

## Universitat de València

*ACORD 192/2023, d'11 de juliol, del Consell de Govern de la Universitat de València, pel qual s'aprova el Document de Política de Signatura i Segell Electrònic i de Certificats de la Universitat de València. [2023/8588]*

### I

El Reglament d'administració electrònica de la Universitat de València (UV) aprovat mitjançant acord del Consell de Govern de 23 de juny de 2020 [ACGUV 91/2020], i publicat en el DOGV de 3 de febrer de 2022, regula dins del seu capítol III «De la identificació i autenticació» els diferents aspectes relatius als sistemes de signatura electrònica admesos en la UV en les seues relacions per mitjans electrònics, en aplicació de les disposicions relatives en les lleis 39/2015 i 40/2015.

### II

La Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, estableix els sistemes d'identificació de les persones interessades en l'article 9 i admet els següents:

- a) Sistemes basats en certificats electrònics qualificats de signatura electrònica.
- b) Sistemes basats en certificats electrònics qualificats de segell electrònic.
- c) Qualsevol altre sistema que les Administracions públiques consideren vàlid en els termes i condicions que s'establisca, sempre que compten amb un registre previ com a persona usuària que permetga garantir la seua identitat i prèvia comunicació a la Secretaria General d'Administració Digital del Ministeri d'Assumptes Econòmics i Transformació Digital. Aquesta comunicació ha d'anar acompanyada d'una declaració responsable que es compleix amb tots els requisits establerts en la normativa vigent. De manera prèvia a l'eficàcia jurídica del sistema, hauran de transcórrer dos mesos des d'aquesta comunicació, durant els quals l'òrgan estatal competent per motius de seguretat pública podrà acudir a la via jurisdiccional, previ informe vinculant de la Secretaria d'Estat de Seguretat, que haurà d'emetre en el termini de deu dies des de la seua sol·licitud.

Al seu torn, en l'article 10 es regulen els sistemes de signatura admesos:

- a) Sistemes de signatura electrònica qualificada i avançada basats en certificats electrònics qualificats de signatura electrònica expedits per prestadors inclosos en la "Llista de confiança de prestadors de serveis de certificació".
- b) Sistemes de segell electrònic qualificat i de segell electrònic avançat basats en certificats electrònics qualificats de segell electrònic expedits per prestador inclòs en la "Llista de confiança de prestadors de serveis de certificació".
- c) Qualsevol altre sistema que les Administracions públiques consideren vàlid en els termes i condicions que s'establisquen, complint els requisits anteriorment ressenyats en la lletra c) de l'article 9.

I s'afegeix que, quan així ho dispose expressament la normativa reguladora aplicable, les Administracions Públiques podran admetre els sistemes d'identificació contemplats en aquesta Llei com a sistema de signatura quan permeten acreditar l'autenticitat de l'expressió de la voluntat i consentiment de les persones interessades. Així es preveu en el Reglament d'administració electrònica de la UV (article 10.2) quan s'indica que la Universitat de València admet altres sistemes de clau concertada mitjançant un registre previ com a persona usuària, publicats en la seua electrònica, en els quals la ciutadania haurà d'identificar-se fefaentment i la utilització de la qual implicarà el consentiment per al seu ús com a sistema d'identificació i de signatura, en aquest últim cas quan permeta acreditar l'autenticitat de l'expressió de la voluntat i consentiment de les persones interessades.

Al seu torn, respecte als sistemes d'identificació i signatura de les Administracions Públiques, la Llei 40/2015, d'1 d'octubre, de règim

## Universitat de València

*ACUERDO 192/2023, de 11 de julio, del Consejo de Gobierno de la Universitat de València, por el cual se aprueba el Documento de Política de Firma y Sello Electrónicos y de Certificados de la Universitat de València. [2023/8588]*

### I

El Reglamento de administración electrónica de la Universitat de València (UV) aprobado mediante acuerdo del Consejo de Gobierno de 23 de junio de 2020 [ACGUV 91/2020], y publicado en el DOGV de 3 de febrero de 2022, regula dentro de su capítulo III «De la identificación y autenticación» los distintos aspectos relativos a los sistemas de firma electrónica admitidos en la UV en sus relaciones por medios electrónicos, en aplicación de las disposiciones relativas en las leyes 39/2015 y 40/2015.

### II

La Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas, establece los sistemas de identificación de las personas interesadas en el artículo 9, admitiendo los siguientes:

- a) Sistemas basados en certificados electrónicos cualificados de firma electrónica.
- b) Sistemas basados en certificados electrónicos cualificados de sello electrónico.
- c) Cualquier otro sistema que las administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como persona usuaria que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Esta comunicación vendrá acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente. De forma previa a la eficacia jurídica del sistema, habrán de transcurrir dos meses desde dicha comunicación, durante los cuales el órgano estatal competente por motivos de seguridad pública podrá acudir a la vía jurisdiccional, previo informe vinculante de la Secretaría de Estado de Seguridad, que deberá emitir en el plazo de diez días desde su solicitud.

A su vez, en el artículo 10 se regulan los sistemas de firma admitidos:

- a) Sistemas de firma electrónica cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".
- b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico expedidos por prestador incluido en la "Lista de confianza de prestadores de servicios de certificación".
- c) Cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, cumpliendo los requisitos anteriormente reseñados en la letra c) del artículo 9.

Y se añade que, cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de las personas interesadas. Así se prevé en el Reglamento de administración electrónica de la UV (art. 10.2) cuando se indica que la Universitat de València admitirà otros sistemas de clave concertada mediante un registro previo como persona usuaria, publicados en la sede electrónica, en los que la ciudadanía deberá identificarse fehacientemente y cuya utilización implicará el consentimiento para su uso como sistema de identificación y de firma, en este último caso cuando permita acreditar la autenticidad de la expresión de la voluntad y consentimiento de las personas interesadas.

A su vez, respecto a los sistemas de identificación y firma de las administraciones públicas, la Ley 40/2015, de 1 de octubre, de régimen



jurídico del sector públic, en el seu article 42 estableix els següents sistemes de signatura per a l'actuació administrativa automatitzada:

a) Segell electrònic d'Administració Pública, òrgan, organisme públic o entitat de dret públic, basat en certificat electrònic reconegut o qualificat que reunisca els requisits exigits per la legislació de signatura electrònica.

b) Codi segur de verificació (CSV) vinculat a l'administració pública, òrgan, organisme públic o entitat de Dret Públic, en els termes i condicions establerts, permetent-se en tot cas la comprovació de la integritat del document mitjançant l'accés a la seua electrònica corresponent.

Per a la signatura electrònica del personal al servei de les administracions públiques l'article 43, la citada Llei preveu que, sense perjudici del que es preveu en els articles 38 (seu electrònica), 41 (actuació administrativa automatitzada) i 42 (sistemes de signatura per a l'actuació administrativa automatitzada), l'actuació d'una Administració pública, òrgan, organisme públic o entitat de dret públic, quan utilitze mitjans electrònics, s'ha de realitzar mitjançant signatura electrònica de la persona titular de l'òrgan o empleat públic. Indica, així mateix, que cada Administració Pública ha de determinar els sistemes de signatura electrònica que ha d'utilitzar el seu personal, els quals podran identificar de manera conjunta a la persona titular del lloc de treball o càrrec i a l'Administració o òrgan en la qual presta els seus serveis.

L'article 9 del Reglament d'administració electrònica de la UV, estableix que l'actuació de la Universitat de València o d'algun dels seus òrgans quan utilitze mitjans electrònics, s'ha d'efectuar mitjançant un sistema de signatura electrònica de la persona titular de l'òrgan o d'empleada o empleat públic, en l'acompliment de les funcions pròpies del lloc que ocupa, que podrà identificar de manera conjunta a la Universitat de València, com a administració en la qual presta els seus serveis, i a la persona titular del lloc de treball o càrrec.

Les citades lleis 39/2015 i 40/2015 configuren un nou escenari en el qual la tramitació electrònica ha de constituir l'actuació normal de les Administracions i organismes del Sector Públic en els seus múltiples vessants de gestió interna, de relació amb la ciutadania i de relació d'aquelles entre si, per tal de fomentar l'ús dels mitjans electrònics en establir que aquest siga obligatori per a determinades persones i col·lectius i facilitar amb caràcter general les actuacions en el procediment administratiu quan només requerisquen que les persones interessades acrediten prèviament la seua identitat a través de qualsevol dels mitjans d'identificació previstos en la llei (articles 14 i 11 de la Llei 39/15), sense perjudici de l'ús obligatori de signatura per a:

- a) Formular sol·licituds.
- b) Presentar declaracions responsables o comunicacions.
- c) Interposar recursos.
- d) Desistir d'accions.
- e) Renunciar a drets.

En aquest sentit, l'article 26.3 de la Llei 39/2015 estableix que no requereixen signatura electrònica els documents electrònics emesos per les administracions públiques que es publiquen amb caràcter merament informatiu, així com aquells que no formen part d'un expedient administratiu. En tot cas, serà necessari identificar l'origen d'aquests documents.

### III

El Reial decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics, regula la Política de signatura electrònica i de certificats en l'àmbit estatal, indicant que està constituïda per les directrius i normes tècniques aplicables a la utilització de certificats i signatura electrònica (article 17).

Dins del títol II del citat Reglament, el capítol II «De la identificació i autenticació de les Administracions Públiques i les persones interessades» estableix que les administracions públiques poden utilitzar els següents sistemes per a la identificació electrònica i garantir l'origen i integritat dels documents electrònics (article 15):

a) Sistemes d'identificació de les seues electròniques i seues electròniques associades.

jurídico del sector público, en su artículo 42 establece los siguientes sistemas de firma para la actuación administrativa automatizada:

a) Sello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público, basado en certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.

b) Código seguro de verificación (CSV) vinculado a la Administración pública, órgano, organismo público o entidad de Derecho Público, en los términos y condiciones establecidos, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Para la firma electrónica del personal al servicio de las administraciones públicas el artículo 43 de la citada Ley prevé que, sin perjuicio de lo previsto en los artículos 38 (sede electrónica), 41 (actuación administrativa automatizada) y 42 (sistemas de firma para la actuación administrativa automatizada), la actuación de una Administración pública, órgano, organismo público o entidad de derecho público, cuando utilice medios electrónicos, se realizará mediante firma electrónica de la persona titular del órgano o empleado público. Indica, así mismo, que cada Administración pública determinará los sistemas de firma electrónica que debe utilizar su personal, los cuales podrán identificar de forma conjunta a la persona titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios.

El artículo 9 del Reglamento de administración electrónica de la UV, establece que la actuación de la Universitat de València o de alguno de sus órganos cuando utilice medios electrónicos, se realizará mediante un sistema de firma electrónica de la persona titular del órgano o de empleada o empleado público, en el desempeño de las funciones propias del puesto que ocupa, que podrá identificar de forma conjunta a la Universitat de València, como administración en la que presta sus servicios, y a la persona titular del puesto de trabajo o cargo.

Las citadas leyes 39/2015 y 40/2015 configuran un nuevo escenario en el que la tramitación electrónica debe constituir la actuación normal de las Administraciones y organismos del Sector Público en sus múltiples vertientes de gestión interna, de relación con la ciudadanía y de relación de aquellas entre sí, fomentando el uso de los medios electrónicos al establecer que este sea obligatorio para determinadas personas y colectivos y facilitando con carácter general las actuaciones en el procedimiento administrativo en cuanto a que solo requieran que las personas interesadas acrediten previamente su identidad a través de cualquiera de los medios de identificación previstos en la ley (art. 14 y 11 de la Ley 39/15), sin perjuicio del uso obligatorio de firma para:

- a) Formular solicitudes.
- b) Presentar declaraciones responsables o comunicaciones.
- c) Interponer recursos.
- d) Desistir de acciones.
- e) Renunciar a derechos.

En ese sentido, el artículo 26.3 de la Ley 39/2015 establece que no requerirán de firma electrónica, los documentos electrónicos emitidos por las administraciones públicas que se publiquen con carácter meramente informativo, así como aquellos que no formen parte de un expediente administrativo. En todo caso, será necesario identificar el origen de estos documentos.

### III

El 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, regula la Política de firma electrónica y de certificados en el ámbito estatal, indicando que está constituída por las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica (art. 17).

Dentro del título II del citado Reglamento, el capítulo II «De la identificación y autenticación de las administraciones públicas y las personas interesadas» establece que las administraciones públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para garantizar el origen e integridad de los documentos electrónicos (art. 15):

a) Sistemas de identificación de las sedes electrónicas y sedes electrónicas asociadas.



b) Segell electrònic basat en un certificat electrònic qualificat i que reunisca els requisits exigits per la legislació de signatura electrònica.

c) Sistemes de signatura electrònica per a l'actuació administrativa automatitzada.

d) Signatura electrònica del personal al servei de les administracions públiques.

e) Intercanvi electrònic de dades en entorns tancats de comunicació, conforme a allò específicament acordat entre les parts.

Les persones interessades poden utilitzar els sistemes d'identificació i signatura previstos en la Llei 39/2015 en les seues relacions electròniques amb les administracions públiques.

#### IV

De conformitat amb el Reglament 910/2014, de 23 de juliol, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior (eIDAS), en funció de la naturalesa de la informació que continguén i de la mena de persona a qui es dirigisca i ateses les mesures de seguretat exigibles pel nou Esquema Nacional de Seguridad (ENS) regulat mitjançant Reial decret 311/2022, de 3 de maig, els procediments podran classificar-se en diversos nivells de seguretat, en la virtut de la qual quedaran determinats els mètodes d'identificació que permeten l'accés.

A aquest efecte és necessari establir una política de signatura que establisca els principis d'interrelació amb les persones usuàries, tenint en compte que la majoria d'elles mantenen una relació de supremacia especial amb la universitat (estudiantat, personal docent i investigador i personal d'administració i serveis). Amb caràcter general, seran de nivell baix els nivells d'exigència d'identificació de les persones físiques que integren aquests col·lectius. Les relacions amb la resta de persones físiques i les persones jurídiques seran normalment de nivell mitjà. La determinació del nivell de seguretat hauria d'establir-se també en la informació que figure en el catàleg de procediments de la seua electrònica.

Per tant, s'han d'establir els sistemes de signatura electrònica en funció del nivell d'identificació i integritat que garanteixen, la qual cosa equival al nivell de seguretat jurídica dels documents electrònics (a major seguretat, major complexitat tècnica) i per això:

Els actes que es consideren de nivell mitjà hauran d'autenticar-se utilitzant sistemes de signatura electrònica avançada basada en certificat reconegut.

Els actes que es consideren de nivell alt han d'autenticar-se necessàriament utilitzant sistemes de signatura electrònica reconeguda o qualificada.

La resta d'actes poden documentar-se amb qualsevol sistema de signatura electrònica i, en concret, realitzar-se amb els sistemes d'autenticació basats en usuari i contrasenya proporcionats per la Universitat una vegada valorada la conveniència i analitzats els riscos.

Els actes d'intercanvi de dades amb les administracions públiques, o l'accés a les dades d'aquestes, ha d'exigir el nivell mínim establert per cada administració que en cedeix o hi dona accés.

La signatura electrònica dels actes de contractació pública i de facturació electrònics ha de ser la que determine la normativa que li siga aplicable.

D'altra banda, també han de contemplar-se els supòsits en els quals la UV es relaciona amb ciutadans de la Unió Europea i fins i tot aliens a ella, i establir mecanismes que faciliten aquesta relació electrònica i mantinguen nivells de seguretat adequats amb els interlocutors.

#### V

Conforme al Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica (ENI), una política de signatura electrònica de certificats és el «conjunt de normes de seguretat, d'organització, tècniques i legals per a determinar com es generen, verifiquen i gestionen signatures electròniques, incloses les característiques exigibles als certificats de signatura».

b) Sello electrónico basado en un certificado electrónico cualificado y que reúna los requisitos exigidos por la legislación de firma electrónica.

c) Sistemas de firma electrónica para la actuación administrativa automatizada.

d) Firma electrónica del personal al servicio de las administraciones públicas.

e) Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicament acordado entre las partes.

Las personas interesadas podrán utilizar los sistemas de identificación y firma previstos en la Ley 39/2015 en sus relaciones electrónicas con las administraciones públicas.

#### IV

De conformidad con el Reglamento 910/2014, de 23 de julio, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS), en función de la naturaleza de la información que contengan y del tipo de persona a quien se dirija y atendiendo a las medidas de seguridad exigibles por el nuevo Esquema Nacional de Seguridad (ENS) regulado mediante Real decreto 311/2022, de 3 de mayo, los procedimientos podrán clasificarse en varios niveles de seguridad, en cuya virtud quedarán determinados los métodos de identificación que permiten el acceso.

A estos efectos es necesario establecer una política de firma que establezca los principios de interrelación con las personas usuarias, teniendo en cuenta que la mayoría de ellos mantienen una relación de supremacia especial con la universidad (estudiantado, personal docente e investigador y personal de administración y servicios). Con carácter general, serán de nivel bajo los niveles de exigencia de identificación de las personas físicas que integran dichos colectivos. Las relaciones con las restantes personas físicas y las personas jurídicas serán normalmente de nivel medio. La determinación del nivel de seguridad debería establecerse también en la información que figure en el catálogo de procedimientos de la sede electrónica.

Por tanto, se deben establecer los sistemas de firma electrónica en función del nivel de identificación e integridad que garantizan, lo que equivale al nivel de seguridad jurídica de los documentos electrónicos (a mayor seguridad, mayor complejidad técnica) y por ello:

Los actos que se consideren de nivel medio deberán autenticarse utilizando sistemas de firma electrónica avanzada basada en certificado reconocido.

Los actos que se consideren de nivel alto deben autenticarse necesariamente utilizando sistemas de firma electrónica reconocida o calificada.

El resto de actos pueden documentarse con cualquier sistema de firma electrónica y, en concreto, podrán realizarse con los sistemas de autenticación basados en usuario y contraseña proporcionados por la Universidad una vez valorada la conveniència 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 electrònics será la que determine la normativa que le sea aplicable.

Por otro lado, también deben contemplarse los supuestos en los que la UV se relaciona con ciudadanos de la Unión Europea e incluso ajenos a ella, estableciendo mecanismos que faciliten dicha relación electrónica y manteniendo niveles de seguridad adecuados con los interlocutores.

#### V

Conforme al 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 (ENI), una política de firma electrónica y de certificados es el «conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma».

L'objectiu és determinar la validesa de la signatura electrònica per a una transacció en particular, especificant la informació que ha d'incloure la persona signant en el procés de generació de la signatura i la informació que s'ha de comprovar en el procés de validació d'aquesta.

L'article 18 de l'ENI estableix que l'Administració general de l'Estat ha de definir una política de signatura electrònica i de certificats que servisca de marc general d'interoperabilitat per al reconeixement mutu de les signatures electròniques basades en certificats de documents administratius en les administracions públiques. La resta d'Administracions Públiques podran acollir-s'hi, sense perjudici de poder aprovar altres polítiques de signatura electrònica dins dels seus respectius àmbits competencials partint, entre altres, de la Norma Tècnica de Política de signatura electrònica i de certificats de l'Administració definida en la seua disposició adicional primera.

## VI

La Resolució de 27 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, aprova la Norma Tècnica d'Interoperabilitat de Política de Signatura i Segell Electrònics i de Certificats de l'Administració (BOE 3 de novembre) que estableix en el seu apartat II.5 que «Les administracions públiques s'han d'acollir preferentment a la «Política Marc de Signatura Electrònica basada en Certificats», sense perjudici que «cada organització ha de valorar la necessitat i conveniència de desenvolupar una política pròpia enfront de la possibilitat d'utilitzar una política marc existent» i que es «poden aprovar altres polítiques de signatura i segell electrònics dins dels seus àmbits competencials si les característiques particulars dels procediments administratius sota la seua competència ho fan necessari».

## VII

En aquest context normatiu, és necessari establir una política de signatura de la Universitat de València (UV) que establisca els principis d'interrelació amb les persones administrades, tenint en compte que la majoria d'elles mantenen una relació de supremacia especial amb la universitat (estudiantat, PDI i PAS), així com harmonitzar la classificació de nivells de seguretat dels procediments i la seua correlativa exigibilitat de mètodes d'identificació i signatura, més o menys rígids en atenció a les relacions de «supremacia especial» amb les citades persones de la comunitat universitària.

Per tot l'exposat, s'adopta la següent Política de Signatura i Segell Electrònics i de Certificats de la Universitat de València:

### *Article 1. Objecte*

L'objecte de la present política és fixar les condicions generals aplicables a la identificació i signatura electrònica per a la seua validació i el seu ús en la relació electrònica de la Universitat de València (UV) amb la ciutadania, pertanguen o no a la comunitat universitària, entre els seus òrgans i unitats i amb altres Administracions Públiques o entitats públiques o privades.

Estableix, per tant, el conjunt de criteris comuns assumits per la Universitat de València en relació amb l'autenticació i el reconeixement mutu de signatures electròniques basades en certificats i de la clau concertada corporativa.

### *Article 2. Política marc de signatura electrònica i certificats*

La UV s'adhereix a la política marc de signatura electrònica i de certificats de l'Administració General de l'Estat, sense perjudici de les peculiaritats establertes en la present Política, la qual pot confluïr amb altres polítiques particulars de la UV per a una transacció determinada en un context concret, sempre basades i desenvolupades a partir d'ella.

### *Article 3. Àmbit d'aplicació*

Aquesta política és aplicable, en l'àmbit de competència de la Universitat de València, per als següents supòsits:

a) Les relacions electròniques de la UV amb la ciutadania (personal o no de la Comunitat Universitària) i proveïdors, en tots els serveis i

El objetivo es determinar la validez de la firma electrónica para una transacción en particular, especificando la información que debe incluir la persona firmante en el proceso de generación de la firma y la información que se debe comprobar en el proceso de validación de la misma.

El artículo 18 del ENI establece que la Administración general del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para el reconocimiento mutuo de las firmas electrónicas basadas en certificados de documentos administrativos en las administraciones públicas. Las restantes administraciones públicas podrán acogerse a la misma, sin perjuicio de que podrán aprobar otras políticas de firma electrónica dentro de sus respectivos ámbitos competenciales partiendo, entre otros, de la Norma Técnica de Política de firma electrónica y de certificados de la Administración definida en su disposición adicional primera.

## VI

La Resolució de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración (BOE 3 de noviembre) que establece en su apartado II.5 que «Las administraciones públicas se acogerán preferentemente a la Política Marco de Firma Electrónica basada en Certificados», sin perjuicio de que «cada organización valorará la necesidad y conveniencia de desarrollar una política propia frente a la posibilidad de utilizar una política marco existente» y de que se «podrán aprobar otras políticas de firma y sello electrónicos dentro de sus ámbitos competenciales si las características particulares de los procedimientos administrativos bajo su competencia lo hacen necesario».

## VII

En este contexto normativo es necesario establecer una política de firma de la Universitat de València (UV) que establezca los principios de interrelación con sus personas administradas, teniendo en cuenta que la mayoría de ellas mantienen una relación de supremacia especial con la universidad (estudiantado, PDI y PAS), así como armonizar la clasificación de niveles de seguridad de los procedimientos y su correlativa exigibilidad de métodos de identificación y firma, más o menos rígidos en atención a las relaciones de «supremacia especial» con las citadas personas de la comunidad universitaria.

Por todo lo expuesto, se procede a adoptar la siguiente Política de Firma y Sello Electrónicos y de Certificados de la Universitat de València:

### *Artículo 1. Objeto*

El objeto de la presente Política es fijar las condiciones generales aplicables a la identificación y firma electrónica para su validación y su uso en la relación electrónica de la Universitat de València (UV) con la ciudadanía, pertenezcan o no a la comunidad universitaria, entre los órganos y unidades de la misma y con otras Administraciones Públicas o entidades públicas o privadas.

Establece, por tanto, el conjunto de criterios comunes asumidos por la Universitat de València en relación con la autenticación y el reconocimiento mutuo de firmas electrónicas basadas en certificados y de la clave concertada corporativa.

### *Artículo 2. Política marco de firma electrónica y certificados*

La UV se adhiere a la política marco de firma electrónica y de certificados de la Administración General del Estado, sin perjuicio de las peculiaridades establecidas en la presente Política, la cual podrá confluïr con otras políticas particulares de la UV para una transacción determinada en un contexto concreto, siempre basadas y desarrolladas a partir de ella.

### *Artículo 3. Ámbito de aplicación*

Esta Política será de aplicación, en el ámbito de competencia de la Universitat de València, para los siguientes supuestos:

a) Las relaciones electrónicas de la UV con la ciudadanía (personal o no de la Comunidad Universitaria) y proveedores, en todos los ser-

procediments posats a la disposició d'aquests a través de la seua Seu electrònica.

b) Les relacions electròniques entre els òrgans, unitats i personal empleat de la Universitat, ja siga internament o amb altres entitats externes.

c) Les relacions electròniques de la universitat amb la resta d'administracions i entitats públiques i privades.

#### *Article 4. Identificació del gestor de la Política*

Nom del gestor	Secretaria General
Direcció de contacte	<a href="mailto:secretariageneral@uv.es">secretariageneral@uv.es</a>
Identificador del gestor (DIR3)	U01800008

#### *Article 5. Atribucions del gestor de la Política*

1. Adopta les mesures i dicta les instruccions necessàries per al desenvolupament, execució i aplicació de la política de signatura i segell electrònics i de certificats de la Universitat de València.

2. És responsable del manteniment, actualització i publicació electrònica de qualsevol aspecte relatiu a la present Política de Signatura i Segell Electrònics i de Certificats de la UV.

#### *Article 6. Sistemes d'identificació i signatura*

1. La UV admet l'ús dels següents certificats electrònics:

a) Certificats electrònics de persona física.

b) Claus concertades del sistema Cl@ve.

c) Certificats d'empleada o empleat públic.

d) Certificats de representant de persona jurídica.

e) Certificats de segell d'òrgan.

2. Els usos i aplicacions de cada tipus de certificat es determinaran en els procediments electrònics que habilite la UV i que hauran d'estar incorporats prèviament al Catàleg de Procediments i Serveis d'aquesta.

3. En tot cas, l'ús de certificats electrònics s'ha de regir atenent als següents criteris:

3.1. El sistema comú d'identificació i signatura en la seu electrònica és el de clau concertada: usuari i contrasenya proporcionada per la UV a tota la comunitat universitària; usuari i contrasenya del sistema Cl@ve; usuari i contrasenya de seu si no es disposa de les claus anteriors, encara que per a aquesta opció el seu ús haurà de ser de manera excepcional i només vàlid per a certs tràmits.

Amb la finalitat de garantir la interoperabilitat, així com assegurar la integritat, inalterabilitat i el no repudi dels documents signats, la UV pot superposar un segell electrònic basat en un certificat electrònic qualificat.

3.2. Es pot articular, en determinats procediments, l'ús de certificats d'empleat públic per a l'acompliment de les funcions pròpies del lloc que ocupen, o per a relacionar-se amb les administracions públiques.

3.3. Es promou l'ús de certificats de segell d'òrgan en les actuacions administratives automatitzades i el codi segur de verificació vinculat a la Universitat de València o a l'òrgan competent, que permetrà la comprovació de la integritat del document mitjançant l'accés a la seu electrònica de la Universitat.

3.4. Per a facilitar l'accés de persones de nacionalitats diferents de l'espanyola en l'ús de procediments de la UV, poden utilitzar-se de manera excepcional altres sistemes d'identificació i signatura per a l'estudiantat estranger o sol·licitants estrangers en convocatòries de la UV, procurant que siguin mecanismes d'identificació que utilitzen credencials de serveis d'identificació de tercers d'àmplia difusió en les relacions electròniques. Aquests mitjans d'identificació no són d'ús general, sinó que han d'autoritzar-se de manera expressa mitjançant resolució de la Secretaria General per a cada procediment en què es demanden.

#### *Article 7. Certificat de persona física*

La Universitat de València permet qualsevol dels sistemes d'identificació i signatura electrònica establerts en els articles 9 i 10, respectivament, de la Llei 39/2015, d'1 d'octubre, del procediment administratiu

vicios y procedimientos puestos a disposición de estos a través de su Sede electrónica.

b) Las relaciones electrónicas entre los órganos, unidades y personal empleado de la Universidad, ya sea internamente o con otras entidades externas.

c) Las relaciones electrónicas de la universidad con el resto de administraciones y entidades públicas y privadas.

#### *Artículo 4. Identificación del gestor de la Política*

Nombre del gestor	Secretaria General
Dirección de contacto	<a href="mailto:secretariageneral@uv.es">secretariageneral@uv.es</a>
Identificador del gestor (DIR3)	U01800008

#### *Artículo 5. Atribuciones del gestor de la Política*

1. Adoptará las medidas y dictará las instrucciones necesarias para el desarrollo, ejecución y aplicación de la Política de Firma y Sello Electrónicos y de Certificados de la Universitat de València.

2. Será responsable del mantenimiento, actualización y publicación electrónica de cualquier aspecto relativo a la presente Política de Firma y Sello Electrónicos y de Certificados de la UV.

#### *Artículo 6. Sistemas de identificación y firma*

1. La UV admitirá el uso de los siguientes certificados electrónicos:

a) Certificados electrónicos de persona física.

b) Claves concertadas del sistema Cl@ve.

c) Certificados de empleada o empleado público.

d) Certificados de representante de persona jurídica.

e) Certificados de sello de órgano.

2. Los usos y aplicaciones de cada tipo de certificado se determinarán en los procedimientos electrónicos que habilite la UV y que deberán estar incorporados previamente al Catálogo de Procedimientos y Servicios de esta.

3. En todo caso, el uso de certificados electrónicos se regirá conforme a los siguientes criterios:

3.1. El sistema común de identificación y firma en la sede electrónica será el de clave concertada: usuario y contraseña proporcionada por la UV a toda la comunidad universitaria; usuario y contraseña del sistema Cl@ve; usuario y contraseña de sede si no se dispone de las claves anteriores, aunque para esta opción, su uso deberá ser de forma excepcional y solo válido para ciertos trámites.

Con el fin de garantizar la interoperabilidad, así como para asegurar la integridad, inalterabilidad y el no repudio de los documentos firmados, la UV podrá superponer un sello electrónico basado en un certificado electrónico cualificado.

3.2. Se podrá articular en determinados procedimientos el uso de certificados de empleado público para el desempeño de las funciones propias del puesto que ocupen, o para relacionarse con las administraciones públicas.

3.3. Se promoverá el uso de certificados de sello de órgano en las actuaciones administrativas automatizadas y el código seguro de verificación vinculado a la Universitat de València o al órgano competente, que permitirá la comprobación de la integridad del documento mediante el acceso a la sede electrónica de la Universitat.

3.4. Para facilitar el acceso de personas de nacionalidades distintas de la española en el uso de procedimientos de la UV podrán utilizarse de manera excepcional otros sistemas de identificación y firma para el estudiantado extranjero o solicitantes extranjeros en convocatorias de la UV, procurando que sean mecanismos de identificación que utilicen credenciales de servicios de identificación de terceros de amplia difusión en las relaciones electrónicas. Estos medios de identificación no serán de uso general, sino que tendrán que autorizarse de forma expresa mediante resolución de la Secretaria General para cada procedimiento donde se demanden.

#### *Artículo 7. Certificado de persona física*

La Universitat de València permitirá cualquiera de los sistemas de identificación y firma electrónica establecidos en los artículos 9 y 10, respectivamente, de la Ley 39/2015, de 1 de octubre, del procedimiento

comú de les administracions públiques, la relació de les quals està disponible en la seua electrònica.

L'expedició de certificats electrònics personals es pot realitzar en les diferents oficines de registre habilitades per a tal fi i per registradors nomenats per la Secretaria General. Aquestes oficines han de col·laborar en el manteniment, renovació i gestió dels certificats i hauran de comunicar a la Secretaria General qualsevol incident que es detecte.

#### *Article 8. Clau concertada de la Universitat de València*

La Universitat de València admet un sistema de clau concertada, basada en el compte institucional i la seua contrasenya associada proporcionades a les persones usuàries de la comunitat universitària i col·lectius assimilats, que facilitarà la relació electrònica amb la universitat, sense perjudici d'altres sistemes d'identificació i signatura que, pel nivell de seguretat del procediment o servei, es requereisca.

Amb caràcter general, seran de nivell baix els nivells d'exigència d'identificació de les persones de la comunitat universitària i assimilats, en funció del que es preveu en el Reglament 910/2014, de 23 de juliol, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior (eIDAS) i ateses les mesures de seguretat exigibles pel nou Esquema Nacional de Seguretat (ENS).

Per tant, el sistema ordinari d'autenticació i firma en la seua electrònica per a les persones de la comunitat universitària i persones físiques que, per raó de relació jurídica preexistent amb la UV, disposen de compte de correu electrònic institucional i actuen com a persones interessades en el procediment administratiu, és el de clau concertada (usuari i contrasenya de la UV), sense perjudici de la utilització de certificat electrònic qualificat.

Aquest sistema de signatura es pot utilitzar per a signar documents en els procediments específics disponibles en la Seu Electrònica de la UV, en la mesura que aquests vagen adaptant-s'hi. En cas que un procediment específic no el tinga implementat es podrà signar mitjançant certificat electrònic qualificat.

#### *Article 9. Certificats d'empleat públic*

1. La UV pot emetre un certificat d'empleat públic (CEP) al personal empleat que considere convenient on es faça constar la seua vinculació amb la institució. La UV pot emetre el CEP per a tots aquells càrrecs i llocs que formulen resolucions o acords que tenen eficàcia fora de la UV o que suposen capacitat específica de signatura o representació en nom de la Universitat.

2. Només s'atorguen certificats d'empleat públic al personal de la UV, empleats públics amb qualsevol vincle jurídic, sempre en situació d'actiu i que exercisquen les seues funcions a la Universitat de València.

3. Els certificats d'empleats seran revocats quan cessen en les seues funcions en la UV, el seu vincle amb ella o per canvi de funcions, de destinació o pel que es disposa en l'apartat 1 d'aquest capítol.

4. La signatura amb CEP acredita la identitat de la persona titular i l'ocupació del lloc o càrrec, en el seu cas, i tindrà plens efectes en el procediment.

5. La sol·licitud de CEP pot realitzar-se a través de la seua electrònica mitjançant una instància interna. Amb anterioritat a l'expedició, es comprovarà que la persona titular presta els seus serveis en la UV. El registre i l'expedició de certificats CEP d'empleat públic es realitza exclusivament en la Gerència. Les altres unitats i serveis de la Universitat han de col·laborar en el manteniment i gestió dels certificats, així com comunicar a la Gerència qualsevol incidència que es detecte.

6. Per a la renovació de claus amb o sense renovació de la targeta física, el procediment és el mateix que per a l'emissió inicial del certificat.

7. La revocació del CEP es produirà quan concórrega algun dels casos següents:

- a) D'ofici, quan una persona deixa de prestar els seus serveis o cessa en el càrrec o lloc, o pel seu ús indegut.
- b) A instàncies de part, per destrucció o pèrdua de la targeta o per necessitat de canvi de la clau personal o per caducitat d'aquesta.

Un certificat revocat no pot tornar a utilitzar-se i no pot alçar-se la revocació ni anul·lar-se de cap altra forma, però pot tornar a sol·lici-

administrativo común de las administraciones públicas, cuya relación estará disponible en la sede electrónica.

La expedición de certificados electrónicos personales se podrá realizar en las diferentes oficinas de registro habilitadas para tal fin y por registradores nombrados por la Secretaría General. Dichas oficinas colaborarán en el mantenimiento, renovación y gestión de los certificados y deberán comunicar a la Secretaría General cualquier incidente que se detecte.

#### *Artículo 8. Clave concertada de la Universitat de València*

La Universitat de València admite un sistema de clave concertada, basada en la cuenta institucional y su contraseña asociada proporcionadas a las personas usuarias de la comunidad universitaria y colectivos asimilados que facilitará la relación electrónica con la universidad, sin perjuicio de otros sistemas de identificación y firma que por el nivel de seguridad del procedimiento o servicio se requiera.

Con carácter general, serán de nivel bajo los niveles de exigencia de identificación de las personas de la comunidad universitaria y asimilados, en función de lo previsto en el Reglamento 910/2014, de 23 de julio, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS) y atendiendo a las medidas de seguridad exigibles por el nuevo Esquema Nacional de Seguridad (ENS).

Por tanto, el sistema ordinario de autenticación y firma en la sede electrónica para las personas de la comunidad universitaria y personas físicas que, por razón de relación jurídica preexistente con la UV, dispongan de cuenta de correo electrónico institucional y actúen como personas interesadas en el procedimiento administrativo, será el de clave concertada (usuario y contraseña de la UV), sin perjuicio de la utilización de certificado electrónico cualificado.

Este sistema de firma se podrá utilizar para firmar documentos en los procedimientos específicos disponibles en la Sede Electrónica de la UV, en la medida que estos se vayan adaptando al mismo. En caso de que un procedimiento específico no lo tenga implementado se podrá firmar mediante certificado electrónico cualificado.

#### *Artículo 9. Certificados de empleado público*

1. La UV podrá emitir un certificado de empleado público (CEP) para el personal empleado que considere conveniente, donde se haga constar su vinculación con la institución. La UV podrá emitir el CEP para todos aquellos cargos y puestos que formulen resoluciones o acuerdos que tienen eficacia fuera de la UV o que supongan capacidad específica de firma o representación en nombre de la Universitat.

2. Solo se otorgarán certificados de empleado público a personal de la UV, empleados públicos con cualquier vínculo jurídico, siempre en situación de activo y que ejerzan sus funciones en la Universitat de València.

3. Los certificados de empleados serán revocados al cesar en sus funciones en la UV, al cesar su vínculo con ella o por cambio de funciones, de destino o por lo dispuesto en el apartado 1 de este capítulo.

4. La firma con CEP acreditará la identidad de la persona titular y la ocupación del puesto o cargo, en su caso, y tendrá plenos efectos en el procedimiento.

5. La solicitud de CEP podrá realizarse a través de la sede electrónica mediante una instancia interna. Con anterioridad a la expedición, se procederá a comprobar que la persona titular presta sus servicios en la UV. El registro y la expedición de certificados CEP de empleado público se realizará exclusivamente en la Gerencia. Las demás unidades y servicios de la Universitat deberán colaborar en el mantenimiento y gestión de los certificados, así como comunicar a la Gerencia cualquier incidencia que se detecte.

6. Para la renovación de claves con o sin renovación de la tarjeta física, el procedimiento será el mismo que para la emisión inicial del certificado.

7. La revocación del CEP se producirá cuando concorra alguno de los siguientes casos:

- a) De oficio, cuando una persona deja de prestar sus servicios o cesa en el cargo o puesto, o por su uso indebido.
- b) A instancia de parte, por destrucción o pérdida de la tarjeta o por necesidad de cambio de la clave personal o por caducidad de la misma.

Un certificado revocado no puede volver a utilizarse y no puede levantarse la revocación ni anularse de ninguna otra forma, pero podrá



tar-se'n un de nou en cas que es modifiquen les circumstàncies de la revocació.

8. Qui siga titular del CEP és també responsable exclusiu de la custòdia i ús de les claus personals de signatura, sense que pugua comunicar, cedir o autoritzar el seu ús a un tercer.

El lliurament de CEP emesos suposa les obligacions següents:

a) Advertir la Gerència de qualsevol error en les dades emmagatzemades.

b) Comunicar igualment a Gerència qualsevol variació en les dades personals a fi de corregir-les en les bases de dades de personal.

c) No comunicar les claus a terceres persones.

d) Sol·licitar la renovació dels certificats continguts en la targeta abans que expire el seu període de validesa.

e) Fer un ús adequat del certificat sobre la base de les competències i facultats atribuïdes pel càrrec o lloc de treball.

f) Assumir la present normativa o la que es dicte en el seu desenvolupament o substitució.

g) Comunicar el cessament o canvi de funcions o destinació.

#### *Article 10. Certificats electrònics de representant d'entitat*

1. La Universitat de València pot emetre certificats electrònics de representant de la Universitat com a persona jurídica a aquelles persones físiques que componen el Consell de Direcció, tenint en compte l'important volum de tràmits i sempre que s'autoritze l'habilitació per acord del Consell de Govern.

2. Els certificats s'expediran sota la responsabilitat dels càrrecs per al desenvolupament de les seues competències. Les persones habilitades tenen l'obligació de custodiar les targetes que contenen els certificats i claus privades d'aquestes.

3. L'ús del certificat comprèn exclusivament les funcions delegades mitjançant resolució del Rectorat i, per tant, queda prohibit qualsevol ús diferent al que està destinat.

#### *Article 11. Certificats de segell d'òrgan*

De conformitat amb l'article 8 del Reglament d'Administració Electrònica de la UV, la creació de segells electrònics vinculats a la Universitat de València i a òrgans administratius d'aquesta s'ha de dur a terme mitjançant resolució del rector o la rectora o persona en qui delegue. Aquesta resolució ha d'assenyalar l'òrgan titular responsable de la seua utilització, les característiques tècniques generals del sistema de signatura i certificat, així com el servei de validació per a la verificació del certificat i les actuacions i procediments en els quals podrà ser utilitzat.

Així mateix, aquest serà el sistema ordinari de signatura de les actuacions i certificacions que passen a ser expedides de manera automatitzada.

#### *Article 12. Signatura de documents per part de la Universitat de València*

1. Els documents electrònics que formen part d'un procediment administratiu com ara resolucions o acords i/o que tinguen efectes enfront de tercers o en altres administracions públiques hauran d'estar signats pel càrrec o pel personal funcionari que tinga les competències per a dictar-los o una delegació expressa. La signatura es fa amb un certificat d'empleat públic o segell d'òrgan o certificat de representant de la UV, segons siga procedent, mitjançant l'eina del Portafirmes de la UV. El document haurà d'incloure un Codi Segur de Verificació (CSV) de l'acte administratiu que permeta la seua verificació a través de la seua electrònica.

2. La signatura de documents en procediments de tramitació interns es realitza ordinàriament amb clau concertada i mitjançant l'ús de l'eina corporativa de portafirmes, en la mesura que la solució de tramitació electrònica ho permeta.

3. En l'actuació administrativa automatitzada s'ha d'utilitzar el segell electrònic de la Universitat de València o òrgan competent i el codi segur de verificació vinculat a la UV o a l'òrgan competent, que permetrà la comprovació de la integritat del document mitjançant l'accés a la seua electrònica de la Universitat, conforme al que es preveu en l'article 8 del Reglament d'Administració Electrònica.

volver a solicitarse uno nuevo en caso de que se modifiquen las circunstancias de la revocación.

8. Quién sea titular del CEP será responsable exclusivo de la custodia y uso de las claves personales de firma, sin que pueda comunicar, ceder o autorizar a un tercero su uso.

La entrega de CEP emitidos supone las siguientes obligaciones:

a) Advertir a la Gerencia de cualquier error en los datos almacenados.

b) Comunicar igualmente a la Gerencia cualquier variación en los datos personales a fin de ser corregidos en las bases de datos de personal.

c) No comunicar las claves a terceras personas.

d) Solicitar la renovación de los certificados contenidos en la tarjeta antes de que expire su período de validez.

e) Realizar un uso adecuado del certificado en base a las competencias y facultades atribuidas por el cargo o puesto de trabajo.

f) Asumir la presente normativa o la que se dicte en su desarrollo o sustitución.

g) Comunicar el cese o cambio de funciones o destino.

#### *Artículo 10. Certificados electrónicos de representante de entidad*

1. La Universitat de València podrá emitir certificados electrónicos de representante de la Universitat como persona jurídica a aquellas personas físicas que componen el Consejo de Dirección, teniendo en cuenta el importante volumen de trámites y siempre que se autorice la habilitación por acuerdo del Consejo de Gobierno.

2. Los certificados se expedirán bajo la responsabilidad de los cargos para el desarrollo de sus competencias. Las personas habilitadas tienen la obligación de custodiar las tarjetas que contienen los certificados y claves privadas de estas.

3. El uso del certificado comprende única y exclusivamente las funciones delegadas mediante resolución del Rectorado y, por tanto, queda prohibido cualquier uso diferente al que está destinado.

#### *Artículo 11. Certificados de sello de órgano*

De conformidad con el artículo 8 del Reglamento de Administración Electrónica de la UV, la creación de sellos electrónicos vinculados a la Universitat de València y a órganos administrativos de la misma se realizará mediante resolución del rector o la rectora o persona en quien delegue. Dicha resolución deberá señalar el órgano titular que será responsable de su utilización, las características técnicas generales del sistema de firma y certificado, así como el servicio de validación para la verificación del certificado, y las actuaciones y procedimientos en los que podrá ser utilizado.

Asimismo, este será el sistema ordinario de firma de las actuaciones y certificaciones que pasen a ser expedidas de modo automatizado.

#### *Artículo 12. Firma de documentos por parte de la Universitat de València*

1. Los documentos electrónicos que formen parte de un procedimiento administrativo tales como resoluciones o acuerdos y/o que tengan efectos frente a terceros o en otras administraciones públicas deberán estar firmados por el cargo o por el personal funcionario que tenga las competencias para dictarlos o una delegación expresa. La firma se realizará con un certificado de empleado público o sello de órgano o certificado de representante de la UV, según proceda, utilizando la herramienta del Portafirmas de la UV. El documento deberá incluir un Código Seguro de Verificación (CSV) del acto administrativo que permita su verificación a través de la sede electrónica.

2. La firma de documentos en procedimientos de tramitación internos se realizará ordinariamente con clave concertada y mediante el uso de la herramienta corporativa de portafirmas, en la medida que la solución de tramitación electrónica lo permita.

3. En la actuación administrativa automatizada se utilizará el sello electrónico de la Universitat de València o del órgano competente para llevar a cabo la misma y el código seguro de verificación vinculado a la UV o al órgano competente, que permitirá la comprobación de la integridad del documento mediante el acceso a la sede electrónica de la Universitat, conforme a lo previsto en el artículo 8 del Reglamento de Administración Electrónica.

*Article 13. Referència temporal dels documents administratius electrònics*

La possibilitat d'emetre vàlidament i per mitjans electrònics els documents administratius ve descrita en la Llei 39/2015 que indica que, a més de la signatura electrònica, han d'incloure una referència temporal quan la naturalesa del document així ho requerisca.

Per tant, la Universitat de València haurà d'associar als documents administratius electrònics una de les següents modalitats de referència temporal, d'acord amb el que determinen les normes reguladores dels respectius procediments:

a) Marca de temps: entenent per tal l'assignació per mitjans electrònics de la data i, si escau, l'hora a un document electrònic. La marca de temps s'utilitza en tots aquells casos en els quals les normes reguladores no establisquen la utilització d'un segell electrònic qualificat de temps.

b) Segell electrònic qualificat de temps: entenent per tal l'assignació per mitjans electrònics d'una data i hora a un document electrònic amb la intervenció d'un prestador qualificat de serveis de confiança que assegure l'exactitud i integritat de la marca de temps del document. Els segells electrònics de temps no qualificats seran assimilables amb caràcter general a les marques de temps.

En tot cas, serà la norma que regule el procediment on constaran els documents electrònics la que indique la conveniència d'usar marca o segell de temps, perquè la Llei 39/2015 exigeix en general una referència temporal del moment en què han sigut emesos per a considerar un document administratiu vàlid, però no exigeix la fehaència que atorga un segell de temps.

L'Esquema Nacional de Seguretat distingeix tres tipus de sistemes d'informació en funció de la seua criticitat i nivell de seguretat exigible (Alta, Mitjana i Bàsica); l'ús de segellament de temps és obligat únicament per als sistemes categoritzats com a nivell Alt. Sense perjudici de l'anterior, s'emprarà segellat de temps en aquells supòsits en els quals la informació siga susceptible de ser utilitzada com a evidència electrònica en un futur.

La informació relativa a les marques i segells electrònics qualificats de temps s'associarà als documents electrònics en la forma que determine l'Esquema Nacional d'Interoperabilitat i la normativa corresponent.

*Article 14. Segellat de temps i signatura electrònica*

El segellat de temps és un mètode per a provar que un conjunt de dades ha existit abans d'un moment donat i que cap d'aquestes dades ha sigut modificada des de llavors. Incloure un segell de temps en una signatura digital és un mitjà per tenir una evidència de l'instant en el qual el document s'ha signat, i atorga aquests mitjans addicionals per a garantir-ne la propietat i no repudi.

El segellat de temps proporciona un valor afegit a la utilització de signatura digital, ja que la signatura per si sola no subministra cap informació sobre el moment de creació de la signatura, i en el cas que el signant la incloguera, aquesta hauria sigut proporcionada per una de les parts, quan allò recomanable és que ho siga per una tercera part de confiança.

La relació de prestadors qualificats de serveis de confiança que presten serveis de segellat de temps en el sector públic haurà d'estar inclosa en la «Llista de confiança de prestadors qualificats de serveis de confiança».

La Universitat de València utilitza el servei de segellat de temps o timestamp service (TSS) proporcionat per l'Autoritat de Certificació de la Comunitat Valenciana (ACCV), ens prestador de Serveis de Certificació Electrònica de la Comunitat Valenciana, constituït mitjançant la Llei 14/2005, de 23 de desembre, de la Generalitat.

Aquest servei proporciona un sistema que assegura que unes dades existeixen i no han sigut modificades des d'una data i hora concretes. Això s'aconsegueix associant les dades a l'instant exacte de temps mitjançant la signatura electrònica de la nostra Autoritat de Segellament de Temps (TSA). El resultat és el que es coneix com a segell de temps electrònic, timestamp o marca de temps.

La signatura de llarga durada PAdES-LTV (Long Term Validation of digital signatures) permet validar la integritat i autenticitat del document al llarg dels anys. És a dir, possibilita que la verificació de la signatura perdure en el temps. Dit d'una altra forma, aporta a la signatura electrònica validesa al llarg del temps. A nivell tecnològic, en el càlcul

*Artículo 13. Referencia temporal de los documentos administrativos electrónicos*

La posibilidad de emitir válidamente por medios electrónicos los documentos administrativos, viene descrita en la Ley 39/2015 que indica que, además de la firma electrónica, deben incluir una referencia temporal cuando la naturaleza del documento así lo requiera.

Por tanto, la Universitat de València deberá asociar a los documentos administrativos electrónicos una de las siguientes modalidades de referencia temporal, de acuerdo con lo que determinen las normas reguladoras de los respectivos procedimientos:

a) Marca de tiempo: entendiendo por tal la asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico. La marca de tiempo será utilizada en todos aquellos casos en los que las normas reguladoras no establezcan la utilización de un sello electrónico cualificado de tiempo.

b) Sello electrónico cualificado de tiempo: entendiendo por tal la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador cualificado de servicios de confianza que asegure la exactitud e integridad de la marca de tiempo del documento. Los sellos electrónicos de tiempo no cualificados serán asimilables a todos los efectos a las marcas de tiempo.

En todo caso, será la norma que regule el procedimiento dónde constarán los documentos electrónicos la que indique la conveniència de usar marca o sello de tiempo, pues la Ley 39/2015 exige en general una referencia temporal del momento en que han sido emitidos para considerar un documento administrativo válido, pero no exige la fehaència que otorga un sello de tiempo.

El Esquema Nacional de Seguridad distingue tres tipos de sistemas de información en función de sus criticidad y nivel de seguridad exigible (Alta, Media y Básica), siendo obligado el uso de sellado de tiempo únicamente para los sistemas categorizados como nivel Alto. Sin perjuicio de lo anterior, se empleará sellado de tiempo en aquellos supuestos en los que la información sea susceptible de ser utilizada como evidencia electrónica en un futuro.

La información relativa a las marcas y sellos electrónicos cualificados de tiempo se asociará a los documentos electrónicos en la forma que determine el Esquema Nacional de Interoperabilidad y normativa correspondiente.

*Artículo 14. Sellado de tiempo y firma electrónica*

El sellado de tiempo es un método para probar que un conjunto de datos existió antes de un momento dado y que ninguno de estos datos ha sido modificado desde entonces. Incluir un sello de tiempo en una firma digital es un medio de tener una evidencia del instante en el que el documento se ha firmado, otorgándole a este medios adicionales para garantizar la propiedad y no repudio.

El sellado de tiempo proporciona un valor añadido a la utilización de firma digital, ya que la firma por sí sola no suministra ninguna información acerca del momento de creación de la firma, y en el caso de que el firmante la incluyese, esta habría sido proporcionada por una de las partes, cuando lo recomendable es que lo sea por una tercera parte de confianza.

La relación de prestadores cualificados de servicios de confianza que prestan servicios de sellado de tiempo en el sector público deberá estar incluida en la «Lista de confianza de prestadores cualificados de servicios de confianza».

La Universitat de València utiliza el servicio de sellado de tiempo o timestamp service (TSS) proporcionado por la Autoridad de Certificación de la Comunidad Valenciana (ACCV), ente prestador de Servicios de Certificación Electrònica de la Comunidad Valenciana, constituido mediante la Ley 14/2005, de 23 de diciembre, de la Generalitat.

Este servicio proporciona un sistema que asegura que unos datos existen y no han sido modificados desde una fecha y hora concretes. Esto se consigue asociando los datos al instante exacto de tiempo mediante la firma electrónica de nuestra Autoridad de Sellado de Tiempo (TSA). El resultado es lo que se conoce como sello de tiempo electrónico, timestamp o marca de hora.

La firma de larga duración PAdES-LTV (Long Term Validation of digital signatures) permitirá validar la integridad y autenticidad del documento a lo largo de los años. Es decir, posibilidad que la verificación de la firma perdure en el tiempo. Dicho de otra forma, aporta a la firma electrónica validez a lo largo del tiempo. A nivel tecnològic, en el càlcul



de l'algorisme de signatura electrònica s'incrusten dues informacions fonamentals:

a) La validació de l'estat de revocació del certificat en el moment de la signatura: s'accedeix a la consulta OCSP i l'Autoritat de Certificació ens diu si aquest certificat digital està caducat o revocat.

b) El segell de temps, o Timestamp, mitjançant el qual un tercer de confiança ens diu l'hora exacta del moment de la signatura.

D'aquesta forma, s'incorporen en el moment signar els certificats de la cadena de confiança i el resultat de la comprovació de validesa d'aquests.

#### *Article 15. Signatura electrònica longeva*

Amb l'ús de la signatura electrònica bàsica, si el certificat està caducat, automàticament es dona la signatura com a no vàlida. Quan la fiabilitat de les signatures electròniques no es puga assegurar per mitjans tècnics, es procedirà a la convalidació de documents, amb l'annexió d'una nova signatura del responsable jeràrquic de l'ens productor del document o responsable de la fe pública, la qual cosa suposa una garantia d'autenticitat i integritat dels documents que es convaliden, però no certificaria la validesa legal o competencial dels actes que se'n deriven.

Per això s'utilitzen les signatures longeves i el segell de temps. Les signatures longeves afegien a la signatura informació addicional i evidències de tercers (autoritats de certificació), així com certificacions de temps que en garanteixen la validesa a llarg termini, ja que realment «certifiquen» quin era l'estat del certificat en el moment de l'operació, amb independència del període de validesa del certificat.

Segons s'indica en la Resolució de 27 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, que aprova la Norma Tècnica d'Interoperabilitat de Política de Signatura i Segell Electrònic i de Certificats de l'Administració (IV.3 Regles de confiança per a signatures longeves), en el cas de signatures longeves, el signant o el verificador de la signatura ha d'incloure un segell de temps que permeta garantir que el certificat era vàlid en el moment en què es va realitzar la signatura. En el cas que siga inclosa pel signant, es podrà realitzar una vegada haja transcorregut el període de precaució o període de gràcia, anomenat al temps d'espera per a comprovar l'estat de revocació d'un certificat.

Atès que eines informàtiques per a la signatura de documents electrònics com Adobe Acrobat generen «per defecte» documents signats amb signatura electrònica bàsica, és molt poc recomanable utilitzar-les per a la signatura de documentació la utilitat de la qual no siga de curt termini (notificacions o oficis amb abast d'un curs acadèmic). Per aquest motiu, tota la documentació generada per la seu electrònica de la UV inclou signatura electrònica longeva, ja siga amb segell d'òrgan en els procediments o signatura del personal en el Portafirmes.

En principi s'utilitzarà l'eina informàtica Adobe Acrobat perquè es garantisca que els documents signats electrònicament es generen en format PDF longeu (tècnicament denominat 'PADES-LTV').

#### *Article 16. Formats de signatura admesos*

La Universitat de València empra els formats admesos en la Política de signatura electrònica i de certificats de l'Administració General de l'Estat segons els següents criteris:

a) L'ús preferent de la signatura electrònica amb format XAdES-T per a tots els documents generats per actuacions administratives automatitzades i per a tots els documents generats pel personal de l'administració excepte restriccions de format o per la utilització d'altres estàndards d'interoperabilitat ja establerts.

b) L'ús obligatori del format PDF amb signatura electrònica PADES per a totes les còpies de documents (amb canvi de format) que tinguen com a destinataris a ciutadans o altres administracions públiques, excepte restriccions de format o per la utilització d'altres estàndards d'interoperabilitat ja establerts.

c) L'ús del format CADES només en aquells supòsits en els quals aspectes relacionats amb el volum dels fitxers o el rendiment dels sistemes que els gestionen desaconsellen l'ús dels formats PADES i XAdES.

culo del algoritmo de firma electrónica, se incrustan dos informaciones fundamentales:

a) La validación del estado de revocación del certificado en el momento de la firma: se accede a la consulta OCSP y la Autoridad de Certificación nos dice si este certificado digital está caducado o revocado.

b) El sello de tiempo, o TimeStamp, mediante el que un tercero de confianza nos dice la hora exacta del momento de la firma.

De esta forma, se incorporan en el momento firmar los certificados de la cadena de confianza y el resultado de la comprobación de validez de los mismos.

#### *Artículo 15. Firma electrónica longeva*

Con el uso de la firma electrónica básica, si el certificado está caducado, automáticamente se da la firma como no válida. Cuando la fiabilidad de las firmas electrónicas no se pueda asegurar por medios técnicos, se procederá a la convalidación de documentos, con la anexión de una nueva firma del responsable jerárquico del ente productor del documento o responsable de la fe pública, lo que supone una garantía de autenticidad e integridad de los documentos que se convalidan, pero no certificaría la validez legal o competencial de los actos que de estos se deriven.

Por ello se utilizan las firmas longevas y el sello de tiempo. Las firmas longevas añaden a la firma información adicional y evidencias de terceros (autoridades de certificación); así como certificaciones de tiempo que garantizan su validez a largo plazo, puesto que realmente «certifican» cuál era el estado del certificado en el momento de la operación, con independencia del período de validez del certificado.

Conforme se indica en la Resolució de 27 de octubre de 2016, de la Secretaria de Estado de Administraciones Públicas, que aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónico y de Certificados de la Administración (IV.3 Reglas de confianza para firmas longevas), en el caso de firmas longevas, el firmante o el verificador de la firma incluirá un sello de tiempo que permita garantizar que el certificado era válido en el momento en que se realizó la firma. En el caso de que sea incluida por el firmante, se podrá realizar una vez haya transcurrido el periodo de precaución o periodo de gracia, llamado al tiempo de espera para comprobar el estado de revocación de un certificado.

Dado que herramientas informáticas para la firma de documentos electrónicos como Adobe Acrobat generan «por defecto» documentos firmados con firma electrónica básica, es muy poco recomendable la utilización de las mismas para la firma de documentación cuya utilidad no sea a corto plazo (notificaciones u oficios con alcance de un curso académico). Por este motivo toda la documentación generada por la Sede Electrónica de la UV incluye firma electrónica longeva, ya sea con sello de órgano en los procedimientos o firma del personal en el Portafirmes.

En principio se utilizará la herramienta informática Adobe Acrobat para que se garantice que los documentos firmados electrónicamente se generen en formato PDF longevo (técnicamente denominado 'PADES-LTV').

#### *Artículo 16. Formatos de firma admitidos*

La Universitat de València emprarà els formats admitidos en la Política de firma electrònica i de certificats de la Administración General del Estado según los siguientes criterios:

a) El uso preferente de la signatura electrònica amb format XAdES-T para todos los documentos generados por actuaciones administrativas automatizadas y para todos los documentos generados por el personal de la administración salvo restricciones de formato o por la utilización de otros estándares de interoperabilidad ya establecidos.

b) El uso obligatorio del formato PDF con firma electrònica PADES para todas las copias de documentos (con cambio de formato) que tengan como destinatarios a ciudadanos u otras administraciones públicas, salvo restricciones de formato o por la utilización de otros estándares de interoperabilidad ya establecidos.

c) El uso del formato CADES solo en aquellos supuestos en los que aspectos relacionados con el volumen de los ficheros o el rendimiento de los sistemas que los gestionan desaconsejen el uso de los formatos PADES y XAdES.



d) En el cas de signatura amb claus concertades, s'admet la seua realització mitjançant certificats generats a l'usuari en el moment de la signatura, amb un sistema que emmagatzeme tal signatura i la part pública del certificat generat i que permeta la seua posterior verificació mitjançant CSV.

Les signatures dels documents amb rellevància externa han de ser prou completes perquè la ciutadania les puga validar sense mitjans que els resulten especialment onerosos o que siguen particularment sofisticats.

*Article 17. Algorismes de signatura*

S'empraran algorismes acreditats pel Centre Criptològic Nacional segons la guia CCN-STIC 807.

*Article 18. Entrada en vigor*

La present Política de Signatura i Segell Electrònic i de Certificats de la Universitat de València entrarà en vigor l'endemà de la seua publicació en el *Diari Oficial de la Generalitat Valenciana*.

València, 11 de juliol de 2023.– La rectora: Maria Vicenta Mestre Escrivá.

d) En el caso de firma con claves concertadas se admite su realización mediante certificados generados al usuario en el momento de la firma, con un sistema que almacene tal firma y la parte pública del certificado generado y que permita su posterior verificación mediante CSV.

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

*Artículo 17. Algoritmos de firma*

Se emplearán algoritmos acreditados por el Centro Criptológico Nacional según la guía CCN-STIC 807.

*Artículo 18. Entrada en vigor*

La presente Política de Firma y Sello Electrónicos y de Certificados de la Universitat de València entrará en vigor al día siguiente de su publicación en el *Diari Oficial de la Generalitat Valenciana*.

València, 11 de julio de 2023.– La rectora: Maria Vicenta Mestre Escrivá.