# Upute za **Trusted Platform Module (TPM)**

Ove upute namijenjene su **vlasnicima i korisnicima** sustava kao pomoć prilikom omogućavanja i aktiviranja TPM opcija.

**Sadržaj:**

# Upozorenje o mogućem gubitku podataka

**VAŽNO UPOZORENJE KORISNICIMA. PROČITAJTE OVE UPUTE PRIJE INICIJALIZACIJE TPM-a.**

Integratori, vlasnici i krajnji korisnici moraju poduzeti odgovarajuće mjere za izbjegavanje rizika od gubitka podataka.

Podaci enkriptirani bilo kojim programom koji koristi Trusted Platform Module (TPM) mogu postati nedohvatljivi ili nepopravljivi ako se dogodi:

**Gubitak lozinke**: Podaci će postati nedostupni ako se izgubi bilo koja lozinka (password) vezana uz TPM.

**Kvar diska**: U slučaju kvara hard diska ili bilo kojeg medija za pohranu podataka koji sadrži enkriptirane podatke potrebno je vratiti sliku (image) diska ili podatke sa sigurnosne kopije (backup). Korisnik mora redovito raditi sigurnosnu pohranu kopija podataka.

**Kvar računala**: Ako je zbog kvara računala potrebna zamjena matične ploče, prenosivi ključevi se mogu restaurirati. Svi neprenosivi ključevi i podaci vezani uz njih će biti izgubljeni. (Infineon* Security Platform i Wave Systems* EMBASSY* Trust Suitekoriste prenosive ključeve. Provjerite prenosivost ključeva ako koristite neki drugi software uz TPM.

**Gubitak vlasništva nad Trusted Platforme Modulom**: Trusted Platform Module Ownership ili sadržaj mogu se izbrisati (kroz BIOS) da bi se omogućio prijenos vlasništva nad sustavom na novoga vlasnika. Ako se TPM ownership obriše, namjerno ili slučajno, postupkom za povrat je moguće vratiti prenosive ključeve i omogućiti dohvat enkriptiranih podataka.

# Što je Trusted Platform Module (TPM)

Trusted Platform Module je komponenta na matičnoj ploči namijenjena povećanju sigurnosti izvan domašaja današnjih programskih alata, kojom se stvara zaštićeni prostor izvođenja ključnih operacija i zadaća vezanih uz sigurnost. Koristeći i hardware i software, TPM štiti ključeve za enkripciju i sigurnosne potpise u njihovoj najranjivijoj fazi – kad se koriste u otvorenom tekstualnom obliku.
TPM je posebno namijenjen skrivanju neenkriptiranih ključeva i informacija za autentikaciju platforme van dometa malicioznih programa.

# Minimalni sistemski zahtjevi

- Intel® Desktop Board poput D915GMH sa Gigabit Ethernetom, s podrškom za TPM
- Microsoft Windows* 2000 Professional (SP4) ili Microsoft Windows XP Professional (SP1)
- NTFS file system
- Microsoft Internet Explorer* 5.5 ili noviji
- Adobe* Acrobat* 5.0 ili noviji (nalazi se na Intel® Express Installer CD-u)

# Sigurnosne mjere

Sigurnost, kao i svaki drugi aspekt održavanja računala, zahtijeva planiranje. Kod sigurnosti je bitno shvatiti tko su nam „prijatelji" i protivnici. TPM daje mehanizme kojima vlasnik/korisnik štiti svoje informacije. S tim ciljem TPM stavlja „brave" na pristupne puteve do podataka. Kao i kod fizičkih brava, ako izgubite ključeve ono što čuvate će postati nedostupno ne samo lopvima nego i vlasniku/korisniku.

TPM omogućuje rad s dvije klase ključeva: prenosivi (migratable) i neprenosivi (non-migratable). Prenosivi ključevi namijenjeni su zaštiti podataka koji se mogu koristiti (recimo dešifrirati) na više platformi. Prednost je mogućnost spremanja i obnavljanja ključnih podataka na različitim strojevima. Razlozi mogu biti različiti (netko može koristiti više strojeva ili podaci moraju biti dostupni raznim osobama na raynim računalima). Prednost je i mogućnost backupa i povrata ključa nakon kvara. No, ovakvi ključevi mogu biti nedovoljni za predviđeni nivo zaštite (npr. ako korisnik smije raditi samo na određenom stroju). Za to je potreban neprenosivi ključ. Iako se može pohraniti i restaurirati (pa npr. kvar diska nije katastrofalan), ovakvi ključevi su opasni u slučaju kvara platforme, tj. matične ploče. U njihovoj je prirodi nemogućnost korištenja na ma kojoj drugoj platformi, pa podaci koji su njima štićeni postaju nedostupni i neupotrebljivi.

**Sljedeće mjere opreza i postupci mogu pomoći u navedenim situacijama. Ukoliko ih ne primijenite, gubitak podataka je neizbježan.**

## Lozinke

Infineon Security Platform omogućuje korisnicima rad sa lozinkama od 6 do 255 znakova.

Dobra lozinka (password) imat će:

- Barem jedno veliko slovo (A do Z)
- Barem jednu brojku (0 do 9)
- Barem jedan simbol (!, @, &, itd.)

Primjer dobroga: "I wear a Brown hat 2 worK @ least once-a-month" ili "uJGFak&%)adf35a9m"

**Napomena**

Izbjegavajte imena i datume koje je lako pogoditi: rođendani, imena djece, kućnih ljubimaca itd.

Lozinke vezane uz Infineon Security Platform software (Owner, Emergency Recovery Token, User password) i Wave Systems EMBASSY Trust Suite se NE MOGU resetirati ili otkriti bez originala. Korisnik mora dokumentirati lozinke i pohraniti ih na sigurno nakon svake promjene (npr. u sef u zalijepljenoj kuverti), kako bi bile dostupne u slučaju potrebe.

## Emergency Recovery File Back Up

Emergency Recovery Token (**SPEmRecToken.xml**) mora biti spremljen na prenosivi medij (floppy, USB drive, CDR, flash media, itd) koji se čuva na sigurnom mjestu. NE OSTAVLJAJTE KOPIJE Emergency Recovery Tokena na disku ili ma kojem backupu. Ako na sistemu ostane kopija Emergency Recovery Tokena, može se zloupotrijebiti za proboj TPM-a i podataka.

Nakon što upotrijebite Infineon Security Platform User Initialization Wizard, kopiju Emergency Recovery Archive (**SPEmRecArchive.xml**) treba spremiti na prenosivi medij na sigurno mjesto. Postupak treba ponoviti prilikom svake promjene lozinke ili dodavanja novog korisnika.

## Hard Drive Image Backup

Redoviti backup diskova i spremanje ovako dobivenih podataka na sigurno jedini je postupak koji omogućuje oporavak u slučaju kvara diska. Za to je potrebno vratiti podatke na disk, što omogućuje i ponovni pristup enkriptiranim podacima.

**Napomena**

Svi enkriptirani i neenkriptirani podaci koji nastanu nakon zadnjeg pohranjivanja bit će izgubljeni.

## Spremanje otvorenog teksta

Preporučljivo je da se korisnici pridržavaju postupka za Hard Drive Image Backup. Određene datoteke mogu se spremati i bez kreiranja slike diska (drive image), bilo prijenosom sa sigurnih diskova na javne odnosno neenkriptirane diskove ili direktorije, prepisati na prenosivi medij i pohraniti na sigurno. Prednost ovakvog postupka je u tome što za povrat podataka nije potreban TPM ključ. Ipak on nije preporučljiv, jer su podaci izloženi tijekom prijenosa i pohrane, odnosno povrata.

# Trusted Platform Module Ownership

Trusted Platform Module je normalno onemogućen prilikom isporuke računala, pa vlasnik ili krajnji korisnik preuzimaju „vlasništvo" nad njime. Time preuzima postupak inicijalizacije i kreiranja lozinki kojima TPM štiti ključeve i podatke.

Proizvođači/system builderi/integratori mogu instalirati Infineon Security Platform software i Wave System EMBASSY Trust Suite, ali NE SMIJU aktivirati ili koristiti TPM ili ma koji navedeni program.

# Omogućivanje TPM-a

Trusted Platform Module je normalno onemogućen prilikom isporuke računala kako bi se osiguralo da vlasnik/korisnik inicijalizira sustav i konfigurira sve lozinke. Korisnik ili vlasnik moraju za inicijalizaciju TPM-a poduzeti sljedeće:

1. Dok PC prikazuje uvodni ekran (splash screen ili POST screen), stisnuti tipku <F2> za ulaz u BIOS.
2. Strelicama otići na Advanced Menu, odabrati Peripheral Configuration, pa stisnuti tipku <Enter>.
3. Selektirati Trusted Platform Module, stisnuti <Enter>, pa selektirati Enabled i opet stisnuti <Enter> (na ekranu bi trebalo pisati: `Trusted Platform Module [Enabled]`).
4. Stisnuti tipku <F10>, selektirati Ok pa pritisnuti <Enter>.
5. Sistem treba restartati i pokrenuti Microsoft Windows.

# Preuzimanje vlasništva nad TPM-om

Kad je TPM omogućen, potrebno je preuzeti vlasništvo putem Infineon Security Platform Softwarea. Vlasnik/korisnik treba poduzeti slijedeće:

1. Uključiti računalo.
2. Pokrenuti Infineon Security Platform Initialization Wizard.
3. Kreirati Owner password (prije toga pogledati preporuke za lozinke navedene ranije).
4. Kreirati Recovery Archive (zapisati ime i lokaciju datoteke).
5. Specificirati Security Platform Emergency Recovery Token password i lokaciju. (Ova lozinka ne bi trebala biti jednaka kao Owner password ili ma koja druga lozinka).
6. Definirati mjesto za spremanje Emergency Recovery Tokena (zapisati ime i lokaciju datoteke).
7. Software će kreirati datoteke i dovršiti posao vezan za vlasništvo (ownership) nad TPM-om.
8. Po izvršenju Infineon Security Platform Initialization Wizarda, potrebno je Emergency Recovery Token (**SPEmRecToken.xml**) prebaciti na prijenosni medij (floppy, CDR, flash media, itd) ako tijekom instalacije nije spremljen na prijenosni medij. Kad je to obavljeno, medij treba pohraniti na sigurno mjesto. Na sustavu ne bi smjela ostati kopija te Emergency Recovery Token datoteke, jer ju je moguće zloupotrijebiti za proboj sigurnosti stroja.
9. Pokrenuti Infineon Security Platform User Initialization Wizard.

10. Kreirati Basic User password (ova se lozinka najčešće koristi i mora biti različita od svih ostalih).
11. Odabrati i konfigurirati Security Platform karakteristike (features) za korisnika.
12. Po izvršavanju Infineon Security Platform User Initialization Wizarda, kopiju Emergency Recovery Archive (**SPEmRecArchive.xml**) prebaciti na prijenosni medij i pohraniti na sigurno mjesto. Ovo treba ponoviti prilikom svake promjene lozinke ili dodavanja korisnika.
13. Restartati računalo.
14. Za backup ključeva za EMBASSY Trust Suite, potrebno je konfigurirati Key Transfer Manager software. Iz Program menua lansirajte Key Transfer Manager.
15. Slijedite upute programa kako biste kreirali i dokumentirali lokacije datoteka ključa i arhive. Treba ih spremiti na prijenosni medij i pohraniti na sigurno mjesto kad se ne koriste.
16. Kreirajte i dokumentirajte lozinku za zaštitu arhive ključa.
17. Unesite TPM Owner password kako bi Key Transfer Manager mogao kreirati datoteke.
18. Nakon konfiguriranja Key Transfer Managera, na taskbaru će se pojaviti ikonica i automatski će se spremiti svi novi i obnovljeni ključevi vezani za EMBASSY Trust Suite. Ako prilikom generiranja ključeva nije prisutan prijenosni medij sa arhivskom datotekom, trebat će ključeve spremiti putem Key Transfer Managera kad budete imali medij.
19. Sve lozinke za Infineon Security Platform Software (Owner, Emergency Recovery Token, User password) i Wave Systems EMBASSY Trust Suite te Key Transfer Manager ne mogu se resetirati ili otkriti bez originala. Treba ih dokumentirati i pohraniti na sigurno, te osvježavati u slučaju promjena.

# Postupak popravka

## Popravak u slučaju kvara hard diska

Potražite posljednji hard drive image i napravite restore s njega – nema posebnog postupka vezanog za TPM.

## Popravak u slučaju kvara matične ploče ili TPM modula

Ovim postupkom mogu se vratiti samo prenosivi ključevi iz Emergency Recovery Archive, a ne prethodni ključevi ili sadržaj TPM-a. Omogućen je pristup u Infineon Security Platform software i Wave Systems EMBASSY Trust Suite osigurane prenosivim ključevima.

**Potrebno**

- Emergency Recovery Archive (kreirana putem Infineon Security Platform Initiation Wizarda)
- Emergency Recovery Token (kreiran putem Infineon Security Platform Initiation Wizarda)
- Emergency Recovery Token Security Password (kreiran putem Infineon Security Platform Initiation Wizarda)
- Upotrebljiva instalacija originalnog operativnog sustava (OS), ili image hard diska
- Wave Systems Key Transfer Manager archive password
- TPM Ownership password

**Ovim postupkom se restauriraju samo prenosivi ključevi koji su pohranjeni u arhive.**

1. Zamijenite pokvarenu matičnu ploču ispravnom pločom istog modela.
2. Instalirajte operativni sutav ili ga vratite koristeći hard drive image.
3. Pokrenite Infineon Security Platform Initialization Wizard i označite "I want to restore the existing Security Platform" box.
4. Slijedite upute za Security Platform Initialization, pa dodajte Emergency Recovery Archive postojećoj arhivi.
5. Unesite sve potrebne lozinke, datoteke i lokacije. Security Platform Initialization Wizardu može trebati 20-ak minuta da restaura sigurnosna podešenja.
6. Pokrenite User Initialization Wizard. Odaberite "Recover your Basic User Key". Unesite izvorni Basic User Key password i nastavite prema uputama wizarda.
7. Da biste rekonfigurirali Personal Secure Drive, odaberite "I want to change my Personal Secure Drive setting", potvrdite da su točne oznake diska i imena, pa produžite dalje.

8. Restartajte sistem kad se to zatraži.
9. Da biste omogućili pristup u EMBASSY Trust Suite, kliknite desnim uhom miša na Key Transfer Manager ikonu na taskbaru, pa selektirajte Restore TPM Keys.
10. Unesite sve potrebne lozinke, imena i lokacije datoteka koje traži Key Transfer Manager.

Po uspješnom izvršavanju svih koraka, pristup do enkriptiranih datoteka bi vam morao biti moguć.

# Brisanje vlasništva nad Trusted Platform Modulom

**Upozorenje: Isključite kabel napajanja iz mreže (AC power) prije otvaranja kućišta i bilo kakve zamjene komponenti ili matične ploče. Ako to ne učinite, možete ugroziti imovinu i/ili osobe. Dijelovi opreme mogu nastaviti raditi i nakon isključenja stroja ukoliko napajanje nije prekinuto.**

**OPREZ! BRISANJEM VLASNIŠTVA NAD TPM-om ENKRIPTIRANI PODACI POSTAT ĆE NEDOSTUPNI**

Moguće je vratiti pristup podacima koji su enkriptirani prenosivim ključevima prema gore opisanim procedurama.

TPM je moguće obrisati kako bi se vlasništvo nad platformom prenijelo na novog korisnika.

1. Pročitajte gornja upozorenja prije otvaranja kućišta računala.
2. Konfiguracijski kratkospojnik (jumper) na matičnoj ploči prebacite na pinove 2-3.
3. Priključite napajanje na PC i uključite ga.
4. Automatski ćete pokrenuti BIOS setup.
5. Strelicama selektirajte Clear Trusted Platform Module, stisnite <Enter>.
6. Ako prihvaćate upozorenje selektirajte Ok i stisnite <Enter>.
7. Stisnite tipku <F10> za spremanje, selektirajte Ok i stisnite <Enter>.
8. Isključite računalo.
9. Odspojite napajanje.
10. Konfiguracijski kratkospojnik (jumper) na matičnoj ploči vratite na 1-2. Obrisani TPM modul je automatski isključen.

# Dodatne informacije

- Pomoć za Infineon Security Platform Software - http://www.infineon.com
- Pomoć za Wave System EMBASSY Trust Suite - http://www.wave.com/support/ets.html
- Dodatne informacije za TPM i PC security - http://www.trustedcomputinggroup.org/home