Cambios y Novedades de Integr@

1.2.2_002 - 2.2.3_001

Documento nº:	@Firma-Integr@-CambiosYNovedades-MAN
Revisión:	020
Fecha:	14-10-2022
Período de retención:	Permanente durante su período de vigencia + 3 años después de su anulación

CONTROL DE MODIFICACIONES

Documento nº:	@Firma-Integr@-CambiosYNovedades-MAN
Revisión:	020
Fecha:	14-10-2022

Rev.	001
Fecha	12-02-2015
Descripción	Documento inicial.

Rev.	002
Fecha	19-05-2015
Descripción	Se añaden los cambios y novedades para la versión 1.3.0_002.

Rev.	003
Fecha	30-07-2015
Descripción	Se añaden los cambios y novedades para la versión 1.3.0_003.

Rev.	004
Fecha	09-03-2016
Descripción	Se añaden los cambios y novedades para la versión 2.0.0_000. Se modifica el tipo de letra del documento de Frutiger a Calibri.

Rev.	005
Fecha	09-03-2016
Descripción	Se añaden los cambios y novedades para la versión 2.1.0_000.

Rev.	006
Fecha	15-03-2016
Descripción	Se añade la fachada de los servicios de comunicación por DSS con TS@.

Rev.	007
Fecha	29-03-2016
Descripción	Se añade la funcionalidad de extracción de Datos Firmados.

Rev.	008
Fecha	18-04-2016
Descripción	Se modifica la gestión de ficheros de propiedades.

Rev.	009
Fecha	28-04-2016
Descripción	Se añade la funcionalidad de generar multi-firmas PAdES (Baseline o no) y generar firmas y multi-firmas PAdES (Baseline o no) con rúbrica.

Rev.	010
Fecha	23-06-2016
Descripción	Se añade la funcionalidad de generación de firmas ASiCs Baseline conteniendo una firma CAdES Baseline o una firma XAdES Baseline. Corrección de errores.

Rev.	011
Fecha	29-12-2016
Descripción	Se añaden todos los aspectos que faltaban para la versión 2.1.0_000.

Rev.	012
Fecha	20-04-2017
Descripción	Se añaden todos los aspectos que faltaban para la versión 2.2.0_000.

Rev.	013
Fecha	16-10-2017
Descripción	Se añaden todos los aspectos que faltaban para la versión 2.2.1_000 pero indicando los cambios producidos desde la última versión publicada en el Portal de Administración Electrónica, la 1.2.2_002.

Rev.	014
Fecha	18-11-2019
Descripción	Se añaden los cambios realizados relacionados con los nuevos elementos ReturnNextUpdate y ProcessAsNotBaseline.

Rev.	015
Fecha	22-12-2020
Descripción	Se añaden los cambios incluidos en la versión 2.2.2_000.

Rev.	016
Fecha	22-02-2022
Descripción	Se añaden los cambios incluidos en la versión 2.2.2_001.

Rev.	017
Fecha	12-04-2022
Descripción	Se añaden los cambios incluidos en la versión 2.2.2_002.

Rev.	018
Fecha	27-09-2022
Descripción	Se añaden los cambios incluidos en la versión 2.2.3_000.

Rev.	019
Fecha	07-10-2022
Descripción	Se añaden los cambios incluidos en la versión 2.2.3_001.

Rev.	020
Fecha	14-10-2022
Descripción	Actualizado cambios incluidos en la versión 2.2.3_001 y homogeneiza los estilos.

CONTROL DE DISTRIBUCIÓN

Documento nº:	@Firma-Integr@-CambiosYNovedades-MAN
Revisión:	020
Fecha:	14-10-2022

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

Distribución en Papel:

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

Índice

1 Objeto 7

2 Alcance 8

3 Siglas y Acrónimos 9

4 Glosario de Términos y Definiciones 10

5 Documentos de Referencia 11

6 Introducción 12

7 Cambios y Novedades 13

7.1 Integr@ 2.2.3_001 13
7.1.1 Características 13
7.1.2 Errores Resueltos 13
7.2 Integr@ 2.2.3_000 13
7.2.1 Características 13
7.2.2 Errores Resueltos 13
7.3 Integr@ 2.2.2_002 13
7.3.1 Características 13
7.3.2 Errores Resueltos 14
7.4 Integr@ 2.2.2_001 14
7.4.1 Características 14
7.4.2 Errores Resueltos 14
7.5 Integr@ 2.2.2_000 14
7.5.1 Características 14
7.5.2 Errores Resueltos 15
7.6 Integr@ 2.2.1_000 15
7.6.1 Características 15
7.6.2 Errores Resueltos 20

1 Objeto

Es objeto de este documento describir el conjunto de cambios, novedades y correcciones aplicadas desde una versión concreta de Integr@ hasta la indicada.

2 Alcance

El presente documento contempla los siguientes objetivos:

- Definir las características principales evolucionadas en la API Integr@.
- Definir las funcionalidades que componen la API.
- Describir las correcciones llevadas a cabo.

3 Siglas y Acrónimos

MINHAP	Ministerio de Hacienda y Administraciones Públicas de España
XML	eXtensible Markup Language
ASN.1	Abstract Syntax Notation One
PDF	Portable Document Format
XAdES	XML Advanced Electronic Signatures
CAdES	CMS Advanced Electronic Signatures
PAdES	PDF Advanced Electronic Signatures
OCSP	Online Certificate Status Protocol
RFC	Request For Comments
HSM	Hardware Security Module
UTF-8	8-bit Unicode Transformation Format
JRE	Java Runtime Environment
DSS	Digital Signature Services
SOAP	Simple Object Access Protocol
CAdES-BES	CAdES Basic Electronic Signature
CAdES-EPES	CAdES Explicit Policy Electronic Signature
CAdES-T	CAdES Timestamp
XAdES-BES	XAdES Basic Electronic Signature
XAdES-EPES	XAdES Explicit Policy Electronic Signature
XAdES-T	XAdES Timestamp
PAdES-BES	PAdES Basic Electronic Signature
PAdES-EPES	PAdES Explicit Policy Electronic Signature
PAdES-LTV	PAdES Long Term Validation
CAdES B-Level	CAdES Basic Level
CAdES T-Level	CAdES Trusted Time for Signature Existence Level
XAdES B-Level	XAdES Basic Level
XAdES T-Level	XAdES Trusted Time for Signature Existence Level
PAdES B-Level	PAdES Basic Level
PAdES T-Level	PAdES Trusted Time for Signature Existence Level
ASiC	Associated Signature Containers
ASiC-S	Simple Associated Signature Containers
ENI	Esquema Nacional de Interoperabilidad

4 Glosario de Términos y Definiciones

TS@	Plataforma de Sellado de Tiempo
@Firma	Plataforma de Validación y Firma Electrónica

5 Documentos de Referencia

- Documento @Firma-Integr@-MAN, Manual de Uso de Integr@.

6 Introducción

El presente documento recoge la lista de cambios y novedades que se han producido desde la versión 1.2.0_002 de Integr@ hasta la versión 2.2.3_001.

7 Cambios y Novedades

7.1 Integr@ 2.2.3_001

7.1.1 Características

- Actualización y homogeneización de dependencias.

7.1.2 Errores Resueltos

- Se corrige el paquete de despliegue y la documentación incluyendo las dependencias reales de cada una de las librerías de integra.
- Se incluye una serie de propiedades en el fichero “tsaApp.properties” que eran requeridas para la integración WS con TS@.

7.2 Integr@ 2.2.3_000

7.2.1 Características

- Cuando se indica el método de canonización de la firma XAdES, se utiliza este mismo método para la transformación de los datos XML. Si no se indica nada, se mantiene el comportamiento anterior.
- Se adapta el desarrollo para la compatibilidad con las RFC 5035 y 5816.
- Se sustituye la utilización de la dependencia JCE de IAIK por la JCE de BouncyCastle.

7.2.2 Errores Resueltos

- Se corrige que en las firmas baseline se utilizase una transformación XML en lugar de la Base 64 cuando los datos son binarios.

7.3 Integr@ 2.2.2_002

7.3.1 Características

- Evolución de la versión de la librería de gestión de logs a Log4j2.
- Adaptación de la configuración para el uso de Log4j2.
- Eliminar referencias a la librería slf4j.

7.3.2 Errores Resueltos

- Se corrige discrepancia en el nombre de la variable de configuración que indica la contraseña del almacén de confianza (JKS) para conexiones seguras. Esta variable, presentaba una variación en una letra mayúscula entre el nombre indicado en el fichero "integra.properties" y el valor esperado dentro del código.

7.4 Integr@ 2.2.2_001

7.4.1 Características

- Adaptación de la librería integra-tsl.jar para su integración con @firma.
- Se modifica la lógica para que en los casos en los que no tenga definida la extensión AdditionalServiceInformation, se compruebe la cualificación del certificado en base al contenido del certificado.
- Se añaden nuevas trazas de logs en el procesado de validación de un certificado frente una TSL.

7.4.2 Errores Resueltos

- Se corrige bug detectado en la validación de certificados de sello de tiempo.

7.5 Integr@ 2.2.2_000

7.5.1 Características

- Se realiza la evolución de las librerías de servicios de Axis 1.4 a Axis 2 (versión 1.7.9).
- Se añade la funcionalidad de permitir la generación de firmas locales en formato CAdES a partir de hash.
- Se añade una nueva funcionalidad que permite el cálculo de la fecha de expiración de las firmas en las operaciones de validación en Integr@.
- Se mejora la generación de XAdES Manifest para permitir la inclusión de varios elementos "ds:Reference" en una misma estructura "ds:Manifest".
- Se incluye en Integr@ un nuevo módulo para la generación de informes de firmas a partir de las plantillas utilizadas en el Sistema eVisor.
- Incluido nuevo módulo que permite la validación de certificados frente a las listas de confianza de prestadores de servicios electrónicos de confianza (TSL).

7.5.2 Errores Resueltos

- Se elimina la opción de enviar peticiones a través de web services con Chunked.
- Se mejoran los mensajes de error devueltos por los servicios de Integr@ para dar más detalles sobre el problema producido.
- Se corrige error en la gestión de los providers de seguridad de Java durante la detección de formatos de firma en peticiones a través de web services.
- Cuando Integr@ intentaba comunicarse con la plataforma eVisor mediante web services con autenticación por certificado, se producía un error en eVisor debido a que el componente Axis de Integr@ no estaba linealizando correctamente la petición.
- Se soluciona bug que provocaba un error durante la generación de los objetos de respuesta en actualizaciones de firmas XAdES. El problema estaba en que no se buscaba correctamente el elemento 'ds:Signature' en la lista de elementos devueltos por la plataforma @firma.
- Se corrige bug que provocaba una recuperación incorrecta de los contrafirmantes de una firma CAdES.
- Se corrige bug que impedía la correcta recuperación de la fecha de generación de los sellos de tiempo XML en firmas XAdES.

7.6 Integr@ 2.2.1_000

7.6.1 Características

- Se añade una fachada de invocación para facilitar a las aplicaciones la integración con los servicios de @firma.
- Se añade una utilidad que permite detectar el formato de firmas XML, ASN.1 y PDF.
- Se incluye la funcionalidad de generación de firma en los formatos XAdES-T, CAdES-T y PAdES-T.
- Se añade la funcionalidad de actualizar firmas CAdES, XAdES y PAdES, esto es, añadir un sello de tiempo a aquellos firmantes que carezcan del mismo.
- Se añade un servicio de obtención de sello de tiempo desde TS@ para los procesos de generación y de actualización de firmas.
- Se añade la funcionalidad para validar firmas PAdES y PDF.

- Se incorpora la validación de la firma del sello de tiempo para los procesos de generación, actualización y validación de firmas.

- Se añade un cliente OCSP que permite la validación de certificados contra servidores OCSP según los estándares RFC 5019 y RFC 2560.

- Se incorpora la posibilidad de validar el certificado firmante de los sellos de tiempo para los procesos de generación, actualización y validación de firmas mediante comunicación con un servidor OCSP.

- Se añade una fachada de invocación para facilitar la generación y validación de firmas electrónicas.

- Se incorpora integración con HSM que permite obtener certificados y claves privadas de los mismos.

- Se añade la funcionalidad de generar y validar firmas con políticas de firma en base a un fichero de propiedades que contiene toda la información asociada a dichas políticas de firma.

- Se actualiza la funcionalidad de validación de firmas de manera que ahora ofrece toda la información asociada a la validación de cada uno de los firmantes que componen la firma.

- Se añade la posibilidad de definir el tipo de firma PAdES a generar, esto es, “certified” o “approval”.

- Se incorpora la funcionalidad que permite validar estructuralmente un sello de tiempo antes de que sea enviado al servicio de renovación de sello de tiempo de TS@, esto, comprobar si el documento de entrada incorporado en la petición de renovación de sello de tiempo es correcto.

- Se incorpora la funcionalidad que permite validar un sello de tiempo antes de que sea enviado al servicio de renovación de sello de tiempo de TS@ enviándolo al servicio de validación de sello de tiempo de TS@.

- Se ha añadido una propiedad al fichero **policy.properties** para indicar los modos de firma permitidos para cada tipo de firma, sólo aplicable a las firmas ASN.1 y XML.

- Se ha definido un nuevo archivo de propiedades, **ocsp.properties**, donde ubicar las propiedades de comunicación con el servidor OCSP. Además, se ha generado una clase de tests para el cliente OCSP.

- Se ha añadido PAdES-Basic como formato válido en la generación de firmas en documentos PDF, si bien, sólo se permite la generación de dicho formato desde la interfaz **es.gob.afirma.signature.Signer**, no desde la clase **es.gob.afirma.integraFacade.IntegraFacade**.

- Se ha añadido la validación del sello de tiempo para los procesos de firma, co-firma, contra-firma y actualización de XAdES, así como para los procesos de actualización de PAdES.

- Se han definido los niveles de validación de certificados como 3, así, el nivel 0 equivale a la no validación, el nivel 1 a la validación simple, y el nivel 2 a la validación completa. Para el caso de operaciones de actualización, siempre se llevará a cabo la validación, es decir, que, si el nivel indicado es 0 o 1 se hará la validación siempre, y si el nivel indicado es 2 se hará la validación completa.

- En el fichero **policy.properties** se sustituye la propiedad que indicaba la ruta completa al documento legible de la política de firma por otra que indica el valor del hash de la política de firma.

- Se ha modificado el mensaje de log que indicaba el modo de la firma a co-firmar por un mensaje donde se expresa que el modo de firma de la co-firma XAdES será el mismo que el de la firma a co-firmar.

- Se ha añadido un mensaje de log al inicio del método de contra-firma para XAdES donde se especifica que, según el estándar XAdES, el modo de firma para todas las contra-firmas será *detached*.

- El fichero de propiedades **integraFacade.properties** se modifica y asigna para ser usado únicamente para la fachada de servicios propios **IntegraFacade**, y se crea un nuevo fichero de propiedades **signer.properties** para su uso exclusivo por la interfaz **Signer**.

- Se verifica compatibilidad con la JRE 1.7 de java.

- Se realizan cambios para que se permita realizar firmas enviando el resumen del documento utilizando el servicio DSS de @firma.

- Se realizan cambios para permitir enviar la firma en la petición para los servicios DSS de co-firma y contra-firma sobre @firma.

- Se añaden las plantillas XML asociadas al servicio de obtención de firmas registradas de @firma.

- Se divide Integr@ funcionalmente, dando lugar a 7 componentes que permiten 5 tipos de integración diferentes.

- Se añade la posibilidad de modificar dinámicamente la propiedad configurable en el fichero afirma5ServiceInvoker.properties que especifica si se cachean o no las respuestas de validación de certificados contra @firma.

- Se añade la generación de firmas, co-firmas y contra-firmas CAdES Baseline en sus formatos B-Level y T-Level, con y sin política de firma, mediante la interfaz **Signer** y la Fachada de Firma.

- Se añade la generación de firmas, co-firmas y contra-firmas XAdES Baseline en sus formatos B-Level y T-Level, con y sin política de firma, mediante la interfaz **Signer** y la Fachada de Firma.

- Se añade la generación de firmas PAdES Baseline en sus formatos B-Level, con y sin política de firma, mediante la interfaz **Signer** y la Fachada de Firma.

- Se añade la actualización de firmantes de una firma CAdES Baseline añadiéndoles un sello de tiempo a cada uno de ellos, siempre que no lo tuviera anteriormente, mediante la interfaz **Signer** y la Fachada de Firma.

- Se añade la actualización de firmantes de una firma XAdES Baseline añadiéndoles un sello de tiempo a cada uno de ellos, siempre que no lo tuviera anteriormente, mediante la interfaz **Signer** y la Fachada de Firma.

- Se añade la inclusión de un diccionario de sello de tiempo a un documento PDF según el estándar PAdES Baseline, mediante la interfaz **Signer** y la Fachada de Firma.

- Se añade la validación de firmantes de una firma CAdES Baseline mediante la interfaz **Signer** y la Fachada de Firma.

- Se añade la validación de firmantes de un documento XML que contiene firmas XAdES Baseline mediante la interfaz **Signer** y la Fachada de Firma.

- Se añade la validación de firmantes de un documento PDF que contiene firmas PAdES Baseline mediante la interfaz **Signer** y la Fachada de Firma.

- Se añade la validación de la estructura y la firma XAdES Baseline o CAdES Baseline contenida dentro de una firma ASiC-S mediante la interfaz **Signer** y la Fachada de Firma.

- Se añade la actualización de firmantes de una firma XAdES Baseline o CAdES Baseline contenida dentro de una firma ASiC-S mediante la interfaz **Signer** y la Fachada de Firma.

- Se modifica la generación de firmas PAdES de manera que ahora, por defecto, las firmas se generan de tipo “approval” y no “certified”.

- Se añade al detector de formatos una funcionalidad para determinar si una firma es ASiC-S.

- Se añade la funcionalidad de indicar con una variable en las opciones de arranque de la máquina virtual de java la ruta donde se ubican los ficheros de configuración.

- Se añade una nueva funcionalidad para poder realizar el cifrado y descifrado de un conjunto de datos tanto simétrica como asimétricamente, indicando el algoritmo que se quiere utilizar y los datos a cifrar o descifrar. Los algoritmos que se pueden utilizar son:

    - Algoritmos de cifrado simétrico: AES, Camellia, 3DES, DES y Blowfish.

- Algoritmos de cifrado asimétrico: RSA-OAEP y RSA-PKCS#1.

- Se añade la fachada de los servicios de comunicación por DSS con TS@. Los diferentes servicios a los que se pueden acceder son:
  - Servicio de Sellado (Timestamp).
  - Servicio de Validación (VerifyTimestamp).
  - Servicio de Resellado (RenewTimestamp).

- Se añade en la interfaz **Signer** y en la fachada de servicios **IntegraFacade**, una nueva funcionalidad para poder extraer los datos originalmente firmados. Esta funcionalidad sólo está disponible para firmas PAdES (Baseline o no), CAdES (Baseline o no) y ASiC-S.

- Se modifica la gestión de los ficheros de propiedades.

- Se añade en la interfaz **Signer** y en la fachada de servicios **IntegraFacade**, una nueva funcionalidad para poder generar multi-Firmas PAdES (Baseline o no).

- Se añade en la interfaz **Signer** y en la fachada de servicios **IntegraFacade**, una nueva funcionalidad para poder generar firmas y multi-firmas PAdES (Baseline o no) con rúbrica.

- Se añade nuevo módulo que ofrece los servicios de integra a través de un servicio web.

- Se añade una nueva funcionalidad para poder generar firmas ASiC-S Baseline conteniendo una firma CAdES Baseline o XAdES Baseline.

- Se incorpora la funcionalidad que permite especificar el algoritmo de canonicalización que usar en la generación de firmas XAdES (Baseline o no) desde la interfaz **Signer**.

- Se establece como algoritmo de canonicalización por defecto para la generación de firmas XAdES (Baseline o no) aquella compatible con la especificación XML de Documento Electrónico según ENI, esto es, http://www.w3.org/2001/10/xml-exc-c14n#.

- Se actualizan los procesos de validación de firmas para que ofrezcan una información más detallada de las validaciones llevadas a cabo, así como de los firmantes y sellos de tiempo que componen cada firma.

- Se elimina la obligatoriedad de indicar el identificador de aplicación cliente en las peticiones de sello de tiempo mediante servicios RFC-3161.

- Se verifica compatibilidad con la JRE 1.8 de java.

- Se añade la posibilidad de indicar el nivel de validación de certificados a la hora de realizar una petición DSS de Validación de Firma a @firma.

- Se ha modificado la generación de firmas para que se permita incorporar un elemento **SignerRole** con más de un elemento **ClaimedRole**.

- Se ha modificado la validación de firmas para que se permita incorporar un nuevo elemento **ReturnNextUpdate** dentro de OptionalInputs. Dicho elemento permite solicitar a la plataforma la fecha de expiración de la firma.

- Se ha modificado la validación y actualización de firmas para que se permita incorporar un nuevo elemento **ProcessAsNotBaseline** dentro de OptionalInputs. Dicho elemento permite forzar a la plataforma a procesar la petición como no baseline, independientemente de la propia configuración de @Firma.

7.6.2 Errores Resueltos

- Se soluciona la incidencia 67851, según la cual no se generaban correctamente firmas XAdES cuando existían caracteres especiales (tildes). Se modifica el código para forzar que siempre se codifique en UTF-8 y se fuerce así la correcta codificación.

- Se soluciona la incidencia 67306, según la cual si se ejecuta Integr@ con la versión 1.5 de la JRE su funcionamiento se producen errores. Además, se ha comprobado que Integr@ no es compatible con dicha JRE, por lo que se modifica el manual para indicar que sólo es compatible con la JRE 1.6.

- Se soluciona un error por el cual, a la hora de obtener la propiedad que indica la contraseña a usar en la autenticación por usuario/contraseña contra la TS@ del archivo de propiedades estáticas, cogía el valor del usuario, por lo que mandaba peticiones a TS@ donde el usuario y la contraseña tenían el mismo valor.

- Se corrigen errores relativos a la obtención de información de las contra-firmas en CAdES y XAdES.

- Solucionados problemas de calidad y estilo en el código.

- Se soluciona un problema en la generación de firmas CAdES-EPES y PAdES-EPES relacionado con la manera de añadir el resumen de la política de firma, que se generaba codificada en Base64 cuando no era correcto.

- Se ha añadido en el JavaDoc de los métodos **es.gob.afirma.signature.Signer.coSign(byte[], byte[], String, PrivateKeyEntry, Properties, boolean, String, String)**, **es.gob.afirma.signature.Signer.counterSign(byte[], String, PrivateKeyEntry, Properties, boolean, String, String)**, **es.gob.afirma.integraFacade.IntegraFacade.generateCoSignature(byte[], byte[], String, PrivateKeyEntry)** y **es.gob.afirma.integraFacade.IntegraFacade.generateCounterSignature(byte[], String,**

PrivateKeyEntry) información acerca de que dichas funcionalidades no están permitidas para firmas PAdES.

- Se corrige un funcionamiento incorrecto en lo referente a la generación del elemento **SignedSignatureProperties** para una firma XAdES, y es que los elementos hijos no se añadían a la firma en el orden correcto.

- Se ha añadido una comprobación que evite la necesidad de hacer uso de un gestor documental para las invocaciones al servicio **DSSAfirmaSign**.

- Se resuelve la incidencia #131729, la cual indicaba que se producía un error si el proveedor de seguridad de BouncyCastle no había sido inicializado antes de utilizar el cliente OCSP para validación de certificados. Se ha añadido una inicialización estática del proveedor de manera que en la clase **es.gob.afirma.ocsp.OCSPClient** se comprueba si no está ya inicializado, en cuyo caso, se procede a inicializarlo.

- Se soluciona la incidencia #84381 por la cual, si se contra-firma una firma que posee sellos de tiempo, estos sellos de tiempo desaparecen. Ahora, los sellos de tiempo se mantienen.

- Se ha añadido una nota en el fichero de propiedades **tsaServiceinvoker.properties** para resaltar que, si se configura que no se debe validar el sello de tiempo antes de llevar a cabo un proceso de renovación de sello de tiempo, dicha actuación va en contra del estándar de OASIS.

- Se ha actualizado el JavaDoc de la interfaz **es.gob.afirma.signature.Signer**, y de la clase **es.gob.afirma.integraFacade.IntegraFacade** para indicar que, en el caso de PAdES, cuando se actualiza una firma, lo que se hace es añadir un diccionario de sello de tiempo y, por consiguiente, si la firma no tenía el formato PAdES-LTV previamente, pasa a tenerlo.

- Se corrige un error por el que, en ocasiones, no se generaba correctamente el mensaje de petición al servicio de validación de firmas DSS de @Firma (DSSAfirmaVerify) desde la fachada de invocación para firmas *enveloping*.

- Se soluciona la incidencia #150530 según la cual, el método **es.gob.afirma.utils.Base64Coder.isBase64Encoded(byte[])**, en ocasiones, determinada que cadenas de bytes que no estaban codificadas en Base64 sí lo estaban.

- Se corrige un error por el que, no se cerraban los recursos en la lectura de los ficheros de propiedades.

- Se corrige un error a la hora de validar las respuestas SOAP firmadas desde @firma.

- Se corrige un error a la hora de validar sellos de tiempo XML obtenidos desde TSA.

- Se corrige un error que no permitía validar firmas XAdES *Enveloped* añadiendo el documento original desde la fachada de servicios de @firma, en lo que respecta a la construcción de la petición de validación contra @firma.

- Se corrige la validación de atributos opcionales de firmas PAdES Baseline: Antes se consideraba que el atributo firmado *commitment-type-indication* no podía estar nunca presente, sin embargo, puede estar presente si la firma incluye el atributo firmado *signature-policy-id*.

- Se modifica el tratamiento de los mensajes de error asociados a propiedades no indicadas en los ficheros **ocsp.properties**, **signer.properties** e **integraFacade.properties**, ya que no se indicaba correctamente el nombre del fichero de propiedades que se estaba procesando respecto a la propiedad que falta o que tiene un valor incorrecto.

- Se corrige un error por el que no se incluía correctamente el resumen del documento legible de la política de firma en la generación de firmas ASN.1 con política de firma.

- Se corrige un error por el que en los procesos de contra-firma con sello de tiempo de una firma ASN.1 dicha contra-firma no se generaba.

- Se modifica el código donde a la hora de generar una firma XAdES Baseline se añadía una referencia al elemento **ds:KeyInfo** que no debe aparecer.

- Se corrige error en el que al generar una contrafirma XAdES Baseline aparecía el atributo **ObjectReference** del **DataObjectFormat** vacío.

- Se modifica el código para que al realizar una contrafirma XAdES, si en los parámetros adicionales no viene ninguno de los siguientes valores: **xades.dataFormatObjectDescription**, **xades.DataFormatObjectMime** o **xades.DataFormatObjectEncoding**, no aparezca el elemento **xades:SignedDataObjectProperties**.

- Se corrige error que ocasionaba en la generación de la petición del servicio **DSSVerify** al indicarle que retorne información sobre el sello de tiempo.

- Se modifica la manera de capturar excepciones en la clase **XAdESBaselineSigner** ya que se había definido en multi-catch y no es soportable por la JRE 1.6.

- Se modifica la manera de capturar excepciones en la clase **UtilsSignatureOp** ya que se había definido en multi-catch y no es soportable por la JRE 1.6.

- Se corrige un error que se producía al parsear las respuestas desde la fachada de servicios DSS de @Firma.

- Se soluciona un error por el que no se validaba correctamente firmas CAdES Baseline que contienen contra-firmantes con política de firma de la AGE 1.9. El error era que se indicaba que la contra-firma no era válida porque carecía del atributo **content-type** ya que se

procesaba el contra-firmante como si fuera un firmante principal. Se ha modificado el código para que el contra-firmante sea procesado como tal y no como firmante.

- Se modifica el modo de validar el núcleo de firma para una firma PAdES ya que se hacía uso de la librería **iText** pero internamente resultaba incompatible con la librería **Bouncycastle** que utiliza Integr@ (1.46) cuando se procesaba una firma cuyo firmante incluía al menos un atributo **signature-time-stamp**. Ahora, la validación del núcleo de firma para una firma PAdES no hace uso de la librería **iText**.

- Debido a una incompatibilidad entre la librería **iText** 2.2 y la librería **Bouncycastle** 1.46 respecto a identificadores de tipo OID ha sido necesario modificar el modo de validación del núcleo de firma ASN.1 para las firmas contenidas en diccionarios de firma de manera que ahora, para firmas PAdES, la validación del núcleo de la firma ASN.1 contenida no se delega a iText.

- Solucionado un bug asociado a la validación de los atributos **signature-time-stamp** para el firmante principal de la firma ASN.1 contenida en un diccionario de firma durante el proceso de validación de firmas PAdES (Baseline y No Baseline) por el que se producía un **NullPointerException**.

- Solucionado un problema asociado a acceder al elemento padre de un sello de tiempo XML contenido en una firma XAdES, ya que en determinados casos no se accedía al elemento que representaba el sello de tiempo XML como una firma XML, lo que provocaba un error al realizar el **unmarshall** del sello de tiempo XML.

- Se corrige un problema por el que en procesos de actualización de firmas XAdES, en determinadas ocasiones, no se accedía al certificado firmante lo que podía producir errores de tipo **NullPointerException**.

- Se corrige un mal funcionamiento por el que, a la hora de realizar una firma PAdES-Basic, se incluía el atributo **signing-certificate** o **signing-certificate-v2**, en función del algoritmo seleccionado, cuando dichos atributos no están permitidos por el estándar.

- Se soluciona un error por el que a la hora de validar una firma XAdES con política de firma si se indicaban elementos no firmados opcionales se procesaba la firma de manera que era obligatorio que tuviera el elemento **UnsignedSignatureProperties**, cuando debía considerarse como opcional.

- Se soluciona un problema asociado a la validación de firma en la clase **es.gob.afirma.integraws.ws.impl.AfirmaServices**.

- Se soluciona un problema asociado al proceso de los parámetros de una firma XML en la clase **es.gob.afirma.integraFacade.GenerateMessageRequest**.

- Se soluciona un problema asociado al servicio de firma Xades Enveloping en la clase **es.gob.afirma.utils.DSSTagsResponse**.

- Se soluciona un problema asociado a la validación de sello de tiempo en la clase **es.gob.afirma.integraws.ws.impl.TSAServices**.

- Se soluciona un problema asociado a la detección del formato de firma PAdES-Basic.

- Cuando se realiza una petición al servicio de validación de certificados por lote y la plataforma @firma devuelve un mensaje de error, la información de dicho error en lugar de incluirse en el elemento **es.gob.afirma.integraFacade.pojo.AsynchronousResponse.batVerCerRes** se incluía en el elemento **es.gob.afirma.integraFacade.pojo.AsynchronousResponse.batVerSigRes**. Se ha corregido el funcionamiento para que se incluya en el elemento adecuado.

- Se corrige un mal funcionamiento de la fachada de servicios de @firma y es que cuando se llevaba a cabo una petición al servicio de validación de certificados por lote no se recuperaban las respuestas individuales de validación para cada certificado.