Universitat Autònoma de Barcelona

Secretaria General

Edifici A · Campus de la UAB · 08193 Bellaterra (Cerdanyola del Vallès) · Barcelona · Spain
Tel. +34 93 581 1336 ·
sec.general@uab.cat · www.uab.cat

Instrucció nº 4/2021 sobre la política d'identificació i de signatura electròniques de la Universitat Autònoma de Barcelona

Universitat Autònoma de Barcelona

1.Preàmbul

La Universitat Autònoma de Barcelona ha aprovat una estratègia d'impuls i d'implementació dels projectes de document i d'expedient electrònic com a element bàsic de la seva actuació electrònica d'acord amb el que regulen la Llei 39/2015, d'1 d'octubre del Procediment Administratiu Comú de les Administracions Públiques i la Llei 40/2015, d'1 octubre, del Règim Jurídic del Sector Públic

L'article 9 de la Llei 39/2015, d'1 d'octubre del procediment Administratiu Comú de les Administracions Públiques, en endavant Llei 39/2015, estableix que les administracions públiques estan obligades a verificar la identitat de les persones interessades en el procediment administratiu la qual es podrà fer de forma electrònica mitjançant qualsevol sistema que compti amb un registre previ com a usuari que permeti garantir-ne la identitat.

Així mateix, l'esmentat article estableix que cada administració podrà determinar quins sistemes d'identificació admet per a dur a terme determinats procediment o tràmits.

L'article 10 de la Llei 39/2015 diu que en el supòsit que les persones interessades optin per relacionar-se amb l'administració pública a través de mitjans electrònics s'haurà d'establir els sistemes que els permetin signar de tal manera que s'acrediti la autenticitat de l'expressió de la voluntat, el consentiment, així com la integritat i inalterabilitat dels documents.

La Llei 40/2015, d'1 octubre, del Règim Jurídic del Sector Públic regula als articles 40 a 45 els sistemes d'identificació de les Administracions Públiques, el sistema de signatura per a les actuacions administratives automatitzades, la signatura electrònica del personal al servei de les Administracions Públiques i la interoperabilitat de la signatura electrònica.

En aquest sentit, l'article 9 del Reglament d'ús de mitjans electrònics en l'àmbit de la UAB aprovat per acord de Consell de Govern de 17 de novembre de 2010 disposa que la Universitat pot establir els sistemes d'identificació i de signatura electrònica basats en certificats de dispositiu segur o un mitjà equivalent.

L'esmentat Reglament regula a l'article 11 els Instruments d'identificació i d'acreditació de la voluntat de les persones que formen part de la comunitat

universitària, així com la necessitat de dotar de sistemes corporatius de signatura adequats a les funcions assignades.

Així mateix, l'article 12 especifica els mecanismes d'identificació i acreditació de les persones que no formen part de la comunitat universitària i a l'apartat 5 es diu que la UAB publicarà la relació dels sistemes de signatura electrònica admesos en les relacions entre la Universitat i els ciutadans i ciutadanes.

Finalment, l'article 13.2 estableix que la UAB decidirà els mecanismes d'identificació i de signatura electrònica per a cada procediment o tràmit d'acord amb els criteris de proporcionalitat, nivell de seguretat jurídica i disponibilitat de la tecnologia i recursos de la UAB.

La Instrucció s'ha adaptat als preceptes del Reglament (UE) núm. 910/2014, de 23 de juliol del Parlament Europeu i del Consell relatiu a la identificació electrònica i als serveis de confiança per a les transaccions electròniques en el mercat interior, així com a les disposicions del Reglament d'Execució de la Comissió Europea 2015/1502 de 8 de Setembre de 2015 pel que fa a l'esquema de nivells de seguretat, els tipus de signatura i de segell electrònic que cada administració podrà acceptar i emprar d'acord al seus requisits normatius i de seguretat.

Per finalitzar, cal tenir en compte les previsions establertes a la Norma Tècnica de Interoperabilitat de Política de Firma i Segell Electrònic i de Certificats de l'Administració, aprovada per Resolució de 27 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques i al Protocol d'identificació i Signatura Electrònica, aprovat pel Departament de Governació i Relacions Institucionals de la Generalitat de Catalunya (Ordre GRI/233/2015, de 20 de juliol del 2015).

2. Objecte de la Instrucció

L'objecte d'aquesta Instrucció és establir uns criteris comuns a la Universitat Autònoma de Barcelona en relació a la autenticació i el reconeixement de signatures electròniques basades en certificats i evidències electròniques. Concretament, estableix les directius pel que fa a l'ús de la signatura electrònica per tal de garantir la autenticitat, integritat i conservació dels documents signats electrònicament.

Així mateix, l'objectiu de la Instrucció és establir quines identitats i quins certificats digitals de ciutadans, tercers i membres de la comunitat universitària accepta la Universitat Autònoma de Barcelona.

3. Àmbit d'aplicació

Aquesta Instrucció s'aplica als tràmits i procediments que es produeixen en les relacions entre la Universitat Autònoma de Barcelona i entre els ciutadans i ciutadanes, entre els membres que formen part de de la comunitat universitària d'acord amb el que estableix l'article 7 del Estatuts del UAB, i en les relacions entre els àmbits administratius següents:

a) En l'àmbit de les relacions interadministratives mitjançant convenis o altres instruments jurídics

b) En l'àmbit de les relacions interorgàniques en els termes que expressament es determini.

4. Òrgans competents i les seves funcions

El secretari o la secretària general és l'òrgan encarregat d'elaborar la Instrucció de la política d'identificació i de signatura electròniques, d'impulsar-la i de vetllar pel seu compliment.

Així mateix, també tindrà les competències següents:

- Aprovar les modificacions de la Instrucció que li proposin les diferents àrees implicades en l'àmbit de l'administració electrònica.
- Validar per a cada tràmit o servei electrònic prestat el mecanisme d'identificació i de signatura electròniques que proposi l'àrea competent, en funció del nivell de seguretat requerit per a cada tràmit o servei electrònic prestat.
- Validar el nivell de seguretat requerit per a cada tràmit o servei electrònic prestat.
- Acordar els mecanismes de difusió i formació d'aquesta instrucció.

La Secretaria General pot encomanar a l'Oficina de Gestió de la Informació i de la Documentació la gestió i distribució dels sistemes de signatura electrònica

seguint els criteris tècnics establerts en aquesta Instrucció ajustant-los a les necessitats de cada procés o document.

5. Identitat i signatura electròniques

Els mecanismes d'identitat, de signatura electròniques i de segell electrònic que es poden fer servir són el regulats pel Reglament (UE) 910/2014 relatiu a la identificació electrònica i serveis de confiança (en endavant ReIDAS) i les normatives autonòmiques i estatals en matèria d'identificació i signatura electròniques i es determinaran en funció del subjecte i el grau de seguretat del tràmit corresponent.

De conformitat amb la normativa europea s'estableixen els nivells de seguretat següents:

- Nivell de seguretat baix: amb l'objectiu de reduir el risc d'ús indegut o alteració de la identitat.

- Nivell de seguretat mitjà o substancial: amb l'objectiu de reduir substancialment el risc d'ús indegut o alteració de la identitat.

- Nivell de seguretat alt: amb l'objectiu d'evitar l'ús indegut o l'alteració de la identitat.

Així mateix, d'acord amb el que estableix l'article 11.2 de la Llei 39/2015 es requereix l'ús obligatori de signatura electrònica per:

a) formular sol·licituds
b) presentar declaracions responsables o comunicacions
c) interposar recursos
d) desistir d'accions
e) renunciar a drets

6. Mecanismes d'identificació i de signatura electròniques de la UAB

LA UAB aprovarà i publicarà a la Seu electrònica el catàleg de tràmits i serveis indicant per a cadascun d'ells el sistema d'identificació i de signatura requerit en funció del nivell de seguretat assignat.

6.1 Identificació i signatura de la Universitat Autònoma de Barcelona

6.1.1 Identificació

- Certificat de segell electrònic basat en un certificat reconegut o qualificat que reuneixi els requisits exigits per la legislació de signatura electrònica.

- Certificats qualificats d'autenticació de lloc web, a nom de la Universitat Autònoma de Barcelona, d'acord amb el que estableix l'article 45 del ReIDAS

- Certificats electrònics qualificats, perfil "Sede electrónica administrativa", emesos per prestadors qualificats de serveis de certificació (PQSC) inclosos en la *Trusted Services List* (en endavant TSL) publicada per l'òrgan competent de qualsevol país de la Unió Europea d'acord amb el que estableix el Reglament eIDAS..

- Certificat de representant de persona jurídica.

6.1.2 Signatura

- En l'àmbit de l'actuació administrativa automatitzada de la UAB, d'acord amb el que disposa l'article 42 de la Llei 40/2015 d'1 d'octubre, de Règim Jurídic del Sector Públic, la UAB podrà utilitzar qualsevol dels sistemes següents:

  - Certificat qualificat de segell electrònic a nom de la Universitat Autònoma de Barcelona, d'acord amb el que estableix la Secció 5 del Reglament eIDAS.

  - Codi segur de verificació (CSV) ofert per la Universitat Autònoma de Barcelona el qual permet comprovar la integritat del document

  En aquests dos supòsits si es tracta d'un document dels explicitats a l'annex II, apartat 1, caldrà afegir, si no en disposa, els elements següents:

    - Segell electrònic
    - Codi CSV
    - Segell de temps

- Quan la UAB signi fora de l'àmbit de l'actuació administrativa automatitzada s'utilitzarà el certificat de representant de persona jurídica.

6.2. Empleats públics de la UAB

6.2.1. Identificació

Els empleats públics de la UAB, PAS i PDI, podran utilitzar qualsevol dels sistemes següents:

- Certificats electrònics qualificats, perfil "Empleado público" o que acrediti la vinculació del titular amb la UAB, emesos per un PQSC inclòs en la TSL publicada per l'òrgan competent de qualsevol país de la Unió Europea d'acord amb el que estableix ReIDAS. És el cas de:
    - Certificats del Consorci AOC: T-CAT P i T-CAT.
- Certificat electrònic qualificat de ciutadà. És el cas de:
    - Certificat idCAT.
    - Certificat del DNI electrònic.
- Autenticació biomètrica.
- Sistemes de claus concertades basades en usuari i contrasenya, com les que facilita la pròpia Universitat en el moment d'atorgar la identitat UAB o qualsevol altre sistema que s'integri en una plataforma de validació.

  En aquest supòsit, cada tràmit i servei electrònic pot establir que addicionalment s'incloguin mecanismes d'identificació com:

  - El registre de l'usuari en el sistema d'autenticació de manera presencial o mitjançant un certificat qualificat.
  - Incloure una clau d'un sol ús.

6.2.2. Signatura

Els empleats públics de la UAB, PAS i PDI, podran utilitzar qualsevol dels sistemes següents:

- Certificats electrònics qualificats, perfil “Empleado público” o que acrediti la vinculació del titular amb la UAB, emesos per un PQSC inclòs en la TSL publicada per l’òrgan competent de qualsevol país de la Unió Europea d’acord amb el que estableix eIDAS. Entre altres, s’admetran els següents:

    - Certificats del Consorci AOC: T-CAT P i T-CAT.

- Certificat electrònic qualificat de ciutadà. És el cas de:

    - Certificat idCAT.
    - Certificat del DNI electrònic.

En aquests dos supòsits si es tracta d’un document dels explicitats a l’annex II, apartat 2, caldrà afegir, si no en disposa, els elements següents:

- Codi CSV
- Segell de temps

- Signatura biomètrica.

- Sistemes de claus concertades basades en usuari i contrasenya, com les que facilita la pròpia Universitat en el moment d’atorgar la identitat UAB o qualsevol altre sistema que s'integri en una plataforma de validació.

  El sistema de claus concertades s’utilitzarà com a signatura electrònica del personal de la Universitat quan actuïn en exercici de les seves competències i funcions i quan es relacioni amb la Universitat.

  El rector o rectora, el secretari o la secretària General, els vicerectors o vicerectores, el gerent o la gerent, el president o la presidenta del Consell Social o qualsevol altre càrrec que actuï per delegació dels esmentats només podran utilitzar el sistema de claus concertades com a signatura electrònica quan no actuïn en el exercici de les seves funcions i competències.

- Codi segur de verificació (CSV) ofert per la Universitat Autònoma de Barcelona com a ens, el qual permet comprovar la integritat del document.

En els supòsits d’utilitzar signatura amb sistemes de claus concertades com amb el cas de signatura amb CSV si es tracta d’un document dels explicitats a l’annex II, apartat 2, caldrà afegir, si no en disposa, els elements següents:

- Segell electrònic
- Codi CSV
- Segell de temps

A més, si s'utilitza el sistema de claus concertades es pot establir addicionalment que calgui afegir als anteriors elements el següent:

- Comprovacions sobre la autenticitat de la declaració de la voluntat de l'interessat: arxivar les evidències i les metadades associades a la signatura i al document.

6.3. Estudiants de la UAB

Els mecanismes d'identificació i signatura que s'especifiquen a continuació pels estudiants de la Universitat també es poden aplicar, amb les adaptacions necessàries, per les persones físiques no pertanyents a la comunitat universitària.

6.3.1. Identificació

- Certificats electrònics qualificats de signatura electrònica emesos per un PQSC inclòs en la TSL publicada per l'òrgan competent de qualsevol país de la Unió Europea d'acord amb el que estableix ReIDAS. Entre d'altres, s'admetran els mecanismes següents:

  - Certificats del Consorci AOC: idCAT.
  - Certificat del DNI electrònic.

- Autenticació biomètrica.

- Sistemes de claus concertades basades en usuari i contrasenya, com el facilitat per la pròpia Universitat en el moment d'atorgar la identitat UAB o qualsevol altre sistema que s'integri en una plataforma de validació.

  Cada tràmit i servei electrònic pot establir que addicionalment s'incloguin mecanismes d'identificació com:

  - El registre de l'usuari en el sistema d'autenticació de manera presencial o mitjançant un certificat qualificat o bé
  - Incloure una clau d'un sol ús.

6.3.2. Signatura

- Certificats electrònics qualificats de signatura electrònica emesos per un PQSC inclòs en la TSL publicada per l'òrgan competent de qualsevol país de la Unió Europea d'acord amb el que estableix ReIDAS. Entre d'altres, s'admetran els mecanismes següents:
  - Certificats del Consorci AOC: idCAT.
  - Certificat del DNI electrònic.

- Signatura biomètrica.

- Sistemes de claus concertades basat en usuari i contrasenya, com el facilitat per la pròpia Universitat en el moment d'atorgar la identitat UAB o qualsevol altre sistema que s'integri en una plataforma de validació.

Si el tràmit està qualificat com d'una categoria alta o substancial es poden exigir els requeriments següents:

- Incorporació per part de la UAB d'un segell electrònic i un segell de temps.
- Comprovacions addicionals sobre la autenticitat de la declaració de la voluntat de l'interessat: arxivar les evidències i les metadades associades a la signatura i al document.

6.4. Persones jurídiques

6.4.1 Identificació i signatura

- Els certificats qualificats emesos a favor d'una persona jurídica o un ens sense personalitat jurídica i custodiats per una persona física, titular del certificat, la qual el pot emprar per actuar en nom de l'empresa o de l'ens indicat en el certificat.

- Els certificats qualificats emesos a favor d'una persona jurídica o un ens sense personalitat jurídica, amb indicació expressa de la representació que exerceix la persona física titular del certificat.

- Els certificats de segell electrònic qualificat, emesos a favor d'una persona jurídica o a un ens sense personalitat, per un dels PQSC inclòs en la TSL publicada per l'òrgan competent de qualsevol país de la Unió Europea d'acord amb el que estableix ReIDAS.

- Els mecanismes emprats per a la identificació de persones físiques que autentiquin la identitat d'un ciutadà que declara representar una persona jurídica. Aquests mecanismes només valdran quan la UAB pugui verificar la representació mitjançant la consulta a un registre en línia de representacions.

6.5 Segells de temps

Addicionalment cada tràmit o servei de la UAB determinarà la necessitat que les signatures electròniques avançades incorporin segells de temps generats, entre altres, pels serveis següents:

- El Consorci AOC.
- Els serveis publicats a la seu electrònica del Ministeri corresponent.
- Qualsevol altre servei de segell de temps qualificat conforme al que estableix la secció 6 de ReIDAS i que hagi estat inclòs en una de les llistes de serveis de confiança publicades pels estats membres de la Unió Europea, d'acord amb el que estableix l'article 22 d'aquest reglament.

6.6 Altres mecanismes d'identificació i de signatura

La incorporació de nous mecanismes d'identificació i de signatura electròniques s'ha de fer d'acord amb el procediment establert en el punt 8 d'aquesta Instrucció.

7. Admissió de mecanismes d'identificació i de signatura electròniques

L'admissió dels mecanismes d'identificació i de signatura electrònica es du a terme conforme als nivells de seguretat requerits en l'Esquema Nacional de Seguretat (ENS) i a l'Annex del Reglament d'Execució 2015/1502 de la Comissió Europea.

Amb caràcter general, els ciutadans i ciutadanes es podran identificar electrònicament davant de la Universitat Autònoma de Barcelona emprant qualsevol sistema d'identificació que compti amb un registre previ com a usuari que permeti garantir la seva identitat.

També podran acreditar mitjançant una signatura electrònica l'autenticitat de l'expressió de la seva voluntat i consentiment, així com la integritat i la inalterabilitat de les dades i/o documents que vulguin signar.

Una persona jurídica o un ens sense personalitat jurídica podrà acreditar l'origen i la integritat de les dades i/o dels documents signats que remeti a la Universitat Autònoma de Barcelona en el context d'un servei electrònic, mitjançant un segell electrònic o una signatura electrònica qualificada del representant de l'ens.

Els mecanismes d'identificació i signatura electròniques considerats admissibles per als tràmits d'una categoria determinada seran també admissibles per als tràmits classificats de categoria inferior.

La UAB determinarà per a cada tràmit i servei electrònic el nivell de seguretat requerit per tal de garantir la protecció de la confidencialitat, la integritat i l'autenticitat de les dades o documents implicats.

8. Actualització i seguiment de l'aplicació de la Instrucció d'identificació i signatura electrònica

El secretari o la secretària general podrà encarregar l'actualització de la Instrucció a l'àrea competent en la matèria; així mateix procedirà a la incorporació o la supressió dels mecanismes d'identificació i de signatura electròniques establerts, així com revisarà els nivells de seguretat d'aquests mecanismes.

L'actualització dels mecanismes d'identificació i signatura es publicaran a la Seu electrònica de la Universitat.

Universitat Autònoma de Barcelona

Signat digitalment per:

Esther Zapater Duque
Secretària general

2021.03.25 12:11:09 +01'00'

Universitat Autònoma de Barcelona

Annexos

-Annex I: “Glossari”
-Annex II: “Procediments i tipus de documents en els que cal utilitzar un Codi Segur de Verificació-CSV”.

Universitat Autònoma de Barcelona

Annex I. Glossari

Actuació Administrativa Automatitzada (AAA)

L'actuació administrativa automatitzada és un acte d'una Administració pública realitzat íntegrament amb mitjans electrònics, en el marc d'un procediment administratiu i sense la intervenció directa d'un empleat públic.

Autenticació i signatura biomètriques

L'autenticació biomètrica es l'aplicació de tècniques sobre els trets físics o de conducta d'una persona, amb l'objectiu de verificar la seva identitat.

La signatura biomètrica és una tecnologia que permet capturar dades biomètriques (paràmetres físics únics d'una persona) durant el procés de signatura manuscrita sobre un dispositiu electrònic.

Certificat digital

Un certificat digital és l'equivalent electrònic d'un document d'identitat i s'acostuma a utilitzar per:

- Identificar una persona, per exemple, per fer un tràmit en línia.
- Signar digitalment un document o un correu electrònics.

Certificat del DNI electrònic

Certificat de ciutadà expedit per la *Dirección General de la Policía (Ministerio del Interior)*.

Certificat idCAT

Certificat de ciutadà expedit pel Consorci Administració Oberta de Catalunya-AOC.

Certificat de representant

Certificat emès a una persona física com a representant d'una persona jurídica.
Un exemple d'aquest certificat és el Certificat de *Representación*, Fábrica Nacional de Moneda y Timbre (FNMT).

Universitat Autònoma de Barcelona

Certificat segell electrònic

És un certificat digital que serveix per a la identificació i l'autenticació de l'exercici de la competència en l'Actuació Administrativa Automatitzada (AAA).

Certificats T-CAT i T-CAT P

Certificat del personal de les administracions públiques catalanes expedit pel Consorci Administració Oberta de Catalunya-AOC.

Codi Segur de Verificació (CSV)

El Codi Segur de Verificació (CSV) permet comprovar la integritat i l'autenticitat de les còpies dels documents signats electrònicament.
Per fer-ho cal introduir aquest CSV, imprès al document, a l'adreça del web de la institució emissora.

Consorci Administració Oberta de Catalunya-AOC

El Consorci Administració Oberta de Catalunya (Consorci AOC), impulsat pels grups polítics del Parlament de Catalunya, el Govern de la Generalitat de Catalunya i els governs locals representats per Localret, té com a objectiu impulsar la transformació digital de les administracions catalanes.

Esquema Nacional de Seguretat (ENS)

L'Esquema Nacional de Seguretat té com a objectiu establir la política de seguretat en la utilització de mitjans electrònic. L'ENS està constituït per principis bàsics i requisits mínims que permeten una protecció adequada de la informació.

Factors d'autenticació

El Reglament d'Execució (UE) 2015/1502 de la Comissió de 8 de setembre de 2015 defineix com a "factor d'autenticació" un factor confirmat com a vinculat a una persona, que es troba en alguna de les categories següents:

- Factor d'autenticació basat en la possessió: factor en el que el subjecte està obligat a demostrar possessió del mateix.

- Factor d'autenticació basat en el coneixement: factor en el que el subjecte està obligat a demostrar el coneixement del mateix.
- Factor d'autenticació inherent: factor que es basa en un atribut físic d'una persona física del qual el subjecte està obligat a demostrar la seva possessió.

Plataforma de validació

Lloc web on es pot comprovar la validesa d'una signatura o d'un certificat electrònic, entre altres utilitats.

- Plataforma Valide, Govern d'Espanya.
- Plataforma Signasuite, Consorci AOC.

Prestador Qualificat de Serveis de Certificació (PQSC)

Un prestador qualificat de serveis de certificació és una persona, física o jurídica que expedeix certificats electrònics o que presta altres serveis en relació amb la signatura electrònica.

Reglament eIDAS

Reglament (UE) Nº 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança en les transaccions electròniques en el mercat interior.

Segell de temps

El segellat de temps permet demostrar que una sèrie de dades han existit i no han estat alterades des d'un instant específic en el temps.

Segell electrònic

És un sistema de signatura, basat en un certificat electrònic, que permet autenticar una actuació administrativa automatitzada.

El signatari no és una persona física, si no un organisme de l'Administració.

Universitat Autònoma de Barcelona

Trusted Services List (TSL)

És un llistat, facilitat per cada Estat membre de la Unió Europea, sobre la qualificació dels serveis electrònics de confiança oferts pels prestadors de serveis de certificació (PQSC) d'acord amb el Reglament eIDAS.

Universitat Autònoma de Barcelona

Annex II: Procediments i tipus de documents en els que cal utilitzar un Codi Segur de Verificació-CSV

1.-Actuació Administrativa Automatitzada (AAA) El CSV en l'AAA només es podrà utilitzar, per autenticar totes aquelles actuacions automatitzades aprovades mitjançant resolució i en tot cas:
1.1.- Comunicacions electròniques amb ciutadans i empreses
1.2.-Generació i emissió de certificats i documents administratius electrònics
1.3.-Generació i emissió de còpies electròniques autèntiques a partir de documents electrònics i de documents en suport no electrònic
1.4.-Processos de segellat de documents electrònics, amb l'objectiu de facilitar la seva interoperabilitat, conservació i llegibilitat
1.5.-Inscripcions, anotacions registrals i arxiu de documents electrònics registrals
1.6.-Generació i emissió d'acusaments de rebut, inclosos els generats pels diferents registres electrònics
2.-Com a signatura d'empleat públic
2.1.- Signatura d'actes resolutoris
2.2.- Signatura d'actes de tràmit
2.3.- Signatura d'actes de mera comunicació
3.-Documentació en paper
3.1.-Documentació en la què l'interessat és una persona física aliena a la comunitat universitària
3.2. -Qualsevol document en què la unitat responsable de la seva tramitació tingui l'evidència, o la sospita, que pot acabar en suport paper. Entre altres: • Documents que afecten o poden interessar a terceres persones • Expedients disciplinaris • Documents requerits durant un procés judicial