SPYRUS®

SPYRUS Soluzione di Protezione Dati Suite B di livello militare...

...per Surface Pro

Data la necessità sempre maggiore di mobilità e sicurezza del dato, gli enti istituzionali e le imprese commerciali richiedono sempre più soluzioni versatili che consentano mobilità e produttività senza sacrificare integrità e sicurezza dei dati. Le persone hanno bisogno di un metodo rapido e facile per proteggere il trasporto e la distribuzione dei documenti, o un ambiente di lavoro totalmente sicuro. Utilizzando il lettore microSD interno di un Surface Pro per inserire SPYRUS Rosetta microSDHC™ come "root of trust" hardwaere, l'utente può operare come al solito, lasciando libera la porta USB per altri dispositivi.

La soluzione consiste nell'applicazione SPYRUS Rosetta® NcryptNshare™ RES Disk™ per la cifratura di volume che permette la creazione di vault cifrati virtuali su dispositivi di memoria come microSDHC, Secure Digital (SD)ccard, flash drive USB, hard drive, SSD, o drive di rete che possono poi venire condivisi con altri utenti autenticati RES Disk. L'hardware security module (HSM) SPYRUS Rosetta viene impiegato per generare e archiviare in modo protetto le chiavi private dell'utente, e per l'autenticazione multifattore e l'accesso condiviso ai vault cifrati RES Disk.

Quando RES Disk viene caricato su un Microsoft Surface Pro 3 o 4 con sistema operativo Windows 10, un dispositivo protetto Rosetta può istantaneamente creare uno spazio di lavoro protetto contenente tutti i software di produttività dell'utente, VPN, e strati di software e hardware encryption. Utilizzare un dispositivo protetto Rosetta con un client VPN richiedente l'autenticazione a due fattori a livello hardware aumenta la sicurezza dei dati senza limitare la produttività.

Rosetta Hardware Security Module (HSM) e Rosetta NcryptNshare RES Disk:

L'applicazione RES Disk consente di creare un vault cifrato (Suite B) per singolo utente o multiutente su un Surface Pro o su un drive di rete utilizzando le funzionalità di sicurezza di Rosetta HSM microSDHC validato FIPS 140-2 Livello 3.

Con le group policy e i permessi di sistema di Microsoft Windows 10, i vault virtuali cifrati di RES Disk possono venire configurati come le sole parti scrivibili sulla macchina host. L'HSM Rosetta è usato come "chiave" per l'autenticazione hardware a RES Disk ed è disponibile in diversi formati che includono Rosetta microSDHC, Smart Card o USB token, P-3X USB 3.0 (storage crittografato) o i live drive WorkSafe Pro Windows To Go.

Configurazione su un tablet Surface Pro Tablet con SO Windows 10:

Se RES Disk viene configurato su un tablet Surface Pro con sistema operativo Windows 10 e la protezione BitLocker per la full drive encryption, l'utente ottiene una versatile e sicura workstation che ha un impatto minimo su usabilità, prestazioni e produttività.

Surface Pro può venire configurato in base alle security group policy in modo che gli utenti accedano solo alle applicazioni preinstallate, ai client VPN ed ai vault virtuali cifrati RES Disk, bloccando tutto il resto del sistema compreso l'hard drive del Surface Pro. Un amministratore può avere privilege di accesso aumentati ed usare un secondo HSM Rosetta per l'autenticazione in modo da provvedere alla manutenzione del sistema operativo e dei contenuti dei vault virtuali cifrati. Dal momento che Rosetta microSDHC comprende sia un PKI HSM che una memoria flash, la card può essere caricata nel lettore microSD interno con un sigillo antimanomissione senza alcun accesso in scrittura alla memoria flash per alcune esigenze istituzionali. Non è necessario che l'utente inserisca alcun altro security token e non c'è bisogno di altri dispositivi esterni di autenticazione.

L'utente finale effettuerà semplicemente il login al suo tablet Surface Pro come di norma. La schermata di login di RES Disk si autocaricherà, l'utente inserirà la sua password RES Disk, autenticandosi per accedere al vault virtuale cifrato RES Disk tramite l'HSM Rosetta. Così facendo, il vault verrà decifrato e diverrà accessibile e modificabile in lettura/scrittura.

SPYRUS®

Configurazione con WorkSafe Pro Windows To Go Live Drive:

WorkSafe Pro USB 3.0 SSD live drive può venire anch'esso configurator con Windows 10 e RES Disk, con il vantaggio supplementare della crittografia hardware Suite B di livello militare. Non è necessario alcun token aggiuntivo in questa configurazione dal momento che WorkSafe Pro ha un HSM Rosetta integrato. Questa configurazione trasforma virtualmente qualunque computer in uno spazio di lavoro protetto semplicemente eseguendo il boot del sistema dell'utente presente sul dispositivo WorkSafe Pro.

Configurazione:

- Installa RES Disk e RES Enterprise Admin Tools nell'immagine base di sistema (senza inizializzare l'HSM Rosetta)
- Crea il dispositivo di sicurezza Rosetta NcryptNshare Recovery Agent (se necessario) che abilita l'Admin all'accesso ai vault di RES Disk nel caso in cui l'HSM Rosetta dell'utente venga smarrito o rubato
- Crea un pacchetto di configurazione (Rosetta configure, RES Disk Virtual Vault creation xml files, RES activation license file, shortcuts personali)
- Carica l'immagine base di Windows su una workstation o un tablet
- Esegui il commando di installazione sileziosa RESWiz, seguito dalla creazione del path di esecuzione per RES Disk encrypted virtual vault
- Setta RES Disk Virtual Vault su Automount e aggiungilo nella lista di esecuzione automatica
- Copia gli shortcuts
- Abilita BitLocker e seta le GPO di sistema
- Quando l'utente finale si autentica in Windows e seta la password RES, ha solo da aggiungere un'ulteriore password da inserire per utilizzare il tablet Windows protetto

Sono possibili servizi di consulenza personalizzata e documentazione su casi d'uso per soddisfare qualunque esigenza.

Specifiche:

PC Windows, dispositivi di sicurezza Rosetta HSM, o WorkSafe Pro

Rosetta MicroSDHC

Rosetta USB

WorkSafe Pro™ for WTG

PocketVault™ P-3X

Microsoft Surface™

Per maggiori informazioni sui prodotti SPYRUS, visita il sito www.digitree.it/spyrus, o contattaci per email o telesono.

Microsoft Partner
Gold OEM Hardware
Silver Independent Software Vendor (ISV)

SUITE B ON BOARD

Distribuito da:

DigiTree
via di Romagna 9/1
34134 Trieste (Italy)
+393668948545
sales@digiree.it