

# Rosetta<sup>®</sup> NcryptNshare<sup>™</sup> (RES Pro)

Con la sicurezza di Rosetta<sup>®</sup> FIPS 140-2 Livello 3

Crittografia e Condivisione sicure dei File per Windows su PC, Tablets e Drive Windows ToGo

## I tuoi File sono Sicuri nel Cloud, le Chiavi Crittografiche stanno con te

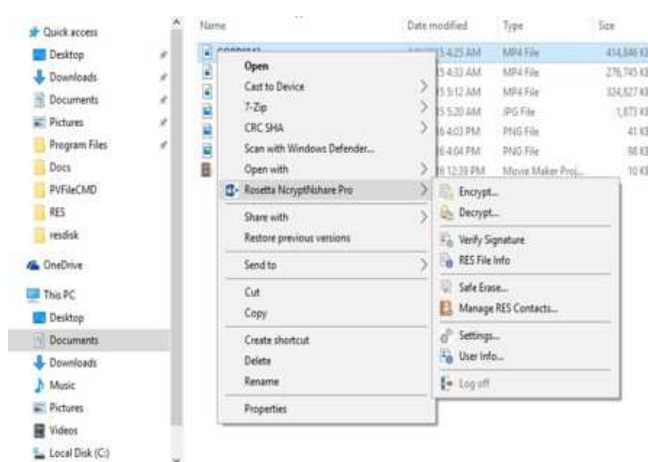
Rosetta NcryptNshare Pro (RES Pro) è un'applicazione che crittografa sia file singoli che folder e permette di condividere la capacità di decifratura con altri collaboratori fidati.

I file e i folder cifrati possono essere inviati in modo sicuro come allegati email o archiviati su dischi esterni, server e persino in cloud.

I file vengono cifrati con chiavi generate ed archiviate in un dispositivo a crittografia hardware di SPYRUS come una smart card o un'USB readerless Rosetta, PocketVault P-3X, WorkSafe, WorkSafe Pro, o la microSDHC Rosetta.

Puoi condividere i file cifrati con altri utenti di RES Pro utilizzando il software per creare e scambiare file e firmare certificati per creare una lista di Contatti RES Pro. Puoi inserire qualunque dei tuoi contatti RES Pro in una lista di condivisione quando effettui la cifratura di un file, e quei contatti possono decifrare quell file sul loro computer con RES Pro. Puoi anche decifrare i file che vengono condivisi con te dai tuoi contatti RES Pro.

RES Pro è compatibile con molte versioni di Windows, inclusi Windows 7, 8.1 e 10 su desktop, laptop, tablet o i drives Windows To Go di SPYRUS Work-Safe/WorkSafe Pro.



## Caratteristiche e Benefici

- RES Pro supporta la caratteristica Rosetta Recovery Agent per mantenere la continuità di decifratura se il tuo dispositivo crittografico viene perso o rubato.
- Tutte le funzioni di gestione delle chiavi e di sicurezza critica sono implementate nell'hardware security module (HSM) Rosetta SPYCOS, certificato FIPS 140-2 Livello 3.
- Cifra e condividi tutti i tipi di file.
- Le funzionalità di Rosetta PKI HSM permettono di generare coppie di chiavi, archiviare certificati digitali, apporre una firma digitale e cifrare le email, ed abilitare alla strong authentication.
- I file protetti con RES Pro possono essere archiviati in cloud collaborativo per aggiungere uno strato aggiuntivo di protezione dei dati mantenendo le chiavi nelle mani dei loro proprietari.

# Specifiche Tecniche

## Compatibilità con Sistemi Operativi

Windows 10

Windows 8.1

## Sicurezza e Standard di Crittografia

- Rosetta SPYRUS Cryptographic Operating System (SPYCOS®)
- FIPS PUB 186-4 Digital Signature Standard (ECDSA P-384)
- FIPS PUB 197 Advanced Encryption Standard (AES 256-bit)
- SP 800-38A Block Modes of Operation (AES 256-bit CBC)
- SP 800-56A Key Establishment Schemes (EC-DH P-384 and KDF)
- SP800-90A. Rev.1 Deterministic Random Bit Generator (HASH\_DRBG)
- FIPS 140-2 Level 3 / CC EAL 5+ validated crypto core
- Key Agreement / Establishment: CVL (ECC CDH), KAS, KTS
- FIPS 180-4 Secure Hash Standard (SHA-384)
- Altri algoritmi approvati FIPS sono disponibili sui dispositivi Rosetta (vedi le specifiche tecniche dei dispositivi per maggiori dettagli)

## Rosetta Hardware Security Modules



Rosetta micro SDHC



Rosetta Smart Card and Rosetta USB



Dispositivi di archiviazione criptata USB 3.0 PocketValut Smart USB 3.0 e P-3X e drive Windows To Go WorkSafe/WorkSafe Pro integrano al loro interno un HSM Rosetta PKI-



Per maggiori informazioni sui prodotti SPYRUS, visita [www.digitree.it](http://www.digitree.it), oppure contattaci per email o telefono.

Corporate Headquarters  
1860 Hartog Drive  
San Jose, CA 95131-2203  
+1 (408) 392-9131 phone  
+1 (408) 392-0319 fax  
info@SPYRUS.com

East Coast Office  
+1 (732) 329-6006 phone  
+1 (732) 832-0123 fax

UK Office  
+44 (0) 113 8800494

Italian Reseller:  
DigiTree  
34134 Trieste, Italy  
via di Romagna 9/1  
m: +39 366 89 48545  
e: sales@digitree.it  
www.digitree.it