

//Instalaziorako eskuliburua
Izenpe ziurtagiri digitala//



GNU/Linux
Ubuntu 8.04 LTS - Hardy Heron

© 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. Oharrak	5
1.5. Beste ohar batzuk	6
2. Driver-ak instalatzea IZENPEren txartel kriptografikorako	6
2.1. Ingurune grafikoaren bidezko instalazioa	6
2.2. Komando-lerroaren bidezko instalazioa	7
3. Irakurgailuak konfiguratzeko	7
3.1. Konfigurazio orokorra	7
3.1.1. Ingurune grafikoaren bidezko konfigurazioa	7
3.1.2. Komando-lerroaren bidezko konfigurazioa	7
3.2. Cherry RS 6600 USB, GemPlus GemPC Twin, C3PO LTC31 eta beste irakurgailu batzuk	8
3.2.1. Ingurune grafikoaren bidezko instalazioa	8
3.2.2. Komando-lerroaren bidezko instalazioa	8
3.3. BIT4ID ACR38 irakurgailua	8
3.3.1. Ingurune grafikoaren bidezko instalazioa	8
3.3.2. Komando-lerroaren bidezko instalazioa	9
4. Aplikazioak konfiguratzeko	9
4.1. Web-nabigatzaileak	9
4.1.1. Firefox.....	9
Ziurtagirietarako modulua instalatzea	9
4.1.2. Opera.....	10
4.2. Posta-bezeroak	10
4.2.1. Thunderbird.....	11
Ziurtagirietarako modulua instalatzea	11
Posta-kontua ziurtagiriarekin konfiguratzeko	11
Egiaztatzea	11
4.2.2. Evolution.....	11
Ziurtagirietarako modulua instalatzea	11
Posta-kontua ziurtagiriarekin konfiguratzeko	11

Egiaztatzea.....	12
4.2.3. KMail.....	12
4.3. Ofimatikako tresnak	12
4.3.1. OpenOffice.org.....	12
■ 5. Ziurtapen-autoritaten ziurtagiriak aplikazioetan instalatzea	13
5.1. Erroko ziurtagiriak eta mendekoak	13
5.1.1. Firefox.....	14
5.1.2. Thunderbird.....	15
5.1.3. Evolution.....	15
5.1.4. OpenOffice.org.....	16
■ 6. Aplikazioen erabileren adibidea	16
6.1. Webguneetan identifikatzea	16
6.1.1. Firefox.....	16
6.2. Digitalki sinatutako posta-mezuak bidaltzea	17
6.2.1. Thunderbird.....	18
Posta-kontua ziurtagiriarekin konfiguratzea	18
Digitalki sinatutako posta-mezua bidaltzea	18
Postaren sinadura digitala egiaztatzea	18
6.2.2. Evolution.....	19
Posta-kontua ziurtagiriarekin konfiguratzea	19
Digitalki sinatutako posta-mezua bidaltzea	20
Postaren sinadura digitala egiaztatzea	20
6.3. Dokumentu ofimatikoak sinatzea	20
6.3.1. OpenOffice.org.....	20
■ 7. Beste aplikazio osagarri batzuk	22
7.1. PINa aldatzea	22
7.1.1. Modu grafikoan, Firefox bidez	22
7.1.2. Komando-lerroaren bidez	23
7.2. PINa desblokeatzea	23
■ 8. Kredituak	23

1. Sarrera

Euskal Autonomia Erkidegoan software librea eta open source erabiltzen dutenei beren ziurtagiriak erabiltzen laguntzeko eta hori errazteko ahaleginean, Izenpek hainbat eskuliburu prestatu ditu Izenperen ziurtagiri digitalak GNU/Linux sistema eragilean instalatzeko eta konfiguratzeko beharrezkoak diren urratsak zehazteko helburuarekin.

Kasu honetan Ubuntu 8.04 LTS banaketan Izenperen ziurtagiri digitalak erabili ahal izateko jarraitu beharreko prozesua deskribatuko dugu, euskal administrazio publikoak eskaintako zerbitzuetarako sarbidea ematen duten aplikaziorik garrantzitsuenekin.

1.2 Agiriaren egitura

Agiriak 5 atal sekuentzial ditu, eta horietan zehatz-mehatz adierazi da Izenperen ziurtagiri digitalak GNU/Linux sisteman instalatzeko, konfiguratzeko eta erabiltzeko prozesu osoa:

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

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

1.2. Agiriaren norainokoa

Agiri honek Debian gisako banaketa guztietarako instalaziorako eskuliburua izatea du xede, hain zuzen ere, .deb paketeak eta paketeak kudeatzeko apt-get eta/edo aptitude tresnak dituztenetarako.

Agirian jaso dugun prozesua Ubuntu 8.04 LTSri dagokion berariaz, baina gainerako antzeko banaketak (hala nola, Debian GNU/Linux, Knoppix, Linux Mint, DreamLinux, Morphix) konfiguratzeko prozesua adierazitakoaren oso antzekoa izango da.

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)
- C3PO LTC31 (firmware: 0.36)

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 eskaintako 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 ziurtagiriekin konfiguratzeko prozesua dokumentatzen saiatu gara.

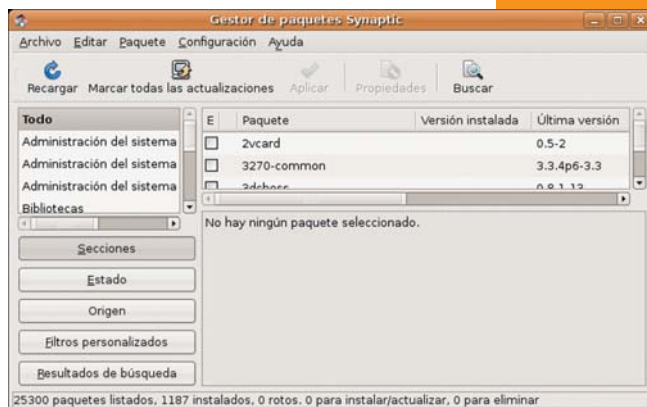
Honakoak dira agiri honetan azalduko ditugun aplikazioak:

- Web-nabigatzaileak
 - Firefox 3
 - Opera 9.63
- Posta-bezeroak:
 - Thunderbird 2
 - Evolution 2.22
 - Kmail 1.9
- Ofimatikako tresnak
 - OpenOffice.org 2.4

1.4. Oharrak

Agirian zehar kasu batzuetan beharrezkoa izango da software edo liburutegi jakin batzuk instalatzea, hardwareko gailuak erabili ahal izateko. Prozesu horri begira, bi hurbilpen zehaztuko ditugu zereginak egiteko. Horien artean erabiltzaileak aukeratu ahal izango du:

- **Modu grafikoa:** ingurune grafikoaren bidez. Instalazio grafikoa Synaptic softwarearen bidez egingo da.



- **Kontsola moduan:** komando-lerroaren bidez. Komando-lerroaren bidezko instalazioa Terminal-aren bidez egingo da. Egingo ditugun ekintzetako batzuetarako ezinbestekoa izango da superrabiltzailearen pribilegioak edo "root" izatea. Hori dela eta, aurrerantzean traol (#) bidez adieraziko ditugu hori behar duten ekintza guztiak.



1.5. 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 GNU/Linux sisteman oinarritutako instalazio eta konfiguraziorako prozesua hobeto ulertzeko helburuarekin.

Ziurtagiri digitalak instalatzeko ezinbestekoa da ordenagailuak Interneteko sarbidea izatea.

Gainera, ezinbestean egiaztatu beharko dugu sistemak Ubuntu-ren ondorengo **Universe** errepositorioetarako sarbidea duela (konfigurazioan lehenesten dira). Synaptic aplikazioan egiaztatzeko hori (**Konfigurazioa** → **Errepositorioak**).



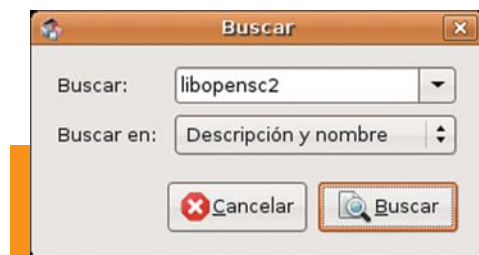
2. Driver-ak instalatzea IZENPERen txartel kriptografikorako

Izenpek jaulkitako azken erabiltzaileko ziurtagiriak txartel kriptografikoan daude barne hartuta. GNU/Linux sistemak txartelean barne hartutako datuekin elkarreragiteko beharrezkoak diren liburutegiak izateko, ezinbestekoa da **opensc** liburutegiak instalatzea.

2.1. Ingurune grafikoaren bidezko instalazioa

Paketeak kudeatzeko **Synaptic** tresnaren bidez ekingo diogu instalazioari.

Synaptic aplikazioaren **Bilatu** botoiaren bidez bilatuko dugu paketea.



Instalatu nahi dugun liburutegia adieraziko dugu, **libopensc2**, eta **Bilatu** sakatuko. Jarraian paketea hautatuko dugu eta instalatzeko markatuko dugu.

Instalatzeko paketea adierazi ostean, aldaketak aplikatuko ditugu eta prozesua osatu arte itxarongo dugu.



2.2. Komando-lerroaren bidezko instalazioa

Komando-lerroaren terminal bat irekiko dugu eta superrerabiltzaile moduan ondorengo komandoa egikarituko dugu:

```
# apt-get install libopensc2
```

3. Irakurgailuak konfiguratzeari

3.1. Konfigurazio orokorra

Aplikazioek txarteletan barne hartutako ziurtagirietarako sarbidea izan dezaten, irakurgailuek middleware softwarea behar dute, hain zuzen ere, komunikazioen eta datuen transakzioak kudeatzeaz arduratuko dena. GNU/Linux sisteman, irakurgailuen driver-ak dinamikoki kargatzeaz/deskargatzeaz eta horietarako konexioak kudeatzeaz arduratzen den zerbitzu baten bidez kudeatzen da middleware hori.

Jarraian **PC/SC** multzoa instalatuko dugu.

3.1.1. Ingurune grafikoaren bidezko instalazioa

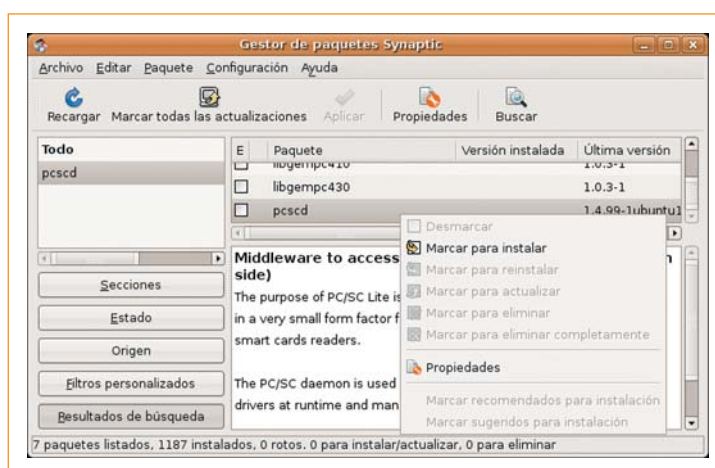
Paketeak kudeatzeko **Synaptic** tresnaren bidez ekingo diogu instalazioari.

Synaptic aplikazioaren **Bilatu** botoiaren bidez bilatuko dugu paketea.



Instalatu nahi dugun liburutegia adieraziko dugu, **pcscd**, eta **Bilatu** sakatuko. Jarraian paketea hautatuko dugu eta instalatzeko markatuko dugu.

Instalatzeko paketea adierazi ostean, aldaketak aplikatuko ditugu eta prozesua osatu arte itxarongo dugu.



3.1.2. Komando-lerroaren bidezko instalazioa

Komando-lerroaren terminal bat irekiko dugu eta superrerabiltzaile moduan ondorengo komandoa egikarituko dugu:

```
# apt-get install pcscd
```

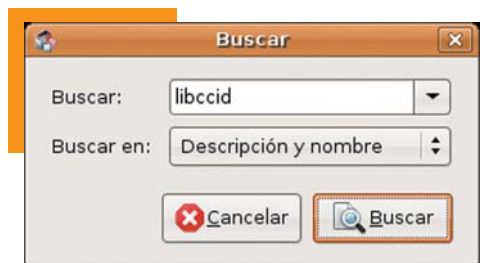
3.2. Cherry RS 6600 USB, GemPlus GemPC Twin, C3PO LTC31 eta beste irakurgailu batzuk

ccid liburutegia, CCID protokoloa (Chip Card Interface Device) ezartzen duena, merkatuko USB irakurgailu gehienen euskarri izaten saiatzen da.

3.2.1. Ingurune grafikoaren bidezko instalazioa

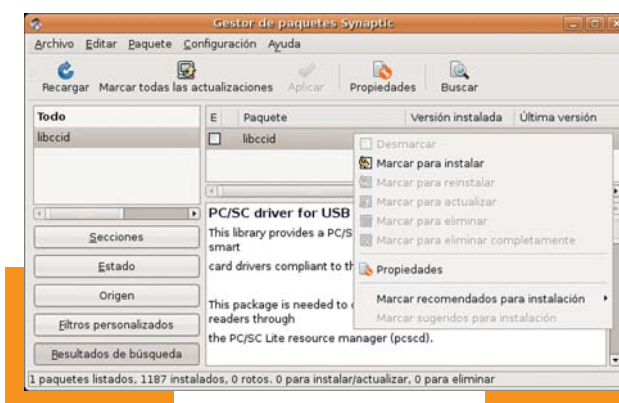
Paketeak kudeatzeko **Synaptic** tresnaren bidez ekingo diogu beharrezko liburutegien instalazioari.

Synaptic aplikazioaren **Bilatu** botoiaren bidez bilatuko dugu paketea.



Instalatu nahi dugun liburutegia adieraziko dugu, **libccid**, eta **Bilatu** sakatuko. Jarraian paketea hautatuko dugu eta instalatzeko markatuko dugu.

Instalatzeko paketea adierazi ostean, aldaketak aplikatuko ditugu eta prozesua osatu arte itxarongo dugu.



3.2.2. Komando-lerroaren bidezko instalazioa

Komando-lerroaren terminal bat irekiko dugu eta superrerrabiltzaile moduan ondorengo komandoa egikarituko dugu:

```
# apt-get install libccid
```

3.3. BIT4ID ACR38 irakurgailua

3.3.1. Ingurune grafikoaren bidezko instalazioa

Paketeak kudeatzeko **Synaptic** tresnaren bidez ekingo diogu instalazioari.

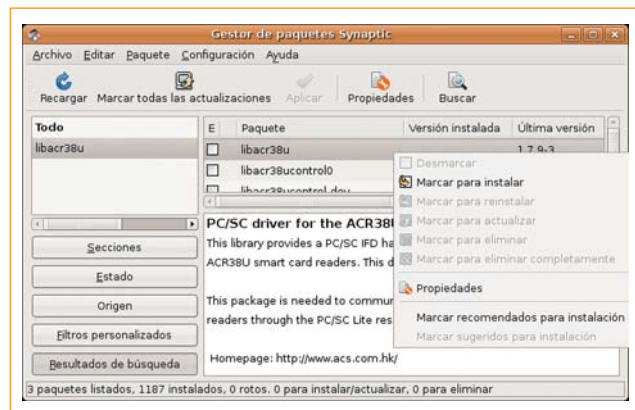
Synaptic aplikazioaren **Bilatu** botoiaren bidez bilatuko dugu paketea.





Instalatu nahi dugun liburutegia adieraziko dugu, **libacr38u**, eta **Bilatu** sakatuko. Jarraian paketea hautatuko dugu eta instalatzeko markatuko dugu.

Instalatzeko paketea adierazi ostean, aldagetak aplikatuko ditugu eta prozesua osatu arte itxarongo dugu.



3.3.2. Komando-lerroaren bidezko instalazioa

Komando-lerroaren terminal bat irekiko dugu eta superrerrabiltzaile moduan ondorengo komandoa egikarituko dugu:

```
# apt-get install libacr38u
```

4. Aplikazioak konfiguratzeko

Zoriturrez, GNU/Linux sistema eragileak ez du ezarrita, sistema eragilearen mailan, ziurtagiri digitalak kudeatzeko arkitektura zentralizatua. Gaur egun Mozilla suitearena da ezarketarik aurreratuena, **PKCS#11** moduluen bidezkoa, eta beste aplikazio askok erabiltzen dute hori, aurrerago ikusi ahal izango dugun bezala.

4.1. Web-nabigatzaileak

4.1.1. Firefox

Firefox da GNU/Linux sistemako nabigatzaile nagusia.

Ziurtagirietarako modulua instalatzea

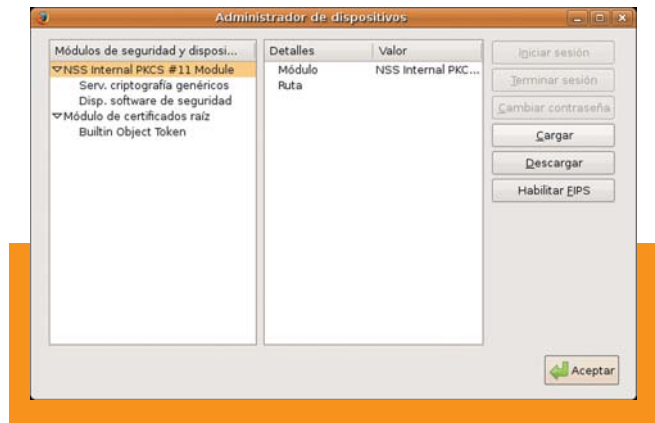
Editatu menuko lehentasunen artean, egin klik **Aurreratu** aukeraren gainean, eta ondoren **Zifratua** fitxaren gainean, irudian ikus dezakegun bezala. Azkenik, berriz ere klik egingo dugu **Segurtasun-gailuak** botoiaren gainean.





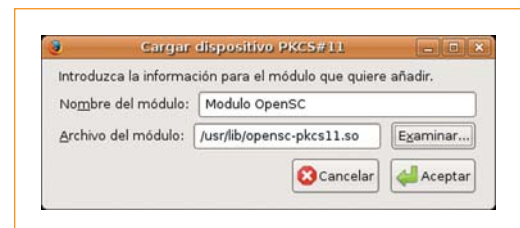
Gailuen administratzailea Firefoxen segurtasun-moduluak kudeatzea ahalbidetzen duen tresna da. Lehenetsitako konfigurazioan 2 segurtasun-modulu izaten ditu, bata, aurrez instalatuta dauden lehenetsitako erroko ziurtagiriak kudeatzeko eta bestea, beharrezko liburutegiekin batera eranstean ditugun eta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

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

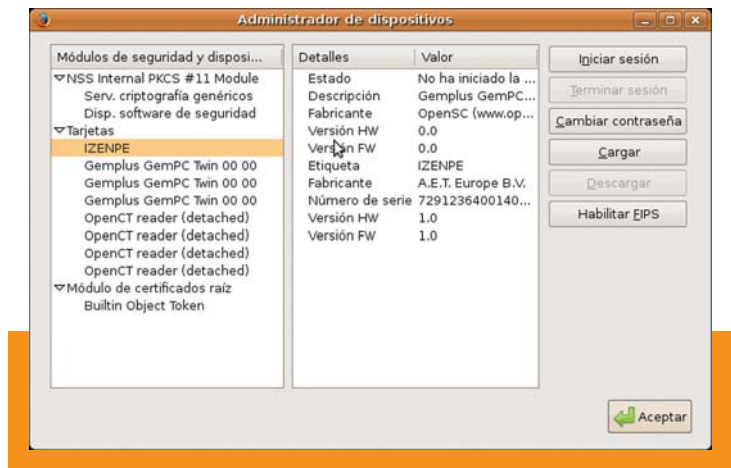


Leiho bat irekiko zaigu eta horrek emango digu aukera PKCS#11 modulu berria definitzeko. Kasu honetan integratzioko PKCS#11 modulu bat definitzea interesatzen zaigu, opensc liburutegiekin. Horretarako, honakoak definitu behar dira:

- **Moduluaren izena:** Opensc liburutegien segurtasun-moduluari erreferentzia egiten dion izen generikoa. Edozein izen jarriko dugu.
- **Moduluaren fitxategia:** moduluaren kokalekuaren ibilbide osoa



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



4.1.2. Opera

Opera nabigatzailearen gaur egungo bertsioak software motako ziurtagirietarako euskarria du (PKCS#12). Beraz, ez da bateragarri Izenpek jaulkitako ziurtagiriekin.

4.2. Posta-bezeroak

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. Thunderbird

Thunderbird konfiguratzeko prozesua Firefox nabigatzailearen antzekoa da oso.

Ziurtagirietarako modulua instalatzea

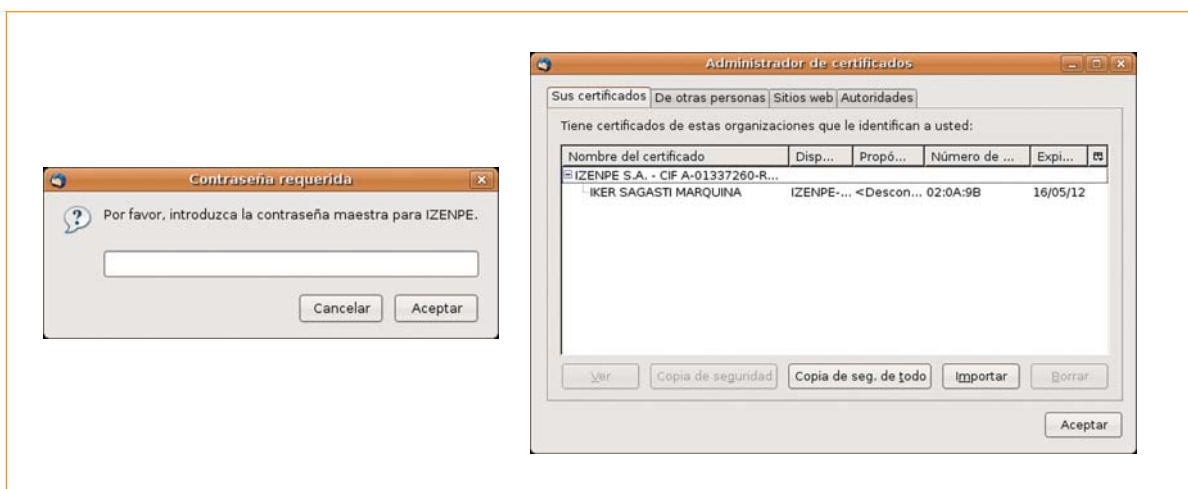
Ziurtagiriak eta PKCS#11 modulua instalatzeko, ikus Firefoxen konfigurazioa dagokion atalean.

Posta-kontua ziurtagiriarekin konfiguratzea

Posta-kontua dagokion ziurtagiriarekin nola konfiguratzen den aurreragoko beste atal batean azalduko dugu.

Egiaztatzea

Egiaztatzea Ziurtagiriak behar bezala kargatu direla egiaztatzeko bide hauxe egingo dugu: [Editatu](#) → [Lehentasunak](#) → [Aurreratua](#) → [Ziurtagiriak](#) → [Ikus ziurtagiriak](#), eta jarraian txartelaren sarbideko PINa eskatuko digu.



4.2.2. Evolution

Ziurtagirietarako modulua instalatzea

Jatorrian software ziurtagiriak (PKCS#12) bakarrik onartzen ditu Evolution kudeatzaileak. Izenpe gailu kriptografikoen bidez bakarrik ditu hardware-ziurtagiriak. Hori dela eta, hori erabili ahal izateko, sisteman egokitzapen txiki bat egin beharko dugu. Evolution kudeatzaileak Mozillaren NSS liburutegiak (Network Security Services) erabil ditzake, eta beraz, Mozillaren ziurtagirien biltegia Evolution kudeatzailearen biltegiarekin lotuko dugu.

Hori egiteko modurik dotoreena lotura sinboliko batzuen bidezkoa da, gisa horretan sinkronizatuta izango ditugulako Firefox eta Evolution-en segurtasun-gailuen konfigurazioak (kopiatu egingo bagenu, zerbait aldatzen dugun bakoitzean berriz ere kopiatu egin beharko genuke).

Horretarako, terminal bat ireki beharko dugu, eta honako komandoa egikaritu:

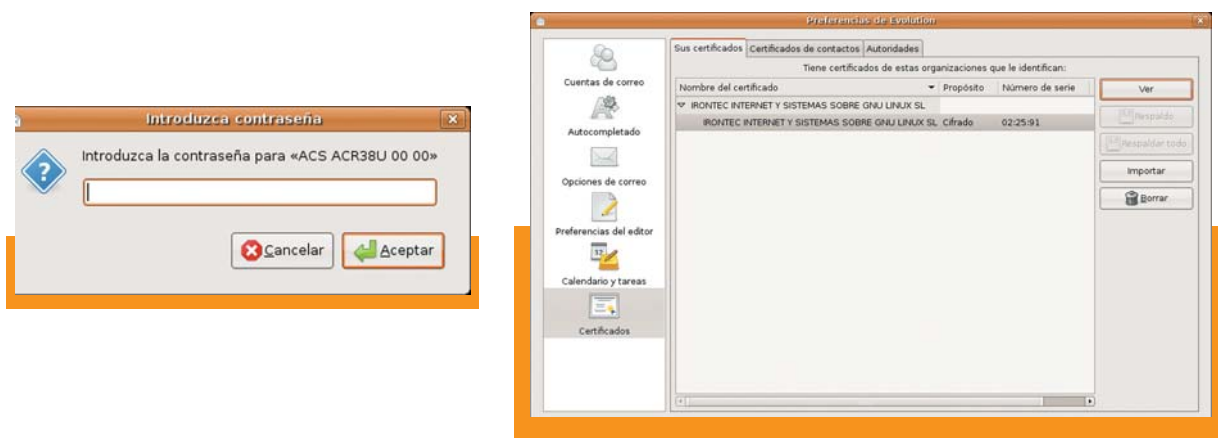
```
$ ln -sf $HOME/.mozilla/firefox/*.*.default/*.*.db $HOME/.evolution/
```

Posta-kontua ziurtagiriarekin konfiguratzea

Posta-kontua dagokion ziurtagiriarekin nola konfiguratzen den dagokion atalean azalduko dugu.

Egiaztatzea

Ziurtagiriak behar bezala kargatu direla egiaztatzeko **Editatu** → **Lehentasunak** aukeratuko dugu, eta jarraian txartelaren sarbideko PINa eskatuko digu.



4.2.3. KMail

KMail-en gaur egungo bertsioak software motako ziurtagirietarako euskarria du (PKCS#12). Beraz, ez da bideragarri lizenpek jaulkitako ziurtagiriekin.

4.3. Ofimatikako tresnak

4.3.1. OpenOffice.org

OpenOffice.org suiteak ez du ziurtagirien kudeatzaile propioirik. Dena dela, sisteman egokitzapen txiki bat eginez gero, Mozillaren suitearen ziurtagirien biltegia erabiltzeko gai da. Hori dela eta, OpenOffice.org suitearekin dokumentu ofimatikoak sinatu ahal izateko, ezinbesteko eskakizun da ziurtagiri digitaletarako sarbidea aurrez konfiguratuta izatea, Firefox edo Thunderbird-en bidez.

OpenOffice.org suiteak ingurunekeo aldagai bat (MOZILLA_CERTIFICATE_FOLDER) erabiltzen du ziurtagirien datu-basearen kokalekua ezagutzeko. Horretarako, aldagai hori definitu beharko dugu, Firefox edo Thunderbird-ek ziurtagiriak gordetzeko erabiltzen duten direktorioari egiteko erreferentzia. Komandoen terminala irekiko dugu eta honakoa egikaritzeko dugu (lerro-jauzirik gabe):

```
$ echo 'export MOZILLA_CERTIFICATE_FOLDER=$(find $HOME/.mozilla/firefox/ -name *.default)' >>  
$HOME/.bashrc
```

Gisa horretan, aldagaiaren definizioa iraunkorra izango da. Saioa itxi egin behar da eta berriz sartu, aldaketa gauza dadin. Erabiltzaile aurreratuek honako komandoa egikaritu ahal izango dute, nahi izanez gero, saiotik irteteko premiarik ez izateko:

```
$ . $HOME/.bashrc
```

5. Ziurtapen-autoritateen ziurtagiriak aplikazioetan 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.

Aplikazio errealetan ziurtagiri digitalak egoki erabili ahal izateko, funtsezkoa da Izenperen erroko ziurtagiriak eta mendekoak inportatzea. Horiek izenperen web-orrian aurki ditzakegu: www.izenpe.com → [Ziurtagiriak deskargatu](#).

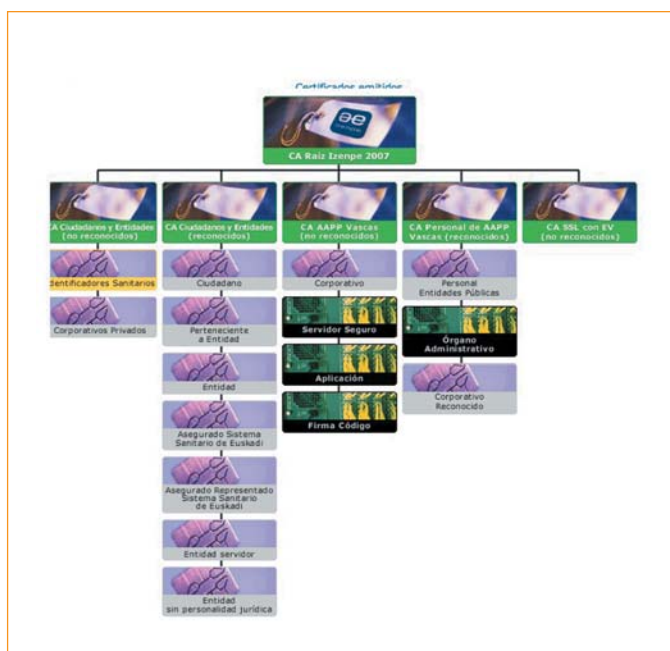
Ziurtagiriak deskargatzeko, etiketa irudikatuta duten irudien gainean egin behar da klik. **Etiketa horietako bakoitzak erroko ziurtagiri bat edo mendeko bat irudikatzen du.**



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):



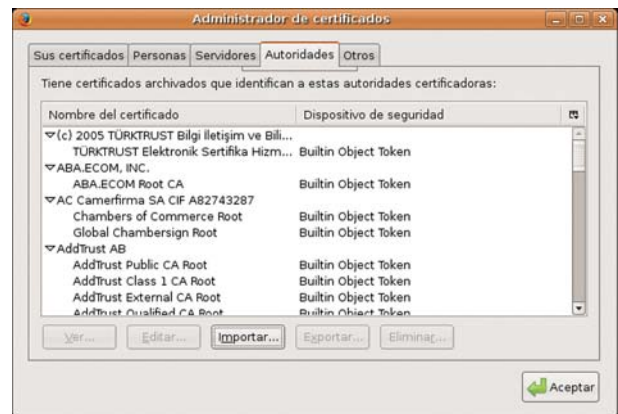
Izenpek definitutako ziurtapen-autoritateen egituraren arabera, txartel bakoitza erroko autoritate batekin eta mendeko batekin bakarrik izango da baliozkoa. Horrek esan nahi du ez dela behar-beharrezkoa ziurtapen-autoritate guztien ziurtagiri guztiak inportatzea, dena delako aplikazioak ez dituelako 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:

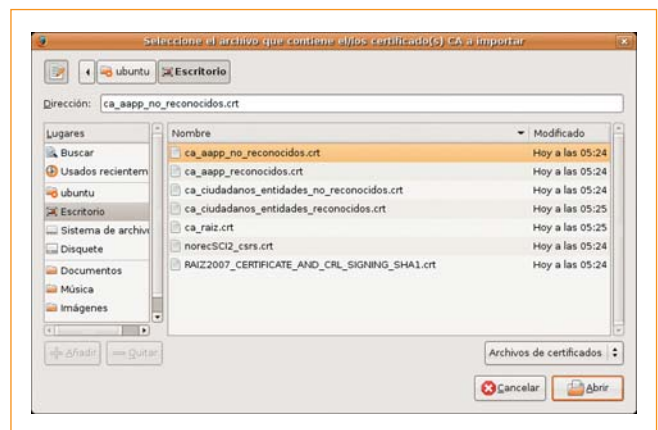
5.1.1. Firefox

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 [Aurreratua](#) aukeraren gainean, editatu menuko lehentasunen 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.



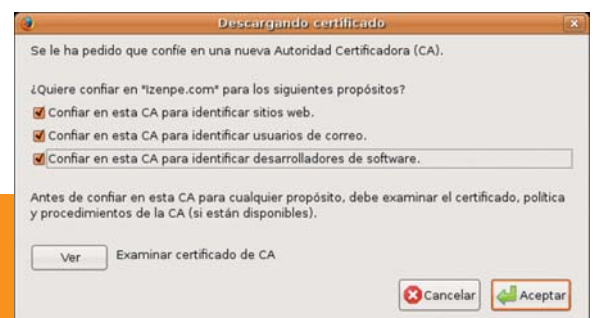
Izenperen erroko ziurtapen-autoritateen eta mendekoen ziurtagiri guztiak inportatuko ditugu, banan-banan, [Inportatu](#) botoian klik eginez.



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

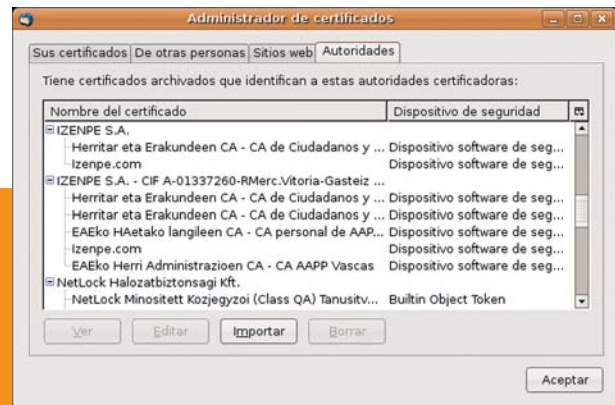
- Webguneak egiaztatzeko konfiantza
- Posta-erabiltzaileak egiaztatzeko konfiantza
- Software-garatzzaileak egiaztatzeko konfiantza

3 kategoriak aukeratuko ditugu.





Prozesu hori ziurtagiri guzti-guztiekin egin behar da. Ziurtagiri berriak agertzen direla egiaztatzea dezakegu:



5.1.2. Thunderbird

Garrantzitsua da ziurtapen-autoritateen erroko ziurtagiriak Thunderbird-era inportatzea posta-mezuen sinadura baliozkotzeko prozesuak egin ahal izateko. Posta-bezeroak ziurtagiri horiek ez baditu, ez da izango gai igorlearen edo postaren osotasunaren kautotasuna bermatzeko.

Thunderbird konfiguratzeko prozesua Firefox nabigatzailearenaren antzekoa da. Beraz, ikus Firefox nabigatzailearen konfigurazioa dagokion atalean.

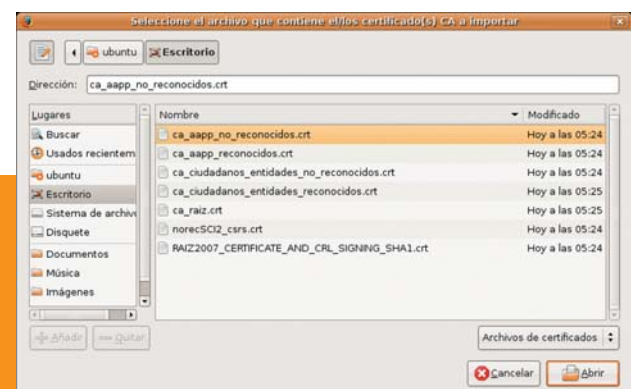
5.1.3. Evolution

Garrantzitsua da ziurtapen-autoritateen erroko ziurtagiriak Evolution-era inportatzea, posta-mezuen sinadura baliozkotzeko prozesuak egin ahal izateko. Posta-bezeroak ziurtagiri horiek ez baditu, ez da izango gai igorlearen edo postaren osotasunaren kautotasuna bermatzeko.

Egin klik **Ziurtagiriak** aukeraren gainean, editatu menuko lehenetsun artean, eta ondoren **Autoritateak** fitxaren gainean. Berriz ere klik egingo dugu **Inportatu** botoiaren gainean.



Izenperen erroko ziurtapen-autoritateen eta mendekoen ziurtagiri guztiak inportatuko ditugu, banan-banan, **Inportatu** botoian klik eginez.





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

- Webguneak egiaztatzeko konfiantza
- Posta-erabiltzaileak egiaztatzeko konfiantza
- Konfianza en verificaciones sobre desarrolladores de software

3 kategoriak aukeratuko ditugu.



Prozesu hori CAko ziurtagiri guzti-guztiekin egin behar da.

Ziurtagiri berriak agertzen direla egiaztatu dezakegu:



5.1.4. OpenOffice.org

OpenOffice.org suiteak ez du ziurtagiriaren kudeatzaile propioirik, eta beraz, Firefox edo Thunderbird-en dauden ziurtagiriak erabiltzen ditu. Autoritateen erroko ziurtagiriak aplikazio horien bidez inportatzen ditu.

6. Aplikazioen erabileren adibidea

6.1. Webguneetan identifikatzea

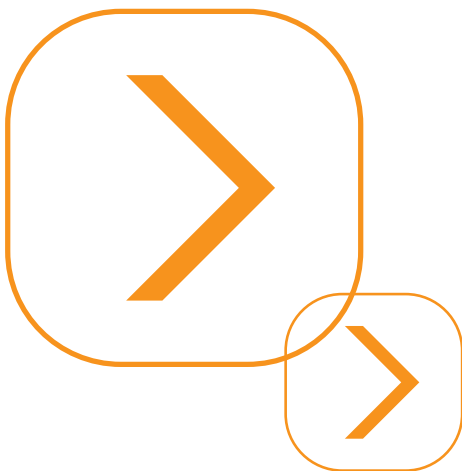
6.1.1. Firefox

Ziurtagiriaren 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.

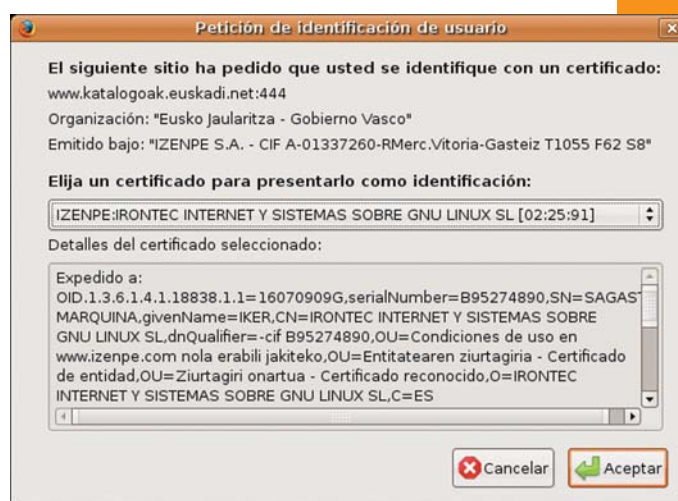
Euskadiko Osasun atarian sartuko gara (<http://www.osanet.euskadi.net/>), eta Zure zita medikoa **erreserbatu** atalean egingo dugu klik. Ondoren agertuko zaigun leihoan **osasun-txartel elektronikoaren bidezko** sarbidea hautatuko dugu.

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

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 behar bezala sartu eta beste leiho bat agertuko zaigu. Zerbitzarian instalatuta dauden ziurtagirien arteko zeinekin kautotu nahi dugun aukeratu ahal izango dugu bertan. Izenperen ziurtagiria hautatuko dugu eta **Ados** aukeraren gainean egingo dugu klik.



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

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

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 Izenperen ziurtagirietako batzuek bakarrik dute erabilera hedatu hori.

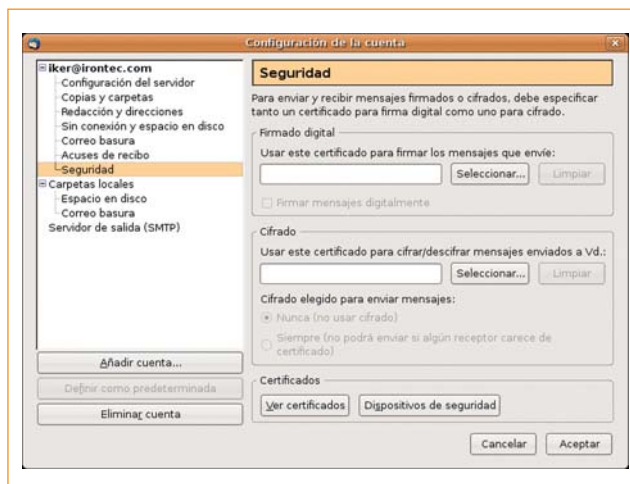
Baliozko ziurtagiria dugunean, beharrezkoa izango da posta-kontua dena delako ziurtagiri hori lotzea. Posta-kontu hori ziurtagirian barne hartutako bera izan daiteke.

Ikus dezagun zeregin hori nola egiten den posta-bezero desberdinetan.

6.2.1. Thunderbird

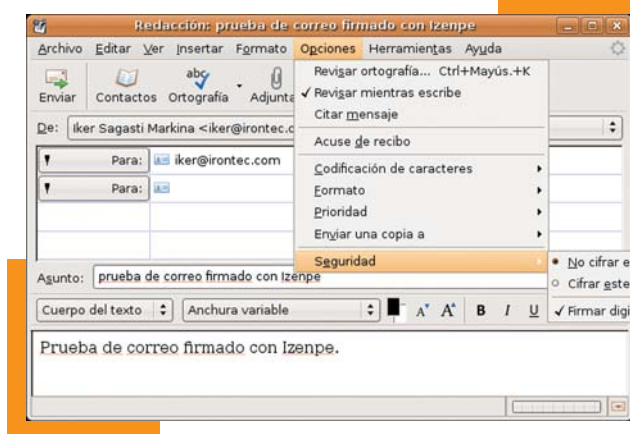
Posta-kontua ziurtagiriarekin konfiguratzeko

Editatu menuko **Kontuen konfigurazioa** atalean, egin klik **Segurtasuna** atalean, dagokion kontuan. Ondoren hautatu ziurtagiria.



Digitalki sinatutako posta-mezua bidaltzea

Digitalki sinatutako posta-mezua bidaltzeko, ezinbestekoa da hori adieraztea. Irtendako posta-mezu guztiak digitalki sinatzeko aukera ez badugu adierazita, hori eskuz egin ahal izango dugu, menu honi jarraiki: **Aukerak** → **Segurtasuna** → **Digitalki sinatzea mezu hau**.



Ikus posta-mezua idazteko leihoaren beheko aldean mezua digitalki sinatzeko aukera hautatu dugula adierazten duen ikonoa.

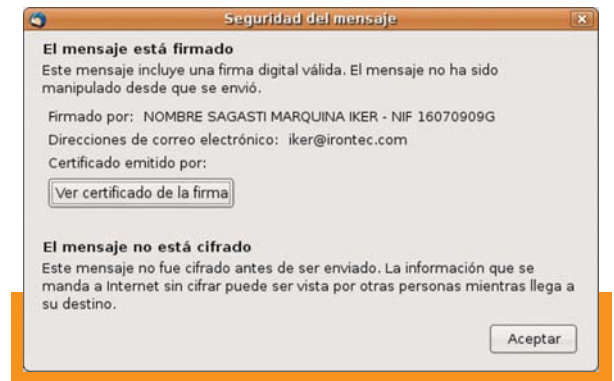
Postaren sinadura digitala egiaztatzea

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

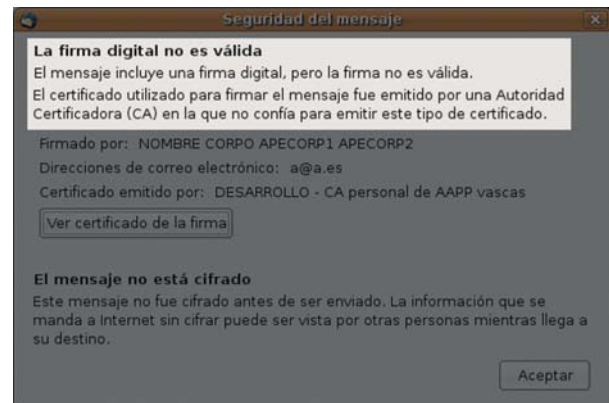
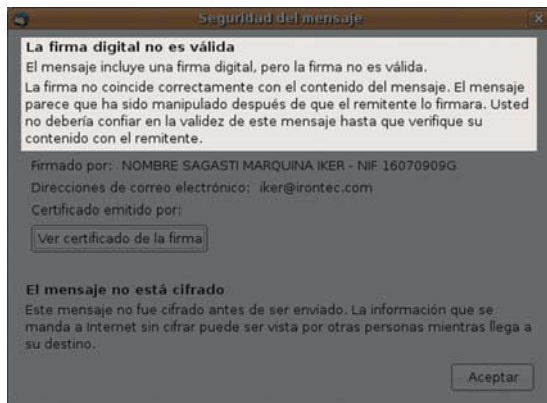




Sinadura baliozkoa den egiaztatu ahal izateko, **ezinbestekoa da ziurtapen-autoritateen eta mendekoen erroko ziurtagiriak inportatuta izatea.**



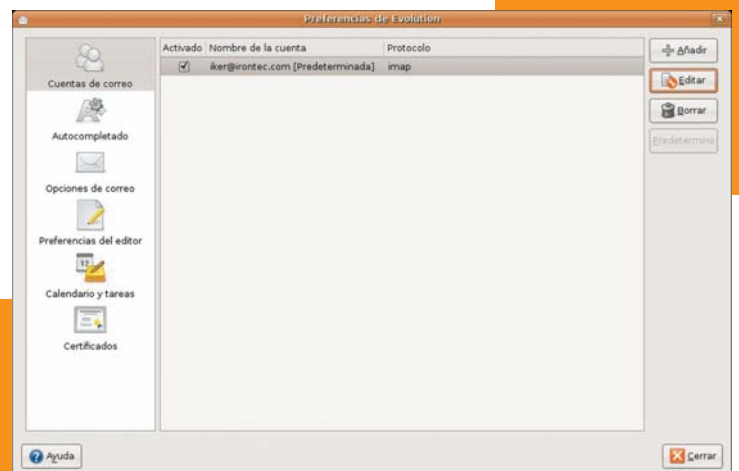
Baliozkoa ez bada, hori ohartaraziko digu. Posta-mezua aldatu delako nahiz ziurtapen-autoritateen eta horien mendekoen erroko ziurtagiriak inportatu ez ditugulako.



6.2.2. Evolution

Posta-kontua ziurtagiriarekin konfiguratzeara

Editatu menuko lehentasunen atalean, **Posta-kontuak** aukeran egingo dugu klik. Konfiguratu nahi dugun kontua hautatuko dugu eta berriz ere **Editatu** botoian egingo dugu klik.



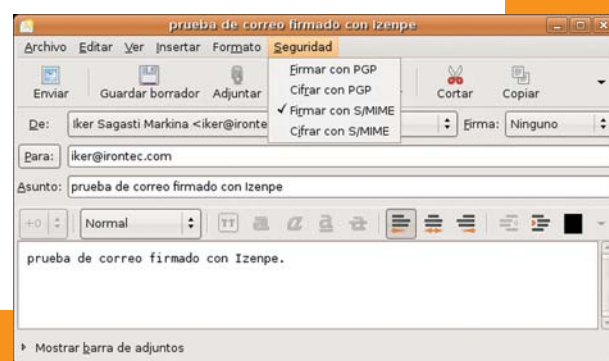


Segurtasuna atalean sartu eta posta-mezuak sinatzeko erabili nahi dugun ziurtagiria hautatuko dugu **Hautatu** botoian klik eginez, **MIME Segurua** atalean.



Digitalki sinatutako posta-mezua bidaltzea

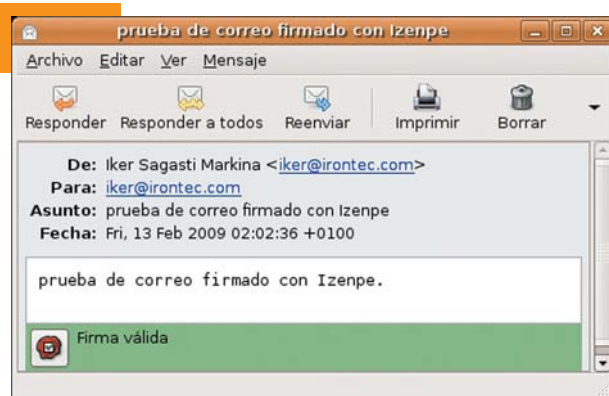
Digitalki sinatutako posta-mezua bidaltzeko, ezinbestekoa da hori adieraztea. Itendako posta-mezu guztiak digitalki sinatzeko aukera ez badugu adierazita, hori eskuz egin ahal izango dugu, menu honi jarraiki: **Segurtasuna** → **Digitalki sinatzea S/MIME** erkin.



Postaren sinadura digitala egiaztatzea

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

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



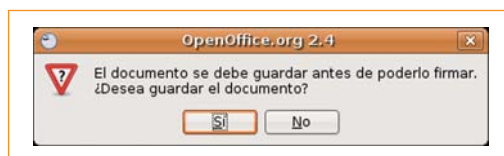
6.3. Dokumentu ofimatikoak sinatzea

6.3.1. OpenOffice.org

Ziurtagirien kokalekua dagokion atalean azaldutakoari jarraiki konfiguratu ostean, dokumentu ofimatiko bat sinatzeko prozesua egingo dugu.

OpenOffice.org suiteak honako dokumentu-motak sinatzeko aukera ematen du:

- Testu-dokumentuak (OOWriter)
- Kalkulu-orriak (OOCalc)
- Aurkezpenak (OOImpress)
- Marrazkiak (OODraw)

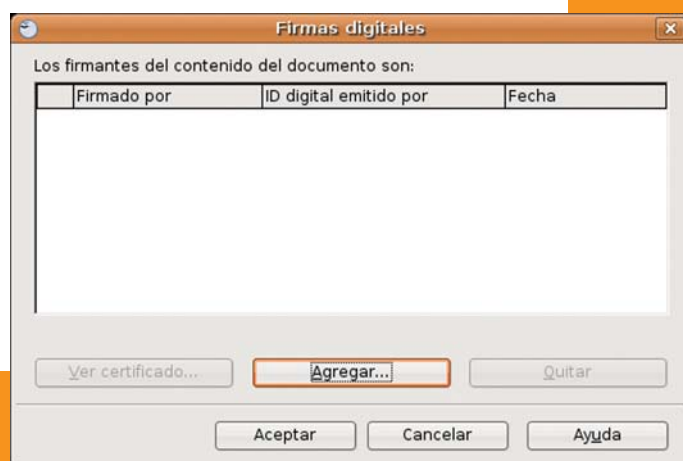


Dokumentua sinatzeari ekiteko, **Sinadura digitalak** aukera hautatuko dugu **Fitxategia** menuan.

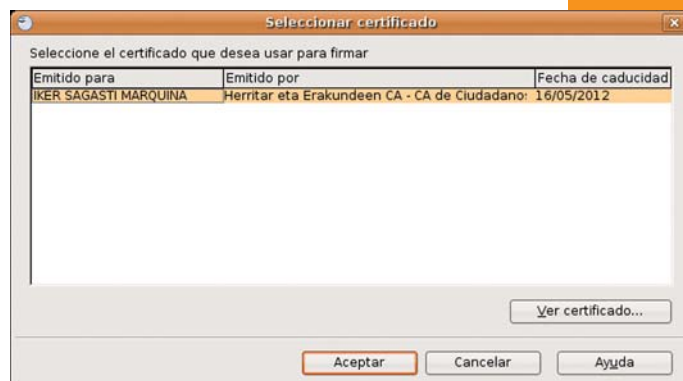


Dagoeneko gordeta dagoen dokumentua da sinatuko dena, alegia, aldatuko ez dena. Dokumentua sinatzen den unean dokumentua aldatuz gero, sinadura galdu egingo da, eta berriz sinatu beharko da.

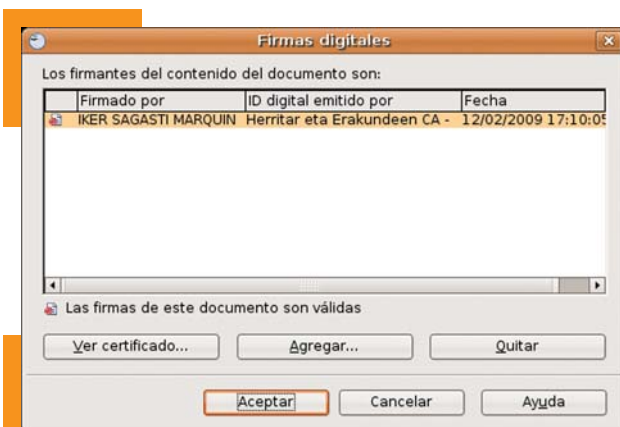
Gorde ostean, OpenOffice.org suitearen sinadura digitalen kudeatzailea erakutsiko digu.



Klik egingo dugu **Gehitu** aukeran, eta konfiguratuta ditugun ziurtagiriak erakutsiko dizkigu erreferentziako ziurtagirien datu-basetik (Firefox).



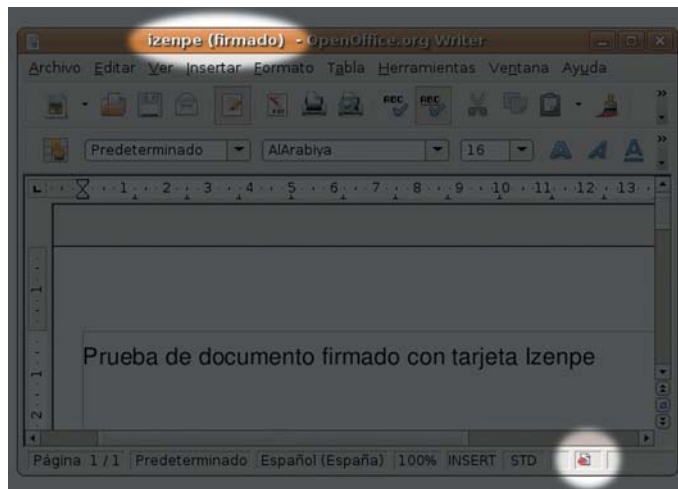
Hori eginez irekitako leihoan konfiguratutako ziurtagiri guztiak agertuko zaizkigu. Dagokion ziurtagiria hautatuko dugu eta **Ados** sakatuko.





Dokumentuen sinadurak baliozkoak izan daitezen, ezinbestekoa da dagozkien erroko ziurtapen-autoritateen eta mendekoen ziurtagiriak inportatuta izatea. Berriz ere **Ados** sakatuko dugu eta dokumentua sinatuta izango dugu. .

Agirian sinadura bat edo gehiago daudela adierazten diguten bi elementu bereiz ditzakegu:



7. Beste aplikazio osagarri batzuk

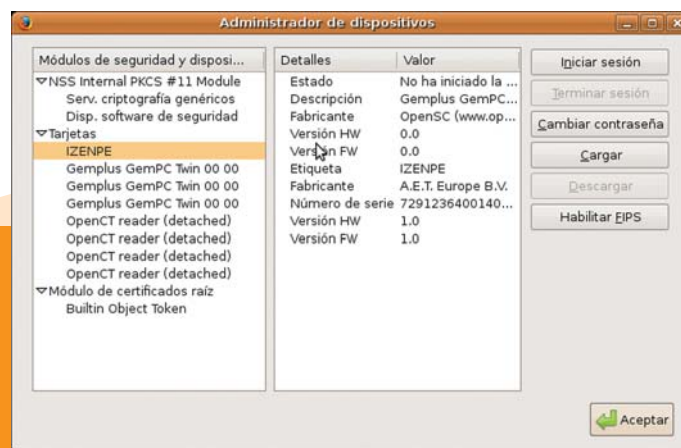
7.1. PINa aldatzea

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

Editatu menuaren lehentasunen artean, egin klik **Aurreratu**a aukeraren gainean, eta ondoren **Zifratua** 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. A través de la línea de comandos

Komando-lerroaren terminal bat irekiko dugu eta superrerrabiltzaile moduan ondorengo komandoak egikarituko ditugu:

```
# apt-get install opensc  
# 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 lizenperen txartelek GNU/Linux plataformetarako.

8. Kredituak

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.

