MXI SECURITY

MXI řešení nabízí tyto výhody

MXI SECURITY

Přenositelnost

“Zero-Footprint” technologie

- Nezanechává žádnou stopu (klíče nebo software) v zařízeních, na kterých je používáno, což je důležité z bezpečnostních důvodů a dovoluje to použití na zařízeních mimo vlastní organizaci.
- Je plně funkční v prostředí OS Windows, Mac, Linux a Unix.
- Na hostitelský systém nemusí být instalován žádný software.

Nevyžaduje udělování žádných zvláštních lokálních administrativních oprávnění

- Mnoho organizací zamezuje instalaci software nebo ovladačů na jejich zařízeních.
- Někteří prodejci požadují aby jejich administrativní programy nebo ovladače byly nainstalovány na hostitelská zařízení. Pouze uživatelé s administrativními právy mohou nainstalovat produkty, které způsobí to, že hostitelská zařízení mnohdy přestanou fungovat.

Bezpečnost

FIPS 140-2 Level 2 bezpečnostní ověřování

- Ověřuje úroveň zabezpečení zařízení nezávislou soustavou.

AES 256-bit hardware šifrování

- Šifrování je vykonáváno v hardware a to znamená, že šifrovací klíče nikdy neopustí zařízení.
- **Až tří faktorová úroveň autentizace**
- Nestačí pouze znát heslo, musíte mít i zařízení a být (biometricky) správná osoba pro uskutečnění úspěšné autentizace.

Firemní postup-doplňuje silnou autentizaci

- Síla hesla a úroveň biometrického zabezpečení může být centrálně zesílena a to poskytuje ještě vyšší úroveň bezpečnosti.

MXI SECURITY

Univerzálnost

MXI produkty nabízejí koexistenci rozmanitých technologií v jednom zařízení a představují tak vysoce funkční celek, který může nahradit rozmanitá existující řešení a zvýšit tak úroveň bezpečnosti a přenositelnosti.

- **Ochrana dat**
  - Šifrování hesla, FDE, šifrování souboru
- **Silná autentizace**
  - Certifikace, RSA, SSO
- **Bezpečná vzdálený přístup**
  - VPN, Citrix
- **Virtualizace**
  - Citrix, VM Ware, MojoPac, RDP

Povolení & regulace

Chrání důvěrná data a intelektuální vlastnictví

- Finanční informace, čísla kreditních karet, evidenční čísla pro sociální zabezpečení, adresy, patenty, zdrojové kódy, návrhy, vzorce.

Shoda s předpisy a nařízeními

- ochraňuje Váš majetek a značku, udržuje v bezpečí Vaše zákazníky a přináší tak srovnatelné výhody.

Ochraňuje dobré jméno

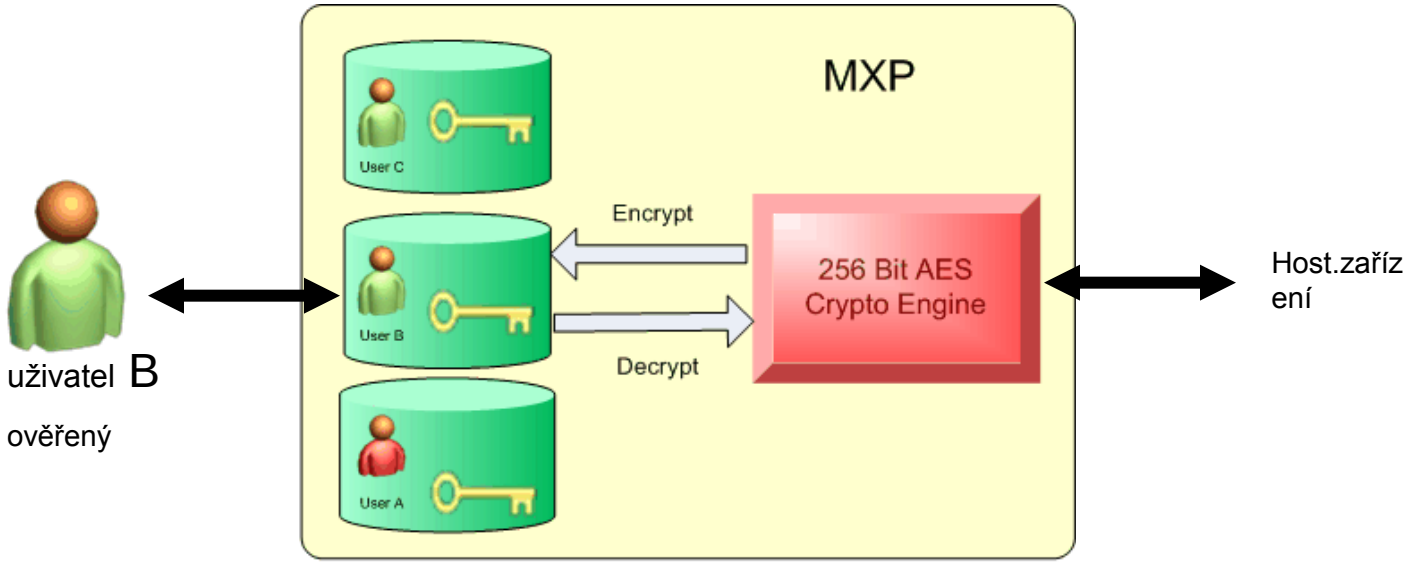
- Nikdy se nemusíte obávat zveřejnění v novinách či televizi v případě, že by se Vaše data dostala do nepovolaných rokou.

MXI SECURITY

Přehled produktové řady MXI

Charakteristika MXI Storage

- Zašifrované přenosné zařízení pro uložení dat
  - Podle uživatelů (až do 5)
  - AES 256 bit šifrování v hardware
  - Dokonale transparentní a přenositelný



MXI – Software řešení

- **ACCESS 7.x - jednotlivý**
  - Správa jednotlivého zařízení

- **ACCESS Enterprise 3.*x* - Manager**
  - Centrálně administrovaná podniková správa zařízení

MXI SECURITY

Centralizovaná správa

Centrální firemní politika a pověřená správa

– Uživatelé nemají žádný vliv na bezpečnostní postupy. Tyto jsou centrálně určovány a řízeny administrátory (správci zodpovědnými za bezpečnost systémů). To zajišťuje dodržování pravidel a nízkou úroveň nákladů na pořízení a provoz.

Nastavení nového hesla, i vzdáleným přístupem

– Umožňuje uživateli přístup k uloženým datům v případě zapomenutí hesla nebo i v případě, že uživatel není schopen provést biometrickou autentizaci.

MXI SECURITY

Centralizovaná správa –pokračování 1

Široká škála nastavení vlastním uživatelem

- Firemní politika je „naložena“ do zařízení a uživatel si může sám nastavit hesla a nespravované otisky prstů bez nutnosti absolvování nějakého speciálního zaškolení. To také zabezpečuje dodržování pravidel a nízké náklady na provoz.

Vymezené aplikace pro přenos na zařízeních uživatelů

- Dodatečná bezpečnostní řešení pro přenos dat jako jsou vzdálený přístup (Citrix, Ringcube, VPN) mohou být stanovena, nakonfigurována a přenášena na zařízení, čímž získají uživatelé neomezený přístup odkudkoliv do firemního prostředí.

Centralizovaná správa –pokračování 2

Kontrolní stopa pro potřeby správy

- Všechny úkoly definované pro zařízení jsou plně kontrolovatelné.

Autodestrukce nebo uzamknutí zařízení při selhání několikanásobné autentizace

- Tímto způsobem jsou data ,které chce hacker získat, navždy ztracena, tudíž i bezpečná.
- Administrátor může znovu získat data ze zařízení v případech, kdy uživatel není ochoten se autentizovat nebo odešel z firmy.

Generování klíčů a oprávnění přímo na hardware

- Šifrofací klíče nikdy neopustí zařízení a tím pádem nemohou být získány ani zkopírovány. Na zařízení mohou být uloženy i další šifrovací klíče a/nebo (PKI) certifikáty a o umožňuje jeho použití pro množství autentizačních funkcí.

MXI SECURITY

Přednosti MXI

- Transparent ní šifrování přenositelných dat
- Hardware ochrana digitálních ověření
- Silná autentizace v rozmanitých systémech
- Jednotné a jednoduché připojení uživatelů
- Nevyžaduje si software stopu
- Centrální správa zařízení
- Konvergence aplikace
- Shoda & pravidla