@firma

Seminario de Migración de las versiones 4.x a versión 5

Sevilla, 17 de Diciembre de 2.007

1. ¿Por qué es aconsejable migrar a @Firma v5?
   - Carencias de @Firma v4
   - Nuevas funcionalidades en @Firma v5
2. ¿Por qué un proceso de migración?
   - Cambios de filosofía entre versiones
3. Impacto
   - Sobre el proceso de adaptación
   - Sobre el entorno de ejecución
   - Sobre la gestión de la plataforma
   - Sobre las aplicaciones clientes
4. Soluciones: Extensión
5. Plan de migración
   - Aspectos a tener en cuenta antes de migrar.
   - Proceso de migración

1. ¿Por qué es aconsejable migrar a @Firma v5?
2. ¿Por qué un proceso de migración?
3. Impacto
4. Soluciones: Extensión
5. Plan de migración

Carencias de @Firma v4 (I)

- No compatibilidad con certificados:
  - E-DNI.
  - Nuevo certificado de FNMT de 2048 bits.
- Gestión de prestadores de certificación
  - Incorporación de nuevos prestadores de certificación y tipos de certificados costosa.
  - Necesita establecer mediante código el tratamiento de la información contenida en cada tipo de certificado.
- Validación de certificados
  - No permite la definición de métodos de validación de certificados.
  - No establece caches de validación.
  - No incorpora métodos on-line de validación como OCSP.
  - No es posible realizar validaciones conforme al estándar RFC 3280.

Carencias de @Firma v4 (II)

- Generación de firmas:
  - Formatos de firma obsoletos.
  - Estructuras electrónicas de firma que albergan sellos de tiempos no cumplen el estándar RFC 3161.
  - No son generados justificantes de firma.
- Administración de la plataforma
  - Requiere instalación de cliente de administración.
- Versiones anticuadas de componentes software en los que se apoya.
- Sobre servicios Web:
  - Securización débil.
  - Interoperabilidad baja.
- Problemática de soporte y evolución.

Nuevas funcionalidades de @Firma v5 (I)

- Módulo de Gestión de Prestadores
  - Gestión del Árbol de Prestadores de Servicios de Certificación (PSC).
  - 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.
- Módulo de Validación
  - Validación Multinivel de certificados según RFC 3280.
  - Validación del estado de revocación de certificados X.509 v3 ante un PSC mediante los protocolos CRL, OCSP y WS.
  - Servidor OCSP multiprestador.
  - Caché de estado de certificados multinivel.

Nuevas funcionalidades de @Firma v5 (II)

- Módulo de Firma
  - Firma, Multifirma y Multifirma masiva de ficheros y páginas Web (CoSign y CounterSign).
  - Firma en bloque.
  - Firmas multiformato (CMS, XMLDSignature, XADES, …).
  - Sellado de Tiempo.
  - Custodia de elementos de No repudio.
  - Custodia de documentos asociados a firmas configurable.
  - Justificante de firma.
  - Validación de Firmas.
  - Consultas de transacciones de firma atendiendo a varios criterios.
- Módulo de custodia
  - Almacenamiento, borrado de contenido y consulta de documentos.
  - Consultas y actualización de transacciones de firmas y bloques de firma.

Nuevas funcionalidades de @Firma v5 (III)

- Nuevo cliente de firma:
  - Modular
  - Ampliable mediante plugins.
  - Multiformato.
  - Modos de firma: simple, Co y counter.
  - Permite realizar firma de ficheros, datos, Web y firma masiva.
  - Funcionalidad criptográfica:
    - Generación de varios tipos de sobre digital (cifrado, firmado, cifrado y firmado).
    - Cálculo de varios tipos de resumen (MD5, SHA1, …).
    - Cifrado simétrico.

Nuevas funcionalidades de @Firma v5 (IV)

- Módulo de Gestión y Registro de Eventos
  - Auditoría y trazabilidad de todas las transacciones realizadas por la plataforma.
  - Generación de estadísticas sobre servicios
  - Gestión de Alarmas.
  - Herramienta Gráfica de Auditoria y Monitorización.
- Módulo de Administración
  - Gestión de tareas.
  - Gestión de usuarios avanzada.
  - Gestión de almacenes de certificados y contraseñas.

1. ¿Por qué es aconsejable migrar a @Firma v5?
2. ¿Por qué un proceso de migración?
3. Impacto
4. Soluciones: Extensión
5. Plan de migración

Cambio de filosofía entre versiones

- Validación de certificados:
  - Gestión de prestadores de certificados y tipos de certificados.
  - Políticas de certificación.
  - Métodos de validación de certificados.
  - Extracción de información de certificados.
- Sistema de custodia:
  - Manipulación de documentos.
  - Generación y custodia de transacciones de firma.
- Generación de firmas:
  - Evolución de formatos.
  - Generación de estructuras de firmas en cliente.
  - Realización de firmas de páginas Web (What You See Is What You Sign)
- Comunicación con la plataforma.

1. ¿Por qué es aconsejable migrar a @Firma v5?
2. ¿Por qué un proceso de migración?
3. Impacto
4. Soluciones: Extensión
5. Plan de migración

Sobre el proceso de adaptación

- Compatibilidad servicios publicados por la plataforma:
  - Autenticación Web.
  - Firma y multifirma masiva de páginas Web.
  - Interfases de servicios comunes a ambas versiones.
  - Protocolos de comunicación de aplicaciones.
  - Securización e interoperabilidad de los servicios Web.
- Sistema de custodia:
  - Transacciones de firma de ficheros.
  - Transacciones de firma de páginas Web.
  - Datos Notario electrónico.
- Formatos de firma.
- Estructuras electrónicas de firma que albergan sellos de tiempos conforme al estándar RFC 3161.
- Componentes software base.

Sobre el entorno de ejecución

- Componente Fachada de Comunicaciones:
  - Fachada de firma de páginas Web.
  - Servidor SSL de Autenticación Web.
- Comunicación entre componentes.
- Prestaciones en servidores que alojan el núcleo.
- Incorporación de elementos hardware para asegurar la alta disponibilidad de la plataforma.

Sobre la gestión de la plataforma

- Herramienta de Administración:
  - Parámetros de aplicaciones:
    - Autenticación Web.
    - Firma de ficheros.
  - Parámetros de páginas Web firmables.
  - Parámetros de multifirmas masivas de páginas Web.
  - Sincronización de aplicaciones.
- Utilidades de generación de claves simétricas.
- Tareas programadas.
- Otros aspectos configurables.

Sobre las aplicaciones cliente

- Interfases publicadas:
  - Métodos obsoletos.
  - Métodos no compatibles.
- Cliente de firma:
  - Librerías utilizadas.
  - Ficheros de script.
- Librerías de comunicación con núcleo de la plataforma.
- Uso de Subjects en componentes clientes del servicio de autenticación Web.

1. ¿Por qué es aconsejable migrar a @Firma v5?
2. ¿Por qué un proceso de migración?
3. Impacto
4. Soluciones: Extensión
5. Plan de migración

Plataforma @Firma v5 – Extensión Junta de Andalucía (I)

- Incorpora los elementos arquitectónicos no presentes en @Firma v5:
  - Servidor SSL de Autenticación Web.
  - Fachada de firma de páginas Web.
- Incorpora elementos software para mantener la compatibilidad hacia atrás, respecto a los servicios ofrecidos:
  - Interfases de servicios Web.
  - Interfases RMI-IIOP.
  - Tipos de datos.
  - Componentes clientes.
  - Componentes descargables.
- Incorpora las estructuras de base de datos necesarias para mantener la compatibilidad:
  - Notario Electrónico Junta de Andalucía.
  - Transacciones de firma de páginas Web.

Plataforma @Firma v5 – Extensión Junta de Andalucía (II)

- Incorpora los elementos de administración necesarios.
- Aporta elementos de adaptación:
  - Configuración de la administración de la plataforma.
  - Sistema de Custodia.
- Permite una adaptación progresiva de las aplicaciones a @firma v5.
- Actualiza y adapta los componentes software en los que se apoya la plataforma.

1. ¿Por qué es aconsejable migrar a @Firma v5?
2. ¿Por qué un proceso de migración?
3. Impacto
4. Soluciones: Extensión
5. Plan de migración

Aspectos a tener en cuenta antes de migrar

- Disponibilidad de elementos hardware.
- Disponibilidad de varios entornos de ejecución.
- Sobre el Sistema de Custodia:
  - Versión del gestor de base de datos Oracle a utilizar.
  - Tipo de transacciones de firma almacenadas.
  - Volumen de información almacenado.
  - Crecimiento del sistema de Custodia.
  - Tiempo de parada de servicio máximo permisible.
- Sobre las aplicaciones clientes:
  - Número de aplicaciones.
  - Funcionalidades utilizadas.
  - Comunicación con la plataforma.

Proceso de migración (I)

1. Despliegue plataforma @Firma v5
   a. Instalación de componentes hardware y configuración de la arquitectura de red.
   b. Instalación de componentes software:
      - Núcleo de la plataforma.
      - Sistema de Custodia.
   c. Importación/Creación de una Política de Certificación básica.

2. Despliegue de la Extensión
   a. Instalación de componentes hardware y configuración de la arquitectura de red.
   b. Instalación de componentes software:
      - Extensión del núcleo de la plataforma.
      - Extensión del sistema de Custodia.
      - Fachada de comunicaciones.

Proceso de migración (II)

3. Ejecución del componente de adaptación de configuración de administración de la plataforma.

4. Ejecución del proceso de migración del sistema de Custodia.

5. Ejecución del plan de pruebas.

6. Paso a producción.

Ruegos y Preguntas