UPV/EHUren Nortasun eta Sinadura Elektronikoko Politika

eman ta zabal zazu

Universidad del País Vasco

Euskal Herriko Unibertsitatea

2024 uztaila

AURKIBIDEA

1. Sarrera eta xedea

Universidad del País Vasco/Euskal Herriko Unibertsitateak («UPV/EHU» edo «unibertsitatea», aurrerantzean) erabaki du Nortasun eta Sinadura Elektronikoko Politika hau («politika» edo «dokumentu hau», aurrerantzean) ezartzea, agerian utziz horrela haren konpromisoa sinadura elektronikoaren erabilerarekin, balio juridiko osoko dokumentu elektronikoen ekoizpenarekin eta dokumentu segurtasunaren ildo nagusiekiko errespetuarekin, erakundean administrazio elektronikoa ezartzeko estrategiaren barruan.

Beraz, politika honek arautzen ditu, unibertsitatearen eskumen esparruan eta aintzat harturik urtarrilaren 8ko 4/2010 Errege Dekretua (Administrazio Elektronikoaren eremuan Elkarreragingarritasunaren Eskema Nazionala arautzen duena) eta Administrazio Publikoen Estatu Idazkaritzaren 2016ko urriaren 27ko Ebazpena (Administrazioaren Sinadura eta Zigilu Elektroniko eta Ziurtagirien Politikaren Elkarreragingarritasunaren Arau Teknikoa onartzen duena):

- Dokumentu honen irismena eta aplikazio eremu subjektiboa.
- Politika hau kudeatzeaz eta garatzeaz arduratuko diren eragileen rolak eta erantzukizunak.
- Erakundearen dokumentu segurtasunaren ildo nagusiak.
- Erakundearen nortasun elektronikoaren jarraibide orokorrak.
- Ziurtagiri elektronikoak jaulkitzeko baimendutako hornitzaileak eta ziurtagiri horiek lortzeko eta kudeatzeko prozedurak.
- Onartutako sinadura elektronikoko sistemak eta formatuak.
- Sinadura elektronikoa erabiliko den kasuak.
- Dokumentuak eta sinadura elektronikoak babesteko estrategia.
- Politika hau mantentzeko eta garatzeko jarraibideak.

Testuinguru horretan, politika honen xedea da zehaztea unibertsitateak onartuko dituen ziurtagiri eta sinadura elektronikoen tipologia, bai haren organo eta unitateei dagokienez, bai unibertsitateko kide guztiei eta unibertsitatearekin harremanak dituzten hirugarrenei dagokienez, bai eta finkatzea ere haien erabilerak eta prozedurak, eskuratzeko metodoak eta epe luzera gordetzeko eta babesteko metodoak, helburua izanik bermatzea unibertsitatearen aplikazio korporatiboen bidez digitalki sinatutako dokumentuen egiazkotasuna, osotasuna eta kontserbazioa.

Zehazki, sinadura elektronikoaren eredua ezartzeak berekin dakar zehaztea zer ziurtagiri elektroniko onartuko diren eta zertarako. Beraz, politika honek zehazten du erabiliko

diren formatu teknikoen eta unibertsitateak sortutako edo onartutako sinadura moten zerrenda.

Halaber, definitzen dira aurretiko erregistroa duten identifikazio eta sinadura sistemak; zehazkiago, arautzen dira gako itunduetan gehi sinatzeko borondatearen ebidentzietan oinarritutako sinadura elektronikoko sistema eta bigarren autentifikazio faktorea duten gako itunduen sistema.

Bestetik, teknologia aurrerapenen eta araudiaren bilakaeraren ondorioz, beste sistema batzuk agertu dira, aukera ematen dutenak elektronikoki sinatzeko sinadura biometrikoa bezalako mekanismoen bidez. Horregatik, politika honek arautzen du ere sinadura digital biometrikoa, egokia presentzialki sinatzeko hirugarrenek sortutako dokumentu elektronikoak.

Amaitzeko, dokumentu honek ezartzen ditu UPV/EHUk sinadura elektronikoak epe luzera babesteko erabiliko dituen estrategiak.

Dokumentu hau egitean, kontuan hartu dira arlo honetan aplikatu beharreko araudiak (estatuz gaindikoa, estatukoa, autonomikoa eta unibertsitatearena berarena), nazioarteko estandarrak eta 3. atalean aipatutako beste konbentzio batzuk.

Nazioarteko estandarrak jaso dira dokumentu honen III. eranskinean.

2. Aplikazio eremu subjektiboa

Dokumentu hau aplikatuko zaie UPV/EHUrekin harremanetan dokumentu elektroniko ziurtatuak sortu edo trukatu behar dituzten pertsona eta erakunde guztiei.

Gainera, UPV/EHUko kide guztiei ere aplikatuko zaie, zuzendaritzako kideak barne, edozein izanik ere kontratu modalitatea, erakundearen hierarkian duten posizioa eta langunea, irakaskuntzan, ikerketan edo kudeaketan.

3. Arautegi aplikagarria

Dokumentu elektronikoaren erabileraren paradigma aldaketa etorri da araudian izan diren aldaketetatik. Aldaketa horiek bultzada eman diete tresna telematikoei, eta parekatu egin dituzte dokumentu elektronikoak eta formatu tradizionalagoak egoera jakin batzuetan. Bestetik, estandarizazio teknikoaz arduratzen diren erakundeek definitu eta dokumentatu egin dituzte dokumentu digitalak kudeatzeko erabiliko diren irizpideak eta formatuak, haien balio juridikoa bermatuta.

Atal honetan aletzen dira UPV/EHUren nortasun eta sinadura elektronikoko politika aplikatzeko arau esparrua, nazioarteko estandarrak eta erreferentziazko beste zenbait konbentzio.

3.1 Europako araudia

- 910/2014 (EB) Erregelamendua, Europako Parlamentuaren eta Kontseiluarena, 2014ko uztailaren 23koa, merkatuko transakzio elektronikoetarako identifikazio elektronikoari eta konfiantzazko zerbitzuei buruzkoa, 1999/93/EE Zuzentaraua indargabetzen duena (eIDAS erregelamendua, aurrerantzean)
- 2015/1506 (EB) Betearazpen Erabakia, Batzordearena, 2015eko irailaren 8koa, ezartzen dituena sektore publikoko erakundeek aitortu behar dituzten sinadura elektroniko aurreratuen eta zigilu aurreratuen formatuei buruzko zehaztapenak, aurretik aipatutako erregelamenduaren 27. artikuluaren 5. atalaren eta 37. artikuluaren 5. atalaren arabera.

3.2 Estatuko araudia

- 39/2015 Legea, urriaren 1ekoa, Administrazio Publikoen Administrazio Prozedura Erkidearena.
- 40/2015 Legea, urriaren 1ekoa, Sektore Publikoaren Araubide Juridikoarena.
- 6/2020 Legea, azaroaren 11koa, konfiantzazko zerbitzu elektronikoen zenbait alderdi arautzen dituena.
- 4/2010 Errege Dekretua, urtarrilaren 8koa, Administrazio Elektronikoaren esparruan Elkarreragingarritasun Eskema Nazionala arautzen duena.
- 203/2021 Errege Dekretua, martxoaren 30ekoa, sektore publikoko bitarteko elektronikoen bidezko jarduera eta funtzionamenduaren erregelamendua onartzen duena.
- 311/2022 Errege Dekretua, maiatzaren 3koa, Segurtasun Eskema Nazionala arautzen duena.

- Ebazpena, 2011ko uztailaren 19koa, Funtzio Publikoaren Estatu Idazkaritzarena, Dokumentu Elektronikoaren Elkarreragingarritasun Arau Teknikoa onartzen duena.
- Ebazpena, 2016ko urriaren 27koa, Administrazio Publikoen Estatu Idazkaritzarena, Sinadura eta Zigilu Elektronikoen eta Administrazio Ziurtagirien Politikako Elkarreragingarritasun Arau Teknikoa onartzen duena.
- Ebazpena, 2017ko uztailaren 14koa, Administrazio Digitalaren Idazkaritza Nagusiarena, interesdunek Estatuko Administrazio Orokorreko administrazio organoekin eta haren organismo publikoekin dituzten harremanetan sinadura elektroniko ez-kriptografikoa erabiltzeko baldintzak ezartzen dituena.

3.3 Autonomia erkidegoko araudia

- 3/2022 Legea, maiatzaren 12koa, Euskal Sektore Publikoari buruzkoa.
- 5/2022 Legea, ekainaren 23koa, Euskal Autonomia Erkidegoko Dokumentu Kudeaketa Integralari eta Dokumentu Ondareari buruzkoa.
- 232/2000 Dekretua, azaroaren 21ekoa, Artxibo Zerbitzuetako Araudia eta Euskal Autonomia Erkidegoko Dokumentazio Ondarearen arauak onartzen dituena.

3.4 Unibertsitatearen araudia

Nortasun eta sinadura elektronikoko politikak osatu eta garatu egiten du UPV/EHUren araudi orokorra:

- UPV/EHUren funtzionamendu eta jarduera elektronikoari buruzko araudia (2024).
- UPV/EHUren Dokumentuak Gestionatu eta Artxibatzeko Araudia (2024).
- UPV/EHUren dokumentu elektronikoak kudeatzeko politika (DEKP) (2024).

3.5 Nazioarteko estandarrak eta beste konbentzio batzuk

III. eranskinak biltzen ditu nazioarteko estandar guztien zerrenda eta dokumentu honetan aipatzen diren formatu, sinadura eta zigilu elektroniko motak eta gainerako teknologiak definitzen dituzten beste konbentzio batzuk.

4. Unibertsitatearen Nortasun eta Sinadura Elektronikoko Politikaren datuak

4.1 Politikaren identifikazioa

Dokumentuaren izena	UPV/EHUren Nortasun eta Sinadura Elektronikoko Politika
Bertsioa	1.0
Politikaren identifikatzailea	UPV/EHUren Nortasun eta Sinadura Elektronikoko Politika
Onarpen data	2024ko uztaila
Aplikazio eremua	Unibertsitateak sortutako edo zaindutako dokumentuak eta espedienteak
Politikaren arduraduna eta harremanetarako datuak	Eraldaketa Digitalaren eta Komunikazioaren arloko Errektoreordetza E-mail: Tel.:

5. Rolak eta erantzukizunak

Politika honek inplikatzen ditu unibertsitatearen hainbat arlo. Hona hemen haien rolak eta erantzukizunak:

5.1 Gobernu Kontseilua

- Politika onartzea.

5.2 Eraldaketa Digitalean eskumena duen organoa

- Politikaren alderdi funtzionalak zehaztea.
- Politika betetzeko soluzio egokiak zehaztea.
- Egiaztatzea politika betetzen den, unibertsitateko kideen benetako beharretara egokitzen den eta eskura dauden teknologiekin bat datorren.
- Politikaren bertsio eguneratuak Egoitza Elektronikoan argitaratzen direla bermatzea.
- Politika mantentzea eta eguneratzea.

5.3 Informazioaren eta Komunikazioen Teknologietan eskumena duen organoa

- Politikaren aplikazioaren alderdi teknikoak zehaztea.
- Plataforma eta soluzio teknologiko egokiak ezartzea eta mantentzea, politika betetzeko.

5.4 Arlo eta ikasketa guztiak

- Politika ezagutzea.
- Haren edukia betetzea.

6. Dokumentu segurtasunaren ildo nagusiak

Unibertsitateko sistema guztiei aplikatu beharreko ildo nagusi batzuk ezarri behar dira, bermatzeko unibertsitatean sortutako dokumentu elektroniko guztiak eta kanpotik jasotakoak egiazkoak eta legez baliozkoak direla, eta ezaugarri horiek epe labur eta luzera gordeko dituztela:

Nortasun elektroniko sendoa: aplikatutako sinadura elektronikoko soluzioek bermatu egin behar dute erabiltzaileen eta prozesuetan parte hartzen duten pertsonen identifikazio zehatza. Autentifikazio tresnetara sartzeko mekanismoek bermatu egin behar dute gutxieneko identifikazioa, eta kontrol batzuk behar dituzte, aurre egiteko iruzurrari edo zabarkeriari.

Dokumentu elektronikoen egiazkotasuna eta egiletza: sinadura elektronikoko soluzioek gai izan behar dute pertsona jakinei egozteko dokumentu elektronikoen eta horiei lotutako gainerako ekintzen egiletza. Beharrezkoa den guztietan, gai izan behar dute nahikoa berme emateko, dokumentu elektronikoaren hartzaileek haren egiazkotasunaren froga izateko eta arbuio arriskutik babestuta egoteko.

Dokumentu elektronikoen osotasuna: informazioaren segurtasun soluzioen mekanismoek aukera eman behar dute egiaztatzeko jada igorri diren dokumentu elektronikoak ez direla aldatu edo ordeztu.

Dokumentuak babestea: dokumentu eta sinadura elektronikoak sortu behar dira formatu egokietan, epe luzera babestuta egongo direla ziurtatzeko mekanismoekin, egiazkotasun eta osotasun helburuak betez beti.

Proportzionaltasuna: prozesu bakoitzari aplikatutako segurtasun mekanismoak egokitu behar dira jarduera mota bakoitzaren behar eta arriskuetara, tresnak eraginkortasunez erabiltzea eragotziko duen neurri edo kontrol zorrotzegirik gabe.

Erabilgarritasuna: ahal denean, aukeratuko dira zerbitzu teknologikoak erraz, azkar, intuitiboki eta era atseginean erabiltzeko aukera emango duten soluzioak, identifikazio, egiazkotasun, osotasun eta babes elementuei eragin gabe.

7. Unibertsitatean onartutako nortasun elektronikoa

Harreman telematiko batean, beharrezkoa da parte hartzen duten alde guztiak modu seguruan eta egiazkoan identifikatzea. Ondorioz, nortasuna elektronikoki egiaztatzeko bitarteko hauek onartzen ditu unibertsitateak:

1. **Aitortutako edo kualifikatutako ziurtagiri elektronikoetan oinarritutako identifikazio sistemak**, dagokion Ministerioaren konfiantzazko zerbitzu elektronikoen emaileen zerrendan jasotako agintari batek emandakoak.

2. **Ziurtagiri elektroniko ez-kualifikatuetan oinarritutako identifikazio sistemak**, dagokion Ministerioaren konfiantzazko zerbitzu elektronikoen emaileen zerrendan jasotako agintari batek emandakoak.

3. **Zigilu elektronikoko aitortutako edo kualifikatutako ziurtagiri elektronikoetan oinarritutako identifikazio sistemak**, dagokion Ministerioaren konfiantzazko zerbitzu elektronikoen emaileen zerrendan jasotako agintari batek emandakoak.

4. **Bitarteko biometrikoen bidezko identifikazio sistemak**. Aukera ematen dute pertsona baten nortasuna erregistratzeko edo baliozkotzeko, haren datuak elektronikoki egiaztatuta; hala nola hatz marka, eskuz idatzitako sinadura edo biometrian oinarritutako beste datu batzuk. Sistema hauek erabiltzeko, gai izan behar da sinatzailearen datu pertsonalak modu konfidentzialean zifratzeko.

5. **Unibertsitatearen beraren identifikazio sistemak, aurretiko erregistroan oinarrituak** (erabiltzailea eta pasahitza).

8. Ziurtagiri elektronikoak

8.1 Unibertsitateak erabilitako ziurtagiri elektronikoak

Aurreko ataletan ezarritakoa betetze aldera, atal honetan aipatzen dira unibertsitateak onartuko dituen ziurtagiri digital motak. Ziurtagiri hauek erabiliko dituzte UPV/EHUko kideek (irakasle-ikertzaileek eta TEKAZEL langileek) eta unibertsitatea hirugarrenen aurrean ordezkatuko duten pertsonek, eta erabiliko dira ere administrazio jardun automatizatuan eta maila teknikoan.

Unibertsitateko langileak

UPV/EHUko langileek erabili behar dute unibertsitatearen sinadura elektronikoko sistema korporatiboa, eta sistema horren ziurtagiri elektronikoak balio du identifikatzeko eta sinatzeko UPV/EHUko langile gisa egin behar dituzten izapide edo jarduera guztietan. Sistema horri deitzen zaio ziurtagiri profesionala:

Ziurtagiri profesionala: unibertsitatearen konfiantzazko zerbitzu elektronikoen emaile kualifikatuak emandako ziurtagiri pertsonala, jasotzen dituena pertsonaren nortasun datuak eta lan egiten duen erakundearekiko (kasu honetan, UPV/EHU) lotura datua. Unibertsitateko erregistro agintariak arduratzen dira unibertsitateko langileen ziurtagiria emateaz eta baliogabetzeaz.

Unibertsitatearen ordezkari diren langileak

Langileek ordezkari ziurtagiria erabiliko dute unibertsitatearen lege ordezkari gisa aritzean (estatutu eskumenekin), haien karguaren arabera bakarrik egin daitezkeen jardueretan:

Ordezkari ziurtagiria: unibertsitatearen konfiantzazko zerbitzu elektronikoen emaile kualifikatuak emandako ziurtagiri pertsonala, erabil dezaketena bakar-bakarrik hirugarrenen aurrean unibertsitatea ordezkatzeko eskumena duten pertsonek. Pertsonaren nortasun datuak eta unibertsitatearenak biltzen ditu. Eraldaketa Digitalean eskumena duen organoa arduratzen da ziurtagiri mota hau emateko eta baliogabetzeko eskabideak kudeatzeaz.

Ziurtagiri teknikoak

Zigilu elektronikoko ziurtagiriak: 40/2015 Legearen 42. artikuluaren arabera administrazio jarduera automatizatua baimentzen duen ziurtagiria. Ziurtagiri mota hau erabil daiteke kopia elektronikoak egiteko, espedienteak orrialdekatzeko eta langile publikoen esku hartzerik behar ez duten dokumentuak sortzeko. UPV/EHUk zigilu ziurtagiri bat du, unibertsitatearen konfiantzazko zerbitzu elektronikoen emaile kualifikatuak emandakoa. Eraldaketa Digitalean eskumena duen organoa arduratzen da ziurtagiri mota hau emateko eta baliogabetzeko eskabideak kudeatzeaz.

Aplikazio ziurtagiriak: balio dute aplikazioak, zerbitzariak, sistemak edo web zerbitzuak identifikatzeko, edo datuak trukatzeko administrazioen eta herritarren artean, edo administrazioen eta enpresen artean. Ziurtagiri mota hau erabiltzen da osotasuna eta egiazkotasuna bermatu behar diren mezuak bidaltzen dituzten aplikazioetan, eta ez du inolako ondorio juridikorik. Informazioaren eta Komunikazioaren Teknologien ardura duen organoa arduratzen da ziurtagiri hauek emateko eta baliogabetzeko eskabideak kudeatzeaz.

Zerbitzari seguruko ziurtagiriak: erakundearen izapidetze telematikoko inguruneetan sarbide segurua bermatzen duten ziurtagiriak; hala nola unibertsitatearen egoitza elektronikoan edo webguneetan. UPV/EHUk egoitza ziurtagiri bat du, unibertsitatearen konfiantzazko zerbitzu elektronikoen emaile kualifikatuak emandakoa, eta ez du inolako ondorio juridikorik sortzen. Eraldaketa Digitalean eskumena duen organoa arduratzen da ziurtagiri mota hau emateko eta baliogabetzeko eskabideak kudeatzeaz.

Dokumentu honen II. eranskinean aipatzen dira unibertsitateak kasu bakoitzean onartutako teknologia eta hornitzaile zehatzak. Eraldaketa Digitalean eta Komunikazioan eskumena duen organoak eguneratu egingo du II. eranskinaren edukia, aintzat harturik teknologiaren edo emaile bakoitzak ziurtatzeko dituen praktiken bilakaera.

8.2 Unibertsitatean ziurtagiri elektronikoa izateko baimena duten pertsonak

Unibertsitateko langile publiko guztiek izan behar dute ziurtagiri profesionala, unibertsitateak kudeatua eta unibertsitatearen zerbitzuen emaile kualifikatuak emandakoa, kontuan harturik 8.4.1 atalean ezarritako prozedura. Zehazki:

- Unibertsitateko langile guztiek erabili behar dute unibertsitatearen ziurtagiri profesionala, beren burua identifikatzeko edo sinatzeko, unibertsitateko langile gisa dagozkien zereginetan. Unibertsitateko langilearen erantzukizuna da bere ziurtagiria indarrean egotea.
- Karguagatik edo izendapenagatik unibertsitatearen ordezkari diren pertsonek eduki ahal izango dute ordezkari ziurtagiri elektroniko bat, II. eranskinean jasotako tipologien arabera.

Unibertsitatearekin lotura duten gainerako pertsonek edo unean-unean unibertsitatearekin kolaboratzen duten hirugarrenek erabili ahal izango dute pertsona fisikoen ziurtagiri bat edo, behar izanez gero, lortu ahal izango dute unibertsitatearekiko lotura ziurtagiri elektroniko bat, haren beharra justifikatuta, hierarkian gorago dagoen pertsonaren edo dagokion zerbitzuaren arduradunaren bitartez, eta Koordinazioan eskumena duen unibertsitateko organoak baliozkotu eta onartu beharko du.

8.3 Unibertsitateak onartutako ziurtagiri elektronikoak

Unibertsitateak herritarrekiko harremanetan onartzen dituen ziurtagiri elektronikoei dagokienez, bi kasuistika nabarmendu behar dira.

8.3.1 Ziurtagiri kualifikatuetan oinarritutako ziurtagiriak

Unibertsitatearekin harremana duten pertsonek erabili ahal izango dituzte Ministerio eskudunak osatutako konfiantzazko zerbitzu elektronikoen emaileen zerrendan (TSL) jasotako ziurtagiriak, beren burua identifikatzeko eta dokumentazioa euskarri digitalean elektronikoki sinatzeko.

Zerrenda hori kontsultatzeko: https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx

8.3.2 Ziurtagiri ez-kualifikatuetan oinarritutako ziurtagiriak

Unibertsitatearekin harremana duten pertsonek erabili ahal izango dituzte Ministerio eskudunak osatutako konfiantzazko zerbitzu elektronikoen emaileen zerrendan (TSL) jasotako ziurtagiria ez-kualifikatuak.

Zehazki, kritikotasun baxuko transakzio edo izapideetan, unibertsitateak Bak ziurtagiri ez-kualifikatua onartuko du identifikazio eta sinadura elektronikorako bitarteko gisa, unibertsitatearen konfiantzazko zerbitzu elektronikoen emaile kualifikatu batek emandakoa.

8.4 Ziurtagiri elektronikoen bizi zikloari lotutako prozedurak

8.4.1 Eskuratzea, berritzea eta baliogabetzea

Eraldaketa Digitalean eskumena duen organoari dagokio prozedura batzuk ezartzea unibertsitatean erabiltzen diren ziurtagiriak eskuratzeko, berritzeko eta baliogabetzeko.

Prozedura horiek ofizioz berrituko dira, beharrezkoa izanez gero araudian edo teknologian izandako aldaketengatik.

Unean-unean indarrean egongo diren prozedurak eskuragarri egongo dira langile guztientzat, dagokion arloan, Intraneten edo Langileen Atarian.

Zeregin hauetarako prozedurak ezarriko dira gutxienez:

- UPV/EHUren ordezkari ziurtagiria lortzea.
- UPV/EHUren ziurtagiri profesionala lortzea.
- Zigilu elektronikoko ziurtagiria lortzea.
- Ziurtagiri elektronikoa baliogabetzea.
- Ziurtagiri elektronikoa berritzea.

8.4.2 Ziurtagiri elektronikoak gordetzea

Unibertsitatearen ziurtagiri elektronikoak gordailu hauetan daude:

Txartel kriptografikoan.

Zerbitzari seguruko eta zigilu elektronikoko ziurtagirietarako zerbitzarien gordailu kriptografikoan.

Softwarean.

Unibertsitatearen konfiantzazko zerbitzu elektronikoen emaile kualifikatuaren hodei zentralizatu eta seguruan.

8.4.3 Unibertsitatearen ziurtagiri elektronikoen inbentarioa mantentzea

Unibertsitatearen ziurtagiri elektronikoen inbentarioa mantentzea dagokio unibertsitatearen konfiantzazko zerbitzu elektronikoen emaile kualifikatuari (unibertsitate ziurtagiriak ematen dituena), eta unibertsitateak aukera izango du informazio hori eskuratzeko.

9. Unibertsitatean onartutako sinadura elektronikoko sistemak

Dokumentu elektronikoak egiazkotzat hartzeko eta balio juridikoa izateko, elektronikoki sinatuta egon behar dute. Sinadura elektronikoa autentifikazio tresna bat da eta dokumentuaren osotasuna ziurtatzen du.

Ondorioz, unibertsitateak onartzen ditu sinadura elektronikoko bitarteko hauek:

1. **Ziurtagiri elektroniko ez-kualifikatuetan oinarritutako sinadura elektronikoko sistemak (pertsona fisikoa)**, dagokion Ministerioaren konfiantzazko zerbitzu elektronikoen emaileen zerrendan jasotako agintari batek emandakoak. Segurtasun maila txikiko sinaduretan erabiltzen da.

2. **Ziurtagiri elektroniko aitortuetan edo kualifikatuetan oinarritutako sinadura elektronikoko sistemak (pertsona fisikoa, profesionala edo ordezkaria)**, dagokion Ministerioaren konfiantzazko zerbitzu elektronikoen emaileen zerrendan jasotako agintari batek emandakoak.

3. **Zigilu elektronikoko aitortutako edo kualifikatutako ziurtagiri elektronikoetan oinarritutako sinadura elektronikoko sistemak**, dagokion Ministerioaren konfiantzazko zerbitzu elektronikoen emaileen zerrendan jasotako agintari batek emandakoak. Sinadura mota hau erabiliko dute soilik administrazio publikoek.

4. **Sinadura elektroniko biometrikoko sistemak**. Sistema hauek erabiliko dira soilik sinadura elektroniko biometrikoa unibertsitatean bertan sortu denean, sinadura elektronikoko politika honen 10.5 artikuluaren arabera.

5. **Gako itunduetan gehi sinatzeko borondatearen ebidentzietan oinarritutako sinadura elektronikoko sistemak** (erabiltzailea eta pasahitza). Sistema hauek erabiliko dira soilik aurretiko erregistroan oinarritutako unibertsitatearen sinaduretan, sinadura elektronikoko politika honen 10.3 eta 10.4 artikuluen arabera.

6. **Egiaztapen kode seguruan (SVC) oinarritutako sinadura elektronikoko sistemak**. Sistema hauek erabiliko dira soilik sinadura administrazio publiko batek sortu badu eta bere sinadura politikan jaso badu SVC sistema dela sinadura elektronikoko sistema bat. Hala, dokumentu sinatua jasoko duten unibertsitate langileek joko dute administrazio publiko jaulkitzailearen Egoitza Elektronikora, dokumentuaren osotasuna egiaztatzera.

10. Unibertsitatean erabilitako sinadura elektronikoko sistemak

Atal honetan aipatutako sinadura elektronikoko sistemak erabil daitezke unibertsitatearen aplikazio korporatiboetan, digitalki sinatutako dokumentuen egiazkotasuna, osotasuna, aldaezintasuna eta kontserbazioa bermatzeko. UPV/EHUko langileek beste erakunde baten prozeduretan parte hartzean, zehaztutako formatuetan sortuko dituzte sinadurak. Gainera, kopia gehitu behar bazaio unibertsitatearen espedienteari, aplikatuko dira IV. eranskinean jasotako egiaztapenak.

10.1 Ziurtagiri elektroniko pertsonal bidezko sinadura elektronikoa (profesionala, ordezkariarena edo pertsona fisikoarena)

Sinadura elektronikoko sistema honetan, abiatuta pertsona baten ziurtagiriaren gako pribatutik, sinatu beharreko dokumentuaren laburpen kriptografikoa zifratzen da, eta sinatzeko erabilitako ziurtagiriaren informazioa gehitu; adibidez, sinadura data edo nortasun eta sinadura elektronikoko politikaren erreferentzia.

UPV/EHUko langileek sistema hau baliatuko dute dokumentu elektronikoak sinatzeko, horretarako erabiliz unibertsitatearen konfiantzazko zerbitzu elektronikoen emaile kualifikatuak emandako ziurtagiri profesionala edo ordezkari ziurtagiria.

10.2 Zigilu elektronikoko sinadura elektronikoa administrazio jarduera automatizatuaren bidez

Sistema honen bidez sina daitezke unibertsitatearen dokumentu elektronikoak, prozesu automatizatuen bitartez, langileen esku-hartze zuzenik gabe.

Abiatuta zigilu elektronikoko ziurtagiri elektroniko baten gako pribatutik, sinatu beharreko dokumentuaren laburpen kriptografikoa zifratzen da, eta sinatzeko erabilitako zigilu elektronikoko ziurtagiriaren informazioa gehitu; adibidez, sinadura data edo nortasun eta sinadura elektronikoko politikaren erreferentzia.

Sinadura mota hau erabili ahal izango da unibertsitateko idazkari nagusiaren erabaki bidez ezarritako administrazio jardun automatizatuetan, aintzat harturik 40/2015 Legearen 41.2 artikulua, egoitza elektronikoan argitaratuko dena.

10.3 Gako itunduetan gehi sinatzeko borondatearen ebidentzietan oinarritutako sinadura elektronikoa

Itundutako gakoak gehi sinatzeko borondatearen ebidentziak erabiltzean datzan sinadura elektronikoko sistema oinarritzen da unibertsitateak emandako erabiltzailearen eta pasahitzaren bidez eginiko sinatzailearen identifikazioan (autentifikazioaren lehenengo ebidentzia da).

Sistema honen erabilgarritasuna izango da unibertsitatearen nortasunak banatzeko mekanismoaren kalitatearen araberakoa. Ondorioz, era honetako sinadurak sortzeko erabili beharreko kredentzialak lortzeko prozedurek bermatu behar dute:

Unibertsitateko langileak pertsonaren nortasuna behar bezala egiaztatzea, kredentzialak eman aurretik, bestela ezin izango delako erabili gako bikotea sinadurak sortzeko, eta hori egiaztatuta geratuko da kredentzialak kudeatzeko sisteman (inguruabar hori jasota uzteko gaitasuna izan beharko du). Nortasuna ondoren egiaztatzeak aukera emango du kredentzialak baliozkotzeko, etorkizunean sinadura mekanismo gisa erabiltzeko.

Kredentzialak kudeatzeko sistemek bermatzea kredentzialak modu seguruan zaintzea, unibertsitatearen segurtasun politiketan ezarritako aldien arabera berritzea eta kredentzialaren blokeoa eragin dezaketen identifikazio saiakera hutsen kopurua kontrolatzea, iruzurrezko erabilera prebenitzeko.

Erabiltzaileek informazio egokia jasotzea kredentzialen sistemaren kritikotasunari eta gakoen konfidentzialtasunaren garrantziari buruz.

Sinadura prozesuan, sinatzaileak eman beharko du sinatzeko baimen esplizitua (dagokion aplikazioan botoi bat sakatuta izan daiteke).

Identifikazioaren sendotasuna bermatzeko neurri gehigarri gisa, erabiltzaileari eska dakioke identifikazio erronka bati erantzuteko: hala nola erabilera bakarreko kode bat bidaltzea posta elektronikoko helbide batera edo aurretik erregistratutako gailu mugikor batera. Neurri hori hartzen da gako bikotearen neurriaren osagarritzat, eta identifikazio faktore bikoitz bat da.

Behin nortasuna egiaztatuta, ebidentzien fitxategi bat sortuko da, dokumentu elektroniko berean gordeko dena. Teknikoki ezinezkoa bada, ebidentziak gordeko dira unibertsitatearen sistema korporatiboetan, eta gordeko diren leku zehatzaren berri emango da administrazio prozeduraren beraren definizioan.

Beraz, gako itunduen gehi sinatzeko borondatearen ebidentzien bidez eginiko sinadura elektronikoko sistemaren balio juridikoa lotuta dago dokumentu elektronikoari eta sinadura onartzen duen sinatzailearen identifikazio prozesuaren ebidentziei.

Administrazio prozedurak hala eskatzen badu, erabili ahal izango dira autentifikazio ebidentzia bikoitz edo hirukoitzeko sistemak, eta faktore horiekin loturiko ebidentziak ere gorde ahal izango dira.

Baliteke dokumentu elektronikoak izatea gako itunduetan gehi sinatzeko borondatearen ebidentzietan oinarritutako sinadura elektroniko bat baino gehiago. Normalean, hori gertatzean, sinadura guztiak izango dira “detached” (bereizita) motakoak, guztiak formatu berean biltegiratzeko baldintzarik gabe, baldin eta bermatu badaiteke sinadura bakoitzaren egiazkotasuna ziurtatzeko aukera.

Gatazkarik sortuz gero dokumentu elektronikoaren sinaduren artean, unibertsitateak akreditatu ahal izango du:

Sinatzeko prozedura espezifikoki araututa dagoela.

Ebidentziak sortu direla mota bereko sinadura guztietan.

Sinadura une jakin batean egin zela, denbora zigilu bat aplikatuz.

Dokumentua ez dela aldatu "hash"-a aplikatuta dokumentuaren ebidentzietan.

Bigarren mailako sinadura bat aplikatu zaiola unibertsitatearen zigilu elektronikoko ziurtagiri bat aplikatzean oinarritutako dokumentu elektronikoari.

10.4 Bigarren autentifikazio faktorearen osagarria

Pertsonaren nortasuna baieztatzen da mezu elektroniko bat bidalita pertsona horri lotuta dagoen helbide elektroniko batera edo, bestela, SMS mezu bat jasota pertsona horren izenean erregistratuta dagoen telefono mugikor batean. Mezu horrek du OTP (One-Time Password) izeneko erabilera bakarreko pasahitz bat.

Azpimarratu behar da garrantzitsua dela erregistratuta egotea pertsonaren eta pasahitza jasotzen den baliabidearen arteko lotura, aurreko egiaztapen batean oinarrituta. Ezin izango da erabili sinadura mekanismo hau baieztapen kodea bidaltzen bada erabiltzaileak unean berean ematen duen helbide edo telefono batera.

Sinadura prozesuan, erabiltzaileak gainditu egingo ditu nortasun erronkak, mezu elektronikoa lehen aipatutako helbidean jasoz edo testu mezuan oinarritutako identifikazio erronka bati erantzunez. Sistema hori osagarria bada gako itunduen kredentzial bidez aplikazioan eginiko erabiltzailearen identifikazioarekin, bi mekanismoen konbinazioa autentifikazio faktore bikoitza da.

Behin nortasuna egiaztatuta, ebidentzien fitxategi bat sortuko da, dokumentu elektroniko berean gordeko dena. Teknikoki ezinezkoa bada, ebidentziak gordeko dira unibertsitatearen sistema korporatiboetan, eta gordeko diren leku zehatzaren berri emango da administrazio prozeduraren beraren definizioan.

Ebidentziak erantsi ondoren, sinatu egingo da dokumentu elektronikoa edo ebidentzien paketea (horiek ezin izan badira sendotu), zigilu elektronikoko ziurtagiri elektroniko bat erabiliz, unibertsitatearen izenean.

Atzeman beharreko ebidentziek honako hauek jasoko dituzte gutxienez:

- Sinatzailearen izena eta identifikazio kodea (IFZ edo antzekoa).
- Sinatutako dokumentuaren izenburua eta laburpen kriptografikoa.
- Sinaduraren data eta ordua.
- Sinatzailea identifikatzeko modua (erabiltzaile izena edo alegatutako nortasuna).

- Erronka gehigarria bidali den helbide elektronikoa edo telefono zenbakia.
- Erronka arrakastaz gainditu dela egiaztatzea.
- Sinadura kudeatzen duen izapidetze sistemaren identifikazioa.
- Erabiltzailea konektatzeko erabiltzen den IP helbidea.

Beraz, OTP gehi sinatzeko borondatearen ebidentzien bidez eginiko sinadura elektronikoaren balio juridikoa lotuta dago, alde batetik, dokumentuari eta, bestetik, sinaduraren onarpenarekin sinatzen duen pertsonaren identifikazio prozesuaren ebidentziei.

Sinadura formatu honetan, egon daiteke mota honetako sinadura bat baino gehiago dokumentuan, eta paraleloan sortu behar da.

Gatazkarik sortuz gero dokumentu elektronikoaren sinaduren artean, unibertsitateak akreditatu ahal izango du:

- Sinatzeko prozedura espezifikoki araututa dagoela.
- Ebidentziak sortu direla edozein motatako sinadura guztien artean.
- Sinadura une jakin batean egin zela, denbora zigilua aplikatuta.
- Dokumentua ez dela aldatu "hash"-a aplikatuta dokumentuaren ebidentzietan.
- Bigarren mailako sinadura bat aplikatu zaiola unibertsitatearen zigilu elektronikoko ziurtagiri bat aplikatzean oinarritutako dokumentu elektronikoari.

10.5 Sinadura elektroniko biometrikoa

Sinadura elektroniko aurreratuko sistema hau sortzen da sinatzailearen datu biometrikoetatik. Datu horiek txertatzen dira sortutako dokumentu elektronikoen laburpen kriptografikoan, modu zifratuan, eta aukera ematen dute egiaztatzeko aplikatutako sinaduraren auditoretza, informazio honen bidez:

Dokumentua eskuz sinatzen duen pertsonaren datu biometrikoak, biltzen direnak dokumentua sinadura ekitaldian bertan bistaratzeko aukera ematen duten atzemate elementu espezifikoen bidez. Besteak beste:

- Denbora xehetasunak; dokumentua sinatzeko prozesuaren hasiera, amaiera eta iraupena (milisegundotan).
- Trazaduraren xehetasunak, haren abiadurari, azelerazioari eta presioari dagokienez (irudi osoan).

Sinadura prozesurako garrantzitsua izan daitekeen beste informazio bat; hala nola sinadura atzemateko erabilitako aplikazioak eta programak identifikatzea edo sinadura jasotzeko erabilitako makinen GPS kokapena.

Sinadura elektroniko aurreratuko sistema hau soilik erabiltzen da eskuzko sinaduraren biometrian, beste neurri biometrikorik erabili gabe; hala nola aurpegi errekonozimendua edo hatz markaren erabilera (bi-biak politika honen eremutik kanpo), alde batera utzi gabe etorkizunean horiek kontuan hartzeko aukera.

Informazioa zifratzen da unibertsitateko zerbitzarietan gordetzen den sinadura elektroniko biometrikoko ziurtagiri espezifiko baten gako publikoaren bidez. Gako pribatua zainduko du konfiantzazko hirugarren batek eta, beharrezkoa denean, eskatu ahal izango zaio sinadura biometrikoak egiaztatzeko, erreklamaziorik edo auzirik egonez gero.

Dokumentu batek izan ditzake sinadura biometriko bat baino gehiago, baina beti elkarren paraleloan.

Behin sinadura biometriko guztiak paraleloan eginda eta atal honen hasieran aipatutako informazioa zifratuta, informazio hori gordeko da dokumentuarekin batera, eta dokumentuaren osotasuna bermatzeko, dokumentuaren gainean egingo da zigilu elektronikoko sinadura elektroniko automatiko bat (unibertsitatearen zigulua), denbora zigilu batez osatua.

Ondorioz, sinadura elektroniko biometrikoaren balio juridikoa lotuta egongo da dokumentuari eta dokumentuaren barruan modu zifratuan gordetzen diren ebidentzia biometrikoei, sinadura elektronikoa eta denbora zigilua aurkeztuta, agerian uzteko haren osotasuna.

Gatazkarik sortuz gero, zifratze ziurtagiriaren gako pribatua zaintzen duen konfiantzazko hirugarrenak datuak deszifratu ondoren, eskatuko da dokumentuan gordetako datu biometrikoen peritaje bat egiteko, alderatzeko antzeko baldintzetan (sinadura eztabaidagarrian erabilitako makinari, aplikazioei eta programei dagokienez) ustez datuak dagozkion pertsonari hartutako datu biometriko berriekin.

10.6 Sinadura anizkoitza

Sinadura anizkoitza gertatzen da dokumentu berean bi sinadura elektroniko edo gehiago daudenean. Sinadurak egin daitezke modu sekuentzialean edo paraleloan:

Sinadura sekuentziala: bigarren sinadura egiten denean aurretik sinatutako objektu digitalaren gainean. Ahal dela, ez da sinadura sekuentziala erabiliko dokumentu elektronikoak aldi berean hainbat pertsonak helburu berarekin sinatu behar dituzten sinadura zirkuituetan.

Sinadura paraleloa: sinadurak laburpen kriptografiko bakarra duen objektu digital berari dagozkionean, dela “detached” (bereizita) formatuan sortu direlako, dela dokumentua “attached” (erantsiak) sinadurak paraleloan jasotzeko prestatuta dagoelako.

Sinadura anizkoitza hainbat zereginetan erabiliko da unibertsitatearen administrazio prozeduren barruan; hala nola pertsona batek baino gehiagok dokumentu elektronikoak sinatzean edo sinadura elektronikoaren baliozkotasun kriptografikoa zalantzan jarri ahal izatearen aurretik sinatutako dokumentuak birzigilatzean, denboran zehar haren legezko baliozkotasuna eguneratzeko helburuarekin.

Ahaleginduko da antzeko teknologiak erabiltzen pertsona batek baino gehiagok dokumentu elektronikoak sinatu behar dituzten kasuetan, eta bereziki saihestuko da dokumentuak sortzea sinatuta, alde batetik, ziurtagirietan oinarrituta eta, bestetik, sinadura biometrikoa erabilita.

Sinadura elektronikoko sistemak konbinatu ahal izango dira kasu hauetan:

Sinadura elektronikoak, ziurtagiri elektronikoak era paraleloan edo modu sekuentzialean erabilita, sinadura bat baino gehiago behar dituen edozein dokumentu elektronikotan.

Sinadura elektroniko biometrikoak, modu sekuentzialean sortuak, hirugarrenen aurrean aurrez aurre sortzen diren eta bi sinadura edo gehiago behar dituzten dokumentu elektronikoetan.

Sinadura elektroniko biometrikoa eta, ondoren, ziurtagiri elektroniko bidezko sinadura elektronikoa (inbrikatua), hirugarren baten aurrean sortzen diren euskarri elektronikoko dokumentuen kasuan, baldin eta, biometrian oinarrituta sinatu ondoren, gerora sinadura elektronikoa behar badute baliozkotasuna osatzeko, zigilu elektroniko bidez.

> Garrantzitsua da ziurtatzea sinadura ez-kriptografikoaren ebidentziak behar bezala gordetzen direla eta azkenean eransten den zigilu elektronikoak dokumentuaren eduki osoa hartzen duela.

Sinadura elektronikoak gako itunduetan oinarritutako sistemen bidez, modu paraleloan edo sekuentzialean, sinadura bat baino gehiago behar dituzten dokumentu elektronikoetan.

Sinadura elektronikoa gako itunduetan oinarritutako sistema baten bidez, eta, ondoren, sinadura elektroniko bat aplikatzea ziurtagiri elektroniko baten bitartez, modu paraleloan edo sekuentzialean, bi pertsonaren sinadura behar duten dokumentu elektronikoetan, horietako batek bakarrik duenean ziurtagiri elektronikoa.

Oro har, ahaleginduko da pertsona guztiek antzeko teknologiak erabil ditzaten dokumentua hainbat pertsonak sinatu behar dutenean (saihestuko da dokumentuak sortzea sinatuta, alde batetik, ziurtagirietan oinarrituta eta, bestetik, sinadura biometrikoa erabilita).

10.7 Denbora zigilua

Denbora zigilua da konfiantzazko hirugarren batek sortutako sinadura elektroniko mota bat, horretarako bereziki sortutako ziurtagiri elektroniko batean oinarrituta, eta ziurtagiri horrek egiaztatzen du egintza zein egun eta ordutan gertatu den. Zehazki:

Dokumentua sinatzeko unea; kasu honetan, denbora zigilua lotuta egongo da aplikatutako sinadura elektronikoarekin.

Dokumentua sortzeko unea; kasu honetan, denbora zigilua lotuta egongo da dokumentu elektronikoarekin.

Sinadura elektroniko mota honek egintza unearen data eta ordua zigilatzen ditu denbora zigilu hornitzaile baten bidez, normalean izango dena unibertsitatearen konfiantzazko zerbitzu elektronikoen emaile kualifikatuaren denbora zigilatzearen zerbitzu kualifikatua.

Denbora zigilua erabiltzeko prozedura datza sinadura elektroniko baten inguruko ebidentzia bat sortzean, dokumentuaren edo sinadura elektronikoen (birzigilatze kasuan) laburpen kriptografikoa kalkulatuta. Hau da, eragiketa matematiko bat egiten da eta aplikatzen zaio informazio multzoari. Informazio horri ezartzen zaio "hash" izeneko bit kate batean sortzen den denbora zigilua, eta zifratzen da eragiketa horretarako erabilitako denbora zigiluaren ziurtagiriaren gako pribatuarekin.

Denbora zigiluaren ziurtagiria aplikatzearen ondorioz, eragiketaren data eta ordua sartzen dira dokumentu elektronikoan, bai eta hura sinatzeko erabilitako denbora zigiluaren ziurtagiriari buruzko informazioa ere.

11. Ziurtagirietan oinarritutako sinadura elektronikoen formatuari buruzko baldintza komunak

Baldintza batzuk bete behar dira unibertsitateak ziurtagiri elektronikoetan oinarritutako sinadura sistemak erabiltzean:

Ziurtagirietan oinarritutako sinadurak erabiltzean, ahal dela "PAdES" motakoak izango dira, ***attached*** (erantsita) sinadura gisa sor daitezkeenean PDF formatuko dokumentu batean; beste kasu batzuetan, dokumentua XML bada, erabiliko da ***attached*** sinadura XAdES formatuan, eta gainerako kasuetan, ***detached*** (bereizia) sinadura XAdES formatuan.

Oro har, sinadurek izan beharko dute denbora zigilua, nahiz eta lau urtetik gorako zaintza denbora duten dokumentuen formatua izango den artxibokoa.

Hona hemen erabili beharreko sinadura formatuak, taula batean bilduak:

	Oro har, denbora zigiluarekin	**Epe luzera gorde beharreko dokumentuak**
Ahal bada, *attached* sinadura (erantsita) PDFn	PAdES-T-Level	PAdES-LTA-Level
XML dokumentuen kasuan, ahal bada, *attached* sinadura (erantsita)	XAdES-T-Level	XAdES-LTA-Level
Beste kasu batzuetan, *detached* sinadura (bereizita)	XAdES-T-Level	XAdES-LTA-Level

OHARRA: epe luzera gorde beharreko dokumentuen sinadura formatuak sortu ahal izango dira zuzenean, sinaduraren unean bertan, edo LTA-Level formatuetarako denbora zigiludun sinadurak osatzeko unibertsitateko barne prozesuetatik abiatuta.

12. Dokumentuak eta sinadura elektronikoak babesteko estrategia

Sinadura elektronikoak aukera ematen badu ere egiaztatzeko borondatearen adierazpenaren egiazkotasuna dokumentu elektronikoetan, badira haien balio osoa arriskuan jar dezaketen zenbait elementu, behar bezala kudeatu beharrekoak, dokumentu elektronikoaren balio juridiko mugagabea bermatzeko.

Arriskuak dira:

Ziurtagiri digitala edo dokumentu elektronikoa sinatzeko erabiltzen den zigilu elektronikoa iraungitzea.

Ziurtagiri digitalaren edo zigilu elektronikoaren balioa sinadura elektronikoa sortzeko unean.

Sinadura elektronikoak sortzeko ziurtagiri digitaletan dauden gako kriptografikoen luzeraren balizko zaharkitze teknologikoa.

Administrazioaren Sinadura eta Zigilu Elektronikoen eta Ziurtagirien Politikaren Elkarreragingarritasunerako Arau Teknikoak mekanismo sail bat zehazten du sinadura/zigilu elektronikoa algoritmoen balizko zaharkitzetik babesteko eta haren ezaugarriak bermatzeko baliagarritasun denboran zehar. Zehatz-mehatz:

Denbora birzigilatzeko mekanismoak erabiltzea, artxibo data eta orduaren zigilu bat gehitzeko, algoritmo sendoago batekin, aurreko zigilua iraungitzear dagoenean. Horretarako erabili behar dira bizitza luzeko sinadurak.

Sinadura elektronikoa gordailu seguru batean biltegiratzea, sinadura aldaketetatik babestuko duena, ziurtatuta horrela sinadura elektronikoa gorde zen data zehatza eta hura osatzen duten elementuen egiazkotasuna eta indarraldia egiaztatu zena.

Unibertsitatearen kasuan, sinaduren birzigilua aplikatzearen alde egin da.

12.1 Dokumentuak eta sinadura elektronikoak ingurune propioetan birzigilatzea eta babestea

Birzigilatze prozesua oinarritzen da dokumentu elektronikoari aplikatutako denbora zigilua berritzean, beste katebegi bat sartuta dokumentuak jada badituen sinadura elektronikoen ebidentzia elektronikoen katean. Prozesuaren helburu nagusia da dokumentu elektronikoaren kontserbazioa, osotasuna eta egiazkotasuna bermatzea denboran zehar.

Birzigilatzea aplikatuko zaie gorde beharreko sinadura elektronikoari aplikatutako azken denbora zigilua iraungitzear dagoen unean unibertsitatearen behin betiko artxibo soluziora transferitu ez diren dokumentu elektronikoei, eta, salbuespen gisa, dokumentu hori sinatzen duten algoritmoen edo gakoen zaharkitze teknologikoa detektatu denean.

Prozesu horrek eskatzen du dokumentuaren sinadurak izatea XAdES-LTA-Level edo PAdES-LTA-Level formatukoak (aldi baterako ebidentziak gehitzea onartzen duten sinadura motak dira). Sinadura ez badago bi formatu horietako batean, dokumentuen sinadura osatu beharko da formatu horietako batean, birzigilatze prozesua egin aurretik.

Une horretan, beste denbora zigilu bat gehituko zaie XAdES-LTA-Level edo PAdES-LTA-Level sinadurei. Denbora zigilu hori:

Duela gutxiko ziurtagiri batekin sortuko da.

Birzigilatu beharreko sinadurak baino balio aldi luzeagoa izango du.

Gako luzera nahikoa izango du, arriskuan egon ez dadin.

Aplikatuko duen algoritmoa edo gakoa ez da egongo haren zaharkitze kriptografikoaren mende (hura igortzeko unean).

Nortasuna egiaztatuz eta sinadura borondatearen ebidentziak bilduz eginiko sinadurei dagokienez, gomendatzen da birzigilatzea bigarren mailako sinadura; hau da, denbora zigilua.

12.1.1 Dokumentuak prestatzea, babesteko

Dokumentuak birzigilatzeko, ziurtatu egin behar da birzigilatzeko moduko sinadura dutela. Gomendatzen da honako hau izatea unibertsitatean sinadura elektronikoen balioa berrikusteko prozesua:

Unibertsitate barruan sortutako sinadura elektronikoen kasuan, sinadurak sortuko dira formatu jakin batzuetan, aukera emango dutenak haien babesa bermatzeko administrazio prozedura izapidetu bitartean. Ondorioz, XML formatuko dokumentuetan, sinadurak aldatuko dira XAdES-LTA-Level formatura; PDF dokumentuetan, PAdES-LTA-Level formatura.

Sinadura elektronikoak kanpoko plataformetatik datozenean, osatuko dira administrazio espedientea itxi eta orrialdekatu ondoren. Ondorioz, XML formatuko dokumentuetan, sinadurak aldatuko dira XAdES-LTA-Level formatura; PDF dokumentuetan, PAdES-LTA-Level formatura.

Edozein arrazoirengatik ezin bada babes bermea duen sinadura elektronikorik sortu, dokumentu originalaren benetako kopia elektroniko bat sortuko da, ahalik eta lasterren. Prozesu hori gauzatzeko, sinadura egingo da egiazko kopia elektronikoa babestea bermatuko duen formatu batean, dokumentu originala ordeztuko duena.

Ezin bada sortu egiazko kopiarik edo sinadurak iraungita badaude, gomendatzen da baliozkotze txosten bat sortzea (automatikoki eraikia), dokumentuaren laburpen kriptografikoa, sinaduraren identifikazioa eta ziurtagiriaren indarraldia egiaztatzeko elementuak jasota. Unibertsitatearen zigilu elektronikoarekin eta denbora zigiluarekin sinatutako txosten hori gordeko da sinatutako dokumentuarekin batera, epe luzera.

Nortasunean gehi sinatzeko borondatean oinarritutako sinadura elektronikoei dagokienez, sinadura sortuko da zigilu elektronikoaren bidez, babesa bermatuko duen formatu batean, ahal dela PAdES-LTA-Level.

Aldiz, sinadura biometrikoei dagokienez, sinadura elektronikoa sortuko da zigilu elektroniko bat aplikatuta, babesa bermatuko duen formatu batean (PAdES-LTA-Level).

12.1.2 Kontserbazio formatuak hautatzea

Dokumentuaren formatua, segurtasun elementuak, sinadura elektronikoak eta denbora zigiluak babesten dituzten zereginak beharrezkoak dira dokumentu elektronikoen ulergarritasuna eta osotasuna bermatzeko epe luzera.

Horrenbestez, dokumentu elektronikoak babesteko sistemak dokumentuen aldizkako kontrolak egin behar ditu, haien irisgarritasuna, berreskuratzeko aukera eta balio juridikoa bermatzeko. Kontrol horiek egiaztatuko dituzte:

Euskarrien irisgarritasuna.

Formatuak irakurtzeko gaitasuna.

Sinadura elektronikoen balio juridikoa.

Dokumentuen osotasuna.

Espedienteen osotasuna.

Dokumentuak unibertsitatetik kanpoko iturri batetik badatoz, proposatzen da PDF/A formatura bihurtzea, gaur egun dokumentu elektronikoak babesteko gehien erabiltzen den formatua. PDF formatua ere onartuko da, baldin eta formatu horretako dokumentuak sortzen dituzten aplikazio korporatiboetatik badator.

Sinadura elektronikoaren balioa bermatzeko, gomendatzen da aurretik ezarritako irizpidea erabiltzea; hots, lehendik dauden sinadurak osatzea denboran zehar babestuko direla bermatuko duten formatuetan:

XAdES-LTA-Level, XML formatuko dokumentuetan, XAdES sinadurekin.

PAdES-LTA-Level, PDF edo PDF/A formatuko dokumentuetan.

Sinadura horietatik abiatuta eta zigilu elektronikoa iraungitzen den unean, gomendatzen da sinadura elektronikoak birzigilatzea, iraungitze denbora nahikoa eta algoritmoak edo sinadura gakoak eguneratuta izango dituen beste zigilu baten bidez.

Espedientearen orrialdekatzeari aplikatutako zaio XML formatua, administrazio jardun automatizaturik onena ahalbidetzen duen formatua delako, espedientearen osotasuna bermatuta.

13. Politika mantentzea

13.1 Politika ezartzea

Politika hau eguneratzeko, egokitu egin beharko dira unibertsitatean erabiltzen diren aplikazioak, tresna informatikoak eta prozesuak. Zeregin horretan, Eraldaketa Digitalean eskumena duen arloak koordinatu egingo du eragindako sistema guztien eguneratzea, Politika honetan ezarritakora egokitzeko, egin beharreko jarduerek eskatzen duten epean, erabili beharreko egutegia egin ondoren.

UPV/EHUren Nortasun eta Sinadura Elektronikoko Politika indarrean jarri ondoren sortutako zerbitzuak eta sistemak politika horren mende egongo dira, martxan jarriko diren unetik beretik.

Eraldaketa Digitalean eta Komunikazioan eskumena duen organoak bi urtean behin aztertuko du Politika zer mailataraino betetzen den, unibertsitateko kideen benetako beharretara egokitzen den eta eskura dauden teknologiekin bat datorren, eta horren berri emango dio Idazkaritza Nagusiari.

13.2 Egoera iragankorrak

Politika honen identifikazio eta sinadura metodoak pixkanaka hasiko dira erabiltzen, unibertsitateak horiek erabiltzeko behar diren aplikazioak, tresnak eta prozesuak eskuratu ahala.

Sistemak eguneratuko dira 13.1 puntuko egutegiaren arabera, Politika hau onartu eta gero, haren xedapenetara egokitzeko.

13.3 Estandar zaharkituak indargabetzea

Nortasun eta Sinadura Elektronikoko Politika hau onartzeak berekin dakar indargabetzea harekin kontraesanean dauden estandar teknikoak eta garapen dokumentuak.

13.4 Indarrean jartzea

Politika hau indarrean jarriko da EHAAn argitaratu eta biharamunean.

I. eranskina. Sinadura elektronikoari lotutako glosarioa eta kontzeptuak

I.1. Glosarioa

Politika honen egileei garrantzitsua iruditu zaie eranskin batean biltzea dokumentuan erabilitako kontzeptuen definizioak, errazago ulertzeko.

Sinadura elektronikoaren erabilira kasuak. Hau da, dokumentu elektroniko sinatuak sortzeko egoera posibleak. Erabilera kasu bakoitzean zehazten dira aplika daitezkeen sinadura elektronikoko formatuak, sinadura maila posibleak, etab.

Sinadura elektroniko motak. Dokumentu honek aipatzen ditu sinadura elektroniko motak eta haien balio juridikoa. eIDAS Erregelamenduaren arabera, hiru motatan sailkatzen dira: sinadura sinplea, aurreratua eta kualifikatua.

Sinadura elektronikoaren formatua. Sinadura elektronikoak kodetzeko modua, formatu ohikoenak izanik: S / MIME, CMS, XAdES, CAdES eta PAdES.

Sinadura maila. Dokumentuak sinadura bat edo gehiago dituen adierazten du, eta, bigarren kasuan, modu paraleloan edo sekuentzialean sortzen diren.

Denbora zigilua. Konfiantzazko hirugarren batek egiaztatzea bitarteko elektronikoen bidez eginiko edozein eragiketa edo transakzioren eguna eta ordua.

Sinadura sistema. Dokumentu elektroniko bat sinatzeko moduari dagokio: sinatzailearen ziurtagiri digital bidez, identifikazio sistema gehi sinadura egintzaren ebidentzia elektronikoaren bidez, sinadura biometrikoaren bidez edo Egiaztapen Kode Seguru (SVC) baten bidez.

Sinadura mota. Adierazten du sinadura elektronikoa eta sinatutako dokumentua lotzeko modua: dokumentu beraren barruan, dokumentu bereizi gisa, XML egituren barruan, etab.

Hauek dira sinadura elektroniko bat sortzeko eta baliozkotzeko prozesuan parte hartzen duten eragileak:

Sinatzailea. Sinadura sortzeko gailu bat duen pertsona, bere izenean edo pertsona fisiko edo juridiko baten izenean diharduena.

Zigilu baten sortzailea. Zigilu elektroniko bat sortzen duen pertsona juridikoa.

Egiaztatzailea. Sinadura elektroniko bat baliozkotzen edo egiaztatzen duen entitatea, izan pertsona fisikoa edo juridikoa, kontuan hartzen dituena harreman elektronikoko plataforma edo dagokion zerbitzua arautzen duen politikaren baldintzak. Izan daiteke konfiantzazko baliozkotze erakunde bat edo sinadura elektroniko baten balioan interesa duen hirugarren bat.

Sinadura elektronikoko zerbitzuen emailea. Ziurtagiri elektronikoak edo sinadura elektronikoarekin lotutako beste zerbitzu batzuk ematen dituen pertsona fisikoa edo juridikoa.

Nortasun eta sinadura elektronikoko politikaren igorlea eta kudeatzailea. Sinadura elektronikoa sortzeko eta baliozkotzeko prozesuetan, sinatzailearen, egiaztatzailearen eta zerbitzu emailearen jarduerak arautzen dituen politikaren dokumentua sortzeaz eta kudeatzeaz arduratzen den organoa edo unitatea.

Dokumentu honek erabiltzen du "sinatzaile" kontzeptua aipatzeko bai sinatzen duen pertsona bai zigilu baten sortzailea. Azken kasu horretan, izan daiteke administrazio jarduketako prozesu automatizatu bat.

I.2. Sinadura elektronikoaren kontzeptuak

Sinadura elektronikoaren definizio juridikoa

Ikuspegi juridikotik, sinadura motak dira:

Sinadura elektroniko sinplea: modu elektronikoan jasotako datu multzoa, beste batzuekin batera kontsignatuak edo elkartuta daudenak, sinatzailea identifikatzeko erabil daitezkeenak. Identifikazioa hartzen da erakundeen autentifikaziotzat.

Sinadura elektroniko aurreratua: modu elektronikoan jasotako datu multzoa, aukera ematen duena sinatzailea identifikatzeko eta sinatu diren datuetan gerora eginiko edozein aldaketa detektatzeko, modu bakarrean lotua sinatzaileari eta aipatzen diren datuei, eta sinatzaileak bakarrik kontrola ditzakeen bitartekoen bidez sortua.

Sinadura elektroniko kualifikatua: ziurtagiri kualifikatu batean oinarritutako sinadura elektroniko aurreratua, sinadurak sortzeko gailu seguru baten bidez sortua.

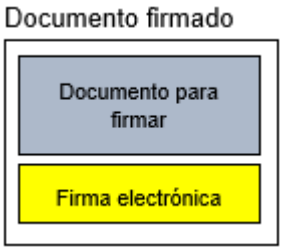
Atal honen definizioetan erabiltzen den ziurtagiri kualifikatuaren kontzeptua dagokie konfiantzazko zerbitzuen emaile kualifikatu batek emandako ziurtagiri elektronikoei, eta zerbitzu emaile horrek betetzen ditu eskatzaileen nortasuna eta gainerako inguruabarrak egiaztatzeko eta emandako ziurtapen zerbitzuen fidagarritasun eta bermeetarako baldintzak.

Sinadura elektronikoaren oinarri teknikoak

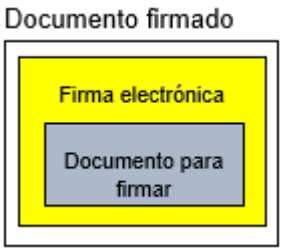
Ikuspuntu teknikotik, honela definitzen dira **sinadura motak**:

Attached* sinadura**: sinadura elektronikoaren datuak daude sinatutako dokumentuan. Beraz, dokumentu horretan bertan dago dokumentuaren egiazkotasuna eta osotasuna egiaztatzeko behar den informazio guztia, bai eta sinadura baliozkotzeko behar den informazio guztia ere. ***Attached sinadura bi motatakoa izan daiteke:

- ***Enveloped* (txertatua)**: dokumentu elektronikoan daude dokumentuaren edukia eta haren sinadura.



- ***Enveloping* (inguratzailea)**: sinatutako dokumentu elektronikoa da sinatu beharreko dokumentu elektronikoaren sinadura, eta haren barruan dago sinatu beharreko dokumentua bera.



***Detached* sinadura**: sinadura elektronikoaren datuak daude sinatu beharreko dokumentutik kanpo, baina dokumentu horri lotuta. Sinaduraren datuak bereizita daude dokumentuaren bizi ziklo osoan. Sinadura baliozkotzeko, sortu behar da ebidentzia elektronikoen dokumentu bat, dokumentua eta sinaduraren datu osoak batera jasoko dituena.

Sinadura mailari dagokionez:

Sinadura sinplea: dokumentuak sinadura bakarra du.

Sinadura anizkoitza: dokumentuak bi sinadura edo gehiago ditu. Sinadura anizkoitza da sinatzaile batek baino gehiagok dokumentua elkarren segidan sinatzea. Sinadura mota hau aplika dakioke aldi bakoitzean dokumentu originalari (sinadura paraleloa) edo sinatutako dokumentuari (sinadura sekuentziala).

> Sinadura anizkoitza hainbat zereginetan erabiliko da unibertsitatearen administrazio prozeduren barruan; hala nola pertsona batek baino gehiagok dokumentu elektronikoak sinatzean edo jada sinatutako dokumentuen birzigilatzean, denboran zehar haien lege balioa eguneratzeko, sinadura elektronikoaren balio kriptografikoa zalantzazkotzat jo aurretik.

II. eranskina. Unibertsitateak eta haren langileek erabiltzeko ziurtagiri elektronikoak

Unibertsitateak eta haren langileek lanpostuko zereginetan erabiltzeko ziurtagiri elektronikoen zerrenda.

Ziurtagiri profesionala:

- **Profesionalaren sinadura elektronikoaren ziurtagiri kualifikatua**, unibertsitateko konfiantzazko zerbitzu elektronikoen emaile kualifikatuak unibertsitateko langile guztiei emana, lanpostuak eskatzen dituen autentifikazio eta sinadura zeregin guztietan erabiltzeko. Titularrari eta unibertsitatearekin langile gisa duen loturari buruzko informazioa du. Eskatzen dira politika honen 8.4 atalean aipatutako prozeduraren bidez.
- UPV/EHU da bere konfiantzazko zerbitzu elektronikoen emaile kualifikatuaren erregistro erakundea, eta unibertsitateak berak berariaz izendatutako bulegoetan egiten dira pertsonak identifikatzeko, dokumentazioa egiaztatzeko eta Ziurtagiri Profesionala emateko operazioak.

Ordezkari ziurtagiria:

- **Erakunde ordezkariaren sinadura elektronikoko ziurtagiri kualifikatua**, unibertsitatearen konfiantzazko zerbitzu elektronikoen emaile kualifikatuak emana. Pertsona juridikoaren ordezkariaren ziurtagiri elektronikoari dagokio, eta identifikazioko eta sinadura aitortu edo kualifikatuko ziurtagiri pertsonal bat da. Titularrari eta unibertsitatean duen ordezkaritzari buruzko informazioa du. Eskatzen dira politika honen 8.4 atalean aipatutako prozeduraren bidez.
- Eskaera zentralizatuko du UPV/EHUn Eraldaketa Digitalean eta Komunikazioan eskumena duen organoak, hura lortzeko ezinbestekoa baita ziurtagiriaren titularra erakundearen ordezkari izendatu izana egiaztatzea. Egiaztapen hori agiri bidez jaso beharko da aldizkari ofizialeko argitalpen batean, erregistro publiko batean edo notario dokumentu batean, 6/2020 Legearen 7. artikuluan ezarritakoaren arabera.

Ziurtagiri teknikoak:

- **Administrazio jarduera automatizatuetarako zigilu elektronikoko ziurtagiria**, unibertsitatearen konfiantzazko zerbitzu elektronikoen emaile kualifikatuak emana. Administrazio jarduketa automatizatua baimentzeko balio duten ziurtagiri digitalei dagozkie, 40/2015 Legearen 42. artikuluan aipatutako baldintzetan. Ziurtagiri hau erabiltzen da espedienteen kopia elektronikoak eta orrialdekatuak egiteko, eta langile publiko baten esku-hartzea behar ez duten ziurtagiriak egiteko.

  - Unibertsitateak zigilu elektronikoko ziurtagiri bakarra du, erabilera guztietarako, eta espezializatu daitezke, hura zaintzen duen organo bakoitzaren eskumenen arabera.

- **Aplikazio ziurtagiria**, unibertsitatearen konfiantzazko zerbitzu elektronikoen emaile kualifikatuak emana. Aplikazioak eta zerbitzariak identifikatzeko balio duten ziurtagiri digitalei dagokie. Ziurtagiri hauek erabil daitezke, besteak beste, datuak trukatzeko administrazioen artean, administrazioen eta herritarren artean, eta administrazioen eta enpresen artean, web sistema edo zerbitzu bat identifikatzeko eta egiaztatzeko, etab.
- **Zerbitzari ziurtagiria edo egoitza elektronikoko ziurtagiria**, unibertsitatearen konfiantzazko zerbitzu elektronikoen emaile kualifikatuak emana. Unibertsitatearen izapidetze telematikoko inguruneetara (hala nola webgune korporatiboa edo, hala badagokio, egoitza elektronikoa) modu seguruan sartzeko erabiltzen diren ziurtagiri digitalei dagozkie.
- Aplikazio ziurtagirien kasuan bezala, horrelako ziurtagiriek egintza juridikorik sortzen ez duten arren, egokitzat jo da ziurtagiri hauek politika honetan aipatzea, haien erabilera eta zaintzaren erantzukizuna arautzeko.

Zerrenda hau eguneratu ahal izango du Eraldaketa Digitalean eta Komunikazioan eskumena duen unibertsitateko organoak, Informazioaren eta Komunikazioen Teknologien Gerenteordetzako informazioaren segurtasuneko arduradunak proposatuta, kontuan izanik teknologian edo agintarien egiaztapen praktiketan gerta daitezkeen aldaketak, baldin eta erabilitako ziurtagiriak badira Ministerio eskudunak mantentzen duen konfiantzazko zerbitzu elektronikoen emaileen zerrendako (TSL) agintariek emandako ziurtagiri kualifikatuak.

III. eranskina. Nazioarteko estandarrak eta beste konbentzio batzuk

ETSI RFC 2315 (1998), ETSE RFC 2630 (1999), IETF RFC 3369 (2002), IETF RFC 3852 (2004): PKCS # 7: Cryptographic Message Syntax (CMS).

ETSI TS 101 733. v.1.6.3, v1.7.4 i v.1.8.1: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).

ETSI TS 119 122-3: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures: Part 3: incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES.

ETSI TR 119 124-1: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.

ETSI TS 119 124-2: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of CAdES baseline signatures.

ETSI TS 119 124-3: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended CAdES signatures.

ETSI TS 119 124-4: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of CAdES baseline signatures.

ETSI TS 119 124-5: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended CAdES signatures.

ETSI TR 119 134-1: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.

ETSI TS 119 134-2: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of XAdES baseline signatures.

ETSI TS 119 134-3: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended XAdES signatures.

ETSI TS 119 134-4: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of XAdES baseline signatures.

ETSI TS 119 134-5: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended XAdES signatures.

ETSI TS 119 142-3: Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS).

ETSI TR 119 144-1: Electronic Signatures and Infrastructures (ESI); PAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview.

ETSI SR 019 020: The framework for standardization of signatures; Standards for AdES digital signatures in mobile and distributed environments.

IETF RFC 5280 (2008): Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

IETF RFC 2560 (1999): X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP.

IETF RFC 3126 (2001): Electronic Signature Formats for Long Term Electronic Signatures.

ISO 19005 (2008): Fitxategiaren formatua / A-1.

ISO / TR 18492: 2005- Long-term preservation of electronic document-based Information.

UNE - ISO/TR 13008: 2010 – Información y documentación. Conversión de documentos digitales y procesos de migración.

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

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

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

ETSI TS 101.861 V1.3.1 Time stamping profile.

ETSE TR 102.038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.

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

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

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

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

IETF RFC 3125, Electronic Signature Policies.

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

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

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

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

IV. eranskina. Hirugarrenen sinadurak baliozkotzean kontuan hartzeko egiaztapenak

Urrats hauek egin behar dira hirugarrenen sinadurak egiaztatzeko eta behar bezala egin direla ziurtatzeko:

IV.1. Sinadura data egiaztatzea

Dokumentu elektroniko baten sinadura data garrantzitsua da sinatzailearen ziurtagiriaren balioa kudeatzeko.

Baliteke dokumentu elektronikoak edukian sinadura data bat izatea eta data hori bat ez etortzea sinadura elektronikoaren datarekin. Ondorioz, egiaztatu egin beharko da dokumentua sinatu den data, eta bereizi, sinadura data ezarri den denbora zigilu baten bitartez edo sinatzailearen gailuaren erloju bidez.

Dokumentua atzemateko aplikazioaren bidez egiaztapen horiek automatikoki egiteko aukera dagoen arren, gomendatzen da egiaztapenak eskuz egitea, egiaztapenen fidagarritasuna bermatzeko.

IV.2. Titulartasuna eta konfiantza katea identifikatzea

Sinadura elektroniko bat sortzeko, erabili behar da ziurtagiri elektroniko aitortu bat, eta konfiantzazko zerbitzu elektroniko kualifikatuak ematen dituen erakunde batek eman beharko du nahitaez ziurtagiri hori. Horrek bermatzen ditu erabilitako sinadura elektronikoaren segurtasuna eta sinatzailearen nortasuna.

Ziurtagiriaren igorlearen egiaztapenak huts egiten badu, unibertsitateak ez du konfiantzarik izango dokumentu elektronikoaren sinaduran, eta sinatzaileari itzuliko zaio, konfiantzazko jaulkitzaile batek sina dezan.

IV.3. Ziurtagiriaren titularraren nortasuna

Kontuan izanik ziurtagiri elektroniko batek informazioa ematen duela identifikatzeko dokumentuaren edukiarekiko konpromisoa duen pertsona fisikoa edo juridikoa, oso garrantzitsua da haren nortasuna egiaztatzea ziurtagiritik atera daitezkeen erreferentzien bidez, dokumentua sinatu beharko lukeen pertsonak sinatu duela ziurtatzeko.

Ordezkaritza bidez sinatzen bada, jaso beharko da ordezkariari eta ordezkatutako pertsonari buruzko informazioa, dagokion eremuan.

Ziurtagiriaren titularra bat badator dokumentuaren sinatzaile gisa ageri den pertsonarekin, ontzat eman daiteke egiaztapena; aldiz, ziurtagiriaren titularra ez badator bat dokumentua sinatu beharko lukeen pertsonaren nortasunarekin, baztertu egin beharko da dokumentua, haren sinadura onargarria ez delako.

IV.4. Sinatzailearen ahalmenak baliozkotzea

Litekeena da batzuetan hirugarren baten izenean sinatzea. Kasu horretan, unibertsitateak egiaztatu egin beharko du sinatzaileak ahalmena duela alegatutako ordezkaritza bere gain hartzeko, baldin eta ahalmen hori ziurtagirian jasota ez badago. Kasu batzuetan, dokumentazio gehigarria eska daiteke ordezkaritza egiaztatzeko, edo kanpoko erregistroetara ere jo daiteke, nortasuna ziurtatzeko.

Ezin bada egiaztatu sinatzaileak ordezkaritza ahalorde nahikoak dituela, igorleari itzuliko zaio dokumentua.

IV.5. Ziurtagiriaren indarraldia egiaztatzea

Ziurtagiri elektronikoak iraungi ahal izango dira, jaulkitzeko unean ezarritako dataren arabera, edo bertan behera gelditu edo ezeztatu ahal izango dira, egun hori baino lehen, hainbat arrazoirengatik: hala nola ziurtagirien datuen indarraldia amaitzea edo txartel kriptografikoa galtzea.

Kontuan izanik aurreko paragrafoan aipatutakoa, unibertsitateak egiaztatu egin beharko du sinaduren balioa, ziurtagiriak edo ziurtapen agintaritzak emandako datuen arabera, prozedura honen bidez:

Ziurtagiriak baliogabetzeko zerrendak (CRL) egiaztatzea, dokumentu sinatuak bistaratzeko aukera ematen duten merkatuko aplikazio gehienek automatikoki inplementatua, froga zehatzik sortzen ez bada ere.

Egiaztapen txosten bat (OCSP) eskatzea, ziurtapen zerbitzu emaileari. Unibertsitatearen sistema informatiko baten bidez eskatu beharko da.

Estatuko Administrazio Orokorraren @firma plataforma zentralizatuaren bidez baliozkotzea.

Litekeena da ziurtagiria iraungitzea dokumentu bat sinatu ondoren, eta horregatik garrantzitsua da unibertsitatea gai izatea egiaztatzeko ziurtagiria indarrean zegoela egiaztapen datan, agintaritza batek emandako denbora zigilua erabilita (TSA).

IV.6. Dokumentuak sinadurarekin duen lotura kriptografikoa egiaztatzea

Egiaztapen hau erabiltzen da ziurtatzeko sinadura elektronikoa dagokiola sinatu dela alegatzen den dokumentuari, litekeena delako dokumentua aldatu izana sinatu ondoren. Beraz, baliteke bat ez etortzea dokumentu elektronikoa eta haren sinadura.

Egiaztapen hau egin ahal izango da dokumentuak PDF formatuan ikustea ahalbidetzen duten aplikazio ofimatikoen bidez; aldiz, dokumentua sisteman txertatzeko prozesuetan, egiaztapena egingo da txertatze hori egiten duen aplikazioaren bidez.

Egiaztapen prozesuak huts egiten badu, sinadura akastuntzat hartuko da, eta igorleari itzuliko zaio dokumentu elektronikoa, baztertzeko arrazoiaren berri emanez.

IV.7. Dokumentuaren edukia egiaztatzea

Dokumentu elektroniko baten edukia egiaztatzea da paperezko dokumentu batena bezain funtsezkoa. Hala ere, dokumentu elektronikoaren kasuan, bereziki begiratuko da edukia egokia den eta balio juridikoa izateko behar diren baldintzak betetzen diren.

Dokumentua unibertsitateak berak sortu badu, gomendatzen da hirugarrenak sinatzea, unibertsitatearen zigilu elektroniko bidez sinatu ondoren, itzuleraren egiaztapena automatizatzeko.

Ezin bada automatikoki egiaztatu, dokumentua berrikusi beharko da, ziurtatzeko ez dela aldaketarik izan sinatzaileari bidalitako bertsioaren eta sinatuta itzuli denaren artean.

Egiaztapenak huts egiten badu, itzuli egingo da hirugarrenak sinatutako dokumentua.

V. eranskina. Sinadura elektronikoko sistemen erabilera kasuak

Ondoren aipatzen dira unibertsitatean eman daitezkeen sinadura elektronikoko sistemen zenbait erabilera kasu, besteak beste aipaturik haien ezaugarri juridikoak, segurtasun baldintzak eta bat edo bestea erabiltzearen komenigarritasuna, aztertutako kasuaren arabera.

V.1. Barne dokumentu baten sinadura elektronikoa

Kasu hau dagokie unibertsitateak sortutako dokumentuei, erakundearen langile batek bere zereginetan edo unean-unean UPV/EHUrekin kolaboratzen duten hirugarrenek sinatuak, erakunde barruko hartzaile bati bidaltzeko edo prozeduran urrats bat betetzeko. Inola ere ez da erabili behar hirugarrenen aurrean ondorio juridikoak izango dituzten dokumentuetan.

Kasu honetan, elektronikoki sinatu ahal izango dira dokumentu elektronikoak haien bizi zikloaren edozein unetan.

Sinadura honen ezaugarri nagusiak dira:

- Sinadura elektronikoa egiten da euskarri elektronikoan dagoen dokumentu original batean.
- Dokumentu originala eta sinadurak sartu behar dira sinadura sisteman.
- Sinadura elektronikoa baliozkotu behar da baliozkotze zerbitzu edo agintaritza baten bidez, haren osotasuna eta egiazkotasuna ziurtatzeko.

Dokumentu elektronikoa denboran zehar gorde behar denean, unibertsitateak onartutako edozein formatutan egongo da, ahal dela PDF/A eta XML.

Kasu honetan aplika daitezkeen sinadura motei dagokienez, baldintza hauek ezartzen dira:

Sinadura sistemak	• Ziurtagiri kualifikatu elektroniko pertsonala, 10.1 atalean aipatutakoaren arabera. • Ziurtagiri ez-kualifikatu elektroniko pertsonala, 10.1 atalean aipatutakoaren arabera. • Klabe itunduak, bigarren autentifikazio faktorearen osagarriarekin, 9.4 atalean aipatutakoaren arabera. Soilik onartuko da dokumentu elektronikoak sinatzeko sinatzailea denean unibertsitateko barne prozedura batean parte hartzen duen atzerritar ez-egoiliarra eta bestelako identifikazio mekanismorik ez duenean.

Ziurtagiri motak	**Unibertsitateko langileak** • Ziurtagiri profesionala. • Ordezkari ziurtagiria. **Parte hartzen duten hirugarrenak** • Pertsona fisikoaren ziurtagiria.
Onartutako formatuak	• PAdES-T-Level • XAdES-T-Level
Sinadura maila	Sinplea, anizkoitza (sekuentziala edo paraleloa).
Sinadura mota	***Attached*** (erantsia) edo ***Detached*** (bereizia), kasuaren arabera.
Denbora zigilua aplikatzea	

V.2. Hirugarrenentzat balioa duen dokumentu baten sinadura elektronikoa

Kasu hau dagokie unibertsitateak sortutako dokumentuei, erakundearen langile batek bere zereginetan edo unean-unean UPV/EHUrekin kolaboratzen duten hirugarrenek sinatuak, eskubideak edo betebeharrak sortzen dituztenak hirugarrenentzat.

Kasu honetan, elektronikoki sinatu ahal izango dira dokumentu elektronikoak haien bizi zikloaren edozein unetan.

Sinadura honen ezaugarri nagusiak dira:

- Sinadura elektronikoa egiten da euskarri elektronikoan dagoen dokumentu original batean.
- Dokumentu originala eta sinadurak sartu behar dira sinadura sisteman.
- Sinadura elektronikoa baliozkotu behar da baliozkotze zerbitzu edo agintaritza baten bidez, haren osotasuna eta egiazkotasuna ziurtatzeko.
- Dokumentu elektronikoa denboran zehar gorde behar denean, unibertsitateak onartutako edozein formatutan egongo da, ahal dela PDF/A eta XML.
- Dokumentu elektronikoaren benetako kopia egingo da, eta egiaztapen kode seguru bat erantsi, bermatuta egongo denean dokumentuaren osotasuna, zaintza eta artxiboko kontsulta. Hori izango da hirugarrenei emango zaien kopia.

Kasu honetan aplika daitezkeen sinadura motei dagokienez, baldintza hauek ezartzen dira:

Sinadura sistemak	• Ziurtagiri kualifikatu elektroniko pertsonala, 10.1 atalean aipatutakoaren arabera.
Ziurtagiri motak	**Unibertsitateko langileak** • Ziurtagiri profesionala. • Ordezkari ziurtagiria. **Parte hartzen duten hirugarrenak** • Pertsona fisikoaren ziurtagiria.
Onartutako formatuak	• PAdES-T-Level • XAdES-T-Level
Sinadura maila	Sinplea, anizkoitza (sekuentziala edo paraleloa).
Sinadura mota	*Attached* (erantsia) edo *Detached* (bereizia), kasuaren arabera.
Denbora zigilua aplikatzea	

V.3. Hirugarrenek dokumentuak elektronikoki sinatzea

Kasu hau dagokie unibertsitateak edo hirugarrenek sortutako dokumentu elektronikoei, azken horiek sinatuak UPV/EHUren kontrolpeko ingurune batean. Dokumentu elektroniko hauek sinatzen badira unibertsitatearen kontroletik kanpoko inguruneetan, kontuan hartuko da V.8 ataleko erabilera kasuan zehaztutakoa.

Zehazki, kasu hau aplikatzen da dokumentuak erregistro elektroniko batean aurkezten diren unean, edo hirugarrenak dokumentu elektronikoak sinatu behar dituenean unibertsitatearen administrazio prozedura batean parte hartu ondorengo une batean.

Sinadura honen ezaugarri nagusiak dira:

- Sinadura elektronikoa egiten da euskarri elektronikoan dagoen dokumentu original batean.
- Dokumentu originala eta sinadurak sartu behar dira sinadura sisteman.
- Sinadura elektronikoa baliozkotu behar da baliozkotze zerbitzu edo agintaritza baten bidez, haren osotasuna eta egiazkotasuna ziurtatzeko.

– Dokumentu elektronikoa denboran zehar gorde behar denean, unibertsitateak onartutako edozein formatutan egongo da, ahal dela PDF/A eta XML.

Kasu honetan aplika daitezkeen sinadura motei dagokienez, baldintza hauek ezartzen dira:

Sinadura sistemak	• Ziurtagiri kualifikatu elektroniko pertsonala, 10.1 atalean aipatutakoaren arabera. • Ziurtagiri ez-kualifikatu elektroniko pertsonala, 10.1 atalean aipatutakoaren arabera. • Gako itunduetan oinarritutako sinadura, 10.3 atalean aipatutakoaren arabera • Klabe itunduetan oinarritutako sinadura, bigarren autentifikazio faktorearen osagarriarekin, 10.4 atalean aipatutakoaren arabera. • Sinadura elektroniko biometrikoa, 10.5 atalean aipatutakoaren arabera.
Ziurtagiri motak	**Unibertsitateko langileak** • Ziurtagiri profesionala. • Ordezkari ziurtagiria. **Parte hartzen duten hirugarrenak** • Pertsona fisikoaren ziurtagiria. Gainerako sinadura mekanismoetan aplikatuko da zigilu elektronikoaren ziurtagiria.
Onartutako formatuak	• PAdES-T-Level • XAdES-T-Level
Sinadura maila	Sinplea.
Sinadura mota	*Attached* (erantsia) edo *Detached* (bereizia), kasuaren arabera.
Denbora zigilua aplikatzea	

V.4. Beste alde batzuekin eginiko kontratuak, hitzarmenak edo akordioak elektronikoki sinatzea

Kasu hau aplikatzen da kontratu izaerako dokumentuetan, unibertsitateak alde batekin edo gehiagorekin eginiko kontratu, hitzarmen edo akordioetan, UPV/EHUk kontrolatutako inguruneetan sinatzen direnak. Dokumentu elektroniko hauek sinatzen badira unibertsitatearen kontroletik kanpoko inguruneetan, kontuan hartuko da V.8 ataleko erabilera kasuan zehaztutakoa.

Sinadura honen ezaugarri nagusiak dira:

- Sinadura elektronikoa egiten da euskarri elektronikoan dagoen dokumentu original batean.
- Dokumentu originala eta sinadurak sartu behar dira sinadura sisteman.
- Sinadura elektronikoa baliozkotu behar da baliozkotze zerbitzu edo agintaritza baten bidez, haren osotasuna eta egiazkotasuna ziurtatzeko.
- Dokumentu elektronikoa denboran zehar gorde behar denean, unibertsitateak onartutako edozein formatutan egongo da, ahal dela PDF/A eta XML.
- Dokumentu elektronikoa behin baino gehiagotan sina dezakete interesdunek, modu paraleloan edo sekuentzialean.

Kasu honetan aplika daitezkeen sinadura motei dagokienez, baldintza hauek ezartzen dira:

Sinadura sistemak	• Ziurtagiri kualifikatu elektroniko pertsonala, 10.1 atalean aipatutakoaren arabera. • Ziurtagiri ez-kualifikatu elektroniko pertsonala, 10.1 atalean aipatutakoaren arabera. • Gako itunduetan oinarritutako sinadura, 10.3 atalean aipatutakoaren arabera • Klabe itunduetan oinarritutako sinadura, bigarren autentifikazio faktorearen osagarriarekin, 10.4 atalean aipatutakoaren arabera.
Ziurtagiri motak	**Unibertsitateko langileak** • Ziurtagiri profesionala • Ordezkari ziurtagiria **Parte hartzen duten hirugarrenak**

	• Pertsona fisikoaren ziurtagiria.
Onartutako formatuak	• PAdES-T-Level • XAdES-T-Level
Sinadura maila	Anizkoitza (sekuentziala edo paraleloa)
Sinadura mota	*Attached* (erantsia) edo *Detached* (bereizia), kasuaren arabera.
Denbora zigilua aplikatzea	

V.6. Sinadura elektroniko automatizatua

Kasu honetan, automatikoki sinatzen dira dokumentu elektronikoak, berme juridiko osoz, zigilu elektronikoko ziurtagiriak erabilita, sinatzaileek prozesuan parte hartu gabe.

Kasu hau pentsatuta dago dokumentuak berme juridiko osoz modu automatizatuan sinatu behar diren zereginetarako. Ziurtagiri elektroniko bat erabiliko da, eta haren bidez sinatuko dira dokumentuak dagokion aplikazioaren eta unibertsitatearen izenean.

Sinadura honen ezaugarri nagusiak dira:

– Elektronikoki sinatzen da automatikoki euskarri elektronikoan dagoen dokumentu original batean.

– Dokumentu elektronikoa egon daiteke unibertsitateak onartutako edozein formatutan (PDF, PDF/A eta XML), ahal bada PDF/A formatuan, interesdunei bidali beharreko dokumentuetan.

Sinadura automatizatuko prozesuak ahalbidetzen dituzten gako pribatuak eta ziurtagiri elektronikoak gordeko dira gordailu seguru batean, unibertsitatearen zerbitzarietan edo zerbitzuak ematen dituen hirugarren erakunde baten zerbitzari batean, baldin eta lagapen hori mugatuta eta kontrolatuta badago. Zehazki, lagapen guztiak xeheki azalduko dira unibertsitatearen eta hirugarrenaren artean eginiko kontratu edo hitzarmen batean, erabilera zehatzetara mugatuta, unibertsitatearen berezko egiaztapen ahalen mende.

Kasu honetan aplika daitezkeen sinadura motei dagokienez, baldintza hauek ezartzen dira:

Sinadura sistemak	• Zigilu elektronikoko ziurtagiri kualifikatu elektronikoa, 10.2 atalean aipatutakoaren arabera.

Ziurtagiri motak	• Unibertsitatearen zigilu elektronikoko ziurtagiria.
Onartutako formatuak	• PAdES-T-Level • XAdES-T-Level
Sinadura maila	Sinplea.
Sinadura mota	*Attached* (erantsia).
Denbora zigilua aplikatzea	

V.7. Digitalizazio segururako sinadura elektronikoa

Kasu honetan, elektronikoki sinatzen da PDF edo PDF/A formatuan dagoen dokumentu digitalizatu bat, benetako kopia elektroniko bat sortzeko. Sinadura garrantzitsua da, dokumentu digitalizatuaren osotasuna eta egiazkotasuna bermatzeko.

Elektronikoki sinatuko dute dokumentua:

Dokumentua digitalizatuko duen profesional gaituak, originala eskuz kontrolatu eta erkatzen bada.

Unibertsitatearen sistemaren zigilu elektronikoak, administrazio jardun automatizatuaren kasuan.

Kasu honetan aplika daitezkeen sinadura motei dagokienez, baldintza hauek ezartzen dira:

Sinadura sistemak	• Ziurtagiri kualifikatu elektroniko pertsonala (eskuzkoa), 10.1 atalean aipatutakoaren arabera. • Zigilu elektronikoko ziurtagiri kualifikatu elektronikoa (automatizatua), 10.2 atalean aipatutakoaren arabera.
Ziurtagiri motak	• Ziurtagiri profesionala. • Zigilu elektronikoko ziurtagiria.
Onartutako formatuak	• PAdES-T-Level

Sinadura maila	Sinplea
Sinadura mota	*Attached* (erantsia)
Denbora zigilua aplikatzea	

V.8. Espedientean sartzea kanpoko iturrietako dokumentu elektroniko sinatuak

Unibertsitatetik kanpoko plataformetatik datozen sinadurei dagokienez, baliozkotu egingo dira, eta, behin baliozkotuta, espedientean sartu, dagozkion baliozkotze ebidentziekin.

Gomendatzen da sinadurak baliozkotzean honako hauek egitea, besteak beste: sinadura data egiaztatzea, titulartasuna eta konfiantza katea identifikatzea, eta ziurtagiriaren indarraldia egiaztatzea.

V.9. Atzerritarren eta ez-egoiliarren identifikazioa eta sinadura

Azken kasu hau dagokie unibertsitateak atzerriko pertsona fisiko edo juridikoekin dituen hartu-emanei, kontratazio publikoan, nazioarteko ikerketa proiektuetan, etab.

Oro har, UPV/EHUk onartzen ditu dagokion Ministerioak homologatutako agintariek aitortutako ziurtagiri elektroniko guztiak, eIDAS Erregelamenduaren arabera. Hala ere, onarpen hori muga dezakete unibertsitateak erabilitako parsing (analisia) eta interpretazio tresnen gaitasunek.

Jarraibide batzuk ezarri dira atzerritarrak eta ez-egoiliarrak diren pertsonak unibertsitatearen eremuan identifikatzeko eta sinatzeko:

Pertsona juridikoek ziurtagiri elektroniko bat behar dute unibertsitatearekin harremanetan jartzeko. Oro har, gomendatzen da erabiltzea eIDAS inguruneko konfiantzazko zerbitzu elektronikoen emaile kualifikatuek jaulkitako ziurtagiri elektronikoak. Ingurune horretatik kanpoko ziurtagiri elektronikoak erabiliz gero, bete egingo da hurrengo puntuan aipatutako egiaztatzeko prozedura.

Unibertsitatearekiko hartu-emanean erakundearen ordezkaritza zereginak edo enplegatu publikoaren lanak egiten dituzten pertsona fisikoek ziurtagiri elektroniko bat lortu beharko dute, haien herrialdeko ziurtapen erakunde baten bidez. EBn bizi diren herritarren kasuan, aitortza automatikoa izango da, eIDAS Erregelamenduak onartutako konfiantza elektronikoko zerbitzu kualifikatuen emaileen arabera; aldiz, EBtik kanpoko ziurtagirien jaulkitzaileen kasuan, egiaztatu egin beharko da ziurtapen agintaritzaren

kaudimena. Ziurtagiria teknikoki zuzena dela egiaztatzen bada, agintaria konfiantzazkoa bada eta dokumentua ondo eginda badago, baliozkotzat hartuko du unibertsitateak. Dokumentu horiek onartzeko, egiaztapen hauek egin behar dira:

- Egiaztatzea ziurtagiria eman duela dagokion herrialdean akreditatutako ziurtapen erakunde batek eta betetzen dituela jatorrizko herrialdeko legeriaren baldintzak, sinatzailearen nortasuna eta dokumentuaren osotasuna bermatuz.
- Kasu honetan, adibidez, gomendagarria litzateke hirugarren batek aurkeztutako dokumentu elektroniko bat onartzea, ziurtagiria jaulki badu SOCIEDAD CAMERAL DE CERTIFICACION DIGITAL - CERTICÁMARA S.A. bezalako ziurtapen erakunde batek (ONAC - Organismo Nacional de Acreditación de Colombia-ren webguneko ziurtapen digitaleko erakundeen direktorioaren barruan dagoena).
- Egiaztatzea ziurtagiriak bete egiten duela ETSI TS 119 403rekin homologa daitekeen segurtasun maila bermatzen duen kriptografia estandar teknikoa.

  Hala ere, ez da erraza automatizatzen agintari batek bi baldintza horiek betetzen dituen erabakitzeko irizpidea. Baliozkotze automatikoa egiteko, konfiantzazko zerbitzu emaileak erregistratuta egon behar du zerrenda homologatu batean, eta horixe egiten du, hain zuzen, eIDAS Erregelamenduak, EBko zerbitzu emaileen kasuan. Dena dela, mundu mailako homologazioa falta da.

  Baldintza horiek betetzen direla egiaztatzeko, ondorengo prozedura beteko du unibertsitateak, aurkeztutako dokumentua berme guztiekin onartzeko:

  - Konfiantzazko zerbitzu emaileen zerrenda bat sortzea, UPV/EHUrena berarena, eta zerrenda horretan pixkanaka EBtik kanpoko zerbitzu emaileak sartuz joatea, baldin eta jarraian aipatzen diren egiaztapenak egin bazaizkie iraganean. Horrela, behin zerbitzu emaile bat kontrastatuta, ez da egiaztapena errepikatu behar.
  - Zerbitzu emailea bere herrialdean onartuta dagoela egiaztatzeko, aukera hauek ditugu:
    - Unibertsitatearen erakunde ziurtatzaileari eskatu ziurtagiriaren ziurtapen zerbitzuen emailea baliozkotzeko eta egiaztatzeko.
    - Dagokion herrialdeko gobernuaren erakunde publiko batera jo (konfiantzazko zerbitzu emaileen zerrenda bat duena). Kolonbiaren kasuan, adibidez, ONAC.
    - Europar Batasunaren edo Espainiaren eta hirugarren herrialdearen artean aldebiko hitzarmenik dagoen ikusi (ziurtagiri hauen elkarrekiko aitortza jasoko duena) Esate baterako, Kanadarekin, Mexikorekin edo Txilerekin dauden hitzarmenek gaia aipatu bai baina ez dute ebazten, eta ez dute, beraz, konponbide zehatzik ematen, baina litekeena da

etorkizunean hitzarmen horietan konfiantza zerrenden elkarrekiko aitortza bat jasotzea.

- Hirugarrenari dokumentu bat aurkezteko eskatu, haren ziurtapen zerbitzu emailearena, zerbitzu emailea bere herrialdean akreditatuta dagoela egiaztatuko duena.

- Ziurtagirien kalitate teknikoa egiaztatzeko, komeni da sartzea ziurtapen zerbitzu emailearen webgunean eta kontsultatzea erabili nahi den ziurtagiriari lotutako praktika edo ziurtapen politika. Informazio hori aurkitzeko modurik egokiena da kontsultatzea ziurtagiriaren beraren "Certificate Policies" eremua. Ziurtapen politikak identifikatuko du ziurtapen agintaritzari dagokion arau teknikoa edo auditoretza esparrua.
- Behin egiaztapenak eginda, emaitza aldekoa bada:
  - UPV/EHUk ziurtapen hornitzaile hori erregistratuko du bere konfiantzazko barne zerrendan, eta lotu egingo ditu bere ziurtapen zerbitzuaren URLa eta egiaztapena egiteko erabilitako dokumentazioa.
  - Dokumentua sartu ahal izango da UPV/EHUren sisteman. Kontuan izan behar da huts egiten jarraituko duela dokumentua @firma, Valide edo Adobe Acrobat Reader bezalako tresnekin egiaztatzeak, hornitzailea ez delako erregistratuta egongo dagozkion konfiantzazko zerrendetan, eta horregatik, komenigarria izan daiteke eginbide bat lotzea dokumentuari, adieraziz egiaztatu egin direla dokumentuaren egiazkotasuna eta sinaduraren kalitatea.
- Emaitza aurkakoa bada, hirugarrenari jakinaraziko zaio ziurtagiria ez dela agertzen konfiantzazko ziurtapen erakunde batek emandako ziurtagiri gisa, eta eskatuko zaio bere herrialdeko legeriarekin bat datozen sinadura bitartekoak lortzeko.

Unibertsitateak mantendu egingo du kontrastatu diren EBtik kanpoko konfiantzazko emaileen zerrenda, eta barne prozedura bat ezarriko du atal honetan aipatutako egiaztapenak egiteko, zerrenda hori zabaltze aldera.

Aurreko paragrafoan aipatutako zereginak egin ez eta dokumentu elektroniko bat sinatu behar duten pertsona fisikoek beren datu pertsonalen bidez identifikatu ahal izango dute beren burua. Datu horietatik abiatuta, nortasun bat sortuko da, kualifikatu gabeko ziurtagiriak jaulkita edo gako sistema itundu bat eginez, bigarren autentifikazio faktorea erabiliz osatuko dena. Sistema horiek oinarrituko lirateke UPV/EHUk kontrolatutako nortasunen erregistro batean, aukera emango lukeena unean-unean erakundearekin kolaboratzen duten hirugarrenak identifikatu, egiaztatu eta sinatzeko.

V.10. Unibertsitatearen sinadura sistemen erabileraren kasu diagramak

<table>
<tr><th colspan="5">Hirugarrenen aurrean ondorio juridikorik ez duten unibertsitatearen barne dokumentuak</th></tr>
<tr><td>Sinatzailea:</td><td colspan="4">Bere eginkizunak betetzen ari den unibertsitateko langilea edo unean-unean unibertsitatearekin kolaboratzen duen hirugarrena.</td></tr>
<tr><td></td><td>Hartzailea:</td><td colspan="3">Erakunde barruko beste erabiltzaile bat edo prozeduran beste urrats bat betetzea.</td></tr>
<tr><td rowspan="3"></td><td rowspan="3"></td><td>Aplikatu beharreko sinadura motak:</td><td colspan="2">Sinplea, aurreratua edo kualifikatua.</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">Sinatzeko tresna:</td><td>Ziurtagiriak (ikus 1. zerrenda).
Nortasuna + 2AF (ikus 2. zerrenda).</td></tr>
<tr><td></td></tr>
<tr><td rowspan="4">Sinatzailea:</td><td colspan="4">Unibertsitateko barne prozeduran parte hartzen duen eta ziurtagiririk ez duen atzerritar ez-egoiliarra.</td></tr>
<tr><td>Hartzailea:</td><td colspan="3">Erakunde barruko beste erabiltzaile bat edo prozeduran beste urrats bat betetzea.</td></tr>
<tr><td rowspan="2"></td><td>Aplikatu beharreko sinadura motak:</td><td colspan="2">Aurreratua</td></tr>
<tr><td>Sinatzeko tresna:</td><td>Ziurtagiriak (ikus 1. zerrenda).
Nortasuna + 2AF (ikus 2. zerrenda)</td></tr>
</table>

Hirugarrenentzat balioa duten dokumentuak				
Sinatzailea:	Unibertsitateko legezko ordezkaria			
	Hartzailea:	Hirugarrenak		
		Aplikatu beharreko sinadura motak:	Aurreratua edo kualifikatua.	
			Sinatzeko tresna:	Ordezkari ziurtagiria
Sinatzailea:	Bere eginkizunak betetzen ari den unibertsitateko langilea edo unean-unean UPV/EHUrekin kolaboratzen duen hirugarrena			
	Hartzailea:	Hirugarrenak		
		Aplikatu beharreko sinadura motak:	Aurreratua edo kualifikatua.	
			Sinatzeko tresna:	Ziurtagiriak (ikus 1. zerrenda).

UPV/EHUk kontrolatutako ingurune batean hirugarrenek sinatutako dokumentuak			
Sinatzailea:	Unibertsitateko langileak eta hirugarrenak		
	Hartzailea:	Unibertsitatea eta hirugarrenak	
		Aplikatu beharreko sinadura motak:	Sinplea, aurreratua edo kualifikatua.

	Sinatzeko tresna:	Ziurtagiriak (ikus 1. zerrenda). Nortasuna + 2AF(ikus 2. zerrenda) Sinadura elektroniko biometrikoa

Kontratu izaerako dokumentuak, alde anitzekoak eta UPV/EHUk kontrolatutako inguruneetan sinatuak				
Sinatzailea:	Unibertsitateko langileak eta hirugarrenak			
	Hartzailea:	Unibertsitatea eta hirugarrenak		
		Aplikatu beharreko sinadura motak:	Sinplea, aurreratua edo kualifikatua.	
			Sinatzeko tresna:	Ziurtagiriak (ikus 1. zerrenda). Nortasuna + 2AF (ikus 2. zerrenda)

Administrazio jardun automatizatua			
Sinatzailea:	Jarduna gauzatzen duen gailua		
	Hartzailea:	Unibertsitatea eta hirugarrenak	
		Aplikatu beharreko sinadura motak:	Aurreratua

	Sinatzeko tresna:	Zigilu elektronikoko ziurtagiria

Dokumentuen digitalizazio segurua				
Sinatzailea:	Langile publiko gaitua			
	Hartzailea:	Unibertsitatea eta hirugarrenak		
		Aplikatu beharreko sinadura motak:	Aurreratua edo kualifikatua.	
			Sinatzeko tresna:	Ziurtagiri profesionala
Sinatzailea:	Administrazio jardun automatizatua			
	Hartzailea:	Unibertsitatea eta hirugarrenak		
		Aplikatu beharreko sinadura motak:	Aurreratua	

	Sinatzeko tresna:	Zigilu elektronikoko ziurtagiria.

1. **UPV/EHUk onartutako ziurtagiri elektronikoetan oinarritutako sinadura elektronikoko sistemen 1. zerrenda**:

   Bere eginkizunak betetzen dituen unibertsitateko langilea

   a. Ziurtagiri elektroniko kualifikatu pertsonalak.

      i. Ziurtagiri elektroniko profesionala.

      ii. UPV/EHUko ordezkariaren ziurtagiri elektronikoa.

   Hirugarrenak

   b. Kualifikatu gabeko ziurtagiri elektroniko pertsonalak (pertsona fisikoa bakarrik).

   c. Ziurtagiri elektroniko kualifikatu pertsonalak.

      i. Pertsona fisikoaren ziurtagiri elektronikoa.

      ii. Ordezkari ziurtagiri elektronikoa.

   d. Zigilu elektronikoko ziurtagiri elektroniko kualifikatuak.

2. **UPV/EHUk onartutako gainerako sinadura elektronikoko sistemen 2. zerrenda**:

   a. Gako itunduak gehi sinatzeko borondatearen ebidentziak.

   b. Gako itunduak gehi sinatzeko borondatearen ebidentziak, bigarren autentifikazio faktorearen osagarriarekin batera.

   c. Sinadura elektroniko biometrikoa