Política de signatura i segell electrònics i de certificats de la Universitat Pompeu Fabra

SUMARI

1. Introducció

La Universitat Pompeu Fabra en la seva estratègia d'implantació del document i expedient electrònic com a element de base per evidenciar la seva actuació administrativa, tal i com estableix la Llei 39/2015 de Procediment Administratiu Comú de les Administracions Públiques, requereix dotar-se d'una Política signatura i segell electrònics i dels certificats, tal com estableix la resolució de 19 de juliol de 2011, de la Secretaria d'Estat per a la Funció Pública, per la qual s'aprova la Norma Tècnica d'Interoperabilitat de política de Signatura Electrònica i de certificats de l'Administració.

Tanmateix i d'acord amb el Reglament d'ús dels mitjans electrònics i del procediment administratiu electrònic en l'àmbit de la Universitat Pompeu Fabra, aprovat per Acord del Consell de Govern de 26 de gener del 2011, la identificació i acreditació de la voluntat dels òrgans administratius i de les persones ha de ser la que en cada cas es defineixi. En l'article 13 d'aquest Reglament s'estableix que la Universitat pot utilitzar diversos sistemes per a la seva identificació electrònica i per a l'autenticació dels documents electrònics que produeixi, com ara sistemes de signatura electrònica basats en la utilització de certificats de dispositiu segur o un mitjà equivalent, per a la publicació d'informació i de documentació; sistemes de signatura electrònica per a l'actuació administrativa automatitzada; signatura electrònica de les persones que formen part de la comunitat universitària; intercanvi electrònic de dades en entorns tancats de comunicació.

D'altra banda, d'acord amb l'article 14 del Reglament, la utilització de signatura electrònica reconeguda és un requisit suficient per identificar i considerar acreditada la voluntat de les persones que presentin escrits per via electrònica en qualsevol procediment o tràmit, de conformitat amb el que preveu el reglament sense perjudici que la Universitat pugui establir altres tipus de signatura electrònica que permetin garantir la seguretat i la integritat en la identificació i l'acreditació de la voluntat de les persones, atenent a una sèrie de criteris com ara les característiques dels canals electrònics que s'hagin habilitat per a la realització del tràmit, la proporcionalitat entre el requisit imposat i la transcendència jurídica que pugui tenir el tràmit concret per a la persona interessada, l'exigència formal de signatura en relació amb l'escrit presentat que es pugui establir en la normativa de procediment administratiu general o sectorial, el nivell de seguretat jurídica en funció dels riscos associats a l'operativa i la disponibilitat de la tecnologia i dels recursos de la Universitat.

Darrerament, en aquest àmbit, la Universitat va aprovar, el passat 7 de març de 2017, una resolució del Rector sobre la Política de signatura i els mecanismes d'identificació o d'autenticació i de signatura electrònica admesos a la Universitat Pompeu Fabra, en la qual es determina aquesta Política com el document que estableix els criteris generals per a l'admissió dels sistemes d'identificació i signatura per mitjans electrònics, alhora que defineix el procediment per ser aprovada i publicada. També estableix els principis bàsics que han de regular aquest política tant pel que fa als mitjans d'autenticació, com de signatura electrònica, preveient d'acord amb el que estableix l'article 10 de la Llei 39/2015

els sistemes de signatura electrònica basats en sistemes d'identificació més evidències electrònica, a part dels ja obligatoris certificats digitals.

Per tant, aquesta Política ha de garantir el correcte ús d'eines de signatura electrònica amb l'objectiu que permetin generar amb caràcter d'autenticitat documents electrònics, expedients electrònics i foliats d'expedients electrònics. Per això aquesta política es fonamenta en els següents criteris:

- La vocació de la Universitat en què la seva activitat administrativa pugui plasmar-se en documents i expedients electrònics autèntics, per donar compliment a la Llei 39/2015.
- Els documents electrònics signats electrònicament, en compliment del que estableix aquesta política, tindran plena validesa i es consideraran originals i definitius.
- El nivell de seguretat tecnològica, el tipus de certificat a utilitzar, el format de la signatura i del segellat i els mecanismes de preservació es fixaran en funció de la importància del document i de l'acte administratiu a què es refereixen.
- Les firmes electròniques que es generin a la Universitat es faran, en origen, amb el format i nivell de seguretat requerit per a la seva conservació durant tot el període de vida útil del document al qual fan referència. En el cas que això no fos possible, es procedirà a la completació d'aquestes signatures. De la mateixa manera, els documents electrònics que es rebin signats seran sotmesos a un procés de validació i completació de les signatures en el moment de la recepció.

En aquest sentit, en aquesta Política es desenvolupen els següents elements:

1. L'objecte amb el qual es desenvolupa la Política de signatura i segell electrònics i de certificats de la Universitat Pompeu Fabra.
2. Les dades identificatives de la política, els seus períodes de validesa i la seva transició a noves polítiques i l'assignació de responsabilitats per a la seva gestió.
3. La definició dels conceptes clau en matèria de signatura electrònica i que són desenvolupats al llarg de la Política.
4. La normativa i estàndards internacionals a la qual està subjecta la Política de signatura i segell electrònics i de certificats de la Universitat i en base a la qual es desenvolupa.
5. L'ús de certificats digitals:
    - Certificats digitals i identitats digitals admesos: quins certificats digitals o identitats digitals (acreditades a través d'un registre previ) poden utilitzar altres persones o entitats per relacionar-se telemàticament amb la Universitat.
    - Certificats digitals i identitats digitals emprats: quins certificats digitals i quines altres identitats digitals poden utilitzar els empleats

de la Universitat en l'exercici de les seves funcions, i quins segells electrònics estan previstos per a l'actuació automatitzada.

6. El cicle de vida dels certificats emprats per la Universitat, identificant el procediment de sol·licitud, de renovació, de revocació i de suspensió d'aquests.
7. Les classes, tipus i nivells de signatura, és a dir, el com i en quin format es generen les signatures electròniques emprades en l'àmbit de la Universitat i el procés seguit per a la seva validació. També assenyalar que es preveu en aquesta Política les signatures electròniques basades en identitats digitals i evidències electròniques associades a la voluntat de la signatura, tal com es recull en el capítol segon de la llei 39/2015 de procediment administratiu comú de les administracions públiques.
8. La definició del segell de temps com element que permet facilitar la preservació d'aquestes i alhora deixar evidència de la data i hora en què s'ha produït un acte.
9. El manteniment i la preservació de signatures electròniques per garantir la introducció en els sistemes de gestió documental de la Universitat de documents autèntics que garanteixin la preservació de la seva validesa jurídica a llarg termini mitjançant processos de ressegellat de temps.
10. La identificació de les metadades previstes en el Vocabulari de Metadades de la Universitat Pompeu Fabra per a la gestió efectiva de signatures electròniques.
11. Les normatives de signatura electrònica aplicades en un context particular que tenen per objectiu determinar la validesa d'una signatura electrònica en una transacció particular identificant quines obligacions assumeix la Universitat en cada cas, tenint en compte l'ús que s'ha de donar als objectes signats electrònicament, documents o expedients electrònics i el tipus d'actuació administrativa que recull l'acte de signatura.
12. La identificació d'un subconjunt representatiu de casos d'ús de la signatura electrònica que identifiquen possibles escenaris en els quals els procediments de la Universitat poden requerir l'ús de signatures electròniques vinculat a una normativa de signatura electrònica concreta:
    - Signatura electrònica d'un document electrònic.
    - Digitalització certificada de documents en paper: còpia certificada electrònica.
    - Còpia electrònica certificada d'un document signat electrònicament.
    - Processos de signatura automatitzada.
    - Signatura electrònica amb identificació i evidència electrònica d'un document electrònic.
    - Incorporació de documents signats digitalment per part del tercer.

Per a l'elaboració d'aquesta Política s'ha tingut en compte el que l'Esquema Nacional d'Interoperabilitat estableix al respecte i molt concretament, el que es defineix en la darrera versió de la Norma Tècnica d'Interoperabilitat de política de signatura electrònica, segells electrònics i de certificats digitals de l'administració, així com la de l'expedient electrònic pel que fa al procés de foliació aquest.

2. Objecte de la Política de signatura i segell electrònics

Aquesta política té per objecte establir el conjunt de criteris comuns assumits per la Universitat Pompeu Fabra en relació amb l'autenticació i el reconeixement de signatures electròniques basades tant en certificats com en evidències electròniques. En concret estableix les directrius a seguir per la Universitat Pompeu Fabra respecte a l'ús de la signatura electrònica en el si de les aplicacions corporatives, per garantir l'autenticitat, integritat i conservació dels documents signats digitalment. És d'aplicació tant a les firmes com als segells electrònics.

Així mateix l'objectiu d'aquesta Política és establir quins identitats digitals i certificats digitals de ciutadans i de tercers, la Universitat Pompeu Fabra accepta i quins certificats digitals utilitzen els empleats de la Universitat.

En aquest últim cas, també s'estableix el seu cicle de vida.

Com a cas particular, s'estableix també la signatura digital basada en identitats digitals més evidències electròniques.

Finalment, estableix les estratègies que la Universitat Pompeu Fabra per a la preservació a llarg termini de les signatures electròniques.

3. Dades de la Política de signatura i segell electrònics

3.1 Identificació de la política

Les dades identificatives de la Política de signatura i segell electrònics i de certificats són els que s'inclouen a continuació:

1. Nom del document: Política de signatura i segell electrònics i de certificat de la Universitat Pompeu Fabra.
2. Versió: 2.0
3. Data d'aprovació: Febrer 2018

3.1.1 Períodes de validesa i transició

La present Política de signatura i segell electrònics i de certificat de la Universitat Pompeu Fabra entrarà en vigor en la data de la seva aprovació i serà vàlida fins que no sigui substituïda o derogada per una altra política posterior.

Si s'estima oportú, una nova versió de la Política de signatura i segell electrònics i de certificat de la Universitat Pompeu Fabra pot facilitar un període de temps

transitori per adequar els diferents sistemes de signatura electrònica i validació utilitzats per la Universitat Pompeu Fabra a les especificacions de la nova versió.

Aquest període de temps de transició s'haurà d'indicar en la nova versió i superat el mateix només serà vàlida la versió actualitzada.

3.1.2 Identificació del gestor del document de la política

A continuació, s'inclouen les dades identificatives del gestor de la Política de signatura i segell electrònics i de certificats de la Universitat Pompeu Fabra:

1. Responsable de la política: Comissió d'Administració Electrònica
2. Adreça de contacte: Plaça de la Mercè, 10-12 08002 Barcelona
3. Correu electrònic de contacte: cdae@upf.edu
4. Telèfon de contacte: 93 542 17 83

4. Conceptes

S'ha cregut important incorporar un capítol de definició de termes, aplicats en aquest document, per fer més comprensible la Política de signatura i segell electrònics i de certificats de la Universitat Pompeu Fabra.

Casos d'ús de la signatura electrònica. En aquest document ens referim als casos d'ús de la signatura electrònica, als escenaris possibles de generació de documents electrònics signats. Per a cada cas d'ús s'identificaran els sistemes de signatura possibles, formats de signatura electrònica, els possibles nivells de signatura, la normativa de signatura electrònica a aplicar, etc. En el cas de la Universitat Pompeu Fabra es defineixen cinc tipus de casos d'ús diferents: signatura electrònica d'un document electrònic, digitalització certificada de documents en paper, còpia electrònica certificada d'un document electrònic signat electrònicament, processos de signatura automatitzada i incorporació de documents signats digitalment per part del tercer.

Classes de signatura electrònica. En aquest document ens referirem a les classes, a la validesa jurídica de la signatura electrònica, segons es defineix en la Llei 59/2003 de signatura electrònica: signatura simple o ordinària, avançada i reconeguda o qualificada.

Evidències electròniques. Conjunt d'informació en format electrònic que permet aportar informació a un acte i que pot ser utilitzat com a prova judicial en cas que hi hagi una disputa sobre aquest acte. En el cas de la Universitat Pompeu Fabra, el repositori del tercer de confiança en el qual es dipositaran aquestes evidències amb validesa jurídica serà la plataforma e-Logs del Consorci de Serveis Universitaris de Catalunya (CSUC).

Format de signatura electrònica. Forma en què es codifiquen les signatures electròniques. Els formats utilitzats són: XAdES, CAdES i PAdES.

Nivell de signatura. Amb aquest nom ens referirem a si el document té una única signatura o múltiples signatures i en aquest cas si es generen en paral·lel o niades.

Estàndards tècnics de signatura electrònica. Documents que detallen les normes relatives a la signatura electrònica, organitzades al voltant dels conceptes de generació i validació de signatura, en un context particular (contractual, jurídic, legal, ...), definint les regles i obligacions de tots els actors involucrats en aquest procés. L'objectiu d'aquest procés és determinar la validesa de la signatura electrònica per als diferents tipus de transacció.

Sistema de signatura. Amb aquest nom ens referim a si la forma electrònica d'un document s'ha realitzat amb un certificat digital del signant, o bé amb un sistema d'identificació més evidència electrònica de l'acte de la signatura.

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

5. Normativa aplicable i estàndards internacionals

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

A més, tant a nivell nacional com a la Unió Europea o internacionalment, les organitzacions d'estandardització tècnica han definit i documentat els criteris i formats que s'utilitzaran per a la gestió dels documents digitals en tots els seus aspectes, garantint la seva validesa jurídica.

En aquest apartat s'identifiquen el conjunt de normatives i estàndards internacionals que s'han tingut en compte per a la definició de la Política de signatura i segell electrònics i de certificats de la Universitat Pompeu Fabra.

5.1 Normativa aplicable

- Resolució del Rector de 7 de març del 2017 sobre política de signatura i els mecanismes d'identificació o autenticació i de signatura electrònica admesos a la Universitat Pompeu Fabra.
- Reglament d'ús dels mitjans electrònics i del procediment administratiu electrònic en l'àmbit de la Universitat Pompeu Fabra, aprovat per Acord del Consell de Govern de 26 de gener del 2011.
- Protocol d'Identificació i Signatura Electrònica, aprovat per Ordre del Departament de Governació i Relacions Institucionals (Ordre GRI/233/2015, de 20 de juliol del 2015), que marca els criteris d'acceptació i ús dels diferents mecanismes en l'àmbit de l'Administració de la Generalitat de Catalunya.

- Guia del Consorci AOC de Protocol d'Identificació i Signatura Electrònica, emesa conforme les competències que li atorga a aquest òrgan la Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya, i que té per objecte oferir un conjunt de criteris comuns similars a la resta d'administracions, quant als aspectes tècnics i organitzatius necessaris per a la implantació dels sistemes de identificació i signatura electrònica per a cada tràmit o servei, als efectes de determinar el seu grau de seguretat.
- Llei 40/2015, d'1 d'octubre, de règim jurídic del Sector Públic.
- Llei 39/2015, d'1 d'octubre de procediment administratiu comú de les administracions públiques.
- Llei 25/2015, de 28 de juliol, de mecanisme de segona oportunitat, reducció de la càrrega financera i altres mesures d'ordre social
- Llei 15/2014, de 16 de setembre, de racionalització del sector públic i altres mesures de reforma administrativa.
- Llei 59/2003, de 19 de desembre de signatura electrònica.
- Reial Decret 4/2010 de 8 de gener de l'Esquema Nacional d'Interoperabilitat.
- Reial Decret 3/2010 de 8 de gener de l'Esquema Nacional de Seguretat.
- Resolució de 19 de juliol de 2011 de la Norma Tècnica d'Interoperabilitat de Política de Signatura Electrònica i de certificats de l'Administració.
- Resolució de 19 de juliol de 2011 de la Norma Tècnica d'Interoperabilitat d'Expedient Electrònic.
- Reglament Europeu (UE) 910/2014 del Parlament Europeu i Consell, relatiu a la identificació electrònica i els serveis de confiança en les transaccions electròniques en el mercat interior.
- Decisió d'Execució (UE) 2015/1506 de la Comissió de 8 setembre 2015 per la qual s'estableixen les especificacions relatives als formats de les signatures electròniques avançades i els segells avançats que han de reconèixer els organismes del sector públic de conformitat amb els articles 27, apartat 5 i 37 apartat 5 de l'anterior Reglament.

5.2 Estàndards internacionals i altres convencions

- Estàndards tècnics de signatura electrònica compartides sota llicència d'ús BY - NC - SA del Creative Commons de l'empresa Astrea la Infopista Jurídica SL: http://astrea.es/web12/biblioesp/_estandares-tecnicos/
- ETSI RFC 2315 (1998), ETSE RFC 2630 (1999), IETF RFC 3369 (2002), IETF RFC 3852 (2004): PKCS # 7: 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".

6. Certificats digitals i altres identitats digitals

El mecanisme d'identificació basat en certificat digital es sustenta en l'existència d'autoritats de certificació que emeten certificats digitals i permeten comprovar que un certificat concret ha estat correctament emès i que continua sent vàlid en el moment del seu ús, és a dir de la signatura o segell d'un document. La relació entre l'Autoritat de Certificació i l'entitat que valida el certificat és una relació que es fonamenta en la confiança: els certificats seran acceptats només en la mesura en què l'entitat que l'ha de validar confiï en l'honestedat de l'Autoritat de Certificació.

Amb l'entrada en vigor de la Llei 39/2015, s'admeten també altres mecanismes d'identificació i/o signatura, més enllà dels certificats digitals, sempre que així ho disposi expressament la normativa reguladora aplicable.

6.1 Certificats digitals admesos per la Universitat Pompeu Fabra

La Universitat Pompeu Fabra admet, des de l'entrada en vigor de la Llei 15/2014, de 16 de setembre, de racionalització del sector públic i altres mesures de reforma administrativa, tots els certificats digitals reconeguts inclosos en la llista de confiança de prestadors de serveis de certificació (TSL) establerts a Espanya. Aquesta llista, està publicada a la seu electrònica del Ministeri d'Indústria, Energia i Turisme.

La Universitat Pompeu Fabra utilitza la plataforma PSIS del Consorci AOC tant per la validació dels seus certificats com per a certificats de tercers, de manera que l'acceptació efectiva de certificats vindrà condicionada per l'actualització dels serveis d'aquesta plataforma.

Si bé tecnològicament això és així, la Universitat decidirà quins sistemes d'identificació i signatura podrà utilitzar per a cada procediment administratiu, en base al nivell de seguretat requerit per al tràmit, així com el rol amb el que actuï el titular del certificat. A títol d'exemple, tot i que els certificats de ciutadà poden ser igual de qualificats que els de representació d'una empresa, per a tràmits amb empresa, només s'acceptaran aquells que siguin de representant.

6.2 Altres identitats digitals admeses per la Universitat Pompeu Fabra

En virtut de l'article, 9.2 de la Llei 39/2015, la Universitat admet, per als membres de la comunitat universitària, com a sistema d'identificació electrònica, el sistema d'usuari i contrasenya del Campus Global, en ser un sistema que compta amb un

registre previ com a usuari que permet garantir la seva identitat i assegurar que el sistema d'identificació és lliurat al seu titular.

Per a la resta de ciutadans (no membres de la comunitat universitària) es podran utilitzar, a mesura que es vagi fent la integració tècnica amb les aplicacions corporatives, els diferents sistemes d'identitat digital validats a través de la plataforma VÀLid del Consorci AOC, entre els quals destaquem: idCAT mòbil del Consorci AOC, MobileID de l'Ajuntament de Barcelona i Localret i el sistema Cl@ve de l'Administración General del Estado.

De la mateixa manera que en el cas dels certificats digitals, per a cada procediment administratiu, la Universitat, en base al nivell de seguretat que requereixi aquest, així com el rol amb el que actuï el titular d'aqueta identitat digital, decidirà quins sistemes d'identificació es podran utilitzar.

6.3 Certificats digitals proveïts per la Universitat Pompeu Fabra

En aquells casos que els empleats de la Universitat requereixin d'un certificat digital, la Universitat Pompeu Fabra els proveirà un certificat digital del Consorci AOC, que és un prestador reconegut o qualificat de serveis de certificació.

La Universitat Pompeu Fabra s'ha constituït com a Entitat de registre del prestador de serveis de certificació Consorci AOC (en avant CAOC) i, per tant, pot generar els certificats necessaris per als seus empleats.

Les targetes UPF inclouen dos certificats: un certificat per autenticar-se (identificat amb l'etiqueta "AUT") i un altre certificat per signar (identificat amb l'etiqueta "SIG").

Pel que fa als segells electrònics la Universitat Pompeu Fabra utilitzarà els del prestador de serveis de certificació CAOC i es generaran des de l'Entitat de registre de la Universitat Pompeu Fabra.

Finalment, pel que fa als certificats de servidor (pàgina web), la Universitat Pompeu Fabra podrà utilitzar diferents certificats digitals de diferents prestadores de serveis de certificació. La decisió de quins certificats s'utilitzaran, vindrà condicionada en cada moment pel nivell d'instal·lació de les claus públiques d'aquests prestadors en els navegadors utilitzats per la comunitat universitària.

No obstant això, a causa de la manca d'interoperabilitat de certes aplicacions de les AAPP, la Universitat Pompeu Fabra disposa i podrà continuar utilitzant certificats digitals emesos per la FNMT o d'altres prestadors per a la relació de la Universitat amb altres administracions públiques.

Pel que fa a l'ús de certificats digitals en servidor per a l'intercanvi segur d'informació entre AAPP s'utilitzarà els del CAOC, o si no, qualsevol dels emesos per altres autoritats de certificació que ja tinguin un alt nivell d'instal·lació, de les seves claus públiques, en els navegadors. Cal assenyalar que si bé aquests certificats no generen actes jurídics, s'ha considerat oportú esmentar-los.

6.4 Sistemes d'identificació proveïts per la Universitat Pompeu Fabra

La Universitat proveeix a tots els empleats de la Universitat Pompeu Fabra que hagin de tenir accés a determinats serveis o aplicacions d'un usuari i contrasenya al Campus Global.

7. Cicle de vida dels certificats digitals lliurats per la Universitat

La Universitat Pompeu Fabra utilitza com a prestador de serveis de certificació de referència el CAOC, del qual és entitat de registre.

Serà aquesta autoritat de certificació la responsable de definir les polítiques de gestió dels certificats digitals que emet, i per tant, és qui defineix la vigència dels certificats, la manera com es revoquen, es renoven, es validen, etc.

A l'efecte d'adoptar els procediments establerts pel prestador de serveis de certificació per operar l'entitat de registre, s'han establert procediments interns que identifiquen les activitats que es realitzen i els seus responsables, així com els procediments a seguir pels usuaris per a la sol·licitud, renovació , revocació, etc. dels seus certificats digitals.

7.1 Estudiants

Els certificats digitals d'estudiant s'emeten des del PIE (Punt d'Informació a l'Estudiant). Quan un estudiant es matricula per primera vegada a la Universitat es fa automàticament una petició de certificat digital, que es lliura a l'estudiant després de què el Banc imprimeixi la targeta, a través d'una campanya de lliurament del carnet de la UPF.

Els estudiants d'altres cursos, o aquells que pugin tenir una incidència amb el seu certificat, han de demanar hora al PIE, qui li generarà el certificat digital dins el seu carnet (targeta amb xip que ha rebut del banc).

Si un alumne perd la targeta ha de trucar al Consorci AOC, que és qui fa la suspensió del certificat digital i després adreçar-se al PIE, que revocarà el certificat. La suspensió deixa el certificat sense validesa durant 120 dies; després d'aquest període, si no s'ha tornat a habilitar, el certificat es revoca, i s'invalida definitivament. Per demanar un nou certificat haurà de seguir el mateix procediment establert per a casos d'incidències.

En els mesos de desembre o gener, el Servei de Gestió Acadèmica generarà un llistat d'estudiants que no s'han tornat a matricular i el farà arribar al PIE, que el revisarà i procedirà a la seva revocació.

7.2 PAS i PDI sense càrrec

Els certificats digitals de PAS i PDI s'emeten des del PIE. Quan un PAS o PDI requereix un certificat digital ha de demanar cita al PIE, que s'encarrega de demanar la targeta al Banc i procedeix a emetre el certificat i a la càrrega del

certificat en el carnet del treballador. Es segueix el mateix procediment en cas d'incidència amb el certificat.

Si un PAS o PDI perd la targeta ha de trucar al Consorci AOC, que és qui fa la suspensió del certificat digital i després adreçar-se al PIE, que revocarà el certificat. Per demanar un nou certificat haurà de seguir el mateix procediment establert per a casos d'incidències.

En el mes de març, el Servei de PAS elaborarà una relació de baixes que ha tingut la Universitat (i que no hagin passat a PDI) i la farà arribar al PIE, que procedirà a la seva revocació.

En els mesos de novembre o desembre, el Servei de PDI elaborarà una relació de baixes que ha tingut la Universitat (i que no hagin passat a PAS). Pel que fa als professors associats, s'inclouran en aquesta relació aquells que durant els dos anys anteriors no hagin estat contractats per la Universitat. La relació de baixes la farà arribar al PIE, que procedirà a la seva revocació.

7.3 Treballador públic amb càrrec

Els certificats digitals de treballador públic amb càrrec de la Universitat s'emeten i revoquen des de la Secretaria General. Quan el treballador és nomenat com a càrrec, el personal de la Secretaria General sol·licita el carnet al PIE. Un cop tenen el carnet generen el certificat digital i el lliuren, amb el carnet i el PIN, al càrrec.

En cas de pèrdua del carnet, el treballador públic ha de trucar al Consorci AOC per suspendre el certificat digital i s'ha d'adreçar després a la Secretaria General per revocar el certificat i generar un nou carnet i un nou certificat.

En el cas que un certificat estigui a punt de caducar, el Consorci AOC informa al sol·licitant i en cas que el càrrec continuï vigent, es procedeix a emetre un nou certificat seguint el mateix procediment com si es demanés de nou, tot revocant l'anterior.

En el cas que el treballador públic amb càrrec deixi el seu càrrec, la Secretaria General revocarà el certificat.

En el cas que el Servei de Personal tingui constància de la baixa d'una persona a la Universitat, haurà de comunicar a Secretaria General per tal que aquesta, en el cas que tingui un certificat amb càrrec, pugui procedir a la seva revocació.

7.4 Segells electrònics

En el cas dels certificats de segell d'òrgan i altres certificats tècnics, el procés de sol·licitud és el següent:

En el moment en què algun Servei necessita un certificat de segell, aquest ho sol·licita a Secretaria General.

Secretaria General constata la necessitat d'aquest segell electrònic i verifica que no n'hi ha cap dels ja emesos que pugui fer aquesta funció. En cas que algun dels certificats existents pugui fer aquesta funció, s'informa al Servei d'Informàtica per tal que l'habiliti pel nou ús. En el cas que no sigui així, es procedeix a sol·licitar un nou segell electrònic.

En el cas que calgui un nou segell electrònic, la Secretaria General fa la petició del segell d'òrgan, que valida el Servei d'Informàtica.

El Servei d'Informàtica és qui fa la sol·licitud i generació del certificat. Al Servei d'Informàtica hi ha dos rols, el de peticionari i el d'aprovador/generador. Les persones que són peticionaries no són aprovadores/generadores.

A continuació el Servei d'Informàtica comunica a Secretaria General la instal·lació del certificat en el servidor. És Secretaria General qui publica a la Seu Electrònica les dades del certificat digital.

En el moment en que el Servei d'Informàtica detecta que un certificat inclòs en l'inventari està a punt de caducar (3 mesos abans), ho comunica a la Secretaria General, que és qui autoritza la generació del nou certificat digital.

En els casos que es requereixi un certificat d'una altra Autoritat de Certificació diferent del CAOC és el Servei d'Informàtica qui comunica a la Secretaria General aquest fet, i serà la Secretaria General qui autoritzarà o no al Servei d'Informàtica a demanar aquest nou certificat digital.

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

8. Segell de temps

Les característiques principals del segell de temps són:

- És un segell electrònic generat per un tercer de confiança en base a un certificat digital especialment destinat a aquest efecte.
- 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 serà el proveïdor de serveis de certificació de referència.

- El proveïdor del servei de segellat de temps és el CAOC a través de la plataforma PSIS.
- El procés consisteix a crear una evidència electrònica sobre una signatura electrònica: es calcula el resum criptogràfic del document i / o les seves signatures electròniques (en el cas del ressegellat), és a dir, una operació matemàtica que s'aplica al conjunt d'informació sobre el que emetre el segell de temps i obté una cadena de bits anomenada "hash" la qual es xifra amb la clau privada del certificat de segell de temps utilitzat per fer l'operació. Es retorna aquesta firma conjuntament amb la data i hora de l'operació, així com informació sobre el certificat de segell de temps utilitzat per fer la signatura.
- El segell de temps s'incorporarà a les signatures electròniques en el format especificat en els estàndards XAdES-T, CAdES-T i PAdES-LTV.

9. Sistemes, classes, tipus i nivells de signatura o segell

En aquest apartat es recopilen els aspectes relacionats amb la signatura electrònica en el marc de la Universitat Pompeu Fabra, incloent els diferents usos de la signatura i segell electrònic en l'àmbit dels sistemes de la Universitat Pompeu Fabra. Els objectius que persegueix la Universitat Pompeu Fabra amb la implantació de la signatura electrònica són fonamentalment tres:

- Dotar a la Universitat Pompeu Fabra d'un sistema per al control, l'ús i la conservació de la documentació original signada electrònicament, gestionada en el desenvolupament habitual de la seva activitat.
- Garantir la gestió adequada dels documents de la Universitat Pompeu Fabra, assegurant l'autenticitat, la fiabilitat, la integritat i la disponibilitat futura al llarg del seu cicle de vida, basat en un programari informàtic que ofereix una capa de gestió de documents i arxiu comú.
- Donar resposta a les exigències en matèria d'arxiu electrònic de la Llei 39/2015 i de l'Esquema Nacional d'Interoperabilitat.

Un cop formulats aquests objectius bàsics, cal tenir present la definició dels sistemes de signatura electrònica, la Universitat podrà usar:

- **Signatura electrònica basada en l'ús d'un certificat digital**. És el sistema de signatura electrònica en la qual, partint de la clau privada d'un usuari, es xifra el resum criptogràfic del document a signatura i s'afegeix a aquesta signatura informació del certificat utilitzat per realitzar-la, la data de la signatura, la política de signatura, etc.

- **Signatura electrònica basada en la identificació més les evidències de la voluntat de la signatura**. Dins aquest tipus de signatura existiran dos casos:

- **Signatura interna amb sistemes propis de la Universitat.** El sistema consisteix en la identificació d'un usuari a partir de les seves credencials a Campus Global i, en el moment de signar, la captura de les evidències de l'autenticació d'aquesta persona, amb un segon factor d'autenticació (contrasenya diferent de la del Campus Global, un PIN que pugui tenir aquest usuari o que pugui rebre al moment a través d'un e-mail o al mòbil), més les dades identificatives del document a signar, així com el seu hash, l'hora i data de la signatura. Aquestes evidències, d'identificació i de voluntat de signatura, s'incorporaran en l'expedient dins el gestor documental de la Universitat, signades amb un segell electrònic de la Universitat, i també s'incorporaran en el sistema de gestió d'evidències electròniques del CSUC. Posteriorment es signa electrònicament, amb segell de temps, el document amb un certificat digital de segell electrònic de la Universitat. Finalment s'envia al signant o signants del document un e-mail informant-los de que s'ha signat aquest document. Aquest darrer e-mail serveix de control de la signatura.
- **Signatura amb la plataforma VÀLid**. En aquest cas la signatura es delega a la plataforma VÀLid i serà aquesta qui demanarà al signatari que s'autentiqui per a generar les evidències de voluntat de signar. En aquest cas, el que es retorna és una evidència en format XML, la qual es guardarà en el sistema de gestió d'evidències electròniques del CSUC, així com dins l'expedient. Posteriorment se signa electrònicament el document amb un segell electrònic de la Universitat amb segell de temps.

Pel que fa a les classes de signatura des d'un punt de vista jurídic:

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

Per a les definicions anteriors, s'utilitza el concepte clau de certificat reconegut o qualificat, que segons la Llei 59/2003, de 19 de desembre, de signatura

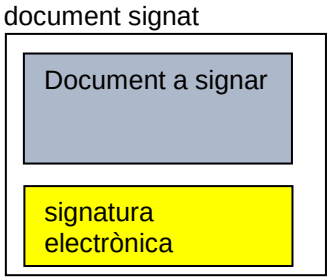
electrònica, en el seu article 11.1, el defineix com aquells certificats electrònics emesos per un prestador de serveis de certificació, que compleixen amb els requisits establerts en la mateixa llei quant a la comprovació de la identitat i la resta de circumstàncies dels sol·licitants i la fiabilitat i les garanties dels serveis de certificació que prestin.

La Universitat regularà per a cada procediment administratiu quin nivell de seguretat de signatura, així com quin rol ha de tenir el signatari i per tant, quins certificats digitals i sistemes de signatura electrònica es podran utilitzar.

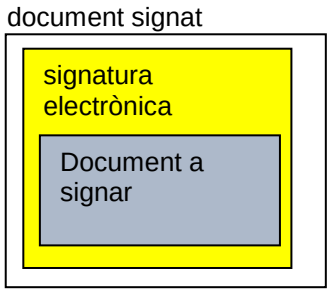
9.1 Tipus de signatura electrònica

Definicions de tipus de signatura utilitzades per la UPF 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 del 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.

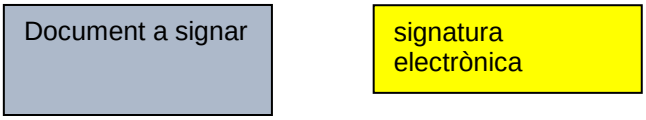


    - Enveloping (envoltant), en aquest cas el document signat és la signatura electrònica del document a signar i dins d'aquesta firma està el propi document a signar.



- **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 disposar del document i de la signatura electrònica. Com a resultat del procés de validació es pot obtenir un document d'evidència.

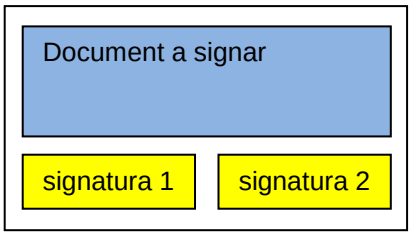


A continuació, definirem el nivell de signatures.

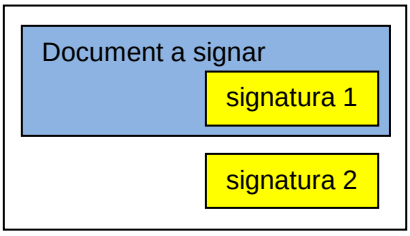
- **Signatura simple**: el document conté una única signatura.

- **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 firma paral·lela, o sobre el document signat, que s'identifica com a firma niuada.

Document signat amb signatura paral·lela:



Document signat amb signatura niada:



La signatura múltiple s'utilitzarà en diverses situacions en el marc dels procediments de la Universitat Pompeu Fabra, com per exemple en la signatura de documents electrònics per més d'una persona o al ressegellat de documents (veure apartat 11.6) ja signats per actualitzar la validesa legal del document al llarg del temps, abans que pugui quedar en entredit la validesa criptogràfica de la signatura electrònica.

9.2 Formats de signatura

Partint dels conceptes bàsics sobre signatura electrònica descrits anteriorment, a continuació, es descriuen els formats de signatura electrònica que utilitzarà la Universitat Pompeu Fabra en el marc d'aquesta Política de signatura i segell electrònics i de certificats.

9.2.1 Signatura electrònica amb política de signatura i amb segell de temps

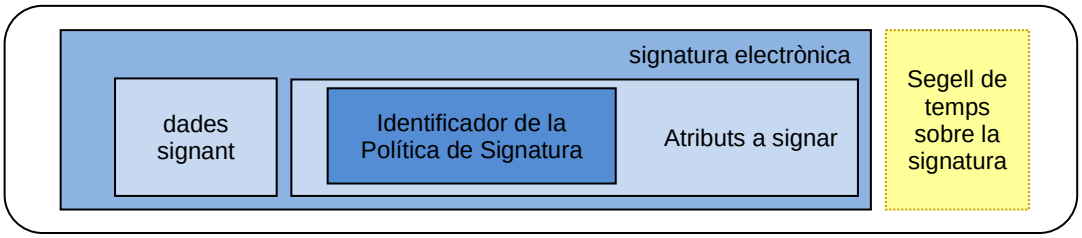
Aquest serà el format de signatura electrònica, avançada o reconeguda, pels documents electrònics i foliat d'expedients que s'hagin de guardar menys que la data de venciment del certificat digital utilitzat per generar el segell de temps associat a la signatura electrònica. En el cas de múltiples signatures, es tindrà en compte:

- En paral·lel: primera data de caducitat del segell de temps dins de les diferents firmes.
- Niades: data de caducitat del segell de temps de l'última signatura.

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

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

AdES



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

9.2.2 Signatura electrònica d'arxiu

Aquest serà el format de signatura electrònica avançada o reconeguda per als documents electrònics i foliat d'expedients que s'hagin de guardar més del temps de caducitat del certificat digital utilitzat per generar el segell de temps associat a la signatura electrònica. En el cas de múltiples signatures, es tindrà en compte:

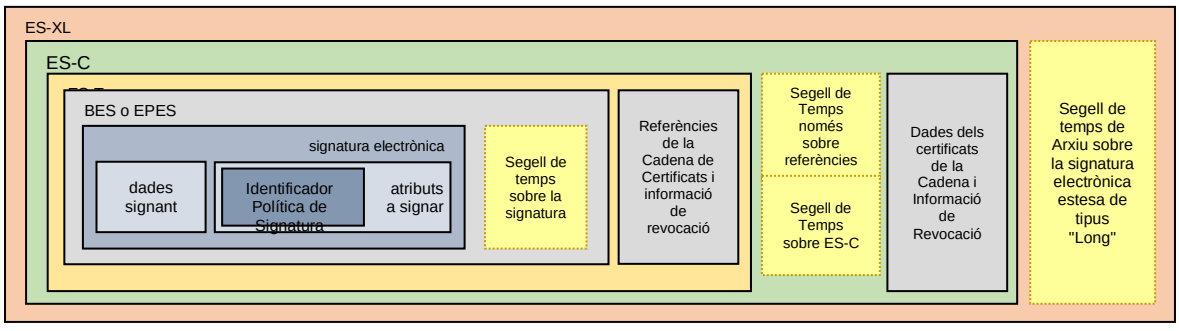
- En paral·lel: primera data de caducitat del segell de temps dins de les diferents firmes.
- Niades: data de caducitat del segell de temps de l'última signatura.

Hi ha dos formats d'arxiu:

9.2.2.1 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 de 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 del signant: 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

9.2.2.2 Signatura PAdES-LTV

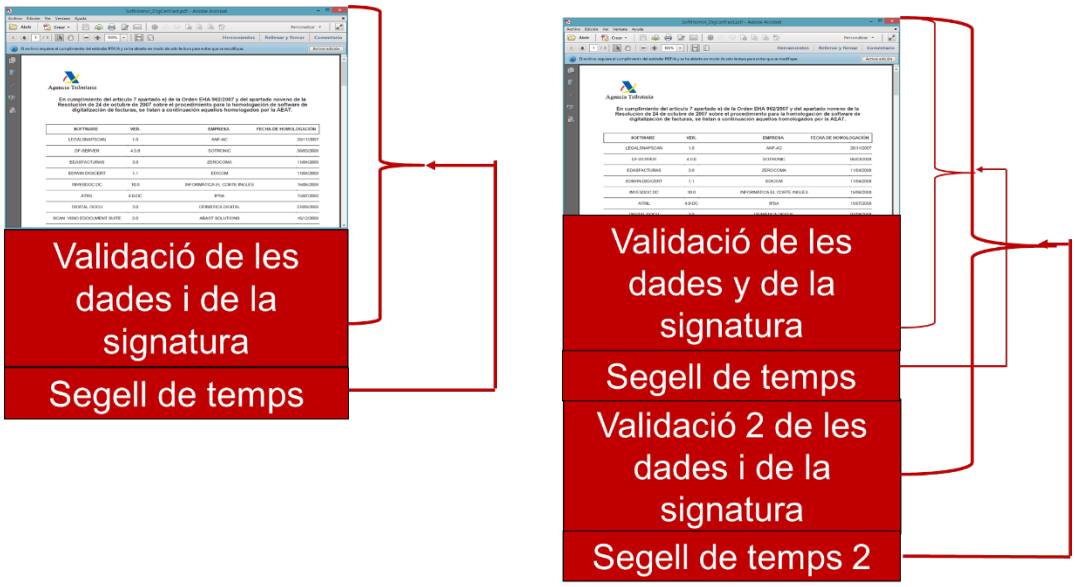
La signatura electrònica de llarga durada (Long Term Validation) és un format específic de la família PAdES. La signatura més bàsica, la PAdES Basic està especificada a la ISO 32000 - 1. La signatura PAdES EPES inclou la signatura electrònica del document (en format CAdES - BES), amb segell de temps (recomanat) i una resposta de validació d'un servei OCSP (recomanat). Pot incloure a més motius de signatura, el lloc de la signatura 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.

Es pot afegir a la signatura, posteriorment, un nou comprovant de verificació que garanteix que la verificació que es va fer en el seu moment continua sent vàlida i

s'afegeix un nou segell de temps per protegir les signatures i les seves validacions.

Exemple:



9.2.3 Signatura electrònica a través d'acreditació de la identitat i d'evidències de la voluntat de signatura.

9.2.3.1 Signatura a través de les eines pròpies de la Universitat.

Aquest serà un format específic, de signatura electrònica avançada per als documents electrònics que signi electrònicament un estudiant o un PAS o PDI a partir de l'ús de la identitat basada en usuari i contrasenya del Campus Global.

El procés de signatura es realitza de la següent manera:

- L'usuari s'haurà acreditat anteriorment en el sistema (primer factor d'autenticació).
- L'usuari omplirà el formulari a signar i premerà el botó de signatura, el qual li demanarà un segon factor d'autenticació).
- Això portarà a una pantalla on podrà introduir una segona contrasenya o un PIN que té aquest usuari, o be un PIN que aquest usuari pugui rebre per e-mail o telèfon mòbil. En el cas que l'usuari entri correctament aquesta segona contrasenya, es generarà una evidència amb dades del signant, del document (identificació del document i hash d'aquest), data i hora de la signatura i tipus de signatura (amb contrasenya (segona contrasenya, PIN fixa o PIN enviat). Aquesta evidència, la qual estarà signada amb un segell electrònic de la Universitat, es guardarà tant en l'expedient dins el gestor documental de la Universitat com al sistema de gestió d'evidències electròniques del CSUC. A continuació, es procedeix a la signatura del document amb un segell electrònic, més segell de temps

(signatura secundària). S'enviarà sempre un e-mail al signant confirmant la seva signatura del document.

En aquest format de signatura pot haver més d'una signatura d'aquest tipus sobre el document i aquestes poden ser en paral·lel o niuades.

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

Per tant, la validesa jurídica de la signatura electrònica a través d'acreditació de la identitat i d'evidències de la voluntat està vinculada al document i a les evidències del procés d'identificació del signant amb el PIN o segona contrasenya (signatura primària). Aquestes evidències es guarden sempre tant a l'expedient com al sistema de gestió d'evidències electròniques del CSUC, aportant la signatura electrònica i el segellat de temps del document signat, únicament evidències d'integritat i no d'autenticitat (signatura secundària). Aquest tipus de signatura s'ha regulat, tal com es requereix en l'article 10 de la Llei 39/2015 a través de la resolució del rector del 7 de març de 2017.

En cas de conflicte, la Universitat pot acreditar que ha aprovat i publicat a la Seu Electrònica la regulació específica, que ha generat les evidències no només en aquesta signatura sinó en qualsevol altra signatura del mateix tipus (signatura primària), que aquesta signatura es va produir en un moment determinat (segell de temps) i que el contingut del document no ha canviat (hash signat amb el primer segell electrònic (signatura primària) i document amb la seva signatura signat amb el segon segell electrònic (signatura secundària).

9.2.3.2 Signatura a través de VÀLid

Aquest serà un format específic, de signatura electrònica avançada per als documents electrònics que signi electrònicament un tercer a través de la plataforma VÀLid del Consorci AOC.

El procés de signatura es realitza de la següent manera:

- L'usuari s'haurà d'acreditar a la plataforma VÀLid, o bé amb certificat digital o bé amb algun dels sistemes previstos per aquesta plataforma: idcat Mòbil, MobileID, Cl@ve, etc.
- L'usuari omplirà el formulari a signar i premerà el botó de signatura. Aquesta acció redirigirà a l'usuari a la plataforma VÀLid amb la funció de signatura. En aquest cas li demanarà a l'usuari que torni a autenticar-se amb voluntat de signatura.
- Això generarà una evidència (XML) signada pel Consorci AOC (signatura primària) on hi ha el nom del document a signar, el hash i les dades del signatari. Aquesta evidència s'haurà de guardar tant en l'expedient com s'haurà d'enviar al sistema de gestió d'evidències electròniques del CSUC.
- A continuació, es procedeix a la signatura del document amb un segell electrònic, més segell de temps (signatura secundària).

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

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

Per tant, la validesa jurídica de la signatura electrònica a través de VÀLid està vinculada al document i a les evidències del procés de signatura del signant (signatura primària).

Aquest tipus de signatura, a l'igual que l'anterior, s'ha regulat, tal com es requereix en l'article 10 de la Llei 39/2015 a través de la resolució del rector del 7 de març de 2017.

En cas de conflicte, la Universitat pot acreditar que ha aprovat i publicat a la Seu Electrònica la regulació específica, que ha generat les evidències no només en aquesta signatura sinó en qualsevol altra signatura del mateix tipus (signatura primària), que aquesta signatura es va produir en un moment determinat (segell de temps) i que el contingut del document no ha canviat (hash signat amb el primer segell electrònic (signatura primària) i document amb la seva signatura signat amb el segon segell electrònic (signatura secundària).

10. Validació de signatures o segells

Per garantir la validesa jurídica dels documents electrònics signats digitalment, qualsevol document que entri o es generi en la Universitat Pompeu Fabra i que contingui una signatura o segell electrònic i / o un segell de temps, prèviament al seu emmagatzematge en el gestor documental, caldrà validar-lo.

Per validar s'utilitzarà algun d'aquests sistemes:

- La plataforma de validació de PSIS i els procediments que aquesta estableixi en cada moment.
- Mitjançant el procés abans especificat per a les signatures a través d'acreditació de la identitat i d'evidències de la voluntat de signatura.

En els casos de les signatures electròniques avançades i reconegudes, només en aquells casos en què el procés de validació de totes les signatures electròniques i dels segells electrònics sigui satisfactori es procedirà a, si no està ja en format AdES-A o PAdES-LTV, a completar-la fins aquest nivell i a emmagatzemar el document electrònic dins del gestor documental de la Universitat Pompeu Fabra.

Per al cas de les signatures a través d'acreditació de la identitat i d'evidències de la voluntat de signatura, es procedirà a emmagatzemar el document electrònic, amb les seves signatures (primària i secundària) en el gestor documental de la Universitat Pompeu Fabra directament sense cap validació addicional, en ser els sistemes de signatura d'aquest tipus de signatura ja segurs i no existir un procés automatitzat de validació.

En el cas de signatures electròniques basades en certificats digitals de prestadores de fora la Unió Europea, i en el supòsit que la Universitat decideixi acceptar aquest document, el procés de validació consistirà en:

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

En el cas que sigui necessària la preservació de la validesa jurídica del document més enllà del temps de vida del certificat digital utilitzat per generar qualsevol signatura associada a aquest document, o del segell de temps associat a la o les signatures electròniques, es procedirà a completar la signatura o signatures electròniques en el cas que aquestes no siguin ja signatura d'arxiu, és a dir "A" o "LTV". El completat es realitzarà a format de signatura d'arxiu.

Per al cas de les signatures a través d'acreditació de la identitat i d'evidències de la voluntat de signatura, es procedirà a la signatura electrònica del document amb un certificat de segell electrònic en format - A o - LTV. Per a aquest cas, només es realitzarà el completat en la signatura secundària.

11. Manteniment i preservació de les signatures i segells electrònics

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

1. **Caducitat del certificat digital amb el qual es signa un document electrònic.** Pot qüestionar-se la validesa d'un document electrònic a partir del dia que caduqui el certificat digital que es va utilitzar per a la signatura, la qual ha de ser evidentment posterior a la data de d'emissió del certificat digital i anterior a la data de revocació o de caducitat d'aquest. Per a garantir el moment en què es va generar la signatura electrònica, aquesta es pot completar amb un segell de temps emès per una Autoritat de Certificació. En el cas de la Universitat Pompeu Fabra estarem parlant de realitzar signatures -AdES-T tant a nivell de PDFs com de XML.

2. **Validesa del certificat digital en el moment de generar la signatura electrònica.** Pot qüestionar-se la validesa d'un document electrònic si

no existeix evidència suficient de que el certificat digital estava vigent el dia en que es va generar la signatura electrònica, es a dir, que no estava revocat. Per guardar l'evidència que un certificat digital, en la data de la signatura, no estava revocat, cal completar la signatura amb la informació de la validació d'aquest aspecte contra l'autoritat de certificació emissora del certificat. En aquest sentit cal tenir en compte que les autoritats de certificació, en el moment en què un certificat digital caduca, eliminen les evidències de revocació de la seva llista de revocats pel que, si no es guarda l'evidència esmentada un cop caducat el certificat, no hi haurà la certesa que el certificat amb què es va generar la signatura no estava revocat en aquell moment. En el cas de la Universitat Pompeu Fabra per garantir aquest cas estarem parlant de signatures AdES-XL o superiors (AdES-A o PAdES-LTV)

3. **Obsolescència tecnològica de la longitud de les claus criptogràfiques contingudes en el certificat digital i amb les que es generen les signatures electròniques.** Un document electrònic pot deixar de tenir validesa jurídica a partir del dia en què es posi en dubte la seguretat de les claus criptogràfiques amb les que es va signar. Davant d'aquest escenari, caldrà prendre mesures per tal de no continuar generant signatures amb aquest problema i assegurar les signatures anteriors. La UPF, per tal de donar resposta a aquest problema d'obsolescència tecnològica de les claus criptogràfiques, procedirà a generar certificats de major longitud de claus i utilitzar algorismes de hash més actualitzats i generar successives resignatures a partir de signatures que permetin incorporar aquests segells de temps. En el cas de la Universitat Pompeu Fabra (AdES-A o PAdES-LTV)

11.1 Ressegellat de signatures electròniques

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 del document.

Per poder aplicar aquest procés, cal que les signatures estiguin en un format que permeti afegir aquestes evidències de temps. Aquestes són les signatures del tipus XAdES - A, CAdES - A o PAdES - LTV. En el cas que una signatura no estigui en aquests formats, previ al ressegellat haurem completar la signatura, que en qualsevol cas estarà com a mínim en un format AdES – T, a un dels formats anteriorment definits.

Aquest serà un procés que es durà a terme, només per aquells documents que encara no s'hagin enviat a l'e-Arxiu, la plataforma de preservació de la Universitat:

- 6 mesos abans de que aquesta signatura li caduqui el darrer segell de temps aplicat.
- 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 longeva: XAdES - A o PAdES - LTV. Sobre aquestes firmes 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 del algoritme en el moment de la seva emissió.

Per al cas de les signatures a través d'acreditació de la identitat i d'evidències de la voluntat de signatura només es realitzarà el ressegellat només 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.

11.2 Manteniment de la validesa jurídica de les signatures en fase de vigència

El procés de manteniment de les signatures electròniques dins la Universitat Pompeu Fabra serà el següent, per al cas d'aquells documents que s'hagin de preservar:

1. En el cas de signatures generades dins de l'entorn de la Universitat Pompeu Fabra (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. Per a documents XML les signatures es transformaran a XAdES - A, com podria ser el cas del foliat de l'expedient i per als documents PDF es generarà una signatura electrònica en format PAdES - LTV.

2. En el cas de signatures que provenen de plataformes externes (altres administracions, eines de client, etc.) es procedirà en el seu cas a completar-les. Aquest procés de completació es realitzarà previ tancament i foliat de l'expedient. Per a documents XML les signatures es passaran a XAdES - A, com per exemple les factures, i per als

documents PDF es generarà una signatura electrònica en format PAdES - LTV.

3. En el cas que no sigui possible generar per algun document una signatura preservable, es procedirà al més aviat possible a foliar l'expedient amb un índex en format XML amb una signatura XAdES - A, de manera que sigui el foliat de l'expedient el que garanteixi la validesa jurídica de la signatura electrònica del document.

12. Metadades de signatura

Les metadades de signatura que utilitzarà la Universitat Pompeu Fabra són les següents:

Id	Nom UPF	Descripció	Nom vocabulari	Tipus	Format	Oblig.
15	Data creació	Data de creació/captura de l'element al sistema	ID_0018 Data de creació	Data	Data i Hora	S
19	Data de validació de la signatura	Data en què la signatura ha estat validada	ID_0027 Data de validació de la signatura	Data	Data i Hora	
24	Data última modificació	Des de l'última modificació de l'objecte		Data	Data i Hora	S
25	Descripció	Breu resum de l'abast cronològic, de l'àmbit geogràfic i del contingut (tipologia, tema principal, procediments administratius) de l'expedient	ID-0011 Descripció	Text	Obert	
37	Format de signatura	Format de la signatura (XAdES, etc.)	ID_0025 Format de signatura	Text	Obert	
38	Id Element [en el sistema]	Identificador propi de l'element al sistema		Identificador	Obert	S

40	Id_objecte_pare	Identificador de l'element on es troba el document. En aquest cas l'expedient.		Identificador	Obert	
9	Identificador de la signatura	Codi que identifica inequívocament a la signatura electrònica.	ID_0022 Identificador de la signatura	Text	Obert	S
39	Identificador del signatari	Número identificatiu del signatari	ID_0030 Identificador del signatari	Identificador	Obert	
	Identificador document	Identificador o vincle amb el document al qual pertany la signatura	ID_0023 Identificador document			S
51	Nivell de classificació evidencial	Identificar els diferents nivells de classificació evidencial segons el Marc Conceptual de Classificació d'evidències de CATCert	ID_0021 Nivell de classificació evidencial	Text	Obert	
46	Nom del signatari	Nom del signatari del document	ID_0029 Nom del signatari	Text	Obert	
52	Organització de la signatura	Nom de l'organisme del qual en depèn orgànicament el signatari	ID_0031 Organització	Text	Obert	S
53	Política de la signatura	Identificador de la política de signatura electrònica	ID_0033 Política signatura	Text	Obert	S
62	Tipus de signatura	Identificar el tipus de signatura	ID_0024 Tipus de signatura	Text	Obert	S
63	Unitat orgànica	Nom de la unitat orgànica del qual en depèn el signatari	ID_0032 Unitat orgànica	Text	Obert	

13. Estàndards tècnics de signatura electrònica dels actes administratius

Un estàndard tècnic de signatura electrònica és un document que conté un conjunt de normes relatives a la signatura electrònica, en un context particular (contractual, jurídic, legal, ...) que té per objectiu poder determinar la validesa d'una signatura electrònica en una transacció en particular.

Aquests estàndards tècnics s'organitzen sobre els conceptes de generació i validació de la signatura electrònica i defineixen les regles i obligacions de tots els actors involucrats en aquests processos. En aquest sentit, especifiquen la informació que ha d'incloure el signant en el procés de generació de la signatura, i la informació que ha de comprovar i complementar el verificador en el procés de validació de la mateixa.

La Universitat Pompeu Fabra, d'acord amb la recomanació del Consorci AOC, fa servir els estàndards tècnics de signatura electrònica compartides sota llicència d'ús BY - NC - SA del Creative Commons per l'empresa Astrea la Infopista Jurídica SL.

Astrea, amb la publicació de la biblioteca del estàndards tècnics de signatura electrònica, pretén facilitar a les eines de creació i de validació de signatures electròniques l'automatització dels processos de tractament de les mateixes, d'acord amb l'estàndard tècnic de signatura electrònica seleccionada en cada cas, mitjançant l'establiment d'unes regles bàsiques, que siguin comuns per a totes les administracions públiques. D'aquesta manera s'homogeneïtza el contingut tècnic de les signatures electròniques i s'afavoreix la interoperabilitat de les signatures electròniques en les relacions interadministratives.

En aquest sentit, els diferents estàndards de signatura electrònica incorporen compromisos de signatura, que són particularitzacions de la política general, i que permeten definir amb major granularitat els controls sobre les regles de creació i validació de les signatures electròniques; com poden ser: els nivells de seguretat acceptats en el certificat de firma, paper o càrrec del responsable de produir la signatura, etc.

A la biblioteca d'Astrea es recullen els estàndards de signatura electrònica associada als actes administratius més rellevants dins dels procediments telemàtics de les administracions públiques. En total es recullen fins a 34 normatives de signatura electrònica, les quals es relacionen a continuació:

- **Ciutadà**
    - *Acte de ciutadà*
    - Acte de declaració de voluntat
    - Acte de comunicació prèvia de ciutadà
    - Acte de conformitat de ciutadà
    - Acte de queixa o suggeriment de ciutadà

- Acte de declaració responsable de ciutadà
- Acte negocial de ciutadà
- Acte de sol·licitud de ciutadà

- **Administració**
  - Acte vistiplau de l'Administració
  - Acte de transmissió electrònica de dades
  - Acte de tràmit
  - Acte de sol·licitud de l'Administració
  - Acte resolutori
  - Acte de recepció electrònica
  - Acte de publicació electrònica
  - Acte de notificació electrònica
  - Acte d'aixecament d'acta
  - Acte de declaració responsable de l'Administració
  - Acte de còpia autèntica migrada
  - Acte de còpia autèntica digitalitzada
  - Acte de còpia autèntica compulsada
  - Acte consultiu
  - Acte de constància electrònica
  - Acte de comunicació electrònica
  - Acte negocial de l’administració
  - Acte de proposta
  - Acte de l’administració
  - Acte de foliat
  - Acte de fiscalització
  - Acte de dació de fe
  - Acte certificant
  - Acte administratiu

14. Casos d'ús de la signatura electrònica

Previ a la descripció dels casos d'ús identificats de signatura electrònica, és interessant comentar un concepte clau en aquest entorn de la documentació electrònica, i que no és altre que l'expedient administratiu, ja completament electrònic i el seu foliat, també electrònic. Per a això s'aprofita la definició que fa la Llei 39/2015, en l'article 70:

- S'entén per expedient administratiu el conjunt ordenat de documents i actuacions que serveixen d'antecedent i fonament a la resolució administrativa, així com les diligències encaminades a executar.
- Els expedients tindran format electrònic i es formaran mitjançant l'agregació ordenada de tots els documents, proves, dictàmens, informes, acords, notificacions i altres diligències hagin d'integrar. Així mateix, ha de constar en l'expedient còpia electrònica certificada de la resolució adoptada.
- Quan en virtut d'una norma calgui remetre l'expedient electrònic, es farà d'acord amb el que preveu l'Esquema Nacional d'Interoperabilitat i en les corresponents Normes Tècniques d'Interoperabilitat i s'enviarà complet, foliat, entrat i acompanyat d'un índex, així mateix autenticat, dels documents que contingui. L'autenticació de l'esmentat índex garantirà la integritat i immutabilitat de l'expedient electrònic generat des del moment de la seva signatura i permetrà la recuperació sempre que calgui. És admissible que un mateix document formi part de diferents expedients electrònics.

Per tant, l'índex de l'expedient, es guardarà en un fitxer XML, que haurà d'estar signat amb segell electrònic de la Universitat Pompeu Fabra. Aquesta signatura serà en format XML, més concretament signatura XAdES - A.

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

14.1 Signatura electrònica d'un document electrònic

Permet signar electrònicament documents en suport electrònic en qualsevol moment del seu cicle de vida. Aquestes signatures es realitzen sota el control de la Universitat Pompeu Fabra.

Les principals característiques d'aquest escenari 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 en el cas de signatures amb certificat digital del signant, validar la signatura.
- Cal incorporar al sistema, l'evidència de validació, que en el nostre cas serà la signatura completada, la qual serà en el cas de XML, el mateix

document amb signatura attached o un XML amb signatura detached i en el cas de PDFs el mateix document o bé signatura attached o bé detached.

- El document electrònic estarà en qualsevol format dels acceptats per la Universitat Pompeu Fabra, preferiblement PDF i XML, sempre que sigui necessari garantir la seva preservació al llarg del temps.
- El document es podrà signar diverses vegades i per diferents usuaris.
- Es podrà signar amb el sistema de signatura electrònica basada en certificat electrònic del signant o bé amb signatura a través d'acreditació de la identitat i d'evidències de la voluntat de signatura.
- Es podrà signar en paral·lel i / o de forma niada.
- En el cas de documents que no s'hagin de guardar més enllà de la validesa del segell de temps que utilitzi la Universitat Pompeu Fabra, la signatura (en el cas de la signatura a través d'acreditació de la identitat i evidències de la voluntat de signatura, la signatura es refereix a la signatura secundària) es generarà en format AdES - T o si no és possible, es completarà a aquest format.
- En el cas que els documents s'hagin de guardar més enllà de la validesa del segell de temps que utilitzi la Universitat Pompeu Fabra, la signatura electrònica es generarà o es completarà a AdES - A. Per als documents PDF serà PDF - LTV o XAdES - A en cas de signatures dettached i per als documents XML serà XAdES - A.

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

- Classe de signatura: Avançada o Reconeguda.
- Sistema de signatura:
    - Amb certificat electrònic: per a les signatures generades per la Universitat Pompeu Fabra: Certificat d'empleat o Certificat de Segell Electrònic del Consorci AOC. Els interessats (treballadors en condició d'interessats, estudiants, empreses, ciutadans) podran utilitzar qualsevol certificat definits en el punt 7.1 del present document.
    - Amb signatura a través d'acreditació de la identitat i d'evidències de la voluntat de signatura: podran generar aquest tipus de signatura els empleats de la Universitat en tràmits concrets i els estudiants. Les empreses no podran utilitzar aquest tipus de signatura.
- Formats: PAdES. Inicialment en format PAdES - T. En el cas de preservació es completarà la signatura a format PAdES - LTV.
- Segell de temps: Sí.
- Nivell de signatura: Simple, Múltiple (niuada o paral·lel).

- Tipus de signatura: Attached o Detached.
- Estàndard tècnic de signatura:
    - En el cas de signatura emesa per la Universitat o una altra administració pública: Acte de l'Administració (OID: 1.3.6.1.4.1.15096.2.3.201104.7)
    - En el cas de signatura emesa per la ciutadania: Acte de ciutadà (OID: 1.3.6.1.4.1.15096.2.3.201104.1)

14.2 Digitalització certificada de documents en paper: còpia certificada electrònica

Les principals característiques d'aquest escenari són:

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

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

- Classe de signatura: Avançada.
- Tipus de certificat: Certificat d'empleat o Certificat de Segell Electrònic del Consorci AOC.
- Formats: PAdES. Inicialment en format PAdES - T. En el cas de preservació es completarà la signatura a format PAdES - LTV.
- Segell de temps: Sí.
- Nivell de signatura: Simple.
- Tipus de signatura: Attached.
- Normativa de signatura: Acte de còpia autèntica digitalitzada (OID: 1.3.6.1.4.1.15096.2.3.201104.20).

14.3 Còpia electrònica certificada d'un document electrònic signat electrònicament

Permet obtenir còpies electròniques de documents originals signats electrònicament aplicant un canvi de format. Aquest seria per exemple el cas de la migració de formats en cas d'obsolescència tecnològica.

Les principals característiques d'aquest escenari són:

- A partir d'un document original signat electrònicament s'obté una còpia (per exemple, PDF / A o un altre format de preservació), certificada digitalment, per preservar.
- La còpia del document electrònic ha d'estar en un format normalitzat i estandarditzat abans de signar.
- El document se signarà automàticament una única vegada amb segell electrònic a nom de la Universitat Pompeu Fabra.

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

- Classe de signatura: Avançada.
- Tipus de certificat: Certificat de Segell Electrònic de l'AOC.
- Formats: Dependrà del format final. Si és PDF / A es generarà en format PAdES - LTV.
- Segell de temps: Sí
- Nivell de signatura: Simple
- Tipus de signatura: Attached o dettached.
- Normativa de signatura: Acte de còpia autèntica migrada (OID:1.3.6.1.4.1.15096.2.3.201104.19).

14.4 Processos de signatura automatitzada

Permet la signatura de diversos documents de forma automàtica amb un nivell important de garanties jurídiques. No requereix la intervenció del signant en el procés de signatura ja que només pot ser realitzada amb certificats de segell electrònic.

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 i XML).

- Es desarà al gestor documental de la Universitat Pompeu Fabra, tant els certificats digitals com els seus corresponents claus públiques que han de permetre generar processos de signatura automatitzada.

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

- Aquest escenari està pensat per a aquelles tasques en què s'han de signar diversos documents de forma automatitzada amb garanties jurídiques. No es contempla el procés de digitalització automàtica de documents, que està contemplat en el cas anterior.
- S'utilitzarà un certificat de segell electrònic o d'òrgan, que signarà els documents en nom de l'aplicació i de la Universitat Pompeu Fabra.
- Hi haurà una evidència que el responsable del certificat guardat al repositori segur de la Universitat Pompeu Fabra, ha autoritzat la signatura automatitzada.

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

- Classe de signatura: Avançada per als certificats de segell electrònic o d'òrgan que són avançats.
- Tipus de certificat: Certificat de Segell Electrònic de l'AOC.
- Formats: Per documents XML: XAdES - T i per a la seva conservació, XAdES - A. Per documents PDF: PAdES - T i per la seva conservació PAdES - LTV.
- Segell de temps: Sí.
- Nivell de signatura: Simple.
- Tipus de signatura: Attached.
- Normativa de signatura: Acte de l'Administració (OID:1.3.6.1.4.1.15096.2.3.201104.7), o la que sigui d'aplicació segons el tipus de document generat o acte realitzat.

Aquest és un escenari que abasta diversos àmbits que es podrien arribar a identificar com subescenaris diferents, com poden ser:

- Signatura automatitzada en processos de digitalització massiva.
- Ressegellat de documents per actualitzar la seva validesa criptogràfica.
- Per procediments d'intercanvi d'informació entre organitzacions i amb administracions.

14.5 Incorporació de documents signats digitalment per part del tercer

En el cas en què el tercer lliuri un document signat electrònicament per ell, caldrà:

- Validar les signatures electròniques del document.
- En el cas que les signatures no siguin o AdES - A / LTV es procedirà a completar.
- A continuació, es procedirà a incorporar al sistema el document amb les seves signatures completades.

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

- Classe de signatura: Avançada o Reconeguda en funció dels certificats utilitzats per a la seva signatura.
- Tipus de certificat: Qualsevol certificat definit en el punt 1.3.1 del present document.
- Formats: Per documents XML: XAdES - A. Per documents PDF: PAdES – LTV.
- Segell de temps: Aconsellat. Un cop completada la signatura: Sí
- Nivell de signatura: Simple, Múltiple (niuada o paral·lel).
- Tipus de signatura: Attached.
- Normativa de signatura: Acte de ciutadà (OID: 1.3.6.1.4.1.15096.2.3.201104.1).