Plan de pruebas del Cliente @firma

Índice de contenidos

[1 Introducción 3](#_Toc327453974)

[2 Definición del alcance de las pruebas 3](#_Toc327453975)

[3 Pruebas 5](#_Toc327453976)

[3.1 Módulos 5](#_Toc327453977)

[3.1.1 Afirma-core 5](#_Toc327453978)

[3.1.2 Afirma-core-keystores 5](#_Toc327453979)

[3.1.3 Afirma-core-massive 7](#_Toc327453980)

[3.1.4 Afirma-crypto-cades 29](#_Toc327453981)

[3.1.5 Afirma-crypto-cms 37](#_Toc327453982)

[3.1.6 Afirma-crypto-odf 45](#_Toc327453983)

[3.1.7 Afirma-crypto-ooxml 50](#_Toc327453984)

[3.1.8 Afirma-crypto-pdf 55](#_Toc327453985)

[3.1.9 Afirma-crypto-xades 62](#_Toc327453986)

[3.2 Applet Cliente @firma 72](#_Toc327453987)

[3.2.1 Pruebas funcionales de usuarios finales 72](#_Toc327453988)

# Introducción

En el presente documento se pretende definir e informar las pruebas que se realizan sobre el Cliente @firma para comprobar su corrección.

# Definición del alcance de las pruebas

Las pruebas son prácticas que se realizan en diversas fases de un proyecto con el fin de verificar:

* El correcto funcionamiento de los componentes del sistema.
* El funcionamiento correcto de las interacciones que se producen entre los subsistemas que componen el proyecto.
* Que el sistema cumple con el funcionamiento esperado.
* Que cambios en uno o más componentes no introducen comportamientos no deseados o errores evitables.

El Cliente @firma es un applet y debe ser ejecutado dentro de un navegador Web e integrado en un flujo de trabajo. Esta particularidad dificulta la automatización de las pruebas y obliga a la prueba manual del aplicativo.

Las funcionalidades de alto nivel objetivo de las pruebas serán:

* Firma electrónica:
  + Formatos: CAdES, XAdES, PAdES, CMS, XMLdSig, ODF y OOXML.
  + Algoritmos: MD2withRSA, MD5withRSA, SHA1withRSA, SHA256withRSA, SHA384withRSA, SHA512withRSA.
  + Modos: Implícito y Explícito.
* Multifirmas:
  + Cofirmas.
  + Contrafirmas:
    - Todos los nodos hojas.
    - Todos los nodos del árbol.
    - Nodos seleccionados.
    - Nodos de firmantes seleccionados.
* Sobres electrónicos:
  + Cifrados.
  + Envueltos.
  + Firmados y envueltos.
  + Autenticados y envueltos.
* Desenvoltura de sobres.
* Cifrado simétrico:
  + Con clave: AES, Alleged RC4, Blowfish, 3DES, DES y RC2.
  + Con contraseña: SHA1 con 3DES, SHA1 con RC2 y MD5 con DES.
* Descifrado simétrico:
  + Con clave: AES, Alleged RC4, Blowfish, 3DES, DES y RC2.
  + Con contraseña: SHA1 con 3DES, SHA1 con RC2 y MD5 con DES.

Adicionalmente, existen múltiples funciones para la configuración de cada una de las funcionalidades principales. Así mismo, el tipo de las entradas que reciban cada una de las funciones principales también determinarán su comportamiento.

Debido a la imposibilidad de realizar la prueba de todas estas funcionalidades sobre cada una de las combinaciones de entorno compatibles con el Cliente (distintas versiones y arquitecturas de sistema operativo, JVM y navegador web) se determinará un conjunto significativo de entornos, acotado por la compatibilidad entre ellos, sobre los que realizar las pruebas.

# Pruebas

## Módulos

### Afirma-core

#### Pruebas unitarias

##### Comprobación de versión de BouncyCastle

* Se busca una versión de BouncyCastle en el *path* del sistema del usuario. Si se encuentra, fallará el test ya que el cliente incorpora su propia versión y cualquier otra podría interferir en su funcionamiento.
* **Resultado esperado:** Se obtendrá null ya que no debe encontrarse ninguna versión de BouncyCastle la path del sistema.

##### Prueba de la extracción del nombre común en nombres X.500

* Se extrae el nombre común de múltiples cadenas con formato X.500 y similares.
* **Resultado esperado:** El nombre común asociado al nombre X.500 asociado, la misma cadena de entrada o null si la entrada fue nula.

##### Detección de MimeType

* Se detecta el MimeType de los siguientes tipos de documento:
  + Texto plano
  + XML
  + PDF
  + DOC
  + XSL
  + PPT
  + MPP
  + VSD
* **Resultado esperado:** El MimeType correcto de cada documento.

##### Toma de dato datos del registro de Windows

* Se extrae del registro de Windows el *path* del directorio raíz del sistema. Esta prueba sólo se realiza en sistemas Microsoft Windows.
* **Resultado esperado:** La ruta del directorio raíz del sistema.

### Afirma-core-keystores

#### Pruebas unitarias

##### Extracción de los alias y los certificados de un almacén PKCS#12

* Se carga un almacén de claves PKCS#12 y se extraen los alias y los certificados contenidos.
* **Resultado esperado:** Alias del almacén y los certificados asociados a los mismos.

##### Acceso al KeyChain del sistema en MacOS X

* En sistemas MacOS X se carga el listado de alias del almacén del sistema y se extraen los datos de los certificados contenidos. Si falla el proceso se lanza el error.
* **Resultado esperado:** En Mac OS X, alias del almacén y los certificados asociados a los mismos. En el resto de sistema, el test no genera resultado.

##### Acceso a un KeyChain en fichero en MacOS X

* En sistemas MacOS X se carga el listado de alias de un almacén KeyChain en fichero y se extraen los datos de los certificados contenidos. Si falla el proceso se lanza el error.
* **Resultado esperado:** En Mac OS X, alias del almacén y los certificados asociados a los mismos. En el resto de sistemas, el test no genera resultado.

##### Obtención de nombres significativos de los certificados del almacén de Microsoft Windows

* En sistemas Microsoft Windows se carga el listado de alias del almacén del sistema y se extraen los datos de los certificados contenidos. Si falla el proceso se lanza el error.
* **Resultado esperado:** En Microsoft Windows, si el certificado no tenía alias o este se corresponde con un nombre X.500, se utilizará el CN del Subject o la OU si este no existía. En otros casos, se devolverá el propio alias. En el resto de sistemas, el test no genera resultado.

### Afirma-core-massive

#### Pruebas unitarias

Las pruebas del módulo de firma masiva se realizarán sobre las funcionalidades de firma masiva de directorios y firma masiva programática. Debido a la naturaleza del proceso de firma masiva de directorios, las pruebas unitarias correspondientes a este proceso se ejecutarán fuera del proceso de integración continua.

##### Firma masiva de directorios con formatos de firma genéricos

* Se ejecuta el proceso de firma masiva de directorios, habiendo configurado la operación de firma, para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XMLDSig Detached
    - XMLDSig Enveloping
  + Modos
    - Implícito
    - Explícito
* Los ficheros presentes en el directorio serán de tipo:
  + Binario
  + XML
  + PDF
  + ODT
  + DOCX
* **Resultado esperado:** Firmas correctas para cada configuración indicada por cada uno de los ficheros del directorio. El nombre de las firmas generadas incorporarán la partícula “.sign”.

##### Firma masiva de directorios con formatos de firma XML enveloped y datos XML

* Se ejecuta el proceso de firma masiva de directorios, habiendo configurado la operación de firma, para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - XAdES Enveloped
    - XMLDSig Enveloped
  + Modos
    - Implícito
* Los ficheros presentes en el directorio serán de tipo:
  + XML
* **Resultado esperado:** Firmas correctas para cada configuración indicada por cada uno de los ficheros del directorio. El nombre de las firmas generadas incorporarán la partícula “.sign”.

##### Firma masiva de directorios con formatos de firma XML enveloped y datos no XML

* Se ejecuta el proceso de firma masiva de directorios, habiendo configurado la operación de firma, para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - XAdES Enveloped
    - XMLDSig Enveloped
  + Modos
    - Implícito
* Los ficheros presentes en el directorio serán de tipo:
  + Binario
  + PDF
  + ODT
  + DOCX
* **Resultado esperado:** No se generará ninguna firma y los errores quedarán indicados en el fichero de log generado durante el proceso de firma masiva.

##### Firma masiva de directorios con formatos de firma XML enveloped y modo explícito

* Se ejecuta el proceso de firma masiva de directorios, habiendo configurado la operación de firma, para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - XAdES Enveloped
    - XMLDSig Enveloped
  + Modos
    - Explícito
* Los ficheros presentes en el directorio serán de tipo:
  + Binario
  + XML
  + PDF
  + ODT
  + DOCX
* **Resultado esperado:** No se generará ninguna firma y los errores quedarán indicados en el fichero de log generado durante el proceso de firma masiva.

##### Firma masiva de directorios con formato de firma PAdES y documentos PDF

* Se ejecuta el proceso de firma masiva de directorios, habiendo configurado la operación de firma, para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - PAdES
* Los ficheros presentes en el directorio serán de tipo:
  + PDF
* **Resultado esperado:** Firmas correctas para cada configuración indicada por cada uno de los ficheros del directorio. El nombre de las firmas generadas incorporarán la partícula “.sign”.

##### Firma masiva de directorios con formato de firma PAdES y ficheros no PDF

* Se ejecuta el proceso de firma masiva de directorios, habiendo configurado la operación de firma, para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - PAdES
* Los ficheros presentes en el directorio serán de tipo:
  + Binario
  + XML
  + ODT
  + DOCX
* **Resultado esperado:** No se generará ninguna firma y los errores quedarán indicados en el fichero de log generado durante el proceso de firma masiva.

##### Firma masiva de directorios con formato de firma ODF y documentos ODF

* Se ejecuta el proceso de firma masiva de directorios, habiendo configurado la operación de firma, para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - ODF
* Los ficheros presentes en el directorio serán de tipo:
  + ODF (ODT, ODS, ODP)
* **Resultado esperado:** Firmas correctas para cada configuración indicada por cada uno de los ficheros del directorio. El nombre de las firmas generadas incorporarán la partícula “.sign”.

##### Firma masiva de directorios con formato de firma ODF y ficheros no ODF

* Se ejecuta el proceso de firma masiva de directorios, habiendo configurado la operación de firma, para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - ODF
* Los ficheros presentes en el directorio serán de tipo:
  + Binario
  + XML
  + PDF
  + DOCX
* **Resultado esperado:** No se generará ninguna firma y los errores quedarán indicados en el fichero de log generado durante el proceso de firma masiva.

##### Firma masiva de directorios con formato de firma OOXML y documentos OOXML

* Se ejecuta el proceso de firma masiva de directorios, habiendo configurado la operación de firma, para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - OOXML
* Los ficheros presentes en el directorio serán de tipo:
  + OOXML (DOCX, XLSX, PPTX)
* **Resultado esperado:** Firmas correctas para cada configuración indicada por cada uno de los ficheros del directorio. El nombre de las firmas generadas incorporarán la partícula “.sign”.

##### Firma masiva de directorios con formato de firma OOXML y ficheros no OOXML

* Se ejecuta el proceso de firma masiva de directorios, habiendo configurado la operación de firma, para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - OOXML
* Los ficheros presentes en el directorio serán de tipo:
  + Binario
  + XML
  + PDF
  + ODT
* **Resultado esperado:** No se generará ninguna firma y los errores quedarán indicados en el fichero de log generado durante el proceso de firma masiva.

##### Cofirma masiva de directorios sobre firmas con el indicador para conservar el formato original

* Se ejecuta el proceso de firma masiva de directorios, habiendo configurado la operación de cofirma y la propiedad para que se conserve el formato original que se utilizase en las firmas. Se realiza la prueba con todas las combinaciones posibles de los siguientes elementos:
  + Formatos por defecto
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XAdES Enveloped
    - XMLDSig Detached
    - XMLDSig Enveloping
    - XMLDSig Enveloped
    - PAdES
    - ODF
    - OOXML
  + Modos
    - Implícito
    - Explícito
* Los ficheros presentes en el directorio serán de tipo:
  + Firma CAdES
  + Firma CMS
  + Firma XAdES Detached
  + Firma XAdES Enveloping
  + Firma XAdES Enveloped
  + Firma XMLdSig Detached
  + Firma XMLdSig Enveloping
  + Firma XMLdSig Enveloped
  + Firma PAdES
  + Firma ODF
  + Firma OOXML
* **Resultado esperado:** Cofirmas correctas para cada configuración indicada. Siendo el resultado siempre una cofirma generada con el mismo algoritmo utilizado en la firma original. El nombre de las firmas generadas incorporarán la partícula “.cosign”.

##### Cofirma masiva de directorios sobre firmas sin el indicador para conservar el formato original

* Se ejecuta el proceso de firma masiva de directorios, habiendo configurado la operación de cofirma y no la propiedad para que se conserve el formato original que se utilizase en las firmas. Se realiza la prueba con todas las combinaciones posibles de los siguientes elementos:
  + Formatos por defecto
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XAdES Enveloped
    - XMLDSig Detached
    - XMLDSig Enveloping
    - XMLDSig Enveloped
    - PAdES
    - ODF
    - OOXML
  + Modos
    - Implícito
    - Explícito
* Los ficheros presentes en el directorio serán de tipo:
  + Firma CAdES
  + Firma CMS
  + Firma XAdES Detached
  + Firma XAdES Enveloping
  + Firma XAdES Enveloped
  + Firma XMLdSig Detached
  + Firma XMLdSig Enveloping
  + Firma XMLdSig Enveloped
  + Firma PAdES
  + Firma ODF
  + Firma OOXML
* **Resultado esperado:** Se generará una cofirma correcta para cada configuración indicada cuando el formato en cuestión permita la cofirma del tipo de documento especificado. En caso contrario, se generará un error en el log resultado de la operación. El nombre de las cofirmas generadas incorporarán la partícula “.cosign”.

##### Cofirma masiva de directorios sobre datos sin el indicador para conservar el formato original

* Se ejecuta el proceso de firma masiva de directorios, habiendo configurado la operación de cofirma y no la propiedad para que se conserve el formato original que se utilizase en las firmas. Se realiza la prueba con todas las combinaciones posibles de los siguientes elementos:
  + Formatos por defecto
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XAdES Enveloped
    - XMLDSig Detached
    - XMLDSig Enveloping
    - XMLDSig Enveloped
    - PAdES
    - ODF
    - OOXML
  + Modos
    - Implícito
    - Explícito
* Los ficheros presentes en el directorio serán de tipo:
  + Binario
  + XML
  + PDF
  + ODT
  + DOCX
* **Resultado esperado:** Se generará una cofirma correcta para cada configuración indicada cuando el formato en cuestión permita la cofirma del tipo de firma especificado. En caso contrario, se generará un error en el log resultado de la operación. El nombre de las cofirmas generadas incorporarán la partícula “.cosign”.

##### Contrafirma masiva de directorios sobre firmas con el indicador para conservar el formato original

* Se ejecuta el proceso de firma masiva de directorios habiendo configurado la operación de contrafirma y la propiedad para que se conserve el formato original que se utilizase en las firmas. Se realiza la prueba con todas las combinaciones posibles de los siguientes elementos:
  + Formatos por defecto
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XAdES Enveloped
    - XMLDSig Detached
    - XMLDSig Enveloping
    - XMLDSig Enveloped
    - PAdES
    - ODF
    - OOXML
  + Modos
    - Implícito
    - Explícito
  + Nodos objetivo
    - Nodos hijos de firma
    - Todos los nodos de firma
* Los ficheros presentes en el directorio serán de tipo:
  + Firma CAdES
  + Firma CMS
  + Firma XAdES Detached
  + Firma XAdES Enveloping
  + Firma XAdES Enveloped
  + Firma XMLdSig Detached
  + Firma XMLdSig Enveloping
  + Firma XMLdSig Enveloped
  + Firma PAdES
  + Firma ODF
  + Firma OOXML
* **Resultado esperado:** Se generará una contrafirma correcta sobre los nodos objetivo para cada configuración. La contrafirma siempre se generará en el mismo formato que la firma original. El nombre de las contrafirmas generadas incorporarán la partícula “.countersign”.

##### Contrafirma masiva de directorios sobre firmas sin el indicador para conservar el formato original

* Se ejecuta el proceso de firma masiva de directorios, habiendo configurado la operación de contrafirma y no la propiedad para que se conserve el formato original que se utilizase en las firmas. Se realiza la prueba con todas las combinaciones posibles de los siguientes elementos:
  + Formatos por defecto
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XAdES Enveloped
    - XMLDSig Detached
    - XMLDSig Enveloping
    - XMLDSig Enveloped
    - PAdES
    - ODF
    - OOXML
  + Modos
    - Implícito
    - Explícito
  + Nodos objetivo
    - Nodos hijos de firma
    - Todos los nodos de firma
* Los ficheros presentes en el directorio serán de tipo:
  + Firma CAdES
  + Firma CMS
  + Firma XAdES Detached
  + Firma XAdES Enveloping
  + Firma XAdES Enveloped
  + Firma XMLdSig Detached
  + Firma XMLdSig Enveloping
  + Firma XMLdSig Enveloped
  + Firma PAdES
  + Firma ODF
  + Firma OOXML
* **Resultado esperado:** Se generará una contrafirma correcta sobre los nodos objetivo para cada configuración indicada cuando el formato en cuestión permita la contrafirma del tipo de documento especificado. En caso contrario, se generará un error en el log resultado de la operación. El nombre de las contrafirmas generadas incorporarán la partícula “.countersign”.

##### Contrafirma masiva de directorios sobre datos sin el indicador para conservar el formato original

* Se ejecuta el proceso de firma masiva de directorios, habiendo configurado la operación de contrafirma y no la propiedad para que se conserve el formato original que se utilizase en las firmas. Se realiza la prueba con todas las combinaciones posibles de los siguientes elementos:
  + Formatos por defecto
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XAdES Enveloped
    - XMLDSig Detached
    - XMLDSig Enveloping
    - XMLDSig Enveloped
    - PAdES
    - ODF
    - OOXML
* Los ficheros presentes en el directorio serán de tipo:
  + Binario
  + XML
  + PDF
  + ODT
  + DOCX
* **Resultado esperado:** No se generará ninguna contrafirma y los errores quedarán indicados en el fichero de log generado durante el proceso de firma masiva.

##### Firma masiva programática con formatos de firma genéricos

* Se ejecuta la operación de firma masiva programática habiendo configurado la operación de firma para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XMLDSig Detached
    - XMLDSig Enveloping
  + Modos
    - Implícito
    - Explícito
  + Ficheros
    - Binario
    - XML
    - PDF
    - ODT
    - DOCX
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros
    - Hash calculados de los ficheros
* **Resultado esperado:** Firmas correctas para cada configuración indicada por cada uno de los ficheros.

##### Firma masiva programática con formatos de firma XML enveloped y datos XML

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de firma para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - XAdES Enveloped
    - XMLDSig Enveloped
  + Modos
    - Implícito
  + Ficheros
    - XML
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros
* **Resultado esperado:** Firmas correctas para cada configuración indicada por cada uno de los ficheros.

##### Firma masiva programática con formatos de firma XML enveloped a partir de un hash

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de firma para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - XAdES Enveloped
    - XMLDSig Enveloped
  + Modos
    - Implícito
  + Ficheros
    - Binario
    - XML
    - PDF
    - ODT
    - DOCX
  + A partir de:
    - Hash calculados de los ficheros
* **Resultado esperado:** Se obtiene null y se registra el error de la operación en el log del proceso de firma masiva.

##### Firma masiva programática con formatos de firma XML enveloped y datos no XML

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de firma para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - XAdES Enveloped
    - XMLDSig Enveloped
  + Modos
    - Implícito
  + Ficheros
    - Binario
    - PDF
    - ODT
    - DOCX
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros
    - Hash calculados de los ficheros
* **Resultado esperado:** Se obtiene null y se registra el error de la operación en el log del proceso de firma masiva.

##### Firma masiva programática con formatos de firma XML enveloped y modo explícito

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de firma para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - XAdES Enveloped
    - XMLDSig Enveloped
  + Modos
    - Explícito
  + Ficheros
    - Binario
    - XML
    - PDF
    - ODT
    - DOCX
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros
    - Hash calculados de los ficheros
* **Resultado esperado:** Se obtiene null y se registra el error de la operación en el log del proceso de firma masiva.

##### Firma masiva programática con formato de firma PAdES y documentos PDF

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de firma para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - PAdES
  + Ficheros
    - PDF
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros
* **Resultado esperado:** Firmas correctas para cada configuración indicada por cada uno de los ficheros.

##### Firma masiva programática con formato de firma PAdES y la huella digital de documentos PDF

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de firma para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - PAdES
  + Ficheros
    - PDF
  + A partir de:
    - Hash calculados de los ficheros
* **Resultado esperado:** Se obtiene null y se registra el error de la operación en el log del proceso de firma masiva.

##### Firma masiva programática con formato de firma PAdES y ficheros no PDF

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de firma para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - PAdES
  + Ficheros
    - Binario
    - XML
    - ODT
    - DOCX
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros
    - Hash calculados de los ficheros
* **Resultado esperado:** Se obtiene null y se registra el error de la operación en el log del proceso de firma masiva.

##### Firma masiva programática con formato de firma ODF y documentos ODF

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de firma para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - ODF
  + Ficheros
    - ODF (ODT, ODS, ODP)
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros
* **Resultado esperado:** Firmas correctas para cada configuración indicada por cada uno de los ficheros.

##### Firma masiva programática con formato de firma ODF y la huella digital de documentos ODF

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de firma para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - ODF
  + Ficheros
    - ODF
  + A partir de:
    - Hash calculados de los ficheros
* **Resultado esperado:** Se obtiene null y se registra el error de la operación en el log del proceso de firma masiva.

##### Firma masiva programática con formato de firma ODF y ficheros no ODF

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de firma para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - ODF
  + Ficheros
    - Binario
    - XML
    - PDF
    - DOCX
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros
    - Hash calculados de los ficheros
* **Resultado esperado:** Se obtiene null y se registra el error de la operación en el log del proceso de firma masiva.

##### Firma masiva programática con formato de firma OOXML y documentos OOXML

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de firma para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - OOXML
  + Ficheros
    - OOXML
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros
* **Resultado esperado:** Firmas correctas para cada configuración indicada por cada uno de los ficheros.

##### Firma masiva programática con formato de firma OOXML y la huella digital de documentos OOXML

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de firma para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - OOXML
  + Ficheros
    - OOXML (DOCX, XSLX, PPTX)
  + A partir de:
    - Hash calculados de los ficheros
* **Resultado esperado:** Se obtiene null y se registra el error de la operación en el log del proceso de firma masiva.

##### Firma masiva programática con formato de firma OOXML y ficheros no OOXML

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de firma para todas las combinaciones posibles de los siguientes elementos:
  + Formatos
    - OOXML
  + Ficheros
    - Binario
    - XML
    - PDF
    - ODT
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros
    - Hash calculados de los ficheros
* **Resultado esperado:** Se obtiene null y se registra el error de la operación en el log del proceso de firma masiva.

##### Cofirma masiva programática sobre firmas con el indicador para conservar el formato original

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de cofirma y la propiedad para que se conserve el formato original que se utilizase en las firmas. Se realiza la prueba con todas las combinaciones posibles de los siguientes elementos:
  + Formatos por defecto
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XAdES Enveloped
    - XMLDSig Detached
    - XMLDSig Enveloping
    - XMLDSig Enveloped
    - PAdES
    - ODF
    - OOXML
  + Modos
    - Implícito
    - Explícito
  + Ficheros
    - Firma CAdES
    - Firma CMS
    - Firma XAdES Detached
    - Firma XAdES Enveloping
    - Firma XAdES Enveloped
    - Firma XMLdSig Detached
    - Firma XMLdSig Enveloping
    - Firma XMLdSig Enveloped
    - Firma PAdES
    - Firma ODF
    - Firma OOXML
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros
* **Resultado esperado:** Cofirmas correctas para cada configuración indicada. Siendo el resultado siempre una cofirma generada con el mismo algoritmo utilizado en la firma original.

##### Cofirma masiva programática sobre firmas sin el indicador para conservar el formato original

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de cofirma y no la propiedad para que se conserve el formato original que se utilizase en las firmas. Se realiza la prueba con todas las combinaciones posibles de los siguientes elementos:
  + Formatos por defecto
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XAdES Enveloped
    - XMLDSig Detached
    - XMLDSig Enveloping
    - XMLDSig Enveloped
    - PAdES
    - ODF
    - OOXML
  + Modos
    - Implícito
    - Explícito
  + Ficheros
    - Firma CAdES
    - Firma CMS
    - Firma XAdES Detached
    - Firma XAdES Enveloping
    - Firma XAdES Enveloped
    - Firma XMLdSig Detached
    - Firma XMLdSig Enveloping
    - Firma XMLdSig Enveloped
    - Firma PAdES
    - Firma ODF
    - Firma OOXML
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros
* **Resultado esperado:** Se generará una cofirma correcta para cada configuración indicada cuando el formato en cuestión permita la cofirma del tipo de documento especificado. En caso contrario, se obtiene null y se registra el error de la operación en el log del proceso de firma masiva.

##### Cofirma masiva programática sobre datos sin el indicador para conservar el formato original

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de cofirma y no la propiedad para que se conserve el formato original que se utilizase en las firmas. Se realiza la prueba con todas las combinaciones posibles de los siguientes elementos:
  + Formatos por defecto
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XAdES Enveloped
    - XMLDSig Detached
    - XMLDSig Enveloping
    - XMLDSig Enveloped
    - PAdES
    - ODF
    - OOXML
  + Modos
    - Implícito
    - Explícito
  + Ficheros
    - Binario
    - XML
    - PDF
    - ODT
    - DOCX
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros
    - Hash calculados de los ficheros
* **Resultado esperado:** Se generará una cofirma correcta para cada configuración indicada cuando el formato en cuestión permita la cofirma del tipo de firma especificado. En caso contrario, se obtiene null y se registra el error de la operación en el log del proceso de firma masiva.

##### Cofirma masiva programática a partir de huella digital

* Se ejecuta el proceso de firma masiva programática a partir de huellas digitales habiendo configurado la operación de cofirma. Se realiza la prueba con todas las combinaciones posibles de los siguientes elementos:
  + Formatos por defecto
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XAdES Enveloped
    - XMLDSig Detached
    - XMLDSig Enveloping
    - XMLDSig Enveloped
    - PAdES
    - ODF
    - OOXML
  + Ficheros
    - Cualquiera
  + A partir de:
    - Hash calculados de los ficheros
* **Resultado esperado:** Se obtiene null y se registra el error de la operación en el log del proceso de firma masiva.

##### Contrafirma masiva programática sobre firmas con el indicador para conservar el formato original

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de contrafirma y la propiedad para que se conserve el formato original que se utilizase en las firmas. Se realiza la prueba con todas las combinaciones posibles de los siguientes elementos:
  + Formatos por defecto
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XAdES Enveloped
    - XMLDSig Detached
    - XMLDSig Enveloping
    - XMLDSig Enveloped
    - PAdES
    - ODF
    - OOXML
  + Modos
    - Implícito
    - Explícito
  + Ficheros
    - Firma CAdES
    - Firma CMS
    - Firma XAdES Detached
    - Firma XAdES Enveloping
    - Firma XAdES Enveloped
    - Firma XMLdSig Detached
    - Firma XMLdSig Enveloping
    - Firma XMLdSig Enveloped
    - Firma PAdES
    - Firma ODF
    - Firma OOXML
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros
  + Nodos objetivo
    - Nodos hijos de firma
    - Todos los nodos de firma
* **Resultado esperado:** Se generará una contrafirma correcta para cada configuración indicada sobre los nodos indicados, generada siempre en el mismo formato que la firma original.

##### Contrafirma masiva programática sobre firmas sin el indicador para conservar el formato original

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de contrafirma y no la propiedad para que se conserve el formato original que se utilizase en las firmas. Se realiza la prueba con todas las combinaciones posibles de los siguientes elementos:
  + Formatos por defecto
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XAdES Enveloped
    - XMLDSig Detached
    - XMLDSig Enveloping
    - XMLDSig Enveloped
    - PAdES
    - ODF
    - OOXML
  + Modos
    - Implícito
    - Explícito
  + Ficheros
    - Firma CAdES
    - Firma CMS
    - Firma XAdES Detached
    - Firma XAdES Enveloping
    - Firma XAdES Enveloped
    - Firma XMLdSig Detached
    - Firma XMLdSig Enveloping
    - Firma XMLdSig Enveloped
    - Firma PAdES
    - Firma ODF
    - Firma OOXML
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros
  + Nodos objetivo
    - Nodos hijos de firma
    - Todos los nodos de firma
* **Resultado esperado:** Se generará una contrafirma correcta sobre los nodos de firma indicados para cada configuración cuando el formato en cuestión permita la contrafirma del tipo de documento especificado. En caso contrario, se obtiene null y se registra el error de la operación en el log del proceso de firma masiva.

##### Contrafirma masiva programática a partir de huella digital

* Se ejecuta el proceso de firma masiva programática, habiendo configurado la operación de contrafirma, a partir de huellas digitales. Se realiza la prueba con todas las combinaciones posibles de los siguientes elementos:
  + Formatos por defecto
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XAdES Enveloped
    - XMLDSig Detached
    - XMLDSig Enveloping
    - XMLDSig Enveloped
    - PAdES
    - ODF
    - OOXML
  + Ficheros
    - Cualquier
  + A partir de:
    - Hash calculados de los ficheros

**Resultado esperado:** Se obtiene null y se registra el error de la operación en el log del proceso de firma masiva.

##### Contrafirma masiva programática sobre datos sin el indicador para conservar el formato original

* Se ejecuta el proceso de firma masiva programática habiendo configurado la operación de contrafirma y no la propiedad para que se conserve el formato original que se utilizase en las firmas. Se realiza la prueba con todas las combinaciones posibles de los siguientes elementos:
  + Formatos por defecto
    - CMS
    - CAdES
    - XAdES Detached
    - XAdES Enveloping
    - XAdES Enveloped
    - XMLDSig Detached
    - XMLDSig Enveloping
    - XMLDSig Enveloped
    - PAdES
    - ODF
    - OOXML
  + Ficheros
    - Binario
    - XML
    - PDF
    - ODT
    - DOCX
  + A partir de:
    - Ficheros
    - Datos leídos de los ficheros

**Resultado esperado:** Se obtiene null y se registra el error de la operación en el log del proceso de firma masiva.

### Afirma-crypto-cades

#### Pruebas unitarias

##### **Firma CAdES-BES**

* Se prueba la firma CAdES en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de datos
    - Texto plano
    - XML
    - Otro formato
  + Modos
    - Implícito
    - Explícito
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado**: Firmas correctas en todos los casos generadas con el algoritmo indicado. Si el modo configurado era implícito, los datos estarán contenidos en la firma y si el algoritmo de firma es SHA2 la firma tendrá el atributo SigningCertificateV2.

##### **Firma CAdES-EPES**

* Se prueba la firma CAdES con la política de firma de a AGE en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de datos
    - Texto plano
    - XML
    - Otro formato
  + Modos
    - Implícito
    - Explícito
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado**: Firmas correctas en todos los casos generadas con el algoritmo indicado y la política de firma declarada. Si el modo configurado era implícito, los datos estarán contenidos en la firma y si el algoritmo de firma es SHA2 la firma tendrá el atributo SigningCertificateV2.

##### **Cofirma CAdES con documento original**

* Se prueba la cofirma de firmas CAdES, indicando el documento originalmente firmado, en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de firma
    - Firma CAdES-BES
    - Firma CAdES-EPES
  + Modos CAdES
    - CAdES-BES
    - CAdES-EPES
  + Modos
    - Implícito
    - Explícito
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Cofirmas correctas en todos los casos generadas con el algoritmo indicado y el modo CAdES. El documento de firma final incluirá o no el documento firmado según el modo indicado en la cofirma.

##### **Cofirma CAdES sin documento original sobre CAdES implícita**

* Se prueba la cofirma de firmas CAdES implícitas sin indicar el documento originalmente firmado. Ya que no se indica el documento firmado, se generará la cofirma a partir de los datos contenidos en la firma original. Se probarán todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de firma
    - Firma CAdES-BES implícita
    - Firma CAdES-EPES implícita
  + Modos CAdES
    - CAdES-BES
    - CAdES-EPES
  + Modos
    - Implícito
    - Explícito
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Cofirmas correctas en todos los casos generadas con el algoritmo indicado y el modo CAdES. El documento de firma final incluirá o no el documento firmado según el modo indicado en la cofirma.

##### **Cofirma CAdES sin documento original sobre CAdES explícita (mismo algoritmo)**

* Se prueba la cofirma de firmas CAdES explícitas sin indicar el documento originalmente firmado. Ya que no se indica el documento firmado y este no está contenido en la firma, sólo será posible generar las firmas si ya disponemos del hash del documento firmado generado con el mismo algoritmo que queremos utiliza en la cofirma. Se probarán todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de firma
    - Firma CAdES-BES explícita
    - Firma CAdES-EPES explícita
  + Modos CAdES
    - CAdES-BES
    - CAdES-EPES
  + Modos
    - Indiferente
  + Algoritmos de firma
    - El mismo que el de la firma
* **Resultado esperado:** Cofirmas CAdES explícitas correctas generadas en todos los casos con el algoritmo utilizado en la firma. El documento de firma final incluirá o no el documento firmado según el modo indicado en la cofirma.

##### **Cofirma CAdES sin documento original sobre CAdES explícita (distinto algoritmo)**

* Se prueba la cofirma de firmas CAdES explícitas sin indicar el documento originalmente firmado. Ya que no se indica el documento firmado y este no está contenido en la firma, sólo será posible generar las firmas si ya disponemos del hash del documento firmado generado con el mismo algoritmo que queremos utiliza en la cofirma. Se probarán todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de firma
    - Firma CAdES-BES explícita
    - Firma CAdES-EPES explícita
  + Modos CAdES
    - CAdES-BES
    - CAdES-EPES
  + Modos
    - Indiferente
  + Algoritmos de firma
    - Distinto al de la firma
* **Resultado esperado:** Lanzará una excepción de tipo AOException indicando que no se ha podido generar por no encontrar ni los datos ni una huella digital válida en la firma.

##### **Cofirma de ficheros**

* Se prueba la cofirma de ficheros que no sean firma CAdES en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Ficheros de datos
    - Cualquier no CAdES
    - Firma CMS
  + Algoritmos de firma
    - Indiferente
* **Resultado esperado:** Lanzará una excepción de tipo AOException informando que ocurrió un error durante la operación.

##### **Contrafirma de firma/cofirma CAdES**

* Se prueba la contrafirma de firmas CAdES en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de firma
    - Firma CAdES implícita
    - Firma CAdES explícita
    - Cofirma CAdES
  + Modos CAdES
    - CAdES-BES
    - CAdES-EPES
  + Nodos objetivo
    - Todos los nodos hijos
    - Todos los nodos
    - Nodos determinados
    - Nodos de firmantes determinados
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Contrafirmas correctas generadas con el algoritmo indicado, el modo CAdES y realizadas sobre los nodos especificado. El documento de firma final incluirá o no el documento firmado si lo incluía ya la firma contrafirmada.

##### **Contrafirma de ficheros**

* Se prueba la contrafirma de ficheros que no sean firma CAdES en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Ficheros de datos
    - Fichero plano
    - XML
    - Fichero binario
    - Firma CMS
  + Algoritmos de firma
    - Indiferente
* **Resultado esperado:** Lanzará una excepción de tipo AOException informando que ocurrió un error durante la operación.

##### Comprobación de documento válido para firma

* Se prueba si un fichero es válido para realizar una firma CAdES sobre él. Se probará con:
  + Ficheros de datos
    - Fichero plano
    - XML
    - Fichero binario
    - Firma CAdES
    - Firma CMS
* **Resultado esperado:** Siempre se devolverá “true”.

##### Comprobación de firmas CAdES

* Se prueba si un fichero es realmente una firma CAdES. Se probará con los siguientes ficheros:
  + Firma CAdES-BES implícita
  + Firma CAdES-BES explicita
  + Firma CAdES-EPES
  + Cofirma CAdES-BES
  + Cofirma CAdES-EPES
  + Contrafirma CAdES-BES
  + Contrafirma CAdES-EPES
* **Resultado esperado:** El método devolverá “true”.

##### Comprobación de firmas CAdES con ficheros no CAdES

* Se prueba si un fichero es realmente una firma CAdES. Se probará con los siguientes ficheros:
  + Fichero plano
  + XML
  + Fichero binario
  + Firma CMS
* **Resultado esperado:** El método devolverá “false”.

##### Extracción de datos generales de firmas CAdES

* Se extrae la información general de una firma CAdES con los siguientes ficheros:
  + Firma CAdES-BES implícita
  + Firma CAdES-BES explicita
  + Firma CAdES-EPES
  + Cofirma CAdES-BES
  + Cofirma CAdES-EPES
  + Contrafirma CAdES-BES
  + Contrafirma CAdES-EPES
* **Resultado esperado:** Objeto AOSignInfo cuyo formato declarado es “CAdES".

##### Extracción de datos generales con ficheros no CAdES

* Se extrae la información general de una firma CAdES con los siguientes ficheros:
  + Fichero plano
  + XML
  + Fichero binario
  + Firma CMS
* **Resultado esperado:** Se lanza la excepción “AOInvalidFormatException”.

##### Extracción de datos firmados de firmas CAdES implícita

* Se extraen los datos firmados de los siguientes ficheros CAdES firmados:
  + Firma CAdES-BES implícita
  + Firma CAdES-EPES implícita
  + Cofirma CAdES-BES implícita
  + Cofirma CAdES-EPES implícita
  + Contrafirma CAdES-BES implícita
  + Contrafirma CAdES-EPES implícita
* **Resultado esperado:** Se extraen los datos originalmente firmados.

##### Extracción de datos firmados de firmas CAdES explícita

* Se extraen los datos firmados de los siguientes ficheros CAdES firmados:
  + Firma CAdES-BES explícita
  + Firma CAdES-EPES explícita
  + Cofirma CAdES-BES explícita
  + Cofirma CAdES-EPES explícita
  + Contrafirma CAdES-BES explícita
  + Contrafirma CAdES-EPES explícita
* **Resultado esperado:** Se devuelve null.

##### Extracción de datos firmados de ficheros no CAdES

* Se extraen los datos firmados de los siguientes ficheros:
  + Fichero plano
  + XML
  + Fichero binario
  + Firma CMS
* **Resultado esperado:** Se lanza la excepción “AOInvalidFormatException”.

##### Obtención de la estructura de firmantes de firmas CAdES

* Se extrae el árbol de firmantes de ficheros del siguiente tipo:
  + Firma CAdES-BES implícita
  + Firma CAdES-BES explicita
  + Firma CAdES-EPES
  + Cofirma CAdES-BES
  + Cofirma CAdES-EPES
  + Contrafirma CAdES-BES
  + Contrafirma CAdES-EPES
* **Resultado esperado:** Se obtiene el árbol de firmas correspondiente a cada documento.

##### Obtención de la estructura de firmantes de ficheros no CAdES

* Se extrae el árbol de firmantes de documentos del siguiente tipo:
  + Fichero plano
  + XML
  + Fichero binario
  + Firma CMS
* **Resultado esperado:** Se lanza una excepción de tipo “AOInvalidFormatException”.

### Afirma-crypto-cms

#### Pruebas unitarias

##### **Firma CMS**

* Se prueba la firma CMS en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de datos
    - Texto plano
    - XML
    - Otro formato
  + Modos
    - Implícito
    - Explícito
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado**: Firmas correctas en todos los casos generadas con el algoritmo indicado. Si el modo configurado era implícito, los datos estarán contenidos en la firma.

##### **Cofirma CMS con documento original**

* Se prueba la cofirma de firmas CMS, indicando el documento originalmente firmado, en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Modos
    - Implícito
    - Explícito
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Cofirmas correctas en todos los casos generadas con el algoritmo indicado. El documento de firma final incluirá o no el documento firmado según el modo indicado en la cofirma.

##### **Cofirma CMS sin documento original sobre firma implícita**

* Se prueba la cofirma de firmas CMS y CAdES implícitas sin indicar el documento originalmente firmado. Ya que no se indica el documento firmado, se generará la cofirma a partir de los datos contenidos en la firma original. Se probarán todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Ficheros
    - Firma CMS implícita
    - Firma CAdES-BES implícita
    - Firma CAdES-EPES implícita
  + Modos
    - Implícito
    - Explícito
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Cofirmas CMS correctas generadas con el algoritmo indicado. El documento de firma final incluirá o no el documento firmado según el modo indicado en la cofirma.

##### **Cofirma CMS sin documento original sobre CMS explícita (mismo algoritmo)**

* Se prueba la cofirma de firmas CMS y CAdES explícitas sin indicar el documento originalmente firmado. Ya que no se indica el documento firmado y este no está contenido en la firma, sólo será posible generar las firmas si ya disponemos del hash del documento firmado generado con el mismo algoritmo que queremos utiliza en la cofirma. Se probarán todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Ficheros
    - Firma CMS explícita
    - Firma CAdES-BES explícita
    - Firma CAdES-EPES explícita
  + Modos
    - Indiferente
  + Algoritmos de firma
    - El mismo que el de la firma
* **Resultado esperado:** Cofirmas CMS explícitas correctas generadas con el algoritmo utilizado en la firma. El documento de firma final incluirá o no el documento firmado según el modo indicado en la cofirma.

##### **Cofirma CMS sin documento original sobre CMS explícita (distinto algoritmo)**

* Se prueba la cofirma de firmas CMS explícitas sin indicar el documento originalmente firmado. Ya que no se indica el documento firmado y este no está contenido en la firma, sólo será posible generar las firmas si ya disponemos del hash del documento firmado generado con el mismo algoritmo que queremos utiliza en la cofirma. Se probarán todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de firma
    - Firma CMS
    - Firma CAdES-BES
  + Modos
    - Indiferente
  + Algoritmos de firma
    - Distinto al de la firma
* **Resultado esperado:** Lanzará una excepción de tipo AOException indicando que no se ha podido generar por no encontrar ni los datos ni una huella digital válida en la firma.

##### **Cofirma de ficheros**

* Se prueba la cofirma de ficheros que no sean firma CMS ni CAdES en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
  + Ficheros de datos
    - Fichero plano
    - XML
    - Fichero binario
  + Algoritmos de firma
    - Indiferente
* **Resultado esperado:** Lanzará una excepción de tipo AOException informando que ocurrió un error durante la operación.

##### **Contrafirma de firma/cofirma CMS**

* Se prueba la contrafirma de firmas CMS en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de firma
    - Firma CMS implícita
    - Firma CMS explícita
    - Cofirma CMS
    - Firma CAdES implícita
    - Firma CAdES explícita
    - Cofirma CAdES
  + Nodos objetivo
    - Todos los nodos hijos
    - Todos los nodos
    - Nodos determinados
    - Nodos de firmantes determinados
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Contrafirmas CMS correctas generadas con el algoritmo indicado y realizadas sobre los nodos especificados. El documento de firma final incluirá o no el documento firmado si lo incluía ya la firma contrafirmada.

##### **Contrafirma de ficheros**

* Se prueba la contrafirma de ficheros que no sean firma CMS en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Ficheros de datos
    - Cualquier no CAdES
    - Firma CMS
  + Algoritmos de firma
    - Indiferente
* **Resultado esperado:** Lanzará una excepción de tipo AOException informando que ocurrió un error durante la operación.

##### Comprobación de documento válido para firma

* Se prueba si un fichero es válido para realizar una firma CMS sobre él. Se probará con:
  + Ficheros de datos
    - Fichero plano
    - XML
    - Fichero binario
    - Firma CAdES
    - Firma CMS
* **Resultado esperado:** Siempre se devolverá “true”.

##### Comprobación de firmas CMS

* Se prueba si un fichero es realmente una firma CMS. Ya que las firmas CAdES son CMS con atributos adicionales, se considerarán también firmas CMS. Se probará con los siguientes ficheros:
  + Firma CMS implícita
  + Firma CMS explicita
  + Cofirma CMS
  + Contrafirma CMS
  + Firma CAdES-BES implícita
  + Firma CAdES-BES explicita
  + Firma CAdES-EPES
  + Cofirma CAdES-BES
  + Cofirma CAdES-EPES
  + Contrafirma CAdES-BES
  + Contrafirma CAdES-EPES
* **Resultado esperado:** El método devolverá “true”.

##### Comprobación de firmas CMS con ficheros no CMS

* Se prueba si un fichero es realmente una firma CMS. Se probará con los siguientes ficheros:
  + Fichero plano
  + XML
  + Fichero binario
* **Resultado esperado:** El método devolverá “false”.

##### Extracción de datos generales de firmas CMS

* Se extrae la información general de una firma CMS o CAdES (que se consideran CMS con datos adicionales) con los siguientes ficheros:
  + Firma CMS implícita
  + Firma CMS explicita
  + Cofirma CMS
  + Contrafirma CMS
  + Firma CAdES-BES implícita
  + Firma CAdES-BES explicita
  + Firma CAdES-EPES
  + Cofirma CAdES-BES
  + Cofirma CAdES-EPES
  + Contrafirma CAdES-BES
  + Contrafirma CAdES-EPES
* **Resultado esperado:** Objeto AOSignInfo cuyo formato declarado es “CMS".

##### Extracción de datos generales con ficheros no CMS

* Se extrae la información general de una firma CMS con los siguientes ficheros:
  + Fichero plano
  + XML
  + Fichero binario
* **Resultado esperado:** Se lanza la excepción “AOInvalidFormatException”.

##### Extracción de datos firmados de firmas CMS implícita

* Se extraen los datos firmados de los siguientes ficheros CMS firmados:
  + Firma CMS implícita
  + Cofirma CMS implícita
  + Contrafirma CMS implícita
  + Firma CAdES-BES implícita
  + Firma CAdES-EPES implícita
  + Cofirma CAdES-BES implícita
  + Cofirma CAdES-EPES implícita
  + Contrafirma CAdES-BES implícita
  + Contrafirma CAdES-EPES implícita
* **Resultado esperado:** Se extraen los datos originalmente firmados.

##### Extracción de datos firmados de firmas CMS explícita

* Se extraen los datos firmados de los siguientes ficheros firmados:
  + Firma CMS explícita
  + Cofirma CMS explícita
  + Contrafirma CMS explícita
  + Firma CAdES-BES explícita
  + Firma CAdES-EPES explícita
  + Cofirma CAdES-BES explícita
  + Cofirma CAdES-EPES explícita
  + Contrafirma CAdES-BES explícita
  + Contrafirma CAdES-EPES explícita
* **Resultado esperado:** Se devuelve null.

##### Extracción de datos firmados de ficheros no CMS

* Se extraen los datos firmados de los siguientes ficheros:
  + Fichero plano
  + XML
  + Fichero binario
* **Resultado esperado:** Se lanza la excepción “AOInvalidFormatException”.

##### Obtención de la estructura de firmantes de firmas CMS

* Se extrae el árbol de firmantes de ficheros del siguiente tipo:
  + Firma CMS implícita
  + Firma CMS explicita
  + Cofirma CMS
  + Contrafirma CMS
  + Firma CAdES-BES implícita
  + Firma CAdES-BES explicita
  + Firma CAdES-EPES
  + Cofirma CAdES-BES
  + Cofirma CAdES-EPES
  + Contrafirma CAdES-BES
  + Contrafirma CAdES-EPES
* **Resultado esperado:** Se obtiene el árbol de firmas correspondiente a cada documento.

##### Obtención de la estructura de firmantes de ficheros no CMS

* Se extrae el árbol de firmantes de documentos del siguiente tipo:
  + Fichero plano
  + XML
  + Fichero binario
* **Resultado esperado:** Se lanza una excepción de tipo “AOInvalidFormatException”.

### Afirma-crypto-odf

#### Pruebas unitarias

##### **Firma ODF**

* Se prueba la firma ODF en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
  + Formatos de ficheros de datos
    - ODT
    - ODS
    - ODP
  + Modos CAdES
    - OpenOffice.org 3.2
    - OpenOffice.org 3.1
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado**: Firmas correctas en todos los casos generadas siempre con SHA1 (se ignora el algoritmo de firma). Es necesario abrir los ficheros con OpenOffice para comprobación manual.

##### **Cofirma de firmas ODF**

* Se prueba la cofirma de ficheros ODF firmados en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
  + Formatos de ficheros de firma
    - ODT
    - ODS
    - ODP
  + Modos CAdES
    - OpenOffice.org 3.2
    - OpenOffice.org 3.1
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Cofirmas correctas en todos los casos generadas siempre con SHA1 (se ignora el algoritmo de firma). Es necesario abrir los ficheros con OpenOffice para comprobación manual.

##### **Cofirma de ficheros ODF**

* Se prueba la cofirma de ficheros ODF sin firmar en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
  + Formatos de ficheros de datos
    - ODT
    - ODS
    - ODP
  + Modos CAdES
    - OpenOffice.org 3.2
    - OpenOffice.org 3.1
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Firmas correctas en todos los casos generadas siempre con SHA1 (se ignora el algoritmo de firma). Es necesario abrir los ficheros con OpenOffice para comprobación manual.

##### **Contrafirma de ficheros**

* Se prueba la contrafirma de ficheros ODF en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
  + Formatos de ficheros de datos
    - ODT
    - ODS
    - ODP
    - ODT firmado
    - ODS firmado
    - ODP firmado
    - Otro formato
  + Modos CAdES
    - OpenOffice.org 3.2
    - OpenOffice.org 3.1
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Cada intento de contrafirma lanzará una excepción de tipo “UnsupportedOperationException”.

##### Firma y cofirma de un fichero en formato no ODF

* Se prueba la firma y cofirma de ficheros no ODF en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
  + Formatos de ficheros de datos
    - No ODF
  + Modos CAdES
    - OpenOffice.org 3.2
    - OpenOffice.org 3.1
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Cada intento de firmar/cofirmar el fichero lanzará una excepción de tipo “AOFormatFileException”.

##### Comprobación de documento ODF

* Se prueba si un fichero es realmente un documento ODF con los siguientes ficheros:
  + ODT
  + ODS
  + ODP
  + ODT firmado
  + ODS firmado
  + ODP firmado
* **Resultado esperado:** El método devolverá “true”.

##### Comprobación de documento no ODF

* Se prueba si un fichero es realmente un documento ODF con los siguientes ficheros:
  + Cualquier documento no ODF.
* **Resultado esperado:** El método devolverá “false”.

##### Comprobación de firmas ODF

* Se prueba si un fichero es realmente un documento ODF firmado con los siguientes ficheros:
  + ODT firmado / cofirmado
  + ODS firmado / cofirmado
  + ODP firmado / cofirmado
* **Resultado esperado:** El método devolverá “true”.

##### Comprobación de firmas de documento distintos a ODF firmados

* Se prueba si un fichero es realmente un documento ODF firmado con los siguientes ficheros:
  + ODT sin firmar
  + ODS sin firmar
  + ODP sin firmar
  + Cualquier documento no ODF
* **Resultado esperado:** El método devolverá “false”.

##### Extracción de datos generales de firmas ODF

* Se extrae la información general de una firma ODF con los siguientes ficheros:
  + ODT firmado
  + ODS firmado
  + ODP firmado
* **Resultado esperado:** Objeto AOSignInfo cuyo formato declarado es “ODF (Open Document Format)".

##### Extracción de datos generales de documentos no ODF firmados

* Se extrae la información general de una firma ODF con los siguientes ficheros:
  + ODT sin firmar
  + ODS sin firmar
  + ODP sin firmar
  + Cualquier documento no ODF
* **Resultado esperado:** Se lanza la excepción “AOInvalidFormatException”.

##### Extracción de datos firmados de firmas ODF

* Se extraen los datos firmados de los siguientes ficheros ODF firmados:
  + ODT firmado
  + ODS firmado
  + ODP firmado
* **Resultado esperado:** Se extraen los datos originalmente firmados.

##### Extracción de datos firmados de ficheros no ODF firmados

* Se extraen los datos firmados de los siguientes ficheros:
  + ODT
  + ODS
  + ODP
  + Cualquier documento no ODF
* **Resultado esperado:** Se lanza la excepción “AOInvalidFormatException”.

##### Obtención de la estructura de firmantes de ODF firmados

* Se extrae el árbol de firmantes de documentos del siguiente tipo:
  + ODT firmado
  + ODT cofirmado
  + ODS firmado
  + ODS cofirmado
  + ODP firmado
  + ODP cofirmado
* **Resultado esperado:** Se obtiene el árbol de firmas correspondiente a cada documento.

##### Obtención de la estructura de firmantes de ficheros ODF sin firmar y no ODF

* Se extrae el árbol de firmantes de documentos del siguiente tipo:
  + ODT
  + ODS
  + ODP
  + Cualquier documento no ODF
* **Resultado esperado:** Se lanza una excepción de tipo “AOInvalidFormatException”.

### Afirma-crypto-ooxml

#### Pruebas unitarias

##### **Firma OOXML**

* Se prueba la firma OOXML en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
  + Formatos de ficheros de datos
    - DOCX
    - XMLS
    - PPTX
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado**: Firmas correctas en todos los casos generadas con el algoritmo de firma indicado. Es necesario abrir los ficheros con Microsoft Office para comprobación manual.

##### **Cofirma de firmas OOXML**

* Se prueba la cofirma de ficheros OOXML firmados en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
  + Formatos de ficheros de firma
    - DOCX firmado
    - XSLX firmado
    - PPTX firmado
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Cofirmas correctas en todos los casos generadas con el algoritmo de firma indicado. Es necesario abrir los ficheros con Microsoft Office para comprobación manual.

##### **Cofirma de ficheros OOXML**

* Se prueba la cofirma de ficheros OOXML sin firmar en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
  + Formatos de ficheros de datos
    - DOCX
    - XMLX
    - PPTX
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Firmas correctas en todos los casos generadas con el algoritmo de firma indicado. Es necesario abrir los ficheros con Microsoft Office para comprobación manual.

##### **Contrafirma de ficheros**

* Se prueba la contrafirma de ficheros OOXML en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
  + Formatos de ficheros de datos
    - DOCX
    - XSLX
    - PPTX
    - DOCX firmado
    - XMLX firmado
    - PPTX firmado
    - Otro formato
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Cada intento de contrafirma lanzará una excepción de tipo “UnsupportedOperationException”.

##### Firma y cofirma de un fichero en formato no OOXML

* Se prueba la firma y cofirma de ficheros no OOXML en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
  + Formatos de ficheros de datos
    - No OOXML
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Cada intento de firmar/cofirmar el fichero lanzará una excepción de tipo “AOFormatFileException”.

##### Comprobación de documento OOXML

* Se prueba si un fichero es realmente un documento OOXML con los siguientes ficheros:
  + DOCX
  + XSLX
  + PPTX
  + DOCX firmado
  + XSLX firmado
  + PPTX firmado
* **Resultado esperado:** El método devolverá “true”.

##### Comprobación de documento no OOXML

* Se prueba si un fichero es realmente un documento OOXML con los siguientes ficheros:
  + Cualquier documento no OOXML.
* **Resultado esperado:** El método devolverá “false”.

##### Comprobación de firmas OOXML

* Se prueba si un fichero es realmente un documento OOXML firmado con los siguientes ficheros:
  + DOCX firmado / cofirmado
  + XSLX firmado / cofirmado
  + PPTX firmado / cofirmado
* **Resultado esperado:** El método devolverá “true”.

##### Comprobación de firmas de documento distintos a OOXML firmados

* Se prueba si un fichero es realmente un documento OOXML firmado con los siguientes ficheros:
  + DOCX sin firmar
  + XSLX sin firmar
  + DOCX sin firmar
  + Cualquier documento no OOXML
* **Resultado esperado:** El método devolverá “false”.

##### Extracción de datos generales de firmas OOXML

* Se extrae la información general de una firma OOXML con los siguientes ficheros:
  + DOCX firmado
  + XSLX firmado
  + PPTX firmado
* **Resultado esperado:** Objeto AOSignInfo cuyo formato declarado es “OOXML (Office Open XML)".

##### Extracción de datos generales de documentos no OOXML firmados

* Se extrae la información general de una firma OOXML con los siguientes ficheros:
  + DOCX sin firmar
  + XSLX sin firmar
  + PPTX sin firmar
  + Cualquier documento no OOXML
* **Resultado esperado:** Se lanza la excepción “AOInvalidFormatException”.

##### Extracción de datos firmados de firmas OOXML

* Se extraen los datos firmados de los siguientes ficheros OOXML firmados:
  + DOCX firmado
  + XSLX firmado
  + PPTX firmado
* **Resultado esperado:** Se extraen los datos originalmente firmados.

##### Extracción de datos firmados de ficheros no OOXML firmados

* Se extraen los datos firmados de los siguientes ficheros:
  + DOCX
  + XSLX
  + PPTX
  + Cualquier documento no OOXML
* **Resultado esperado:** Se lanza la excepción “AOInvalidFormatException”.

##### Obtención de la estructura de firmantes de OOXML firmados

* Se extrae el árbol de firmantes de documentos del siguiente tipo:
  + DOCX firmado
  + DOCX cofirmado
  + XLSX firmado
  + XSLX cofirmado
  + PPTX firmado
  + PPTX cofirmado
* **Resultado esperado:** Se obtiene el árbol de firmas correspondiente a cada documento.

##### Obtención de la estructura de firmantes de ficheros OOXML sin firmar y no OOXML

* Se extrae el árbol de firmantes de documentos del siguiente tipo:
  + DOCX
  + XLSX
  + PPTX
  + Cualquier documento no OOXML
* **Resultado esperado:** Se lanza una excepción de tipo “AOInvalidFormatException”.

### Afirma-crypto-pdf

#### Pruebas unitarias

##### **Firma PAdES-BES**

* **Pruebas de firma con todas las combinaciones posibles de los siguientes elementos:**
  + Certificados
    - ANF Persona Física
    - CatCert
  + **Algoritmos**
    - SHA1withRSA
    - SHA-512withRSA
    - SHA-256withRSA
    - SHA-384withRSA
  + **Ficheros**
    - **PDF**
    - **PDF con adjuntos y ficheros empotrados**
* **Resultado esperado:** Se obtiene el PDF con una firma PAdES-BES.

##### **Firma PAdES-EPES**

* **Pruebas de firma con la política de firma de la AGE con todas las combinaciones posibles de los siguientes elementos:**
  + Certificados
    - ANF Persona Física
    - CatCert
  + **Algoritmos**
    - SHA1withRSA
    - SHA-512withRSA
    - SHA-256withRSA
    - SHA-384withRSA
  + **Ficheros**
    - **PDF**
    - **PDF con adjuntos y ficheros empotrados**
* **Resultado esperado:** Se obtiene el PDF con una firma PAdES-EPES.

##### **Firma PAdES-T**

* **Pruebas de firma con sello de tiempo de CatCert y todas las combinaciones posibles de los siguientes elementos:**
  + **Algoritmos**
    - SHA1withRSA
    - SHA-512withRSA
    - SHA-256withRSA
    - SHA-384withRSA
  + **Ficheros**
    - **PDF**
    - **PDF con adjuntos y ficheros empotrados**
* **Resultado esperado:** Se obtiene el PDF con una firma PAdES-T con el sello de tiempo de CatCert.

##### **Firma PAdES de un PDF certificado con la propiedad “allowSigningCertifiedPdfs”**

* **Pruebas de firma PAdES de un PDF certificado con la propiedad activa “allowSigningCertifiedPdfs”, que se salta la restricción de no firmar PDFs certificados sin mostrar un diálogo de confirmación, y con todas las combinaciones posibles de los siguientes elementos:**
  + Certificados
    - ANF Persona Física
    - CatCert
  + **Modos:**
    - **Indiferente**
  + **Algoritmos**
    - Indiferente
* **Resultado esperado:** Se obtiene el PDF invalidado con la firma generada.

##### **Firma PAdES de un PDF certificado con la propiedad “headless”**

* **Pruebas de firma PAdES de un PDF certificado con la propiedad “headless”. Con la propiedad “allowSigningCertifiedPdfs” el Cliente debería mostrar un mensaje de confirmación al usuario ya que el PDF resultado sería inválido, pero al tener configurada la propiedad “headless” no se puede mostrar este diálogo. Se realizará la prueba con las siguientes confinaciones:**
  + Certificados
    - ANF Persona Física
    - CatCert
  + **Modos:**
    - **Indiferente**
  + **Algoritmos**
    - Indiferente
* **Resultado esperado:** Se lanza una excepción de tipo UnsupportedOperationException.

##### **Firma PAdES con contraseña**

* **Pruebas de firma de un PDF protegido con contraseña con todas las combinaciones posibles de los siguientes elementos:**
  + Certificados
    - ANF Persona Física
    - CatCert
  + **Modos**
    - **PAdES-BES**
    - **PAdES-EPES**
    - **PAdES-T (con sello de tiempo de CatCert)**
  + **Algoritmos**
    - SHA1withRSA
    - SHA-512withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Se obtiene el PDF con una firma del tipo que fuese (BES, EPES, T) generada con el algoritmo de firma concreto.

##### **Firma PAdES con contraseña incorrecta**

* **Pruebas de firma de un PDF protegido con contraseña utilizando una contraseña incorrecta y la propiedad “headless” establecida a “true”. Al indicar programáticamente una contraseña incorrecta se le pregunta al usuario, mediante una ventana de diálogo, por la contraseña del PDF. Sin embargo, al indicar la propiedad “headless” no se puede mostrar ventanas por lo que directamente se lanza una excepción de tipo “AOException” al fallar la contraseña indicada programáticamente. Se realizará la prueba con las siguientes combinaciones:**
  + Certificados
    - ANF Persona Física
    - CatCert
  + **Modos**
    - **PAdES-BES**
    - **PAdES-EPES**
    - **PAdES-T (con sello de tiempo de CatCert)**
  + **Algoritmos**
    - Indiferente
* **Resultado esperado:** Se lanzará una AOException.

##### **Cofirma de firmas PDF (Multifirma)**

* Se prueba la cofirma de ficheros PDF firmados en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
  + **Modos**
    - **PAdES-BES**
    - **PAdES-EPES**
    - **PAdES-T (con sello de tiempo de CatCert)**
  + Formatos de ficheros de firma
    - PDF firmado PAdES-BES
    - PDF firmado PAdES-EPES
    - PDF firmado PAdES-T
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Cofirmas correctas en todos los casos generadas con el algoritmo de firma indicado. Es necesario abrir los ficheros con Adobe Reader para comprobación manual.

##### **Cofirma de documentos PDF sin firmar**

* Se prueba la cofirma de un documento PDF sin firmar en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Firmas correctas en todos los casos generadas con el algoritmo de firma indicado. Es necesario abrir los ficheros con Adobe Reader para comprobación manual.

##### **Contrafirma de ficheros**

* Se prueba la contrafirma de ficheros PDF en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
  + Formatos de ficheros de datos
    - PDF sin firmar
    - PDF firmado PAdES-BES
    - PDF firmado PAdES-EPES
    - PDF firmado PAdES-T
    - Cualquier documento no PDF
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Cada intento de contrafirma lanzará una excepción de tipo “UnsupportedOperationException”.

##### Firma y cofirma de un fichero en formato no PDF

* Se prueba la firma y cofirma de ficheros no PDF en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
  + Formatos de ficheros de datos
    - Cualquier documento no PDF
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Cada intento de firmar/cofirmar el fichero lanzará una excepción de tipo “AOFormatFileException”.

##### Comprobación de documento PDF

* Se prueba si un fichero es realmente un documento PDF con los siguientes ficheros:
  + PDF
  + PDF certificado
  + PDF con contraseña
  + PDF firmado BES
  + PDF firmado EPES
  + PDF firmado T
* **Resultado esperado:** El método devolverá “true”.

##### Comprobación de documento no PDF

* Se prueba si un fichero es realmente un documento OOXML con los siguientes ficheros:
  + Cualquier documento no PDF.
* **Resultado esperado:** El método devolverá “false”.

##### **Comprobación de una firma PDF**

* **Prueba de reconocimiento de ficheros PDF firmados. Se probará con:**
  + **Ficheros:**
    - **PDF firmado PAdES-BES**
    - **PDF firmado PAdES-EPES**
    - **PDF firmado PAdES-T (con sello de tiempo CarCert)**
  + **Algoritmos**
    - **Indiferente**
* **Resultado esperado:** El método devolverá “true”.

##### **Comprobación de documentos distintos de PDF firmados**

* **Prueba de reconocimiento de ficheros PDF firmados. Se probará con:**
  + **Ficheros:**
    - **PDF sin firmar**
    - **Cualquier documento no PDF**
* **Resultado esperado:** El método devolverá “false”.

##### Extracción de datos generales de firmas PDF

* Se extrae la información general de una firma OOXML con los siguientes ficheros:
  + PDF firmado PAdES-BES
  + PDF firmado PAdES-EPES
  + PDF firmado PAdES-T
* **Resultado esperado:** Objeto AOSignInfo cuyo formato declarado es “Adobe PDF".

##### Extracción de datos generales de documentos no PDF firmados

* Se extrae la información general de una firma PDF con los siguientes ficheros:
  + PDF sin firmar
  + Cualquier documento no PDF
* **Resultado esperado:** Se lanza la excepción “AOInvalidFormatException”.

##### Extracción de datos firmados de firmas PDF

* Se extraen los datos firmados de los siguientes ficheros PDF firmados:
  + PDF firmado PAdES-BES
  + PDF firmado PAdES-EPES
  + PDF firmado PAdES-T
* **Resultado esperado:** Se extraen los datos originalmente firmados.

##### Extracción de datos firmados de ficheros no PDF firmados

* Se extraen los datos firmados de los siguientes ficheros:
  + PDF no firmado
  + Cualquier documento no PDF
* **Resultado esperado:** Se lanza la excepción “AOInvalidFormatException”.

##### Obtención de la estructura de firmantes de PDF firmados

* Se extrae el árbol de firmantes de documentos del siguiente tipo:
  + PDF firmado PAdES-BES
  + PDF cofirmado PAdES-BES
  + PDF firmado PAdES-EPES
  + PDF cofirmado PAdES-EPES
  + PDF firmado PAdES-T
  + PDF cofirmado PAdES-T
* **Resultado esperado:** Se obtiene el árbol de firmas correspondiente a cada documento.

##### Obtención de la estructura de firmantes de ficheros PDF sin firmar y no PDF

* Se extrae el árbol de firmantes de documentos del siguiente tipo:
  + PDF sin firmar
  + Cualquier documento no PDF
* **Resultado esperado:** Se lanza una excepción de tipo “AOInvalidFormatException”.

##### **Prueba específica de firma según los casos de pruebas ETSI PAdES PlugTest**

* **Prueba de firma de documentos PDF según los casos de prueba ETSI PAdES del PlugTest con las siguientes configuraciones:**
  + **Certificado específico ETSI**
* **Resultado esperado: Se obtiene el PDF firmado.**

### Afirma-crypto-xades

#### Pruebas unitarias

##### **Firma XAdES-BES Detached**

* Se prueba la firma XAdES Detached en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de datos
    - Texto plano
    - XML
    - Otro formato
  + Modos
    - Implícito
    - Explícito
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado**: Firmas correctas en todos los casos generadas con el algoritmo indicado. Si el modo configurado era implícito, los datos estarán contenidos en la firma.

##### **Firma XAdES-BES Enveloping**

* Se prueba la firma XAdES Enveloping en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de datos
    - Texto plano
    - XML
    - Otro formato
  + Modos
    - Implícito
    - Explícito
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado**: Firmas correctas en todos los casos generadas con el algoritmo indicado. Si el modo configurado era implícito, los datos estarán contenidos en la firma.

##### **Firma XAdES-BES Enveloped**

* Se prueba la firma XAdES Enveloped en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de datos
    - XML
  + Modos
    - Implícito
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado**: Firmas correctas en todos los casos generadas con el algoritmo indicado.

##### **Firma XAdES-BES Enveloped de documentos no XML**

* Se prueba la firma XAdES Enveloped en todas las combinaciones posibles de los siguientes elementos:
  + Formatos de ficheros de datos
    - Fichero plano
    - Fichero binario
  + Modos
    - Implícito
  + Algoritmos de firma
    - Indiferente
* **Resultado esperado:** Se lanza la excepción “AOFormatFileException”.

##### **Firma XAdES-BES Enveloped explícita**

* Se prueba la firma XAdES Enveloped en todas las combinaciones posibles de los siguientes elementos:
  + Formatos de ficheros de datos
    - XML
  + Modos
    - Explícito
  + Algoritmos de firma
    - Indiferente
* **Resultado esperado:** Se lanza la excepción “UnsupportedOperationException”.

##### **Firma XAdES-EPES Detached**

* Se prueba la firma XAdES-EPES Detached con la política de firma de a AGE en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de datos
    - Texto plano
    - XML
    - Otro formato
  + Modos
    - Implícito
    - Explícito
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado**: Firmas correctas en todos los casos generadas con el algoritmo indicado y la política de firma declarada. Si el modo configurado era implícito, los datos estarán contenidos en la firma.

##### **Firma XAdES-EPES Enveloping**

* Se prueba la firma XAdES-EPES Enveloping con la política de firma de a AGE en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de datos
    - Texto plano
    - XML
    - Otro formato
  + Modos
    - Implícito
    - Explícito
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado**: Firmas correctas en todos los casos generadas con el algoritmo indicado y la política de firma declarada. Si el modo configurado era implícito, los datos estarán contenidos en la firma.

##### **Firma XAdES-EPES Enveloped**

* Se prueba la firma XAdES-EPES Enveloped con la política de firma de a AGE en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de datos
    - XML
  + Modos
    - Implícito
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado**: Firmas correctas en todos los casos generadas con el algoritmo indicado y la política de firma declarada.

##### **Cofirma XAdES**

* Se prueba la cofirma de firmas XAdES, indicando el documento originalmente firmado, en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de firma
    - Firma XAdES-BES Detached
    - Firma XAdES-BES Enveloping
    - Firma XAdES-BES Enveloped
    - Firma XAdES-EPES Detached
    - Firma XAdES-EPES Enveloping
    - Firma XAdES-EPES Enveloped
  + Modos XAdES
    - XAdES-BES
    - XAdES-EPES
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Cofirmas correctas en todos los casos generadas con el algoritmo indicado y siempre con la misma estructura de firma que la firma original (detached, enveloping o enveloped).

##### **Cofirma de ficheros**

* Se prueba la cofirma de ficheros que no sean firmas XAdES en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Ficheros de datos
    - Fichero plano
    - XML
    - Fichero binario
    - Firma XMLdSig
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Lanzará una excepción de tipo AOInvalidFormatException.

##### **Contrafirma de firma/cofirma XAdES**

* Se prueba la contrafirma de firmas XAdES en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Formatos de ficheros de firma
    - Firma XAdES-BES Detached implícita
    - Firma XAdES-BES Detached explícita
    - Firma XAdES-EPES Detached implícita
    - Firma XAdES-EPES Detached explícita
    - Firma XAdES-BES Enveloping implícita
    - Firma XAdES-BES Enveloping explícita
    - Firma XAdES-EPES Enveloping implícita
    - Firma XAdES-EPES Enveloping explícita
    - Firma XAdES-BES Enveloped
    - Firma XAdES-EPES Enveloped
    - Cofirma XAdES Detached
    - Cofirma XAdES Enveloping
    - Cofirma XAdES Enveloped
  + Modos XAdES
    - XAdES-BES
    - XAdES-EPES
  + Nodos objetivo
    - Todos los nodos hijos
    - Todos los nodos
    - Nodos determinados
    - Nodos de firmantes determinados
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Contrafirmas correctas generadas con el algoritmo indicado, el modo XAdES y realizadas sobre los nodos especificado.

##### **Contrafirma de ficheros**

* Se prueba la contrafirma de ficheros que no sean firma XAdES en todas las combinaciones posibles de los siguientes elementos:
  + Certificados
    - ANF Persona Física
    - CatCert
    - Camerfirma
  + Ficheros de datos
    - Fichero plano
    - XML
    - Fichero binario
    - Firma XMLdSig
  + Algoritmos de firma
    - SHA1withRSA
    - SHA-512withRSA
    - MD2withRSA
    - MD5withRSA
    - SHA-256withRSA
    - SHA-384withRSA
* **Resultado esperado:** Lanzará una excepción de tipo AOInvalidFormatException.

##### Comprobación de documento válido para firma

* Se prueba si un fichero es válido para realizar una firma XAdES sobre él. Se probará con:
  + Ficheros de datos
    - Fichero plano
    - XML
    - Fichero binario
    - Firma XAdES
    - Firma XMLdSig
* **Resultado esperado:** Siempre se devolverá “true”.

##### Comprobación de firmas XAdES

* Se prueba si un fichero es realmente una firma XAdES. Se probará con los siguientes ficheros:
  + Firma XAdES-BES Detached implícita
  + Firma XAdES-BES Detached explicita
  + Firma XAdES-BES Enveloping implícita
  + Firma XAdES-BES Enveloped explicita
  + Firma XAdES-BES Enveloping
  + Firma XAdES-EPES Detached implícita
  + Firma XAdES-EPES Detached explicita
  + Firma XAdES-EPES Enveloping implícita
  + Firma XAdES-EPES Enveloped explicita
  + Firma XAdES-EPES Enveloping
  + Cofirma XAdES-BES
  + Cofirma XAdES-EPES
  + Contrafirma XAdES-BES
  + Contrafirma XAdES-EPES
* **Resultado esperado:** El método devolverá “true”.

##### Comprobación de firmas XAdES con ficheros no XAdES

* Se prueba si un fichero es realmente una firma XAdES. Se probará con los siguientes ficheros:
  + Fichero plano
  + XML
  + Fichero binario
  + Firma XMLdSig
* **Resultado esperado:** El método devolverá “false”.

##### Extracción de datos generales de firmas XAdES

* Se extrae la información general de una firma XAdES con los siguientes ficheros:
  + Firma XAdES-BES Detached implícita
  + Firma XAdES-BES Detached explicita
  + Firma XAdES-BES Enveloping implícita
  + Firma XAdES-BES Enveloped explicita
  + Firma XAdES-BES Enveloping
  + Firma XAdES-EPES Detached implícita
  + Firma XAdES-EPES Detached explicita
  + Firma XAdES-EPES Enveloping implícita
  + Firma XAdES-EPES Enveloped explicita
  + Firma XAdES-EPES Enveloping
  + Cofirma XAdES-BES
  + Cofirma XAdES-EPES
  + Contrafirma XAdES-BES
  + Contrafirma XAdES-EPES
* **Resultado esperado:** Objeto AOSignInfo cuyo formato declarado es “XAdES" y la variante la correspondiente al fichero (Detached, Enveloping o Enveloped).

##### Extracción de datos generales con ficheros no XAdES

* Se extrae la información general de una firma XAdES con los siguientes ficheros:
  + Fichero plano
  + XML
  + Fichero binario
  + Firma XMLdSig
* **Resultado esperado:** Se lanza la excepción “AOInvalidFormatException”.

##### Extracción de datos firmados de firmas XAdES implícita sobre XML

* Se extraen el XML firmado de los siguientes ficheros XAdES firmados:
  + Firma XAdES-Detached implícita de datos XML
  + Cofirma XAdES-Detached implícita de datos XML
  + Contrafirma XAdES-Detached implícita de datos XML
  + Firma XAdES- Enveloping implícita de datos XML
  + Cofirma XAdES- Enveloping implícita de datos XML
  + Contrafirma XAdES- Enveloping implícita de datos XML
  + Firma XAdES-Enveloped
  + Cofirma XAdES- Enveloped
  + Contrafirma XAdES- Enveloped
* **Resultado esperado:** Se extrae el XML originalmente firmado.

##### Extracción de datos firmados de firmas XAdES implícitas sobre datos binarios

* Se extraen los datos originalmente firmados de los siguientes ficheros XAdES firmados:
  + Firma XAdES-Detached implícita de datos binarios
  + Cofirma XAdES-Detached implícita de datos binarios
  + Contrafirma XAdES-Detached implícita de datos binarios
  + Firma XAdES- Enveloping implícita implícita de datos binarios
  + Cofirma XAdES- Enveloping implícita de datos binarios
  + Contrafirma XAdES- Enveloping implícita de datos binarios
* **Resultado esperado:** Se extraen los datos binarios originalmente firmados.

##### Extracción de datos firmados de firmas XAdES explícitas

* Se extraen los datos originalmente firmados de los siguientes ficheros XAdES firmados:
  + Firma XAdES-Detached explícita
  + Cofirma XAdES-Detached explícita
  + Contrafirma XAdES-Detached explícita
  + Firma XAdES- Enveloping explícita
  + Cofirma XAdES- Enveloping explícita
  + Contrafirma XAdES- Enveloping explícita
* **Resultado esperado:** Se extrae la huella digital de los datos originalmente firmados.

##### Extracción de datos firmados de ficheros no XAdES

* Se extraen los datos firmados de los siguientes ficheros:
  + Fichero plano
  + XML
  + Fichero binario
  + Firma XMLdSig
* **Resultado esperado:** Se lanza la excepción “AOInvalidFormatException”.

##### Obtención de la estructura de firmantes de firmas XAdES

* Se extrae el árbol de firmantes de ficheros del siguiente tipo:
  + Firma XAdES Detached implícita
  + Firma XAdES Detached explicita
  + Firma XAdES Enveloping implícita
  + Firma XAdES Enveloped explicita
  + Firma XAdES Enveloping
  + Cofirma XAdES
  + Contrafirma XAdES
* **Resultado esperado:** Se obtiene el árbol de firmas correspondiente a cada documento.

##### Obtención de la estructura de firmantes de ficheros no XAdES

* Se extrae el árbol de firmantes de documentos del siguiente tipo:
  + Fichero plano
  + XML
  + Fichero binario
  + Firma XMLdSig
* **Resultado esperado:** Se lanza una excepción de tipo “AOInvalidFormatException”.

##### Generación de firmas XAdES sin la cadena de certificación completa (Ticket 209544)

* Se generan firmas XAdES con la propiedad “includeOnlySignningCertificate” configurada a “true”.
  + Los tipos de firmas generados son:
    - XAdES-BES Detached
    - XAdES-BES Enveloping
    - XAdES-BES Enveloped
* **Resultado esperado:** Se obtiene una firma sólo con el certificado firmante.

##### Generación de cofirmas XAdES sin la cadena de certificación completa (Ticket 209544)

* Se generan cofirmas XAdES con la propiedad “includeOnlySignningCertificate” configurada a “true”.
  + Los tipos de firmas generados son:
    - XAdES-BES Detached
    - XAdES-BES Enveloping
    - XAdES-BES Enveloped
* **Resultado esperado:** Se obtiene una cofirma sólo con el certificado firmante.

##### Generación de contrafirmas XAdES sin la cadena de certificación completa (Ticket 209544)

* Se generan contrafirmas XAdES con la propiedad “includeOnlySignningCertificate” configurada a “true”.
  + Los tipos de firmas generados son:
    - XAdES-BES Detached
    - XAdES-BES Enveloping
    - XAdES-BES Enveloped
  + Los nodos objetivos son:
    - Todos los nodos.
* **Resultado esperado:** Se obtiene una contrafirma sólo con el certificado firmante.

## **Applet Cliente @firma**

### **Pruebas funcionales de usuarios finales**

#### **Entorno contemplados en las pruebas**

**Las pruebas funcionales de usuario final se realizan en los siguientes entornos:**

* **Sistemas Operativos**
  + **Windows 7 64 bits**
  + **Windows 7 32 bits**
  + **Windows XP 32 bits**
  + **Mac OS X Lion (64 bits)**
  + **Ubuntu 32 bits**
* **Navegadores Web**
  + **Internet Explorer 9 (únicamente Windows 7)**
  + **Internet Explorer 9 64 bits (únicamente Windows 7)**
  + **Internet Explorer 8 (únicamente Windows XP)**
  + **Mozilla Firefox 3.6**
  + **Mozilla Firefox 12**
  + **Apple Safari 5.1 (excepto Linux)**
  + **Google Chrome 19**
  + **Opera 11 (excepto Mac OS X)**
* **Entorno de ejecución de Java (Siempre en la misma arquitectura que el navegador)**
  + **6u32 32 bits**
  + **6u32 64 bits**
  + **7u4 32 bits (excepto Mac OS X)**
  + **7u4 64 bits (excepto Mac OS X)**

#### **Operaciones probadas**

* Carga del Applet
  + Se comprueba la correcta carga del Applet mediante las funciones estándar de carga.
* Prueba de firma
  + Se firma un fichero (sin establecerlo, usando diálogo gráfico del Applet) usando todos los formatos de firma posibles (CAdES, XAdES, OOXML, ODF, PAdES, CMS, XMLDSig). La prueba se realiza primero con un certificado software y se repite con un DNIe.
    - Esta prueba permite asegurar una correcta carga del almacén de claves (incluyendo la agregación de módulos PKCS#11 en Mozilla) y la correcta incorporación de todas los módulos relacionados.
* Prueba de cofirma
  + En base a ficheros de prueba (los mismos de las pruebas unitarias), se repiten las mismas pruebas que en la firma, solo que indicando una cofirma. La prueba se repite con contrafirma (cambiando el conjunto de ficheros de prueba).
* Prueba de firma masiva
  + Prueba básica de firma de directorios. Usando un conjunto de ficheros y carpetas de prueba que replican las situaciones menos habituales.
  + Prueba básica de firma masiva programática. Usando un conjunto de ficheros y carpetas de prueba que replican las situaciones menos habituales.
* Prueba de firma Web
  + Prueba básica de firma Web.
* Prueba de cifrado
  + Cifrado y descifrado de ficheros usando todos los algoritmos posibles, tanto basados en claves como basados en contraseñas.
* Pruebas de sobre digital
  + Ensobrado y apertura de sobres usando todos los formatos soportados de sobre.
  + Prueba específica de lectura de claves públicas:
    - Desde LDAP
    - Desde certificado en disco (CER/BER/PEM)
    - Desde la libreta de direcciones de Windows (únicamente en Windows)
* Pruebas de almacenes de claves y certificados
  + Pruebas de establecimiento forzado de almacén de claves (pasando del nativo a PKCS#12). La operación de prueba concluye con una firma para comprobar la corrección del cambio.