NOR08 – Política de signatura electrònica i de certificats

Classificació de la Informació:

Nivel del Document	Procediment
Nom del Fitxer	NOR08 – Politica de firma electronica va.docx
Tipus	Públic
Ámbit de Difusió	Comité de Seguretat de l'AYUNTAMIENTO DE PAIPORTA
Responsable	Responsable de Seguretat de l'AYUNTAMIENTO DE PAIPORTA

CONTROL DE MODIFICACIONES		
Descripción	**Versión**	**Fecha**
Primera aprovació por la Junta de Govern Local.	1.0	18/02/2022
Publicació en el BOP nº 55	1.0	21/03/2022

ÍNDEX DE CONTINGUT

1. OBJECTE

El present document té per objecte la definició dels diferents mecanismes d'identificació i signatura admesos en la Seu electrònica i resta de subsistemes de la plataforma d'administració electrònica SEDIPUALBA que utilitza l'Ajuntament de Paiporta sota conveni amb la Diputació d'Albacete. Aquesta plataforma integra els sistemes de gestió d'expedients i d'arxiu electrònic corporatiu. D'aquesta manera es pretén establir l'esquema de referència de l'organització per a la identificació, l'autenticació i el reconeixement de signatures electròniques basades en certificats, arreplegats en la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.

Els objectius perseguits amb l'ús de certificats de signatura electrònica són els següents:

- En la signatura de documents i continguts electrònics, garantir l'autenticitat, la integritat i el no repudi d'aquests.
- En la signatura electrònica de transmissió de dades, garantir l'autenticació dels actors involucrats, així com la integritat del contingut del missatge de dades i el no repudi dels missatges en una comunicació telemàtica.

Els certificats electrònics de signatura electrònica podran ser utilitzats, així mateix, per part de la ciutadania i del personal empleat públic de l'organització, com a mitjà d'autenticació de la identitat, com a mitjà de signatura electrònica de documents i de certificació de la integritat d'un document.

D'altra banda, en el present document es concreten els procediments a seguir per l'organització per a la generació, validació i conservació de signatures electròniques, així com les característiques i requisits exigibles als sistemes de signatura electrònica, els certificats, els serveis de segellament de temps, i altres elements de suport de les signatures de l'organització.

La present política, de primer nivell normatiu, proporciona resposta al que es disposa pel Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica (d'ara en avant, ENS) i, més en concret, a les previsions que segueixen:

- Article 33. Signatura electrònica.
- Marc organitzatiu. Procediments de seguretat [org.3].
- Mesures de protecció de la informació. Signatura electrònica[mp.info.4].

2. ABAST

L'àmbit d'aplicació de la present política serà el de les signatures electròniques realitzades per l'organització que afectaran a:

- Les relacions de la ciutadania amb l'organització.
- Les relacions de l'organització amb altres administracions.

3. NORMATIVA Y ESTÀNDARDS D'APLICACIÓ

A continuació, es relaciona la normativa legal i els estàndards, que s'han tingut en consideració per a l'elaboració de la present norma.

- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança
- Llei 25/2013, de 27 de desembre, d'impuls de la factura electrònica i creació del registre comptable de factures en el sector públic.
- Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica.
- Reial decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració electrònica.
- Reial decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics.
- Reglament (UE) núm. 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior i pel qual es deroga la Directiva 1999/93/CE.
- 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.
- NOR-01: política de seguretat de la informació.
- NOR-02: normativa general de la seguretat de la informació.
- Guia de seguretat de les TIC. CCN-STIC-807 Criptologia d'ocupació en l'Esquema Nacional de Seguretat.

4. GLOSSARI

TERME	DESCRIPCIÓ
Signatura electrònica	Conjunt de dades en forma electrònica, consignats al costat d'uns altres o associats amb ells, que poden ser utilitzats com a mitjà d'identificació del signant.
Política de signatura electrònica	Conjunt de normes de seguretat, d'organització, tècniques i legals per a determinar com es generen, verifiquen i gestionen les signatures electròniques, incloent les característiques exigibles als certificats de signatura.
Signant	Persona que posseeix un dispositiu de creació de signatura i que actua en nom propi o en nom d'una persona física o jurídica a la qual representa.
Verificador	Entitat, ja siga persona física o jurídica, que valida o verifica una signatura electrònica recolzant-se en les condicions exigides per la política de signatura concreta per la qual es regeix la plataforma de relació electrònica o el servei concret al qual s'estiga invocant. Podrà ser una entitat de validació de confiança o una tercera part que estiga interessada en la validesa d'una signatura electrònica.

Prestador de serveis de certificació (PSC)	Persona física o jurídica que expedeix certificats electrònics o presta altres serveis en relació amb la signatura electrònica.
Emissor i gestor de la política de signatura	Entitat que s'encarrega de generar i gestionar el document de política de signatura, pel qual s'han de regir el signant, el verificador i els prestadors de serveis en els processos de generació i validació de signatura electrònica.

5. DADES IDENTIFICATIVES I VALIDESA DE LA POLÍTICA

El present document de política de signatura electrònica i de certificats tindrà un identificador únic, i s'assignarà els dos últims dígits a la versió que corresponga, a fi de distingir les versions successives que puguen existir quan es realitzen actualitzacions.

La present política de signatura electrònica i de certificats serà vàlida des de la data d'emissió indicada fins que siga derogada o es publique una nova versió. Els períodes de transició seran indicats en les noves versions i, una vegada transcorreguts els terminis indicats, seran vàlides únicament les versions actualitzades.

A més, en el cas d'actualització de la present política de signatura electrònica i de certificats, s'identificarà l'enllaç URL on trobar les versions anteriors per a verificar una signatura electrònica anterior a la política vigent.

	IDENTIFICADOR DE LA POLÍTICA
Nom del document	*Política de signatura electrònica i de certificats de l'Ajuntament de Paiporta.*
Versió	*1.0*
Identificació del document	*OID 2.16.724.1.3.1.1.2.1.0*

Al gestor de la present política de signatura electrònica i de certificats correspon el manteniment, actualització i publicació electrònica dels criteris sobre signatura electrònica.

	IDENTIFICADOR DEL GESTOR
Nom del gestor de la política	Àrea d'Innovació de l'Ajuntament de Paiporta
Direcció de contacte	C/ Mestre Músic Vicent Prats i Tarazona, s/n Paiporta (València, Espanya) 46200

6. REGLES COMUNES

Les regles comunes estableixen les responsabilitats respecte a la signatura electrònica sobre la persona o entitat que crea la signatura i la persona o entitat que la verifica, defineixen els

requisits mínims que han de presentar-se, i hauran d'estar signats si són requisits per al signant, o no signats si són requisits per al verificador.

Aquestes regles es defineixen d'acord amb els formats de signatura electrònica admesos, tenint en compte els diferents usos de la signatura electrònica basada en certificats, l'ús d'algorismes i els processos de creació i validació de signatura.

6.1. REGLAS DEL SIGNANT

El signant serà responsable que el fitxer que es vol signar no incorpora contingut dinàmic que poguera modificar el resultat de la signatura durant el temps. Si el fitxer que es vol signar no ha sigut creat pel signant, s'assegurarà que no existeix contingut dinàmic dins del fitxer, com poden ser macros.

El signant haurà de proporcionar, com a mínim, la informació continguda en les següents etiquetes dins del camp (SignedProperties) que conté les propietats conjuntament signades a l'hora de la generació de la signatura XMLDsig de caràcter obligatori, a saber:

- SigningTime: indica la data i l'hora. En el cas de signatura en client sense accedir a servidor, serà merament indicativa (perquè la data en el dispositiu client és fàcilment manipulable) i/o serà utilitzada amb finalitats diferents a conèixer la data i hora de signatura. Les polítiques particulars de signatura electrònica podran determinar característiques i restriccions particulars respecte a generació en client de les referències temporals i sincronització del rellotge.
- SigningCertificate: conté referències als certificats i algorismes de seguretat utilitzats per a cada certificat. Aquest element haurà de ser signat a fi d'evitar la possibilitat de substitució del certificat.
- SignaturePolicyIdentifier: identifica la política de signatura sobre la qual es basa el procés de generació de signatura electrònica, i ha d'incloure els següents continguts en els elements en què se subdivideix com segueix.
    - Una referència explícita al present document de política de signatura en l'element xades:SigPolicyId. Per a això, apareixerà el OID que identifique la versió concreta de la política de signatura o la URL de la seua localització. <xades:SigPolicyId> <xades:Identifier> ... </xades:Identifier>
    - L'empremta digital del document de política de signatura corresponent i l'algorisme utilitzat, en l'element <xades:SigPolicyHash>, de manera que el verificador puga comprovar, calculant al seu torn aquest valor, que la signatura està generada segons la mateixa política de signatura que s'utilitzara per a la seua validació.
    - DataObjectFormat: defineix el format del document original, i és necessari perquè el receptor conega la manera de visualitzar el document.

Les etiquetes restants que poden agregar-se en el camp SignedProperties seran considerades de caràcter opcional, sense perjudici de la seua consideració obligatòria en polítiques particulars, sempre basades en la política marc:

- SignatureProductionPlace: defineix el lloc geogràfic on s'ha realitzat la signatura del document.

- SignerRole: defineix el rol de la persona en la signatura electrònica. Almenys un d'aquests elements ClaimedRoles o CertifiedRoles han d'estar presents en aquest camp: ○ "supplier" o "emissor": quan la signatura la realitza l'emissor.
- "customer" o "receptor": quan la signatura la realitza el receptor.
- "third party" o "tercer": quan la signatura la realitza una persona o entitat diferent a l'emissor o al receptor.

- CommitmentTypeIndication: defineix l'acció del signant sobre el document signat (l'aprova, l'informa, el rep, el certifica, ...)
- AllDataObjectsTimeStamp: conté un segell de temps, calculat abans de la generació de la signatura, sobre tots els elements continguts en ds: Reference.
- IndividualDataObjectsTimeStamp: conté un segell de temps, calculat abans de la generació de la signatura, sobre alguns dels elements continguts en ds: Reference.

6.2. REGLES DEL VERIFICADOR

L'encarregat de la verificació de la signatura serà responsable de definir els processos de validació i d'arxivat, de conformitat amb els requisits de la política de signatura particular a la qual s'ajusta el servei i amb el que s'estableix en la NTI de política de gestió de documents electrònics.

El format bàsic de signatura electrònica avançada no inclou cap informació de validació més enllà del certificat signant, que està inclòs en l'etiqueta Signing Certificate, i de la política de signatura que s'indique en l'etiqueta Signature Policy.

Els atributs que podrà utilitzar el verificador per a comprovar que es compleixen els requisits de la política de signatura, segons la qual s'ha generat la signatura, independentment del format utilitzat (XAdES, CAdES o PAdES), són les següents:

- Signing Time: només s'utilitzarà en la verificació de les signatures electròniques com a indicació per a comprovar l'estat dels certificats en la data assenyalada, ja que únicament es pot assegurar les referències temporals mitjançant un segell de temps (especialment en el cas de signatures en dispositius client). Si s'ha realitzat el segellament de temps, el segell més antic dins de l'estructura de la signatura s'utilitzarà per a determinar la data de la signatura.
- Signing Certificate: s'utilitzarà per a comprovar i verificar l'estat del certificat (i, si escau, la cadena de certificació) en la data de la generació de la signatura, en el cas que el certificat no haja caducat i es puga accedir a les dades de verificació (CRL, OCSP, etc.) o bé en el cas que el prestador de serveis de certificació (PSC) oferisca un servei de validació històric de l'estat del certificat.
- Signature Policy: s'haurà de comprovar, que la política de signatura que s'ha utilitzat per a la generació de la signatura es correspon amb la que s'ha d'utilitzar per a un servei en qüestió.

Existeix un temps d'espera, conegut com a període de precaució o període de gràcia, per a comprovar l'estat de revocació d'un certificat.

L'encarregat de la verificació podrà esperar aquest termini per a validar la signatura o realitzar-la en el mateix moment i revalidar-la després. El període des que es realitza la signatura o el segellament de temps deurà, com a mínim, el temps màxim permès per al refresc complet de les CRLs o el temps màxim d'actualització de l'estat del certificat en el servei OCSP. Aquests terminis podran variar en funció del prestador de serveis de certificació.

7. REGLES DE CONFIANÇA

7.1. REGLAS DE CONFIANÇA DE CERTIFICATS ELECTRÒNICS

Per a executar la signatura electrònica de contingut es consideraren vàlids aquells certificats reconeguts de conformitat amb la Llei 59/2003, de 19 de desembre, i amb la Directiva 1999/93/CE de 13 de desembre de 1999, així com les noves tipologies de certificats definits en la Llei 11/2007, de 22 de juny i els sistemes de signatura i certificats electrònics d'acord amb l'article 10 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.

En conseqüència, amb l'anterior, els certificats admesos són els que segueixen:

a) Sistemes de signatura electrònica reconeguda o qualificada i avançada basats en certificats electrònics reconeguts o qualificats de signatura electrònica expedits per prestadors inclosos en la "Llista de confiança de prestadors qualificats de serveis electrònics de confiança"[1].

Sistemes de segell electrònic reconegut o qualificat i de segell electrònic avançat basats en certificats electrònics reconeguts o qualificats de segell electrònic inclosos en la "Llista de confiança de prestadors qualificats de serveis electrònics de confiança".

b) Altres sistemes que l'organització puga considerar vàlid per a realitzar determinats tràmits o procediments del seu àmbit de competència, en els termes i condicions que s'establisquen.

Els certificats de signatura electrònica d'empleat públic emesos per la Fàbrica Nacional de Moneda i Timbre-Real Casa de la Moneda (FNMT-RCM) es consideren vàlids per a la realització de signatura electrònica per part dels empleats i empleades de l'organització i, en conseqüència, garanteixen la identificació i signatura de les persones participants en la tramitació de quants procediments electrònics es determinen.

La relació de segells electrònics utilitzats per l'Ajuntament de Paiporta, que indica les característiques dels certificats electrònics i els prestadors que els expedeixen, serà pública i accessible a través de la seua seu electrònica. Addicionalment, la verificació dels segells i certificats electrònics, incloent el de la pròpia Seu, es podrà efectuar a través de l' "Aplicació de validació de signatura i certificats en línia i demostrador de serveis de @firma"[2] o altres sistemes reconeguts de validació electrònica.

[1] https://sede.serviciosmin.gob.es/prestadores/paginas/inicio.aspx

[2] https://valide.redsara.es/valide/inicio.html

7.2. REGLES DE CONFIANÇA PER ALS SEGELLS DE TEMPS

El segell electrònic de temps assegura que tant les dades originals del document que serà segellat com la informació de l'estat dels certificats, en cas que s'hagen inclòs en la signatura electrònica, es van generar abans d'una determinada data. El format del segell de temps haurà de complir les recomanacions d'IETF, RFC 5816, "Internet X.509 Public Key Infrastructure; Time-Stamp Protocol (TSP)". Els elements bàsics que componen un segell digital de temps són:

https://sede.serviciosmin.gob.es/prestadores/paginas/inicio.aspx

https://valide.redsara.es/valide/inicio.html

- Dades sobre la identitat de l'autoritat emissora (identitat jurídica, clau pública a utilitzar en la verificació del segell, nombre de bits de la clau, l'algorisme de signatura digital i la funció hash utilitzats).
- Tipus de sol·licitud cursada (si és un valor hash o un document, quin és el seu valor i dades de referència).
- Paràmetres del seqüenciador (valors hash "anterior", "actual" i "següent").
- Data i hora UTC.
- Signatura digital de tot l'anterior amb la clau pública i esquema de signatura digital especificats.

El segellament de temps pot ser afegit per l'emissor, el receptor o un tercer i s'ha d'incloure com a propietat no signada en el camp Signature Time Stamp. El segellament de temps ha de realitzar-se en un moment pròxim a la data inclosa en el camp Signing Time i, en qualsevol cas, sempre abans de la caducitat del certificat del signant. La present política admet segells de temps expedits per prestadors de serveis de segellament de temps que complisquen les especificacions tècniques ETSI TS 102 023, "Electronic Signatures and Infrastructures (ESI); Policy requirements for estafe-stamping authorities".

7.3. REGLES DE CONFIANÇA PER A SIGNATURES LONGEVES

Els estàndards XAdES (ETSI TS 101 903) en les seues diferents versions contemplen la possibilitat d'incorporar a les signatures electròniques informació addicional per a garantir la validesa d'una signatura a llarg termini, una vegada vençut el període de validesa del certificat. La informació podrà ser inclosa pel signant o pel verificador, i haurà de fer-se transcorregut el període de precaució o de gràcia.

Existeixen dos tipus de dades a incloure com a informació addicional de validació:

- La informació de l'estat del certificat en el moment en què es produeix la validació de la signatura o una referència a aquests.
- Els certificats que conformen la cadena de confiança.

En el cas que es desitgen generar signatures longeves, s'haurà d'incloure la informació de validació anterior, i afegir-li un segell de temps. En aquests tipus de signatura la validesa de la signatura resultant ve determinada per la duració del segell de temps que s'afig a la signatura longeva. En el cas que es desitge incorporar a la signatura la informació de validació, s'haurà d'usar validació mitjançant OCSP (Online Certificate Estatus Protocol), ja que mitjançant aquest mètode les propietats o atributs a incloure són de menor grandària.

Si la consulta a l'estat de validació de la signatura generara un elevat volum d'informació, alternativament a la informació de validació indicada anteriorment, es podrà incloure en la signatura longeva referències a aquesta informació. Dins del format de signatura XAdES, el format estès XAdES-C incorpora aquestes entre altres propietats no signades:

- CompleteCertificateRefs, que conté referències a tots els certificats de la cadena de confiança necessària per a verificar la signatura, excepte el certificat signant.
- CompleteRevocationRefs, que conté referències a les CRLs i/o respostes OCSP usades en la verificació dels certificats.

En el cas que es desitge incorporar a la signatura la informació de validació, s'utilitzarà el format XAdES-X, que afig un segell de temps a la informació anterior. El format XAdES-XL a més de la informació inclosa en XAdES-X, inclou dues noves propietats no signades:

- CertificateValues.
- RevocationValues.

Aquestes propietats inclouen, addicionalment a les referències a la informació de validació, la cadena de confiança completa i la CRL o resposta OCSP obtinguda en la validació. Per als atributs CertificateValues i Revocation-Values es recomana fer la validació per OCSP, ja que aquests valors poden ser molt voluminosos en cas de realitzar la validació mitjançant CRL.

En el cas que es desitge incorporar a la signatura aquesta informació de validació, es recomana usar el format XADES-A, que afig un segell de temps a la informació anterior.

7.4. SIGNATURA BIOMÉTRICA

La signatura biomètrica es considerarà, amb caràcter general, equivalent a la signatura manuscrita i es realitzarà en presència de personal empleat públic que garantirà la identitat del signant.

Se seguirà el següent procediment:

1. El personal empleat públic sol·licita el DNI a la persona signant i comprova que les seues dades identificatives es corresponen amb les que consten en el sistema.

2.- El sistema compon el document de signatura combinat:

2.1.- S'eliminen els espais en blanc, i s'obté la seua forma canònica segons el procediment estàndard del W3C (https://www.w3.org/tr/xmlc14n11/).

2.2.- Es calcula el hash SHA3-512.

3.- S'informa la persona signant sobre les dades a signar:

3.1.- D'una banda, es mostren en la pantalla del dispositiu de signatura tant el hash calculat com la data i hora del PC al qual està connectat.

3.2.- D'altra banda, aqueix mateix hash i la corresponent relació de documents PDF a signar es posaran a la disposició de la persona signant a través d'una pantalla de visualització, per al seu acarament, abans de sol·licitar-li que signe.

4.- La persona signant realitza la signatura.

5.- El personal empleat públic comprova que la signatura traçada correspon amb la signatura que consta en el DNI i l'accepta.

6.- El sistema emmagatzema el fitxer de signatura generat pel dispositiu i el dibuix de la signatura.

7.- El sistema segella electrònicament el document XML corresponent a la signatura biomètrica, amb el següent format, que conté el hash mostrat en la pantalla del dispositiu abans de signar i el contingut del fitxer de signatura generat, així com les dades personals de la persona signant i les dades personals del personal empleat que arreplega la signatura.

Per motius de seguretat de la informació i protecció de les dades de caràcter personal, ni la signatura biomètrica ni el segell de temps seran accessibles públicament mitjançant el CSV. Sí que ho serà el traç de la signatura, igual que seria visible la rúbrica de la signatura manuscrita en un document en paper.

Els administradors de la Seu podran accedir a la informació de forma completa en cas que fora necessari.

7.5. SIGNATURA AMB PSEUDÒNIM (OCULTA)

La signatura amb pseudònim (o oculta) en l'àmbit de la present política consisteix en una signatura electrònica o biomètrica les dades de la qual no estan disponibles públicament en verificar el corresponent CSV. Entre aquestes dades es troben la signatura pròpiament dita i les dades identificatives de la persona signant (NIF, nom i cognoms).

Únicament els administradors de la seu poden obtenir totes les dades relatives a aquesta signatura, en cas de ser necessari. La resta de persones únicament podran visualitzar el pseudònim utilitzat en la signatura.

8. IDENTIFICACIÓ

Es reconeixen els següents sistemes d'identificació de tercers en la seua relació amb l'Ajuntament de Paiporta en l'àmbit de la present política.

8.1. MITJANÇANT CERTIFICAT DE SIGNATURA ELECTRÒNICA

A fi de comparèixer davant la Seu i relacionar-se amb la plataforma s'admet la identificació basada en els següents tipus de certificats:

- Certificat de persona física, inclòs el de personal empleat públic.
- Certificat de representant.
- Certificat jurídic.

Únicament es reconeixeran certificats electrònics qualificats de signatura electrònica expedits per prestadors inclosos en la ''Llista de confiança de prestadors de serveis de certificació'', accessible en el moment d'aprovació de la present política a través de la següent adreça: https://sedeaplicaciones.minetur.gob.es/prestadores/

8.2. MITJANÇANT "CL@VE PIN" Y "CL@VE PERMANENT"

S'admet la identificació de les persones físiques mitjançant el sistema Cl@ve, en les seues modalitats de "Cl@ve PIN" i "Cl@ve permanent", per a la realització de qualsevol tràmit.

Cl@ve és un sistema orientat a unificar i simplificar l'accés electrònic dels ciutadans i ciutadanes als serveis públics. El seu objectiu principal és que la ciutadania puga identificar-se davant l'Administració mitjançant claus concertades (usuari més contrasenya), sense haver de recordar claus diferents per a accedir als diferents serveis.

El sistema Cl@ve va ser aprovat per acord del Consell de Ministres, en la seua reunió del 19 de setembre de 2014, i les seues condicions d'utilització són determinades per la Direcció de Tecnologies de la Informació i les Comunicacions.

Més informació, accessible en el moment d'aprovació de la present política, a través de la següent adreça: https://clave.gob.es/

8.3. MITJANÇANT CERTIFICATS DE SEGELL ELECTRÒNIC

A l'hora de la integrar aplicacions de tercers amb la plataforma d'administració electrònica i garantir la seua identificació s'admetran exclusivament certificats electrònics qualificats de segell electrònic expedits per prestadors inclosos en la ''Llista de confiança de prestadors de serveis de certificació''.

No s'admetran certificats de segell a l'efecte de compareixença de la persona titular del mateix en la Seu electrònica (accés a notificacions electròniques, accés a la carpeta ciutadana per a consultar estat de tramitació, compareixença en el tràmit, etc.) ni per a la presentació de sol·licituds o la realització de qualsevol altre tràmit administratiu.

9. GESTIÓ DE LA POLÍTICA DE SIGNATURES

El manteniment, actualització i publicació electrònica del present document correspondrà a l'àrea d'Innovació de l'Ajuntament de Paiporta.

L'àrea d'Innovació de l'Ajuntament de Paiporta mantindrà, en els portals destinats a tal funció, tant la versió actualitzada del present document com un repositori amb l'historial de les versions anteriors de la política de signatura electrònica per a l'organisme.

En el cas d'actualització del present document, s'identificarà el lloc on un validador pot trobar les versions anteriors per a verificar una signatura electrònica anterior a la política vigent.

En el moment de la signatura s'inclourà la referència de l'identificador únic de la versió del present document de política de signatura electrònica sobre el qual s'ha basat, el qual determina les condicions que ha de complir la signatura electrònica en un moment determinat. El camp destinat per a incloure aquesta referència serà, en els formats de signatura avançada (XAdES, CAdES i AdES), el camp SignaturePolicyIdentifier.

9.1. ARXIU I CUSTÒDIA

Les transmissions de dades signades s'emmagatzemaran el temps que resulte imprescindible per a l'acreditació de la seua validesa a llarg termini.

El contingut signat, per a garantir la fiabilitat d'una signatura electrònica i que aquesta tinga efectes jurídics enfront de tercers al llarg del temps, haurà de ser complementada amb la informació de l'estat del certificat associat en el moment en què la mateixa es va produir, així com els certificats que conformen la cadena de confiança incorporant segells de temps per als elements afegits. Tota aquesta informació s'emmagatzemarà en el repositori de no repudi.

En aquest repositori, s'emmagatzemaran totes les signatures del contingut, tant les realitzades amb certificat de persona física o jurídica com amb segell d'òrgan o equivalent, ja hagen sigut realitzades internament en l'àmbit de les aplicacions de l'organisme (s'emmagatzemaran en el moment de la seua creació) com en l'exterior (s'emmagatzemaran en el moment de la seua validació).

En qualsevol dels casos, s'emmagatzemarà com a mínim la signatura i un segell de temps.

En el repositori de no repudi s'emmagatzemarà, com a mínim, la signatura amb segell de temps (formats XAdEST/CAdES-T/PAdES-EPES amb atribut signature-estafe-stamp). Si es necessitara conservació a llarg termini de la signatura, s'emmagatzemarà en format XAdES-A/CAdES-A/PAdES-LTV que assegura la totalitat del document i les signatures contingudes.

Es procedirà al resegellat de les signatures quan així calga o qualssevol altres mesures tècniques necessàries.

9.2. CONSERVACIÓ A LLARG TERMINI

Per a protegir la signatura electrònica enfront de la possible obsolescència dels algorismes i poder continuar assegurant les seues característiques de validesa, s'emmagatzemaran en un depòsit segur, que garantirà la seua protecció contra falsificacions i assegurarà la data exacta

en què es van guardar. Les operacions de datat es garanteixen mitjançant el repositori de no repudi.

Per a garantir la conservació a llarg termini s'utilitzaran mecanismes de segellament i resegellat de temps. Les signatures guardades en el repositori de no repudi han de ser segellades.

Els casos en els quals es necessitarà realitzar un resegellat de les signatures segellades i emmagatzemades en el repositori de no repudi, seran els que segueixen:

- Quan algun dels algorismes utilitzats en un segell de temps usat per a segellar una signatura haja sigut declarat obsolet. El resegellat, en aqueix cas, el realitzarà una autoritat de segellament que use algorismes actuals, segurs i adaptats a aquesta situació.
- Quan el certificat de l'autoritat de segellament que ha sigut usat per a segellar una signatura haja sigut revocat, caducat o estiga pròxim a caducar. En aquest cas s'utilitzarà una autoritat de segellament el certificat del qual siga vàlid i tinga un període de validesa adequat.

10. AUTENTICITAT DELS DOCUMENTS

L'autenticitat de les signatures electròniques i documents produïts en l'àmbit d'aquesta política s'acreditarà i verificarà en les següents condicions.

10.1. CODI SEGUR DE VERIFICACIÓ (CSV)

El codi segur de verificació d'un document identifica biunívocament a un document i un conjunt de signatures i/o segells electrònics.

Consta de fins a 20 dígits alfanumèrics, i el seu coneixement permet l'accés a un document PDF segellat electrònicament pel certificat de segell d'aquesta Seu per a garantir l'autenticitat i interoperabilitat. En ell s'inclou el document íntegre originalment signat i la corresponent informació de les signatures.

El PDF segellat serà conforme l'especificació tècnica ETSI TS 102 778-3 versió 1.2.1 i ETSI TS 102 778-4.

El CSV proporcionarà accés a la següent informació:

- Document CSV.
- Document original.
- Signatures electròniques en format XAdES.
- Una altra informació relativa al document signat (identificació de les persones signants, data i hora de les signatures, títol del document, etc.).

10.2. PROCEDIMIENT DE VERIFICACIÓ DELS DOCUMENTS AMB CSV GENERATS PER LA PLATAFORMA

Es garantirà que qualsevol, empleat o empleada públic d'aquesta administració o tercera part independent, tinga la capacitat de comprovar d'una banda la validesa, autenticitat i integritat dels documents amb CSV generats en l'àmbit d'aquesta política i, per un altre, la validesa, autenticitat i integritat de la informació i signatures associades a aquests.

Per a realitzar la verificació s'hauran d'utilitzar mitjans o dispositius informàtics en condicions segures (no compromesos o lliures de programari maliciós).

Quan s'accedisca mitjançant un navegador web a l'adreça de la Seu electrònica, lloc on es podran verificar els documents CSV, s'haurà de comprovar que no mostra cap alerta sobre la validesa del certificat SSL.

A continuació, es detallen els diferents procediments de verificació.

10.2.1. VERIFICACIÓ DE DOCUMENTS AMB CSV LLIURATS EN PAPER

Una vegada s'estiga en possessió del document en paper amb CSV se seguiran els següents passos per a la seua verificació:

1. Accedir mitjançant un navegador web a l'adreça de verificació de CSV de la Seu electrònica (així mateix reflectida en el propi document): https://paiporta.sedipualba.es/csv/

2. Introduir el codi CSV imprès en el marge del document.

3. Comprovar que la Seu electrònica indica que existeix un document amb aqueix CSV i que en descarregar-lo coincideix amb el document imprès (han de ser idèntics).

6.1.1 VERIFICACIÓ DE DOCUMENTS AMB CSV LLIURATS EN FORMAT ELECTRÒNIC (PDF)

Una vegada s'estiga en possessió del document electrònic amb CSV se seguiran els següents passos per a la seua verificació:

1. Validar les signatures del document CSV mitjançant l'aplicació Valide de l'Administració General de l'Estat o mitjançant un programa lector de documents PDF amb la capacitat de verificar signatures electròniques en format PAdES LTA-level:

    1.1 Si el CSV consta de 20 dígits: comprovar que l'aplicació acredita que la signatura és vàlida i que el document està signat mitjançant un certificat de segell electrònic inclòs en el llistat al qual es fa referència en l'apartat 7 de la present política.

Si la signatura conté segellat de temps, aquest també ha de presentar-se com a vàlid (PAdES LTA-level).

1.2 Si el CSV consta de menys de 20 dígits: comprovar que l'aplicació acredita que les signatures són vàlides. Si la signatura conté segellat de temps, aquest també ha de presentar-se com a vàlid.

2. Addicionalment, comprovar que el document CSV existeix en la Seu electrònica:

2.1 Accedir mitjançant un navegador web a l'adreça de verificació de CSV de la Seu electrònica (així mateix reflectida en el propi document): https://paiporta.sedipualba.es/csv/

2.2 Introduir el codi CSV imprès en el marge del document.

2.3 Comprovar que la Seu electrònica indica que existeix un document amb aqueix CSV i que en descarregar-lo coincideix amb el document electrònic (han de ser idèntics).

10.2.2. VERIFICACIÓ DE DOCUMENTS DE FIRMA ELECTRÒNICA XAdES

Els documents de signatura XAdES produïts en l'àmbit d'aquesta política estaran associats als seus corresponents documents originals o als seus corresponents documents CSV.

L'autenticitat i validesa de les signatures electròniques XAdES s'acreditarà i verificarà seguint el següent procediment:

1. Recaptar la següent informació:

- Document original.
- Fitxer de signatura electrònica en format XAdES-A.
- Títol del document.
- Informació de la persona signant.
- Codi aleatori (salt o sal) amb la qual es va generar la empremta signada en el document XAdES-A.

2. Validar el fitxer de signatura electrònica mitjançant l'aplicació Valide de l'Administració General de l'Estat. Al ser un format estàndard, es poden usar altres eines amb capacitat de validació de signatures.

3. Comprovar que la signatura validada en el punt anterior es correspon amb el document signat:

3.1 Calcular el hash SHA3-512 sobre el resultat de concatenar el document binari original + el títol del document codificat en UTF-8 + la informació del signant codificada en UTF-8 + la "sal".

3.2 Obrir el fitxer XAdES-A i comprovar que l'element en la ruta XPath /ds:Signature/ds:Object/documents_signats conté un element documente_signat amb el hash calculat anteriorment i la "sal" utilitzada (tots dos codificats en Base64).

3.3 Comprovar que el XPath anterior es troba inclòs en alguna de les referències de l'element SignedDataObjectProperties, i per tant signat.

En cas que totes les comprovacions anteriors hagen resultat satisfactòries, quedaria provat que el document original es correspon amb la signatura XAdES-A, la qual garanteix la integritat del document, la seua autenticitat i el no repudi.

Atès que la validació de la signatura XAdES resulta un procediment complex, es publicarà una eina que de forma automàtica permeta verificar la seua correspondència amb el document original signat.

Addicionalment, el codi font d'aquesta eina es publicarà sense restriccions d'accés en un repositori a aquest efecte. D'aquesta manera els tercers que disposen dels mitjans i coneixements tecnològics precisos podran generar l'eina que els permeta verificar de forma autònoma i independent la validesa dels documents produïts en l'àmbit d'aquesta política.

11. POLÍTICA DE SIGNATURA DE L'ADMINISTRACIÓ GENERAL DE L'ESTATAT

Es consideraran vàlids, i per tant s'admetran, tots aquells mecanismes d'identificació i signatura reconeguts en la política de signatura electrònica i de certificats de l'Administració General de l'Estat, així com tots aquells documents produïts o resultants d'aquests.

12. ROLS I RESPONSABILITATS

ROL	DESCRIPCIÓ
Responsable de seguretat	a) Col·laborar amb el gestor de la política de signatura en l'especificació en el manteniment i actualització del present document.
Responsable del sistema	b) Col·laborar amb el gestor de la política de signatura en el manteniment, actualització i publicació electrònica del present document

NOR08 – Política de firma electrónica y de certificados

Clasificación de la Información:

Nivel del Documento	Procedimiento
Nombre del Fichero	NOR08 – Politica de firma electronica.docx
Tipo	Publico
Ámbito de Difusión	Comité de Seguridad del AYUNTAMIENTO DE PAIPORTA
Responsable	Responsable de Seguridad del AYUNTAMIENTO DE PAIPORTA

CONTROL DE MODIFICACIONES		
Descripción	**Versión**	**Fecha**
Primera aprobación por la Junta de Gobierno Local.	1.0	18/02/2022
Publicación en el BOP nº 55	1.0	21/03/2022

ÍNDICE DE CONTENIDO

1. OBJETO

El presente documento tiene por objeto la definición de los distintos mecanismos de identificación y firma admitidos en la sede electrónica y resto de subsistemas de la plataforma de administración electrónica SEDIPUALBA que utiliza el Ayuntamiento de Paiporta bajo convenio con la Diputación de Albacete. Esta plataforma integra los sistemas de gestión de expedientes y de archivo electrónico corporativo. De este modo se pretende establecer el esquema de referencia de la Organización para la identificación, la autenticación y el reconocimiento de firmas electrónicas basadas en certificados, recogidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Los objetivos perseguidos con el uso de certificados de firma electrónica son los siguientes:

- En la firma de documentos y contenidos electrónicos, garantizar la autenticidad, la integridad y el no repudio de los mismos.
- En la firma electrónica de transmisión de datos, garantizar la autenticación de los actores involucrados, así como la integridad del contenido del mensaje de datos y el no repudio de los mensajes en una comunicación telemática.

Los certificados electrónicos de firma electrónica podrán ser utilizados, asimismo, por parte de los ciudadanos y empleados públicos de la Organización, como medio de autenticación de la identidad, como medio de firma electrónica de documentos y de certificación de la integridad de un documento.

Por otra parte, en el presente documento se concretan los procedimientos a seguir por la Organización para la generación, validación y conservación de firmas electrónicas, así como las características y requisitos exigibles a los sistemas de firma electrónica, los certificados, los servicios de sellado de tiempo, y otros elementos de soporte de las firmas de la Organización.

La presente política, de primer nivel normativo, proporciona respuesta a lo dispuesto por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS) y, más en concreto, a las previsiones que siguen:

- Artículo 33. Firma electrónica.
- Marco organizativo. Procedimientos de seguridad [org.3].
- Medidas de protección de la información. Firma electrónica[mp.info.4].

2. ALCANCE

El ámbito de aplicación de la presente política será el de las firmas electrónicas realizadas por la Organización afectando a:

- Las relaciones de los ciudadanos con la Organización.
- Las relaciones de la Organización con otras Administraciones.

3. NORMATIVA Y ESTÁNDARES DE APLICACIÓN

A continuación, se relaciona la normativa legal y los estándares, que se han tenido en consideración para la elaboración de la presente norma.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
- Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración.
- NOR-01: Política de seguridad de la información.
- NOR-02: Normativa general de la seguridad de la información.
- Guía de Seguridad de las TIC. CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad.

4. GLOSARIO

TÉRMINO	DESCRIPCIÓN
Firma electrónica	Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
Política de firma electrónica	Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan las firmas electrónicas, incluyendo las características exigibles a los certificados de firma.
Firmante	Persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

Verificador	Entidad, ya sea persona física o jurídica, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por la política de firma concreta por la que se rige la plataforma de relación electrónica o el servicio concreto al que se esté invocando. Podrá ser una entidad de validación de confianza o una tercera parte que esté interesada en la validez de una firma electrónica.
Prestador de servicios de certificación (PSC)	Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.
Emisor y gestor de la política de firma	Entidad que se encarga de generar y gestionar el documento de política de firma, por el cual se deben regir el firmante, el verificador y los prestadores de servicios en los procesos de generación y validación de firma electrónica.

5. DATOS IDENTIFICATIVOS Y VALIDEZ DE LA POLÍTICA

El presente documento de política de firma electrónica y de certificados tendrá un identificador único, asignándose los dos últimos dígitos a la versión que corresponda, al objeto de distinguir las versiones sucesivas que puedan existir cuando se realicen actualizaciones.

La presente política de firma electrónica y de certificados será válida desde la fecha de emisión indicada hasta que sea derogada o se publique una nueva versión. Los períodos de transición serán indicados en las nuevas versiones y, una vez transcurridos los plazos indicados, serán válidas únicamente las versiones actualizadas.

Además, en el caso de actualización de la presente política de firma electrónica y de certificados, se identificará el enlace URL donde encontrar las versiones anteriores para verificar una firma electrónica anterior a la política vigente.

	IDENTIFICADOR DE LA POLÍTICA
Nombre del documento	Política de Firma Electrónica y de Certificados del Ayuntamiento de Paiporta.
Versión	1.0
Identificación del documento	OID 2.16.724.1.3.1.1.2.1.0
URL de referencia	https://paiporta.sedipualba.es/
Fecha de emisión	18/02/2022
Ámbito de aplicación	Ayuntamiento de Paiporta

Al gestor de la presente política de firma electrónica y de certificados corresponde el mantenimiento, actualización y publicación electrónica de los criterios sobre firma electrónica.

	IDENTIFICADOR DEL GESTOR
Nombre del gestor de la Política	Área de Innovación del Ayuntamiento de Paiporta
Dirección de contacto	C/ Mestre Músic Vicent Prats i Tarazona, s/n Paiporta (Valencia, España) 46200

6. REGLAS COMUNES

Las reglas comunes establecen las responsabilidades respecto a la firma electrónica sobre la persona o entidad que crea la firma y la persona o entidad que la verifica, definiendo los requisitos mínimos que deben presentarse, debiendo estar firmados si son requisitos para el firmante, o no firmados si son requisitos para el verificador.

Estas reglas se definen de acuerdo con los formatos de firma electrónica admitidos, teniendo en cuenta los diferentes usos de la firma electrónica basada en certificados, el uso de algoritmos y los procesos de creación y validación de firma.

6.1. REGLAS DEL FIRMANTE

El firmante será responsable de que el fichero que se quiere firmar no incorpora contenido dinámico que pudiese modificar el resultado de la firma durante el tiempo. Si el fichero que se quiere firmar no ha sido creado por el firmante, se asegurará que no existe contenido dinámico dentro del fichero, como pueden ser macros.

El firmante deberá proporcionar, como mínimo, la información contenida en las siguientes etiquetas dentro del campo (SignedProperties) que contiene las propiedades conjuntamente firmadas a la hora de la generación de la firma XMLDsig de carácter obligatorio, a saber:

- SigningTime: indica la fecha y la hora. En el caso de firma en cliente sin acceder a servidor, será meramente indicativa (pues la fecha en el dispositivo cliente es fácilmente manipulable) y/o será utilizada con fines distintos a conocer la fecha y hora de firma. Las políticas particulares de firma electrónica podrán determinar características y restricciones particulares respecto a generación en cliente de las referencias temporales y sincronización del reloj.
- SigningCertificate: contiene referencias a los certificados y algoritmos de seguridad utilizados para cada certificado. Este elemento deberá ser firmado con objeto de evitar la posibilidad de sustitución del certificado.
- SignaturePolicyIdentifier: identifica la política de firma sobre la que se basa el proceso de generación de firma electrónica, y debe incluir los siguientes contenidos en los elementos en que se subdivide como sigue.

- Una referencia explícita al presente documento de política de firma en el elemento xades:SigPolicyId. Para ello, aparecerá el OID que identifique la versión concreta de la política de firma o la URL de su localización. <xades:SigPolicyId> <xades:Identifier> ... </xades:Identifier>
- La huella digital del documento de política de firma correspondiente y el algoritmo utilizado, en el elemento <xades:SigPolicyHash>, de manera que el verificador pueda comprobar, calculando a su vez este valor, que la firma está generada según la misma política de firma que se utilizara para su validación.

- DataObjectFormat: define el formato del documento original, y es necesario para que el receptor conozca la forma de visualizar el documento.

Las etiquetas restantes que pueden agregarse en el campo SignedProperties serán consideradas de carácter opcional, sin perjuicio de su consideración obligatoria en políticas particulares, siempre basadas en la política marco:

- SignatureProductionPlace: define el lugar geográfico donde se ha realizado la firma del documento.
- SignerRole: define el rol de la persona en la firma electrónica. Al menos uno de estos elementos ClaimedRoles o CertifiedRoles deben estar presentes en este campo: ○ "supplier" o "emisor": cuando la firma la realiza el emisor.
    - "customer" o "receptor": cuando la firma la realiza el receptor.
    - "third party" o "tercero": cuando la firma la realiza una persona o entidad distinta al emisor o al receptor.
- CommitmentTypeIndication: define la acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, ...)
- AllDataObjectsTimeStamp: contiene un sello de tiempo, calculado antes de la generación de la firma, sobre todos los elementos contenidos en ds:Reference.
- IndividualDataObjectsTimeStamp: contiene un sello de tiempo, calculado antes de la generación de la firma, sobre algunos de los elementos contenidos en ds:Reference.

6.2. REGLAS DEL VERIFICADOR

El encargado de la verificación de la firma será responsable de definir los procesos de validación y de archivado, de conformidad con los requisitos de la política de firma particular a la que se ajusta el servicio y con lo establecido en la NTI de Política de gestión de documentos electrónicos.

El formato básico de firma electrónica avanzada no incluye ninguna información de validación más allá del certificado firmante, que está incluido en la etiqueta Signing Certificate, y de la política de firma que se indique en la etiqueta Signature Policy.

Los atributos que podrá utilizar el verificador para comprobar que se cumplen los requisitos de la política de firma, según la cual se ha generado la firma, independientemente del formato utilizado (XAdES, CAdES o PAdES), son las siguientes:

- Signing Time: sólo se utilizará en la verificación de las firmas electrónicas como indicación para comprobar el estado de los certificados en la fecha señalada, ya que únicamente se puede asegurar las referencias temporales mediante un sello de tiempo (especialmente en el caso de firmas en dispositivos cliente). Si se ha realizado el sellado de tiempo, el sello más antiguo dentro de la estructura de la firma se utilizará para determinar la fecha de la firma.
- Signing Certificate: se utilizará para comprobar y verificar el estado del certificado (y, en su caso, la cadena de certificación) en la fecha de la generación de la firma, en el caso que el certificado no haya caducado y se pueda acceder a los datos de verificación (CRL, OCSP, etc) o bien en el caso de que el prestador de servicios de certificación (PSC) ofrezca un servicio de validación histórico del estado del certificado.
- Signature Policy: se deberá comprobar, que la política de firma que se ha utilizado para la generación de la firma se corresponde con la que se debe utilizar para un servicio en cuestión.

Existe un tiempo de espera, conocido como periodo de precaución o periodo de gracia, para comprobar el estado de revocación de un certificado.

El encargado de la verificación podrá esperar este plazo para validar la firma o realizarla en el mismo momento y revalidarla después. El periodo desde que se realiza la firma o el sellado de tiempo deberá, como mínimo, el tiempo máximo permitido para el refresco completo de las CRLs o el tiempo máximo de actualización del estado del certificado en el servicio OCSP. Estos plazos podrán variar en función del Prestador de Servicios de Certificación.

7. REGLAS DE CONFIANZA

7.1. REGLAS DE CONFIANZA DE CERTIFICADOS ELECTRÓNICOS

Para ejecutar la firma electrónica de contenido se consideraran válidos aquellos certificados reconocidos de conformidad con la Ley 59/2003, de 19 de diciembre, y con la Directiva 1999/93/CE de 13 de diciembre de 1999, así como las nuevas tipologías de certificados definidos en la Ley 11/2007, de 22 de junio y los sistemas de firma y certificados electrónicos de acuerdo con el artículo 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En consecuencia, con lo anterior, los certificados admitidos son los que siguen:

a) Sistemas de firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos reconocidos o cualificados de firma electrónica expedidos por prestadores incluidos en la “Lista de confianza de prestadores cualificados de servicios electrónicos de confianza”[1].

[1] https://sede.serviciosmin.gob.es/prestadores/paginas/inicio.aspx

Sistemas de sello electrónico reconocido o cualificado y de sello electrónico avanzado basados en certificados electrónicos reconocidos o cualificados de sello electrónico incluidos en la «"Lista de confianza de prestadores cualificados de servicios electrónicos de confianza".

b) Otros sistemas que la Organización pueda considerar válido para realizar determinados trámites o procedimientos de su ámbito de competencia, en los términos y condiciones que se establezcan.

Los certificados de firma electrónica de empleado público emitidos por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM) se consideran válidos para la realización de firma electrónica por parte de los empleados de la Organización y, en consecuencia, garantizan la identificación y firma de los participantes en la tramitación de cuantos procedimientos electrónicos se determinen.

La relación de sellos electrónicos utilizados por el Ayuntamiento de Paiporta, indicando las características de los certificados electrónicos y los prestadores que los expiden será pública y accesible a través de su sede electrónica. Adicionalmente, la verificación de los sellos y certificados electrónicos, incluyendo el de la propia sede, se podrá efectuar a través de la "Aplicación de VALIdación de firma y certificados Online y Demostrador de servicios de @firma"[2] u otros sistemas reconocidos de validación electrónica.

7.2. REGLAS DE CONFIANZA PARA LOS SELLOS DE TIEMPO

El sello electrónico de tiempo asegura que tanto los datos originales del documento que va a ser sellado como la información del estado de los certificados, en caso de que se hayan incluido en la firma electrónica, se generaron antes de una determinada fecha. El formato del sello de tiempo deberá cumplir las recomendaciones de IETF, RFC 5816, "Internet X.509 Public Key Infrastructure; Time-Stamp Protocol (TSP)". Los elementos básicos que componen un sello digital de tiempo son:

- Datos sobre la identidad de la autoridad emisora (identidad jurídica, clave pública a utilizar en la verificación del sello, número de bits de la clave, el algoritmo de firma digital y la función hash utilizados).
- Tipo de solicitud cursada (si es un valor hash o un documento, cuál es su valor y datos de referencia).
- Parámetros del secuenciador (valores hash "anterior", "actual" y "siguiente").
- Fecha y hora UTC.
- Firma digital de todo lo anterior con la clave pública y esquema de firma digital especificados.

El sellado de tiempo puede ser añadido por el emisor, el receptor o un tercero y se debe incluir como propiedad no firmada en el campo Signature Time Stamp. El sellado de tiempo debe

[2] https://valide.redsara.es/valide/inicio.html

realizarse en un momento próximo a la fecha incluida en el campo Signing Time y, en cualquier caso, siempre antes de la caducidad del certificado del firmante. La presente política admite sellos de tiempo expedidos por prestadores de servicios de sellado de tiempo que cumplan las especificaciones técnicas ETSI TS 102 023, "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities".

7.3. REGLAS DE CONFIANZA PARA FIRMAS LONGEVAS

Los estándares XAdES (ETSI TS 101 903) en sus diferentes versiones contemplan la posibilidad de incorporar a las firmas electrónicas información adicional para garantizar la validez de una firma a largo plazo, una vez vencido el periodo de validez del certificado. La información podrá ser incluida por el firmante o por el verificador, y deberá hacerse transcurrido el periodo de precaución o de gracia.

Existen dos tipos de datos a incluir como información adicional de validación:

- la información del estado del certificado en el momento en que se produce la validación de la firma o una referencia a los mismos.
- los certificados que conforman la cadena de confianza.

En el caso de que se deseen generar firmas longevas, se deberá incluir la información de validación anterior, y añadirle un sello de tiempo. En estos tipos de firma la validez de la firma resultante viene determinada por la duración del sello de tiempo que se añade a la firma longeva. En el caso que se desee incorporar a la firma la información de validación, se deberá usar validación mediante OCSP (Online Certificate Status Protocol), ya que mediante este método las propiedades o atributos a incluir son de menor tamaño.

Si la consulta al estado de validación de la firma generara un elevado volumen de información, alternativamente a la información de validación indicada anteriormente, se podrá incluir en la firma longeva referencias a dicha información. Dentro del formato de firma XAdES, el formato extendido XAdES-C incorpora estas entre otras propiedades no firmadas:

- CompleteCertificateRefs, que contiene referencias a todos los certificados de la cadena de confianza necesaria para verificar la firma, excepto el certificado firmante.
- CompleteRevocationRefs, que contiene referencias a las CRLs y/o respuestas OCSP usadas en la verificación de los certificados.

En el caso que se desee incorporar a la firma la información de validación, se utilizará el formato XAdES-X, que añade un sello de tiempo a la información anterior. El formato XAdES-XL además de la información incluida en XAdES-X, incluye dos nuevas propiedades no firmadas:

- CertificateValues
- RevocationValues

Estas propiedades incluyen, adicionalmente a las referencias a la información de validación, la cadena de confianza completa y la CRL o respuesta OCSP obtenida en la validación. Para los atributos CertificateValues y Revocation-Values se recomienda hacer la validación por OCSP, ya que estos valores pueden ser muy voluminosos en caso de realizar la validación mediante CRL.

En el caso que se desee incorporar a la firma esta información de validación, se recomienda usar el formato XADES-A, que añade un sello de tiempo a la información anterior.

7.4. FIRMA BIOMÉTRICA

La firma biométrica se considerará, a todos los efectos, equivalente a la firma manuscrita y se realizará en presencia de un empleado público que garantizará la identidad del firmante.

Se seguirá el siguiente procedimiento:

1. El empleado público solicita el DNI al firmante y comprueba que sus datos identificativos se corresponden con los que constan en el sistema.

2. El sistema compone el documento de firma combinado:

   2.1. Se eliminan los espacios en blanco, obteniendo su forma canónica según el procedimiento estándar del W3C (https://www.w3.org/TR/xmlc14n11/).

   2.2. Se calcula el hash SHA3-512.

3. Se informa al firmante acerca de los datos a firmar:

   3.1. Por un lado, se muestran en la pantalla del dispositivo de firma tanto el hash calculado como la fecha y hora del PC al que está conectado.

   3.2. Por otro lado, ese mismo hash y la correspondiente relación de documentos PDF a firmar se pondrán a disposición del firmante a través de una pantalla de visualización, para su cotejo, antes de solicitarle que firme.

4. El firmante realiza la firma.

5. El empleado público comprueba que la firma trazada corresponde con la firma que consta en el DNI y la acepta.

6. El sistema almacena el fichero de firma generado por el dispositivo y el dibujo de la firma.

7. El sistema sella electrónicamente el documento XML correspondiente a la firma biométrica, con el siguiente formato, que contiene el hash mostrado en la pantalla del dispositivo antes de

firmar y el contenido del fichero de firma generado, así como los datos personales del firmante y los datos personales del empleado que recoge la firma.

Por motivos de seguridad de la información y protección de los datos de carácter personal, ni la firma biométrica ni el sello de tiempo serán accesibles públicamente mediante el CSV. Sí lo será el trazo de la firma, al igual que sería visible la rúbrica de la firma manuscrita en un documento en papel.

Los administradores de la sede podrán acceder a la información de forma completa en caso de que fuera necesario.

7.5. FIRMA CON PSEUDÓNIMO (OCULTA)

La firma con pseudónimo (u oculta) en el ámbito de la presente política consiste en una firma electrónica o biométrica cuyos datos no están disponibles públicamente al verificar el correspondiente CSV. Entre estos datos se encuentran la firma propiamente dicha y los datos identificativos del firmante (NIF, nombre y apellidos).

Únicamente los administradores de la sede pueden obtener todos los datos relativos a esta firma, en caso de ser necesario. El resto de personas únicamente podrán visualizar el pseudónimo utilizado en la firma.

8. IDENTIFICACIÓN

Se reconocen los siguientes sistemas de identificación de terceros en su relación con el Ayuntamiento de Paiporta en el ámbito de la presente política.

8.1. MEDIANTE CERTIFICADO DE FIRMA ELECTRÓNICA

Al objeto de comparecer ante la sede y relacionarse con la plataforma se admite la identificación basada en los siguientes tipos de certificados:

- Certificado de persona física, incluido el de empleado público.
- Certificado de representante.
- Certificado jurídico.

Únicamente se reconocerán certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’, accesible en el momento de aprobación de la presente política a través de la siguiente dirección: https://sedeaplicaciones.minetur.gob.es/Prestadores/

8.2. MEDIANTE “CL@VE PIN” Y “CL@VE PERMANENTE”

Se admite la identificación de las personas físicas mediante el sistema Cl@ve, en sus modalidades de “Cl@ve PIN” y “Cl@ve permanente”, para la realización de cualquier trámite.

Cl@ve es un sistema orientado a unificar y simplificar el acceso electrónico de los ciudadanos a los servicios públicos. Su objetivo principal es que el ciudadano pueda identificarse ante la Administración mediante claves concertadas (usuario más contraseña), sin tener que recordar claves diferentes para acceder a los distintos servicios.

El sistema Cl@ve fue aprobado por Acuerdo del Consejo de Ministros, en su reunión del 19 de septiembre de 2014, y sus condiciones de utilización son determinadas por la Dirección de Tecnologías de la Información y las Comunicaciones.

Más información, accesible en el momento de aprobación de la presente política, a través de la siguiente dirección: https://clave.gob.es/

8.3. MEDIANTE CERTIFICADOS DE SELLO ELECTRÓNICO

A la hora de la integrar aplicaciones de terceros con la plataforma de administración electrónica y garantizar su identificación se admitirán exclusivamente certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.

No se admitirán certificados de sello a efectos de comparecencia del titular del mismo en la sede electrónica (acceso a notificaciones electrónicas, acceso a la carpeta ciudadana para consultar estado de tramitación, comparecencia en el trámite, etc.) ni para la presentación de solicitudes o la realización de cualquier otro trámite administrativo.

9. GESTIÓN DE LA POLÍTICA DE FIRMAS

El mantenimiento, actualización y publicación electrónica del presente documento corresponderá al Área de Innovación del Ayuntamiento de Paiporta.

El Área de Innovación del Ayuntamiento de Paiporta mantendrá, en los portales destinados a tal función, tanto la versión actualizada del presente documento como un repositorio con el historial de las versiones anteriores de la política de firma electrónica para el organismo.

En el caso de actualización del presente documento, se identificará el lugar donde un validador puede encontrar las versiones anteriores para verificar una firma electrónica anterior a la política vigente.

En el momento de la firma se incluirá la referencia del identificador único de la versión del presente documento de política de firma electrónica sobre el que se ha basado, el cual determina las condiciones que debe cumplir la firma electrónica en un momento determinado. El campo destinado para incluir esta referencia será, en los formatos de firma avanzada (XAdES, CAdES y PAdES), el campo SignaturePolicyIdentifier.

9.1. ARCHIVO Y CUSTODIA

Las transmisiones de datos firmadas se almacenarán el tiempo que resulte imprescindible para la acreditación de su validez a largo plazo.

El contenido firmado, para garantizar la fiabilidad de una firma electrónica y que ésta tenga efectos jurídicos frente a terceros a lo largo del tiempo, deberá ser complementada con la información del estado del certificado asociado en el momento en que la misma se produjo, así como los certificados que conforman la cadena de confianza incorporando sellos de tiempo para los elementos añadidos. Toda esta información se almacenará en el repositorio de no repudio.

En dicho repositorio, se almacenarán todas las firmas del contenido, tanto las realizadas con certificado de persona física o jurídica como con sello de órgano o equivalente, ya hayan sido realizadas internamente en el ámbito de las aplicaciones del organismo (se almacenarán en el momento de su creación) como en el exterior (se almacenarán en el momento de su validación).

En cualquiera de los casos, se almacenará como mínimo la firma y un sello de tiempo.

En el repositorio de no repudio se almacenará, como mínimo, la firma con sello de tiempo (formatos XAdEST/CAdES-T/PAdES-EPES con atributo signature-time-stamp). Si se necesitara conservación a largo plazo de la firma, se almacenará en formato XAdES-A/CAdES-A/PAdES-LTV que asegura la totalidad del documento y las firmas contenidas.

Se procederá al resellado de las firmas cuando así sea preciso o cualesquiera otras medidas técnicas necesarias.

9.2. CONSERVACIÓN A LARGO PLAZO

Para proteger la firma electrónica frente a la posible obsolescencia de los algoritmos y poder seguir asegurando sus características de validez, se almacenarán en un depósito seguro, garantizando su protección contra falsificaciones y asegurando la fecha exacta en que se guardaron. Las operaciones de fechado se garantizan mediante el repositorio de no repudio.

Para garantizar la conservación a largo plazo se utilizarán mecanismos de sellado y resellado de tiempo. Las firmas guardadas en el repositorio de no repudio deben ser selladas.

Los casos en los que se necesitará realizar un resellado de las firmas selladas y almacenadas en el repositorio de no repudio, serán los que siguen:

- Cuando alguno de los algoritmos utilizados en un sello de tiempo usado para sellar una firma haya sido declarado obsoleto. El resellado, en ese caso, lo realizará una autoridad de sellado que use algoritmos actuales, seguros y adaptados a esta situación.
- Cuando el certificado de la autoridad de sellado que ha sido usado para sellar una firma haya sido revocado, caducado o esté próximo a caducar. En este caso se utilizará una autoridad de sellado cuyo certificado sea válido y tenga un periodo de validez adecuado.

10. AUTENTICIDAD DE LOS DOCUMENTOS

La autenticidad de las firmas electrónicas y documentos producidos en el ámbito de esta política se acreditará y verificará en las siguientes condiciones.

10.1. CÓDIGO SEGURO DE VERIFICACIÓN (CSV)

El código seguro de verificación de un documento identifica biunívocamente a un documento y un conjunto de firmas y/o sellos electrónicos.

Consta de hasta 20 dígitos alfanuméricos, y su conocimiento permite el acceso a un documento PDF sellado electrónicamente por el certificado de sello de esta sede para garantizar la autenticidad e interoperabilidad. En él se incluye el documento íntegro originalmente firmado y la correspondiente información de las firmas.

El PDF sellado será conforme la especificación técnica ETSI TS 102 778-3 versión 1.2.1 y ETSI TS 102 778-4.

El CSV proporcionará acceso a la siguiente información:

- Documento CSV.
- Documento original.
- Firmas electrónicas en formato XAdES.
- Otra información relativa al documento firmado (identificación de los firmantes, fecha y hora de las firmas, título del documento, etc.).

10.2. PROCEDIMIENTO DE VERIFICACIÓN DE LOS DOCUMENTO CON CSV GENERADOS POR LA PLATAFORMA

Se garantizará que cualquiera, empleado público de esta administración o tercera parte independiente, tenga la capacidad de comprobar por un lado la validez, autenticidad e integridad de los documentos con CSV generados en el ámbito de esta política y, por otro, la validez, autenticidad e integridad de la información y firmas asociadas a éstos.

Para realizar la verificación se deberán utilizar medios o dispositivos informáticos en condiciones seguras (no comprometidos o libres de software malicioso).

Cuando se acceda mediante un navegador web a la dirección de la sede electrónica, lugar dónde se podrán verificar los documentos CSV, se deberá comprobar que no muestra ninguna alerta sobre la validez del certificado SSL.

A continuación, se detallan los diferentes procedimientos de verificación.

Una vez se esté en posesión del documento en papel con CSV se seguirán los siguientes pasos para su verificación:

1. Acceder mediante un navegador web a la dirección de verificación de CSV de la sede electrónica (asimismo reflejada en el propio documento):

https://paiporta.sedipualba.es/csv/

2. Introducir el código CSV impreso en el margen del documento.

3. Comprobar que la sede electrónica indica que existe un documento con ese CSV y que al descargarlo coincide con el documento impreso (deben ser idénticos).

10.2.1. VERIFICACIÓN DE DOCUMENTOS CON CSV ENTREGADOS EN FORMATO ELECTRÓNICO (PDF)

Una vez se esté en posesión del documento electrónico con CSV se seguirán los siguientes pasos para su verificación:

1. Validar las firmas del documento CSV mediante la aplicación VALIDe de la Administración General del Estado o mediante un programa lector de documentos PDF con la capacidad de verificar firmas electrónicas en formato PAdES LTA-level:

    1.1. Si el CSV consta de 20 dígitos: comprobar que la aplicación acredita que la firma es válida y que el documento está firmado mediante un certificado de sello electrónico incluido en el listado al que se hace referencia en el apartado 7 de la presente política. Si la firma contiene sellado de tiempo, éste también debe presentarse como válido (PAdES LTA-level).

    1.2. Si el CSV consta de menos de 20 dígitos: comprobar que la aplicación acredita que las firmas son válidas. Si la firma contiene sellado de tiempo, éste también debe presentarse como válido.

2. Adicionalmente, comprobar que el documento CSV existe en la sede electrónica:

    2.1. Acceder mediante un navegador web a la dirección de verificación de CSV de la sede electrónica (asimismo reflejada en el propio documento): https://paiporta.sedipualba.es/csv/

    2.2. Introducir el código CSV impreso en el margen del documento.

    2.3. Comprobar que la sede electrónica indica que existe un documento con ese CSV y que al descargarlo coincide con el documento electrónico (deben ser idénticos).

10.2.2. VERIFICACIÓN DE DOCUMENTOS DE FIRMA ELECTRÓNICA XAdES

Los documentos de firma XAdES producidos en el ámbito de esta política estarán asociados a sus correspondientes documentos originales o a sus correspondientes documentos CSV.

La autenticidad y validez de las firmas electrónicas XAdES se acreditará y verificará siguiendo el siguiente procedimiento:

1. Recabar la siguiente información:

- Documento original.
- Fichero de firma electrónica en formato XAdES-A.
- Título del documento.
- Información del firmante.
- Código aleatorio (salt o sal) con la que se generó la huella firmada en el documento XAdES-A.

2. Validar el fichero de firma electrónica mediante la aplicación VALIDe de la Administración General del Estado. Al ser un formato estándar, se pueden usar otras herramientas con capacidad de validación de firmas.

3. Comprobar que la firma validada en el punto anterior se corresponde con el documento firmado:

3.1. Calcular el hash SHA3-512 sobre el resultado de concatenar el documento binario original + el título del documento codificado en UTF-8 + la información del firmante codificado en UTF-8 + la “sal”.

3.2. Abrir el fichero XAdES-A y comprobar que el elemento en la ruta XPath /ds:Signature/ds:Object/documentos_firmados contiene un elemento documento_firmado con el hash calculado anteriormente y la “sal” utilizada (ambos codificados en Base64).

3.3. Comprobar que el XPath anterior se encuentra incluido en alguna de las referencias del elemento SignedDataObjectProperties, y por tanto firmado.

En caso de que todas las comprobaciones anteriores hayan resultado satisfactorias, quedaría probado que el documento original se corresponde con la firma XAdES-A, la cual garantiza la integridad del documento, su autenticidad y el no repudio.

Dado que la validación de la firma XAdES resulta un procedimiento complejo, se publicará una herramienta que de forma automática permita verificar su correspondencia con el documento original firmado.

Adicionalmente, el código fuente de esta herramienta se publicará sin restricciones de acceso en un repositorio al efecto. De esta manera los terceros que dispongan de los medios y conocimientos tecnológicos precisos podrán generar la herramienta que les permita verificar de forma autónoma e independiente la validez de los documentos producidos en el ámbito de esta política.

11. POLÍTICA DE FIRMA DE LA ADMINISTRACIÓN GENERAL DEL ESTADO

Se considerarán válidos, y por tanto se admitirán, todos aquellos mecanismos de identificación y firma reconocidos en la Política de firma electrónica y de certificados de la Administración General del Estado, así como todos aquellos documentos producidos o resultantes de los mismos.

12. ROLES Y RESPONSABILIDADES

ROL	DESCRIPCIÓN
Responsable de Seguridad	• Colaborar con el gestor de la política de firma en la especificación en el mantenimiento y actualización del presente documento.
Responsable del Sistema	• Colaborar con el gestor de la política de firma en el mantenimiento, actualización y publicación electrónica del presente documento