

Política de firma electrónica de la Universitat Oberta de Catalunya

Texto aprobado por el Comité de Dirección Ejecutivo el 5 de mayo de 2014, actuando por delegación del Consejo de Gobierno

Sumario

I. Introducción	3
1.1. Identificación de la política de firma electrónica	3
1.2. Fecha de emisión de la política general de firma electrónica	3
1.3. Identificación del emisor de la política general de firma electrónica	3
1.4. Ámbito de aplicación de la política general de firma electrónica	4
II. Normas generales en relación con la tipología de acto	4
III. Tipología de certificados a emplear	4
IV. Relación entre la firma y el documento firmado	5
V. Formato de la firma	5
VI. Perfil de la firma	6
VII. Procesos en relación con la firma electrónica	6
VIII. Organización y desarrollo de la política general	7

I. Introducción

Este documento contiene las normas de firma electrónica en relación con los documentos de procedimientos académicos y de gestión electrónicos de la Universitat Oberta de Catalunya.

La naturaleza de la UOC, el servicio que presta y la necesidad que tiene de interoperar con otras universidades y la administración universitaria del Gobierno de la Generalitat de Cataluña, exigen que el documento sea conforme con los requisitos de seguridad y proporcionalidad correspondientes a los sistemas electrónicos de apoyo a procedimientos, establecidos por las normas:

- Ley 1/2003, de 19 de febrero, de Universidades de Cataluña.
- Ley orgánica 6/2001, de 21 de diciembre, de universidades.
- Ley 3/1995, de 6 de abril, de reconocimiento de la Universitat Oberta de Catalunya.
- Acuerdo GOB/140/2010, de 3 de agosto, por el cual se aprueban las Normas de organización y funcionamiento de la Universitat Oberta de Catalunya.
- Ley 11/2007, de 11 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (LAECSP).
- Ley 26/2010, de 3 de agosto, de régimen jurídico y procedimiento de las administraciones públicas de Cataluña (LRPJCAT).
- Ley 29/2010, de 3 de agosto, de uso de los medios electrónicos en el sector público de Cataluña (LUMESPC).
- Real decreto 3/2010, de 8 de enero, por el que se regula el Esquema nacional de seguridad en el ámbito de la Administración electrónica.
- 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 legislativo 3/2011, de 14 de noviembre, por el cual se aprueba el texto refundido de la Ley de contratos del sector público.
- Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el sector público.

Así, pues, el documento debe entenderse como una política de firma electrónica de acuerdo con el artículo 18.2 del Real decreto 4/2010, de 8 de enero, por el cual se regula el Esquema nacional de interoperabilidad en el ámbito de la Administración electrónica, y que se ha producido de acuerdo con los requisitos de la Norma técnica de interoperabilidad “política de firma electrónica y de certificados de la Administración”.

Los contenidos de esta política general de firma electrónica se han estructurado para cubrir los controles que prevé la norma internacional ISO/IEC 27002:2006 – Tecnología de la información: Técnicas de seguridad: Código de prácticas para la gestión de la seguridad de la información, en especial la sección 15.1.3 Contenidos generales de la política general de firma electrónica.

1.1. Identificación de la política de firma electrónica

Esta política general de firma electrónica se identificará con un identificador de objeto (OID) número: 1.3.6.1.4.1.43653.1.5.

1.2. Fecha de emisión de la política general de firma electrónica

Esta política general de firma electrónica se ha emitido en fecha 28 de abril de 2014, momento a partir del cual entrará en vigor.

1.3. Identificación del emisor de la política general de firma electrónica

Esta política general de firma electrónica se ha emitido por el Comité de Dirección Ejecutivo, actuando por delegación del Consejo de Gobierno de acuerdo con lo establecido en el artículo 13.2 de las NOF (Acuerdo GOB 140/2010, de 3 de agosto), el artículo 4 del Reglamento del Consejo de Gobierno y el Acuerdo de Consejo de Gobierno de 15/07/13.

1.4. Ámbito de aplicación de la política general de firma electrónica

Esta política general resulta aplicable a todos los sistemas de información de apoyo a procedimientos y actividades académicos y de gestión electrónicos, así como a las relaciones por medios electrónicos con terceros ajenos a la comunidad universitaria.

También resulta aplicable a la firma de manifestaciones de documentos y expedientes al intercambiarlos con entidades distintas a esta Universidad, en particular de acuerdo con lo establecido por el Real decreto 4/2010, Esquema nacional de interoperabilidad.

II. Normas generales en relación con la tipología de acto

La Universitat Oberta de Catalunya debe establecer estándares para la firma de los diferentes tipos de actos jurídicos documentados.

Los actos realizados por los órganos deben documentarse, bien en un documento ofimático o libro-registro electrónico de forma autenticada preferentemente con firma electrónica avanzada basada en certificado reconocido de persona física (en caso de actuación manual) o de persona jurídica (en caso de actuación automatizada), por tratarse, en general, de activos cuya categoría de seguridad en las dimensiones de integridad y autenticidad es de nivel medio.

Los actos que se consideren de nivel alto deben autenticarse necesariamente utilizando sistemas de firma electrónica reconocida (en caso de actuación manual) o de persona jurídica (en caso de actuación automatizada); en ambos casos preferentemente mediante dispositivos certificados.

En ningún caso podrá utilizarse exclusivamente un código seguro de verificación para la generación de documentos originales.

El resto de actos pueden documentarse con cualquier sistema de firma electrónica y, en concreto, generar entradas en registros electrónicos de actividad siempre que la persona se haya autenticado con certificado electrónico reconocido, o con un mecanismo que proporcione garantía equivalente.

En particular, por los actos en los respectivos procesos académicos y de gestión de los estudiantes, profesorado y del personal docente colaborador como el de firma de actas, entrega de información, etcétera, podrán realizarse estos con los sistemas de autenticación basados en firma y contraseña proporcionados por la Universitat Oberta de Catalunya una vez valorada la conveniencia y analizados los riesgos.

Los actos de intercambio de datos con las administraciones públicas, o el acceso a los datos de estas, exigirá el nivel mínimo establecido por cada Administración que cede datos o da acceso a datos.

La firma electrónica de los actos de contratación pública y de facturación electrónicos será la que determine la normativa que le sea aplicable.

En todos los casos, deben emplearse algoritmos aprobados en la política de seguridad criptográfica.

III. Tipología de certificados a emplear

En el caso de firma basada en certificados, los certificados a emplear tienen que ser, en general, los siguientes:

– Actuación de la Universitat Oberta de Catalunya calificada como nivel alto:

Actuación manual: Todos los certificados de persona física admitidos para este uso de acuerdo con la política general de certificación de la Universitat Oberta de Catalunya, de nivel 4.

Actuación automática: Todos los certificados de persona jurídica admitidos para este uso de acuerdo con la política general de certificación de la Universitat Oberta de Catalunya, de nivel 4.

– Resto de actuaciones de la Universitat Oberta de Catalunya:

Actuación manual: Todos los certificados de persona física admitidos para este uso de acuerdo con la política general de certificación de la Universitat Oberta de Catalunya, de nivel 3 o superior.

Actuación automática: Todos los certificados de persona jurídica admitidos para este uso de acuerdo con la política general de certificación de la Universitat Oberta de Catalunya, de nivel 3 o superior.

– Actuación de la Universitat Oberta de Catalunya en la expedición de facturas:

Alternativamente puede establecerse un servicio de sello de entidad de acuerdo con lo que dispone la Ley 25/2013.

– Actuación de intercambio de datos o acceso a datos con las administraciones:

Los certificados admitidos por cada Administración que cede o da acceso a datos a la Universitat Oberta de Catalunya.

– Actuación de los estudiantes y de los ciudadanos:

El certificado de firma electrónica incorporado al DNI electrónico.

Todos los certificados admitidos para este uso de acuerdo con la política general de certificación de la Universitat Oberta de Catalunya, de nivel 3 o superior.

IV. Relación entre la firma y el documento firmado

Siempre que sea posible, el formato de la firma debe ser independiente del formato del documento o registro firmado, con el objetivo de reducir al máximo la dependencia entre los dos objetos de negocio.

Los documentos originales que vayan a permanecer en poder de la Universidad (por ejemplo, resoluciones, actas, informes) deben producirse con firma independiente del documento, evitando el uso de firmas envueltas en formatos documentales. La relación entre el documento firmado y la firma se establecerá mediante el uso de metadatos del documento.

Cuando los documentos deban entregarse a terceros, se creará una copia auténtica electrónica, en un formato adecuado al destinatario. Dicha copia se firmará o sellará por medio electrónico y la firma o sello se envolverán en el formato documental.

Como excepción, los documentos originales dirigidos al ciudadano (estudiante, proveedor...), por ejemplo una certificación o una notificación, deben contener la firma envuelta en el propio formato documental (ejemplo: un fichero PDF firmado o sellado). Es recomendable que, adicionalmente, los documentos incorporen un código de verificación electrónica, que permita consultarlos en línea e imprimirlos como copias auténticas.

En relación con los actos de intercambio de datos o acceso a datos entre administraciones, la relación entre la firma electrónica y el documento firmado será típicamente establecida por cada Administración que cede datos o da acceso a datos, sin perjuicio de que dichas condiciones se establezcan por convenio.

Con respecto a los documentos ofimáticos, firmados o no, que presenten los ciudadanos adjuntos a la solicitud administrativa, no se les puede aplicar la política de firma electrónica propia de la Universitat Oberta de Catalunya, puesto que son documentos previos, que no se han creado específicamente por el ciudadano (estudiante, proveedor...) para su relación jurídica con la Universidad.

En cualquier caso, deben aceptarse –y poderse validar– las firmas de los documentos ofimáticos que se determinen en el Esquema nacional de interoperabilidad y en el Esquema nacional de seguridad.

Es recomendable proteger estos documentos, en todo caso, con la firma electrónica de la solicitud (ejemplo: mediante la inclusión de los resúmenes criptográficos de los documentos en campos ocultos del formulario que vaya a firmarse). Así, siempre existe una prueba de los documentos que se entregaron a la Universitat Oberta de Catalunya, con independencia de la validez de la firma de los documentos, o incluso de que estén firmados o no.

V. Formato de la firma

En general, el formato de la firma depende del formato del documento que vaya a firmarse (por ejemplo, PDF exige firmar de acuerdo con CMS, ODF exige firmar de acuerdo con una variante de XML Digital Signature).

La Universitat Oberta de Catalunya utiliza de forma indistinta los formatos de firma XAdES, CAdES, o PAdES, en función de la sintaxis correspondiente a los datos que vayan a firmarse, siempre y cuando el formato del documento o el protocolo correspondiente permitan utilizarlos.

Las normas concretas en relación con la firma electrónica de cada formato documental deben establecerse en los estándares técnicos de firma electrónica de formato documental correspondientes.

VI. Perfil de la firma

Las firmas de los documentos con relevancia externa deben ser suficientemente completas para que los ciudadanos las puedan validar sin medios que les resulten especialmente gravosos o que sean particularmente sofisticados.

La Universidad debe producir firmas electrónicas de clase EPES explícito, donde el OID de la política de firma coincida con el estándar técnico de firma electrónica de acto jurídico aplicable, siempre que ello sea técnicamente posible.

En general se requiere el uso del perfil AdES-T- LT de acuerdo con ETSI TS 103 171 (XAdES Baseline Profile), TS 103 173 (CAAdES Baseline Profile), o ETSI TS 103 172 (PAAdES Baseline Profile), para toda firma electrónica de un documento entregado, y es recomendable utilizar este perfil para todos los documentos de la Universidad.

Las firmas del resto de actos pueden ser más básicas, puesto que la Universitat Oberta de Catalunya puede establecer controles adicionales que eviten la necesidad de completar la firma electrónica. En general, se recomienda sellar la firma electrónica, empleando el perfil AdES-T.

Las firmas de los actos de intercambio o el acceso a datos con las administraciones públicas se tienen que ajustar al perfil que determine cada Administración que cede datos o da acceso a datos.

Las firmas de los actos de los ciudadanos pueden ser básicas, puesto que la Universitat Oberta de Catalunya dispone de los mecanismos para validar y completar la firma electrónica. En general, la Universidad admitirá documentos externos con firma electrónica de perfil AdES-EPES con política implícita, y debe verificar las firmas de acuerdo con el perfil AdES-EPES con política explícita, siempre que esta sea conforme con las disposiciones de los artículos 18 y siguientes del Real decreto 4/2010.

En general, la Universitat Oberta de Catalunya tiene que completar la firma de los ciudadanos de acuerdo con el perfil T-LT, o mecanismo de repositorio seguro equivalente.

En relación con la custodia a largo plazo de las firmas de los documentos, la Universitat Oberta de Catalunya garantizará, cuando resulte necesario, la conservación tanto de los documentos como de las firmas y los metadatos de estos. Al efecto pueden emplearse los métodos siguientes:

- Completado de las evidencias electrónicas mediante la utilización de formatos AdES-LTA.
- Técnicas de gestión segura de registros para garantizar la longevidad de los documentos internos.

La conservación de la firma electrónica asociada a documento electrónico obedecerá a los plazos legales y a las políticas de conservación de documentos tomando el ENI como referencia.

VII. Procesos en relación con la firma electrónica

En relación con la firma electrónica, deben implantarse los procesos siguientes:

- Proceso de creación de la firma electrónica:

Consiste en la sucesión de pasos necesarios para obtener una firma digital para un tipo de contenido concreto. Incluye la posibilidad de seleccionar y visualizar contenidos y atributos de firma, efectuar flujos de firma y ver el estado de una firma realizada.

- Proceso de validación inicial de la firma electrónica:

Consiste en la sucesión de pasos necesarios para verificar una firma digital para un tipo de contenido concreto, en el momento de recibirlo. Se trata de una verificación parcial, puesto que, normalmente, al recibir una firma electrónica no es posible determinar el estado actual de revocación de un certificado (debido a que la información de revocación se publica con un día de retraso). La verificación, por ejemplo, no incorpora en la firma un sello de fecha y hora; tampoco la completa.

El proceso debe basarse en el uso del servicio de validación de la Universitat Oberta de Catalunya, el cual podrá delegar parte del proceso de verificación (en servicios como el servicio Validador –PSIS– del Consorcio AOC).

– Proceso de validación definitiva de la firma electrónica:

Consiste en la sucesión de pasos necesarios para verificar, de forma definitiva, una firma digital para un tipo de contenido concreto. Se trata de una verificación definitiva, en un momento en el que ya es posible determinar el estado definitivo de revocación de un certificado (normalmente al menos un día después de la recepción de la firma). La verificación, cuando resulta apropiado, incorpora un sello de fecha y hora en la firma electrónica, o la completa con los datos necesarios para disfrutar de evidencia electrónica.

El proceso debe basarse en el uso de la plataforma de validación de la Universitat Oberta de Catalunya, el cual podrá delegar parte del proceso de verificación (en servicios como el servicio Validador –PSIS– del Consorcio AOC).

– Proceso de mantenimiento de la validez de la firma electrónica:

Consiste en la sucesión de pasos necesarios para mantener a lo largo del tiempo la validez de una firma digital para un tipo de contenido concreto, en el momento de recibirlo. Se trata de un proceso de adición de garantías criptográficas adicionales (típicamente, informaciones adicionales y sellos de fecha y hora) que permiten acreditar la producción de una firma en un momento concreto del tiempo, incluso en caso de ruptura u obsolescencia matemática de los algoritmos de firma electrónica.

El proceso debe basarse en el uso de la plataforma de validación de la Universitat Oberta de Catalunya, el cual podrá delegar parte del proceso de verificación en el servicio Validador (PSIS) del Consorcio AOC o en otros.

VIII. Organización y desarrollo de la política general

La aprobación de la política de firma electrónica corresponde al Consejo de Gobierno de la Universitat Oberta de Catalunya, y la responsabilidad recae en la Secretaría General.

Esta política general debe desarrollarse mediante los instrumentos siguientes:

- Estándares técnicos de firma electrónica de actos.
- Estándares técnicos de firma electrónica de formatos documentales.
- Guías y recomendaciones de firma electrónica.
- Procedimientos operativos de firma electrónica.

Corresponde al área de responsable de las tecnologías y sistemas de información de la Universitat Oberta de Catalunya, el desarrollo de la política de firma electrónica por medio de los instrumentos indicados.