POLÍTICA DE SIGNATURA ELECTRÒNICA I CERTIFICATS DE LA UNIVERSITAT ROVIRA I VIRGILI

Aprovada en Consell de Govern el 27 de juliol de 2020

ÍNDEX

1. INTRODUCCIÓ

La Universitat Rovira i Virgili ha de seguir unes directrius sobre l'ús de la signatura electrònica en les aplicacions corporatives per garantir l'autenticitat, integritat i conservació dels documents signats digitalment.

La implantació d'un model de signatura electrònica requereix definir quins seran els certificats digitals admesos, utilitzats i per a quins usos, així com el cicle de vida que tindran.

D'altra banda, l'evolució de la tecnologia, però sobretot de la normativa, ha originat l'aparició d'altres sistemes que permeten la signatura electrònica a través de mecanismes com les claus concertades, el codi segur de verificació i la signatura biomètrica. La Universitat considera que és important utilitzar-los i en aquest document se'n regula l'ús.

Per tant, la política regula, d'una banda, la signatura electrònica basada en claus concertades, les quals es fonamentaran en l'usuari i contrasenya que l'estudiantat, PDI i PAS ja tenen, proporcionats per la mateixa Universitat, i addicionalment en el sistema que permetrà recollir les evidències de voluntat de signatura. D'altra banda, també es permetrà la generació de signatures electròniques basada en identitats del sistema UNIFICAT, més les mateixes evidències de voluntat de signatura. Finalment també es preveu utilitzar la plataforma VALid del Consorci AOC, amb les identitats acceptades per aquesta plataforma i les seves evidències de voluntat de signatura proporcionades per aquesta, com a sistema de signatura electrònica.

De la seva banda, la signatura a través de la generació del codi segur de verificació (CSV) s'emprarà per signar automàticament determinats documents.

Així mateix, aquesta política també descriu la signatura digital biomètrica, que s'utilitzarà per signar documents electrònics generats presencialment davant d'un tercer.

Al document s'ha d'especificar quins són els tipus de signatura que s'han d'utilitzar a l'hora de signar els documents electrònics generats i gestionats per la Universitat, i per aquesta raó s'hi inclou tant una relació de formats utilitzats com tipus de signatura generats o acceptats per la Universitat.

Finalment, s'estableixen les estratègies que la Universitat Rovira i Virgili implementarà per preservar les signatures electròniques a llarg termini.

Cal assenyalar que en aquest document s'utilitzen indistintament els termes signatura digital i signatura electrònica, ja que corresponen al mateix concepte.

Per redactar aquest document s'ha tingut en compte la normativa aplicable en la matèria tan estatal com supranacional. Especialment, es destaca el que l'Esquema Nacional d'Interoperabilitat estableix i, molt concretament, el que es defineix en la Norma tècnica d'interoperabilitat de política de signatura electrònica i de certificats digitals de l'Administració, així com la de l'expedient electrònic pel que fa a la signatura electrònica dels expedients. A més, s'han considerat com a marc d'elaboració d'aquesta política els estàndards internacionals i altres convencions en l'àmbit de la signatura electrònica.

El detall de la normativa i estàndards internacionals de referència es pot trobar a l'annex III.

2. OBJECTE DE LA POLÍTICA DE SIGNATURA ELECTRÒNICA I DE CERTIFICATS

Aquesta política té per objecte establir el conjunt de criteris comuns assumits per la Universitat, pel que fa a l'autenticació, l'ús i el reconeixement de signatures electròniques basades en certificats digitals, codi segur de verificació i evidències electròniques.

3. DADES DE LA POLÍTICA DE SIGNATURA ELECTRÒNICA I DE CERTIFICATS

3.1. IDENTIFICACIÓ DE LA POLÍTICA

Les dades identificatives de la política són els que s'inclouen a continuació:

Nom de el document	Política de signatura electrònica i de certificats de la Universitat Rovira i Virgili
Versió	1.0
Identificador de la Política	1.3.6.1.4.1.11188.2.2.2 Polítiques de certificació i CPSs
URL de referència de la política	S'inclourà en l'apartat de normativa de la seu electrònica: https://seuelectronica.urv.cat/normativa.html

Data d'aprovació	Acord de Consell de Govern de 27 de juliol de 2020
Àmbit d'aplicació	Documents i expedients produïts i/o custodiats per la Universitat.
Responsable de la política	Secretaria General

3.2. PERÍODES DE VALIDESA I TRANSICIÓ

Aquesta política entra en vigor en la data d'aprovació i serà vàlida fins que no sigui substituïda o derogada per una altra política posterior.

3.3. GESTIÓ DE LA POLÍTICA DE SIGNATURA ELECTRÒNICA I DE CERTIFICATS

El manteniment, actualització i publicació electrònica d'aquesta política correspon a la Secretaria General de la Universitat. Els canvis a la política s'han de consensuar amb les parts implicades, així com el període de temps transitori per adaptar-hi les plataformes.

La Secretaria General és responsable de garantir que a la seu electrònica de la Universitat hi estigui dipositada tant la versió actualitzada de la política com l'accés a versions anteriors del document, perquè es puguin verificar les signatures electròniques realitzades en el marc d'una política anterior a la vigent.

4. CONCEPTES

Casos d'ús de la signatura electrònica: són entesos com els escenaris possibles de generació de documents electrònics signats. Per a cada cas d'ús, s'han d'identificar els formats de signatura electrònica, els possibles nivells de signatura, etc.

Classes de signatura electrònica: segons es defineix en la Llei 59/2003, diferents tipus de validesa jurídica de la signatura electrònica: signatura simple, avançada i reconeguda.

Format de signatura electrònica: forma en què es codifiquen les signatures electròniques. Els formats més utilitzats són S / MIME, CMS, XAdES, CAdES i PAdES.

Nivell de signatura: amb aquest nom definim si el document té una única signatura o diverses, i en aquest cas si es generen en paral·lel o niades.

Segell de temps: acreditació, a càrrec d'un tercer de confiança, de la data i hora de realització de qualsevol operació o transacció per mitjans electrònics.

Sistema de signatura: forma en què se signa un document electrònic, mitjançant un certificat digital del signant, amb un sistema d'identificació més evidència electrònica de l'acte de la signatura, amb signatura biomètrica o mitjançant codi segur de verificació (CSV).

Tipus de signatura: forma com es relaciona la signatura electrònica amb el document signat: dins el mateix document, com un document a part, dins d'estructures XML, etc.

5. ACTORS INVOLUCRATS

Els actors involucrats en el procés de creació i validació d'una signatura electrònica són els següents:

a) *Signant:* persona que posseeix un dispositiu per crear una signatura i actua en nom propi o en nom d'una persona física o jurídica.

b) *Creador d'un segell:* persona jurídica que crea un segell electrònic.

c) *Verificador:* entitat, tant si es tracta d'una persona física com jurídica, que valida o verifica una signatura electrònica basant-se en les condicions exigides per la política per la qual es regeix la plataforma de relació electrònica o el servei concret que es demana. Podrà ser una entitat de validació de confiança o una tercera part que estigui interessada en la validesa d'una signatura electrònica.

d) *Prestador de serveis de signatura electrònica:* persona física o jurídica que expedeix certificats electrònics o presta altres serveis relacionats amb la signatura electrònica.

e) *Emissor i gestor de la política de signatura electrònica i de certificats:* entitat que s'encarrega de generar i gestionar el document de la política, que regirà les actuacions del signant, el verificador i els prestadors de serveis, en els processos de generació i validació de signatura electrònica. En el cas de la URV, és la mateixa Universitat.

En aquest document el terme signant tant es refereix a la persona que signa com al creador d'un segell. En el segon dels casos, es pot tractar d'un procés d'actuació administrativa automatitzada.

6. US DE CERTIFICATS I ALTRES IDENTITATS DIGITALS

6.1 CERTIFICATS DIGITALS ADMESOS PER LA UNIVERSITAT PER A LA IDENTIFICACIÓ I SIGNATURA DE TERCERS

Tal com estableixen els articles 9 i 10 de la Llei 39/2015, la Universitat té l'obligació d'admetre tots els certificats digitals inclosos en la llista de confiança de prestadors qualificats de serveis electrònics de confiança (TSL) del Ministeri d'Indústria, Comerç i Turisme.

D'aquesta manera, les persones que es relacionen amb la Universitat podran utilitzar els certificats relacionats en la llista de confiança per identificar-se en les diferents actuacions en què intervinguin, així com per signar electrònicament documentació en suport digital.

La Universitat, basant-se en el nivell de seguretat de cada procediment administratiu, així com en el paper amb el qual actuï el titular d'aquesta identitat digital, podrà decidir en quins procediments s'haurà d'utilitzar només el certificat digital.

6.2. ALTRES IDENTITATS DIGITALS ADMESES PER LA UNIVERSITAT PER A LA IDENTIFICACIÓ I SIGNATURA ELECTRÒNICA DE TERCERS

En virtut de l'article, 9.2 de la Llei 39/2015, la Universitat admet, com a sistema d'identificació electrònica, el sistema de clau concertada.

Aquest sistema es fonamenta en l'existència d'un registre previ com a usuari, que permet garantir la identitat i assegurar que el sistema d'identificació es lliura al titular.

La comunitat universitària disposa en aquests moments d'usuaris i contrasenyes emesos per la mateixa Universitat (sistema de clau concertada). Aquests usuaris i contrasenyes són utilitzats com a sistemes d'identificació i autenticació, i també per signar electrònicament. Per a això es requereix que les evidències electròniques generades continguin la informació suficient per demostrar les accions que han tingut lloc en el sistema, que es relacionin entre si i es completin amb la signatura dels segells electrònics de la Universitat.

D'aquesta manera, en el moment que un estudiant o una persona del col·lectiu del PAS o del PDI de la Universitat s'identifiqui mitjançant usuari i contrasenya, s'emmagatzemaran evidències electròniques; de la mateixa manera, en el moment de signar un document a través d'usuari i contrasenya, el sistema emmagatzemarà les evidències de voluntat de signatura.

El detall de la identificació i signatura a través d'usuari i contrasenya es troba en l'apartat 8.4 d'aquest document.

Addicionalment, el sistema també es pot basar en mecanismes d'identitat digital que es puguin validar a través de la plataforma VALid, com l'idCAT i la resta d'identitats que es validin a través de la plataforma Cl@ve, com ara el sistema PIN24H o Cl@ve Permanent.

Finalment, també es podran utilitzar les identitats digitals generades en altres universitats que es verifiquen a través del servei UNIFICAT, del Consorci de Serveis Universitaris de Catalunya (CSUC). Aquest servei és una plataforma de col·laboració que possibilita que l'estudiantat, el PDI i el PAS accedeixin a diversos serveis de diferents proveïdors, amb una única identitat digital. La signatura es farà de la mateixa forma que en el cas de la signatura amb usuaris i contrasenyes de la URV.

De la mateixa manera que en el cas dels certificats digitals, per a cada procediment administratiu, la Universitat, basant-se en el nivell de seguretat que requereixi, així com en el paper amb el qual actuï el titular d'aquesta identitat digital, decidirà si es pot utilitzar aquest sistema tant com a sistema d'identificació com sobretot de signatura electrònica.

6.3. CERTIFICATS DIGITALS EMPRATS PER LA UNIVERSITAT

El personal de la Universitat (PDI o PAS) que hagi de signar documents digitalment o tenir accés a determinats serveis o aplicacions en què es requereixi un alt nivell d'autenticació, poden requerir certificats digitals. Per a aquest propòsit la Universitat utilitzarà els certificats següents:

- Certificats de treballador públic i estudiant:

o Certificats electrònics qualificats d'empleat públic T-CAT (Consorci AOC): correspon al certificat personal d'identificació i signatura reconeguda o qualificada que va adreçat a persones físiques i disposa d'informació referent

al titular que permet identificar-lo i vincular-lo a la Universitat. Se subministra en targeta criptogràfica. Es generen des de l'entitat de registre de la Universitat.

- Certificats electrònics qualificats d'empleat públic T-CAT-P (Consorci AOC): correspon al certificat personal d'identificació i signatura avançada, que va adreçat a persones físiques i disposa d'informació referent al titular que permet identificar-lo i vincular-lo a la Universitat. Se subministra en programari. Es generen des de l'entitat de registre de la Universitat i es pugen a la plataforma de custòdia de certificats digitals, excepte per a aquells usuaris que tinguin com a lloc de treball un ordinador MAC o el necessitin al mòbil o en una tauleta.

- Certificats de representant:

- Certificats electrònics qualificats de representant T-CAT (Consorci AOC): correspon al certificat electrònic de representant davant les administracions públiques. És un certificat personal d'identificació i signatura reconeguda o qualificada. Se subministra en targeta criptogràfica. Aquest certificat acredita que el titular del certificat pot representar la Universitat en general o davant d'altres administracions públiques. Es generen des de l'entitat de registre de la Universitat i es pugen a la plataforma de custòdia de certificats digitals, excepte per a aquells usuaris que tinguin com a lloc de treball un ordinador MAC o el necessitin al mòbil o en una tauleta.

- La Universitat també disposa de certificats de la FNMT de representant de persona jurídica de la Universitat. No es generen des de l'entitat de registre de la Universitat sinó que cal anar a una entitat de registre de la FNMT. Aquests certificats també es pugen a la plataforma de custòdia de certificats digitals, excepte per a aquells usuaris que tinguin com a lloc de treball un ordinador MAC o el necessitin al mòbil o en una tauleta.

- Certificats tècnics del Consorci AOC:

- Certificat de segell electrònic: correspon al certificat digital que serveix per a l'actuació administrativa automatitzada, segons l'article 42 de la Llei 40/2015, de regim jurídic del sector públic. Aquest certificat pot utilitzar-se per a compulses i còpies electròniques, llibres foliats d'expedients o emissió de certificats acadèmics, entre d'altres. Per a aquests certificats, la Universitat utilitzarà els del Consorci AOC i es generaran des de l'entitat de registre de la Universitat.

- Certificats d'aplicació: correspon al certificat digital que serveix per identificar aplicacions i servidors. Aquest certificat pot utilitzar-se per l'intercanvi de dades (entre administracions, administracions i ciutadania i entre administracions i empreses), la identificació i autenticació d'un sistema o servei web, entre d'altres. Per a aquests certificats, la Universitat utilitzarà els del Consorci AOC i es generaran des de l'entitat de registre de la Universitat.

- Pel que fa a l'ús de certificats digitals de seu electrònica, o de servidor, els utilitzats per a l'intercanvi segur d'informació entre l'usuari i la Universitat (pagament electrònic, enviament de dades personals, etc.), la Universitat pot utilitzar els de RedIris, FNMT o qualsevol dels emesos per altres autoritats de certificació que ja tinguin un alt nivell d'instal·lació de les seves claus públiques en els navegadors. Cal assenyalar que, si bé aquests certificats no generen actes jurídics, igual que els d'aplicació, s'ha considerat oportú incorporar-los a les polítiques.

6.4. EMMAGATZEMATGE DELS CERTIFICATS

Els certificats digitals de la Universitat es poden trobar als repositoris següents:

a) A la plataforma de custòdia de certificats digitals del Consorci de Serveis Universitaris de Catalunya (CSUC) (per a certificats digitals de treballador públic en programari del Consorci AOC (T-CAT-P) i de representant en programari de la FNMT). El certificat T-CAT-P i el certificat en programari de la FNMT seran eliminats, tant els fitxers que el contenen com si han estat prèviament instal·lats als llocs de treball, una vegada carregats a la plataforma de custòdia.

b) Només per a aquells usuaris que tinguin com a lloc de treball un ordinador MAC o el necessitin al mòbil o en una tauleta, al repositori de gestió de certificats digitals dels llocs de treball (per a certificats de treballador públic en programari (T-CAT-P) i de representant de persona jurídica de la FNMT).

c) En targeta criptogràfica (per a certificats de treballador públic en targeta o de representant del Consorci AOC (T-CAT)). Els certificats digitals guardats en targeta criptogràfica permeten generar signatura qualificada o reconeguda, mentre que els certificats digitals guardats en la resta de suports permeten generar signatura avançada.

d) En el repositori de gestió de certificats digitals dels servidors de la Universitat (per a certificats de segell electrònic per a l'actuació administrativa automatitzada, els d'aplicació o per a certificats de servidor web i de seu electrònica).

7. CICLE DE VIDA DELS CERTIFICATS DIGITALS I ALTRES IDENTITATS DIGITALS: CREACIÓ, VERIFICACIÓ I CONSERVACIÓ.

La Universitat és entitat de registre del Consorci AOC per emetre els certificats digitals que requereixi per a la realització de les seves activitats.

Així doncs, el Consorci AOC és el responsable de definir les polítiques de gestió dels certificats digitals que emet i, per tant, defineix la vigència dels certificats, la manera com es revoquen, es renoven, es validen, etc.

Per emetre certificats digitals, la Universitat disposa d'una Entitat de Registre interna en dependència del CAOC. A l'efecte d'adoptar els procediments establerts pel CAOC per operar, a l'Entitat de Registre s'han establert procediments interns que identifiquen les activitats que s'hi duen a terme i els responsables, així com els procediments que els usuaris han de seguir per a la sol·licitud, renovació, revocació, etc. dels seus certificats digitals.

7.1. CERTIFICATS DE TREBALLADOR/APÚBLIC O D'ESTUDIANT

Els certificats digitals dels treballadors públics o d'estudiants de la Universitat són del Consorci AOC, i els emet i els revoca el Servei de Recursos Informàtics i TIC, a través del servei de certificació digital de la Universitat, a partir de la sol·licitud de la persona interessada adreçada a aquest servei.

Aquesta sol·licitud s'ha de fer per mitjans electrònics i ha d'anar acompanyada del

formulari on se'n justifica la necessitat. Aquest formulari es troba disponible a la intranet de la Universitat.

A partir d'aquesta sol·licitud, el Servei de Recursos Informàtics i TIC (SRITIC), a través del servei de certificació digital de la Universitat, validarà que les dades siguin correctes i la justificació sigui oportuna. En cas afirmatiu, emetrà el certificat. En cas que no sigui oportú, ho comunicarà a la persona interessada.

Una vegada generat el certificat, el SRITIC, n'ha d'informar la persona interessada, que haurà de personar-se al servei per lliurar-li el certificat digital i signar el document de lliurament proporcionat pel Consorci AOC.

En aquest moment el SRITIC ha d'anotar la informació d'aquest certificat a l'inventari de certificats digitals de la Universitat.

En cas de pèrdua, la persona usuària del certificat digital està obligada a informar-ne el SRITIC d'aquesta circumstància i se l'hi revocarà. En el cas que continuï sent necessari el certificat, la persona usuària haurà de sol·licitar-ne un de nou segons el procediment. El SRITIC ha d'introduir a l'inventari de certificats digitals aquests fets.

En general, dos mesos abans de la caducitat del certificat digital, la persona usuària ha de presentar una nova sol·licitud d'acord amb el procediment indicat.

En el cas que la persona usuària del certificat digital deixi d'estar vinculada a la Universitat, el Servei de Recursos Humans ha de comunicar el canvi de vinculació al servei de certificació digital prestat des del Servei de Recursos Informàtics i TIC que:

- En el cas que sigui de PAS o PDI i el certificat estigui en la PCCD, li retirarà l'accés fins que no torni a la Universitat.
- En el cas que sigui de PAS o PDI i el certificat estigui en una targeta o en el lloc de treball de la persona usuària, revocarà el certificat.

En el cas que la persona usuària del certificat digital sigui estudiant i per alguna raó motivada disposi de certificat digital, el Servei de Recursos Informàtics i TIC, mitjançant l'automatització del cicle de vida de la identitat de l'estudiantat, haurà de revocar-li el certificat quan detecti que hi ha desvinculació amb la Universitat.

El Servei de Recursos informàtics i TIC, a través del servei de certificació digital de la Universitat, conjuntament amb el Servei de Recursos Humans i el Servei de Gestió Acadèmica de la Universitat han de fer, cada tres mesos, una revisió proactiva dels diferents certificats digitals de l'organització, a través de l'inventari de certificats digitals, per revocar els certificats resultants de les baixes de personal de la Universitat. El Servei de Recursos Informàtics i TIC, a través del servei de certificació digital de la Universitat, ha d'introduir a l'inventari la revocació d'aquests certificats digitals.

El Servei de Recursos Informàtics i TIC, a través del servei de certificació digital de la Universitat, ha de mantenir un inventari dels diferents certificats digitals de treballador públic o d'estudiant que existeixen en l'organització. Aquest inventari inclou la informació necessària per a la gestió, la persona titular del certificat, el tipus, l'emissor i la data de caducitat del certificat, entre d'altres.

7.2. CERTIFICAT DE REPRESENTANT

7.2.1 Consorci AOC

Aquests certificats digitals de representat són del Consorci AOC, i els emet i els revoca el SRITIC, a partir de la sol·licitud de la persona interessada adreçada a aquest Servei i amb el vistiplau de la Secretaria General.

El procediment per sol·licitar-lo és el següent:

La persona interessada ha de sol·licitar, per mitjans electrònics, la generació d'aquest certificat a la Secretaria General. En el cas que l'interessat tingui capacitat de representar la Universitat, la Secretaria General ho ha de comunicar al SRITIC, que generarà el certificat digital. La Secretaria General també ha de comunicar a la persona interessada que s'ha donat l'ordre d'emissió del certificat digital.

En el moment que el SRITIC hagi emès el certificat, ho ha de comunicar a la persona interessada perquè es personi al Servei per lliurar-li el certificat digital i signar el document de lliurament proporcionat pel Consorci AOC.

En aquest moment el SRITIC ,ha d'anotar la informació d'aquest certificat a l'inventari de certificats digitals de la Universitat.

En el cas de pèrdua, la persona usuària del certificat digital està obligada a informar el SRITIC d'aquesta circumstància i se l'hi revocarà. En el cas que continuï sent necessari el certificat i sigui vigent la capacitat de representació, la persona usuària haurà de sol·licitar-ne un de nou segons el procediment. El SRITIC , ha d'introduir a l'inventari de certificats digitals aquests fets.

Quan el certificat digital caduqui, la persona usuària és la responsable de renovar-lo . En el cas que aquesta persona deixi de tenir la capacitat de representació de la Universitat, la mateixa persona o la Secretaria General ha de demanar al SRITIC que li revoqui el certificat. El SRITIC, ha introduir a l'inventari de certificats digitals la revocació d'aquest certificat digital.

El Servei de Recursos Informàtics i TIC, a través del servei de certificació digital de la Universitat, conjuntament amb la Secretaria General han de fer, cada tres mesos, una revisió proactiva dels diferents certificats digitals de representant, a través de l'inventari de certificats digitals, per revocar els certificats resultants de les revocacions de capacitat de representació del personal de la Universitat. El SRITIC ha d'introduir a l'inventari de certificats digitals la revocació.

El SRITIC ha de mantenir un inventari dels diferents certificats digitals de representant que existeixen en l'organització. Aquest inventari inclou la informació necessària per a la gestió, el titular del certificat, el tipus, l'emissor i la data de caducitat del certificat, entre d'altres.

7.2.2 FNMT

Pel que fa als certificats de representant de la FNMT, el procediment per sol·licitar-los és el següent:

1. La persona interessada ha de sol·licitar, per mitjans electrònics, la generació d'aquest certificat a la Secretaria General. En el cas que l'interessat tingui capacitat de representar la Universitat, la Secretaria General ho ha de comunicar al SRITIC , que serà el responsable de cursar la sol·licitud a la FNMT. La Secretaria General també ha de comunicar a la persona interessada que s'ha donat permís per obtenir el certificat digital.

2. El SRITIC, ha de fer-ne la sol·licitud, a nom de la persona interessada. Un cop finalitzat el procés, la persona interessada rebrà un correu electrònic amb la informació necessària perquè pugui anar-lo a buscar a una de les oficines que actuen com a entitat de registre de la FNMT, on haurà d'acreditar la identitat i capacitat de representar la Universitat.

3. Finalment, caldrà descarregar el certificat a través d'internet i carregar-lo a la PCCD o al lloc de treball corresponent si és un MAC, un telèfon mòbil o una tauleta.

4. El SRITIC ha d'introduir aquesta dada a l'inventari de certificats digitals de la Universitat.

En el cas de pèrdua, el representant ha de comunicar-ho al SRITIC perquè en tingui coneixement i alhora serà el mateix interessat qui haurà d'iniciar el procediment de revocació corresponent davant la FNMT. Una vegada finalitzat el procés, també n'informarà el SRITIC perquè ho apunti a l'inventari de certificats digitals de la Universitat.

En el cas que la persona usuària deixi de tenir la capacitat de representació, la mateixa persona usuària o la Secretaria General hauran de demanar la revocació del certificat.

En aquests dos casos, el servei de certificació haurà d'anotar a l'inventari de certificats digitals aquest fet.

El Servei de Recursos Informàtics i TIC, a través del servei de certificació digital de la Universitat, conjuntament amb la Secretaria General han de fer, cada tres mesos, una revisió proactiva dels diferents certificats digitals de representant, a través de l'inventari de certificats digitals, per revocar els certificats resultants de les revocacions de capacitat de representació del personal de la Universitat. El Servei de Recursos Informàtics i TIC, a través del servei de certificació digital de la Universitat, ha d'informar l'inventari de certificats digitals de la revocació d'aquests certificats digitals.

El SRITIC, a través del servei de certificació digital de la Universitat, ha de mantenir un inventari dels diferents certificats digitals de representant que existeixen en l'organització. Aquest inventari inclou la informació necessària per a la gestió, el titular del certificat, el tipus, l'emissor i la data de caducitat del certificat, entre d'altres.

7.3. SEGELLS ELECTRÒNICS

Aquests certificats digitals de segell electrònic són del Consorci AOC, i els emet i els revoca el Servei de Recursos Informàtics i TIC, a través del servei de certificació digital de la Universitat, a instància de la persona interessada adreçada a la Secretaria General.

En el cas dels certificats de segell electrònic, el procés de sol·licitud és el següent:

1. La persona interessada ha d'adreçar una sol·licitud a la Secretaria General.

2. La Secretaria General ha d'avaluar si escau o no l'ús del certificat de segell electrònic. 3. En el cas que es consideri procedent, n'ha d'informar el Servei de Recursos informàtics i TIC, a través del servei de certificació digital de la Universitat, perquè verifiqui si ja existeix algun certificat de segell electrònic que pugui servir per a l'ús requerit. En el cas que no existeixi, ha d'emetre un certificat digital de segell nou.

4. El SRITIC, a través del servei de certificació digital de la Universitat, és el responsable de fer la sol·licitud i l'emissió del certificat de segell electrònic.

5. Una vegada es tingui el nou certificat de segell electrònic, s'instal·larà en l'aplicació corresponent.

En el cas que el certificat de segell ja existís, s'instal·larà el corresponent certificat de segell a l'aplicació corresponent.

El Servei de Recursos Informàtics i TIC, a través del servei de certificació digital de la Universitat, ha d'informar l'inventari de certificats digitals de l'emissió i/o de l'ús d'aquest certificat digital.

El SRITIC, a través del servei de certificació digital de la Universitat, ha de mantenir un inventari dels diferents certificats de segell que existeixen en l'organització, emesos pel CAOC. Aquest inventari inclou la informació necessària per a la gestió, el nom de certificat, el tipus, l'emissor, l'aplicació que el gestiona i la data de caducitat del certificat, entre d'altres.

En el moment que el servei certificació digital detecta que un certificat de segell inclòs en l'inventari està a punt de caducar, ho ha de comunicar alsserveis que el van sol·licitara la Secretaria General. Aquesta última ha d'autoritzar, si s'escau, la generació del nou certificat digital, seguint el procediment establert.

La Universitat pot cedir segells electrònics a tercers. En aquest cas, sempre s'ha de signar un document de cessió del certificat de segell amb l'organisme a qui se li cedeix el certificat i sempre serà un certificat de segell específic, per poder tenir un control dels usos que es puguin fer amb aquests certificats.

7.4. CERTIFICAT DE SEU ELECTRÒNICA

En el cas dels certificats de seu electrònica, el procés de sol·licitud és el següent:

1. La Secretaria General l'ha de demanar al Servei de Recursos Informàtics i TIC, a través del servei de certificació digital de la Universitat. El SRITIC, a través del servei de certificació digital de la Universitat, demana el certificat digital al prestador de serveis de confiança que consideri més escaient en cada moment. Quan tingui el certificat digital, introduirà a l'inventari de certificats digitals l'emissió d'aquest certificat digital.

2. El Servei de Recursos Informàtics i TIC és el responsable d'instal·lar-lo al servidor.

El SRITIC, a través del servei de certificació digital de la Universitat, ha de mantenir un inventari dels diferents certificats de seu electrònica que existeixen en l'organització. Aquest inventari inclou la informació necessària per a la gestió, el nom del certificat, el tipus, l'emissor, l'aplicació que el gestiona i la data de caducitat del certificat, entre d'altres.

En el moment que el servei certificació digital detecta que un certificat de seu electrònica està a punt de caducar, ho ha de comunicar a la Secretaria General, que és qui autoritza la generació del nou certificat digital, seguint el procediment establert.

7.5. CERTIFICATS D'APLICACIÓ I DE WEB

En el cas dels certificats d'aplicació i de web, el procés de sol·licitud és el següent:

La persona interessada ha d'enviar la sol·licitud al servei de certificació digital del Servei de Recursos Informàtics i TIC de la Universitat. Aquest verifica que no hi ha cap dels ja emesos que pugui realitzar aquesta funció i, en cas que algun dels certificats existents la pugui realitzar, n'informa el sol·licitant perquè l'utilitzi.

En el cas que cap dels certificats digitals existents serveixi, el SRITIC, a través del servei de certificació digital de la Universitat, ha de sol·licitar i descarregar un nou certificat digital d'aplicació o de web al prestador de serveis de confiança que correspongui en cada moment. Una vegada obtingut el certificat l'ha de fer arribar al sol·licitant, perquè l'instal·li al servidor o en l'aplicació que correspongui.

El SRITIC, a través del servei de certificació digital de la Universitat, ha introduir a l'inventari de certificats digitals l'emissió i els usos d'aquests certificats digitals.

El Servei de Recursos Informàtics i TIC, a través del servei de certificació digital de la Universitat, ha de mantenir un inventari dels diferents certificats d'aplicació i de web que existeixen en l'organització, emesos pel prestador de serveis de certificació corresponent. Aquest inventari inclou la informació necessària per a la gestió, el nom del certificat, el tipus, l'emissor, l'aplicació que el gestiona i la data de caducitat del certificat, entre d'altres.

En el moment que el Servei de Recursos Informàtics i TIC, a través del servei de certificació digital de la Universitat, detecta que un certificat digital d'aquest tipus està a punt de caducar, haurà de fer la sol·licitud per generar el nou certificat digital seguint el procediment establert.

8. SISTEMES DE SIGNATURA ELECTRÒNICA

Els sistemes de signatura electrònica que la Universitat pot utilitzar són els següents:

8.1. SIGNATURA ELECTRÒNICA MITJANÇANT CERTIFICAT DIGITAL DE TREBALLADOR PÚBLIC DE LA UNIVERSITAT

És el sistema de signatura electrònica en la qual, partint de la clau privada d'un certificat digital d'una persona, se xifra el resum criptogràfic del document a signar i s'afegeix a aquesta firma informació del certificat utilitzat per realitzar-la, la data de la signatura, la política de signatura, etc.

La Universitat utilitza aquest sistema perquè el personal de la Universitat signi documents electrònics i admet documents signats amb aquest sistema de signatura per part de tercers que es relacionin amb la Universitat.

La signatura a realitzar és del tipus AdES-T i es completa posteriorment a format AdES-A o PAdES-LTV. Aquest procés de completar la signatura electrònica s'ha de fer, sempre que sigui possible, dins el mateix dia.

8.2. SIGNATURA ELECTRÒNICA MITJANÇANT SEGELL ELECTRÒNIC

És el sistema de signatura electrònica mitjançant actuació administrativa automatitzada, en què partint de la clau privada d'un certificat digital de segell electrònic se xifra el resum criptogràfic del document a signar i s'afegeix a aquesta firma informació del certificat de segell electrònic utilitzat per realitzar-la, la data de la signatura, la política de signatura, etc.

Aquest sistema permet signar documentació electrònica emesa per la Universitat, de manera transparent per al personal al seu servei. D'aquesta manera, es vincula aquesta documentació a l'actuació administrativa automatitzada, la qual té la regulació específica en una norma aprovada a l'efecte.

La signatura és del tipus AdES-T i es completa posteriorment a format AdES-A o PAdES-LTV. Aquest procés de completar la signatura electrònica es farà sempre que sigui possible dins el mateix dia.

8.3. SIGNATURA ELECTRÒNICA BASADA EN UN CODI SEGUR DE VERIFICACIÓ (CSV)

L'article 42.b de la Llei 40/2015 regula l'ús de el codi segur de verificació com a mitjà de signatura, vinculat a l'Administració pública, òrgan, organisme públic o entitat de dret públic, que permet comprovar la integritat del document mitjançant l'accés a la seu electrònica corresponent.

Aquest sistema, que només es pot utilitzar en actuació administrativa automatitzada, consisteix a afegir un codi únic de verificació a un document perquè es pugui validar la seva autenticitat a través de l'accés a la seu electrònica.

Es considera signatura electrònica d'acord amb el que preveu l'article 42, de sistemes de signatura per a l'actuació administrativa automatitzada, apartat b de la Llei 40/2015.

La Universitat té previst aquest sistema de signatura per la relació amb el col·lectiu d'estudiants, PDI, PAS i tercers.

8.4. SIGNATURA ELECTRÒNICA BASADA EN CLAUS CONCERTADES MÉS LES EVIDÈNCIES DE VOLUNTAT DE SIGNATURA.

El sistema es basa en la identificació d'una persona a partir del seu usuari i contrasenya (primera evidència d'autenticació) proporcionats per la Universitat o bé per una identitat proveïda per UNIFICAT i la prestació del consentiment durant el procés de la signatura (pot ser a través de prémer un botó en l'aplicació corresponent). En aquest moment es crearà un fitxer d'evidències que s'emmagatzemaran en el mateix document. En el cas que per algun motiu tècnic no fos possible emmagatzemar aquest fitxer d'evidències en el mateix document, es desaran en els sistemes corporatius de la Universitat; en aquests casos, en el mateix procediment administratiu s'informarà del lloc on s'emmagatzemaran les evidències. Posteriorment se signarà automàticament, amb actuació administrativa automatitzada, el document mitjançant un certificat digital de segell electrònic a nom de la Universitat.

La signatura amb el certificat digital de segell electrònic és del tipus AdES-T i es completa posteriorment a format AdES-A o PAdES-LTV. Aquest procés de compleció de la signatura electrònica s'ha de fer sempre que sigui possible dins el mateix dia.

Per tant, la validesa jurídica de la signatura electrònica, realitzada amb claus concertades més evidències de voluntat de signatura, està vinculada, d'una banda, al document i, d'una altra, a les evidències del procés d'identificació de la persona que firma amb l'acceptació de la signatura.

Es podran preveure sistemes de doble o triple evidència d'autenticació en el cas que el procediment ho requereixi i, per tant, es podran emmagatzemar també les evidències associades a aquests factors.

En aquest format de signatura hi pot haver més d'una signatura d'aquest tipus sobre el document, que poden ser en paral·lel o niades.

Aquesta signatura pot combinar-se amb un altre tipus de signatura basada en el certificat digital.

En cas de conflicte amb alguna signatura, la Universitat podrà acreditar que ha aprovat i publicat a la seu electrònica la regulació específica, que ha generat les evidències no només en aquesta signatura sinó en qualsevol altra signatura del mateix tipus (signatura primària), que aquesta signatura es va produir en un moment determinat (segell de temps) i que el contingut del document no ha canviat (marca, coixinet del document en l'evidència (signatura primària)) i al seu torn tenir el document signat amb el segon segell electrònic (signatura secundària).

8.5. SIGNATURA ELECTRÒNICA UTILITZANT LA PLATAFORMA VALID

Es preveu aquest sistema de signatura com un cas particular de signatura electrònica amb claus concertades més voluntat de signatura, però delegant la generació de les evidències en el sistema VALid.

Aquest sistema es basa en l'ús de la plataforma VALid i, per tant, aquesta sol·licitarà al signant que s'autentiqui i posteriorment, generi les evidències tant d'identificació com de voluntat de signar.

VALid genera un fitxer amb les evidències d'identificació, les quals es desaran, com en el cas anterior, dins el mateix document a signar i, en el cas que per algun motiu tècnic no fos possible emmagatzemar aquest fitxer d'evidències en el mateix document, es desaran en els sistemes corporatius de la Universitat. En aquests casos, s'informarà en el mateix procediment administratiu del lloc on s'emmagatzemaran les evidències. Posteriorment se signarà el document mitjançant un certificat digital de segell electrònic a nom de la Universitat.

En aquest format de signatura hi pot haver més d'una signatura d'aquest tipus sobre el document i seran tant en paral·lel com niades.

Aquesta signatura pot combinar-se amb un altre tipus de signatura basada en certificat digital.

En cas de conflicte amb alguna signatura, la Universitat podrà acreditar que ha aprovat i publicat a la seu electrònica la regulació específica, que ha obtingut les evidències no només en aquesta signatura sinó en qualsevol altra signatura de el mateix tipus (signatura primària), que aquesta signatura es va produir en un moment determinat (segell de temps) i que el contingut del document no ha canviat perquè està signat amb el segon segell electrònic (signatura secundària).

8.6. SIGNATURA ELECTRÒNICA BIOMÈTRICA

Aquest és un sistema específic de signatura electrònica avançada per als documents electrònics que es generen presencialment davant d'un tercer i en el qual es guarda xifrada, conjuntament amb el resum criptogràfic del document, la informació següent:

- Dades biomètriques de la persona que signa manuscritament el document, entre els quals:
    - Detall temporal de la realització de la signatura (inici, final i durada en mil·lisegons).

- Detall de la traça, en relació amb la velocitat, acceleració i pressió de la traça en tota la seva figura.

Les dades biomètriques es recullen amb elements específics de captura i permeten a la persona signant veure el document que ha de signar en el mateix acte de signatura.

- Altra informació que pugui resultar rellevant per al procés de signatura o el document signat, com pot ser la identificació del programari i maquinari de captura de signatura o la localització GPS de l'element maquinari de captura de signatura.

El xifratge d'informació es realitza amb la clau pública d'un certificat digital específic de signatura electrònica biomètrica que s'emmagatzema en els servidors de la Universitat. La clau privada és custodiada per un tercer de confiança i se la hi requerirà quan sigui necessari verificar una signatura biomètrica, en cas de reclamació o litigi.

En aquest format de signatura hi pot haver més d'una signatura biomètrica sobre el document, però sempre seran en paral·lel. En qualsevol cas, un cop finalitzades totes les firmes biomètriques i xifrades, la informació esmentada anteriorment es desarà de forma conjunta amb el document i, per garantir-ne la integritat, s'hi realitzarà una signatura electrònica automàtica de segell electrònic d'aplicació pertanyent ala Universitat completada amb segell de temps.

Per tant, la validesa jurídica de la signatura electrònica biomètrica està vinculada al document i a les evidències biomètriques que es guarden dins del mateix document de forma xifrada. Així doncs, la signatura electrònica i el segell de temps aporten únicament evidències d'integritat i no d'autenticitat. En cas de conflicte, un cop desxifrades les dades per part del tercer de confiança que custodia la clau privada del certificat de xifratge, s'haurà de generar un peritatge de les dades biomètriques guardades en el document i comparar-les amb una nova presa de dades biomètriques de la persona a qui suposadament corresponen les dades biomètriques. S'ha de fer amb les mateixes condicions o similars pel que fa a elements del maquinari i programari amb les que es va fer la signatura que s'ha de verificar.

En aquest sentit, el tercer de confiança que custodiï la clau privada del certificat digital d'encriptació ha de tenir o se li ha de proporcionar en el moment del peritatge un client lleuger de l'aplicació de generació de signatures biomètriques, així com de l'aplicació que permeti el desxifratge en interpretació de les dades biomètriques.

9. FORMATS DE SIGNATURA MITJANÇANT CERTIFICAT DIGITAL

Partint dels conceptes bàsics sobre signatura electrònica descrits a l'annex I, es descriuen, a continuació, els formats de signatura electrònica que s'apliquen sobre els sistemes de signatura basats en certificats digitals, que utilitzarà la Universitat en el marc d'aquesta política de signatura.

- Per a documents PDF o PDF/A, s'utilitzarà el format de signatura PAdES-T
- Per a documents XML, s'utilitzarà el format de signatura XAdES-T attached enveloping

- Per a la resta dels formats de documents, s'utilitzarà el format XAdES-T detached.

Un cop aquests fitxers hagin estat signats es completarà, si és possible durant el mateix dia de la signatura, a firmes longeves: PAdES-LTV i XAdES-A.

Es preveu dins el primer cas la signatura de documents en formats diversos que s'hagin incrustat dins d'un document PDF o PDF / A.

10. SIGNATURA MÚLTIPLE

La signatura múltiple es produeix quan el document conté dues o més signatures i consisteix que diverses persones el signen consecutivament. Aquesta signatura es pot aplicar sobre el document original cada vegada, que s'anomena signatura paral·lela, o sobre el document signat, que s'anomena signatura niada.

La signatura múltiple s'utilitza en diverses situacions en el marc dels procediments de la Universitat, com ara quan més d'una persona han de signar documents electrònics o en el ressegellament de documents (vegeu apartat 12.1) ja signats per actualitzar-ne la validesa legal al llarg del temps, abans que no pugui quedar en entredit la validesa criptogràfica de la signatura electrònica.

La combinació de sistemes de signatura és possible en els casos següents:

- Signatures electròniques mitjançant certificats digitals (paral·lela o niada), per a qualsevol document en suport electrònic que requereixi més d'una signatura.
- Signatures electròniques mitjançant sistemes basats en claus concertades (inclou Cl@ve) (paral·lela o niada), en el cas de documents en suport electrònic que requereixin més d'una signatura d'estudiant, PAS i PDI.
- Signatures electròniques biomètriques (niada), per a documents en suport electrònic que es generin presencialment davant de tercers i requereixin dues o més de les seves signatures.
- Signatura electrònica mitjançant sistema basat en claus concertades (inclou Cl@ve) i, posteriorment, signatura electrònica mitjançant certificat digital (paral·lela o imbricada), per a aquells documents en suport electrònic que requereixin la signatura d'estudiants, PAS o PDI, i requereixi una signatura electrònica posterior per completar-ne la validesa mitjançant certificat digital.
- Signatura electrònica biomètrica i, posteriorment, signatura electrònica mitjançant certificat digital (imbricada), en el cas de documents en suport electrònic que es generin davant d'un tercer i que, després d'haver-los signat sobre la base de biometria, requereixi la signatura electrònica posterior per completar-ne la validesa mitjançant certificat digital.

11. VALIDACIÓ DE SIGNATURES O SEGELLS

Per garantir la validesa jurídica dels documents electrònics signats digitalment, qualsevol document que entri o es generi a la Universitat i que contingui una signatura electrònica i/o un segell de temps, abans d'emmagatzemar-lo en el gestor

documental, cal validar-lo. Per fer-ho s'utilitzaran els sistemes següents:

- La plataforma de validació de certificats i signatura electrònica del Ministeri, @firma.
- La plataforma de validació PSIS del Consorci AOC.
- Per a documents PDF que ho requereixin, s'utilitzarà el servei de validació que aporten les eines Adobe.
- Per als documents signats basats en claus concertades més les evidències de la voluntat de signatura, mitjançant el procés anteriorment descrit a l'apartat 8.4.
- Per al del codi segur de verificació (CSV), mitjançant la comprovació en la seu electrònica corresponent.
- Per a les firmes biomètriques, s'utilitzaran els mecanismes descrits en l'apartat 8.6. d'aquest document.

Pel que fa a les signatures electròniques avançades i reconegudes, només en aquells casos en què el procés de validació de totes les signatures electròniques i dels segells electrònics sigui satisfactori es completarà fins a aquest nivell, si no està ja en format XAdES-A o PAdES-LTV, i s'emmagatzemarà el document electrònic dins del gestor documental de la Universitat.

Pel que fa a les firmes biomètriques, s'emmagatzemarà el document electrònic en el gestor documental de la Universitat directament sense cap validació addicional, atès que aquests sistemes de captació d'aquesta signatura són segurs i no existeix un procés automatitzat de validació.

En el cas que sigui necessari preservar la validesa jurídica del document més enllà del temps de vida del certificat digital utilitzat per generar qualsevol signatura associada a aquest document o del segell de temps associat a la o les signatures electròniques, es completarà la signatura o signatures electròniques en el cas que no siguin ja signatura d'arxiu, és a dir -A o -LTV. La compleció es farà a format de signatura d'arxiu.

Pel que fa ales signatures biomètriques, la signatura electrònica del document es farà amb un certificat de segell electrònic en format -A o -LTV.

Pel que fa a signatures electròniques basades en certificats digitals de prestadors de fora la Unió Europea, i en el cas que la Universitat decideixi acceptar aquest document, el procés de validació consistirà a:

1. Validar que la signatura electrònica correspon a la marca del document.
2. Anar al regulador del país que ha emès aquest certificat digital i comprovar que l'autoritat de certificació és una de les reconegudes pel regulador.
3. Comprovar que el certificat digital utilitzat per a la signatura d'aquest document era vigent en el moment de la signatura.
4. En el cas que sigui correcte, fer una còpia autèntica del document signat, amb un segell de la Universitat. Aquest nou document serà el que es guardarà en l'expedient. Es desarà el document original en un repositori específic de la Universitat.

En cas que sigui necessari preservar la validesa jurídica del document més enllà del temps de vida del certificat digital utilitzat per generar qualsevol signatura associada a aquest document o del segell de temps associat a la o les signatures electròniques, es completarà la signatura o signatures electròniques si no són ja signatura d'arxiu, és a dir "A" o "LTV". La compleció es farà a format de signatura d'arxiu.

Pel que fa a les signatures a través d'acreditació de la identitat i d'evidències de la voluntat de signatura amb eines pròpies de la Universitat, s'emmagatzemarà el document electrònic, amb les seves signatures (primària i secundària) en el gestor documental de la Universitat, directament sense cap validació addicional, ja que els sistemes de captació d'aquesta tipologia de signatura ja són segurs i no hi ha cap procediment automatitzat de validació.

Pel que fa ales signatures a través d'acreditació de la identitat i d'evidències de la voluntat de signatura, com a través de VALid, es validarà la signatura electrònica del document amb un certificat de segell electrònic en format - A o - LTV. Per a aquest cas, només es farà la compleció en la signatura secundària.

Pel que fa a les signatures a través d'acreditació de la identitat i d'evidències de la voluntat de signatura d'altres sistemes, s'emmagatzemarà el document electrònic, amb les seves evidències de voluntat en el gestor documental de la Universitat, directament sense cap validació addicional, ja que la Universitat considera segurs els sistemes de captació d'aquesta tipologia de signatura i no hi ha cap procediment automatitzat de validació.

Finalment, pel que fa a de signatures amb CSV de documents emesos per altres administracions públiques, la forma de validar-los és a través de la corresponent seu electrònica, tal com es descriu en l'article 42.b de la Llei 40/2015.

12. MANTENIMENT I PRESERVACIÓ DE LES SIGNATURES I SEGELLS ELECTRÒNICS

La signatura electrònica atorga validesa jurídica als documents electrònics. No obstant això, aquesta validesa està subjecta a certs riscos que s'han de gestionar degudament per garantir una validesa jurídica indefinida del document en suport electrònic. Aquests riscos poden ser:

- Caducitat del certificat digital o del segell electrònic amb el qual se signa un document electrònic.
- Validesa del certificat digital o del segell electrònic en el moment de generar-se la signatura electrònica.
- Obsolescència tecnològica de la longitud de les claus criptogràfiques contingudes en el certificat digital i amb les quals es generen les signatures electròniques.

Per contrarestar els riscos descrits, la Universitat es dota de dos mecanismes diferenciats: el ressegellament de les signatures i les còpies electròniques de documents electrònics jurídicament vàlids amb signatura caducada.

12.1. RESSEGELLAMENT DE LES SIGNATURES

L'objectiu principal d'aquesta funció és garantir la signatura electrònica al llarg del temps.

El procés de ressegellament consisteix a renovar el segell de data i hora, afegint-hi

una nova baula a la cadena d'evidències electròniques a la signatura electrònica que ja és al document.

Per poder aplicar aquest procés, cal que les signatures estiguin en un format que permeti afegir-hi aquestes evidències de temps. Aquestes són les firmes del tipus XAdES-A o PAdES-LTV. En el cas que una signatura no estigui en aquests formats, abans del ressegellament s'haurà de completar la signatura a un dels formats anteriorment definits.

Aquest serà un procés que es durà a terme per a aquells documents que no s'hagin transferit a la solució d'Arxiu de la Universitat:

- En el moment en què estigui a punt de caducar l'últim segell de temps aplicat a la signatura electrònica que s'ha de preservar.
- Excepcionalment, quan es detecti una possible obsolescència tecnològica dels algoritmes o de les claus que signen el document.

Partirem, tal com s'ha comentat en el punt anterior, del supòsit que els documents tindran ja una signatura del tipus longeu: XAdES-A o PAdES-LTV. A aquestes signatures s'incorporarà un nou segell de temps, ja que l'estructura permet aquesta possibilitat. Aquest nou segell de temps estarà generat amb un certificat recent, amb un període de validesa superior a l'actual en la signatura que s'ha de ressegellar, amb una longitud de clau que no estarà compromesa i amb un algoritme que no estigui subjecte a l'obsolescència criptogràfica de l'algoritme en el moment de la seva emissió.

Pel que fa a firmes realitzades a través d'acreditació de la identitat i d'evidències de la voluntat de signatura, es farà el ressegellament de la signatura secundària.

En definitiva, el ressegellament consisteix, doncs, a mantenir la validesa de la signatura incorporant-hi nou material criptogràfic, concretament segells de data i hora, a la mateixa estructura de la signatura electrònica.

El procés de revisió de la validesa de les signatures electròniques en la Universitat és el següent:

1. Per a signatures generades dins de l'entorn de la Universitat (aquelles signatures generades amb les eines de signatura internes), en fase de tramitació, es generaran les signatures electròniques en format preservable, és a dir, en format de signatura d'arxiu.

Així, per a documents XML les signatures es transformaran en XAdES-A, com podria ser el cas del foliat de l'expedient, i per als documents PDF es generarà una signatura electrònica en format PAdES - LTV.

2. Les signatures que provenen de plataformes externes (altres administracions, eines de client, etc.) es completaran, si s'escau. Aquest procés de compleció es farà després d'haver tancat i foliat l'expedient. Per a documents XML les signatures es passaran a XAdES - A, com ara les factures, i per als documents PDF es generarà una signatura electrònica en format PAdES - LTV.

3. En cas que no sigui possible generar una signatura preservable per a algun document, al més aviat possible s'haurà de generar una còpia autèntica del document electrònic original, amb una actuació administrativa automatitzada o amb la signatura electrònica d'un funcionari habilitat. Aquesta signatura ja serà en un format preservable i s'haurà de substituir l'original per aquesta còpia autèntica .

4. Per a signatures electròniques basades en identitat més voluntat de signatura, es generarà la signatura mitjançant el segell electrònic ja amb un format preservable (PAdES-LTV).

5. Per a signatures electròniques basades en CSV, es mantindrà en el repositori de consulta una versió del document amb signatures electròniques preservades.

6. Per a signatures biomètriques, es generarà una signatura mitjançant segell electrònic ja amb format preservable (PAdES-LTV).

12.2. CÒPIES ELECTRÒNIQUES DE DOCUMENTS SIGNATS DIGITALMENT.

En el cas que algun document tingui caducada la signatura electrònica, la Universitat podrà generar-ne una còpia autèntica mitjançant la signatura electrònica basada en un certificat de segell electrònic i actuació administrativa automatitzada, o la còpia d'aquest mitjançant la signatura electrònica d'una persona funcionària habilitada, sempre que:

1. Hi hagi evidències suficients que la signatura del document era vàlida en el moment d'accedir a la Universitat.

2. Que el document no s'ha modificat ni s'ha substituït per un altre durant tot el temps que ha estat a la Universitat.

Només en aquests casos se'n podrà generar la còpia electrònica. La còpia es farà amb una diligència del secretari o secretària general de la Universitat, o persona en qui delegui, un cop analitzats els antecedents dels documents que tinguin la signatura caducada i se'n pugui assegurar els dos punts anteriors.

A continuació, es generarà un nou document, amb el mateix contingut i format que l'original, i es podrà signar amb un segell electrònic o amb un certificat digital d'una persona funcionària habilitada. Aquesta signatura ha de complir els requeriments d'aquesta política pel que fa a format i completesa. Així mateix s'ha d'indicar, en les corresponents metadades que el document és una còpia autèntica d'un document original electrònic o d'una còpia electrònica autèntica.

Finalment s'ha de substituir el document original amb la signatura caducada pel nou document dins el sistema de gestió documental de la Universitat.

13. SEGELL DE TEMPS

El segell de temps és una signatura electrònica generada per un tercer de confiança basat en un certificat digital especialment destinat a l'efecte. Les seves característiques principals són:

- Evidència de la data i hora en què s'ha produït un acte. S'utilitza conjuntament amb un document en qualsevol format i que pot estar signat electrònicament. El segell de temps pot fer referència a:
  - Signatura del document: el segell de temps està associat a la signatura electrònica.
  - Creació del document: el segell de temps està associat al document.

- Mitjançant un proveïdor de segells de temps, es constatarà la data i hora de l'instant en què s'ha realitzat l'acte. El proveïdor podrà ser tant el Consorci AOC, a través de la plataforma PSIS, com la TSA d'@firma del Ministerio, en funció de les aplicacions que utilitzi la Universitat.

- Es disposa d'un proveïdor de segell de temps alternatiu per garantir la disponibilitat d'aquest procediment. Aquest proveïdor ha d'estar sincronitzat amb fonts fiables de temps com ara la Reial Armada Espanyola reconeguda com a tal per l'Esquema Nacional d'Interoperabilitat. Hi ha diverses fonts de segells de temps al mercat i caldrà triar la que més convingui segons de la disponibilitat del servei, la qualitat de proveïdor, el cost del servei, la possibilitat de signatura d'acords de nivell de servei i l'autoritat certificada per a aquest servei.

El procés consisteix a crear una evidència electrònica sobre una signatura electrònica: es calcula el resum criptogràfic del document i les signatures electròniques (en el cas del ressegellament), és a dir, una operació matemàtica que s'aplica al conjunt d'informació sobre el qual s'emet el segell de temps i obté una cadena de bits anomenada coixinet, la qual se xifra amb la clau privada del certificat de segell de temps utilitzat per fer l'operació. Es retorna aquesta firma conjuntament amb la data i hora de l'operació, així com informació sobre el certificat de segell de temps utilitzat per fer la signatura.

ANNEX I. CONCEPTES EN SIGNATURA ELECTRÒNICA

1. DEFINICIÓ JURÍDICA DE LA SIGNATURA ELECTRÒNICA

Cal tenir en consideració la definició de les classes de signatura des d'un punt de vista jurídic:

- Ordinària: conjunt de dades en forma electrònica, consignades conjuntament amb d'altres o que hi estan associades, que poden ser utilitzades com a mitjà d'identificació de la persona que firma (identificació s'ha d'entendre com autenticació d'entitats, segons el que estableix la Directiva 99/93/CE, de 13 de desembre, de signatura electrònica).
- Signatura electrònica avançada: signatura electrònica que permet identificar la persona signant i detectar qualsevol canvi posterior de les dades signades, que està vinculada a la persona signant de manera única i a les dades a què fa referència. Ha estat creada per mitjans que la persona signant pot mantenir sota el seu control exclusiu.
- Signatura electrònica reconeguda: signatura electrònica avançada que es basa en un certificat reconegut i ha estat generada mitjançant un dispositiu segur de creació de signatura, segons estableix l'article 3.3 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.

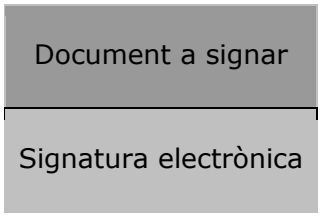
Per a les definicions anteriors, s'utilitza un concepte clau, el del certificat reconegut, que segons l'article 11.1 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, el defineix com aquells certificats electrònics emesos per un prestador de serveis de certificació, que compleixen amb els requisits establerts en la mateixa llei quant a la comprovació de la identitat i la resta de circumstàncies de les persones sol·licitants, i la fiabilitat i les garanties dels serveis de certificació que prestin.

2. FONAMENTS TÈCNICS DE LA SIGNATURA ELECTRÒNICA

Es defineixen els tipus de signatura des d'un punt de vista tècnic:

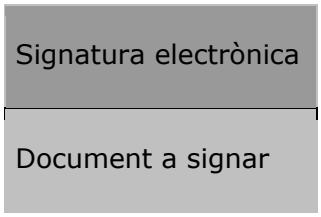
- Signatura djunta: les dades de signatura resideixen en el document signat. Per tant, el mateix document disposa de tota la informació per comprovar-ne l'autenticitat i integritat, així com la informació necessària per validar la signatura. Cal diferenciar entre dos tipus de signatura adjunta:
  - Incrustada (enveloped): en aquest cas el document signat està compost pel contingut del mateix document que s'ha designar més la signatura d'aquest contingut.

Document signat



- Embolcallant (enveloping), signatura electrònica que inclou el document electrònic que s'ha signat.

  Document signat



- Signatura separada: Les dades de signatura resideixen fora del document que s'ha de signar, però hi estan associades. Les dades de la firma es mantindran per separat durant tot el cicle de vida del document. Per validar la signatura cal crear un document d'evidència electrònica que contingui de forma conjunta el document i les dades completes de la signatura.

3. NIVELL DE SIGNATURES:

- Signatura simple: el document conté una única signatura.
- Signatura múltiple: el document conté dues signatures o més. Consisteix que diverses persones signen el document consecutivament. Aquesta signatura es pot aplicar sobre el document original cada vegada, que s'anomena signatura **paral·lela**, o sobre el document signat, que s'anomena signatura **niada.**

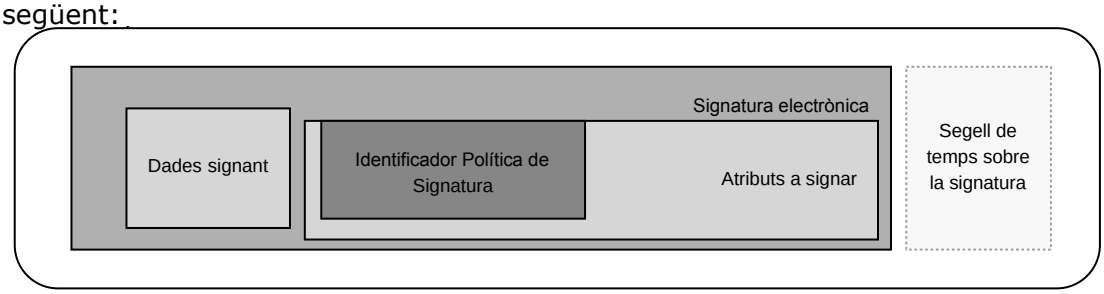
La signatura múltiple s'utilitza en diverses situacions en el marc dels procediments de la Universitat, com ara en la signatura de documents electrònics per més d'una persona o en el ressegellament de documents (vegeu apartat 11) ja signats per actualitzar-ne la validesa legal al llarg de el temps, abans que no pugui quedar en entredit la validesa criptogràfica de la signatura electrònica.

4. ESPECIFICACIONS TÈCNIQUES DELS FORMATS DE SIGNATURA ELECTRÒNICA

a) Signatura electrònica amb política de signatura i amb segell de temps

Format de signatura derivat de la signatura electrònica avançada amb identificador de política (en la nostra nomenclatura, normativa de signatura electrònica), també coneguda EPES, amb la incorporació d'un segell de temps que situa la signatura electrònica en un moment determinat del temps.

La representació gràfica d'aquest format de signatura, identificat com AdES-T, és la següent:



La signatura electrònica amb política explícita (XAdES-T) ha de contenir tots els elements que es llisten a continuació dels quals tots, excepte l'últim, corresponen al format XAdES-EPES (signatura electrònica avançada amb identificador de política):

- Les dades signades per la persona usuària, com el contingut d'un document electrònic o una imatge
- El tipus de contingut signat: ContentType
- El resum criptogràfic del missatge: MessageDigest
- El certificat emprat per signar: ESSSigningCertificate o OtherSigningCertificate
- La data i hora de la signatura: SigningTime (opcional)
- Les pistes sobre el contingut signat: ContentHints (opcional)
- La identificació del contingut: ContentIdentifier (opcional)
- La referència als continguts: ContentReference (opcional)
- La indicació del tipus de compromís: CommitmentTypeIndication (opcional)
- La localització del signant: SignerLocation (opcional)
- Els atributs del signant: SignerAttributes (opcional)
- El segell de data i hora sobre el contingut: ContentTimestamp (opcional)
- Contrafirma: Countersignature (opcional)
- Identificació de la política de signatura: SignaturePolicyIdentifier (en la nostra nomenclatura, normativa de signatura electrònica)
- Segell de data i hora de la signatura: SignatureTimeStamp

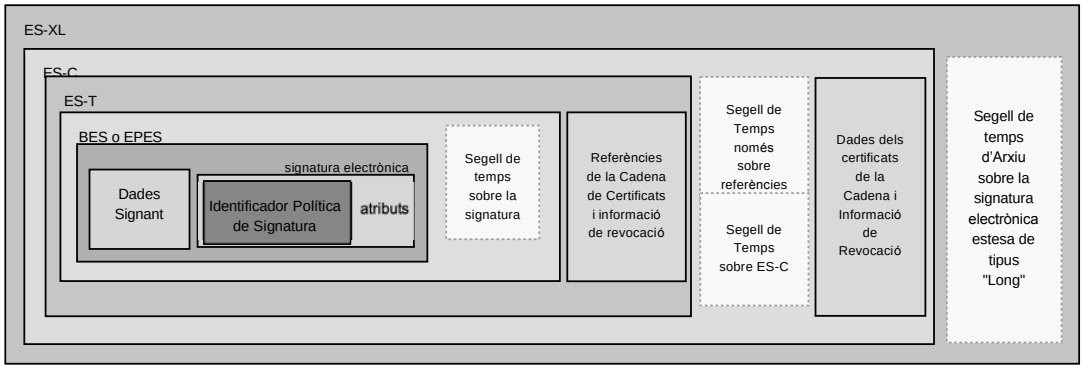
b) Signatura electrònica d'arxiu

La signatura electrònica d'arxiu accepta dos formats:

b.1. Signatura AdES

La signatura electrònica d'arxiu (AdES-A) parteix del format de signatura electrònica extensa (XL), que inclou tots els elements de verificació de la vigència del certificat per poder repetir la validació de manera autònoma. Sobre aquest format extens de signatura, afegeix un segell de temps, que preveu el ressegellament successiu de manera periòdica. Aquest és el format de signatura més complet i està pensat expressament per als documents als quals es vol garantir la disponibilitat al llarg de el temps.

Signatura electrònica d'Arxiu (ES-A)



- La signatura electrònica XML: Signature
- El certificat utilitzat per signar: SigningCertificate o KeyInfo: X509Data
- La data i hora de la signatura: SigningTime (opcional)
- El format de l'objecte de dades signat: DataObjectFormat (opcional)
- La indicació del tipus de compromís: CommitmentTypeIndication (opcional)
- El lloc de producció de la signatura: SignatureProductionPlace (opcional)
- El paper de la persona que signa: SignerRole (opcional)
- El segell de data i hora sobre el contingut: AllDataObjectsTimeStamp o IndividualDataObjectsTimeStamp (opcional)
- La contrafirma: Reference o CounterSignature (opcional)
- Identificació de la política de signatura: SignaturePolicyIdentifier (en la nostra nomenclatura, normativa de signatura electrònica)
- Segell de data i hora de la signatura: SignatureTimeStamp
- Referències completes de certificats: CompleteCertificateRefs
- Referències completes de revocació: CompleteRevocationRefs
- Referències completes de certificats d'atributs: AttributeCertificateRefs
- Referències completes de revocació d'atributs: AttributeRevocationRefs
- Segell de data i hora sobre la signatura completa: SigAndRefsTimeStamp
- Segell de data i hora sobre les referències de certificats i revocacions: RefsOnlyTimeStamp
- Valors de certificats: CertificateValues
- Valors de revocació: RevocationValues
- Valors de certificats d'atribut: AttrAuthoritiesCertsValues
- Valors de revocació de certificats d'atribut: AttributeRevocationValues
- Segell de data i hora d'arxiu: ArchiveTimeStamp Obligatori

b.2. Signatura PAdES-LTV

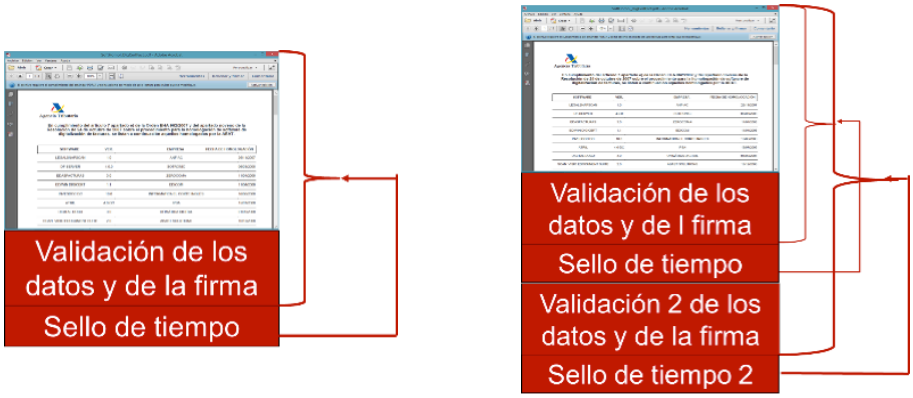
La signatura electrònica de llarga durada (Long Term Validation) és un format específic de la família PAdES. La signatura més bàsica, la PAdES Basic, s'especifica

en la ISO 32000 - 1. La signatura PAdES EPES inclou la signatura electrònica del document (en format CAdES - BES), amb segell de temps (recomanat) i una resposta de validació d'un servei OCSP (recomanat). Pot incloure, a més, motius de signatura, el lloc de la signatura, dades de contacte del signant i la política de signatura.

Sobre aquestes firmes es pot construir una signatura PAdES - LTV que inclou els elements següents, per a la verificació de les signatures i del contingut: les autoritats de certificació en el moment de la validació eren correctes, la resposta del servei de validació OCSP i un segell de temps sobre aquesta verificació de signatures.

A la signatura es pot afegir, a posteriori, un nou comprovant de verificació que garanteix que la que es va fer continua sent vàlida i, a més, s'afegeix un nou segell de temps que protegeix les firmes i les validacions.

Exemple:



Aquesta signatura s'utilitza per a qualsevol document que hagi de conservar-se més que el temps de validesa del segell de temps corresponent.

C) CODI SEGUR DE VERIFICACIÓ

c.1. Generació del codi segur de verificació

El codi segur de verificació consisteix en una seqüència de lletres i números generada de manera pseudoaleatòria i associada unívocament al document. Es crea basant-se en un sistema de generació d'un URI (identificador uniforme de recursos) únic per a cada un dels documents electrònics que s'han d'imprimir de forma segura.

La Universitat utilitza el procediment següent per generar els CSV:

1. Es generarà una cadena de caràcters que uneixen l'adreça MAC de servidor, el temps actual en mil·lisegons, un nombre aleatori i la petició rebuda com a cadena de caràcters.

2. Sobre aquesta cadena de caràcters resultant, s'aplicarà un algoritme SHA-2 que es truncarà a 15 bytes.

3. Un cop obtingut aquest codi, es codificarà en base 64 per obtenir 20 caràcters alfanumèrics.

c.2. Procediment de validació dels documents signats amb CSV

Per confrontar els documents, les persones interessades s'han d'adreçar a la seu electrònica de la Universitat.

A través de la seu electrònica es podrà accedir al servei de validació de documents

electrònics amb codi segur de verificació. En aquest servei s'ha d'introduir íntegrament el CSV que consta en el document que es compara i si el CSV coincideix amb un document disponible per a la consulta, el sistema retornarà:

- En el cas de documents generats d'origen amb CSV, el document original des de la ubicació corresponent en el sistema de gestió documental.
- En el cas de còpies autèntiques de documents no previstos per la seva impressió segura des de la creació, el document còpia autèntica amb canvi de format des de la ubicació específica de el sistema de gestió documental d'impressió segura.

ANNEX II. CASOS D'ÚS DE LA SIGNATURA ELECTRÒNICA.

Abans de descriure els casos d'ús identificats de signatura electrònica, és necessari tenir en compte el concepte d'expedient administratiu, ja completament electrònic i el foliat, també electrònic. La definició d'expedient administratiu està establerta a l'article 70 de la Llei 39/2015:

- S'entén per expedient administratiu el conjunt ordenat de documents i actuacions que serveixen d'antecedent i fonament a la resolució administrativa, així com les diligències encaminades a executar-la.

- Els expedients tenen format electrònic i es formen mitjançant l'agregació ordenada de tots els documents, proves, dictàmens, informes, acords, notificacions i altres diligències. Així mateix, ha de constar en l'expedient una còpia electrònica certificada de la resolució adoptada.

- Quan en virtut d'una norma sigui necessari remetre l'expedient electrònic, s'ha de fer d'acord amb el que preveuen l'Esquema Nacional d'Interoperabilitat i les corresponents normes tècniques d'interoperabilitat i enviar-lo complet, foliat, entrat i acompanyat d'un índex, també autenticat, dels documents que contingui. L'autenticació d'aquest índex garanteix la integritat i immutabilitat de l'expedient electrònic generat des del moment de la signatura i permet recuperar-lo sempre que sigui necessari. És admissible que un mateix document formi part de diferents expedients electrònics.

Per tant, l'índex de l'expedient s'ha de desar en un fitxer XML, que ha d'estar signat amb segell electrònic de la Universitat. Aquesta signatura ha de tenir format XML, més concretament signatura XAdES - A.

Després de definir els conceptes d'expedient electrònic i de foliació, es descriuen els escenaris identificats:

1. SIGNATURA ELECTRÒNICA D'UN DOCUMENT ELECTRÒNIC

Permet signar electrònicament documents en suport electrònic en qualsevol moment del cicle de vida, tant documents creats o com generats electrònicament per altres aplicacions.

Les característiques principals d'aquest escenari són:

- Es fa la signatura sobre un document original en suport electrònic.

- El document original i les signatures s'han d'incorporar al sistema.

- Per assegurar la integritat i l'autenticitat de la signatura rebuda de l'aplicació de creació de signatures, serà necessari validar-la, utilitzant un servei o autoritat de validació.

- Després de validar-la, si és possible dins el mateix dia de la signatura, s'ha de completar a un format PAdES-LTV o XAdES-A.

- El document electrònic estarà en qualsevol format dels acceptats per la Universitat, preferiblement PDF/A i XML, sempre que sigui necessari garantir-ne la preservació al llarg del temps.

- El document es podrà signar diverses vegades i diferents usuaris.

- Es podrà signar en paral·lel i/o de forma niada.

Finalment, concretant el tipus de signatura, s'estableixen les característiques següents o requeriments:

- Classe de signatura: avançada o reconeguda.
- Tipus de certificat: per a les signatures generades per la Universitat: certificat de treballador públic del Consorci AOC ,certificat de segell electrònic del Consorci AOC o certificat de representant tant del Consorci AOC com de la FNMT. Per a les signatures generes pels estudiants o tercers (empreses, persones físiques, etc.):qualsevol certificat definit al punt 6 d'aquest document.
- Formats: PAdES_LTV amb segell de temps o XAdES-A.
- Segell de temps: sí
- Nivell de signatura: simple, múltiple (imbricada o paral·lel)
- Tipus de signatura: adjunta

2. CÒPIA AUTÈNTICA ELECTRÒNICA DE DOCUMENTS EN PAPER

Permet obtenir documents electrònics amb consideració de còpia autèntica a partir de documents en suport paper.

Les característiques principals d'aquest escenari són:

- Consisteix en la signatura electrònica d'un document digitalitzat, en format PDF o PDF/A, per crear una còpia autèntica electrònica.
- La signatura és necessària per garantir la integritat i l'autenticitat del document digitalitzat, així com la data de la digitalització.
- El personal de la Universitat que digitalitza la documentació és el responsable de signar electrònicament el document digitalitzat i ha d'estar habilitat per fer-ho.
- Els documents digitalitzats se signen incorporant-hi un segell de temps. Es genera una signatura PAdES-LTV amb segell de temps.
- Per assegurar la integritat i l'autenticitat de la signatura rebuda de l'aplicació de creació de signatures, serà necessari validar-la.

Finalment, concretant el tipus de signatura, s'estableixen les característiques següents o requeriments:

- Tipus de signatura: avançada
- Tipus de certificat: certificat de segell electrònic del CAOC.
- Formats: PAdES-LTV.
- Segell de temps: sí
- Nivell de signatura: simple

- Tipus de signatura: adjunta

3. CÒPIA AUTÈNTICA ELECTRÒNICA D'UN DOCUMENT SIGNAT ELECTRÒNICAMENT

Permet obtenir còpies electròniques de documents originals signats electrònicament aplicant un canvi de format a PDF/A per lliurar-los a l'estudiant o a altres administracions. Aquest seria el cas de generar un document electrònic com a còpia autèntica d'un altre document electrònic en què s'incorpora un codi segur de verificació (CSV), de manera que es pugui imprimir i posteriorment, mitjançant aquest CSV, comprovar a la seu electrònica que el document imprès esmentat no s'ha manipulat.

Les característiques principals d'aquest escenari són:

- A partir d'un document signat electrònicament se n'obté una còpia autèntica (per exemple, en PDF), signada digitalment, per lliurar-la a la persona interessada.
- La còpia de el document electrònic ha d'estar en un format normalitzat i estandarditzat abans de signar-la.
- El document se signarà de manera automatitzada una única vegada amb segell electrònic de la Universitat.

Finalment, concretant el tipus de signatura s'estableixen les característiques o requeriments següents:

- Tipus de signatura: avançada
- Tipus de certificat: certificat de segell electrònic del CAOC
- Formats: PAdES-LTV amb segell de temps més CSV
- Segell de temps: sí
- Nivell de signatura: simple
- Tipus de signatura: adjunta

4. PROCESSOS DE SIGNATURA AUTOMATITZADA

Permet signar diversos documents de forma automàtica amb garanties jurídiques. No requereix la intervenció del signant en el procés de signatura, ja que només es pot fer amb certificats de segell electrònic.

Les característiques principals d'aquest escenari són:

- Signatura de diversos documents de forma automàtica.
- El document electrònic pot estar en qualsevol format dels acceptats (PDF, PDF / A i XML).
- Es desarà al repositori segur al servidor de la Universitat, tant els certificats digitals com les corresponents claus privades que han de permetre generar processos de signatura automatitzada.

Un cop descrites les característiques concretes d'aquest escenari, s'enumeren els criteris d'aplicació i actuació:

- Aquest escenari està pensat per a aquelles tasques en què s'han de signar diversos documents de forma automatitzada amb garanties jurídiques.
- S'utilitzarà un certificat de segell electrònic, que signarà els documents en nom de l'aplicació i de la Universitat.

Finalment, concretant el tipus de signatura s'estableixen les característiques o requeriments següents:

- Tipus de signatura: avançada per als certificats de segell electrònic que són avançats
- Tipus de certificat: certificat de segell electrònic del CAOC
- Formats: documents XML: XAdES-BES i es completarà posteriorment a XAdES-A. Documents PDF o PDF/A: PAdES-BES i es completarà posteriorment a PAdES-LTV amb segell de temps.
- Segell de temps: sí
- Nivell de signatura: simple
- Tipus de signatura: adjunta

Aquest escenari abasta diversos àmbits que es podrien arribar a identificar com a subescenaris diferents, per exemple:

- Signatura automatitzada en processos de digitalització massiva.
- Ressegellament de documents per actualitzar-ne la validesa criptogràfica.
- Procediments d'intercanvi d'informació entre administracions.

5. INCORPORACIÓ DE DOCUMENTS SIGNATS DIGITALMENT PER PART DE LA CIUTADANIA.

En el cas en què un ciutadà lliuri un document signat electrònicament per ell, serà necessari:

- Validar les signatures electròniques del document. La validació es farà d'acord amb el que estableix el punt 11 de la present política.
- En el cas que les signatures no siguin XAdES-A o PAdES-LTV, s'hauran de completar fins a un d'aquests nivells. En el cas que no es puguin completar, un funcionari habilitat haurà de generar una còpia electrònica XAdES-A o PAdES-LTV amb segell de temps del document presentat mitjançant un segell electrònic o signatura.
- A continuació, s'incorporarà al sistema el document amb les signatures completes.

Finalment, concretant el tipus de signatura, s'estableixen les característiques o requeriments següents:

- Tipus de signatura: avançada o reconeguda en funció dels certificats utilitzats per a la signatura.

- Tipus de certificat: qualsevol certificat dels definits als punts 6 i 7 d'aquest document.
- Formats: per a documents XML: XAdES-T i per conservar-los, XAdES-A. Per a documents PDF: PAdES-T i per conservar-los, PAdES-LTV.
- Segell de temps: aconsellat. Un cop completada la signatura: sí.
- Nivell de signatura: simple, múltiple (niada o paral·lel)
- Tipus de signatura: adjunta.

6. SIGNATURA ELECTRÒNICA BIOMÈTRICA D'UN DOCUMENT ELECTRÒNIC

Permet signar electrònicament documents en suport electrònic en qualsevol moment del cicle de vida, per exemple, documents creats o generats electrònicament per altres aplicacions.

Les característiques principals d'aquest escenari són:

- Es fa la signatura sobre un document original en suport electrònic.
- La signatura forma part del mateix document.
- Els documents originals amb les signatures s'han d'incorporar al sistema.
- El mateix sistema garanteix la integritat i l'autenticitat de la signatura i, per tant, no és necessari validar-la.
- En el cas que el document s'hagi de conservar al llarg del temps, se'n farà la signatura electrònica avançada amb un segell electrònic.
- En aquest cas sí que s'haurà de validar la signatura avançada corresponent. Cal incorporar al sistema l'evidència de validació, que en el nostre cas serà la signatura completa. Com que és en PDF, la trobarem al mateix document amb signatura adjunta.
- El document electrònic ha d'estar en format PDF.
- El document el podran signar diferents usuaris diverses vegades .
- Es podrà signar només en paral·lel.
- En el cas que els documents s'hagin de conservar durant períodes llargs de temps, la signatura electrònica que es generarà amb el segell electrònic serà PDF-LTV.

Finalment, concretant el tipus de signatura, s'estableixen les característiques o requeriments següents:

- Classe de signatura: avançada.
- Tipus de certificat: per al xifratge de les dades biomètriques i el resum criptogràfic del document, el certificat d'encriptació guardat als servidors de la Universitat. Per a les signatures generades amb el segell electrònic de la Universitat, certificat de segell electrònic del CAOC.
- Formats
    - Signatura biomètrica: signatura específica.
    - Signatura amb segell electrònic: PAdES en format PAdES-LTV.

- Segell de temps: sí (per a la signatura del segell electrònic)
- Nivell de signatura: simple, múltiple (niada o paral·lel)
- Tipus de signatura: adjunta.
- Normativa de signatura: aquella que s'hi hagi d'aplicar segons el tipus de document generat o acte realitzat.

7. SIGNATURA MITJANÇANT CODI SEGUR DE VERIFICACIÓ (CSV)

Permet signar documents a través de l'actuació administrativa automatitzada, afegint un codi segur de verificació (CSV) al document definitiu.

Aquest procés pot incorporar també una signatura amb segell electrònic. En aquest cas tampoc es requereix la intervenció del signant en el procés de signatura, ja que només es pot fer amb certificats de segell electrònic.

Les característiques principals d'aquest escenari són:

- Signatura de diversos documents de forma automàtica.
- El document electrònic ha d'estar en format PDF/A.
- Opcionalment, el document electrònic se signa amb un segell electrònic de la Universitat. Aquesta signatura ha de ser PAdES-LTV amb segell de temps.
- El document signat es guarda al repositori de documents amb CSV, des d'on es pot consultar a través de la seu electrònica introduint-hi aquest CSV.

Els criteris d'aplicació i actuació són:

- Aquest escenari està pensat per a aquelles tasques en què s'han de signar diversos documents de forma automatitzada amb garanties jurídiques, el destinatari dels quals és un ciutadà.
- S'incorpora el CSV més un text descriptiu de com validar-lo través de la seu electrònica.
- Es podrà utilitzar un certificat de segell electrònic, que signaria els documents en nom de l'aplicació i de la Universitat.

Finalment, concretant el tipus de signatura s'estableixen les característiques o requeriments següents:

- Tipus de signatura: avançada.
- Tipus de certificat: sense certificat i en alguns casos amb certificat de segell electrònic del CAOC.
- Formats: per a documents PDF o PDF/A, signatura amb CSV i en el cas de signatura amb segell, PAdES-EPES, la qual es podrà completar a PAdES-LTV amb segell de temps.
- Segell de temps: no, excepte si s'inclou signatura amb segell.
- Nivell de signatura: simple.
- Tipus de signatura: adjunta.

ANNEX III. NORMATIVA APLICABLE I ESTÀNDARDS INTERNACIONALS.

En aquest apartat es recullen les normatives i estàndards internacionals que s'han tingut en compte per definir d'aquesta política.

La recent revolució en l'ús del document electrònic és el resultat de l'aparició de canvis normatius que han donat impulsat les eines telemàtiques i han equiparat, en determinades circumstàncies, els documents en format electrònic als documents en formats més tradicionals.

A més, tant en l'àmbit nacional com a la Unió Europea o internacionalment, les organitzacions d'estandardització tècnica han definit i documentat els criteris i formats que s'utilitzaran per gestionar els documents digitals en tots els seus aspectes, de manera que se'n garanteix la validesa jurídica.

A continuació s'exposa la llista de normatives i estàndards internacionals que s'han tingut en compte per definir la política de signatura i segell electrònics i de certificats de la Universitat Rovira i Virgili.

Normativa aplicable

- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques
- Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic
- Llei 15/2014, de 16 de setembre, de racionalització del sector públic i altres mesures de reforma administrativa
- Llei 25/2015, de 28 de juliol, de mecanisme de segona oportunitat, reducció de la càrrega financera i altres mesures d'ordre social
- Reial decret 3/2010, de 8 de gener, de l'Esquema Nacional de Seguretat
- Reial decret 4/2010, de 8 de gener, de l'Esquema Nacional d'Interoperabilitat
- Resolució de 19 de juliol de 2011, de la Norma tècnica d'interoperabilitat de política de signatura electrònica i de certificats de l'administració
- Resolució de 19 de juliol de 2011, de la Norma tècnica d'interoperabilitat d'expedient electrònic
- Reglament europeu (UE) 910/2014 del Parlament Europeu i Consell, sobre la identificació electrònica i els serveis de confiança en les transaccions electròniques en el mercat interior
- Decisió d'execució (UE) 2015/1506 de la Comissió de 8 de setembre de 2015, per la qual s'estableixen les especificacions relatives als formats de les firmes electròniques avançades i els segells avançats que han de reconèixer els organismes del sector públic d'acord amb els articles 27, apartat 5 i 37, apartat 5 de l'anterior Reglament
- Llei 59/2003, de 19 de desembre, de signatura electrònica
- ORDRE GRI/233/2015, de 20 de juliol, per la qual s'aprova el Protocol d'identificació i signatura electrònica
- Resolució de 14 de juliol de 2017, de la Secretaria General d'Administració Digital, per la qual s'estableixen les condicions d'ús de signatura electrònica no criptogràfica, en les relacions dels interessats amb els òrgans administratius de l'Administració General de l'Estat i els seus organismes públics

ESTÀNDARDS INTERNACIONALS I ALTRES CONVENCIONS

- Estàndards tècnics de signatura electrònica compartits sota llicència d'ús BY - NC - SA del CreativeCommons de l'empresa Astrea la Infopista Jurídica SL: http://astrea.es/web12/biblioesp/_estandares-tecnicos/
- ETSI RFC 2315 (1998), ETSE RFC 2630 (1999), IETF RFC 3369 (2002), IETF RFC 3852 (2004): PKCS # 7: CryptographicMessageSyntax (CMS)
- ETSI TS 101 733. v.1.6.3, v1.7.4 i v.1.8.1: Electronic Signatures andInfrastructures (ESI), CMS Advanced Electronic Signatures (CAdES)
- ETSI TS 119 122-3: Electronic Signatures andInfrastructures (ESI),CAdES digital signatures, Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES
- ETSI TR 119 124-1: Electronic Signatures andInfrastructures (ESI),CAdES digital signatures - TestingConformanceand Interoperability, Part 1: Overview.
- ETSI TS 119 124-2: Electronic Signatures andInfrastructures (ESI),CAdES digital signatures - TestingConformanceand Interoperability, Part 2: Test suites for testinginteroperability of CAdESbaseline signatures.
- ETSI TS 119 124-3: Electronic Signatures andInfrastructures (ESI),CAdES digital signatures - TestingConformanceand Interoperability, Part 3: Test suites for testinginteroperability of extendedCAdES signatures.
- ETSI TS 119 124-4: Electronic Signatures andInfrastructures (ESI),CAdES digital signatures - TestingConformanceand Interoperability, Part 4: TestingConformance of CAdESbaseline signatures.
- ETSI TS 119 124-5: Electronic Signatures andInfrastructures (ESI),CAdES digital signatures - TestingConformanceand Interoperability, Part 5: TestingConformance of extendedCAdES signatures.
- ETSI TR 119 134-1 Electronic Signatures andInfrastructures (ESI),XAdES digital signatures - TestingConformanceand Interoperability, Part 1: Overview.
- ETSI TS 119 134-2: Electronic Signatures andInfrastructures (ESI),XAdES digital signatures - TestingConformanceand Interoperability, Part 2: Test suites for testinginteroperability of XAdESbaseline signatures.
- ETSI TS 119 134-3: Electronic Signatures andInfrastructures (ESI),XAdES digital signatures - TestingConformanceand Interoperability, Part 3: Test suites for testinginteroperability of extendedXAdES signatures.
- ETSI TS 119 134-4: Electronic Signatures andInfrastructures (ESI),XAdES digital signatures - TestingConformanceandInteroperability, Part 4: TestingConformance of XAdESbaseline signatures
- ETSI TS 119 134-5: Electronic Signatures andInfrastructures (ESI),XAdES digital signatures - TestingConformanceandInteroperability, Part 5: TestingConformance of extendedXAdES signatures
- ETSI TS 119 142-3: Electronic Signatures andInfrastructures (ESI),PAdES digital signatures, Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS)
- ETSI TR 119 144-1 Electronic Signatures andInfrastructures (ESI),PAdES digital signatures - TestingConformanceandInteroperability, Part 1: Overview
- ETSI SR 019 020: Theframework for standardization of signatures,Standards for AdES digital signatures in mobileanddistributed environments

- IETF RFC 5280 (2008): Internet X.509 PublicKeyInfrastructureCertificateand CRL Profile
- IETF RFC 2560 (1999): X.509 Internet PublicKeyInfrastructure, Online Certificate Status Protocol – OCSP
- IETF RFC 3126 (2001): Electronic Signature Formats for Long Term Electronic Signatures
- ISO 19005 (2008): Format del fitxer / A-1
- ISO / TR 18492: 2005- Long-termpreservation of electronic document-basedInformation
- UNE - ISO / TR 13008: 2010 - Informació i documentació. Conversió de documents digitals i processos de migració
- ETSI TS 102 176-1 V2.0.0 Electronic Signatures andInfrastructures (ESI); AlgorithmsandParameters for Secure Electronic Signatures; Part 1: Hashfunctionsandasymmetricalgorithms
- ETSI TS 102 023, v.1.2.1 i v.1.2.2. Electronic Signatures andInfrastructures (ESI); Policyrequirements for time-stampingauthorities
- ETSI TS 102 023, v.1.2.1 i v.1.2.2. Electronic Signatures andInfrastructures (ESI); Policyrequirements for time-stampingauthorities
- ETSI TS 101.861 V1.3.1 Timestampingprofile
- ETSE TR 102.038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.
- ETSE TR 102.041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.
- ETSE TR 102.045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.
- ETSE TR 102.272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.
- IETF RFC 2560, X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP.
- IETF RFC 3125, Electronic Signature Policies.
- IETF RFC 3161 actualitzada per RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- IETF RFC 5280, RFC 4325 i RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.
- IETF RFC 5652, RFC 4853 i RFC 3852, Cryptographic Message Syntax (CMS).
- ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".