Izenpe Kita

Linuxerako instalazioa eta erabiltzailearen eskuliburua

IZENPE
Beato Tomás de Zumarraga 71 - 1ª Planta
01008 Vitoria - Gasteiz
Tel.: 945 067 723
www.izenpe.com

Aurkibidea

Sarrera

Eskuliburu hau gida baliagarria izango da Izenpe Kitaren instalazio-prozesua arrakastaz gauzatzeko garaian –IZENPEren txartel kriptografikoak (eta USB cryptoKEY tokenak ekartzen dituenak ere) erabiltzeko kita da–, baita kudeaketa-aplikazioan sartzeko eta erabiltzeko prozedura arrakastaz gauzatzeko garaian ere. Izenpe Kitak osagai hauek ditu:

- **Izenpe Middleware:** sistema eragilearen edozein aplikaziori adierazitako txartel kriptografikoekin lan egiteko aukera ematen dioten liburutegiak
- **Izenpe PIN Manager:** txartela kudeatzeko aplikazioa, hainbat eragiketa egiteko aukera ematen duena: PINa edo PUKa aldatzea, PINa desblokeatzea, txartelari buruzko informazioa lortzea…
- **Token cryptoKEY kontrolagailuak:** sistema eragileari USB cryptoKEY tokenarekin zuzen elkarreragiteko aukera ematen dioten liburutegiak **(txartela USB cryptoKEY token batean txertatuta datorrenean besterik ez)**

Eskuliburu honek modu errazean gidatuko zaitu Izenpe Kita instalatzeko eta erabiltzeko prozesuan.

Norentzat da agiri hau?

- IZENPEren txipdun txartela Linux inguruneetan erabili nahi duten ***azken erabiltzaileentzat.***

Hasi aurretik

Ziurtatu hauek dauzkazula:

- Txartel-irakurgailu estandarra, PC/SC bateragarria, behar bezala konektatua, instalatua eta konfiguratua. Jarraitu irakurgailuaren fabrikatzaileak emandako argibideei, behar bezala instalatuta dagoela eta ongi funtzionatzen duela egiaztatzeko **(token cryptoKEY bat baldin baduzu ez da beharrezkoa)**.
- Izenpe Kitaren azken bertsioa. IZENPEren webgunea bisitatzea gomendatzen dizugu, bertsio eguneratua daukazula egiaztatzeko.
- Instalazioa egin ahal izateko, ezinbestekoa da administratzailearen baimenak izatea. Baimenik ezean instalazioa ukatu egingo da.
- Daemon pcscd zuzen instalatuta eta exekuzioan, libccid eta libpcsclite1 liburutegiak barnean dituena, pcscd paketeaz gain.

Bit4id-en USB cryptoKEY token bat baldin baduzu, ez konektatu ordenagailuarekin instalazioa amaitu arte.

Instalatzea

Aplikazioa eskuragarri egongo da IZENPEren webgunearen bitartez, "Ziurtagiria kudeatzea" > 'Ziurtagiria abian jartzea' atalaren bitartez:

Deskarga ezazu Linux-i dagokion instalatzailea, eta deskonprima ezazu zure tresnerian.

CryptoKEY kontrolagailuen instalazioa

Sekzio hau token cryptoKEY bat duten erabiltzaileentzat besterik ez da. Hala ez bada, pasa zaitez zuzenean hurrengo atalera.

IZENPEren webgunetik deskarga dezakezun fitxategi konprimatuaren barruan cryptoKEY tokenaren driver-ak daude, .deb formatuan. Debian eta Ubuntu-rako autoinstalagarriak dira.

Nahikoa izango da klik bikoitza egitea dagokizun 32 bit-eko bertsioaren gainean (`libminilector38u-ccid-bit4id-i386.deb`) edo 64 bit-eko bertsioaren gainean (`libminilector38u-ccid-bit4id-amd64.deb`), betiere zure sistemaren arkitekturaren arabera, eta instalaziorako morroiari jarraitzea.

Une honetan, Bit4id-ren cryptoKEY tokena ordenagailuan libre duzun USB ataka batean konekta dezakezu. Linux-ek automatikoki ezagutuko du, eta ez du mezurik bistaratuko pantailan. Gailuaren LED berdea finko geratuko da, tokenaren eta ordenagailuaren arteko komunikazioa egokia dela eta denak zuzen funtzionatzen duela adieraziz.

Izenpe Middleware-ren eskuzko instalazioa

Prozedura horrek daemon `pcscd`-ren eta PC/SC txartel-irakurgailu bateragarri baten funtzionamendu zuzena eskatzen du.

Puntu honetan eskuz instalatzeko egin behar diren urratsak deskribatzen dira. Horretarako, liburutegiak behar diren direktorioetara kopiatzen dira. Honako fitxategi hauek osatzen dute Linux-erako Izenpe Middleware:

`libbit4ipki.so`

`libbit4ipki.so.conf`

`libbit4ipki.so.interop.plugin`

Hiru fitxategiak elkarrekin kopiatu behar dira beti liburutegien karpeta berean (karpeta bat edo beste izango da erabilitako bertsioaren arabera). Esate baterako:

`/usr/local/lib`

`/usr/lib`

Bi karpetak dituen Linux bertsioren bat duzu, berdin dio batean edo bestean kopiatzea fitxategiak.

Fitxategiak kopiatu ostean, beharrezkoa izan daiteke liburutegietako cache-a eguneratzea etorkizunean erroreak gerta daitezen. Komando hau exekutatuta eguneratuko da:

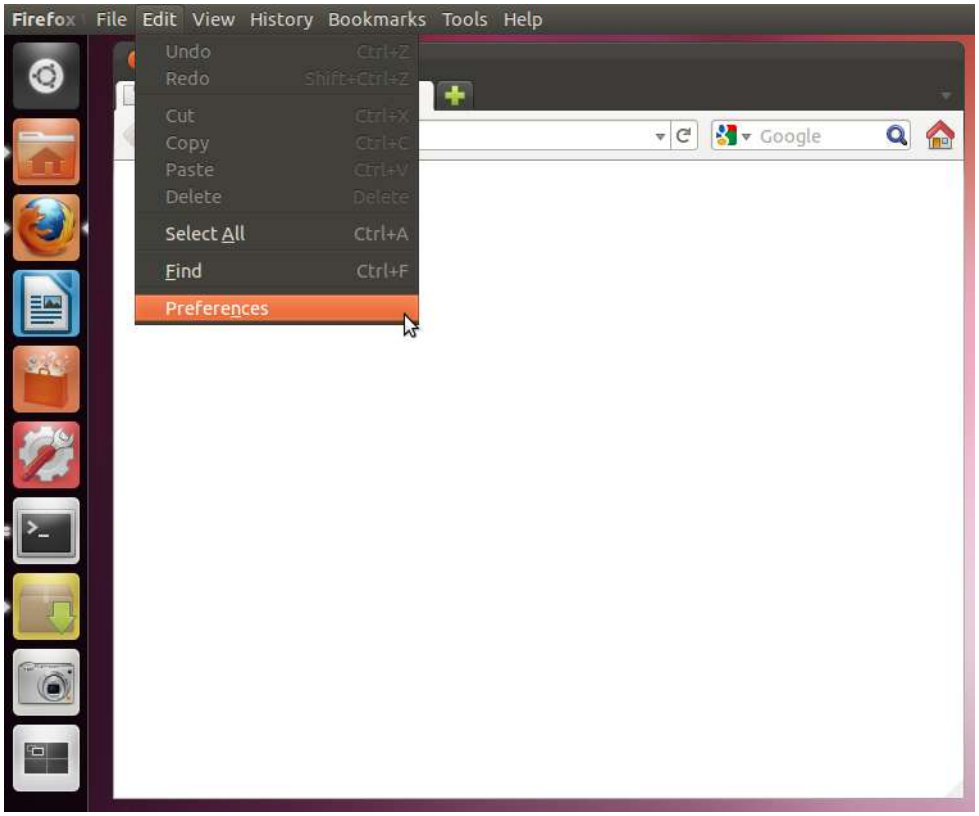
```
# ldconfig
```

Gerta daiteke `libbit4ipki.so` fitxategiaren goiburuari buruzko oharren bat agertzea, baina ez du esanahi arazoak sortu direla.

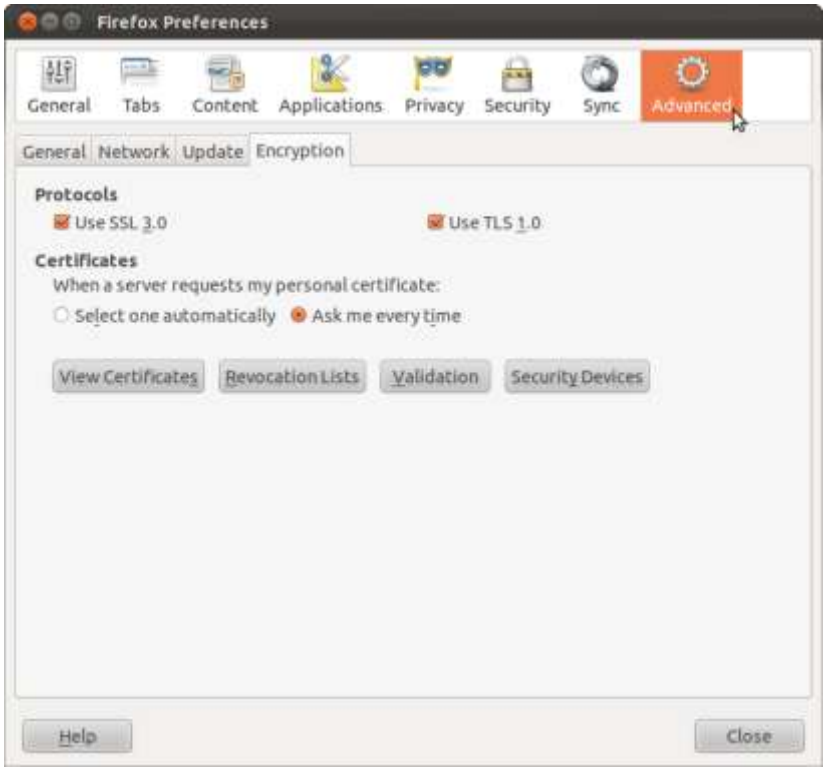
Konfigurazioa Firefox-en

Txartel adimenduna Mozilla Firefox nabigatzailean erabili ahal izateko, Izenpe Universalaren liburutegietarako euskarria eskuz gehitu behar da. Segurtasun-gailuak Firefox-en automatizatuta txertatzeko aukera desgaitu egin zen 3.5 bertsiotik aurrera, segurtasun-neurri gisa.

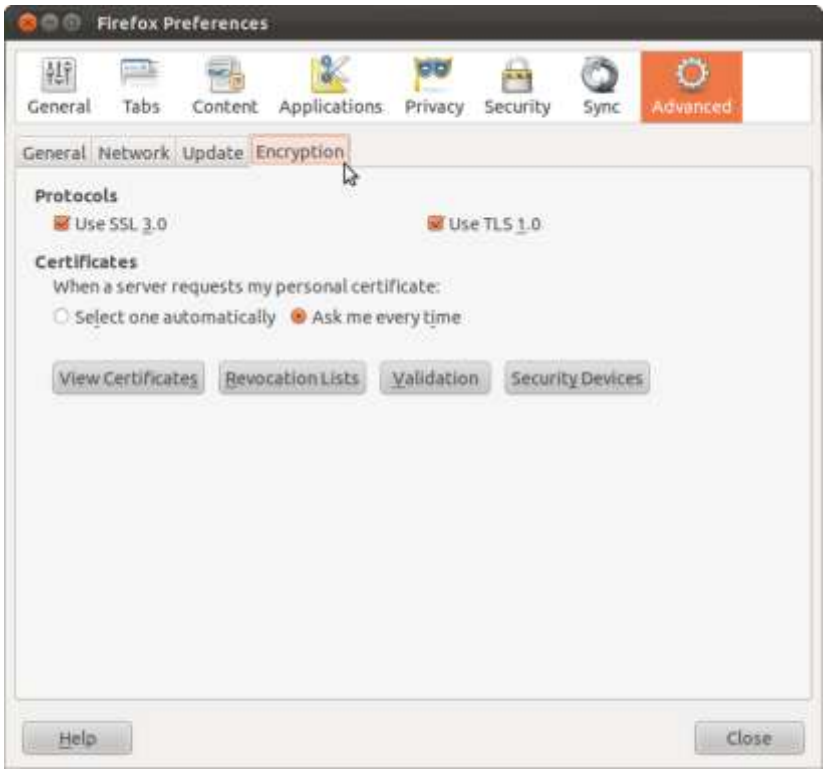
Mozilla Firefox zabaldu ostean, klik egin beharko da *Edizioa (Edit)* → *Lehentasunak (Preferences)* aukeren gainean



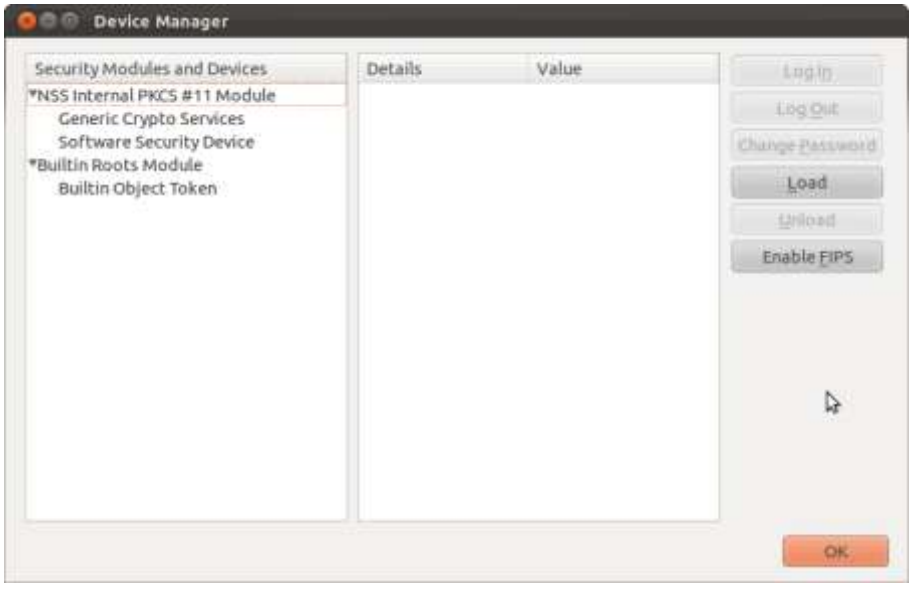
Ondoren, *Aurreratua (Advanced)* multzoa hautatu beharko da.



Ondoren Zifraketa (Encryption) hautatu beharko da, eta klik egin beharko da *Segurtasun-gailuak (Security Devices)* aukeran.



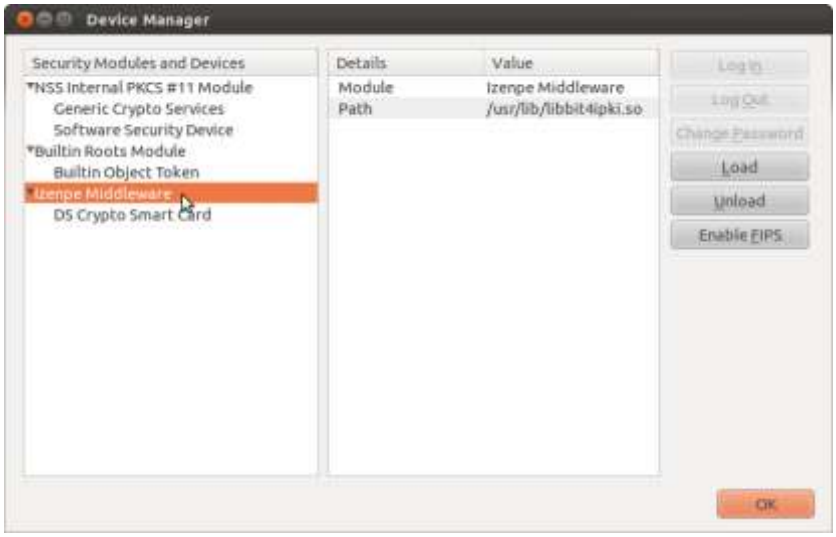
Segurtasun-gailuen administratzailearen pantailan *(Device Manager), Kargatu (Load)* botoian klik egin.



PKCS#11 gailua kargatzeko pantailan (Load PKCS#11) leihoan datu hauek sartu behar dira:

- Moduluaren izena *(Module Name)*: *Izenpe Middleware*
- Moduluaren fitxategia *(Module filename)*: `/usr/lib/libbit4ipki.so`

Ondoren, *Ados (OK)* botoian klik egin. Modulua behar bezala gehituko da eta Firefox-eko instalazioa amaituta izango da. Arazorik izanez gero, ziurta ezazu zure ordenagailuaren eta sistemaren arkitekturarako (32 edo 64 bit) liburutegi egokiak erabiltzen ari zarela.



Izenpe Kita erabiltzen hasi aurretik

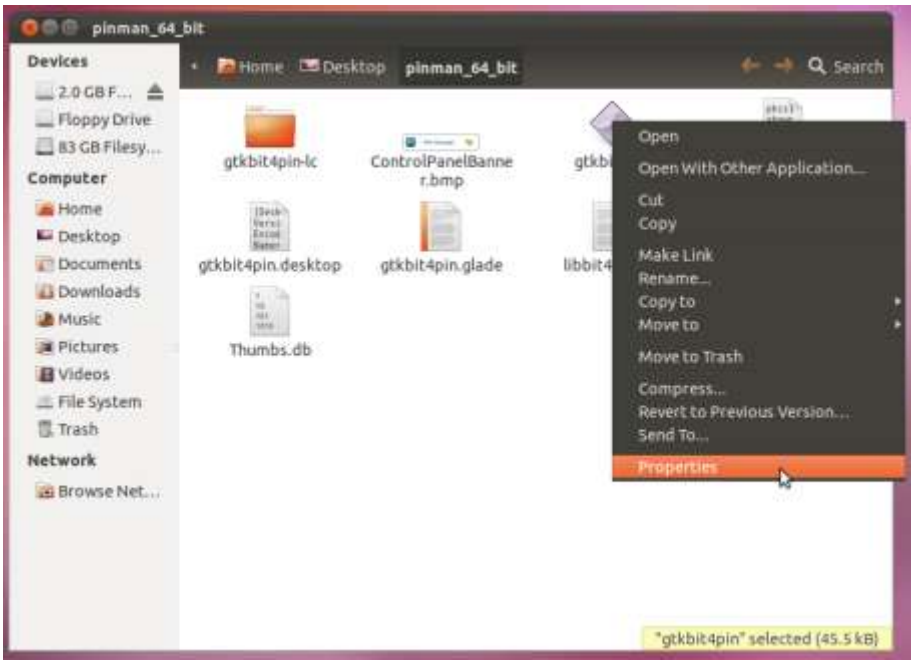
Sekzio hau token cryptoKEY bat duten erabiltzaileentzat besterik ez da. Hala ez bada, pasa zaitez zuzenean hurrengo atalera.

Ziurta ezazu zure CryptoKEY tokena konektatuta duzula ordenagailuan libre duzun USB ataka batean, eta tokenak txartel adimenduna (SIM tamainakoa) daukala barruan.

PIN Manager erabiltzea

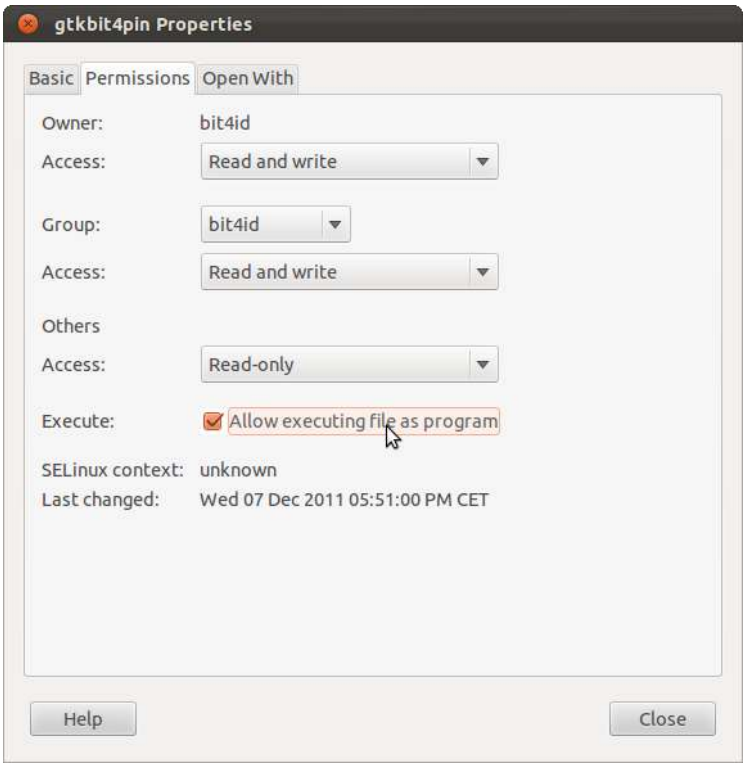
Izenpe PIN Manager aplikazioa ZIParen barruan duzu eskura, `pinman_32_bit` edo `pinman_64_bit` karpetan.

Segurtasun-arrazoiak tarteko, gerta daiteke zure sisteman bi fitxategi exekutatzeko baimena eman behar izatea: `gtkbit4pin` eta `gtkbit4pin.desktop`. Horien gainean eskuineko botoiarekin klik egin beharko da, eta ondoren *Propietateetara (Properties)* jo beharko da.

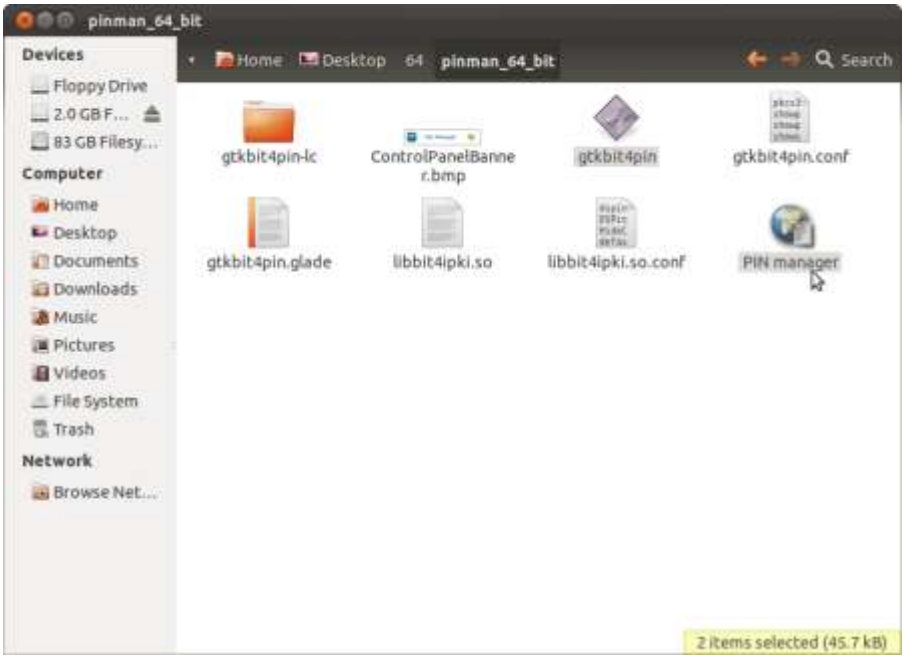


Gero, biak exekutatzeko baimena gaitu beharko da, eta, horretarako, sistema eragileari erabiliko ditugun programak direla adieraziko diogu.

Hurrengo pantaila-atzipenean adierazten den laukia markatu beharko da.



Izenpe `PIN Managerrera` sartu ahal izango da PIN manager gainean edo `gtkbit4pin` gainean klik bikoitza eginez.



Izenpe Kita erabiltzen hasi aurretik

Izenpe PIN Manager-ek txartel-irakurgailu estandarra eskatzen du, PC/SC bateragarria, hasi aurretik behar bezala konektatua, instalatua eta konfiguratua.

Jarraitu irakurgailuaren fabrikatzaileak emandako argibideei, behar bezala instalatuta dagoela eta ongi funtzionatzen duela egiaztatzeko.

CryptoKEY token bat baldin baduzu, ziurtatu ordenagailuan libre duzun USB ataka batean konektatuta daukazula eta tokenak txartel adimenduna (SIM tamainakoa) daukala barruan.

Funtzionaltasunak

Izenpe PIN Managerrek funtzionaltasun ugari ditu, pantaila nagusitik eskuragarri daudenak:

[1. irudia]

Funtzioen taula

Ondorengo taulan Izenpe PIN Managerren pantaila nagusian adierazitako funtzioak laburtzen dira.

Funtzioa	Deskribapena
Change PIN	Txartelaren PINa aldatzeko funtzioa (ikus 2. irudia)
Unblock PIN	Txartelaren PINa bere PUKaren bitartez desblokeatzeko funtzioa (ikus 3. irudia)
Change PUK	Txartelaren PUKa aldatzeko funtzioa (ikus 4. irudia)
Card informations	Txartelari buruzko informazioa (modeloa, serie-zenbakia, fabrikatzailearen identifikazioa eta etiketa) erakusten duen leihoa (ikus 5. irudia)

PINa aldatu

Txartelaren PIN zaharra eta PIN berria idatzi. PIN berriak 6 eta 8 digitu alfanumeriko artean izan behar du.

[2. irudia]

PINa desblokeatu

PINa desblokeatzeko txartelaren PUKa idatzi eta PIN berria idatzi. PIN berriak 6 eta 8 digitu alfanumeriko artean izan behar du.

[3. irudia]

PUKa aldatu

Txartelaren PUK zaharra eta PUK berria idatzi. PUK berriak 6 eta 8 digitu alfanumeriko artean izan behar du.

[4. irudia]

Txartelaren informazioa

Txartelaren informazio zehatza eskaintzen du: modeloa, serie-zenbakia, fabrikatzailea eta etiketa. Baliteke Erabiltzaileen Arreta Guneak informazio hori eskatzea erabiltzen ari zaren txartel-mota ezagutzeko.

[5. irudia]

Maiz egiten diren galderak

Zer gerta daiteke aplikazio guztiak instalatu ondoren nire cryptoKEY tokena konektatzen badut eta argi berdea pizten ez bada?

Konektatu irakurgailua beste ordenagailu baten USB ataka batean. Funtzionatzen ez badu, probatu beste ordenagailu batean. LED berdea inoiz pizten ez bada, kontsultatu IZENPErekin cryptoKEY tokena aldatzeko.

Nola egiazta dezaket nire cryptoKEY tokenak barruan SIM tamainako txartel adimenduna daramala?

Ireki USB konektorearen beste aldean dagoen mihia eta egiaztatu barruan SIM tamainako txartel adimenduna behar bezala txertatuta duela, beheko argazkiaren arabera.

Konbina ditzaket zenbakiak eta letrak txartelaren PIN zenbakirako?

Bai, ez dago arazorik, betiere PIN berriak 6 eta 8 digitu artean badu.

Zalantzaren bat badut eta nire PIN zenbakia zein den gogoratzen ez badut, zenbat aldiz idatz dezaket PINa? Noiz gera daiteke blokeatuta txartela?

PIN kodea hirutan baino gehiagotan gaizki idazten baduzu, blokeatu egingo da. Jarri harremanetan IZENPErekin desblokeatzeko.

Zenbat aldiz idatz dezaket PUKa PINa desblokeatzen ahalegintzeko? Zer gertatzen da txartela blokeatuta geratzen bada?

PUK kodea hirutan baino gehiagotan gaizki idazten baduzu, blokeatu egingo da. Segurtasunagatik, txartela erabat blokeatzen da. Jarri harremanetan IZENPErekin.

Glosarioa

Autoritate ziurtagiri-emailea: sinadura elektronikoan erabilitako ziurtagiri elektronikoak idatzi eta ezeztatzeaz arduratzen den konfiantzazko entitatea da. Autoritate ziurtagiri-emaileak, bere aldetik edo erregistro-autoritate batek esku hartuta, ziurtagiri baten eskatzailearen nortasuna egiaztatzen du ziurtagiria igorri aurretik; edo, ezeztatze-baldintzekin luzatutako ziurtagirien kasuan, nortasun hori egiaztatu ondoren ziurtagirien ezeztatzea ezabatzen du.

Ziurtagiri digitala iraungitzea: ziurtagiri digitalak ziurtagirian bertan adierazten den indarraldia du. Normalean 2 urtekoa da, legez 5 urte arteko indarraldia baimendu arren. Ziurtagiriak iraungi ondoren, ezin izango dira sinadura elektronikoa eskatzen duten Administrazioak eskainitako zerbitzuak erabili, eta orduz geroztik egingo den edozein sinadura elektronikok ez du baliorik izango.

Ziurtagiri digitala: autoritate ziurtagiri-emaileak egin eta sinatutako informatika-euskarrian egindako agiria, bere jabearen nortasuna bermatzen duena.

Ziurtagiri onartua: Ziurtapen Zerbitzuen Egile batek emandako ziurtagiria. Ziurtapen Zerbitzuen Egile horrek Legean ezarritako baldintzak beteko ditu, eskatzaileen identitateari eta inguruko bestelako gaiei dagokienez, baita ematen dituzten ziurtapen-zerbitzuen fidagarritasunari eta bermeei dagokienez ere. Guztia, Sinadura Elektronikoari buruzko abenduaren 19ko 59/2003 Legearen II. tituluko II. kapituluan xedatutakoarekin bat etorrita.

Sinadura elektronikoa: datuen multzoa, modu elektronikoan, beste datu elektronikoei erantsiak edo funtzionalki haiei lotuak, hura biltzen duen agiriaren egilea edo egileak identifikatzeko baliabide gisa erabilita. 3 motatako sinadura elektronikoak daude: sinadura elektroniko sinplea, aurreratua eta onartua.

Sinadura elektroniko sinplea: beste datu batzuei erantsitako datu multzoa, forma elektronikoa dutenak.

Sinadura elektroniko aurreratua: sinatzailea identifikatzen duen sinadura elektronikoa da, eta sinatutako datuen ostean egondako edozein aldaketa hauteman dezake. Sinadura sinatzailearekin eta adierazten dituen datuekin soil-soilik dago lotuta, eta sinatzaileak bakarrik kontrolatzen dituen bitartekoen bidez sortu da.

Sinadura elektroniko onartua: sinadura elektroniko onartua ziurtagiri onartu batean oinarritzen den eta sinadura sortzeko gailu seguru baten bidez sortu den sinadura elektroniko aurreratua da. Eskuz egindako sinadurak paperean idatzitako datuekin duen balio bera izango du sinadura elektroniko onartuak modu elektronikoan idatzitako datuekin.

Hash funtzioa: edozein tamainatako datu-multzo baten gainean egiten den eragiketa da. Horrenbestez, jatorrizkoaren tamaina edozein dela ere, lortutako emaitza neurri finkoko beste datu-multzo bat da. Hasierako datuei unibokoki lotuta egotearen propietatea du, hau da, hash funtzioa aplikatzean ezin dira emaitza bera sortuko duten bi mezu desberdin aurkitu.

Hash edo hatz-marka: mezu bati hash funtzioa aplikatu ostean lortzen den tamaina finkoko emaitza, hasierako datuetara modu unibokoan lotuta egoteko propietatea betetzen duena.

Integritatea: integritatea da aldatu ez duten dokumentu edo fitxategi batek duen ezaugarria. Gainera, jatorrizko dokumentuan inolako manipulaziorik egin ez dela egiaztatzeko aukera ematen du.

Ziurtagiriak ezeztatzeko zerrendak edo ezeztatutako ziurtagirien zerrendak: ezeztatutako edo etendako ziurtagiriak (iraungitakoak ez) bakarrik agertzen diren zerrenda.

Onarpenak: dokumentu bat elektronikoki sinatzen duen igorleak ezin izango du ukatu jatorrizko mezua igorri zuela. Izan ere, mezu hori igorleari egotz dakioke, berak bakarrik ezagutzen duen eta babestera behartuta dagoen gako pribatuaren bitartez. Ukorik ezak, gainera, transakzio batean nork hartu zuen parte egiaztatzeko aukera ematen du.

Ukorik eza edo ukaezintasuna kautotzearekin oso lotuta dagoen segurtasun-zerbitzua da, eta komunikazio batean aldeen parte-hartzea frogatzeko aukera ematen du. Kautotzearekiko funtsezko diferentzia da aurrenekoa komunikazioa finkatzen duten aldeen artean gertatzen dela eta uko ez egiteko zerbitzua, berriz, hirugarren baten aurrean gertatzen dela.

Ziurtapen Zerbitzuen Egilea edo ZZE: ziurtagiri elektronikoak jaulkitzen dituen edota sinadura elektronikoarekin lotutako bestelako zerbitzuak ematen dituen pertsona fisiko edo juridikoa da. Ikus autoritate ziurtagiri-emailea.

PIN: ziurtagirietan sartzea ahalbidetzen duten karaktereen sekuentzia. Identifikazio pertsonaleko zenbakia, zenbaitetan IPZ ere esaten zaiona.

PUK: PINa aldatzea edo desblokeatzea ahalbidetzen duten karaktereen sekuentzia. Desblokeatzeko gako pertsonala.

Berritzea: berritzea da beste ziurtagiri bat eskatzea indarrean dagoen baina iraungitzear dagoen ziurtagiri baten bitartez. Horrela, ziurtagiri bat iraungi aurretik hura berritzea eska daiteke eta, ondorioz, beste ziurtagiri baliagarria egin behar da.

Ezeztatzea: harpidedun batek eskatuta edo, gakoen segurtasunean zalantza badago, autoritate ziurtagiri-emailearen ekimenagatik ziurtagiri digital bat behin betiko ezeztatzea. Ezeztatzea atzera ezineko egoera da. Etete-egoera baten ondoren edo eskatzeko baimena duten pertsonek hala nahi dutelako, ziurtagiri bat ezeztatzeko eska daiteke. Era berean, etendako ziurtagiri baten kasuan, gehieneko etete-epea igaro bada, ziurtagiria gaitu ez badute, behin betiko ezeztatua egotera pasako da. Ziurtatze-entitateak ziurtagiri bat ezeztatu edo eteten duenean, Ziurtagiri Ezeztatuen Zerrendetan (ZEZ) adierazi beharko du gertakari hori ezagutarazteko. Zerrenda horiek publikoak dira eta beti eskuragarri egon behar dute.

Txartel adimenduna (SmartCard): neurri bateko logika programatua gauzatzea ahalbidetzen duen zirkuitu integratudun edozein txartel.