

# Desktop systémy Microsoft Windows

IW1/XMW1 2012/2013

**Jan Fiedor**

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 29.10.2012

# Sdílení a zabezpečení prostředků

# Povolení sdílení prostředků

- 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 in the Windows Control Panel, titled 'Změnit možnosti sdílení pro různé síťové profily'. It has sections for 'Doma nebo Práce' and 'Zjišťování sítě'. Under 'Zjišťování sítě', the 'Zapnout zjišťování sítě' radio button is selected. Below that, the 'Sdílení souborů a tiskáren' section has the 'Zapnout sdílení souborů a tiskáren' radio button selected. The foreground window is titled 'Připojení k místní síti - vlastnosti' and shows the 'Síť' tab. It lists the network connection as 'Intel(R) PRO/1000 MT Network Connection'. Below this, a list of protocols is shown, with two items circled in blue: 'Klient sítě Microsoft' and 'Sdílení souborů a tiskáren v sítích Microsoft'. Both have their checkboxes checked. Other visible items include 'Microsoft Network Monitor 3 Driver', 'Plánovač paketů technologie QoS', and 'Protokol IP verze 6 (TCP/IPv6)'. Buttons for 'Nainstalovat...', 'Odinstalovat', 'Vlastnosti', 'OK', and 'Storno' are visible at the bottom of the foreground window.

Centrum síťových připojení a sdílení ► Pokročilé nastavení sdílení

## 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

### Připojení k místní síti - vlastnosti

Síť

Připojit pomocí:

Intel(R) PRO/1000 MT Network Connection

Konfigurovat...

Toto připojení používá následující položky:

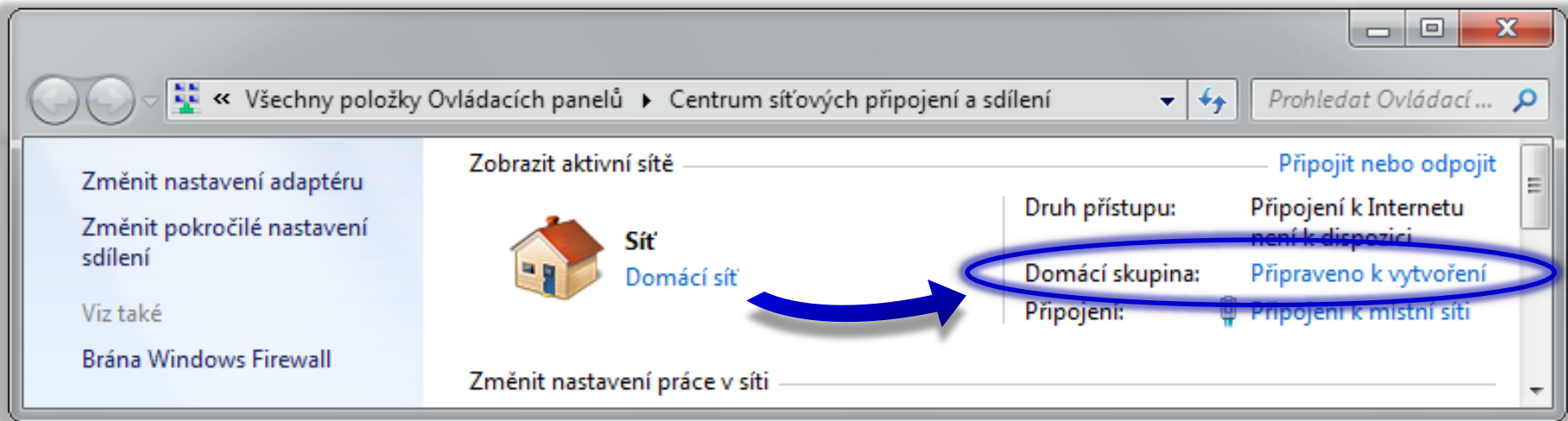
- Klient sítě Microsoft
- Microsoft Network Monitor 3 Driver
- Plánovač paketů technologie QoS
- Sdílení souborů a tiskáren v sítích Microsoft
- Protokol IP verze 6 (TCP/IPv6)
- Protokol IP verze 4 (TCP/IPv4)

Nainstalovat... Odinstalovat Vlastnosti

OK Storno

# Domácí skupiny (HomeGroups)

- Umožňují jednoduché sdílení souborů a tiskáren v systémech **Windows 7** a **novějších**
  - 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:

<input checked="" type="checkbox"/> Obrázky	<input type="checkbox"/> Dokumenty
<input checked="" type="checkbox"/> Hudba	<input checked="" type="checkbox"/> Tiskárny
<input checked="" type="checkbox"/> Videa	

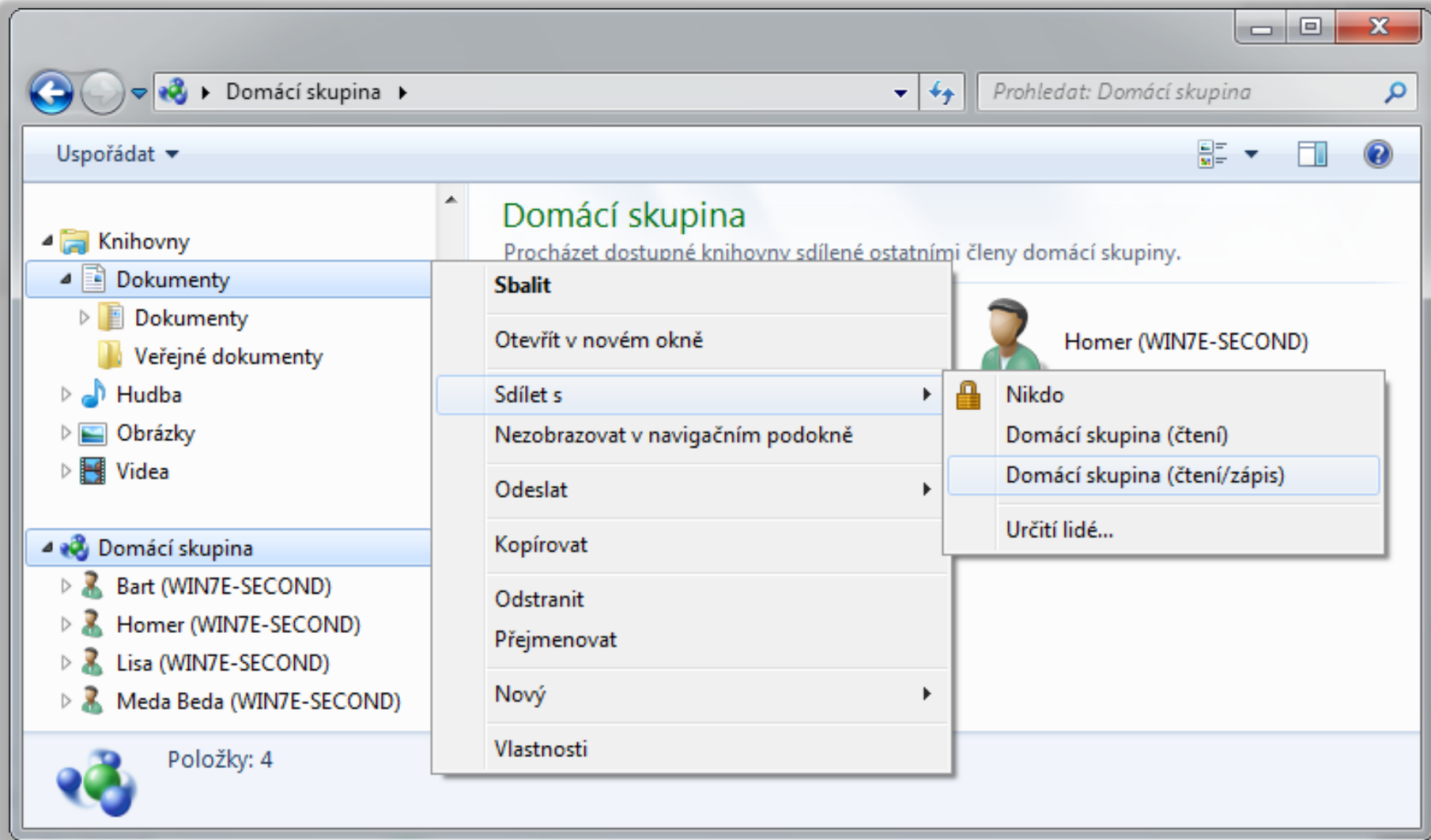
**Další** **Storno**

Připraveno k vytvoření

# 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

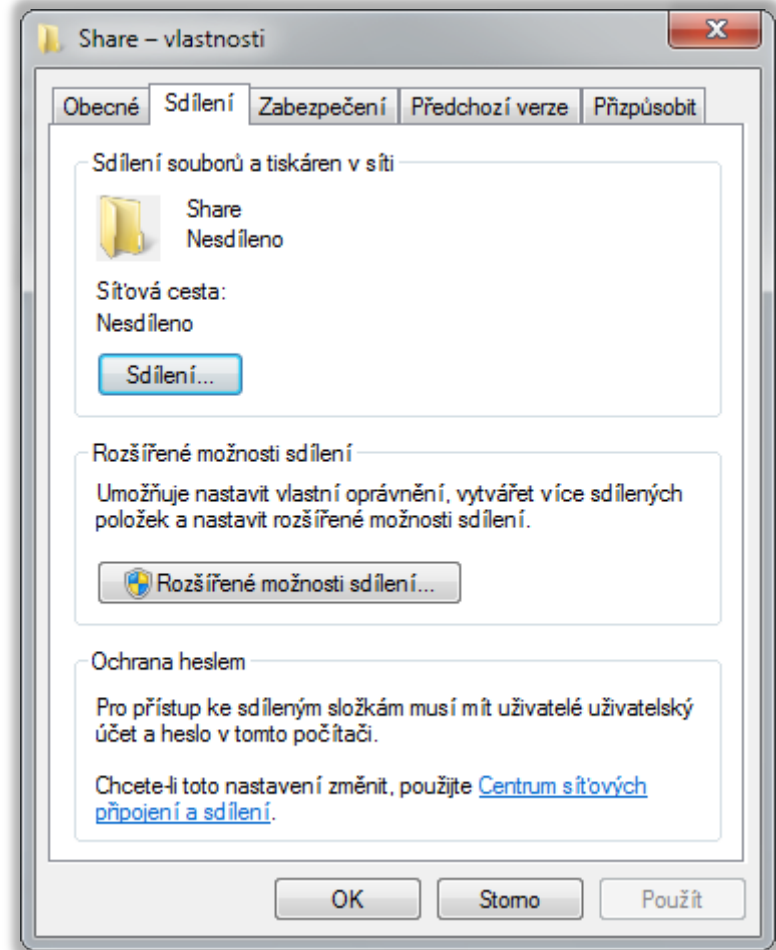
# Sdílení adresářů v domácí skupině





# 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 (zahrnuje i spouštění)
  - 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 titled 'Share - vlastnosti' (Share - properties) and shows the 'Sdílení' (Sharing) tab. It displays a folder named 'Share' with the status 'Nesdíleno' (Not shared). A blue arrow points from the 'Sdílení...' button in this window to the foreground window.

The foreground window is titled 'Sdílení souborů' (Share files) and contains the following text and elements:

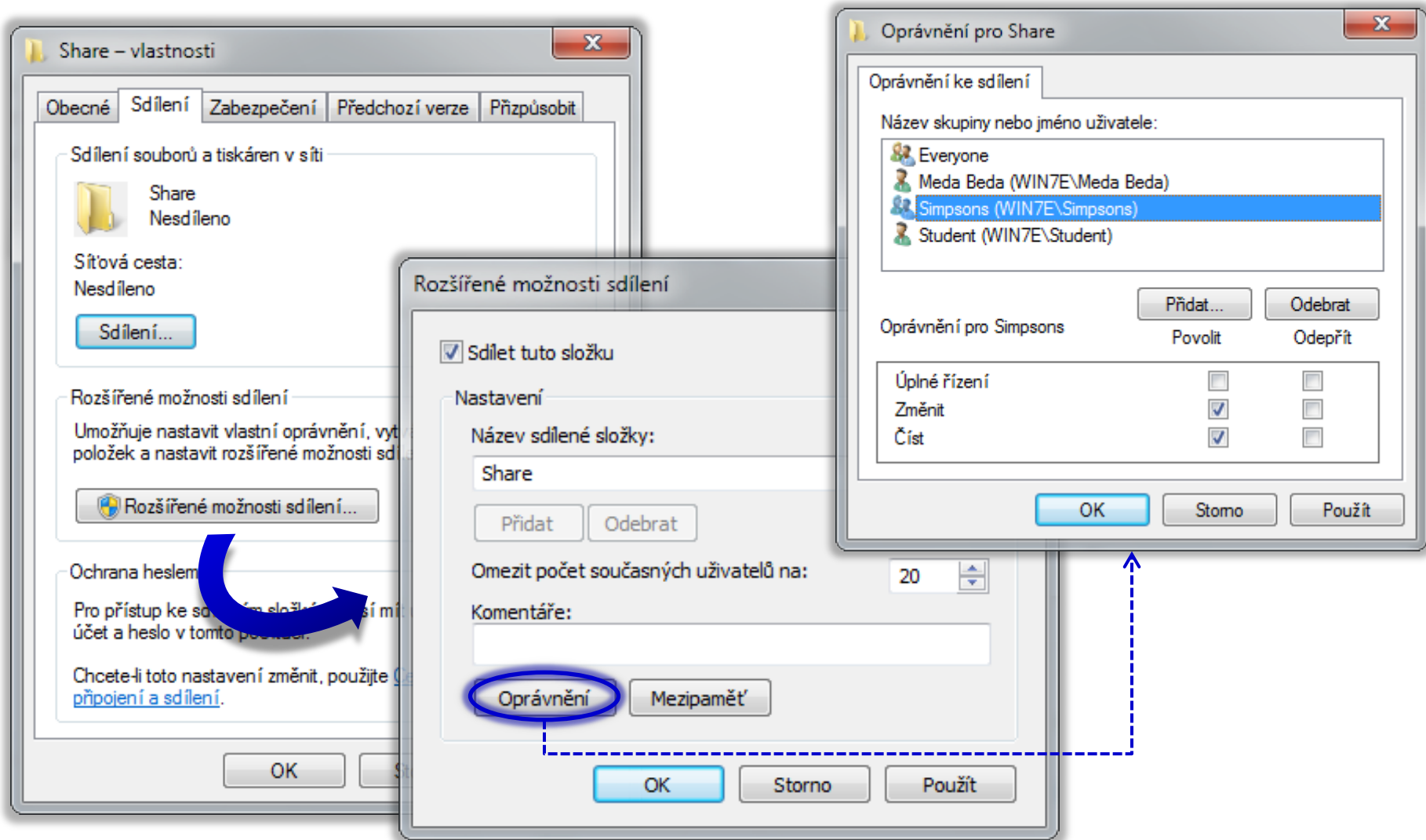
- Header: 'Zvolte osoby pro sdílení.' (Choose people to share with.)
- Instruction: 'Zadejte jméno a klikněte na tlačítko Přidat nebo uživatele vyhledejte kliknutím na šipku.' (Enter a name and click the Add button or find a user by clicking the arrow.)
- A search input field with a dropdown arrow and a 'Přidat' (Add) button.
- A table with two columns: 'Jméno' (Name) and 'Úroveň oprávnění' (Permission level).
- A context menu is open over the 'Student' row, showing options: 'Čtení' (Read) with a checkmark, 'Čtení/zápis' (Read/Write), and 'Odebrat' (Remove).
- Buttons at the bottom: 'Sdílet' (Share) and 'Storno' (Cancel).
- A link at the bottom: 'Problémy se sdílením' (Share problems).

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

# Pokročilé sdílení adresářů

- Rozlišuje 3 typy oprávnění
  - Číst (zahrnuje i spouštění)
  - 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



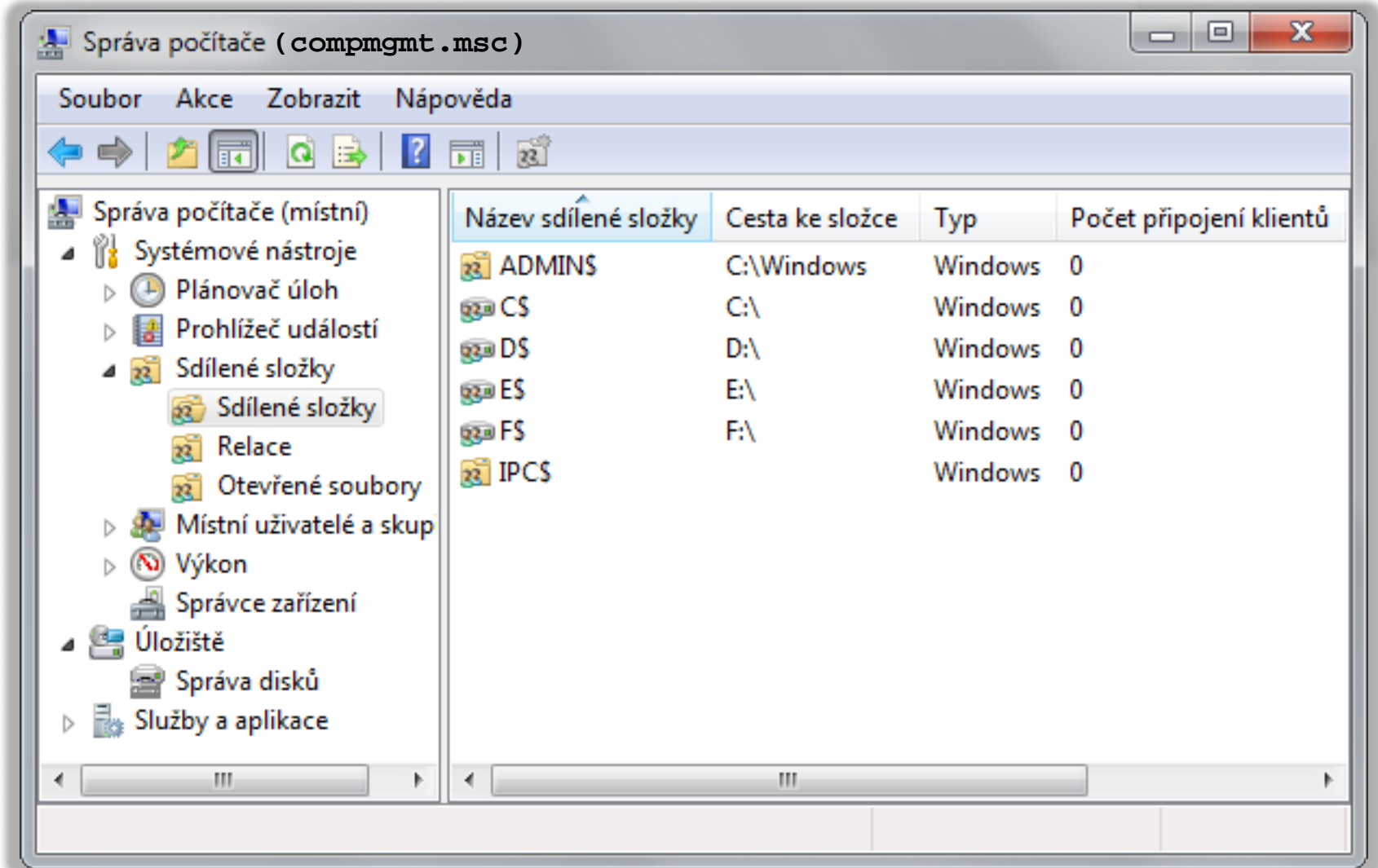
# Skryté sdílené adresáře

- Název **ukončen** znakem \$ (např. C\$)
- Nejsou viditelné při **prohledávání sítě**
  - Jsou **přístupné** pomocí **UNC cesty**
- UNC (*Uniform Naming Convention*) cesta
  - Popis **umístění** sdíleného prostředku **na síti**
  - Obecný tvar **\\<server>\<sdílení>\<prostředek>**
    - Prostředkem může být např. adresář, soubor nebo tiskárna

# 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





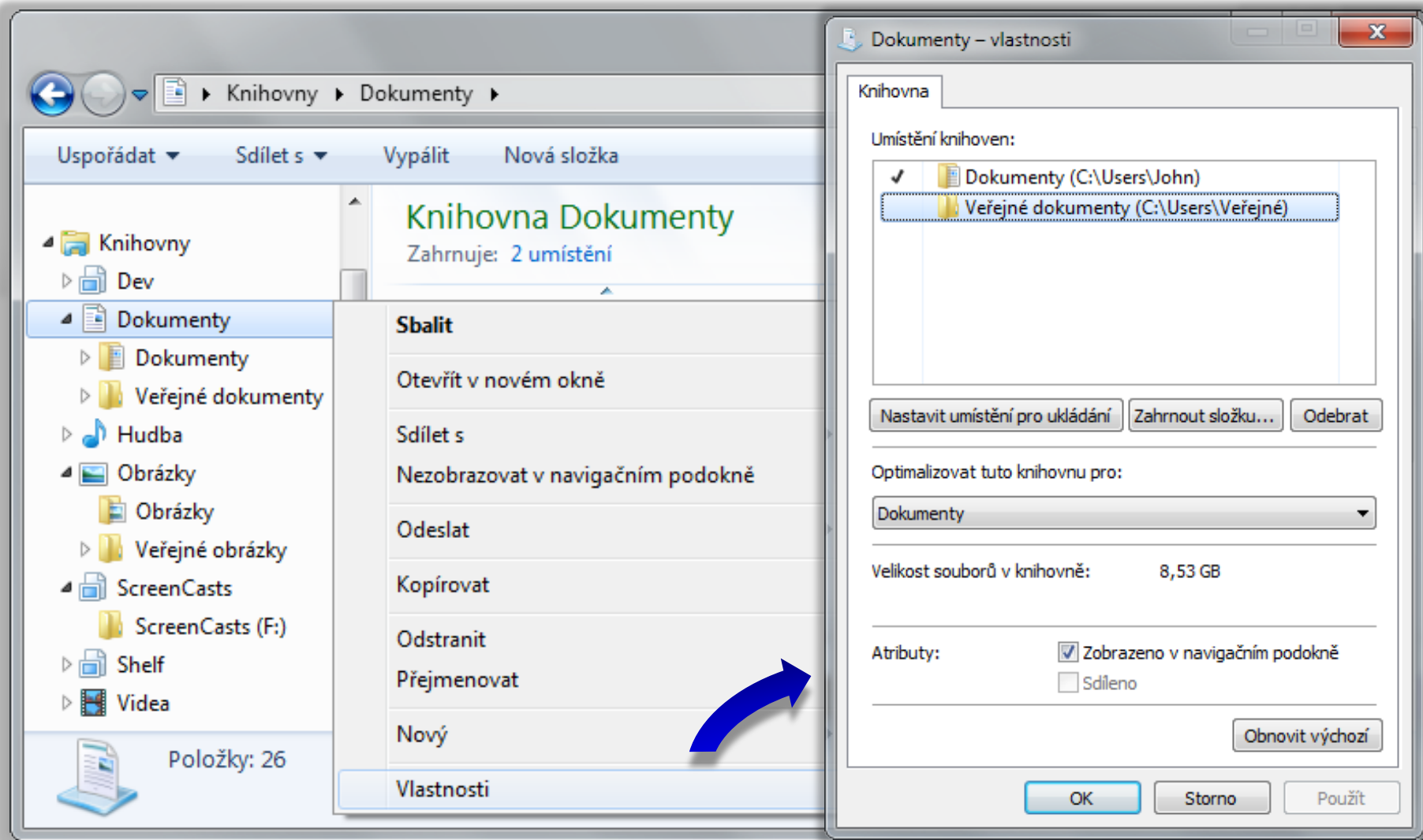
# Správa pomocí příkazové řádky

- 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

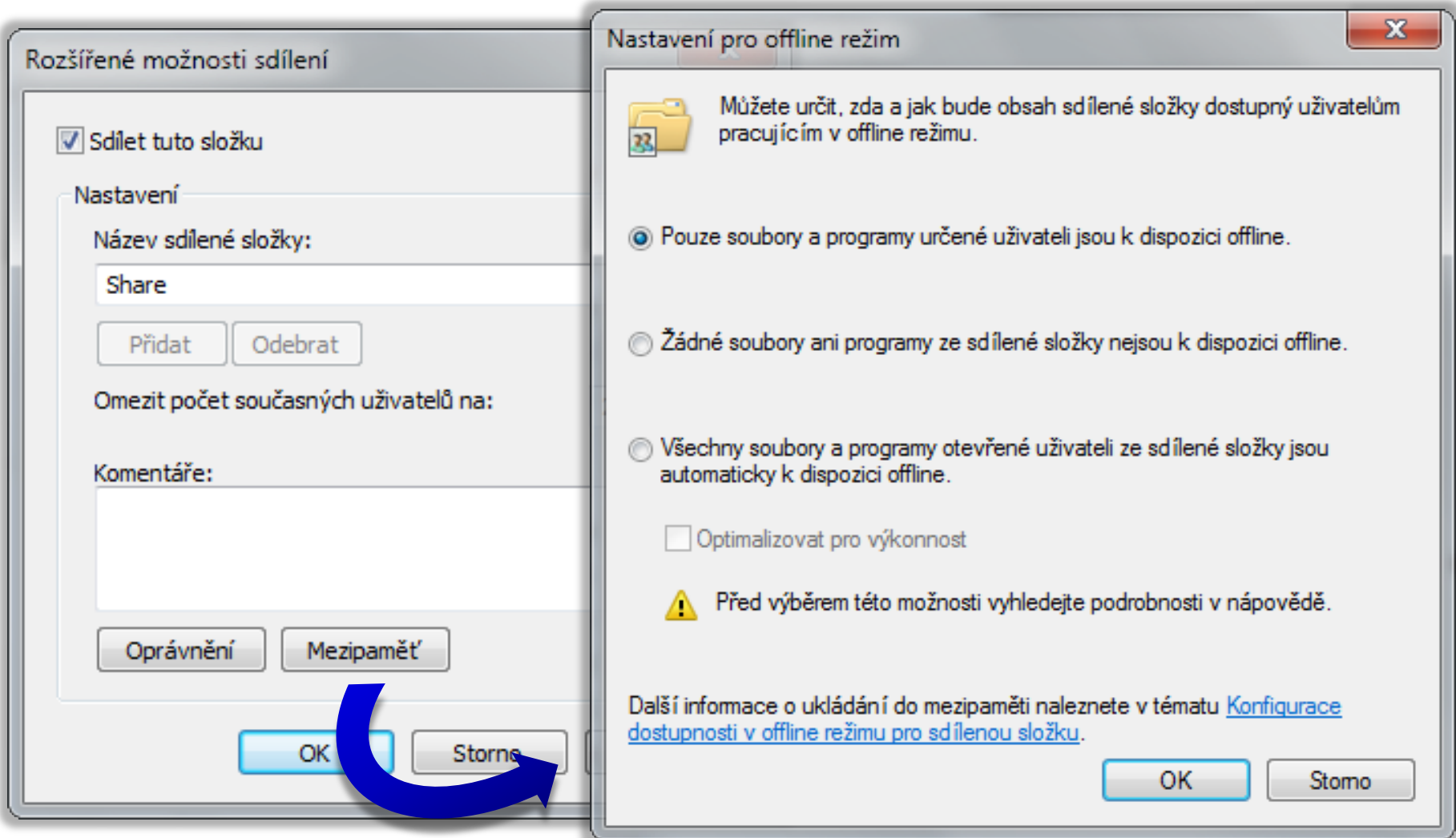
# Povolení a nastavení souborů offline

- Povolení souborů offline v **Centru synchronizace**
- Výběr souborů, jenž budou k dispozici offline
  - **Manuálně** 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 titled 'Offline soubory' and has tabs for 'Obecné', 'Využití disku', 'Šifrování', and 'Síť'. The 'Obecné' tab is selected, showing a message: '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.' Below this message is a button 'Zakázat offline soubory' (Disable Offline Files) and the text 'Funkce Offline soubory je právě povolena.' (Offline Files feature is currently enabled). There is also a button 'Spustit Centrum synchronizace' (Run Sync Center) and the text 'Centrum synchronizace použijte v případě, že chcete spustit synchronizaci offline souborů nebo vyhledat konflikty synchronizace.' (Use Sync Center if you want to start synchronization of offline files or search for synchronization conflicts). At the bottom of the dialog is a button 'Zobrazit offline soubory' (Show Offline Files). The dialog also has 'OK', 'Storno', and 'Použít' buttons at the bottom.

# 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

The image shows a Windows synchronization control panel on the left and a conflict resolution dialog box on the right. The control panel has a sidebar with options like 'Zobrazit konflikty synchronizace' and a main area showing a file 'offline.txt'. A context menu is open over the file, with a blue arrow pointing to 'Zobrazit možnosti řešení...'. The dialog box, titled 'Vyřešení konfliktu', asks the user to choose a version to keep. It lists three options: 'Zachovat tuto verzi' for the local file (9 bytes, 10/31/2011 6:26 PM), 'Zachovat tuto verzi' for the network share file (9 bytes, 10/31/2011 6:27 PM (novější)), and 'Zachovat obě verze' (the newer version will be renamed 'offline.txt (Meda Beda v1).txt)'). A 'Storno' button is at the bottom right.

**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 prostředků

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

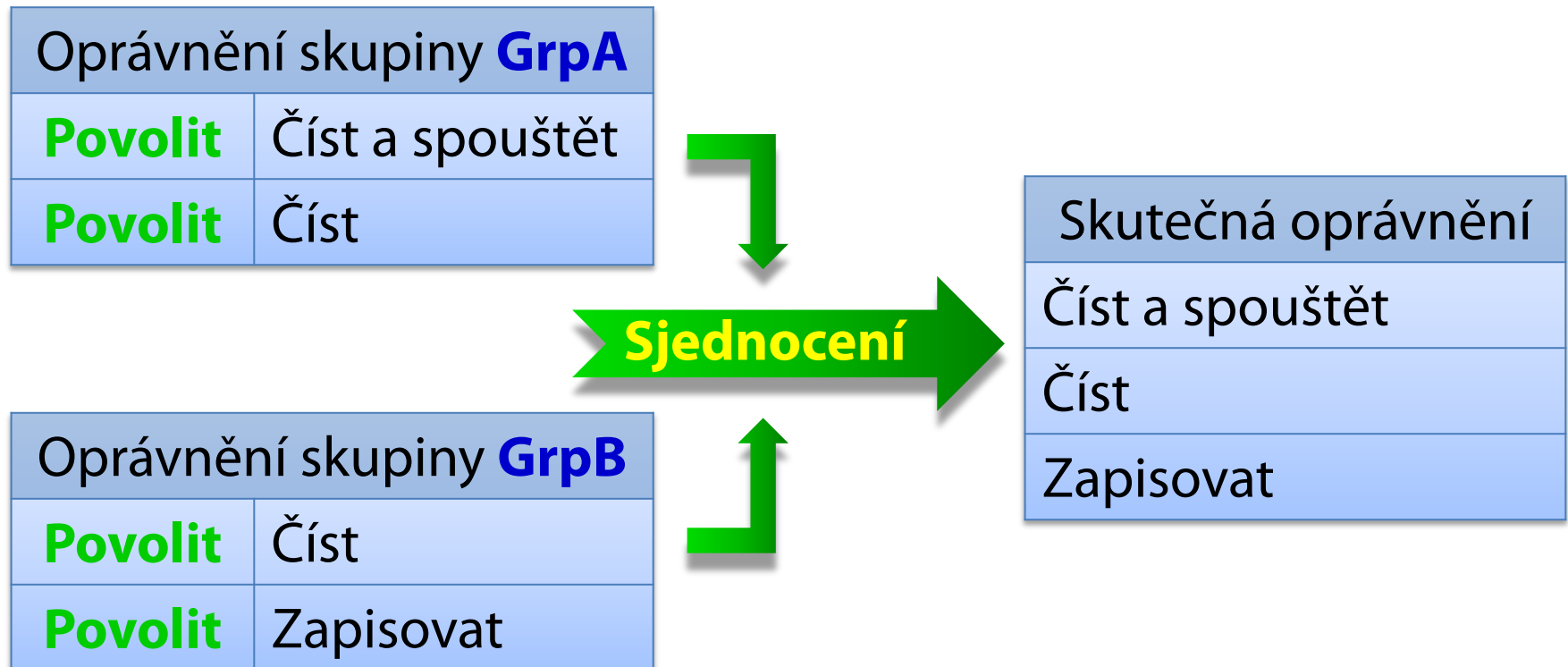
# Výpočet skutečných NTFS oprávnění

- 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 **odepřená** pro daného uživatele nebo skupinu, jenž je členem
  - 4) Vrať oprávnění **obsažená** v množině **S**



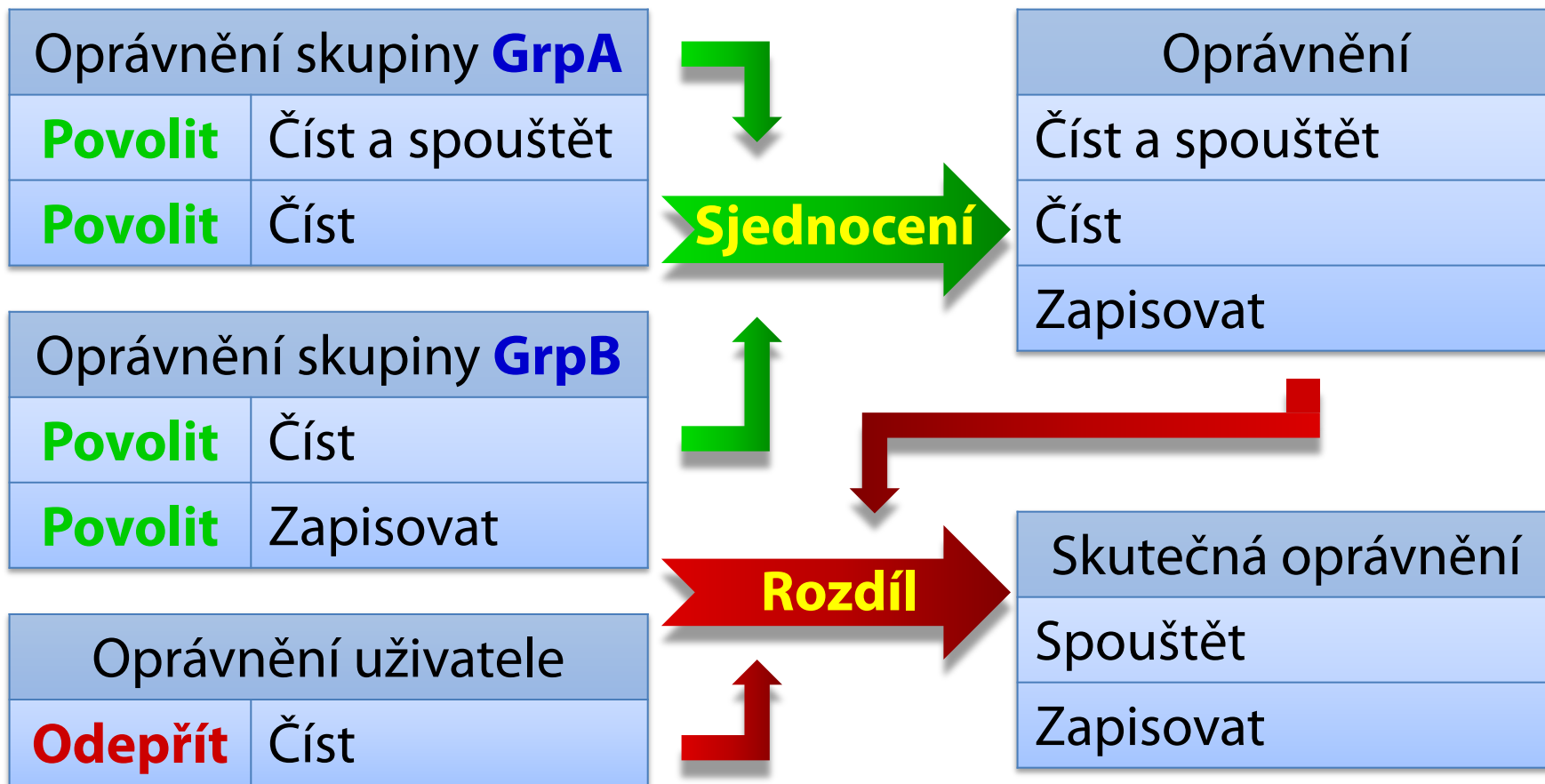
# Příklad s povolením (allow) oprávnění

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

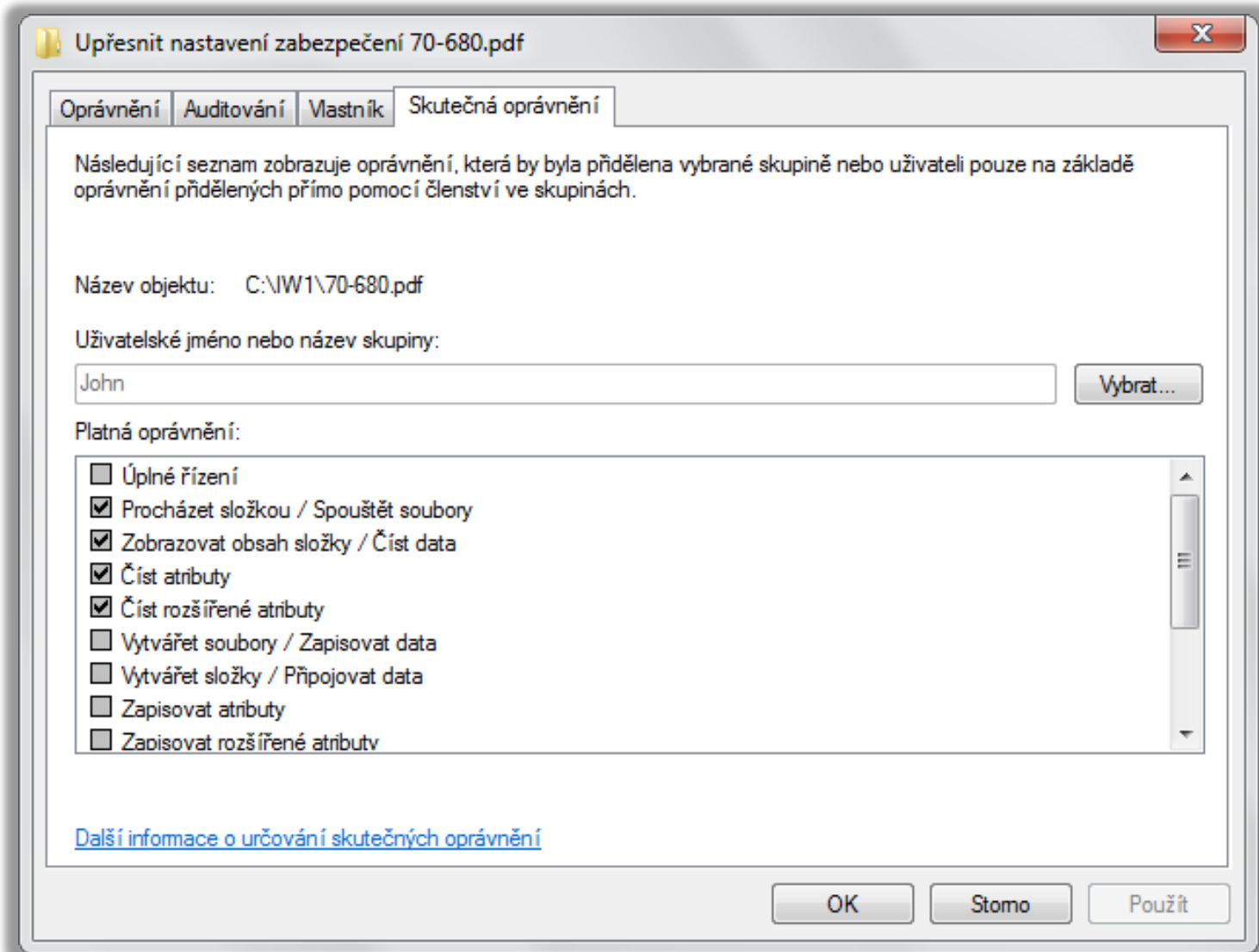


# Příklad s odepřením (deny) oprávnění

- 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 <soubor/adresář>`
- **Změna** NTFS oprávnění
  - **Povolení**
    - `icacls <soubor/adresář> /grant <uživatel>:<oprávnění>`
  - **Odepření**
    - `icacls <soubor/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
<b>Přesun</b>	Zachovává oprávnění	Dědí oprávnění od cílového adresáře	Nezachovává oprávnění
<b>Kopírování</b>	Dědí oprávnění od cílového adresáře	Dědí oprávnění od cílového adresáře	Nezachovává oprávnění

- Při použití nástroje **robocopy**

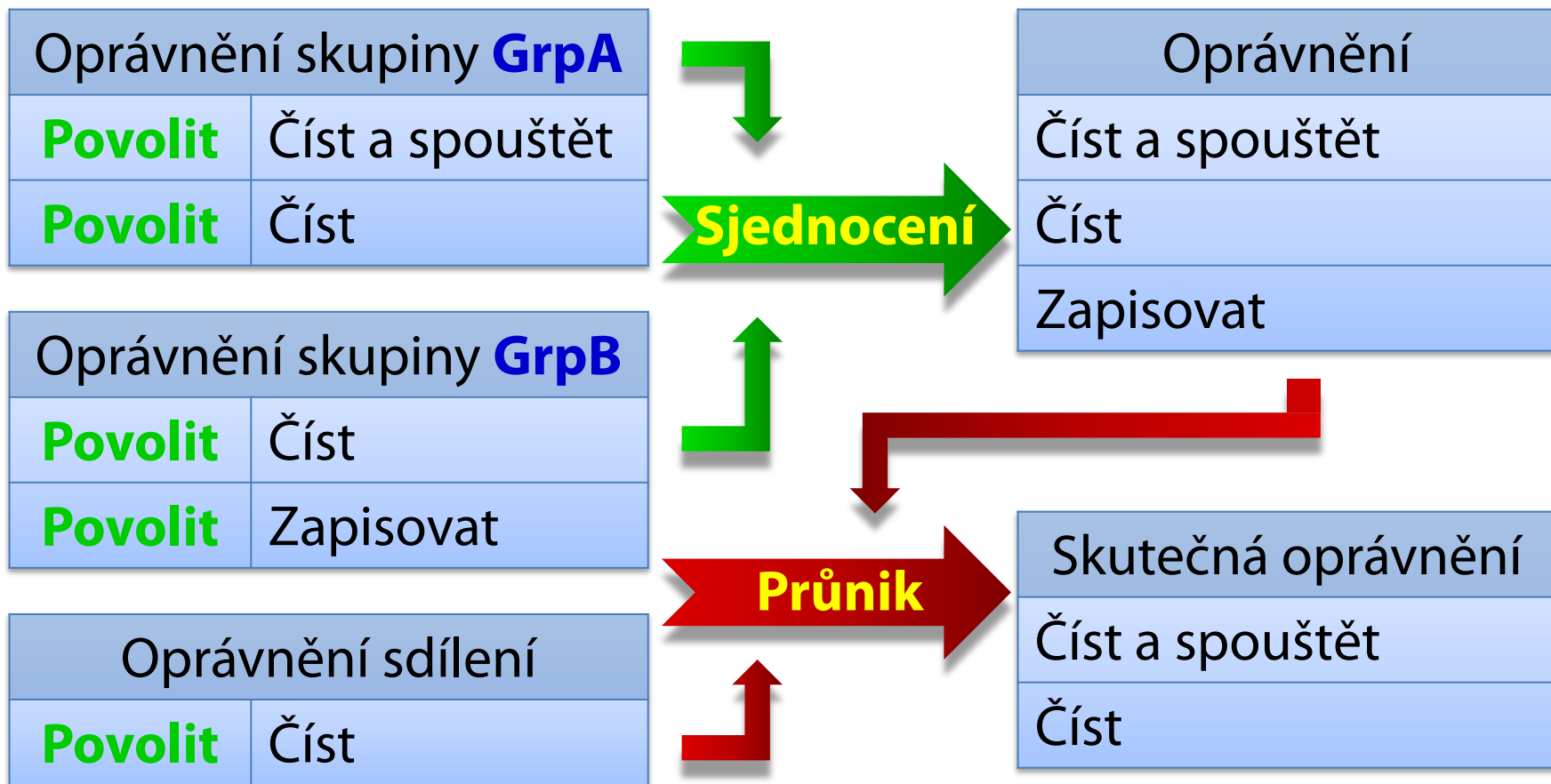
	V rámci stejného oddílu	Mezi různými oddíly	Na oddíl FAT/FAT32
<b>Přesun</b>	Zachovává oprávnění	Zachovává oprávnění	Nezachovává oprávnění
<b>Kopírování</b>	Zachovává oprávnění	Zachovává oprávnění	Nezachovává oprávnění

# 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**





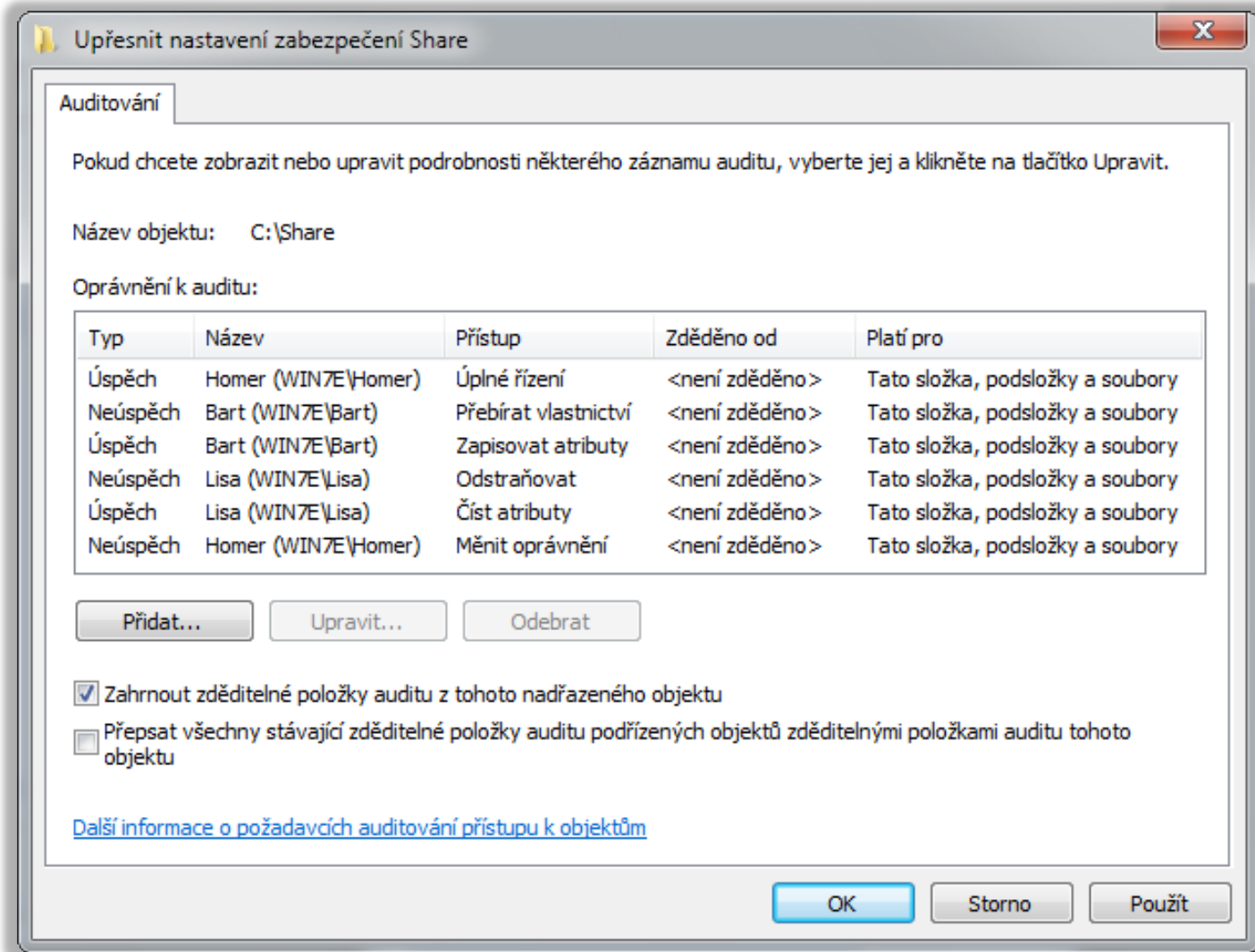
# Auditování přístupu k prostředkům

- 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** (**nespouští** monitorování)

# Nastavení auditování

- **Nastavení** ve vlastnostech jednotlivých souborů a adresářů (**spuštění** 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**)

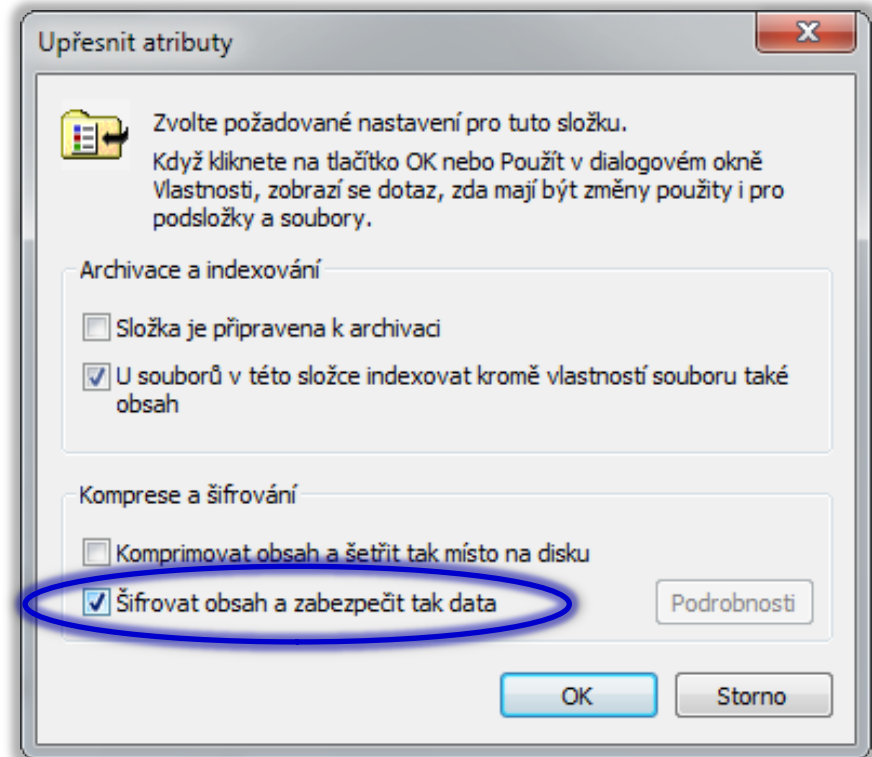
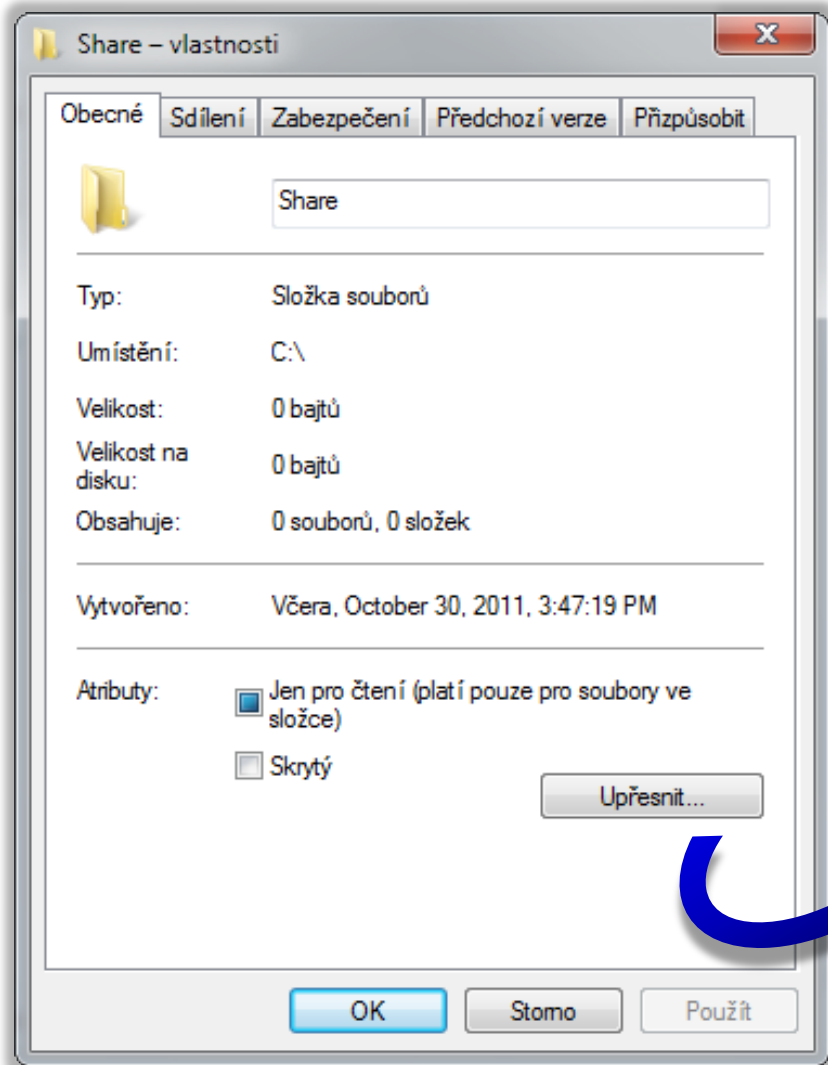
# Výběr monitorovaných oprávnění



# 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



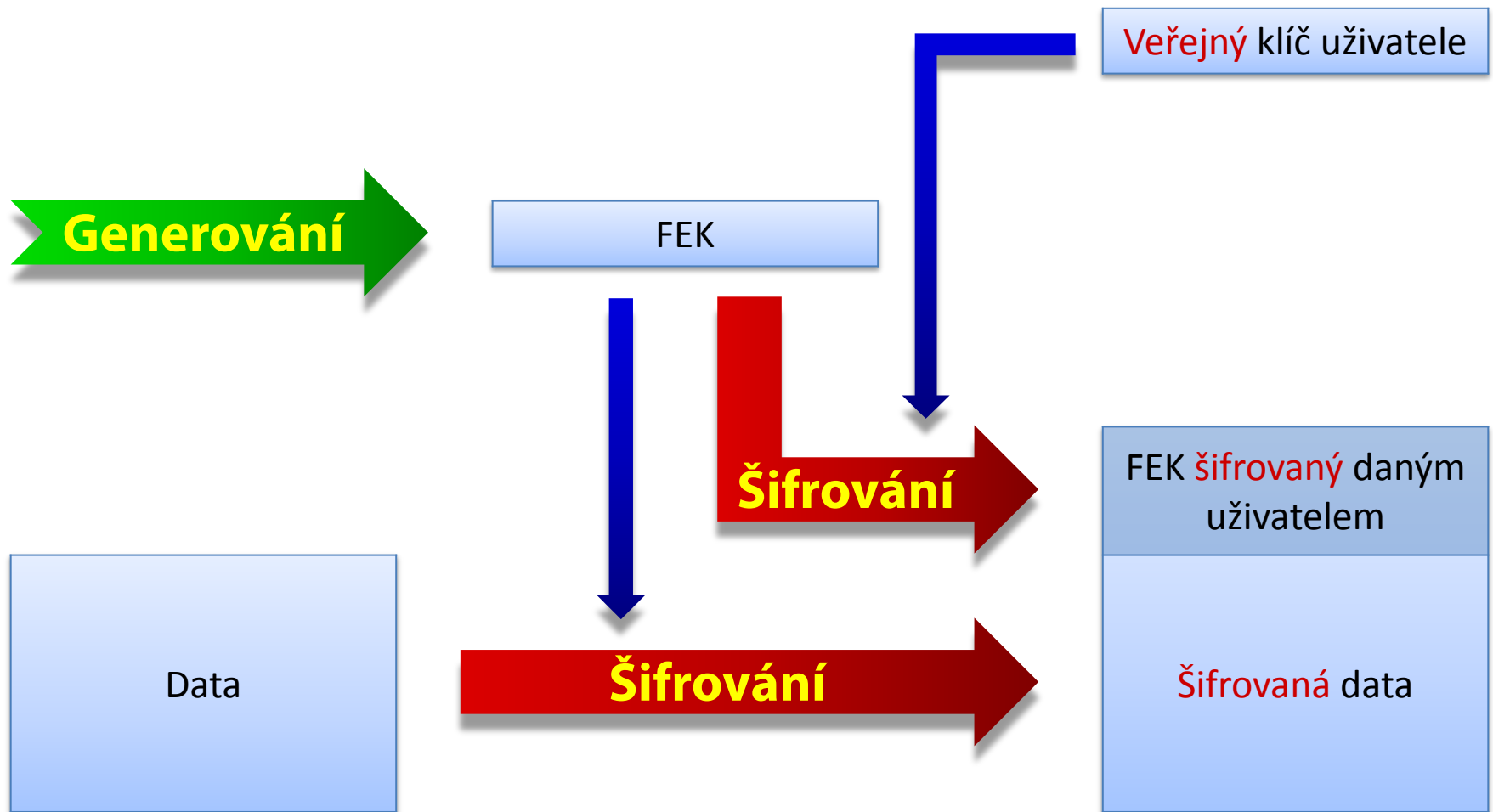
# Šifrování

- 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

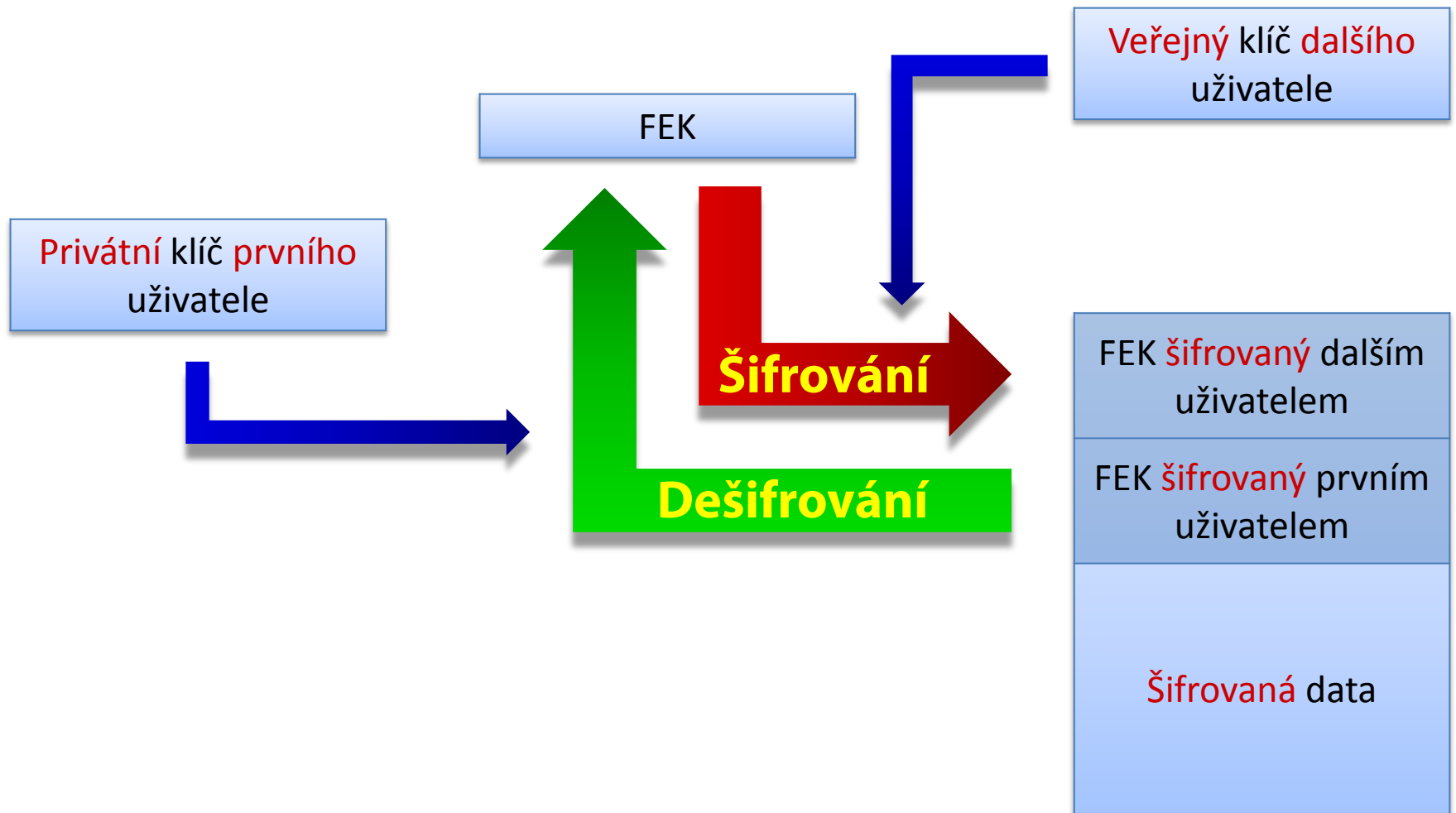
- FEK klíč (*File Encryption Key*)
  - Unikátní pro každý šifrovaný soubor
  - Generován při šifrování souboru prvním uživatelem
- Veřejný klíč (*public key*)
  - Uložen ve formě certifikátu v úložišti certifikátů
  - K dispozici všem uživatelům
- Privátní klíč (*private key*)
  - Uložen ve formě certifikátu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

# Šifrování souboru prvním uživatelem

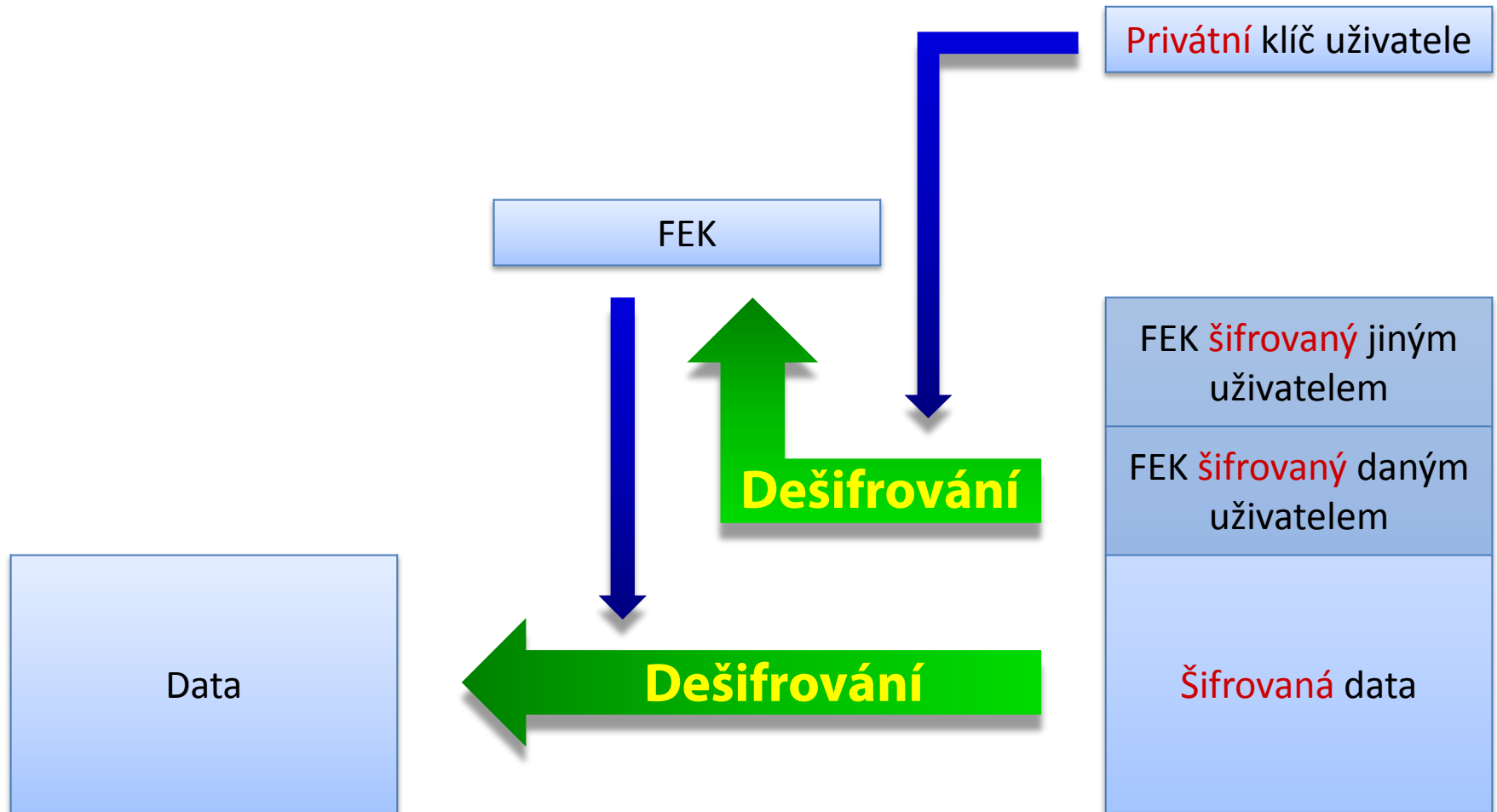




# Šifrování souboru dalším uživatelem



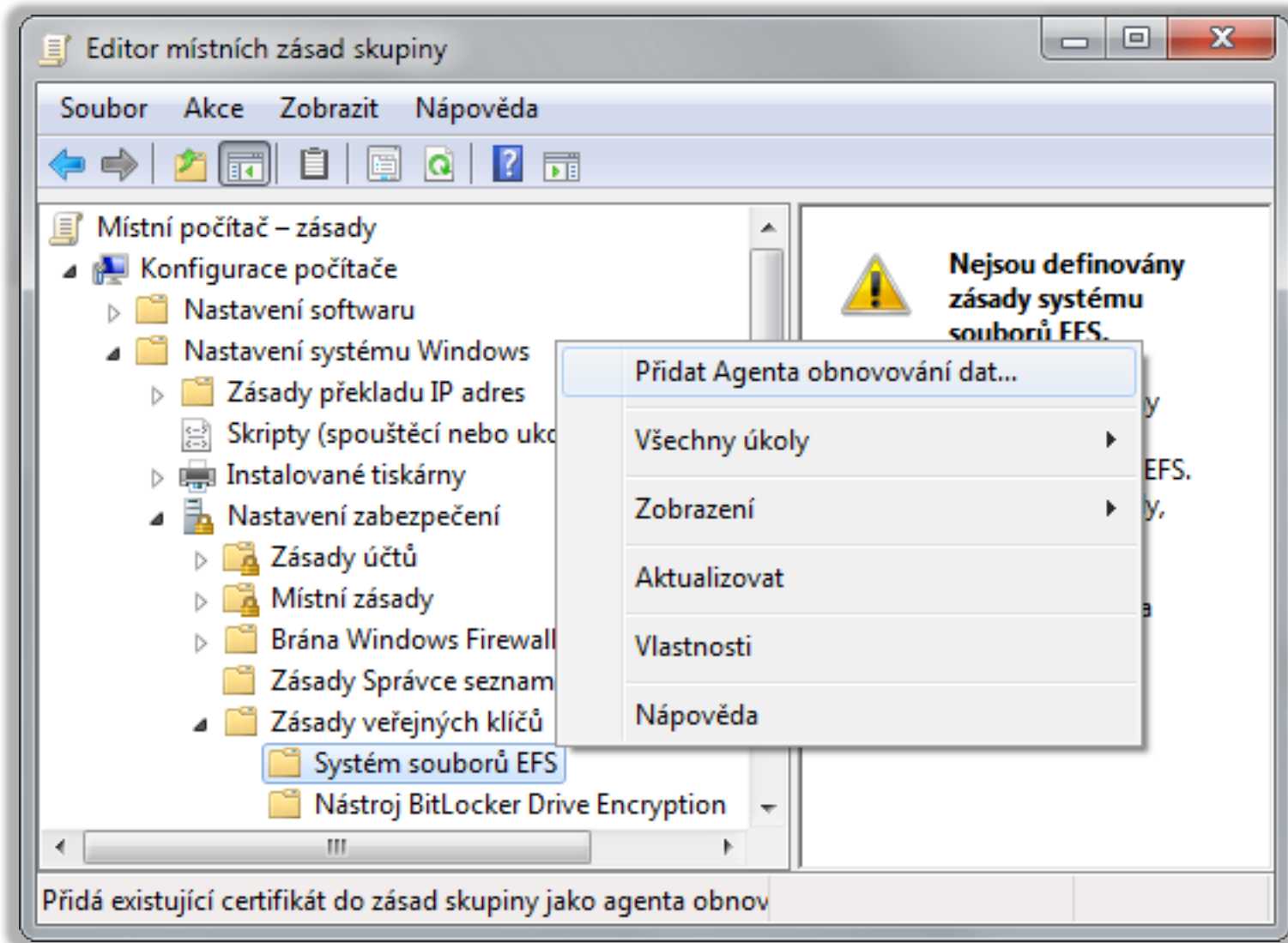
# Dešifrování souboru uživatelem



# 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