INSTRUCCIONS DE DESENVOLUPAMENT DE LA POLÍTICA D'IDENTITAT I SIGNATURA ELECTRÒNIQUES

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Juliol de 2022

SUMARI

1. INTRODUCCIÓ I OBJECTE

La Universitat Politècnica de Catalunya (UPC) en la seva estratègia d'implantació de l'administració electrònica ha aprovat una Política d'Identitat i Signatura Electròniques (en endavant la Política). Aquesta política faculta, en la seva **Disposició final segona, a la Secretaria General** de la UPC per elaborar i actualitzar les instruccions de desenvolupament de la Política.

En aquest context, el present document d'Instruccions de desenvolupament de la Política (en endavant Instruccions) conté els mecanismes tecnològics, els procediments operatius aplicables i els casos d'ús per a la producció de documents electrònics segurs, en el marc del que determina la Política.

2. NORMATIVA APLICABLE

Per a l'elaboració d'aquest document s'ha tingut en compte la normativa aplicable en la matèria tan supranacional, estatal, autonòmica com pròpia. Especialment, es destaca el Reial decret 4/2010, de 8 de gener que estableix l'Esquema Nacional d'Interoperabilitat i, molt concretament, el que es defineix en la Resolució de 27 d'octubre de 2016, que aprova la Norma Tècnica d'Interoperabilitat de Política de signatura i segell electrònics i de certificats de l'Administració, així com la de l'expedient electrònic pel que fa a la signatura electrònica dels expedients. Per la seva banda, s'han considerat com a marc d'elaboració d'aquestes Instruccions els estàndards internacionals i altres convencions en l'àmbit de la signatura electrònica.

El detall de la normativa i de tots els estàndards internacionals que defineixen els diferents formats, tipus de signatura i segell de temps i la resta de tecnologies que s'han fet servir per construir aquestes Instruccions es troben a l'Annex I.

2.1 Normativa d'àmbit europeu

- Reglament Europeu (UE) 910/2014 del Parlament Europeu i Consell, relatiu a la identificació electrònica i als 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 conforme a els articles 27, apartat 5 i 37, apartat 5 de l'anterior Reglament.

2.2 Normativa d'àmbit estatal

- 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 6/2020, de 11 de novembre, reguladora de determinats aspectes del serveis electrònics de confiança.
- 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.
- Reial Decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació o funcionament del sector públic per mitjans electrònics.
- Resolució de 27 d'octubre de 2016 de la Norma Técnica d'Interoperabilitat de Política de Signatura i Segell Electrònic i de Certificats de l'Administració.
- Resolució de 19 de juliol de 2011 de la Norma Tècnica d'Interoperabilitat d'Expedient Electrònic.
- Resolució de 19 de juliol de 2011 de la Norma Técnica d'Interoperabilitat de Document Electrònic.
- Resolució de 14 de juliol de 2017, de la Secretaría General de Administración Digital, segons 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.

2.3 Normativa d'àmbit autonòmic

- Llei 26/2010, de 3 d'agost, del Procediment Administratiu de Catalunya.
- Llei 29/2010, del 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya.

2.4 Normativa pròpia UPC

La política complementa i desenvolupa el que ja preveu la normativa pròpia UPC que es detalla a continuació:

- Reglament d'ús dels mitjans electrònics en l'àmbit de la UPC, aprovat per l'Acord del Consell de Govern de 30 de gener de 2013;
- Normativa de creació i funcionament de la Seu Electrònica, aprovada per la Resolució del rector de 18 d'octubre de 2010;
- Reglament del Registre General de la UPC, aprovat per l'Acord del Consell de Govern d'11 de desembre de 2019;
- Política d'Identitat i Signatura electròniques de la Universitat Politècnica de Catalunya, aprovada per acord CG/2022/03/40, de 5 d'abril de 2022, del Consell de Govern i publicat al Diari Oficial de la Generalitat de Catalunya (DOGC). Núm. 8676 - 26.5.2022

3. DADES DE LES INSTRUCCIONS DE DESENVOLUPAMENT DE LA POLÍTICA D'IDENTITAT I SIGNATURA ELECTRÒNIQUES

3.1 Identificació de les Instruccions

Les dades identificatives de les Instruccions són les que s'inclouen a continuació:

Nom del document	Instruccions de desenvolupament de la Política d'Identitat i Signatura Electròniques de la Universitat Politècnica de Catalunya.
Versió	1.0
Identificador de les Instruccions	Instruccions de desenvolupament de la Política d'Identitat i Signatura Electròniques de la UPC v1.0 de 2022
URL de referència de les Instruccions	https://seuelectronica.upc.edu
Data d'expedició	Juliol 2022 (Data de la signatura electrònica)
Àmbit d'aplicació	Documents i expedients produïts i/o custodiats per la Universitat.
Responsable de les Instruccions	Secretaria General

3.2 Òrgan responsable

La Secretaria General de la UPC és l'òrgan responsable d'aquestes Instruccions, de la seva publicació i actualització, i compta amb el suport del Servei de Desenvolupament Organitzatiu (o la unitat organitzativa responsable de l'administració electrònica a la UPC) per portar a terme la seva implementació i vetllar per la seva correcta aplicació.

4. IDENTITAT ELECTRÒNICA A LA UNIVERSITAT

A partir de les dades recollides a la Identitat Digital, la universitat facilita als membres de la comunitat universitària de la UPC (Estudiants, PDI i PAS) i a les terceres persones que participen o col·laboren puntualment amb la UPC la seva identitat electrònica (credencials, claus, certificació,...).

Les dades a la Identitat Digital provenen:

- treballadors i treballadores públics de la UPC: dades recollides en el sistema de gestió del servei de personal en el moment de la contractació o del nomenament.
- estudiants i les estudiants de la UPC, informació recollida en el sistema de suport a la gestió dels estudis en el moment de la matrícula i la verificació posterior de la identitat en el moment que necessiten unes credencials per fer una signatura.
- personal vinculat, dades recollides en l'aplicació de personal vinculat de la UPC.
- persones externes, que participen puntualment en algun procés de la UPC registre propi i una OTP (contrasenya d'un sol ús).

  En el cas del personal vinculat i de les persones externs es definiran i publicaran a la Seu els procediments de verificació de la identitat previs a la provisió de claus de signatura.

5. CERTIFICATS DIGITALS

5.1 Certificats digitals emprats

A continuació es llisten els prestadors i tecnologies concretes dels certificats digitals emprats per la Universitat i establerts en l'apartat 9 de la Política.

- **Certificats de treballador públic**:
  - **Certificats electrònics qualificats d'Empleat Públic T-CAT (Consorci AOC)**. Correspon al certificat personal d'identificació i signatura reconeguda o qualificada, que conté la dada de la vinculació del treballador amb la Universitat. Es subministra en targeta criptogràfica i l'emet la UPC en qualitat d' Entitat de Registre del Consorci d'Administració Oberta de Catalunya (CAOC). La universitat ha deixat d'emetre aquest tipus de certificat i, els que continuïn vigents, es revocaran a 31 de desembre de 2022.
  - **Certificats electrònics qualificats d'Empleat Públic T-CAT-P (Consorci AOC)**: Correspon al certificat personal d'identificació i signatura avançada, que conté la dada de la vinculació del treballador amb la Universitat. Es subministra en programari i l'emet la UPC en qualitat d'Entitat de Registre del Consorci d'Administració Oberta de Catalunya (CAOC).

- **Certificats de Segell electrònic per actuacions administratives automatitzades**

L'entitat certificadora d'aquest tipus de certificat és el Consorci d'Administració Oberta de Catalunya (CAOC).

En base a la resolució 051-2022-1601/5 del Rector, la universitat disposa de dos segell electrònics emesos pel CAOC:

  - **Serveis administració electrònica**. L'ús d'aquest certificat ha estat "cedit en exclusivitat" al consorci AOC, en concret per fer-lo servir en les aplicacions informàtiques de l'AOC que ha sol·licitat prèviament la UPC.
  - **Serveis eAdministració – Universitat Politècnica de Catalunya**. aquest segell s'haurà d'utilitzar per la signatura dels tràmits o procediments de la UPC subjectes a actuacions administratives automatitzades que figuren com a annex a la resolució de rector i en posteriors instruccions de la secretaria general. La incorporació de nous usos d'aquest certificat ha de ser sol·licitada al Servei de Desenvolupament Organitzatiu (o la unitat organitzativa responsable de l'administració electrònica a la UPC) i haurà de ser aprovada per la secretaria general i publicada a la Seu electrònica.

- **Certificats d'aplicació**

Corresponen als certificats digitals que serveixen per a la identificació d'aplicacions i servidors. Aquest tipus de certificats no són qualificats i no es poden fer servir per generar signatures electròniques, però són rellevants per a la seguretat de molts processos tecnològics.

Aquest tipus de certificats es poden sol·licitar a diferents entitats de certificació i la seva gestió, govern i custòdia correspon a l'Àrea TIC.

En el cas que l'entitat de certificació sigui l'AOC la sol·licitud es realitzarà a traves del Servei de Desenvolupament Organitzatiu (o la unitat organitzativa responsable de l'administració electrònica a la UPC) i el procediment a seguir es troba descrit a l'annex II.

- **Certificats de servidor o de seu electrònica.**

Aquests certificats s'utilitzen per garantir l'accés segur als entorns de tramitació telemàtica amb la Universitat (pàgines web, seu electrònica en el seu cas). Amb aquesta finalitat es podran utilitzar els certificats emesos per autoritats de certificació que tinguin un alt nivell de reconeixement de les seves claus públiques, en els navegadors d'ús més estès.

La gestió, govern i custòdia d'aquest tipus de certificat correspon a l'Àrea TIC. En el cas del certificat de Seu, el Servei de Desenvolupament organitzatiu (o la unitat organitzativa responsable de l'administració electrònica a la UPC) haurà de validar l'entitat certificadora.

5.2 Cicle de vida, emmagatzematge i manteniment dels certificats digitals emprats

5.2.1 Obtenció, renovació i revocació

Per a l'emissió dels certificats digitals del Consorci AOC, la Universitat Politècnica de Catalunya és entitat de registre d'aquest prestador.

Correspon al Servei de Desenvolupament Organitzatiu (o la unitat organitzativa responsable de l'administració electrònica a la UPC) establir els procediments a seguir per a l'obtenció, renovació i revocació dels diferents tipus de certificats en ús a la Universitat, atenen als procediments d'emissió i registre de cada prestador.

La renovació d'aquests procediments es farà d'ofici, sempre que els canvis en les circumstàncies normatives ho facin necessari.

Els procediments vigents en cada moment es faran públics a la Seu Electrònica de la UPC.

En el moment d'aprovar aquesta Instrucció, els procediments que s'estableixen són els que figuren a l'Annex II.

5.2.2 Emmagatzematge dels certificats

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

a) En el repositori de gestió de certificats digitals dels ordinadors dels respectius llocs de treball (per a certificats de treballador públic T-CAT-P o de representant en suport programari i de representant de persona jurídica de la FNMT).

b) En targeta criptogràfica (certificats de representant).

c) En la Plataforma de Custodia de Certificats Digitals del Consorci de Serveis Universitaris de Catalunya (CSUC).

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 certificats de servidor web i de seu electrònica).

Els certificats de segell electrònic es podran instal·lar també en el servidor d'un tercer, prestador de serveis de seguretat, en cas que sigui imprescindible per a l'execució de tasques automàtiques per ordre de la Universitat. Aquest tipus de cessions haurà d'estar descrita en un contracte o conveni, acotada a usos concrets i subjecte a les potestats de verificació apropiades per part de la Universitat.

En el moment de publicació d'aquesta instrucció únicament està "cedit en exclusivitat" el segell **Serveis administració electrònica** tal com es descriu anteriorment.

5.2.3 Manteniment de l'inventari de certificats

El manteniment de l'inventari de certificats personals de la UPC el porta a terme el Servei de Desenvolupament Organitzatiu (o la unitat organitzativa responsable de l'administració electrònica a la UPC). Aquest inventari és únic per a tots els certificats personals, no importa qui sigui l'autoritat de certificació que els ha emès. N'existeix un altre, per a certificats tècnics o tecnològics, sota la responsabilitat de l'Àrea TIC.

Aquests inventaris inclouen la informació necessària per a la gestió del certificat, com a mínim: Titular, autoritat emissora, tipus de certificat i data de caducitat.

Amb una periodicitat mínima semestral s'ha de realitzar una revisió proactiva de la vigència dels diferents certificats digitals. Arrel d'aquesta revisió es pot haver de procedir a la revocació de certificats digitals l'existència dels quals ja no sigui conforme a aquestes instruccions.

En relació amb les polítiques d'emissió, gestió i vigència dels certificats, s'atendrà al que estableixin les autoritats de certificació responsables.

5.3 Certificats digitals admesos

Els interessats que es relacionen amb la Universitat podran fer ús dels certificats relacionats en la llista de prestadors qualificats de serveis electrònics de confiança (TSL), que manté el ministeri competent, per identificar-se en les diferents actuacions en què intervinguin, així com per a la signatura electrònica de documentació en suport digital.

La Universitat es recolza, per a la validació dels certificats, en els serveis que presta el Consorci AOC a través de la plataforma PSIS i el servei VÀLid. Els prestadors o les tipologies de certificat que, malgrat estar a la llista del Ministeri, no siguin reconeguts per aquests sistemes, no podran ser emprats en els tràmits o procediments que impliquin una validació automàtica, en tant no s'hagin actualitzat els criteris de reconeixement del Consorci AOC.

6. SISTEMES DE SIGNATURA ELECTRÒNICA

Els sistemes de signatura electrònica que contempla la Política que es podran utilitzar en el si de les aplicacions corporatives de la Universitat, per a poder garantir l'autenticitat, integritat, inalterabilitat i conservació dels documents signats digitalment, són els següents:

6.1 Signatura electrònica mitjançant certificat digital personal (de treballador públic o de representant)

És el sistema de signatura electrònica en la qual, partint de la clau privada d'un certificat digital d'una persona, es 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.

Des del punt de vista del format tecnològic, la signatura a realitzar serà del tipus PAdES preferiblement quan es pugui generar com a signatura attached a un document PDF, altrament es farà servir signatura detached en format XAdES. Generalment es preferirà que incorporin segell de temps, a menys que s'hagi avaluat per al procediment en concret que el temps previst de custòdia dels documents no ho requereix. Per tant:

	Amb caràcter general, segell de temps	Quan s'hagi avaluat que no cal segell de temps
Quan sigui possible, signatura attached sobre PDF	PAdES-LTV	PAdES-BES
Altrament, signatura detached	XAdES-B-T	XAdES-B-B

Aquests tipus de signatura es podran produir activant el certificat des de la Plataforma de Custòdia de Certificats Digitals que el CSUC ha posat a disposició de les Universitats.

En el cas que un certificat estigui instal·lat a la PCCD, serà necessari configurar les condicions per a la seva activació:

- Com s'autentica davant de la PCCD el signant per tal d'activar el certificat.
- Des de quines ubicacions es permet la connexió per a la seva activació.
- Per a quins usos es pot activar el certificat.

Les signatures o els actes d'autenticació basats en aquests certificats no seran distingibles de les que es produirien si el certificat s'activés directament en l'ordinador de l'usuari. De tota manera, la PCCD ha de guardar registre dels esdeveniments que provoquen l'activació del certificat, incloses les condicions llistades més amunt (forma d'identificació, origen de la connexió i ús autoritzat).

Sempre que un certificat s'instal·li a la PCCD se'n deixarà registre en el inventari de certificats a que fa referència l'apartat 4.2.3.

6.2 Signatura electrònica mitjançant segell electrònic per actuació administrativa automatitzada

Aquest sistema permet la signatura de documents electrònics que emet la Universitat a través de processos automatitzats sense la intervenció directa del personal al seu servei, en què partint de la clau privada d'un certificat digital de segell electrònic es 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.

Des del punt de vista del format tecnològic, la signatura a realitzar serà del tipus PAdES preferiblement quan es pugui generar com a signatura attached a un document PDF, altrament es farà servir signatura detached en format XAdES. Generalment es preferirà que incorporin segell de temps, a menys que s'hagi avaluat per al procediment en concret que el temps previst de custòdia dels documents no ho requereix. Per tant:

	Amb caràcter general, segell de temps	Quan s'hagi avaluat que no cal segell de temps
Quan sigui possible, signatura attached sobre PDF	PAdES-LTV	PAdES-BES
Altrament, signatura detached	XAdES-B-T	XAdES-B-B

6.3 Signatura electrònica basada en un codi segur de verificació per actuació administrativa automatitzada

Tal com indica la Política, en els casos d'actuació administrativa automatitzada també s'admetrà l'ús de Codi Segur de Verificació, Per fer-ho s'haurà de resoldre autoritzant l'automatització del procediment en els termes previstos en l'article 41.2 de la Llei 40/2015.

A més, el codi segur de verificació s'incorpora també en els documents electrònics que han de ser verificats a la Seu electrònica.

Per la confrontació i validació dels documents signats amb CSV, els interessats s'han d'adreçar a la Seu Electrònica de la Universitat, on 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 seva creació, el document còpia autèntica amb canvi de format des de la ubicació específica del sistema de gestió documental d'impressió segura.

6.4 Signatura electrònica basada en claus concertades més les evidències de voluntat de signatura

La usabilitat d'aquesta modalitat de signatura està condicionada per la qualitat del mecanisme de distribució de les identitats. El sistema es basa en la identificació d'una

persona a partir del seu usuari i contrasenya (primera evidència, d'autenticació). La parella de claus haurà estat proporcionada prèviament per la Universitat.

Els procediments d'obtenció de les credencials que es puguin fer servir per a generar aquests tipus de signatures hauran de garantir:

- Previ a l'entrega de les credencials, la identitat de la persona ha estat verificada de manera certa per un empleat de la Universitat. Si no es compleix aquesta condició, no es podrà fer servir la parella de claus per generar signatures i el sistema de gestió de credencials haurà de tenir la capacitat per deixar constància d'aquesta circumstància. Una verificació posterior de la identitat permetrà convalidar les credencials per al seu ús futur com a mecanisme de signatura.
- Els sistemes de gestió de les credencials han de garantir la seva custodia segura, la seva renovació amb una periodicitat conforme a les polítiques de seguretat de la Universitat i un control sobre el número d'intents d'identificació fallits que provoquin el bloqueig de la credencial.
- Els usuaris hauran de rebre informació oportuna sobre la criticitat d'aquest sistema de credencials i la importància de la seva confidencialitat.

Durant el procés de la signatura, l'usuari haurà de donar el seu consentiment explícit de signatura (pot ser a través de prémer un botó en l'aplicació corresponent). Com a mesura addicional per garantir la robustesa de la identificació, es requerirà a l'usuari la resposta a un repte d'identificació basat en els codis numèrics inclosos de manera única en el sistema d'identificació personal (actualment el PAN). Aquesta mesura es considera complementària a la de la parella de claus, constituint un doble factor d'identificació.

Un cop verificada la identitat, es crearà un fitxer d'evidències i aquestes 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, aquestes es guardaran en els sistemes corporatius; en aquests casos, en la pròpia definició del procediment administratiu s'informarà del lloc on s'emmagatzemaran les evidències. Un cop incorporades les evidències, es signarà el document (o el paquet d'evidències, en cas que no s'hagin pogut consolidar) mitjançant un certificat digital de segell electrònic a nom de la Universitat.

Les evidències a capturar inclouran, com a mínim:

- Nom i codi identificador (NIF o similar) del signant
- Títol i resum criptogràfic del document signat
- Data i hora de la signatura
- Forma d'identificació del signant: nom d'usuari, sistema que l'ha identificat i forma d'autenticació (claus concertades + doble factor d'identificació, OTP).
- Repte addicional emès (el repte, no la resposta).
- Identificació del sistema de tramitació que gestiona la signatura
- IP des de la que es connecta l'usuari

En el cas que la identificació o signatura es realitzin a través de sistemes de clau concertada més voluntat de signatura, la Universitat recollirà unes evidències de caràcter específic:

Identificació	
evidència	**Observacions**
IP de l'usuari	IP dels ordenats des del qual l'usuari s'ha identificat
Nom de l'usuari	En el sistema en el qual s'identifiqui
Data d'accés	Data en la qual l'usuari accedeix a sistema
Repte addicional emès	Per garantir la robustesa de la identificació es requerirà el codi numèric inclòs de manera única en el sistema d'identificació personal (actualment el PAN).

signatura electrònica	
evidència	**Observacions**
IP de l'usuari	IP de l'ordinador des del qual l'usuari ha signat.
Identificació de l'usuari	Nom de l'usuari que ha signat.
Integritat del document	Resum criptogràfic del document
Data de la signatura	Data del moment en que l'usuari ha signat.
En cas que s'utilitzin altres casos d'autenticació podrà haver altres evidències, com, per exemple:	
Còpia correu electrònic informatiu	Còpia de l'e-mail que s'envia a la persona que realitza la signatura informant de l'acció de signatura realitzada.
Altres	Per a cada procediment s'han d'establir les evidències que s'han obtingut en el moment de la signatura.

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, per altra, a les evidències del procés d'identificació de la persona que firma amb l'acceptació de la signatura.

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

Quan sobre el document hi ha més d'una signatura d'aquest tipus totes seran detached i, en el cas de signatura múltiple, totes es conserven en un mateix format per garantir la verificabilitat de l'autenticitat de cadascuna d'elles.

En cas de conflicte amb alguna signatura, la Universitat pot acreditar que el procediment de signatura està regulat de manera 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 (hash del document en l'evidència (signatura primària)) i al seu torn tenir el document signat amb el segon segell electrònic (signatura secundària).

Des del punt de vista del format tecnològic, la signatura a realitzar serà del tipus detached en format XAdES. Haurà d'incorporar un segell de temps, a menys que s'hagi avaluat per al procediment en concret que el temps previst de custòdia dels documents no ho requereix.

	Amb caràcter general, segell de temps	Quan s'hagi avaluat que no cal segell de temps
Altrament, signatura detached	XAdES-B-T	XAdES-B-B

6.5 Signatura electrònica simple basada en claus concertades

La usabilitat d'aquesta modalitat de signatura està condicionada per la qualitat del mecanisme de distribució de les identitats. Apliquen, per tant, totes les consideracions fetes en el sistema interior respecte a l'obtenció de la identitat.

En aquests casos, mitjançant una identitat certa, l'usuari s'identifica en una eina o plataforma de tramitació en relació amb una acció concreta, que normalment serà aportar o validar un document o una proposta de document.

És rellevant observar que, donat que la identificació es basa únicament en la parella de claus concertades, la seguretat de la identificació està condicionada per la seguretat de l'eina de tramitació i el seu sistema de registre d'evidències. Serà preferible, per exemple, que la identificació es produeixi singularment per a l'acte o acció concreta, que no pas que el sistema tingui a l'usuari identificat en sessió activa per un període de temps indefinit abans que es produeixi l'acció que es considera esdeveniment de signatura. També serà preferible que l'eina no permeti la memorització de les credencials d'identificació en el equip o navegador de l'usuari. Cadascun d'aquests elements contribueix a la fiabilitat o no del mecanisme de signatura, que s'ha de valorar en proporcionalitat amb la criticitat de l'acte de signatura que es registra.

Un cop s'ha produït la identificació de l'usuari sobre l'esdeveniment concret, es genera un paquet d'evidències que normalment s'emmagatzema en una base de dades capaç de garantir al seva integritat i la data i hora de creació de la evidència (com ara el propi registre d'evidències de l'aplicació). Si el registre d'evidències intern no és prou segur, es pot optar per la creació d'un paquet d'evidències extern, similar al que s'ha descrit en el sistema descrit a l'apartat 5.4.

Aquest sistema de signatura aporta una força de prova menor que la dels sistemes descrits en altres apartats d'aquesta secció, en particular en relació amb la voluntat del signant i el no repudi; en conseqüència, només es recomanarà el seu ús en casos concrets que no siguin susceptibles de generar efectes jurídics per a tercers.

6.6 Signatura electrònica basada en contrasenyes d'un sol ús

El sistema es basa en la confirmació de la identitat d'una persona mitjançant l'enviament d'un correu electrònic a una adreça de correu electrònic que consti efectivament vinculada a aquesta persona, o bé, la recepció d'un missatge SMS en un telèfon mòbil que també consti registrat prèviament a nom d'aquesta persona. Aquest missatge conté una contrasenya d'un sol ús denominada OTP (One-Time Password)

La vinculació entre la persona i el mitjà on es rebi la contrasenya ha d'estar registrada prèviament en base a una verificació anterior. No es pot fer servir aquest mecanisme de signatura si el codi de confirmació s'envia a una adreça o telèfon que l'usuari subministra en aquell mateix moment.

Durant el procés de la signatura, l'usuari haurà superat els reptes d'identitat mitjançant la recepció del correu electrònic a l'adreça abans esmentada o donant resposta a un repte d'identificació basat en missatge de text. Si aquest sistema és complementari amb una identificació de l'usuari en l'aplicació mitjançant credencial de claus concertades, la combinació d'ambdós mecanismes constitueix un doble factor d'autenticació.

Un cop verificada la identitat, es crearà un fitxer d'evidències i aquestes 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, aquestes es guardaran en els sistemes corporatius; en aquests casos, en la pròpia definició del procediment administratiu s'informarà del lloc on s'emmagatzemaran les evidències. Un cop incorporades les evidències, es signarà el document (o el paquet d'evidències, en cas que no s'hagin pogut consolidar) mitjançant un certificat digital de segell electrònic a nom de la Universitat.

Les evidències a capturar inclouran, com a mínim:

- Nom i codi identificador (NIF o similar) del signant
- Títol i resum criptogràfic del document signat
- Data i hora de la signatura
- Forma d'identificació del signant: nom d'usuari o identitat al·legada.
- Correu electrònic o número de telèfon on s'ha enviat el repte.

- Verificació de que el repte ha esta respost amb èxit.
- Identificació del sistema de tramitació que gestiona la signatura
- IP des de la que es connecta l'usuari

Identificació	
evidència	**Observacions**
IP de l'usuari	IP dels ordenats des del qual l'usuari s'ha identificat
Nom de l'usuari	En el sistema en el qual s'identifiqui
Data d'accés	Data en la qual l'usuari accedeix a sistema
Repte addicional emès	Per garantir la robustesa de la identificació es requeriran els codis numèrics impresos de manera única en la seva tarja d'identificació

signatura electrònica	
evidència	**Observacions**
IP de l'usuari	IP de l'ordinador des del qual l'usuari ha signat.
Identificació de l'usuari	Nom de l'usuari que ha signat.
Integritat del document	Resum criptogràfic del document
Data de la signatura	Data del moment en que l'usuari ha signat.
Si s'utilitzin altres casos d'autenticació podrà haver altres evidències, com, per exemple:	
Còpia correu electrònic informatiu	Còpia de l'e-mail que s'envia a la persona que realitza la signatura informant de l'acció de signatura realitzada.
Altres	Per a cada procediment s'han d'establir les evidències que s'han obtingut en el moment de la signatura.

Des del punt de vista del format tecnològic, la signatura a realitzar serà del tipus PAdES preferiblement quan es pugui generar com a signatura attached a un document PDF, altrament es farà servir signatura detached en format XAdES. Generalment es preferirà que incorporin segell de temps, a menys que s'hagi avaluat per al procediment en concret que el temps previst de custòdia dels documents no ho requereix. Per tant:

	Amb caràcter general, segell de temps	Quan s'hagi avaluat que no cal segell de temps
Quan sigui possible, signatura attached sobre PDF	PAdES-LTV	PAdES-BES
Altrament, signatura detached	XAdES-B-T	XAdES-B-B

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

En aquest format de signatura pot haver més d'una signatura d'aquest tipus sobre el document, que s'hauran de generar en paral·lel.

En cas de conflicte amb alguna signatura, la Universitat pot acreditar que el procediment de signatura està regulat de manera 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 (hash del document en l'evidència (signatura primària)) i al seu torn tenir el document signat amb el segon segell electrònic (signatura secundària).

6.7 Signatura electrònica biomètrica

Aquest és un sistema de signatura electrònica avançada que es genera a partir de les dades biomètriques del signant. En els documents electrònics que es generen es guarda xifrada, conjuntament amb el resum criptogràfic del document, la informació necessària per poder acreditar l'autoria:

- Dades biomètriques de la persona que signa de forma manuscrita el document, entre ells:
    - Detall temporal de la realització de la signatura (inici, final i durada en milisegons).
    - Detall de la traça, en relació a la velocitat, acceleració i pressió del traç en tota la seva figura.

  Les dades biomètriques es recullen amb elements específics de captura permetent al signant la visualització del document a 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.
- En aquest tipus de signatura biomètrica estem contemplant només la biometria de la signatura manuscrita, i no altres mesures biomètriques que es podrien considerar en el futur però actualment estan fora de l'abast d'aquestes instruccions, com ara el reconeixement facial o de la petjada dactilar.

El xifrat d'informació es realitza amb la clau pública d'un certificat digital específic de signatura electrònica biomètrica, la clau pública del qual s'emmagatzema en els servidors de la Universitat. La clau privada és custodiada per un tercer de confiança al qual es podrà requerir quan sigui necessari verificar una signatura biomètrica, en cas de reclamació o litigi.

En aquest format de signatura 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 xifrada la informació esmentada anteriorment es guardarà de forma conjunta amb el document i, per garantir la seva integritat, es realitzarà sobre el mateix una signatura electrònica automàtica de segell electrònic d'aplicació pertanyent a la 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 aportant la signatura electrònica i el segellat de temps 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 xifrat, s'haurà de sol·licitar 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 i que s'ha de fer sota condicions similars, quant a elements maquinari i programari, amb les que es va realitzar la signatura a verificar.

6.8 Segell de temps

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

- Evidencia 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 segellat de temps, es segellarà 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 Ministeri d'Hisenda i Administracions Públiques, en funció de les aplicacions que estigui utilitzant la Universitat.
- Es podrà disposar d'un proveïdor de segell de temps alternatiu per garantir la disponibilitat dels procediments de segellat de temps. 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.

6.9 Signatura electrònica utilitzant la plataforma VÀLid

El present sistema de signatura es basa en l'ús de la plataforma VÀLid del Consorci AOC per part del signant mitjançant la seva autenticació a la plataforma que, posteriorment, generarà les evidències tant de la identificació com de la voluntat de signar.

Aquest sistema de signatura electrònica és una particularització del previst en el apartat 6.1 i 6.6 segons el mecanisme d'identificació que faci servir l'usuari davant VÀLid (certificat electrònic o mecanismes de registre previ amb contrasenya d'un sol ús).

VÀLid ofereix també la possibilitat de generar una evidència de signatura, en la que el signant fa servir la seva identitat per associar-la a un document o una declaració de voluntat, generant d'aquesta manera una signatura electrònica de les que admet l'article 10.4 de la Llei 39/2015.

El fitxer amb les evidències d'identificació que genera la plataforma es guardarà com en el cas anterior dins el mateix document a signar.

Es pot donar el cas que per algun motiu tècnic no fos possible emmagatzemar aquest fitxer d'evidències en el mateix document; en aquests casos, el paquet d'evidències s'emmagatzemarà en base de dades o en el gestor documental de la Universitat. Per major garantia és possible composar un document (en XML) amb l'objecte signat i les dades proporcionades per VÀLid i aquest és el document que la Universitat signa amb el seu segell electrònic de custòdia.

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 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 a l'estar signat amb el segon segell electrònic (signatura secundària).

6.10 Signatura múltiple

Quan en qualsevol dels sistemes descrits anteriorment, participa més d'un signant es produirà signatura múltiple. Aquesta serà seqüencial o paral·lela:

- Es considera que s'han realitzat signatures seqüencials quan la segona signatura es realitza sobre l'objecte digital ja signat anteriorment.
- Es considera que s'han realitzat signatures paral·leles quan les signatures es refereixen a un mateix objecte digital (un mateix resum criptogràfic), ja sigui perquè es generen en format detached o perquè el document ha estat preparat prèviament per acceptar signatures attached en paral·lel.

En la mesura del possible, s'evitarà l'ús de la signatura seqüencial per als circuits de signatura on els documents s'hagin de signar a la vegada i amb el mateix objectiu per part de diverses persones.

La signatura múltiple s'utilitzarà 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 al ressegellat de documents (veure apartat 8.1) ja signats per actualitzar la seva validesa legal al llarg del temps, abans que es pugui posar en dubte la validesa criptogràfica de la signatura electrònica.

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

- Signatures electròniques mitjançant certificats digitals (paral·lela o seqüencial), 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 seqüencial), en el cas de documents en suport electrònic que requereixin més d'una signatura.
- Signatures electròniques biomètriques (seqüencial), per a documents en suport electrònic que es generin presencialment davant 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 seqüencial), per a aquells documents en suport electrònic que requereixin la signatura d'una persona (càrrecs de representació, empleats, els licitadors i proveïdors, altres terceres persones) i requereixi una signatura electrònica posterior per completar la seva validesa, mitjançant segell electrònic.
- Signatura electrònica Biomètrica i, posteriorment, signatura electrònica mitjançant certificat digital (seqüencial), en el cas de documents en suport electrònic que es generin davant d'un tercer i que, posteriorment a la seva signatura sobre la base de biometria, requereixi la signatura electrònica posterior per completar la seva validesa, mitjançant segell electrònic.

- Es procurarà que en tots els casos de signatura del document per vàries persones, totes les persones participants facin servir tecnologies similars (s'evitarà generar documents signats per una part amb signatura basada en certificats, i una altra part amb signatura biomètrica).

7. CASOS D'ÚS DE LA SIGNATURA ELECTRÒNICA

Per a cadascun dels casos que es presenten, es comenta la seva caracterització jurídica, es concreten els nivells de seguretat aplicables i els sistemes de signatura a emprar d'entre els que s'han descrit a l'apartat 5.

7.1 Signatura electrònica d'un document intern

Aquest cas d'ús aplica a documents produïts internament a la Universitat, que han de ser signats per un membre de la comunitat universitària, en l'exercici de les seves funcions, i/o tercers que participin o col·laborin puntualment amb la UPC, i tenen com a destinatari un altre usuari intern o el simple compliment d'un pas en el procediment. No aplica a documents que han de tenir efectes jurídics davant de tercers.

Aquests documents es poden signar electrònicament en qualsevol moment del seu cicle de vida.

Les principals característiques són:

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

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

- Classe de signatura:
  - Avançada o Qualificada, segons descrita a 6.1.
  - Signatura basada en claus concertades, segons descrita a 6.4
  - Signatura basada en OTP, segons descrita a 6.6. Aquest mecanisme només serà admissible per a signar documents d'aquet tipus quan el signant sigui una persona que participa en un procediment intern de la Universitat de manera puntual i no tingui accés a altres mecanismes d'identificació (veure apartat 6.10).

- Tipus de certificat: Certificat de treballador públic o Certificat de representant. En el cas de signatures basades en claus concertades o signatura basada en OTP, es complementen amb un Certificat de Segell Electrònic del Consorci AOC en els termes descrits a l'apartat 6.4 d'aquesta Instrucció.
- Formats: PAdES-LTV amb segell de temps o XAdES-B-T.
- Segell de temps: Sí
- Nivell de signatura: Simple, Múltiple (seqüencial o paral·lel)
- Tipus de signatura: Attached o Detached segons el cas.

7.2 Signatura de documents preparatoris i actes de tràmit

Aquest cas d'ús aplica a documents o actes del procediment administratiu que no produeixen efectes jurídics per a tercers. Entenem com a actes preparatoris les validacions prèvies de documents, la formulació de propostes de resolució i qualsevol altre acte en el que es reculli el vistiplau d'un empleat públic previ a la signatura definitiva de l'acte per part del seu responsable.

Els actes de tràmits són accions d'impuls que només certifiquen que s'han realitzat actuacions preceptives dins dels procediments, però en si mateixos no produeixen efectes jurídics.

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

- Classe de signatura:
  - Signatura electrònica simple basada en claus concertades, segons descrita a l'apartat 6.5.
  - També s'acceptaran els sistemes previstos en el cas 6.1.

7.3 Signatura electrònica d'un document amb valor per a tercers.

Aquest cas d'ús aplica a documents produïts internament la Universitat, que han de ser signats per un membre de la comunitat universitària, o per tercers que participin o col·laborin puntualment amb la UPC; i que són susceptibles de generar drets o obligacions per a tercers.

Aquests documents es poden signar electrònicament en qualsevol moment del seu cicle de vida.

Les principals característiques són:

- Es realitza 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.
- El document electrònic estarà en qualsevol format dels acceptats per la Universitat, preferiblement PDF/A i XML, per tal de garantir la seva preservació al llarg del temps.
- Quan escaigui garantir la protecció de les dades del signant, del document original se n'expedirà una còpia autèntica en la que s'ocultin les dades del DNI del signant, i s'hi incorporarà un Codi de Verificació Electrònica, que permeti la seva eventual verificació en un entorn de validació de documents disponibles a la Seu Electrònica. Aquesta còpia serà la que es lliuri a tercers.

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

- Classe de signatura: Avançada o Qualificada (segons descrita a 6.1).
- Tipus de certificat: Certificat de treballador públic o Certificat de representant.
- Formats: PAdES-LTV amb segell de temps o XAdES-B-T.
- Segell de temps: Sí
- Nivell de signatura: Simple, Múltiple (seqüencial o paral·lel)
- Tipus de signatura: Attached o Detached segons el cas.

7.4 Signatura electrònica de documents per part d'un tercer

Aquest cas d'ús aplica a documents que són signats pel tercer en un entorn controlat per la UPC. És irrellevant si el document és aportat pel tercer o produït per la Universitat sempre que la signatura es produeixi en un entorn controlat per la UPC, com ara la Seu electrònica o el Portafirmes. Els casos en que el document el signa el tercer en el seu propi entorn i l'aporta signat, es contemplen a la secció 7.9.

En particular, aplica a la signatura de documents en el moment de la seva presentació en un registre electrònic, o al cas en que el tercer ha de signar electrònicament documents en passos posteriors de la seva participació en un procés administratiu de la Universitat. Les principals característiques són:

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

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

- Classe de signatura:
  - Avançada o Qualificada, segons descrita a 6.1.
  - Signatura basada en claus concertades, segons descrita a 6.5.
  - Signatura basada en OTP, segons descrita a 6.6.
- Tipus de certificat:
  - Per a les signatures generades per tercers amb certificat electrònic: Qualsevol certificat definit en el punt 9 de la Política vigent.
  - Per als altres mecanismes de signatura, certificat de segell electrònic.
- Formats: PAdES-LTV amb segell de temps o XAdES-B-T.
- Segell de temps: Sí
- Nivell de signatura: Simple
- Tipus de signatura: Attached o Detached segons el cas

7.5 Signatura electrònica d'un tercer en actes presencials

Aquest cas d'ús aplica a tercers que no disposen d'una identitat creada en els sistemes de la Universitat i participen en processos que es produeixen presencialment en l'àmbit de la Universitat en els termes següents:

- Crear sol·licituds presencialment en el registre electrònic.
- Signar documents de consentiment informat en determinades actuacions de caràcter medicosanitari.
- Cessió de drets d'imatge o, qualsevol altre tipus de drets personals, com a conseqüència de la participació presencial en un esdeveniment.
- Altres de característiques similars.

Finalment, concretant el tipus de signatura s'estableixen les característiques o requeriments que consten a l'apartat 6.7.

7.6 Signatura electrònica de contractes, convenis o acords amb altres parts:

Aquest cas d'ús aplica a documents contractuals multilaterals en els que participa la Universitat conjuntament amb una o més parts. En aquest cas, les parts signen els documents en un entorn controlat per la Universitat.

Els casos en que el document el signa el tercer i l'aporta signat per a la seva signatura posterior per part de la Universitat, queden englobats dins les previsions que es contemplen a la secció 7.9.

Les principals característiques són:

- Es realitza 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.
- El document electrònic estarà en qualsevol format dels acceptats per la Universitat, preferiblement PDF/A i XML, per tal de garantir la seva preservació al llarg del temps.
- El document es podrà signar diverses vegades i per diferents usuaris.
- Es podrà signar en paral·lel i/o de forma seqüencial.

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

- Classe de signatura: Qualificada, segons descrit a 6.1 en combinació amb qualificada, avançada o claus concertades, segons descrit a 6.10.
- Tipus de certificat:
  - Per a les signatures generades per part de la Universitat: Certificat de representant o treballador públic.
  - Per a les signatures generades per tercers. Qualsevol certificat definit en el punt 5 d'aquest document.
- Formats: PAdES-LTV amb segell de temps o XAdES-B-T.
- Segell de temps: Sí
- Nivell de signatura: Múltiple (seqüencial o paral·lela)
- Tipus de signatura: Attached o Detached en funció del procediment.

7.7 Signatura electrònica automatitzada

Es la signatura de diversos documents de forma automàtica amb plenes garanties jurídiques, mitjançant certificats de segell electrònic sense la intervenció d'un signant en el procés de signatura.

Les principals característiques 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), però es preferirà el format PDF per a documents que s'hagin de compartir amb els interessats.
- Els certificats digitals, així com les corresponents claus privades que han de permetre generar processos de signatura automatitzada es guardaran en un repositori segur al servidor de la Universitat, o el d'un tercer prestador de serveis, sempre que la cessió estigui limitada i controlada d'acord amb el que disposa l'apartat 5.2.3 d'aquesta Instrucció.

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 següents característiques o requeriments:

- Tipus de signatura:
  - Avançada, segons descrita a 6.2.
  - CSV, segons descrita a 6.3
- Tipus de certificat: Certificat de Segell Electrònic.
- Per documents PDF o PDF/A: PAdES-LTV amb segell de temps.
- Nivell de signatura: simple
- Tipus de signatura: Attached.

7.8 Signatura electrònica per a digitalització segura

Consisteix en la signatura electrònica d'un document digitalitzat, en format PDF o PDF/A, per crear una còpia autèntica electrònica. La signatura, així com la data de digitalització, és important per tal de garantir la integritat i l'autenticitat del document digitalitzat. Signarà electrònicament:

- El empleat públic habilitat que digitalitzi el document, en cas de control manual i acarament de l'original.
- Un segell electrònic del sistema en cas d'actuació administrativa automatitzada (un cas específic dels que es preveuen a l'apartat anterior) mitjançant l'eina del CAOC per a la digitalització segura.

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

- Tipus de signatura: Avançada segons descrit als punts 6.1 i 6.2
- Tipus de certificat: Certificat d'empleat o públic o de Segell Electrònic.
- Formats: PAdES-LTV.
- Segell de temps: Sí
- Nivell de signatura: Simple
- Tipus de signatura: Attached.

7.9 Incorporació de documents electrònics signats de fonts externes

En el cas de signatures que provenen de plataformes externes (altres administracions, eines de client, etc.) es procedirà a validar-les, i s'incorporaran a l'expedient, si és possible, les evidències de validació.

Per poder realitzar la validació d'un document electrònic i verificar les signatures de tercers cal fer les següents comprovacions:

Identificació del certificat i la cadena de confiança

Per tal de generar una signatura electrònica serà necessària la utilització d'un certificat electrònic reconegut. Els qui emeten aquests tipus de certificats són els prestadors de serveis electrònics de confiança qualificats per emetre certificats electrònics reconeguts. Per tal d'acreditar que la signatura és segura i que la persona que hi apareix és realment el signant, cal verificar que el certificat ha estat emès per un prestador de confiança. Tal com s'ha indicat a 5.3, la Universitat delega la seva confiança en la plataforma PSIS.

Si un cop realitzada la validació, del emissors dels certificats, aquesta falla, l'emissor no es considerarà emissor de confiança i la Universitat no dipositarà confiança en la firma del Document i aquest serà retornat a l'emissor per tal que el signi un emissor de confiança.

Identitat del titular del certificat

Un certificat electrònic ens ofereix informació que serveix per identificar a la persona o entitat que s'ha compromès amb el contingut del document. Per tant, verificar la identitat del titular del certificat és important per poder establir que el document ha estat signat per la persona correcta.

En el cas que el signant sigui una persona física en representació d'una persona jurídica, en el camp que correspongui haurà de constar les dades identificatives d'ambdós.

Si el titular del certificat coincideix amb la persona que consta com a signant en el text del document, la verificació pot entendre's com a finalitzada, però en cas que el titular del certificat no coincideixi amb la identitat de la persona que hauria de firmar el document, no es podrà admetre la signatura i es rebutjarà el document.

Validar les facultats del signant

Habitualment, pot passar que el signant del document no signi en nom propi sinó que ho faci en representació d'un tercer. La Universitat haurà de comprovar que el representant està capacitat per a exercir la representació, en cas que aquestes facultats no constin en el propi certificat. Pot ser necessari requerir la presentació de documentació addicional per acreditar la representació, o la verificació de registres externs.

En cas que no es pugui verificar o validar la suficiència dels poders de representació del signant, el document es retornarà a l'emissor.

Verificar la vigència del certificat

Els certificats electrònics consten d'una data de caducitat fixada en el moment de la seva emissió.

Els certificats, es poden suspendre o revocar inclús abans de las seva caducitat per motius com: pèrdua de la vigència de dades dels certificats, pèrdua de la targeta criptogràfica, etc.

La importància de realitzar aquesta validació rau en que només és vàlida la signatura electrònica realitzada amb un certificat que sigui vigent i per tant, no pot estar caducat, revocat o suspès. La informació per a realitzar la validació de la caducitat s'extrau directament del certificat o l'autoritat de certificació. Es poden seguir els següents procediments:

- Verificació de llistes de revocació de certificats (CRLs). Aquesta validació s'implementa automàticament per la majoria d'aplicacions que permeten veure els documents signats, però no generen proves concretes.
- Sol·licitud d'un informe de verificació (OCSP). Es tracta d'un protocol que es pot sol·licitar des del prestador del servei de certificació, però que ha de sol·licitar un sistema informàtic des de la Universitat.
- Validació a través d'una plataforma centralitzada, com @firma.

Pot succeir, que el certificat caduqui després d'haver signat un document, per aquest motiu és important que la Universitat pugui acreditar, que el certificat es trobava vigent en la data de verificació, per aquest motiu és necessari que el document consti d'un segell de temps emès per una Autoritat (TSA).

Verificar la vinculació criptogràfica del document amb la signatura

La verificació de la vinculació criptogràfica del document amb la signatura es porta a terme per validar que la signatura electrònica fa referència al document en qüestió.

El document pot haver patit modificacions posteriors al moment de la signatura, l'eina de signatura no ha realitzat correctament el procés de signatura, etc. i, per tant, pot succeir que la vinculació entre el document i la signatura no corresponguin.

Aquesta verificació es pot portar a terme mitjançant alguna aplicació ofimàtica que permeti la visualització de documents PDF, però en els processos d'incorporació del document al sistema es podrà fer a través d'una aplicació que n'executi la incorporació.

En cas que falli aquesta comprovació, el document es considerarà mal signat i la Universitat realitzarà la devolució del document al seu emissor informant del succeït.

Verificar el contingut del document

La verificació del contingut d'un document electrònic es tan necessària com la verificació de qualsevol document en format paper.

En aquest cas les comprovacions es centraran en analitzar si el contingut del document és adequat i s'ajusta a les necessitats jurídiques oportunes. Per tant, parlem de validació jurídica del contingut del document.

En cas que el document hagi estat originalment produït per la Universitat, la recomanació és oferir-lo a signar al tercer prèvia signatura d'un segell d'òrgan de la Universitat, per tal d'automatitzar la verificació del retorn.

En cas que la verificació no es pugui realitzar automàticament caldrà analitzar el document per assegurar-se que no s'ha realitzat cap canvi entre la versió enviada al signant i la versió que es retorna signada. En el cas que aquesta comprovació falli i, per tant, el document hagi estat modificat, el document signat pel tercer serà retornar a l'emissor.

Verificar la data de la signatura

La verificació de la data de la signatura és rellevant pels dos motius que es citen a continuació:

- El document pot tenir en el seu contingut una data de signatura, però pot passar que aquesta no coincideixi amb la data de signatura electrònica.
- La data de signatura es rellevant per gestionar la vigència del certificat del signant.

Cal validar la data en la qual s'ha produït la signatura i diferenciar si la data de signatura s'ha establert mitjançant un segell de temps o l'hora de l'ordinador del signant.

Aquestes comprovacions s'han de realitzar de manera manual malgrat que existeix la possibilitat de realitzar-les de manera automàtica mitjançant la aplicació de captura del document.

7.10 Identificació i signatura de persones estrangeres

La Universitat té relació puntual amb persones estrangeres, físiques o jurídiques, tant en temes de contractació pública, en projectes internacionals de recerca o de docència.

En general, admetem tots els certificats electrònics reconeguts per les autoritats homologades al Ministeri d'Indústria, Comerç i Turisme, segons el Reglament eIDAS. Aquest reconeixement creuat pot estar limitat per les capacitats de les eines de *parsing* i interpretació (VÀLid, PSIS, @firma) que faci servir la Universitat.

En el cas que una persona estrangera no disposi d'un certificat:

- Si és una persona jurídica, aquesta no podrà relacionar-se amb la Universitat pels mitjans descrits.
- Si és una persona física i la seva relació amb la Universitat implica la realització de tasques de representació de la Universitat o d'empleat públic, també necessitarà obtenir els mecanismes d'identificació apropiats, dels tipus que es preveuen l'apartat 5.
- Si és una persona física i la seva relació amb la Universitat no implica la realització de tasques de representació i d'empleat públic, les quals exigeixen signar amb certificat, li permetrem identificar-se al·legant les seves dades, amb les quals es generarà una identitat, mitjançant el sistema de clau concertada (que es troba explicat en detall a l'apartat 6.4., o el sistema de contrasenya d'un sol ús (apartat 6.6), la validesa dels quals està condicionada a la verificació de les dades d'identitat.

8. ESTRATÈGIA DE PRESERVACIÓ DE DOCUMENTS I SIGNATURES ELECTRÒNIQUES

La signatura electrònica permet acreditar l'autenticitat de l'expressió de voluntat i consentiment 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 es 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 que es generen les signatures electròniques.

Per contrarestar els riscos descrits, la Universitat es dota de dos mecanismes diferenciats:

- Preservació basada en signatures longeves: consisteix en el ressegellat consecutiu dels documents i les signatures electròniques en entorns propis.
- Preservació basada en la seguretat de l'arxiu: La preservació de documents i signatures electrònics contingudes en expedients transferits a un arxiu definitiu que garanteix, mitjançant el seu procés d'ingesta i la seva seguretat estructural, la integritat i autenticitat dels documents que custodia.

8.1 Ressegellat i preservació de documents i signatures electròniques d'expedients vius

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

El procés de ressegellat consisteix a renovar el segell de data i hora, afegint 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 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, previ al ressegellat haurem de completar la signatura a un dels formats anteriorment definits.

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

- En el moment en què estigui a punt de caducar l'últim segell de temps aplicat a la signatura electrònica a 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. Sobre aquestes signatures s'incorporarà un nou segell de temps, ja que la seva estructura permet aquesta possibilitat. Aquest nou segell de temps estarà ja generat amb un certificat recent, amb un període de validesa superior a l'actual en la signatura a 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.

En el cas de les firmes realitzades a través d'acreditació de la identitat i d'evidències de la voluntat de signatura, es realitzarà el ressegellat de la signatura secundària.

En definitiva, el ressegellat consisteix, doncs, a mantenir la validesa de la signatura incorporant 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, serà el següent:

- En el cas de signatures generades dins de l'entorn d'aquesta (aquelles signatures generades amb les eines de signatura internes) es procedirà, en fase de tramitació, a la generació de les signatures electròniques en format preservable, és a dir en format de signatura d'arxiu. Així, per 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.

- En el cas de signatures que provenen de plataformes externes (altres administracions, els licitadors i proveïdors, terceres persones, etc.) es procedirà si s'escau a completar-les. Aquest procés de compleció es realitzarà previ tancament i foliació l'expedient. Per 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.

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

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

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

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

8.2 Preservació de documents i signatures electròniques en expedients transferits a l'arxiu definitiu

8.2.1 Selecció de formats documentals de conservació

Per garantir la intel·ligibilitat i integritat a llarg termini dels document electrònics, són necessàries actuacions que permetin preservar el format del document i dels seus elements de seguretat, així com signatures electròniques o segells de temps.

El sistema de preservació de documents electrònics controla de forma periòdica els documents electrònics per garantir la seva accessibilitat, la possibilitat de recuperar-los i la seva validesa jurídica. En aquest procés es comproven els aspectes següents:

- Accessibilitat a suports
- Capacitat de lectura de formats
- Validesa jurídica de les signatures electròniques.
- Integritat dels documents.
- Integritat dels expedients.

Actualment, el format més utilitzat per a la preservació digital és el PDF/A, per tant, en cas que els documents provinguin d'una tercera font es convertiran al format citat anteriorment. El PDF també s'acceptarà sempre i quan provingui d'aplicacions corporatives existents que generin aquest format.

Per a garantir la signatura electrònica i la seva validesa jurídica, s'aplica el criteri, descrit en les presents instruccions, de completar les signatures existents a formats preservables:

- XAdES-A, per als documents XML amb firmes XAdES, com seria el cas de la factura electrònica o el Foliat,
- PAdES-LTV per als documents en format PDF o PDF/A.

Aquests tipus de signatura estan definits en diferents estàndards internacionals com ETSI TS 101.903 XAdES. o la ETSI TS 102.778 PAdES.

A partir d'aquestes firmes i en el moment en què el segell electrònic caduqui, es procedirà al ressegellat de les signatures electròniques amb un nou segell, amb una caducitat suficient i amb uns algoritmes de signatura actualitzats.

Els formats del foliat d'expedient serà XML, pel fet que són els que permeten millor l'actuació administrativa automatitzada, que garanteix la integritat de l'expedient electrònic.

8.2.2 Requeriments dels elements a transferir a l'eina d'arxiu

Per poder transferir un expedient electrònic a l'eina d'arxiu longeu s'hauran de complir els següents requeriments:

1. Els expedients han d'estar en el gestor documental.
2. Els expedients han d'estar tancats.
3. Els expedients han d'estar foliats. La foliació ha de ser íntegre amb els documents que formen part d'aquest i amb els resums criptogràfics d'aquests.
4. Les metadades obligatòries dels documents, expedients i signatures han d'estar correctament informats.
5. Els documents han de tenir un format reconegut, gestionable i no obsolet per part de l'eina d'arxiu longeu.
6. Les signatures electròniques dels documents i expedients electrònics han d'estar completades a un format preservable.

8.2.3 Manteniment i migració de formats

Malgrat la selecció de formats electrònics s'hagi fet en origen garantint l'ús dels formats més preservables, cal preveure la inevitable circumstància que els formats escollits puguin acabar quedant obsolets, ja sigui per motius de seguretat o per ser substituïts per altres tecnologies, de tal manera que els formats inicialment escollits deixen de ser estàndards generalment acceptats.

Per tal de garantir la seva intel·ligibilitat, els documents en formats obsolets o en procés d'obsolescència hauran de migrar-se a un nou format que permeti complir millor amb les funcions de preservació.

La UPC, per complir amb la finalitat de superar l'obsolescència del format, opta, amb caràcter general, per una estratègia de migració en front d'altres tècniques com l'emulació, la preservació de la tecnologia o l'encapsulació, atès que la migració és l'opció més recomanable per a poder garantir l'accés a la documentació amb independència del temps transcorregut, aplicant les recomanacions dels estàndards internacionals ISO 18492 (2008) i el model OAIS definit per la ISO 14721 (2003).

La manera com s'implementi tecnològicament la migració dependrà de les solucions tecnològiques disponibles en cada moment, però es contemplen a priori dos alternatives:

- Poder definir un procediment de migració certificada dins del propi Sistema de Gestió de Documents Electrònics o Arxiu Electrònic de la Universitat, sempre que aquest procediment sigui capaç de garantir la equivalència funcional entre l'element original i el fruit de la migració, i certificar la migració amb les mesures d'autenticitat apropiades.

- Delegar el procés de migració en una plataforma facilitada per un tercer de confiança (com ara la solució iArxiu del CSUC), sempre que la transferència i recuperació del document es puguin executar de manera segura, i el producte resultant compleixi amb els requisits establerts en el punt anterior.

En qualsevol dels casos, si el document original conté signatures electròniques de caire criptogràfic vinculades al document original en base al seu resum criptogràfic, la signatura i el document original es conservaran per tal de poder-ne seguir acreditant l'autoria, malgrat a efectes de consulta e intel·ligibilitat s'emprarà exclusivament el producte resultant de la migració.

9. PERIODE DE VALIDESA I TRANSICIÓ D'AQUESTES INSTRUCCIONS

Aquestes Instruccions seran valides des de la data de la seva signatura i publicació a la Seu Electrònica i fins que no siguin substituïda per una posterior.

Annex I – Estàndards internacionals i altres convencions

- ETSI RFC 2315 (1998), ETSE RFC 2630 (1999), IETF RFC 3369 (2002), IETF RFC 3852 (2004): PKCS # 7: Cryptographic Message Syntax (CMS).
- ETSI TS 101 733. v.1.6.3, v1.7.4 i v.1.8.1: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).
- ETSI TS 119 122-3: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures: Part 3: incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES.
- ETSI TR 119 124-1: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.
- ETSI TS 119 124-2: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of CAdES baseline signatures.
- ETSI TS 119 124-3: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended CAdES signatures.
- ETSI TS 119 124-4: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of CAdES baseline signatures.
- ETSI TS 119 124-5: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended CAdES signatures.
- ETSI TR 119 134-1 Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.
- ETSI TS 119 134-2: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of XAdES baseline signatures.
- ETSI TS 119 134-3: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended XAdES signatures.
- ETSI TS 119 134-4: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of XAdES baseline signatures.
- ETSI TS 119 134-5: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended XAdES signatures.

- ETSI TS 119 142-3: Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS).
- ETSI TR 119 144-1 Electronic Signatures and Infrastructures (ESI); PAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.
- ETSI SR 019 020: The framework for standardization of signatures; Standards for AdES digital signatures in mobile and distributed environments.
- IETF RFC 5280 (2008): Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- IETF RFC 2560 (1999): X.509 Internet Public Key Infrastructure, 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-term preservation of electronic document-based Information.
- 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 and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
- ETSI TS 102 023, v.1.2.1 i v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- ETSI TS 102 023, v.1.2.1 i v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- ETSI TS 101.861 V1.3.1 Time stamping profile.
- 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".

Annex II – Procediments d'obtenció, renovació i revocació de certificats

Certificat d'empleat públic T-CAT P en programari

Procediment d'obtenció

Sol·licitud

- La persona contactarà amb l'Entitat de Registre (Servei de Desenvolupament Organitzatiu (o la unitat organitzativa responsable de l'administració electrònica a la UPC) per sol·licitar l'emissió del seu certificat com a treballador públic. En aquesta sol·licitud ha d'indicar les dades personals i de contacte.

Validació de la Identitat

- L'operador contactarà amb el sol·licitant del certificat per verificar que les dades personals que consten a la Identitat Digital de la UPC (registre previ dels treballadors de la UPC) són exactament les mateixes que figuren al document oficial que l'identifica i per tant, amb les que s'emetrà el certificat.

Emissió i lliurament del certificat

- L'operador procedirà a l'emissió del certificat.
- El titular rep un correu electrònic del Consorci d'Administració Oberta de Catalunya (CAOC) amb les indicacions per fer la descarrega i la instal·lació.
- L'operador envia el full de lliurament al titular del certificat per tal que el signi.
- El titular del certificat retorna signat el full de lliurament a l'entitat de Registre. La UPC ha de custodiar aquest document signat durant un període mínim de 15 anys.
- En cas que el full de lliurament no es retorni signat, l'entitat de Registre revocarà el certificat.

Procediment de renovació

- El Consorci d'Administració Oberta de Catalunya envia dos correus electrònics al titular del certificat, avisant-lo de la caducitat. El primer correu s'envia 60 dies abans de la data de caducitat i el segon 30 dies abans si encara no s'ha renovat el certificat.
- En aquest correu, s'indica que el titular ha de contactar amb el Responsable del Servei de certificació (Servei de Desenvolupament Organitzatiu (o la unitat organitzativa responsable de l'administració electrònica a la UPC) si vol renovar el certificat.
- El procés a seguir per a la renovació d'un certificat serà el mateix que per a l'emissió de certificats nous. L'operador haurà de comprovar que la informació utilitzada per verificar la identitat i la resta de dades continuen sent vàlides. Si qualsevol informació ha canviat, es registrarà adequadament la nova informació.

Procediment de revocació

- La revocació suposa invalidar definitivament un certificat digital. Es pot revocar d'ofici quan algú en fa un mal ús, el titular deixa de ser membre de la comunitat o aquells certificats suspesos que han superat el període de 120 dies sense que s'hagin habilitat.
- El titular també pot sol·licitar per voluntat pròpia la revocació del seu certificat, contactant amb el Centre d'Atenció a l'Usuari de l'AOC (900905090) o bé amb l'Entitat de Registre habilitada a la UPC, i facilitar el codi de suspensió que consta al Full de Lliurament que li van lliurar en el moment de la gravació del certificat digital.
- L'operador del Centre d'Atenció a l'Usuari de l'AOC, o el de l'Entitat de Registre procediran a revocar el certificat digital.

Procediment de suspensió

- Si la persona perd o li roben el certificat digital, ha de trucar al Centre d'Atenció a l'Usuari de l'AOC (900905090) o bé a l'entitat de Registre habilitada a la UPC, i facilitar el codi de suspensió que consta al Full de Lliurament que li van lliurar en el moment de la gravació del certificat digital.
- L'operador de l'Entitat de Registre procedirà a realitzar la suspensió del certificat. El període de suspensió és de 120 dies hàbils , durant el qual es pot sol·licitar que sigui habilitat de nou, si la persona el recupera.
- Passat aquest període, si no s'habilita, el certificat quedarà automàticament revocat.

Certificat de representant

Procediment d'obtenció

Aquest certificat s'expedeix a les persones físiques com a representants de les persones jurídiques .

Sol·licitud

- La petició d'aquests tipus de certificats únicament la podrà fer:
  - el propi representant o persona autoritzada
  - el/la secretari/a General
- La sol·licitud d'expedició així com les de suspensió, cancel·lació de la suspensió i revocació hauran d'estar sempre avalades per la Secretaria General.
- El Servei de Desenvolupament Organitzatiu (o la unitat organitzativa responsable de l'administració electrònica a la UPC), amb el suport dels Serveis Jurídics, portarà a terme les accions necessàries per gestionar la sol·licitud del certificat complint amb els requeriments de l'entitat certificadora emissora (AOC, FNMT, ...).

Validació de la identitat

S'ha d'acreditar:

- la identificació de la persona representant. Documentació d'identificació vàlida i vigent: DNI, Passaport o altres mitjans admesos en dret a efectes d'identificació en els que consti el seu número de DNI/NIF.
- la identificació de l'entitat representada (UPC) i de la seva existència.
- acreditar la capacitat i vigència de la representació per mitjà de document públic (nomenament). Nomenament (Rector) o poder notarial (Gerent) i certificat de la Secretaria General en el que s'acrediti la vigència del nomenament.

Emissió i lliurament del certificat

En funció del que determini l'entitat certificadora el certificat es lliurarà al Representant en targeta en el cas del certificat de l'AOC o el descarregà el propi representant en el cas del certificat de la FNMT.

Procediment de revocació

La revocació es farà a petició del propi representant o persona autoritzada o del/la secretari/a General, quan la persona física deixi de representar a la UPC.

Certificat de segell electrònic

La sol·licitud, renovació i revocació d'aquest tipus de certificats es competència de la Secretaria General.

La petició i gestió d'aquests tipus de certificats és responsabilitat del Servei de Desenvolupament Organitzatiu (o la unitat organitzativa responsable de l'administració electrònica a la UPC).

El procediment de sol·licitud es:

- El sol·licitant ha d'accedir a EACAT identificant-se amb certificat digital.
- Ha d'emplenar, signar i enviar el formulari.
- El Servei de Certificació Digital informa al Responsable del Servei l'emissió del certificat.
- A la Carpeta del Subscriptor estarà disponible el certificat per a la seva descàrrega.

L'Àrea TIC, s'encarregarà de la descarrega i instal·lació del certificat en el servidor corresponent.

Certificats d'aplicació i de servidor segur

Procediment d'obtenció

La petició i gestió d'aquests tipus de certificats, excepte el de segell electrònic, és responsabilitat de l'Àrea TIC que establirà els criteris per a la petició d'aquests tipus de certificats. Es poden sol·licitar certificats de diferents entitats de certificació amb l'aprovació d'aquesta Àrea.

En el cas que l'entitat de certificació sigui l'AOC:

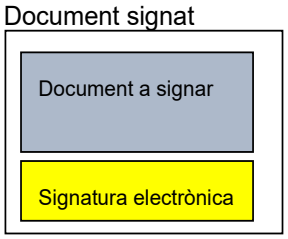
- El sol·licitant ha d'accedir a EACAT identificant-se amb certificat digital.
- Ha d'emplenar, signar i enviar el formulari.
- El Servei de Certificació Digital informa al Responsable del Servei l'emissió del certificat.
- A la Carpeta del Subscriptor estarà disponible el certificat per a la seva descàrrega.

Annex III – Glossari i conceptes

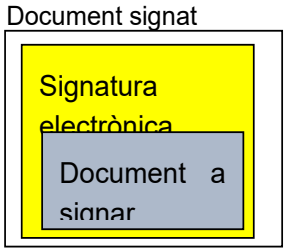
Fonaments tècnics de la Signatura electrònica

S'ha considerat important definir els **tipus de signatura** des d'un punt de vista tècnic:

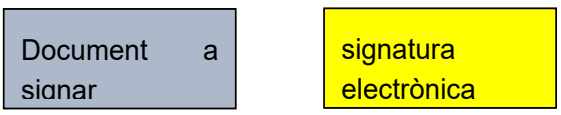
- **Signatura attached**: les dades de signatura resideixen en el document signat. Per tant, el mateix document disposa de tota la informació per comprovar l'autenticitat i integritat de el document, així com la informació necessària per a la validació de la signatura. Cal diferenciar entre dos tipus diferents de signatura attached:
    - Enveloped (incrustada), en aquest cas el document signat està compost pel contingut del document a signar més la signatura d'aquest contingut.



    - Enveloping (envoltant), en aquest cas el document signat és la signatura electrònica del document a signar i dins d'aquesta firma hi ha el mateix document a signar.



- **Signatura detached**: Les dades de signatura resideixen fora del document a signar, però associats a aquest. 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 seves dades completes de la signatura.



A continuació, definirem el nivell de signatures.

- **Signatura simple**: el document conté una única signatura.
- **Signatura múltiple**: el document conté dues o més signatures. Aquesta signatura múltiple consisteix en que diversos signants signin el document consecutivament. Aquesta signatura es pot aplicar sobre el document original cada vegada, el que s'identifica com a signatura **paral·lela**, o sobre el document signat, que s'identifica com a signatura **seqüencial**.

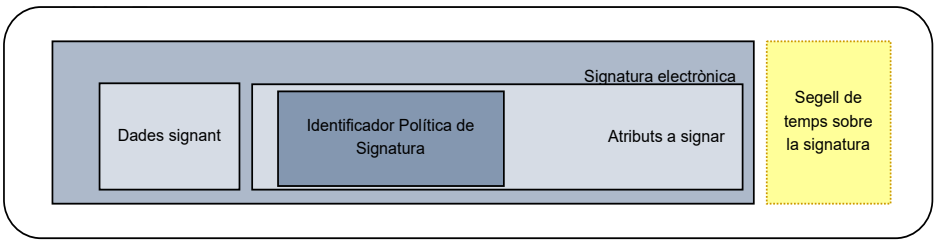
La signatura múltiple s'utilitzarà en diverses situacions en el marc dels procediments de la Universitat, com ara en la signatura de documents electrònics per més d'una persona o al ressegellat de documents ja signats per actualitzar la validesa legal de el document al llarg de el temps, abans que pugui quedar en entredit la validesa criptogràfica de la signatura electrònica.

Especificacions Tècniques dels formats de signatura electrònica

- **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 de el 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 a el format XAdES-EPES (signatura electrònica avançada amb identificador de política):

- Les dades signats per l'usuari, com per exemple un document electrònic
- El tipus de contingut signat: ContentType

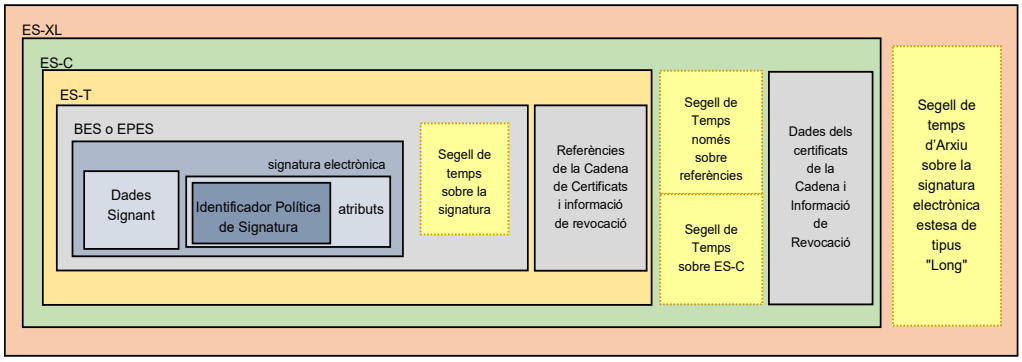
- El resum criptogràfic del missatge: MessageDigest
- El certificat emprat per signar: ESSSigningCertificate o OtherSigningCertificate
- La data i hora al·legada de la signatura: SigningTime (Opcional)
- Les pistes sobre el contingut signat: ContentHints (Opcional)
- La identificació del contingut: ContentIdentifier (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

- **Signatura electrònica d'Arxiu**

La signatura electrònica d'arxiu accepta dos formats:

1. **Signatura AdES.** La signatura electrònica d'arxiu (AdES-A) part 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, preveient el ressegellat successiu de manera periòdica. Aquest és el format de signatura més complet i està pensat expressament per als documents que es vol garantir la disponibilitat al llarg del temps.

   Signatura electrònica d'Arxiu (ES-A)



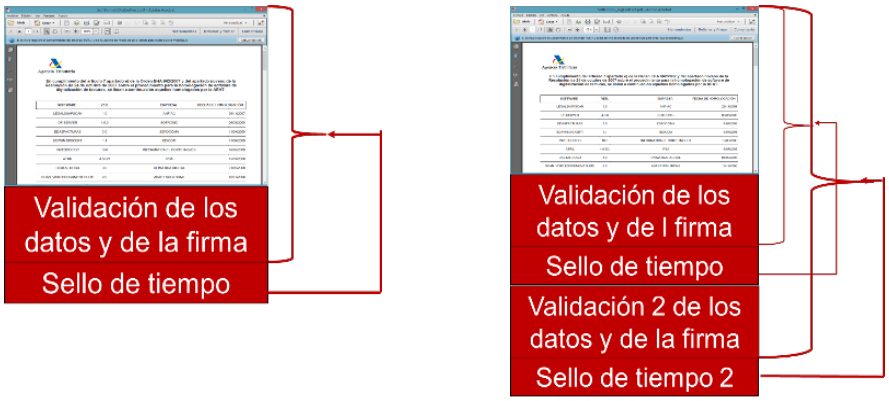
   - La signatura electrònica XML: Signature

- El certificat utilitzat per signar: SigningCertificate o KeyInfo: X509Data
- La data i hora al·legada 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

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 està s'especifica en la ISO 32000 - 1. La signatura PAdES EPES inclou la signatura electrònica de el 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 i dades de contacte del signant. Inclou, a més, la política de signatura.

Sobre aquestes firmes es pot construir una signatura PAdES - LTV que inclou, per a la verificació de les signatures i del contingut, que 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 verificació que es va fer en el seu moment continua sent vàlida i, a més, s'afegeix un nou segell de temps que protegeix les firmes i els seus validacions.



Aquest tipus de signatura s'usa per a qualsevol tipus de document, que hagi de conservar-se més que el temps de validesa del segell de temps corresponent.

Codi segur de verificació (CSV)

El codi segur de verificació consisteix en una seqüència de lletres i números generada de manera pseudoaleatòria i associada unívocament al document. La seva creació es realitza en base a un sistema de generació d'una URI (Uniform Resource Identifier) única per a cada un dels documents electrònics a imprimir de forma segura.

La Universitat utilitza el següent procediment per generar els CSV:

1. Es generarà una cadena de caràcters unint l'adreça MAC de servidor, el temps actual en milisegons, 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 per capolar, el qual serà truncat a 15 bytes.
3. Un cop obtingut aquest codi, es codificarà en base64 per tal d'obtenir 20 caràcters alfanumèrics.