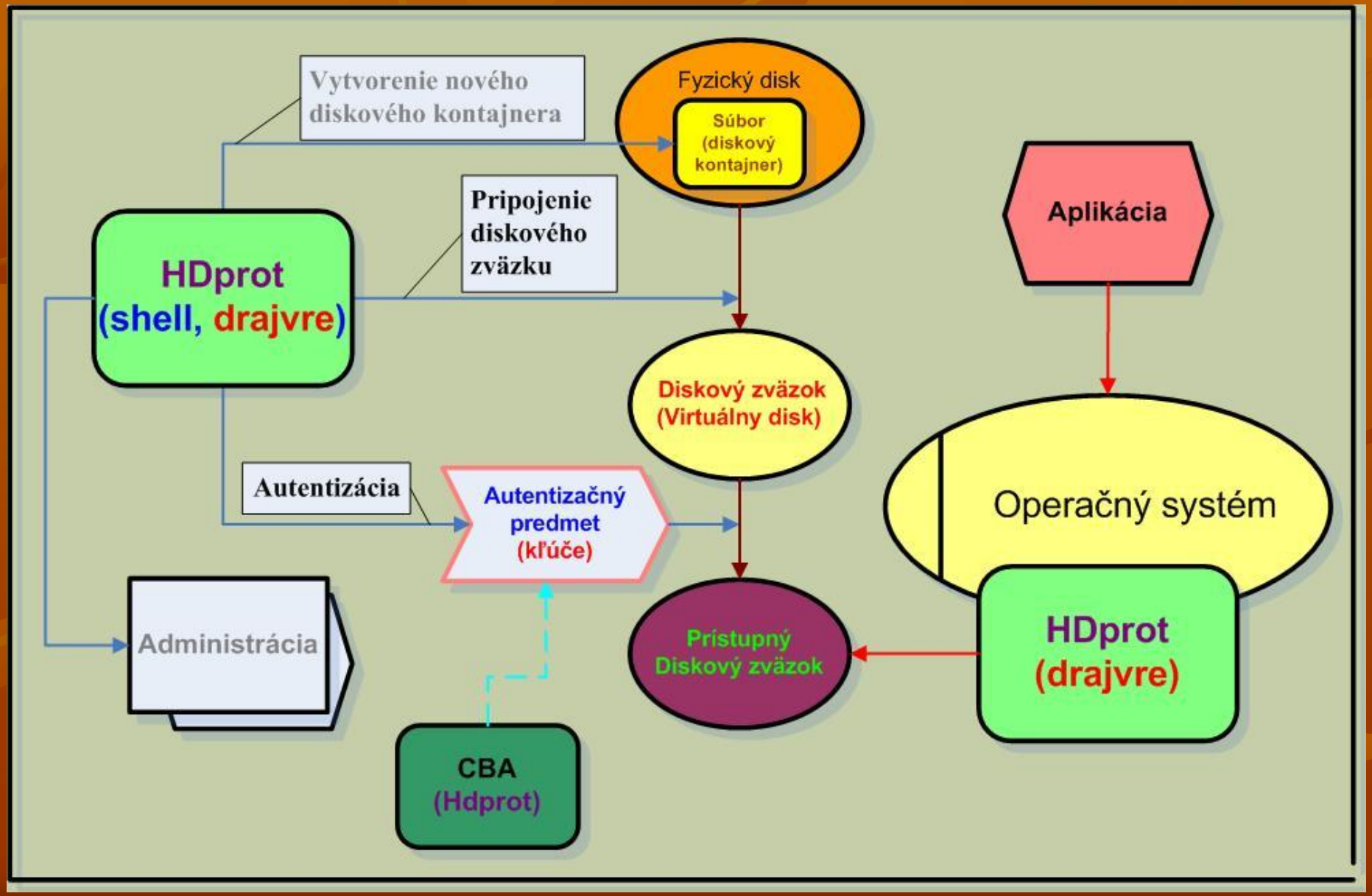
HDprot

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



Práca systému HDprot

- **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),
- **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).

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).

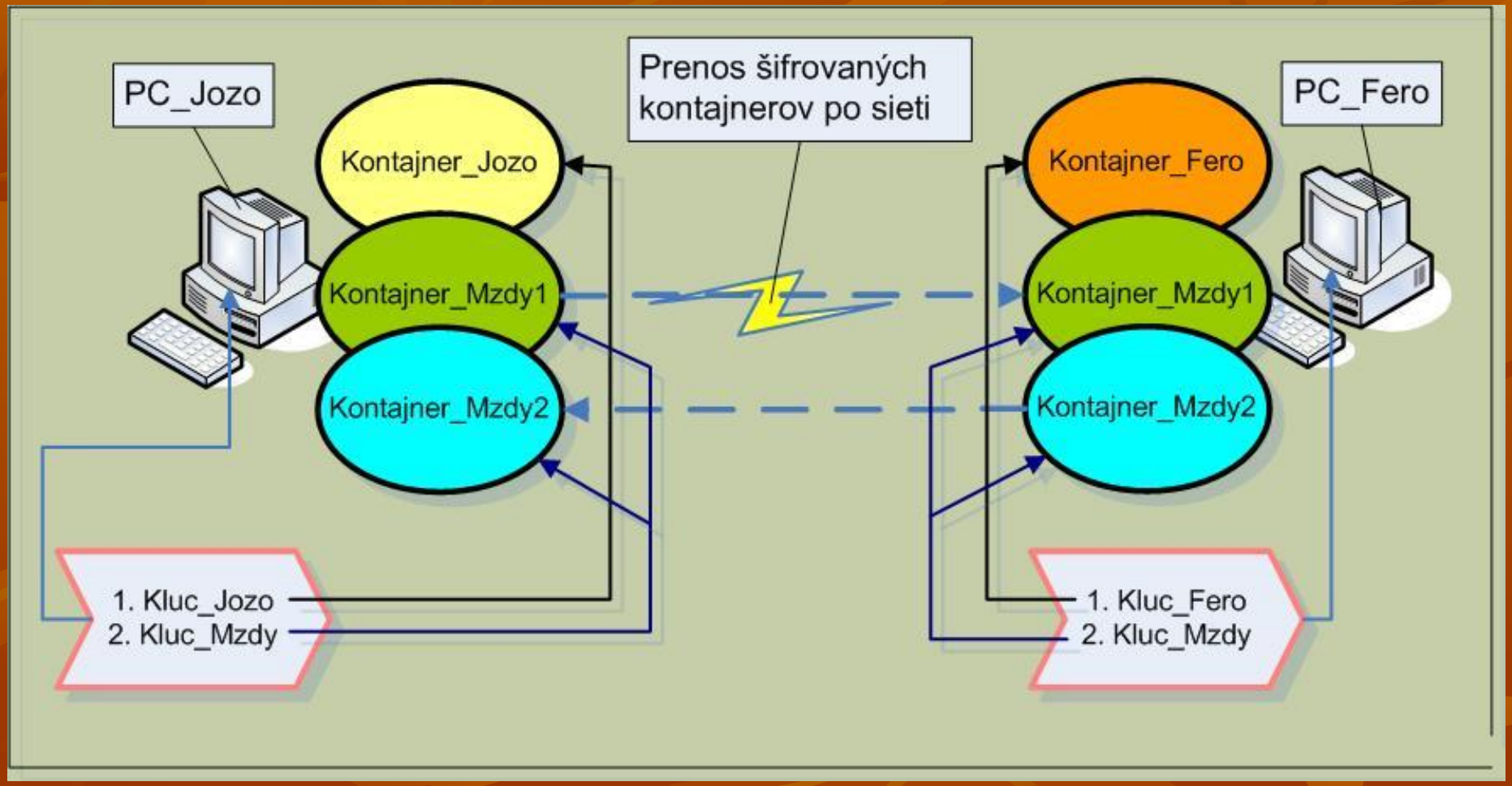
Bezpečnostné opatrenia – rozdiely v OS

- predpokladá sa, že používateľ po skončení práce so šifrovaným virtuálnym diskom odpojí jeho zväzok od kontajnera alebo ho aspoň deautentizuje,
- **Windows 2000:**
  - pred prepnutím do iného používateľského profilu sa musí pôvodný používateľ odhlásiť,
  - v prípade zabudnutia odpojenia disku týmto používateľom:
    - disk alebo disky sa odpájajú so súčasnou deautentizáciou automaticky,
    - systémový disk sa len deautentizuje.
- **Windows XP až Windows 11:**
  - pri použití bezpečnostných nastavení sa systém správa rovnako ako vo Windows 2000,
  - pri nepoužití bezpečnostných nastavení je umožnené prepínanie medzi používateľskými profilmi:
    - je umožnené pripojené disky ponechať autentizované, aby prípadne bežiace aplikácie mohli s nimi pracovať,
    - pri odhlasovaní sa z týchto profilov sú disky automaticky odpájané,
    - závisí na používateľovi, či odpojí disky manuálne alebo to ponechá na systém.

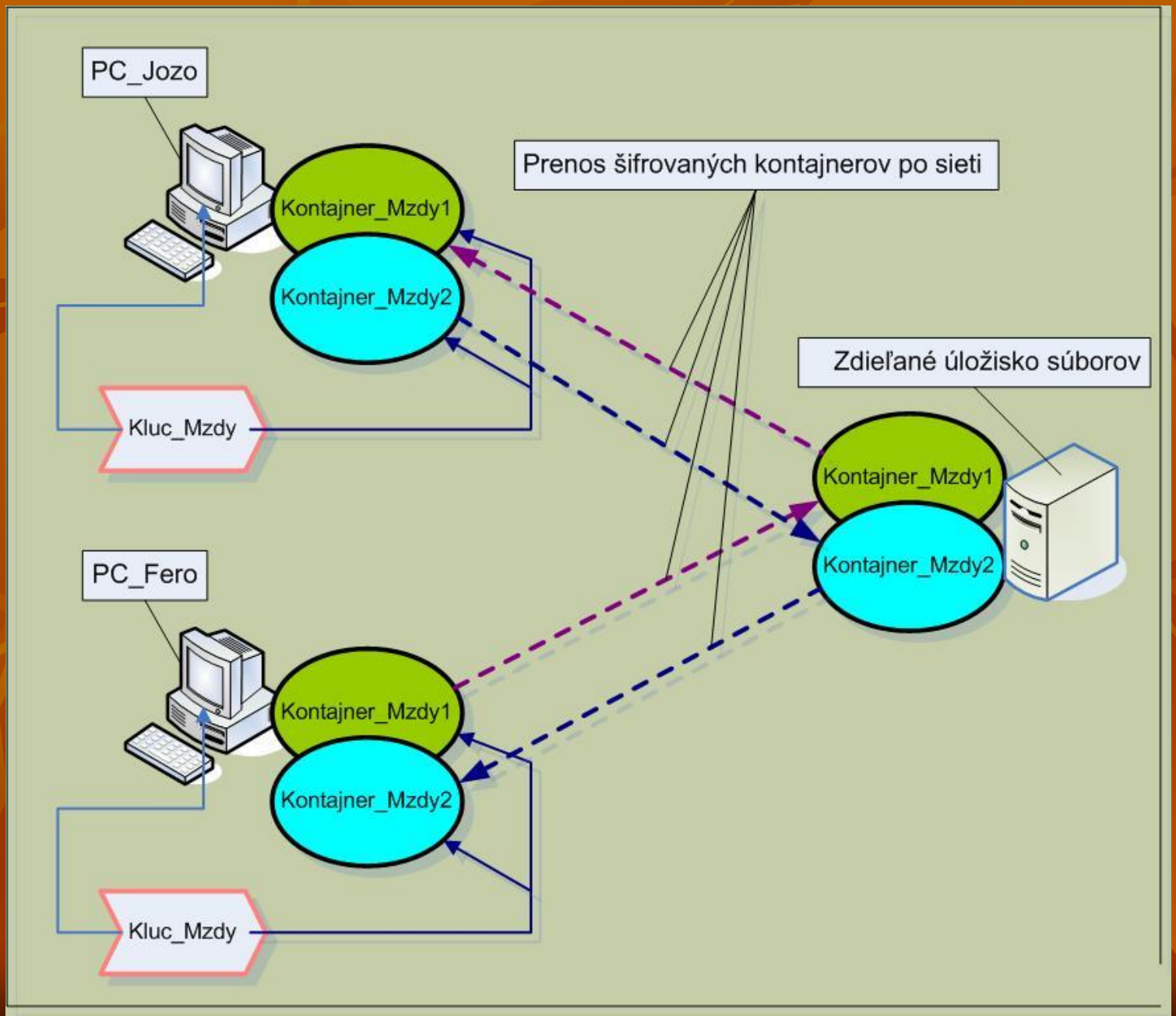
Výhody systému HDprot

- 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.

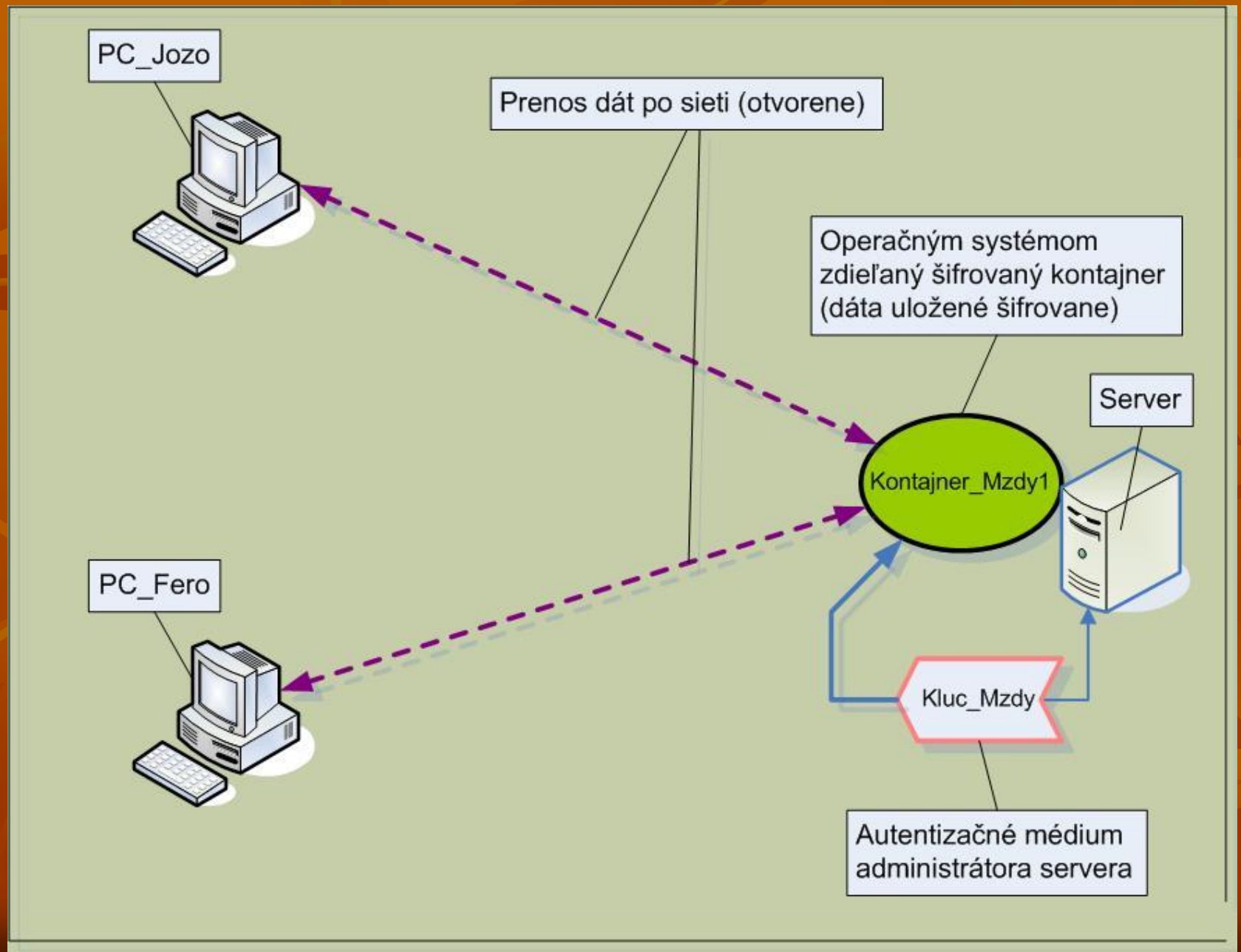
1. Príklad riadenej distribúcie a uloženia citlivých dát



2. Príklad riadenej distribúcie a uloženia citlivých dát



3. Príklad riadenej distribúcie a uloženia citlivých dát



„Nevýhody“ systému HDprot

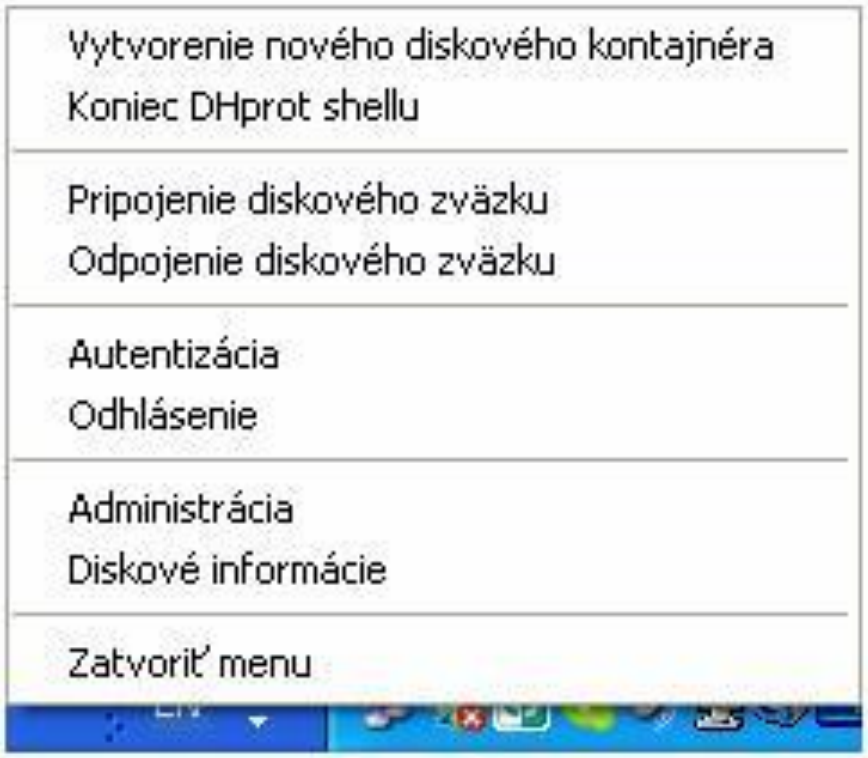
- potreba CBA (Centrálna bezpečnostná autorita), kde sa plnia kľúčové médiá,
- potreba zásahu administrátora, pri vytváraní šifrovaných diskových kontajnerov,
- potreba kľúčového média u používateľa a zapamätanie si PIN-u k nemu,
- potrebná administrácia systému.

Odporúčania pre používateľov

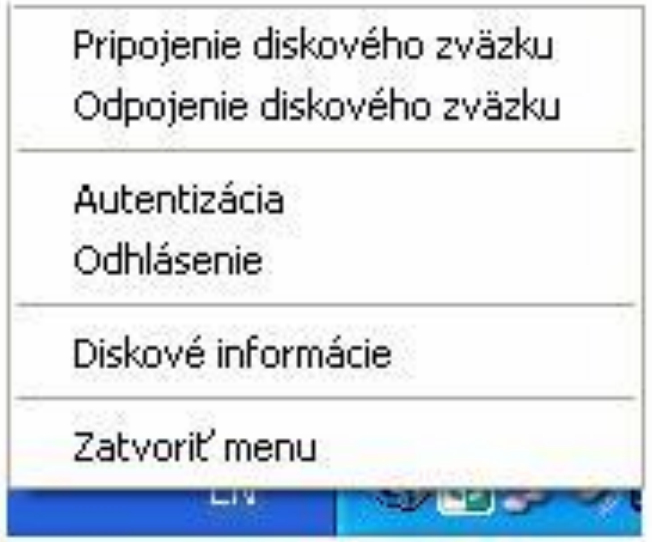
- súbory diskových kontajnerov vytvárať len v definovaných adresároch na pevných resp. logických diskoch, napríklad: **Meno_disku:\DiskoveKontajnery**,
- názvy súborov diskových kontajnerov voliť tak, aby sa už z mena dalo zistiť:
  - ktorý nosič kľúčov (token) je k nemu priradený,
  - ktorý kľúč je k nemu priradený,

napríklad: **Disk_T023_K3**, kde ide o ***token číslo 023*** a z neho ***kľúč číslo 3***.

Kontextové menu shell-u systému



Administrátorský režim



Užívateľský režim

Položky kontextového menu

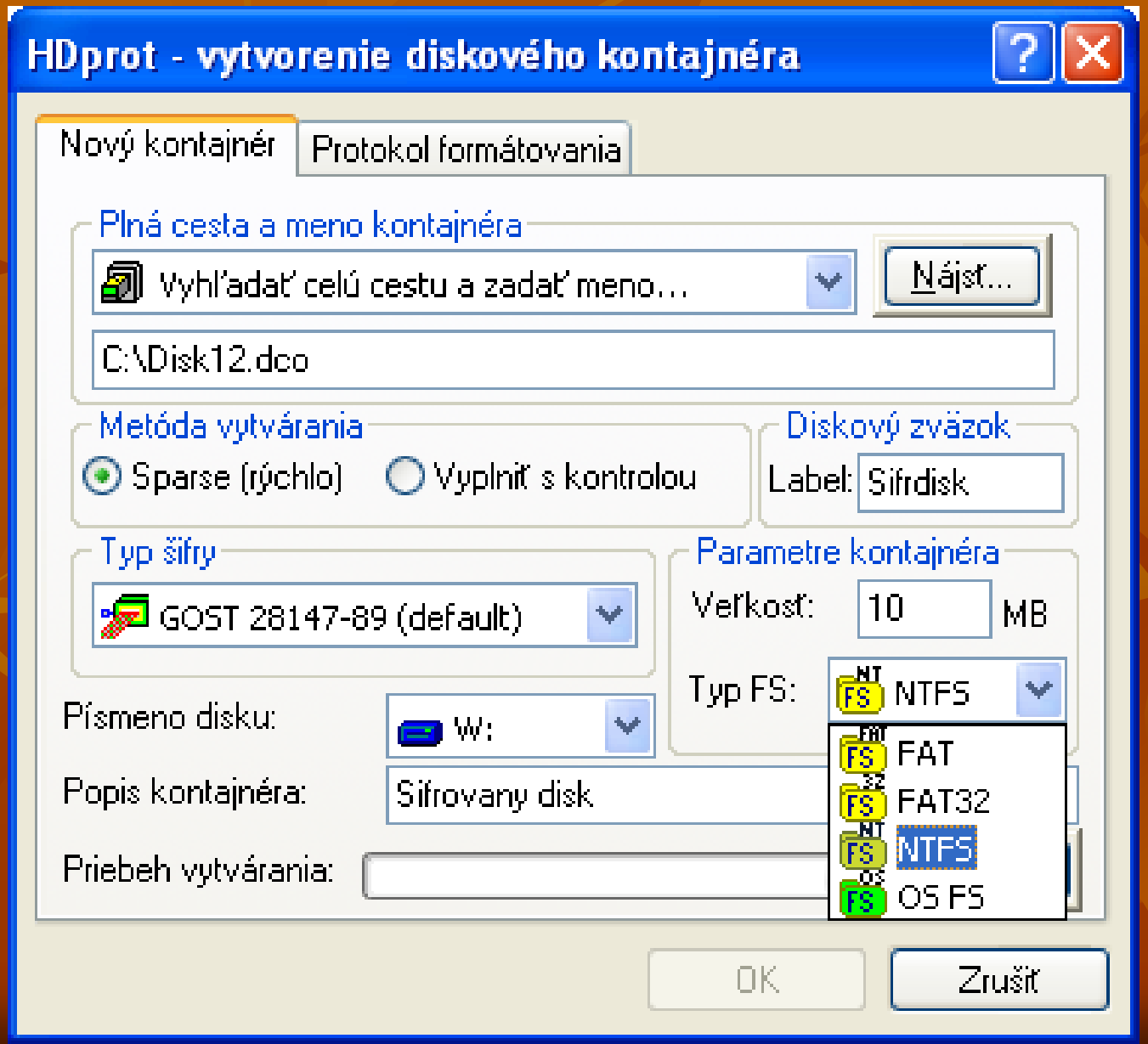
- **Vytvorenie nového diskového kontajnera** – administrátor touto funkciou vytvorí nový diskový kontajner v podobe šifrovaného súboru, ktorý bude prístupný používateľovi s príslušným šifrovacím kľúčom, ktorý mu pridelí administrátor (používateľ si ho potom pripojí a autentizuje sa k nemu).
- **Koniec HDprot shellu** – slúži administrátorovi na zastavenie HDprot shellu:
  - jadro zostáva funkčné,
  - používa sa napríklad pri preinštalovaní alebo upgrade HDprot systému.
- **Pripojenie diskového zväzku** – pripája existujúci diskový kontajner ako diskový zväzok k súborovému systému so súčasnou autentizáciou používateľa k pripájanému kontajneru.
- **Odpojenie diskového zväzku** – odpája autentizovaný alebo neautentizovaný diskový zväzok od diskového kontajnera.
- **Autentizácia** – funkcia pre prihlásenie sa používateľa k už pripojenému kontajneru; prihlásiť sa môže len ten používateľ, ktorého kľúč korešponduje so šifrovaným diskovým kontajnerom.
- **Odhlásenie** - funkcia pre odhlásenie sa používateľa od pripojeného a autentizovaného kontajnera.
- **Administrácia** – funkcie pre administráciu systému HDprot:
  - funkcie systémového chráneného auditu,
  - funkcie pre automatické pripojenie spoločného chráneného systémového kontajnera, ktorý sa pripája vo fáze bootu operačného systému, ale zostáva deautentizovaný; používatelia s oprávnením sa k nemu potom môžu prihlásiť.
- **Diskové informácie** – informácie o pripojených diskoch a kontajneroch.
- **Zatvoriť menu** – zrušenie kontextového menu pre prípad keď ho nie je možné zrušiť iným spôsobom, napríklad kliknutím na plochu.

Predvedenie činnosti systému HDprot

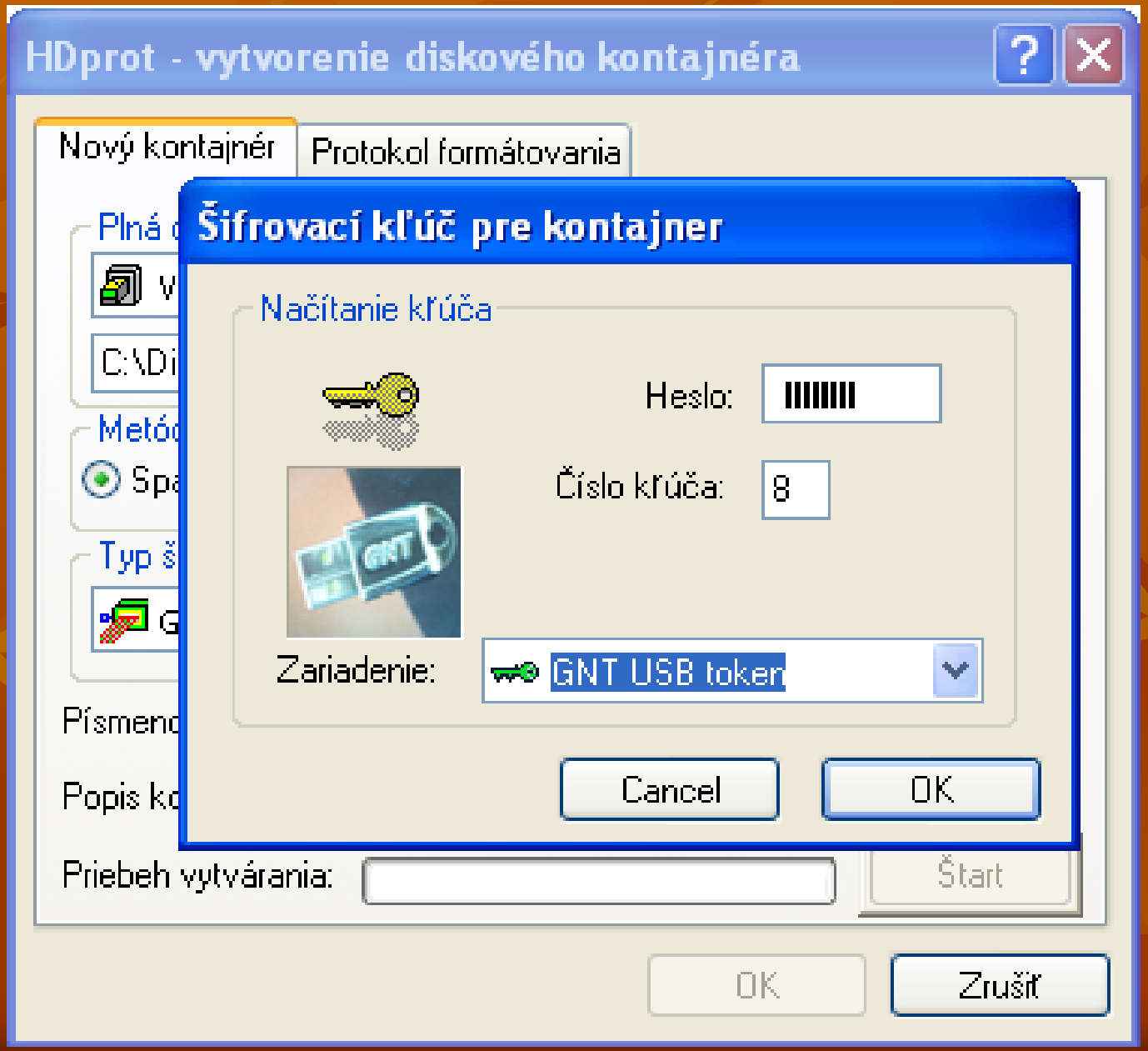
- **Práca v administrátorskom režime:**
  - Vytvorenie diskového kontajnera,
  - Administrácia.
- **Práca v užívateľskom režime:**
  - Pripojenie diskového kontajnera,
  - Autentizácia k diskovému kontajneru.
  - Odhlásenie - deautentizácia diskového kontajnera.
  - Odpripojenie diskového kontajnera,
  - Diskové informácie
- **Inštalácia systému HDprot**

Vytvorenie nového diskového kontajnera

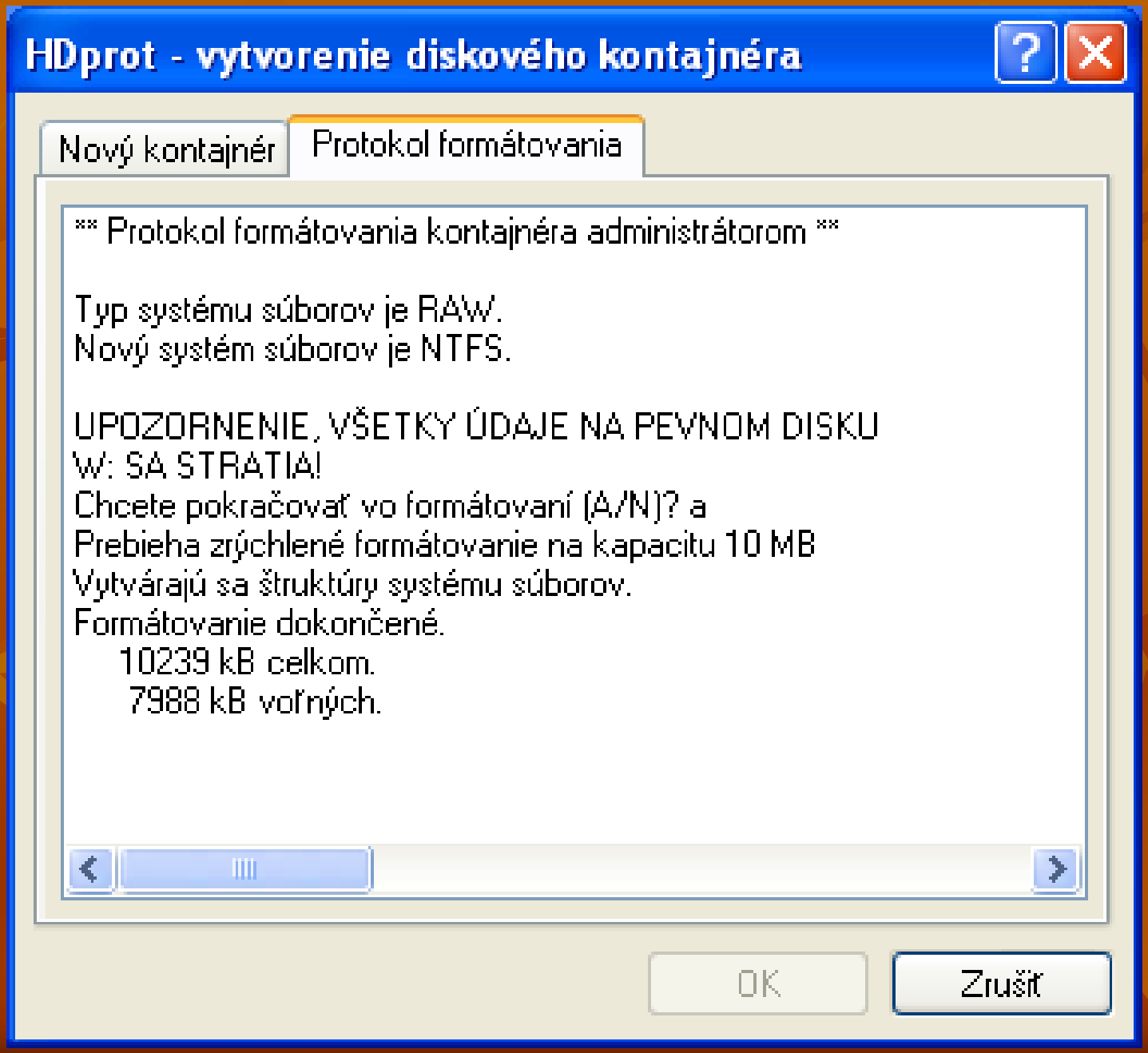
1.krok – zadanie parametrov



2.krok – zadanie šifrovacieho kľúča nového diskového kontajnera

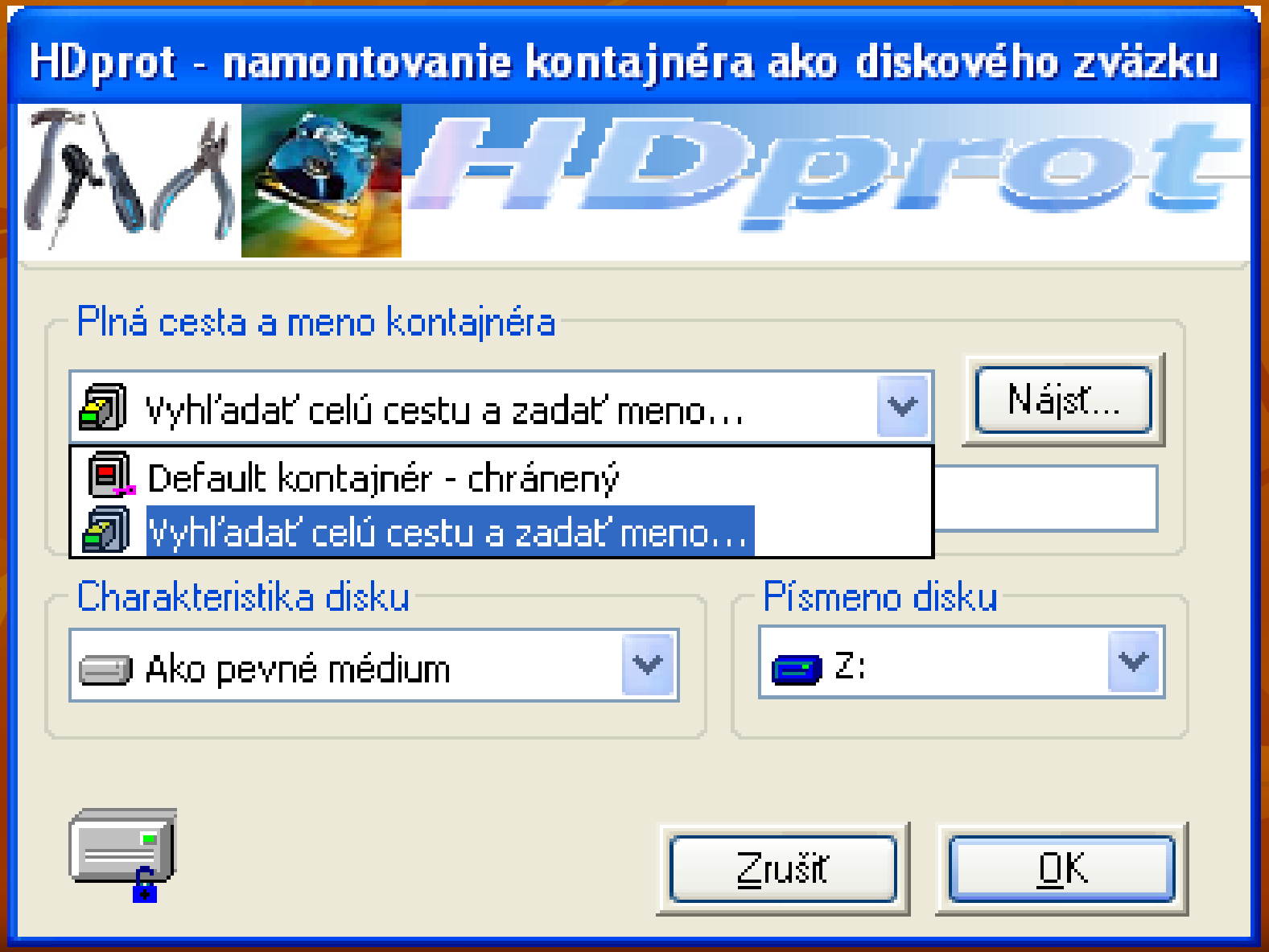


3.krok – naformátovanie nového diskového kontajnera

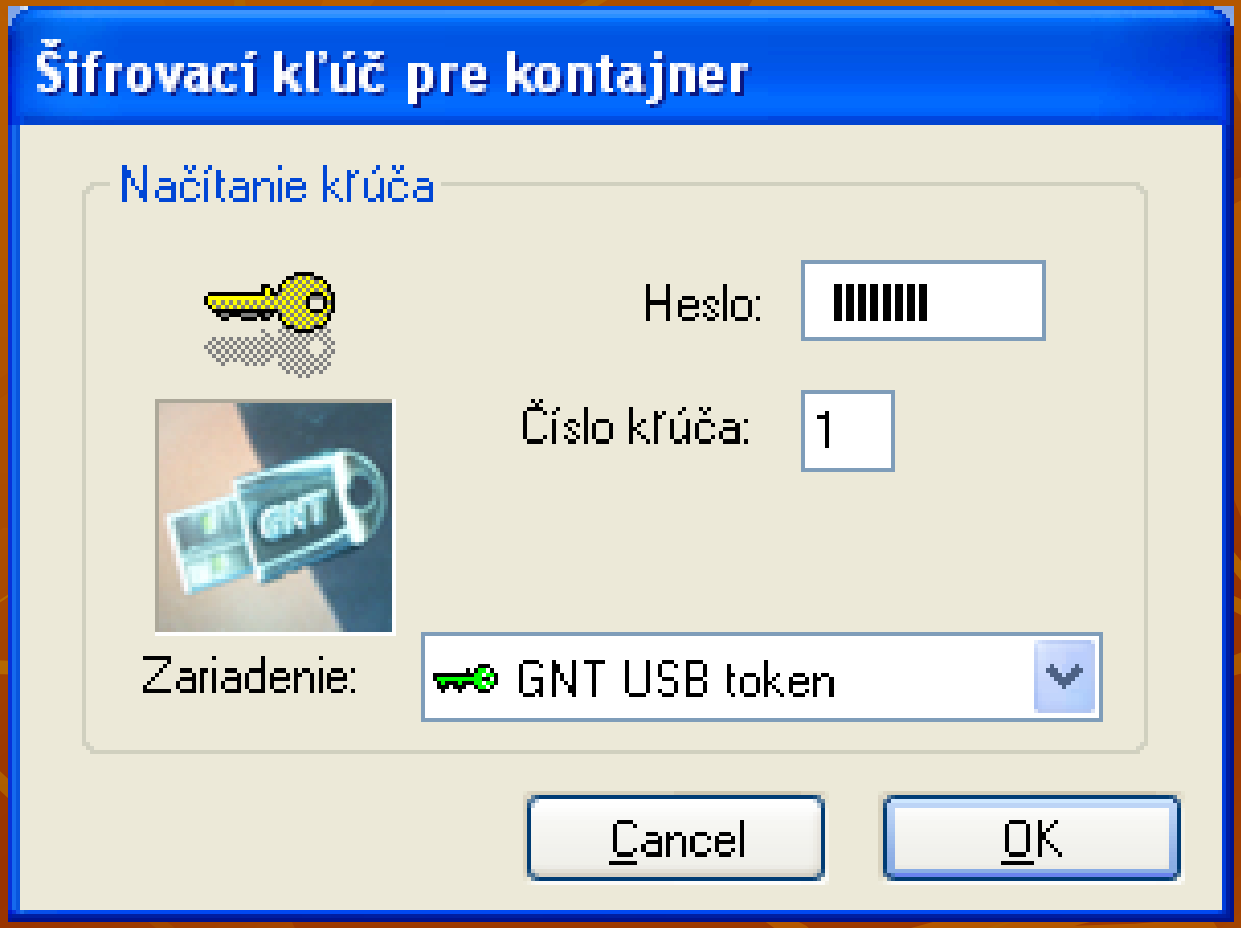


Pripojenie diskového zväzku ku kontajneru

1.krok – zadanie parametrov

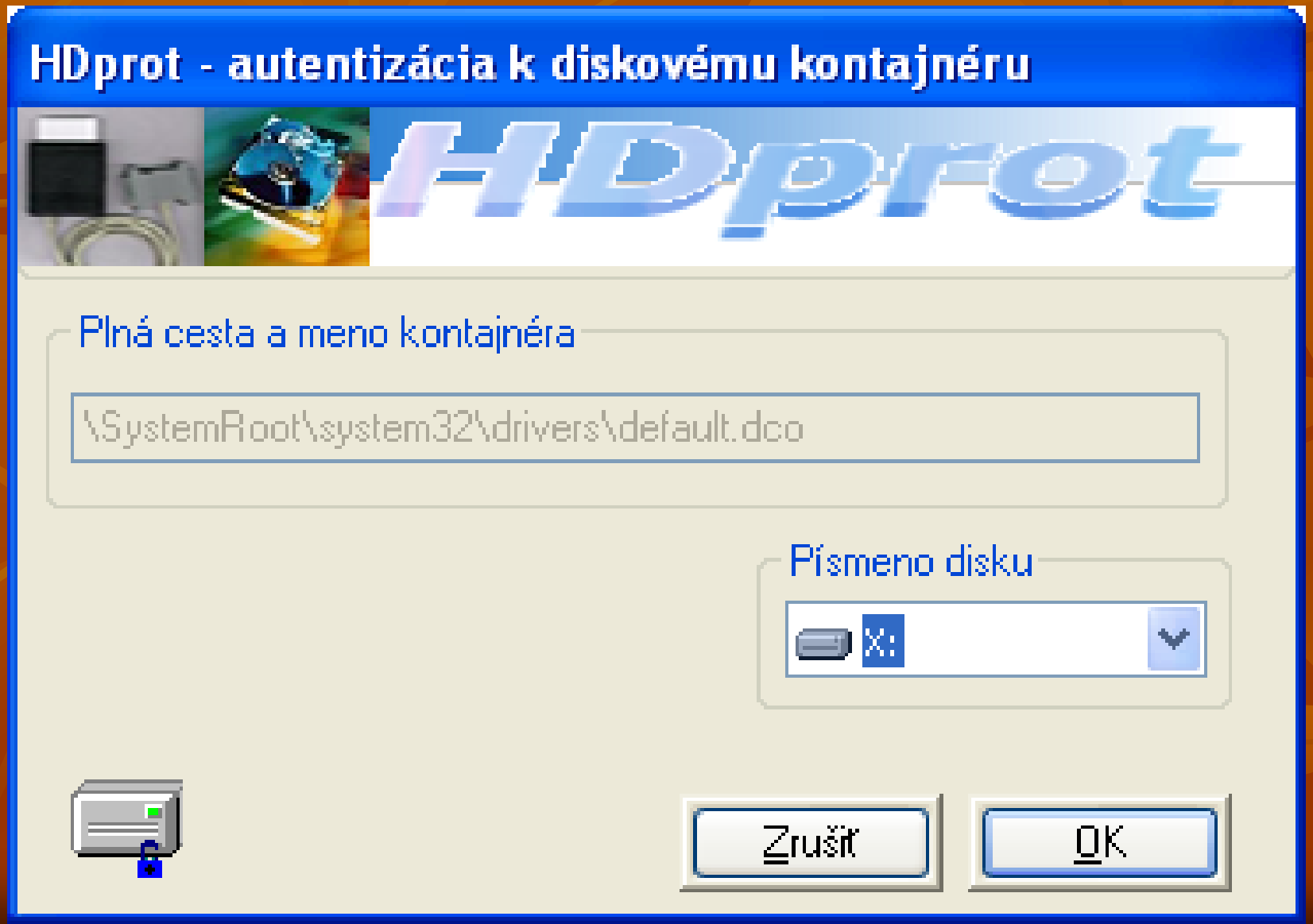


2.krok – zadanie šifrovacieho kľúča pripájaného diskového kontajnera

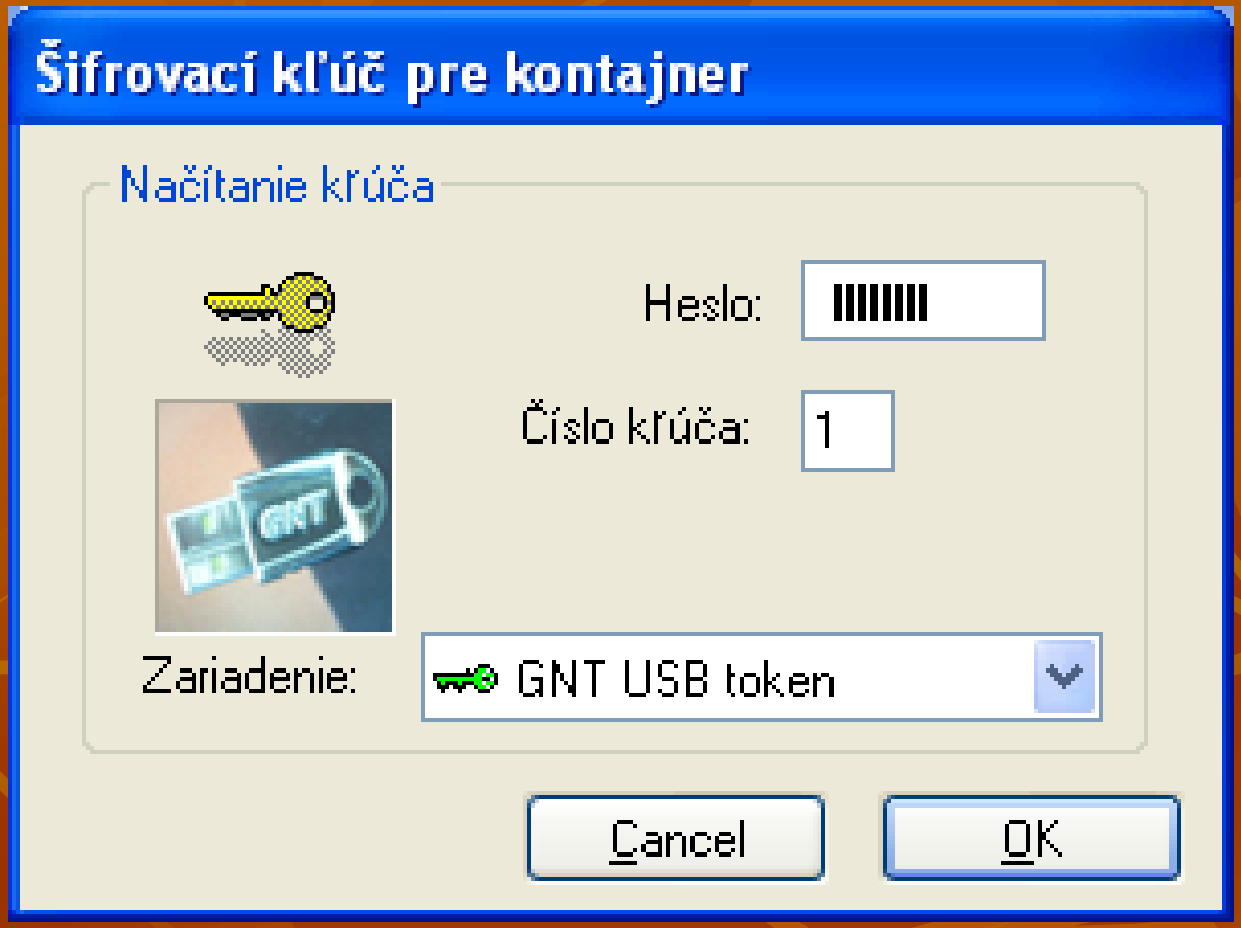


Autentizácia k diskovému zväzku kontajnera

1.krok – výber už pripojeného diskového zväzku

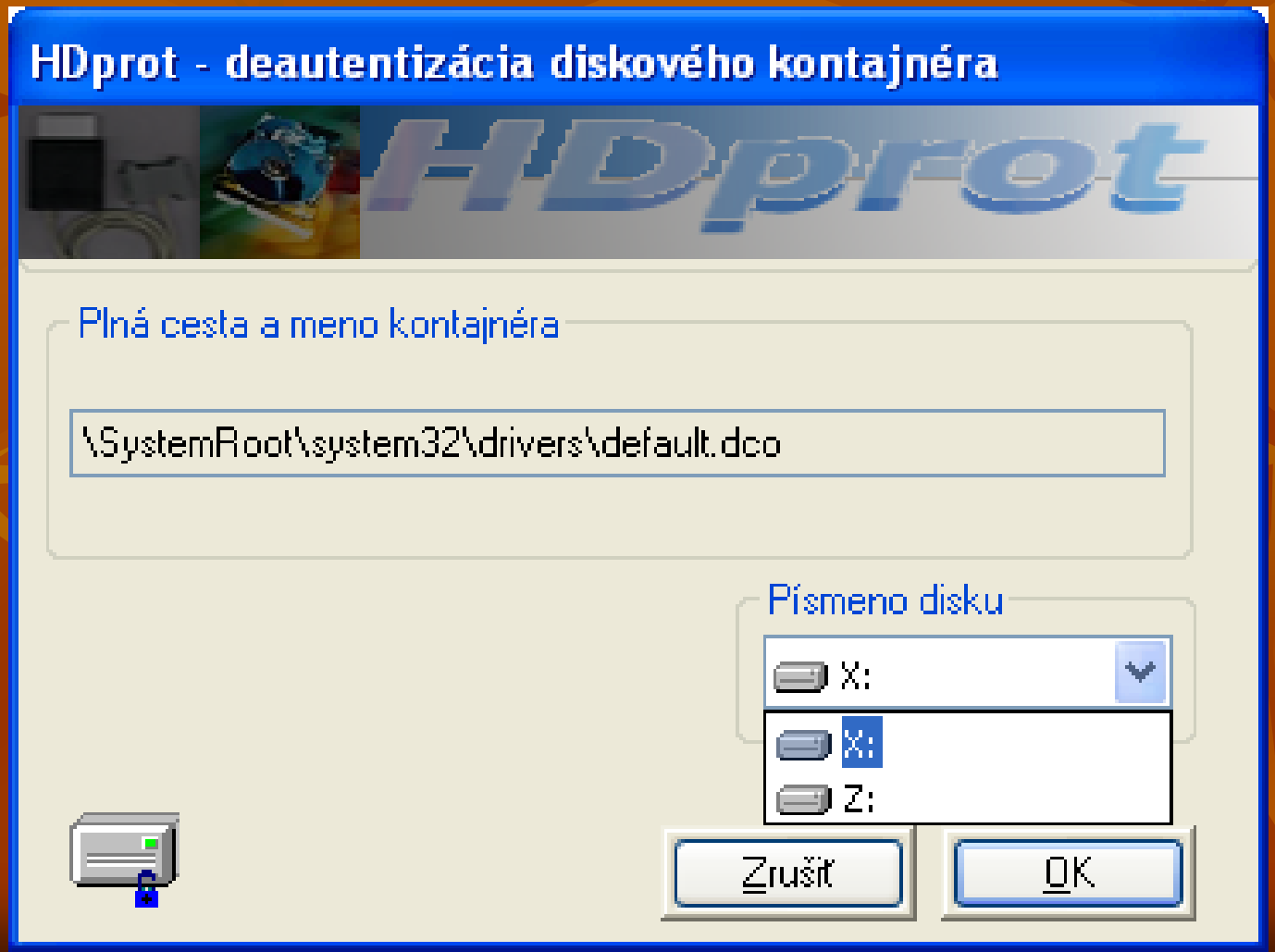


2.krok – zadanie šifrovacieho kľúča diskového kontajnera ku ktorému sa autentizuje



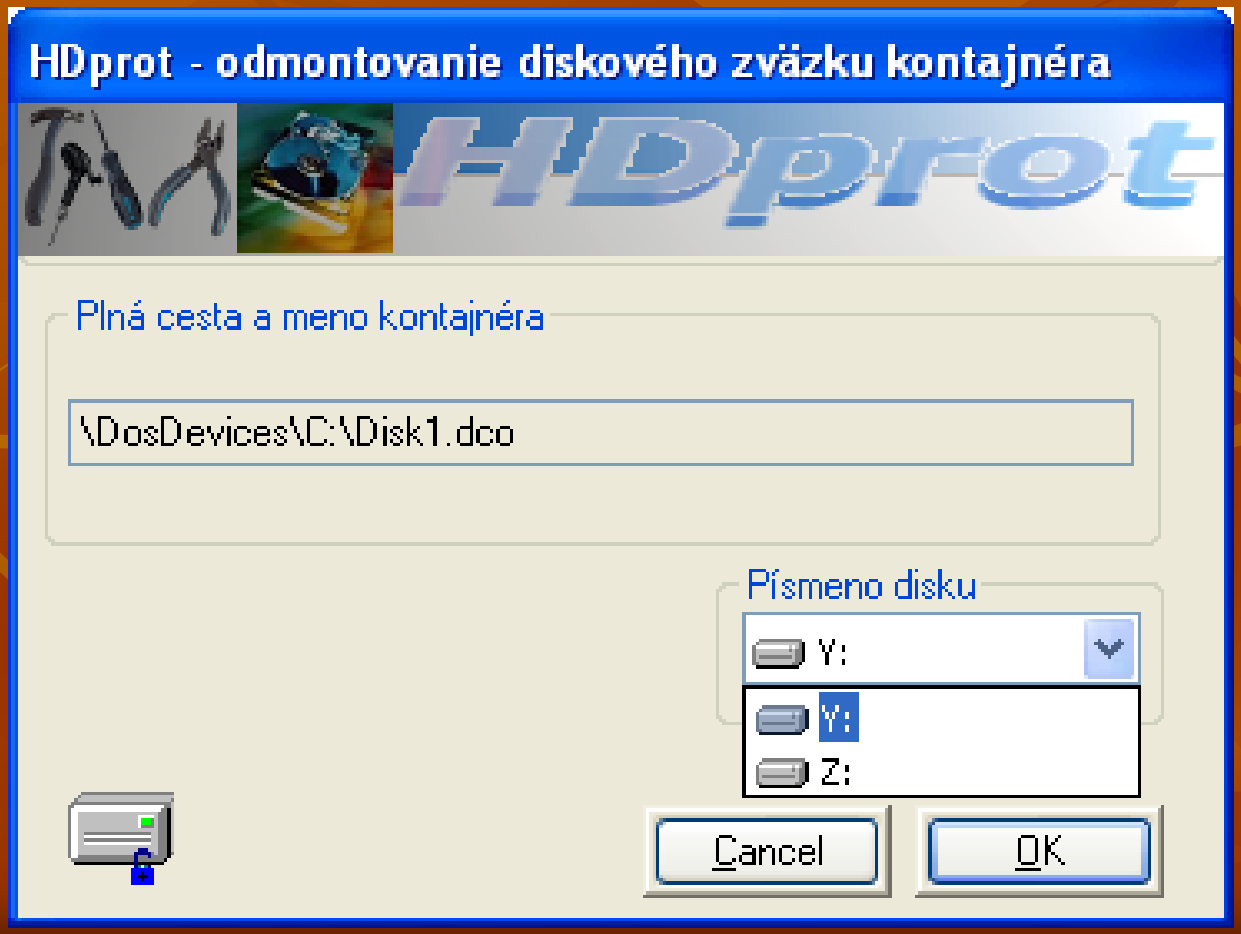
Odhlásenie - deautentizácia diskového zväzku kontajnera

- zablokovanie prístupu na disk a fyzické vymazanie zo systému jeho šifrovacieho kľúča,
- vykonáva sa tzv. bezpečná deautentizácia - ak na pozadí ešte prebieha napríklad zápis na daný disk, tento sa najprv ukončí, a až keď sú všetky buffre a keše súborového systému súvisiace s týmto diskom vyprázdnené, tak potom sa vykoná

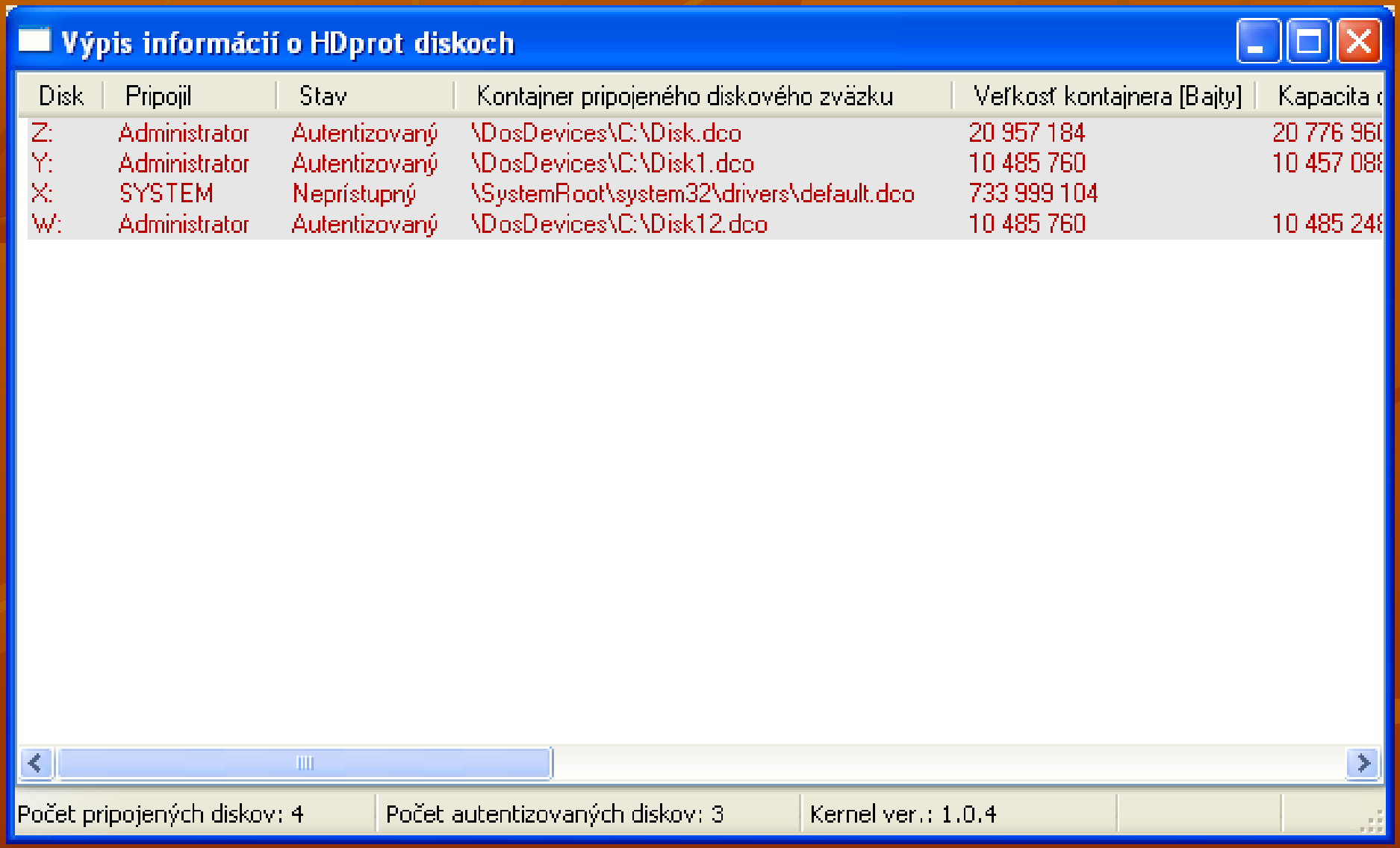


Odpojenie - diskového zväzku od kontajnera

- zruší sa existencia požadovaného virtuálneho disku so zvoleným písmenom,
- zablokovanie prístupu na disk a fyzické vymazanie zo systému jeho šifrovacieho kľúča,
- vykonáva sa tzv. bezpečné odpojenie - ak na pozadí ešte prebieha napríklad zápis na daný disk, tento sa najprv ukončí, a až keď sú všetky buffre a keše súborového systému súvisiace s týmto diskom vyprázdnené, tak potom sa vykoná najskôr deautentizácie a potom odpojenie



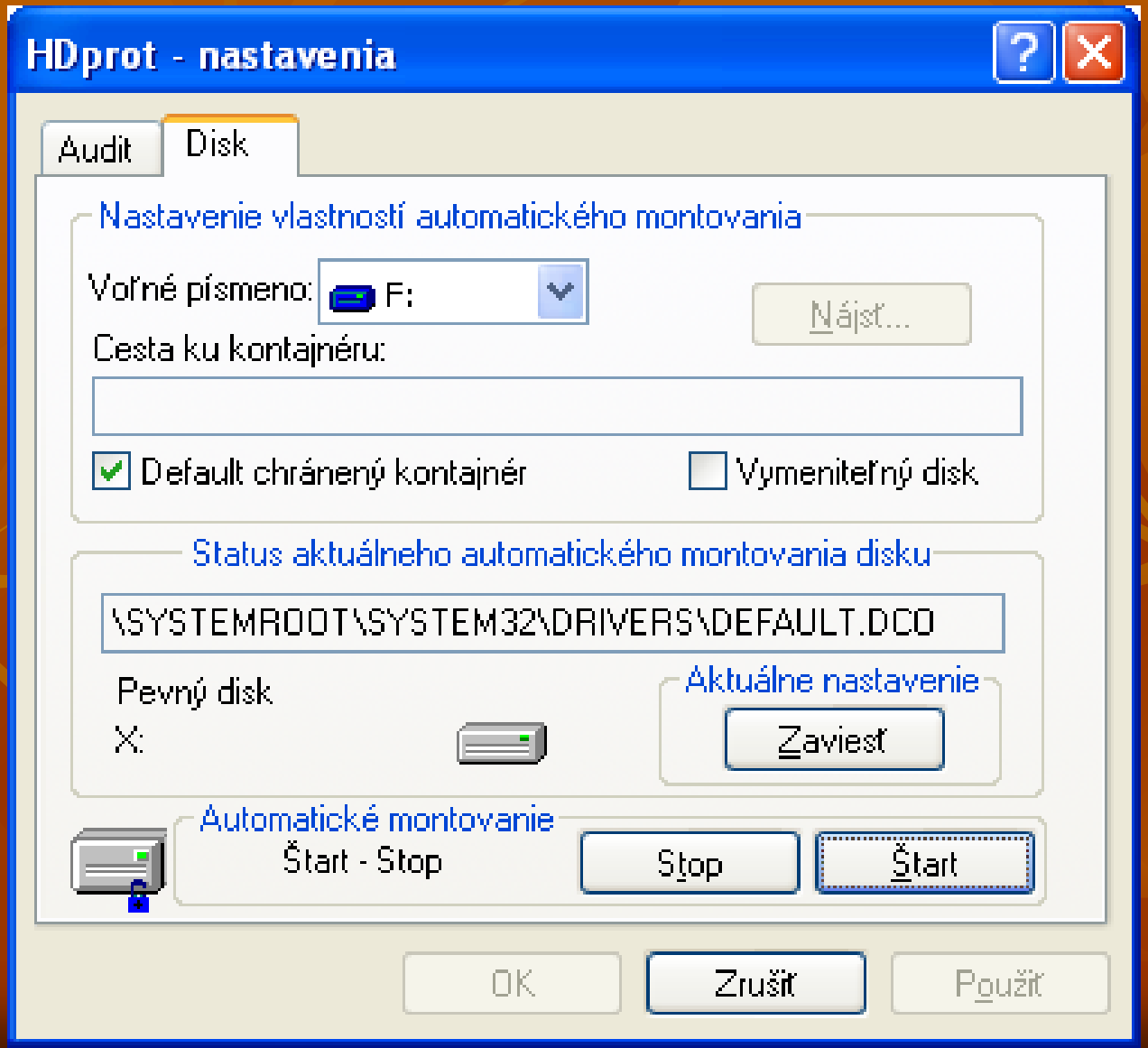
Diskové informácie



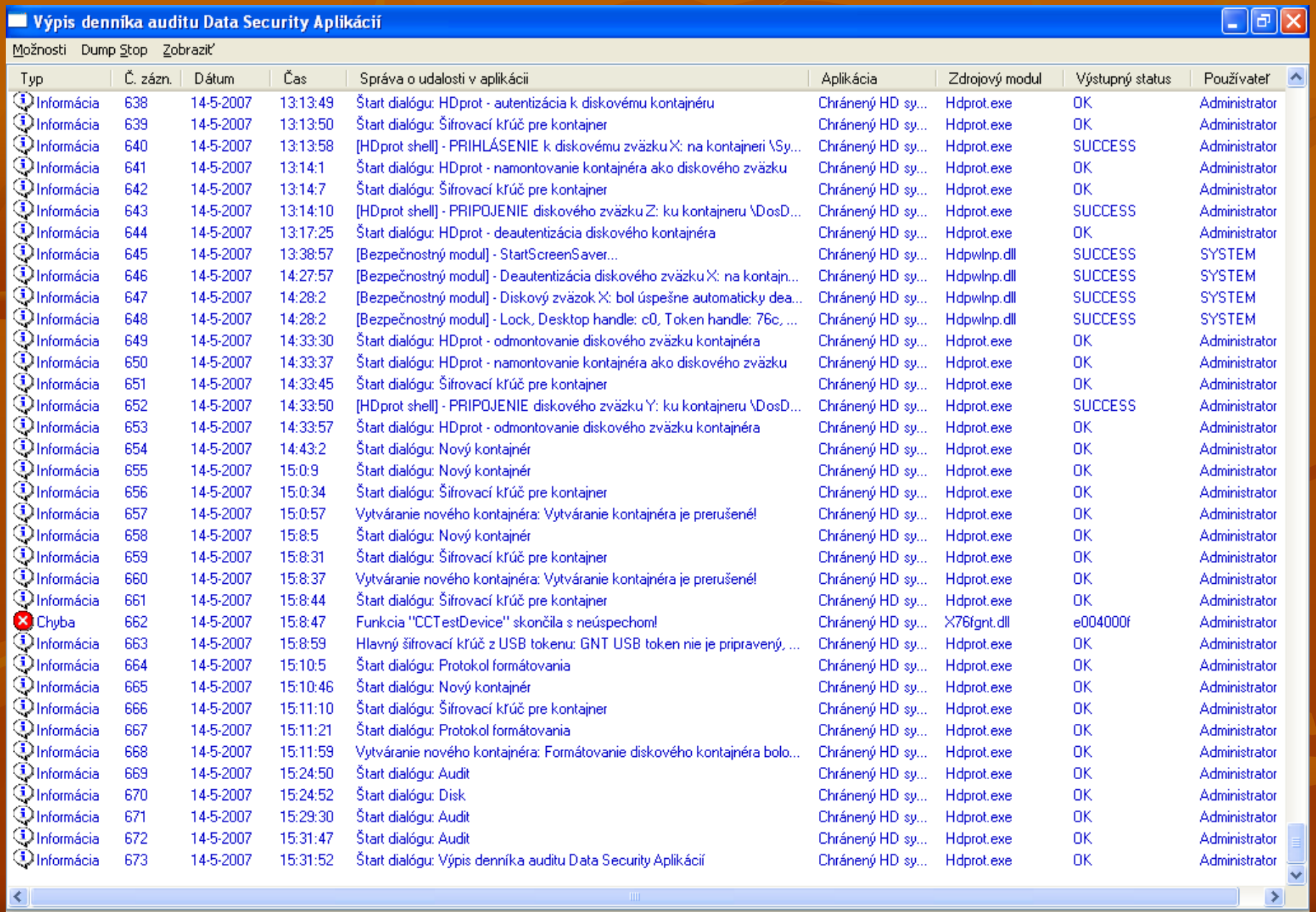
Administrácia chráneného diskového systému

- nastavenie vlastností automaticky pripájaného diskového zväzku,
- záznam do denníka udalostí – auditu.
  - nastavenia parametrov,
  - prehliadanie záznamov.

Nastavenie vlastností automaticky pripájaného diskového zväzku



Záznam do denníka udalostí



Typ	Č. zázn.	Dátum	Čas	Správa o udalosti v aplikácii	Aplikácia	Zdrojový modul	Výstupný status	Používateľ
Informácia	638	14-5-2007	13:13:49	Štart dialógu: HDprot - autentizácia k diskovému kontajnéru	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	639	14-5-2007	13:13:50	Štart dialógu: Šifrovací kľúč pre kontajner	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	640	14-5-2007	13:13:58	[HDprot shell] - PRIHLÁSENIE k diskovému zväzku X: na kontajneri \Sy...	Chránený HD sy...	Hdprot.exe	SUCCESS	Administrator
Informácia	641	14-5-2007	13:14:1	Štart dialógu: HDprot - namontovanie kontajnéra ako diskového zväzku	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	642	14-5-2007	13:14:7	Štart dialógu: Šifrovací kľúč pre kontajner	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	643	14-5-2007	13:14:10	[HDprot shell] - PRIPOJENIE diskového zväzku Z: ku kontajneru \DosD...	Chránený HD sy...	Hdprot.exe	SUCCESS	Administrator
Informácia	644	14-5-2007	13:17:25	Štart dialógu: HDprot - deautentizácia diskového kontajnéra	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	645	14-5-2007	13:38:57	[Bezpečnostný modul] - StartScreenSaver...	Chránený HD sy...	Hdpwlnp.dll	SUCCESS	SYSTEM
Informácia	646	14-5-2007	14:27:57	[Bezpečnostný modul] - Deautentizácia diskového zväzku X: na kontajn...	Chránený HD sy...	Hdpwlnp.dll	SUCCESS	SYSTEM
Informácia	647	14-5-2007	14:28:2	[Bezpečnostný modul] - Diskový zväzok X: bol úspešne automaticky dea...	Chránený HD sy...	Hdpwlnp.dll	SUCCESS	SYSTEM
Informácia	648	14-5-2007	14:28:2	[Bezpečnostný modul] - Lock, Desktop handle: c0, Token handle: 76c, ...	Chránený HD sy...	Hdpwlnp.dll	SUCCESS	SYSTEM
Informácia	649	14-5-2007	14:33:30	Štart dialógu: HDprot - odmontovanie diskového zväzku kontajnéra	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	650	14-5-2007	14:33:37	Štart dialógu: HDprot - namontovanie kontajnéra ako diskového zväzku	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	651	14-5-2007	14:33:45	Štart dialógu: Šifrovací kľúč pre kontajner	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	652	14-5-2007	14:33:50	[HDprot shell] - PRIPOJENIE diskového zväzku Y: ku kontajneru \DosD...	Chránený HD sy...	Hdprot.exe	SUCCESS	Administrator
Informácia	653	14-5-2007	14:33:57	Štart dialógu: HDprot - odmontovanie diskového zväzku kontajnéra	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	654	14-5-2007	14:43:2	Štart dialógu: Nový kontajnér	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	655	14-5-2007	15:0:9	Štart dialógu: Nový kontajnér	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	656	14-5-2007	15:0:34	Štart dialógu: Šifrovací kľúč pre kontajner	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	657	14-5-2007	15:0:57	Vytváranie nového kontajnéra: Vytváranie kontajnéra je prerušené!	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	658	14-5-2007	15:8:5	Štart dialógu: Nový kontajnér	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	659	14-5-2007	15:8:31	Štart dialógu: Šifrovací kľúč pre kontajner	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	660	14-5-2007	15:8:37	Vytváranie nového kontajnéra: Vytváranie kontajnéra je prerušené!	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	661	14-5-2007	15:8:44	Štart dialógu: Šifrovací kľúč pre kontajner	Chránený HD sy...	Hdprot.exe	OK	Administrator
Chyba	662	14-5-2007	15:8:47	Funkcia "CCTestDevice" skončila s neúspechom!	Chránený HD sy...	X76fgnt.dll	e004000f	Administrator
Informácia	663	14-5-2007	15:8:59	Hlavný šifrovací kľúč z USB tokenu: GNT USB token nie je pripravený, ...	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	664	14-5-2007	15:10:5	Štart dialógu: Protokol formátovania	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	665	14-5-2007	15:10:46	Štart dialógu: Nový kontajnér	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	666	14-5-2007	15:11:10	Štart dialógu: Šifrovací kľúč pre kontajner	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	667	14-5-2007	15:11:21	Štart dialógu: Protokol formátovania	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	668	14-5-2007	15:11:59	Vytváranie nového kontajnéra: Formátovanie diskového kontajnéra bolo...	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	669	14-5-2007	15:24:50	Štart dialógu: Audit	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	670	14-5-2007	15:24:52	Štart dialógu: Disk	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	671	14-5-2007	15:29:30	Štart dialógu: Audit	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	672	14-5-2007	15:31:47	Štart dialógu: Audit	Chránený HD sy...	Hdprot.exe	OK	Administrator
Informácia	673	14-5-2007	15:31:52	Štart dialógu: Výpis denníka auditu Data Security Aplikácií	Chránený HD sy...	Hdprot.exe	OK	Administrator