

I. COMUNIDAD DE MADRID

C) Otras Disposiciones

Universidad Autónoma de Madrid

- 19** *RESOLUCIÓN de 25 de febrero de 2014, por la que se aprueban sistemas de identificación y autenticación distintos de la firma electrónica avanzada para relacionarse electrónicamente con la Universidad Autónoma de Madrid.*

El artículo 13 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, se refiere a las formas de identificación y autenticación y establece, en su apartado 2, los sistemas de firma electrónica que los ciudadanos podrán utilizar para relacionarse con las Administraciones Públicas, de acuerdo con lo que cada Administración determine.

El citado precepto se refiere expresamente a los sistemas de firma electrónica incorporados al documento nacional de identidad para personas físicas, a los sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones Públicas, y a otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen.

La Ley 59/2003, de 19 de diciembre, define la firma electrónica como “conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante”.

Por otra parte, la precitada Ley 11/2007 establece como principio general de aplicación a las relaciones electrónicas con los ciudadanos el de proporcionalidad, en cuya virtud solo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones. En virtud de dicho principio, y en el ámbito competencial propio de la Universidad Autónoma de Madrid, se considera procedente la no exigencia de certificados electrónicos o el uso del documento nacional de identidad electrónico para el caso de determinados trámites, actuaciones o colectivos en los que concurren circunstancias que hagan aconsejable la admisión de otros sistemas de identificación electrónica, relacionados en la presente Resolución.

El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, contiene algunas previsiones relativas a los mencionados sistemas de firma electrónica. Así, en su artículo 11, contempla “otros sistemas de firma electrónica” diferentes de los incorporados al documento nacional de identidad y de los sistemas de firma electrónica avanzada, indicando que su admisión deberá aprobarse, en el caso de los organismos públicos, mediante resolución del titular en el caso de los organismos públicos.

El objeto de la presente Resolución es la aprobación de determinados sistemas de identificación y autenticación electrónica distintos de la firma electrónica avanzada en el ámbito de la Universidad Autónoma de Madrid, conteniendo la denominación y descripción general de dichos sistemas de identificación, órgano responsable de su aplicación y garantías de funcionamiento, tal y como exige el artículo 11.3 del Real Decreto 1671/2009.

En su virtud, de conformidad con las competencias atribuidas por la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, y los Estatutos de la Universidad Autónoma de Madrid aprobados por Decreto 214/2003, de 16 de octubre, del Consejo de Gobierno de la Comunidad de Madrid, y modificados por Decreto 94/2009, de 5 de noviembre,

DISPONGO

Primero

Aprobación de sistemas de identificación y autenticación distintos de la firma electrónica avanzada para relacionarse electrónicamente con la Universidad Autónoma de Madrid

1. Los ciudadanos podrán utilizar para relacionarse electrónicamente con la Universidad Autónoma de Madrid, a través de los canales que se encuentren disponibles en cada momento, sistemas de identificación y autenticación electrónica distintos de la firma electrónica avanzada de los mencionados en el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y normativa de desarrollo, tales como la utilización de claves concertadas en un registro previo como usuario, aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos establecidos en la presente Resolución.

2. En virtud del principio de proporcionalidad recogido en el artículo 4 de la Ley 11/2007, los sistemas de identificación y autenticación descritos en la presente Resolución ofrecerán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los trámites, actuaciones o colectivos para los que se autorice la utilización de aquellos.

3. Se aprueba la utilización por los ciudadanos de los siguientes sistemas de identificación y autenticación electrónica distintos de la firma electrónica avanzada, cuya descripción y garantías específicas de funcionamiento se contienen en los Anexos I, II y III de la presente Resolución.

- a) Sistema de firma con clave o número de referencia.
- b) Sistema de firma con información conocida por ambas partes.
- c) Sistema de firma con clave de acceso en un registro previo como usuario.

4. La Universidad Autónoma de Madrid podrá habilitar la utilización de sistemas combinados a partir de los mencionados en el apartado anterior, manteniendo las mismas garantías de funcionamiento establecidas para dichos sistemas. Asimismo, la Universidad Autónoma de Madrid garantizará el funcionamiento de los sistemas de firma regulados en la presente Resolución conforme a los criterios de seguridad, integridad, confidencialidad, autenticidad y no repudio previstos en la Ley 11/2007 y su normativa de desarrollo.

Segundo

Órgano responsable de la aplicación de los sistemas de identificación y autenticación electrónica distintos de la firma electrónica avanzada

De conformidad con lo dispuesto en el artículo 7 del precitado Reglamento por el que se crea la Sede Electrónica de la Universidad Autónoma de Madrid, corresponde al Servicio de Tecnologías de la Información la implantación de las medidas de seguridad que garanticen la accesibilidad e integridad de la información y los servicios que se ofrecen en la Sede, siendo la Secretaría General el órgano responsable de la gestión y seguridad de la misma.

DISPOSICIÓN ADICIONAL PRIMERA

Tratamiento de datos personales

Los datos personales cuyo tratamiento resulte de la utilización de los sistemas de identificación y autenticación electrónica distintos de la firma electrónica avanzada cumplirán y se ajustarán a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

El uso por los ciudadanos de los sistemas de firma electrónica regulados en la presente norma implicará que la Universidad Autónoma de Madrid pueda tratar los datos personales consignados a los efectos de la verificación de la firma.

DISPOSICIÓN FINAL ÚNICA

Entrada en vigor y publicación en la Sede Electrónica

La presente Resolución entrará en vigor a partir del día siguiente a su publicación en el BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID. Asimismo, será objeto de publicación en la Sede Electrónica de la Universidad Autónoma de Madrid, donde se detallarán las actuaciones en las que son admisibles estos medios de identificación y autenticación y las garantías asociadas a los mismos.

Madrid, a 25 de febrero de 2014.—El Rector, PD (Resolución de 23 de mayo de 2013, BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID de 6 de junio), la Secretaria General, Ana de la Puebla Pinilla.

ANEXO I

SISTEMA DE FIRMA CON CLAVE O NÚMERO DE REFERENCIA

Primero*Descripción del sistema*

El ciudadano recibe, previa solicitud a la Universidad Autónoma de Madrid, o de oficio, una clave o número de referencia, que permitirá la realización por vía electrónica de los trámites o actuaciones que se determinen. Las solicitudes recibidas serán objeto de verificación en cuanto a la identidad del solicitante y la posibilidad de uso de este sistema.

La clave o número de referencia se genera de forma automática en un entorno seguro, asociado de manera exclusiva a los trámites o actuaciones para los que se habilita y a los ciudadanos afectados en cada caso. Para su creación se utilizará un algoritmo que relacione una serie de datos conocidos y únicos para un ciudadano determinado y un concreto trámite o actuación, pudiendo ser almacenado en el sistema de información de la Universidad Autónoma de Madrid. Dicha clave o número de referencia constará de un número fijo y determinado de caracteres numéricos y/o alfanuméricos, función del algoritmo y datos seleccionados para la formación del mismo.

La comunicación al interesado de la clave o número de referencia se realizará a través de un canal seguro, ya sea por vía electrónica, postal, presencial o telefónica. En dicha comunicación se informará, asimismo, al ciudadano de sus posibilidades y/o límites de utilización, en relación con los trámites o actuaciones para los que ha sido habilitado dicho número o clave. Mediante la utilización de la clave o número indicado el ciudadano podrá acceder electrónicamente, a través de los canales que se encuentren disponibles en cada momento, a los trámites y actuaciones determinados para los que se haya habilitado este sistema. Adicionalmente, la Universidad Autónoma de Madrid podrá solicitar al ciudadano la aportación de otros datos referidos al mismo, distintos del número o clave antes indicados, y conocidos por él y la Universidad.

La validez del sistema podrá estar limitada temporalmente en función de los plazos asociados a los trámites o actuaciones para los que se haya determinado su utilización.

La utilización del sistema descrito por parte del ciudadano implicará el consentimiento para su uso como sistema de firma electrónica.

Cuando la actuación realizada por el ciudadano implique la presentación de documentos electrónicos utilizando alguno de los sistemas de firma contemplados en la presente Resolución la Universidad Autónoma de Madrid generará automáticamente un acuse de recibo o recibo de presentación, en los términos señalados en el artículo 13 del Reglamento de Organización y Funcionamiento del Registro General y de Creación y Regulación del Registro Electrónico de la Universidad Autónoma de Madrid, de 14 de diciembre de 2012 (BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID número 22, de 26 de enero de 2013).

Segundo*Garantías de funcionamiento*

Conforme a los principios de seguridad y proporcionalidad, el sistema descrito en el apartado anterior garantiza adecuadamente su funcionamiento con arreglo a criterios de integridad, confidencialidad, autenticidad y no repudio previstos en la Ley 11/2007 y normativa de desarrollo. La clave o número de referencia se genera en un entorno seguro, de forma automática y sin intervenciones manuales.

La confidencialidad, autenticidad y no repudio se garantizan mediante el conocimiento exclusivo por parte del ciudadano y de la Universidad Autónoma de Madrid, de la clave o número de referencia y, en su caso, del resto de información requerida. El conocimiento exclusivo de la clave o número de referencia por parte del ciudadano se garantiza mediante la comunicación del mismo a través de un canal seguro, ya sea por vía electrónica, postal, presencial o telefónica.

Cuando la actuación realizada por el ciudadano implique la presentación de documentos electrónicos utilizando alguno de los sistemas de firma contemplados en la presente Resolución se garantizará la integridad de la información presentada mediante su incorporación inmediata al sistema de información de la Universidad Autónoma de Madrid. El acuse de recibo emitido por la Universidad Autónoma de Madrid y firmado con su propio código seguro de verificación o CSV será el documento con valor probatorio de la presentación realizada. La integridad de los documentos electrónicos autenticados mediante CSV podrá comprobarse mediante el acceso directo y gratuito a la sede electrónica de la Universidad Autónoma de Madrid, en tanto no se acuerde la destrucción de dichos documentos con arreglo a la normativa que resulte de aplicación o por decisión judicial.

La seguridad del sistema se ve reforzada por la limitación en cuanto a los trámites o actuaciones para las que puede ser utilizado, no siendo posible su uso fuera de dicho ámbito.

El sistema no permitirá el acceso o la firma electrónica mediante claves o números de referencia o datos incorrectos, no válidos o que no estén vigentes en el momento de su uso.

ANEXO II

SISTEMA DE FIRMA CON INFORMACIÓN CONOCIDA POR AMBAS PARTES

Primero

Descripción del sistema

El sistema consiste en la aportación por el ciudadano de determinados datos, conocidos solamente por él y la Universidad Autónoma de Madrid, distintos de la clave o número de referencia mencionado en el Anexo I, que sean requeridos para la realización, por vía electrónica, de determinados trámites o actuaciones que no impliquen acceso o consulta de datos personales más allá de los propios del procedimiento e identificación del interesado al que va referido dicho trámite o actuación.

Mediante la aportación de los datos indicados, el ciudadano podrá acceder electrónicamente, a través de los canales que se encuentren disponibles en cada momento, a los trámites y actuaciones determinados para los que se haya habilitado este sistema. La validez del sistema podrá estar limitada temporalmente en función de los plazos asociados a los trámites o actuaciones para los que se haya determinado su utilización.

La utilización del sistema descrito por parte del ciudadano implicará el consentimiento para su uso como sistema de firma electrónica. Cuando la actuación realizada por el ciudadano implique la presentación de documentos electrónicos utilizando alguno de los sistemas de firma contemplados en la presente Resolución, la Universidad Autónoma de Madrid generará automáticamente un acuse de recibo o recibo de presentación, en los términos señalados en el artículo 13 del Reglamento de Organización y Funcionamiento del Registro General y de Creación y Regulación del Registro Electrónico de la Universidad Autónoma de Madrid, de 14 de diciembre de 2012 (BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID número 22, de 26 de enero de 2013).

Segundo

Garantías de funcionamiento

Conforme a los principios de seguridad y proporcionalidad, el sistema descrito en el apartado anterior garantiza adecuadamente su funcionamiento con arreglo a criterios de integridad, confidencialidad, autenticidad y no repudio previstos en la Ley 11/2007 y normativa de desarrollo. La confidencialidad, autenticidad y no repudio se garantizan mediante el conocimiento exclusivo por parte del ciudadano, así como de la Universidad Autónoma de Madrid, de los datos requeridos.

Cuando la actuación realizada por el ciudadano implique la presentación de documentos electrónicos utilizando alguno de los sistemas de firma contemplados en la presente Resolución, se garantizará la integridad de la información presentada mediante su incorpo-

ración inmediata al sistema de información de la Universidad Autónoma de Madrid. La integridad y conservación de los documentos electrónicos almacenados y de sus metadatos asociados obligatorios quedará garantizada a través de las medidas técnicas que aseguren su inalterabilidad. El acuse de recibo emitido por la Universidad Autónoma de Madrid y firmado con su propio código seguro de verificación o CSV será el documento con valor probatorio de la presentación realizada. La integridad de los documentos electrónicos autenticados mediante CSV podrá comprobarse mediante el acceso directo y gratuito a la sede electrónica de la Universidad Autónoma de Madrid, en tanto no se acuerde la destrucción de dichos documentos con arreglo a la normativa que resulte de aplicación o por decisión judicial.

La seguridad del sistema se ve reforzada por la limitación en cuanto a los trámites o actuaciones para las que puede ser utilizado, no siendo posible su uso fuera de dicho ámbito, ni permitiéndose el acceso o consulta de datos personales más allá de los propios del procedimiento e identificación del interesado al que va referido dicho trámite o actuación. El sistema no permitirá el acceso o la firma electrónica mediante datos incorrectos, no válidos o que no estén vigentes en el momento de su uso.

ANEXO III

SISTEMA DE FIRMA CON CLAVE DE ACCESO EN UN REGISTRO PREVIAMENTE COMO USUARIO

Primero

Descripción del sistema

El sistema se basa en la inscripción por el ciudadano en un registro de usuarios. Una vez inscrito, la Universidad proporcionará al ciudadano un código y una clave de acceso. El usuario podrá en todo momento gestionar dicha clave.

A través del código y la clave de acceso el ciudadano podrá acceder electrónicamente, a través de los canales que se encuentren disponibles en cada momento, a los trámites y actuaciones determinados para los que se haya habilitado este sistema, que no podrá implicar acceso o consulta de datos personales más allá de los propios del procedimiento e identificación del interesado al que va referido dicho trámite o actuación.

La validez del sistema podrá estar limitada temporalmente en función de los plazos asociados a los trámites o actuaciones para los que se haya determinado su utilización.

La utilización del sistema descrito por parte del ciudadano implicará el consentimiento para su uso como sistema de firma electrónica. Cuando la actuación realizada por el ciudadano implique la presentación de documentos electrónicos utilizando alguno de los sistemas de firma contemplados en la presente Resolución, la Universidad Autónoma de Madrid generará automáticamente un acuse de recibo o recibo de presentación, en los términos señalados en el artículo 13 del Reglamento de Organización y Funcionamiento del Registro General y de Creación y Regulación del Registro Electrónico de la Universidad Autónoma de Madrid, de 14 de diciembre de 2012 (BOLETÍN OFICIAL DE LA COMUNIDAD DE MADRID número 22, de 26 de enero de 2013).

Segundo

Garantías de funcionamiento

Conforme a los principios de seguridad y proporcionalidad, el sistema descrito en el apartado anterior garantiza adecuadamente su funcionamiento con arreglo a criterios de integridad, confidencialidad, autenticidad y no repudio previstos en la Ley 11/2007 y normativa de desarrollo.

La confidencialidad, autenticidad y no repudio se garantizan mediante el conocimiento exclusivo por parte del ciudadano y la Universidad Autónoma de Madrid del código y la clave de acceso a dicho registro y, en su caso, de los datos proporcionados por el ciudadano en el formulario de inscripción en el registro.

Cuando la actuación realizada por el ciudadano implique la presentación de documentos electrónicos utilizando alguno de los sistemas de firma contemplados en la presente Resolución, se garantizará la integridad de la información presentada mediante su incorporación inmediata al sistema de información de la Universidad Autónoma de Madrid. La integridad y conservación de los documentos electrónicos y de sus metadatos asociados obligatorios quedará garantizada a través de las medidas técnicas que aseguren su



inalterabilidad. El acuse de recibo emitido por la Universidad Autónoma de Madrid y firmado con su propio código seguro de verificación o CSV será el documento con valor probatorio de la presentación realizada. La integridad de los documentos electrónicos autenticados mediante CSV podrá comprobarse mediante el acceso directo y gratuito a la sede electrónica de la Universidad Autónoma de Madrid, en tanto no se acuerde la destrucción de dichos documentos con arreglo a la normativa que resulte de aplicación o por decisión judicial.

La seguridad del sistema se ve reforzada por la limitación en cuanto a los trámites o actuaciones para las que puede ser utilizado, no siendo posible su uso fuera de dicho ámbito, ni permitiéndose el acceso o consulta de datos personales más allá de los propios del procedimiento e identificación del interesado al que va referido dicho trámite o actuación. El sistema no permitirá el acceso o la firma electrónica mediante datos, códigos o claves de acceso incorrectas, no válidas o que no estén vigentes en el momento de su uso.

(03/7.559/14)

