

//Instalaziorako eskuliburua
Izenpe ziurtagiri digitala//

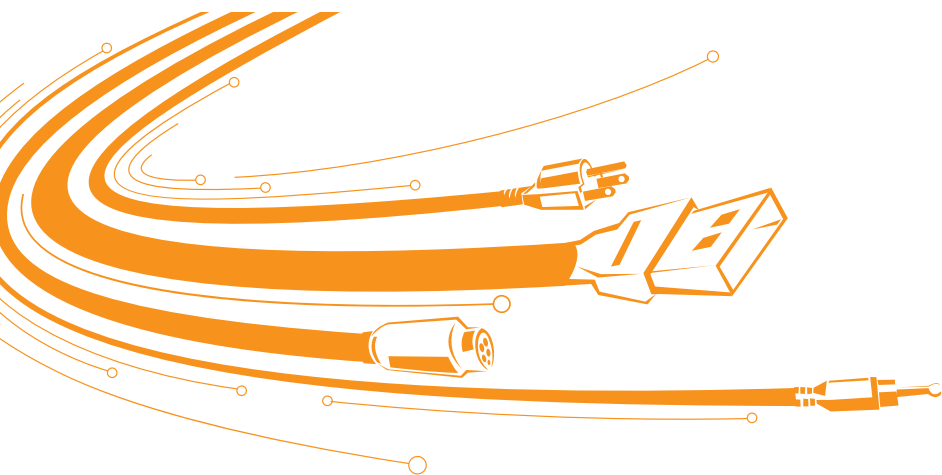


GNU/Linux
OpenSUSE 11

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.

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



4.2.2. Evolution.....	9
● 5. Ziurtapen-autoritateen ziurtagiriak aplikazioetan instalatzea	11
5.1. Erroko ziurtagiriak eta mendekoak	11
5.1.1. Firefox.....	11
5.1.2. Thunderbird.....	12
5.1.3. Evolution.....	12
5.1.4. OpenOffice.org.....	14
● 6. Aplikazioen erabileren adibidea	14
6.1. Webguneetan identifikatzea	14
6.1.1. Firefox.....	14
6.2. Digitalki sinatutako posta-mezuak bidaltzea	15
6.2.1. Thunderbird.....	15
Posta-kontua ziurtagiriarekin konfiguratzea	15
Digitalki sinatutako posta-mezua bidaltzea	15
Postaren sinadura digitala egiaztatzea	15
6.2.2. Evolution.....	16
Posta-kontua ziurtagiriarekin konfiguratzea	16
Digitalki sinatutako posta-mezua bidaltzea	17
Postaren sinadura digitala egiaztatzea	17
6.2.3. Dokumentu ofimatikoak sinatzea	17
OpenOffice.org.....	17
● 7. Beste aplikazio osagarri batzuk	18
7.1. PINa aldatzea	18
7.1.1. Modu grafikoan, Firefox bidez	19
7.1.2. Komando-lerroaren bidez	19
7.2. PINa desblokeatzea	19
● 8. Agiri honi buruz	19

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 openSUSE 11 banaketan 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 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 SUSE gisako banaketa guztietarako instalaziorako eskuliburua izatea du xede, hain zuzen ere, .rpm paketeak eta paketeak kudeatzeko zypper tresna dituztenetarako.

Agirian jaso dugun prozesua berariaz dagokio openSUSE 11ri, baina gainerako antzeko banaketak (hala nola, SUSE Linux Enterprise, Novell Linux Desktop, Linkat) 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 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 ziurtagiriarekin konfiguratzeko prozesua dokumentatzen saiatu gara.

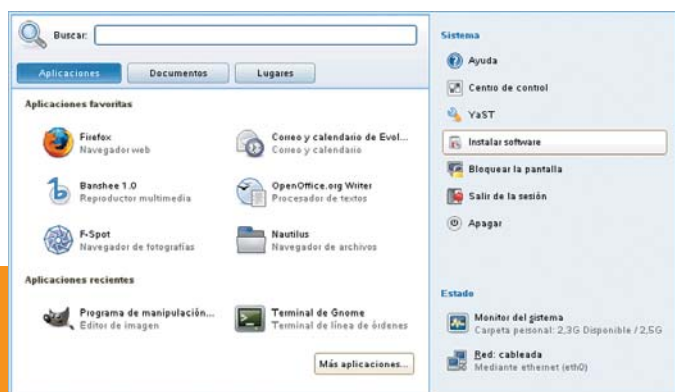
Honakoak dira agiri honetan azalduko ditugun aplikazioak:

- 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 YaST 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 Internetarako sarbidea izatea.

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.

openSUSE 11k oinarrizko konfigurazioan dakar opensc liburutegia.

3. Irakurgailuak konfiguratzeko

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.

PC/SC multzoa openSUSE 11 sistemaren oinarrizko instalazioan dago barne hartuta, nahiz eta ez den automatikoki abiatzen sistema abiatzeko prozesuan. Honakoa da abiatze automatizatua konfiguratzeko prozesua:

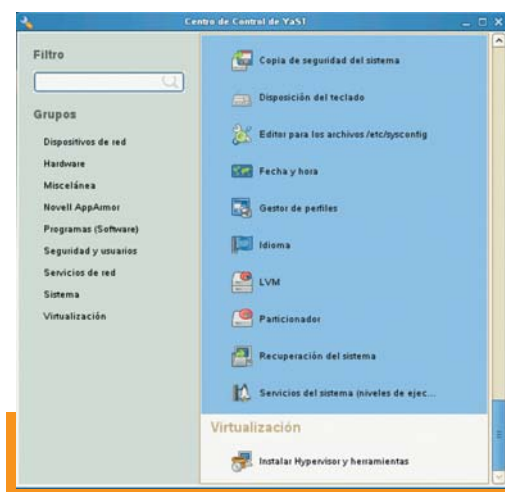
3.1.1. Ingurune grafikoaren bidezko konfigurazioa

Zerbitzuak kudeatzeko YaST tresnaren bidez ekingo diogu konfigurazioari.



Sistema multzoaren gainean egingo dugu klik eta **Sistemaren zerbitzuak** (egikaritze-mailak) hautatuko dugu, zerbitzuen kudeaketara sartzeko. Zerbitzuen zerrenda luzean egingo dugu aurrera pcsd aurkitu arte, eta **Aktibatu** aukeran egingo dugu klik (ohar ez dagoela aktibatuta adierazten duela zutabea).

Azkenik **Amaitu** sakatuko dugu eta egindako aldaketak gordeko ditugu.



3.1.2. Komando-lerroaren bidezko konfigurazioa

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

```
# chkconfig pcsd on
```

Komando horrekin abiatzen den bakoitzean pcsd zerbitzua abiatzeko konfiguratu dugu sistema.

Uneko saioan abiarazi nahi izanez gero (sistema berrabiarazi gabe):

```
# service pcsd start
```

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

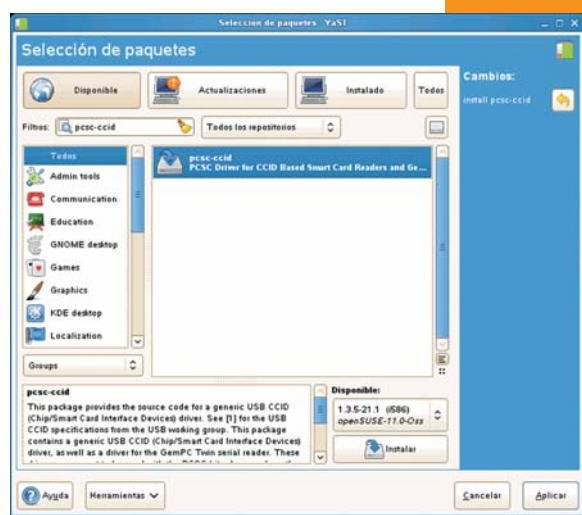
ccid liburutegia, CCID protokoloa (Chip Card Interface Device) ezartzen duena, merkatuko USB irakurgailu gehienen euskarri izaten saiatzen da.

3.2.1. Ingurune grafikoaren bidezko instalazioa

Paketeak kudeatzeko YaST tresnaren bidez ekingo diogu beharrezko liburutegien instalazioari.

Instalatu nahi dugun liburutegia adieraziko dugu, pcsc-ccid, hautatu, eta **Instalatu** aukeraren gainean egingo dugu klik.

Hautatu ondoren instalatu egingo dugu **Aplikatu** botoiaren gainean klik eginez.



3.2.2. Komando-lerroaren bidezko instalazioa

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

```
# zypper install pcsc-ccid
```

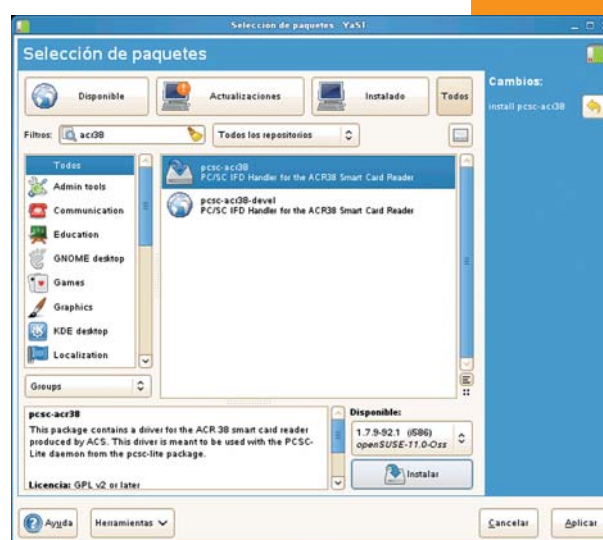
3.3. BIT4ID ACR38 irakurgailua

3.3.1. Ingurune grafikoaren bidezko instalazioa

Paketeak kudeatzeko YaST tresnaren bidez ekingo diogu instalazioari.

Instalatu nahi dugun liburutegia adieraziko dugu, pcsc-acr38, hautatu, eta **Instalatu** aukeraren gainean egingo dugu klik.

Hautatu ondoren instalatu egingo dugu **Aplikatu** botoiaren gainean klik eginez.



3.3.2. Komando-lerroaren bidezko instalazioa

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

```
# zypper install pcsc-acr38
```

4. Aplikazioak konfiguratzeara

Zoritxarrez, GNU/Linux sistema eragileak ez du ezarrita, sistema eragilearen mailan, ziurtagiri digitalak kudeatzeko arkitektura zentralizatua. Gaur egun Mozilla suitearena da ezarketarik aurreratuenak, 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 moduluak instalatzea

Editatu menuko lehentasunen artean, egin klik **Aurreratua** 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 kudeatzeko ahalbidetzen duen tresna da. Lehenetsitako konfigurazioan 2 segurtasun-modulu izaten ditu, bata, aurrez instalatuta dauden lehenetsitako erroko ziurtagiriak kudeatzeko eta bestea, beharrezko liburutegiekin batera erantsen ditugun eta kanpokoak ez diren gainerako ziurtagiri guztietarako.

Behar dugun segurtasun-moduluaren erantsateko, klik egingo dugu **Kargatu** botoiaren gainean.

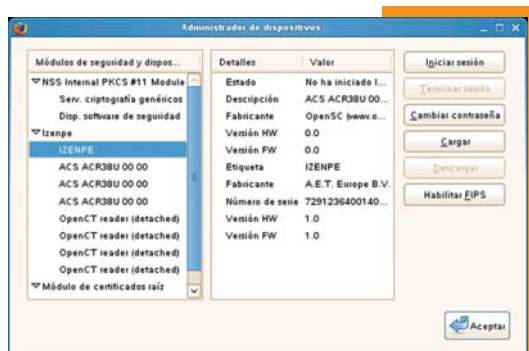


Lehi bat irekiko zaigu eta horrek emango digu aukera PKCS#11 modulu berria definitzeko. Kasu honetan integratzioko PKCS#11 modulu bat definitzea interesatzen zaigu, **opensc** liburutegiekin. Horretarako, honakoak definitu behar dira:

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



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



4.1.2. Opera

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

4.2. Posta-bezeroak

Sinatutako posta-mezuak bidali ahal izateko, ezinbestekoa da gakoaren erabilera hedatua izatea atributu gisa ziurtagiriak, zehatza esateko, posta elektronikoko babes (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

Ziurtagiriak behar bezala kargatu direla egiaztatzeko bide haxe 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 bagenitu, zerbait aldatzen dugun bakoitzean berriz ere kopiatu egin beharko genuke).

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

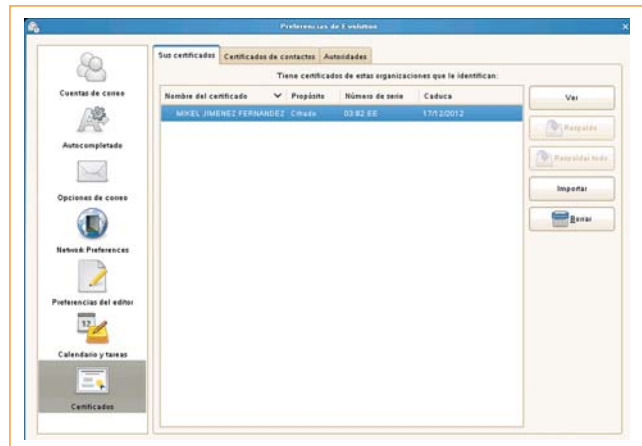
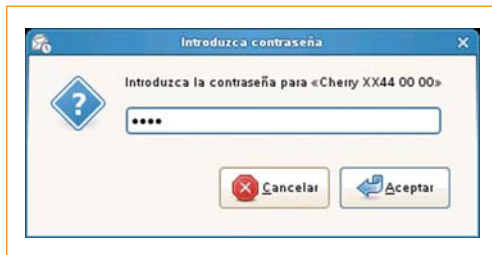
```
$ ln -sf $HOME/.mozilla/firefox/*.default/cert8.db $HOME/.evolution/cert8.db
$ ln -sf $HOME/.mozilla/firefox/*.default/key3.db $HOME/.evolution/key3.db
$ ln -sf $HOME/.mozilla/firefox/*.default/secmod.db $HOME/.evolution/secmod.db
```

Posta-kontua ziurtagiriarekin konfiguratzea

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

Egiaztatzea

Ziurtagiriak behar bezala kargatu direla egiaztatzeko **Editatu** → **Lehentasunak** aukeratu dugu, eta jarraian txartelaren sarbideko PINa eskatu dugu.



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 ingurune 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 egikaritu 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

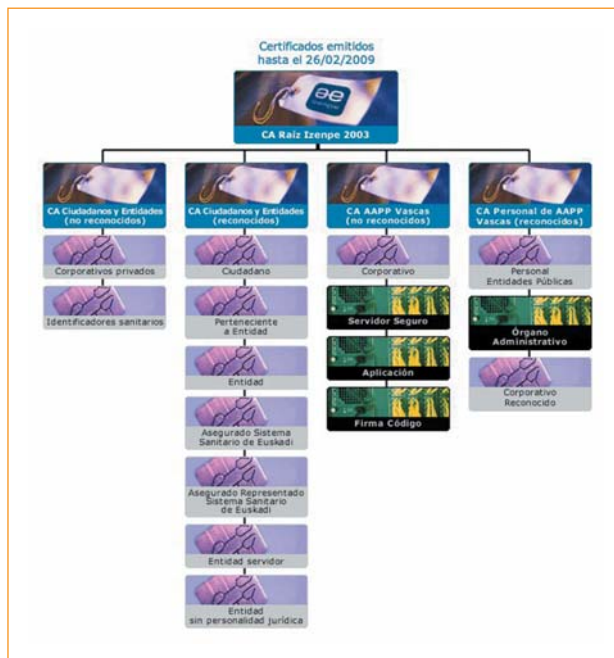
5.1. Erroko ziurtagiriak eta mendekoak

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 lehenetsuen 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 aukeratzeko ditugu.



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

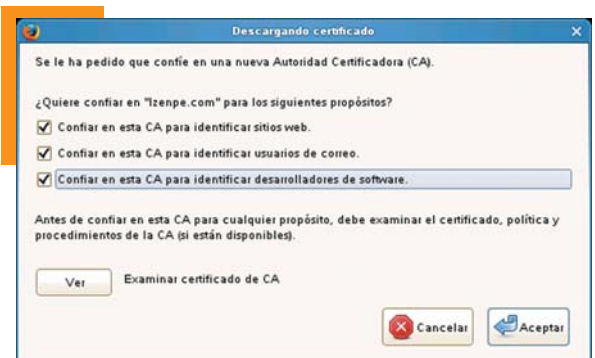
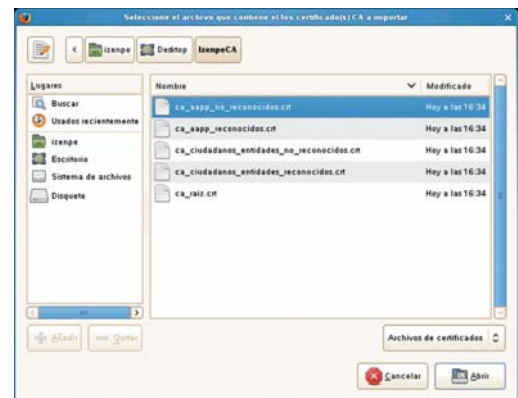
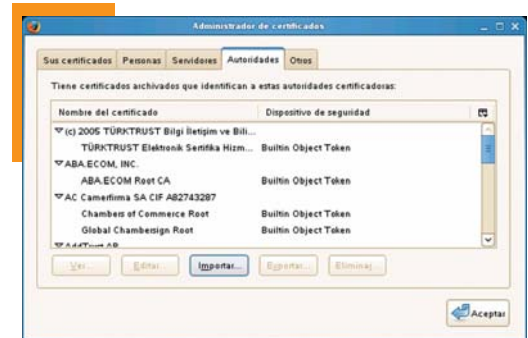
5.1.2. Thunderbird

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 nabigatzailearen antzekoa da. Beraz, ikus Firefox nabigatzailearen konfigurazioa dagokion atalean.

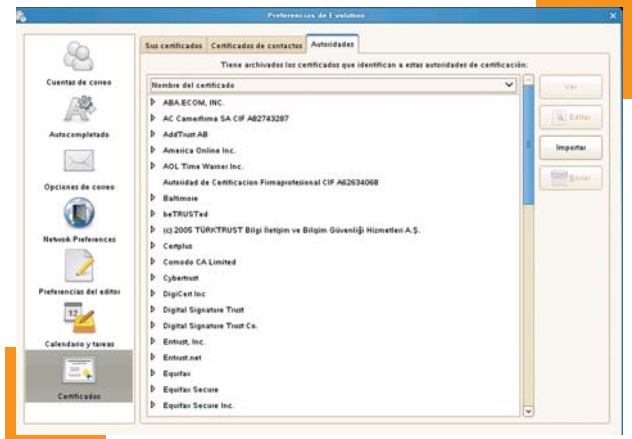
5.1.3. Evolution

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.

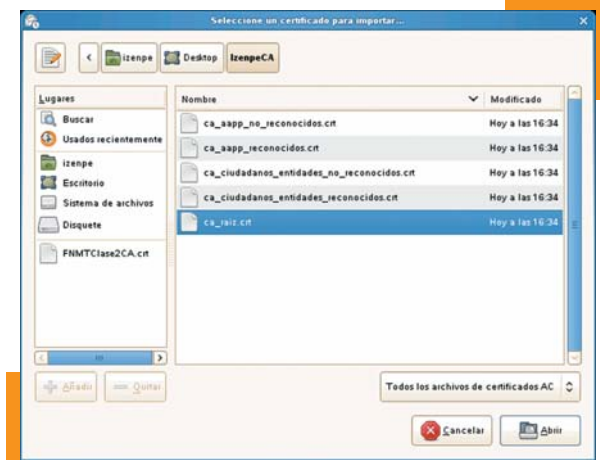




Egin klik **Ziurtagiriak** aukeraren gainean, editatu menuko lehentasunen artean, eta ondoren **Autoritateak** fitxaren gainean. Berriz ere klik egingo dugu **Inportatu** botoiaren gainean.



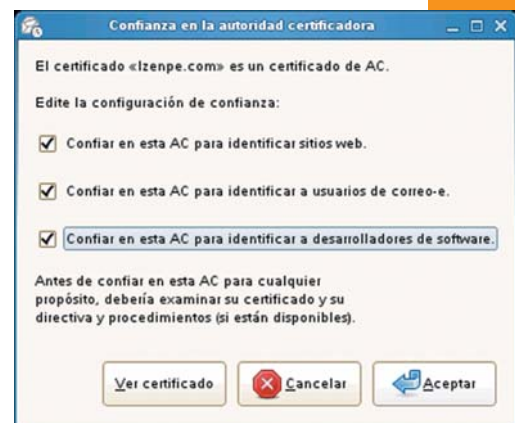
Izenperen erroko ziurtapen-autoritateen eta mendekoen ziurtagiri guztiak inportatuko ditugu, banan-banan, **Inportatu** botoian klik eginez.



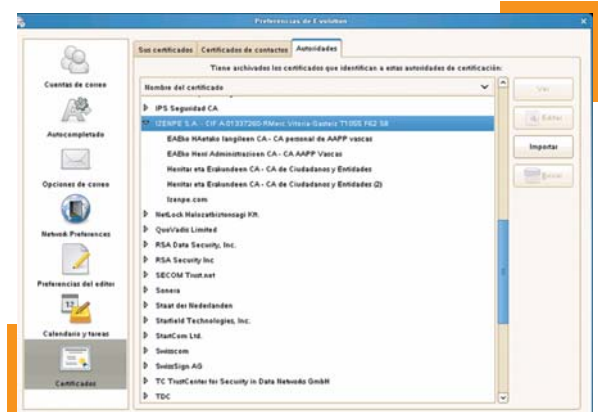
Erroko ziurtagiriak inportatzeko garaian, ziurtagirian jarriko dugun konfiantzari buruz galdetuko digu nabigatzaileak. 3 konfiantza-kategoria daude:

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

3 kategoriak aukeratzeko 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 ziurtagirien kudeatzailerik, eta beraz, Firefox edo Thunderbird-en dauden ziurtagiriak erabiltzen ditu. Autoritateen erroko ziurtagiriak aplikazio horien bidez inportatzen ditu.

6. Aplikazioen erabileren adibidea

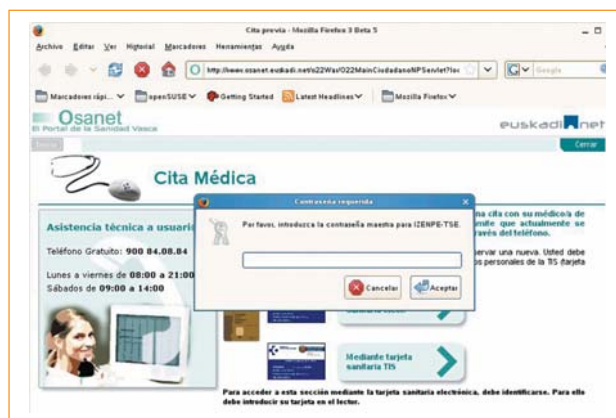
6.1. Webguneetan identifikatzea

6.1.1. Firefox

Ziurtagirien kokalekua dagokion atalean azaldutakoari jarraiki konfiguratu ostean, kautotzeko prozesu bat egingo dugu webgune batean, hain zuzen ere, Izenpek 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 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 genituzkeen 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 lizenperen ziurtagiritako batzuek bakarrik dute erabilera hedatu hori.

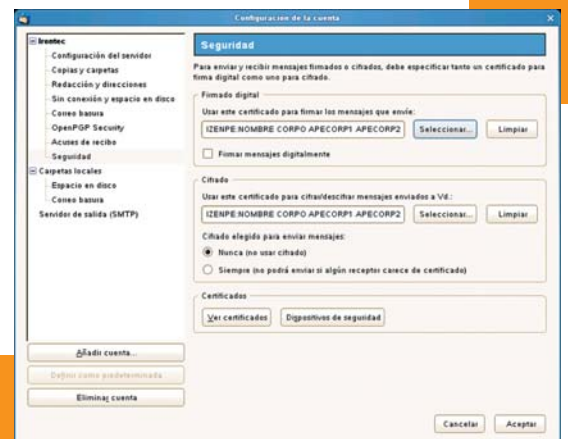
Baliozko ziurtagiria dugunean, beharrezkoa izango da posta-kontua dena delako ziurtagiri horri lotzea. Posta-kontu hori ziurtagirian barne hartutako bera izan daiteke.

Ikus dezagun zeregin hori nola egiten den posta-bezero desberdinetan

6.2.1. Thunderbird

Posta-kontua ziurtagiriarekin konfiguratzeko

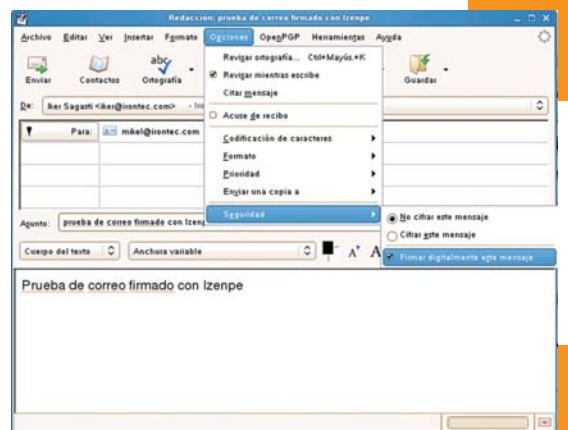
Editatu menuko **Kontuen konfigurazioa** atalean, egin klik **Segurtasuna** atalean, dagokion kontuan. Ondoren hautatu ziurtagiria.



Digitalki sinatutako posta-mezua bidaltzea

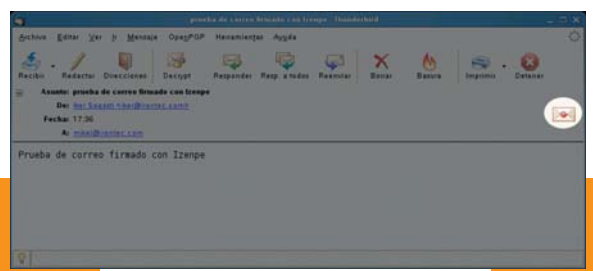
Digitalki sinatutako posta-mezua bidaltzeko, ezinbestekoa da hori adieraztea. Irteerako posta-mezu guztiak digitalki sinatzeko aukera ez badugu adierazita, hori eskuz egin ahal izango dugu, menu honi jarraiki: **Aukerak** → **Segurtasuna** → **Digitalki** sinatzea mezu hau.

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



Postaren sinadura digitala egiaztatzea

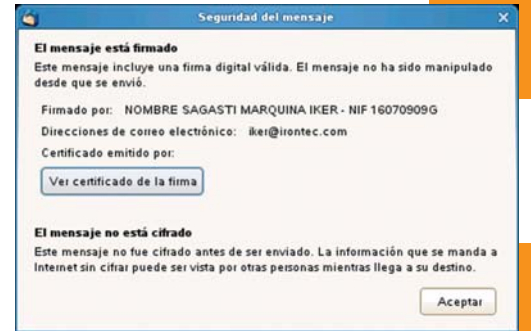
Thunderbird-ek posta-mezua digitalki sinatuta dagoela adierazten digun ikono bat erakusten digu.





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

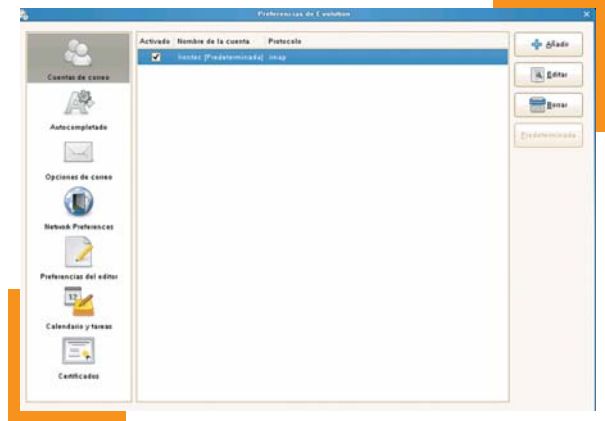
Baliozkoa ez bada, hori ohartaraziko digu. Posta-mezua aldatu delako nahiz ziurtapen-autoritateen eta horien mendekoen erroko ziurtagiriak inportatu ez ditugulako.



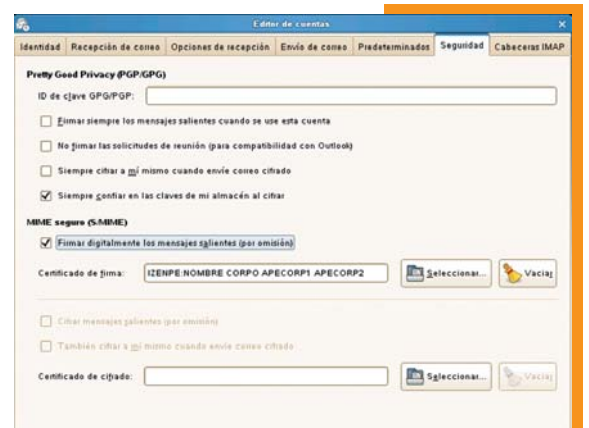
6.2.2. Evolution

Posta-kontua ziurtagiriarekin konfiguratzea

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



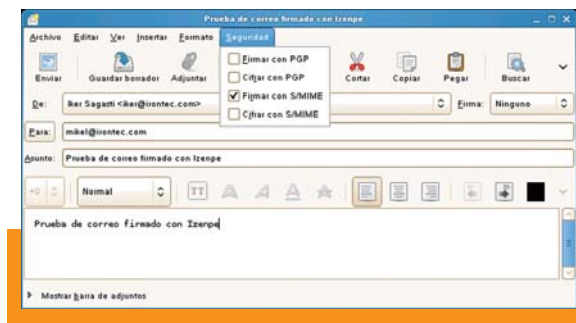
Segurtasuna atalean sartu eta posta-mezuak sinatzeko erabili nahi dugun ziurtagiria hautatuko dugu **Hautatu** botoian klik eginez, **MIME Segurua** atalean.





Digitalki sinatutako posta-mezua bidaltzea

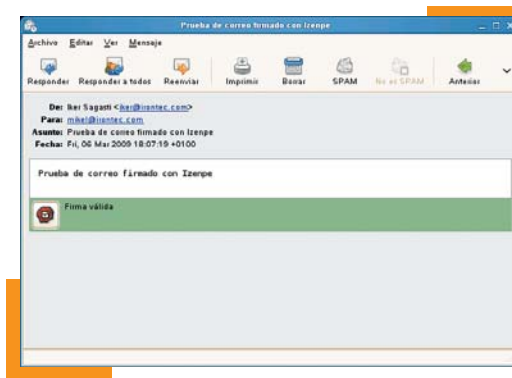
Digitalki sinatutako posta-mezua bidaltzeko, ezinbestekoa da hori adieraztea. Irteerako posta-mezu guztiak digitalki sinatzeko aukera ez badugu adierazita, hori eskuz egin ahal izango dugu, menu honi jarraiki: **Segurtasuna** → **Digitalki** sinatzea S/MIMEekin.



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 ziurtagapen-autoritateen eta mendeakoen erroko ziurtagiriak inportatuta izatea.**



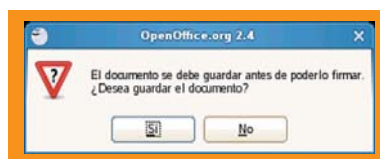
6.3. Dokumentu ofimatikoak sinatzea

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)

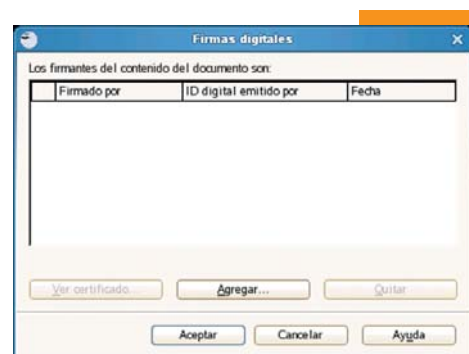


Dokumentua sinatzeari ekiteko, **Sinadura digitalak** aukera hautatuko dugu **Fitxategia** menuan.



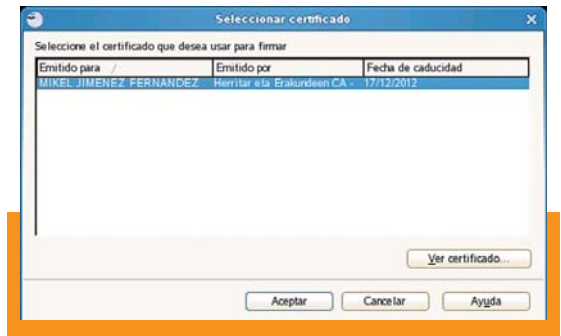
Dagoeneko gordeta dagoen dokumentua da sinatuko dena, alegia, aldatuko ez dena. Dokumentua sinatzen den unean dokumentua aldatuz gero, sinadura galdu egingo da, eta berriz sinatu beharko da.

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).

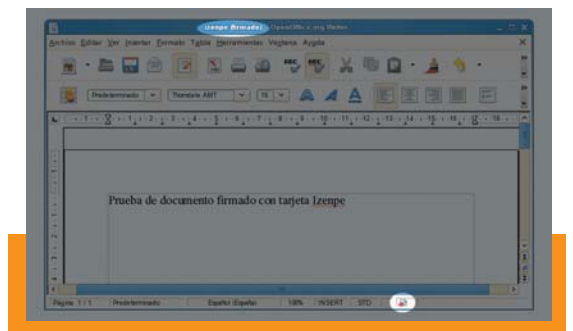


Hori eginez irekitako leihoan konfiguratutako ziurtagiri guztiak agertuko zaizkigu. Dagokion ziurtagiria hautatuko dugu eta **Ados** sakatuko.

Dokumentuen sinadurak baliozkoak izan daitezen, ezinbestekoa da dagozkien erroko ziurtagirien 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.

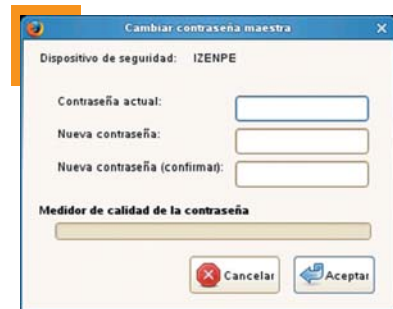
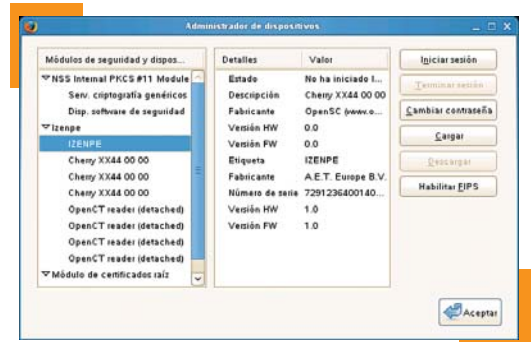
Izenperen txarteletan 4 eta 8 karaktere alfanumeriko artean erabil daitezke PINa definitzeko (a-z, A-Z, 0-9).

7.1.1. Modu grafikoan, Firefox bidez

Editatu menuaren lehentasunen artean, egin klik **Aurreratu**a aukeraren gainean, eta ondoren **Zifratu**a 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

Komando-lerroaren terminal bat irekiko dugu eta superrerabiltzaile moduan ondorengo komandoak egikaritzeko ditugu:

```
# 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 GNU/Linux plataformetarako.

8. 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.

