Política de identidad y firma electrónica de la Universidad del País Vasco/ Euskal Herriko Unibertsitatea

eman ta zabal zazu

Universidad del País Vasco

Euskal Herriko Unibertsitatea

Julio de 2024

ÍNDICE

1. Introducción y objeto

La Universidad del País Vasco/Euskal Herriko Unibertsitatea (en adelante «UPV/EHU» o «Universidad») establece la presente Política de identidad y firma electrónica (en adelante «política» o «este documento»), que evidencia el compromiso de la institución con el establecimiento del uso de la firma electrónica y la producción de documentos electrónicos con plena validez jurídica y respeto a las líneas maestras de la seguridad documental dentro de la estrategia de implantación de la administración electrónica en la institución.

Esta política regula, dentro del ámbito competencial de la Universidad y de acuerdo con lo previsto en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica y la Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración:

- El alcance y ámbito de aplicación subjetivo de este documento.
- La atribución de roles y responsabilidades a los diferentes actores que deben regir la gestión y desarrollo de la presente política.
- Las líneas maestras de la seguridad documental de la institución.
- Las directrices generales relativas a la identidad electrónica en la institución.
- La identificación de proveedores admitidos para emitir certificados electrónicos y la descripción de los procedimientos para su obtención y gestión.
- Los sistemas y formatos de firma electrónica admitidos.
- Los casos de uso de la firma electrónica.
- La estrategia de preservación de documentos y firmas electrónicas.
- Directrices al respecto del mantenimiento y desarrollo de la política.

En este contexto, la política tiene por objeto establecer la tipología de certificados y firmas electrónicas que la Universidad acepta, tanto en relación a sus órganos y unidades como respecto a todos los miembros de la comunidad universitaria y terceros en sus relaciones con la Universidad, establecer sus usos y procedimientos, los métodos de obtención y su almacenamiento y preservación a largo plazo para poder garantizar la autenticidad, integridad y conservación de los documentos firmados digitalmente mediante las aplicaciones corporativas de la Universidad.

En particular, la implantación del modelo de firma electrónica requiere definir qué certificados electrónicos se admitirán y para qué usos. Por lo tanto, la presente política incluye una relación de los formatos técnicos usados y los tipos de firma generados o aceptados por la Universidad.

También se establecen los sistemas de identificación y firma con registro previo; más concretamente, se regulan el sistema de firma electrónica basada en claves concertadas más las evidencias de la voluntad de firma y el sistema de claves concertadas con segundo factor de autenticación.

Por otro lado, el avance de la tecnología y la consecuente evolución de la normativa aplicable ha propiciado la aparición de otros sistemas que permiten el uso de la firma electrónica mediante mecanismos como la firma biométrica. Por este motivo, esta política también regula la firma digital biométrica, que se podrá usar para firmar presencialmente documentos electrónicos generados por terceros.

Para finalizar, este documento establece las estrategias que la UPV/EHU implementará para la preservación a largo plazo de las firmas electrónicas.

En la elaboración de este documento se ha tenido en cuenta la normativa aplicable en la materia, tanto a nivel supranacional, estatal, autonómico, propia de la universidad y estándares internacionales y otras convenciones detalladas en el apartado 3.

El detalle de los estándares internacionales de referencia es el contemplado en el Anexo III. Estándares internacionales y otras convenciones del presente documento.

2. Ámbito de aplicación subjetivo

Este documento se aplica a todas aquellas personas o entidades que establezcan relaciones con la UPV/EHU que requieran la producción o intercambio de documentos electrónicos auténticos.

La política también se aplica a todo el personal, incluido el directivo, de la Universidad, con independencia de la modalidad contractual que determine su relación con la institución, la posición jerárquica que ocupen dentro de la organización y sea cual fuere su centro de trabajo, donde preste servicio, tanto sea en el ámbito docente, de investigación o de soporte.

3. Normativa aplicable

El reciente cambio de paradigma que ha supuesto el uso del documento electrónico es el resultado de la aparición de cambios normativos que han impulsado las herramientas telemáticas y que, en determinadas circunstancias, han equiparado los documentos electrónicos a los documentos en formatos más tradicionales. Por otro lado, las organizaciones encargadas de la estandarización técnica han definido y documentado los criterios y formatos que se usarán para la gestión de los documentos digitales en todos sus aspectos, garantizando su validez jurídica.

El contenido del presente apartado contempla el marco normativo y los estándares internacionales y otras convenciones de referencia para la aplicación de la presente Política de identidad y firma electrónicas de la UPV/EHU.

3.1 Normativa de ámbito europeo

- Reglamento (UE) 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 y por la que se deroga la Directiva 1999/93/CE. (Reglamento eIDAS en adelante)
- 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 anteriormente referenciado.

3.2 Normativa de ámbito estatal

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

- 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 Documento Electrónico.
- Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración.
- Resolución de 14 de julio de 2017, de la Secretaría General de Administración Digital, por la que se establecen las condiciones de uso de firma electrónica no criptográfica, en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado y sus organismos públicos.

3.3 Normativa de ámbito autonómico

- Ley 3/2022, de 12 de mayo, del Sector Público Vasco.
- Ley 5/2022, de 23 de junio, de Gestión Documental Integral y Patrimonio Documental de la Comunidad Autónoma del País Vasco.
- Decreto 232/2000, de 21 de noviembre, por el que se aprueban el Reglamento de los Servicios de Archivo y las normas reguladoras del Patrimonio Documental del País Vasco.

3.4 Normativa propia de la Universidad

La Política complementa y desarrolla lo que ya prevé la normativa general de la UPV/EHU que se detalla a continuación:

- Reglamento de funcionamiento y actuación por medios electrónicos de la Universidad Vasco/Euskal Herriko Unibertsitatea (2024).
- Reglamento de Archivo y Gestión Documental de la Universidad del País Vasco/Euskal Herriko Unibertsitatea (2024).
- Política de gestión de documentos electrónicos (PGDE) de la Universidad del País Vasco / Euskal Herriko Unibertsitatea (2024).

3.5 Estándares internacionales y otras convenciones

El Anexo III. Estándares internacionales y otras convenciones incluye la relación de todos los estándares internacionales y otras convenciones que definen los distintos formatos, tipos de firma y sello electrónico y el resto de las tecnologías que inspiran este documento.

4. Datos de la Política de identidad y firma electrónica de la Universidad

4.1 Identificación de la Política

Nombre del documento	Política de identidad y firma electrónica de la Universidad del País Vasco/ Euskal Herriko Unibertsitatea
Versión	1.0
Identificador de la política	Política de identidad y firma electrónica de la Universidad del País Vasco/ Euskal Herriko Unibertsitatea
Fecha de aprobación	Julio 2024
Ámbito de aplicación	Documentos y expedientes producidos y/o custodiados por la Universidad
Responsable de la Política y datos de contacto	Vicerrectorado de Transformación Digital y Comunicación E-mail: Telf.:

5. Roles y responsabilidades

A continuación, se establece la atribución de roles y responsabilidades de las áreas de la Universidad implicadas por el presente documento:

5.1 Consejo de Gobierno

- Aprobar la política.

5.2 Órgano competente en Transformación Digital

- Determinar los aspectos funcionales de la política.
- Determinar las soluciones apropiadas para dar cumplimiento a esta política.
- Comprobar el estado de cumplimiento de la política, su adecuación a las necesidades reales de la comunidad universitaria y su alineamiento con las tecnologías disponibles.
- Garantizar la publicación en Sede Electrónica de las versiones actualizadas de la presente política.
- Mantener y actualizar la política.

5.3 Órgano competente en Tecnologías de la Información y las Comunicaciones

- Determinar los aspectos técnicos en la aplicación de la política.
- Implantar y mantener las plataformas y soluciones tecnológicas apropiadas para dar cumplimiento a esta política.

5.4 Todas las áreas y estudios

- Conocer la política.
- Cumplir con su contenido.

6. Líneas maestras de la seguridad documental

Con la finalidad de garantizar que todos los documentos electrónicos producidos en la Universidad, así como los recibidos de fuentes externas, sean auténticos y legalmente válidos y que preserven esas características a corto y largo plazo, es necesario establecer las siguientes líneas maestras que deben aplicarse a todos los sistemas de la Universidad:

Identidad electrónica robusta: las soluciones de firma electrónica aplicadas deben garantizar la identificación cierta de los usuarios/as y de las personas que participan en los procesos. Los mecanismos aplicados para el acceso a instrumentos de autenticación deben garantizar una identificación suficiente, así como incorporar controles para evitar un uso fraudulento o negligente.

Autenticidad y autoría de los documentos electrónicos: las soluciones de firma electrónica aplicadas deben poder atribuir la autoría de los documentos electrónicos y el resto de acciones relacionadas con los mismos a personas concretas. Siempre que sea necesario deberán ser capaces de dar garantías autocontenidas y suficientes con la finalidad de que los destinatarios del documento electrónico tengan prueba de su autenticidad y estén protegidos contra el riesgo de repudio.

Integridad de los documentos electrónicos: las soluciones de seguridad de la información aplicadas deben aportar mecanismos que permitan acreditar y verificar que los documentos electrónicos ya emitidos no estén alterados o hayan sido sustituidos.

Preservación documental: los documentos y firmas electrónicas deben generarse en formatos adecuados, que incorporen los mecanismos necesarios para poder garantizar su preservación a largo plazo cumpliendo constantemente con los objetivos de autenticidad e integridad.

Proporcionalidad: los mecanismos de seguridad aplicados a cada proceso deben ajustarse a las necesidades y riesgos asociados a cada tipo de actuación, sin exigir medidas o controles excesivamente gravosos que impidan un uso eficiente de los instrumentos.

Usabilidad: cuando sea posible, se optará por aquellas soluciones que, sin afectar a los elementos aplicados de identificación, autenticidad, integridad y preservación, permitan un uso sencillo, rápido, intuitivo y grato de los servicios tecnológicos.

7. Identidad electrónica admitida en la Universidad

El uso de las relaciones telemáticas implica la necesidad de identificar a todas las partes participantes de forma segura y cierta. En consecuencia, la Universidad admite los siguientes medios de acreditación electrónica de la identidad.

1. **Sistemas de identificación basados en certificados electrónicos reconocidos o cualificados**, emitidos por una autoridad contemplada en la lista de prestadores de servicios electrónicos de confianza del Ministerio competente.

2. **Sistemas de identificación basados en certificados electrónicos no cualificados**, emitidos por una autoridad contemplada en la lista de prestadores de servicios electrónicos de confianza del Ministerio competente.

3. **Sistemas de identificación basados en certificados electrónicos reconocidos o cualificados de sello electrónico**, emitidos por una autoridad contemplada en la lista de prestadores de servicios electrónicos de confianza del Ministerio competente.

4. **Sistemas de identificación por medios biométricos**. Estos sistemas permiten el registro o validación de la identidad de una persona mediante la comprobación electrónica sobre datos de su misma persona como pueden ser la huella dactilar, la firma manuscrita u otros basados en biometría. El uso de estos sistemas está condicionado a la capacidad para cifrar de forma confidencial los datos personales de la persona firmante.

5. **Sistemas de identificación de la propia Universidad basados en registro previo** (usuario y contraseña)

8. Certificados electrónicos

8.1 Certificados electrónicos utilizados por la Universidad

Con el objetivo de dar cumplimento a las previsiones de los apartados anteriores a continuación, se indican los tipos de certificados digitales que la Universidad utilizará, tanto a nivel de persona empleada de la UPV/EHU (Personal Docente e Investigador y Personal Técnico, de Gestión y de Administración y Servicios) como para aquellas personas que puedan representar a la Universidad frente a terceros, como para la actuación administrativa automatizada como finalmente a nivel técnico.

Personas empleadas de la Universidad

Las personas empleadas de la UPV/EHU deben hacer uso del sistema corporativo de firma electrónica, proporcionado por la Universidad, que incluye un certificado electrónico, valido para la identificación y la firma en todos aquellos trámites o actuaciones que deban realizar en su condición de personal al servicio de la UPV/EHU. Dicho sistema se denomina certificado profesional:

Certificado profesional: Certificado personal, emitido por el prestador cualificado de servicios electrónicos de confianza de la Universidad, que contiene los datos de identidad de la persona y el dato de vinculación con el ente en el que trabaja, en este caso la Universidad del País Vasco/ Euskal Herriko Unibertsitatea. La gestión de la emisión y revocación del Certificado de las personas empleadas en la Universidad, la realizan las autoridades de registro de la Universidad (RAs).

Personas empleadas representantes de la Universidad

Las personas empleadas cuando actúen como representantes legales, con competencia estatutaria de la Universidad, y que sea una actuación que solo puedan realizar en virtud de su cargo, harán servir el Certificado de Representante:

Certificado de representante: Certificado personal, emitido por el prestador cualificado de servicios electrónicos de confianza de la Universidad., que solo pueden disponer las personas que tienen atribuida la competencia de representar a la Universidad, frente terceros. Contiene los datos de identidad de la persona y los de la Universidad. La gestión de las solicitudes para la emisión y revocación de este tipo de certificados se realiza desde el Órgano competente en la Transformación Digital

Certificados Técnicos

Certificados de sello electrónico: Certificado, que sirve para autorizar la actuación administrativa automatizada según el artículo 42 de la Ley 40/2015. Cabe usar este tipo de certificado para realizar copias electrónicas, foliado de expedientes y emisión de documentos que no requieran la intervención del personal público. La UPV/EHU dispone de un Certificado de Sello emitido por el prestador cualificado de servicios electrónicos de confianza de la

Universidad. La gestión de las solicitudes para la emisión y revocación de este tipo de certificados se realiza desde el Órgano competente en la Transformación Digital.

Certificados de aplicación: Certificados que sirven para la identificación de aplicaciones, servidores, sistemas o servicios web o para el intercambio de datos entre administraciones, administraciones y ciudadanía y entre administraciones y empresas. Este tipo de certificado es el requerido para una aplicación que envía mensajes que requieran asegurar su integridad y autenticidad. El uso de este tipo de certificado no produce efecto jurídico alguno. La gestión de las solicitudes para la emisión y revocación de este tipo de certificados se realiza desde el órgano responsable de las Tecnologías de la Información y Comunicación.

Certificados de servidor seguro: Certificados que permiten garantizar el acceso seguro en los entornos de tramitación telemática de la institución, como la sede electrónica o las páginas web de la Universidad. La Universidad dispone de un Certificado de Sede emitido por el prestador cualificado de servicios electrónicos de confianza de la Universidad. El uso de este tipo de certificado no produce efecto jurídico alguno. La gestión de las solicitudes para la emisión y revocación de este tipo de certificados se realiza desde el órgano responsable de la Transformación Digital.

El Anexo II. Certificados electrónicos para uso por parte de la Universidad y su personal de este documento identifica las tecnologías y proveedores concretos admitidos por la Universidad en cada caso. El Órgano competente en Transformación Digital y Comunicación realizará la actualización del contenido del Anexo II. Certificados electrónicos para uso por parte de la Universidad y su personal en función de la evolución de la tecnología o de las prácticas de certificación de cada prestador.

8.2 Personas autorizadas a disponer de certificado electrónico en la Universidad

Toda persona empleada pública de la Universidad debe disponer del certificado profesional, gestionado por la Universidad y emitido por el prestador de servicios cualificados de la Universidad, de acuerdo con el procedimiento establecido en el apartado 8.4.1. En particular:

- Todo el personal de la Universidad debe utilizar el Certificado profesional de la Universidad en las actuaciones que realice por razón de su condición de personal empleado de la Universidad que requieran de la identificación y/o firma. Es responsabilidad de la persona empleada por la Universidad asegurarse de la vigencia de su certificado.
- Las personas que por cargo o designación puedan representar a la Universidad podrán disponer de un certificado electrónico de representante, de las tipologías previstas en el Anexo II. Certificados electrónicos para uso por parte de la Universidad y su personal.

El resto de las personas vinculadas a la Universidad o personas que participen o colaboren puntualmente con ella, podrán usar un certificado de persona física u obtener un certificado electrónico de vinculación con la Universidad, si este fuese preciso, acompañando la

justificación de su necesidad que será verificada por su superior jerárquico o por la persona responsable del servicio con quien que colabore y requerirá para su emisión de la validación y aceptación del órgano Competente de la Coordinación de la Universidad.

8.3 Certificados electrónicos admitidos por la Universidad

En relación con los certificados electrónicos admitidos por la Universidad, para su relación con la Ciudadanía, cabe destacar dos casuísticas.

8.3.1 Certificados basados en certificados cualificados

Las personas interesadas que se relacionen con la Universidad podrán hacer uso de los certificados referenciados en la lista de prestadores de servicios electrónicos de confianza (TSL) que mantiene el Ministerio competente para identificarse en las actuaciones en las que intervengan, así como para la firma electrónica de la documentación en soporte digital.

Esta lista es consultable en https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx

8.3.2 Certificados basados en certificados no cualificados

Las personas interesadas que se relacionen con la Universidad podrán hacer uso de certificados no cualificados emitidos por un prestador de servicios electrónicos de confianza (TSL) de los listados por el Ministerio competente.

Concretamente, la Universidad admitirá como medio de identificación y firma electrónica la Bak certificado no cualificado emitido por el prestador cualificado de servicios electrónicos de confianza de la Universidad, en aquellas transacciones o trámites que de baja criticidad

8.4 Procedimientos relacionados con el ciclo de vida de los certificados electrónicos

8.4.1 Obtención, renovación y revocación

Corresponde al Órgano competente en Transformación Digital, el establecimiento de los procedimientos a seguir para la obtención, renovación y revocación de los diferentes tipos de certificados en uso en la Universidad.

La renovación de estos procedimientos se hará de oficio, siempre que los cambios en las circunstancias normativas o tecnológicas lo hagan necesario.

Los procedimientos vigentes en cada momento se harán accesibles a todo el personal en el ámbito que corresponda dentro de la Intranet o en el portal web del empleado.

Como mínimo se deberá formular procedimiento para:

- Obtención de un certificado de representante de UPV/EHU.
- Obtención de un certificado profesional de la UPV/EHU.

- Obtención de un certificado de sello electrónico.
- Revocación de un certificado electrónico.
- Renovación de un certificado electrónico.

8.4.2 Almacenamiento de los certificados electrónicos

Los certificados electrónicos de la Universidad se pueden encontrar en los siguientes repositorios:

En tarjeta criptográfica.

En el repositorio criptográfico de servidores para los certificados de servidor seguro y de sello electrónico.

En software.

En la nube centralizada y segura del prestador cualificado de servicios electrónicos de confianza de la Universidad.

8.4.3 Mantenimiento del inventario de certificados electrónicos de la Universidad

El mantenimiento del inventario de los certificados electrónicos de la Universidad recae en el prestador cualificado de servicios electrónicos de confianza de la Universidad, que emite los certificados de la Universidad y la Universidad dispondrá de acceso a esa información.

9. Sistemas de firma electrónica admitidos en la Universidad

Para que los documentos electrónicos sean considerados auténticos y tengan validez jurídica, es necesario que estén firmados electrónicamente. La firma electrónica actúa como una herramienta de autenticación y asegura la integridad del documento.

En consecuencia, la Universidad admite los siguientes medios de firma electrónica.

1. **Sistemas de firma electrónica basados en certificados electrónicos no cualificados (de persona física)**, emitidos por una autoridad contemplada en la lista de prestadores de servicios electrónicos de confianza del Ministerio competente. Utilizado para firmas de nivel de seguridad bajo.

2. **Sistemas de firma electrónica basados en certificados electrónicos reconocidos o cualificados (de persona física, profesional o de representante)**, emitidos por una autoridad contemplada en la lista de prestadores de servicios electrónicos de confianza del Ministerio competente.

3. **Sistemas de firma electrónica basados en certificados electrónicos reconocidos o cualificados de sello electrónico**, emitidos por una autoridad contemplada en la lista de prestadores de servicios electrónicos de confianza del Ministerio competente. Este tipo de firma solo se podrá utilizar para firmas por parte de administraciones públicas.

4. **Sistemas de firma electrónica biométrica**. Estos sistemas de firma electrónica solo se podrán usar si la firma electrónica biométrica se ha generado en la misma universidad de acuerdo con el artículo 10.5 de la presente política de firma electrónica.

5. **Sistemas de firma electrónica basada en claves concertadas más las evidencias de la voluntad de firma** (usuario y contraseña). Este sistema de firma solo se admitirá para firmas generadas con registro previo en la Universidad y de acuerdo con los artículos 10.3 y 10.4 de la presente política de firma electrónica.

6. **Sistemas de firma electrónica basado en Código Seguro de Verificación (CSV).** Este sistema solo se admitirá si ha sido generado por una administración pública y esta ha declarado en su política de firma que el CSV es un sistema de firma electrónica. Para ello, el personal de la Universidad que reciba el documento firmado deberá ir a la Sede Electrónica de la Administración Pública emisora y comprobar la integridad del documento presentado.

10. Sistemas de firma electrónica usados por la Universidad

Los sistemas de firma electrónica contemplados en este apartado son los que se podrán usar en las aplicaciones corporativas de la Universidad y tendrán la finalidad de garantizar la autenticidad, integridad, inalterabilidad y conservación de los documentos firmados digitalmente. Cuando el personal de la Universidad participe en procedimientos definidos por otra organización generarán las firmas en los formatos determinados; y, si es necesario añadir copia al expediente de la Universidad, se aplicarán las comprobaciones indicadas en el Anexo IV. Comprobaciones para tener en cuenta en la validación de firmas de terceros.

10.1 Firma electrónica mediante certificado electrónico personal (profesional o de representante o de persona física)

Consiste en el sistema de firma electrónica en el que, partiendo de la clave privada del certificado de una persona, se cifra el resumen criptográfico del documento a firmar y se incorpora información del certificado usado para efectuar la firma, por ejemplo, la fecha de firma o referencia a la política de identidad y firma electrónica.

El personal empleado de la UPV/EHU usará este sistema para firmar documentos electrónicos haciendo uso del Certificado Profesional o el Certificado de Representante emitido por prestador cualificado de servicios electrónicos de confianza de la Universidad.

10.2 Firma electrónica mediante sello electrónico por actuación administrativa automatizada

Este sistema de firma permite la firma de documentos electrónicos de la Universidad mediante procesos automatizados sin intervención directa del personal a su servicio.

Consiste en el sistema en que, partiendo de la clave privada de un certificado electrónico de sello electrónico, se cifra el resumen criptográfico del documento a firmar y se le añade información del certificado de sello electrónico usado para efectuar la firma, por ejemplo, la fecha de firma o referencia a la política de identidad y firma electrónica.

Este tipo de firma se podrá usar en las actuaciones administrativas automatizadas previamente establecidas mediante resolución del Secretario o de la Secretaria General de la Universidad, de acuerdo con el artículo 41.2 de la Ley 40/2015, que se publicará en la sede electrónica.

10.3 Firma electrónica basada en claves concertadas más las evidencias de la voluntad de firma

El sistema de firma electrónica consistente en el uso de claves concertadas más las evidencias de voluntad de firma se basa en la identificación de la persona firmante mediante su usuario

y contraseña previamente proporcionados por la Universidad, que constituye una primera evidencia de autenticación.

La usabilidad de este sistema estará condicionada a la calidad del mecanismo de distribución de identidades de la Universidad. En consecuencia, los procedimientos de obtención de las credenciales a usar para generar este tipo de firmas deberán garantizar:

Que la identidad de la persona haya sido verificada de forma cierta por una persona empleada de la Universidad con carácter previo a la emisión de las credenciales, ya que en caso de no cumplirse tal condición no se podrá usar la pareja de claves para generar firmas, hecho que quedará acreditado en el sistema de gestión de credenciales, que deberá tener capacidad para dejar constancia de tal circunstancia. La verificación posterior de la identidad permitirá convalidar las credenciales para su uso futuro como mecanismo de firma.

Que los sistemas de gestión de las credenciales garanticen su custodia segura, su renovación de acuerdo con los periodos establecidos en las políticas de seguridad de la Universidad y un control sobre el número de intentos fallidos de identificación que lleven al bloqueo de la credencial para prevenir un uso fraudulento.

Que las personas usuarias reciban la información oportuna sobre la criticidad del sistema de credenciales y la importancia de la confidencialidad de las claves.

Durante el proceso de firma, la persona firmante deberá dar su consentimiento explícito para la firma (puede ser a través de pulsar un botón en la aplicación correspondiente).

Como medida adicional para garantizar la robustez de la identificación, se puede requerir adicionalmente a la persona usuaria la respuesta a un reto de identificación basado en el envío de un código de un solo uso a una dirección de correo electrónico o a un dispositivo móvil registrado previamente. Esta medida se considera complementaria a la de la pareja de claves, constituyendo un doble factor de identificación.

Una vez verificada la identidad se creará un fichero de evidencias que se almacenará en el mismo documento electrónico. En el caso en que no fuera técnicamente posible, las evidencias se guardarán en los sistemas corporativos de la Universidad, informando sobre el lugar concreto en el que se almacenarán en la definición del propio procedimiento administrativo.

Por lo tanto, la validez jurídica del sistema de firma electrónica efectuada mediante claves concertadas más evidencias de la voluntad de firma está vinculada al documento electrónico y a las evidencias del proceso de identificación de la persona firmante que acepta la firma.

En el caso en que el procedimiento administrativo lo requiera, se podrán contemplar sistemas de doble o triple evidencia de autenticación, pudiéndose almacenar también las evidencias relacionadas a tales factores.

Es posible que el documento electrónico contenga más de una firma electrónica basada en claves concertadas más las evidencias de voluntad de firma. Normalmente, cuando se dé tal

caso, todas las firmas serán del tipo "detached" (separadas) sin el requisito de que todas estas se almacenen en el mismo formato, siempre que se pueda garantizar la posibilidad de verificar la autenticidad de cada una de ellas.

En el caso de conflicto entre las firmas que incorpore el documento electrónico, la Universidad podrá acreditar:

Que el procedimiento de firma está regulado de forma específica.

Que se han generado las evidencias en todas las firmas del mismo tipo.

Que la firma se produjo en un momento determinado mediante la aplicación de un sello de tiempo.

Que el documento no ha sido modificado mediante la aplicación del "hash" en las evidencias del documento.

Que se ha aplicado una firma secundaria al documento electrónico consistente en la aplicación de un certificado de sello electrónico de la Universidad.

10.4 Complemento de segundo factor de autenticación

El sistema se basa en la confirmación de la identidad de una persona mediante el envío de un correo electrónico a una dirección de correo electrónico que conste efectivamente vinculada a esa persona, o bien, la recepción de un mensaje SMS en un teléfono móvil que también conste registrado previamente a nombre de esa persona. Este mensaje contiene una contraseña de un solo uso llamada OTP (***One-Time Password***).

Es necesario insistir en la importancia de que la vinculación entre la persona y el medio donde se reciba la contraseña debe estar registrada previamente en base a una verificación anterior. No se podrá utilizar este mecanismo de firma si el código de confirmación se envía a una dirección o teléfono que el usuario suministra en ese mismo momento.

Durante el proceso de firma, el usuario habrá superado los retos de identidad mediante la recepción del correo electrónico en la dirección antes citada o dando respuesta a un reto de identificación basado en mensaje de texto. Si este sistema es complementario con una identificación del usuario en la aplicación mediante credencial de claves concertadas, la combinación de ambos mecanismos constituye un doble factor de autenticación.

Una vez verificada la identidad se creará un fichero de evidencias que se almacenará en el mismo documento electrónico. En el caso en que no fuera técnicamente posible, las evidencias se guardarán en los sistemas corporativos de la Universidad, informando sobre el lugar concreto en el que se almacenarán en la definición del propio procedimiento administrativo.

Posteriormente a la incorporación de las evidencias, se procederá a firmar el documento electrónico o el paquete de evidencias si estas no se han podido consolidar, mediante el uso de un certificado electrónico de sello electrónico en nombre de la Universidad.

Las evidencias objeto de captura deberán incluir, como mínimo:

- Nombre y código identificador (NIF o similar) de la persona firmante.
- Título y resumen criptográfico del documento firmado.
- Fecha y hora de la firma.
- Forma de identificación de la persona firmante (nombre de usuario o identidad alegada)
- Correo electrónico o número de teléfono al que se ha mandado el reto adicional emitido.
- Verificación de que el reto ha sido superado con éxito.
- Identificación del sistema de tramitación que gestiona la firma.
- Dirección IP desde la que se conecta la persona usuaria.

Por lo tanto, la validez jurídica de la firma electrónica, realizada con OTP más evidencias de voluntad de firma, está vinculada, por un lado, al documento y, por otro, a las evidencias del proceso de identificación de la persona que firma con la aceptación de la firma.

En este formato de firma puede haber más de una firma de este tipo sobre el documento, que deberá generarse en paralelo.

En el caso de conflicto entre las firmas que incorpore el documento electrónico, la Universidad podrá acreditar:

- Que el procedimiento de firma está regulado de forma específica.
- Que se han generado las evidencias en todas las firmas de cualquier tipo.
- Que la firma se produjo en un momento determinado mediante la aplicación del sello de tiempo.
- Que el documento no ha sido modificado mediante la aplicación del "hash" en las evidencias del documento.
- Que se ha aplicado una firma secundaria al documento electrónico consistente en la aplicación de un certificado de sello electrónico de la Universidad.

10.5 Firma electrónica biométrica

Este sistema de firma electrónica avanzada se genera a partir de los datos biométricos de la persona firmante, que se incorporan, de forma cifrada, al resumen criptográfico de los documentos electrónicos generados, de forma que permiten acreditar la auditoría de la firma aplicada mediante la siguiente información necesaria:

Datos biométricos de la persona que firma el documento de forma manuscrita que se recogen mediante elementos específicos de captura que permiten la visualización del documento en el mismo acto de firma, entre ellos:

- El detalle temporal concretado en el inicio, final y duración en milisegundos del proceso de firma del documento.
- El detalle del trazado, en relación con la velocidad, aceleración y presión de éste en toda su figura.

Otra información que pueda resultar relevante para el proceso de firma, como puede ser la identificación de las aplicaciones y programas usados para la captura de la firma o la localización GPS de las máquinas usadas para captar la firma.

Este sistema de firma electrónica avanzada solo se aplica en la biometría de la firma manuscrita, sin usar otras medidas biométricas como el reconocimiento facial o el uso de la huella dactilar que quedan fuera del ámbito de esta política, sin perjuicio de que se puedan considerar en un futuro.

El cifrado de la información se lleva a cabo mediante la clave pública de un certificado específico de firma electrónica biométrica que se almacena en los servidores de la Universidad. La clave privada la custodiará un tercero de confianza al que se le podrá requerir cuando sea necesario para que verifique las firmas biométricas en caso de reclamación o litigio.

Un mismo documento podrá incluir más de una firma biométrica, pero siempre de forma paralela entre ellas.

Una vez se hayan realizado todas las firmas biométricas en paralelo y se haya cifrado la información detallada al principio de este apartado, esta se guardará de forma conjunta con el documento y, con el objetivo de garantizar la integridad de este último, se realizará, sobre este, una firma electrónica automática de sello electrónico de aplicación perteneciente a la Universidad completada con un sello de tiempo.

En consecuencia, la validez jurídica de la firma electrónica biométrica estará vinculada al documento y a las evidencias biométricas que se guardan dentro de este mismo de forma cifrada con la aportación de la firma electrónica y el sello de tiempo para evidenciar su integridad.

En caso de conflicto, una vez descifrados los datos por parte del tercero de confianza que custodia la clave privada del certificado de cifrado, se deberá solicitar un peritaje de los datos biométricos guardados en el documento y cotejarlas con una nueva toma en condiciones similares, por lo que respecta a la maquinaria, aplicaciones y programas usados en la firma controvertida, de datos biométricos de la persona a quien se alega que pertenecen.

10.6 Firma múltiple

El caso de la firma múltiple se da cuando existen dos o más firmas electrónicas en el mismo documento. Dependiendo de la forma en que se estas se han efectuado, se considera que se han realizado de forma secuencial o paralela:

Firma secuencial: Cuando la segunda firma se realiza sobre el objeto digital ya firmado anteriormente. Siempre que sea posible se evitará su uso para los circuitos de firma en los que los documentos electrónicos se tengan que firmar a la vez con el mismo objetivo por parte de una pluralidad de personas.

Firma paralela: Cuando las firmas se refieren al mismo objeto digital que tiene un único resumen criptográfico, sea porque se han generado en formato "detached" (separado) o porque el documento está preparado para recibir firmas "attached" (adjuntas) en paralelo.

El uso de la firma múltiple se dará en varias actuaciones en el marco de los diversos procedimientos administrativos de la Universidad, como la firma de documentos electrónicos por parte de más de una persona o el resellado de documentos firmados con carácter previo a que se pueda poner en duda la validez criptográfica de la firma electrónica, con el objetivo de actualizar su validez legal a lo largo del tiempo.

Se procurará que en todos los casos de firma de documentos electrónicos por más de una persona se usen tecnologías similares, evitando particularmente que se generen documentos firmados por una parte basándose en certificados y otra mediante el uso de la firma biométrica.

La combinación de diversos sistemas de firma electrónica será posible en los siguientes casos:

Firmas electrónicas mediante el uso de certificados electrónicos de forma paralela o secuencial para cualquier documento electrónico que requiera más de una firma.

Firmas electrónicas biométricas, que serán de forma secuencial, para documentos electrónicos que se generen presencialmente frente a terceros y requieran dos o más firmas.

Firma electrónica biométrica y, posteriormente, firma electrónica mediante certificado electrónico (imbricada), en el caso de documentos en soporte electrónico que se generen ante un tercero y que, posteriormente a su firma sobre la base de la biometría, requiera la firma electrónica posterior para completar su validez, mediante sello electrónico.

> Es importante asegurarse de que se conservan correctamente las evidencias de la firma no criptográfica y que el sello electrónico que se incorpora en último lugar de cobertura a todo el contenido del documento.

Firmas electrónicas mediante sistemas basados en claves concertadas, de forma paralela o secuencial, en el caso de documentos electrónicos que requieran más de una firma.

Firma electrónica mediante un sistema basado en claves concertadas y, posteriormente, la aplicación de una firma electrónica mediante un certificado electrónico, de forma paralela o

secuencial, para aquellos documentos electrónicos que requieran la firma de dos personas, solo una de las cuales cuenta con certificado electrónico.

Con carácter general se procurará que, en todos los casos de firma del documento por varias personas, todas las personas participantes utilicen tecnologías similares (se evitará generar documentos firmados por una parte con firma basada en certificados, y otra parte con firma biométrica).

10.7 Sello de tiempo

El sello de tiempo es un tipo de firma electrónica generada por un tercero de confianza en base a un certificado electrónico especialmente diseñado a tal efecto que permite acreditar la fecha y hora en la que se ha producido el acto, que puede hacer referencia a:

El momento de firma del documento, en este caso el sello de tiempo estará asociado a la firma electrónica aplicada.

El momento de la creación del documento, en este otro caso el sello de tiempo estará asociado al documento electrónico.

Este tipo de firma electrónica sella la fecha y hora del instante en que se realiza el acto mediante un proveedor de sellado de tiempo que, con carácter general, será el servicio cualificado de sellado de tiempo del prestador cualificado de servicios electrónicos de confianza de la Universidad.

El procedimiento de uso del sello de tiempo consiste en la creación de una evidencia sobre una firma electrónica mediante el cálculo del resumen criptográfico del documento y/o de las firmas electrónicas en caso de resellado. Es decir, se realiza una operación matemática que se aplica al conjunto de información sobre la que se emitirá el sello de tiempo que resulta en una cadena de bits llamada "hash" y que se cifra con la clave privada del certificado de sello de tiempo usado para tal operación.

El resultado de la aplicación del certificado de sello de tiempo da como resultado la incorporación de la fecha y hora de la operación en el documento electrónico, así como información del certificado de sello de tiempo usado para su firma.

11. Requisitos comunes sobre el formato de las firmas electrónicas basadas en certificados

En caso de usar por parte de la Universidad sistemas de firma basados en certificados electrónicos se indican los siguientes requisitos comunes a cumplir.

Cuando se usen firmas basadas en certificados, estas serán preferentemente del tipo "PAdES" cuando se puedan generar como una firma attached (adjunta) a un documento en formato PDF; en otros casos, si el documento es XML se usará firma attached en formato XAdES y en el resto de casos se usará la firma detached (separada) en formato XAdES.

Con carácter general las firmas deberán incorporar sello de tiempo, pero para aquellos documentos cuyo tiempo de custodia sea superior a cuatro años el formato será de archivo.

A continuación, se adjunta una tabla que detalla los formatos de firma a usar:

	Generalmente, con sello de tiempo	**Documentos conservación a largo plazo**
Cuando sea posible, firma *attached* (adjunta) sobre PDF	PAdES-T-Level	PAdES-LTA-Level
En caso de documentos XML cuando esto sea posible firma *attached* (adjunta)	XAdES-T-Level	XAdES-LTA-Level
En otros casos, firma *detached* (separada)	XAdES-T-Level	XAdES-LTA-Level

NOTA: el proceso de generación de los formatos de firma para documentos de conservación a largo plazo se podrá realizar o bien directamente en el momento de la firma, o bien se podrán generar a partir de procesos internos en la Universidad de completado de las firmas con sello de tiempo a estos formatos LTA-Level

12. Estrategia de preservación de documentos y firmas electrónicas

Pese a que la firma electrónica permite acreditar la autenticidad de la expresión de la voluntad en documentos electrónicos, existen ciertos riesgos para su plena validez que deben gestionarse debidamente para garantizar la validez jurídica indefinida del documento electrónico.

Tales riesgos son:

La caducidad del certificado digital o del sello electrónico mediante el cual se firma un documento electrónico.

La validez del certificado digital o del sello electrónico en el momento en que se genera la firma electrónica.

La posible obsolescencia tecnológica de la longitud de las claves criptográficas contenidas en los certificados digitales mediante los cuales se generan firmas electrónicas.

En la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración se especifican una serie de mecanismos para la protección de la firma/sello electrónico frente a la posible obsolescencia de los algoritmos y el aseguramiento de sus características a lo largo del tiempo de validez. Concretamente:

Utilización de mecanismos de resellado de tiempo, para añadir, cuando el anterior sellado este próximo a su caducidad, un sello de fecha y hora de archivo con un algoritmo más robusto. Para ello, es necesario el uso de firmas longevas.

Almacenamiento de la firma electrónica en un depósito seguro, que garantice la protección de la firma contra modificaciones y asegurando la fecha exacta en que se guardó la firma electrónica, y en la que se comprobó la autenticidad y vigencia de los elementos que la conforman.

En el caso de la Universidad se opta por aplicar el resellado de las firmas.

12.1 Resellado y preservación de documentos y firmas electrónicas en entornos propios

El proceso de resellado consiste en la renovación del sello de tiempo aplicado al documento electrónico, mediante la incorporación de un nuevo eslabón en la cadena de evidencias electrónicas a las firmas electrónicas que el documento ya contiene. El objetivo principal del proceso es garantizar la conservación, integridad y autenticidad del documento electrónico a lo largo del tiempo.

El resellado se aplicará a aquellos documentos electrónicos que no hayan sido transferidos a la solución de archivo definitivo de la Universidad en el momento en que esté a punto de caducar el último sello de tiempo aplicado a la firma electrónica a preservar y, de forma excepcional, cuando se haya detectado la obsolescencia tecnológica de los algoritmos o claves que firman el documento en cuestión.

Este proceso requiere que las firmas del documento sean del formato XAdES-LTA-Level o PAdES-LTA-Level que son los tipos de firma que admiten añadir evidencias temporales. En el caso en que la firma no esté en uno de los dos formatos, antes de llevar a cabo el proceso de resellado, habrá que completar la firma de los documentos en uno de los formatos indicados.

Se añadirá entonces, un nuevo sello de tiempo a las firmas XAdES-LTA-Level o PAdES-LTA-Level que deberá:

Estar generado con un certificado reciente.

Tener periodo de validez superior a las firmas a resellar.

Tener una longitud de clave suficiente con el objetivo de que no pueda resultar comprometida.

Aplicar un algoritmo o clave que no esté sujeto a la obsolescencia criptográfica del mismo en el momento en que se emite.

Por lo que respecta a las firmas realizadas mediante la acreditación de la identidad y la recogida de evidencias de la voluntad de firma, se recomienda que se proceda al resellado de la firma secundaria, es decir, el sello de tiempo.

12.1.1 Preparación de los documentos para la preservación

Para que los documentos puedan estar sujetos al resellado se deberá asegurar que tienen una firma susceptible de ser resellada. Se recomienda que el proceso de revisión de la validez de las firmas electrónicas en la Universidad sea el siguiente:

En el caso de firmas electrónicas generadas dentro del entorno de la Universidad se procederá a la generación de las firmas en formatos que permitan garantizar su preservación durante la fase de tramitación del procedimiento administrativo. En consecuencia, para los documentos en formato XML, las firmas se transformarán al formato XAdES-LTA-Level y para los documentos PDF, en formato PAdES-LTA-Level.

Cuando las firmas electrónicas provengan de plataformas externas se procederá a completarlas en un momento posterior al cierre y foliación del expediente administrativo. En consecuencia, para los documentos en formato XML, las firmas se transformarán al formato XAdES-LTA-Level y para los documentos PDF, en formato PAdES-LTA-Level.

Cuando por cualquier motivo no sea posible generar firmas electrónicas con garantías de preservación, se procederá, lo más brevemente posible, a generar una copia electrónica auténtica del documento original. Tal proceso resultará en la aplicación de una firma en formato que garantice la preservación de la copia electrónica auténtica, que substituirá al documento original.

En caso de que no pueda generarse una copia autentica o que las firmas ya estén caducadas, se recomienda generar un informe de validación (construido de forma automática) que incorpore el resumen criptográfico del documento, la identificación de la firma y los

elementos de verificación de vigencia del certificado. Este informe firmado con sello electrónico de la Universidad y sello de tiempo se conservará juntamente con el documento firmado y será objeto de preservación a largo plazo.

En lo que se refiere a las firmas electrónicas basadas en la identidad más la voluntad de firma, se generará la firma mediante la aplicación del sello electrónico en un formato que garantice la preservación, preferentemente PAdES-LTA-Level

En referencia a las firmas biométricas, se generará firma electrónica mediante la aplicación de un sello electrónico en formato que garantice su preservación (PAdES-LTA-Level).

12.1.2 Selección de formatos de conservación

Las actuaciones que permiten la preservación del formato del documento, sus elementos de seguridad, firmas electrónicas y sellos de tiempo son necesarias para garantizar la inteligibilidad e integridad de los documentos electrónicos a largo plazo.

De acuerdo con el párrafo anterior, el sistema de preservación de documentos electrónicos debe realizar controles periódicos sobre estos mismos para garantizar su accesibilidad, la posibilidad de recuperarlos y su validez jurídica, que comprobarán:

La accesibilidad de sus soportes.

La capacidad de lectura de sus formatos.

La validez jurídica de las firmas electrónicas.

La integridad de los documentos.

La integridad de los expedientes.

En el caso en que los documentos provengan de una fuente externa a la Universidad, se propone su conversión al formato PDF/A, que actualmente es el formato más usado para la preservación de documentos electrónicos. El formato PDF también se aceptará siempre que provenga de aplicaciones corporativas existentes que generen documentos en tal formato.

Con la finalidad de garantizar la validez de la firma electrónica, se recomienda que se aplique el criterio establecido previamente que consiste en completar las firmas existentes en formatos que permitan garantizar su preservación a lo largo del tiempo, concretándose estos en:

XAdES-LTA-Level para los documentos en formato XML con firmas XAdES.

PAdES-LTA-Level para los documentos en formato PDF o PDF/A.

Partiendo de estas firmas y en el momento en que el sello electrónico caduque, se recomienda que se proceda al resellado de las firmas electrónicas mediante la aplicación de un nuevo sello, con una caducidad suficiente y con los algoritmos o claves de firma actualizados.

El formato aplicado al foliado del expediente deberá ser XML, puesto que es el formato que permite una mejor actuación administrativa automatizada garantizando la integridad del expediente.

13. Mantenimiento de la política

13.1 Despliegue de la política

La actualización de la presente política requerirá que se lleve a cabo la adecuación de las diversas aplicaciones, herramientas informáticas y procesos que se usen en la Universidad. En ese caso, el área competente en Transformación Digital coordinará la actualización de todos los sistemas afectados para adecuarlos a lo que dispone la presente Política en un plazo que requieran las distintas actuaciones necesarias y previa identificación y elaboración del calendario de aplicación.

Los servicios y sistemas que se pongan en funcionamiento con posterioridad a la entrada en vigor de la Política de identidad y firma electrónica de la UPV/EHU estarán sujetos a esta desde el momento en que empiecen a operar.

El Órgano competente en Transformación Digital y Comunicación deberá examinar, con una periodicidad bianual, con la finalidad de comprobar el estado de cumplimiento de la política, su adecuación a las necesidades reales de la comunidad universitaria y su alineamiento con las tecnologías disponibles, informando de ello a la Secretaría General.

13.2 Situaciones transitorias

Los métodos de identificación y firma contemplados en la presente política se empezarán a usar de forma progresiva, conforme a que la Universidad disponga de las aplicaciones, herramientas y procesos necesarios para su uso.

Se actualizarán los sistemas afectados en el plazo que se prevea en el calendario definido en el punto 13.1 a partir de la aprobación de esta Política con la finalidad de adecuarlos a sus disposiciones.

13.3 Derogación de estándares obsoletos

La aprobación de la Política de identidad y firma electrónica supone la derogación de los estándares técnicos y otros documentos de desarrollo que las contradigan.

13.4 Entrada en vigor

La presente política entrará en vigor a los veinte días de su publicación en el Boletín Oficial del País Vasco.

Anexo I. Glosario y conceptos de firma electrónica

I.1. Glosario

Se ha considerado importante la incorporación de un anexo de definición de conceptos aplicados en este documento, con la finalidad de hacerlo más comprensible.

Casos de uso de la firma electrónica. Hace referencia a los casos de uso de la firma electrónica, entendidos como los posibles escenarios de generación de documentos electrónicos firmados. Por cada caso de uso se identifican los formatos de firma electrónica aplicables, los posibles niveles de firma, etc.

Clases de firma electrónica. Este documento se refiere a las clases de firma electrónica y a su validez jurídica. Según se define en el Reglamento eIDAS, se clasifican en firma simple, avanzada y cualificada.

Formato de firma electrónica. La forma en la que se codifican las firmas electrónicas, siendo sus formatos más comunes: S / MIME, CMS, XAdES, CAdES y PAdES.

Nivel de firma. Hace referencia a si el documento dispone de una o múltiples firmas y que si en ese caso se generan de forma paralela o secuencial.

Sellado de tiempo. Consiste en una acreditación de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos a cargo de un tercero de confianza.

Sistema de firma. Se refiere a la forma de firma de un documento electrónico, sea mediante un certificado digital de la persona firmante, por medio de un sistema de identificación más evidencia electrónica del acto de firma, firma biométrica o mediante un Código Seguro de Verificación (CSV).

Tipo de firma. Indica la forma de relación de la firma electrónica con el documento firmado, dentro del mismo documento, como un documento aparte, dentro de estructuras XML, etc.

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

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.

Creador de un sello. Persona jurídica que crea un sello electrónico.

Verificador. Entidad, sea persona física o jurídica, 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 en el 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.

Prestador de servicios de firma electrónica. Una persona física o jurídica, que expide certificados electrónicos o presta otros servicios relacionados con la firma electrónica.

Emisor y gestor de la Política de identidad y firma electrónica. Órgano o unidad que se encarga de generar y gestionar el documento de la política, que rige las actuaciones del firmante, el verificador y el prestador de servicios, en los procesos de generación y validación de firma electrónica.

Este documento usa el concepto "firmante" para referirse tanto a la persona que firma como al creador de un sello. En este último caso, se puede tratar de un proceso de actuación administrativa automatizada.

I.2. Conceptos de firma electrónica

Definición jurídica de firma electrónica

Desde una perspectiva jurídica, las diferentes clases de firma se definen como:

Firma electrónica simple: Conjunto de datos en forma electrónica, consignados juntamente con otros o que están asociados, que pueden ser usados como medio de identificación de la persona firmante. Se entiende identificación como autenticación de entidades.

Firma electrónica avanzada: Conjunto de datos en forma electrónica que permiten identificar al firmante y detectar cualquier cambio posterior de los datos que se hayan firmado, vinculada al firmante de forma única y a los datos a los que hace referencia, creada por medios que el firmante puede mantener bajo su control exclusivo.

Firma electrónica cualificada: Firma electrónica avanzada basada en un certificado cualificado y que ha sido generada mediante un dispositivo seguro de creación de firmas.

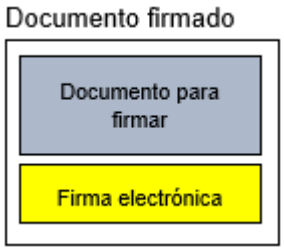
El concepto de certificado cualificado al que se hace referencia en las definiciones del presente apartado se refiere a aquellos certificados electrónicos emitidos por un prestador cualificado de servicios de confianza, y que cumple los requisitos establecidos en lo referente a la comprobación de la identidad y el resto de las circunstancias de los solicitantes y a la fiabilidad y garantías de los servicios de certificación que prestan.

Fundamentos técnicos de la firma electrónica

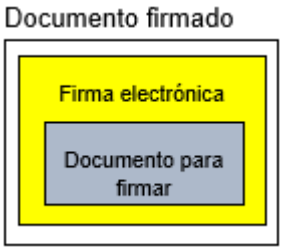
Desde un punto de vista técnico, los **tipos de firma** se definen como:

Firma attached: los datos de la firma electrónica residen en el documento firmado. Por lo tanto, el mismo documento dispone de toda la información necesaria para comprobar la autenticidad e integridad de este, así como la información necesaria para validar la firma. Existen dos tipos diferentes de firma attached:

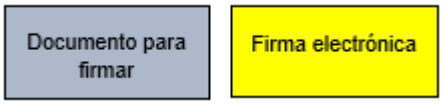
- **Enveloped (incrustada)**: el documento electrónico dispone del contenido y de la firma de este.



- **Enveloping (envolvente)**: el documento electrónico firmado es la firma del documento electrónico a firmar, dentro del cual está el mismo documento a firmar.



Firma detached: los datos de la firma electrónica 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 es necesario crear un documento de evidencias electrónicas que contenga conjuntamente el documento y los datos completos de la firma.



En relación con el **nivel de firma**:

Firma simple: el documento contiene una única firma.

Firma múltiple: el documento contiene dos o más firmas. La firma múltiple consiste en que varios firmantes firmen el documento de forma consecutiva. Este tipo de firma se puede aplicar sobre el documento original cada vez (firma paralela) o sobre el documento firmado (firma secuencial).

> La firma múltiple se usará en diversas actuaciones en el marco de los procedimientos de la Universidad, como, por ejemplo, en la firma de documentos electrónicos por más de una persona o el resellado de documentos ya firmados para actualizar su validez legal a lo largo del tiempo, antes que la validez criptográfica de la firma electrónica pueda quedar en entredicho.

Anexo II. Certificados electrónicos para uso por parte de la Universidad y su personal

Relación de Certificados electrónicos para uso por parte de la Universidad y su personal en el desempeño efectivo de su puesto de trabajo para los trámites y actuaciones que realice por razón de su condición de personal empleado de la Universidad

Certificado de Profesional:

- **Certificado cualificado de firma electrónica de Profesional** emitido por el prestador cualificado de servicios electrónicos de confianza de la Universidad, a toda persona empleada de la Universidad, para su uso en todas las tareas de autenticación y firma que requiera su puesto de trabajo. Dispone de información referente al titular y a su vinculación como persona empleada de la Universidad. Se solicitan siguiendo el procedimiento establecido en el apartado 8.4 de la presente política.
- La Universidad del País Vasco / Euskal Herriko Unibertsitatea es entidad de registro de su prestador cualificado de servicios electrónicos de confianza y las operaciones de identificación de la persona, verificación de la documentación y emisión del Certificado Profesional, se realiza en las oficinas que la propia Universidad ha designado a tal efecto.

Certificado de representante:

- **Certificado cualificado de firma electrónica de Representante de entidad** emitido por el prestador cualificado de servicios electrónicos de confianza de la Universidad. Corresponde al certificado electrónico de representante de persona jurídica que consiste en un certificado personal de identificación y de firma reconocida o cualificada, que dispone de la información referente al titular y a su representación de la Universidad. Se solicitan siguiendo el procedimiento establecido en el apartado 8.4 de la presente política.
- El Órgano competente en Transformación Digital y Comunicación de la UPV/EHU centralizará la solicitud, dado que su obtención está condicionada a la acreditación del nombramiento de la persona titular del certificado como representante de la institución. Tal acreditación deberá constar documentalmente en una publicación en el boletín oficial, inscripción en un registro público o documento notarial, de acuerdo con lo que establece el artículo 7 de la Ley 6/2020.

Certificados técnicos:

- **Certificado de sello electrónico para actuaciones administrativas automatizadas,** emitido por el prestador cualificado de servicios electrónicos de confianza de la Universidad. Corresponden a los certificados digitales que sirven para autorizar la actuación administrativa automatizada en los términos descritos en el artículo 42 de la Ley 40/2015. Este certificado se utiliza para llevar a cabo copias

electrónicas, foliados de expedientes y para la emisión de certificados que no requieren la intervención de un empleado público.

  - La Universidad dispone de un único certificado de sello electrónico para todos los usos y cabe la posibilidad de especializarlos en función de las competencias de cada uno de los órganos que lo custodien.

- **Certificado de aplicación,** emitido por el prestador cualificado de servicios electrónicos de confianza de la Universidad. Corresponde a los certificados digitales que sirven para la identificación de aplicaciones y servidores. Estos certificados podrán usarse para el intercambio de datos entre administraciones, entre administraciones y la ciudadanía y entre administraciones y empresas, la identificación y autenticación de un sistema o servicio web, entre otros.
- **Certificado de servidor o de sede electrónica,** emitido por el prestador cualificado de servicios electrónicos de confianza de la Universidad. Corresponden a los certificados digitales que se usan para garantizar el acceso seguro a los entornos de tramitación telemática con la Universidad como la página web corporativa o, en su caso, la sede electrónica.
- Al igual que los certificados de aplicación, pese a que este tipo de certificados no generan actos jurídicos, se ha considerado oportuno mencionarlos en esta política con la finalidad de regular su uso y la responsabilidad de la custodia.

La presente lista podrá actualizarse por el Órgano competente en Transformación Digital y Comunicación de la Universidad a propuesta de la persona responsable de seguridad de la información de la Vicegerencia de Tecnologías de la Información y las Comunicaciones, en función de las posibles modificaciones en la tecnología o en las prácticas de certificación de las autoridades, siempre que los certificados que se usen sean certificados cualificados emitidos por autoridades de la lista de prestadores de servicios electrónicos de confianza (TSL) que mantiene el Ministerio competente.

Anexo III. Estándares internacionales y otras convenciones

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, v1.7.4 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): Formato del fichero / 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".

Anexo IV. Comprobaciones para tener en cuenta en la validación de firmas de terceros

Hay que seguir los siguientes pasos para verificar las firmas de terceros y su correcto cumplimiento:

IV.1. Verificación de la fecha de firma

La fecha de firma de un documento electrónico es relevante para gestionar la validez del certificado de la persona firmante.

Es posible que el documento electrónico tenga una fecha de firma en su contenido pero que esta no coincida con la fecha de la firma electrónica. En consecuencia, se deberá verificar que la fecha en la que se ha firmado el documento y diferenciar si la fecha de firma se ha establecido mediante un sello de tiempo o usando el reloj del dispositivo de la persona firmante.

Pese a que exista la posibilidad de realizar tales comprobaciones de forma automática mediante la aplicación de captura del documento, se recomienda realizar comprobaciones manuales para garantizar la fiabilidad de las comprobaciones.

IV.2. Identificación de la titularidad y la cadena de confianza

La generación de una firma electrónica requiere el uso de un certificado electrónico reconocido, que deberá ser necesariamente emitido por parte de una entidad prestadora de servicios electrónicos de confianza cualificados. Este hecho permite acreditar que la firma electrónica usada es segura y garantizar la identidad de la persona firmante.

Si la verificación del emisor del certificado falla, la Universidad no depositará su confianza en la firma del documento electrónico y este será devuelto al firmante para que sea firmado por un emisor de confianza.

IV.3. Identidad del titular del certificado

Teniendo en cuenta que un certificado electrónico proporciona información para identificar a la persona física o jurídica que se compromete con el contenido del documento, verificar su identidad mediante las referencias que se puedan extraer del certificado es muy importante para poder establecer que un documento ha estado firmado por la persona que debe.

En el caso de firma mediante representación deberá constar información del representante y de la persona representada en el campo correspondiente.

Si el titular del certificado coincide con la persona que consta como firmante del documento se pude dar la verificación por buena, mientras que en el caso en que el titular del certificado no coincida con la identidad de la persona que debería firmar el documento, se deberá rechazar el documento por no poder admitirse su firma.

IV.4. Validación de las facultades del firmante

Es posible que algunas veces se firme en nombre de un tercero. En ese caso, la Universidad deberá comprobar que el firmante está capacitado para ejercer la representación alegada, en el caso en que esas facultades no consten en el propio certificado. En algunos casos puede resultar adecuado requerir la presentación de documentación adicional que permita acreditar la representación u optar por la opción de verificar su identidad mediante el acceso a registros externos.

Cuando no sea posible verificar la suficiencia de poderes de representación de la persona firmante, se deberá retornar el documento a su emisor.

IV.5. Verificación de la vigencia del certificado

Los certificados electrónicos podrán caducar de acuerdo con la fecha fijada en el momento de su emisión, o incluso ser suspendidos o revocados antes de tal fecha por varios motivos, como, por ejemplo, la pérdida de vigencia de los datos de los certificados o la pérdida de la tarjeta criptográfica.

Teniendo en cuenta lo expuesto en el párrafo anterior, la Universidad deberá comprobar la validez de las firmas emitidas de acuerdo con los datos aportados por el certificado o la autoridad de certificación siguiendo los siguientes procedimientos:

Verificación de las listas de revocación de certificados (CRLs), implementada automáticamente por la mayoría de las aplicaciones que permiten la visualización de los documentos firmados del mercado, pese a que no generen pruebas concretas.

Solicitud de un informe de verificación (OCSP), por parte del prestador de servicio de certificación, pero que se deberá solicitar mediante un sistema informático de la Universidad.

Validación mediante una plataforma centralizada como @firma de la Administración General del Estado.

Es posible que el certificado caduque después de la firma de un documento, por ese mismo motivo es importante que la Universidad sea capaz de acreditar que el certificado era vigente en la fecha de verificación mediante la aplicación de un sello de tiempo emitido por una autoridad (TSA).

IV.6. Verificación de la vinculación criptográfica del documento con la firma

Esta verificación se lleva a cabo para validar que la firma electrónica hace referencia al documento que se alega haber firmado, ya que es posible que el documento pueda haber sufrido modificaciones posteriores al momento de su firma. Por lo tanto, es posible que la vinculación entre el documento electrónico y su firma no corresponda.

Se podrá realizar tal verificación mediante el uso de aplicaciones ofimáticas que permitan la visualización de documentos en formato PDF, mientras que, en los procesos de incorporación

del documento al sistema, se podrá llevar a cabo tal verificación mediante la aplicación que lleve a cabo tal incorporación.

Cuando tal proceso de verificación falle se considerará que la firma es defectuosa y se procederá a la devolución del documento electrónico a su emisor informando del motivo de rechazo.

IV.7. Verificación del contenido del documento

La verificación del contenido de un documento electrónico es tan esencial como la de un documento en papel, aunque en el caso del documento electrónico las comprobaciones se centrarán en el análisis sobre la adecuación del contenido y si se ajusta a los requisitos necesarios para gozar de validez jurídica.

En el caso en que el documento se haya producido en origen por la propia Universidad se recomienda hacerlo firmar al tercero previa firma mediante un sello electrónico de la Universidad, a fin de automatizar la verificación del retorno.

Si no se puede verificar de forma automática, se deberá revisar el documento para garantizar que no se ha producido ningún cambio entre la versión mandada al firmante y la versión que se devuelve firmada.

Si la verificación falla, se procederá a la devolución del documento firmado por el tercero.

Anexo V. Casos de uso de los sistemas de firma electrónica

A continuación, se presentan diversos casos de uso de los sistemas de firma electrónica que pueden darse en la Universidad, caracterizándolos jurídicamente, recomendando el uso de uno u otro en función del caso analizado y determinando sus requisitos de seguridad.

V.1. Firma electrónica de un documento interno

Este caso de uso hace referencia a los documentos producidos internamente por la Universidad, firmados por una persona empleada en el ejercicio de sus funciones o por parte de terceros que participen o colaboren puntualmente con la UPV/EHU, que tengan como destinataria a otra persona usuaria interna o el cumplimiento de un paso en el procedimiento. En ningún caso aplica a documentos que vayan a surtir efectos jurídicos ante terceros.

En este caso se permitirá aplicar la firma electrónica en documentos electrónicos en cualquier momento de su ciclo de vida.

Sus principales características son:

- La firma electrónica se realiza sobre un documento original en soporte electrónico.
- El documento original y las firmas deben incorporarse al sistema de firma.
- La firma electrónica deberá ser validada mediante un servicio o autoridad de validación con la finalidad de asegurar su integridad y autenticidad.

Siempre que sea necesaria la preservación del documento electrónico a lo largo del tiempo, este deberá estar en cualquiera de los formatos admitidos por la Universidad, preferiblemente en PDF/A y XML.

En relación con los tipos de firma aplicables a este caso, se establecen los siguientes requisitos:

Sistemas de firma	• Certificado cualificado electrónico personal, de acuerdo con lo descrito en el apartado 10.1 • Certificado no cualificado electrónico personal de acuerdo con lo descrito en el apartado 10.1 • Claves concertadas con complemento de segundo factor de autenticación, de acuerdo con lo descrito en el apartado 10.4, que solo será admisible para firmar documentos electrónicos en relación con el presente caso cuando la persona firmante sea extranjera no residente que participe en un procedimiento interno de la Universidad de forma puntual y que no disponga de otros mecanismos de identificación.

Tipos de certificado	**Las personas empleadas de la Universidad** • Certificado Profesional. • Certificado de Representante. **Terceros que participen** • Certificado de persona física.
Formatos aceptados	• PAdES-T -Level • XAdES-T-Level
Nivel de firma	Simple, múltiple (secuencial o paralela).
Tipo de firma	***Attached*** (adjunta) o ***Detached*** (separada) según el caso.
Aplicación de sello de tiempo	

V.2. Firma electrónica de un documento con valor para terceros

Este caso de uso se refiere a documentos producidos internamente en la Universidad que tienen que estar firmados por una persona empleada en el ejercicio de sus funciones, o por terceros que colaboren puntualmente con la UPV/EHU que generan derechos y/u obligaciones a terceros.

Se permitirá aplicar la firma electrónica en documentos electrónicos en cualquier momento de su ciclo de vida.

Sus principales características son:

- La firma electrónica se realiza sobre un documento original en soporte electrónico.
- El documento original y las firmas deben incorporarse al sistema de firma.
- La firma electrónica deberá ser validada mediante un servicio o autoridad de validación con la finalidad de asegurar su integridad y autenticidad.
- El documento electrónico deberá estar en cualquiera de los formatos admitidos por la universidad, preferiblemente en PDF/A y XML, con el objetivo de garantizar su preservación a lo largo del tiempo.
- Se expedirá una copia auténtica del documento electrónico, y se añadirá un código seguro de verificación, cuando quede garantizada la integridad del documento, su custodia y consulta en el archivo. Esta será la copia que se facilitará a terceros.

En relación con los tipos de firma aplicables a este caso, se establecen los siguientes requisitos:

Sistemas de firma	• Certificado cualificado electrónico personal, de acuerdo con lo descrito en el apartado 10.1
Tipos de certificado	**Las personas empleadas de la Universidad** • Certificado Profesional. • Certificado de Representante. **Terceros que participen** • Certificado de persona física.
Formatos aceptados	• PAdES-T-Level • XAdES-T-Level
Nivel de firma	Simple, múltiple (secuencial o paralela).
Tipo de firma	*Attached* (adjunta) o *Detached* (separada) según el caso.
Aplicación de sello de tiempo	

V.3. Firma electrónica de documentos por parte de terceros

Este caso de uso hace referencia a aquellos documentos electrónicos producidos por la Universidad o terceros que son firmados por estos últimos en un entorno controlado por la UPV/EHU. En el caso en que este tipo de documentos electrónicos se firmen en entornos fuera del control de la Universidad habrá que atenerse al caso de uso presentado en el apartado V.8

Concretamente, este caso aplica en la firma de documentos en el momento de su presentación ante un registro electrónico, o en aquellas situaciones en que el tercero ha de firmar documentos electrónicos en momentos posteriores en su participación en un procedimiento administrativo de la Universidad.

Sus principales características son:

- La firma electrónica se realiza sobre un documento original en soporte electrónico.
- El documento original y las firmas deben incorporarse al sistema de firma.
- La firma electrónica deberá ser validada mediante un servicio o autoridad de validación con la finalidad de asegurar su integridad y autenticidad.

– Siempre que sea necesaria la preservación del documento electrónico a lo largo del tiempo, este deberá estar en cualquiera de los formatos admitidos por la universidad, preferiblemente en PDF/A y XML.

En relación con los tipos de firma aplicables a este caso, se establecen los siguientes requisitos:

Sistemas de firma	• Certificado cualificado electrónico personal, de acuerdo con lo descrito en el apartado 10.1 • Certificado no cualificado electrónico personal de acuerdo con lo descrito en el apartado 10.1 • Firma basada en claves concertadas, de acuerdo con lo descrito en el apartado 10.3 • Firma basada en claves concertadas con complemento de segundo factor de autenticación, de acuerdo con lo descrito en el apartado 10.4 • Firma electrónica biométrica, de acuerdo con lo descrito en el apartado 10.5
Tipos de certificado	**Las personas empleadas de la Universidad** • Certificado Profesional. • Certificado de representante. **Terceros que participen** • Certificado de persona física. Para el resto de los mecanismos de firma, se deberá aplicar certificado de sello electrónico.
Formatos aceptados	• PAdES-T-Level • XAdES-T-Level
Nivel de firma	Simple.
Tipo de firma	*Attached* (adjunta) o *detached* (separada) según el caso.
Aplicación de sello de tiempo	

V.4. Firma electrónica de contratos, convenios o acuerdos con otras partes

Este caso de uso aplica a los documentos de carácter contractual multilaterales en los que participa la Universidad de forma conjunta con una o más partes, que se firmarán en entornos controlados por la UPV/EHU. En el caso en que este tipo de documentos electrónicos se firmen en entornos fuera del control de la Universidad habrá que atenerse al caso de uso presentado en el apartado V.8

Sus principales características son:

- La firma electrónica se realiza sobre un documento original en soporte electrónico.
- El documento original y las firmas deben incorporarse al sistema de firma.
- La firma electrónica deberá ser validada mediante un servicio o autoridad de validación con la finalidad de asegurar su integridad y autenticidad.
- El documento electrónico deberá estar en cualquiera de los formatos admitidos por la universidad, preferiblemente en PDF/A y XML, con el objetivo de garantizar su preservación a lo largo del tiempo.
- El documento electrónico se podrá firmar más de una vez, por parte de diversas personas usuarias y de forma paralela o secuencial.

En relación con los tipos de firma aplicables a este caso, se establecen los siguientes requisitos:

Sistemas de firma	• Certificado cualificado electrónico personal, de acuerdo con lo descrito en el apartado 10.1 • Certificado no cualificado electrónico personal de acuerdo con lo descrito en el apartado 10.1 • Firma basada en claves concertadas, de acuerdo con lo descrito en el apartado 10.3 • Firma basada en claves concertadas con complemento de segundo factor de autenticación, de acuerdo con lo descrito en el apartado 10.4
Tipos de certificado	**Las personas empleadas de la Universidad** • Certificado Profesional • Certificado de Representante **Terceros que participen** • Certificado de persona física.

Formatos aceptados	• PAdES-T-Level • XAdES-T-Level
Nivel de firma	Múltiple (secuencial o en paralelo)
Tipo de firma	*Attached* (adjunta) o *detached* (separada) según el caso.
Aplicación de sello de tiempo	

V.6. Firma electrónica automatizada

Este caso de uso permite la firma de documentos electrónicos de forma automática con plenas garantías jurídicas mediante el uso de certificados de sello electrónico sin la intervención de personas firmantes en el proceso.

Este supuesto está pensado para aquellas tareas en las que se deben firmar documentos de forma automatizada con plenas garantías jurídicas. Para su ejecución se usará un certificado electrónico que firmará los documentos en nombre de la aplicación en cuestión y de la Universidad.

Sus principales características son:

- La firma electrónica se realiza sobre un documento original en soporte electrónico de forma automática.
- El documento electrónico podrá estar en cualquiera de los formatos admitidos por la Universidad (PDF, PDF/A y XML), aunque se preferirá el uso del formato PDF/A para documentos que deban remitirse a las personas interesadas.

Los certificados electrónicos y las claves privadas que permiten generar procesos de firma automatizada se guardarán en un repositorio seguro en los servidores de la Universidad o en un servidor de una tercera entidad prestadora de servicios, siempre que esa cesión esté limitada y controlada. Concretamente, todas las cesiones deberán estar descritas en un contrato o convenio a celebrar entre la Universidad y el tercero, acotadas a usos concretos y sujetas a las potestades de verificación propias de la Universidad.

En relación con los tipos de firma aplicables a este caso, se establecen los siguientes requisitos:

Sistemas de firma	• Certificado cualificado electrónico de sello electrónico, de acuerdo con lo descrito en el apartado 10.2
Tipos de certificado	• Certificado de sello electrónico de la Universidad.

Formatos aceptados	• PAdES-T-Level • XAdES-T-Level
Nivel de firma	Simple.
Tipo de firma	*Attached* (adjunta).
Aplicación de sello de tiempo	

V.7. Firma electrónica para digitalización segura

Este caso de uso consiste en la firma electrónica de un documento digitalizado en formato PDF o PDF/A, con la finalidad de crear una copia auténtica electrónica. Su firma es importante para garantizar la integridad y autenticidad del documento digitalizado.

Firmarán electrónicamente el documento:

El Profesional habilitado que digitalice el documento, en el caso en que se proceda al control manual y cotejo del original.

El sello electrónico del sistema de la Universidad en el caso de actuación administrativa automatizada.

En relación con los tipos de firma aplicables a este caso, se establecen los siguientes requisitos:

Sistemas de firma	• Certificado cualificado electrónico personal (manual), de acuerdo con lo descrito en el apartado 10.1 • Certificado cualificado electrónico de sello electrónico (automatizada), de acuerdo con lo descrito en el apartado 10.2
Tipos de certificado	• Certificado Profesional. • Certificado de sello electrónico.
Formatos aceptados	• PAdES-T-Level
Nivel de firma	Simple.
Tipo de firma	*Attached* (adjunta).
Aplicación de sello de tiempo	

V.8. Incorporación de documentos electrónicos firmados de fuentes externas

En lo referente a las firmas provenientes de plataformas ajenas a la Universidad, se procederá a su validación, y, una vez validadas, se incorporarán al expediente con las correspondientes evidencias de validación.

Se recomienda que la validación de las firmas consista en, sin carácter limitativo, la verificación de la fecha de firma, la identificación de la titularidad y la cadena de confianza, la verificación de la vigencia del certificado, entre otros aspectos.

V.9. Identificación y firma de personas no nacionales ni residentes

Teniendo en cuenta que la Universidad tiene relación con personas físicas o jurídicas extranjeras en lo referente a varios temas como, por ejemplo, la contratación pública o los proyectos internacionales de investigación, se contempla este último caso de uso.

Con carácter general, la UPV/EHU admite todos los certificados electrónicos reconocidos por las autoridades homologadas por el Ministerio correspondiente, de acuerdo con el Reglamento eIDAS. Pese a esto, tal reconocimiento puede estar limitado por las capacidades de las herramientas de parsing (análisis) e interpretación que use la Universidad.

Se establecen las siguientes directrices con relación a la identificación y firma de personas no nacionales ni residentes en el ámbito de la Universidad:

Las personas jurídicas necesitarán un certificado electrónico para relacionarse con la Universidad. Con carácter general se recomendará el uso de certificados electrónicos emitidos por prestadores cualificados de servicios electrónicos de confianza del entorno eIDAS; en caso de usar certificados electrónicos fuera del entorno eIDAS se deberá seguir el procedimiento de verificación que se detalla en el siguiente punto.

Las personas físicas que, en su relación la Universidad, realizan tareas de representación de la institución o propias de un empleado público, deberán obtener un certificado electrónico, que podrá obtenerse por parte de una entidad de certificación de su país. En el caso de ciudadanos residentes en la UE, el reconocimiento será automático en base a los prestadores de servicios de confianza electrónica cualificados reconocidos por el Reglamento eIDAS, mientras que, en el caso de emisores de certificados situados fuera de la UE, será necesario verificar la solvencia de la autoridad de certificación. Si se verifica que el certificado es técnicamente correcto, la autoridad es de confianza y el documento está bien formado, la Universidad podría admitirlo como válido. Para poder admitir tales documentos es imprescindible realizar las siguientes comprobaciones:

- Verificar si el certificado ha sido emitido por una entidad de certificación acreditada en su país y, por lo tanto, cumple con los requisitos exigidos por la legislación del país de origen garantizando la identidad del firmante y la integridad del documento.
- En este caso, por ejemplo, sería recomendable aceptar un documento electrónico presentado por un tercero si el certificado ha sido emitido por una entidad de certificación como puede ser la SOCIEDAD CAMERAL DE CERTIFICACION DIGITAL - CERTICÁMARA S.A., que se encuentra en el directorio de entidades de certificación digital del sitio web del Organismo Nacional de Acreditación de Colombia (ONAC).
- Verificar que el certificado responde a un estándar técnico de criptografía que garantiza un nivel de seguridad homologable al ETSI TS 119 403.

  No obstante, el criterio para determinar si una autoridad cumple con estos dos requisitos no es fácil de automatizar – la validación automática implica que el proveedor de servicios de confianza esté registrado en una lista homologada, que es precisamente lo que crea el Reglamento eIDAS para los proveedores UE, pero no está resuelto a nivel mundial.

  Para poder verificar el cumplimiento de dichos requisitos, la Universidad seguirá el siguiente procedimiento que permitirá admitir el documento presentado con todas las garantías:

  - Crear una lista de prestadores de confianza, propia de la UPV/EHU, en la que ir registrando los prestadores externos a la UE para los cuáles ya se hayan hecho en el pasado las verificaciones que se indican a continuación. De este modo, una vez un prestador ha sido contrastado, no hay que repetir la comprobación.
  - Para comprobar que el proveedor está autorizado en su país podremos utilizar los medios siguientes:
    - Solicitar a la entidad certificadora de la Universidad, la validación y comprobación del prestador de servicios de certificación del certificado
    - Acudir a algún recurso público del gobierno de dicho país donde pueda haber una lista de prestadores de confianza. Así, en el caso de Colombia existe la ONAC.
    - Comprobar si existen convenios bilaterales entre la Unión Europea o España y el país tercero, en los que se establezca el reconocimiento mutuo de tales certificados. Existen, por ejemplo, convenios con Canadá, México o Chile, en los que el tema se aborda, pero no queda resuelto, por lo que actualmente estos Convenios no aportan una solución concreta, pero es de prever que lo hagan en el futuro mediante el reconocimiento mutuo de las listas de confianza.

- Solicitar al tercero que aporta el documento, que obtenga de su proveedor de servicios de certificación la información o documentación necesaria para verificar que el prestador está acreditado en su país.

- Para comprobar la calidad técnica de los certificados, conviene acceder a la página web del prestador de servicios de certificación y consultar la práctica o política de certificación asociada al certificado que se pretende usar. La manera más certera de encontrar esta información es consultar el campo "Certificate Policies" del propio certificado. La política de certificación identificará la norma técnica o el marco de auditoría al que se somete la autoridad de certificación.
- Una vez realizadas las comprobaciones, si el resultado es favorable:
  - La UPV/EHU registrará este proveedor de certificación en su lista interna de confianza, asociando la URL de su servicio de certificación y la documentación que sea utilizado para hacer la verificación.
  - El documento se podrá incorporar al sistema de la UPV/EHU. Conviene tener en cuenta la advertencia que la verificación del documento con herramientas como @firma, Valide o Adobe Acrobat Reader seguirá fallando, porque el proveedor no estará registrado en las listas de confianza correspondientes. Por este motivo, puede ser conveniente asociar al documento una diligencia indicando que se ha verificado la autenticidad del documento y la calidad de la firma.
- Si el resultado es desfavorable, será necesario informar al tercero de que el certificado no consta como un certificado expedido por una entidad de certificación de confianza, y requerirla para que obtenga medios de firma acordes con la legislación de su país.

La Universidad mantendrá la lista de prestadores de confianza no UE que han sido contrastados y dispondrá de un procedimiento interno para la realización de las comprobaciones que se indican en este apartado, a efectos de ampliar dicha lista.

Las personas físicas que no lleven a cabo las tareas descritas en el párrafo anterior pero que deban firmar algún documento electrónico, podrán identificarse alegando sus datos personales, a partir de los cuales se elaborará una identidad mediante la emisión de certificados no cualificados o un sistema de clave concertada, que podrá complementarse con el uso del segundo factor de autenticación. Estos serían sistemas basado en un registro de identidades controlado por la UPV/EHU, que permita la identificación, autenticación y firma de terceros que participan o colaboran puntualmente con la organización.

V.10. Diagramas de caso de uso de los sistemas de firma contemplados en la Universidad

<table>
<tr><th colspan="4">Documentos internos de la Universidad que no producen efectos jurídicos ante terceros</th></tr>
<tr><td rowspan="5">Firmante:</td><td colspan="3">Persona empleada de la Universidad en ejercicio de sus funciones o un tercero que participe o colabore puntualmente con la Universidad</td></tr>
<tr><td>Destinatario:</td><td colspan="2">Otra persona usuaria interna o el cumplimiento de un paso en el procedimiento</td></tr>
<tr><td rowspan="3"></td><td>Clases de firma a aplicar:</td><td>Simple, avanzada o cualificada</td></tr>
<tr><td colspan="2">Instrumento de firma:</td><td>Certificados (ver Lista 1).
Identidad + 2FA (ver Lista 2).</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="5">Firmante:</td><td colspan="3">Persona extranjera no residente que participa en procedimiento interno de la Universidad y que no disponga de certificados</td></tr>
<tr><td>Destinatario:</td><td colspan="2">Otra persona usuaria interna o el simple cumplimiento de un paso más en el procedimiento</td></tr>
<tr><td rowspan="3"></td><td>Clases de firma a aplicar:</td><td>Avanzada</td></tr>
<tr><td colspan="2">Instrumento de firma:</td><td>Certificados (ver Lista 1).
Identidad + 2FA (ver Lista 2)</td></tr>
<tr><td colspan="3"></td></tr>
</table>

Documentos con valor para terceros				
Firmante:	Representante legal de la Universidad			
	Destinatario:	Terceros		
		Clases de firma a aplicar:	Avanzada o cualificada	
			Instrumento de firma:	Certificado de representante
Firmante:	Persona empleada de la Universidad en el ejercicio de sus funciones o terceros que colaboran puntualmente con la UPV/EHU			
	Destinatario:	Terceros		
		Clases de firma a aplicar:	Avanzada o cualificada	
			Instrumento de firma:	Certificados (ver Lista 1).

Documentos firmados por terceros en un entorno controlado por la UPV/EHU				
Firmante:	Personal vinculado a la Universidad y terceros			
	Destinatario:	La Universidad y terceros		
		Clases de firma a aplicar:	Simple, avanzada o cualificada	
			Instrumento de firma:	Certificados (ver Lista 1). Identidad + 2FA (ver Lista 2) Firma electrónica biométrica.

Documentos de carácter contractual, multilaterales y firmados en entornos controlados por la UPV/EHU				
Firmante:	Personal vinculado a la Universidad y terceros			
	Destinatario:	La Universidad y terceros		
		Clases de firma a aplicar:	Simple, Avanzada o cualificada	
			Instrumento de firma:	Certificados (ver Lista 1). Identidad + 2FA (ver Lista 2)

Actuación administrativa automatizada				
Firmante:	Dispositivo que lleva a cabo la actuación			
	Destinatario:	La Universidad y terceros		
		Clases de firma a aplicar:	Avanzada	
			Instrumento de firma:	Certificado de sello electrónico

Digitalización segura de documentos				
Firmante:	Empleado público habilitado			
	Destinatario:	La Universidad o terceros		
		Clases de firma a aplicar:	Avanzada o cualificada	
			Instrumento de firma:	Certificado Profesional
Firmante:	Actuación administrativa automatizada			
	Destinatario:	La Universidad o terceros		
		Clases de firma a aplicar:	Avanzada	
			Instrumento de firma:	Certificado de sello electrónico.

1. **Lista 1 de sistemas de firma electrónica basada en certificados electrónicos admitidos por la UPV/EHU:**

   Persona empleada de la Universidad en el ejercicio de sus funciones

   a. Certificados cualificados electrónicos personales.

      i. Certificado electrónico Profesional.

      ii. Certificado electrónico de representante de la UPV/EHU

   Terceros

   b. Certificados no cualificados electrónicos personales (solo persona física)

   c. Certificados cualificados electrónicos personales.

      i. Certificado electrónico de persona física.

      ii. Certificado electrónico de representante.

   d. Certificados cualificados electrónicos de sello electrónico.

2. **Lista 2 del resto de sistemas de firma electrónica admitidos por la UPV/EHU:**

   a. Claves concertadas más las evidencias de voluntad de firma.

   b. Claves concertadas más las evidencias de voluntad de firma junto a complemento de segundo factor de autenticación (2FA)

   c. Firma electrónica biométrica.