



CRYPTONOX MULTIPPOINT CRYPT



Novinka v zabezpečení dôverných informácií

Unavuje Vás množstvo softwarových aplikácií, komplikované IT riešenia, odkázanosť na pomoc externých IT špecialistov a príliš drahé systémy ochrany Vašich informácií v počítačoch? Pracujete s informáciami, ktoré musia byť zabezpečené? Potrebujete riešenie pre bezpečný prenos informácií s inými subjektami?

Práve pre Vás je tu doposiaľ technicky a ekonomicky najvýhodnejší spôsob ochrany informácií

produktová rada MULTIPPOINT Crypt.

V čom je MULTIPPOINT Crypt iný?

Používa kombináciu 3 technologických ochranných prvkov:

- Software – ochrana všetkých druhov súborov pomocou silného kryptovacieho algoritmu.
- Hardware – kryptovanie a dekryptovanie súborov je možné výhradne za prítomnosti HW kľúča (v prevedení USB). Toto hardwarové zariadenie nevyžaduje inštaláciu žiadneho špeciálneho ovládača.
- Heslo – Pre prístup k zabezpečeným súborom je nutné zadať heslo, ktoré si užívateľ môže kedykoľvek zmeniť. Toto heslo sa vygeneruje automaticky po zadaní zdrojového reťazca (max. 64 znakov), ktoré si užívateľ zvolí sám.

Pre koho je MULTIPPOINT Crypt určený?

Pre jednotlivcov, uzavreté skupiny, ale aj ako prostriedok pre chránenú komunikáciu medzi viacerými skupinami, ktoré:

- požadujú moderné bezpečnostné riešenia
- požadujú individuálny prístup
- nemajú dôveru v programoch „masového šírenia“
- nemajú dôveru v technológiách akejkoľvek formy „zdieľaných kľúčov“





Prečo používať MULTIPOINT Crypt:

- jednoduchá implementácia do Vášho bezpečnostného režimu
- možnosť výberu algoritmu kryptovania 3-DES 168 alebo AES 256
- jednoduchá práca so súborom, súborami alebo priečkami
- využitie pre prácu jedného užívateľa, uzavretej skupiny alebo viacerých uzavretých skupín
- využitie pre prácu na lokálnom, ale aj vzdialenom (zdieľanom) úložisku
- vytvorenie unikátneho hesla na základe užívateľom zadaného reťazca
- tri prvky bezpečnosti (software, hardware, heslo)
- jedinečný pracovný režim – safety mode
- individuálne riešenia na mieru
- každá licencia je unikátna – SW sa prispôbuje požiadavkám klienta
- bez obmedzeného počtu inštaláčnych miest (možnosť nainštalovať SW na PC v práci, doma, laptop)

Ako to funguje?

Nainštalujete softvér do počítača. Heslo je už od výroby jedinečné, ale v prípade potreby si ho môžete kedykoľvek zmeniť.

Vytvoríte súbor, ktorého obsah chcete chrániť.

Spustíte program MULTIPOINT Crypt a autorizujete sa Vaším jedinečným HW kľúčom.

Zvolíte súbor, ktorý chcete chrániť, potvrdíte úlohu heslom a Vaše informácie sú chránené (prípona súboru sa nemení).

Prístup k zakryptovaným súborom/dátam má len ten užívateľ, ktorý vlastní jedinečný HW kľúč a pozná heslo - teda VY!

Súbory sa nenachádzajú na HW USB kľúči, ale sú uložené vo Vašom PC resp. vzdialenom úložisku v zakryptovanej forme.

Ak využívate skupinovú licenciu

Vďaka MULTIPOINT Crypt môžete komunikovať aj s inými subjektmi.

Pre prácu v skupine sa upravuje SW na konkrétne množstvo užívateľov v kombinácii s konkrétnymi unikátnymi HW kľúčmi.

Jednoducho pošlete chránený súbor emailom členovi Vašej skupiny alebo chránený súbor uložíte na vzdialené úložisko.

Pri tejto forme komunikácie neposielate šifru, kľúč a ani nápovedu hesla alebo formy kryptovania.

Jedine člen Vašej skupiny, ktorý má unikátnu licenciu SW, jedinečný HW kľúč a heslo má prístupové právo k informáciám.

NOT LEAVE TRACES IN THE COMPUTER



Spojenie software + HW kľúč + heslo znamená že každý produkt MULTIPOINT Crypt je unikátny a pre prácu s produktom sú všetky prvky ochrany vzájomne závislé. V praxi to znamená že užívateľ musí vlastniť správnu licenciu software, konkrétny HW kľúč so správnym „seed code“ a musí poznať užívateľské heslo.

Pri vývoji produktu sa k jedinečnej licenci software priradzuje jedinečný HW kľúč pričom software predstavuje len užívateľské rozhranie. Samotné kryptovanie je vykonané na základe pokynov z HW kľúča. Týmto krokom je eliminovaný nežiaduci prvok – a to stopa v PC s informáciami o forme a sile kryptovania ktorú zanechávajú štandardné produkty.

Výrazným prvkom ochrany je užívateľom volený „seed code“ na základe ktorého je vypočítané heslo, pričom sa „seed code“ v zakryptovanej forme uschová v HW kľúči a slúži ako ochrana proti klonovaniu tohto HW kľúča.



Produkty rady MULTIPOINT Crypt je možné využívať :

- * individuálne
- * v uzavretej skupine užívateľov
- * medzi viacerými uzavretými skupinami užívateľov

A to

- lokálne - zabezpečením citlivých informácií na pracovisku
- vzdialene - prácou so zabezpečenými citlivými informáciami zo vzdialeného úložiska (užívateľ nechce mať uložené citlivé informácie vo svojom PC)

Modelové príklady:



Pri vývoji bol kladený dôraz na to aby samotná práca s produktmi MULTIPOINT Crypt bola užívateľsky veľmi jednoduchá a dala sa obšíchnúť do niekoľkých krochov:

- 1, vytvorenie súboru s chránenými informáciami
- 2, spustenie programu MULTIPOINT Crypt (len za prítomnosti HW kľúča)
- 3, výber súboru ktorý užívateľ potrebuje chrániť
- 4, zvolenie úkonu zašifrovať a potvrdenie tohto úkonu užívateľským heslom
- 5, súbor je chránený a uložený v užívateľovom PC



Ale ak má užívateľ zakúpený produkt MULTIPOINT Crypt v „skupinovom“ prevedení tak chránený súbor môže poslať členovi jeho skupiny ktorý:

- 3, spustením programu MULTIPOINT Crypt (len za prítomnosti HW kľúča)
- 2, výberom šifrovaného súboru ktorý užívateľ prijal od člena jeho skupiny
- 1, zvolením úkonu „dešifrovať“ a potvrdením tohto úkonu užívateľským heslom

Získa prístup k jemu určeným informáciám.

Pre koho je MULTIPOINT Crypt určený?

Pre jednotlivcov, uzavreté skupiny, ale aj ako prostriedok pre chránenú komunikáciu medzi viacerými skupinami.

Napríklad advokátske kancelárie - komunikácia v rámci spoločnosti, zabezpečená komunikácia firma - klient. Klient môže komunikovať so svojim advokátom z ktoréhokoľvek miesta na svete. Advokát obdrží 2 licencie produktu CRYPTONOX MULTIPOINT Crypt (2xDVD box s CD a HW kľúčom) ktoré sú nastavené do režimu uzavretej skupiny 2 užívateľov. V PC je pre každého klienta inštalovaný unikátny software v kombinácii s unikátnym HW kľúčom. Ak klient pošle kryptovaný dokument tak ho oprávnená osoba dešifruje a odovzdá nadriadenej osobe.

Exekútorské, Notárske úrady, spoločnosti s pridanou hodnotou -výskum, vývoj – komunikácia v rámci spoločnosti, zabezpečená komunikácia firma - klient.

Všetky formy elektronickej archivácie údajov a dát. Ochrana osobných údajov.

Všetky spoločnosti ktoré kladú dôraz na vysoký bezpečnostný štandard pri komunikácii

- zabezpečená komunikácia firma - klient
- komunikácia v rámci spoločnosti - interne medzi exekutívou



pre užívateľa



pre užívateľov



pre skupiny



Výhody produktu MULTIPOINT Crypt:

- + dáta sú uložené a kryptované pomocou hardwarového kľúča v počítači (nie sú uložené na kľúči)
- + bezpečnostné ukončenie práce odpojením HW kľúča
- + možnosť pracovať v uzavretej skupine, ale aj medzi viacerými skupinami
- + bez možnosti "klonovania" HW kľúča

Technická špecifikácia:

Typ kryptovania: **256-bit AES (Advanced Encryption Standard)**
168-bit 3-DES (Triple-DES)

Ochrana: podmienené prítomnosťou hardwarového kľúča

HW kľúč: prostriedok globálne unikátnej HID bez potreby inštalácie driverov.

Typ HW kľúča: Model USB s rozhraním USB 2.0 (späťne kompatibilný).

Ochrana: jedinečný HW modul chránený HW adresou, heslom a seed kódom.

Heslo: Heslo je generované z užívateľom zadaného 64 bytového reťazca (seed code)

SW prostredie: jednoduché užívateľské rozhranie a „no-ADMIN-needed“ inštalácia

Operačný systém: Podpora Windows XP a vyšší



Kontakt: