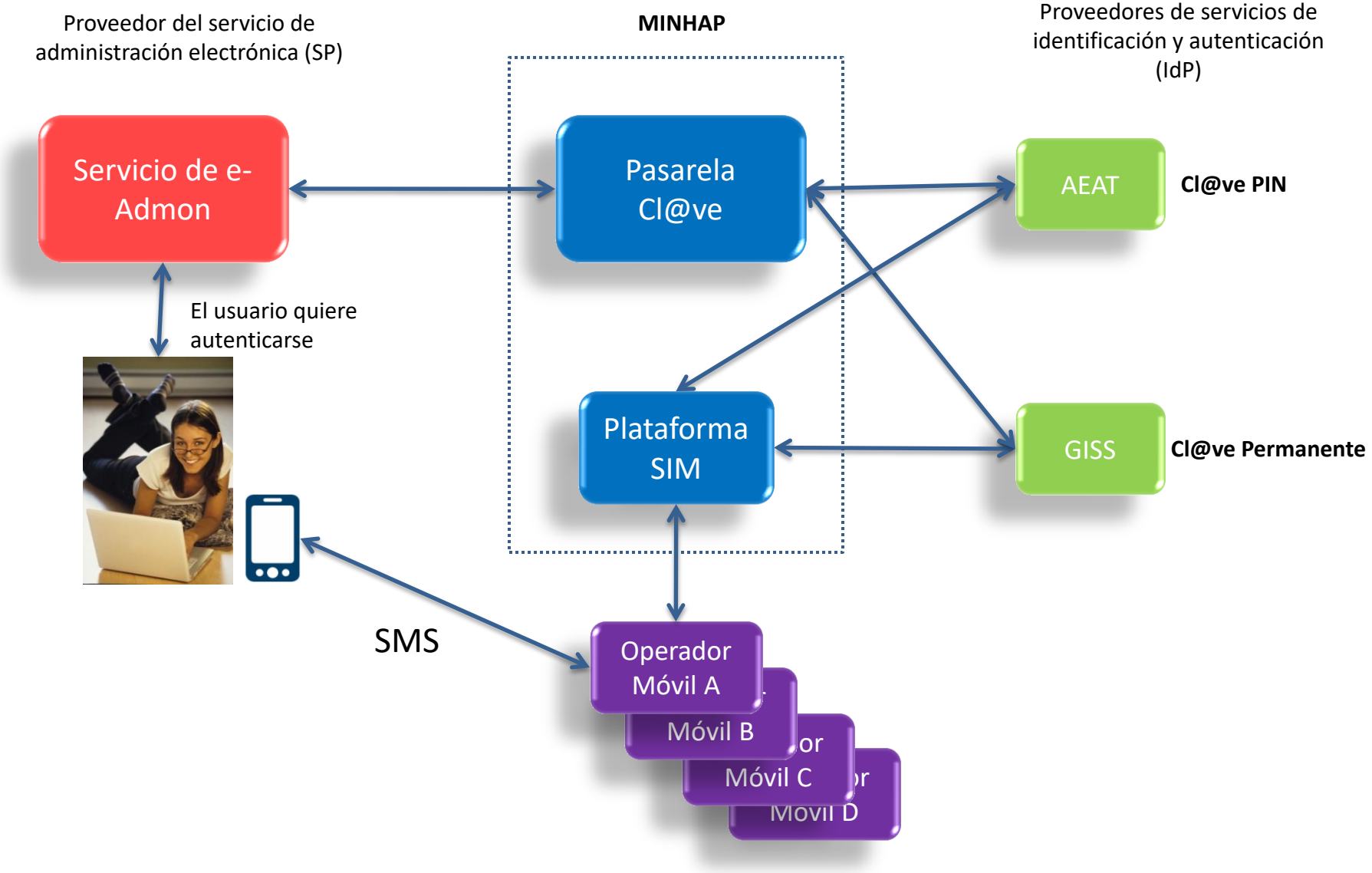
Cl@ve Permanente

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



Importante

- **SMS de prueba**

  Las pruebas iniciales de conexión con la plataforma SIM pueden requerir el envío de SMS de prueba.

- **Estado del contrato de Telefonía:**

  La plataforma SIM no hace un seguimiento del estado del contrato de los organismos con su operador. Será responsabilidad del organismo mantener activo el contrato con el operador para que el servicio de envío de SMS pueda ofrecerse sin interrupciones.

Muchas gracias