Migración de la plataforma @firma versiones 4.x a versión 5.0
Consejería de Justicia y Administración Pública

Documento nº:	TI-20-1074-PlMigr_CJAP
Revisión:	004
Fecha:	12/01/2006
Período de retención:	Permanente durante su período de vigencia + 3 años después de su anulación

Control de Comprobación y Aprobación

Documento nº:	TI-20-1074-PlMigr_ CJAP
Revisión:	004
Fecha:	02-05-2006

Realizado

02-05-2006

Pedro Luis
Alvarez-Ossorio
Torres
Analista Firma Electrónica

Comprobado

02-05-2006

José Antonio	Carlos
Márquez	Gómez
Contreras	Pérez
Director Técnico @firma	Jefe de Proyecto

Aprobado

José Antonio	Carlos

Márquez	Gómez
Contreras	Pérez
Director Técnico @firma	Jefe de Proyecto

Control de Modificaciones

Documento nº: TI-20-1074-PlMigr_ CJAP

Revisión: 004

Fecha: 12/01/2007

Rev. 1

Fecha 02/05/2006

Autor/es Pedro Luis Álvarez – Ossorio

Descripción Documentación inicial

Rev. 2

Fecha 23/10/2006

Autor/es Pedro Luis Álvarez – Ossorio, José Angel Román

Descripción Se ha actualizado el estado actual de la plataforma con las modificaciones realizadas desde la fecha de la primera versión.

Se ha ajustado la propuesta de arquitectura a las necesidades de la Consejería de Justicia y Administración Pública.

Se ha completado el plan de migración con nuevos items aparecidos y un desarrollo mas exaustivo de los existentes.

Se ha incorporado el impacto de la migración sobre la plataforma de firma existente.

Rev. 3

Fecha 05/01/2007

Autor/es Pedro Luis Álvarez – Ossorio

Descripción	Se incorpora al apartado de impacto de migración sobre la plataforma de firma existente el listado de aplicaciones en el entorno de producción que deben modificar su generador de Subject a GeneradorSubjectGenericoJA. Se incorpora al apartado de impacto de migración sobre la plataforma de firma existente los listados de clases y métodos que se encuentran obsoletos y eliminados por interfaz públicada. Se incorpora un nuevo apartado en el que se detalla la configuración de la plataforma en alta disponibilidad.

Rev.	4
Fecha	12/01/2007
Autor/es	Pedro Luis Álvarez – Ossorio
Descripción	Se incorpora al apartado de impacto de migración sobre la plataforma de firma existente la inclusión del SubjectGenerico para recuperar información sobre procesos de validación de certificados del prestador de servicios de certificación FNMT y el tratamiento del mismo.

Rev.	5
Fecha	23/04/2007
Autor/es	Pablo Pizarro Armendáriz
Descripción	Se ajusta el documento a los impactos producidos en la migracion de la plataforma.

Control de Distribución

Documento nº: TI-20-1074-PlMigr_ CJAP

Revisión: 005

Fecha: 23/04/2007

Copias Electrónicas:

La distribución de este documento ha sido controlada a través del sistema de información.

Copias en Papel:

La vigencia de las copias impresas en papel está condicionada a la coincidencia de su estado de revisión con el que aparece en el sistema electrónico de distribución de documentos.

El control de distribución de copias en papel para su uso en proyectos u otras aplicaciones es responsabilidad de los usuarios del sistema electrónico de información.

Fecha de impresión 02/05/2006

Distribución en Papel:

Nombre o Cargo y (Organización)	Nº de Ejemplares	Referencia de la carta de transmisión y fecha

Índice

1. Impacto de la migración

En este apartado se recoge el impacto que tendrá el proceso de migración sobre la plataforma de firma existente en la Consejería de Justicia y Administración Pública de la Junta de Andalucía.

1.1 Impacto a nivel de arquitectura.

A nivel de arquitectura el único impacto se encuentra en las maquinas encargadas de alojar el núcleo de la plataforma. Estas maquinas están descritas en la propuesta de arquitectura de la plataforma junto con el resto de componentes hardware.

1.2 Impacto a nivel funcional.

1.2.1 Impacto sobre las interfaces publicadas

En esta nueva versión de @firma se eliminarán aquellas clases y aquellos métodos obsoletos, y que habían caído en desuso, publicados en las interfaces ofrecidas por las versiones 4.x de la plataforma. De la misma forma, se declararán como obsoletos aquellos métodos o clases que se prevén que caigan en desuso en futuras versiones.

1.2.1.1 Clases obsoletas o eliminadas

En este apartado se enumeran las diferentes clases que han sido declaradas como obsoletas o han sido eliminadas para cada una de los interfaces publicadas por la plataforma en versiones anteriores.

Las clases que han sido declaradas como obsoletas son las siguientes:

- Módulo de Autenticación:
    - com.telventi.autenticacion.Subject
    - com.telventi.autenticacion.SubjectGenerico
    - com.telventi.autenticacion.SubjectGenericoJA

Las clases que desaparecen son:

- Módulo de Autenticación:
    - com.telventi.autenticacion.FabricaGeneradoresSubject
    - com.telventi.autenticacion.GeneradorSubject
    - com.telventi.autenticacion.GeneradorSubjectGenerico
    - com.telventi.autenticacion.GeneradorSubjectGenericoJA
    - com.telventi.autenticacion.x509validacion.VerifCert

1.2.1.2 Mótodos obsoletos y eliminados

En este apartado se enumeran los diferentes métodos que han sido declarados como obsoletos o se han eliminado para cada una de los interfaces publicadas por la plataforma en versiones anteriores.

Los métodos que han sido declarados como obsoletos son los siguientes:

- Módulo Custodia
    - Interfaz com.telventi.custodia.CustodiaDocumentosFacade
        - addDocumento
        - cambiarEstado
        - getDatosNotarioTransaccion
- Módulo de firma de páginas Web:
    - Interfaz com.telventi.ejb.FirmaAPIFacade:
        - getASN1EFE
        - getASN1AR
    - Interfaz com.telventi.ejb.MultiFirmaAPIFacade:
        - getASN1EFE
        - getASN1AR
- Módulo de firma masiva de páginas Web:
    - Interfaz com.telventi.multifirmamasiva.MultiFirmaWebMasiva:
        - getASN1EFE
        - getASN1AR

Por su parte, los siguientes métodos han sido eliminados de las interfaces a las que pertenecen:

- Módulo de firma de páginas Web:
    - Interfaz com.telventi.ejb.FirmaAPIFacade:
        - IsCertificateTrusted
        - IsCertificateNotExpired

- IsCertificateRevoked
- getListadoNIF

- Interfaz com.telventi.firma.data.AppData
  - getFormReference : este método ya devolvía en la versión 4 de @firma la cadena "OBSOLETO"

1.2.2 Impacto sobre el módulo Autenticación.

La nueva versión de @firma permite a las aplicaciones clientes configurar el mapeo de certificados de una forma mas dinámica y sencilla que las versiones anteriores, por lo que se dejarán de implementar nuevos Subjects y generadores de Subjects tras la migración, aconsejándose a las aplicaciones la utilización de las interfaces de @firma 5.0.

Por último, todas aquellas aplicaciones que hagan uso del generador de Subjects, GeneradorSubjectGenerico, sólo podrán validar certificados expedidos por FNMT.

Esto es así debido a que es difícil y tedioso mantener los mapeos de campos de certificado mediante los oid´s como lo hace GeneradorSubjectGenerico, desde el punto de vista de la administración. Y desde el punto de vista del desarrollo es poco intuitivo acceder a la información obtenida de un certificado a partir de sus oid´s.

Por lo que este tipo de Subject será generado a mediada mediante código, para los prestadores anteriormente mencionados, y no mediante las nuevas utilidades que ofrece @Firma 5.0.

Las aplicaciones en el entorno de producción implicadas son:

Aplicaciones que hacen uso del SubjectGenerico en el entorno de producción			
Lsr	cec-praut	webempleado_fgg	webempleado_desfun
coop	Aass	wfpo	cjem26e
coopi	pr-autx	cec	cecx
pasenIntranet	Sioca	sac	consultaexpertos
Scec	Sxcec	webempleado_desarrollo	gest_info_ciudadano
Info_ciudadano_int	info_ciudadano	autocitas	pasenInternet2
solicitudes_cjap	Solicitudes_cjap_int	sicess	sicess_int
autocitas_cice_int	consultaexpertos_cice	consultaexpertos_cice_int	itracker

cibs	cibs_des	becasfi	becasfiinterno
itrackerExt	premiosAEdes	itrackerWanda	itrackerWandaExt
supuestogobExt	id_admPROD	id_admPRODW	id_intranetPROD
sol_registro	QAM_Aut	intersas	sgo
res_ins	Patrimonio	WebModuloPublica	plutonDesc
safo_ext	RIIBP	sirhus	dssintegra
Dssintegradiscoverer	Alega	alegalogin	pro1APDE
crono_justicia_respaldo	Etc	etc_adm	id_intranet_prod
intranet_prueba_temp	Webempleado	Aassdes	pasenInternet
DSS_INTEGRA	dss_discoverer	pasenIntranet2	autocitas_cice
Supuestogob	crono_justicia	CarnetJoven	id_intranetPRODW
sgoWebUser	safo_int	dssintegragestion	faqAdmin
fassTAJ65_int			

1.2.3 Impacto sobre el Notario Electrónico de la Junta de Andalucía.

Para que una TSA pueda ser integrada en la plataforma de firma debe cumplir el estándar definido por la Internet Engineering Task Force (IETF) para el protocolo Time Stamp descrito en su RFC 3161 "Internet X.509 Public Key Infrastructure Time Stamp Protocols ", de esta forma, @firma podrá utilizar distintas TSAs que sigan dicho estándar.

Es importante tener en cuenta que la TSA deberá suministrar un componente a través del cual se producirá la comunicación entre la plataforma @firma y el Servidor TSA.

La política de firma y el cliente de Notario Electrónico (cliente TSA) utilizados en la plataforma @firma 4.0 no cumple los requisitos necesarios para su implantación en @firma 5.0 en los siguientes puntos:

- El cliente TSA que realiza las peticiones y el componente de comunicación con la TSA está integrado en un único componente. Estos componentes han de estar separados para cumplir con el escenario de integración de @firma y no ligar la plataforma de firma a una integración concreta de TSA.

- La verificación del TimeStampToken la realiza el servidor de TSA en lugar del cliente TSA, incumpliendo el protocolo Time Stamp estándar (RFC 3161).

- La Estructura de Firma Electrónica (EFE) es propietaria de la Junta de Andalucía y no cumple con el estándar (RFC 3161).

- Según la política de firma Electrónica de la Junta de Andalucía, la TSA realiza un sellado de tiempo sobre la estructura EFData, no sobre el CMS original, con lo que no sería un TimeStampToken válido para incluir en el CMS.

1.2.4 Impacto sobre el módulo Firma de fichero.

Las estructuras de firma generadas por la plataforma @firma 5.0 difieren de las estructuras generadas en la versión anterior.

Las transacciones de firma que se efectúen tras la migración se realizarán por el núcleo de la plataforma @firma 5.0 por lo tanto seguirán las estructuras de firma generadas en esta versión.

La multifirma de alguna estructura distinta a las de @firma 5.0, daría lugar a la generación de una estructura de firma no homogénea y por lo tanto no válida.

Además, no se generarán nuevas estructuras EFE y AR (ver apartado 1.2.2).

1.2.5 Impacto sobre el módulo Firma de Páginas Web

En el módulo de Firma de Paginas Web se han identificado los siguientes aspectos a tener en cuenta:

- Capa de persistencia objeto/relacional. Para conservar la homogeneidad con la empleada por la versión 5.0, se ha adaptado la utilizada por este módulo al nuevo modelo.

- Estructuras de firma. Las nuevas estructuras de firma que se generen se verán modificadas, al igual que ocurría en la firma de ficheros, en aquellas transacciones de firma que deben incorporar un sello de tiempo (TimeStampToken) para poder respetar los estándares establecidos a tal efecto.

- Política de TimeStamp. Las firmas generadas desde este módulo seguirá la misma política de TimeStamp que la plataforma @firma 5.0, por lo que no se generarán nuevas estructuras EFE y AR (ver apartado 1.2.2).

- Validación de firmas. Para las nuevas firmas generadas se verificará el sello de tiempo en caso de tener activada la política de Timestamp la aplicación a la cual pertenece dicha transacción de firma.

1.2.6 Impacto sobre el módulo Sistema de Custodia

Se conservará en el Sistema de Custodia las estructuras EFE y AR generadas por las versiones anteriores de la plataforma de firma a modo de consulta.

1.2.7 Impacto sobre el módulo de Administración

La administración de la plataforma se realizará a través de la herramienta de administración de @firma 5.0 a la que se añadirá una extensión para gestionar aquellos parámetros existentes en versiones anteriores y no contemplados en la nueva versión de la plataforma.

1.2.8 Impacto sobre la fachada de comunicaciones Web.

No se ha detectado ningún punto crítico en la migración.

1.3 Impacto en componentes clientes.

Las aplicaciones clientes deben utilizar los componentes clientes implementados para la migración y que se suministrarán en el despliegue de la plataforma.