Shënimet teknike për HIGHSEC eID App Middleware

Version 2.1.1

Gusht 2014.

**Përmbajtja**

[1 Shënimet teknike 3](#_Toc396932923)

[1.1 Të gjitha sistemet operative 3](#_Toc396932924)

[1.1.1 Ngadalësimi i kartelave gjatë çiftëzimit 3](#_Toc396932925)

[1.1.2 Leximi i PKCS#11 në Desktop-in PGP 3](#_Toc396932926)

[1.1.3 Detektimi i komponentëve për eID në web kontrolluesin 4](#_Toc396932927)

[1.1.3.1 Internet Explorer 4](#_Toc396932928)

[1.1.3.2 Mozilla Firefox 5](#_Toc396932929)

[1.1.4 Detektimi i bibliotekës PKCS#11 në aplikacionet e klientëve 6](#_Toc396932930)

[1.1.4.1 Internet Explorer 6](#_Toc396932931)

[1.1.4.2 Mozilla Firefox 6](#_Toc396932932)

[1.1.4.3 Mozilla Thunderbird 9](#_Toc396932933)

[1.1.5 Gjenerimi i çelësit në PGP Desktopin 11](#_Toc396932934)

[1.1.6 Autentikimi on-line me ndihmën e Internet Exploreri-it 11](#_Toc396932935)

[1.1.7 Deskripsioni i dosjes me ndihmën e Adobe Acrobat-it 13](#_Toc396932936)

[1.1.8 Aplikcioni administrativ dhe Desktop-i PGP 13](#_Toc396932937)

[1.1.9 Regjistrimi në Windows dhe Desktop-in PGP 13](#_Toc396932938)

[1.1.10 Firefox/Thunderbird ekstensionet për përdoruesit (e rinj). 14](#_Toc396932939)

[1.1.11 Çregjistrimi/fikja e Windows-it dhe çertifikatat e përdoruesve 14](#_Toc396932940)

[1.2 Windows XP SP3 x32 14](#_Toc396932941)

[1.2.1 Problemi me Word-in 2003 14](#_Toc396932942)

[1.2.2 Internet Explorer 7 14](#_Toc396932943)

[1.2.3 Internet Explorer 8 14](#_Toc396932944)

[1.2.4 Mozilla Thunderbird 14](#_Toc396932945)

[1.3 Windows 7 dhe Windows Vista 15](#_Toc396932946)

[1.3.1 Office 2010 15](#_Toc396932947)

[1.3.2 Windows Live 2011 15](#_Toc396932948)

[1.3.3 Mozilla Thunderbird 15](#_Toc396932949)

[1.3.4 CAN/PIN Dokuyimi ne çështjet e dialogut 15](#_Toc396932950)

[1.4 Windows 8 dhe Serveri 2012 15](#_Toc396932951)

# Shënimet teknike

## Të gjitha sistemet operative

Instaloni shtesat më të reja dhe paketat e servisit për sistemin tuaj operativ.

### Ngadalësimi i kartelave gjatë çiftëzimit

Nëqoftëse ndodhen shumë karta të ndryshme tashmë të çiftuara në kompjuter, atëhere cilido çiftim i ardhshëm do të jetë gjithnjë edhe më i ngadalshëm. Zgjidhja: Në Administration aplikacion do të gjeni opsionin “Fshi çiftimet” dhe në këtë mënyrë i fshini të gjitha.

### Leximi i PKCS#11 në Desktop-in PGP

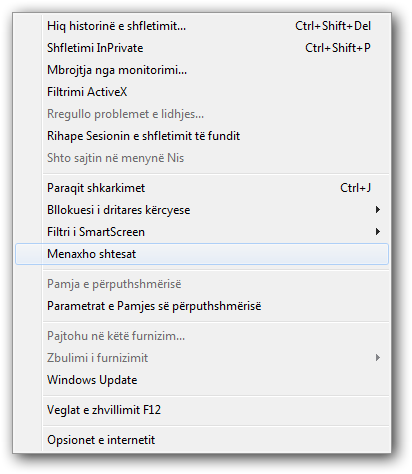
Që të përdorni eID App në Desktop-in PGP, në fillim lexoni modulin PKCS#11.

1. Instaloni eID App.
2. Hapni Desktopin-in PGP.
3. Zgjidhni menunë Tools > PGP Options.
4. Zgjidhni kartën Keys dhe ndryshoni opsionin “synchronize with smart cards and tokens” në Other dhe mbas kësaj zgjidhni modulin tuaj PKCS#11. Mund t’a gjeni edhe dosjen, në të cilën është instaluar eID App, ndërsa emri i modulit është hsmwp11\_x86.dll.
5. Shtypni OK dhe kthehuni në dritaren kryesore PGP të Desktop-it.
6. Zgjidhni menunë Tools > Options > Keys.
7. Mbas pak kohe do të shfaqet asistenti për importimin e çertifikatave PGP të Desktop-it.
8. Shtyp Cancel.
9. Rinisni Desktop-in PGP.
10. Nëqoftëse të gjitha janë kryer me sukses, atëhere në kornizën e Desktop-it PGP do të shfaqet një tufë e re me çelësa e quajtur Smart Card Keys, përveç atyre që tashmë ekzistojnë (psh., All Keys, My private Keys).

### Detektimi i komponentëve për eID në web kontrolluesin

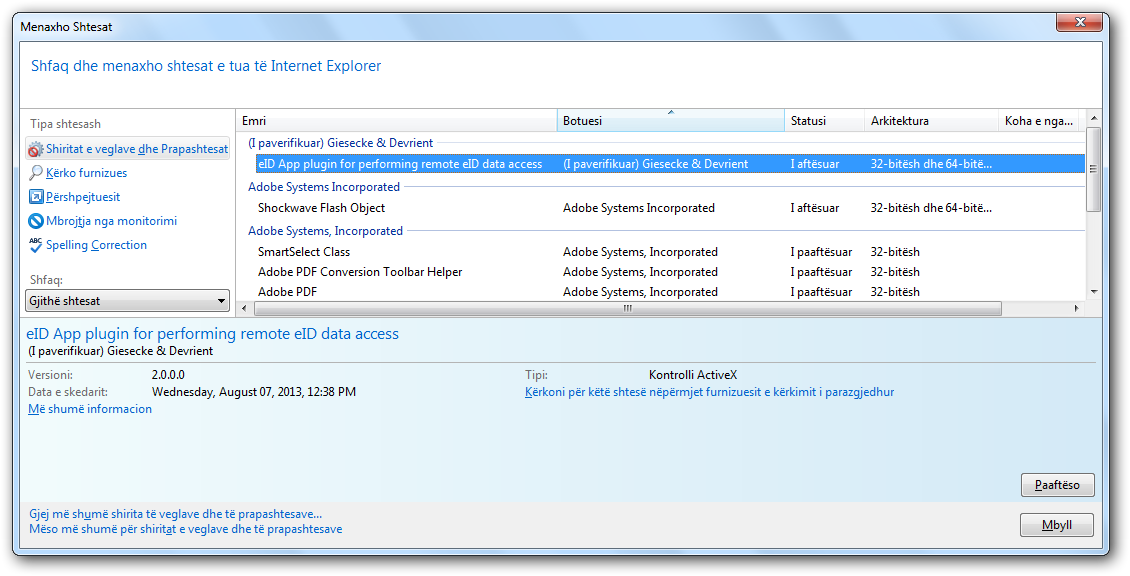
#### Internet Explorer

Startoni Internet Explorer-in dhe zgjidhni menunë *Vegla > Menaxho shtesat*.



Fotoja 1: Klikoni në Menaxho shtesat

Në dialogun *Menaxho Shtesat* ndryshoni tekstin listës rënëse duke shpresuar për listën *Gjithe shtesat*.



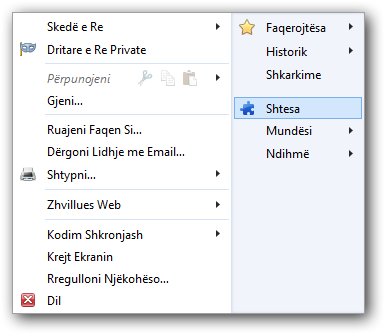
Fotoja 2: Teksti *Të gjitha shtesat* në listën rënëse *Shfaq*



Fotoja 3: Komponenti i instaluar eID App

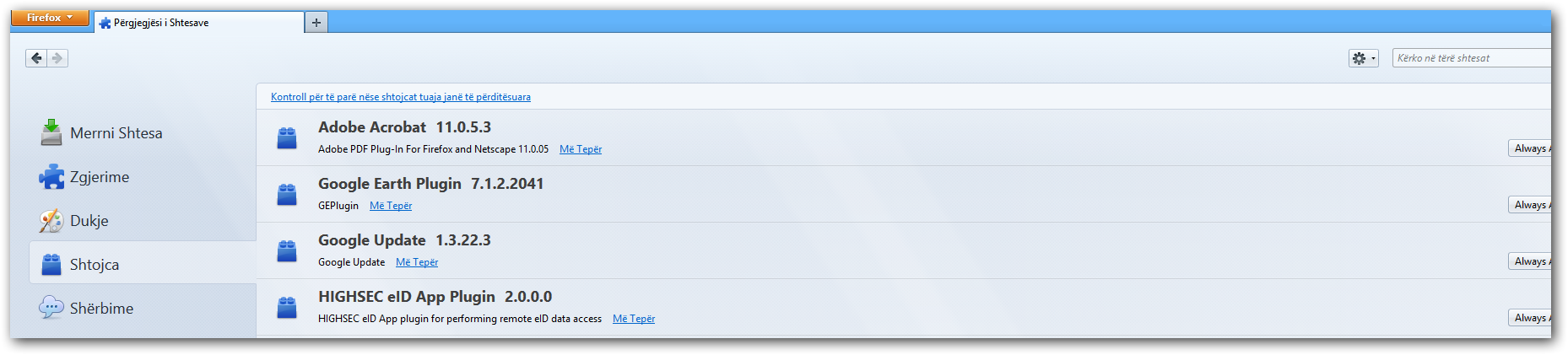
#### Mozilla Firefox

Startoni Firefox dhe hapni përgjegjësi i shtesave.



Fotoja 4: Hapni menunë e Firefoxit dhe zgjidhni Shtesa

Në Përgjegjësin e shtesave klikoni në *Shtojca* dhe gjeni komponentin HIGSEC eID App.



Fotoja 5: Komponenti HIGSEC eID App në Firefox

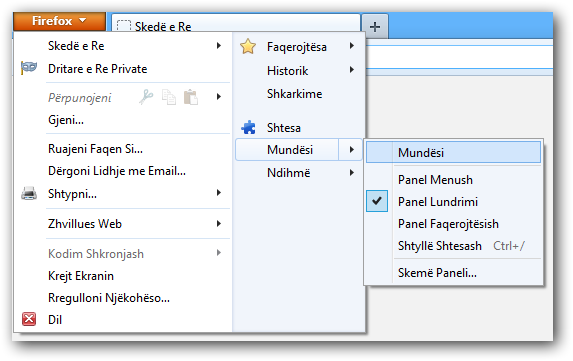
### Detektimi i bibliotekës PKCS#11 në aplikacionet e klientëve

#### Internet Explorer

Internet Explorer nuk e përdor bibliotekën PKCS#11, sepse është i orientuar në CryptoAPI.

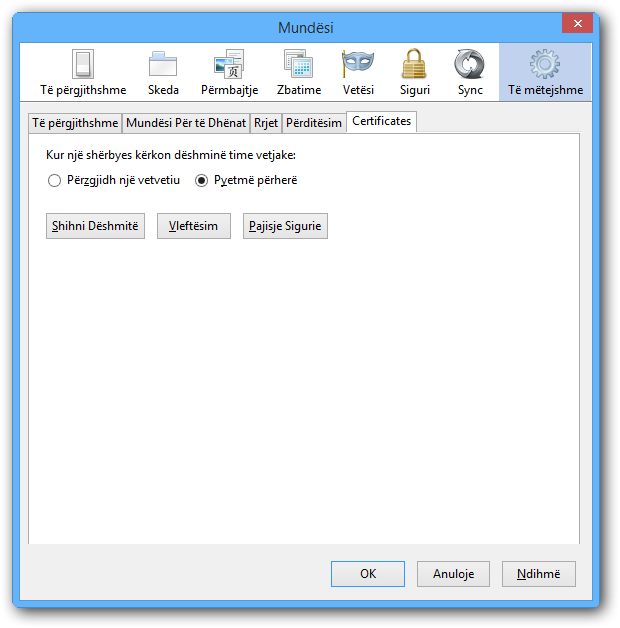
#### Mozilla Firefox

Startoni Mozilla Firefox dhe hapni menunë *Mundësi*.



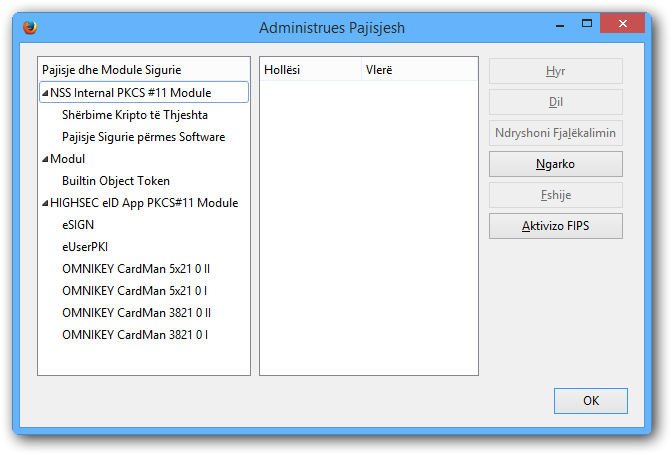
Fotoja 6: Mundësitë në Mozilla Firefox

Në dritaren me opsionet hapni seksionin *Të mëtejshme*, edhe në këtë seksion në kartën *Cerificates,* dhe mbas kësaj klikoni në butonin *Pajisjeve te sigurisë*.



Fotoja 7: Skeda e Certificates në mundësitë e Të mëtejshme

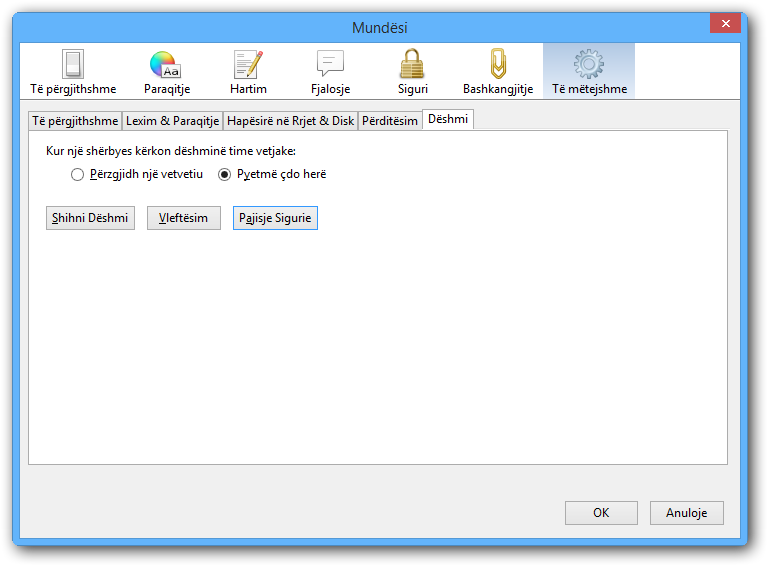
Do të tregohet Administrues Pajisjesh. Në anën e majtë të dritares ndodhet lista *Pajisje dhe Module Sigurie*. Moduli HIGHSEC eID App PKCS#11 do të jetë në këtë listë.



Fotoja 8: Moduli HIGHSEC eID App PKCS#11 në Firefox

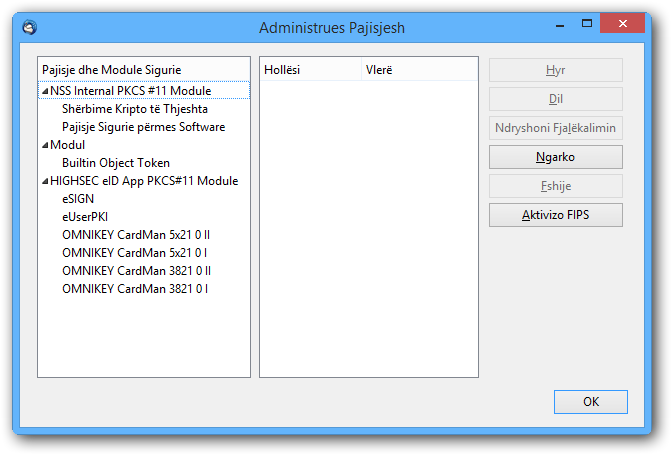
#### Mozilla Thunderbird

Klikoni në *Veglat > Mundësitë > Të mëtejshme > Dëshmi* dhe pastaj në butonin *Pajisje Sigurie*.



Fotoja 9: Menyja e mundësive në Thunderbird

Do të tregohet *Administrues Pajisjesh*. Në anën e majtë të dritares ndodhet lista *Pajisje dhe Module Sigurie*. Moduli HIGHSEC eID App PKCS#11 do të jetë në këtë listë.



Fotoja 10: Moduli HIGHSEC eID App PKCS#11 në Thunderbird

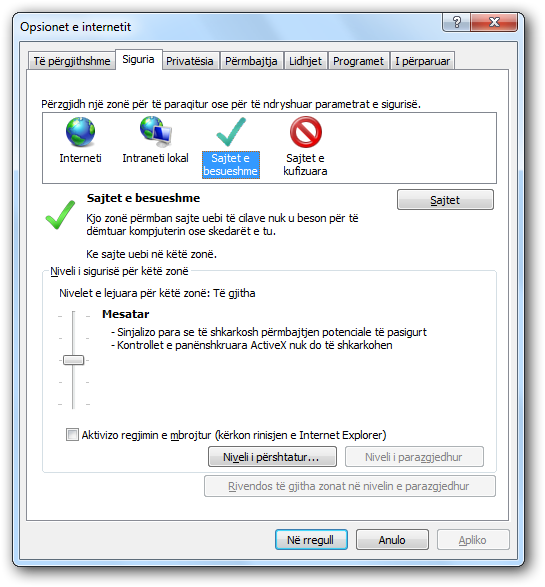
### Gjenerimi i çelësit në PGP Desktopin

Desktopi PGP nuk mund të përdoret për gjenerimin e çiftit të çelësave në kartën smart, sepse tenton të gjenerojë çiftin e çelësave për nevojat e enkripsionit dhe nënshkrimit dixhital, gjë që karta smart nuk e lejon.

### Autentikimi on-line me ndihmën e Internet Exploreri-it

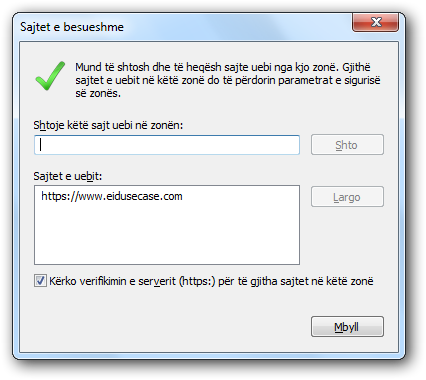
Në mënyrë që përdoruesi, me anë të Internet Explorerit, të hyjë në web lokacionin me rrjetin me autentikacionin, ai duhet të shtojë këtë web lokacion në listën e web lokacioneve të besueshme në Internet Explorer.

Mbas starimit të Internet Exploreri-it zgjidhni menunë *Veglat > Opsionet e internetit > Siguria*, mbas kësaj zgjidhni *Sajtet e besueshme* dhe klikoni në butonin *Sajtet*.



Fotoja 11: Karta *Siguria* në dritaren *Opsionet e internetit*

Do të hapet dialogu i ri. Regjistroni emrin e lokacionit (psh. <https://www.eidusecase.com>) dhe klikoni në Shto. Emri i web lokacionit do të shfaqet në listën Web lokacionet të dialogut Lokacionet e besueshme.



Fotoja 12: Dritarja e lokacioneve të besueshme

Mbylleni dialogun dhe aplikoni ndryshimet.

### Deskripsioni i dosjes me ndihmën e Adobe Acrobat-it

Nëqoftëse përdoruesi tenton të hapë dokumentin PDF të shifruar me Adobe Acrobat-in, Adobe Acrobat do të kërkojë nga përdoruesi që dy herë të regjistrojë PIN-in e kartën smart.

### Aplikcioni administrativ dhe Desktop-i PGP

PGP Desktop Services shkakton probleme të lidhura me hyrjen ekskluzive të kartës smart. Hyrja ekskluzive është e nevojshme për aplikacionin Adminitration eID App për disa prej operacioneve. Për shkak të problemit të përmendur aplikacioni Adminitration do të lajmërojë gabimin “Momentalisht është tashmë aktiv sesioni CAPI ose PKCS#11”. Në mënyrë që aplikacioni të jetë plotësisht funksionale Desktop-i PGP, duhet të jetë i deinstaluar.

### Regjistrimi në Windows dhe Desktop-in PGP

Nëqoftëse është instaluar Desktop-i PGP dhe përdoruesi tenton që të regjistrohet në sistemin operativ Windows, dialogu për regjistrimin mund të ndalojë të reagojë ndaj komandave të përdoruesit, gjithë kohën deri sa përdoruesi nuk shtyp kombinimin e tastierës Ctrl+Alt+Delete. Që kjo sjellje të ndërpritet, Desktop-i PGP duhet të jetë i deinstaluar.

### Firefox/Thunderbird ekstensionet për përdoruesit (e rinj)

Çdo përdorues idividualisht duhet të mundësojë ekstensionet eID App për nevojën personale. Ekstensionet për Firefox dhe Thunderbird u janë çmundësuar atyre përdoruesve, të cilët akoma nuk i kanë mundësuar. Ekstensionet u janë mundësuar edhe atyre përdoruesve, profilet e të cilëve janë krijuar mbasi eID App tashmë është instaluar.

### Çregjistrimi/fikja e Windows-it dhe çertifikatat e përdoruesve

Windows nuk lejon modifikimin e magazinës së çertifikatave të përdoruesve mbasi procedura e fikjes dhe/ose e çregjistrimit është filluar. Për këtë arsye eID App nuk mund të deinstalojë çertifikatat e përdoruesve prej magazinave të çertifikatave të përdoruesve dhe ato do të qëndrojnë të disponueshme dhe mbas startimit/regjistrimit në Windows edhe pse karta smart potencialisht më nuk është e disponueshme.

## Windows XP SP3 x32

### Problemi me Word-in 2003

Për nënshkrimet digjitale Word 2003 përdoren vetëm ato çertifikata dhe çelësat, vlera KeySpec e të cilave është vendosur në AT\_KEYEXCHANGE. Çertifikatat, vlera KeySpec e të cilave është vendosur në AT\_SIGNATURE, nuk do të procesohen (nuk do të përfillen). Zgjidhje: të përdoret versioni i ri i Word-it (psh. Word 2007), i cili merr parasysh edhe çertifikatat me AT\_SIGNATURE KeySpec.

### Internet Explorer 7

Web aplikacionet ekzistuese mund të kërkojnë kombinimin shifror për SSL, të cilat IE7 nuk e mbështet. Nëqoftëse SSL është i fikur atëhere komponenti do të punojë saktësisht.

### Internet Explorer 8

Web aplikacionet ekzistuese mund të kërkojnë kombinimin shifror për SSL, të cilat IE8 nuk i mbështet. Nëqoftëse SSL është i fikur atëhere komponenti do të punojë saktësisht.

### Mozilla Thunderbird

Çertifikatat kryesore CA dhe çertifikatat tjera në zinxhir, duhet të jenë të shënuara si të besueshme në magazinën Thunderbird-it të çertifikatave autoritative. Nëqoftëse cilado prej çertifikatave në zinxhir, nuk është shënuar si e besueshme, atëhere Thunderbird nuk do të ketë mundësi të verifikojë validitetin e çertifikatës së përdoruesit.

## Windows 7 dhe Windows Vista

### Office 2010

Për Office 2010 duhet të jenë të instaluara korrigjimet më të reja dhe paketat e servisit. Nëqoftëse përdoruesi nuk instalon korrigjimet më të reja dhe paketat e servisit, Word 2010 do të tentojë që nëpërmjet CNG Key Storage Provider-it të depërtojë deri tek çelësit privat të lidhur me çertifikatën ESIGN në kartën smart, dhe përdoruesi nuk do të ketë mundësi të nënshkruajë dokumentin. Zgjidhja është nisja e Office-it 2010 në regjimin e kompatibilitetit për Windows XP SP3, ose të instalojë korrigjimet më të reja. Korrigjimi urgjent kb2412320 për Office-in 2010.

Nëqoftëse përdoruesi nuk instalon korrigjimet më të reja dhe paketat e servisit, dhe nëqoftëse çertifikata që përdoret për enkripsionin e e-postës nuk posedon mundësitë SMIME, Outlook 2010 do të përdori algoritmin RC2 të enkripsionit në vend të 3DES (ashtu siç është vendosur në opsionet siguruese të e-postës për këtë urdhër në Outlook), prandaj deskripsioni nuk do të jetë i mundur në Outlook 2010. Korrigjimi urgjent kb2475877 për Outlook-in 2010.

### Windows Live 2011

Windows Live 2011 përdor algoritmin RC2 të enkripsionit në vend të 3DES. 3DES duhet që të përdoret, sepse kështu është adaptuar në konfiguracionin e urdhërit. Karta nuk mund të përdoret.

### Mozilla Thunderbird

Çertifikatat kryresore CA dhe çertifikatat e tjera në zinxhir duhet të jenë të shënuara si të besueshme në magazinën Thunderbird të çertifikatave autoritative. Nëqoftëse cilado prej çertifikatave në zinxhir nuk është shënuar si e besueshme atëhere Thunderbird nuk do të ketë mundësi të verifikojë validitetin e çertifikatës së përdoruesit.

### CAN/PIN Dokuyimi ne çështjet e dialogut

Përdoruesi duhet të klikojë në dialogun CAN/PIN kur të shfaqet për herë të parë. Duke filluar nga sistemi operativ Windows Vista, aplikacioneve nuk u lejohet të shkarkojnë fokusin nga aplikacionet e tjera.

## Windows 8 dhe Serveri 2012

Instaloni shtesat më të reja dhe paketat e servisit për sistemin operativ të tuajin.