eID App Administration – Udhëzime për përdorimin

Përmbajtja

[1 Hyrje 3](#_Toc397015454)

[2 Pasqyrimi i Aplikacionit 3](#_Toc397015455)

[3 Konfiguracioni HIGHSEC eID App 3](#_Toc397015456)

[3.1 Fshirja e çiftimeve ekziszuese në kartë 4](#_Toc397015457)

[4 Analizimi i kartës smart 5](#_Toc397015458)

[5 Operacionet mbi kartën smart 6](#_Toc397015459)

[5.1 Ndryshimi i mesazhit të sigurisë 6](#_Toc397015460)

[5.2 Operacionet mbi PIN-in 7](#_Toc397015461)

[5.2.1 ID PIN 7](#_Toc397015462)

[5.2.2 Zhbllokimi i ID PIN-it 8](#_Toc397015463)

[5.2.3 ESIGN-PIN 10](#_Toc397015464)

[5.2.4 Zhbllokimi i ESIGN PIN-it 11](#_Toc397015465)

[5.3 Operacionet me çertifikatat 12](#_Toc397015466)

[5.3.1 Importimi i çertifikatës 12](#_Toc397015467)

[5.3.2 Azhurnimi i çertifikatës 15](#_Toc397015468)

[5.3.3 Mënjanimi i çertifikatës 17](#_Toc397015469)

[6 Funksionet shtesë 19](#_Toc397015470)

[7 Third Party Software 20](#_Toc397015471)

[7.1 OpenSSL Toolkit 20](#_Toc397015472)

[7.1.1 OpenSSL License 20](#_Toc397015473)

[7.1.2 Original SSLeay License 21](#_Toc397015474)

[7.2 BouncyCastle Crypto APIs 22](#_Toc397015475)

[7.2.1 License 23](#_Toc397015476)

# Hyrje

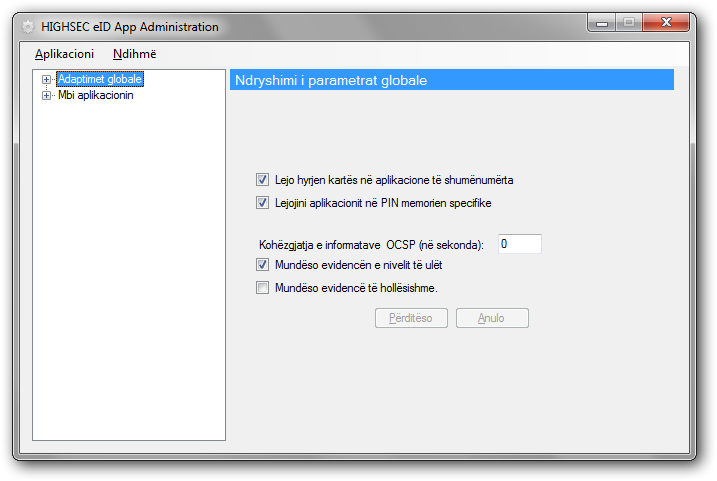
Aplikacioni i Administrimit të HIGHSEC eID App (në vazhdim aplikacioni) shërben për të drejtuar dhe të kontrollojë funksionalitetin e pjesës tjetër të sistemit eID App. Gjithashtu shërben edhe që të mundësojë shikimin e përmbajtjes së kartës smart, si dhe të drejtojë çertifikatat të depozituara në kartën smart. Aplikacionit është i nevojshëm Framework .NET 3.5 SP1 ose .NET Framework 4, por përdor funksionalitetin e dhënë në bibliotekën kriptografike Bouncy Castle, të prodhuesit të pavarur, e cila është pjesë e instalimit.

# Pasqyrimi i Aplikacionit

Aplikacioni ka vetëm një dritare kryesore. Dritarja është ndarë në dy pjesë kryesore, pamja e shtyllës në të majtë dhe hapësira e lirë në dritare nga ana e djathtë. Kur përdoruesi e zgjedh njësinë në pamjen e shtyllës formulari përkatës do të pasqyrohet në hapësirën e lirë të dritares. Në menunë që ndodhet lartë përdoruesi mund të ndryshojë gjuhën e aplikacionit.

# Konfiguracioni HIGHSEC eID App

Disa opsione kontrollojnë sjelljen e pjesës së mbetur të sistemit eID App. Të gjitha ato mund të gjënden dhe të kontrollohen nga paragrafi i shtyllës “Adaptimet globale”.



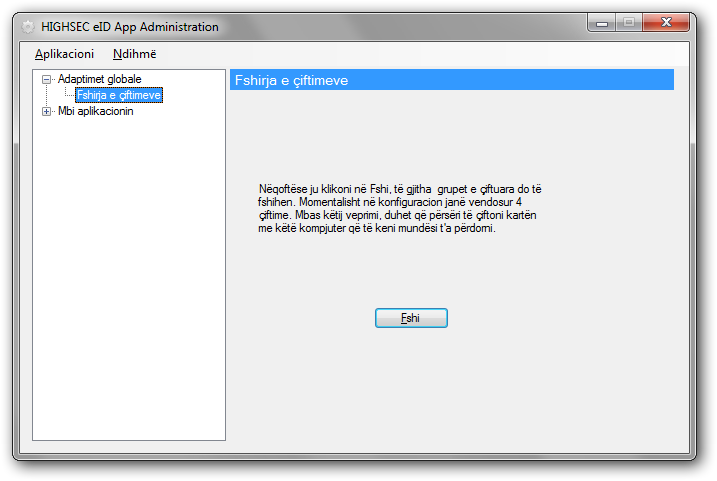
Në vazhdim është dhënë një përshkrim i shkurtër i këtyre opsioneve:

* *Lejo hyrjen kartës në aplikacione të shumënumërta*: Kur ky opsion është aktiv, disa aplikacione të Windows-it mund të shfrytëzojnë kartën smart. Nëqoftëse opsioni nuk është aktiv vetëm një aplikacion mund të shfrytëzojë kartën në momentin e dhënë.
* *Lejoji aplikacioneve të rimemorizojnë PIN-in*: Rimemorizimi i PIN-it ka kuptim vetëm nëqoftëse më shumë aplikacione kanë mundësi që në të njëjtën kohë të hyjnë në kartë. Kur ky opcion është në funksion, PIN-i do të kërkohet nga përdoruesi vetëm njëherë për çdo aplikacion, kur aplikacioni për herë të parë do të kërkojë hyrje në kartë. Nëqoftëse opsioni nuk është aktiv, PIN-i do të kërkohet nga përdoruesi çdo herë kur ndonjë aplikacion hyn në kartë.
* *Validiteti i përgjigjes OCSP*: Periudha kohore, në të cilën mendohet se çertifikata është valide mbasi është verifikuar nëpërmjet OCSP-së (Protokoll për verifikimin e statusit të çertifikatës në rrjet).
* *Mundëso evidentimin e nivelit të ulët*: Kur ky opcion është aktiv të gjitha komunikimet midis kartës smart dhe eID App do të ruhen në dosje të veçantë të evidencës. Komunikimi është i shifruar, prandaj edhe përmbajta e dosjes së evidencës është i shifruar.
* *Mundëso evidencën e zgjeruar*: Kur ky opsion është aktiv eID App do të shkruajë të dhëna shtesë të dhe detajuara në dosjen e evidencës. Ky opsion është i dobishëm për diagnostifikimin e problemeve në punë.

Nëse përdoruesi ndryshon një ose më shumë opsione butoni Azhurno do të mundësohet. Kur përdoruesi klikon Azhurno, opsionet e reja do të ruhen. Nëqoftëse përdoruesi klikon në Anulo të gjitha opsionet do të kthehen në gjendjen e tyre të mëparshme.

## Fshirja e çiftimeve ekziszuese në kartë

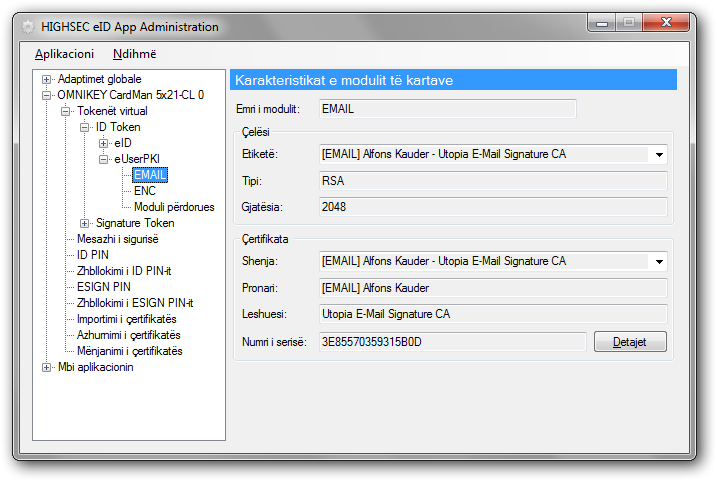
Për të përdorur kartën smart, ajo duhet të çiftohet me kompjuterin. Për të fshirë të gjitha çiftimet nga kompjuteri zgjidhni paragrafin e shtyllës “Fshirja e çiftimeve”. Në faqen e re shtypni butonin Fshi.



Mbasi të gjitha çiftimet ekzistuese janë fshirë, që t’a përdorni kartën përsëri, ju duhet të çiftoni kartën përsëri.

# Analizimi i kartës smart

Kur karta smart vendoset në lexues, në shtyllë do të shtohet paragrafi i zgjeruar i shtyllës me emrin e lexuesit. Përdoruesi mund të analizojë përmbajtjen e kartës smart me kërkimin nëpër nën paragrafin e shtyllës “Tokenët virtualë”.



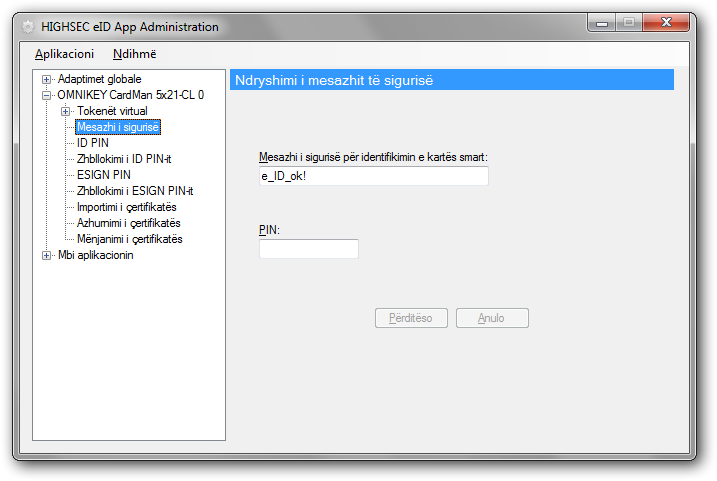
Çertifikatat përdoren për funksionalitete të ndryshme të kartës smart. Çertifikatat dhe çelsat përkatës janë të bashkuara me entitete të quajtura module, të cilat përmbahen në aplikacionet e kartave inteligjente, të cilat ndodhen në tokenët virtualë. Hyrja në tokenët virtualë mbrohet me PIN-ët. Struktura, e cila lidh të gjitha këto elemente është transformuar në paragrafet e shtyllës. Paragrafet përfundimtare çertifikatat të bashkuara me çdo modul. Në shumicën e rasteve është vetëm një çertifikatë për çdo modul, por atje ku ka më tepër se një, përdoruesi mund të zgjedh çertifikatën nga lista zbritëse, në të cilën janë shfletuar për çdo pronar.

# Operacionet mbi kartën smart

Kur karta smart vendoset në lexues, përdoruesi mund të kryejë disa operacione në lidhje me kartat smart. Të gjitha ato kërkojnë që të shkruajë PIN-in.

## Ndryshimi i mesazhit të sigurisë

Mesazhi i sigurisë është një formë e funksionalitetit të sigurisë në kartën smart jokontakte. Ky mesazh ndodhet në kartën smart, dhe përdoruesi duhet të dijë përmbajtjen e saj. Çdo herë kur karta smart kërkon kërkon vërtetimin e identitetit nga përdoruesi, ky mesazh i sigurisë do ti tregohet në shikim.



Përdoruesi mund të ndryshojë këtë mesazh të sigurisë me ndihmën e procedurës së mëposhtëme:

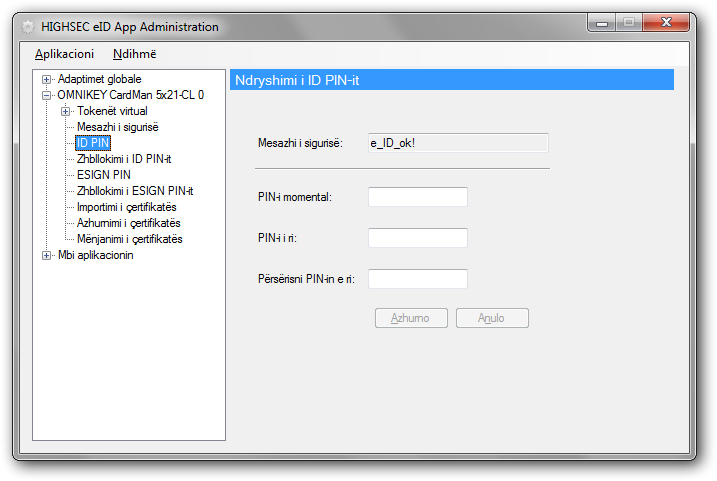
* Zgjidhni paragrafin e shtyllës “mesazhi i sigurisë”. Ky paragraf nuk do të ekzistojë në shtyllë nëqoftëse karta smart nuk është jokontakte. Do të tregohet faqja nën titullin “Ndryshimi i mesazhit të sigurisë”, kurse në anë do të shkruhet mesazhi momental i sigurisë.
* Zëvendësoni tekstin e mesazhit momental të sigurisë me mesazhin e sigurisë të ri.
* Regjistroni ID PIN në fushën “PIN”.
* Klikoni në Azhurnim. Do të tregohet mesazhi, i cili vërteton se operacioni është kryer me sukses.

## Operacionet mbi PIN-in

SCeID përmban dy tokena, të cilët përdoren për qëllime të ndryshme: ID dhe ESIGN.

### ID PIN

I vetmi operacion i lejuar mbi ID PIN-in (përveç zhbllokimit) është ndryshimi i PIN-it.



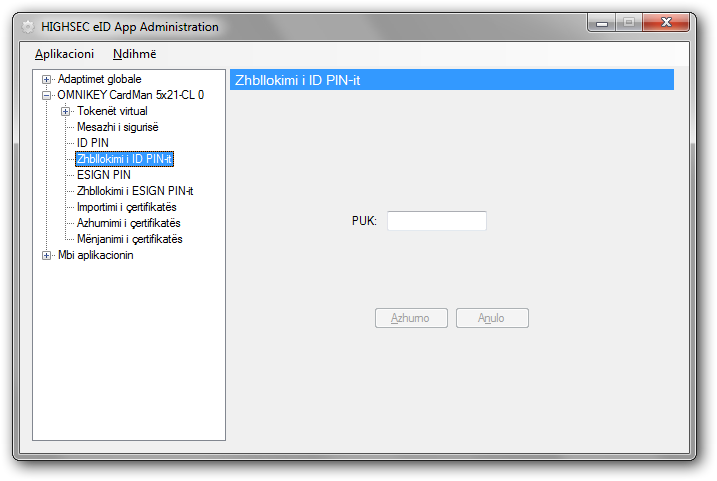
Përdorni procedurën e mëposhtëme që të ndryshoni ID PIN:

* Zgjidhni paragrafin e shtyllës ID PIN. Do të tregohet faqja me titullin “Ndryshimi i ID PIN-it”
* Nëqoftëse karta smart është jokontakte, vërtetoni që mesazhi i sigurisë është i saktë. Nëqoftëse karta smart nuk është jokontakte, mesazhi i sigurisë nuk ekziston.
* Regjistroni ID PIN-in valid momental në fushën “PIN-i momental”.
* Regjistroni PIN-in e ri në fushat “PIN-i i ri” dhe “Përsërisni PIN-in e ri”.
* Nëqoftëse përmbajtja e fushave “PIN-i i ri” dhe “Përsërisni PIN-in e ri” është identike, dhe fusha “PIN-i momental” nuk është e zbrazët, butoni Azhurno do të mundësohet.
* Kliknite në Azhurno. Do të tregohet mesazhi, i cili vërteton se operacioni është kryer me sukses.

### Zhbllokimi i ID PIN-it

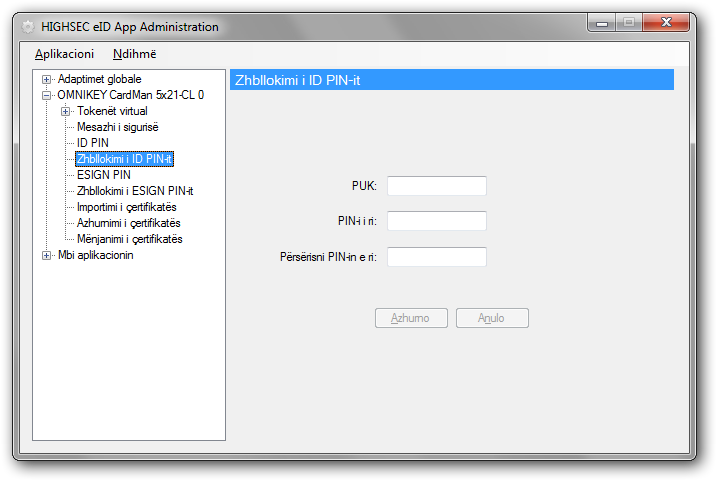
Nëqoftëse përdoruesi tre here rrjesht regjistron gabimisht ID PIN-in, si pjesë e cilitdo operacioni, për të cilin kërkohet PIN, karta smart do të bllokojë tentimet e mëvonshme për të përdorur PIN-in. Në këtë rast PIN-i duhet të zhbllokohet me ndihmën e PUK-ut (çelësi për çkyçjen te PIN-it). Përdorni procedurën e mëposhtëmeqë të zhbllokoni ID PIN-in, nëqoftëse regjistrimi i PIN-it të ri nuk është i domosdoshëm:

* Zgjidhni paragrafin e ri të shtyllës “Zhbllokimi i ID-PIN-it”. Do të tregohet faqja me titullin “Zhbllokimi i PIN-it”.
* Regjistroni PUK-un në fushën “PUK”.
* Klikoni në Azhurno. Do të tregohet mesazhi, i cili konfirmon se operacioni është përfunduar me sukses.



Përdorni procedurën e mëpshtëme që të zhbllokoni ID-PIN-in, nëqoftëse është e domosdoshme regjistrimi i PIN-it të ri:

* Zgjidhni paragrafin e shtyllës “Zhbllokimi i ID-PIN-it”. Do të tregohet faqja me titullin “Zhbllokimi i ID PIN-it”.
* Regjistroni PUK-un valid në fushën “PUK”.
* Regjistroni PIN-in e ri në fushat “PIN-i i ri” dhe “Përsërisni PIN-in e ri”.
* Nëqoftëse përmbajtja e fushave “PIN-i i ri” dhe “Përsërisni PIN-in e ri” është identike, dhe fusha “PUK” nuk është e zbrazët, butoni Azhurno do të mundësohet.
* Klikoni në Azhurno. Do të tregohet mesazhi, i cili konfirmon se operacioni është përfunduar me sukses.

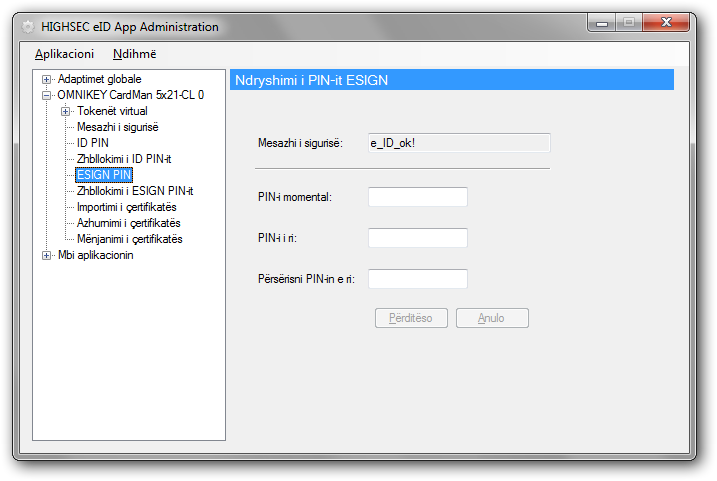


### ESIGN-PIN

I vetmi operacion i lejuar mbi ESIGN-PIN (përveç zhbllokimit) është ndryshimi i PIN-it.

Përdorni procedurën e mëposhtëme për të ndryshuar ESIGN-PIN:

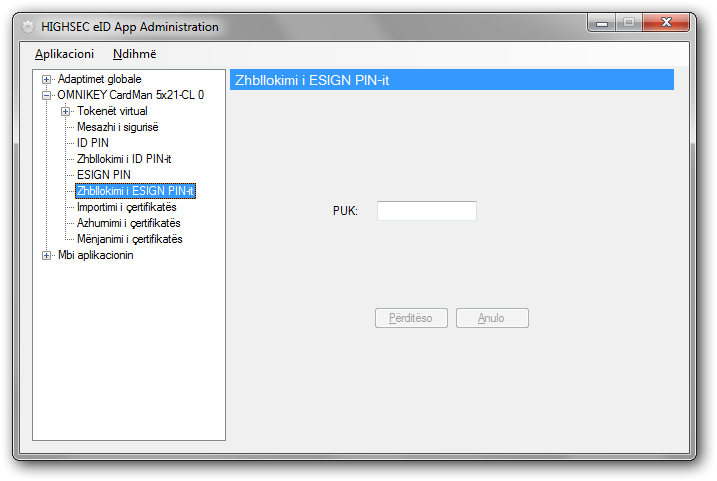
* Zgjidhni paragrafin e shtyllës ESIGN PIN. Do të tregohet faqja me titull “Ndryshimi i PIN-it ESIGN”.
* Nëqoftëse karta smart është jokontakte, konfirmoni se mesazhi i sigurisë është i saktë. Nëqoftëse karta smart nuk është jokontakte, mesazhi i sigurisë nuk ekziston.
* Regjistroni ESIGN PIN momental valid në fushën “PIN-i momental”.
* Regjistroni PIN-in e ri në fushat “PIN-i ri” dhe “Përsërisni PIN-in e ri”.
* Nëqoftëse përmbatja e fushave“PIN-i i ri” dhe “Përsërisni PIN-in e ri” janë identike, dhe fusha “PIN-i momental” nuk është e zbrazët, butoni Azhurno do të mundësohet.
* Klikoni në Azhurno. Do të tregohet mesazhi, i cili konfirmon se operacioni është përfunduar me sukses.



### Zhbllokimi i ESIGN PIN-it

Nëqoftëse përdoruesi tre herë rrjesh regjistron gabimisht ESIGN PIN, si pjesë e cilitdo operacioni për të cilin kërkohet PIN, smart kartica do të bllokojë tentimet e mëtejshme që të përdoret PIN-i. Në këtë rast PIN-i duhet të zhbllokohet me ndihmën e PUK-ut (çelësi për çkyçjen e PIN-it – PIN Unlock Key). përdorni procedurën e mëposhtëme që të zhbllokoni ESIGN PIN-in:

* Zgjidhni paragrafin e shtyllës “Zhbllokimi i ESIGN PIN-it”. Do të tregohet faqja me titullin “Zhbllokimi i ESIGN PIN-it”.
* Regjistroni PUK-un valid në fushën “PUK”.
* Klikoni në Azhurnim. Do të tregohet mesazhi, i cili konfirmon se operacioni është përfunduar me sukses.



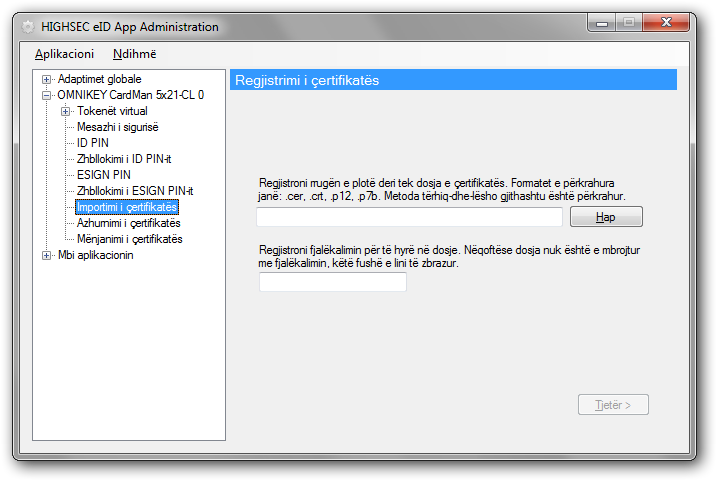
## Operacionet me çertifikatat

Çertifikatat përdoren për të garantuar identitetin e dikujt. Pronari i çertifikatës është personi, i cili posedon çelësin privat të shoqëruar me çertifikatën e dhënë. Smart karta mund të përmbajë më shumë çertifikata, ku sejcila, ka qëllim të ndryshëm. Nëqoftëse çertifikata nuk ekziston në kartë, atëhere në fillim duhet *të importohet.* Nëqoftëse çertifikata tashmë ekziston në kartë, atëhere mund të *azhurnohet* me tjetrën. Çertifikata, gjithashtu, mund të jetë edhe *e fshirë* nga karta.

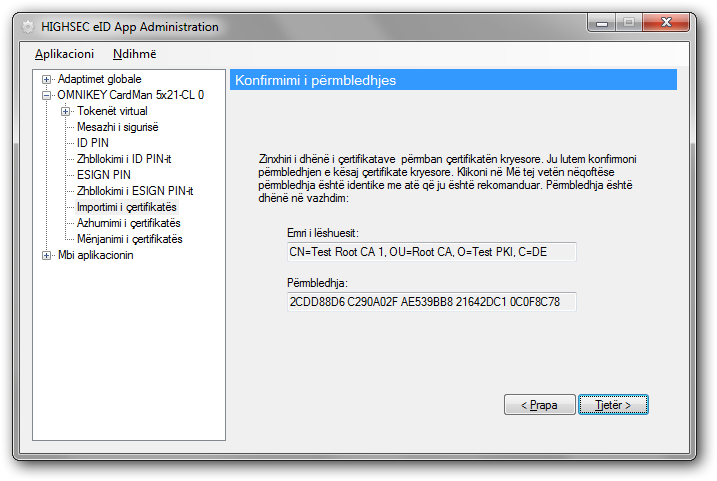
### Importimi i çertifikatës

Importimi i çertifikatës në kartën smart është procedurë, e cila kryhet në disa hapa, prej të cilëve disa mund të jenë të lënë mbas dore, në varësi nga rrethanat. Përdorni procedurën e mëposhtëme për importimin e çertifikatës:

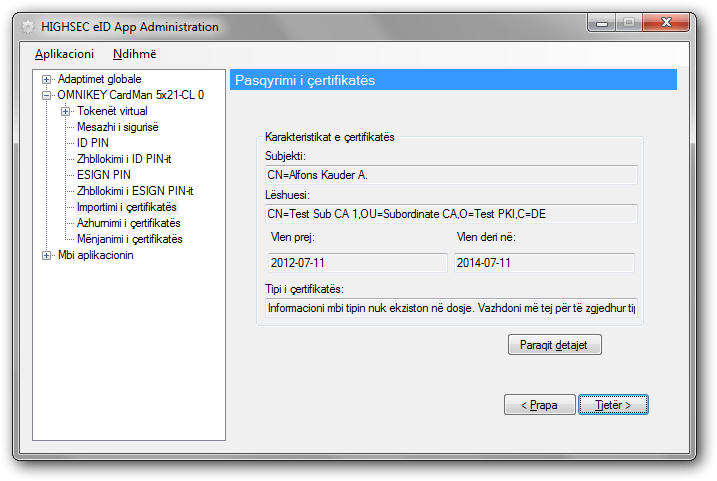
* Parakusht: tipi i çertifikatës, i cili duhet të importohet nuk mundet që tashmë të ndodhet në kartën smart.
* Zgjidhni paragrafin e shtyllës “Importimi i çertifikatës”. Do të shfaqet faqja nën titullin “Regjistrimi i çertifikatës”. Kjo është faqja e parë e ekspertit për importimin.



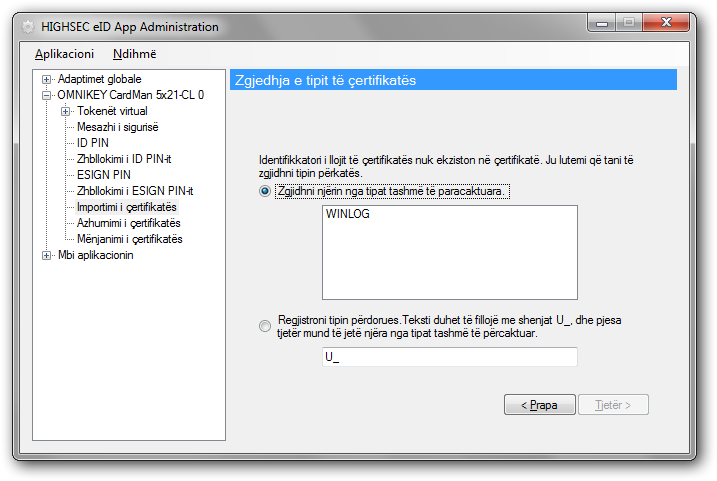
* Në fushën e parë regjistroni rrugën e plotë deri tek çertifikata. Çertifikatën mund t’a gjeni lehtë me klikun në butonin Hape.
* Nëqoftëse është i nevojshëm fjalëkalimi për leximin e çertifikatës importuese, regjistroni fjalëkalimin në fushën e dytë sipas rradhës.
* Klikoni në Tjetri. Nëqoftëse në zhinxhirin e importimit të çertifikatave ndodhet edhe çertifikata kryesore, do të shfaqet faqja “Konfirmimi i përmbledhjes”. Nëqoftëse çertifikata kryesore nuk ndodhet, kaloni në faqen tjetër.



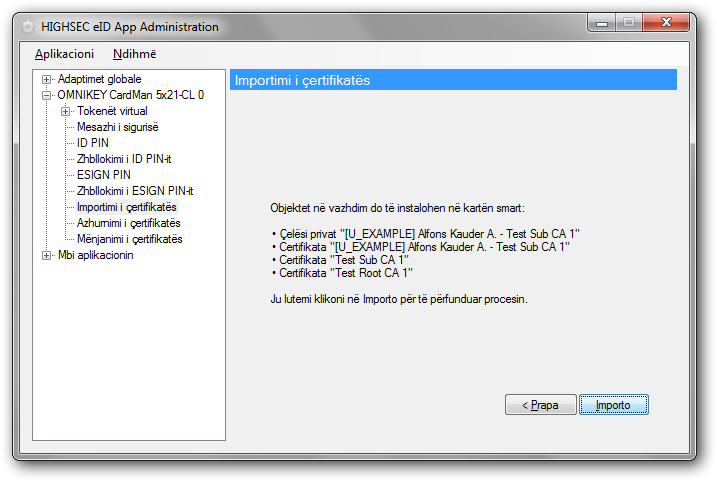
* Klikoni në Tjetri. Do të shfaqet faqja nën titullin “Pasqyrimi i çertifikatës”.



* Konfirmoni se kjo është çertifikata, të cilën dëshironi t’a importoni. Mund të klikoni në “Paraqit detajet”, që të shikoni të gjitha informatat lidhur me çertifikatën. Në fushën “Tipi i çertifikatës” do të tregohet tipi i çertifikatës, nëqoftëse informata për tipin ekziston në çertifikatë.
* Klikoni Tjetri. Nëqoftëse nuk është gjetur tipi i çertifikatës, do të shfaqet faqja “Zgjedhja e tipit të çertifikatës”. Nëqoftëse tipi tashmë është gjetur, kaloni në faqen tjetër.



* Përdoruesi duhet të zgjedhë tipin e çertifikatës manualisht. Mundësia e parë është që përdoruesi të zgjedhë njërin nga tipet e përcaktuara më parë, të cilët tashmë nuk ndodhen në kartë. Mundësia tjetër është që përdoruesi të regjistrojë emrin e ri të tipit. Emri i ri duhet të fillojë me gërmën latine U, mbas së cilës pason shenja “\_” (nënvizim), mbas të cilës pason emri i ri.
* Klikoni në Tjetri. Do të shfaqet faqja me titullin “Importimi i çertifikatës”.



* Kjo ështe faqja e fundit, mbas së cilës çertifikata do të importohet në kartën smart.
* Klikoni në Importo. Do të shfaqet faqja me titullin “Statusi i operacioneve”, me rezultatin e treguar të importimit. Nëqoftëse rezultati është i suksesshëm, përdoruesi mund të klikojë në butonin Përsëri, për të importuar çertifikatë tjetër.

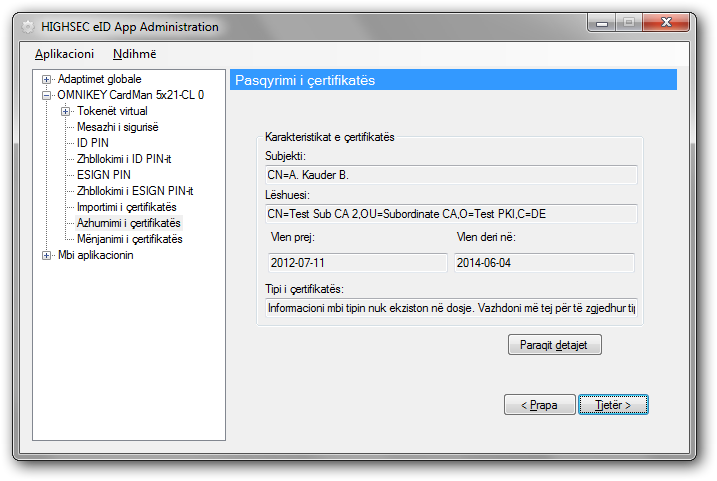
### Azhurnimi i çertifikatës

Azhurnimi i çertifikatës në kartën smart është procedurë, e cila kryhet në disa hapa, prej të cilëve disa mund të jenë të lënë mbas dore, në varësi nga rrethanat. Shfrytëzoni procedurën e mëposhtëme për azhurnimin e çertifikatës:

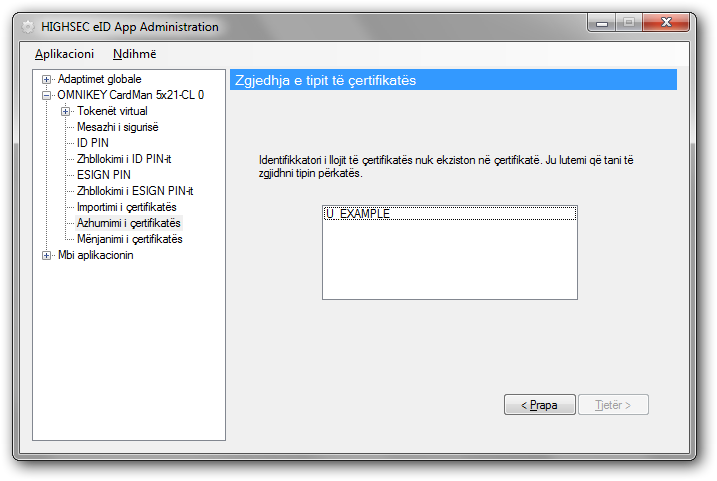
* Parakusht: Tipi i çertifikatës që duhet të azhurnohet duhet që tashmë të ndodhet në kartën smart.
* Zgjidhni paragrafin e shtyllës “Azhurnimi i çertifikatës”. Do të shfaqet faqja nën titullin “Regjistrimi i çertifikatës”. Kjo është faqja e parë e ekspertit për azhurnimin.



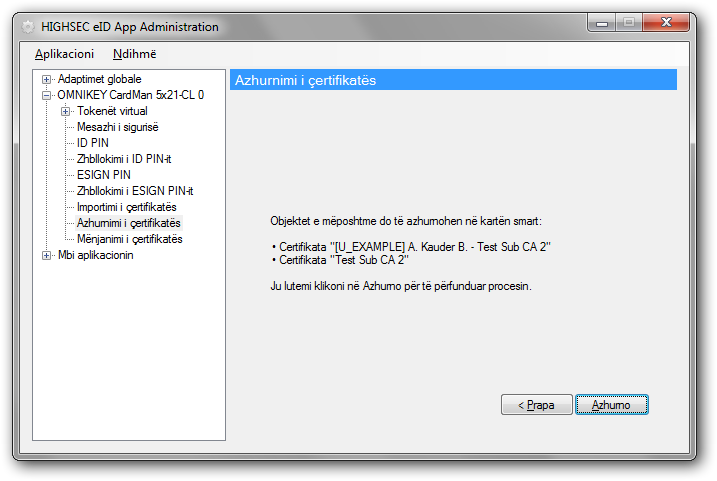
* Regjistroni rrugën e plotë deri tek çertifikata. Çertifikatën mund t’a gjeni lehtë me klikun në butonin Hap.
* Klikoni ne Tjetri. Do të do të shfaqet faqja me titullin “Pasqyrimi i çertifikatës”.



* Konfirmoni se kjo është çertifikata, të cilën dëshironi të azhurnoni. Mund të klikoni në “Paraqit detajet”, në mënyrë që të shikoni të gjitha informatat e lidhura me çertifikatën. Në fushën “Tipi i çertifikatës” do të tregohet tipi i çertifikatës, nëqoftëse informata mbi tipin ekziston në çertifikatë.
* Klikoni në Tjetri. Nëqoftëse nuk është gjetur tipi i çertifikatës, do të shfaqet faqja “Zgjedhja e tipit të çertifikatës”. Nëqoftëse tipi është zgjedhur, kaloni në faqen në vazhdim.



* Përdoruesi duhet të zgjedhë manualisht tipin e çertifikatës. Janë ofruar vetëm tipet e çertifikatave të pëdoruesve, të cilat tashmë ndodhen në kartë.
* Klikoni në Tjetri. Do të shfaqet faqja me titullin “Azhurnimi i çertifikatës”.

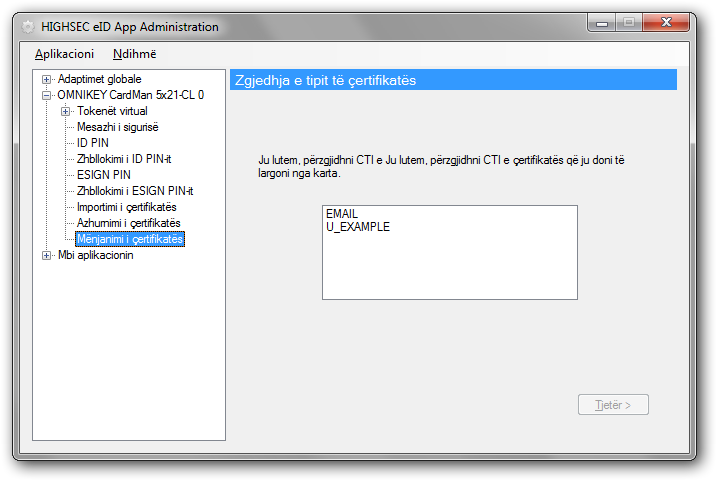


* Kjo është faqja e fundit, mbas të cilës çertifikata do të azhurnohet në kartën smart.
* Klikoni në Azhurnim. Do të shfaqet faqja me titullin “Statusi i operacioneve”, me rezultatin e treguar të azhurnimit. Nëqoftëse rezultati ishte i suksesshëm, përdoruesi mund të klikojë në butonin Përsëri që të azhurnojë çertifikatën tjetër.

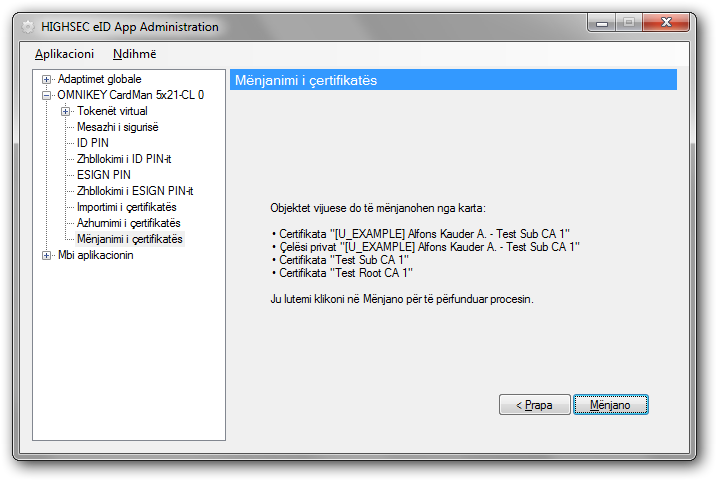
### Mënjanimi i çertifikatës

Mënjanimi i çertifikatës nga karta smart është procedurë që kryhet në disa hapa. Shfrytëzoni procedurën e mëposhtëme për mënjanimin e çertifikatës:

* Parakusht: tipi i çertifikatës që do të mënjahohet duhet që tashmë të ndodhet në kartën smart.
* Zgjidhni paragrafin e shtyllës “Mënjanimi i çertifikatës”. Do të shfaqet faqja me titullin “Zgjedhja e tipit të çertifikatës”. Kjo është faqja e parë e ekspertit për mënjanimet.



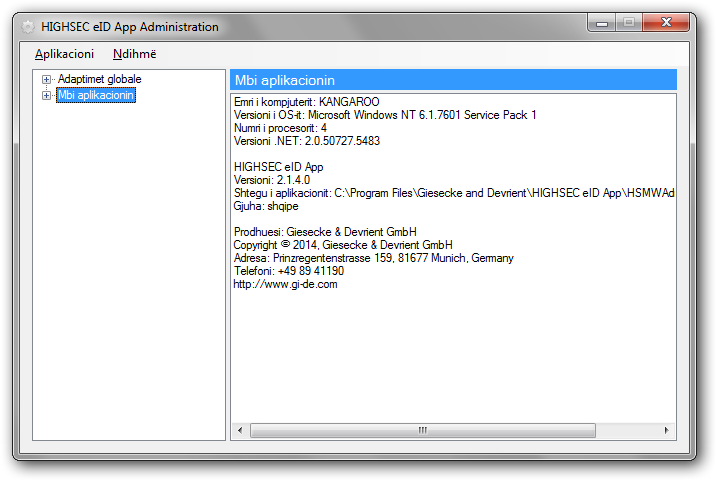
* Përdoruesi duhet të zgjedhë tipin e çertifikatës manualisht. Janë ofruar vetëm tipet e çertifikatave të përdoruesve, të cilat tashmë ndodhen në kartë, por që mund të mënjanohen.
* Klikoni në Tjetri. Do të shfaqet faqja me titullin “Mënjanimi i çertifikatës”.



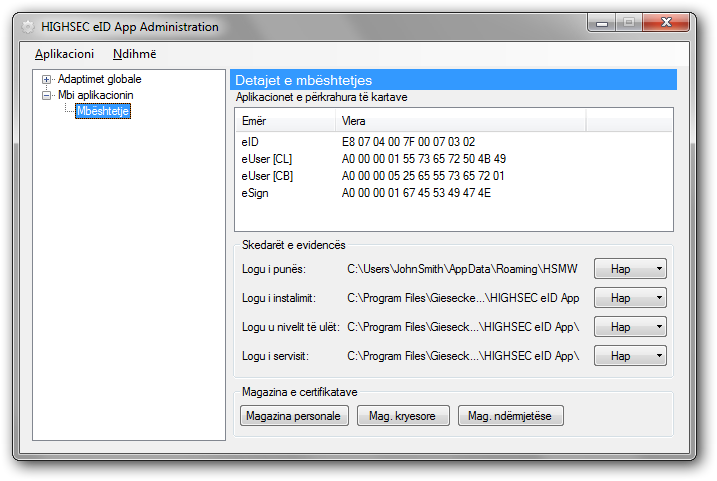
* Klikoni në Mënjano. Do të shfaqet faqja me titullin “Statusi i operacioneve”, me rezultatet e treguara të mënjanimit. Nëqoftëse rezultati është i suksesshëm, përdoruesi mund të klikojë në butonin Përsëri për të mënjanuar çertifikatën tjetër.

# Funksionet shtesë

Në faqjen me titullin “Mbi aplikacionin”, përdoruesi mund të gjejë informata të ndryshme mbi aplikacionin, si edhe mbi rrethimin operativ.



Në faqen e titulluar “Mbështetje” përdoruesi mund të gjejë informata shtesë, siç është lista e aplikacioneve të kartave, të cilat i mbështet eID App, rrugët deri tek dosjet evidentuese të ndryshme, si edhe hyrja në magazinat kryesore të çertifikatave.



Për çdo dosje evidentuese, butoni përkatës do të hapë dosjen evidentuese më relevante dhe më të fundit, kurse dosjet e tjera janë të disponueshme nëqoftëse përdoruesi shtyp shigjetën poshtë butonit të dhënë, dhe mbas kësaj zgjedh “Hap dosjen përkatëse”.

Dosja e evidencës së punës (log-u i punës) përmban aksionet e krijuara me përdorimin e bibliotekës CSP dhe PKCS#11. Nëqoftëse asnjë aksion i tillë nuk është kryer, atëhere dosja e evidencës nuk do të ekzistojë.

Dosja e evidencës së instalimit (log-u i instalimit) krijohet gjatë proçesit të instalimit. Kliku në Hape do të hapë dosjen më të re të evidencës, ndërsa dosjet e tjera janë të disponueshme fashikullën përkatëse.

Dosja e evidencës së nivelit të ulët përmban komunikimin direkt ndërmjet kartës smart dhe shërbimit eID App. Ky komunikim është i shifruar, prandaj edhe mesazhet në dosjen e evidencës janë të shifruara.

Dosja e evidencës së shërbimeve përmban aksione, të cilat i ka kryer shërbimi eID App.

Tre butonet në fund të faqjes shërbejnë për pasqyrën e përmbajtjes së magazinave përkatëse të çertifikatave. Kur pasqyrohet lista e çertifikatave, përdoruesi mund të shikojë detajet e cilësdo, në mënyrë të tillë që do të zgjedhë njërin dhe do të ndjekë lidhjen e dhënë në linjën e fundit.

Magazina personale përmban çertifikata, të cilat i përkasin vetë përdoruesit.

Magazina kryesore përmban çertifikata kryesore të besuara. Çertifikatat kryesore janë vetnënshkruese, garantojnë vetë për veten e tyre dhe për ato çertifikata që nënshkruajnë.

Magazina ndërmjetëse përmban çertifikatat e autoritetit për çertifikimin ndërmjetëse. Ato nënshkruajnë dhe garantojnë për përdoruesit e çertifikatës, kurse për to garantojnë çertifikatat kryesore.

# Third Party Software

The HIGHSEC eID App installation package contains software developed by third parties:

## OpenSSL Toolkit

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)). The usage of the OpenSSL Toolkit is provided under the license conditions as stated here: <http://www.openssl.org/source/license.html>.

### OpenSSL License

Copyright (c) 1998-2011 The OpenSSL Project.  All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

1. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
2. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
3. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)  
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

### Original SSLeay License

Copyright (C) 1995-1998 Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)) All rights reserved.

This package is an SSL implementation written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to.  The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com))"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

1. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com))"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed.  i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

## BouncyCastle Crypto APIs

This product includes software developed by the Legon of Bouncy Castle [http://www.bouncycastle.org](http://www.bouncycastle.org/).

The usage of the BouncyCastle Crypto API is provided under the license terms as stated here: <http://bouncycastle.org/licence.html>

Please note this should be read in the same way as the [MIT license](http://opensource.org/licenses/MIT).

### License

Copyright (c) 2000 - 2013 The Legion of the Bouncy Castle Inc. ([http://www.bouncycastle.org](http://www.bouncycastle.org/))

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.