




Izenpe Kita


Mac OS X sistemarako instalazioa eta
erabiltzailearen eskuliburua



	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa

Aurkibidea

¡Error! Marcador no definido.Sarrera	3
Norentzat da agiri hau?	3
Hasi aurretik	3
Instalatzea.....	5
CryptoKEY kontrolagailuen instalazioa	5
Izenpe Middleware-ren instalazioa	9
Izenpe Middleware-ren eskuzko instalazioa	12
Arazo ezagunak	13
Konfigurazioa Firefox-en	13
Izenpe Kita erabiltzen hasi aurretik.....	15
PIN Manager erabiltzea.....	16
Funtzionaltasunak	16
Funtzioen taula	18
Maiz egiten diren galderak	20
Glosarioa	21

	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa

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 elkarrengaitzeko 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 Mac OS X inguruneetan erabili nahi duten *azken erabiltzaileentzat*.

Hasi aurretik


Ziurtatu hauek daukazula:

- 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.
- CryptoKEY token bat baldin baduzu, ziurtatu tokenaren kontrolatzaileen azken bertsioa daukazula. IZENPEren webgunea bisitatzea gomendatzen dizugu, bertsio eguneratua daukazula egiaztatzeko.

	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa

- Instalazioa egin ahal izateko, ezinbestekoa da administratzailearen baimenak izatea. Baimenik ezean instalazioa ukatu egingo da.

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

	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa

Instalatzea

Aplikazioa eskuragarri egongo da IZENPEren webgunearen bitartez, “Ziurtagiria kudeatzea” > ‘Ziurtagiria abian jartzea’ atalaren bitartez:




Deskargatu Mac OS X sistemari dagokion instalatzailea.

CryptoKEY kontrolagailuen instalazioa

Instalatzailea deskargatu ondoren, zip fitxategia deskonprimatu behar duzu eta irakurgailuaren driver-ak instalatzen hasi. Horretarako, egin klik bikoitza *bit4id-drivers.mpkg* fitxategiaren gainean (**criptoKEY token bat duzunean besterik ez da egin behar urrats hau**).

Instalatzailea abiaraziko da. Egin klik *Continuar* (jarraitu) botoian.

	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08 4.0.1.0 bertsioa
	Produktua: Izenpe Kita	



Hurrengo pausoan, instalazio-jarraibideak irakurri eta *Continuar* jarraitu botoian klik egin.



Ondoren, helburuko unitatea aukeratu. Oso garrantzitsua da instalazio estandarra disko nagusian egiten uztea.




Dokumentuaren izenburua:
Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua

2014/07/08

4.0.1.0 bertsioa

Produktua:
Izenpe Kita

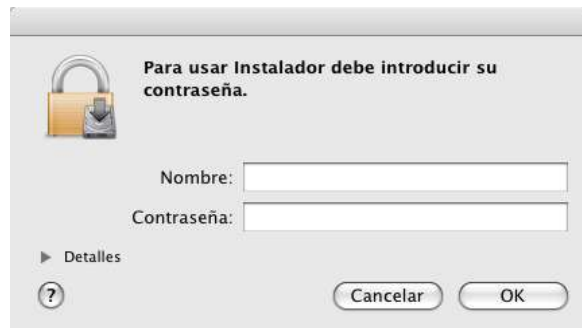


	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa


Jarraitu botoian klik egin instalazioa abiarazteko.



Tresneriarako administratzailearen sarrera eskatuko da, liburutegi garrantzitsuak instalatu eta konfiguratuko direlako.



Instalazioa amaitzean, berrabiarazi. Ordenagailua berrabiarazi denean, ekin hurrengo pausoari.

	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08 4.0.1.0 bertsioa
	Produktua: Izenpe Kita	



Izenpe Middleware-ren instalazioa


Instalatzailearen ikonoan (*Izenpe-middleware.pkg.dmg*) klik bikoitza egin, instalatzailea (*Izenpe-middleware.pkg*) duen unitatea muntatzeko.

Instalatzailea abiaraziko da. Egin klik *Continuar* (jarraitu) botoian.



Hurrengo pausoan, instalazio-jarraibideak irakurri eta *Continuar* (jarraitu) botoian klik egin.

KONTUZ: erabilgarri dauden hiru hizkuntzak, gaztelania, euskara, eta ingelesa, alboko barra labainkorra jaitsez berrikus daitezke.

	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa




Ondoren, lizentzia-akordioa zabaltzen da.

KONTUZ: erabilgarri dauden hiru hizkuntzak: gaztelania, euskara, eta ingelesez azter daiteke barra labainkorra jaitsiz.




Aurrera jarraitzeko ezinbestekoa da lizentzia-akordioa onartzea. *Acepto* (ados) botoian klik egin.

	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa

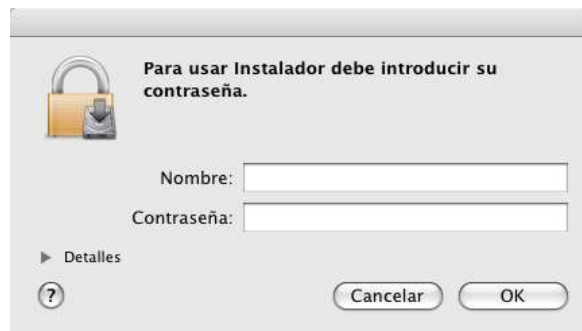


Garrantzitsua da instalazio estandarra egiten uztea, aurrez zehaztutako direktorioan, konfigurazioa errazteko helburuarekin. *Instalar* (instalatu) botoian klik egin.



	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08 4.0.1.0 bertsioa
	Produktua: Izenpe Kita	

Tresneriarako administratzailearen sarrera eskatuko da, liburutegi garrantzitsuak instalatu eta konfiguratu direlako.




Instalazioa zuzen egin da:



Une honetan, Bit4id-ren cryptoKEY tokena ordenagailuan libre duzun USB ataka batean konekta dezakezu. Mac OS X sistemak automatikoki ezagutuko du, eta ez du mezurik bistaratu 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

Puntu honetan eskuz instalatzeko egin behar diren urratsak deskribatzen dira. Horretarako, liburutegiak behar diren direktorioetara kopiatzen dira. Mac OS X sistemarako Izenpe Middleware-ren PKCS#11 interfazeak bi fitxategi ditu:

	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa

libbit4ipki.dylib.conf

libbit4ipki.dylib

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

/System/Library/Izenpe/pkcs11

Arazo ezagunak

Liburutegia Mozilla Firefox-ekin erabil daiteke client SSL kautotze baterako.

Dena dela, Mozilla-ren bug batek ez du uzten liburutegiaren bide-izena zehazten interfaze grafikoa erabilia; izan ere, gerta liteke liburutegia hautatu ondoren Firefox-ek honen gisako bide-izen bat bistaratzea:

AAAAAAFWAAIAAAxNYWNpbnRvc2ggSEQAAAAAAAAAAAAAAAAAAAAAC

Arazoa saihesteko, liburutegiaren bide-izen osoa eskuz sartu behar da dagokion eremuan. Esate baterako:


/System/Library/Izenpe/pkcs11/libbit4ipki.dylib

Konfigurazioa Firefox-en

Txartel adimenduna Mozilla Firefox nabigatzailean erabili ahal izateko, Universal Middleware-ren liburutegietarako euskarria eskuz gehitu behar da. Instalazio automatizatuak huts egiten duenean besterik ez da egin behar prozedura hori.


Mozilla Firefox ireki ondoren, hemen klik egin behar da: *Firefox* → *Preferencias*



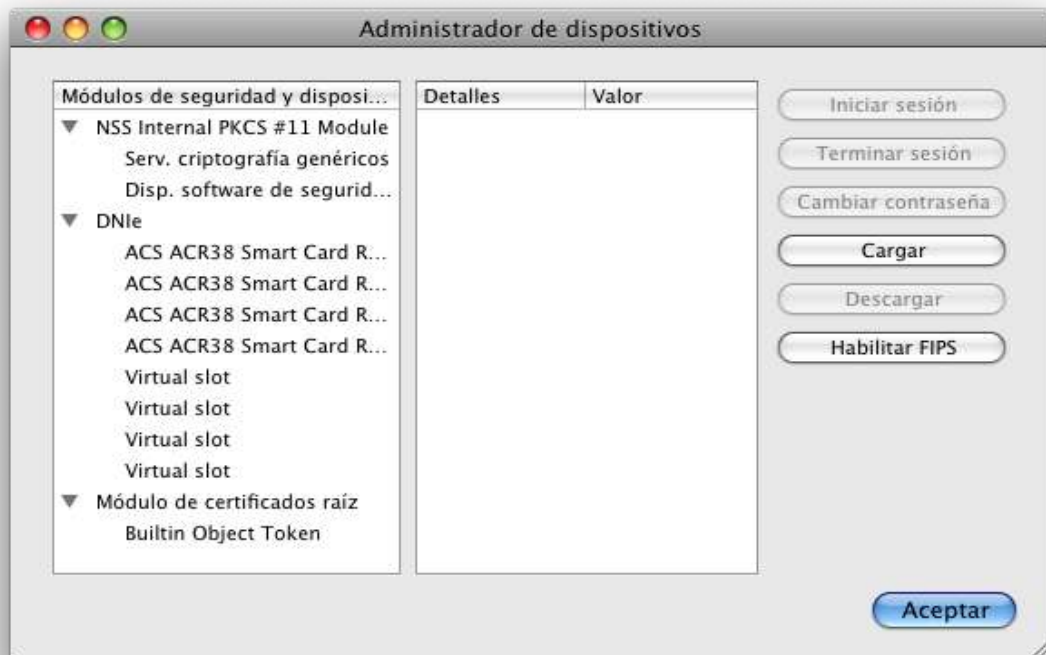
	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa

Ondoren, *Cifrado* (zifraketa) fitxa hautatu eta *Dispositivos de Seguridad* (segurtasun-gailuak) botoian klik egin.



	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa

Segurtasun-gailuen administratzailearen pantailan, *Cargar* (kargatu) botoian klik egin.



Cargar dispositivo PKCS#11 (Kargatu PKCS#11 gailua) leihoan datu hauek sartu behar dira:


- Moduluaren izena: *Izenpe Middleware*
- Moduluaren fitxategia:
`/System/Library/Izenpe/pkcs11/libbit4ipki.dylib`

Ondoren, *Aceptar* (ados) botoian klik egin. Modulus behar bezala gehituko da eta Firefox-eko instalazioa amaituta izango da.

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.

	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa

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




PIN Manager erabiltzea

Izenpe PIN Manager aplikazioa erabilgarri dago aplikazioen menuan.




Funtzionaltasunak

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

	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa



[1. irudia]

	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa

Funtzioen taula

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


Funtzioa	Deskribapena
PINa aldatu	Txartelaren PINa aldatzeko funtzioa (ikus 2. irudia)
PINa desblokeatu	Txartelaren PINa bere PUKaren bitartez desblokeatzeko funtzioa (ikus 3. irudia)
PUKa aldatu	Txartelaren PUKa aldatzeko funtzioa (ikus 4. irudia)
Txartelaren informazioa	Txartelari buruzko informazioa (modelo, 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]

	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa

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.

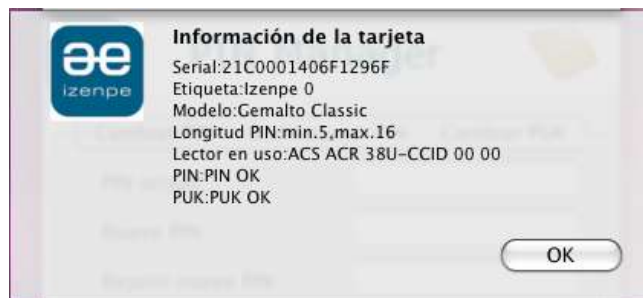


[4. irudia]

	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa

Txartelaren informazioa

Txartelaren informazio zehatza eskaintzen du: modelo, 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.

	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08
	Produktua: Izenpe Kita	4.0.1.0 bertsioa



Konbina ditzaket zenbakiak eta letrak txartelaren PIN zenbakirako?

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

Zalantza 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.

	Dokumentuaren izenburua:	2014/07/08
	Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	4.0.1.0 bertsioa
Produktua:		
Izenpe Kita		

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 etorrira.

Sinadura elektronikoa: datuen multzoa, modu elektronikoa, 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 elektronikoa sinplea, aurreratua eta onartua.

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

Sinadura elektronikoa 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 elektronikoa onartua: sinadura elektronikoa onartua ziurtagiri onartu batean oinarritzen den eta sinadura sortzeko gailu seguru baten bidez sortu den sinadura elektronikoa aurreratua da. Eskuz egindako sinadurak paperean idatzitako datuekin duen balio bera izango du sinadura elektronikoa onartuak modu elektronikoa 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 ezeztatze 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 norik hartu zuen parte egiaztatze aukera ematen du.

	Dokumentuaren izenburua: Mac OS X sistemarako instalazioa eta erabiltzailearen eskuliburua	2014/07/08 4.0.1.0 bertsioa
	Produktua: Izenpe Kita	

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

Ziurtagiri 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 iraungitzean 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, gakoaren segurtasunean zalantza badago, autoritate ziurtagiri-emailearen ekimenagatik ziurtagiri digital bat behin betiko ezeztatzea. Ezeztatzea atzera ezinezko egoera da. Etete-egoera baten ondoren edo eskatzeko baimena duten pertsonak hala nahi dutelako, ziurtagiri bat ezeztatzeke eska daiteke. Era berean, etendako ziurtagiri baten kasuan, gehieneko etete-egoera igaro bada, ziurtagiria gaitu ez badute, behin betiko ezeztatua egotera pasako da. Ziurtagiri-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.