HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

TrueCrypt alat za kriptiranje Windows datotečnih sustava

CCERT-PUBDOC-2005-12-142

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Jedan od važnih aspekata zaštite digitalnih podataka pohranjenih na tvrdim diskovima računala od neovlaštenog pristupa je enkripcija datotečnog sustava. Ovom metodom moguće je zaštititi povjerljive podatke pohranjene na tvrdom disku u slučaju gubitka ili krađe prijenosnog računala, kao i u slučaju pristupa povjerljivim podacima od strane neovlaštenog napadača koji je ostvario fizički pristup računalu. Moderni operacijski sustavi dolaze s već ugrađenim mehanizmima za enkripciju podataka pohranjenih na tvrdim diskovima, ali se u tu svrhu mogu koristiti i dodatna aplikacijska rješenja i sustavi kao funkcionalna nadogradnja na mehanizme samog operacijskog sustava. Time je moguće poboljšati već postojeću funkcionalnost operacijskog sustava ili dodati posve novu funkcionalnost.
Glavni zahtjevi prilikom korištenja mehanizama za enkripciju podataka na tvrdim diskovima su dovoljna razina zaštite podataka i jednostavnost korištenja. Neki od osnovnih zahtjeva koje sustav za enkripciju podataka mora zadovoljiti su:

- **Zaštita sadržaja kriptiranih datoteka** – osim što sadržaj kriptiranih datoteka mora biti nerazumljiv korisniku koji nema odgovarajući pristupni ključ, sama metoda enkripcije podataka mora biti otporna na moguće napade i otkrivanje ključa korisnika.
- **Zaštita osjetljivih meta podataka** –uz sami sadržaj datoteke, potrebno je zaštititi i meta podatke vezane uz samu datoteku koji neovlaštenom korisniku mogu otkriti povjerljive informacije. Poseban naglasak je na onemogućavanju čitanje imena kriptiranih datoteka, bez odgovarajućeg ključa.
- **Transparentan pristup datotekama** – kriptirane datoteke ne bi se smjele razlikovati od običnih datoteka pohranjenih na disku (jednom kada korisnik unese ispravan ključ), tj. pristup tim datotekama od strane aplikacija mora biti transparentan za krajnjeg korisnika.
- **Transparentne performanse** – brzina pisanja i čitanja podatka na kriptiranom datotečnom sustavu neizbježno je manja od one na uobičajenim datotečnim sustavima. Unatoč tome, kriptirani sustav morao bi biti izveden tako da se ne naruši normalan rad korisnika na računalu i na taj način obeshrabri korisnika da koristi enkripciju datotečnog sustava.
- **Istovremeni pristup** – sustav mora omogućavati istovremeni pristup kriptiranim datotekama svim korisnicima i procesima koji posjeduju ovlasti pristupa tj. pristupne ključeve.
- **Zaštita mrežnog prometa** – prilikom korištenja distribuiranih datotečnih sustava, postoji mogućnost prisluškivanja mrežnog prometa od strane napadača, u svrhu prikupljanja osjetljivih informacija. Ukoliko su podaci na distribuiranom datotečnom sustavu kriptirani, neophodno je da se u takvom obliku prenose i putem računalne mreže.
- **Jednostavno upravljanje ključevima** – pristup zaštićenim podacima ostvaruje se pomoću korisničkih ključeva. Sustav mora biti izveden tako da od korisnika ne zahtijeva unošenje ključeva prilikom svake operacije čitanja i pisanja po datotečnom sustavu, već da se jednom unesen ključ smatra pouzdanim sve dok traje korisnička sjednica.

TrueCrypt je softversko rješenje za uspostavu i održavanje on-the-fly enkripcije Windows datotečnih sustava. On-the-fly enkripcija podataka znači da se podaci automatski enkriptiraju ili dekriptiraju prilikom pohrane ili dohvata podataka s diska bez ikakve intervencije korisnika. Podaci pohranjeni unutar kriptiranog datotečnog sustava ne mogu se pročitati (dekriptirati) bez poznavanja ispravne zaporke ili posjedovanja ispravnog ključa. TrueCrypt, uz kriptiranje samog sadržaja datoteka pohranjenih unutar kriptiranog datotečnog sustava, kriptira i meta podatke vezane uz datoteke (kao što su imena datoteka). Podatke koje dekriptira TrueCrypt niti u jednom trenutku ne pohranjuje u permanentnu memoriju računala, već se dekriptirani čuvaju isključivo u RAM-u računala.

2. Mogućnosti TrueCrypt alata

TrueCrypt programski alat služi za kriptiranje Windows FAT i NTFS datotečnih sustava. Pomoću TrueCrypt-a moguće je:

- kriptirati kompletne Windows particije,
- kriptirati samo dio već postojeće Windows particije, u ovom slučaju TrueCrypt stvara novu kriptiranu virtualnu Windows particiju kojoj se pristupa posve jednako kao i normalnoj Windows particiji.

Dodatna mogućnost TrueCrypt alata je stvaranje skrivenih particija. Osim što su kriptirane, ove particije su i nevidljive korisnicima koji ne znaju za njih (nije ih moguće vidjeti iz programskih alata kao što je npr. Windows Explorer). Isključivo oni korisnici koji znaju da postoji skrivena particija mogu joj i pristupiti.

Za kriptiranje datotečnog sustava TrueCrypt može koristiti sljedeće kriptografske algoritme:

- **AES** – TrueCrypt koristi AES s 14 iteracija uz primjenu 256 bitnog ključa (AES-256) u LRW načinu rada.
- **Blowfish** – koristi se 16 iteracija i 448 bitni ključ u LRW načinu rada.
- **CAST5** – koristi se 128 bitni ključ, za kriptiranje se koriste 64 bitni blokovi podataka i LRW način rada.
- **Serpent** – koristi se veličina ključa od 256 bita, kriptiraju se blokovi od 128 bita uz primjenu LRW načina rada.
- **Triple DES** – za kriptiranje se koriste tri nezavisna ključa veličine 56 bita u LRW načinu rada. Ovaj algoritam za kriptiranje je dosta sporiji u odnosu na ostale algoritme koje TrueCrypt podržava.
- **Twofish** – kriptiranje je izvedeno 256 bitnim ključem u LRW načinu rada, kriptiraju se 128 bitni blokovi podataka.
- **AES-Twofish** – u ovom načinu rada se za kriptiranje podataka koriste dva algoritma u kaskadi (podaci se prvo kriptiraju jednim algoritmom (AES) a odmah nakon toga drugim algoritmom (Twofish)). Ključevi obaju algoritama su međusobno različiti i nezavisni.
- **AES-Twofish-Serpent** – za kriptiranje se koriste tri algoritma u kaskadi. Algoritmi imaju različite i međusobno nezavisne ključeve.
- **Serpent-AES** – za kriptiranje se koriste dva algoritma u kaskadi. Algoritmi imaju različite i međusobno nezavisne ključeve.
- **Serpent-Twofish-AES** - za kriptiranje se koriste tri algoritma u kaskadi. Algoritmi imaju različite i međusobno nezavisne ključeve.
- **Twofish-Serpent** - za kriptiranje se koriste dva algoritma u kaskadi. Algoritmi imaju različite i međusobno nezavisne ključeve.

TrueCrypt koristi nekoliko različitih *hash* algoritama u svrhu generiranja pseudo slučajnih brojeva. Sljedeći *hash* algoritmi su podržani:

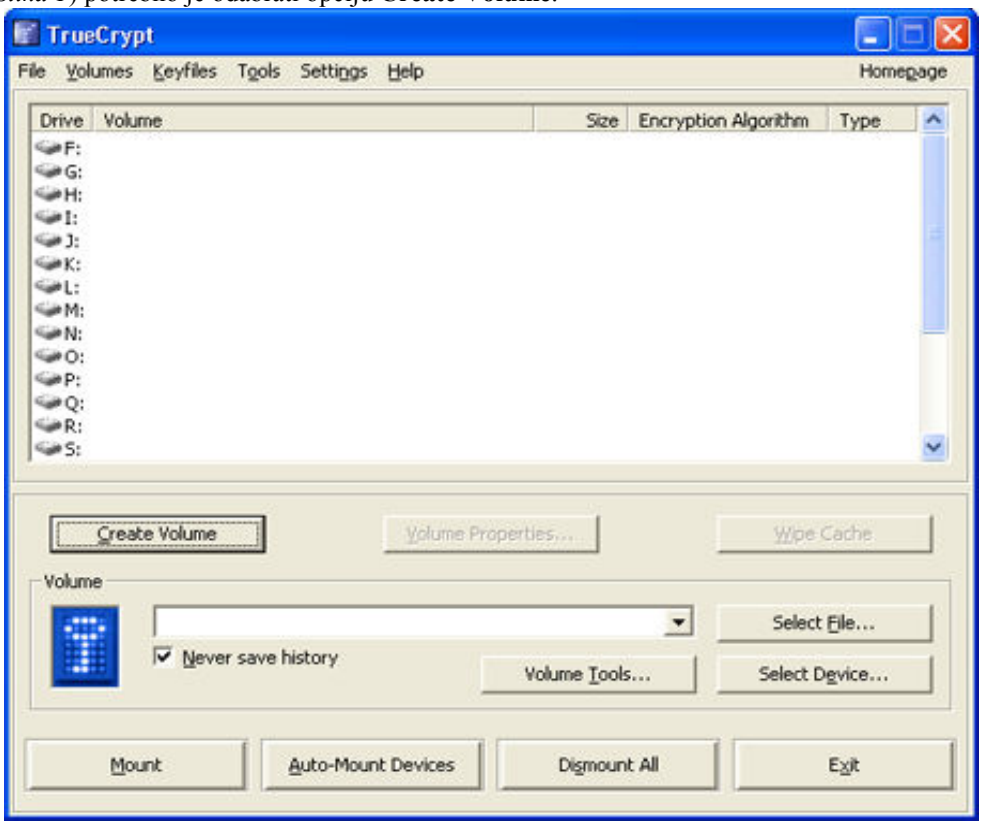
- **Whirlpool** – generira *hash* veličine 512 bita,
- **SHA-1** – generira *hash* veličina 160 bita.
- **RIPEMD-160** – generira *hash* veličine 160 bita.

Operativni sustavi koje trenutno podržava TrueCrypt su:

- Windows XP
- Windows XP x64 Edition
- Windows 2000
- Windows Server 2003
- Windows Server 2003 x64 Edition
- Linux (jezgra 2.6.5 ili novija)

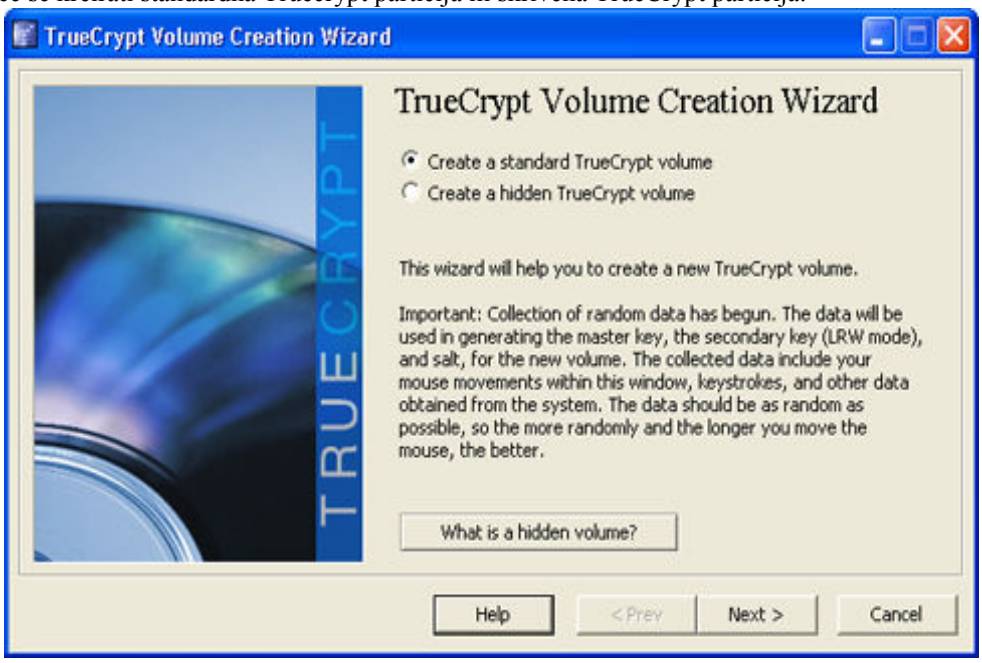
3. Kreiranje kriptirane Windows particije

Kako bi se kreirala nova kriptirana Windows particija, u glavnom prozoru TruCrypt alata (prikazan na slici *Slika 1*) potrebno je odabrati opciju **Create Volume**.



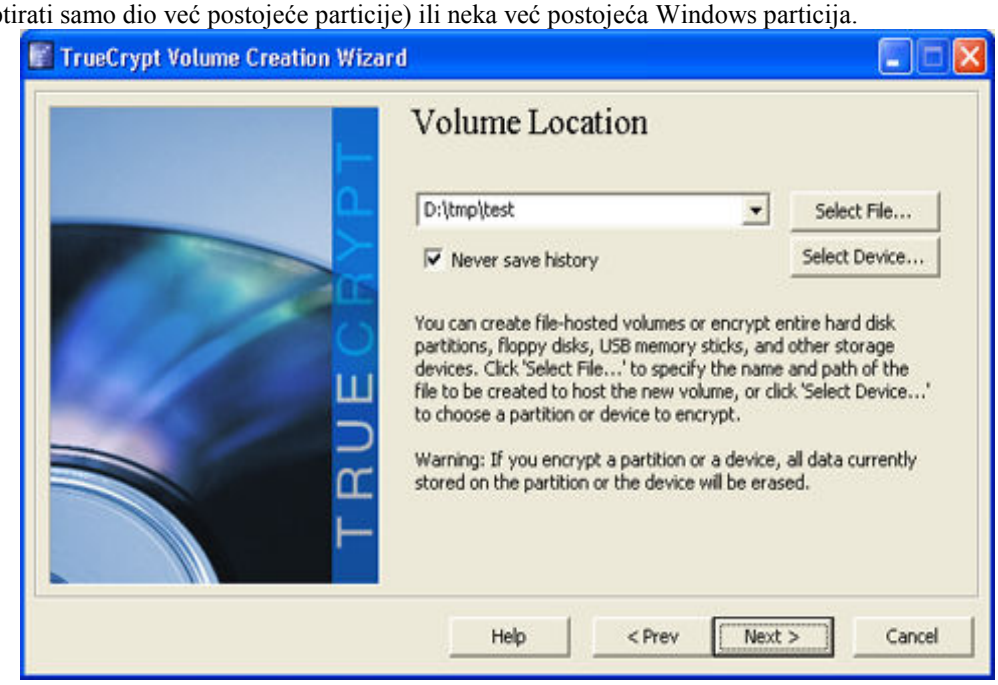
Slika 1: Glavni prozor TrueCrypt alata

Nakon odabira ove opcije otvara se novi prozor prikazan na slici Slika 2 u kojem je potrebno odabrati da li će se kreirati standardna Truecrypt particija ili skrivena TrueCrypt particija.



Slika 2: Odabir vrste particije

Nakon odabira vrste particije otvara se prozor (Slika 3) u kojem je potrebno odrediti fizičku lokaciju novokreirane particije. Fizička lokacija može biti datoteka (ova opcija se koristi u slučaju da se želi kriptirati samo dio već postojeće particije) ili neka već postojeća Windows particija.

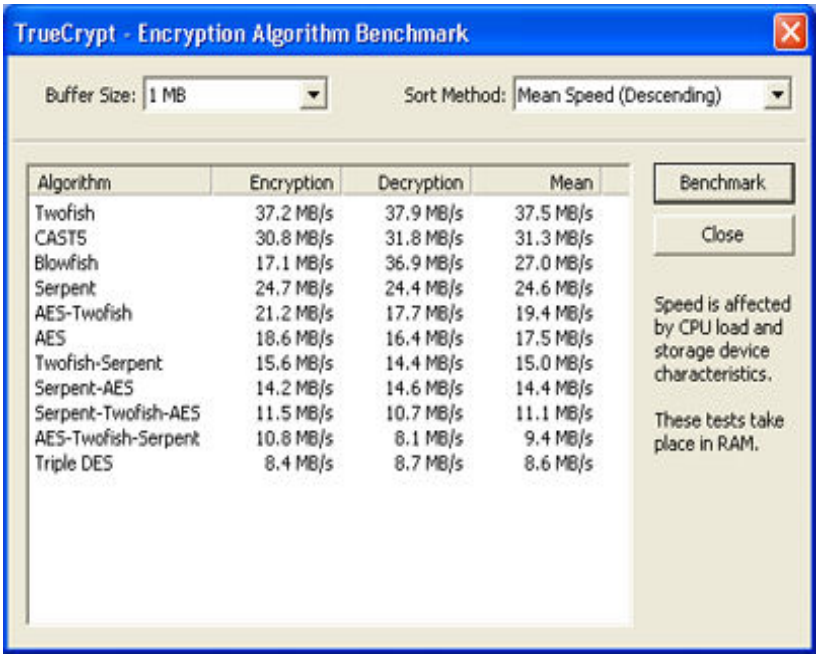


Slika 3: Odabir fizičke lokacije novokreirane particije

Nakon što je odabrana fizička lokacija moguće je podesiti koji će algoritam za kriptiranje i *hash* algoritam biti korišteni za enkripciju nove particije (Slika 4).

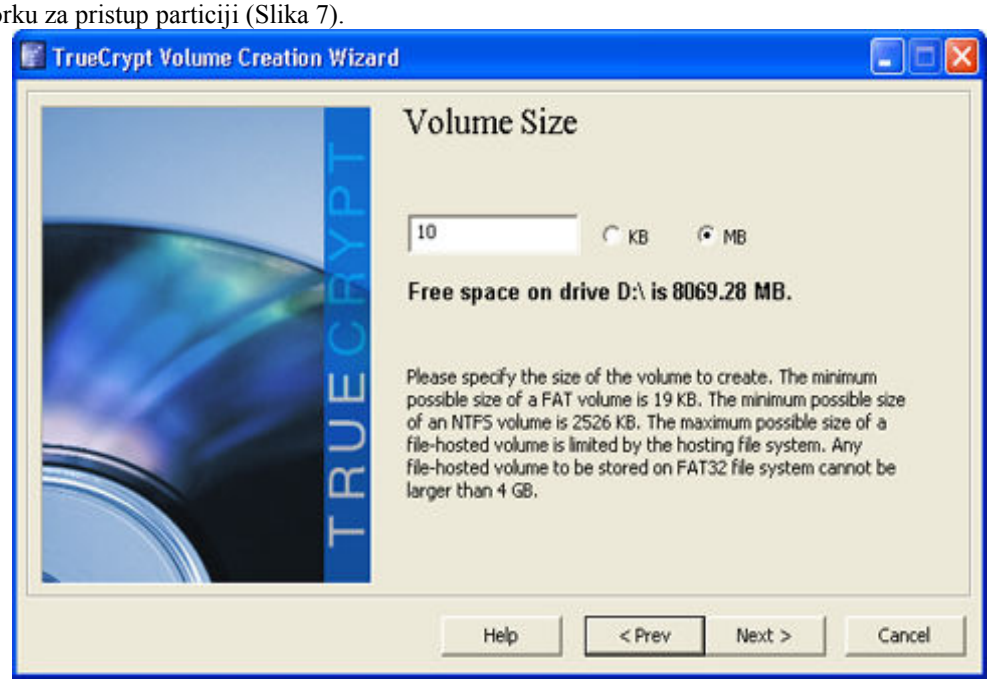
Slika 4: Odabir algoritma za kriptiranje.

Isto tako, odabirom opcije **Benchmark** u ovom prozoru, moguće je dobiti usporedni prikaz performansi pojedinih algoritama za kriptiranje na računalu na kojem je TrueCrypt instaliran (Slika 5).

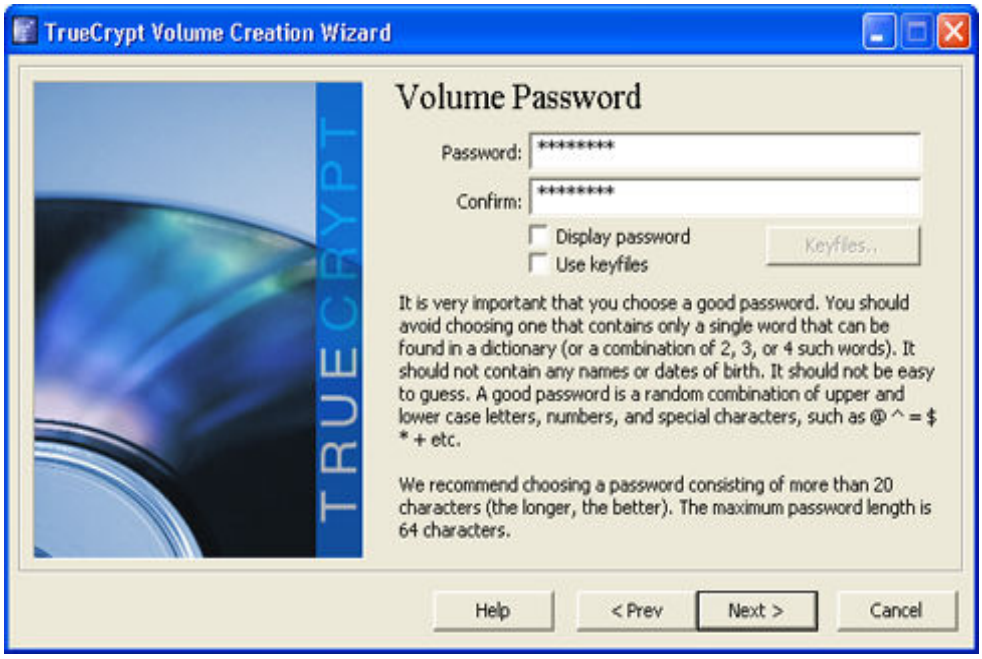


Slika 5: Usporedba performansi pojedinih algoritama za kriptiranje

Nakon odabira algoritma za kriptiranje potrebno je odrediti veličinu nove particije (Slika 6) i odabrati zaporku za pristup particiji (Slika 7).



Slika 6: Odabir veličine particije

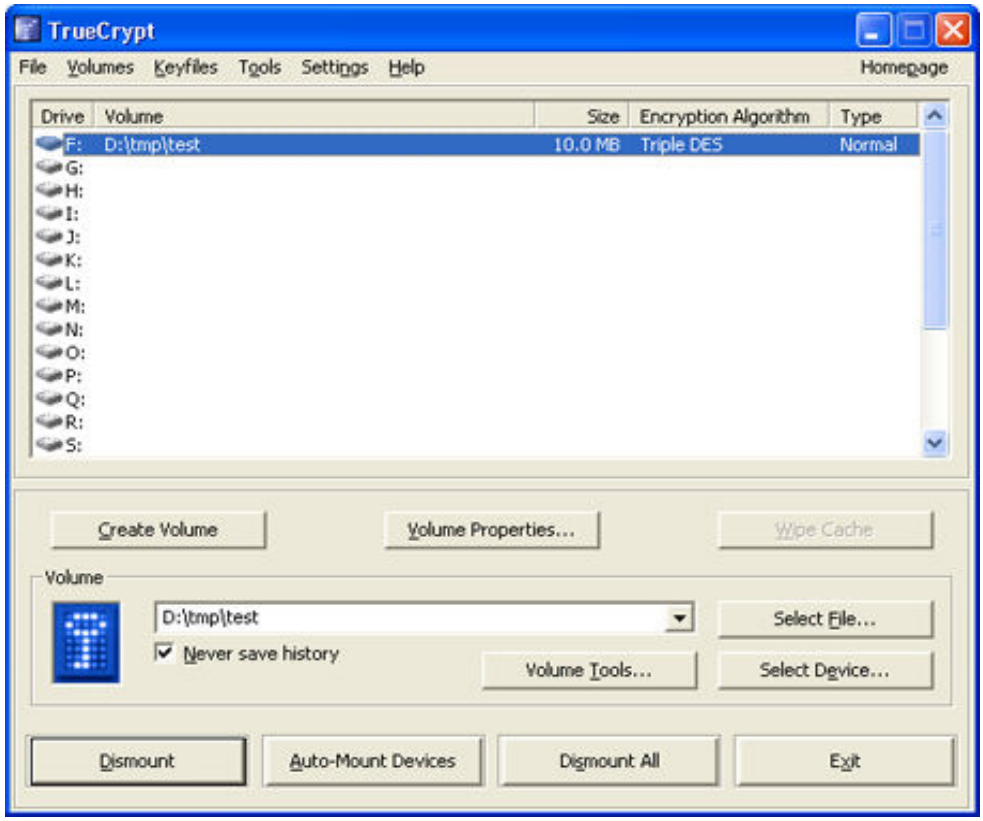


Slika 7: Podešavanje zaporke za pristup particiji

Na kraju je potrebno odabrati vrstu datotečnog sustava (FAT ili NTFS) i pokrenuti formatiranje nove particije (Slika 8).

Slika 8: Odabir datotečnog sustava

Nakon što je nova particija kreirana, potrebno joj je omogućiti pristup. U glavnom prozoru TruCrypt-a potrebno je izabrati slovo pod kojim će se pristupati novoj particiji, datoteku u kojoj je pohranjena novokreirana particija (u slučaju da je kriptirana kompletna Windows particija, potrebno je odabrati tu particiju) i zatim izabrati opciju **Mount**. Iza toga potrebno je unijeti zaporku za pristup odabranoj particiji. Nakon što je unesena ispravna zaporka, TrueCrypt omogućava pristup kriptiranoj particiji (Slika 9).

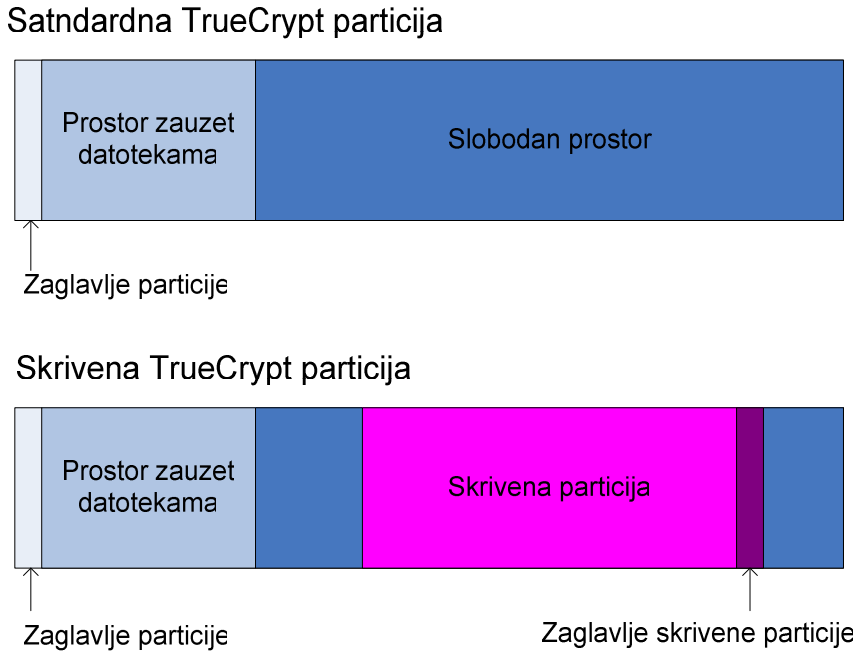


Slika 9: Omogućavanje pristupa kriptiranoj particiji

4. Kreiranje skrivene particije

Skrivena particija može biti kreirana isključivo ako matična particija koristi FAT datotečni sustav. NTFS datotečni sustav pohranjuje podatke po cijeloj particiji, ostavljajući vrlo malo mjesta za stvaranje skrivene particije. Skrivena particija može koristiti bilo koji datotečni sustav (i FAT i NTFS).

Skrivena TrueCrypt particija uvijek se kreira unutar neke već postojeće kriptirane particije (za stvaranje nove particije unutar već postojeće koristi se preostali prazni prostor unutar postojeće kriptirane particije). Budući da u kriptiranoj TrueCrypt particiji i prazni prostor (prostor u particiji u kojem nisu pohranjene stvarne datoteke) sadrži neke slučajne podatke, korisnici koji ne znaju da se tamo nalazi još jedna skrivena particija, ne mogu razlikovati da li se radi o skrivenoj particiji ili samo o slučajnim podatcima matične particije. Ovaj princip prikazan je na slici Slika 10.



Slika 10: Kreiranje skrivene particije

Zaporka pomoću koje se pristupa skrivenoj particiji mora biti drugačija od one pomoću koje se pristupa matičnoj particiji (particija unutar koje se nalazi skrivena particija).

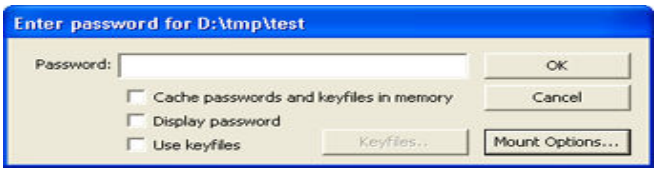
Pristup skrivenoj particiji omogućava se na isti način kao i standardnoj TrueCrypt particiji. U glavnom prozoru TrueCrypt potrebno je odabrati matičnu particiju, ali prilikom unosa zaporke za omogućavanje pristupa particiji potrebno je unijeti zaporku za skrivenu particiju. Naime, TrueCrypt određuje koju će particiju omogućiti na temelju zaporke koja je unesena. Ako je unesena zaporka za pristup matičnoj particiji, TrueCrypt omogućava pristup matičnoj particiji. U slučaju da je unesena zaporka za omogućavanje pristupa skrivenoj particiji, TrueCrypt će omogućiti pristup skrivenoj particiji koja se nalazi unutar selektirane matične particije.

Skrivena TrueCrypt particija kreira se posve jednako kao i standardna TrueCrypt particija. Jedina razlika je u tome što prilikom odabira vrste particije treba odabrati opciju **Create hidden TrueCrypt volume** (Slika 2).

4.1. Zaštita skrivene particije od oštećenja

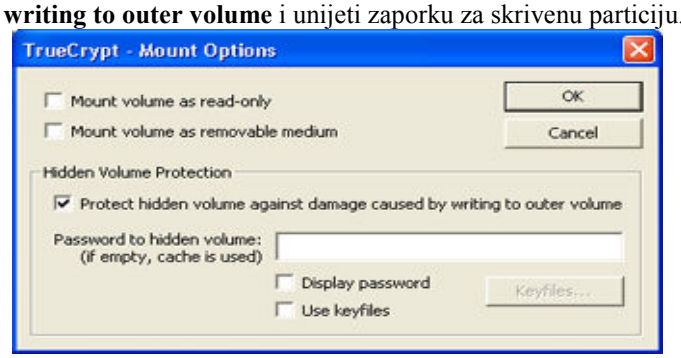
Podaci pohranjeni unutar matične particije se mogu čitati bez ikakvog utjecaja na skrivenu particiju pohranjenu unutar matične. Ali prilikom zapisivanja podataka u matičnu particiju postoji opasnost da se novi podaci prepišu preko dijelova skrivene particije i tako je oštete. Kako bi se izbjegla oštećenja skrivene particije potrebno je primijeniti sljedeću proceduru.

Prilikom omogućavanja pristupa matičnoj particiji potrebno je odabrati opciju **Mount Options** (Slika 11).



Slika 11: Podešavanje opcija prilikom omogućavanja pristupa particiji

U novootvorenom prozoru (Slika 12) potrebno je selektirati opciju **Protect hidden volume against damage caused by writing to outer volume** i unijeti zaporku za skrivenu particiju.



Slika 12: Zaštita od oštećenja skrivene particije

Obje zaporke, i zaporka za matičnu particiju, i zaporka za skrivenu particiju, moraju biti ispravno unesene. U protivnom pristup matičnoj particiji neće biti omogućen.

5. Zaključak

TrueCrypt alat može se koristiti za kriptiranje Windows datotečnih sustava i stoga je pogodan za zaštitu podataka pohranjenih na tvrdom disku od neovlaštenog pristupa. Ovo se posebice odnosi na radne stanice i prijenosna računala.

Alat je jednostavan za korištenje, dobro se integrira u Windows okolinu i vrlo je transparentan za korištenje. Proces kriptiranja i dekriptiranja podataka ne utječe pretjerano na performanse sustava i ne usporava svakodnevni rad korisnika.

Opcija stvaranja skrivenih particija pruža dodatnu razinu sigurnosti pohrane povjerljivih podataka.

6. Reference

[1] TrueCrypt Users Guide,
http://www.truecrypt.org/