

//Instalazionako eskuliburua
Izenpe ziurtagiri digitala//



Mac OS
Mac OS X 10.4 - Tiger

Izenpe s.a. 2009

Obra hau Creative Commons-en 3.0 lizentziaren mendekoa da (aitortu, ez komertziala, partekatu baimen beraren arabera). Kopia, bana eta jendaurrean komunika daiteke, betiere egilea zehazten bada eta helburu komertzialekin erabiltzen ez bada. Lizentzia osoa hemen kontsulta daiteke: <http://creativecommons.org/licenses/by-nc-sa/3.0/deed.es>. Izenpe, S.A. ez da izango dokumentuaren edizioan gerta litezkeen akatsen edo aipatu gabe gera litezkeen alderdien erantzule.

Edukiaren aurkibidea

1. Sarrera	4
1.1. Agiriaren egitura	4
1.2. Agiriaren norainokoa	4
1.3. Ofizialki onartzen diren hardware eta aplikazioak	4
1.4. Beste ohar batzuk	5
2. Driver-ak eta middlewareak instalatzea IZENPEren txartel kriptografikorako	5
2.1. Instalazioa	6
3. Irakurgailuak konfiguratzeko	7
3.1. Cherry RS 6600 USB irakurgailua eta beste batzuk	7
3.2. Gemplus GemPC Twin irakurgailua	7
3.3. BIT4ID ACR38 irakurgailua	7
3.3.1. Instalazioa	7
4. Aplikazioak konfiguratzeko	7
4.1. Web-nabigatzaileak	8
4.1.1. Safari.....	8
4.1.2. Firefox.....	8
Ziurtagirietarako modulua instalatzea	8
4.2. Posta-bezeroa	9
4.2.1. Mail.....	9
5. Ziurtapen-autoritateen ziurtagiriak instalatzea	9
5.1. Erroko ziurtagiriak eta mendekoak	9
5.2. Gakoen giltzatak	10
5.3. Firefox	11
6. Aplikazioen erabileren adibidea	12
6.1. Webguneetan identifikatzea	12
6.1.1. Safari.....	12
6.1.2. Firefox.....	13
6.2. Digitalki sinatutako posta-mezuak bidaltzea	13
6.3. Mail.....	13
6.3.1. Posta-kontua ziurtagiriarekin konfiguratzeko	13
6.3.2. Digitalki sinatutako posta-mezua bidaltzea	14
6.3.3. Postaren sinadura digitala egiaztatzea	14
7. Beste aplikazio osagarri batzuk	14
7.1. PINa aldatzea	14
7.1.1. Modu grafikoan, Firefox bidez	15
7.1.2. Komando-lerroaren bidez	15
7.2. PINa desblokeatzea	15
7.3. Agiri honi buruz	15

1. Sarrera

Euskal Autonomia Erkidegoan Mac erabiltzen dutenei beren ziurtagiriak erabiltzen laguntzeko eta hori errazteko ahaleginean, Izenpek hainbat eskuliburu prestatu ditu Izenperen ziurtagiri digitalak Mac OS X sistema eragilean instalatzeko eta konfiguratzeko beharrezkoak diren urratsak zehazteko helburuarekin.

Kasu honetan Tiger bertsioan Izenperen ziurtagiri digitalak erabili ahal izateko jarraitu beharreko prozesua deskribatuko dugu, euskal administrazio publikoak eskainitako zerbitzuetarako sarbidea ematen duten aplikaziorik garrantzitsuenekin.

1.1. Agiriaren egitura

Agiriak 5 atal sekuentzial ditu, eta horietan zehatz-mehatz adierazi da Izenperen ziurtagiri digitalak Mac OS X sisteman instalatzeko, konfiguratzeko eta erabiltzeko prozesu osoa:

- Driver-ak instalatzea Izenperen txartel kriptografikorako
- Onartzen dituen irakurgailuak konfiguratzea
- Onartzen dituen aplikazioak konfiguratzea
- Ziurtapen-autoritateen ziurtagiriak instalatzea
- Aplikazioen erabileren adibidea

Atal horietako bakoitzean prozesu osoa gauzatu ahal izateko beharrezko zereginak azalduko dira.

1.2. Agiriaren norainokoa

Agiri honek Mac OS X 10.4 sistemarekin erabil daitezkeen hardware plataforma guztiak instalatzeko eskuliburu izatea du xede, dela PowerPC plataforman, dela Intel plataforman.

Instalatzeko eta konfiguratzeko prozesuan zehar software libreko liburutegiak erabiltzen saiatu gara, betiere horiek ez badute izan ondorio zerbitzuaren kalitatea txikitzea.

1.3. Ofizialki onartzen diren hardware eta aplikazioak

Agiri honetan ezin diegu tartea egin merkatuan diren hardwareko gailu guztiei. Hori dela eta, Izenpek euskarria ofizialki txartel kriptografikoen honako USB irakurgailuei ematea erabaki da:

- Cherry RS 6600 USB (firmware: 1.06)
- Gemplus GemPC Twin (firmware: 1.0)
- BIT4ID ACR38 (firmware: 1.0)

Horiek guztiak Izenperen web-orriko dendaren bidez (<http://www.izenpedenda.com/>) edo baimendutako beste edozein hornitzailearen bidez lor daitezke. Gainera, beste irakurgailu batzuek ere funtzionatu ahal izango dute, eskura ditugun driver-en arabera.

Izenpek eskainitako zerbitzuetarako sarbidea izateko, ezinbestekoa da Izenperen ziurtagiriak erabiltzen dituzten tresnak eta aplikazioak izatea eskura. Ziurtagiri horiek erabiltzen dituzten aplikaziorik ohikoenak hiru kategoriatan multzokatu ditugu eta horiek instalatzeko eta Izenperen ziurtagiriek konfiguratzeko prozesua dokumentatzen saiatu gara.

Honakoak dira agiri honetan azalduko ditugun aplikazioak:

- Web-nabigatzaileak
 - Safari 3.1
 - Firefox 3.0
- Posta-bezeroa
 - Mail 2.1

1.4. Beste ohar batzuk

Multzo bakarrera bil genitzakeen urratsak izan badiren arren, agiri honetan egin beharreko ekintzak urratsez urrats azaltzen saiatu gara, ziurtagiri digitalen arkitektura eta Mac OS X sisteman oinarritutako instalazio eta konfiguraziorako prozesua hobeto ulertzeko helburuarekin.

Ziurtagiri digitalak instalatzeko ezinbestekoa da ordenagailuak Internetarako sarbidea izatea.

Ezinbestekoa da Mac OS X bertsioa 10.4.4. edo ondorengoa izatea. Erabilgarri dugun Mac OS X bertsioa zein den ezagutzeko egin klik hemen: [Apple](#) → [Mac honi buruz](#)



Aurreko bertsioen bat izanez gero, sistema eguneratu beharko duzu, honako menuaren bidez: [Apple](#) → [Softwarea eguneratzea](#).

Sistema instalatu eta konfiguratzeko prozesuan egin beharreko zereginetako batzuetan, beharrezkoa izango da fitxategi batzuen luzapena aldatzea. Mac OS X sisteman, fitxategi baten izena edo luzapena aldatzeko, hautatu egin behar da (aldatu nahi dugun fitxategiaren ikonoaren gainean klik eginez) eta ondoren “Enter” tekla sakatu. Fitxategiaren izena idazteko moduan egongo gara hori egin ondoren.

2. Driver-ak eta middlewareak instalatzea IZENPERen txartel kriptografikorako

Izenpek jaulkitako azken erabiltzaileko ziurtagiriak txartel kriptografikoan daude barne hartuta. Mac OS X sistemak txartelean barne hartutako datuekin elkarreragiteko beharrezkoak diren liburutegiak izateko, ezinbestekoa da opensc liburutegiak instalatzea.

Horrezaz gain, aplikazioek txarteletan barne hartutako ziurtagirietarako sarbidea izan dezaten, irakurgailuek middleware softwarea behar dute, hain zuzen ere, komunikazioen eta datuen transakzioak kudeatzeaz arduratuko dena. Mac OS X sisteman, irakurgailuen driver-ak dinamikoki kargatzeaz/deskargatzeaz eta horietarako konexioak kudeatzeaz arduratzen den zerbitzu baten bidez kudeatzen da middleware hori. [TokenD](#) izenarekin ezagutzen da zerbitzu hori.

Mac OS X Tiger bertsioak TokenD zerbitzurako 3 modulu baino ez ditu lehenetsita instalazioan.

- CAC: EEBBetako Gobernu Federalak erabiltzen duena.
- BELPIC: Belgian Personal Identity Card
- JPKI: Japanese Public Key Infrastructure card

Hori dela eta, ezinbestekoa da TokenD-rako OpenSC-ren modulua instalatzea Izenperen txartelean driver libreen bidez elkarreragiteko.

2.1. Instalazioa

Gutziz ezinbestekoa da Mac OS X bertsioa 10.4.4. edo ondorengoa izatea.

Proiektuaren web-orriaren deskargaren bidez ekingo diogu instalazioari.

<http://www.opensc-project.org/sca>

"Download" atalean OpenSC SCA-ren 0.2.2 bertsioa deskargatuko dugu (hori da Mac OS X Tiger bertsiorako gomendatutakoa).

<http://www.opensc-project.org/files/sca/sca-0.2.2.dmg>



Deskarga amaitutakoan, oharra agertuko zaigu eta onartu egin beharko dugu. Une horretan hasiko da instalazioa.

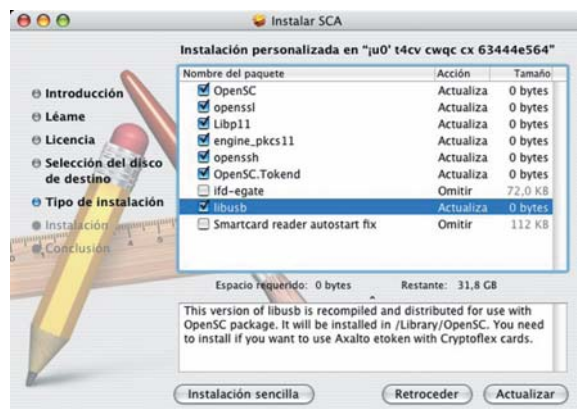


USB irakurgailuek euskarria izan dezaten, ezinbestekoa da instalazioan lehenetsita hornitzen ez den liburutegi bat instalatzea. Horretarako, instalazioa **Pertsonalizatzeko** aukera ematen digun tokian egingo dugu etena.



Pertsonalizatu sakatuko dugu eta **libusb**. markatuko.

Amaitzeko, **Eguneratu** sakatu. Instalazio amaituko da eta ekipoa berrabiaraziko dugu.



3. Irakurgailuak konfiguratzeari

3.1. Cherry RS 6600 USB irakurgailua eta beste batzuk

ccid liburutegia, CCID protokoloa (Chip Card Interface Device) ezartzen duena, merkatuko USB irakurgailu gehienek euskarri izaten saiatzen da. Mac OS X sistemetan barne hartuta dator.

Irakurgailu honen eta beste askoren euskarria osatuta egongo litzateke.

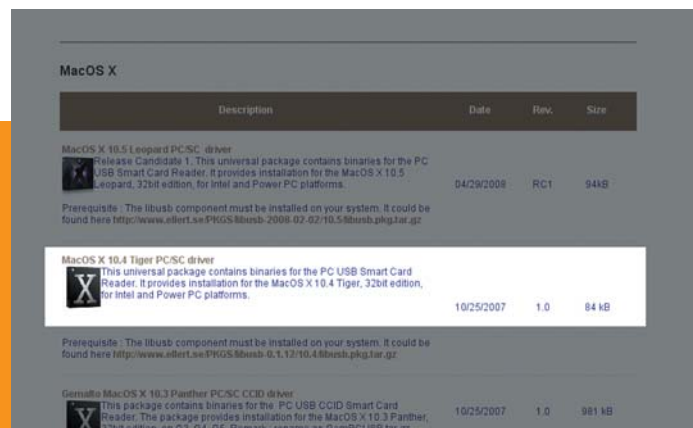
3.2. Gemplus GemPC Twin irakurgailua

Gemplus GemPC Twin irakurgailuak fabrikatzaileak emandako driver osagarri bat behar du. Ondorengo URLtik deskargatuko dugu. Mac 10.4 bertsiorako driver-a hautatuko dugu.

Irakurgailu honen eta beste askoren euskarria osatuta egongo litzateke.

<http://support.gemalto.com/?id=46>

Fabrikatzaileak emandako paketea deskargatuko dugu eta lehenetsita agertzen diren aukerekin instalatuko dugu. Amaitutakoan, sistema berrabiaraziko dugu.



BIT4ID ACR38 irakurgailua

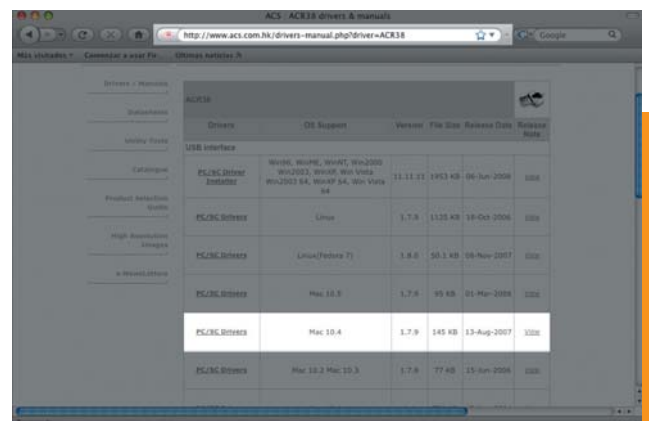
3.3.1. Instalazioa

BIT4ID ACR38 irakurgailuak fabrikatzaileak emandako driver bat behar du. Ondorengo URLtik deskargatuko dugu, 10.4 bertsiorako ataletik.

<http://www.acs.com.hk/drivers-manual.php?driver=ACR38>

Deskargatu beharreko fitxategiaren izenaren gainean egingo dugu klik. Instalazioari ekin eta lehenetsitako parametroak hautatu ondoren amaituko dugu.

Amaitutakoan, sistema berrabiaraziko dugu.



4. Aplikazioak konfiguratzeari

Mac OS X konektatu eta funtzionatu filosofiari jarraitzen saiatzen da. Horretarako, TokenD izeneko arkitektura zentralizatua garatu du, ziurtagiri digitalak kudeatzeko. Mac OS X sistemaren jatorrizko aplikazio guztiek erabiltzen dute arkitektura hori. Mozilla suiteko aplikazioek, aldiz, OpenSC-ren PKCS#11 modulua erabiltzen dute.

4.1. Web-nabigatzaileak

4.1.1. Safari

Safari nabigatzailean ez da konfiguraziorik egin behar ziurtagiri digitalak erabili ahal izateko.

4.1.2. Firefox

Ziurtagirietarako modulua instalatzea

Firefox menuko lehentasunen artean, egin klik **Aurreratu** aukeraren gainean, eta ondoren **Zifratu** fitxaren gainean, irudian ikus dezakegun bezala. Azkenik, berriz ere klik egingo dugu **Segurtasun-gailuak** botoiaren gainean.



Gailuen administratzailea Firefoxen segurtasun-moduluak kudeatzea ahalbidetzen duen tresna da. Lehenetsitako konfigurazioan 2 segurtasun-modulu izaten ditu, bata, aurrez instalatuta dauden lehenetsitako erroko ziurtagiriak kudeatzeko eta bestea, beharrezko liburutegiekin batera eranstean ditugun eta kanpokoak ez diren gainerako ziurtagiri guztietarako.

Behar dugun segurtasun-modulua eransteko, klik egingo dugu **Kargatu** botoiaren gainean.

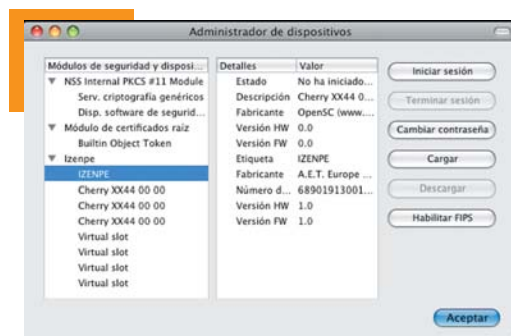
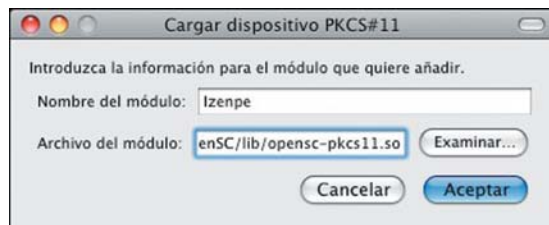
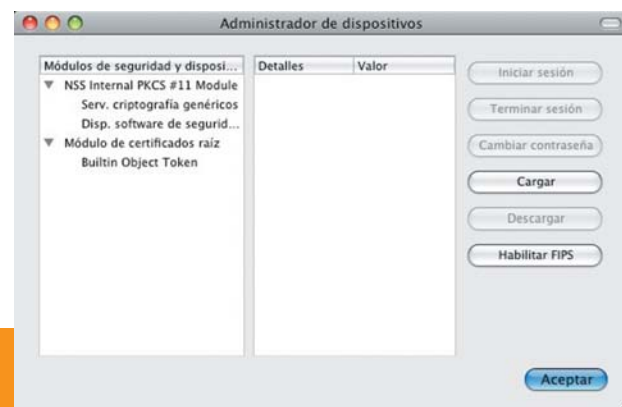


Leihu bat irekiko zaigu eta horrek emango digu aukera PKCS#11 modulua berria definitzeko. Kasu honetan integratzioko PKCS#11 modulua bat definitzea interesatzen zaigu, opensc liburutegiekin. Horretarako, honakoak definitu behar dira:

- **Moduluaren izena:** Opensc liburutegien segurtasun-moduluari erreferentzia egiten dion izen generikoa. Edozein izen jarriko dugu.
- **Moduluaren fitxategia:** moduluaren kokalekuaren ibilbide osoa (/Library/OpenSC/lib/opensc-pkcs11.so)



Ziurtagiria behar bezala instalatu dela egiaztatzeko, modulua berria egoki kargatu dela egiaztatu behar dugu:



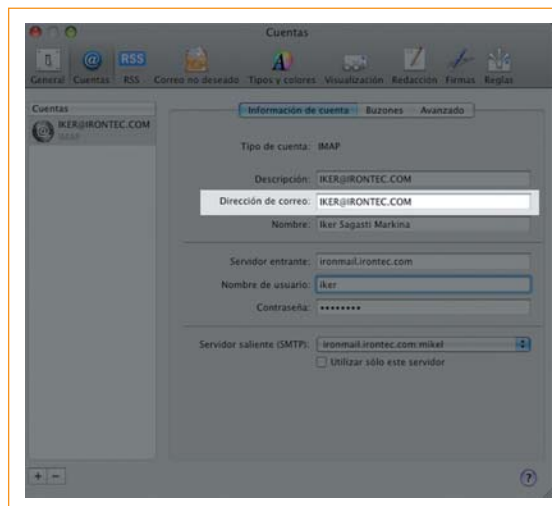
4.2. Posta-bezeroa

Sinatutako posta-mezuak bidali ahal izateko, ezinbestekoa da gakoaren erabilera hedatua izatea atributu gisa ziurtagiriak, zehatza esateko, posta elektronikoko babesa (OID 1.3.6.1.5.5.7.3.4). **Izenperen txarteletako batzuek bakarrik dute erabilera hedatu hori.**

4.2.1. Mail

Mail-en ez da konfiguraziorik egin behar ziurtagiri digitalak erabili ahal izateko.

Behar-beharrezkoa da gure posta-kontuan konfiguratutako posta-helbidea bat etortzea erabat gure ziurtagiriko posta-helbidearekin (letra larriak eta xeheak ere barne direla).



5. Ziurtapen-autoritateen ziurtagiriak instalatzea

5.1. Erroko ziurtagiriak eta mendekoak

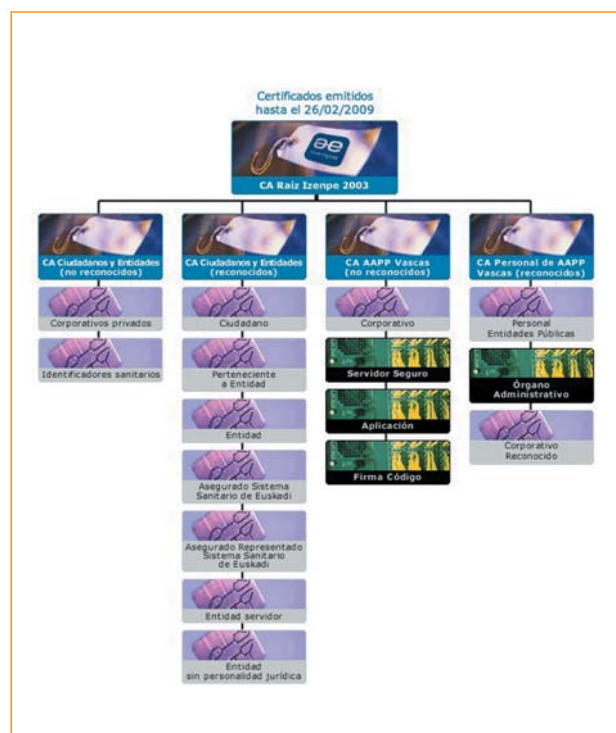
Izenpek ziurtapen-autoritateen eta mendekoen hierarkia bat prestatu du Internet bidez eskaintzen diren zerbitzuetara sartzerakoan sortzen diren premia desberdinei erantzun ahal izateko eta, hori dela eta, erabiltzaileak hainbat profilekin egiaztatzen ditu, kasuan kasu.

Ziurtagiri digitalak egoki erabiltzeko, ziurtagiri horiek sistemako datu-base batera inportatu behar dira, eta Safari eta Mail horrekin integratuko dira.

Erroko eta mendeko ziurtagiri horiek izenperen web-orrian aurki ditzakegu: www.izenpe.com Ziurtagiriak deskargatu.

Ziurtagiriak deskargatzeko, etiketa irudikatuta duten irudien gainean egin behar da klik. **Etiketa horietako bakoitzak erroko ziurtagiri bat edo mendeko bat irudikatzen du.**

Eskema hau Izenperen ziurtagirien **lehen hierarkiari** dagokio (2009ko otsailaren 26a baino lehen Izenpek jaulkitako ziurtagirietarako):

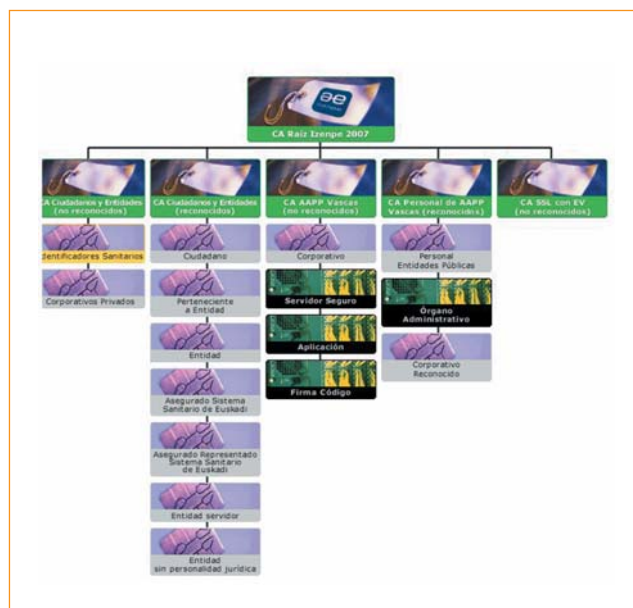




Eskema hau Izenperen ziurtagirien **hierarkia berriari** dagokio (2009ko otsailaren 26az geroztik Izenpek jaulkitako ziurtagirietarako):

Izenpek definitutako ziurtapen-autoritateen egituraren arabera, txartel bakoitza erroko autoritate batekin eta mendeko batekin bakarrik izango da baliozkoa. Horrek esan nahi du ez dela behar-beharrezkoa ziurtapen-autoritate guztien ziurtagiri guztiak inportatzea, dena delako aplikazioak ez dituelako horiek gure txartelarekin erabiliko. Haatik, autoritateen hierarkiaren funtzionamendua ez baduzu ondo ezagutzen, guztiak instalatzea gomendatzen dizugu, alegia, Izenperen aurreko ziurtapen-hierarkiari dagozkionak nahiz berriari dagozkionak.

Ondoren ikusiko dugu nola instalatu behar diren deskargatutako ziurtagiriak aplikazioetan:



5.2. Gakoen giltzatakhoa

Mac OS Xek "giltzen" sistema zentralizatu erabiltzen du, eta bertatik kudeatzen dira ziurtagiri guztiak. Kudeatzaile horrekin integratzen dira Mac OS Xen suiteko aplikazio guztiak, hala nola, Safari eta Mail. Ondoren ikusiko dugu nola instalatu behar diren deskargatutako ziurtagiriak **sistemaren gakoen giltzatakhoa**:

Aurrez aipatutako 5 ziurtagiriak deskargatuko ditugu, saguaren eskuineko botoiarekin klik eginez (edo teklatuko kontrol teklarekin) lotutako fitxategia deskargatzeko aukeran.



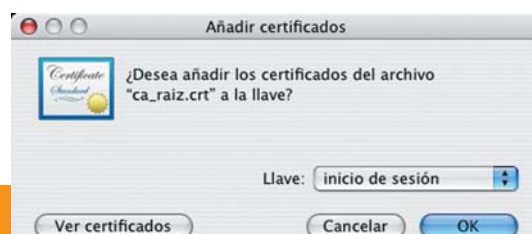
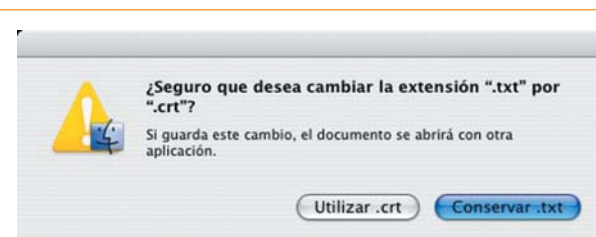
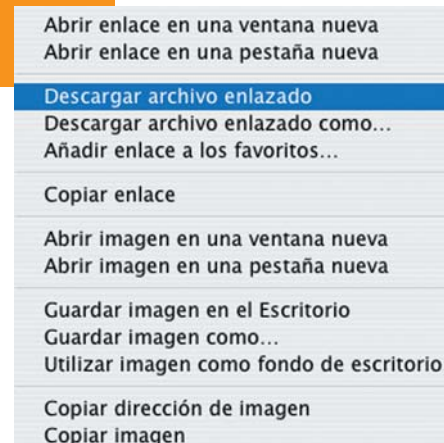
Fitxategia deskargatu ostean, fitxategiaren izena aldatu behar da, ".txt" luzapena kentzeko.

Izenperen CA deskargatzerakoan "ca_raiz.crt.txt" izeneko fitxategia deskargatzen bazaigu, izena aldatu eta "ca_raiz.crt" izena jarri beharko diogu.

Hori egiterakoan oharra agertuko zaigu, eta bertan crt. erabili erantzun dugu.



Klik bikoitza egingo dugu deskargatutako fitxategietan sistemaren Giltzatakhoetarakoan instalatzeko.

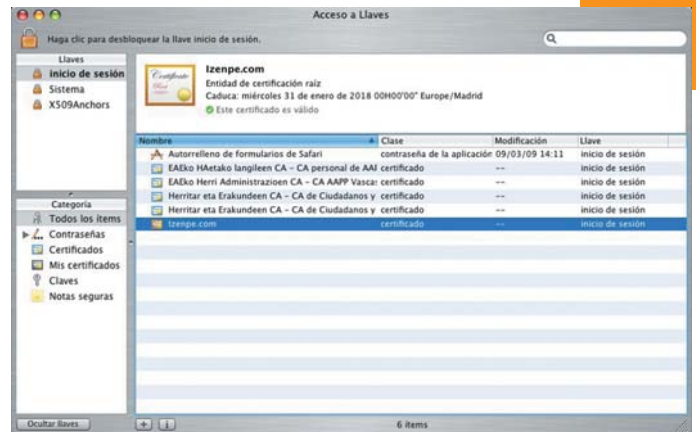




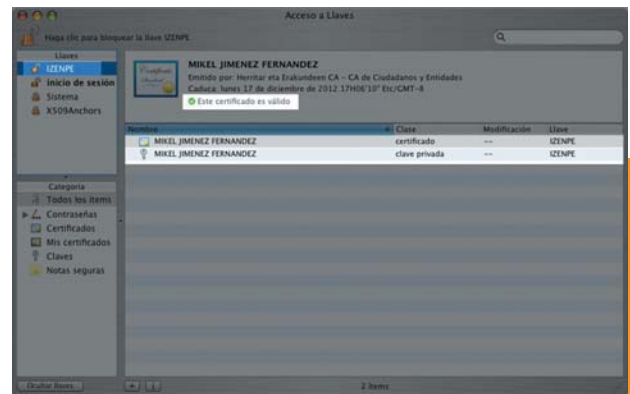
OK sakatu eta lizenperen erroko CA inportatuta izango dugu.

Gainerako mendekoekin ere prozesu berbera egingo dugu.

Inportazioa behar bezala egin dela egiaztatzeko, [Aplikazioak Giltzakoetarako](#) sarbidea aukeratu dugu, sistemako ziurtagirien kudeatzailean sartzeko.



lizenperen txartela sartzen badugu, ezkerrean eta goian IZENPE giltzen kudeatzailea agertzen dela ikusi ahal izango dugu, baita ziurtagiria konfiantzako dela adierazten duela ere.



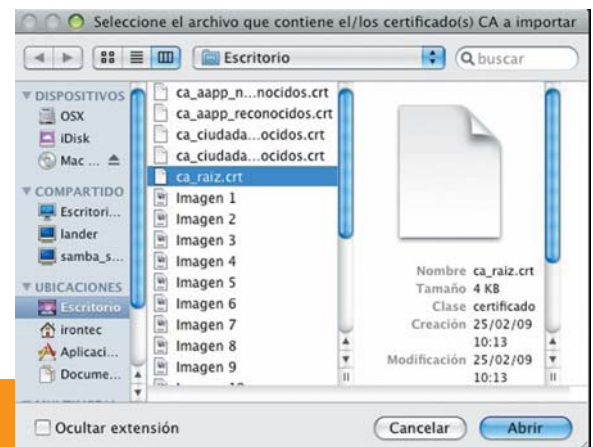
5.3. Firefox

Funtsezkoa da ziurtapen-autoritateen erroko ziurtagiriak Firefox nabigatzailean inportatzea kautotzeko eta sinatzeko prozesuak egin ahal izateko webguneetan. Nabigatzaileak ez baditu ziurtagiri horiek, zerbitzariak ezetsi egingo du sarbidea.

Inportatzeko, egin klik [Aurreratu](#) aukeraren gainean, Firefox menuko lehenetsun artean, eta ondoren [Zifratua](#) fitxaren gainean. Azkenik, [Ikus ziurtagiriak](#) botoiaren eta [Autoritateak](#) fitxaren gainean egingo dugu klik, irudian ikusten den bezala, erroko ziurtapen-autoritateen nahiz mendekoen ziurtagiriak inportatu ahal izateko.



lizenperen erroko ziurtapen-autoritateen eta mendekoen ziurtagiri guztiak inportatuko ditugu, banan-banan, [Inportatu](#) botoian klik egingez.





Erroko ziurtagiriak inportatzeko garaian, ziurtagirian jarriko dugun konfiantzari buruz galdetuko digu nabigatzaileak. 3 konfiantza-kategoria daude:

- Webguneak egiaztatzeko konfiantza
- Posta-erabiltzaileak egiaztatzeko konfiantza
- Software-garatzzaileak egiaztatzeko konfiantza

3 kategoriak aukeratuko ditugu.



Prozesu hori ziurtagiri guzti-guztiekin egin behar da.

Ziurtagiri berriak agertzen direla egiaztatzea.



6. Aplikazioen erabileren adibidea

6.1. Webguneetan identifikatzea

Egoki irizten ditugun kudeaketa-lanak egin ostean, oso garrantzitsua da webguneko saioa eta nabigatzailea ixtea, beste pertsona batzuk gure datuak erabiliz Interneten sartu ahal izatea saihesteko.

6.1.1. Safari

Ziurtagirien kokalekua dagokion atalean azaldutakoari jarraiki konfiguratu ostean, kautotzeko prozesu bat egingo dugu webgune batean, hain zuzen ere, Izenpek jaulkitako ziurtagiriarekin bertarako sarbidea egiaztatzen duen webgune batean: OSANET atarian.

Euskadiko Osasun atarian sartuko gara (<http://www.osanet.euskadi.net/>), eta **Zure zita medikoa erreserbatu** atalean egingo dugu klik. Ondoren agertuko zaigun leihoan **osasun-txartel elektronikoaren bidezko sarbidea** hautatuko dugu.

Guztia behar bezala konfiguratu badugu, beste leiho bat agertuko da, eta bertan Izenperen txartelaren PINa eskatuko digute.

PINa zuzen sartuko dugu eta gure ziurtagiria baliozkoa bada aplikazioan sartzeko eta ez badago ezeztatuta, aplikazioak sarbidea ahalbidetuko digu, bertaratu izan bagina izango genituzkeen berme bereberekin.



6.1.2. Firefox

Ziurtagirien kokalekua dagokion atalean azaldutakoari jarraiki konfiguratu ostean, kautotzeko prozesu bat egingo dugu webgune batean, hain zuzen ere, lizenpe jaulkitako ziurtagiriekin bertarako sarbidea egiaztatzen duen webgune batean: OSANET atarian.

Euskadiko Osasun atarian sartuko gara (<http://www.osanet.euskadi.net/>), eta Zure zita medikoa erreserbatu atalean egingo dugu klik. Ondoren agertuko zaigun leihoan osasun-txartel elektronikoaren bidezko sarbidea hautatuko dugu.

Guztia behar bezala konfiguratu badugu, beste leiho bat agertuko da, eta bertan lizenperen txartelaren PINa eskatuko digute.

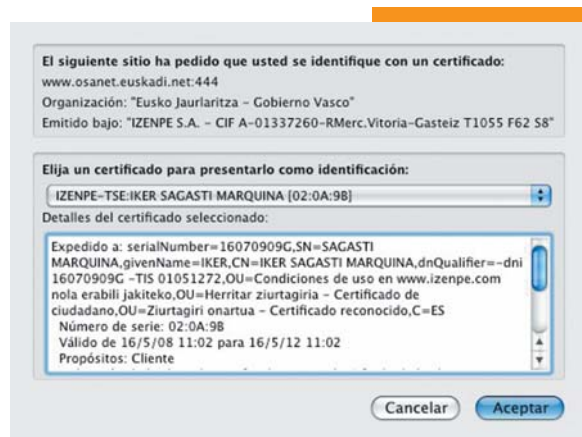


OHARRA: OSANET atarian sartzen garen lehen aldian, laster-leihoak baimentzearekin edo ez baimentzearekin zerikusia duen oharra agertuko zaigu. Kasu honetan laster-leihoak baimenduko ditugu.



PINa zuzena bada, beste leiho bat agertuko zaigu eta bertan hautatuko dugu erabili nahi dugun ziurtagiria.

Gure ziurtagiria baliozkoa bada aplikazioan sartzeko eta ez badago ezeztatuta, aplikazioak sarbidea ahalbidetuko digu, bertaratu izan bagina izango genituzkeen berme bereberekin.



6.2. Digitalki sinatutako posta-mezuak bidaltzea

Aurrez esan dugun bezala, sinatutako posta-mezuak bidali ahal izateko, ezinbestekoa da gakoaren erabilera hedatua izatea atributu gisa ziurtagiriak, eta lizenperen ziurtagirietako batzuek bakarrik dute erabilera hedatu hori.

Baliozko ziurtagiria izanda, nahikoa izango da posta-mezu berria sortzea, erabilgarri izango dugu eta mezuak sinatzeko aukera.

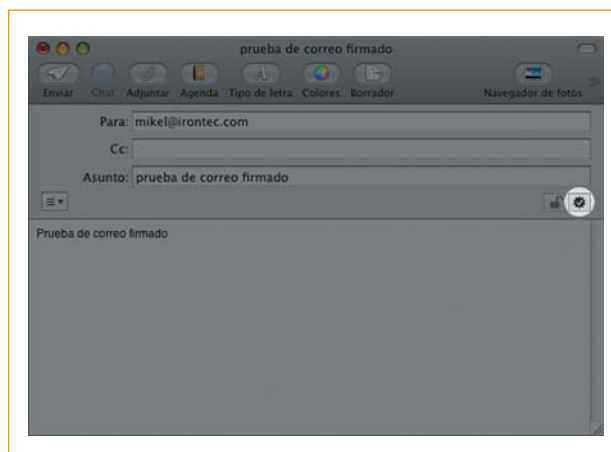
6.3. Mail

6.3.1. Posta-kontua ziurtaginiarekin konfiguratzeko

Ez da inolako konfigurazio osagarririk egin behar postako bezeroan, Mail-ek sistemako giltzatakoan konfiguratuta dauden ziurtagiriak erabiltzen dituelako.

6.3.2. Digitalki sinatutako posta-mezua bidaltzea

Digitalki sinatutako posta-mezua bidaltzeko, ezinbestekoa da hori adieraztea. Horretarako, ikonoak mezua digitalki sinatuko dela "tik" bidez adierazten duela ziurtatu beharko dugu.



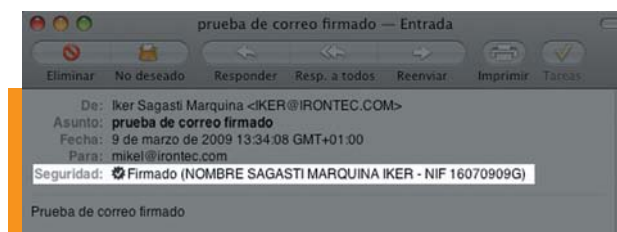
Ikus posta-mezua idazteko leihoaren erdialdean mezua digitalki sinatzeko aukera hautatu dugula adierazten duen ikonoa. Sinatutako mezua bidaltzen dugun lehen aldian sinatzea baimendu nahi dugun edo ez galdetuko digun leihoa agertuko zaigu. Beti baimentzeko aukeratuko dugu eta ez zaigu berriz agertuko ohar hori.



6.3.3. Postaren sinadura digitala egiaztatzea

Mail-ek posta-mezua digitalki sinatuta dagoela adierazten digun ikono bat erakusten digu.

Sinadura baliozkoa den egiaztatu ahal izateko, **ezinbestekoa da ziurtapen-autoritateen eta mendekoen erroko ziurtagiriak inportatuta izatea.**



Baliozkoa ez bada, hori ohartaraziko digu. Posta-mezua aldatu delako nahiz ziurtapen-autoritateen eta horien mendekoen erroko ziurtagiriak inportatu ez ditugulako.

7. Beste aplikazio osagarri batzuk

7.1. PINa aldatzea

PINa txartela galduz gero edo baimenik gabe erabiliz gero txartelean barne hartutako ziurtagiriaren segurtasuna bermatzeko erabiltzen den zifratze-sistema simetrikoa da. PINa aldatzeko, ezinbestekoa da uneko PINa ezagutzea. Gainera, txartelak ez du blokeatuta egon behar PINa sartzeko saioetan 3 kale edo gehiago egin direla eta.

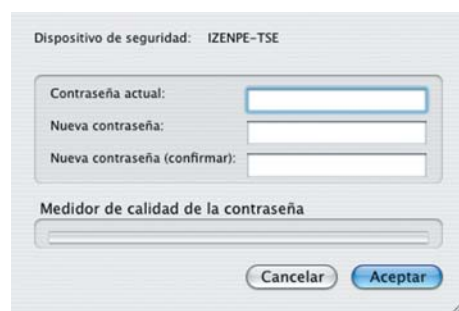
Izenperen txarteletan 4 eta 8 karaktere alfanumeriko artean erabil daitezke PINa definitzeko (a-z, A-Z, 0-9).

7.1.1. Modu grafikoan, Firefox bidez

Firefox menuaren lehentasunen artean, egin klik **Aurreratu** aukeraren gainean, eta ondoren **Zifratu** fitxaren gainean, irudian ikus dezakegun bezala. Azkenik, berriz ere klik egingo dugu **Segurtasun-gailuak** botoiaren gainean, eta jarraian **Aldatu pasahitza** sakatuko dugu.



Ondoren agertuko zaigun leihoak PINa aldatzeko aukera emango digu, betiere uneko PINa sartu ondoren.



7.1.2. Komando-lerroaren bidez

PINa aldatzeko, terminal batean sartu eta komando bat egikaritu behar dugu.

Terminalean sartzeko, hona joko dugu: Aplikazioak, terminala.

Terminalean sartu eta honako komandoa egikarituko dugu:

```
$ /Library/OpenSC/bin/pkcs11-tool --change-pin  
Please enter the current PIN:  
Please enter the new PIN:  
Please enter the new PIN again:  
PIN successfully changed
```

7.2. PINa desblokeatzea

Une honetan funtzio hori ez dute onartzen Izenperen txartelek Mac OS X plataformetarako.

7.3. Agiri honi buruz

Agiri hau elkarrekin prestatu dute Irontec, Internet y Sistemas sobre GNU/Linux enpresak eta zylk.net enpresak.

Agiri hau prestatzeko garaian, aztertzeko eta abian jartzeko metodologia benetan zaindua garatu da, eta bide horretatik bermatu da agiria erabiltzaileen premietara egokitzea.

Irakurleak alderdiren bat okerra dela uste badu edo akatsen bat aurkitzen badu, e-mail bidez jakinaraz diezaguke **cau-izenpe@izenpe.net** helbidean, eta agiriaren hurrengo bertsioetan kontuan hartzen saiatuko gara.

