tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

163

@FIRMA: INICIATIVA PARA EXTENDER EL USO DE DNI-*e* Y LA FIRMA-e EN LA ADMINISTRACIÓN

Ricardo Cantabrana González
Alfonso Berral López
Ministerio de Administraciones públicas

Ricardo Cantabrana González
Alfonso Berral López

Palabras clave

@firma:
Producto de firma y certificación electrónica propiedad de las Administraciones públicas y que constituye la base tecnológica de los servicios de firma-e de la Iniciativa desarrollada.

DNI-e:
Documento Nacional de Identidad electrónico. Se prevé su lanzamiento de forma experimental para el primer semestre de 2006.

Plataforma de firma-e
Plataforma física de servicios de certificación y firma basada en el producto @firma ofrecida por el MAP a los organismos que se adhieran al convenio de uso de los servicios.

PSC o "Prestador de Servicios de Certificación"
Proveedor de servicios de certificación conforme es recogido en la Ley 59/2003, de 19 de diciembre, de firma electrónica. Son entidades publicas o privadas que expiden certificados digitales y ofrecen servicios asociados.

BRIDGE-CA europea
Proyecto desarrollado en el marco de la Unión Europea a través del programa IDABC, consistente en la creación de un punto neutral de confianza donde se distribuyen estructuras de prestadores y certificados electrónicos a importar entre los países miembros.

S.A.R.A. –Sistema de Aplicaciones y Redes para las Administraciones-, una nueva infraestructura tecnológica que permite y garantiza la comunicación entre las distintas administraciones además de servir de plataforma de intercambio de aplicaciones.

Resumen de su Comunicación

La introducción de la firma-e en las organizaciones es ya una necesidad, fundamentalmente a raíz de la puesta en circulación del DNI-e.

La iniciativa @firma se constituye como el complemento necesario para incorporar en los sistemas los medios necesarios para implementar la autenticación y firma electrónica avanzada basada en certificados digitales. Se reconoce, además, el acceso a una solución tecnológica @firma propiedad de las Administraciones públicas, y se establece una estrategia de colaboración y evolución óptima de los servicios con el máximo respaldo de sus usuarios.

Ricardo Cantabrana González
Alfonso Berral López

@FIRMA: INICIATIVA PARA EXTENDER EL USO DE DNI-e Y LA FIRMA-e EN LA ADMINISTRACIÓN

1. Introducción

Entre las competencias de las Administraciones públicas en materia de Administración electrónica se encuentra el obtener unos niveles óptimos de calidad, agilidad y rendimiento de los servicios telemáticos que la Administración pone a disposición de los ciudadanos y empresas; conseguir unos niveles de eficiencia en el uso de los recursos públicos; reducir y rentabilizar los costes e inversiones, y mejorar la integración interdepartamental y la simplificación administrativa.

Para conseguir estos objetivos, una de las medidas adoptadas ha sido el impulso del uso de la firma y certificación electrónica. De entre ellas, una de las de mayor trascendencia ha sido la sustitución gradual del Documento Nacional de Identidad actual por el equivalente en formato electrónico, lo que se ha venido en denominar DNI-e.

La introducción de la firma-e y el DNI-e es ya una necesidad en la tramitación telemática de todas las Administraciones públicas, sin embargo, el desarrollo y extensión tecnológica que están teniendo está siendo desigual y pausada en el tiempo. Entre los inhibidores del uso generalizado de estas nuevas técnicas de identificación y firma, está la complejidad tecnológica que hay que introducir en los sistemas de información, los elevados costes e inversiones a realizar o la falta de recursos especializados disponibles en los diferentes organismos Públicos.

Conocedores de estos condicionantes y en el ejercicio de las potestades que tiene atribuidas, el Ministerio de Administraciones Públicas (en adelante MAP) promueve una iniciativa para el desarrollo y prestación de servicios que impulsen el uso de la certificación y firma electrónica en los sistemas de información de las diferentes Administraciones públicas.

2. Fundamentos

En los últimos años se han venido desarrollando múltiples iniciativas materializadas en diferentes planes estratégicos de todos los ámbitos de la Administraciones. Estos planes disponen de líneas de actuación que se desarrollan conforme a un marco jurídico que evoluciona en consecuencia. Entre las acciones y medidas particulares para cubrir sus objetivos se encuentran las siguientes:

• Acelerar la introducción del DNI-e y su desarrollo pleno en su papel de facilitador de transacciones electrónicas.

• Establecer una infraestructura de información segura, eliminando la brecha tecnológica y cultural que acompaña el desarrollo de la Administración electrónica y del comercio electrónico.

• Establecimiento de estándares mínimos en cuanto a sistemas básicos, interfases, modelos de datos y presentación que faciliten el desarrollo de servicios.

• Implantar un marco de interoperabilidad para facilitar la prestación de servicios de administración electrónica.

• Fomentar la promoción y aprovechamiento de buenas prácticas, a partir del desarrollo de proyectos por las Administraciones públicas en el ámbito de la Administración electrónica.

Se requiere una reflexión sobre dos aspectos fundamentales, la designación de la línea de trabajo a desarrollar y el modelo de colaboración y servicio elegido para alcanzar los objetivos deseados.

Fruto de esta reflexión, y en consenso con el resto de Administraciones beneficiarias de estos servicios, durante el año 2005 se ha lanzado en el MAP un proyecto denominado "Plataforma de servicios de validación de certificados y firma-e: Iniciativa @firma". Este proyecto cubre directa o indirectamente varios de los objetivos relacionados y se centra en **facilitar a las aplicaciones los complementos de seguridad necesarios para implementar la autenticación y firma electrónica avanzada basada en certificados digitales.**

Desde el punto de vista tecnológico, construye una capa de abstracción de seguridad a nivel de aplicación que desacopla la lógica de negocio de las aplicaciones de la introducción de mecanismos de seguridad a nivel de control de accesos, firma, cifrado, control del no repudio y validez de los certificados, etc.

3. Expectativas en materia de firma-e

La introducción de la firma-e y el DNI-e es ya una necesidad en la tramitación telemática de las Administraciones públicas. Existen multitud de planes e iniciativas destinadas a generalizar su uso entre la Administración y los ciudadanos: Plan de Choque, Plan Avanza, Plan Conecta, eEurope, i2010, etc. Sin embargo, todas las entidades públicas implicadas demandan una labor de coordinación y acoplamiento para que las iniciativas desarrolladas de forma unilateral por las distintas Administraciones puedan converger con el interés general.

Entre otros elementos o condicionantes que aplican de igual forma a todos los colectivos en materia de firma-e, tanto Administración como ciudadanos o empresas, se encuentran:

• La existencia de una base legal clara en la que se soportan los servicios de certificación y firma electrónica como la Ley 59/2003, de 19 de diciembre, de firma electrónica y la Directiva Comunitaria de Firma Electrónica 1999/93/EC, Real Decretos 263/1996, 209/2003, ...

• La transformación gradual que está experimentando la aplicación de la tramitación telemática de los procedimientos administrativos.

• El número de certificados digitales expedidos está próximo a 1 Millón de unidades. Esta cifra tendrá un incremento exponencial a partir de marzo de 2006 con la puesta en circulación del DNI-e que incluye los certificados digitales para autenticar y firmar electrónicamente.

• En muchos casos, las aplicaciones de firma y certificación digital en la Administración tienen un uso común: registros telemáticos, portafirmas, firma de formularios y ficheros, ...

• La validez de una firma digital ha de ser ubicua tanto para organismos como para ciudadanos. Los criterios de utilización de la firma-e y la forma de acercarla a los ciudadanos en forma de justificantes, documentos firmados, verificación de elementos firmados, etc., ha de ser homogénea.
Un elemento firmado por un organismo ha de ser válido ante cualquier otro.

• Los escenarios operativos son complejos de gestionar, con múltiples Prestadores de Servicios de Certificación (en adelante PSC) que ofrecen sus certificados y con los que se habrían de establecer convenios o acuerdos bilaterales; los certificados digitales X.509 v.3, aunque siguiendo los estándares que lo rigen, no distribuyen la información con los mismos criterios.

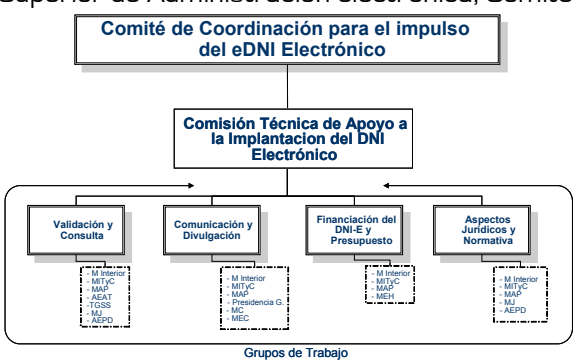
Estos y otros factores han servido para determinar el alcance de la iniciativa de cooperación interadministrativa para impulsar la firma-e.

Ricardo Cantabrana González
Alfonso Berral López

4. Cómo satisfacer las expectativas de las AAPP

Como se ha señalado, el MAP tiene atribuida una serie de competencias en materia de Administración electrónica para el impulso de la firma-e.

Además, ejerce como catalizador y facilitador del intercambio de iniciativas entre Administraciones en diferentes foros, como la Comisión Permanente del Consejo Superior de Administración electrónica, Comité Sectorial de Administración electrónica con las Comunidades Autónomas, grupos de trabajo en la Unión Europea.



Y más concretamente, en el plan de lanzamiento del DNI-e promovido por el Gobierno, se han creado varios grupos de trabajo (ver Gráfico 1) que han evolucionado uniformemente para cubrir los objetivos. En todos estos grupos, el MAP ha tenido una aportación valiosa y ha sabido transmitir e impulsar las medidas adoptadas hacia otros agentes externos: Departamentos Ministeriales, Comunidades Autónomas o Entidades Locales.

Entre las medidas específicas adoptadas más significativas se encuentra la de incorporar unos servicios de validación del estado de los certificados del DNI-e a través de la iniciativa de @firma y ofrecer estos servicios a cualquier organismo del sector público que lo solicite.

Partiendo de todos los antecedentes descritos y conocedores de la pluralidad que caracteriza a los diferentes organismos destinatarios de los servicios en lo organizativo, lo tecnológico o en los económico, **la elección del modelo de colaboración constituía el factor más importante del proyecto.**

De esta forma, la iniciativa @firma se construye con las siguientes premisas:

• El objetivo primordial no ha de ser otro que el de impulsar la implantación de la firma-e y el DNI-e mostrando una visión uniforme a los ciudadanos. Toda finalidad diferente de esta no estaría justificada.

• Se dispone de los recursos económicos suficientes para implementar y desarrollar la iniciativa hasta conseguir el estado de madurez en los sistemas y en el modelo de explotación.
A la vez , se reducen los costes en licencias, soporte, infraestructuras, etc por parte de los organismos usuarios.

• Poder ofrecer los servicios a cualquier nivel de la Administración: local, autonómico o nacional, y donde todos se vean representados.

• La solución técnica seleccionada es la más idónea para nuestro ámbito de aplicación. Dicha solución se basa en las siguientes premisas:

- Se trata de una solución nada intrusiva a la hora de integrarse en arquitecturas y soluciones existentes en los organismos.
- Además de gestionar la validación de los certificados del DNI-e, está abierto a otros de diferentes PSCs: MultiPSC, MultiPolítica, MultiCertificados, MultiFirma o MultiFormatos. Igualmente, se establecerían redes de confianza paneuropeas: BRIDGE-CA.

Ello estimula la creación de redes de confianza mutua entre los PSCs acreditados por la Administración y los diferentes organismos públicos usuarios de estos servicios.

- La administración y evolución del software de @firma será diseñada y articulada por los organismos usuarios.
- La solución atesora las máximas garantías de seguridad y robustez: certificación de procesos y productos, óptimo rendimiento, alta disponibilidad, portabilidad, ...

• El porfolio de servicios a ofrecer han de complementar las capacidades existentes en cada organización, no sustituirlas.

• El nivel de interoperabilidad y reusabilidad de sistemas existentes ha de ser óptimo.

5. Concepción de la Iniciativa

Para la adecuación del proyecto a las expectativas de los agentes intervinientes se inicia un conjunto de actividades en un proceso continuo de estudio y desarrollo. La puesta a disposición de los diferentes organismos de un conjunto de servicios de certificación y firma electrónica podría resolver las necesidades en un corto plazo, pero sería claramente insuficiente a medio y largo plazo conforme la visión uniforme y universal de la firma electrónica.

En el gráfico 2 podemos identificar las numerosas líneas de trabajo iniciadas con la iniciativa @firma que certifica la globalidad del estudio.

Gráfco 1: Líneas de trabajo con @firma

Identificar servicios horizontales de firma-e
De esta forma de realiza un análisis de las necesidades mayores en el seno de los organismos Públicos, concentrando los esfuerzos en aquellos aspectos más complejos, tanto técnicamente como organizativamente, y que pudieran ofrecerse con una solución débilmente acoplada a los desarrollos existentes.

Evaluar soluciones técnicas para la Plataforma de firma-e
Existen múltiples productos comerciales en el mercado que ofrecen frameworks de desarrollo para implantar servicios con autenticación y firma electrónica. La solución elegida por el grupo de trabajo ha sido @firma. Además de las capacidades funcionales y tecnológicas que ofrece, hay un factor diferenciador sobre el resto: **la propiedad intelectual y los derechos sobre @firma pertenecen a las Administraciones públicas.** Ver apartado 6.

Implementar la Plataforma de firma-e
Se inicia un proceso gradual en el que se implementa un núcleo tecnológico donde se disponen los componentes que constituyen la base de @firma y se van incorporando paulatinamente servicios disponibles para los organismos accesibles mediante servicios web u otros estándares.

Inventario de procedimientos administrativos
A partir del lanzamiento del DNI-e, y como parte de una estrategia conjunta de apoyo a dicho documento por parte de las Administraciones públicas, se pone en funcionamiento un observatorio de procedimientos administrativos disponibles por vía telemática con el DNI-e.

Comisiones ministeriales y comités sectoriales lanzamiento DNI-e
Tanto el impulso sobre el inventario de procedimientos telemáticos como otras actividades informativas del DNI-e, son llevadas a cabo por el MAP a través del Consejo Superior de Administración Electrónica en la Administración General del Estado y el Comité Sectorial de Administración Electrónica en las Comunidades Autónomas.

Establecer redes de confianza paneuropeas: BRIDGE-CA
La presencia del MAP en grupos de desarrollo de proyectos paneuropeos a través del programa IDABC, facilita la extensión de la iniciativa @firma más allá de nuestras fronteras. De esta forma se establecen grupos de confianza a partir de los certificados electrónicos emitidos por PSCs de múltiples países. Ciudadanos extranjeros podrán emplear sus certificados electrónicos emitidos por Autoridades de sus países de origen en trámites telemáticos de nuestras Administraciones, y viceversa.

Revisión de aspectos jurídicos y normativos
Un proyecto de estas características requiere de la revisión normativa necesaria que apoye los servicios interoperables entre Administraciones con todas las garantías.

Acuerdos con PSCs y Dirección General de la Policía
Una de las actividades más valoradas lo ha constituido la realización de unos convenios únicos con todos aquellos PSCs registrados por el Ministerio de Industria, Turismo y Comercio, e individualmente con la Policía para el servicio de validación de certificados del DNI-e.

Lo más relevante de estos acuerdos lo constituye la aplicación del concepto de **transitividad:** un solo convenio con un PSC cubre todas las aplicaciones usuarias de los organismos usuarios de @firma, sin necesidad de que estos últimos hayan de suscribir acuerdos bilaterales con los primeros.

6. Una solución basada en @firma

@ firma es la solución tecnológica de firma y certificación electrónica propiedad de la Junta de Andalucía que constituye la base tecnológica de los servicios de firma-e ofrecidos por el MAP a través de esta iniciativa. La versión actual evolucionada a partir de múltiples organismos públicos intervinientes es la 5.0.
Para seleccionar la @firma como base tecnológica del proyecto, se tuvieron en consideración múltiples condicionantes:

- @firma v4.0 es una solución con una alta base de implantación que se encuentra operativa desde 2003. Dispone de instalaciones en la Junta de Andalucía (con más de 100 procedimientos), Junta Castilla León y Consejo General de la Abogacía.
Es por lo tanto una solución con una sólida base de conocimiento por parte de los integradores y personal de soporte a las aplicaciones.

- Mantiene un alta grado de interoperabilidad con las aplicaciones.

Así ofrece sus servicios a través de servicios web u OCSP construidos a partir de estándares.
Como valor añadido, cuenta con recursos de integración de servicios de firma electrónica aplicaciones legacy. Eje: APIs para Oracle Developer, Oracle Form, Visual Basic, ...

• Al tratarse de una solución propiedad de las Administraciones públicas, desde sus inicios ha habido un creciente interés por publicar información técnica. Ello ha motivado a que actualmente se cuente con una base importante de integradores con conocimientos técnicos sobre @firma.

• Incorporación de Políticas de eFirma (artículo 4 Ley de Firma 59/2003).

Finalmente, otra de las grandes ventajas aportadas por @firma lo constituye el alto nivel tecnológico de sus componentes:

• Solución basada en software libre, estándares abiertos y en J2EE: servidores web Apache, JBOSS, Sistema Operativo Solaris/Linux, AXIS, etc.
• Disponibilidad de Cliente de firma, verificación, validación, ...

• Entorno cliente con múltiples navegadores: Netscape, Mozilla, iExplorer, Firefox, y sistemas operativos (Windows y Linux).

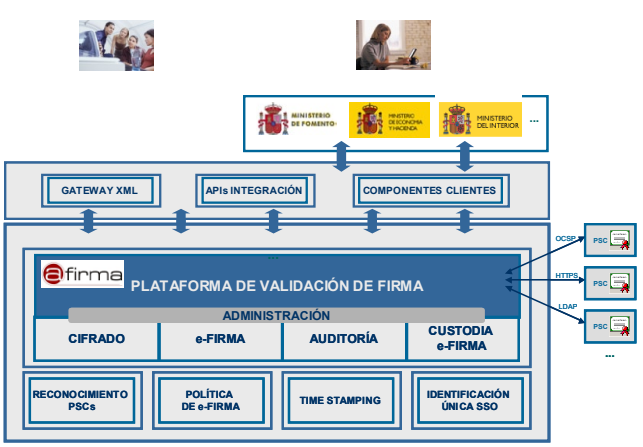
• Sujeción a normas y estándares de ámbito nacional y europeo: EESSI, ETSI, CEN, Directiva y Ley de firma-e, IETF, OASIS, ...

• Alta auditabilidad de la Plataforma: gestión de transacciones de cada módulo, agentes de monitorización, logs de operaciones, ...

• Múltiples formatos de firma: PKCS#7 v 1.5, CMS, S/MIME, XMLSignature, XMLSignature Avanzado (XaDES).

Los servicios que pone a disposición @firma a los organismos se resume en los siguientes:

I. Módulo de Registro y Gestión de Eventos:
• Auditoría y trazabilidad de todas las transacciones realizadas por la plataforma.
• Contabilidad de transacciones. Posibilidad de hacer un seguimiento concreto a las transacciones generadas en la plataforma para poder gestionarlas posteriormente.
• Reporting de actividades.
• Gestión de Alarmas.



II. Módulo Gestión de Prestadores
• Gestión del Árbol de PSCs.
• Gestión de los distintos tipos de certificados por cada PSC.
• Analizador semántico de certificados y mapeo de campos.
• Gestión de Políticas de Confianza.
• Importación y Exportación de Elementos de Confianza entre distintas plataformas @firma.

III. Módulo de Validación
• Validación Multinivel de certificados
• Validación de certificados X.509 v3 ante un PSC mediante los protocolos http, ftp, LDAP y OSCP.

• Servidor OCSP.
• Reconocimiento y validación de certificados del DNI-e emitido por la Dirección General de la Policía, Ministerio del Interior.
• Caché de validación configurable en tiempo

IV. Módulo de Firma
• Firma, Multifirma y Multifirma web masiva.
• Firma, Multifirma de Ficheros en cliente.
• Firma de Ficheros por Certificado de Organización.
• Firmas realizadas en varios formatos.
• Custodia de los elementos de No Repudio.

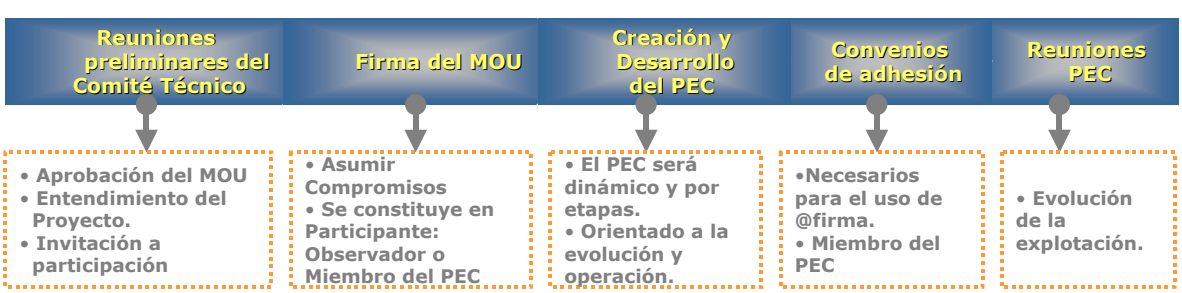
V. Autoridad de sellado de tiempo (TSA)
• Integración de la plataforma @firma con Autoridades de Sellado de Tiempo (TSA) que sigan el estándar definido para ello por la IETF mediante la RFC 3161.
• Disponibilidad de la TSA disponible en el MAP.

7. Modelo colaborativo de progreso

Sin embargo, aunque disponer de una buena base tecnológica constituye una base sólida para facilitar la expansión de la firma electrónica, aun es más importante encontrar el modelo de colaboración y cooperación que permita consolidarse como una solución de futuro.

Como ya se ha señalado anteriormente, el producto @firma es propiedad de las Administraciones públicas y no supone coste alguno su implantación o uso de sus servicios. Una solución como esta requiere de un estudio minucioso sobre el mejor modelo de operación.

La base del modelo propuesto por el MAP y consensuado por los organismos usuarios se resume en los siguientes puntos:



1. Establecimiento de grupos de trabajo en diferentes ámbitos de la Administración. Pretenden conciliar y materializar las necesidades de los organismos públicos en materia de firma-e y certificación digital a través de @firma; es un foro de encuentro para compartir y desarrollar iniciativas de firma y certificación electrónica en la Administración.

2. Acuerdo de Intenciones (MOU). Se define para determinar el escenario de colaboración en el que se desarrolla esta cooperación Programa. Constituye el marco de trabajo para incorporarse al grupo de trabajo, la definición del PEC y articular la adhesión al convenio de uso de @firma.

3. Programa de Evolución Continua (PEC). Mientras que el MOU y el convenio de adhesión establecen las cláusulas de utilización de @firma, el PEC se establece cómo es el Plan de Proyecto de ejecución de mejoras y explotación. Participarán aquellos miembros de Comunidades Autónomas, Ministerios o Entidades

Locales que hayan firmado el convenio de adhesión.

4. convenios de adhesión. Se constituyen como elementos que otorga a los firmantes las capacidades de uso de los servicios de @firma que ofrece el MAP o la instalación del producto en sus dependencias. Conlleva la incorporación al Programa de Evolución Continua (PEC).

5. Reuniones de progreso. Finalmente, la aplicación de un calendario de reuniones de trabajo periódicas permiten avanzar en el despliegue de nuevas necesidades y coordinar el convenientemente el progreso del modelo descrito.

Como modelos operativos dentro de la iniciativa de @firma, se han contemplado varios modos de utilización de los servicios. Independientemente del modo de utilización elegido, a través del PEC los organismos participan en el progresivo desarrollo de @firma aportando mejoras o evoluciones del producto.

1. Ofreciendo servicios de Firma electrónica desde la Plataforma de @firma del MAP. Consiste en la modalidad denominada ASP o Aplication Service Provider. A través de este modelo, las diferentes aplicaciones de diferentes organismos acceden a los servicios comunes de la Plataforma MAP a través de servicios web u otros protocolos específicos, como OCSP.

Otras de las características que lo definen son:

- Utilización de los servicios a través de la Intranet Administrativa y el Punto Neutro de la Extranet de las Administraciones públicas (SARA).
- Administración delegada para organismos.
- Se suministran reportes de actividad y transacciones de diferente naturaleza.
- Se dispone de Servicio de Soporte especializado de segundo nivel a organismos usuarios.
- Reducción de costes é inversiones: desarrollo, soporte, plataforma, etc.
- Accesibilidad a últimas versiones de servicios con total transparencia.

2. El segundo de los modelos es el denominado **Federado/Distribuido.**

La diferencia con el modelo ASP radica en que se distribuye el producto @firma al organismo solicitante para su instalación y parametrización en Centro de Procesos de Datos particulares. En este modelo se contempla la posibilidad de conformar una red de confianza e interoperabilidad entre diferentes instalaciones a través de la Federación de elementos lógicos.

Igualmente se admite la solicitud de consultas de validación provenientes de otras entidades o plataformas de validación incorporadas a la iniciativa.

Entre las particularidades de este modelo se encuentran las siguientes:

- Incluye la libre distribución de nuevas versiones, parches, etc.
- La configuración del "Servidor Central" se podrá propagar a las implantaciones delegadas.
- Es la opción apropiada para aquellas implementaciones que se basan en arquitecturas singulares, requieren condiciones de seguridad especial o contemplan un uso interno de los servicios.
- Admiten una configuración de centros de respaldo entre las diferentes Plataformas operativas.

8. Cómo contactar

Se dispone de un equipo de apoyo disponible para cooperar con los diferentes organismos en las actividades de soporte y ayuda a la evaluación e integración a los servicios de @firma.
eMail: soporte.afirma5@map.es