

Desktop systémy Microsoft Windows

IW1/XMW1 2011/2012

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií
Vysoké Učení Technické v Brně
Božetěchova 2, 612 66 Brno

Revize 1.11.2011

Sdílení a zabezpečení zdrojů

Povolení sdílení zdrojů

- Na úrovni **síťových profilů** (v části pokročilých nastavení sdílení)
 - **Povolit Sdílení souborů a tiskáren**
- Na úrovni **síťových rozhraní** (ve vlastnostech jednotlivých síťových rozhraní)
 - **Povolit Sdílení souborů a tiskáren v síti Microsoft**
 - **Povolit Klient sítě Microsoft**

Nastavení sdílení pro profil a adaptér

The image shows two overlapping Windows windows. The background window is the 'Advanced sharing settings' page, and the foreground window is the 'Local Area Connection Properties' dialog.

Background Window: Změnit možnosti sdílení pro různé síťové profily

System Windows vytvoří samostatný síťový profil pro každou používající specifické možnosti.

Doma nebo Práce _____

Zjišťování sítě _____

Pokud je zapnuté zjišťování sítě, tento počítač uvidí jiné počítače v síti také uvidí tento počítač. [Co je zjišťování sítě?](#)

- Zapnout zjišťování sítě
- Vypnout zjišťování sítě

Sdílení souborů a tiskáren _____

Je-li zapnuto sdílení souborů a tiskáren, mohou mít uživatelé nastaveným jako sdílené z tohoto počítače.

- Zapnout sdílení souborů a tiskáren
- Vypnout sdílení souborů a tiskáren

Foreground Window: Připojení k místní síti - vlastnosti

Sítě

Připojit pomocí:

Intel(R) PRO/1000 MT Network Connection Konfigurovat...

Toto připojení používá následující položky:

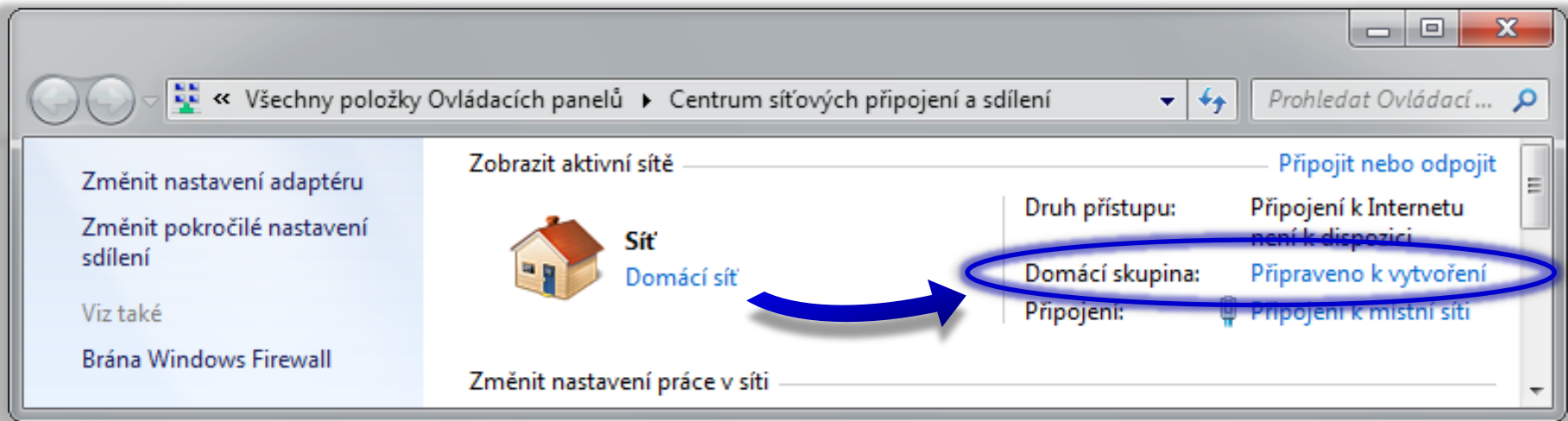
- Klient sítě Microsoft
- Microsoft Network Monitor 3 Driver
- Plánovač paketů technologie QoS
- Sdílení souborů a tiskáren v sítích Microsoft
- Protokol IP verze 6 (TCP/IPv6)
- Protokol IP verze 4 (TCP/IPv4)

Nainstalovat... Odinstalovat Vlastnosti

OK Storno

Domácí skupiny (HomeGroups)

- Umožňují jednoduché sdílení souborů a tiskáren v systémech **Windows 7**
 - Povolení vyžaduje **oprávnění správce**
 - Co sdílet si volí jednotliví **uživatelé**
- Dostupné **pouze** v **domácí síti**



Vytvoření domácí skupiny

Vytvořit domácí skupinu

Sdílení s jinými domácími počítači používajícími systém Windows 7

Tento počítač může sdílet soubory a tiskárny s ostatními počítači používajícími systém Windows 7. Můžete také vysílat datový proud médií do zařízení používajících domácí skupinu. Domácí skupina je chráněná heslem a vždy budete mít možnost vybrat, co budete v rámci skupiny sdílet.

[Další informace o domácích skupinách](#)

Vyberte položky, které chcete sdílet:

- Obrázky
- Dokumenty
- Hudba
- Tiskárny
- Videá

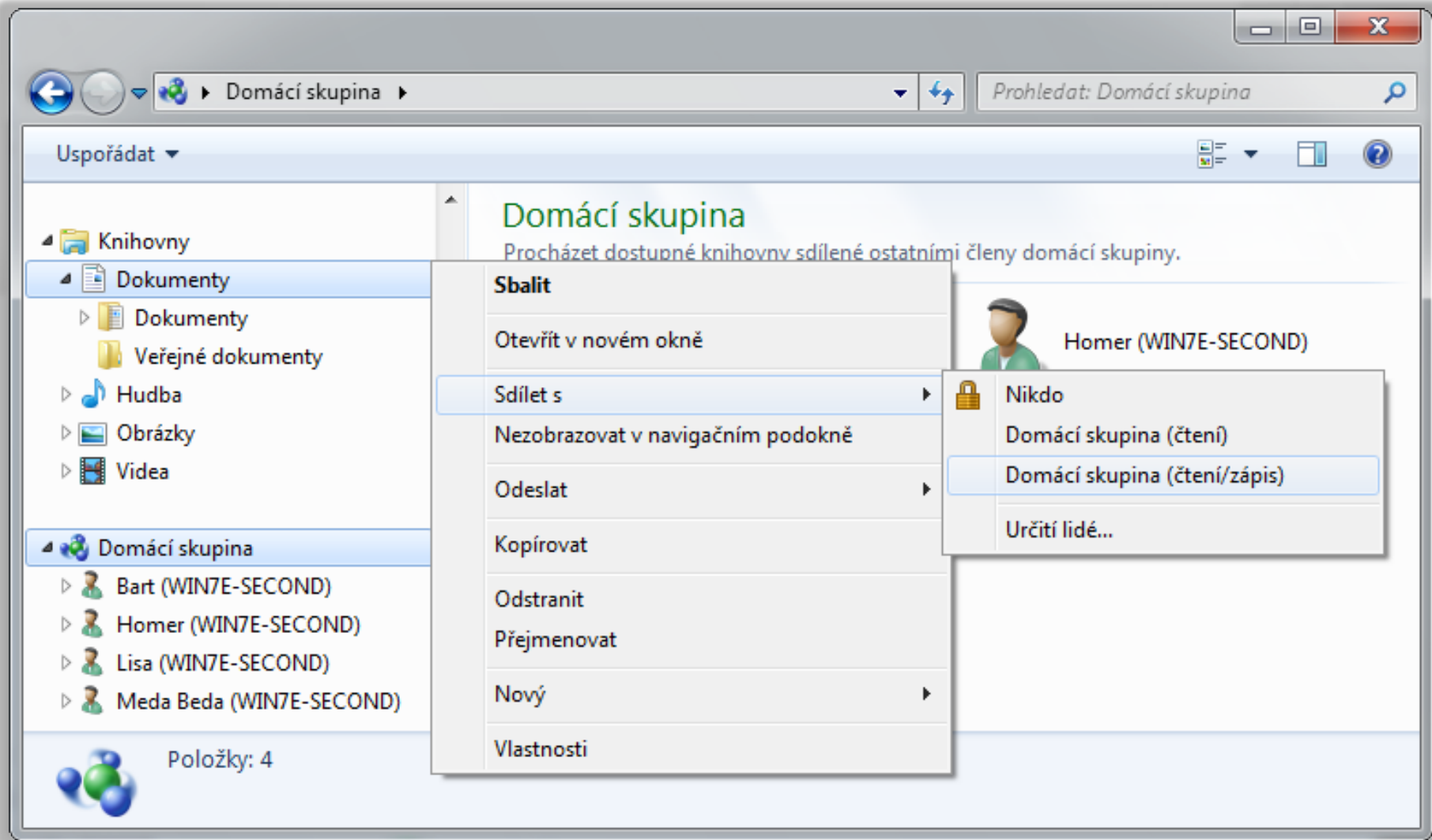
Připraveno k vytvoření

Další **Storno**

Připojení a přístup k domácí skupině

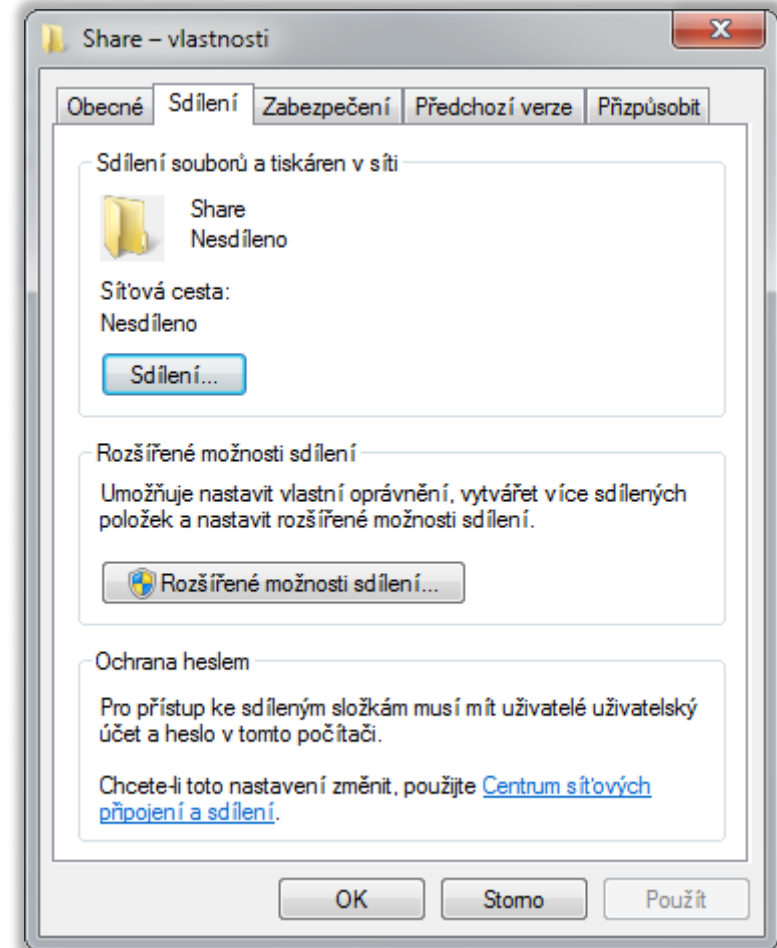
- Připojení k domácí skupině
 - Přes **Centrum síťových připojení a sdílení**
 - Pro připojení je vyžadováno sdílené **heslo**
- Přístup k domácí skupině
 - Přes **průzkumníka Windows** (samostatný uzel)
 - Rozlišovány na základě **uživatele** a **počítače**
 - Dostupné vždy když **běží** daný **počítač** (i pokud není **přihlášen** konkrétní uživatel)
 - K přístupu lze použít **vlastní** nebo **sdílený** účet

Sdílení adresářů v domácí skupině



Sdílené adresáře (Shared Folders)

- **Povolení a nastavení** ve vlastnostech adresáře (záložka **sdílení**)
- 2 typy sdílení
 - Jednoduché (*simple*) sdílení
 - Pokročilé (*advanced*) sdílení



Jednoduché sdílení adresářů

- Rozlišuje 3 typy oprávnění (nastavuje **vlastník**)
 - Čtení
 - Čtení/zápis (zahrnuje i úpravy a mazání)
 - Vlastník (**nelze** nastavit, přiřazeno **automaticky** účtu uživatele, jenž daný adresář **nasdílel**)
- Oprávnění lze nastavovat **pouze**
 - Lokálním uživatelům
 - Lokálním skupinám **Everyone** a **HomeGroup**
 - Doménovým skupinám a uživatelům

Nastavení jednoduchého sdílení

The image shows two overlapping windows from a Windows operating system. The background window is the 'Share - vlastnosti' (Share - properties) window, showing the 'Sdílení' (Sharing) tab. It displays a folder named 'Share' with the status 'Nesdíleno' (Not shared). A blue arrow points from the 'Sdílení...' button to the foreground window.

The foreground window is the 'Sdílení souborů' (Share files) dialog box. It prompts the user to 'Zvolte osoby pro sdílení.' (Select people to share with.) and provides instructions: 'Zadejte jméno a klikněte na tlačítko Přidat nebo uživatele vyhledejte kliknutím na šipku.' (Enter a name and click the Add button or find a user by clicking the arrow.)

The dialog box contains a search field and a 'Přidat' (Add) button. Below is a table of users and their permissions:

Jméno	Úroveň oprávnění
Everyone	Čtení/zápis
Meda Beda	Vlastník
Student	Čtení

A context menu is open over the 'Student' user, showing the following options:

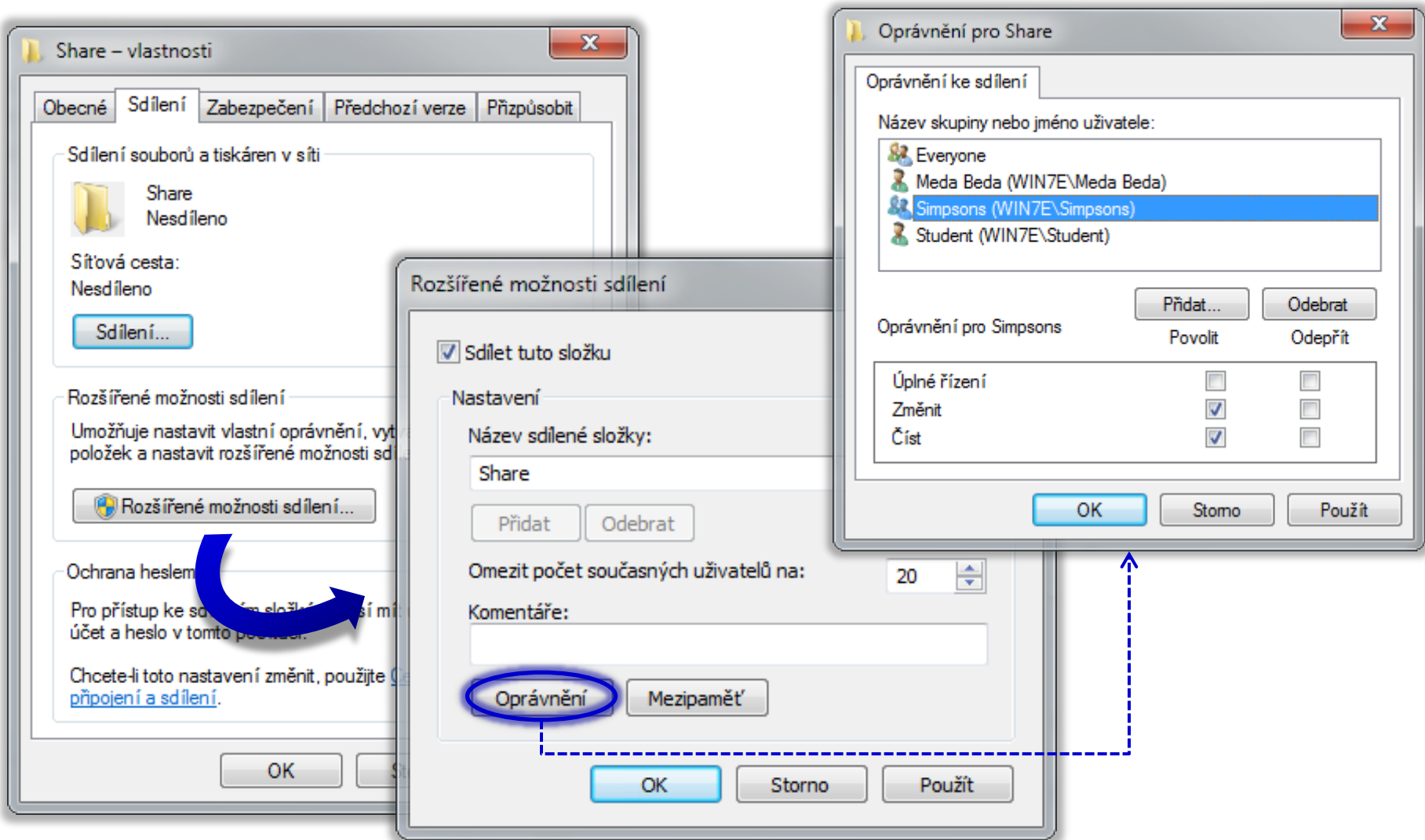
- Čtení (checked)
- Čtení/zápis
- Odebrat

At the bottom of the dialog box, there is a link for 'Problémy se sdílením' (Share problems) and buttons for 'Sdílet' (Share) and 'Storno' (Cancel).

Pokročilé sdílení adresářů

- Rozlišuje 3 typy oprávnění
 - Číst
 - Změnit (čtení + zápis, úpravy a mazání)
 - Úplné řízení (možnost nastavovat **oprávnění**)
- Oprávnění lze nastavovat
 - Lokálním i doménovým uživatelům a skupinám
- Možnost **limitování** počtu **připojeným** uživatelů
 - Hodnota **0** zastupuje nekonečno (**neomezený** limit)
- Podpora **souborů offline** (*offline files*)

Nastavení pokročilého sdílení



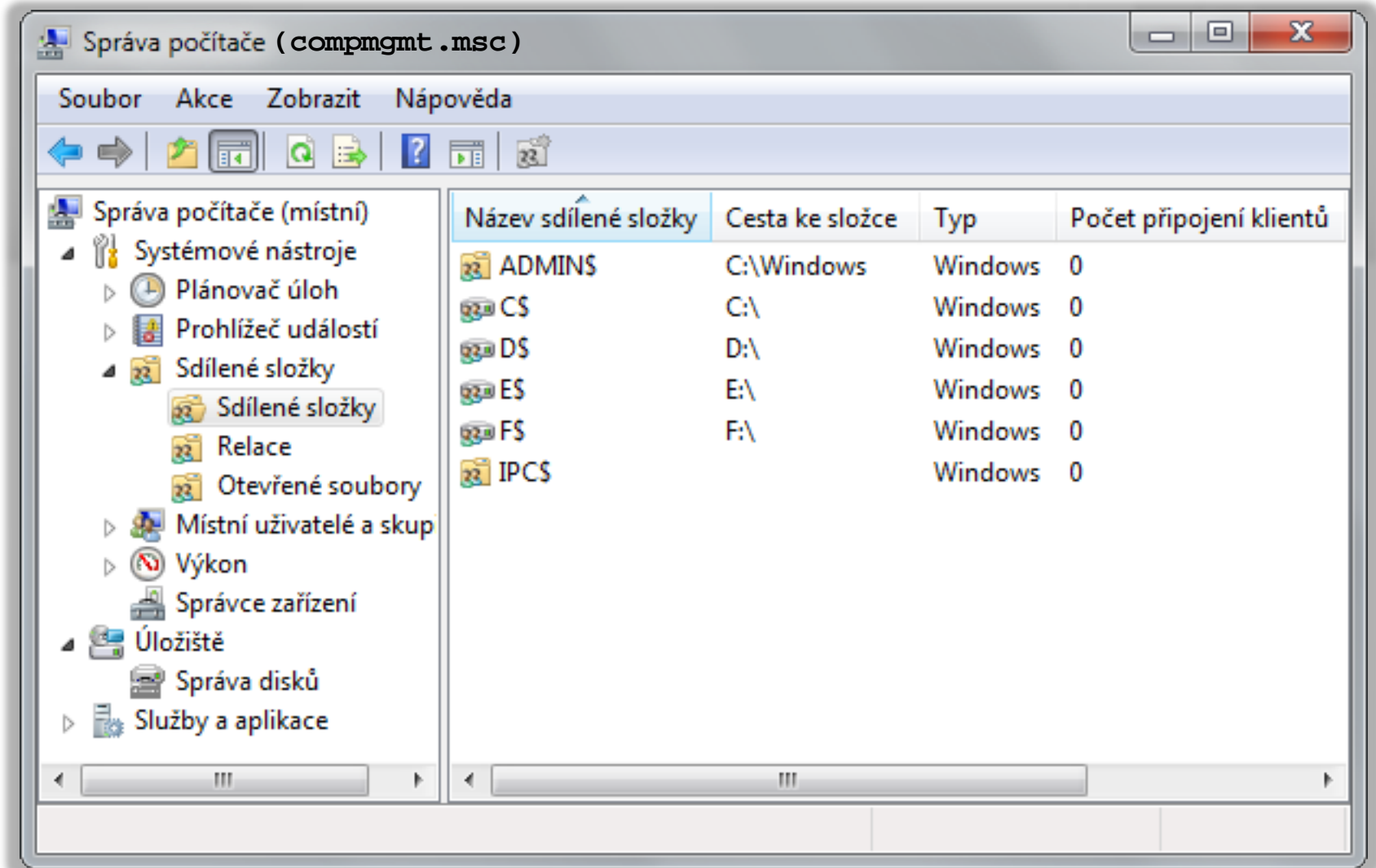
Skryté sdílené adresáře

- Název **ukončen** znakem \$ (např. C\$)
- Nejsou viditelné při **prohledávání sítě**
 - Jsou **přístupné** pomocí **UNC cesty**
- UNC (*Uniform Naming Convention*) cesta
 - Popis **umístění** sdíleného zdroje **na síti**
 - Obecný tvar **\\<server>\<sdílení>\<zdroj>**

Speciální sdílené adresáře

- Vytvářeny **automaticky** systémem **Windows**
 - Vždy **skryté**
 - Přístupné **pouze** uživatelům s **oprávněními správce**
- **ADMIN\$**
 - Sdílení **kořenového** adresáře **systému Windows**
- **IPC\$** (*Inter Process Communication*)
 - Sdílení souborů mezi počítači při **komunikaci procesů**
- **<jednotka>\$** pro **každý** připojený oddíl disku
 - Sdílení **kořenového** adresáře **oddílu disku**

Správa pomocí MMC konzole



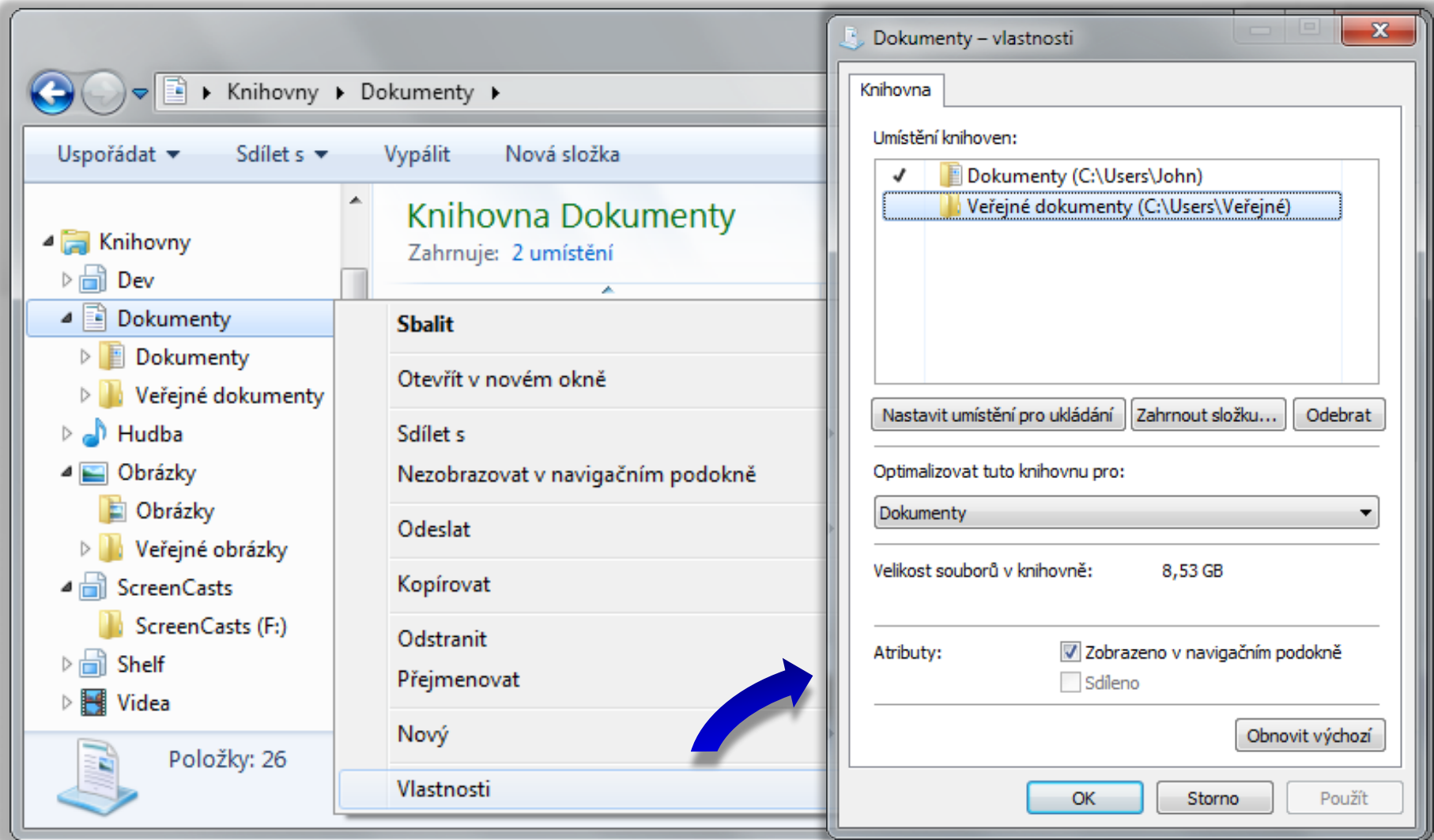
Správa pomocí příkazové řádky

- **Vypsání seznamu** sdílených adresářů na počítači
 - **net share**
- **Vypsání informací** o sdíleném adresáři
 - **net share <název>**
- **Vytvoření** nového sdíleného adresáře
 - **net share <název>=<lokální-cesta> [/users:<počet> | /unlimited] [/grant:<uživatel>,{read | change | full}]**
 - **Název** musí být **unikátní**
 - **Počet nesmí** být **0**

Knihovny (Libraries)

- **Virtuální adresáře** zahrnující jiné adresáře
 - Tvořeny **odkazy** na (**lokální** nebo **síťové**) adresáře
 - Fyzicky XML soubory s příponou **.library-ms**
- **Přístup** a **správa** pomocí **průzkumníka Windows**
 - Definice obsažených adresářů (a **výchozího** adresáře pro ukládání dat) ve vlastnostech dané knihovny
- Možnost **optimalizace** pro **konkrétní typy** dat
- Možnost **sdílení** (normálně nebo v rámci **domácí skupiny**)

Přístup ke knihovnám a jejich správa



Sdílení tiskáren

- Nastavení ve **vlastnostech tiskárny**
- 3 základní typy oprávnění
 - **Tisk** (a správa **vlastních** dokumentů v tiskové frontě)
 - **Správa této tiskárny** (změna nastavení a oprávnění tiskárny, sdílení tiskárny, pozastavení tiskárny, ...)
 - **Správa dokumentů** (správa **veškerých** dokumentů v tiskové frontě)
- Možnost dodat **ovladače** pro starší systémy
 - Automatické **stažení** a **instalace** při přidání tiskárny

Soubory offline (Offline Files)

- Přístup k **vybraným** souborům na nějaké síti **bez** nutnosti **připojení** k této síti
 - **Kešování** souborů na **lokálním** počítači
 - **Synchronizace** souborů při opětovném **připojení** k síti
- K dispozici u edicí **Professional** a **vyšších**
- Možnost **šifrování** dat ve vyrovnávací paměti

Povolení a nastavení souborů offline

- Povolení souborů offline v **Centru synchronizace**
- Výběr souborů, jenž budou k dispozici offline
 - **Manuálně** uživatele pomocí **průzkumníka Windows**
 - **Musí** být podporovány (resp. **povoleny**) na úrovni **adresáře** v **rozšířených možnostech sdílení**
 - **Automaticky** povolením na úrovni **adresáře**
 - **Centrálně** pomocí **zásad skupiny**
- Vyloučení jednotlivých **typů** souborů
 - **Centrálně** pomocí **zásad skupiny**

Globální povolení souborů offline

The image shows a Windows Control Panel window with the 'Spravovat offline soubory' (Manage Offline Files) link highlighted in blue. A large blue arrow points from this link to the 'Offline soubory' (Offline Files) dialog box. The dialog box is open and shows the 'Obecné' (General) tab. It contains the following text and buttons:

Offline soubory

Obecné | Využití disku | Šifrování | Síť

Pomocí offline souborů lze v místním počítači uchovávat kopie souborů uložených v síti. To umožňuje pracovat s nimi i v době, kdy nejste připojeni nebo server není dostupný.

Zakázat offline soubory

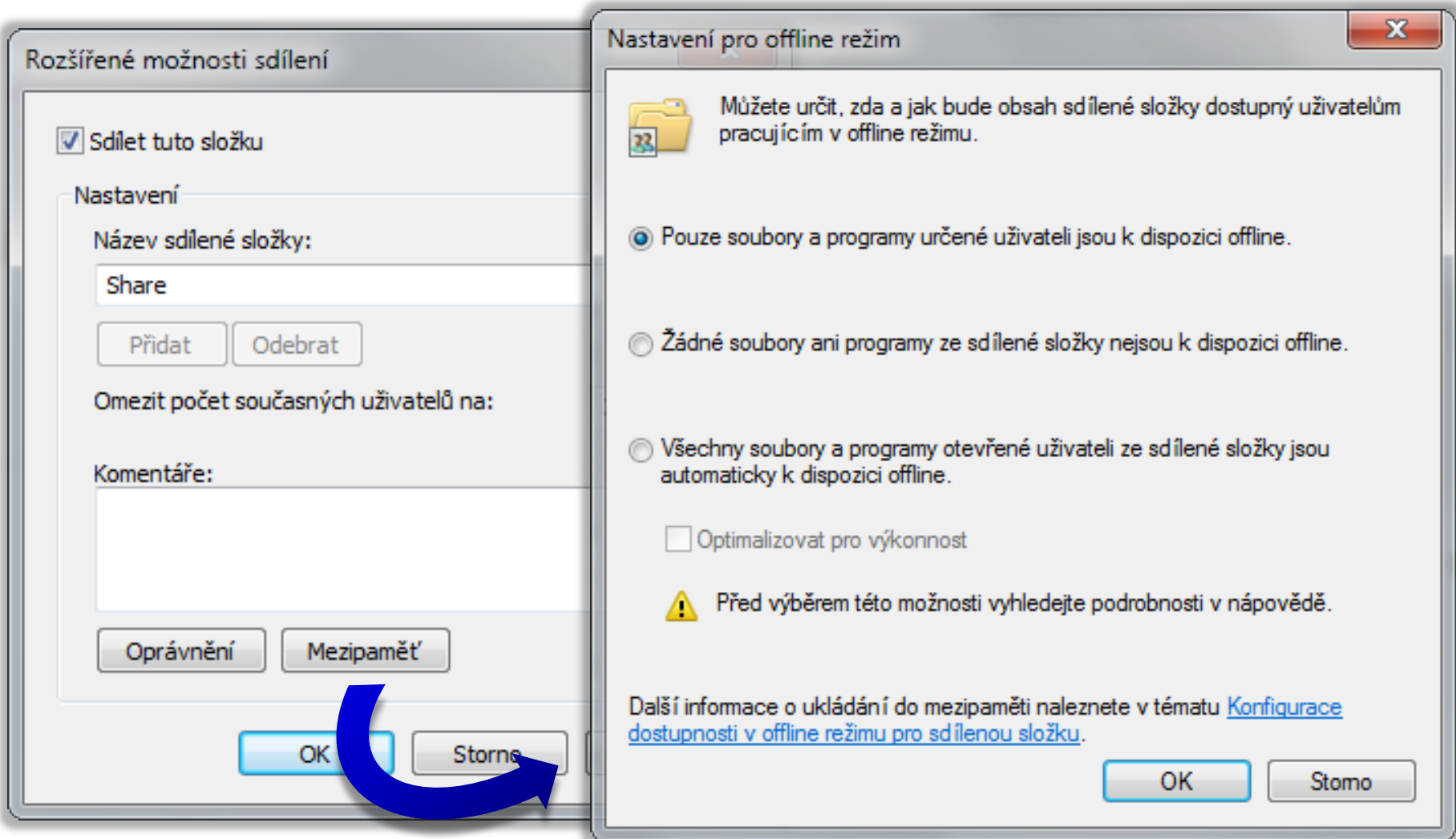
Funkce Offline soubory je právě povolena.

Centrum synchronizace použijte v případě, že chcete spustit synchronizaci offline souborů nebo vyhledat konflikty synchronizace.

[Informace o offline souborech](#)

OK Storno Použít

Povolení na úrovni sdíleného adresáře



Režimy souborů offline (1)

- Online režim
 - Čtení z **vyrovnávací paměti** (*cache*), zápis do **sdílení**
 - Synchronizace prováděna **automaticky**
- Automatický offline režim
 - Čtení a zápis do **vyrovnávací paměti** (*cache*)
 - Ověřování připojení do sítě co 2 minuty

Režimy souborů offline (2)

- Manuální offline režim
 - Čtení a zápis do **vyrovnávací paměti** (*cache*)
 - Ověřování **neprobíhá**
 - **Zapnutí** / **vypnutí** v **průzkumníkovi Windows**
- Režim pomalé linky (*slow-link*)
 - Čtení a zápis do **vyrovnávací paměti** (*cache*)
 - **Povolen** automaticky při **pomalém** připojení do sítě (**práh** lze nastavit ve **zásadách skupiny**)
 - Pouze **manuální** synchronizace

Synchronizace

- Probíhá **automaticky** nebo **manuálně**
- Řešení **konfliktů** při synchronizaci
 - Ponechání **lokální** verze (**přepsání** verze ve sdílení)
 - Ponechání verze **ve sdílení** (**přepsání** lokální verze)
 - Ponechání **obou** verzí (**přejmenování** lokální verze)

Řešení konfliktů při synchronizaci

Vyřešení konfliktu

Klikněte na verzi, kterou chcete zachovat.
Od poslední aktualizace byly obě verze aktualizovány.

- **Zachovat tuto verzi**
offline.txt.txt
V tomto počítači
Velikost: 9 bajtů
Datum změny: 10/31/2011 6:26 PM
- **Zachovat tuto verzi**
offline.txt.txt
\\WIN7E-SECOND\Share
Velikost: 9 bajtů
Datum změny: 10/31/2011 6:27 PM (novější)
- **Zachovat obě verze**
(Nejvyšší verze bude přejmenována offline.txt (Meda Beda v1).txt.)

[Jak odstranit konflikty synchronizace?](#)

Storno

Zabezpečení zdrojů

- Oprávnění
 - Sdílení
 - Souborového systému NTFS
 - Tiskáren
- Šifrování
 - EFS (*Encrypted File System*)
 - BitLocker

NTFS oprávnění

- Zabezpečení na úrovni **přístupů** k datům
- Lze nastavovat **lokálním** i **doménovým** skupinám a uživatelům
- **Nelze** použít u souborových systémů FAT a FAT32
- Ověřovány i při přístupu ze **sítě**
- Uloženy v **ACL seznamech** (*Access Control Lists*)

Skupiny NTFS oprávnění

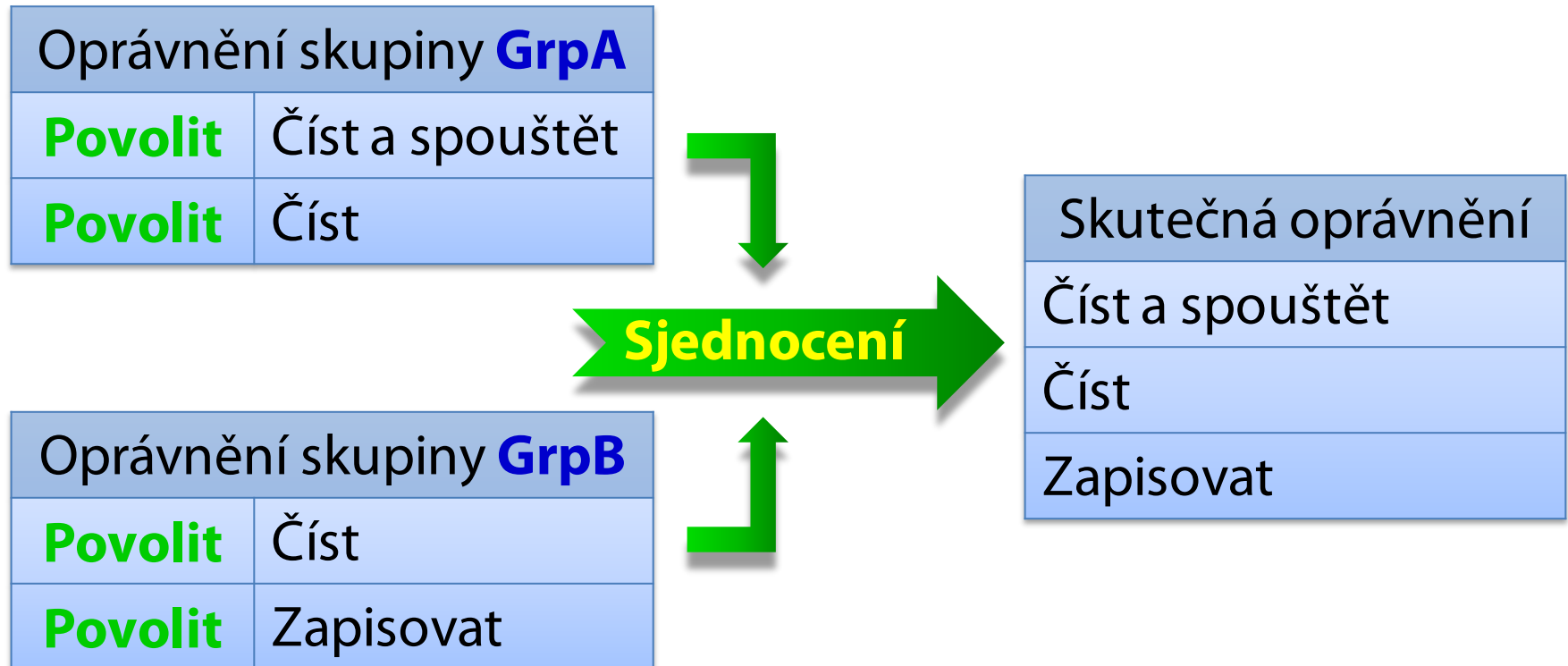
Oprávnění	Zdroj	Popis
Úplné řízení	Adresář	Zobrazení a přístup k obsahu, vytváření souborů a adresářů, změny oprávnění, odstraňování souborů a adresářů
	Soubor	Čtení, zápis, úpravy a odstraňování, změny oprávnění
Měnit	Adresář	Zobrazení a přístup k obsahu, vytváření souborů a adresářů
	Soubor	Čtení, zápis, úpravy a odstraňování
Číst a spouštět	Adresář	Přístup k obsahu (ne jeho zobrazení) a jeho spouštění
	Soubor	Přístup k souboru a jeho spouštění
Zobrazovat obsah složky	Adresář	Zobrazení obsahu
Číst	Adresář	Přístup k obsahu (ne jeho zobrazení)
	Soubor	Přístup k souboru
Zapisovat	Adresář	Vytváření souborů a adresářů (ne jejich odstraňování)
	Soubor	Zápis a úpravy (ne odstraňování)

Výpočet skutečných NTFS oprávnění

- Každé oprávnění lze **povolit** nebo **odepřít**
 - **Odepření** má vždy **vyšší** prioritu (**přepisuje** **povolení**)
- Obecný algoritmus
 - 1) Vytvoř **prázdnou** množinu oprávnění **S**
 - 2) **Přidej** do množiny **S** oprávnění, která jsou **povolená** pro daného uživatele nebo skupinu, jenž je členem
 - 3) **Odeber** z množiny **S** oprávnění, která jsou **odepřena** pro daného uživatele nebo skupinu, jenž je členem
 - 4) Vrať oprávnění **obsažená** v množině **S**

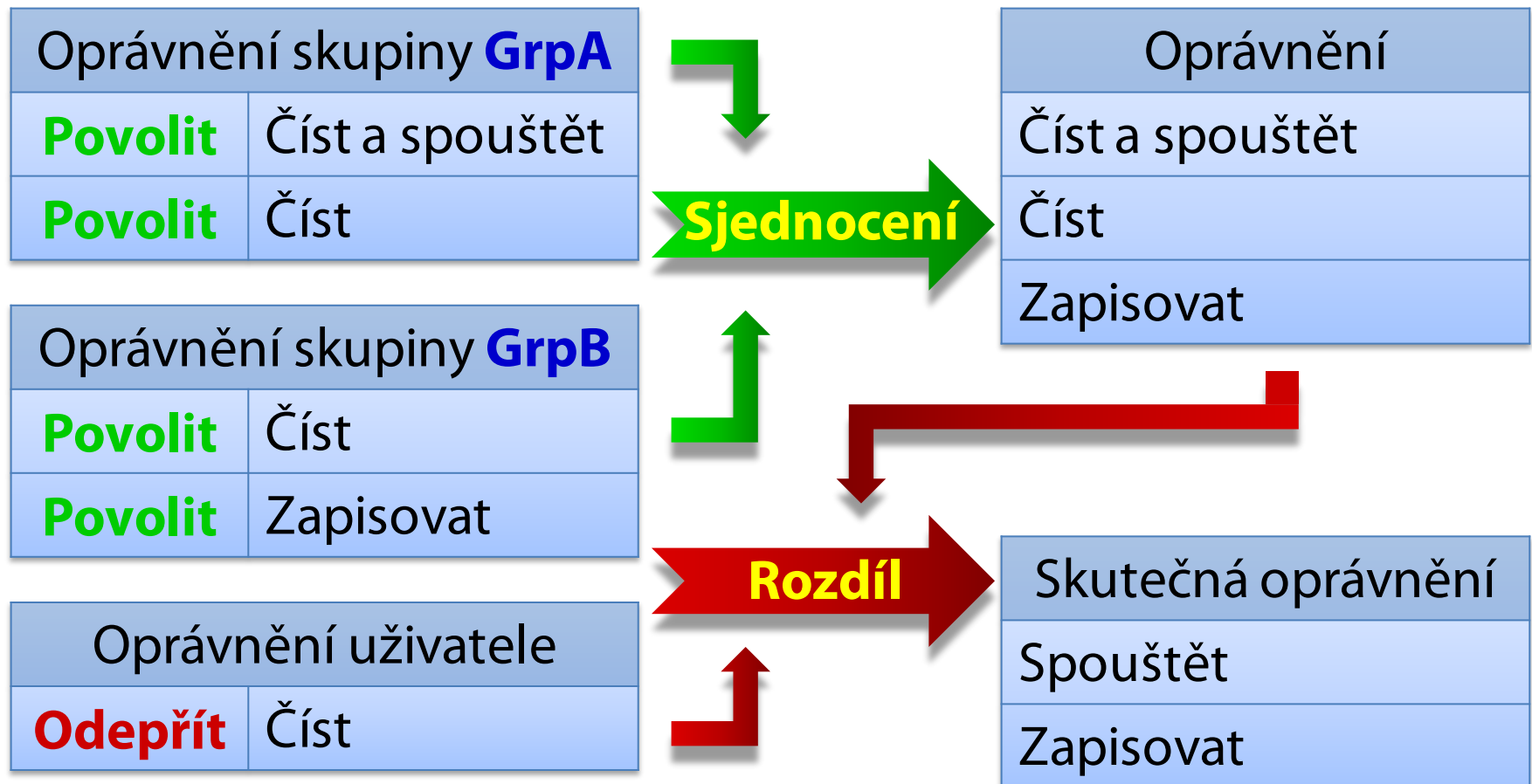
Příklad s povolením (allow) oprávnění

- Uživatel je členem skupin **GrpA** a **GrpB**

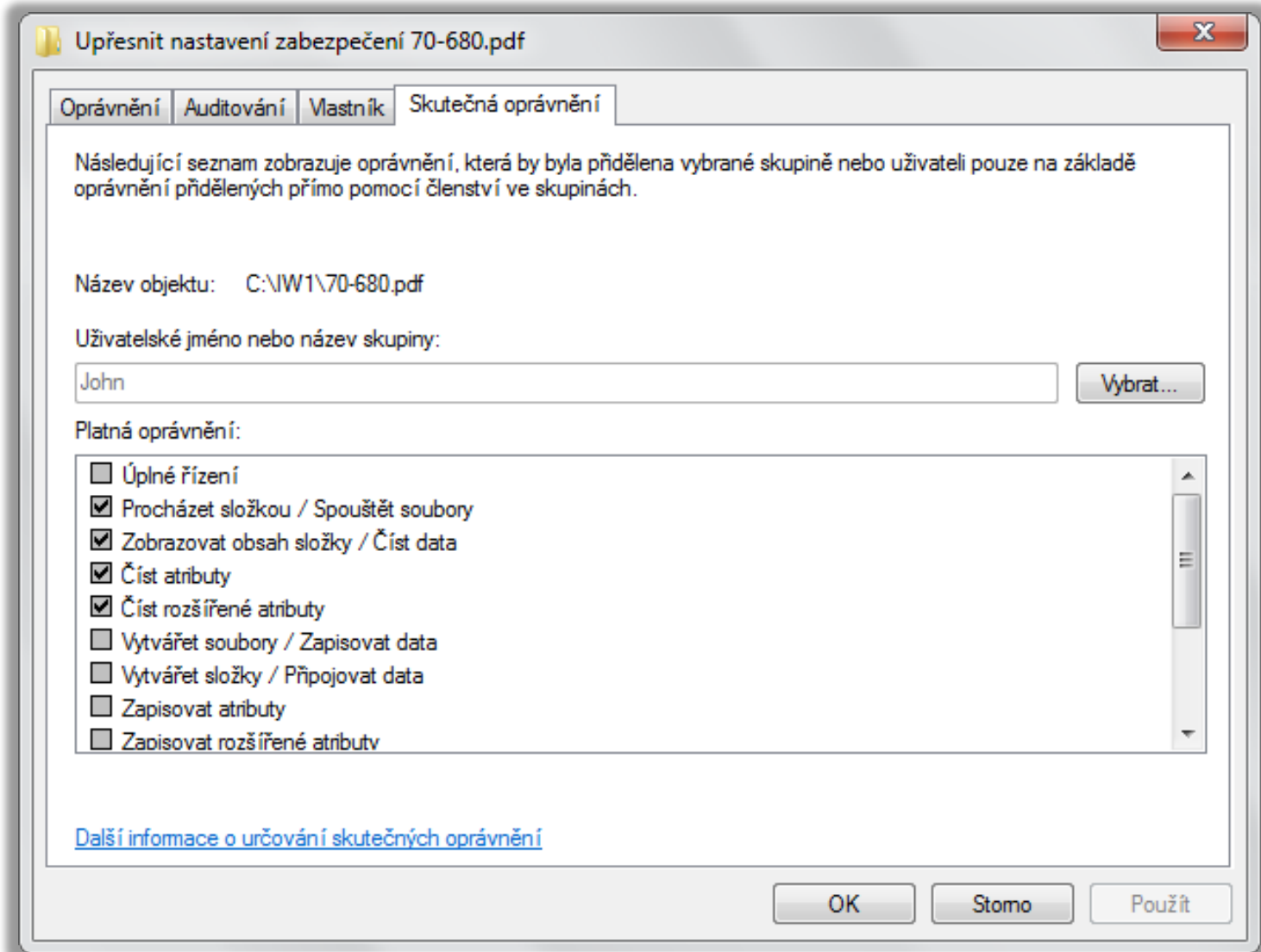


Příklad s odepřením (deny) oprávnění

- Uživatel je členem skupin **GrpA** a **GrpB**



Zjištění skutečných NTFS oprávnění



Dědičnost NTFS oprávnění

- **Nově vytvářené** soubory a adresáře dědí NTFS oprávnění **adresáře**, ve kterém byly vytvořeny
- Lze **zakázat** ve vlastnostech souboru/adresáře
 - **Zkopírování** zděděných NTFS oprávnění
 - **Odstranění** zděděných NTFS oprávnění
- Lze **vynutit** dědičnost na **podřízených** souborech a adresářích (*child objects*)
 - **Přepsání** NTFS oprávnění u podřízených objektů
 - Uživatel **musí** být schopen **měnit oprávnění**

Správa pomocí příkazové řádky

- **Výpis** NTFS oprávnění
 - `icacls <subor/adresář>`
- **Změna** NTFS oprávnění
 - **Povolení**
 - `icacls <subor/adresář> /grant <uživatel>:<oprávnění>`
 - **Odepření**
 - `icacls <subor/adresář> /deny <uživatel>:<oprávnění>`
 - Oprávnění mohou být jak **skupiny**, tak **konkrétní** NTFS oprávnění (odděleny čárkami a uvedeny v závorce)

Kopírování a přesun

- Standardní chování

	V rámci stejného oddílu	Mezi různými oddíly	Na oddíl FAT/FAT32
Přesun	Zachovává oprávnění	Dědí oprávnění od cílového adresáře	Nezachovává oprávnění
Kopírování	Dědí oprávnění od cílového adresáře	Dědí oprávnění od cílového adresáře	Nezachovává oprávnění

- Při použití nástroje **robocopy**

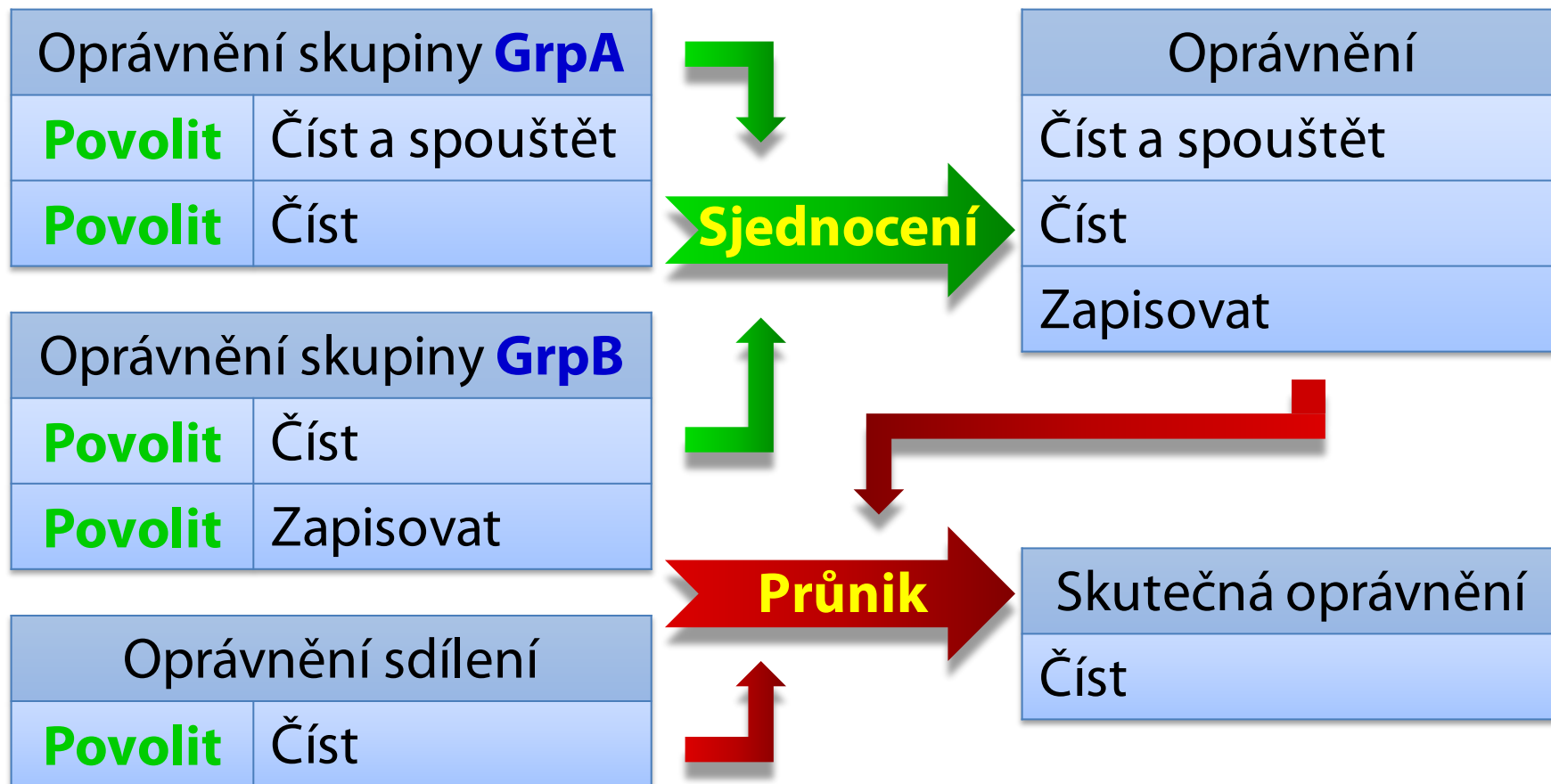
	V rámci stejného oddílu	Mezi různými oddíly	Na oddíl FAT/FAT32
Přesun	Zachovává oprávnění	Zachovává oprávnění	Nezachovává oprávnění
Kopírování	Zachovává oprávnění	Zachovává oprávnění	Nezachovává oprávnění

Vypočet oprávnění při přístupu ze sítě

- Ověřují se **oprávnění sdílení** i **NTFS oprávnění**
- Obecný algoritmus
 - 1) Vypočti množinu skutečných **oprávnění sdílení**
 - 2) Vypočti množinu skutečných **NTFS oprávnění**
 - 3) Vrať oprávnění obsažená v **obou** množinách

Příklad s oprávněními sdílení (share)

- Uživatel je členem skupin **GrpA** a **GrpB**



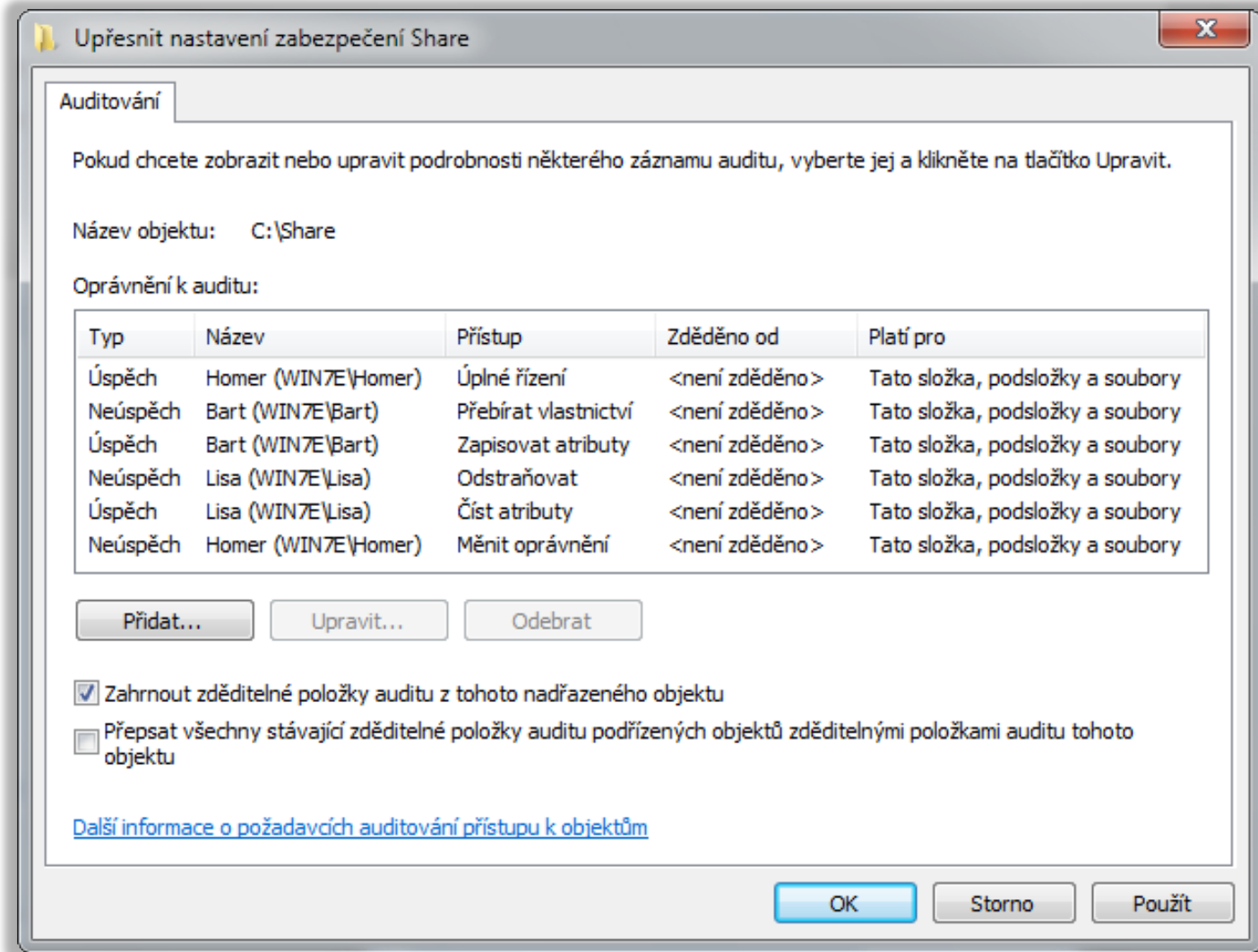
Auditování přístupu ke zdrojům

- Monitorování **přístupu** k souborům a adresářům
 - **Uložení** informací o přístupech v protokolu událostí (protokol **Zabezpečení**)
- **Povolení** v zásadách skupiny
 - Zásada **Auditovat přístup k objektům**
 - Od **Windows Vista** lze povolovat auditování jednotlivých typů objektů (musí se **explicitně** povolit)
 - Lze monitorovat **úspěšné** a/nebo **neúspěšné** pokusy
 - Pouze **umožňuje** monitorovat přístup k **souborům** a **adresářům**

Nastavení auditování

- **Nastavení** ve vlastnostech jednotlivých souborů a adresářů (**zapnutí** monitorování)
 - Výběr **oprávnění**, jejichž **aplikace** (čtení, zápis, apod.) má být monitorována a zaznamenána
 - Výběr **uživatelů** a **skupin**, kteří mají být monitorováni (pro monitorování **všech** uživatelů a skupin lze použít skupinu **Everyone**)

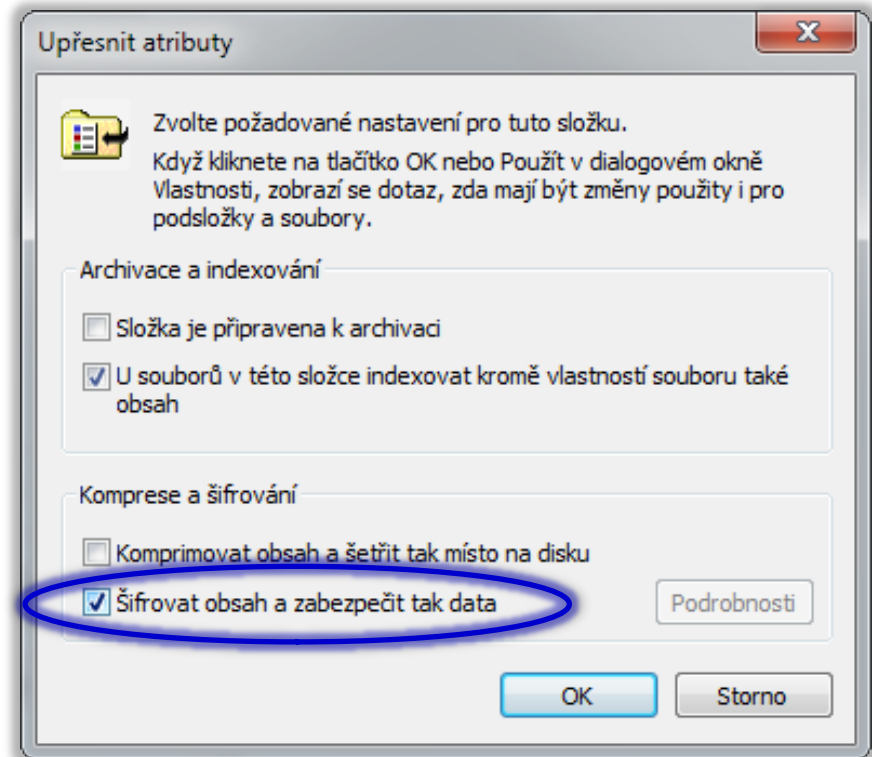
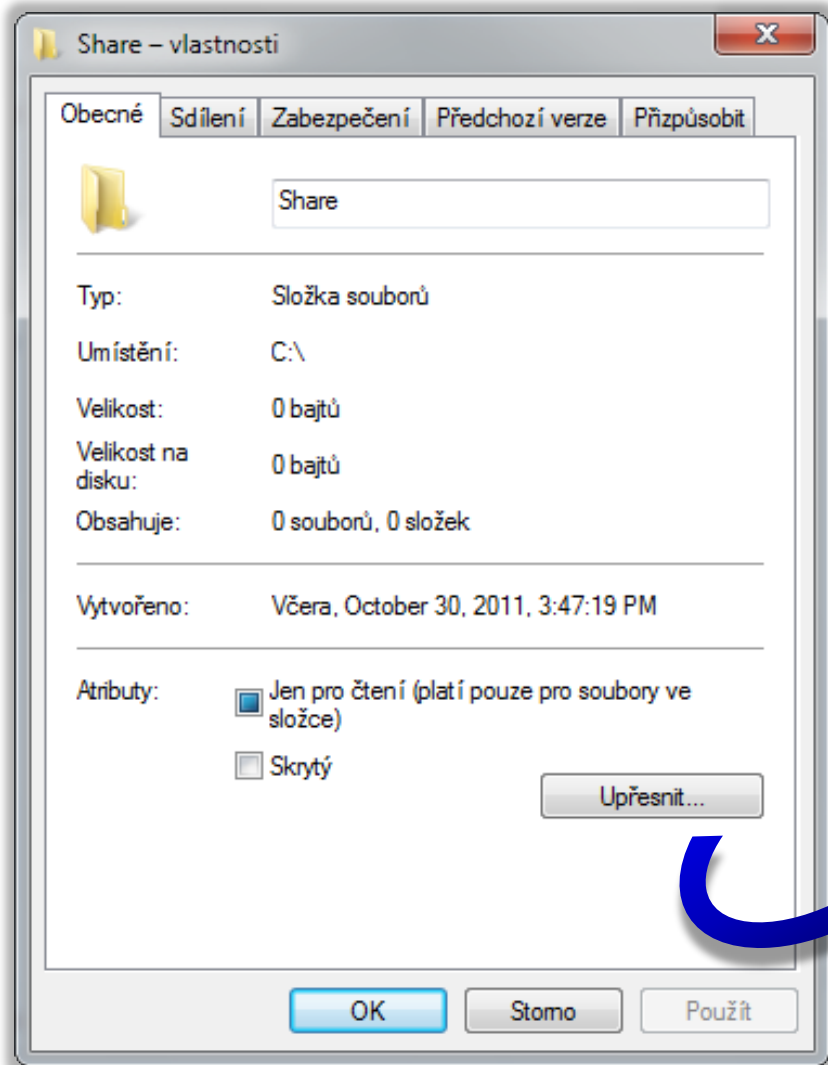
Výběr monitorovaných oprávnění



EFS (Encrypted File System)

- Pouze u edicí **Professional** a **vyšších**
- Šifrování jednotlivých **souborů**
 - Zabezpečení na úrovni **dat**
 - Šifrování na úrovni **uživatele**
 - **Nelze** šifrovat systémové soubory
- Služba **souborového systému NTFS**
 - **Nelze** použít u souborových systémů FAT ani FAT32
- **Transparentní** uživateli
 - Práce s **šifrovanými** soubory stejná jako s normálními

Šifrování obsahu souboru



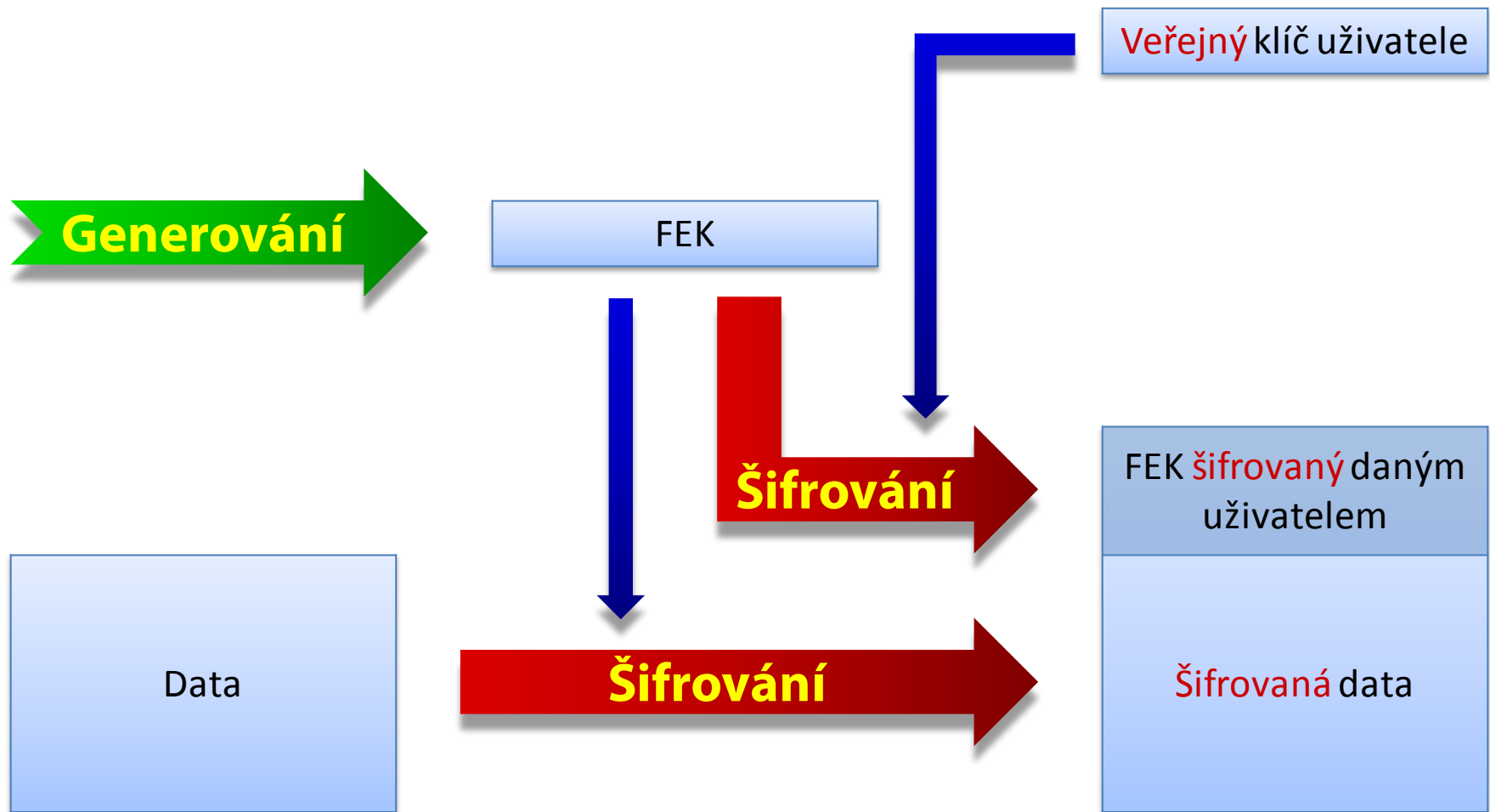
Šifrování

- Založeno na hybridní kryptografii
 - Data šifrována (a dešifrována) **sdíleným** klíčem (FEK, *File Encryption Key*) pomocí **symetrické** kryptografie
 - FEK klíč šifrován **veřejným** (a dešifrován **privátním**) klíčem **uživatele** pomocí **asymetrické** kryptografie
- Výhody hybridní kryptografie
 - **Rychlé** šifrování dat (**symetrická** kryptografie)
 - **Bezpečné** sdílení FEK klíče (**asymetrická** kryptografie)
 - **Jednoduchá** (a také **efektivní**) realizace přístupu **více** uživatelů k šifrovaným souborům

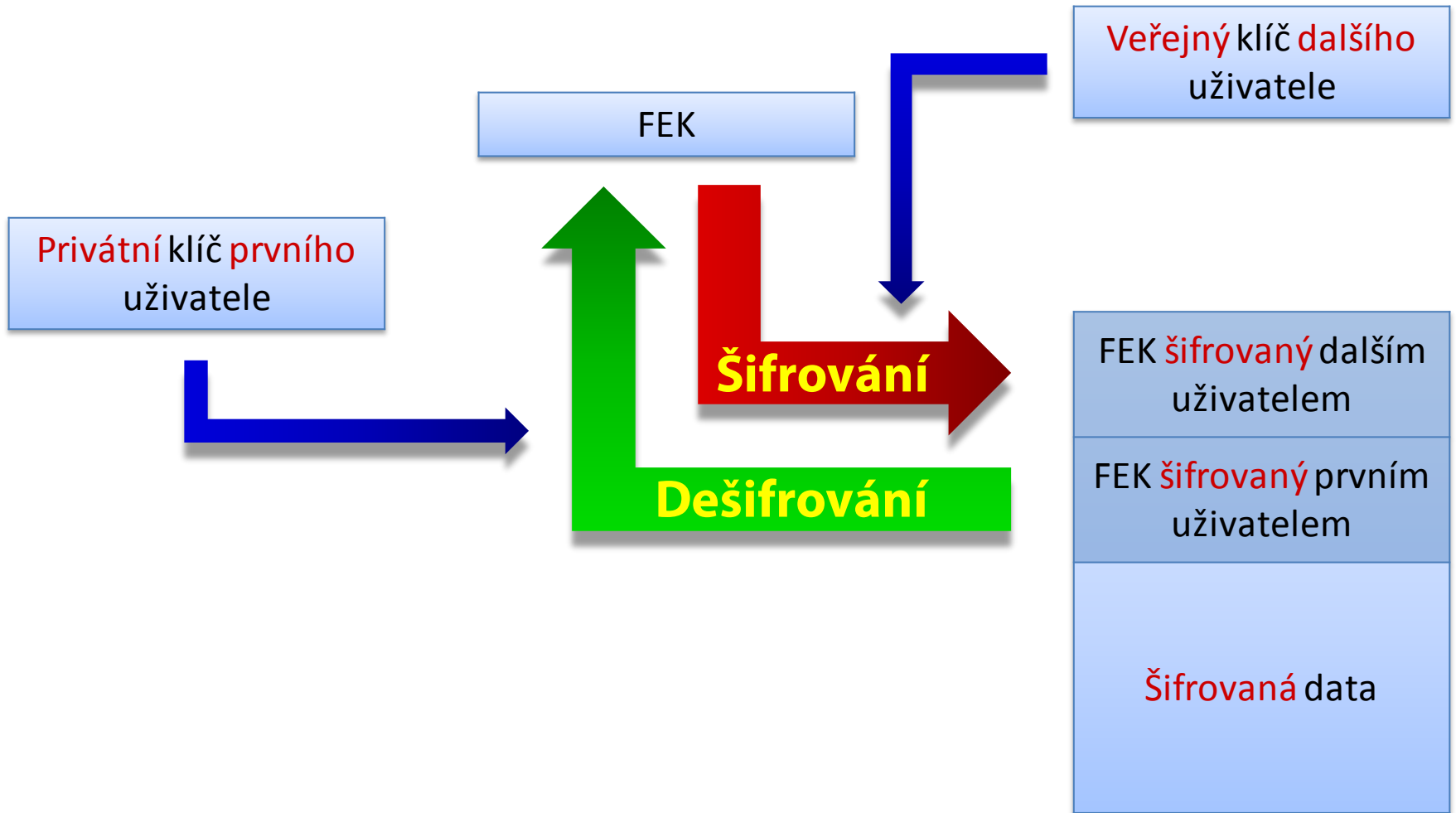
Klíče

- FEK klíč (*File Encryption Key*)
 - Unikátní pro každý šifrovaný soubor
 - Generován při šifrování souboru prvním uživatelem
- Veřejný klíč (*public key*)
 - Uložen ve formě certifikátu v úložišti certifikátů
 - K dispozici všem uživatelům
- Privátní klíč (*private key*)
 - Uložen ve formě certifikátu v úložišti certifikátů
 - K dispozici pouze danému uživateli

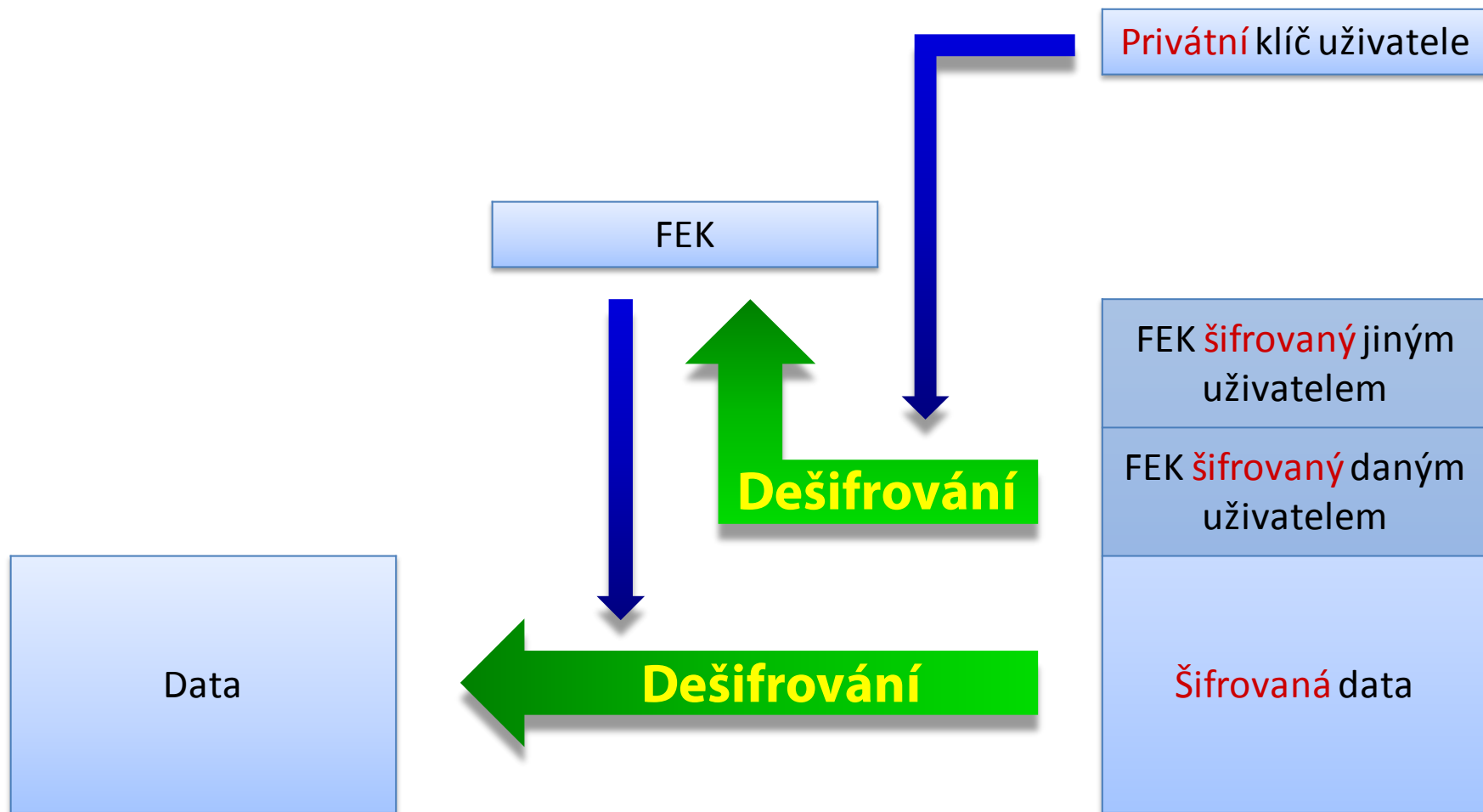
Šifrování souboru prvním uživatelem



Šifrování souboru dalším uživatelem



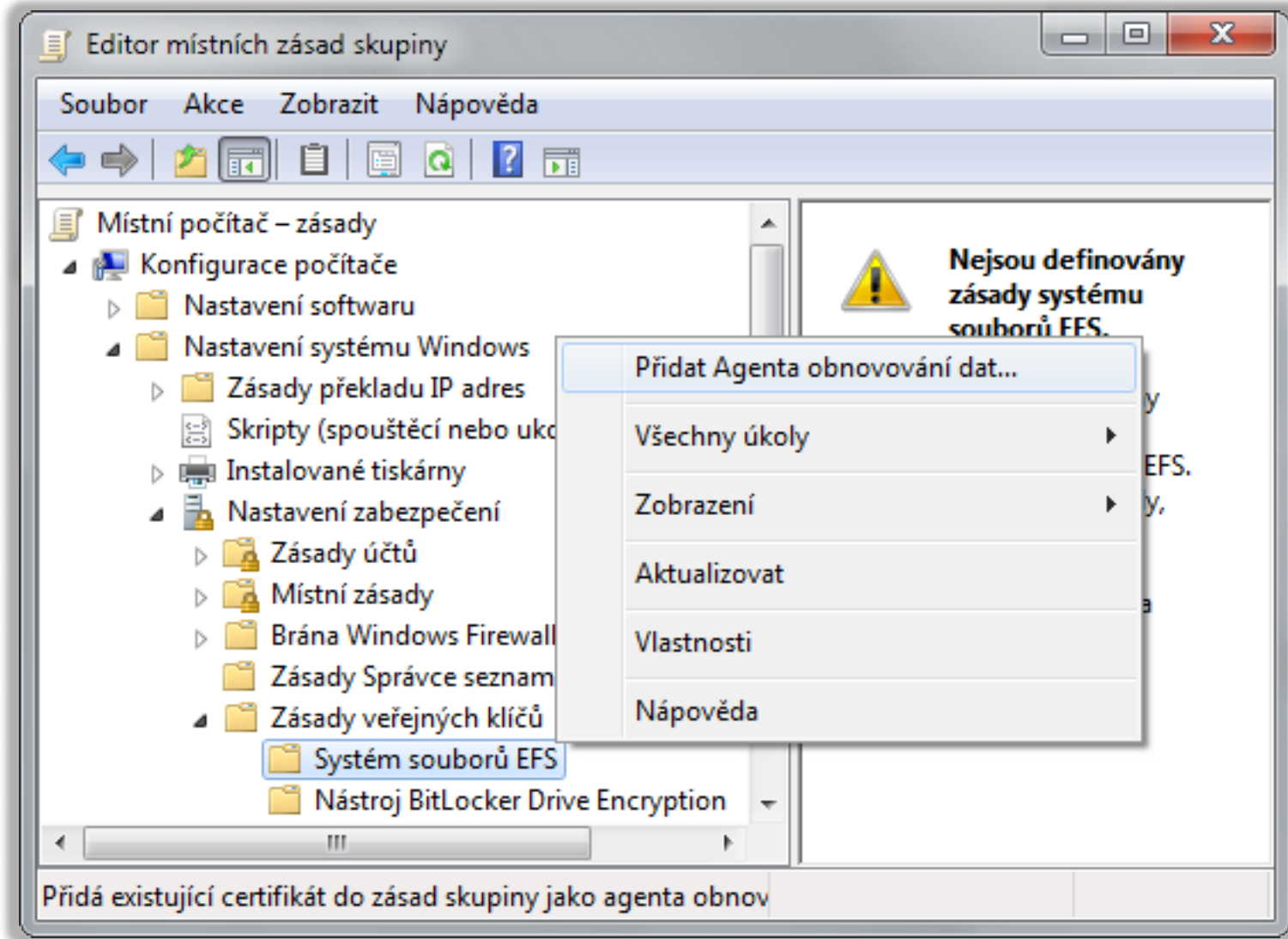
Dešifrování souboru uživatelem



Agent obnovení (RA, Recovery Agent)

- Umí **dešifrovat jakákoliv** data zašifrovaná pomocí EFS v době **po jeho vytvoření**
 - Při šifrování je FEK klíč (navíc) **automaticky** zašifrován pomocí **veřejného** klíče **agenta obnovení**
 - Zašifrování dříve vytvořených FEK klíčů pomocí **cipher /u**
- **Vytvoření** agenta obnovení
 - 1) Vygenerování **veřejného** a **privátního** klíče **agenta obnovení** (certifikátu) pomocí **cipher /r:<název>**
 - 2) Vytvoření **agenta obnovení** (RA) v zásadách skupiny **importováním** certifikátu obsahujícího **veřejný** klíč

Vytvoření agenta obnovení



BitLocker

- Pouze u edicí **Enterprise** a **Ultimate**
- Šifrování celých **oddílů disků**
 - Zabezpečení na úrovni **dat**
 - Šifrování na úrovni **počítače**
 - **Lze** šifrovat i systémový oddíl (systémové soubory)
- Chrání **integritu** operačního systému
 - Nemožnost **externí** modifikace systémových souborů
- Pro **šifrování** a **dešifrování** se používá **sdílený** klíč (FVEK, *Full Volume Encryption Key*)

Základní pojmy

- TPM (*Trusted Platform Module*)
 - Speciální **čip** (většinou na základní desce) pro uložení celého (nebo části) **FVEK klíče**
- PIN (*Personal Identification Number*)
 - **Heslo** ověřované při **startu** počítače
 - Uloženo v **TPM čipu** nebo na **klíči pro start**
- Klíč pro start (*Startup key*)
 - **Zařízení USB** obsahující soubor celý (nebo část) **FVEK klíče** (tzv. *keying material*)

Jen TPM

- Klíč pro dešifrování dat je uložen na **TPM čipu**
 - **Nejméně** bezpečný režim (**celý** FVEK v TPM čipu)
- Plně **transparentní** uživateli
 - Dešifrování obsahu probíhá **automaticky**
- **Chrání** proti
 - Zpřístupnění dat při odcizení pevného disku
 - Změně nebo úpravám bootovacího prostředí
- **Nechrání** proti
 - Zpřístupnění dat při odcizení počítače

TPM + PIN a/nebo klíč pro start

- Při použití TPM pouze s **PINem**
 - Uložení **celého** FVEK klíče i PINu v **TPM čipu**
- Při použití TPM s **klíčem pro start** a/nebo **PINem**
 - Uložení **½** FVEK klíče v **TPM čipu** a **½** na **klíči pro start**
 - Při použití PINu je PIN uložen na **klíči pro start**
- **Chrání** proti
 - Zpřístupnění dat při odcizení pevného disku
 - Zpřístupnění dat při odcizení počítače
 - Změně nebo úpravám bootovacího prostředí

BitLocker bez TPM

- **Celý** FVEK klíč je uložen na **klíči pro start**
 - Klíč **není** nijak chráněn (**žádné** šifrování apod.)
- **Chrání** proti
 - Zpřístupnění dat při odcizení pevného disku
 - Zpřístupnění dat při odcizení počítače
- **Nechrání** proti
 - Změně nebo úpravám bootovacího prostředí

Dešifrování oddílu (při použití TPM)

- 1) Aktualizace PCR registrů TPM čipu
- 2) Dešifrování (celého nebo ½) FVEK klíče pomocí klíče daného obsahem PCR registrů TPM čipu
 - Při jakékoliv změně bootovacího prostředí (procesu bootování) nebude možné FVEK klíč dešifrovat
- 3) Doplnění 2. ½ FVEK klíče z klíče pro start
- 4) Ověření PINu
- 5) Dešifrování obsahu oddílu disku pomocí FVEK klíče

Agent obnovení (Recovery Agent)

- Umí **dešifrovat** oddíly disku zašifrované pomocí technologie **BitLocker**
- Založen na **certifikátech**
 - Importování certifikátu s **veřejným** klíčem, jenž bude použit pro **zašifrování** FVEK klíče, v **zásadách skupiny**
 - Zašifrovaný VFEK klíč je uložen na **šifrovaném** oddíle
- **Obnovení** dat
 - **manage-bde.exe -unlock <oddíl> -Certificate -ct <otisk> [-PIN]**

BitLocker To Go

- BitLocker **umožňující** šifrování oddílů **USB disků**
- Lze **konfigurovat** v edicích **Enterprise** a **Ultimate**
 - **Číst** a **zapisovat** lze ve všech edicích **Windows 7**
 - U předchozích verzí systému Windows lze **pouze číst** (vyžaduje **BitLocker To Go Reader**)
- Data chráněná **heslem** nebo **čipovou kartou**
 - **Nepotřebuje** TPM čip
- Možnost **zakázat zápis** na USB disky **nechráněné** technologií BitLocker