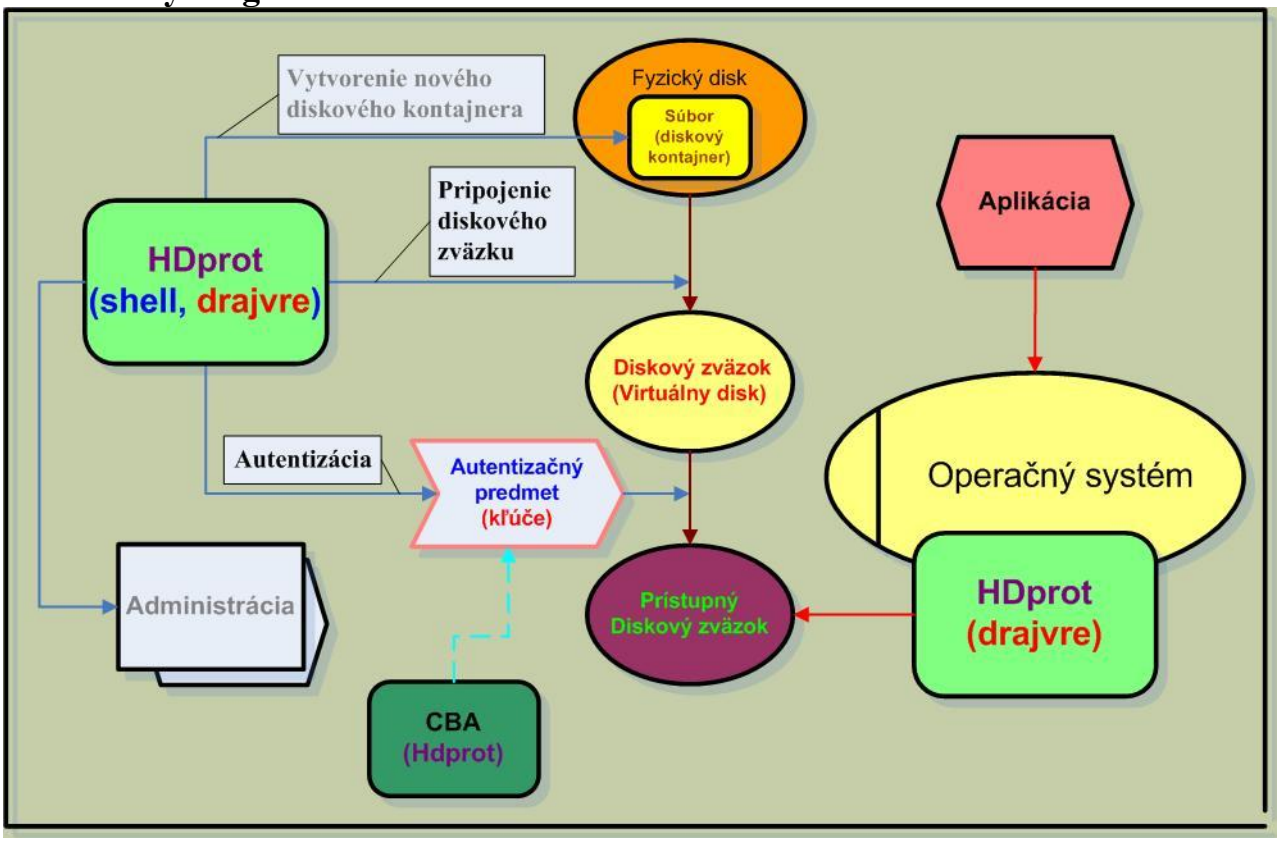
HDprot - chránený diskový systém

Základná charakteristika

- Ide o **systém ochrany údajov** uložených **na pevných diskoch šifrovaním**. Šifrovanie je vykonávané úplne transparentne online spôsobom.
- Šifrujú sa údaje ukladané súborovým systémom do **diskových kontajnerov**, pripojených ako **virtuálne diskové zväzky**.
- **Prístup na disky** je umožnený ***len oprávneným osobám*** po ***úspešnej autentizácii a vložení správneho šifrovacieho kľúča***, ktorý je umiestnený na čipovej karte alebo USB tokene.
- **Diskový kontajner** sa javí ako **šifrovaný súbor**, ktorý je ***ľubovoľne premiestniteľný***.

Blokový diagram



Diskové kontajnery

- sú reprezentované diskovými súbormi na HD alebo na iných externých diskových zariadeniach (prípona .DCO), a sú voliteľne chránené pred vymazaním,
- vytvárané:
  - dynamicky v administrátorskom režime,
  - nakopírovaním súboru reprezentujúceho už skôr vytvorený kontajner,
- počet je neobmedzený,
- veľkosť je limitovaná len veľkosťou fyzického disku (keď sú použité bezpečnostné nastavenia operačného systému nie je vhodné vytvárať väčšie kontajnery ako 1 Gbajt, čo je maximálna veľkosť údajov pre šifrovanie jedným šifrovacím kľúčom podľa bezpečnostného štandardu),

- typ súborového systému môže byť FAT12, FAT16, FAT32 alebo NTFS (nezávisle od typu súborového systému hostiteľského disku),
- parametre šifrovania:
  - algoritmus SEA-64A s dĺžkou kľúča 256 bitov (pre každý kontajner môže byť iný kľúč),
  - kľúč je uchovávaný mimo PC (čipové karty, USB tokeny – prístupné po zadaní PIN-u),
  - šifruje sa každý sektor virtuálneho disku zvlášť s dynamickou zmenou inicializačného vektora,
  - šifrujú sa kompletne celé virtuálne disky aj so systémovými oblasťami
  - šifruje sa online - ovládačom zakomponovaným do jadra operačného systému.

Virtuálne disky (diskové zväzky)

- vytvárajú sa dynamicky pomocou pripájania kontajnerových súborov a tvorby nových diskových zariadení,
- ich pripájanie alebo odpájanie ako aj autentizovanie alebo deautentizovanie sa k pripojeným diskom je umožnené za behu operačného systému,
- počet pripojených virtuálnych diskových zariadení je obmedzený len systémovými prostriedkami počítača,
- sú sprístupnené až po úspešnej autentizácii (zadaní PIN-u ku kľúčovému médiu a načítaní kľúča),
- jeden je možné predvoliť ako tzv. systémom automontovateľný:
  - po štarte systému je v zložke *„Tento počítač“* viditeľná jeho ikona,
  - je prístupný až po úspešnej autentizácii,
  - nie je odpojiteľný používateľom, odpája ho systém pri vypínaní PC,
- pripojené a autentizované zostávajú v činnosti aj po ukončení shellu,
- dajú sa zdieľať (nastavením v operačnom systéme).

Základné požiadavky

- **požiadavky na HW PC:**
  - CPU Intel Pentium a kompatibilný,
  - Minimálne 64 MB RAM,
  - aspoň 10 MB volného miesta na disku,
  - CD ROM mechanika pre inštaláciu z CD ROM prípadne USB port pre inštaláciu z Intelligent Stick média.
- **požiadavky na operačný systém:**
  - všetky typu NT (Windows2000 a Windows XP až Windows 11),

Práca a ovládanie

- **režimy práce shell-u:**
  - administrátorský (v konte s administrátorskými právami v OS):
    - vytváranie diskových kontajnerov,
    - administrácia,
  - užívateľský (tieto funkcie sú prístupné aj v administrátorskom režime):
    - pripojenie a odpojenie diskového zväzku,
    - autentizácia a odhlásenie (deautentizácia),
    - diskové informácie,
- ovládanie cez ikonu na systémovej lište a kontextové menu (shell),
- činnosti a udalosti sú zaznamenávané do denníka udalostí (auditu).

Výhody systému HDprot

- dynamické vytváranie virtuálnych diskov (neobmedzený počet, veľkosť),
- úplne transparentná práca s takýmto diskom (nezaťažuje to používateľa),
- jednoduchá používateľská obsluha,
- bezproblémová prenositeľnosť (kopírovanie) diskových kontajnerov,
- bezpečná ochrana uložených dát v PC aj pri ich prenose po sieti (príloha e-mailu a pod.),
- šifrovací kľúč je uložený mimo PC a jeho zavedenie vyžaduje autentizáciu PIN-om ku kľúčovému médiu,
- systém má bezpečnostný certifikát NBÚ SR ako prostriedok šifrovej ochrany informácií stupňa „V“,
- systém umožňuje (vyžaduje) administráciu, čiže vnáša ďalší prvok bezpečnosti do správy dát,
- v organizácii kde sa používa umožňuje zaviesť riadenú distribúciu a uloženie citlivých dát.

„Nevýhody“ systému HDprot

- potreba CBA (Centrálna bezpečnostná autorita), kde sa plnia kľúčové médiá,
- potreba zásahu administrátora, pri vytváraní šifrovaných diskových kontajnerov,
- potreba kľúčového média u používateľa a zapamätanie si PIN-u k nemu,
- potrebná administrácia systému.