

Política de Signatura Electrònica de la Universitat Oberta de Catalunya

Text aprovat pel Comitè de Direcció Executiu el 5 de maig de 2014, actuant per delegació del Consell de Govern

SUMARI

I. Introducció	3
1. Identificació de la política general de signatura electrònica	4
2. Data D'emissió de la política general de signatura electrònica	4
3. Identificació de l'emissor de la política general de signatura electrònica	4
4. Àmbit d'aplicació de la política general de signatura electrònica	4
II. Normes generals en relació amb la tipologia d'actes	4
III. Tipologia de certificats a emprar	5
IV. Relació entre la signatura i el document signat	5
V. Format de la signatura	6
VI. Perfil de la signatura	6
VII. Processos en relació amb la signatura electrònica	7
VIII. Organització i desenvolupament de la política general	8

I. Introducció

Aquest document conté les normes de signatura electrònica en relació amb els documents de procediments acadèmics i de gestió electrònics de la Universitat Oberta de Catalunya.

La naturalesa de la UOC, el servei que presta i la necessitat que té d'interoperar amb altres universitats i l'administració universitària del Govern de la Generalitat de Catalunya, fan que aquest document hagi de resultar conforme amb els requisits de seguretat i proporcionalitat corresponents als sistemes electrònics de suport a procediments, establerts per les normes:

- Llei 1/2003, de 19 de febrer, de Universitats de Catalunya.
- Llei Orgànica 6/2001, de 21 de desembre, de Universitats.
- Llei 3/1995, de 6 d'abril, de reconeixement de la Universitat Oberta de Catalunya.
- Acord GOV/140/2010, de 3 d'agost, pel qual s'aproven les Normes d'organització i funcionament de la Universitat Oberta de Catalunya.
- Llei 11/2007, d'11 de juny, d'accés electrònic dels ciutadans als serveis públics (LAECSP).
- Llei 26/2010, de 3 d'agost, de règim jurídic i procediment de les administracions públiques de Catalunya (LRPJCAT).
- Llei 29/2010, de 3 d'agost, d'ús dels mitjans electrònics al sector públic de Catalunya (LUMESPC).
- Reial Decret 3/2010, de 8 de gener, pel que es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica.
- Reial Decret 4/2010, de 8 de gener, pel que es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica.
- Reial Decret Legislatiu 3/2011, de 14 de novembre, pel qual s'aprova el text refós de la Llei de Contractes del Sector Públic.
- Llei 25/2013, de 27 de desembre, d'impuls de la factura electrònica i creació del registre comptable de factures en el Sector Públic.

Cal entendre doncs aquest document com una política de signatura electrònica d'acord amb l'article 18.2 del Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració electrònica, i ha estat produïda d'acord amb els requisits de la Norma Tècnica de Interoperabilitat "política de signatura electrònica i de certificats de l'Administració".

Els continguts d'aquesta política general de signatura electrònica s'han estructurat per cobrir els controls que preveu la norma internacional ISO/IEC 27002:2006 – Tecnologia de la Informació: Tècniques de seguretat: Codi de pràctiques per a la gestió de la seguretat de la informació, en especial la secció 15.1.3. Continguts generals de la política general de signatura electrònica

1.1. Identificació de la política de signatura electrònica

Aquesta Política general de signatura electrònica s'identificarà amb un identificador d'objecte (OID) número: 1.3.6.1.4.1.43653.1.5.

1.2. Data d'emissió de la política general de signatura electrònica

Aquesta política general de signatura electrònica ha estat emesa en data 28 d'abril de 2014, moment a partir del qual entrarà en el que entrarà en vigor.

1.3. Identificació de l'emissor de la política general de signatura electrònica

Aquesta política general de signatura electrònica ha estat emesa per Comitè de Direcció Executiu, actuant per delegació del Consell de Govern d'acord amb allò establert en l'article 13.2 de les NOF (Acord GOV /140/2010, de 3 d'agost), l'article 4 del reglament del Consell de Govern i l'Acord de Consell de Govern de 15/7/13.

1.4. Àmbit d'aplicació de la política general de signatura electrònica

Aquesta política general resulta aplicable a tots els sistemes d'informació de suport a procediments i activitats acadèmics i de gestió electrònics, així como a les relacions per mitjans electrònics amb tercers que no formen part de la comunitat universitària.

Aquesta política general també resulta aplicable a la signatura de manifestacions de documents i expedients en el moment del seu intercanvi amb entitats diferents d'aquesta Universitat, en particular d'acord amb allò establert pel Reial Decret 4/2010, Esquema Nacional d'Interoperabilitat.

II. Normes generals en relació amb la tipologia d'acte

La Universitat Oberta de Catalunya ha d'establir estàndards per a la signatura dels diferents tipus d'actes jurídics documentats.

Els actes realitzats pels òrgans s'han de documentar, bé en un document ofimàtic o llibre-registre electrònic de forma autenticada preferentment amb signatura electrònica avançada basada en certificat reconegut de persona física (en cas d'actuació manual) o de persona jurídica (en cas d'actuació automatitzada), per tractar-se, en general, d'actius la categoria de seguretat dels quals en les dimensions d'integritat i autenticitat és de nivell mig.

Els actes que es considerin de nivell alt s'han d'autenticar necessàriament utilitzant sistemes de signatura electrònica reconeguda (en cas d'actuació manual) o de persona jurídica (en cas d'actuació automatitzada), en ambdós casos amb utilització preferentment de dispositius certificats.

En cap cas es podrà utilitzar exclusivament un codi segur de verificació per a la generació de documents originals.

La resta d'actes es poden documentar amb qualsevol sistema de signatura electrònica i, en concret, generar entrades en registres electrònics d'activitat sempre que la persona s'hagi autenticat amb certificat electrònic reconegut, o amb un mecanisme que proporcioni garantia equivalent

En particular, pels actes en els respectius processos acadèmics i de gestió dels estudiants, professorat i del personal docent col·laborador com el de signatura d'actes, entrega d'informació,... es podran realitzar aquests amb els sistemes d'autenticació basats en signatura i contrasenya proporcionats per la Universitat Oberta de Catalunya un cop avaluada la conveniència i analitzats els riscos.

Els actes d'intercanvi de dades amb les Administracions Públiques, o l'accés a les dades de les mateixes, exigirà el nivell mínim establert per cada Administració que cedeix dades o dona accés a dades.

La signatura electrònica dels actes de contractació pública i de facturació electrònics serà la que vingui determinada per la normativa que li sigui d'aplicació.

En tots els casos, s'han d'emprar algorismes aprovats en la política de seguretat criptogràfica.

III. Tipologia de certificats a emprar

En el cas de signatura basada en certificats, els certificats a emprar han de ser, en general, els següents:

- Actuació de la Universitat Oberta de Catalunya qualificada com nivell alt:
 - Actuació manual: Tots els certificats de persona física admesos per aquest ús d'acord amb la política general de certificació de la Universitat Oberta de Catalunya, de nivell 4.
 - Actuació automàtica: Tots els certificats de persona jurídica admesos per aquest ús d'acord amb la política general de certificació de la Universitat Oberta de Catalunya, de nivell 4.
- Resta d'actuacions de la Universitat Oberta de Catalunya:
 - Actuació manual: Tots els certificats de persona física admesos per aquest ús d'acord amb la política general de certificació de la Universitat Oberta de Catalunya, de nivell 3 o superior.
 - Actuació automàtica: Tots els certificats de persona jurídica admesos per aquest ús d'acord amb la política general de certificació de la Universitat Oberta de Catalunya, de nivell 3 o superior.
- Actuació de la Universitat Oberta de Catalunya en l'expedició de factures:
 - Alternativament es pot fer un servei de segell d'entitat d'acord amb el que disposa la Llei 25/2013.
- Actuació d'intercanvi de dades o accés a dades amb les Administracions:
 - Els certificats admesos per cada Administració que cedeix o dona accés a dades a la Universitat Oberta de Catalunya.
- Actuació dels estudiants i del ciutadans:
 - El certificat de signatura electrònica incorporat al DNI electrònic.
 - Tots els certificats admesos per aquest ús d'acord amb la política general de certificació de la Universitat Oberta de Catalunya, de nivell 3 o superior.

IV. Relació entre la signatura i el document signat

El format de la signatura ha de ser, sempre que sigui possible, independent del format del document o registre signat, amb l'objectiu de reduir al màxim la dependència entre tots dos objectes de negoci.

En relació amb els documents originals que hagin de restar en poder de la universitat (exemple: resolucions, actes, informes) s'han de produir amb signatura independent del document, evitant l'ús de signatures embolcallades a formats documentals. La relació entre el document signat i la signatura s'ha d'establir mitjançant l'ús de metadades del document.

Quan calgui lliurar a tercers aquests documents, s'ha de crear una còpia autèntica electrònica, en un format adient al destinatari, que serà signada o segellada electrònicament, embolcallant la signatura o segell en el format documental.

Com a excepció, els documents originals a lliurar al ciutadà (estudiant, proveïdor,...) com per exemple una certificació o una notificació, han d'incloure la signatura embolcallada al propi format documental (exemple: un fitxer PDF signat o segellat). Es recomana que, addicionalment, els documents incorporin un codi de verificació electrònica, que permeti la seva consulta en línia i la impressió en concepte de còpia autèntica.

En relació amb els actes d'intercanvi de dades o accés a dades entre Administracions, la relació entre la signatura electrònica i el document signat serà típicament establerta per cada Administració que cedeix dades o dona accés a dades, sense perjudici d'establir aquestes condicions per conveni.

Respecte als documents ofimàtics, signats o no, que puguin presentar els ciutadans acompanyant a la sol·licitud administrativa, no se'ls hi pot aplicar la política de signatura electrònica pròpia de la Universitat Oberta de Catalunya, ja que són documents previs, que no han estat creats específicament pel ciutadà (estudiant, proveïdor,...) per a la seva relació jurídica amb la Universitat.

En qualsevol cas, s'han d'acceptar – i poder validar – les signatures dels documents ofimàtics que es determinin a l'Esquema Nacional d'Interoperabilitat i a l'Esquema Nacional de Seguretat.

Es recomana protegir aquests documents, en tot cas, amb la signatura electrònica de la sol·licitud (exemple: mitjançant la inclusió dels resums criptogràfics dels documents en camps ocults del formulari a signar). D'aquesta forma, sempre existeix una prova dels documents que es van lliurar a la Universitat Oberta de Catalunya, amb independència de la validesa de la signatura dels documents, o fins i tot de que estiguin signats o no.

V. Format de la signatura

En general, el format de la signatura depèn del format del document a signar (exemple: PDF exigeix signar d'acord amb CMS, ODF exigeix signar d'acord amb una variant d'XML Digital Signature).

La Universitat Oberta de Catalunya utilitza de forma indistinta els formats de signatura XAdES, CAdES, o PAdES, en funció de la sintaxi corresponent a les dades a signar, sempre i quan el format del document o el protocol corresponent permeti la utilització dels mateixos.

Les normes concretes en relació amb la signatura electrònica de cada format documental s'han d'establir en els corresponents estàndards tècnics de signatura electrònica de format documental.

VI. Perfil de la signatura

Les signatures dels documents amb rellevància externa han de ser suficientment completes perquè els ciutadans les puguin validar sense mitjans que els resultin especialment gravosos o que siguin particularment sofisticats.

La Universitat ha de produir signatures electròniques de classe EPES explícit, on l'OID de la política de signatura coincideixi amb l'estàndard tècnic de signatura electrònica d'acte jurídic aplicable, sempre que sigui tècnicament possible.

En general s'ha d'utilitzar el perfil AdES-T-LT d'acord amb ETSI TS 103 171 (XAdES Baseline Profile), TS 103 173 (CAdES Baseline Profile), o ETSI TS 103 172 (PAdES Baseline Profile), per a tota signatura electrònica d'un document entregat, essent recomanable utilitzar aquest perfil per a tots els documents de la Universitat.

Les signatures de la resta d'actes poden ser més bàsiques, ja que la Universitat Oberta de Catalunya pot establir controls addicionals que evitin la necessitat de completar la signatura electrònica. En general, es recomana segellar la signatura electrònica, emprant el perfil AdES-T.

Les signatures dels actes d'intercanvi o l'accés a dades de dades amb les Administracions Públiques s'han d'ajustar al perfil que determini cada Administració que cedeix o dona accés a dades.

Les signatures dels actes dels ciutadans poden ser bàsiques, ja que la Universitat Oberta de Catalunya disposa dels mecanismes per validar i completar la signatura electrònica. En general, la Universitat ha d'admetre documents externs amb signatura electrònica de perfil AdES-EPES amb política implícita, i ha de verificar les signatures conforme amb el perfil AdES-EPES amb política explícita, sempre que la mateixa sigui conforme amb allò establert en els articles 18 i següents del Reial Decret 4/2010.

En general, la Universitat Oberta de Catalunya ha de completar la signatura dels ciutadans d'acord amb el perfil T-LT, o mecanisme de repositori segur equivalent.

En relació amb la custòdia a llarg termini de les signatures dels documents, la Universitat Oberta de Catalunya garantirà en els casos que resulti necessari tant la conservació dels documents com de les seves signatures i les metadades. A l'efecte es poden emprar els següents mètodes:

- Completat de les evidències electròniques mitjançant la utilització de formats AdES-LTA.
- Tècniques de gestió segura de registres per a garantir la longevitat dels documents interns.

La conservació de la signatura electrònica associada a document electrònic obeeirà als terminis legals i a les polítiques de conservació de documents prenent com a referència l'ENI.

VII. Processos en relació amb la signatura electrònica

S'han d'implantar els següents processos en relació amb la signatura electrònica:

- Procés de creació de la signatura electrònica:
 - Consisteix en la successió de passes necessàries per obtenir una signatura digital per a un tipus de contingut concret. Inclou la possibilitat de seleccionar i visualitzar continguts i atributs de signatura, efectuar fluxos de signatura i veure l'estat d'una signatura realitzada.
- Procés de validació inicial de la signatura electrònica:
 - Consisteix en la successió de passes necessàries per verificar una signatura digital per a un tipus de contingut concret, en el moment de la seva recepció. Es tracta d'una verificació parcial, ja que, normalment, a la recepció d'una signatura electrònica no es pot determinar l'estat actual de revocació d'un certificat (degut a que la informació de revocació es publica amb un dia d'endarreriment). Aquesta verificació no incorpora, per exemple, un segell de data i hora a la signatura, ni la completa.
 - Aquest procés s'ha de basar en l'ús del servei de validació de la Universitat Oberta de Catalunya, el qual podrà delegar part del procés de verificació (a serveis com el servei Validador (PSIS) del Consorci AOC).
- Procés de validació definitiva de la signatura electrònica.

- Consisteix en la successió de passes necessàries per verificar una signatura digital per a un tipus de contingut concret, de forma definitiva. Es tracta d'una verificació definitiva, en un moment en que ja es pot determinar l'estat definitiu de revocació d'un certificat (normalment al menys un dia després de la recepció de la signatura). Aquesta verificació, quan resulta apropiat, incorpora un segell de data i hora a la signatura electrònica, o la completa amb les dades necessàries per gaudir d'evidència electrònica.
 - Aquest procés s'ha de basar en l'ús de la plataforma de validació de la Universitat Oberta de Catalunya, , el qual podrà delegar part del procés de verificació (a serveis com el servei Validador (PSIS) del Consorci AOC).
- Procés de manteniment de la validesa de la signatura electrònica.
- Consisteix en la successió de passes necessàries per mantenir al llarg del temps la validesa d'una signatura digital per a un tipus de contingut concret, en el moment de la seva recepció. Es tracta d'un procés d'addició de garanties criptogràfiques addicionals (típicament, informacions addicionals i segells de data i hora) que permeten acreditar la producció d'una signatura en un moment concret del temps, fins i tot en cas de ruptura o obsolescència matemàtica dels algorismes de signatura electrònica.

Aquest procés s'ha de basar en l'ús de la plataforma de validació de la Universitat Oberta de Catalunya, la qual podrà delegar part del procés de verificació al servei Validador (PSIS) del Consorci AOC o altres.

VIII. Organització i desenvolupament de la política general

Correspon l'aprovació de la política de signatura electrònica al Consell de Govern de la Universitat Oberta de Catalunya, essent responsable de la mateixa la Secretaria General.

Aquesta política general s'ha de desenvolupar mitjançant els següents instruments:

- Estàndards tècnics de signatura electrònica d'actes.
- Estàndards tècnics de signatura electrònica de formats documentals.
- Guies i recomanacions de signatura electrònica.
- Procediments operatius de signatura electrònica.

Correspon a l'àrea de responsable de les tecnologies i el sistemes d'informació de la Universitat Oberta de Catalunya, el desenvolupament de la Política de signatura electrònica per mitjà dels instruments indicats.