LORENZO PEREZ SARRION, SECRETARIO GENERAL DE LA SINDICATURA DE COMPTES, CERTIFICO:

1. Que el presente documento ha sido aprobado por la Comisión de Informática y Gestión de los Sistemas de Información de la Sindicatura de Comptes (CIGSI), en su sesión celebrada el día 3 de julio de 2019.
2. Que en fecha de hoy se procede a su publicación en la sede electrónica de la Sindicatura de Comptes de la Comunitat Valenciana.

Fecha y firma electrónica según codificación al margen.

Política de firma y sello electrónicos y de certificados de la Sindicatura de Comptes de la Comunitat Valenciana

Julio 2019

Abstract del documento

La *Política de firma y sellos electrónicos y certificados* tiene por objeto establecer el conjunto de criterios comunes asumidos por la Sindicatura de Comptes de la Comunitat Valenciana en relación con la autenticación y el reconocimiento de firmas electrónicas basadas tanto en certificados digitales como con evidencias electrónicas del acto de voluntad de firma.

En concreto, la *Política* establece las directrices a seguir por la Sindicatura de Comptes respecto al uso de la firma electrónica, en el seno de las aplicaciones corporativas, para garantizar la autenticidad, integridad y conservación de los documentos firmados digitalmente.

Así mismo, el objetivo de esta política es establecer qué identidades digitales y certificados digitales de ciudadanos y de terceros acepta la Sindicatura y qué certificados digitales utilizan los empleados de la Sindicatura para los que se establece el procedimiento para gestionar su ciclo de vida.

Finalmente, la política establece las bases estratégicas para la preservación a largo plazo de las firmas electrónicas y garantizar así su validez jurídica durante el tiempo necesario para preservar los documentos firmados.

Índice

1 Introducción

La Sindicatura de Comptes de la Comunitat Valenciana (de ahora en adelante, Sindicatura de Comptes), en su estrategia de implantación del documento y expediente electrónico como elemento de base para evidenciar su actuación administrativa, tal y como establece la Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas, ha decidido dotarse de una política de firma y sello electrónicos y de certificados, tal como establece la Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de Certificados de la Administración.

Esta política debe garantizar el correcto uso de herramientas de identidad digital y de firma electrónica con el objetivo que permitan generar con carácter de autenticidad documentos electrónicos, expedientes electrónicos y foliados de expedientes electrónicos. Para ello, esta política se fundamenta en los siguientes criterios:

- La vocación de la Sindicatura de que su actividad administrativa pueda plasmarse en documentos y expedientes electrónicos auténticos, a fin de dar cumplimiento a la Ley 39/2015.
- Los documentos electrónicos firmados electrónicamente, en cumplimiento de lo que establece esta política, tendrán plena validez y se considerarán originales y definitivos.
- El nivel de seguridad tecnológica, el tipo de certificado a utilizar, el formato de la firma y del sellado y los mecanismos de preservación se fijarán en función de la importancia del documento y del acto administrativo al que se refieren.
- Las firmas electrónicas que se generen en la Sindicatura se efectuarán, en origen, con el formato y nivel de seguridad requeridos para su conservación durante todo el periodo de vida útil del documento al que se refieren. En el supuesto de que no fuera posible, se procederá a la completación de estas firmas. Del mismo modo, los documentos electrónicos que se reciban firmados se someterán a un proceso de validación y completación de las firmas en el momento de la recepción.

En este sentido, en esta política se desarrollan los siguientes elementos:

1. El objeto con el que se desarrolla la política de firma y sello electrónicos y de certificados de la Sindicatura de Comptes.
2. Los datos identificativos de la política, sus periodos de validez y su transición a nuevas políticas y la asignación de responsabilidades para su gestión.
3. La definición de los conceptos clave en materia de firma electrónica y que se desarrollan a lo largo de la política.

4. La normativa y los estándares internacionales a los que está sujeta la política de firma y sello electrónicos y de certificados de la Sindicatura, sobre cuya base se desarrolla.
5. El uso de certificados digitales:
    - Certificados digitales e identidades digitales admitidos: qué certificados digitales o identidades digitales (acreditadas a través de un registro previo) pueden utilizar otras personas o entidades para relacionarse telemáticamente con la Sindicatura.
    - Certificados digitales e identidades digitales empleados: qué certificados digitales y qué otras identidades digitales pueden utilizar los empleados de la Sindicatura, en el ejercicio de sus funciones, y los sellos electrónicos previstos para la actuación automatizada.
6. El ciclo de vida de los certificados empleados por la Sindicatura, identificando el procedimiento de solicitud, de renovación, de revocación y de suspensión de estos.
7. Las clases, tipos y niveles de firma, es decir, cómo y en qué formato se generan las firmas electrónicas empleadas en el ámbito de la Sindicatura y el proceso seguido para su validación. También debe señalarse que se prevén en esta política las firmas electrónicas basadas en identidades digitales y evidencias electrónicas asociadas a la voluntad de la firma, tal como se recoge en el capítulo segundo de la Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas.
8. La definición del sello de tiempo como elemento que permite facilitar la preservación de estas y a la vez dejar evidencia de la fecha y hora en que se ha producido un acto.
9. El mantenimiento y la preservación de firmas electrónicas para garantizar la introducción en los sistemas de gestión documental de la Sindicatura de documentos auténticos que garanticen la preservación de su validez jurídica a largo plazo mediante procesos de resellado de tiempos.
10. La identificación de los metadatos previstos en el vocabulario de metadatos de la Sindicatura de Comptes para la gestión efectiva de firmas electrónicas.
11. Las normativas de firma electrónica aplicadas en un contexto particular que tienen por objetivo determinar la validez de una firma electrónica en una transacción particular identificando qué obligaciones asume la Sindicatura en cada caso, teniendo en cuenta el uso que se tiene que dar a los objetos firmados electrónicamente, documentos o expedientes electrónicos, y el tipo de actuación administrativa que recoge el acto de firma.
12. La identificación de un subconjunto representativo de casos de uso de la firma electrónica que identifican posibles escenarios en los que los procedimientos de

la Sindicatura pueden requerir el uso de firmas electrónicas vinculado a una normativa de firma electrónica concreta:

- Firma electrónica de un documento electrónico.
- Digitalización certificada de documentos en papel: copia certificada electrónica.
- Copia electrónica certificada de un documento firmado electrónicamente.
- Procesos de firma automatizada.
- Firma electrónica con identificación y evidencia electrónica de un documento electrónico.
- Incorporación de documentos firmados digitalmente por el tercero.

Para la elaboración de esta política se ha tenido en cuenta lo que establece al respecto el Esquema Nacional de Interoperabilidad, y muy concretamente lo que se define en la última versión de la Norma Técnica de Interoperabilidad de política de firma electrónica, sellos electrónicos y de certificados digitales de la Administración, así como la del expediente electrónico en cuanto a su proceso de foliación.

2 Alcance de esta política

Esta política tiene por objeto establecer el conjunto de criterios comunes asumidos por la Sindicatura de Comptes en relación con la autentificación y el reconocimiento de firmas electrónicas basadas tanto en certificados como en evidencias electrónicas. En concreto, establece las directrices a seguir por la Sindicatura de Comptes respecto al uso de la firma electrónica, en el seno de las aplicaciones corporativas, para garantizar la autenticidad, integridad y conservación de los documentos firmados digitalmente. Es de aplicación tanto a las firmas como a los sellos electrónicos.

Así mismo, el objetivo de esta política es establecer qué identidades digitales y certificados digitales de ciudadanos y de terceros acepta la Sindicatura de Comptes y qué certificados digitales utilizan los empleados de la Sindicatura.

En este último caso, también se establece su ciclo de vida.

Por último, establece las estrategias de la Sindicatura de Comptes para la preservación a largo plazo de las firmas electrónicas.

2.1 Datos identificativos de la política

A efectos de referencia y seguimiento, se identifica formalmente esta política con el siguiente cuadro de características:

Nombre del documento	Política de firma, sellos electrónicos y de certificados de la Sindicatura de Comptes de la Comunitat Valenciana.
Versión	1.0
Identificador del gestor	Sindicatura de Comptes de la Comunitat Valenciana, con código DIR3 I00000847
URL de referencia de la política	Política_firma_electrónica_I00000847_1.0
URL de referencia	http://www.sindicom.gva.es/web/wdweb.nsf/menu/menunormativa

Fecha de expedición	La que consta en la firma electrónica
Ámbito de aplicación	Gestión de documentos y expedientes electrónicos firmados producidos y custodiados por la Sindicatura de Comptes de la Comunitat Valenciana. Afecta a la totalidad de su personal, tanto de carácter funcionarial como contratado, sea en grado de dependencia directa o a través de empresas externas mediante convenio o cualquier otra modalidad contractual.
Responsable de la política y datos de contacto	Comisión de Informática y Gestión de la Seguridad de la Información. Correo electrónico: cigsi_sindicom@gva.es Teléfono: 963 869 300

Tabla 1. Datos identificativos de la política de firma, sellos electrónicos y certificados

2.2 Entrada en vigor de la política

Esta política de firma, sello electrónicos y certificados entrará en vigor en la fecha de su expedición y será válida hasta que no sea sustituida o derogada por una política posterior, pudiendo determinar un periodo de tiempo transitorio en el que convivan ambas versiones que permita la adecuación de los diferentes sistemas de gestión de documentos a las especificaciones de la nueva versión.

Este periodo de tiempo de transición se tendrá que indicar en la nueva versión y superado el mismo solo será válida la versión actualizada.

3 Normativa aplicable y estándares internacionales

La reciente revolución en el uso del documento electrónico es el resultado de la aparición de cambios normativos que han dado impulso a las herramientas telemáticas y han equiparado, en determinadas circunstancias, los documentos en formato electrónico a los documentos en formatos más tradicionales.

Además, tanto a nivel nacional como en la Unión Europea o internacionalmente, las organizaciones de estandarización técnica han definido y documentado los criterios y formatos que se utilizarán para la gestión de los documentos digitales en todos sus aspectos, garantizando su validez jurídica.

En este apartado se identifica el conjunto de normativas y estándares internacionales que se han tenido en cuenta para la definición de la política de firma y sello electrónicos y de certificados de la Sindicatura de Comptes.

3.1 Normativa aplicable

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 25/2015, de 28 de julio, de Mecanismo de Segunda Oportunidad, Reducción de la Carga Financiera y Otras Medidas de Orden Social.
- Ley 15/2014, de 16 de septiembre, de Racionalización del Sector Público y Otras Medidas de Reforma Administrativa.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Real Decreto 4/2010, de 8 de enero, del Esquema Nacional de Interoperabilidad.
- Real Decreto 3/2010, de 8 de enero, del Esquema Nacional de Seguridad.
- Resolución de 19 de julio de 2011, de la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de Certificados de la Administración.
- Resolución de 19 de julio de 2011, de la Norma Técnica de Interoperabilidad de Expediente Electrónico.
- Reglamento Europeo (UE) 910/2014, del Parlamento Europeo y Consejo, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior.
- Decisión de Ejecución (UE) 2015/1506 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer

los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento anterior.

3.2 Estándares internacionales y otras convenciones

- Estándares técnicos de firma electrónica compartida bajo licencia de uso BY - NC - SA del Creative Commons de la empresa Astrea La Infopista Jurídica SL: *http://astrea.es/web12/biblioesp/_estandares-tecnicos/*.
- ETSI RFC 2315 (1998), ETSE RFC 2630 (1999), IETF RFC 3369 (2002), IETF RFC 3852 (2004): PKCS # 7: Cryptographic Message Syntax (CMS).
- ETSI TS 101 733. v.1.6.3, v.1.7.4 i v.1.8.1: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).
- ETSI TS 119 122-3: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures: Part 3: incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES.
- ETSI TR 119 124-1: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.
- ETSI TS 119 124-2: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of CAdES baseline signatures.
- ETSI TS 119 124-3: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended CAdES signatures.
- ETSI TS 119 124-4: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of CAdES baseline signatures.
- ETSI TS 119 124-5: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended CAdES signatures.
- ETSI TR 119 134-1: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.
- ETSI TS 119 134-2: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of XAdES baseline signatures.
- ETSI TS 119 134-3: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended XAdES signatures.

- ETSI TS 119 134-4: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of XAdES baseline signatures.
- ETSI TS 119 134-5: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended XAdES signatures.
- ETSI TS 119 142-3: Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS).
- ETSI TR 119 144-1 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.
- ETSI SR 019 020: The framework for standardization of signatures; Standards for AdES digital signatures in mobile and distributed environments.
- IETF RFC 5280 (2008): Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- IETF RFC 2560 (1999): X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP.
- IETF RFC 3126 (2001): Electronic Signature Formats for Long Term Electronic Signatures.
- ISO 19005 (2008): Format del fitxer / A-1.
- ISO / TR 18492: 2005- Long-term preservation of electronic document-based Information.
- UNE - ISO / TR 13008: 2010 - Información y documentación. Conversión de documentos digitales y procesos de migración.
- ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
- ETSI TS 102 023, v.1.2.1 i v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- ETSI TS 102 023, v.1.2.1 i v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- ETSI TS 101.861 V1.3.1 Time stamping profile.
- ETSE TR 102.038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.
- ETSE TR 102.041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.

- ETSE TR 102.045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.
- ETSE TR 102.272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.
- IETF RFC 2560, X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP.
- IETF RFC 3125, Electronic Signature Policies.
- IETF RFC 3161 actualizada por RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- IETF RFC 5280, RFC 4325 i RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.
- IETF RFC 5652, RFC 4853 i RFC 3852, Cryptographic Message Syntax (CMS).
- ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

4 Conceptos

Existen conceptos bastante especializados en el caso de esta política, por lo que se considera necesario incorporar un capítulo de definición de términos para hacer más comprensible la política de firma y sello electrónicos y de certificados de la Sindicatura de Comptes de la Comunitat Valenciana.

- **Casos de uso de la firma electrónica**. En este documento nos referimos a los casos de uso de la firma electrónica, a los escenarios posibles de generación de documentos electrónicos firmados. Para cada caso de uso se identificarán los sistemas de firma posibles, los formatos de firma electrónica, los posibles niveles de firma, la normativa de firma electrónica a aplicar, etc. En el caso de la Sindicatura de Comptes, se definen cinco tipos de casos de uso diferentes: firma electrónica de un documento electrónico, digitalización certificada de documentos en papel, copia electrónica certificada de un documento electrónico firmado electrónicamente, procesos de firma automatizada e incorporación de documentos firmados digitalmente por el tercero.
- **Clases de firma electrónica**. En este documento nos referiremos a las clases, a la validez jurídica de la firma electrónica, según se define en la Ley 59/2003, de Firma Electrónica: firma simple u ordinaria, avance y reconocida o cualificada.
- **Evidencias electrónicas**. Conjunto de información en formato electrónico que permite aportar información a un acto, y que puede ser utilizado como prueba judicial en el caso de que haya una disputa sobre este acto. En el caso de la Sindicatura de Comptes, se guardarán en los sistemas de información de la Sindicatura o en la plataforma que gestione el servicio.
- **Formato de firma electrónica**. Forma en la que se codifican las firmas electrónicas. Los formatos utilizados son XAdES, CAdES y PAdES.
- **Nivel de firma**: Con este nombre nos referiremos a si el documento tiene una única firma o múltiples firmas y, en este caso, si se generan en paralelo o en cascada.
- **Estándares técnicos de firma electrónica**. Documentos que detallan las normas relativas a la firma electrónica, organizadas en torno a los conceptos de generación y validación de firma, en un contexto particular (contractual, jurídico, legal...), definiendo las reglas y obligaciones de todos los actores involucrados en este proceso. El objetivo de este proceso es determinar la validez de la firma electrónica para los distintos tipos de transacción.
- **Sistema de firma**. Con este nombre nos referimos a si la forma electrónica de un documento se ha realizado con un certificado digital del firmante o con un sistema de identificación más evidencia electrónica del acto de la firma.

- **Tipo de firma**. Forma en la que se relaciona la firma electrónica con el documento firmado: dentro del mismo documento, como un documento aparte o dentro de estructuras XML.

5 Actores involucrados

Los actores involucrados en el proceso de creación y validación de la firma electrónica son los siguientes:

a. **Firmante**: persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica.

b. **Creador de un sello**: persona jurídica que crea un sello electrónico.

c. **Verificador**: entidad –persona física o jurídica indistintamente– que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por la política por la que se rige la plataforma de relación electrónica o el servicio concreto al que se está invocando. Podrá ser una entidad de validación de confianza o una tercera parte que esté interesada en la validez de una firma electrónica.

d. **Prestamista de servicios de firma electrónica**: Una persona física o jurídica que expide certificados electrónicos o presta otros servicios relacionados con la firma electrónica.

e. **Emisor y gestor de la política de firma electrónica y de certificados**: entidad que se encarga de generar y gestionar el documento de la política, que regirá las actuaciones del firmante, el verificador y de los prestadores de servicios, los procesos de generación y validación de firma electrónica.

En este documento se utilizará el término *firmado* tanto para referirse al firmado como al creador de un sello. En el segundo caso puede tratarse de un proceso de actuación administrativa automatizada.

6 Certificados digitales y otras identidades digitales

6.1 Certificados digitales admitidos por la Sindicatura de Comptes

Los mecanismos de identificación basados en certificado digital se sustentan en la existencia de autoridades de certificación (AC) que emiten certificados digitales y permiten comprobar que un certificado concreto ha sido correctamente emitido y que continúa siendo válido en el momento de su uso, es decir, de la firma o sello de un documento. La relación entre la autoridad de certificación y la entidad que valida el certificado es una relación que se fundamenta en la confianza: los certificados serán aceptados solo en la medida en que la entidad que lo tiene que validar confíe en la honestidad de la autoridad de certificación.

En este contexto, la Sindicatura tiene la obligación de aceptar todos los certificados digitales incluidos en la lista de confianza de prestadores cualificados de servicios electrónicos de confianza (TSL) del Ministerio de Industria, Comercio y Turismo y validados con la plataforma de validación gestionada por el Ministerio de Hacienda y Administraciones Públicas de España, conocida como @firma, la cual establece un listado de entidades y de perfiles de certificados que cumplen con los estándares de calidad y niveles de seguridad establecidos por el Ministerio de Industria, Comercio y Turismo según lo establecido en el artículo 9 de la Ley 40/2015, de Régimen Jurídico del Sector Público.

6.2 Otros sistemas de terceros de identificación admitidos por la Sindicatura de Comptes

La Sindicatura de Comptes también admitirá como sistema de identificación los mecanismos de identificación admitidos por la plataforma Cl@ve: Cl@ve PIN, Cl@ve permanente...

Para la validación de estas identidades se utilizará la plataforma Cl@ve.

6.3 Certificados digitales empleados por la Sindicatura

En aquellos casos en los que los empleados de la Sindicatura requieran un certificado digital de empleado público, la Sindicatura de Comptes les proveerá de un certificado digital de la Agencia de Tecnología y Certificación Electrónica (ACCV), que es un prestador reconocido o cualificado de servicios de certificación.

En cuanto a los sellos electrónicos, la Sindicatura de Comptes utilizará los de los prestadores de servicios de certificación de la ACCV y se generarán desde la entidad de registro de la ACCV.

Para aquellos casos en los que el certificado digital emitido por la ACCV no sea válido, por limitaciones técnicas o de compatibilidad, el personal adscrito a la Sindicatura utilizará certificados emitidos por la Fábrica Nacional de Moneda y Timbre o por Camerfirma.

Por último, y en cuanto a los certificados de servidor (página web), la Sindicatura de Comptes podrá utilizar diferentes certificados digitales de distintos prestadores de servicios de certificación. La decisión sobre qué certificados se utilizarán vendrá condicionada en cada momento por el nivel de instalación de las claves públicas de estos prestadores en los navegadores utilizados por el conjunto de la sociedad.

Por lo que respecta al uso de certificados digitales de servidor, los utilizados para el intercambio seguro de información entre el ciudadano y la Sindicatura, esta utilizará los de la ACCV o, en su defecto, cualquiera de los emitidos por otras autoridades de certificación que ya tengan un alto nivel de instalación de sus claves públicas en los navegadores. Debe señalarse que, si bien estos certificados no generan actos jurídicos, se ha considerado oportuno incorporarlos a las políticas.

6.4 Sistemas de identificación provistos por la Sindicatura de Comptes de la Generalitat Valenciana

Así mismo, la Sindicatura provee a todos sus empleados que han de tener acceso a determinados servicios o aplicaciones de un usuario y contraseña único de la intranet propia.

7 Ciclo de vida de los certificados digitales entregados por la Sindicatura de Comptes

La Sindicatura de Comptes utiliza la ACCV como prestador de servicios de certificación de referencia. Para servicios no compatibles con la ACCV, utilizará certificados emitidos por la FNMT y/o Camerfirma.

Serán estas autoridades de certificación las responsables de definir las políticas de gestión de los certificados digitales que emiten y, por lo tanto, son quienes definen la vigencia de los certificados, la manera en que se revocan, se renuevan, se validan, etc.

A efectos de adoptar los procedimientos establecidos por el prestador de servicios de certificación, la ACCV, para operar con la entidad de registro, se han establecido procedimientos internos que identifican las actividades que se realizan y sus responsables, así como los procedimientos a seguir por los usuarios para la solicitud, renovación, revocación, etc. de sus certificados digitales.

La Sindicatura de Comptes llevará un control de los certificados emitidos dentro de su estructura mediante un inventario exhaustivo que contemplará como mínimo la persona solicitante, la fecha de emisión, la fecha de caducidad, la fecha de revocación, el tipo de certificado emitido y el proveedor, que será responsabilidad de la Secretaría General.

Los certificados digitales de la Sindicatura se encuentran alojados en el puesto de trabajo o en el HSM (*hardware security module*) del gestor de certificados, o en el *hardware* emitido por la ACCV o en el repositorio de gestión de certificados digitales de los servidores (para certificados de sello electrónico para la actuación administrativa automatizada, para certificados de servidor web o de sede electrónica).

Los certificados digitales se almacenan a partir de un apoyo *software* y, por tanto, tendrán capacidad de generar firma avanzada.

La decisión de si un trabajador de la Sindicatura debe tener un certificado digital de trabajador público o de trabajador público con cargo se tomará en la Comisión de Informática y Gestión de la Seguridad de la Información, en adelante CIGSI.

7.1 Trabajador público

Los certificados digitales de trabajador público de la Sindicatura se emiten y revocan desde el departamento de Informática. Cuando un trabajador de la Sindicatura necesita un certificado digital, lo solicita por correo electrónico, en tanto no se disponga de la herramienta de tramitación electrónica en el departamento de Informática. Ha de informar del DNI, nombre y apellidos del trabajador, y a partir de esta información se hace la petición del certificado. Desde el departamento de Informática se hace la solicitud a la ACCV. Los certificados se piden en *software*. En el momento en que el departamento de Informática recibe el certificado y su clave de protección, procede a cargarlo en el HSM y, una vez comprobado que se ha hecho correctamente, elimina el fichero con el certificado digital recibido de la ACCV. A continuación se procede a hacer

firmar la hoja de entrega que ha emitido la ACCV con el trabajador público y se le da el PIN de acceso al certificado digital que está en el HSM, y se le pide que lo cambie por uno personal que solo conoce él.

Será responsabilidad del trabajador el buen uso y conservación de los PIN.

La hoja de entrega, una vez firmada por el trabajador, se envía a la ACCV.

En el caso de que un empleado de la Sindicatura olvide el PIN, tiene que solicitarlo por correo electrónico mientras no se disponga de la herramienta de tramitación electrónica al departamento de Informática, que es el que hace el proceso de pedir la revocación del certificado ante la ACCV.

En el supuesto de que un certificado esté a punto de caducar, se informará al solicitante y, si este lo continúa necesitándolo, se procede a emitir un nuevo certificado siguiendo el mismo procedimiento como si se pidiera de nuevo.

En el caso de que el departamento de Recursos Humanos y Servicios Generales tenga constancia de la baja de una persona en la Sindicatura, tendrá que comunicarlo al departamento de Informática para que pueda proceder a su revocación.

7.2 Trabajador con cargo

Los certificados digitales de trabajador público con cargo en la Sindicatura se emiten y revocan igualmente desde el departamento de Informática. Cuando un trabajador de la Sindicatura con cargo necesita un certificado digital, lo solicita por correo electrónico al departamento de Informática. Debe informar sobre el nombre y apellidos del trabajador y del cargo que tiene y, a partir de esta información, mientras no se disponga de la herramienta de tramitación electrónica, el departamento de Informática realiza la comprobación del cargo en el departamento de Recursos Humanos y se hace la petición del certificado. Desde el departamento de Informática se hace la solicitud a la ACCV. Los certificados se piden en *software*. En el momento en que el departamento de Informática recibe el certificado y su clave de protección, procede a cargarlo en el HSM y, una vez comprobado que se ha hecho correctamente, elimina el fichero con el certificado digital recibido de la ACCV. A continuación se procede a hacer firmar la hoja de entrega que ha emitido la ACCV al trabajador público y se le da el PIN de acceso al certificado digital que está en el HSM, y se le pide que lo cambie por uno personal que solo conoce él.

La hoja de entrega, una vez firmada por el trabajador, se envía a la ACCV.

En el caso de que un empleado de la Sindicatura olvide el PIN, tiene que avisar al departamento de Informática, que es el que realiza el proceso de revocación del certificado ante la ACCV.

En el supuesto de que el departamento de Recursos Humanos y Servicios Generales tenga constancia de la baja de una persona en la Sindicatura o del cambio de cargo de esta, deberá comunicarlo al departamento de Informática para que pueda proceder a su revocación.

En el caso de que un certificado esté a punto de caducar, se informará al solicitante y, si este necesita continuar teniéndolo y que el cargo continúe vigente, se procederá a su renovación o, en caso de que haya caducado, a emitir un nuevo certificado siguiendo el mismo procedimiento como si se pidiera por primera vez.

7.3 Representante de la Sindicatura

Los certificados digitales de representante de la Sindicatura se emiten y revocan desde el departamento de Informática. Este certificado solo lo pueden pedir los representantes legales o voluntarios de la Sindicatura, según lo que marca el artículo de la ley 6/85 de la Generalitat Valenciana de Sindicatura de Comptes de la Sindicatura, que como mínimo serán el síndico o su sustituto en caso de vacante.

Cuando se necesite emitir un certificado digital de representante para uno de los sujetos contemplados anteriormente, la Secretaría General debe certificar la capacidad de la persona para representar a la Sindicatura y posteriormente el departamento de Informática podrá realizar la petición a la ACCV, a la FNMT o a Camerfirma en función de la aceptación de estos certificados para realizar distintos trámites.

El certificado digital se pedirá en *software* para poder instalarlo en el HSM. También se podrá pedir en tarjeta criptográfica de la ACCV para que el representante o representantes de la Sindicatura puedan generar firmas cualificadas para aquellos puestos que lo puedan requerir.

En cuanto a los certificados generados en *software*, una vez generados es necesario que el departamento de Informática los suba al HSM. Una vez comprobado que se ha subido correctamente se procederá a eliminar el fichero del certificado digital que ha emitido la autoridad de certificación. El PIN del certificado digital en el HSM se entrega en el mismo momento en que se hace firmar la hoja de entrega del certificado digital al representante. En ese mismo momento se le indicará que debe cambiar el PIN por uno personal que solo conozca él.

La hoja de entrega, una vez firmada por el trabajador, se enviará a la ACCV.

Tanto si el certificado está en el HSM como si está en tarjeta, y en el caso de que el representante olvide el PIN, debe avisar al departamento de Informática para que este pueda efectuar el proceso de revocación del certificado ante la autoridad de certificación.

En el supuesto de que un certificado esté a punto de caducar, se informará al representante y, si el cargo continúa vigente, se procederá a emitir un nuevo certificado siguiendo el mismo procedimiento como si se pidiera de nuevo.

En el caso de que el representante deje el cargo y deje de ser el representante de la Sindicatura, la Secretaría General lo comunicará al departamento de Informática para que proceda a la revocación de este certificado.

7.4 Sello de órgano

Los certificados de sellos de órgano y otros certificados técnicos se emiten y revocan desde la Secretaría General. En el caso de que un servicio requiera un certificado de sello de órgano y otros certificados técnicos de la Sindicatura de Comptes, este servicio realizará la petición a la Secretaría General, que gestionará el procedimiento con el departamento de Informática.

Antes de empezar el proceso de emisión de un nuevo sello de órgano u otro certificado técnico, la Secretaría General pedirá al departamento de Informática que realice las comprobaciones pertinentes para constatar la necesidad del sello de órgano por este órgano y que ninguno de los emitidos puede dar servicio. En el caso de que estas comprobaciones concluyan que ya existe un sello de órgano que pueda hacer la función pedida, el departamento de Informática habilitará, de acuerdo con la resolución de la Secretaría General, el sello o certificado existente para el nuevo uso.

En caso de que sea necesario un nuevo sello o certificado técnico, la Secretaría General iniciará el proceso de solicitud del nuevo sello al proveedor pertinente.

El departamento de Informática realiza la descarga del sello o certificado y lo instala en el servidor y en la aplicación o aplicaciones que corresponda. En el caso de sellos de órgano y de sede electrónica se requiere una resolución del síndico.

Este tipo de certificado se podrán instalar en el HMS corporativo, y será responsabilidad del departamento de Informática.

En el momento en que el departamento de Informática detecte que un certificado está a punto de caducar, se consultará con el departamento o área responsable del servicio para comprobar si el certificado continúa siendo necesario una vez finalizada su vigencia y, en caso afirmativo, se procederá a su renovación.

La Sindicatura podrá ceder sellos electrónicos a terceros. En este caso, se firmará un documento de cesión del certificado de sello con el organismo al que se cede el certificado, y será siempre un certificado de sello específico, para poder tener un control de los usos que se pueden efectuar con estos certificados.

8 Sello de tiempo

Las características principales del sello de tiempo son:

- El sello de tiempo es un sello electrónico generado por un tercero de confianza sobre la base de un certificado digital especialmente destinado a estos efectos.
- Evidencia de la fecha y hora en que se ha producido un acto. Se utiliza conjuntamente con un documento en cualquier formato y que puede estar firmado electrónicamente. El sello de tiempo puede hacer referencia a:
    - Firma del documento: el sello de tiempo está asociado a la firma electrónica.
    - Creación del documento: el sello de tiempo está asociado al documento.
- Mediante un proveedor de sellado de tiempo, se sellará la fecha y hora del instante en que se ha realizado el acto. El proveedor será el proveedor de servicios de certificación de referencia.
- El proveedor del servicio de sellado de tiempo es la ACCV.
- El proceso consiste en crear una evidencia electrónica sobre una firma electrónica: se calcula el resumen criptográfico del documento y/o sus firmas electrónicas (en el caso del resellado), es decir, una operación matemática que se aplica al conjunto de información sobre el cual emitir el sello de tiempo y obtiene una cadena de bits denominada *hash*, que se cifra con la clave privada del certificado de sello de tiempo utilizado para hacer la operación. Se devuelve esta firma conjuntamente con la fecha y hora de la operación, así como información sobre el certificado de sello de tiempo utilizado para hacer la firma.
- El sello de tiempo se incorporará a las firmas electrónicas en el formato especificado en los estándares XAdES-T, CAdES-T y PAdES-LTV.

9 Sistemas, clases, tipos y niveles de firma o sello

En este apartado se recopilan los aspectos relacionados con la firma electrónica en el marco de la Sindicatura de Comptes de la Comunitat Valenciana, incluyendo distintos usos de la firma y sello electrónico en el ámbito de los sistemas de la Sindicatura de Comptes. Los objetivos que persigue la Sindicatura con la implantación de la firma electrónica son fundamentalmente tres:

- Dotar a la Sindicatura de Comptes de un sistema para el control, el uso y la conservación de la documentación original firmada electrónicamente, gestionada en el desarrollo habitual de su actividad política y administrativa.
- Garantizar la gestión adecuada de los documentos de la Sindicatura de Comptes, asegurando su autenticidad, fiabilidad, integridad y disponibilidad futura a lo largo de su ciclo de vida, basado en un *software* informático que ofrece una capa de gestión de documentos y archivo común.
- Dar respuesta a las exigencias en materia de archivo electrónico de la Ley 39/2015 y del Esquema Nacional de Interoperabilidad.

Una vez formulados estos objetivos básicos, hay que tener presente la definición de los sistemas de firma electrónica. La Sindicatura podrá usar:

- **Firma electrónica basada en el uso de un certificado digital**. Es el sistema de firma electrónica en el que, partiendo de la clave privada de un usuario, se cifra el resumen criptográfico del documento a firmar, y se añade a esta firma información del certificado utilizado para la firma, la fecha de la firma, la política de firma, etc.
- **Firma basada en la identificación más voluntad de firma.** En los procedimientos que determine la CIGSI, y con las condiciones que se marquen según la aplicación utilizada para el procedimiento y solo a efectos internos, se podrán establecer otros mecanismos de firma, basada en la identificación de la persona que ha participado en el proceso y la plasmación de su voluntad de firma, a través de evidencias.
- **Firma ordinaria en TeamMate.** En el caso de los documentos que se gestionen en TeamMate, la Sindicatura considerará que están firmados digitalmente todos aquellos documentos en los que se aplique la opción de firma dentro de la aplicación. Esta firma tendrá validez mientras el documento esté dentro de TeamMate. En el caso de que algún documento tenga que salir de TeamMate y requiera mantener su validez jurídica, se podrá hacer una copia electrónica del documento aplicando un sello electrónico o la firma de un funcionario habilitado para realizar copias auténticas. Para poder hacerlo, habrá que verificar que el documento dentro de TeamMate ha sido firmado de acuerdo con lo que se especifica en este punto.

En cuanto a las clases de firma desde un punto de vista jurídico:

- **Simple u ordinaria**. Es el conjunto de datos en formato electrónico consignados a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.
- **Firma electrónica avanzada**. Es la firma electrónica que permite identificar al firmante y detectar cualquier cambio posterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que hace referencia y que ha sido creada por medios que el firmante puede mantener bajo su control exclusivo.
- **Firma electrónica reconocida o cualificada**. Es la firma electrónica avanzada que se basa en un certificado reconocido o cualificado y que ha sido generada mediante un dispositivo seguro de creación de firma, según establece el artículo 3.15 del Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Para las definiciones anteriores, se utiliza el concepto clave de certificado reconocido o cualificado que el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, define en su artículo 3 como un certificado que ha sido emitido por un prestador de servicios de confianza que cumple con los requisitos en materia de composición y contenido establecidos en los respectivos anexos del reglamento para los diferentes tipos de certificado reconocidos.

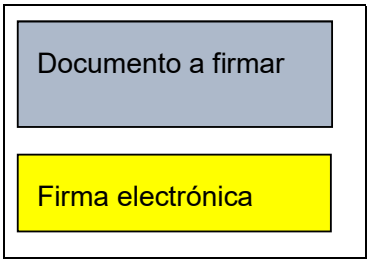
La Sindicatura regulará para cada procedimiento administrativo el nivel de seguridad de firma, así como el rol que debe tener el firmante y, por lo tanto, qué sistema de firma electrónica se utilizará y, en caso de que sea criptográfica, qué certificados digitales se emplearán.

9.1 Tipos de firma electrónica

Definiciones de tipos de firma utilizadas por la Sindicatura desde un punto de vista técnico:

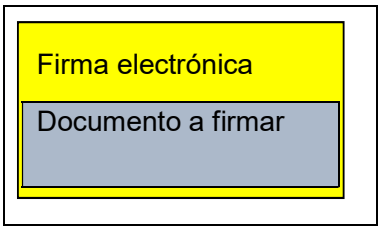
- **Firma *attached***. Los datos de firma residen en el documento firmado. Por lo tanto, el propio documento dispone de toda la información para comprobar la autenticidad e integridad del documento, así como la información necesaria para la validación de la firma. Hay que diferenciar entre dos tipos diferentes de firma *attached*:
    - *Enveloped* (incrustada). En este caso, el documento firmado está compuesto por el contenido del documento a firmar más la firma de este contenido.

Documento firmado:

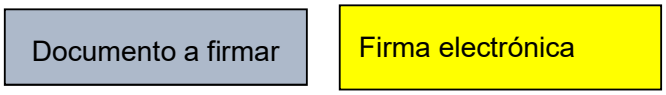


- *Enveloping* (envolvente). En este caso, el documento firmado es la firma electrónica del documento a firmar y dentro de la firma está el propio documento a firmar.

Documento firmado:



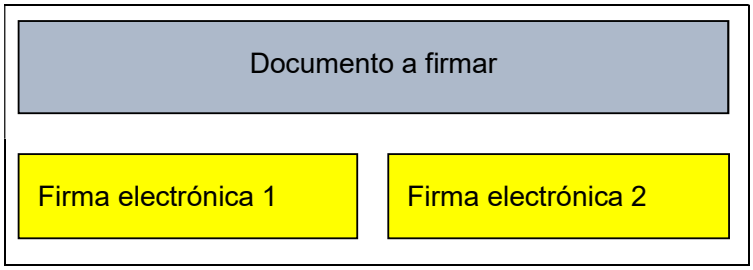
- **Firma *detached***. Los datos de firma residen fuera del documento a firmar, pero asociados a este. Los datos de la firma se mantendrán por separado durante todo el ciclo de vida del documento. Para validar la firma hay que crear un documento de evidencia electrónica que contenga de forma conjunta el documento y sus datos completos de la firma.



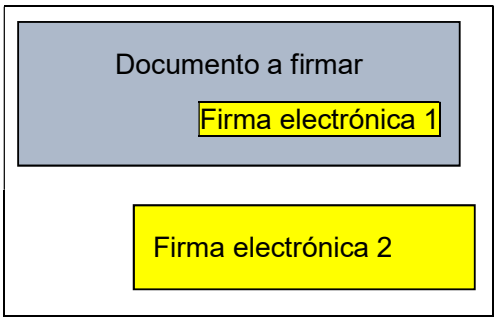
A continuación, definiremos el nivel de firmas.

- **Firma simple**. El documento contiene una única firma.
- **Firma múltiple**. El documento contiene dos o más firmas. Esta firma múltiple consiste en que varios firmantes firmen el documento consecutivamente. Esta firma se puede aplicar sobre el documento original cada vez, lo que se identifica como firma en paralelo, o sobre el documento firmado, que se identifica como firma en cascada.

- ***Documento firmado con firma en paralelo:***



- ***Documento firmado con firma en cascada:***



La firma múltiple se utilizará en distintas situaciones en el marco de los procedimientos de la Sindicatura, como por ejemplo en la firma de documentos electrónicos por más de una persona o en el resellado de documentos ya firmados para actualizar la validez legal del documento a lo largo del tiempo, antes de que pueda quedar en entredicho la validez criptográfica de la firma electrónica.

9.2 Formatos de firma

Partiendo de los conceptos básicos sobre firma electrónica descritos anteriormente, se describen a continuación los formatos de firma electrónica que utilizará la Sindicatura de Comptes en el marco de esta política de firma y sello electrónicos y de certificados.

9.2.1 Firma electrónica con política de firma y con sello de tiempo

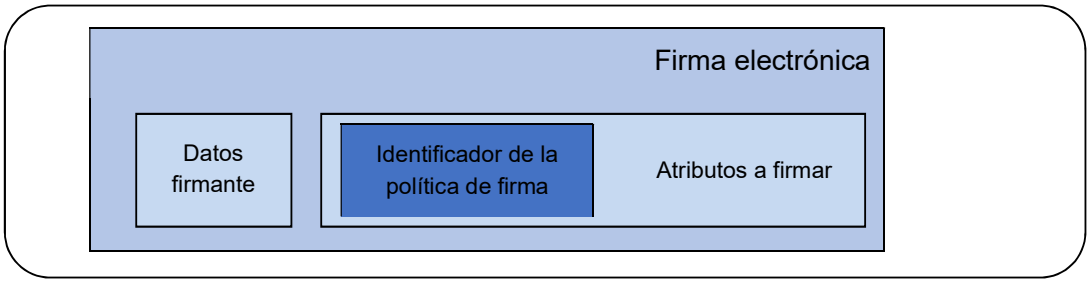
Este será el formato de firma electrónica, avanzada o reconocida, para los documentos electrónicos y foliado de expedientes que se tengan que guardar menos que la fecha de vencimiento del certificado digital utilizado para generar el sello de tiempo asociado a la firma electrónica. En el caso de múltiples firmas, se tendrá en cuenta:

- En paralelo: primera fecha de caducidad del sello de tiempo dentro de las diferentes firmas.
- En cascada: fecha de caducidad del sello de tiempo de la última firma.

Formato de firma derivado de la firma electrónica avanzada con identificador de política (en nuestra nomenclatura normativa de firma electrónica), también conocida como EPES, con la incorporación de un sello de tiempo que sitúa la firma electrónica en un momento determinado del tiempo.

La representación gráfica de este formato de firma, identificado como AdES-EPES, es la siguiente:

AdES-EPES:

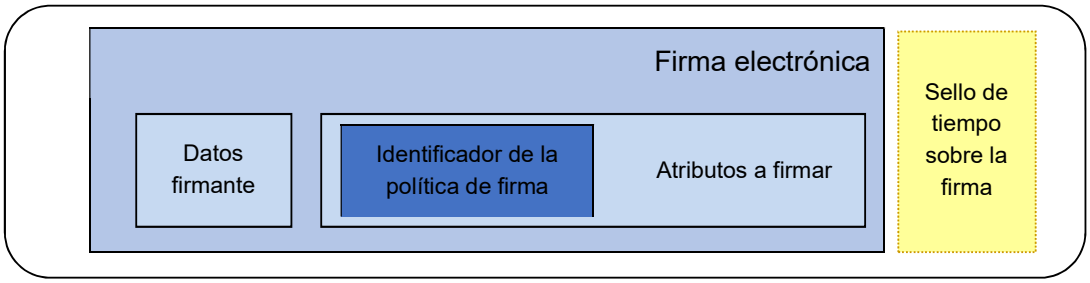


La firma electrónica con política explícita (XAdES-EPES o PAdES-EPES) ha de contener todos los elementos que se listan a continuación:

- Los datos firmados por el usuario, como por ejemplo un documento electrónico.
- El tipo de contenido firmado: *ContentType*.
- El resumen criptográfico del mensaje: *messageDigest*.
- El certificado empleado para firmar: *ESSSigningCertificate* o *OtherSigningCertificate*.
- La fecha y hora alegada de la firma: *signingTime* (opcional).
- Las pistas sobre el contenido firmado: *ContentHints* (opcional).
- La identificación del contenido: *ContentIdentifier* (opcional).
- La referencia a los contenidos: *ContentReference* (opcional).
- La indicación del tipo de compromiso: *CommitmentTypeIndication* (opcional).
- La localización del firmante: *SignerLocation* (opcional).
- Los atributos del firmante: *SignerAttributes* (opcional).
- El sello de fecha y hora sobre el contenido: *ContentTimestamp* (opcional).
- Contrafirma: *Countersignature* (opcional).
- Identificación de la política de firma: *SignaturePolicyIdentifier* (en nuestra nomenclatura normativa de firma electrónica)

La representación gráfica del formato de firma con sello de tiempo, identificado como AdES-T, es el siguiente:

AdES-T:



La firma electrónica con sello de tiempo (XAdES-T o PAdES-T) ha de contener los elementos de la firma XAdES-EPES o PAdES-EPES (firma electrónica avanzada con identificador de política), más el siguiente elemento:

- Sello de fecha y hora de la firma: *SignatureTimeStamp*.

9.2.2 Firma electrónica de archivo

Este será el formato de firma electrónica avanzada o reconocida para los documentos electrónicos y foliado de expedientes que se tengan que guardar más del tiempo de caducidad del certificado digital utilizado para generar el sello de tiempo asociado a la firma electrónica. En el caso de múltiples firmas, se tendrá en cuenta:

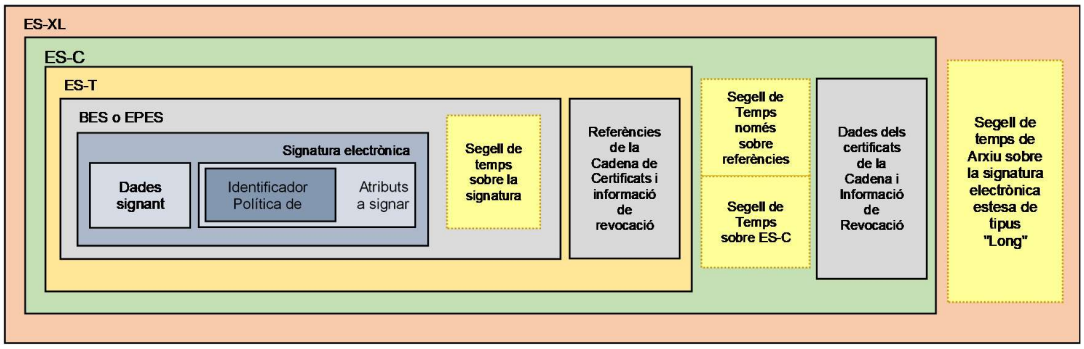
- En paralelo: primera fecha de caducidad del sello de tiempo dentro de las diferentes firmas.
- En cascada: fecha de caducidad del sello de tiempo de la última firma.

Hay dos formatos de archivo:

9.2.2.1 Firma AdES

La firma electrónica de archivo (ADES-A) parte del formato de firma electrónica extensa (XL), que incluye todos los elementos de verificación de la vigencia del certificado para poder repetir la validación de manera autónoma. Sobre este formato extenso de firma, añade un sello de tiempo, previendo el resellado sucesivo de manera periódica. Este es el formato de firma más completo y está pensado expresamente para los documentos de los que se quiere garantizar su disponibilidad a lo largo del tiempo.

Firma electrónica de archivo (ES-A):



- La firma electrónica XML: *Signature*.
- El certificado utilizado para firmar: *SigningCertificate* o *KeyInfo: X509Data*.
- La fecha y hora alegada de la firma: *signingTime* (opcional).
- El formato del objeto de datos firmado: *DataObjectFormat* (opcional).
- La indicación del tipo de compromiso: *CommitmentTypeIndication* (opcional).
- El lugar de producción de la firma: *SignatureProductionPlace* (opcional).
- El papel del firmante: *SignerRole* (opcional).
- El sello de fecha y hora sobre el contenido: *AllDataObjectsTimeStamp* o *IndividualDataObjectsTimeStamp* (opcional).
- La contrafirma: *Reference* o *CounterSignature* (opcional).
- Identificación de la política de firma: *SignaturePolicyIdentifier* (en nuestra nomenclatura normativa de firma electrónica).
- Sello de fecha y hora de la firma: *SignatureTimeStamp*.
- Referencias completas de certificados: *CompleteCertificateRefs*.
- Referencias completas de revocación: *CompleteRevocationRefs*.
- Referencias completas de certificados de atributos: *AttributeCertificateRefs*.
- Referencias completas de revocación de atributos: *AttributeRevocationRefs*.
- Sello de fecha y hora sobre la firma completa: *SigAndRefsTimeStamp*.
- Sello de fecha y hora sobre las referencias de certificados y revocaciones: *RefsOnlyTimeStamp*.
- Valores de certificados: *CertificateValues*.
- Valores de revocación: *RevocationValues*.
- Valores de certificados de atributo: *AttrAuthoritiesCertsValues*.
- Valores de revocación de certificados de atributo: *AttributeRevocationValues*.
- Sello de fecha y hora de archivo: *ArchiveTimeStamp*.

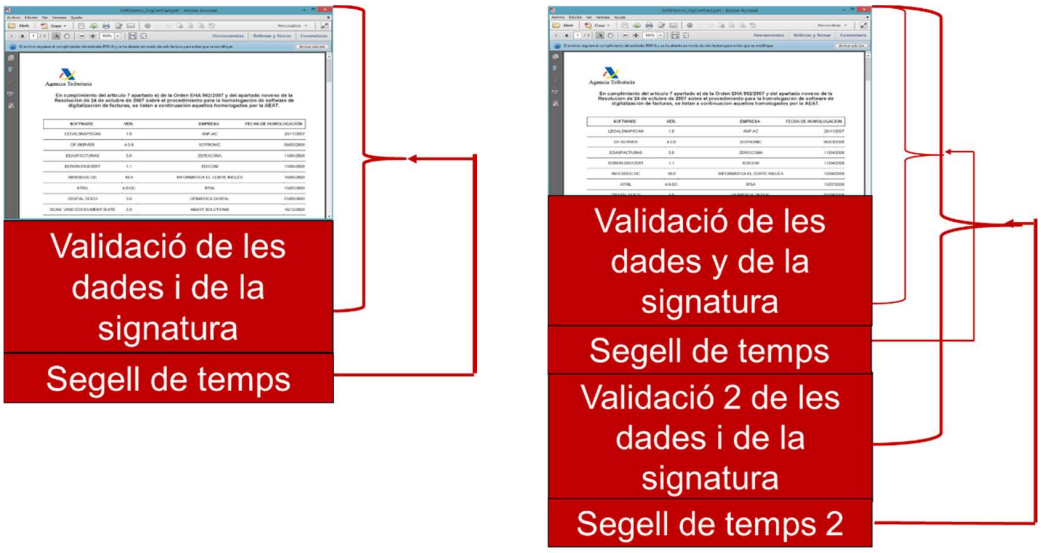
9.2.2.2 Firma PAdES-LTV

La firma electrónica de larga duración (*Long Term Validation*) es un formato específico de la familia PAdES. La firma más básica, la PAdES Basic, está especificada en una ISO, la ISO 32000-1. La firma PAdES EPES incluye la firma electrónica del documento (en formato CAdES-BES), con sello de tiempo (recomendado) y una respuesta de validación de un servicio OCSP (recomendado). Puede incluir además motivos de firma, el lugar de la firma y datos de contacto del firmante. Incluye además la política de firma.

Sobre estas firmas se puede construir una firma PAdES-LTV, que incluye para la verificación de las firmas y del contenido que las autoridades de certificación en el momento de la validación eran correctas, la respuesta del servicio de validación OCSP y un sello de tiempo sobre esta verificación de firmas.

Se puede añadir a la firma, posteriormente, un nuevo comprobante de verificación que garantiza que la verificación que se hizo en su momento continúa siendo válida y se añade un nuevo sello de tiempo para proteger las firmas y sus validaciones.

Ejemplo:



9.2.3 Firma electrónica a través de acreditación de la identidad de evidencias de la voluntad de firma

El proceso de firma se realiza de la siguiente manera:

- El usuario se habrá acreditado anteriormente en el sistema (primer factor de autenticación).
- El usuario cumplimentará el formulario a firmar y pulsará el botón de firma, que le pedirá un segundo factor de autenticación.
- Esto llevará a una pantalla donde podrá introducir una segunda contraseña o un PIN que tiene este usuario, o un PIN que este usuario pueda recibir por correo

electrónico o teléfono móvil. En el supuesto de que el usuario introduzca correctamente esta segunda contraseña, se generará una evidencia con datos del firmante, del documento (identificación y *hash* del documento), fecha y hora de la firma y tipo de firma con contraseña (segunda contraseña, PIN fijo o PIN enviado). Esta evidencia se guarda tanto en el expediente como en la plataforma e-Logs de la Sindicatura. A continuación se procede a la firma del documento con un sello electrónico, más sello de tiempo (firma secundaria). Se enviará siempre un correo electrónico al firmante confirmando su firma del documento.

En este formato de firma puede haber más de una firma de este tipo sobre el documento, y estas pueden ser en paralelo o en cascada.

Esta firma puede combinarse con otro tipo de firma basada en certificado digital.

Por lo tanto, la validez jurídica de la firma electrónica a través de acreditación de la identidad y de evidencias de la voluntad está vinculada al documento y a las evidencias del proceso de identificación del firmante con el PIN o segunda contraseña (firma primaria). Estas evidencias se guardan siempre tanto en el expediente como en los sistemas de la Sindicatura de Comptes, aportando la firma electrónica y el sellado de tiempo del documento firmado, únicamente evidencias de integridad y no de autenticidad (firma secundaria).

En caso de conflicto, la Sindicatura puede acreditar que ha aprobado y publicado en la sede electrónica la regulación específica, que ha generado las evidencias no solo en esta firma sino en cualquier otra firma del mismo tipo (firma primaria), que esta firma se produjo en un momento determinado (sello de tiempo) y que el contenido del documento no ha cambiado: *hash* firmado con el primer sello electrónico (firma primaria) y documento con su firma firmado con el segundo sello electrónico (firma secundaria).

9.2.4 Firma con la plataforma Cl@ve

Este será un sistema específico de firma electrónica avanzada para los documentos electrónicos que firme electrónicamente un tercero a través de la plataforma Cl@ve del MINHAP.

El proceso de firma se realiza de la siguiente manera:

- El usuario deberá acreditarse en la plataforma Cl@ve con certificado digital o con alguno de los sistemas previstos para esta plataforma: Cl@ve PIN, Cl@ve permanente, etc.
- El usuario cumplimentará el formulario a firmar y pulsará el botón de firma. Esta acción redirigirá el usuario a la plataforma Cl@ve. En este caso, pedirá al usuario que vuelva a autenticarse y para la Sindicatura será la prueba de la voluntad de firma.
- Se generará una evidencia (XML) firmada por MINHAP (firma primaria), donde hay información sobre esta segunda identificación. Esta evidencia se tendrá que guardar en el expediente y deberá enviarse al sistema de gestión de evidencias electrónicas de la Sindicatura de Comptes.

- A continuación se procede a la firma del documento con un sello electrónico, más sello de tiempo (firma secundaria).

En este formato de firma puede haber más de una firma de este tipo sobre el documento, que serán tanto en paralelo como en cascada.

Esta firma puede combinarse con otro tipo de firma basada en certificado digital.

Por lo tanto, la validez jurídica de la firma electrónica a través de Cl@ve está vinculada al documento y en las evidencias del proceso de firma del firmante (firma primaria).

En caso de conflicto, la Sindicatura puede acreditar que ha aprobado y publicado en la sede electrónica la regulación específica, que ha generado las evidencias no solo en esta firma sino en cualquier otra firma del mismo tipo (firma primaria), que esta firma se produjo en un momento determinado (sello de tiempo) y que el contenido del documento no ha cambiado: *hash* del documento guardado en la evidencia (firma primaria) y documento con su firma firmado con el segundo sello electrónico (firma secundaria).

9.2.5 Firma basada en un código seguro de verificación (CSV)

El artículo 42.*b* de la Ley 40/2015, de Régimen Jurídico del Sector Público, regula el uso del código seguro de verificación como medio de firma, vinculado a la Administración pública, órgano, organismo público o entidad de derecho público, y permite en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Los mecanismos de firma basados en CSV se prevén con el objetivo de ofrecer un servicio de firma automatizada para los documentos emitidos por la Sindicatura

La Sindicatura ha previsto el uso de este sistema de firma electrónica solo en el caso de documentos destinados exclusivamente a la comunicación con terceros, y principalmente para la emisión de documentos firmados electrónicamente y que puedan transformarse en documentos en soporte papel.

9.2.6 Firma ordinaria en TeamMate

La Ley 59/2003 prevé el uso de la firma ordinaria como sistema de firma electrónica. La Sindicatura considera firma ordinaria el proceso de firma que existe dentro de la herramienta TeamMate. Esta firma tendrá validez jurídica siempre y cuando el documento haya sido firmado utilizando la opción de firma dentro de la herramienta TeamMate. En el momento en que sea necesario sacar un documento firmado del TeamMate para enviarlo a otra aplicación o incluso fuera de la Sindicatura, habrá que hacer una copia auténtica, firmada digitalmente, y será esta copia la que mantendrá la validez jurídica del documento fuera de TeamMate.

10 Validación de firmas o sellos

Para garantizar la validez jurídica de los documentos electrónicos firmados digitalmente, hay que validar cualquier documento que entre o que se genere en la Sindicatura de Comptes y que contenga una firma o sello electrónico y/o un sello de tiempo, previamente a su almacenamiento en el gestor documental.

Para validar se utilizará alguno de estos sistemas:

- La plataforma de validación de la AGE: @firma.
- La plataforma de validación de la ACCV.
- Para documentos PDF que así lo requieran, se utilizará el servicio de validación que aportan las herramientas Adobe.
- Mediante el proceso antes especificado para las firmas a través de acreditación de la identidad y de evidencias de la voluntad de firma.
- Mediante la comprobación en sede electrónica del organismo emisor del documento del código seguro de verificación (CSV).

En los casos de las firmas electrónicas avanzadas y reconocidas, solo en aquellos casos en que el proceso de validación de todas las firmas electrónicas y de los sellos electrónicos sea satisfactorio se procederá, si no está ya en formato AdES-A o PAdES-LTV, a completarla hasta este nivel y a almacenar el documento electrónico dentro del gestor documental de la Sindicatura de Comptes.

Para el caso de las firmas a través de acreditación de la identidad y de evidencias de la voluntad de firma, se procederá a almacenar el documento electrónico, con sus firmas (primaria y secundaria), en el gestor documental de la Sindicatura de Comptes directamente sin ninguna validación adicional, al ser los sistemas de firma de este tipo de firma ya seguros y no existir un proceso automatizado de validación.

En el caso de firmas electrónicas basadas en certificados digitales de prestadores de fuera la Unión Europea, y en el supuesto que la Sindicatura decida aceptar este documento, el proceso de validación consistirá en:

1. Validar que la firma electrónica corresponde al *hash* del documento.
2. Consultar la información disponible del regulador del país que ha emitido este certificado digital y comprobar que la autoridad de certificación és una de las reconocidas por el regulador.
3. Comprobar que el certificado digital utilizado por la firma de este documento era vigente en el momento de la firma.
4. En el supuesto de que sea correcto, hacer una copia auténtica del documento firmado, con un sello de la Sindicatura. Este nuevo documento será el que se guardará en el expediente. Se guardará el documento original en un repositorio específico en la Sindicatura.

En el supuesto de que sea necesaria la preservación de la validez jurídica del documento más allá del tiempo de vida del certificado digital utilizado para generar cualquier firma asociada a este documento, o del sello de tiempo asociado a la o las firmas electrónicas, se procederá a completar la firma o firmas electrónicas en el supuesto de que estas no sean ya firma de archivo, es decir, A o LTV. El completado se realizará en formato de firma de archivo.

Para el caso de las firmas a través de acreditación de la identidad y de evidencias de la voluntad de firma, se procederá a la firma electrónica del documento con un certificado de sello electrónico en formato A o LTV. Para este caso solo se realizará el completado en la firma secundaria.

11 Mantenimiento y preservación de las firmas y sellos electrónicos

La firma o sello electrónico otorga validez jurídica a los documentos electrónicos. Sin embargo, esta validez está sujeta a ciertos riesgos que se tienen que gestionar debidamente para garantizar una validez jurídica indefinida del documento en soporte electrónico. Estos riesgos son:

1. **Caducidad del certificado digital con el que se firma un documento electrónico.** Puede cuestionarse la validez de un documento electrónico a partir del día que caduque el certificado digital que se utilizó para la firma, la cual ha de ser posterior a la fecha de emisión del certificado digital y anterior a su fecha de revocación o de caducidad. Para garantizar el momento en que se generó la firma electrónica, esta se puede completar con un sello de tiempo emitido por una autoridad de certificación. En el caso de la Sindicatura de Comptes, hablamos de realizar firmas AdES-T tanto a nivel de PDF como de XML.
2. **Validez del certificado digital en el momento de generar la firma electrónica.** Puede cuestionarse la validez de un documento electrónico si no existe evidencia suficiente de que el certificado digital estaba vigente el día en que se generó la firma electrónica, es decir, que no estaba revocado. Para guardar la evidencia de que un certificado digital, en la fecha de la firma, no estaba revocado, hay que completar la firma con la información de la validación de este aspecto contra la autoridad de certificación emisora del certificado. Al respecto, hay que tener en cuenta que las autoridades de certificación, en el momento en que un certificado digital caduca, eliminan las evidencias de revocación de su lista de revocados, por lo que si no se guarda la mencionada evidencia una vez caducado el certificado no existirá la certeza de que el certificado con el que se generó la firma no estaba revocado en aquel momento. En el caso de la Sindicatura de Comptes, para garantizar este caso estaremos hablando de firmas AdES-XL o superiores (AdES-A o PAdES-LTV).
3. **Obsolescencia tecnológica de la longitud de las claves criptográficas contenidas en el certificado digital y con las que se generan las firmas electrónicas.** Un documento electrónico puede dejar de tener validez jurídica a partir del día en que se pone en entredicho la seguridad de las claves criptográficas con las que se firmó. Ante este escenario, habrá que tomar medidas para no continuar generando firmas con este problema y asegurar las firmas anteriores, las que tengan este problema. La Sindicatura, para dar respuesta a este problema de obsolescencia tecnológica de las claves criptográficas, procederá a generar certificados de mayor longitud de claves y utilizar algorismas de *hash* más actualizados, y generar sucesivas refirmas a partir de firmas que permitan incorporar estos sellos de tiempos. En el caso de la Sindicatura de Comptes, AdES-A o PAdES-LTV.

11.1 Resellado de firmas electrónicas

El objetivo principal de esta función es garantizar la firma electrónica a lo largo del tiempo.

El proceso de resellado consiste en renovar el sello de fecha y hora añadiendo un nuevo eslabón a la cadena de evidencias electrónicas en la firma electrónica del documento.

Para poder aplicar este proceso, es necesario que las firmas estén en un formato que permita añadir estas evidencias de tiempos. Estas son las firmas del tipo XAdES-A, CAdES-A o PAdES-LTV. En el supuesto de que una firma no esté en estos formatos, previo al resellado debemos completar la firma, que en cualquier caso estará como mínimo en un formato AdES-T, en uno de los formatos anteriormente definidos.

Es un proceso que se llevará a cabo solo para aquellos documentos que todavía no se hayan enviado a la plataforma de preservación de la Sindicatura:

- 6 meses antes de que en esta firma caduque el último sello de tiempo aplicado.
- Excepcionalmente, cuando se detecte una posible obsolescencia tecnológica de los algoritmos o de las claves que firman el documento.

Partiremos, tal y como se ha comentado en el punto anterior, del supuesto de que los documentos tendrán ya una firma del tipo longeva: XAdES-A o PAdES-LTV. Sobre estas firmas se incorporará un nuevo sello de tiempo, puesto que su estructura permite esta posibilidad. Este nuevo sello de tiempo estará ya generado con un certificado reciente, con un periodo de validez superior al actual en la firma a resellar, con una longitud de clave que no estará comprometida y con un algoritmo que no esté sujeto a la obsolescencia criptográfica del algoritmo en el momento de su emisión.

Para el caso de las firmas a través de acreditación de la identidad y de evidencias de la voluntad de firma solo se realizará el resellado de la firma secundaria.

En definitiva, el resellado consiste, pues, en mantener la validez de la firma incorporando nuevo material criptográfico, concretamente sellos de fecha y hora, a la propia estructura de la firma electrónica.

11.2 Mantenimiento de la validez jurídica de las firmas en fase de vigencia

El proceso de mantenimiento de las firmas electrónicas dentro de la Sindicatura de Comptes será el siguiente, para el caso de aquellos documentos que sea necesario preservar:

1. En el caso de firmas generadas en el entorno de la Sindicatura de Comptes, es decir, que las firmas se hayan generado mediante las herramientas de firma de este, se procederá en fase de tramitación a la generación de las firmas electrónicas ya en formato preservable, es decir, en formato de firma de archivo. Para documentos XML, las firmas se transformarán en XAdES-A,

como podría ser el caso del foliado del expediente, y para los documentos PDF se generará una firma electrónica en formato PAdES-LTV.

2. En el caso de firmas que provienen de plataformas externas: otras administraciones, herramientas de cliente, etc., se procederá en su caso a completar la firma. Este proceso de completación de la firma se realizará previo cierre y foliado de l'expediente. Para documentos XML, las firmas se pasarán a XAdES-A, como podría ser el caso del foliado del expediente, y para los documentos PDF se generará una firma electrónica en formato PAdES-LTV.
3. En el supuesto de que no sea posible generar por algún documento una firma preservable, se procederá lo antes posible a foliar l'expediente con un índice en formato XML con una firma XAdES-A, de forma que sea el foliado de l'expediente lo que garantice la validez jurídica de la firma electrónica del documento.

12 Metadatos de firma

Los metadatos de firma que utilizará la Sindicatura de Comptes para describir las firmas electrónicas son los siguientes:

Id	Nombre Sindicatura	Descripción	Nombre vocabulario	Tipo	Formato	Oblig.
1	Categoría	Valor del tipo de entidad que se está describiendo	EMSINDICOM_0001	Texto	Abierto	Obligatorio
2	Identificador	Secuencia de caracteres que identifica un objeto en el sistema	EMSINDICOM_0002	Texto	Abierto	Obligatorio
3	Esquema del identificador	Esquema utilizado para crear la secuencia de identificador	EMSINDICOM_0003	Texto	Abierto	Condicional
6	Fecha inicio	Fecha y hora en la que una entidad inicia su existencia	EMSINDICOM_0006	Fecha	Fecha y hora	Obligatorio
7	Fecha fin	Fecha y hora en la que una entidad finaliza su existencia	EMSINDICOM_0007	Fecha	Fecha y hora	Condicional
13	Nivel de seguridad	Término normalizado que denota el nivel de seguridad en conformidad con el ENS	EMSINDICOM_00013	Tabla codificada	Abierto	Condicional
40	Tipo de firma	Denominación normalizada del formato de firma utilizado	EMSINDICOM_0040	Texto	Abierto	Obligatorio
41	Formato de firma	Formato de firma empleado en una firma con certificado electrónico	EMSINDICOM_0041	Tabla codificada	Abierto	Obligatorio
42	Perfil de firma	Perfil de firma empleado en una firma con certificado electrónico	EMSINDICOM_0042	Tabla codificada	Abierto	Condicional
43	Rol de firma	Indicador normalizado de la función que ejerce la firma utilizada	EMSINDICOM_0043	Tabla codificada	Abierto	Condicional

Id	Nombre Sindicatura	Descripción	Nombre vocabulario	Tipo	Formato	Oblig.
44	Valor CSV	Valor del código seguro de verificación utilizado para firmar el documento o expediente	EMSINDICOM_0044	Texto	Abierto	Condicional
45	Normativa CSV	Referencia a la orden, resolución o documento que define la creación del CSV correspondiente	EMSINDICOM_0045	Texto	Abierto	Condicional
59	Interesado	Secuencia de identificador del interesado	EMSINDICOM_0059	Texto	Abierto	Obligatorio

13 Casos de uso de la firma electrónica

Previamente a la descripción de los casos de uso identificados de firma electrónica, es interesante comentar un concepto clave en este entorno de la documentación electrónica, y que no es otro que el expediente administrativo, ya completamente electrónico, y su foliado, también electrónico, para lo cual se aprovecha la definición que realiza la Ley 39/2015, en el artículo 70:

- Se entiende por expediente administrativo el conjunto ordenado de documentos y actuaciones que sirven de antecedente y fundamento a la resolución administrativa, así como las diligencias encaminadas a ejecutarla.
- Los expedientes tendrán formato electrónico y se formarán mediante la agregación ordenada de cuantos documentos, pruebas, dictámenes, informes, acuerdos, notificaciones y demás diligencias deban integrarlos. Así mismo, debe constar en el expediente copia electrónica certificada de la resolución adoptada.
- Cuando en virtud de una norma sea preciso remitir el expediente electrónico, se hará de acuerdo con lo previsto en el Esquema Nacional de Interoperabilidad y en las correspondientes normas técnicas de interoperabilidad, y se enviará completo, foliado, autentificado y acompañado de un índice, asimismo autentificado, de los documentos que contenga. La autenticación del citado índice garantizará la integridad e inmutabilidad del expediente electrónico generado desde el momento de su firma y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

Por lo tanto, el índice del expediente, se guardará en un fichero XML, que deberá estar firmado con sello electrónico de la Sindicatura de Comptes. Esta firma será en formato XML, y más concretamente firma XAdES-A. Después de definir los conceptos de expediente electrónico y de foliado del mismo, se describen los escenarios identificados:

13.1 Firma electrónica de un documento electrónico

Permite firmar electrónicamente documentos en soporte electrónico en cualquier momento de su ciclo de vida. Estas firmas se realizan bajo el control de la Sindicatura de Comptes.

Las principales características de este escenario son:

- Se realiza la firma sobre un documento original en soporte electrónico.
- El documento original y las firmas se tienen que incorporar al sistema.
- Para asegurar la integridad y la autenticidad de la firma recibida de la aplicación de creación de firmas, será necesario en el caso de firmas usando certificados digitales del firmante validar la firma.

- Debe incorporarse al sistema la evidencia de validación, que en nuestro caso será la firma completada, que en el caso de XML será el mismo documento con firma *attached* o un XML con firma *detached*, y en el caso de PDF, el mismo documento o firma *attached* o *detached*.
- El documento electrónico estará en cualquier formato de los aceptados por la Sindicatura de Comptes, preferiblemente PDF y XML, siempre que sea necesario garantizar su preservación a lo largo del tiempo.
- El documento se podrá firmar varias veces y por diferentes usuarios.
- Se podrá firmar con el sistema de firma electrónica basada en certificado electrónico del firmante o con firma a través de acreditación de la identidad y de evidencias de la voluntad de firma.
- Se podrá firmar en paralelo y/o en cascada.
- En el caso de documentos que no se deban guardar más allá de la validez del sello de tiempo que utilice la Sindicatura de Comptes, la firma (en el caso de la firma a través de acreditación de la identidad y evidencias de la voluntad de firma, la firma se refiere a la firma secundaria) se generará en formato AdES-T o, si no es posible, se completará en este formato.
- En el supuesto de que los documentos se tengan que guardar más allá de la validez del sello de tiempo que utilice la Sindicatura de Comptes, la firma electrónica se generará o se completará en AdES-A. Para los documentos PDF será PAdES-LTV o AdES-A en el caso de firmas *detached* y para los documentos XML será XAdES-A.

Por último, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

- **Clase de firma**: Avanzada o reconocida.
- **Sistema de firma**:
    - **Con certificado electrónico**: Para las firmas generadas por la Sindicatura de Comptes: certificado de empleado o certificado de sello electrónico de la ACCV. Los terceros podrán utilizar cualquier certificado de los definidos en los puntos 6.1 y 6.2 del presente documento.
    - **Con firma a través de acreditación de la identidad y de evidencias de la voluntad de firma**: Podrán generar este tipo de firma los empleados de la Sindicatura en trámites concretos y los terceros.
- **Formatos**: PAdES. Inicialmente en formato PAdES-T. En el caso de preservación, se completará la firma en formato PAdES-LTV.
- **Sello de tiempo**: Sí.
- **Nivel de firma**: Simple, múltiple (en cascada o en paralelo).

- **Tipo de firma**: *Attached* o *detached*.

13.2 Firma mediante código seguro de verificación (CSV)

Permite la firma de documentos a través de la actuación administrativa automatizada, añadiendo un código seguro de verificación (CSV) en el documento definitivo.

Este proceso de firma puede incorporar también una firma con sello electrónico. En este caso tampoco se requiere la intervención del firmante en el proceso de firma, puesto que solo puede ser realizada con certificados de sello electrónico.

Las principales características de este escenario son:

- Firma de varios documentos de forma automática.
- El documento electrónico tiene que estar en formato PDF, PDF / A.
- El documento firmado se guarda en el repositorio de documentos con CSV, desde donde se puede consultar a través de la sede electrónica introduciendo este CSV.

Una vez descritas las características concretas de este escenario, se enumeran los criterios de aplicación y actuación:

- Este escenario está pensado para aquellas tareas en las que se tienen que firmar varios documentos de forma automatizada con garantías jurídicas, cuyo destinatario es un ciudadano.
- Se incorpora el CSV más un texto descriptivo de cómo validar través de la sede electrónica.
- Se podrá utilizar un certificado de sello electrónico o de órgano, que firmaría los documentos en nombre de la aplicación y de la Sindicatura de Comptes.

Por último, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

- **Tipo de firma**: Avanzada.
- **Tipo de certificado**: Sin certificado y en algunos casos con certificado de sello electrónico de la ACCV.
- **Formatos**: Para documentos PDF, CSM, y en caso de firma con sello, PAdES-T, y para su conservación, PAdES-LTV.
- **Sello de tiempo**: No, excepto si se incluye firma con sello.
- **Nivel de firma**: Simple.
- **Tipo de firma**: *Attached*.

Este es un escenario que comprende varios ámbitos que se podrían llegar a identificar como subescenarios diferentes, como pueden ser:

- Firma automatizada de documentos en los que el destinatario es un ciudadano.

13.3 Copia auténtica electrónica de documentos en papel

Permite obtener documentos electrónicos con consideración de copia auténtica a partir de documentos en soporte papel.

Las principales características de este escenario son:

- Consiste en la firma electrónica de un documento digitalizado, en formato PDF, para crear una copia auténtica electrónica.
- La firma es necesaria para garantizar la integridad y la autenticidad del documento digitalizado, así como la fecha de la digitalización.
- El personal de la Sindicatura de Comptes que digitaliza la documentación es el responsable de firmar electrónicamente el documento digitalizado, y debe estar habilitado para hacerlo.
- Los documentos digitalizados se firman incorporando un sello de tiempo. Se genera una firma PAdES-T.
- Para asegurar la integridad y la autenticidad de la firma recibida de la aplicación de creación de firmas, será necesario validarla.
- En el supuesto de que los documentos se tengan que guardar más allá de la validez del sello de tiempo que utilice la Sindicatura, la firma electrónica se generará o se completará en PAdES-A.

Por último, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

- **Tipo de firma**: Avanzada.
- **Tipo de certificado**: Certificado de trabajador público o certificado de sello electrónico de la ACCV.
- **Formatos**: PAdES. Inicialmente, en formato PAdES-T. En el caso de preservación se completará la firma en formato PAdES-LTV.
- **Sello de tiempo**: Sí.
- **Nivel de firma**: Simple.
- **Tipo de firma**: *Attached*.

13.4 Copia electrónica certificada de un documento electrónico firmado electrónicamente

Permite obtener copias electrónicas de documentos originales firmados electrónicamente aplicando un cambio de formato. Este seria el caso, por ejemplo, de la migración de formatos en caso de obsolescencia tecnológica.

Las principales características de este escenario son:

- A partir de un documento original firmado electrónicamente se obtiene una copia (por ejemplo, PDF / A u otro formato de preservación), certificada digitalmente, para guardar.
- La copia del documento electrónico tiene que estar en un formato normalizado y estandarizado, antes de firmar.
- El documento se firmará automáticamente una única vez con sello electrónico a nombre de la Sindicatura de Comptes.

Por último, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

- **Clase de firma**: Avanzada.
- **Tipo de certificado**: Certificado de sello electrónico de ACCV.
- **Formatos**: Dependerá del formato final. Si es PDF / A, se generará en formato PAdES-LTV.
- **Sello de tiempo**: Sí.
- **Nivel de firma**: Simple.
- **Tipo de firma**: *Attached* o *detached*.

13.5 Procesos de firma automatizada

Permite la firma de varios documentos de forma automática con un nivel importante de garantías jurídicas. No requiere la intervención del firmante en el proceso de firma, puesto que solo puede ser realizada con certificados de sello electrónico.

Las principales características de este escenario son:

- Firma de varios documentos de forma automática.
- El documento electrónico puede estar en cualquier formato de los aceptados (PDF y XML).
- Se guardará en el repositorio seguro del servidor de la Sindicatura de Comptes, tanto los certificados digitales como sus correspondientes claves públicas, que tienen que permitir generar procesos de firma automatizada.

Una vez descritas las características concretas de este escenario, se enumeran los criterios de aplicación y actuación:

- Este escenario está pensado para aquellas tareas en las que se tienen que firmar varios documentos de forma automatizada con garantías jurídicas. No se contempla el proceso de digitalización automática de documentos, pues está contemplado en el caso anterior.
- Se utilizará un certificado de sello electrónico o de órgano, que firmará los documentos en nombre de la aplicación y de la Sindicatura de Comptes.
- Habrá una evidencia que demostrará que el responsable del certificado guardado en el repositorio seguro de la Sindicatura de Comptes ha autorizado la firma automatizada.

Por último, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

- **Clase de firma**: Avanzada para los certificados de sello electrónico o de órgano que son avanzados.
- **Tipo de certificado**: Certificado de sello electrónico de la ACCV.
- **Formatos**: Para documentos XML, XAdES-T, y para su conservación, XAdES-A. Para documentos PDF, PAdES-T, y para su conservación, PAdES-LTV.
- **Sello de tiempo**: Sí.
- **Nivel de firma**: Simple.
- **Tipo de firma**: *Attached*.

Este es un escenario que comprende varios ámbitos que se podrían llegar a identificar como subescenarios diferentes, como pueden ser:

- Resellado de documentos para actualizar su validez criptográfica.
- Para procedimientos de intercambio de información entre organizaciones y con administraciones.

13.6 Incorporación de documentos firmados digitalmente por parte del tercero

En el caso de que el tercero entregue un documento firmado electrónicamente por él, será necesario:

- Validar las firmas electrónicas del documento.
- En el caso de que las firmas no sean AdES- A/LTV, se procederá a completar.
- A continuación, se procederá a incorporar en el sistema el documento con sus firmas completadas.

Por último, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

- **Clase de firma**: Avanzada o reconocida en función de los certificados empleados para su firma.
- **Tipo de certificado**: Cualquier certificado definido en el punto 6 del presente documento.
- **Formatos**: Para documentos XML, XAdES-A. Para documentos PDF, PAdES-LTV.
- **Sello de tiempo**: Aconsejado. Una vez completada la firma: sí.
- **Nivel de firma**: Simple, múltiple (en cascada o en paralelo).
- **Tipo de firma**: *Attached*.