EUSKO JAURLARITZA GOBIERNO VASCO

JUSTIZIA ETA HERRI ADMINISTRAZIO SAILA

DEPARTAMENTO DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA

Sinadura elektronikoaren politika, Euskal Autonomia Erkidegoko Administrazioko ziurtagirietan oinarritua

Donostia - San Sebastián, 1 – 01010 VITORIA-GASTEIZ
tef. 945 01 85 71 – Fax 945 01 87 01

Edukia

1. Sarrera

Administrazio Elektronikoari buruzko otsailaren 21eko 21/2012 Dekretuaren helburua da Euskal Autonomia Erkidegoko Herri Administrazioan garatzea herritarrek duten eskubidea Herri Administrazioarekin dituzten harremanetan baliabide elektronikoz baliatzeko, zerbitzu publikoetara jotzeko edo administrazio-prozedurak izapidetzeko.

Orokorrean, dekretuak hainbat alderdi arautzen ditu: egoitza elektronikoa, iragarki-taula elektronikoa, identifikazioa eta autentikazioa, erregistro elektronikoak, komunikazio eta jakinarazpenak, agiri elektronikoak eta horien kopiak, izapidetze elektronikoa edota zerbitzu elektroniko erkideak.

Hain zuzen ere *Identifikatzea eta autentifikatzea*ri buruzko tituluko “Sinadura elektronikorako eta ziurtagirietarako politika” izeneko artikuluan ezartzen denez, Administrazioak sinadura elektronikorako eta ziurtagirietarako politika onartu, eta argitaratuko du; politika horretan, berriz, zehaztu egingo zu zer prozesu erabili sinadura elektronikoak sortu, balioztatu eta gordetzeko, eta zer baldintza bete behar dituzten sinadurek. Era berean, ezartzen du politika hori administrazio elektronikoaren gaineko eskumenak dituen sailak argitaratuko duela, agindu bidez.

Sinadura elektronikorako eta ziurtagirietarako politika onartzen duen Agindua, beraz, tresna bat da, politika hori argitaratzeko eta herritarrei zabaltzeko.

Dokumentu honek sinadura elektronikoaren nondik norakoak eta erabilera deskribatzen ditu, Euskal Autonomia Erkidegoko (aurrerantzean EAE) Herri Administrazioko testuinguruan transakzio zehatzak egiteko baldintzak betetzeko asmoaz, eta, horretarako, dokumentu honek zabaldu egiten du sinadura elekktronikorako eta ziurtagirietarako politika onartzen duen Aginduak zehazten duena, eta, Europako estandar teknikoak aintzakotzat hartuta, dokumentu elektronikoen egitura normalizatzen du, sinadura elektronikoak sortu eta balioztatzeko, eta dokumentu horien elkarreragingarritasuna errazteko.

2. Sinadura-politikaren nondik norakoak

Dokumentu honek modu elektronikoan sinatzeko politika proposatzen du. Politika horrek, batetik, zehaztu egiten du zein baldintza orokor bete behar diren sinadura elektronikoa sortu, balioztatu eta gordetzeko, eta, bestetik, zerrenda batean jasotzen du objektu bitarreko eta erreferentzia-fitxategietako zer formatu onartu beharko dituzten plataforma guztiek, Administrazioek herritarrekin, erakunde autonomoekin, zuzenbide pribatuko erakundeekin eta Adminitrazio Elektronikoari buruzko Dekretua aplikatu behar duten gainerako eremuetako erakundeekin dituen harremanak bideratzeko.

Adiera bakarraz identifikatzeko, sinadura-politika honek URI itxurako identifikatzaile bat izango du: derrigorrez sartu beharko da sinadura elektronikoan, eta, horretarako, sinadura-politika identifikatzeko eremua eta bertsioa erabili beharko dira, sinadura balioztatzeko baldintza orokor, zehatz, eta guzti; era berean, une jakin batean sinadura elektronikoak bete behar dituen baldintzak zehaztuko ditu.

Sinadura-politika honek formatu irakurterraza izan beharko du, baldintza horiek sinadura elektronikoa sortu eta balioztatzeko testuinguruan aplikatu daitezen.

2.1. Sinadura elektronikoaren eragileak

Eragile hauek parte hartzen dute sinadura elektronikoa sortu eta balioztatzeko prozesuan:

- Sinatzailea: sinadura sortzeko gailua du, eta bere izenean edo ordezkatzen duen pertsona fisiko edo juridikoaren izenean dihardu.

- Egiaztatzailea: sinadura-politika jakin batek ezartzen dituen baldintzetan oinarrituta, sinadura elektronikoa balioztatu edo egiaztatzen duen erakundea, dela pertsona fisikoa, dela juridikoa. Konfiantzaz balioztatzeko erakunde bat izan daiteke edo hirugarren alderdi bat, interesa duena jakiteko sinadura elektroniko jakin bat baliozkoa den ala ez.

- Sinadura elektronikoaren zerbitzu-emailea: ziurtagiri elektronikoak edo sinadura elektronikoarekin zerikusia duten beste zerbitzu batzuk ematen dituen pertsona fisikoa edo juridikoa.

- Sinadura-politikaren jaulkitzailea: sinadura-politikako agiria sortu eta kudeatzeaz arduratzen den erakundea; agiri horrek zuzenduko ditu sinatzailea eta egiaztatzailea, sinadura elektronikoa sortu eta balioztatzeko prozesuetan.

2.2. Onartutako sinadura-formatuak

Dokumentu elektronikoek sinadura elektroniko aurreratua eta onartua –Administrazioak onartutako ziurtagiri elektronikoen bidez aplikatu, eta administrazio-barneko edo administrazioarekiko harremanetan erabiltzen dena- izateko, dokumentu horien formatuak bete egin beharko du hala Europako estandarrek zehazten dutena sinadura elektronikoko formatuei buruz, nola Espainiako legediak dioena onartutako sinaduren gainean.

Administrazio Elektronikoaren gaineko eskumenak dituen zuzendaritzak argitaratu eta eguneratu beharko du sinadura-politika honetan onartzen diren formatuei buruzko zehaztapenen zerrenda, egoitza elektronikoan.

Administrazio Elektronikoaren gaineko eskumenak dituen zuzendaritzak biltegi bat izango du, sinadura elektronikorako eta ziurtagirietarako onartzen diren politika-bertsio guztiak jasotzeko. Biltegi horretara jo beharko da, indarrean den politikaren aurreko sinadura elektroniko guztiak egiaztatzeko. Ezer sinatzen denean, berriz, sinadura elektronikorako eta ziurtagirietarako politika-bertsioaren identifikatzailea aipatu beharko da; izan ere, politika-bertsioak zehaztuko du beti zer baldintza betetzen duen sinadura elektronikoak.

Kontuan izango da zer legedi duen Europako Batasunak onartutako sinadura-formatuei buruz, eta batez ere zer estandar definitu dituen Europak sinadura elektronikorako.

Administrazio Elektronikoari buruzko Dekretua aplikatu behar duten organo eta erakundeek XadES formatu motak kontuan izan beharko dituzte, sinadurak sortzeko sistemak egokitzeko, gutxienez, oinarrizko formatura; era berean, EPES motako sinadura-politikari buruzko informazioa erantsi beharko dute, bai eta XADES formatu-maila guztiak -1.3.2 bertsioa- egiaztatzeko aukera ere, betiere ETSI TS 101 903 zehaztapen teknikoan jasotzen denaren arabera.

Elkarreragingarritasuneko sinadura elektronikoaren politika definitzeko, sinadura elektronikoaren oinarrizko mailak EPES izan behar du, AdES estandarren arabera. EPES oinarrizko formatu hori oinarritzat hartuta, informazio aproposa sartu ahal da, sinadura bat epe luzerako balioztatzeko.

Epe luzerako balioztatzeko, XAdES- A formatua erabili beharko da; formatu horrek, berriz, propietate osagarriei aldian behin denbora-zigilua sartzeko aukera eskaini behar du, esaterako, ziurtagirien erreferentziei eta ezeztatze-balioei informazioa sartzeko, eta ziurtagiriak eurak eta CRLs ezeztatze-zerrendetan edo OCSPs zerbitzuetan lortutako ezeztatze-balioak sartzeko.

2.2.1. Datuak transmititzeko sinadura elektronikoa

Elkarreragingarritasun Eskema Nazionalalak ezartzen duenez (aurrerantzean EEN), Estandaren Katalogoko elkarreragintasunari buruzko arau teknikoan jasotzen diren estandarretan oinarrituko da datuak transmititzeko sinadura elektronikoa.

Sinadura-politika honen kasuan, datu-transmititzeko, web zerbitzuak erabili behar dira. Beraz, sinadura elektronikoak erabiltzeko, nahitaez erabili beharko da *WS- Security* estandarra, eta bereziki OASISen *SOAP Message Security*, *X.509 Certificate Token Profile* zehaztapen estandarraz.

2.2.2. Edukien gaineko sinadura elektronikoa

Sinadura-politikan, zehaztu egin beharko da zer formatu onartzen diren edukien sinadurarako. Estandarren Katalogoko elkarreragingarritasunari buruzko arau teknikoa eta sinadura-politika honetako ezaugarri bereziak kontuan hartuta, formatu hau onartzen da:

a. XAdES (XML Advanced Electronic Signature), ETSI TS 101 903 zehaztapeneko 1.3.2 bertsioaren arabera.

Era berean, formatu horrek aldaera hauek izan ahal izango ditu:

- ✓ T: Eusko Jaurlaritzaren sinadura-politika betetzeko gutxieneko formatua. Denbora zigilatzeko eremu bat erantsi da, atzera botatzearen kontra babesteko.
- ✓ -A: Ziurtagiriak eta ezeztatze-zerrendez gain, ziurtagiriei eta indargabetze-zerrendei jarritako erreferentzien gaineko aldizkako zigilua sartzen du. Horrela, bizitza luzeko sinadurak lortzen dira, luzaroan irauteko.

2.3. Sinadura elektronikoa sortzea

Sinadura elektronikoak sortzeko erabiltzen diren platoformek funtzionaltasun jakin batzuk eskaini egin beharko dituzte sinadurak sortzeko prozesua betetzeko. Hona funtzionaltasunok zertan oinarrituko diren:

1. Erabiltzaile sinatzaileak fitxategia aukeratu ahal izango du, gero sinatzeko. Plataformek onartu beharko dituzten fitxategi-formatuak egoitza elektronikoan argitaratuko dira, dokumentu elektroniko onartuen atalean.

   Sinatzaileak egiaztatu egin beharko du sinatu nahi duen fitxategiak ez duela eduki dinamikorik, fitxategiaren balioan eragin, eta epe luzean sinaduraren emaitza alda dezakeenik.

2. Sinadura sortu aurretik, sinadura elektronikoaren zerbitzuak honako hauek egiaztuko ditu:

   - Sinadura elektronikoa, politika honen arabera balioztatu ahal dela sinatu behar den fitxategiaren formaturako.

- Erabili beharreko ziurtagiriak Ziurtapen Politiken Deklarazio onartu baten arabera ematen direla. Egoitza elektronikoan argitaratuko dira: sinatzeko zer sistema eta zer ziurtagiri elektroniko onartzen diren (zerrenda batean jasota), zein prozeduratarako balio duten eta zer zehaztapen izango duten horiekin jartzen diren sinadura elektronikoek.

- Ziurtagiriaren balioa –horretarako, egiaztatu egingo da ziurtagiria ezeztatu edo eten egin den–, balio-epearen barruan dagoen, eta ziurtatze-katearen balidazioa, kateko ziurtagiri guztiak baliozkotzat jotzea barnean sartuta.

  Akats baten ondorioz ezer egiaztatzen bada, eten egingo da sinatzeko prozesua.

  Hori guztia egiaztatzerik ez badago, sinatzen denean, sistemek aukera izango dute ez onartzeko sinatutako fitxategia edo aldi batean itxaroteko berriro egiaztatu arte.

3. Zerbitzuak XAdES formatuko fitxategi bat sortuko du, halakorik behar denean. Ateratzen den fitxategiak luzapen bakarra izatea gomendatzen da, dokumentu sinatuen ikustaileak lotu ahal izateko luzapen horri, eta, horrela, erabiltzaileek errazago erabili ahal izango dituzte era honetako fitxategiak. Luzapena hau izan daiteke:

   - ✓ .xsig: ezarritako sinadura hori XadES estandarrean oinarritu da.

2.4. Sinadura elektronikoa egiaztatzea

Egiaztatzaileak edozein metodo erabili ahal du, politika honen arabera sortutako sinadurak egiaztatzeko. Sinadurak balioztatzeko, gutxienez, baldintza hauek bete beharko dira:

1. Bermatu egin beharko da sinadurak balio duela sinatu den fitxategirako

2. Ziurtagiriak ezeztatzeari buruzko informazioa duten sinaduren kasuan, ziurtagiriek baliozkoak izan behar dute sinatzen direnean; bestela, ziurtagiriek baliozkoak izan behar dute balioztatzen direnean: ziurtagiri ezeztatugabeak, etenak edo amaituak, eta ziurtatze-katearen balidazioa (kateko ziurtagiri guztiak balioztatzea barne). Bizitza luzeko sinaduren kasuan, informazio hori sinadurak berak eduki ahal du.

3. Sinatzen denean, onartutako Praktiken Ziurtapen Deklaraziopean emandako ziurtagiria Egoitza elektroniko atalera jo ahal izango da, onartutako ziurtagiri guztien zerrenda osoa kontsultatzeko.

4. Ezarritako formatua duten denbora-zigilurik badago, zigiluak eurak eta zigiluen balio-epeak egiaztatu beharko dira.

2.5. Sinadurak birzigilatzea

Sinadura elektronikoa denboran zehar fidagarria izango dela bermatzeko, sinatzen denean gehitu egingo zaio bai lotutako ziurtagiriaren egoerari buruzko informazioa, bai onartu ezin den informazioa, halakorik badago; era berean, denbora-zigilua jarri, eta konfiantzazko katea osatzen duten ziurtagiriak gehituko zaizkio.

Ondorioz, denboran zehar balioztatu ahal den sinadura izan nahi badugu, sortzen dugun sinadura elektronikoak balioari buruzko ebidentziak izan behar ditu, inork atzera bota ez dezan. Zerbitzu bat egongo da, era horretako sinadurek ebidentzia horiek manten ditzaten, eta sinadurak eguneratzeko eskatu beharko da, gakoak eta lotutako material kriptografikoa kaltetu baino lehenago.

Hona bizitza luzeko sinadura elektronikoak bete beharko dituen baldintzak:

1. Lehenengo eta behin, egiaztatu egin beharko da sortutako edo egiaztatutako sinadura elektronikoa; horretarako, baliozkotzat jo beharko dira: sinadura osoa, dagokion estandarra betetzen dela, eta erreferentziak.

2. Sinadura elektronikoa osatzeko prozesua bete beharko da, eta horretarako:

    a. Ziurtagirien erreferentziak lortu, eta sinatzaileen ziurtagiriak biltegian gorde beharko dira.

    b. Lortu egin beharko dira: ziurtagirien egoerari buruzko informazioen erreferentziak, ziurtagiriak ezeztatzeko zerrendak (CRLs) edo OCSP erantzunak; horiek denak biltegian gorde beharko dira.

3. Gutxienez, ziurtagirien erreferentziak eta egoera-informazioak zigilatu beharko dira.

Sinadura elektronikotik ateratzen den dokumentuan bertan gordeko dira ziurtagiriak eta egoera-informazioak. Horretarako, fitxategi-sinadurako modalitate bat erabiliko da.

Sinadura elektronikoko algoritmoak ez zaharkitzeko, eta ezaugarriak balio-denboran zehar seguru mantentzeko, birzigilatzeko mekanismoak aplikatu beharko dira, algoritmo iraunkorrago batekin aldian-aldian fitxategiaren data-orduen zigilua jartzeko.

Sinadurek aukera eman behar dute etorkizunean berriztatzeko (zigilua berriro jartzeko edo berresteko) eta konfiantza-elementuak (denbora-eremuak) eguneratzeko; horrela, sinadura elektronikoa fidagarria dela bermatuko da.

Sinadura elektronikoko algoritmoak ez zaharkitzeko, eta ezaugarriak balio-denboran zehar seguru mantentzeko, birzigilatzeko mekanismoak aplikatu beharko dira, algoritmo iraunkorrago batekin aldian-aldian fitxategiaren data-orduen zigilua jartzeko.

3. Sinadura elektronikoa balioztatzeko politika

Atal honetan daude zehaztuta sinadura elektronikoa sortzeko prozesuan sinatzaileak kontuan hartu beharreko baldintzak eta sinadura balioztatzeko prozesuan egiaztatzaileak kontuan hartu beharrekoak.

3.1. Dokumentua identifikatzea

Dokumentuaren izena	Sinadura elektronikoko politika, Euskal Autonomia Erkidegoko Administrazioko ziurtagirietan oinarritua
Bertsioa	1
Politikaren identifikatzailea	urn:ejgv:dss:policy:1
Politikaren erreferentziako URI	http://www.euskaltel.es
Noiz emanda	2012ko uztailaren 27a
Aplikazio-eremua	Administrazio elektronikoari buruzko Dekretuaren aplikazio-eremua

3.2. Balio-aldia

Sinadura elektronikorako politika honen balio-aldia aurreko paragrafoa ematen denetik bertsio eguneratu berria ematen den artekoa da. Dena den, denboraldi iragankor bat ere finkatu ahal izango da harik eta herri-administrazioen plataforma ezberdinak bertsio berriaren zehaztapenetara egokitu arte. Denboraldi horretan bi bertsioak erabili ahal izango dira. Denboraldi iragankor hori adierazi egin beharko da bertsio berrian, eta behin igarota bertsio eguneratuak baino ez du balio izango.

3.3. Dokumentuaren kudeatzailea identifikatzea

Politikaren kudeatzailearen izena	Berrikuntzaren eta Administrazio Elektronikoaren Zuzendaritza - Justizia eta Herri Administrazio Saila
Harremanetarako helbidea	Donostia kalea, 1. 01010 Vitoria-Gasteiz.

3.4. Aldaketak kontrolatzea

Atal honen bitartez, dokumentuak izan dituen bertsio guztien jarraipena egin ahal izango da, denborak igaro ahala gertatutako aldaketa guztien kontrol zehatza eduki ahal izateko, hain zuzen.

Horretarako, unean-unean sortutako bertsio guztiak agertzen dira taula batean.

Kodea	Bertsioa	Eguna	Egindako aldaketen laburpena
-	1	27/07/2012	Lehen bertsioa

3.5. Sinadura elektronikoaren erabilerak

Dauden kanal telematikoen bitartez informazioa babesteko tresna da sinadura elektronikoa. Eremu eta irismen jakin baterako aurreikusitako erabilerak adieraztea da sinadura politikaren helburua. Horretarako, erabilera bakoitzean beharrezkoak diren baldintzak zehaztu egingo dira.

3.5.1. Datuak transmititzeko sinadura elektronikoa

Datuak transmititzeko sinadura elektronikoa beharrezkoa izango da. Datuak elkartrukatzean segurtasuna bermatu behar da, prozesuan parte hartuko dutenen identitatea autentifikatu, igorritako datuei buruzko mezuaren edukiaren osotasuna, eta bi zerbitzariren artean (puntuz puntu) mezuei ez zaiela uko egiten bermatu. Sinadura garraioko protokoloari lotuta dago, eta komunikazio seguru batean ezarri beharreko zifratze-mekanismoetako bat da.

Horrela bada, herri administrazioen atalen artean egingo diren komunikazio guztiek, dokumentu honetan adierazitako sinadura politika erabili behar badute, Web Service-Security (WSS) goiburu bat erabili beharko dute SOAP mezuak sinatzeko, E-Administraziorako Plataforma Teknologikoak (PLATEA) uler ditzan. Plataforma horrek berbideratuko ditu SOAP mezu horiek, modu gardenean, Eusko Jaurlaritzaren sinadura-zerbitzuen plataformara.

3.5.2. Edukien gaineko sinadura elektronikoa

Sinadura mota hau eskuz idatzitako ohiko sinaduraren baliokidea da ingurune digitalean. Edukiari dago zuzenean lotuta eta haren benetakotasuna bermatzen du.

Datuak transmititzeko sinaduretan ez bezala, edukien gaineko sinadurak osotasuna eta autentifikazioa ematen du, eta mutur bien artean ez dagoela uko egiterik, edukia elkartrukatzeko mekanismo bat edo beste erabilita ere.

Elkartrukatze kasuetan, sinadura zein edukia bera, transmisioari edota elkartrukatzeari berari atxikita joango dira. Beraz, azaldutako sinaduraren erabilerak ez dira osagarriak, bateragarriak baizik, eta aldi berean erabil daitezke.

3.6. Guztientzako arauak

Sinadura elektronikoaren eragileentzat (sinatzailea eta egiaztatzailea) diren arauak edozein sinadura-politiketan agertu beharreko nahitaezko eremua dira. Sinadura sortzen duen pertsona edo entitatearen sinadura elektronikoarekiko erantzukizunak finkatzeko balio dute eta aurkeztu behar diren gutxieneko eskakizunak definitzen dituzte. Sinatzailearentzako eskakizunak badira, sinatuta egongo dira, baina egiaztatzailearentzat badira, sinatu gabe.

3.6.1. Sinatzaileak bete beharreko arauak

Sinatzailearen erantzukizuna izango da sinatu nahi den fitxategiak ez duela eduki dinamikorik ziurtatzea, epe luzean sinaduraren emaitza alda dezakeena, alegia. Sinatu nahi den fitxategia ez badu sinatzaileak sortu, ziurtatu egin beharko du fitxategian ez dagoela eduki dinamikorik, makroak esaterako.

3.6.1.1. XAdES formatua

Sinadura politika honetan aurreikusitako XadES bertsioa 1.3.2 bertsioa da. Arreta berezia jarriko da eta uneoro adieraziko da zein bertsio erabiltzen ari garen bertsio-zenbakiari erreferentzia egiten zaion tag guztietan.

Sinadura elektronikoaren egitura izeneko II. eranskinean dago zehaztuta egiaztatzaileak baliozkotzat jotzeko sinadura elektronikoak eduki behar duen egitura.

Dokumentu honetan deskribatutako sinadura politikari dagokionez, sinadura mota bi onartuko dira Elkarreragingarritasuneko Eskema Nazionalaren arabera:

- ✓ **XAdES Detached: Ez dauka jatorrizko dokumenturik, URI baten bitartez egiten zaio erreferentzia eta hura aurkitzeko balio du. Eskaeretan, URI hori igorritako datuekin lotuko da, hau da, berezo-aplikazioak du datuak emateko ardura**.

- OHARRA: Sinadura mota honetan aplikatutako terminologia @Firma bezalako beste plataforma batzuetan erabilitakoa da: **XAdES Externally Detached**.

✓ **XAdES Enveloped**: sinatutako edukiak eta sinadurak XML egitura bera daukate, sinadura balioztatzeko beharrezkoa dena. sinatutako edukiaren justu jarraian joango da sinadura.

Sinadura-mota bi horien aldaerak hauek izan daitezke:

✓ -T: Sinatutako dokumentuak denbora-zigilu bat izango du, gutxienez, uko ez egitetik babestuko duena.

✓ -A: Bizitza luzeko sinadura, dokumentu honetan zehaztutako sinadura politika behar bezala betetzeko erabiliko dena. Aldizkako denbora-zigilua jarriko zaie ziurtagirien eta ezezte-egoeren erreferentziei zein ziurtagiriei eta ezezte-erantzunei.

Sinatzaileak, gutxienez, ***SignedProperties*** eremu barruan dauden ondorengo etiketetako informazioa eman beharko du, **nahitaezkoak** baitira. Eremu horrek XMLDsig sinadura sortzeko hainbat propietate ditu, batera sinatuak.

- **SigningTime**: data eta ordua adierazten ditu. Zerbitzari batera atzitu gabeko bezeroaren sinaduraren kasuan, adierazpen hutsa da (bezero-dispositiboan data erraz manipula baitaiteke) eta sinaduraren data eta ordua ezagutzea ez den beste helburu batzuetarako erabiliko da. Sinadura elektronikorako politika partikularrek ezaugarriak eta mugapenak zehaztu ahal izango dituzte bezeroek denbora eta erlojuaren sinkronizazio erreferentziak sortzeko.

- **SigningCertificate**: ziurtagiri bakoitzerako erabilitako ziurtagiri eta segurtasuneko algoritmoei buruzko aipamenak ditu. Elementu hau sinatu egin beharko da, ziurtagiria ordezkatzeko aukera saihesteko.

- **SignaturePolicyIdentifier**: sinadura elektronikoa sortzeko prozesuak oinarrian duen sinadurari buruzko politika identifikatzen du. Hainbat elementutan dago zatitua eta honako eduki hauek jaso beharko dituzte elementu horiek:

  - Sinadura politika honi buruzko dokumentuaren berariazko aipamena, edota erakunde bakoitzaren sinadura partikularraren politikari buruzko dokumentuaren aipamena. Hori guztia, xades:SigPolicyId elementuan. Horretarako agertuko da sinadura politikaren bertsio zehatza identifikatuko duen OIDa edota hura lokalizatzeko URLa.

```
<xades:QualifyingProperties>
    <xades:Identifier> ... </xades:Identifier>
```

  - Dena delako sinadura politikaren dokumentuaren hatz-marka digitala eta erabilitako algoritmoa. Hori guztia, <xades:SigPolicyHash> elementuan. Horrela, egiaztatzaileak egiaztatu ahal izango du – aldi berean balore hau kalkulatuta- sinadura sortzeko politika eta hura balioztatzeko erabiliko den politika bera izango direla.

- **DataObjectFormat**: jatorrizko dokumentuaren formatoa definitzen du, eta beharrezkoa da jasotzaileak dokumentua bistaratzeko modua jakin dezan.

SignedProperties eremuan erants daitezkeen gainerako etiketak aukerakoak dira.

- **SignatureProductionPlace**: dokumentua zein toki geografikotan sinatu den definitzen du.

- **SignerRole**: pertsonaren rola definitzen du sinadura elektronikoan.

- **CommitmentTypeIndication**: sinatutako dokumentuarekiko sinatzailearen eragiketa definitzen du (onartu egin du, informatu, jaso, egiaztatu, etab.).

- **AllDataObjectsTimeStamp**: denbora-zigilu bat du, sinadura sortu aurretik kalkulatua ds:Reference-n eduki guztien gainean.

- **IndividualDataObjectsTimeStamp**: denbora-zigilu bat du, sinadura sortu aurretik kalkulatua ds:Reference-n eduki guztien gainean.

CounterSignature etiketa, sinadura elektronikoaren berrespena, eta UnsignedProperties eremuan bil daitekeena, aukerakoa izango da. Hurrengo sinadurak, sailean edo paraleloan, XadES estandarrak adierazi bezala erantsiko dira, ETSI TS 101 903 v1.3.2. dokumentuaren arabera.

3.6.2. Egiaztatzaileak bete beharreko arauak

Sinadura elektroniko aurreratuaren oinarrizko formatoak daukan balioztatze-informazioari dagokionez, *SigningCertificate* etiketan dagoen sinatzailearen ziurtagirira eta *SignaturePolicy* etiketan adierazitako sinadura politikara mugatzen da.

Hona hemen sinadura sortzeko erabilitako sinadura-politikaren araberako betekizunak betetzen diren egiaztatzeko egiaztatzaileak erabili ahal izango dituen atributoak:

- ***SigningTime***: adierazitako datan ziurtagirien egoera egiaztatzeko baino ez da erabiliko sinadura elektronikoen egiaztatzeetan, denbora-zigiluarekin baino ezin baitira egiaztatu denbora erreferentziak (bezero-dispositiboetako sinadura kasuetan bereziki). Denbora zigiluak erabili badira, sinaduraren egituraren barruko zigilurik zaharrena erabiliko da sinaduraren data zehazteko.

- ***SigningCertificate***: Sinadura sortu/sorrarazi zen datan ziurtagiriaren (eta ziurtatze-katearena, kasuan kasu) egoera begiratu eta egiaztatzeko erabiliko da, ziurtagaria iraungita ez baldin badago eta balioztatze datuetara (CRL, OCSP, etab.) sar ahal badaiteke.

- ***SignaturePolicy***: sinadura sortzeko erabilitako sinadura-politika, halako zerbitzu batean erabili beharrekoarekin bat datorrela egiaztatu beharko da.

Dokumentu berean sinadura bat baino gehiago bat dago, lehenbiziko sinadurarekin egindako balioztatze-prozesu berbera jarraituko da. Horretarako, sinatu gabeko propietateen eremuan sortutako sinadura berrespenen berri ematen den *CounterSignature* etiketa egiaztatuko da.

Sinadura balioztatzeko arduradunak balioztatzeko eta artxibatzeko prozedurak definitu beharko ditu sinadura-politikaren betekizunen arabera.

Badago itxarote-denbora bat, zuhurtasun-epe edo graziazko epe deiturikoa, ziurtagiri baten ezeztatze-egoera egiaztatzeko dena. Egiaztatzaileak epe hori baliatu dezake sinadura balioztatzeko edota une horretan balioztatu eta geroago berriz balioztatzeko. Izan ere, gerta daiteke atzerakizunen bat egotea sinatzaileak ziurtagiri baten ezeztatzea hasten duenetik eta ziurtagiaren ezeztatze-egoeraren berri dagokion informazio puntuetara banatu arte. Denbora-tarte horri dagokionez, gomendatzen dena da sinadura egiten denetik edota denbora-zigilua ezartzen denetik, gutxienez CRLak erabat freskatu artekoa izan daila, edota OCSP zerbitzuan ziurtagiriaren egoera eguneratzeko beharrezkoa den bestekoa. Denbora-tarte horiek aldatu egin daitezke, Ziurtapen Zerbitzuen Emailearen arabera.

Dena delako sistemak ezarriko du onartzeko prest dagoen graziazko epea. Baina eperik ez ezartzea ere erabaki dezake eta, beraz, sinadura ez litzateke balioztatuko.

3.6.3. Denbora-zigiluei buruzko arauak

Denbora-zigiluek ziurtatzen dutena da sinatuko den dokumentuaren jatorrizko datuak zein ziurtagirien egoerari buruzko informazioa (sinadura elektronikoan sartu badira) data jakin baten aurretik sortuak izan zirela. Denbora-zigiluaren formatoa honako hauek gomendatutakoaren araberakoa izango da: IETF, RFC 5816, “Internet X.509 Public Key Infrastructure; Time-Stamp Protocol (TSP)”.

Hona hemen zigilu digitalaren oinarrizko elementuak:

1. Agintaritza jaulkitzailearen identitateari buruzko datuak (nortasun juridikoa, zigilua egiaztatzeko erabili beharreko gako publikoa, gakoaren bit kopurua, sinadura digitalaren algoritmoa eta erabilitako hash funtzioa).

2. Egindako eskabide-mota (hash balioa edo dokumentua den, zein den bere balioa eta erreferentziako datuak).

3. Sekuentziadorearen parametroak (hash balioak “aurrekoa”, “unekoa” eta “hurrengoa”).

4. Eguna eta ordua UTC.

5. Aurreko guztiaren sinadura digitala, gako publikoa eta sinadura digitalaren eskema zehaztuta.

Denbora-zigilua eta balioztatze-informazioa igorleak, jasotzaileak edota hirugarren batek erants dezake, eta **SignatureTimeStamp** eremuan sartu behar dira sinatu gabeko propietate bezala.

Denbora-zigilua **SigningTime** eremuan sartutako datatik hurbileko uneren batean jarri behar da, eta beti ere, sinatzailearen ziurtagiria iraungi aurretik.

Sinadura politika honek onartzen ditu, hala ere, denbora-zigiluak jartzea eskaintzen dituen emaileek emandako denbora-zigiluak, baldin eta ETSI TS 102 023, “*Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities*” zehaztapen teknikoak betetzen badituzte.

3.6.4. Bizitza luzeko sinadurei buruzko konfiantza-arauak

XAdES (ETSI TS 101 903) estandarrak aukera ematen du sinadura elektronikoei bizitza luzeko sinadura baten balioa bermatuko duen informazio osagarria gehitzeko, behin ziurtagiriaren balio-epea iraungita. Informazio hori sinatzaileak zein egiaztatzaileak sar dezake, eta zuhurtasun-epea edo graziazko epea igaro eta gero sartzea gomendatzen da. Balioztatzeko informazio gehigarri bezala sartzeko datu-mota bi daude:

- Ziurtagiriaren egoerari buruzko informazioa sinadura balioztatzen den unean edo haiei buruzko erreferentzia.

- Konfiantza-katea osatzen duten ziurtagiriak.

Bizitza luzeko sinadurak sortu nahi badira, balioztatze-informazioa gehitu beharko da, aldez aurrekoa, eta denbora-zigilua jarri. Sinadura-mota hauetan emaitzazko sinaduraren balioa bizitza luzeko sinadurari gehitzen zaion denbora-zigiluak zehazten du.

Sinadurari balioztatze-informazioa gehitu nahi bazaio, OCSP bidezko balioztatzea erabiltzea gomendatzen da, gehitu beharreko propietate edo atributoak txikiagoak baitira metodo honetan.

3.6.4.1. XAdES formatua

XadES sinadura-fomatuaren barruan, XAdES-C formatu luzatuak sinatu gabeko beste propietate batzuen artean honako hauek biltzen ditu:

- **CompleteCertificateRefs,** sinadura egiaztatzeko beharrezkoak diren konfiantza-kateko ziurtagiri guztien erreferentziak biltzen dituena, sinatzailearen ziurtagiria izan ezik.

- **CompleteRevocationRefs**, ziurtagiriak egiaztatzeko erabili diren CRL-ei eta OCSP erantzunei buruzko erreferentziak biltzen dituena.

XAdES-X formatuak, aurreko informazioari denbora-zigilua gehitzen dio.

XAdES-XL formatuak, XAdES-X formatuan bildutako informazioaz gain, sinatu gabeko beste propietate bi eransten ditu:

- **CertificateValues**

- **RevocationValues**

Propietate hauek, balioztatze-informazioari buruzko erreferentziez gain, konfiantza-katea osoa eta balioztatzean lortutako CRL edo OCSP erantzuna ere biltzen dituzte. CertificateValues eta RevocationValues atributuentzat OCSP bidezko balioztatzea gomendatzen da, balio horiek bolumen handiegia izan dezakete-eta CRL bidez egiteko.

EAEko Herri Administrazioaren sinadura-politika egoki betetzeko, **XADES-A** formatua erabili beharko da. Formatu honek aurreko informazioaz gain, denbora-zigilua eransten du bizitza luzeko sinadurak gordetzeko mekanismo gisa.

3.7. Atributu-ziurtagiriei buruzko konfiantza-arauak

Sinadura-politika honetan ez da arau zehatzik finkatu atributu-ziurtagiriei buruz.

Politika esparru honetan oinarrituta, EAEko erakunde edo entitate bakoitzaren sinadura-politika partikularrek ezarri ahal izango dituzte ematen dituzten zerbitzuentzako arau zehatzak. Betekizun horiek betetzea ezinbestekoa izango da sinadura baliozkotzat jotzeko testuinguru horretan.

3.8. Algoritmoak erabiltzeko arauak

Segurtasun-inguruneetan, oro har, onartutako sinadura-formatu gisa XadES zehaztapenean erabilitako hash funtzioak eta sinadura algoritmoak argitaratzen diren URN-ren (Uniform Resource Name) erreferentzia hartuko da, ETSI TS 102 176-1 sobre "*Electronic Signatures and Infraestructures (ESI); Algorithms and parameters for secure electronic signatures: Part 1: Hash functions and asymmetric algorithms"* zehaztapen teknikoen arabera*. Part 1: Hash functions and asymmetric algorithms*".

Sinadura-politika honek baliozkotzat jotzen ditu XMLDSig estandarrean definitutako hash sortzeko algoritmoak, 64baseko kodifikazioa, sinadura, normalizazio eta transformazioak.

Sinadura elektronikorako ondorengo algoritmoetatik edozein erabili ahal izango da: RSA/SHA1 (formatu hau algoritmo sendoagoagatik ordezkatzea gomendatzen da epe ertainean),

RSA/SHA256 eta RSA/SHA512. Azken hau, dokumentu elektronikoak artxibatzeko gomendatzen da (very long term signatures).

Denbora-zigiluak sortzeko, Denbora Zigilatzeko Autoritatea (*Time Stamping Authority* edo TSA) erabiltzen duten denbora zigilatzeko sistema bat erabiliko da. TSA-k zigilatu beharreko dokumentua jasotzen du, unean uneko data eta ordua gehitzen dio eta sinadura elektronikoko prozesua burutzen du kriptosistema elektroniko baten bitartez.

3.9. Konpromisoei buruzko arau espezifikoak

Sinadura-politika honek ez du konpromiso espezifikoei buruzko arau zehatzik finkatzen.

Politika esparru honetan oinarrituta, EAEko erakunde edo entitate bakoitzaren sinadura-politika partikularrek ezarri ahal izango dituzte ematen dituzten zerbitzuentzako arau zehatzak. Betekizun horiek betetzea ezinbestekoa izango da sinadura baliozkotzat jotzeko testuinguru horretan.

I. eranskina: Erreferentziak

Edukia garatzeko, kontuan izan dira zehaztapen tekniko hauek:

- ETSI TS 101 903, v.1.3.2. Electronic Signatures and Infrastructures (SEI); XML Advanced Electronic Signatures (XAdES).

- ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.

- ETSI TS 102 023, v.1.2.1 eta v.1.2.2.. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.

- ETSI TS 101 861 V1.3.1 Time stamping profile.

- ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.

- ETSI TR 102.041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.

- ETSI TR 102.045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.

- ETSI TR 102.272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.

- IETF RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

- IETF RFC 3125, Electronic Signature Policies.

- IETF RFC 3161, honek eguneratua: RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

- IETF RFC 5280, RFC 4325 eta RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.

- IETF RFC 5652, RFC 4853 eta RFC 3852, Cryptographic Message Syntax (CMS).

- ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

- CCN-STIC-807: IKT segurtasun-araua/-gida. Segurtasun Eskema Nazionaleko Enpleguko kriptologia.

Horiez gain, honako hauek gai honetan aplikatu beharreko oinarrizko arautzat jotzen dira:

- 1999/93/CE Zuzentaraua, Europako Parlamentuarena eta Kontseiluaarena, 1999ko abenduaren 13koa, modu elektronikoan sinatzeko erkidego-esparrua (aldizkari ofiziala, L 013 zenbakia, 2000/01/19koa, 0012-0020. orr.).

- 59/2003 Legea, abenduaren 19koa, sinadura elektronikoari buruzkoa.

- 11/2007 Legea, ekainaren 22koa, Herritarrek Zerbitzu Publikoetan Sarbide Elektronikoa izateari buruzkoa.

- 56/ 2007 Legea edo Informazioaren Gizartea sustatzeari buruzkoa.

- 1671/2009 Errege Dekretua, azaroaren 6koa, 11/2007 Legea partzialki garatzen duena (11/2007 Legea, ekainaren 22koa, herritarrek zerbitzu pulikoetara modu elektronikoan jotzeari buruzkoa).

- 3/2010 Errege Dekretua, urtarrilaren 8koa, Segurtasun Eskema Nazionala arautzen duena Administrazio Elektronikoaren eremuan.

- 4/2010 Errege Dekretua, urtarrilaren 8koa, Elkarreragingarritasun Eskema Nazionala arautzen duena Administrazio Elektronikoaren eremuan.

- 15/1999 Lege Organikoa, abenduaren 13koa, Datu Pertsonalak Babesteari buruzkoa.

- 1720/2007 Errege Dekretua, abenduaren 21ekoa, 15/1999 Lege Organikoa garatzeko erreglamendua onartzen duena (15/1999 Lege Organikoa, abenduaren 13koa, datu pertsonalak babesteari buruzkoa).

- 1/1996 Legegintzako Errege Dekretua, apirilaren 7koa, Jabetza Intelektualari buruzko Legearen Testu Bategina onartzen duena.

- 1553/2005 Errege Dekretua, abenduaren 23koa, arautzen duena nola eman nortasun-agiri nazionala eta horren sinadura elektronikoko ziurtagiriak.

- 11/200 Legearen ziurtagiri-profilak deskribatzea, sinadura-polika honi lotuta egongo baitira: Ziurtagiri-profilak, eskura dagoen aken bertsioakoak.

- 21/2012 Dekretua, otsailaren 21ekoa, Administrazio Elektronikoari buruzkoa.

- Agindua, 2012ko ekainaren 27koa, sinadura elektronikorako eta ziurtagirietarako politika onartzen duena.

II. eranskina: Sinadura elektronikoaren egitura

Eranskin honetan azaltzen da zer oinarrizko egitura sarraitu behar den XAdES-EPES sinadura elektronikoa sortzeko, ETSI TS 101 903 zehaztapen teknikoko 1.3.2. bertsioaren arabera.

Estandarraren hurrengo bertsietarako, aztertuko da zer aldaketa egin sintaxian, eta, estandar berriaren bertsiora egokitzea onartuko da, politikari eranskin bat gehituta.

XAdES-EPES sinadura elektroniko aurreratuaren formatua

dsig eta *xades* aurrizkiak erabiliko dira, XML-Dsig eta XadES estandarretan –hurrenez hurren– zehaztutako elementuak aipatzeko.

```
<dsig:Signature ID ? >
                        <dsig:SignedInfo>
                          <dsig:CanonicalizationMethod/>
                          <dsig:SignatureMethod/>
                          (<dsig:Reference URI ? >
                            (<dsig:Transforms/>) ?
                            <dsig:DigestMethod/>
                            <dsig:DigestValue/>
                          </dsig:Reference>) +
                        </dsig:SignedInfo>
                        <dsig:SignatureValue/>
                        (<dsig:KeyInfo>) ?
                        <dsig:Object>
                          <xades:QualifyingProperties>
                            <xades:SignedProperties>
                              <xades:SignedSignatureProperties>
                                xades:SigningTime
                                xades:SigningCertificate
                                xades:SignaturePolicyIdentifier
                                (xades:SignatureProductionPlace) ?
                                (xades:SignerRole) ?
                              </xades:SignedSignatureProperties>
                              <xades:SignedDataObjectProperties>
                                (xades:DataObjectFormat) +
                                (xades:CommitmentTypeIndication) *
                                (xades:AllDataObjectsTimeStamp) *
                                (xades:IndividualDataObjectsTimeStamp) *
                               </xades:SignedDataObjectProperties>
```

```
                    </xades:SignedProperties>
                    <xades:UnsignedProperties>
                        <xades:UnsignedSignatureProperties>
                            (xades:CounterSignature) *
                        </xades:UnsignedSignatureProperties>
                        <xades:UnsignedDataObjectProperties>
                        </xades:UnsignedDataObjectProperties>
                    </xades:UnsignedProperties>
                </xades:QualifyingProperties>
            </dsig:Object>
</dsig:Signature>
```

Hona “+”, “?” eta “*” ikurren esanahia:

- ✓ **+** : agerraldi bat edo gehiago
- ✓ **?** : agerraldirik ez edo agerraldi bat
- ✓ ***** : agerraldirik ez edo agerraldi bat

III. eranskina: Onartutako fitxategien formatua

EAEk herritarrekin eta beste herri-administrazioekin dituen harreman elektronikoak kudeatzeko erabiltzen diren plataformek onartu beharreko erreferentzia-fitxategiei buruzko baldintza orokor hauen bidez, ezarri nahi dira, batetik, kontsiderazio orokorrak, eta, bestetik, plataforma guztiek onartu beharko dituzten fitxategi-formatuen zerrenda, elkarreragingarritasuna errazteko. Dena dela, plataforma horiek beste formatu batzuk ere onartu ahal izango dituzte, kasuan kasuko premia zehatzen arabera.

Fitxategi-formatuen baldintza orokorren zerrenda osoa ezartzen du Elkarreragingarritasun Eskema Nazionala garatzeko arau-esparruak, betiere horren lehenengo xedapen gehigarriak ezartzen duenez.

Dokumentu elektronikoetarako onartutako formatuen zerrenda argitara eman da EAEko Herri Administrazioko egoitza elektronikoan, onartutako dokumentu elektronikoen atalean.

Kontsiderazio orokorrak

- ✓ Onartutako dokumentu elektronikoen formatuak hainbat sistema operatiboetan ikusi edo inprimatzeko, ez da beharrezkoa izan beharko lizentziarik izatea. Ahal den neurrian, formatu jabedunak saihestu behar dira; izan ere, ezin da bermatu enpresak bizirik irautea. Ildo horretatik, nazioarteko estadarrei atxikitzea behar-beharrezko baldintza da, dokumentua epe luzean eskuragarri egongo dela bermatzeko.

- ✓ Komenigarria da formatua eta haren bertsioa automatikoki egiaztatzeko aukera izatea, sisteman onartu baino lehenago, hau da, bakar-bakarrik onartu beharko dira fitxategiak, baldin eta makina batek horien formatua egiaztatu ahal badu Erregistro elektronikoak onartu baino lehen.

- ✓ Formatu egonkorrak baino ez dira onartu beharko, harrera ona izan, eta luzaroan irauten dutenak. Formatuak bilakatzean, aurreko formatuekin bateragarri izaten jarraitu beharko dute.

- ✓ Kanpo-dokumentuekin loturak dituzten dokumentuak saihestu behar dira; izan ere, zeinek bere edukiak baino ez ditu izan behar. XML formatuei lotutako balioztatze-eskemak, berriz, salbuespentzat joko dira.

- ✓ Kode gaiztoak sartzeko arriskua dagoenez, arreta bereziaz erreparatu beharko zaie kode exekutagarria duten formatuei, esaterako, makroei. Aurkezten den dokumentazioak ez du informatika-birusik izan beharko.