CONVENIO DE COLABORACIÓN ENTRE LA ADMINISTRACIÓN GENERAL DEL ESTADO (MINHAP) Y EL PRINCIPADO DE ASTURIAS PARA LA PRESTACIÓN MUTUA DE SOLUCIONES BÁSICAS DE ADMINISTRACIÓN ELECTRÓNICA

ANEXO: ESPECIFICACIONES TÉCNICAS DE LAS SOLUCIONES BÁSICAS DE ADMINISTRACIÓN ELECTRÓNICA

APARTADOS

I) **RED DE COMUNICACIONES DE LAS ADMINISTRACIONES PÚBLICAS ESPAÑOLAS: SERVICIO DE CONEXIÓN A LA RED SARA**

II) **UTILIZACIÓN DE SISTEMAS DE FIRMA ELECTRÓNICA AVANZADA: SISTEMAS DE IDENTIFICACION, FIRMA Y REPRESENTACION.**

III) **COMUNICACIONES ENTRE ADMINISTRACIONES PÚBLICAS POR MEDIOS ELECTRÓNICOS:**

III.a) Intermediación de datos entre Administraciones Públicas.

III.b) Intercambios de información a través del Portal de Comunidades Autónomas

IV) **PRÁCTICA DE LA NOTIFICACIÓN POR MEDIOS ELECTRÓNICOS: DIRECCIÓN ELECTRÓNICA HABILITADA Y CATÁLOGO DE PROCEDIMIENTOS DEL SERVICIO DE NOTIFICACIONES ELECTRÓNICAS.**

APARTADO I): RED DE COMUNICACIONES DE LAS ADMINISTRACIONES PÚBLICAS ESPAÑOLAS: SERVICIO DE CONEXIÓN A LA RED SARA

I.1. DESCRIPCIÓN GENERAL

I.1.1 Descripción de la Red SARA

La “Red SARA” permite el intercambio seguro de información entre las aplicaciones de las Administraciones Públicas conectadas mediante la conexión a una plataforma básica de comunicaciones de ámbito privado.

La Red SARA está formada actualmente por:

- la Intranet Administrativa, que ofrece un amplio número de servicios que se prestan en cooperación en el ámbito de la Administración General del Estado
- los elementos de conexión con TESTA II, que es la Red transeuropea que enlaza la Red Corporativa de la Comisión de la Unión Europea, con las de los Estados Miembros, para el soporte de intercambio de datos y cooperación en la prestación de servicios, y
- la Extranet de las Administraciones Públicas, compuesta por los elementos de enlace con las Redes Corporativas de las Comunidades Autónomas.

I.1.2. Servicios incluidos

Los servicios ofrecidos por la Red SARA son:

- Comunicaciones de datos
- Servicios básicos
- Política de seguridad común
- Aseguramiento de la calidad
    - Portal de Administradores
    - Servicio de soporte central
    - Servicio de soporte adicionales

Las Comunidades Autónomas y la Administración General del Estado, así como sus entidades de derecho público vinculadas o dependientes, podrán utilizar, a través de las aplicaciones informáticas correspondientes, cualquiera de los servicios de la Red SARA, previo acuerdo entre el prestador del servicio y el usuario del mismo, y la posterior comunicación al servicio de soporte central de la Red SARA.

I.2. ESPECIFICACIONES TÉCNICAS

I.2.1 Comunicaciones de datos

La Red SARA permite a la Red Corporativa de la Comunidad Autónoma las comunicaciones de manera segura, a través de un Área de Conexión (AC), a:

- la Extranet (redes corporativas de otras Administraciones y entidades públicas conectadas a la Red SARA)
- la Intranet Administrativa de la Administración General del Estado, y
- la Red TESTA II de la Comisión Europea.

I.2.2 Esquema y funciones del Área de Conexión (AC)

En el estado actual de la tecnología, el AC responde básicamente al esquema de una zona desmilitarizada (DMZ) formada por:

- un cortafuegos externo (que conecta con el resto de la red)
- un servidor donde residen los servicios básicos y
- un cortafuegos interno (hacia la Red Corporativa de la Comunidad Autónoma).

El sistema que actúa como cortafuegos externos es también el encargado, siempre que sea posible, de cerrar una VPN con el Centro de Acceso Remoto (CAR) de la Intranet Administrativa de la Administración General del Estado o con el AC de otro Organismo conectado directamente a la Red S.A.R.A. Este cortafuegos puede realizar igualmente funciones de traducción de direcciones de red (Network Address Translation - NAT) dinámico para las conexiones entrantes desde el resto de la Extranet hacia la Comunidad Autónoma.

Por su parte, el sistema que actúa como cortafuegos interno puede realizar también funciones de NAT contra destinos situados en el interior de la Comunidad Autónoma.

Las labores de conectividad y despliegue necesarias para poder acceder desde sus propias dependencias o instalaciones a la Red SARA a través del AC se realizan por la Comunidad Autónoma, que gestiona y mantiene los elementos activos de conexión de su Red Corporativa a SARA, permitiendo al centro directivo correspondiente del MINHAP el acceso de lectura y monitorización de los mismos, con independencia de que estas tareas sean asumidas por la propia Comunidad Autónoma o por un proveedor externo que ésta haya designado.

I.2.3 Descripción de los elementos que componen el Área de Conexión (AC)

En el estado actual de la tecnología, el AC se compone de:

- Router externo: este elemento conecta con la línea que une con la Red Troncal de la Extranet de las AA.PP.
- Conmutador LAN: para el conjunto de conexiones LAN de los elementos que componen la solución. Se configuran tres VLAN para separar el tráfico correspondiente a tres zonas:
  - Tráfico entre el router y el firewall externo (VLAN externa)
  - Tráfico de la propia AC (VLAN DMZ)
  - Tráfico hacia el interior de la Comunidad Autónoma.
- Cluster externo: formado por dos servidores en una configuración activo-activo. En condiciones normales los sistemas prestan las funciones que se describen a continuación; en degradado, cualquiera de ellos puede suministrar ambas funciones:
  - Cortafuego externo: cumple las funciones de cortafuegos y cierre de VPNs. Reside en un servidor Linux utilizándose productos de licencia GPL para cumplir estas funciones.
  - Servidor para los servicios de la Extranet: en él residen los servicios básicos de la Extranet de las AAPP que haya que implementar. Los servicios instalados son DNS, correo, proxy, servidor web, servidor socks y servidor NTP. También en este caso se trata de un servidor Linux con productos bajo licencia GPL.
- Cluster interno: formado por dos servidores en una configuración activo-pasivo. Las funciones que cumplen son:
  - Cortafuego interno: cumple las funciones de cortafuegos y NAT hacia el interior del organismo. Reside en un servidor Linux y se utilizan productos con licencia GPL.
  - Servidor de backup: es el nodo pasivo del cluster. En caso de fallo del nodo activo los servicios de cortafuego interno basculan a este servidor.
- Sistema de alimentación ininterrumpida (SAI): para mejorar la disponibilidad de los elementos en caso de cortes de alimentación. Este elemento estará conectado a uno de los servidores que actúa como maestro y es capaz de controlar a agentes disponibles en los otros servidores. Se instalará siempre que sea posible.
- Armario de media altura (rack): todos los elementos de la solución se integran en un único armario de media altura. Se instalará siempre que sea posible.

I.2.4 Características del recinto de instalación del Área de Conexión (AC)

La Comunidad Autónoma designa el lugar donde se instala el AC, que debe tener condiciones idóneas tanto para facilitar la conexión con su correspondiente Red Corporativa como para asegurar la continuidad del servicio.

Actualmente, los elementos que componen el AC se integran en un armario básico para montaje en Rack de todos los elementos, que apoya directamente en el suelo y que tiene las siguientes dimensiones:

Ancho	610 mm
Alto	1.200 mm
Profundo	1.000 mm
Peso Máximo	300 Kg

Las condiciones de alimentación eléctrica que actualmente requiere son las siguientes:

- Tensión de alimentación: 220V (+6 –10 %).
- Frecuencia de alimentación: 50Hz (+3 –3 %).
- Distorsión armónica total: < 5%.
- Tolerancia a micro-cortes sin perturbación en el funcionamiento, duración:< 20 ms.
- Potencia armario AC: 3.500 W (configuración inicial).

Las condiciones medioambientales del recinto que contenga el AC son de limpieza básica, de aislamiento de la radiación directa del sol, y de adecuada ventilación para evitar acumulaciones excesivas del calor disipado.

Actualmente los servidores que se integran en el AC no exigen la dotación de aire acondicionado ya que están diseñados para trabajar en un ambiente de oficina.

Por ello, el recinto que contenga el AC debe estar dentro de los límites siguientes:

- Temperatura comprendida entre 15 y 32º C.
  (Temperatura óptima recomendada: 22º C.)
- Gradiente horario máximo T < 5º C/h.
- Humedad relativa entre 20 y 80 %
  (Humedad relativa óptima recomendada: 50%)
- Gradiente horario máximo HR < 10% /h

Si por otros condicionantes fuera necesaria la instalación de aire acondicionado, se ha de tener en cuenta que el desprendimiento térmico máximo del conjunto de los elementos instalados dentro del armario en su configuración inicial es de 7.000 Btu/h.

I.2.5 Política de seguridad común

El AC comunica la Red Corporativa de la Comunidad Autónoma con las redes corporativas de otras Administraciones y entidades públicas conectadas a la red SARA (Extranet), con la Intranet Administrativa de la Administración General del Estado y con la Red TESTA II de la Comisión Europea.

Para garantizar que se hace de manera segura, es requisito el establecimiento de una política de seguridad común que corresponde aplicar al MINHAP, y que actualmente consiste en el establecimiento de VPNs y el cifrado del tráfico.

Por este motivo el AC es instalado, administrado y mantenido por el MINHAP, conforme a la documentación técnica que se facilita por el centro directivo correspondiente del MINHAP a la Comunidad Autónoma.

Asimismo, por este motivo se proporcionará al centro directivo correspondiente del MINHAP accesos de lectura y monitorización a los elementos que corresponda, con independencia de que el servicio de Red Corporativa de la Comunidad Autónoma sea propio o prestada por un operador.

I.2.6 Servicios básicos de la Extranet

Los servicios básicos de la Extranet son aquellos fundamentales que soportan la interoperabilidad entre aplicaciones o los complementan. La infraestructura integrada en el AC se encargará de la interoperabilidad de estos servicios.

Los servicios básicos que actualmente componen la Extranet son:

- DNS,
- relay SMTP,
- WWW,
- PROXY y
- NTP (sincronizado con el Real Observatorio de la Armada del Ministerio de Defensa).

I.2.7. Aseguramiento de la calidad del servicio

Con el fin de asegurar la calidad del servicio en todos sus componentes, se dispone de los siguientes elementos:

- el Portal de Administradores
- los servicios de soporte.

I.2.8. Portal de Administradores

El Portal de Administradores contiene información sobre el servicio proporcionado, notificación de incidencias, paradas programadas, publicación

de nuevos servicios u otros elementos necesarios para el correcto funcionamiento del sistema. Dicha información estará accesible para los responsables técnicos que designe la Comunidad Autónoma.

I.2.9. Servicios de soporte

El MINHAP dispone de un servicio de soporte central al cual corresponde recibir la notificación de incidencias, la resolución de las mismas cuando le corresponda, y la gestión de la resolución cuando intervengan agentes externos (fabricantes, operadores, u otros Organismos con acceso al Sistema), así como atender las consultas técnicas relacionadas con el servicio y las peticiones de nuevos accesos.

La Comunidad Autónoma podrá disponer de un servicio de soporte adicional, a ser posible 24x7, con este mismo cometido, tanto para garantizar los servicios de la Red SARA como aquellos otros que no haya proporcionado el MINHAP.

A través de la Comisión de Seguimiento se intercambiarán y actualizarán los contactos, tanto de los responsables de la conexión a la Red SARA en la Comunidad Autónoma y Entidades Locales en su caso, como los de los servicios de soporte que correspondan.

I.2.10. Mantenimiento y resolución de incidencias

La gestión, mantenimiento y resolución de incidencias de los elementos activos de la Red Corporativa de la Comunidad Autónoma conectados a Red SARA se harán por la propia Comunidad Autónoma, sin perjuicio del acceso de lectura y monitorización a la lectura y monitorización de los mismos que corresponda al centro directivo correspondiente del MINHAP, con independencia de que estas tareas sean realizadas por la Administración autonómica o por su operador.

La detección, diagnóstico y resolución de las incidencias por el centro directivo correspondiente del MINHAP puede requerir la colaboración de la Comunidad Autónoma, pudiendo incluir esta colaboración la realización de pequeñas comprobaciones o actuaciones en el AC, dirigidas desde el servicio de soporte central de la Red SARA, con el fin de reducir los tiempos de resolución de las incidencias que pudieran ocurrir.

I.2.11 Niveles de servicio iniciales

Se define el siguiente nivel de servicio inicial respecto al servicio de soporte central:

Tiempo de respuesta de soporte de Red SARA (24x7)	**120 minutos**

La Comisión de Seguimiento podrá determinar nuevos valores cuando corresponda por motivos técnicos o legales.

APARTADO II: UTILIZACIÓN DE SISTEMAS DE FIRMA ELECTRÓNICA AVANZADA: SISTEMAS DE IDENTIFICACION, FIRMA Y REPRESENTACION

II.1. PLATAFORMA DE VALIDACIÓN Y FIRMA ELECTRÓNICA @FIRMA

II.1.1 Descripción de @firma

@firma es un conjunto de productos y servicios de certificación y firma electrónica desarrollada por el MINHAP, que se pone a disposición de las Administraciones Públicas y de sus entidades de derecho público vinculadas o dependientes, para fomentar la puesta en marcha y el despliegue de aplicaciones informáticas y servicios de Administración Electrónica que requieran validación de firma electrónica basada en certificados, autenticación, generación de firma electrónica o sellado de tiempo en su relación con los ciudadanos, empresas y organismos.

De esta forma se establece un ecosistema de seguridad e interoperabilidad al permitir verificar el estado y validez de los distintos certificados electrónicos empleados por el ciudadano en cualquier procedimiento telemático, entre ellos, los del DNI-e, y se da cumplimiento al artículo 21.3 de la Ley 11/2007 que establece que la Administración General del Estado dispondrá, al menos, de una plataforma de verificación del estado de revocación de todos los certificados admitidos en el ámbito de las Administraciones Públicas que será de libre acceso por parte de todos los Departamentos y Administraciones.

También el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos establece en el artículo 25.1 que “El Ministerio de la Presidencia (ahora Ministerio de Hacienda y Administraciones Públicas) gestionará una plataforma de verificación del estado de revocación de los certificados admitidos en el ámbito de la Administración General del Estado y de los organismos públicos dependientes o vinculados a ella”

El artículo 47 de dicho Real Decreto, establece la necesidad de incorporar una referencia temporal de los documentos administrativos electrónicos, siendo una de las modalidades de referencia temporal, el «Sello de tiempo», entendiendo por tal la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento. El sello de tiempo es una parte indispensable de la firma electrónica, sobre todo en el caso de las firmas longevas, que necesiten ser validadas mucho tiempo después de su generación.

La Dirección de Tecnologías de la Información y las Comunicaciones, en el ejercicio de sus competencias de desarrollo, impulso, planificación y ejecución de proyectos dirigidos a facilitar el acceso de los ciudadanos a la

Administración Electrónica, proporciona la Plataforma @firma, como plataforma de validación de certificados y firma electrónica, que facilita el cumplimiento del derecho de los ciudadanos a la utilización de medios de identificación y firma electrónica que establecen los apartados g y h del artículo 6 de la Ley 11/2007 de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, siendo la plataforma de validación que dispone la AGE como marca el artículo 21.3 de la misma ley. Dicha plataforma se complemente con la TS@, para la generación y verificación de los sellados de tiempo.

Otro de los servicios prestados es STORK: una plataforma de reconocimiento transfronterizo de identidades electrónicas nacionales, que paulatinamente irá permitiendo a los ciudadanos acceder e identificarse en servicios de gobierno electrónico de otro país usando sus identidades electrónicas nacionales.

A efectos del presente apartado se utilizará la referencia a @firma para referirse al conjunto de servicios prestados por la plataforma.

II.1.2. Servicios incluidos

Los servicios ofrecidos por @firma son:

- Validación de firmas y certificados electrónicos a través de la Plataforma @firma.
- Firma electrónica de ficheros y formularios en entorno cliente, tanto en equipos de sobremesa como plataformas móviles, a través del Cliente @firma.
- Sellado de tiempo mediante la Autoridad de Sellado TS@.
- Bróker de proveedores de servicios de identidad (cl@ve).
- Validación de identidades de ciudadanos de otros países de la Unión Europea mediante Stork.

@firma habilita a cualquier aplicación informática de los órganos o entidades dependientes de la Comunidad Autónoma a validar certificados digitales y firmas electrónicas en procesos de autenticación y firma, entre los certificados digitales admitidos por la Plataforma.

Asimismo, la plataforma dispone de entornos de prueba para facilitar la integración de aplicaciones y poder garantizar la correcta operación con carácter previo a la puesta a disposición de los usuarios finales.

II.1.3. ESPECIFICACIONES TÉCNICAS

II.1.3.1 Características de @firma

Para facilitar al máximo la integración con las arquitecturas, aplicaciones y soluciones ya existentes, @firma es “no intrusiva”, es decir, no modifica ni impacta en los esfuerzos ya realizados en sistemas y aplicaciones existentes.

Sus principales características son:

- Se basa en Servicios Web que son utilizados por las distintas AAPP.
- Es una plataforma de validación MultiAC (múltiples Autoridades de certificación), MultiPolítica, MultiCertificados, MultiFirma, MultiFormatos..., de tal manera que permite la utilización de múltiples tipos de Certificados y Autoridades de Validación a los ciudadanos, en su relación telemática con las distintas Administraciones Públicas.
- Proporciona seguridad a las firmas electrónicas, a través de las funciones de Sellado de Tiempo y actualización de firmas a formatos longevos.
- Permite la validación de firmas electrónicas realizadas con certificados electrónicos reconocidos expedidos por Prestadores de Servicios de Certificación europeos en cumplimiento de la legislación europea vigente en materia de firma electrónica.
- Facilita la integración de la firma electrónica en los portales de Administración electrónica, a través del Cliente @firma, un componente MultiSistema Operativo y MultiNavegador.
- Proporciona las máximas garantías de seguridad y robustez, garantizando en su funcionamiento:
  - un rendimiento óptimo,
  - alta disponibilidad,
  - interoperabilidad, y
  - portabilidad.

II.1.3.2 Modo de acceso a la plataforma @firma

El acceso a los servicios de la Plataforma se realiza exclusivamente a través de la Red SARA, descrita en su correspondiente apartado.

Las solicitudes de acceso se realizarán a través del centro de soporte, atendiendo al procedimiento establecido al efecto.

II.1.3.3. Auditabilidad

@firma registra todas las peticiones realizadas, identificando siempre al empleado público y/o aplicación (mediante certificado electrónico), el momento de dicha petición y el proceso que se han realizado. Estas peticiones podrán ser auditadas a través de los elementos de auditoría de los que dispone el MINHAP, por ejemplo para certificar que no se produce “no repudio” de transacciones.

@firma no almacena los documentos incluidos en las peticiones de validación o solicitud de firma, y actúa únicamente como responsable del tratamiento de los datos de carácter personal incluidos en los certificados, pero no como responsable de dichos datos. La aplicación usuaria deberá ser responsable de declarar los datos de carácter personal que traten sus aplicaciones ante la AEPD o equivalente.

II.1.3.4 Servicios de soporte a usuarios

En el estado actual de definición, los servicios de soporte a usuarios cuentan con las siguientes características:

- Alcance
  El servicio de soporte y atención a usuarios abarca a los siguientes interlocutores:
  - Para el primer nivel: los propios organismos usuarios de la Plataforma.
  - Para el segundo nivel: CAU para atender a agentes externos al servicio como organismos, otros CAUs de los organismos o de los Prestadores de Servicio de Certificación (PSCs).
  - Para el tercer nivel: CAU que atiende las peticiones de actuación en sistemas y desarrollos del CAU de 2º nivel.
  - Niveles adicionales:
    - Prestadores de Servicio de Certificación (PSCs)
    - Gestores del proyecto del MINHAP.
    - Otros proveedores de servicios e infraestructura base para solicitar su asistencia ante incidencias o actuaciones preventivas en los sistemas.

- Funciones
  Las funciones del servicio de soporte y atención al usuario son
  - Recepción de solicitudes a través de los canales de entrada que se establezcan (formularios a través de una web).
  - Registro y clasificación de incidencias y peticiones en función de su tipología y asignación de prioridades (a partir del cruce entre la urgencia y el impacto en el servicio).

- Evaluación, investigación y diagnóstico de las incidencias y peticiones
- Escalado funcional a los diferentes niveles de soporte
- Escalado jerárquico, de manera que los diferentes niveles de responsabilidad de las organizaciones implicadas posean visibilidad de los casos más relevantes y puedan tomar las acciones necesarias para minimizar el impacto de dichas incidencias
- Seguimiento de incidencias y peticiones a lo largo de todo su ciclo de vida, hasta su cierre y verificación, manteniendo a los usuarios informados respecto del estado y el grado de progreso de sus incidencias/peticiones

II.1.3.5 Aseguramiento de la calidad de servicio

La calidad del servicio se medirá mediante la continua revisión de los valores de aquellos parámetros que midan los niveles de servicio.

Se contemplarán tanto los parámetros propios del servicio (disponibilidad de los servicios de validación y firma o de sellado de tiempo contemplados en @firma, estado de las comunicaciones, monitorización de sistemas), como los de soporte a los usuarios para la gestión y resolución de consultas e incidencias.

El Acuerdo de Nivel de Servicio se publicará en el Centro de Transferencia de Tecnología (solución @firma).

II.2. PLATAFORMA Cl@ve

II.2.1 Descripción del sistema 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 electrónica 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.

La 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, regula el funcionamiento de este sistema.

Aunque el alcance inicial del sistema es el Sector Público Administrativo Estatal, podrán adherirse al mismo mediante convenio otras Administraciones Públicas en las condiciones técnicas, económicas y organizativas que se determinen.

II.2.1.1. Funcionamiento de la plataforma (identificación y autenticación)

En lo que respecta a la identificación y autenticación, Cl@ve adopta la filosofía de un sistema de federación de identidades electrónicas, integrando a diferentes actores:

- Proveedores de servicios de administración electrónica (SP): Entidades que proporcionan servicios de administración electrónica y utilizan la plataforma para la identificación y autenticación de ciudadanos.

- Proveedores de servicios de identificación y autenticación (IdP): Entidades que proporcionan mecanismos de identificación y autenticación de los ciudadanos para ser utilizados como medios comunes por otras entidades.

- Pasarela / Gestor de Identificación: Sistema intermediador que posibilita el acceso de los proveedores de servicios a los distintos mecanismos de identificación.

De acuerdo con esta aproximación, los SP únicamente tienen que integrarse con el Gestor de Identificación, encargándose este de establecer las relaciones pertinentes con los distintos sistemas de identificación. Para ello se establecen círculos de confianza entre los distintos actores que se integran entre sí, soportadas por el intercambio de certificados electrónicos y el envío de mensajes firmados entre ellos.

Para implementar esta federación de identidades, la solución desarrollada para Cl@ve se basa esencialmente en los resultados obtenidos por los proyectos STORK y STORK 2.0, adaptándolos convenientemente a las necesidades del proyecto. Esto supone que la interoperabilidad en Cl@ve se consigue con la utilización del estándar SAML 2.0, un framework basado en XML para reunir y organizar información de seguridad e identidad e intercambiarla entre

diferentes dominios, y que la integración entre sistemas se realiza no de manera directa, sino siempre a través redirecciones desde el navegador el usuario.

En relación a los mecanismos de identificación, Cl@ve contempla inicialmente la utilización de dos tipos de claves concertadas:

- Cl@ve PIN: sistema de contraseña de validez muy limitada en el tiempo, orientado a usuarios que acceden esporádicamente a los servicios, provisto por la Agencia Estatal de Administración Tributaria (AEAT).

- Cl@ve permanente: sistema de contraseña de validez duradera en el tiempo pero no ilimitada, orientado a usuarios habituales, provisto por la Gerencia de Informática de la Seguridad Social (GISS).

Ambos mecanismos de identificación contemplan la posibilidad de que el usuario reciba en su teléfono móvil, mediante un mensaje corto de texto (SMS), un código que deberá utilizar durante el proceso de autenticación. La provisión del servicio de envío de dicho SMS no es objeto del presente Convenio, y deberá ser gestionada directamente por las entidades que se integran con la plataforma, en este caso la Administración de la Comunidad Autónoma del Principado de Asturias, y, eventualmente, las Entidades de derecho público dependientes y las Entidades Locales adheridas al presente Convenio.

Además de los dos mecanismos de identificación anteriores, Cl@ve se integra con otros dos sistemas de identificación adicionales:

- @firma, para la gestión de la identificación mediante certificados electrónicos y DNI electrónico.

- STORK, la plataforma europea de interoperabilidad que permite el reconocimiento transfronterizo de identidades electrónicas, desarrollada durante la ejecución de los proyectos STORK y STORK 2.0, y que servirá de referencia para la construcción del futuro sistema de reconocimiento de identidades electrónicas previsto en Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (reglamento eIDAS).

II.2.1.2 Funcionamiento de la plataforma (firma mediante certificados centralizados)

El sistema Cl@ve permitirá también el acceso a servicios de firma electrónica, en particular, a servicios de firma de documentos electrónicos mediante certificados electrónicos personales centralizados, si el usuario no usase otros

certificados admitidos, todo ello a efectos de su presentación ante las Administraciones Públicas en aquellos trámites en que sea requerido o admitido el uso de certificados electrónicos. Se tendrán en cuenta las siguientes consideraciones:

- Para poder acceder al servicio, el usuario deberá solicitar previa y expresamente la emisión de sus certificados electrónicos personales centralizados. La emisión al ciudadano de su certificado electrónico centralizado para firma se llevará a cabo la primera vez que el ciudadano acceda al procedimiento de firma con la plataforma Cl@ve. El sistema informará al ciudadano de que se le va a emitir su certificado centralizado y generará en ese momento su clave privada y la almacenará en el sistema de forma protegida, de modo que se garantice su uso bajo el control exclusivo de su titular.
- Los certificados electrónicos personales serán emitidos con las mismas garantías de identificación del DNI electrónico del ciudadano.
- En cualquier proceso de firma electrónica con el certificado centralizado, deberá garantizarse que el acceso a dicha clave sólo podrá ser efectuado por el titular de la misma, por lo que para su uso se deberá haber autenticado previamente al ciudadano mediante un mínimo de 2 factores de autenticación, como por ejemplo los mecanismos de identificación Cl@ve PIN y Cl@ve permanente.

II.2.2. Uso del sistema Cl@ve

Las condiciones técnicas, económicas y organizativas para la incorporación al sistema Cl@ve de la Administración de la Comunidad Autónoma del Principado de Asturias, y, en su caso, las Entidades de derecho público dependientes y las Entidades Locales adheridas al presente Convenio, están determinadas por la *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.* Eventualmente, la Comunidad Autónoma del Principado de Asturias, y, en su caso, las Entidades de derecho público dependientes y las Entidades Locales adheridas al presente Convenio, podrán constituir Oficinas de Registro Presencial del sistema Cl@ve, para lo cual deberán estar a lo dispuesto en la *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*.

Las solicitudes de acceso se realizarán a través del centro de soporte, atendiendo al procedimiento establecido al efecto.

II.2.2.1. Auditabilidad

El sistema Cl@ve registrará todas las peticiones realizadas, identificando siempre a la entidad que realiza la petición y el momento de dicha petición, así

como la operación efectuada y la respuesta proporcionada por el sistema. Estas peticiones podrán ser auditadas a través de los elementos de auditoría de los que disponen las entidades que intervienen en la operación del sistema, de acuerdo con las responsabilidades asignadas a cada una establecidas en la *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.*

El sistema Cl@ve no almacena los datos de carácter personal incluidos en las respuestas a las peticiones de identificación y autenticación, y actúa únicamente como responsable del tratamiento de los datos de carácter personal incluidos en los certificados, pero no como responsable de dichos datos. La aplicación usuaria deberá ser responsable de declarar los datos de carácter personal que traten sus aplicaciones ante la AEPD o equivalente.

II.2.2.2. Servicios de soporte a las entidades usuarias

El servicio de soporte y atención a entidades usuarias del sistema Cl@ve será prestado en sus diferentes niveles por los siguientes actores:

- Centro de Atención a Integradores y Desarrolladores (CAID) del Ministerio de Hacienda y Administraciones Públicas (MINHAP), como punto de contacto con las entidades usuarias.
- Servicios de soporte de los Proveedores de Servicios de Identificación (AEAT o GISS), en el caso de que sea necesaria su participación.

Las funciones de este servicio de soporte y atención a las entidades usuarias son:

- Recepción de solicitudes a través de los canales de entrada que se establezcan (formularios a través de una web).
- Registro y clasificación de incidencias y peticiones en función de su tipología y asignación de prioridades (a partir del cruce entre la urgencia y el impacto en el servicio).
- Evaluación, investigación y diagnóstico de las incidencias y peticiones
- Escalado funcional a los diferentes niveles de soporte.
- Seguimiento de incidencias y peticiones a lo largo de todo su ciclo de vida, hasta su cierre y verificación, manteniendo a los usuarios informados respecto del estado y el grado de progreso de sus incidencias/peticiones.

II.2.2.3. Aseguramiento de la calidad de servicio

La calidad del servicio se medirá mediante la continua revisión de los valores de aquellos parámetros que midan los niveles de servicio.

Se contemplarán tanto los parámetros propios del servicio como los de soporte a los usuarios para la gestión y resolución de consultas e incidencias.

El Acuerdo de Nivel de Servicio es el de aplicación a la solución @firma, publicado en el Centro de Transferencia de Tecnología.

II.3. REGISTRO ELECTRONICO DE APODERAMIENTOS

II.3.1 DESCRIPCION GENERAL

El registro electrónico de representación y apoderamientos (REA), permite hacer constar y gestionar las representaciones que los interesados otorguen a terceros, con el fin de actuar en su nombre de forma electrónica ante las Administraciones Públicas y/o sus organismos públicos vinculados o dependientes.

Los Actores que intervienen en un apoderamiento son:

- El ciudadano que actúa como poderdante puede apoderar a cualquier otro ciudadano o empresa para que actúe en su nombre.
- El ciudadano que actúa como apoderado puede representar a cualquier otro ciudadano o empresa.

El apoderamiento se inscribe en el Registro para un determinado trámite o conjunto de ellos. La descripción, la gestión de los trámites y las categorías es competencia de cada organismo que se adhiere al REA.

El registro REA permite, previa identificación con certificado digital o DNI electrónico realizar ciertas operaciones necesarias para inscribir o gestionar el apoderamiento:

Como poderdante:

- Crear un apoderamiento sobre un trámite o una categoría de trámites.
- Consultar sus apoderamientos
- Revocar sus apoderamientos
- Modificar la vigencia de sus apoderamientos

Como apoderado:

- Consultar sus apoderamientos
- Renunciar a apoderamientos
- Confirmar apoderamientos, para trámites o categorías que así lo requieran

Un organismo puede realizar la gestión y consulta de los apoderamientos de su competencia en REA, bien a través del subsistema Intranet del REA, o bien integrando sus propias aplicaciones con el Registro a partir de los servicios Web puestos a disposición por el sistema. El sistema permite a los organismos la descarga de sus trámites y categorías en diversos formatos normalizados.

II.3.2. ESPECIFICACIONES TECNICAS

II.3.2.1. MODOS DE ACCESO AL REA

II.3.2.1.1 Acceso a través de una aplicación Web

La dirección es:

https://rea.redsara.es/funcionarioHabilitado/

El acceso a la aplicación se realiza exclusivamente a través de la Red SARA.

Las solicitudes de acceso se harán a través del centro de soporte, atendiendo al procedimiento establecido al efecto.

El manual de usuario de la aplicación puede consultarse en:

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

II.3.2.1.2. Acceso a través de una interfaz de servicios Web

El acceso a los servicios Web del REA se realiza exclusivamente a través de la Red SARA.

Las reglas de validación que se aplican son las que define el lenguaje WSDL y los documentos esquema XSD.

Los Servicios Web disponibles son los siguientes:

1. Consulta de Apoderamientos WS
2. Dar de Alta Apoderamientos WS
3. Revocar Apoderamientos WS
4. Modificar Apoderamientos WS
5. Renunciar Apoderamientos WS
6. Confirmar Apoderamientos WS
7. Descarga de Apoderamientos WS
8. Descarga de Categorías y Trámites WS

La descripción detallada de los servicios Web puede consultarse en:

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

II.3.3. Servicios de soporte a las entidades usuarias

El servicio de soporte a usuarios tiene las siguientes características:

- Alcance

  El servicio de soporte y atención a usuarios abarca a los siguientes interlocutores:

  - Para el primer nivel: los propios organismos usuarios del REA.
  - Para el segundo nivel: CAU para atender a agentes externos al servicio como organismos, otros CAUs de los organismos.
  - Para el tercer nivel: CAU que atiende las peticiones de actuación en sistemas y desarrollos del CAU de 2º nivel.
  - Niveles adicionales:
    - Gestores del proyecto del MINHAP.
    - Los proveedores de servicios e infraestructura base para solicitar su asistencia ante incidencias o actuaciones preventivas en los sistemas.

- Funciones

  Las funciones del servicio de soporte y atención al usuario son:

  - Recepción de solicitudes a través de los canales de entrada que se establezcan (formularios a través de una página web).
  - Registro y clasificación de incidencias y peticiones en función de su tipología y asignación de prioridades (a partir del cruce entre la urgencia y el impacto en el servicio).
  - Evaluación, investigación y diagnóstico de las incidencias y peticiones
  - Escalado funcional a los diferentes niveles de soporte
  - Escalado jerárquico, de manera que los diferentes niveles de responsabilidad de las organizaciones implicadas posean visibilidad de los casos más relevantes y puedan tomar las acciones necesarias para minimizar el impacto de dichas incidencias

- Seguimiento de incidencias y peticiones a lo largo de todo su ciclo de vida, hasta su cierre y verificación, manteniendo a los usuarios informados respecto del estado y el grado de progreso de sus incidencias/peticiones.

II.3.4. Aseguramiento de la calidad de servicio

La calidad del servicio se medirá mediante la continua revisión de los valores de aquellos parámetros que midan los niveles de servicio.

Se contemplarán tanto los parámetros propios del servicio como los de soporte a los usuarios para la gestión y resolución de consultas e incidencias.

El Acuerdo de Nivel de Servicio es el de aplicación a la solución @firma, publicado en el Centro de Transferencia de Tecnología.

APARTADO III): COMUNICACIONES ENTRE ADMINISTRACIONES PÚBLICAS POR MEDIOS ELECTRÓNICOS:

Subapartado III.a): Intermediación de datos entre Administraciones Públicas.

III.a.1. DESCRIPCIÓN GENERAL

III.a.1.1 Descripción

La plataforma de intermediación de datos permite a las Administraciones Públicas interesadas la consulta por medios electrónicos de datos de ciudadanos de los que ya disponen otras Administraciones Públicas por su competencia.

De esta forma, el ciudadano no tiene que aportar los documentos acreditativos de los mismos. Asimismo, la Administración Pública puede realizar comprobaciones de dichos datos. Para ello debe existir el adecuado soporte legal o que el ciudadano haya dado su consentimiento.

III.a.1.2. Servicios incluidos

Los servicios ofrecidos por la plataforma de intermediación de datos entre administraciones son:

- Conexión a la plataforma de intercambio de datos
- Servicio de comunicación de cambio de domicilio a organismos de la Administración General del Estado
- Carta de servicios

La carta de servicios recogerá en este servicio los efectos que se derivan del intercambio de datos entre Administraciones Públicas para la prestación de un servicio determinado, así como los requisitos para su tramitación, el plazo para su efectividad y cualquier otra información que deba conocer el interesado, y será actualizada con los nuevos servicios intermediados que se incorporen.

III.a.2. ESPECIFICACIONES TÉCNICAS

III.a.2.1 Características de la plataforma de intermediación de datos entre administraciones

La plataforma de intermediación de datos es un servicio horizontal que permite integrar múltiples Administraciones Públicas, tanto para proveer datos a otras Administraciones Públicas como para consultar datos de otras, de forma segura.

III.a.2.2 Modo de acceso a la plataforma de intermediación de datos

El acceso a los servicios de la plataforma se realiza exclusivamente a través de la Red SARA, descrita en su correspondiente apartado.

III.a.2.3. Especificaciones de seguridad

Debido a la criticidad de la información intercambiada, para asegurar plenas garantías de seguridad, confidencialidad y protección de datos se cumplirán las siguientes especificaciones:

- Autenticación: identificación de los usuarios que acceden al servicio mediante certificado electrónico reconocido en vigor que cumpla la recomendación UIT X.509 versión 3 o superiores, o mediante otros sistemas de identificación recogidos en la Ley 11/2007 para la identificación de las Administraciones Públicas.
- Gestión de autorizaciones: Sólo se dará acceso a los empleados públicos y las aplicaciones, y sólo para realizar aquellas consultas para las que han sido habilitados.
- Firma electrónica: Todas las peticiones irán firmadas (XMLDSig) con certificado electrónico (X509 v3).
- Trazabilidad: El sistema registrará todas las consultas realizadas, identificando siempre al empleado público y/o aplicación (mediante certificado electrónico), el momento de dicha consulta (sellado en tiempo) y la finalidad con la que se han realizado. El sistema garantiza la integridad de los datos registrados mediante el uso de firma electrónica.
- Confidencialidad: El sistema garantizará la confidencialidad de los datos intercambiados. Todas las comunicaciones que se realicen entre distintos organismos van sobre protocolo https (SSL) y además la red SARA proporciona, en el tramo troncal, medidas adicionales de cifrado de datos.
- Integridad: Todas las consultas que se realicen, así como las respuestas que se devuelvan serán firmadas electrónicamente para garantizar tanto la integridad de los datos intercambiados como la identidad de las partes que intervienen y el no repudio de la consulta.
- Sellado de tiempo: Para certificar la fecha y el tiempo de las actividades y sucesos registrados en la plataforma de intermediación de datos se hará uso de una marca de tiempo o, en su caso, del Servicio de Sellado de Tiempo de la Plataforma de Firma Electrónica del MINHAP, sincronizada con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara el Laboratorio de la Armada como laboratorio depositario del padrón nacional de Tiempo y laboratorio asociado al centro Español de Metrología, y según las condiciones técnicas y protocolos que el citado Organismo establezca.
- Auditabilidad: Cada petición y su correspondiente respuesta se registra en el sistema con la consiguiente firma electrónica y sellado de tiempo.

Todas las peticiones van identificadas con un identificador único, que permite su posterior recuperación ante posibles reclamaciones o auditorías del servicio.

- Auditoría: La plataforma de intermediación de datos dispondrá de un módulo de auditoría, en el que quedarán registrados todas las consultas de datos realizadas, información de contexto asociada, la identidad del solicitante, la fecha y la finalidad de la consulta, y aquellos eventos relevantes desencadenados a partir de la propia consulta. Se garantizará la integridad y no repudio de la información registrada mediante técnicas de firma electrónica y sellado de tiempo, estableciéndose, asimismo, medidas técnicas para garantizar la disponibilidad y recuperación de aquella información que no se mantenga on-line por motivos de eficiencia técnica o seguridad. Sólo personal de la Administración Pública debidamente autorizado y acreditado podrá acceder a las funcionalidades de auditoría de la plataforma.
- Calidad de la información: La calidad de los datos será responsabilidad del organismo que los custodia.
- Administración delegada: para facilitar la gestión de usuarios (altas/bajas/modificaciones) el sistema permite que cada organismo pueda tener un administrador encargado de esta gestión. Para ello, se da la posibilidad de limitar la administración del sistema por organismos.

- Política de seguridad común: las medidas de seguridad necesarias para proteger debidamente la información y los servicios de intermediación ofrecidos se definirán sobre:
    a. Cumplimiento de los criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades aprobados por el Consejo Superior de Administración Electrónica mediante Resolución de 26 de mayo de 2003 y revisiones posteriores, y aquellas que sean de aplicación del 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.
    b. Realización de análisis y gestión de riesgos, preferiblemente con la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) del Consejo Superior de Administración Electrónica.
    c. Cumplimiento de la normativa de Protección de Datos de Carácter Personal, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

III.a.2.4. Especificaciones de disponibilidad

Se promoverá que la plataforma de intermediación de datos esté disponible los 7 días de la semana las 24 horas del día. Los organismos cedentes deberán contar con la misma disponibilidad en sus sistemas o plataformas.

III.a.2.5 Incorporación de nuevos servicios

Las administraciones adheridas a este Convenio podrán incorporar nuevos conjuntos de datos intermediados, promoviendo la correspondiente actualización de la Carta de Servicios e informando de los nuevos servicios intermediados al MINHAP para actualizar la Carta de Servicios.

III.a.2.6 Incorporación de nuevos intermediadores de datos

Las Administraciones Públicas usuarias de este servicio podrán desarrollar sus propios intermediadores de datos, en cuyo caso se conectarán a la plataforma de intermediación de datos como un usuario más, atendiendo los mismos requisitos y obligaciones que la plataforma en cuanto a seguridad y niveles de servicio.

III.a.2.7 Niveles de servicio de partida

Inicialmente los niveles de servicio serán los siguientes:

Servicios de soporte

Los que correspondan a @firma

La Comisión de Seguimiento podrá determinar nuevos valores cuando corresponda por motivos técnicos o legales.

Subapartado III.b): Remisión de información a través del Portal de Comunidades Autónomas.

III.b.1. DESCRIPCIÓN GENERAL

III.b.1.1 Descripción del servicio

El portal de Comunidades Autónomas de la Secretaría de Estado de Administraciones Públicas (SEAP) provee servicios a las Administraciones Públicas que le permiten disponer, de forma centralizada, de un conjunto de aplicaciones y utilidades usuarios con perfiles, de manera que se gestione la identidad de estos empleados públicos en su relación con la SEAP.

Por otro lado, la documentación que las Entidades Locales ponen a disposición de la SEAP se almacena en el servicio de gestión de documentación de las Entidades Locales.

Cuando el marco legal lo permita, la documentación que las Entidades Locales han puesto a disposición podrá ser puesta a disposición de la Comunidad Autónoma en un servicio de gestión de documentación propio de la Comunidad, evitándole así nuevas obligaciones a las Entidades Locales y promoviendo con ello el reaprovechamiento de la información.

III.b.1.2 Servicios incluidos

La Comunidad Autónoma accederá a la documentación que las Entidades Locales han puesto a disposición de la SEAP a través de su propio servicio de gestión de documentación.

Además, la Comunidad Autónoma podrá realizar un conjunto de tramitaciones básicas, como son:

- Recepción de la documentación.
- Obtención del justificante de registro emitido por el Registro Electrónico Común.
- Posibilidad de efectuar requerimientos a las entidades locales.
- Adjuntar documentación privada a los expedientes recibidos.
- Archivado del expediente.

Adicionalmente, conforme a los servicios básicos de infraestructura de la propia Red Sara, se realiza:

- Un servicio de backup de la información remitida por las entidades locales, así como de los datos introducidos por las Comunidades Autónomas.
- Posibilidad de realizar auditoría de accesos de las acciones que se hayan efectuado durante un año completo, pudiendo recuperar la información necesaria en este plazo de tiempo.

III.b.2. ESPECIFICACIONES TÉCNICAS

III.b.2.1 Acceso al servicio

El acceso al servicio de gestión de documentación se realiza a través del Portal de Comunidades Autónomas, el cual está sincronizado con el Directorio Común de Unidades Orgánicas y Oficinas (DIR 3). A cada una de las unidades de este Directorio pueden asignarse empleados públicos de las mismas, con el perfil necesario para acceder a la aplicación de gestión mediante un sistema de autoprovisión que permite establecer cargos y/o perfiles para cada empleado.

III.b.2.2 Aseguramiento de la calidad del servicio

Con el fin de asegurar la buena calidad del servicio, el portal de Comunidades Autónomas cuenta con un punto de notificación de incidencias, resolución de las mismas, consultas técnicas relacionadas con el servicio, así como peticiones de nuevos accesos. Dicho punto está disponible en 24x7 mediante un sistema web, y con un horario de resolución de incidencias de 9 a 18:30.

El MINHAP, a través del Portal de Entidades Locales, ha habilitado un espacio en el que se publica información sobre el servicio proporcionado: manuales, notificación de incidencias, paradas de servicio programadas, publicación de nuevos servicios u otros elementos necesarios para el correcto funcionamiento del sistema. Dicha información estará accesible a través de dicho portal.

La detección, diagnóstico y resolución de las incidencias por la DTIC (MINHAP) puede requerir la colaboración de la Comunidad Autónoma, pudiendo abarcar esta colaboración la realización de pequeñas comprobaciones o actuaciones a nivel de usuario final, dirigidas desde el Centro de Soporte de la aplicación, con el fin de reducir los tiempos de resolución de las incidencias.

III.b.2.3 Requisitos de utilización del servicio

Para la correcta utilización del portal y del servicio de gestión de documentación de las entidades locales es imprescindible que el empleado público de la Comunidad Autónoma cuente con un certificado digital activo en alguno de los estándares soportados por la plataforma de @firma del MINHAP.

Este certificado digital se usará: para la autenticación del empleado público; para la emisión de requerimientos a la entidad local; para la firma de la documentación; y, en caso necesario, para la firma de las peticiones de apunte registrales en el REC que sean necesarias para el cumplimiento del procedimiento de requerimiento.

III.b.2.4 Niveles de servicio de partida

Inicialmente los niveles de servicio serán los siguientes:

Servicios de soporte

Los que correspondan a @firma

La Comisión de Seguimiento podrá determinar nuevos valores cuando corresponda por motivos técnicos o legales.

APARTADO IV): PRÁCTICA DE LA NOTIFICACIÓN POR MEDIOS ELECTRÓNICOS: DIRECCIÓN ELECTRÓNICA HABILITADA Y CATÁLOGO DE PROCEDIMIENTOS DEL SERVICIO DE NOTIFICACIONES ELECTRÓNICAS.

IV.1. DESCRIPCIÓN GENERAL

IV.1.1 Descripción

El artículo 38.2 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado establece que “bajo responsabilidad del Ministerio de la Presidencia existirá un sistema de dirección electrónica habilitada para la práctica de estas notificaciones que quedará a disposición de todos los órganos y organismos públicos vinculados o dependientes de la Administración General del Estado que no establezcan sistemas de notificación propios. Los ciudadanos podrán solicitar la apertura de esta dirección electrónica, que tendrá vigencia indefinida, excepto en los supuestos en que se solicite su revocación por el titular, por fallecimiento de la persona física o extinción de la personalidad jurídica, que una resolución administrativa o judicial así lo ordene o por el transcurso de tres años sin que se utilice para la práctica de notificaciones, supuesto en el cual se inhabilitará ésta dirección electrónica, comunicándose así al interesado”.

La Orden PRE/878/2010, de 5 de abril, por la que se establece el régimen del sistema de dirección electrónica habilitada previsto en el artículo 38.2 del Real Decreto 1671/2009, de 6 de noviembre, fija las condiciones que ha de reunir la entidad habilitada para la prestación del servicio de dirección electrónica, así como las condiciones para su prestación, establece en su artículo 2.1 que “la titularidad de la dirección electrónica a partir de la que se construyan las direcciones electrónicas habilitadas de los interesados corresponde al Ministerio de la Presidencia”.

En aplicación de lo dispuesto en la normativa anteriormente citada, el Ministerio de Hacienda y Administraciones Públicas (MINHAP) ha desarrollado un servicio de notificaciones electrónicas y de dirección electrónica habilitada para la Administración General del Estado, que es prestado en colaboración con la Sociedad Estatal Correos y Telégrafos, S.A. (CORREOS), gracias al Convenio de colaboración que ambas partes tienen suscrito con esta finalidad.

El MINHAP, con el objetivo de impulsar la implantación de la administración electrónica, quiere facilitar a las administraciones y entidades públicas la utilización de los sistemas que ha desarrollado para prestar este servicio en el ámbito de la AGE. El objeto del presente anexo es la regulación de los

derechos y obligaciones que se establecen para la prestación, por parte del MINHAP, del Servicio de Dirección Electrónica Habilitada y Catálogo de procedimientos del Servicio de Notificaciones Electrónicas.

La plataforma de Dirección Electrónica Habilitada (DEH) permite la práctica de la notificación por medios electrónicos al facilitar a los interesados el acceso al contenido del acto objeto de notificación, acreditando fecha y hora de la puesta a disposición y la del acceso al contenido, de forma segura y fehaciente.

Las funcionalidades del Servicio de Notificaciones Electrónicas (SNE) son:

- Gestionar las Direcciones Electrónicas que se otorgan al ciudadano para identificar su buzón.
- Gestionar los procedimientos para los cuales se puede recibir notificaciones de forma telemática.
- Gestionar la entrega de notificaciones administrativas desde el emisor al ciudadano de forma telemática.
- Gestionar la información de retorno (entrega de las notificaciones o rechazo o vencimiento de plazo)
- Identificar al ciudadano mediante certificado digital o eDNI, así como comprobar la validez del certificado.
- Recabar la firma del ciudadano para los documentos de “solicitud de nueva dirección electrónica”, “suscripción a procedimientos” “rechazo o entrega de notificación”.
- Realizar un sellado de tiempo de las acciones realizadas por el ciudadano.
- Almacenar los documentos necesarios para asegurar la validez jurídica de la notificación.

IV.1.2 Servicios incluidos

Los servicios ofrecidos por el Sistema de Dirección Electrónica Habilitada y el Catálogo de Procedimientos del Servicio de Notificaciones Electrónicas (SNE) son los siguientes:

a. Gestión de la Dirección Electrónica Habilitada (DEH).
b. Gestión del Catálogo de Procedimientos SNE.
c. Publicación de procedimientos.
d. Gestión de la suscripción a procedimientos.

Cualquier medida de informatización que pueda afectar a la compatibilidad de la DEH y a la publicación de los procedimientos a los que el ciudadano puede suscribirse se comunicará mutuamente.

IV.1.3 Coste asociado a la gestión de la entrega de la notificación

Los servicios prestados por el Servicio de Dirección Electrónica Habilitada y Catálogo de procedimientos del Servicio de Notificaciones Electrónicas del MINHAP se realizarán sin coste alguno. Los costes asociados a la gestión de la entrega de la notificación (buzón, puesta a disposición, entrega, acuses de recibo, etc.), se inscribirán dentro de las relaciones entre Correos y el usuario del servicio.

IV.2. DESCRIPCIÓN TÉCNICA DEL SISTEMA

IV.2.1 Prestador del servicio

El servicio de notificaciones electrónicas y de dirección electrónica habilitada es prestado por la Sociedad Estatal Correos y Telégrafos, S.A. (CORREOS), gracias al Convenio de colaboración que ambas partes tienen suscrito con esta finalidad.

IV.2.2 Determinación de niveles de servicio

La determinación de niveles de servicio aplicable es la que se fije en el Convenio MINHAP-Correos en vigor.