
Estrategia de Validación del DNI electrónico



Luis de Eusebio Ramos

S.G. Coordinación de Recursos Tecnológicos de la AGE
Ministerio de Administraciones Públicas

- 1. Génesis**
- 2. Situación real de la firma electrónica (DNle, otros PSCs)**
- 3. Desarrollo de la Plataforma de Validación @Firma v5.0**
- 4. Actividades de Cooperación (DGP, AA.PP, PSCs)**
- 5. Situación del Servicio**
- 6. Modos de utilización**
- 7. Administración y Entorno de pruebas a integración para organismos.**

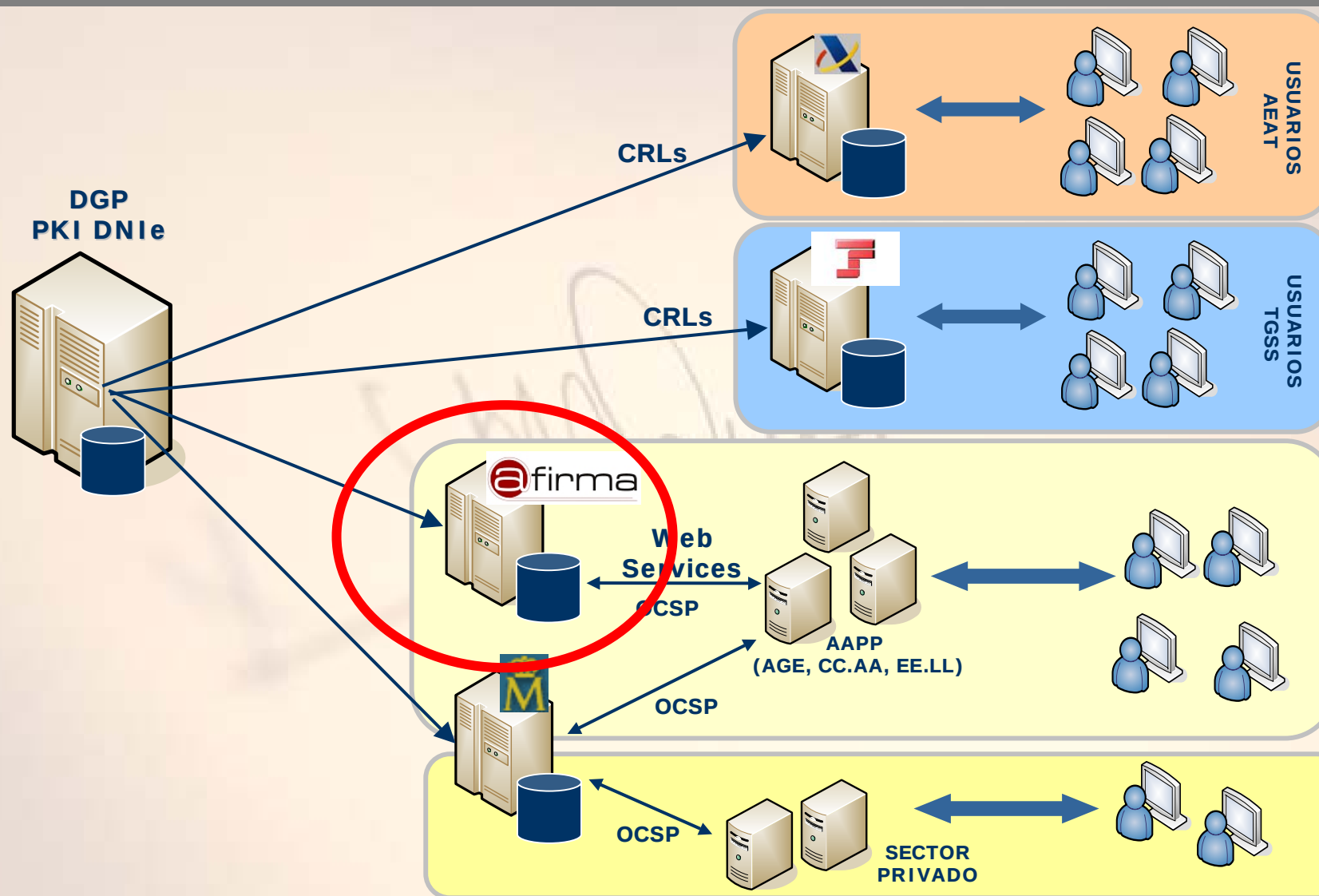
- Los servicios de certificación digital y firma electrónica tienen una base legal clara.
- Los escenarios operativos son complejos de gestionar:
 - ▶ Múltiples Prestadores de Servicios de Certificación. Convenios múltiples.
 - ▶ Certificados digitales X.509 v.3 con información no homogénea
 - ▶ Multi-CA: Varios canales de validación de certificados (OCSP, LDAP, ...), ...
- Normalización de muchas de las facilidades necesarias:
 - ▶ Algoritmos de cifrado y firma, Sellado de tiempos, ...
- Análogas necesidades para el despliegue de la e-Administración: registros telemáticos, sistemas de intercambio, portafirmas, ...
- No existen escenarios de confianza afines entre Organismos de la AAPP.
- Algunos Organismos de diferentes AAPPs ya disponen de soluciones tecnológicas análogas.
- La aparición del DNle va a ayudar a ordenar el contexto de la identificación y Firma

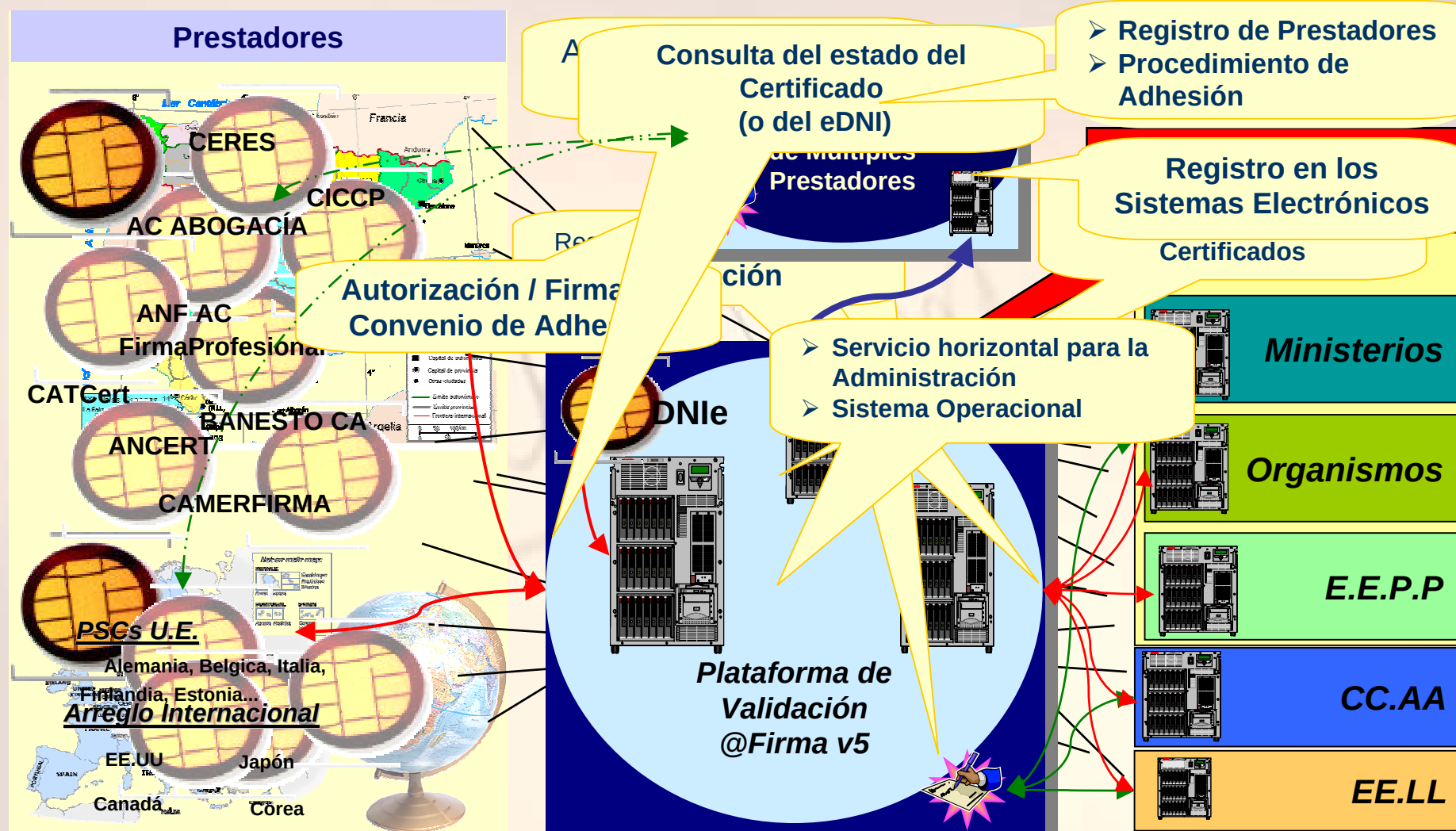


¿ Cómo podemos ayudar ?



Esquema de Validación del DNle





Reconocimiento de PSCs

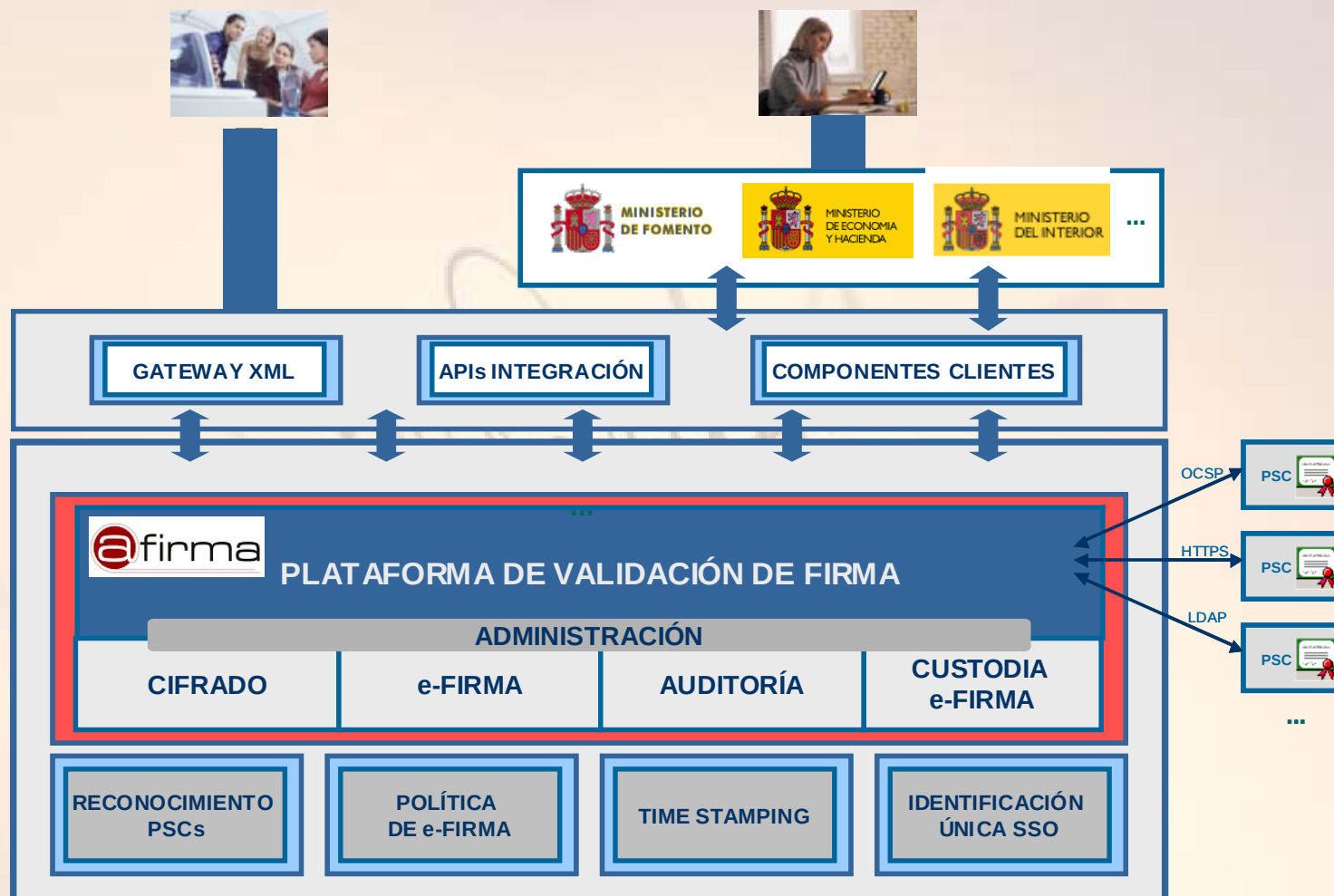
Facilitar la utilización tanto de los certificados electrónicos emitidos por los diferentes emisores tanto estatales (DNI-e, CERES, CATCert, Firma Profesional, ...) como internacionales (e-ID electrónica Italia, Finlandia, Bélgica...)

- Gestionar el Registro de Prestadores adheridos a la plataforma y las características asociadas a los tipos de certificados que expidan.
- Verificar los requisitos de Interoperabilidad Técnica para la adhesión
- Tramitar el proceso / procedimiento administrativo de Adhesión conforme a la Política de Firma
- Responsable del reconocimiento de certificados a Nivel Internacional

Plataforma de Validación de Firma-e

Establece un ecosistema de seguridad que permite a las entidades de carácter público determinar la vigencia y validez de los certificados digitales empleados en cualquier procedimiento telemático así como de las firmas generadas.

- Autoridad de Validación del eDNI
- Plataforma multiPKI operativa de servicios de firma y validación.
- No intrusiva en los procedimientos administrativos
- Servicios de Valor Añadido
 - Cliente de firma electrónica universal
 - Interacción con TSA del MAP
 - Integración de otras fuentes de datos como el Registro Central de Personal



Ordenación efectiva de la firma electrónica:

- **Normativa**
- **Técnico-Organizativa**
- **Operativa**

Garantías

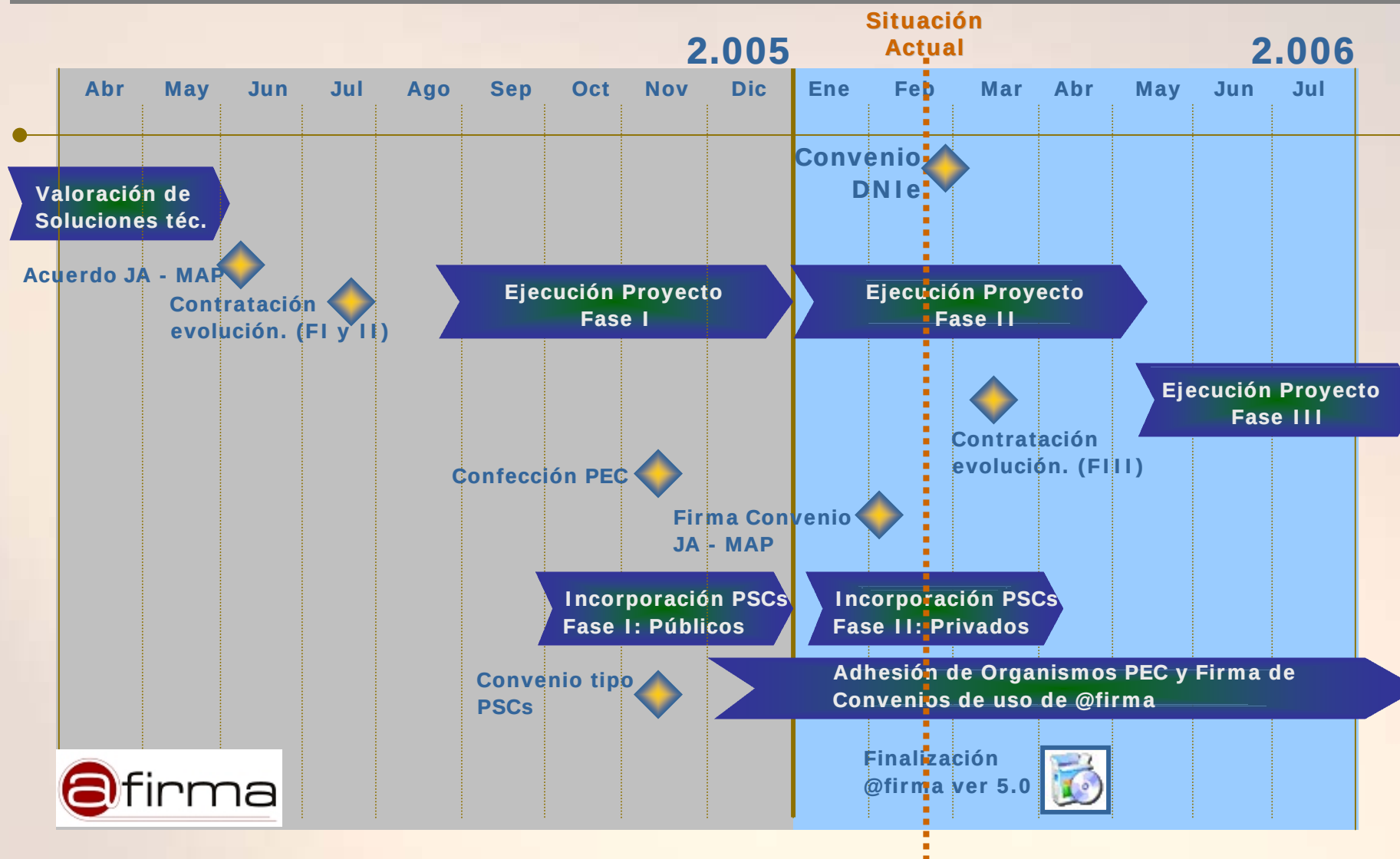
- **Facilita la Adopción de la Firma Electrónica en los procedimientos**
- **Elimina Complejidad asociada al nº de Prestadores**
- **No intrusión** en el ejercicio de las competencias atribuidas a cada ministerio
- **Cumplimiento de requisitos** por parte de los prestadores adheridos
- **Supresión de incertidumbres** derivadas de la existencia de diferentes grupos de PSCs en función del departamento
- **Seguridad y Eficiencia.**

Autonomía en la Gestión de Prestadores

- **Transparencia** a la plataforma de validación y a sistemas de los departamentos
- **Interlocutor** único con todos prestadores (Nacionales e Internacionales)

- **Evolución de @firma v4 de la Junta de Andalucía.** Solución con una **alta base de implantación**:
 - Operativa desde **2003**
 - **Implantaciones** en la Junta de Andalucía (+100 procedimientos), Junta Castilla León, Consejo Gral. de la Abogacía, ...
- **Normalización** de aplicación de Firma-e por usuarios y AAPP.
- Mantiene un **alta grado de interoperabilidad** con las aplicaciones:
 - Servidor OCSP en Plataforma
 - Web Services basados en WS-I
 - Integración de Firma-e en aplicaciones Legacy. Eje: APIs para Oracle Developer, Oracle Form, Visual Basic, ...
- **Múltiples integradores** con conocimiento de la Plataforma.
- **Copropiedad del resultado** (v5.0):
 - Junta de Andalucía – MAP
 - **Todos los organismos adheridos** a la plataforma

- Accesibilidad a través de **Intranet Administrativa** y el **Punto Neutro de las Extranets de las AA.PP.**
- Solución basada en **software libre** y estándares abiertos y en J2EE :
 - ▶ Servidores web Apache, JBOSS, Sistema Operativo Solaris/Linux.
- 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, RFCs, ...
- Alta **Auditabilidad** de la Plataforma: **Informe de Evidencia Judicial**, 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)

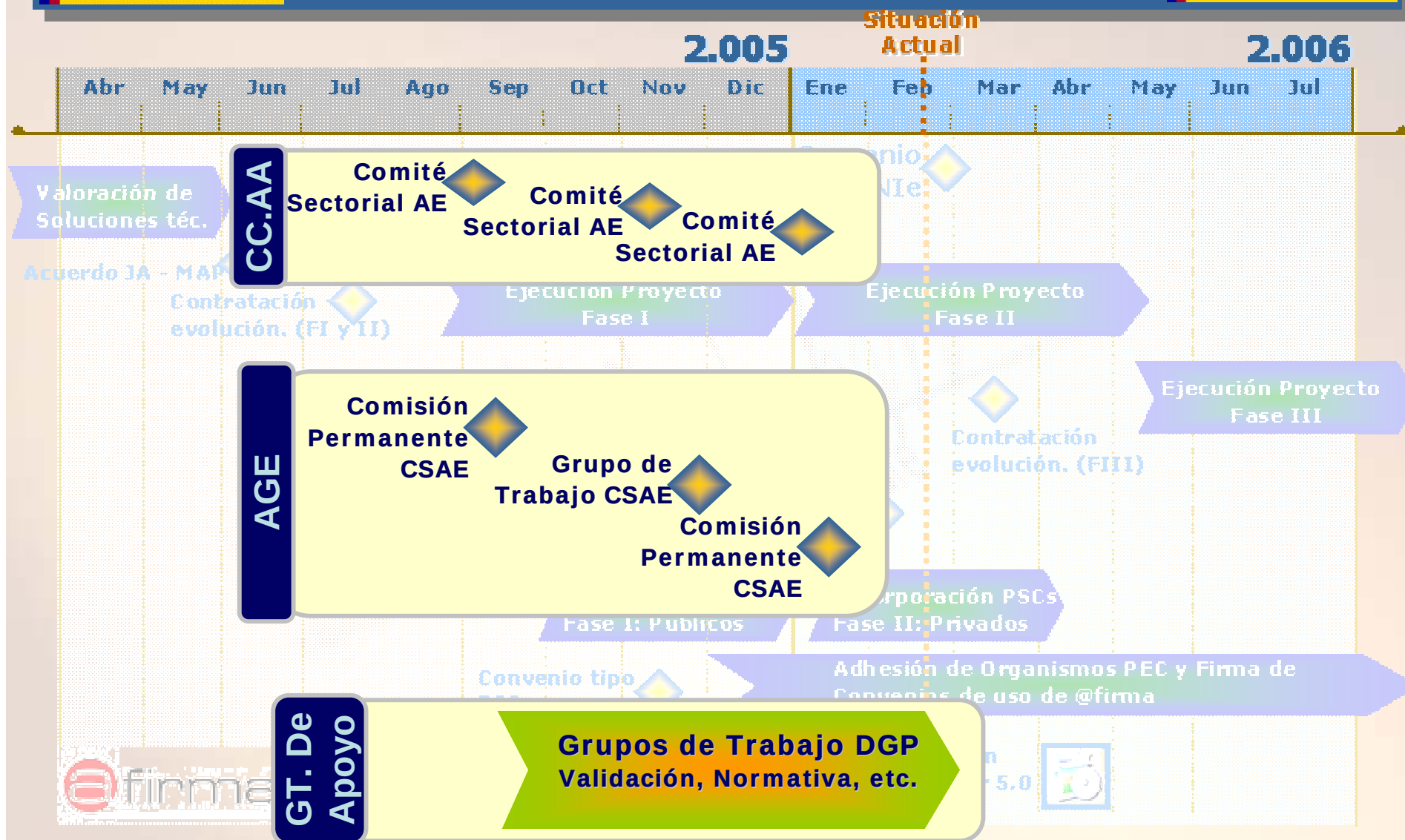


Administración General del Estado

- ⇒ Ministerio de Economía y Hacienda
- ⇒ Agencia Española de Protección de Datos.
- ⇒ Ministerio del Interior
- ⇒ Ministerio de Fomento
- ⇒ Ministerio de Sanidad y Consumo
- ⇒ Ministerio de Industria, Turismo y Comercio
- ⇒ Guardia Civil
- ⇒ Ministerio de Defensa
- ⇒ Ministerio de Cultura
- ⇒ Ministerio de Medio Ambiente
- ⇒ INEM
- ⇒ Centro Criptológico Nacional
- ⇒ Ministerio de Cultura
- ⇒ Ministerio de Trabajo y Asuntos Sociales
- ⇒ Banco de España

Comunidades Autónomas

- ⇒ Junta de Castilla y León
- ⇒ Comunidad de Madrid
- ⇒ Gobierno de Cantabria
- ⇒ Gobierno de Canarias
- ⇒ Generalitat de Cataluña
- ⇒ Junta de Extremadura
- ⇒ Principado de Asturias
- ⇒ Generalitat Valenciana
- ⇒ Gobierno de Navarra
- ⇒ Junta de Andalucía
- ⇒ Comunidad Autónoma de La Rioja
- ⇒ Junta Comunidades Castilla La Mancha
- ⇒ Gobierno de Aragón
- ⇒ Región de Murcia



- **Servicios en Producción** desde el 13 de Febrero de 2006:
 - **Validación de Certificados** (OCSP y WS)
 - **Validación de Firma.**
 - **Sellado de Tiempo.**
- **Incorporación** de múltiples **Prestadores de Servicios de Certificación** (PSCs)
- **Gestión y Administración** de la Plataforma
- Mecanismos de **auditoria**
- **Análisis de Riesgos** en desarrollo utilizando MAGERIT v. 2 y PILAR
- **Servicio de Soporte** a los organismos para integración.
- Ultimando **Convenios con los PSC** para el reconocimiento en @firma de todos los presentados del registro del MITyC.
- Conexión a través de **Intranet Administrativa y el Punto Neutro de las Extranets de las AA.PP** (PSCs públicos y Organismos):

● **OCSP Responder MultiPKI** (Requisito DGP)

- ⇒ Indica estado de Revocación de un certificado
- ⇒ Interpretar cada certificado recae sobre el organismo usuario.
- ⇒ Firma de respuestas

● **Servicio Web (WS) de Validación de Certificados.**

- ⇒ Con interpretación de los campos de los certificados a un XML homogéneo.
- ⇒ Firma de respuestas

● **Servicio Web (WS) de Validación de Firma**

- ⇒ Validación de un elemento firmado: indicando si la firma es correcta y la validez, fechado, etc.
- ⇒ Incluye la interpretación de los campos del certificado firmante a un XML homogéneo

- **Garantiza EL MISMO NIVEL DE SEGURIDAD.** Pueden recibir peticiones firmadas y las respuestas son firmadas y selladas temporalmente (Timestamping)
- **Facilita la integración.** La adaptación de una aplicación para incluir una llamada a un WS tiene **menor impacto** que la adaptación asociada a la inclusión de una petición OCSP.
- **Independencia del Prestador y Certificado.** La traducción de la **información del certificado** a un **XML homogéneo** requiere de **una única adaptación** en las aplicaciones independientemente del número de PSCs y Certificados.*
- **Servicios Adicionales.** Toda la **validación** asociada a un **documento firmado** puede resolverse en **una única petición**.*
- En la **misma petición** se devuelve **toda la información contenida en campos y extensiones del certificado**.

* El protocolo OCSP sólo informa del estado de revocación. El resto de actividades dependerá del Organismo.

- Recepción de especificaciones de certificados y elementos electrónicos de ejemplo: **16/01/06**
- Primera reunión de trabajo: **17/01/06**

Prestador Servicios Certificación	Certificado	Protocolo*	Fecha de Inicio de Integración	DPC	Fecha de Puesta en Marcha
DGP – DNle	Persona Física Firma	CRLs completas y particionadas*	16/1/2006	22/11/2005	30/02/2006
DGP – DNle	Persona Física Autenticación	CRLs completas y particionadas*	16/1/2006	22/11/2005	30/02/2006

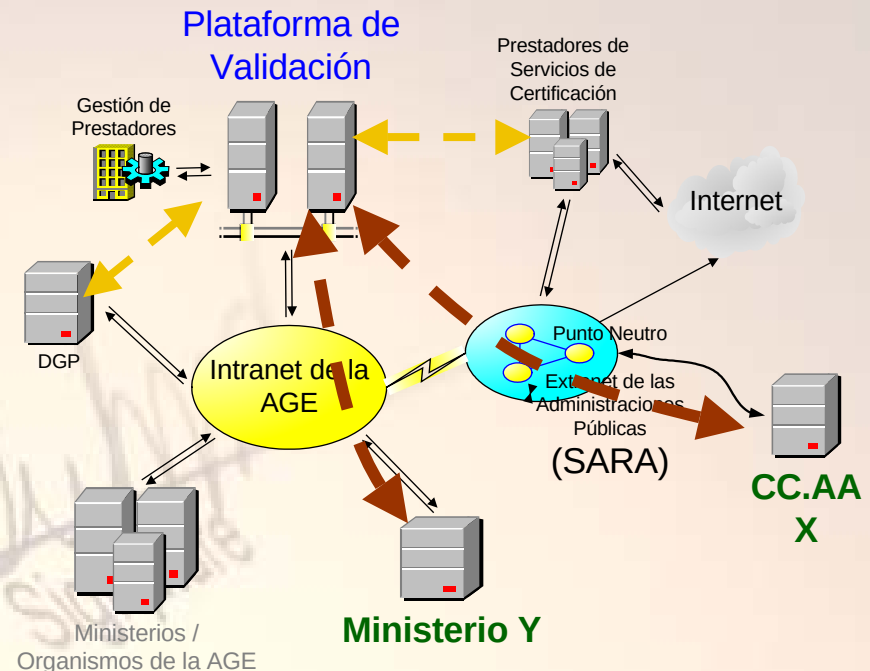
* El protocolo de actualización de CRLs no esta disponible. La integración se realiza a través de las CRLs de Prueba y se requerirán acciones de integración de la descargar de CRLs desde la DGP cuando su servicio esté disponible.

Pendiente de disponer del mecanismo de actualización de CRLs por la DGP-PKI

Prestador Servicios Certificación	Certificado	Protocolo	Fecha de Inicio de Integración	DPC	Fecha de Puesta en Marcha
FNMT-RCM	Persona Física	LDAP	3/11/2005	20/11/2005	1/12/2005
FNMT-RCM	Persona Jurídica	LDAP	3/11/2005	20/11/2005	1/02/2006
ACCV	Persona Física sw	OCSP+CRL+LDAP	3/11/2005	05/10/2005	25/11/2005
ACCV	Persona Física hw	OCSP+CRL+LDAP	3/11/2005	06/10/2005	25/11/2005
IZENPE	Persona Física	CRL	9/01/2006	21/03/2005	23/01/2006
IZENPE	Persona Jurídica en tarjeta hw	CRL	9/01/2006	21/03/2005	23/01/2006
IZENPE	Persona Jurídica en soporte sw	CRL	9/01/2006	21/03/2005	23/01/2006
CATCert	IdCAT c/ cifrado	OCSP+CRL	1/11/2005	31/01/2005	8/12/2005
CATCert	IdCAT s/ cifrado	OCSP+CRL	1/11/2005	31/01/2005	8/12/2005

Prestador Servicios Certificación	Certificado	Protocolo	Fecha de Inicio de Integración	DPC	Fecha de Puesta en Marcha *Estimada
ANF A.C.	Persona Física	OCSP	20/12/2005	2/03/2005	15/3/2006
ANF A.C.	Persona Jurídica	OCSP	20/12/2005	2/03/2005	15/3/2006
aNcert	Pendiente	OCSP	10/01/2006	-	15/3/2006
Firmaprofesional	Pendiente	OCSP	12/01/2006	-	15/3/2006
Camerfirma	Pendiente	-	20/01/2006	-	15/3/2006
Consejo General de de Abogacía	Pendiente	-	-	-	15/3/2006

- Utilización del servicio de validación a través de la **Intranet Administrativa** y el **Punto Neutro de la Extranet de las AAPP (SARA)**.
- **Disponible Diciembre '05**
- **Administración delegada** para Organismos
- **Reportes de actividad** y transacciones de diferente naturaleza.
- Cumplimiento de un **SLA**
- Disponibilidad de **Servicio de Soporte** a organismos usuarios
- **Beneficiarse de acuerdos con PSCs.**
 - Transitividad de los acuerdos con PSCs reducen la necesidad de establecer N*M acuerdos PSC-Organismo
 - Acuerdo marco con FNMT.
- **Reducción de costes** é inversiones: desarrollo, soporte, plataforma, ...
- **Transparencia en actualización** de versiones, parches, etc.



- Se **distribuye el sw.** para la instalación en Plataformas propias.
- Libre distribución de **nuevas versiones, parches**, etc.
- La **configuración** del “Servidor Central” **se propagará** a las implantaciones delegadas
- Utilizando **definiciones IDA-BGCA** (Preparada para PSCs Internacionales)
- Disponible **Mayo '06**
- **Adecuación a las necesidades** de rendimiento y arquitecturas de cada Comunidad.
- Posibilidad de **configuración de respaldo** entre las diferentes Plataformas.



En ambos modelos, a través del **Programa de Evolución Continua (PEC)** los organismos **participan en el progresivo desarrollo de @firma aportando mejoras o evoluciones del producto**

2.006

1 Marzo

15 Marzo

31 Marzo

30 Abril

Lanzamiento DNle

- Servicios TSA-MAP.
- SLA y DPC de servicio
- Carga y actualización de CRLs de DNle
- Servicios de soporte
- Análisis y Gestión de Riesgos

Seguimiento Inicial

- Incorporación de PSCs
- Módulo de Firma
- Cliente de Firma
- Documentación del Sistema

Seguimiento Final

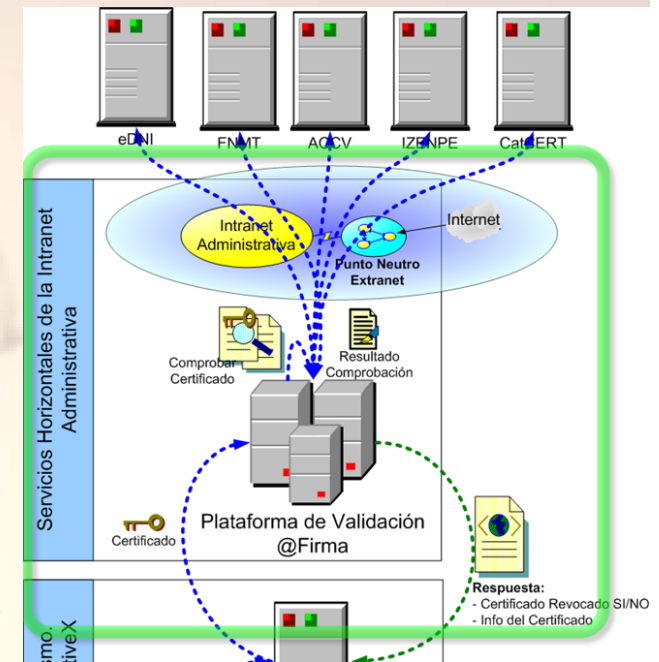
- Nueva configuración de TSA y Fachada.
- Implantación de Custodia
- Formación y casos de uso en .NET y java
- Análisis y Gestión de Riesgos final

Cierre Proyecto FII

- Gestión de representantes
- Cachés de validación
- Solución SSO
- Paquetización de @firma ver. 5.0
- Implementación Modelos F3derado y Distribuido



- Interfaz gráfica avanzada - IGUAX
- Configuración de árbol de PSCs y sus certificados,
- Registro de eventos generados,
- Analizador semántico de campos del certificado,
- Registros de auditabilidad de actividad del sistema.
- Política de confianza: una sola política hasta la fecha con todos los PSCs y sus certificados.
- Monitorización de alarmas



Configuración del Árbol de PSCs y sus Certificados

Configuración de Métodos de Validación

Consulta de Auditoría Inicial

Lista de Eventos

Informe de Auditoría

Informe de la transacción 1137085015575003 Fecha: 12/01/2006 05:57:55

Aplicacion: appPrueba Unidad organizativa:

Modulo de validacion 12/01/2006 05:57:55 Solicitud de Validacion MODO DE VALIDACION POLITICA DE VALIDACION CERTIFICADO EMISOR DE CERTIFICADO

Modulo de validacion 12/01/2006 05:57:55 Resultado del proceso de discriminacion

RESULTADO: CORRECTO IDCAT-ConCifrado

Modulo de validacion 12/01/2006 05:57:55 Discriminacion del tipo de certificado LISTA DE TIPOS

Modulo de validacion 12/01/2006 05:57:55 Evaluacion del tipo de certificado TIPO DE CERTIFICADO EVALUACION

TIPO DE CERTIFICADO IDCAT-ConCifrado

EVALUACION true

RESULTADO:

Validación MultiPKI

Web Services que retornan el **estado de revocación de un Certificado** electrónico emitido por cualquiera de los prestadores adheridos a la plataforma. **Y el desglose de la Información de Mapeo**

Piloto de Servicio para Pruebas

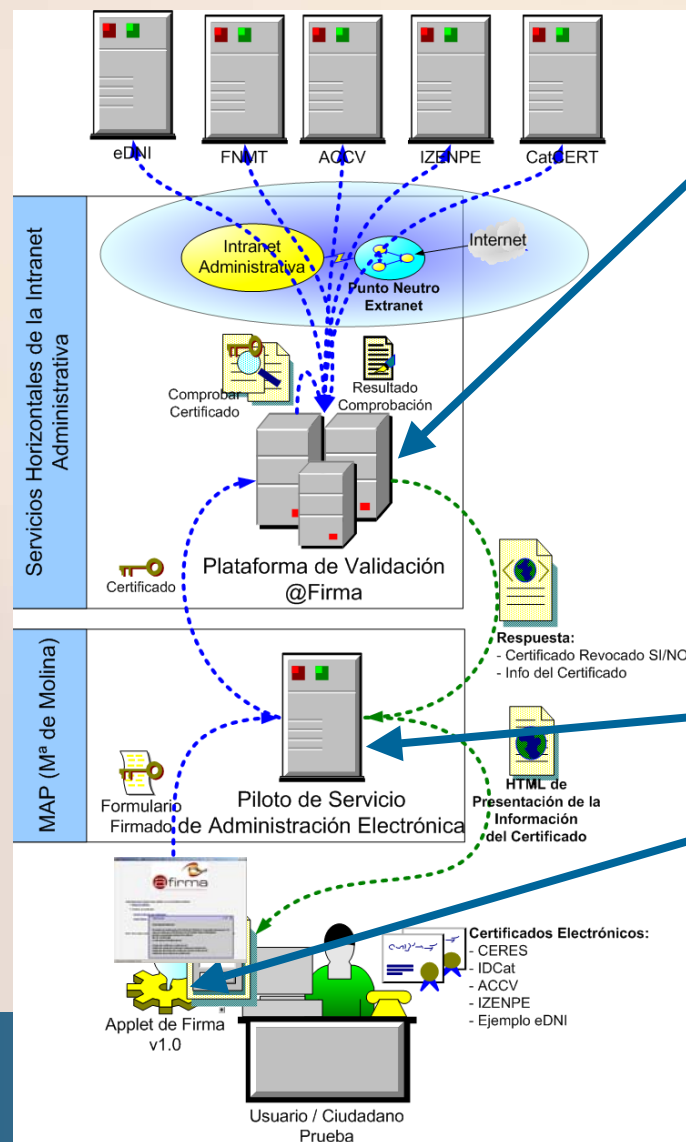
Aplicación web (demostrador) que permite **firmar un formulario** con un certificado de cualquier prestador y **realizar una validación** contra @firma **mostrando el estado y la información** asociada al certificado.

Incluye:

- **Aplicación Web Java** instalada en el MAP accesible a través de la IA.
- Primera versión del **Applet Cliente de firma**

Permite:

- Pasos de inicio en la construcción.
- Esqueleto de funciones a utilizar.



Dirección General de Modernización Administrativa

<http://www.map.es/>

Portal de difusión del DNI electrónico

<http://www.policia.es/hortaleza/samaca/mic/sites/index.html>

Muchas gracias

Ministerio de Administraciones Públicas