Descripción del sistema de firma electrónica de SEDIPUALB@

DIPUTACIÓN DE ALBACETE

SEDIPUALB@

Autor: Javier Vico Egea

Servicio de Modernización Administrativa y TIC

Diputación de Albacete

Versión 1.0 - Fecha de la última edición: 29 de abril de 2022

Índice

Introducción

El sistema de firma es el encargado de:

- Recoger las firmas de los usuarios y verificarlas.
- Sellar electrónicamente documentos por parte de la Sede.
- Asegurar la integridad de los documentos, firmas y demás datos asociados.
- Permitir el acceso a todo ello, de la forma más transparente posible, con las restricciones que se expondrán más adelante en este documento.

El sistema de firma depende de aplicaciones clientes, tales como SEFYCU o SERES, para determinar qué documentos deben firmarse, cómo deben firmarse y quiénes deben firmarlos.

Principios básicos de criptografía relativos a la firma digital

Antes de empezar, conviene revisar rápidamente algunos conceptos básicos de criptografía.

La firma digital garantiza las siguientes propiedades:

- Autentificación: el autor de la firma queda perfectamente identificado.
- Integridad: cualquier modificación (pequeña o grande) del documento firmado invalida la firma.
- No repudio: el autor de la firma no puede negar haber sido él quien lo firmó.

Para firmar un documento se sigue el siguiente patrón:

1. Se calcula el hash del documento original a firmar.
2. Se utiliza la clave privada del certificado digital para cifrar el hash. Esto es la firma digital.
3. Según el estándar de firma usado (PAdES, CAdES, XAdES Attached, Detached, Enveloped) se elabora un fichero tomando la firma digital del paso anterior más el hash o el documento original completo y otros datos como el certificado y la cadena de certificación del mismo.

Puesto que la firma digital deja de considerarse válida cuando caduca el certificado digital utilizado, se añade un cuarto paso:

4. Se sella el documento firmado por una autoridad en la que se confía. Dicho sello consiste en un timestamp y una firma, que se hace igual que en los pasos 1 y 2

anteriores, e inserta el resultado en el mismo fichero estándar generado en el paso 3. Este sello garantiza que la firma del paso 2 era válida en el momento del sello.

Esta nueva firma también deja de considerarse válida cuando caduca el certificado digital utilizado por la autoridad correspondiente, por lo que antes de que esto ocurra debe realizarse un resellado con un nuevo certificado que prorrogue la validez tantas veces como se necesite. Esta operación debe hacerse antes de que caduque el certificado con el que se realizó el último sello (o la firma original, si es el primer sello que se hace).

Por otra parte, el proceso de validación sigue la siguiente secuencia:

1. Se calcula el hash del documento firmado.
2. Se descifra la firma digital utilizando la clave pública del certificado.
3. El resultado del paso 1 y del paso 2 deben ser idénticos
4. Se comprueba que el certificado no esté caducado ni revocado, y que la firma del mismo por parte del certificado anterior en la cadena de certificación sea válida. Esto se repite para cada certificado en la cadena de certificación hasta llegar a una autoridad de certificación en la que se confíe. Si se llega a la raíz de la cadena de certificación y no se confía en él, la firma no se considerará válida.

Si el documento contiene sellos de tiempo, se sigue un esquema similar con la firma del último sello incluido.

Puesto que la firma digital usa criptografía asimétrica y ésta es muy costosa para aplicarse directamente sobre muchos datos, hemos visto que se usa una función hash r(m), la cual cumple las siguientes propiedades:

1. r(m) es de longitud fija, independientemente de la longitud de m.
2. Dado m es sencillo calcular r(m).
3. Dado r(m), es computacionalmente intratable recuperar m.
4. Dado m, es computacionalmente intratable obtener un m' tal que r(m)=r(m').

La propiedad 4 anterior es muy importante, pues sin dicha propiedad un firmante podría alegar que él no firmó un determinado documento sino otro, ya que a la fuerza deben existir muchos documentos (m') que generan el mismo hash (r(m')). Sin embargo, gracias a esta propiedad, por mucho que busque otros documentos no será capaz de encontrarlos durante un periodo de tiempo razonable. Sin esta propiedad, no se podría garantizar el no repudio ni la integridad de la firma.

Funcionamiento

La firma de los usuarios

Cuando la aplicación que usa la firma electrónica y el usuario determinan los documentos a firmar, a los que llamaremos *“documentos originales”*, se inicia una sesión de firma, en la que el usuario puede revisar dichos documentos antes de firmarlos.

Una vez confirmada la operación, el sistema elabora un fichero XML, que llamaremos *“documento de firma combinado”*, y lo envía al firmante, que lo firma usando uno de los clientes de firma oficiales de *@firma* (*AutoFirma*, *Cliente de @firma Móvil*, etc.) y compone el documento firmado resultante según el estándar *XAdES-BES enveloping*.

El documento firmado resultante se envía de vuelta al servidor, que lo valida, lo actualiza inmediatamente al formato *XAdES-A* (para garantizar su verificabilidad en el futuro) y lo almacena.

A continuación, para cada *“documento original”*, se elabora un nuevo documento PDF que, además del contenido original del documento, incluye una serie de datos adicionales. Llamaremos a este documento *“documento auténtico”* a modo de certificación emitida por la Sede de que las firmas que se han realizado son correctas.

Periódicamente, antes de que caduque el certificado de sello de tiempo del Ministerio de Defensa (con el que @firma sella los documentos XAdES-A) se realiza un nuevo resellado para prorrogar la validez del sello anterior.

El *“documento de firma combinado”*

En el “documento de firma combinado”, mencionado anteriormente, se enumeran las huellas digitales de cada uno de los documentos del lote que el usuario se dispone a firmar en la sesión de firma.

De este modo, aunque el usuario pretenda firmar 200 documentos de gran tamaño, el cliente de firma sólo recibe un único documento XML de tamaño pequeño.

La *“huella digital del documento para el firmante”*

Llamaremos “huella digital del documento para el firmante” a la huella digital de cada documento mencionada anteriormente (pues es diferente para cada documento y firmante), y se calcula aplicando el algoritmo de hash SHA3-512 sobre el resultado de concatenar:

- Los datos del documento a firmar en binario.

- El título del documento codificado en UTF-8.
- El texto del firmante codificado en UTF-8, que es el texto que se muestra en el margen del PDF, donde se indica en calidad de qué cargo se realiza la firma, pudiendo incluir también el propósito de la firma (certificar, visto bueno, etc).
- Un código de 128 Bytes aleatorios llamado *"sal"* (en relación con el concepto *salted hashing*) para reducir las probabilidades de encontrar una colisión (*second-preimage attack*).

Formato del *"documento de firma combinado"*

El formato de este documento XML tiene la siguiente estructura:

```
<documentos_firmados>
      <documento_firmado>
            <id>
                  [Identificador del firmante en el documento]
            </id>
            <hash>
                  [Huella digital del documento para este
firmante
                                          codificada en Base64]
            </hash>
            <salt>
                  [Sal de 128 bytes en Base64 usada para el hash]
            </salt>
      </documento_firmado>
      <documento_firmado>
            <id>
                  [Identificador del firmante en el documento]
            </id>
            <hash>
                  [Huella digital del documento para este
firmante
                                          codificada en Base64]
            </hash>
            <salt>
                  [Sal de 128 bytes en Base64 usada para el hash]
            </salt>
      </documento_firmado>
      ...
</documentos_firmados>
```

El certificado de sello electrónico de la Sede

Certificado digital emitido por alguno de los prestadores de servicios electrónicos de confianza cualificados según el Ministerio de Energía, Turismo y Agenda Digital, y que pertenece a la categoría de "certificado de sello electrónico". Cada Sede puede tener un único certificado de sello electrónico en vigor.

En el caso de que una Sede no disponga de un certificado propio, se utilizará por defecto el certificado de sello electrónico de la plataforma Sedipualb@.

El certificado de sello electrónico de cada Sede puede obtenerse en la URL siguiente:

https://[dominio de la sede]/certificadosello/

El *"documento auténtico"*

Este documento, en formato PDF PAdES, funciona a modo de certificación emitida por la Sede para asegurar que el documento original fue firmado (en formato XAdES) por los firmantes descritos en él, como se describió anteriormente.

Este documento se genera la primera vez que se accede a él, e incluye los siguientes datos:

- El *código seguro de verificación* (*CSV*), que permite acceder a este documento desde la Sede, así como a la información de los firmantes y demás datos necesarios para reproducir y verificar las firmas.
- El título del documento.
- Identificación de la Sede Electrónica a la que pertenece y su URL.
- Instrucciones para llegar al documento auténtico bajo custodia.
- Código QR con la URL directa para acceder a toda la información relativa a este documento, incluida su descarga.
- Para cada firmante: "la huella digital del documento para el firmante" (en código QR) y el texto de su firma.
- El número total de páginas.
- El logo de la entidad.

Estos datos se pueden presentar en diferentes formatos:

- Convencional:
    - Solo documentos de tamaño A4, en vertical o apaisado, (si las páginas tienen otro tamaño, se ajustan a A4 automáticamente).

    - En el margen de cada una de las páginas del documento aparecen los firmantes, siempre y cuando el número de estos sea menor o igual que 4. Para un mayor número de firmantes, éstos se muestran en una o varias páginas adicionales al final del documento, del mismo modo que para el formato reducido.
    - También se numera cada página del documento.
- Reducido:
    - Las páginas del documento original no se alteran.
    - Permite cualquier tamaño de página.
    - Toda la información relacionada anteriormente se añade en una o varias páginas al final o principio del documento.

El documento PDF resultante se firma en formato PAdES, usando el certificado de sello electrónico de la Sede.

En un proceso diferido, y en horario nocturno, se intenta periódicamente la actualización de este documento al formato *PAdES LTV,* para asegurar su validez tras la caducidad del certificado de sello electrónico de la Sede. Sin embargo, aunque este proceso no tenga éxito (ver apartado *Problemas de rendimiento del sistema @firma*), la caducidad de esta firma se puede subsanar simplemente descargando de nuevo el documento desde la Sede, usando el CSV correspondiente. El sistema detectará que el documento PDF previo ya no es válido y generará en ese momento un nuevo PDF, firmándolo otra vez con el certificado de sello electrónico en curso.

Cada firma adicional que se realice posteriormente sobre este documento generará de nuevo el *"documento auténtico"*, repitiendo todo el proceso descrito en este apartado.

Sellos electrónicos de la Sede

Algunas de las firmas electrónicas realizadas sobre un documento pueden ser sellos electrónicos realizados por la Sede. Solo se diferencian de las firmas de los usuarios en que, en lugar de realizarlas una persona con su certificado digital, las realiza el propio sistema empleando el certificado de sello electrónico de la Sede. Por lo demás, se aplica lo mismo que se ha explicado para las firmas de los usuarios.

Al igual que las firmas de los usuarios, los sellos electrónicos también constan de un *"texto del firmante"*, que determina el propósito del sello. Por ejemplo, en el caso de instancias electrónicas consiste en la fecha y número de entrada en registro. En el caso de oficios de remisión de notificaciones, consiste en el número y fecha del registro de salida. También se utiliza para certificar el pago de una tasa o el acceso por parte de un interesado a una notificación electrónica.

Este sello electrónico (realizado por la Sede) no debe confundirse con los sellos de tiempo que realiza @firma al efectuar la actualización desde XAdES-BES a XAdES-A o desde PAdES a PAdES LTV.

Por otra parte, la actualización a XAdES-A de la firma correspondiente al sello electrónico de la Sede sirve como garantía adicional de la fecha y hora del sistema, pues dicha actualización incluye la marca de tiempo del Real Observatorio de la Armada (que determina la hora legal oficial en España), que la plataforma TS@ genera a través de @firma.

Firmas biométricas

El sistema también permite que las firmas se puedan realizar mediante tabletas de firma manuscrita, que capturan, además del dibujo de la firma, datos biométricos tales como presión y velocidad. Actualmente solo se admite el modelo WACOM STU-430.

Para la captura de la firma, al igual que ocurre con la firma electrónica y los clientes de firma, es necesario tener instalada una aplicación auxiliar llamada BiofirmaDipualba, que se encarga de la comunicación con el dispositivo y el envío del resultado de la firma al servidor. También es necesario tener instalados los drivers del dispositivo correspondiente.

El procedimiento completo es:

1. El empleado público solicita el documento de identidad (DNI, pasaporte o documento de identidad de la Unión Europea) al firmante y comprueba que sus datos personales corresponden con los que constan en el sistema.
2. Se compone el *"documento de firma combinado"* del mismo modo que para una firma electrónica de usuario.
3. Se eliminan los espacios en blanco y se canonicaliza según el procedimiento estándar del W3C (https://www.w3.org/TR/xml-c14n11/).
4. Se calcula el hash SHA3-512 y se codifica en Base64. Llamaremos al resultado *"huella digital combinada"*.
5. Esta huella y la hora y fecha del PC conectado a la tableta de firma se muestran en la pantalla de esta. El mismo hash se mostrará en la web de firma, donde también estará disponible el listado de PDFs a firmar para que el empleado público pueda facilitárselos al firmante.
6. El firmante firma.
7. El empleado público comprueba que la firma trazada corresponde con la firma que consta en el DNI.
8. En el servidor se almacena el fichero de firma generado por el dispositivo y el dibujo de la firma.
9. Se sella electrónicamente (siguiendo el mismo proceso descrito en el apartado *"Sellos electrónicos de la Sede"*) un documento XML que contiene tanto la huella mostrada en la pantalla del dispositivo antes de firmar, como el contenido del fichero de firma generado por este después de firmar. También se incluye el *"documento de firma combinado"*, los datos personales del firmante y los datos personales del empleado que recoge la firma. El formato del documento XML sellado es el siguiente:

```
<firma_biometrica>
	<contenido_firma>
		[Resultado de la firma biometrica codificado en Base64]
	</contenido_firma>
	<texto_pantalla>
		[Texto mostrado en la pantalla del dispositivo al firmar]
	</texto_pantalla>
	<documentos_firmados>
		<documento_firmado>
			<id>
				[Identificador del firmante en el documento]
			</id>
			<hash>
				[Huella digital del documento para este firmante
                                                codificada en Base64]
			</hash>
			<salt>
				[Sal de 128 bytes en Base64 usada para el hash]
			</salt>
		</documento_firmado>
		…
	</documentos_firmados>
	<firmante>
		<documento_identidad>[...]</documento_identidad>
		<nombre>[...]</nombre>
		<apellido1>[...]</apellido1>
		<apellido2>[...]</apellido2>
	</firmante>
	<empleado>
		<nif>[...]</nif>
		<nombre>[...]</nombre>
		<apellido1>[...]</apellido1>
		<apellido2>[...]</apellido2>
	</empleado>
</firma_biometrica>
```

Firmas bajo pseudónimo

Las aplicaciones que definen las firmas que se deben realizar en un documento pueden establecer opcionalmente que estas se hagan bajo pseudónimo, lo que hace que se oculten al público sus datos personales en la información que se muestra en la web al acceder con el CSV correspondiente (ver apartado “Información disponible en la Sede Electrónica”).

En el caso de firmas electrónicas, tampoco está accesible al público el documento XAdES de la firma electrónica (pues revelaría los datos personales, ya que incluye el certificado digital del firmante).

En el caso de firmas biométricas, además de los datos que normalmente se ocultan al público (ver apartado *"Información disponible en la Sede Electrónica"*), tampoco está accesible al público el dibujo de la firma.

Todos estos datos sí están disponibles para los administradores de la Sede.

Importación de firmas ajenas al sistema

Cuando el *"documento original"* a firmar sea un documento PDF con firmas PAdES realizadas de forma externa al sistema (por ejemplo, realizadas mediante herramientas como Adobe Reader, XolidoSign o, incluso, AutoFirma, si la operación de firma no se inició desde la Sede), el sistema intentará validarlas usando la plataforma @firma.

Si la validación es satisfactoria, se importarán los datos del firmante y se mostrará como una firma electrónica más del documento, con una salvedad: debido a que no es posible garantizar que la fecha y hora de la firma no hayan podido ser manipuladas por el firmante, se incluirá un mensaje indicando que dicha fecha y hora procede del equipo del firmante.

Periódicamente se intentará el sellado PAdES LTV del documento original para asegurar la verificabilidad de las firmas tras la caducidad del certificado original de la firma o del último sello PAdES. Ver apartado *Problemas de rendimiento del sistema @firma*.

Si la validación de las firmas no es satisfactoria, no se importarán, pero se mostrará un mensaje indicando que el documento original contenía firmas que no se pudieron validar, invitando al usuario a que acceda al documento original con dichas firmas, para que las considere o no bajo su responsabilidad.

Si el documento original a firmar corresponde a un *"documento auténtico"* y, por tanto, va firmado con el certificado de sello electrónico de la Sede, se importarán sin ninguna distinción las firmas y sellos asociados al CSV correspondiente. No se importará la firma del certificado de sello electrónico de la Sede del PDF, pues no aportaría nada. Para más información ver apartado *"Códigos CSV"*.

Información disponible en la Sede Electrónica

El *"documento original"*, el *"documento auténtico"*, el *"documento de firma combinado"*, la *"huellas digitales del documento para los firmantes"* y toda la información de las firmas están a disposición de los ciudadanos en la Sede Electrónica, de forma totalmente transparente, siempre que se disponga del código CSV correspondiente.

También está disponible la explicación de este proceso de firma y del proceso a seguir para verificarlas.

Sin embargo, algunos datos de la firma son de acceso restringido. Solo los administradores de la Sede pueden acceder a ellos. En concreto, son:

- Los ficheros generados por las tabletas de firma en las firmas biométricas, así como los correspondientes sellos electrónicos y los datos personales de los empleados públicos que las recogen. Sí estará disponible públicamente el dibujo de la firma.
- En el caso de firmas bajo pseudónimo, se restringirá el acceso a los datos indicados en el apartado *"Firmas bajo pseudónimo"*.

Códigos CSV

El código CSV, o Código Seguro de Verificación, es un código alfanumérico de 20 caracteres que da acceso al *"documento auténtico"*, *"documento original"* y al resto de datos relacionados en el apartado anterior *"Información disponible en la Sede Electrónica"*.

Un mismo *"documento original"* puede usarse para generar diferentes códigos CSV, con diferentes conjuntos de firmantes (electrónicos o biométricos) y sellos electrónicos de la Sede.

El sistema es capaz de detectar e importar firmas y sellos de otro CSV en un nuevo CSV de la misma Sede.

Por ejemplo, en el caso de que un ciudadano anexe a una instancia de la Sede un "documento auténtico" correspondiente a un CSV con dos firmas, al registrarlo, se generará un nuevo CSV con las dos firmas del CSV original y un nuevo sello electrónico con el número de entrada en registro de la nueva instancia. En este caso las firmas asociadas al CSV original permanecen inalteradas y el nuevo sello electrónico solo se mostrará en el segundo CSV generado.

Otro ejemplo es el de un documento firmado por una persona A, que se decide notificar electrónicamente a dos destinatarios, produciendo dos números de registro de salida cuyos valores se incluirían, respectivamente, en los sellos electrónicos B y C. Así, podríamos tener un CSV que muestre solo la firma A, otro que se use para la notificación del primer destinatario incluyendo la firma A y el sello con el número de registro de salida B, y otro CSV para la notificación del segundo destinatario con la firma A y el sello con el número de registro de salida C. De este modo tendríamos 3 CSVs compartiendo la misma firma A, a pesar de que el firmante solo firmó una vez, incluso antes de que se decidiera generar los dos CSVs de las notificaciones.

Además, las aplicaciones pueden seguir añadiendo más firmas y sellos a un CSV posteriormente, aunque nunca eliminar las ya realizadas.

Un ejemplo de esto sería el de un SEFYCU que firma una persona y se completa pero, más tarde, se decide añadirle otro firmante, cuya firma aparecerá en el mismo CSV de antes.

Respecto al formato de los códigos CSV, estos constan de 20 caracteres para garantizar las combinaciones suficientes para todas las Sedes en SEDIPUALB@ actuales y futuras, así como la seguridad necesaria para evitar descubrir códigos mediante ataques por fuerza bruta.

Los caracteres que pueden aparecer en los códigos CSV son números y letras mayúsculas, en los que se eliminan algunos caracteres que pueden confundirse entre sí, como el 0 y O, 8 y B, etc. Así, cada carácter consta de 26 posibles valores: ACDEFHJKLMNPQRTUVWXYZ23479.

La composición del código sería:

- 2 dígitos para identificar la entidad de la Sede.
- 2 dígitos flexibles, que se pueden usar, o bien para codificar la entidad de la Sede, o bien el identificador único del CSV dentro de dicha Sede.
- 5 dígitos para codificar el identificador único del CSV para una Sede concreta.
- 10 dígitos aleatorios para garantizar la seguridad.
- 1 dígito de control que se calcula a partir del resto.

Dependiendo de cómo se usen los dígitos flexibles, habrá cabida para un número de Sedes entre 676 y 456.976 y un número de CSVs para cada Sede entre 11.881.376 y 8.031.810.176.

Inicialmente se usarán los 2 dígitos flexibles para codificar la Sede, es decir, 4 en total, pero se asignarán a cada Sede de modo que no se solapen los dos primeros dígitos de ninguna entidad.

Por ejemplo:

- AAAA: Ayuntamiento de Albacete
- ACAA: Ayuntamiento de Cartagena
- ADAA: Ayuntamiento de Abengibre
- ...

Así, en caso de que una entidad necesite más de 11 millones de códigos CSV, se le asignarán también los códigos de entidad de 4 dígitos contiguos que compartan los 3 primeros dígitos o, incluso, los 2 primeros dígitos:

- AAA*: Ayuntamiento de Albacete (308.915.776 CSVs diferentes)
- AC**: Ayuntamiento de Cartagena (8.031.810.176 CSVs diferentes)
- ADAA: Ayuntamiento de Abengibre (11.881.376 CSVs diferentes)

Los siguientes 10 dígitos aleatorios permiten más de 141 billones de combinaciones, lo que, suponiendo un ataque que intente 1000 combinaciones por segundo, requeriría más de 4.400 años para probar todas las combinaciones. Como medida de seguridad adicional, se bloquean los accesos en los que se detecta el intento de descubrir códigos CSV mediante ataques por fuerza bruta.

El dígito de control será el carácter del alfabeto de 26 caracteres que ocupa la posición resultante del siguiente cálculo:

1. Se comienza con el valor 0 en producción y 1 en preproducción.
2. Para cada dígito, se suma al valor anterior el resultado de multiplicar el índice del mismo (comenzando en 1 en el dígito más a la izquierda) con el código ASCII de éste.

3. Se obtiene el resto de dividir el valor anterior entre el número de caracteres del alfabeto (26).

Para facilitar la lectura y escritura del código, los dígitos se agrupan de 4 en 4.

El procedimiento de verificación de una firma

Aunque puede parecer obvio, es necesario concretar y dar difusión al procedimiento a seguir para verificar que un documento auténtico que llega a nuestras manos es válido y ha sido firmado correctamente por las personas que en él se indican. No es admisible que se dé por válido un documento supuestamente firmado, simplemente porque tiene un código de barras o QR impreso.

La verificación rápida

Esta verificación sería la habitual por parte de un empleado público o cualquier otro usuario que, **confiando** en nuestro sistema, quiera comprobar que un documento ha sido correctamente firmado. Constaría de los siguientes pasos:

- Si el documento llega a manos del usuario en formato papel:
    a. Desde un ordenador o dispositivo libre de malware, actualizado y en el que no haya sido instalada ninguna autoridad de certificación falsa, acceder a la web de la Sede Electrónica correspondiente. El usuario (especialmente si es un empleado público) debería conocer dicha dirección y no debería usar la URL impresa en el documento, pues esta podría haber sido manipulada maliciosamente para que el usuario acceda a una web falsa (phishing).
    b. Comprobar que el navegador no muestra ninguna alerta sobre la validez del certificado SSL de la web.
    c. Al introducir el código CSV impreso en el documento, podrá obtener la copia electrónica del documento auténtico.
    d. Los documentos impreso y electrónico deben ser iguales. En otro caso, estaríamos ante una posible falsificación.
- Si el documento llega al usuario en formato electrónico (fichero PDF):
    a. Desde un ordenador o dispositivo libre de malware, actualizado y en el que no haya sido instalada ninguna autoridad de certificación falsa, abrir *Adobe Reader* (o software equivalente con capacidad para validar firmas PAdES en que se confíe). También se puede emplear la herramienta “validar firma” de la plataforma VALIDe (https://valide.redsara.es/).
    b. Comprobar que el documento ha sido firmado electrónicamente por el certificado de sello electrónico correspondiente a la Sede Electrónica en cuestión, y que dicha firma es válida.
    El certificado de sello electrónico en vigor de cada Sede está disponible en la dirección:
    https://[dominio de la Sede]/certificadosello/
    c. Si la firma no es válida, puede deberse a que el certificado de sello usado originalmente ya ha caducado (y no fue posible hacer la actualización a PAdES

LTV, ver apartado *Problemas de rendimiento del sistema @firma*). En este caso puede usarse el CSV para descargar el documento auténtico actualizado, del mismo modo que se indicó en el caso del formato papel.

Una vez verificado el documento por el procedimiento anterior, se puede confiar en que los firmantes impresos en el documento PDF efectivamente lo han firmado.

La verificación avanzada

Esta verificación sería la que un usuario que **desconfía** de nuestro sistema debe llevar a cabo para comprobar que un documento ha sido firmado correctamente.

Puesto que el proceso de firma solo usa estándares, cualquier usuario (con la habilidad necesaria) podría verificarlo. Todos los elementos necesarios están disponibles en la Sede (contando con que se dispone del CSV correspondiente).

Para cada firmante del documento:

1. Descargar el fichero XAdES-A desde la Sede usando el CSV.
2. Al ser un formato estándar, se pueden usar herramientas externas para validar las firmas e identificar a los firmantes, como por ejemplo, VALIDe (https://valide.redsara.es/).
3. Calcular el hash SHA3-512 sobre el resultado de concatenar el documento binario original + el título del documento codificado en UTF-8 + el texto del firmante codificado en UTF-8 + la "sal". Todos estos datos están accesibles desde la Sede mediante CSV.
4. Abrir el fichero XAdES-A y comprobar que en él aparece un elemento *documento_firmado* con el hash calculado anteriormente y la "sal" utilizada, ambos codificados en Base64:

```
<documentos_firmados>
      ...
      <documento_firmado>
            <id>
                  [Identificador del firmante en el documento]
            </id>
            <hash>
                  [Huella digital del documento para este
firmante
                                          codificada en Base64]
            </hash>
            <salt>
                  [Sal de 128 bytes en Base64 usada para el hash]
            </salt>
      </documento_firmado>
      ...
```

5. Comprobar que lo anterior está cubierto por las firmas del documento XAdES, es decir, el XPath anterior debe estar incluido en alguna de las referencias en SignedDataObjectProperties.
6. Siendo todo lo anterior correcto, quedaría demostrado que el documento original fue firmado electrónicamente con todas las garantías: autenticidad, integridad y no repudio.

Problemas de rendimiento del sistema @firma

Como se ha visto en los apartados anteriores, este sistema de firma depende de @firma para realizar las siguientes operaciones:

1. Validación de firmas XAdES-BES y obtención de los datos de la personas que lo firman.
    - Se utiliza al validar la firma electrónica de los usuarios (ver apartado *"La firma de los usuarios"*).
2. Conversión y sellado de XAdES-BES a XAdES-A y resellado periódico de XAdES-A.
    - Se utiliza para asegurar la verificabilidad a largo plazo de las firmas electrónicas, biométricas y sellos electrónicos de la Sede (ver apartados *"La firma de los usuarios"*, *"Sellos electrónicos de la Sede"* y *"Firmas biométricas"*).
3. Validación de firmas PAdES y obtención de los datos de las personas que lo firman.
    - Se utliza para validar las firmas de los documentos originales que puedan ir firmados externamente (ver apartado *"Importación de firmas ajenas"*).
4. Conversión y sellado de PAdES a PAdES LTV y resellado periódico de PAdES LTV.
    - Se utiliza para asegurar la verificabilidad a largo plazo de los documentos firmados externamente (ver apartado *"Importación de firmas ajenas"*) y de los "documentos auténticos" generados por la Sede (ver apartado *"El documento auténtico"*).

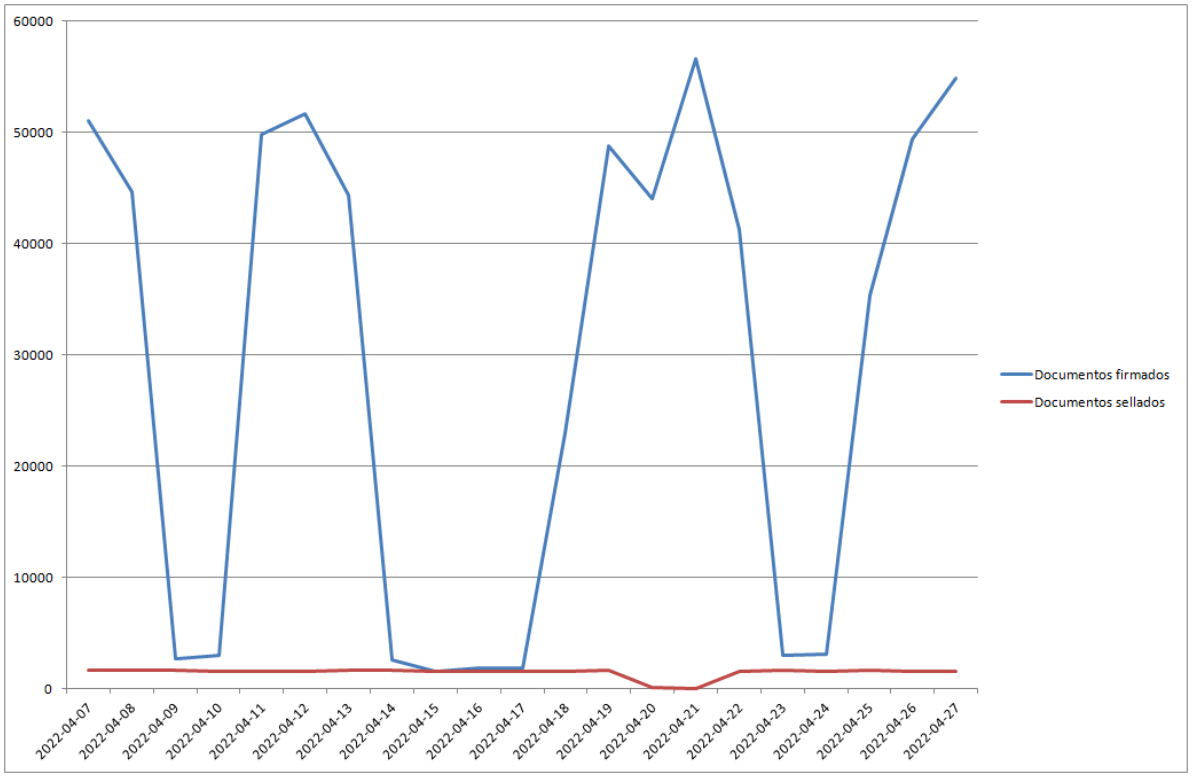
Los casos 1 y 2, al tratarse de documentos XML que solo contienen huellas digitales, y no el contenido completo de los documentos originales firmados, resultan en ficheros de pequeño tamaño (habitualmente unos 70-80 KB). Esto permite que la ejecución de las operaciones en el sistema @firma sea relativamente rápida y no plantee demasiados problemas. La validación y primera conversión de los documentos de XAdES-BES a XAdES-A se realizan inmediatamente después de la operación de firma o sello electrónico, sin perjudicar el tiempo de respuesta del sistema.

Sin embargo, en los casos 3 y 4, al tratarse de documentos PDF de tamaño variable, el escenario es completamente diferente, obteniendo frecuentes timeouts tras varios minutos de espera en el proceso.

El caso 3, si el documento ocupa menos de 1 MB se intenta hacer en el mismo momento en que se procesa el documento original (pues no es viable posponerlo). Los documentos mayores directamente se dejan sin validar y se procede como se indica en el apartado "Importación de firmas ajenas al sistema" cuando la validación no es satisfactoria.

Sin embargo, las operaciones correspondientes al caso 4 se relegan a un horario de baja carga del sistema, pues realizar la actualización de PAdES a PAdES LTV en el mismo momento de generación del *"documento auténtico"* resulta en un colapso del sistema.

De hecho, incluso realizando este proceso solo sobre documentos de tamaño inferior a 1 MB y en horario nocturno (0:00 a 8:00), @firma (tanto el nodo de la ACCV como el de Madrid) no es capaz de procesar más que una pequeña parte (unos 1600 documentos) del total de documentos que se generan en un día laborable (que actualmente ronda los 45000 - 55000), y no llega a cubrir, siquiera, la cuota de documentos generados en días festivos (unos 2000):



Esto genera un déficit diario de documentos que quedan sin actualizar a PAdES LTV, que irremediablemente acaban por caducar.

Para el caso de los *"documentos auténticos"*, como se ha visto en el apartado "El documento auténtico", esto no supone demasiado problema, ya que basta con que el usuario vuelva a descargar el PDF desde la Sede, mediante su CSV. El documento automáticamente se volverá a generar y firmar con el certificado de sello electrónico actual de la Sede.

En el caso de los documentos firmados externamente, sus firmas simplemente caducarán, como habría ocurrido si siempre hubieran permanecido ajenos a la Sede.

Glosario de términos

- Documento original: el documento que se pretende firmar o sellar.
- Documento auténtico: el documento PDF que el sistema genera para mostrar la información relativa a las firmas y sellos que contiene, así como el resto de datos que se indican en el apartado *"el documento auténtico"*.
- Documento de firma combinado: documento XML generado por el sistema y que engloba todo el conjunto de documentos que se firman o sellan en una sesión. Para cada documento, se incluye la huella digital del documento para ese firmante, la sal usada para generar dicha huella y un identificador de firmante de uso interno. Véase el apartado *"El Documento de firma combinado"*.
- Huella digital del documento para el firmante: hash obtenido a partir del documento original, título del documento, texto del firmante y la sal. Véase el apartado *"La huella digital del documento para el firmante"*.
- Huella digital combinada: hash obtenido a partir de del documento de firma combinado, tras haber sido canonicalizado, y que se utiliza en la firma biométrica. Ver apartado "firmas biométricas".
- Canonicalización: proceso por el que se obtiene la forma canónica o normalizada de un documento XML, con el fin de descartar posibles variantes equivalentes del mismo, y lograr que los pasos posteriores en un proceso (como la obtención de un hash) obtengan siempre el mismo resultado independientemente de quién lo realice.
- Sal: en criptografía, la sal es una secuencia de bits aleatorios que se usan en la entrada de una función de hash para dificultar los ataques de diccionario.
- Texto del firmante: texto configurable para un firmante concreto, que se imprime en el documento y que puede contener información sobre la persona que firma, su cargo, el propósito de la firma, la fecha o, en el caso de sellos electrónicos, numeración de registro de entrada, salida, etc.
- Hash / huella digital: secuencia de longitud fija de bits que se obtiene al aplicar sobre una entrada de longitud variable una función de hash con las propiedades descritas en el apartado *"Principios básicos de criptografía relativos a la firma digital"*.

Historial de cambios

Versión 1.0 - 29/04/2022

- Versión inicial de este documento