

PŘIHLÁŠKA VYNÁLEZU

zveřejněná podle § 31 zákona č. 527/1990 Sb.

(21) Číslo dokumentu:

2002 - 2788

(19)
ČESKÁ
REPUBLIKA



ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

(22) Přihlášeno: **29.11.2001**

(32) Datum podání prioritní přihlášky: **18.12.2000**

(31) Číslo prioritní přihlášky: **2000/00204637**

(33) Země priority: **EP**

(40) Datum zveřejnění přihlášky vynálezu: **15.01.2003**

(Věstník č. 1/2003)

(86) PCT číslo: **PCT/EP01/14245**

(87) PCT číslo zveřejnění: **WO02/050638**

(13) Druh dokumentu: **A3**

(51) Int. Cl. ⁷:

G 06 F 1/00

(71) Přihlašovatel:

**KONINKLIJKE PHILIPS ELECTRONICS N. V.,
Eindhoven, NL;**

(72) Původce:

**Staring Antonius Adriaan Maria, Eindhoven, NL;
Kamperman Franciscus Lucas Antonius Johannes,
Eindhoven, NL;**

(74) Zástupce:

Zelený Pavel JUDr., Hálkova 2, Praha 2, 12000;

(54) Název přihlášky vynálezu:

**Způsob bezpečné superdistribuce uživatelských
dat, systém bezpečné superdistribuce, zařízení
pro reprodukci a záznam, a nosič dat**

(57) Anotace:

Vynález se týká způsobu pro zabezpečenou super distribuci uživatelských dat, uložených na prvním nosiči dat obsahujícího kroky a) zkopírování uživatelských dat z prvního nosiče dat na druhý nosič dat; b) uložení na druhý nosič dat informací, které jsou vyžadovány servisním střediskem pro přidělení přístupových práv ke kopii uživatelských dat; a c) získání přístupových práv ke kopii uživatelských dat přenesením alespoň uložených informací do servisního střediska, dokončení transakce a přijetí přídatných přístupových informací tím, že servisní středisko používá uložené informace pro přidělení přístupových práv ke kopii uživatelských dat pro druhý nosič dat. Prostřednictvím obsahu s řízeným přístupem se tak provádí řízení kopírování. Dále se mohou vlastníkově originálních nosičů dat poskytnout výhody. Vynález se také týká systému pro zabezpečenou super distribuci, zařízení pro reprodukci a/nebo záznam uživatelských dat na nosič dat.

2002-2788
15.10.02

ZPŮSOB BEZPEČNÉ SUPERDISTRIBUCE UŽIVATELSKÝCH DAT, SYSTÉM
BEZPEČNÉ SUPERDISTRIBUCE, ZAŘÍZENÍ PRO REPRODUKCI A ZÁZNAM,
A NOSIČ DAT

Oblast techniky

Vynález se týká způsobu pro zabezpečenou super distribuci uživatelských dat uložených na prvním nosiči dat. Vynález se dále týká systému pro zabezpečenou super distribuci uživatelských dat, zařízení pro reprodukci a/nebo záznam uživatelských dat a nosiče dat pro uložení uživatelských dat.

Dosavadní stav techniky

Super distribuce je přístupem k distribuci softwaru, ve kterém je software volně dostupný a bez omezení, ale je chráněn před úpravami a režimy provozu, ke kterým nemá od dodavatele právo. Architektura super distribuce, která je známá například od R. Mori a M. Kawahara, "Super distribution - The concept and the Architecture" ("Super distribuce - koncept a architektura"), zpráva IEICE, Vol. E, No. 7, str. 1133 - 1146, červenec 1990 (k nalezení na <http://www.virtualschool.edu/mon/electronicproperty/morisuperdist.html>) poskytuje tři principy činnosti: administrativní úpravy pro sbírání účtovacích informací o používání softwaru a poplatků za používání softwaru; postup účtování, který zaznamenává a sčítá poplatky za používání, platby a přidělování poplatků za používání mezi různé dodavatele

Software ze super distribuce se distribuuje přes veřejné kanály v zašifrovaném tvaru. Má následující kombinaci požadovaných vlastností:

- Softwarové produkty jsou distribuovány volně, bez omezení. Uživatel softwaru platí za používání produktu, nikoli za jeho vlastnění.

- Dodavatel softwarového produktu může pro jeho použití nastavit pravidla a podmínky pro jeho používání ve splátkovém kalendáři, ale nemusí.

- Softwarové produkty mohou spouštět libovolní uživatele, kteří mají vhodné vybavení, poskytnuté pouze tehdy, když uživatel dodrží podmínky použití, které dodavatel nastaví, a zaplatí poplatky, které dodavatel stanoví.

- Správná funkce systému super distribuce včetně vynucení podmínek stanovených poskytovateli je zajištěna elektronickými zařízeními odolnými proti falšování, např. kartami smart card.

Super distribuce se nemusí používat pouze k distribuci softwaru, ale obecně také k distribuci uživatelských dat, jako jsou audio a video data. Super distribuce audio a video obsahů může být přitažlivým obchodním modelem pro nahrávací a filmové společnosti. Důvodem je, že v tomto modelu uživatelé přebírají část role distributora tím, že si data zkopírují, např. jejich oblíbené album pro jejich přátele. Stejně tak se může, např. v závislosti na úspěchu alba, cena výroby a distribuce fyzických médií výrazně snížit. Obchodní model spočívající na super distribuci je zřetelně přístupný pouze tehdy, když je použití kopie správně zapláceno, což vyžaduje nasazení spolehlivého systému ochrany obsahu. Takový systém se bude zakládat na mechanismu řízení

přehrávání, které používá kódování a s největší pravděpodobností technologii vodoznaků.

Podstata vynálezu

Cílem vynálezu je poskytnout způsob pro zabezpečenou super distribuci uživatelských dat, která také umožňuje realizaci různých obchodních modelů.

Tohoto cíle se dosáhne způsobem podle nároku 1, obsahujícím kroky:

a) zkopírování uživatelských dat z prvního nosiče dat na druhý nosič dat;

b) uložení na druhý nosič dat informací, která jsou požadována servisním střediskem pro přidělení přístupových práv ke kopii uživatelských dat a

c) získání přístupových práv ke kopii uživatelských dat přenesením alespoň uložených informací servisnímu středisku, dokončení transakce a přijetí dalších přístupových informací, přičemž servisní středisko používá uložené informace pro přidělení přístupových práv ke kopii uživatelských dat pro druhý nosič dat.

Vynález je založen na následující myšlence:

a) řízení kopírování: kopírování super distribuovaného obsahu - které ještě není přístupné, protože se ještě nedokončila transakce se servisním střediskem - na jiné místo, než je druhý nosič dat, je nepoužitelné, protože servisní středisko pro toto místo nepřidělí přístup; a

b) řízení přístupu: po dokončení transakce se servisním střediskem může být přístup na super distribuovanou kopii na druhém nosiči dat pouze prostřednictvím systému správy

digitálních práv (Digital Rights Management, DRM).

Další zdůvodnění pro zavedení konceptu, jako je tzv. unicast super distribuce je, že poskytuje prostředky pro to, aby byly originály atraktivnější, než kopie, přestože mezi nimi není žádný zřejmý rozdíl, a tím podporuje maloobchodní trh. V případě unicast super distribuce například existuje přímé spojení mezi vlastníkem originálního nosiče dat a vlastníkem druhého nosiče dat, pro kterého je super distribuovaná kopie určena. Unicast super distribuce tedy (ne)přímo využívá společenských vztahů mezi lidmi a může tyto vztahy dokonce posilovat tím, že podporuje vytváření společenství. Dále může poskytnout unicast super distribuce více bezpečnosti, protože není příliš užitečné vystavovat na internetu (šifrovaná) uživatelská data pro všeobecné stahování, protože servisní středisko ke kopii uživatelských dat, která byla takto získána, nepřidělí přístup.

Rozhodnutí, zda přístup k takové kopii přidělit, nebo odmítnout, je zcela na servisním středisku; v podstatě neexistuje žádný důvod, proč by servisní středisko přístup přidělit nemohlo, např. z důvodu nedostatku informací. Jestliže jsou konečně pro super distribuci způsobilé pouze originály - což je způsob, jak zatraktivnit originály oproti kopiím, např. systémem odměn spojených se super distribucí, např. cestou získávání "zvukových kilometrů" - se předpokládá, že bude růst počtu super distribuovaných kopií přibližně stejný, jako je růst počtu prodaných originálů (předpokládá se, že z každého prodaného originálu se udělá asi jedna super distribuovaná kopie). To je opět vlastnost, která podporuje maloobchodní trh.

Informace, které jsou potřeba pro servisní středisko

pro přidělení přístupových práv ke kopii uživatelských dat, mohou být libovolné informace, které umožní servisnímu středisku identifikovat uživatelská data. Informace se mohou skládat například z některého následujícího nebo z kombinace následujících:

- jedinečný identifikátor uživatelských dat, např. ISRC číslo hudební stopy;
- jedinečný identifikátor souboru uživatelských dat, např. název alba;
- dešifrovací klíč uživatelských dat zašifrovaný ve veřejném klíči servisního střediska;
- jedinečný identifikátor původního nosiče dat;
- jedinečný identifikátor cílového nosiče dat;
- identifikátor původního majitele uživatelských dat;
- kódové hodnoty odvozené od libovolných výše uvedených identifikátorů.

Z důvodu podpory realizace obchodního modelu, který je založen na zabezpečené super distribuci, je upřednostňované provedení vynálezu založeno na myšlence zanést na první nosič dat jedinečný identifikátor nosiče, tj. jedinečné ID disku na předem nahraném (ROM) disku. Z tohoto jedinečného identifikátoru nosiče se určí kódová hodnota, přednostně přehrávačem prvního nosiče dat, která se uloží v záznamovém zařízení na druhý nosič dat společně s jedinečným identifikátorem nosiče z prvního nosiče dat. Aby se povolil druhý nosič dat, tj. kopie prvního nosiče dat, je nutné přenést kódovou hodnotu a jedinečný identifikátor nosiče do servisního střediska, např. vlastníka obsahu uživatelských dat uložených na prvním nosiči dat, kde se tato data dekódují a/nebo ověří a v případě kladného výsledku se požadovaná práva a informace přenesou zpět do záznamového zařízení nebo přehrávače druhého nosiče dat, čímž se povolí.

V upřednostňovaných provedeních vynálezu jsou dále použity identifikátory, aby se zvýšila funkčnost navrhovaného způsobu super distribuce, např. od koho pro koho se kopie pořizuje. Konkrétně lze použít identifikátor super distribuce, který může být uložen na prvním nosiči dat a použit k určení kódové hodnoty a k potvrzení kódové hodnoty v servisním středisku.

V dalším provedení vynálezu se k zašifrování uživatelských dat, která jsou uložena v zašifrovaném tvaru na prvním nosiči dat, používá jeden nebo více klíčů, které mohou být součástí hierarchie klíčů. Pro povolení druhého nosiče dat je třeba ze servisního střediska tyto klíče dodat. Tyto klíče mohou být odvozeny například od fyzického označení disku, např. drážky na optickém nosiči dat.

V dalším hledisku vynálezu se k zašifrování kódové hodnoty před jejím uložením na druhém nosiči dat používá klíč přehrávače super distribuce a klíč záznamového zařízení super distribuce. Dešifrování potom provede servisní středisko potom, co se zašifrovaná kódová hodnota zašle do servisního střediska pro povolení druhého nosiče dat.

Navíc se v dalším hledisku vynálezu používají identifikátor přehrávače a identifikátor záznamového zařízení, které jsou také uloženy na druhém nosiči dat a přenášejí se do servisního střediska pro dešifrování klíče přehrávače super distribuce a klíče záznamového zařízení, pro povolení druhého nosiče dat.

Dále, dešifrování dvakrát zašifrované kódové hodnoty může také provést výrobce přehrávače a/nebo záznamového

zařízení pomocí identifikátorů přehrávače a/nebo záznamového zařízení. Výrobci zařízení se tak zapojí do procesu povolování druhého datového nosiče a lze tak zajistit, aby se používala pouze schválená zařízení, což také zvyšuje zabezpečení navrhovaného způsobu super distribuce.

V upřednostňovaném provedení vynálezu se navrhuje poskytovat ze servisního střediska výhody vlastníkovu prvního nosiče dat jako odpověď na zabezpečenou super distribuci uživatelských dat uložených na prvním nosiči dat. Takové poskytování výhod je součástí obchodního modelu, kde kopírování a zabezpečená distribuce uživatelských dat by měla být stimulující. Výhodami může být odměna ve formě originálního zdroje super distribuovaného obsahu s "hudebními kilometry", pokud si přístup k tomuto obsahu někdo koupí. Jinými příklady jsou volný přístup k "osobnímu přístupovému kódu", což popisuje evropská patentová přihláška 00 201 663.2, čímž se odemkne bonusová stopa na původním nosiči dat, nebo bonusové body na slevu při příštím nákupu. Lze také řídit poskytování těchto výhod pouze pokud se provede přímá kopie z originálního nosiče dat. Tento mechanismus zaručuje, že je stále atraktivní koupit původní nosič dat, který poskytuje mechanismus pro ochranu před kopírováním obsahu s řízeným přístupem.

V dalším upřednostňovaném provedení se do servisního střediska přenáší bonusová kódová hodnota vytvořená alespoň z jedinečného identifikátoru prvního nosiče dat, aby se bonusové výhody shromažďovaly. Servisní středisko tak může určit, zda a kolika výhodami se má odměnit vlastník prvního nosiče dat.

Jako nosiče dat podle vynálezu se přednostně používají

15.10.02

optické nosiče záznamu, přednostně zapisovatelná a/nebo přepisovatelná CD nebo DVD. Jako nosiče dat ve smyslu vynálezu je však možné dále použít všechny ostatní druhy úložných médií. Způsob podle vynálezu se přednostně používá pro super distribuci softwaru, video a/nebo audio dat uložených na takových nosičích záznamu.

V jednom provedení vynálezu obsahuje druhý nosič dat také jedinečný identifikátor nosiče, který se používá pro určení kódové hodnoty, a který se také posílá do servisního střediska pro povolení druhého nosiče dat. Tento jedinečný identifikátor nosiče na druhém nosiči dat se přednostně používá, pokud je důležitý cíl použitých dat.

Vynález se dále týká systému pro bezpečnou super distribuci uživatelských dat, obsahujícího přehrávač a záznamové zařízení, přenosové prostředky a servisní středisko podle nároku 14. Vynález se dále týká zařízení pro reprodukci a/nebo záznam uživatelských dat pro použití v tomto systému a nosiče dat pro uložení uživatelských dat a dat super distribuce, která se mají použít ve způsobu pro zabezpečenou super distribuci podle vynálezu. Je třeba pochopit, že takový systém, zařízení a nosič dat podle vynálezu se může dále vyvinout a může mít další provedení, která jsou stejná nebo podobná jako výše popsaná provedení a jak jsou uvedena v závislých nárocích nároku 1.

Hrubá podstata způsobu a systému podle vynálezu je následující. Předem zaznamenaný disk obsahuje obsah, který je zašifrován aktivním klíčem, který může být uložen v zámku klíče, jak je popsáno v evropské patentové přihlášce 00 202 888.4. Lze ale použít také klíč, který je odvozen z první fyzické značky na disku, např. lze použít drážka na optickém

nosiči záznamů. Tento klíč může být součástí hierarchie klíčů a jako takový se nepoužívá pro přímé zašifrování obsahu, ale spíše jako mezisada klíčů. Pro správnou funkci způsobu a systému se vyžaduje, aby byl obsah této značky disku tajný, tj. aby byl přístupný pouze pro spolupracující přehrávače. Obsah je jedinečný pro titul disku, ale nemusí být jedinečný pro disk, tj. klíče a zašifrovaný obsah na všech před zaznamenaných discích jsou stejné. To by pro vlastníka obsahu neměl být problém, jelikož všechny předem zaznamenané disky jsou originály známého původu.

Kromě první fyzické značky na disku existuje druhá, přednostně tajná značka na předem zaznamenaném (ROM) disku, která je pro každý disk jedinečná. Obsah této druhé značky se může použít během všech fází procesu super distribuce pro zamezení nekontrolované super distribuci. Klíč pro přehrávání, tj. aktivní klíč, dodá (bezpečně) servisní středisko. Na kopii se provedou opatření, aby se zajistilo, že obsah bude přehratelný pouze na daném konkrétním disku, aby se zamezilo nekontrolované distribuci přes Internet. Pro tyto účely obsahuje zapisovatelný nebo přepisovatelný disk jedinečnou značku disku, která se použije k odvození klíče (klíčů), který je potřeba pro dešifrování obsahu. Pro zapisovatelné nebo přepisovatelné disky může být tato jedinečná značka disku předem vylisována na disku nebo zaznamenaná na záznamovém zařízení.

Hlediskem vynálezu je zajistit, aby bylo možné vytvořit kopii zdroje pouze na jeden datový spotřebič. Kopie z jednoho zdroje na více datových spotřebičů, tj. prostřednictvím Internetu, by se také neměla umožnit. Umožnilo by to nepoužití jedinečného identifikátoru disku pro výstup. Systém bonusů by však nemusel v tomto případě

15.10.02

pracovat spravedlivě. Pokud by někdo otevřel oblíbenou webovou stránku, ze které by všichni stahovali soubory, mohl by posbírat všechny bonusové výhody. Kdyby na druhou stranu pro kopii potřeboval vždy původní disk, byli by oceněni pouze kupující původních disků.

Po dokončení transakce poskytne vlastník obsahu, tj. servisní středisko, klíč(e), které použije záznamové zařízení k vytvoření hratelné kopie (a to pouze této jediné kopie). V jistém bodě transakce byl vlastník obsahu schopen určit jedinečný identifikátor nosiče původního disku. Pro povzbuzení spotřebitele k vytváření super distribuovaných kopií pro přátele se může vlastník obsahu rozhodnout poskytnout vlastníkovu originálního disku nějaké výhody. Například mu může dát volný přístup k "osobnímu přístupovému kódu", který lze použít k odemčení bonusové stopy na původním disku; všechny bonusové body se mohou sčítat pro slevu při příštím nákupu. Když se tak majitel obsahu rozhodne, může super distribuovanou kopii také použít k vytvoření další super distribuované kopie, ať už donekonečna, nebo do předem stanovaného limitu. V tom případě se může majitel obsahu rozhodnout poskytnout výhody spojené se super distribuovaným obsahem libovolnému podílníkovi v řetězu počínajícím u originálního disku (jako u pyramidového systému). Zabezpečená super distribuce obsahu zřetelně umožňuje přehršel obchodních modelů, která lze u různých alb volit různě, a může poskytovat bohatý zdroj obchodních informací.

Přehled obrázků na výkresech

Vynález bude blíže vysvětlen prostřednictvím

konkrétních příkladů provedení znázorněných na výkresech, na kterých představuje

obr. 1 blokové schéma systému super distribuce podle tohoto vynálezu

obr. 2 blokové schéma hierarchie klíčů použité v provedení podle tohoto vynálezu

obr. 3A, 3B rozložení disku na originálu a na kopii

obr. 4 kroky při kopírování podle prvního provedení tohoto vynálezu,

obr. 5 kroky při povolování podle prvního provedení tohoto vynálezu

obr. 6 kroky při sbírání výhod podle prvního provedení tohoto vynálezu

obr. 7 kroky při kopírování podle druhého provedení tohoto vynálezu

obr. 8A, 8B kroky při povolování podle druhého provedení tohoto vynálezu

obr. 9A, 9B kroky při sbírání výhod podle druhého provedení tohoto vynálezu

Příklady provedení vynálezu

V blokovém schématu na obr. 1, ukazujícím provedení systému super distribuce podle tohoto vynálezu, je zobrazen přehrávač 1 pro reprodukci předem nahraného nosiče dat, např. předem nahraného (ROM) disku obsahujícího uživatelská data, např. software, video nebo audio data. Pro záznam dat uložených na prvním nosiči dat reprodukováných přehrávačem 1 na druhý nosič dat, např. na přepisovatelný nebo zapisovatelný disk, se používá záznamové zařízení 2. Po přenesení uživatelských dat a všech dat nezbytných pro super distribuci z přehrávače 1 na záznamové zařízení 2, se tato data uloží na druhý nosič dat, se tento nosič povolí, tj. poskytnou se mu všechna nezbytná práva a informace pro zamýšlené použití druhého nosiče dat, a to tak, že se přenesou požadovaná data super distribuce do servisního střediska 3, kde se tato data ověří a v případě úspěšného ověření se záznamovému zařízení 2 vrátí data pro povolení. Pro účely ověření dat pro super distribuci, která poskytuje záznamové zařízení 2 může servisní středisko 3 poslat část dat super distribuce výrobci 4 přehrávače a/nebo výrobci 5 záznamového zařízení pro rozšifrování a/nebo ověření. Spojení mezi přehrávačem a servisním střediskem a mezi servisním střediskem a výrobcem záznamového zařízení/přehrávače nejsou podstatná, ale volitelná. Spojení mezi přehrávačem a servisním střediskem je pro případné sbírání výhod. Ostatní spojení se používají pro zapojení výrobců "do procesu", pokud je to žádoucí. Systém a způsob pro super distribuci budou podrobněji popsány níže.

Obrázek 2 ukazuje blokové schéma představující hierarchii klíčů používanou v upřednostňovaném provedení vynálezu. Nejprve se použije čtečka 6 značky disku, která

přečte fyzické značky na disku, čímž se získá první sada klíčů. Z těchto klíčů 7 vytvoří tzv. klíč zámku klíčů KL_klíč. Stejně tak se čtečka 8 zámku klíčů použije pro získání zašifrované verze aktivních klíčů, přičemž aktivní klíče se používají pro šifrování uživatelských dat. Funkce čtečky 8 zámku klíčů spočívá ve čtení obsahu zámku klíčů z disku. Samotný zámek klíčů je zvláštní oblast na disku, kde se uchovávají dešifrovací klíče (aktivní klíče) a uživatelská práva k obsahu. Obsah zámku klíčů je zašifrovaný použitím klíče zámku klíčů, který se odvodí podle hierarchie klíčů zobrazené na obrázku.

V bloku 9 se aktivní klíče použitím klíče zámku klíčů dešifrují, přičemž aktivní klíč se potom použije v bloku 10, aby se zašifrovaný obsah, tj. uživatelská data uložená na disku, dešifroval. Je třeba poznamenat, že hierarchie klíčů zobrazená na obr. 2 je pouze možností systému, který může být jako spodní vrstva systému podle vynálezu. Mohou existovat i jiná, stejně dobře fungující provedení.

Na obrázcích 3A a 3B je zobrazeno rozložení na originálu a kopii nosiče dat, tj. dat super distribuce uložených na originálu a na zkopírovaném nosiči dat, přičemž oba nosiče jsou optické disky. Originální disk zobrazený na obr. 3A obsahuje následující data super distribuce:

- ID titulu: identifikátor dat, kterým může být nějaké číslo identifikující titul obsahu, který není tajný;
- UDI-RO: jedinečný identifikátor nosiče (disku), konkrétně ROM disku, který není tajný; UDI-RO je uložen na originálním disku (pouze pro čtení) ve fyzické značce disku, a identifikuje konkrétní disk (tj. funguje jako obdoba sériového čísla). Není určeno ke kopírování. Na kopii je ekvivalentem UDI-RO identifikátor UDI-R, který může být na

kopii buďto předem zapsán (např. výrobcem), nebo může být zapsáno záznamovým zařízením, které je podrobeno většímu počtu pravidel na robustnost a náhodnost. Je třeba poznamenat, že UDI-R se může nacházet uvnitř zámku klíčů.

- EKB: blok povolovacího klíče (není tajný), což je blok dat obsahující klíč, který je zašifrován různými klíči přehrávače;

- PDM(s): fyzická značka (značky) disku. Tyto fyzické značky disků mohou přečíst pouze spolupracující zařízení a jsou přednostně tajné. Pokud se používá EKB, ani PDM nemusí být tajné;

- SD-ID: identifikátor super distribuce, což může být nějaké číslo používané pro podporu funkčnosti super distribuce, které je tajné a které se může nacházet v zámku klíčů;

- AK: aktivní klíč, který se používá pro zašifrování nějaké části obsahu uživatelských dat (aktiva).

Místo identifikátoru nosiče UDI-RO obsahuje zkopírovaný disk zobrazený na obr. 3B identifikátor nosiče UDI-R, který není tajný a jedná se o jedinečný identifikátor disku zapisovatelného nebo přepisovatelného disku. Když však servisní středisko povolí aktivum/stopu, tak se na disku uloží klíč AK. Navíc se na zkopírovaném disku uloží odlišný identifikátor super distribuce SD-ID'. SD-ID' se může vytvořit v záznamovém zařízení, ale lze jej získat také prostřednictvím nějaké komunikace se servisním střediskem. V prvním případě je potřeba ho přenést do servisního střediska přes zabezpečený ověřený kanál.

Obr. 4 ukazuje kroky pro kopírování uživatelských dat uložených na prvním nosiči dat reprodukováných přehrávačem na druhý nosič dat, přičemž záznam obstarává záznamové

zařízení. V prvním kroku se obsah prvního nosiče dat přenesse v zašifrované verzi na záznamové zařízení a zaznamená se na druhý nosič dat. Ve druhém kroku vrátí záznamové zařízení jedinečný identifikátor UDI-R druhého nosiče dat (cílového disku) tak, aby bylo možné super distribuovanou kopii povolit pouze na tomto disku. V kroku 3 vrátí přehrávač informace, které se požadují pro povolení super distribuované kopie. Tyto informace obsahují kódovou hodnotu, např. hash nebo funkci F, která obsahuje jedinečný identifikátor nosiče UDI-RI prvního nosiče dat, aby se identifikoval tento konkrétní zdrojový disk, jedinečný identifikátor nosiče UDI-R druhého nosiče, aby se identifikoval tento konkrétní cílový disk, a identifikátor super distribuce SD-ID, aby se zajistilo, že kódovou hodnotu nebo výsledek hashe mohl vypočítat pouze spolupracující přehrávač. Kód může vypočítat pouze spolupracující přehrávač, protože pouze spolupracující přehrávač může získat SD-ID. Dále se pošle jedinečný identifikátor nosiče UDI-RO, které bude později vyžadovat servisní středisko pro ověření kódové hodnoty (výsledku hashe), a datového identifikátoru ID titulu, který požaduje servisní středisko pro určení identifikátoru super distribuce SD-ID, na záznamové zařízení a uloží se na druhém nosiči dat. Volitelně může být UDI-R také poskytnuto v čisté formě ve druhé komunikaci z přehrávače do záznamového zařízení.

Na obr. 5 jsou zobrazeny kroky pro povolení druhého nosiče dat. Záznamové zařízení nejprve pošle informace požadované pro povolení kopie do servisního střediska, přičemž informace zahrnují kódovou hodnotu F, identifikátor originálního nosiče UDI-RO a datový identifikátor ID titulu. K těmto informacím se přidá identifikátor zkopírovaného nosiče UDI-R, aby se servisnímu středisku umožnilo ověřit

15.10.02

kódovou hodnotu (výsledek hashe). Pro přenos dat se nastaví zabezpečený ověřený kanál SAC pro identifikaci žádajícího záznamového zařízení, a také pro pozdější použití. Takový zabezpečený ověřený kanál SAC je rozhraní, které lze použít pro bezpečný přenos dat.

V dalším kroku určí servisní středisko z datového identifikátoru ID titulu identifikátor super distribuce SD-ID a aktivní klíč AK, přednostně použije databázi, a ověří kódovou hodnotu (výsledek hashe). Spolu s přidělenými výhodami, pokud existují, se v servisním středisku v tomto kroku uloží také identifikátor originálního nosiče UDI-RO.

Nakonec v posledním kroku vrátí servisní středisko aktivní klíč AK, práva zakoupená záznamovým zařízením a další identifikátor super distribuce SD-ID'. Do této transakce lze navíc zahrnout i určitý druh převodu peněz. Zabezpečený ověřený kanál SAC tak zajišťuje, že tuto informaci může získat pouze spolupracující záznamové zařízení.

Obr. 6 dále vysvětluje kroky pro shromažďování výhod v prvním provedení. V prvním kroku pošle přehrávač reprodukcující originál do servisního střediska informace požadované pro shromažďování výhod. Tyto informace zahrnují další kódovou hodnotu nebo hash, který je jiný, než je kódová hodnota zobrazená na obr. 4 a 5. Hash používaný pro shromažďování výhod obsahuje identifikátor originálního nosiče UDI-RO pro identifikaci disku, pro který se výhody shromažďují, a identifikátor super distribuce SD-ID originálu pro zajištění toho, že výsledek hashe mohl vypočítat pouze spolupracující přehrávač. Dále tyto informace přenášené do servisního střediska obsahují UDI-RO,

15.10.02

které bude dále servisní středisko vyžadovat k ověření výsledku hashe, a datový identifikátor ID-titulu, který servisní středisko vyžaduje k určení identifikátoru super distribuce SD-ID. Znovu se založí zabezpečený ověřený kanál SAC pro identifikaci zdrojového přehrávače a pro použití, později v kroku 3.

Ve druhém kroku určí servisní středisko z datového identifikátoru ID-titulu identifikátor super distribuce SD-ID, přednostně z databáze, a ověří výsledek hashe. Z identifikátoru nosiče UDI-RO se potom určí výhody, znovu přednostně z databáze. Ve třetím kroku se přehrávači vrátí výhody nebo přehled stavu výhod pomocí zabezpečeného ověřeného kanálu SAC, který zaručuje, že tuto informaci přijme správný spolupracující přehrávač. V závislosti na obchodních požadavcích mohou být výhody spojeny se zdrojovým diskem nebo s přehrávačem, nikoliv pouze s diskem.

Provedení zobrazené na obr. 4 až 6 a popsané výše používá pro zavedení zabezpečeného ověřeného kanálu (SAC) šifrování s asymetrickými klíči a umožňuje kopírování pouze z originálního disku. Dále výrobci zařízení nejsou v procesu transakcí. Vynález však není omezen na systém a způsob s těmito vlastnostmi. Vynález lze také použít pouze se šifrováním se symetrickými klíči, kde je možné kopírování také u již zkopírovaných disků. Dále do procesu transakcí mohou být zahrnuti také výrobci zařízení, jak ukazují obrázky 7 až 9 a jak bude popsáno v následujícím provedení.

Obr. 7 ukazuje kroky pro postup kopírování podle druhého provedení vynálezu. V kroku 1 se v zašifrovaném tvaru přenese do záznamového zařízení obsah prvního nosiče dat. V kroku 2 vrátí opět záznamové zařízení identifikátor

15.10.02

nosiče UDI-R cílového disku, aby mohla být super distribuovaná kopie povolena pouze na tomto disku. V kroku 3 vrátí přehrávač informace požadované pro povolení super distribuované kopie, přičemž informace obsahují hash (funkci F) identifikátoru nosiče UDI-RO, pro identifikaci konkrétního zdrojového disku, identifikátor nosiče UDI-R, pro identifikaci konkrétního cílového disku, a identifikátor super distribuce SA-ID, aby se zajistilo, že výsledek hashe mohl vypočítat pouze spolupracující přehrávač a že hashovací funkci může invertovat pouze držitel práv (přednostně pomocí databáze). Před tím, než se informace přenesou na záznamové zařízení, se výsledek hashe případně zašifruje použitím přehrávacího klíče super distribuce SDPK, který je jedinečný pro každý přehrávač, aby se zaručilo, že výrobci přehrávače a záznamového zařízení budou mít v povolovací fázi procesu symetrickou roli. Dále se do záznamového zařízení přenesou identifikátor nosiče UDI-ROM, který bude později vyžadovat servisní středisko pro určení identifikátoru super distribuce SD-D, stejně jako identifikátor přehrávače ID-přehrávače pro identifikaci zdrojového přehrávače. Samozřejmě může být během druhé komunikace dodáno z přehrávače do záznamového zařízení také UDI-R.

Obr. 8a ukazuje kroky pro povolení podle tohoto provedení. V prvním kroku pošle záznamové zařízení informace vyžadované pro povolení kopie. K těmto informacím se přidá UDI-R, aby se umožnilo servisnímu středisku ověřit výsledek hashe. Před zasláním se výsledek hashe zašifruje klíčem záznamového zařízení super distribuce SDRK, aby se zaručilo, že informace poslalo konkrétní záznamové zařízení. Dále se přidá identifikátor záznamového zařízení ID záznamového zařízení, aby se identifikovalo zdrojové záznamové zařízení. Ve druhém kroku kontaktuje servisní středisko výrobce

přehrávače a záznamového zařízení, aby dešifrovali výsledek hashe, a následně určí z datového identifikátoru ID titulu identifikátor super distribuce SD-ID a aktivní klíč AK, přednostně pomocí databáze, a ověří výsledek hashe. V servisním středisku se s identifikátorem nosiče UDI-RO dodaným záznamovým zařízením uloží přidělené výhody.

Ve třetím kroku vrátí servisní středisko aktivní klíč AK a práva zakoupená záznamovým zařízením. Tyto informace se nejprve zašifrují pomocí klíče odvozeného z identifikátoru nosiče UDI-R, aby se zajistilo, že tuto informaci výrobce záznamového zařízení nezneužije. Zašifrované informace poté dále zašifruje výrobce záznamového zařízení, aby se zaručilo, že tyto informace může přijmout pouze správné záznamové zařízení. Šifrování zajistí, že informace vrácené servisním střediskem se mohou použít pouze pro povolení konkrétní kopie, jmenovitě té, která je identifikována UDI-R.

Obr. 8b ukazuje komunikaci mezi servisním střediskem a výrobcem záznamového zařízení nebo přehrávače během šifrování.

Obr. 9a ukazuje kroky pro shromažďování výhod podle druhého provedení. Zde pošle v kroku 1 přehrávač servisnímu středisku informace požadované pro shromažďování výhod. Tyto informace zahrnují hash, který obsahuje identifikátor nosiče UDI-RO pro identifikaci disku, pro který se výhody shromažďují, a identifikátor super distribuce SD-ID pro zajištění, že výsledek hashe mohl vypočítat pouze spolupracující přehrávač a že hashovací funkci může invertovat pouze vlastník práv. Dále informace přenášené do servisního střediska zahrnují identifikátor nosiče UDI-RO,

15.10.02

který bude později servisní středisko požadovat pro ověření výsledku hashe a datový identifikátor ID titulu, který servisní středisko požaduje pro určení identifikátoru super distribuce SD-ID. Před přenosem se výsledek hashe zašifruje klíčem přehrávače super distribuce, aby se zaručilo, že tuto informaci posílá spolupracující přehrávač.

Ve druhém kroku kontaktuje servisní středisko výrobce přehrávače, aby dešifroval výsledek hashe, a následně určí z datového identifikátoru ID titulu identifikátor super distribuce SD-ID, přednostně pomocí databáze, a ověří výsledek hashe. Navíc se z identifikátoru nosiče UDI-RO určí výhody, přednostně pomocí databáze.

Ve třetím kroku se přehrávači vrátí výhody nebo přehled stavu výhod. Před přenosem informací se nejprve klíčem odvozeným z identifikátoru nosiče UDI-RO zašifrují, aby se zajistilo, že tyto informace nemůže výrobce přehrávače zneužít. Výrobce záznamového zařízení provede druhé zašifrování těchto informací, aby se zaručilo, že tyto informace může přijmout pouze správný přehrávač.

$E\{SDRK\}$ a $E\{SDPK\}$ označují symetrické šifrování. Je samozřejmě také možné použít již přítomného asymetrického šifrování nebo SAC. Jelikož by měl být aktivní klíč AK tajný, tak může být při komunikaci s výrobcem záznamového zařízení chráněn zašifrováním UDI-R(O). UDI na disku nemusí být tajné. Zašifrováním pomocí UDI-R(O) však získáme zvýšenou úroveň zabezpečení, jelikož výrobce záznamového zařízení nezná UDI používané během super distribuce.

Obr. 9b ukazuje komunikaci mezi servisním střediskem a výrobcem záznamového zařízení nebo výrobcem přehrávače pro

15.10.02

šifrování.

Podle tohoto vynálezu je navržen způsob a systém pro zabezpečenou super distribuci uživatelských dat. V něm se mohou realizovat různé obchodní modely, ve kterých se obsahy distribuují řízeným domácím kopírováním. Kopie zůstávají nehratelné, dokud se nedokončí správná transakce. Dále se díky přímému kontaktu mezi vlastníkem obsahu a spotřebitelem zajišťují nové obchodní možnosti. Pro kopírování uživatelských dat se mohou spotřebitelům dávat podněty. Např. kopie mohou být levnější než originály a vlastníkům originálů se mohou poskytovat výhody, jako volný přístup k přístupovým kódům pro bonusové stopy nebo slevy pro příští nákupy ("zvukové kilometry"). Dále je takovýto způsob super distribuce vhodnější, než stahování celého alba z Internetu.

Pro atraktivitu originálů lze přijmout různá opatření, například tím, že se pro super distribuci určí pouze originály, čímž se zamezí "tovární" super distribuci.

Způsob a systém podle tohoto vynálezu lze použít pro sbírání obchodních informací, např. pomocí hudebních kilometrů. Zařízení použité pro transakce může zůstat anonymní, nebo nemusí. Dále je možné se rozhodnout, zda lze umožnit kopírování pro super distribuce online, nebo také offline. Celkově tedy vynález umožňuje řízení kopírování, která se uskutečňuje přes obsah s řízeným přístupem.

Zastupuje:

Dr. Pavel Zelený v.r.

PATENTOVÉ NÁROKY

1. Způsob pro zabezpečenou super distribuci uživatelských dat uložených na prvním nosiči dat obsahující kroky:

a) zkopírování uživatelských dat z prvního nosiče dat na druhý nosič dat;

b) uložení na druhý nosič dat informací, které jsou vyžadovány servisním střediskem pro přidělení přístupových práv ke kopii uživatelských dat; a

c) získání přístupových práv ke kopii uživatelských dat přenesením alespoň uložených informací do servisního střediska, ukončení transakce a přijetí přídatných přístupových informací;

vyznačující se tím, že servisní středisko používá uložené informace pro přidělení přístupových práv kopii uživatelských dat druhého nosiče dat.

2. Způsob podle nároku 1, **vyznačující se tím**, že přístup k uživatelským datům uloženým na prvním nosiči dat je řízen správou digitálních dat nebo systémem podmíněného přístupu.

3. Způsob podle nároků 1 nebo 2, **vyznačující se tím**, že každý z prvního a druhého nosiče dat obsahuje jedinečný identifikátor nosiče, a uložené informace se skládají lespoň z kódové hodnoty určené alespoň z jedinečného identifikátoru nosiče prvního a druhého nosiče dat.

4. Způsob podle nároku 3, **vyznačující se tím**, že jedinečné identifikátory nosiče se také přenášejí do

servisního střediska.

5. Způsob podle nároků 3 nebo 4, *vyznačující se tím*, že první nosič dat obsahuje identifikátor super distribuce, který se používá pro určení kódové hodnoty.

6. Způsob podle nároku 3, *vyznačující se tím*, že před uložením na druhý nosič dat je kódová hodnota zašifrována klíčem přehrávače super distribuce, a zašifrovaná kódová hodnota se před přenosem do servisního střediska dále zašifruje klíčem záznamového zařízení super distribuce.

7. Způsob podle nároku 6, *vyznačující se tím*, že identifikátor přehrávače odpovídající klíči přehrávače super distribuce se uloží na druhý nosič dat, a identifikátor přehrávače a identifikátor záznamového zařízení odpovídající klíči záznamového zařízení super distribuce se přenesou do servisního střediska.

8. Způsob podle nároku 7, *vyznačující se tím*, že dešifrování zašifrované kódové hodnoty je provedeno výrobcí přehrávače, a/nebo respektive záznamového zařízení.

9. Způsob podle nároků 1 nebo 2, *vyznačující se tím*, že servisní středisko odměňuje vlastníka prvního nosiče dat jako odpověď na zakončený proces zabezpečené super distribuce uživatelských dat uložených na prvním nosiči dat.

10. Způsob podle nároku 9, *vyznačující se tím*, že kódová hodnota odměny generovaná alespoň z jedinečného identifikátoru nosiče dat se přenáší do servisního střediska

15.10.02

pro shromažďování přidělených výhod.

11. Způsob podle nároku 1 nebo 2, *vyznačující se tím*, že jako datové nosiče jsou použity optické disky, konkrétně zapisovatelná a/nebo přepisovatelná CD nebo DVD.

12. Způsob podle nároku 1 nebo 2, *vyznačující se tím*, že uživatelská data jsou audio data, video data nebo software.

13. Způsob podle nároku 1, *vyznačující se tím*, že servisní středisko používá uložené informace pouze pro přidělování přístupových práv ke kopii uživatelských dat na druhém nosiči dat.

14. Systém pro zabezpečenou super distribuci uživatelských dat uložených na prvním nosiči dat obsahující

a) přehrávač a záznamové zařízení pro kopírování uživatelských dat z prvního nosiče dat na druhý nosič dat a pro ukládání super distribuovaných dat na druhý nosič dat;

b) přenosové prostředky pro přenášení uložených super distribuovaných dat do servisního střediska; a

c) servisní středisko pro přidělování přístupových práv ke kopii uživatelských dat na druhém nosiči dat,

kde přehrávač je opatřen pro určení kódové hodnoty alespoň z jedinečných identifikátorů nosiče prvního a druhého nosiče dat, a záznamové zařízení je opatřeno pro uložení alespoň kódové hodnoty a jedinečného identifikátoru prvního nosiče dat na druhý nosič dat.

15. Zařízení pro reprodukci a/nebo záznam uživatelských dat pro použití v systému podle nároku 14.

15.10.02

16. Nosič dat pro ukládání uživatelských dat a dat super distribuce pro použití ve způsobu pro zabezpečenou super distribuci podle nároku 1, přičemž data super distribuce obsahují

a) jedinečný identifikátor nosiče identifikující nosič dat,

b) datový identifikátor identifikující uživatelská data uložená na nosiči,

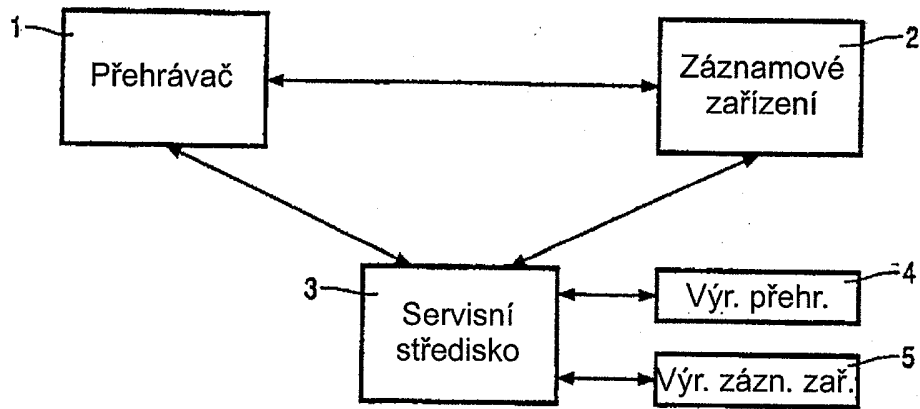
c) identifikátor super distribuce používaný pro zajištění funkcí super distribuce; a

d) jeden nebo více klíčů pro šifrování uživatelských dat a/nebo dat super distribuce.

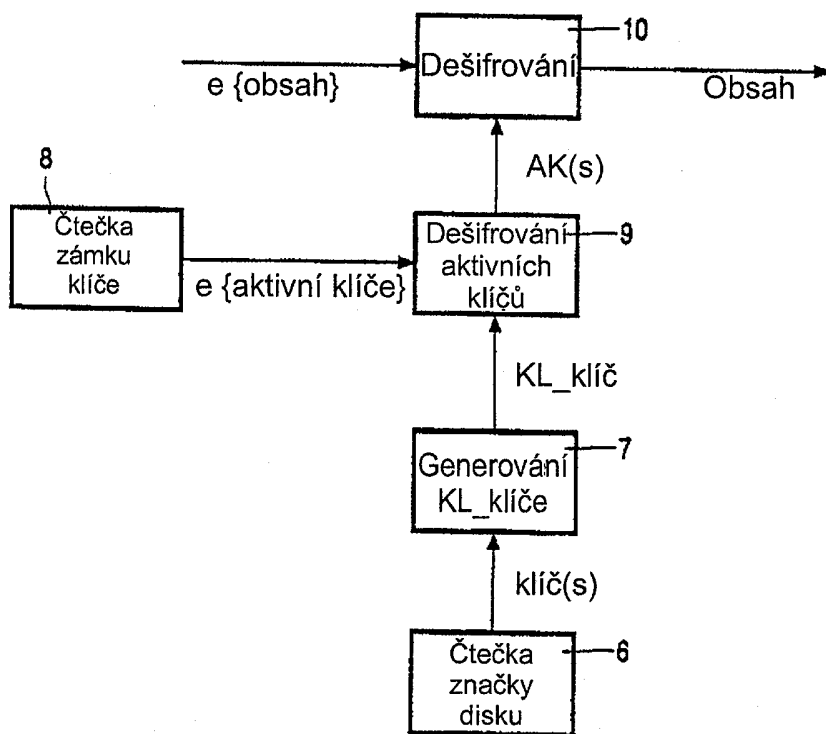
Zastupuje:

Dr. Pavel Zelený v.r.

1/6

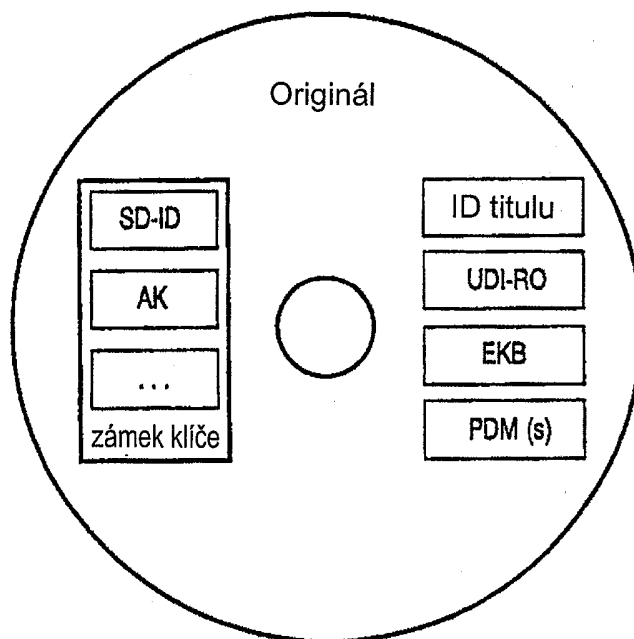


Obr. 1

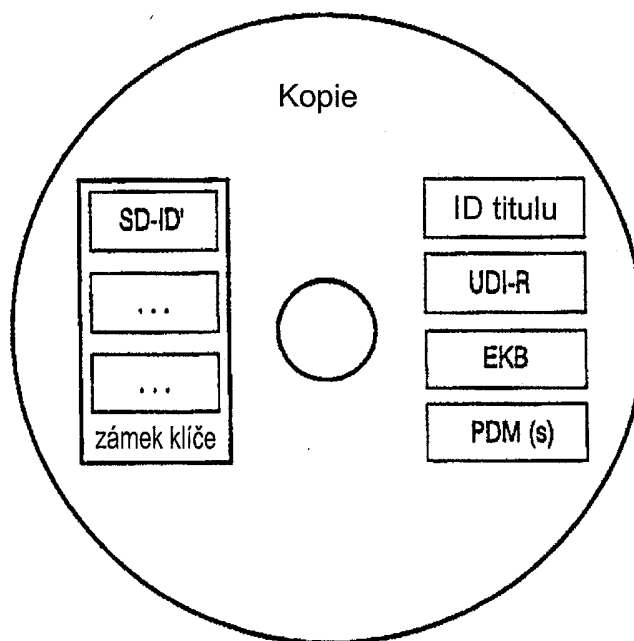


Obr. 2

2/6



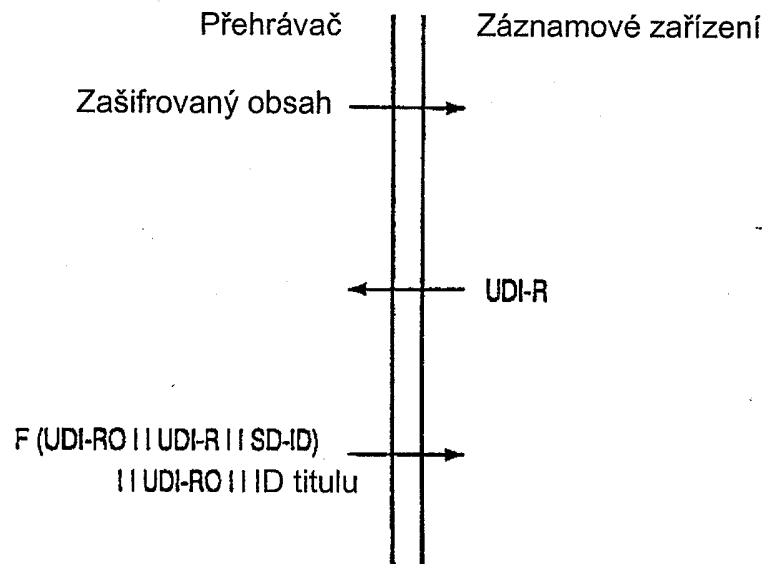
Obr. 3A



Obr. 3B

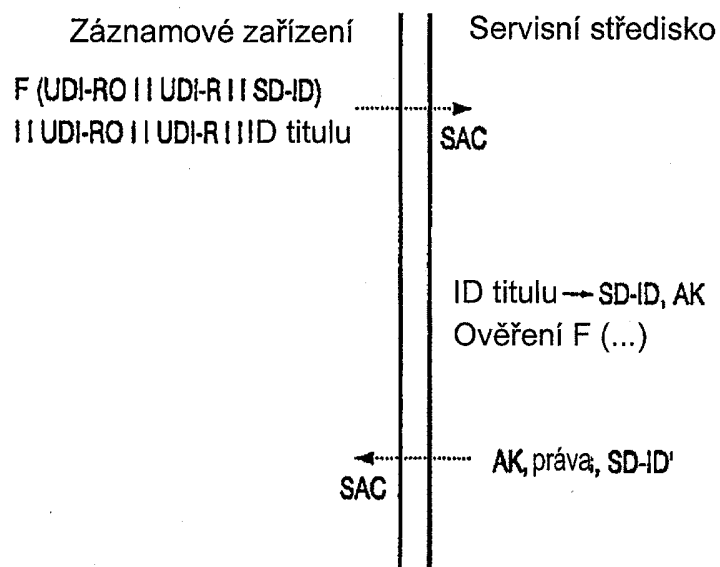
3/6

Kopírování



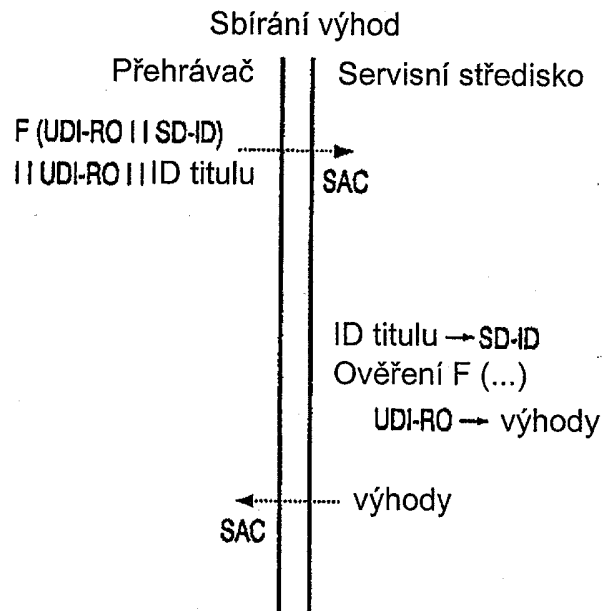
Obr. 4

Povolování

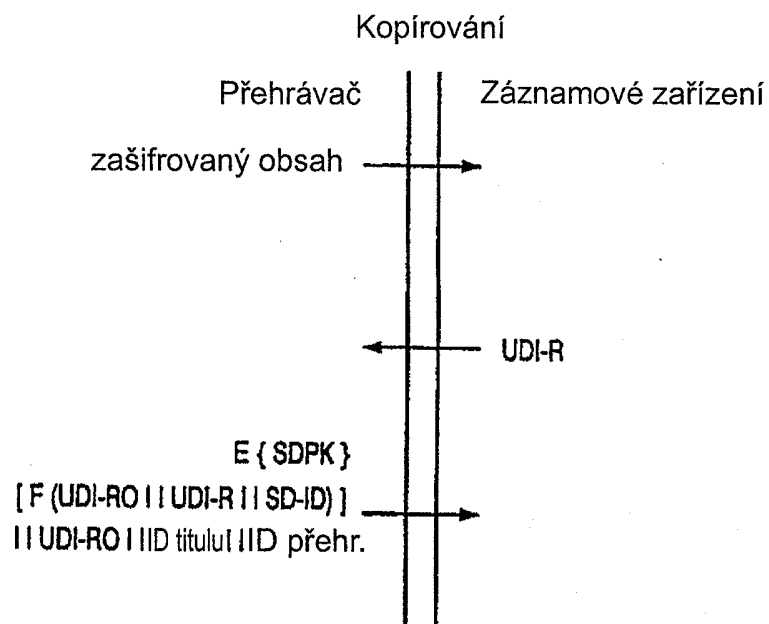


Obr. 5

4/6



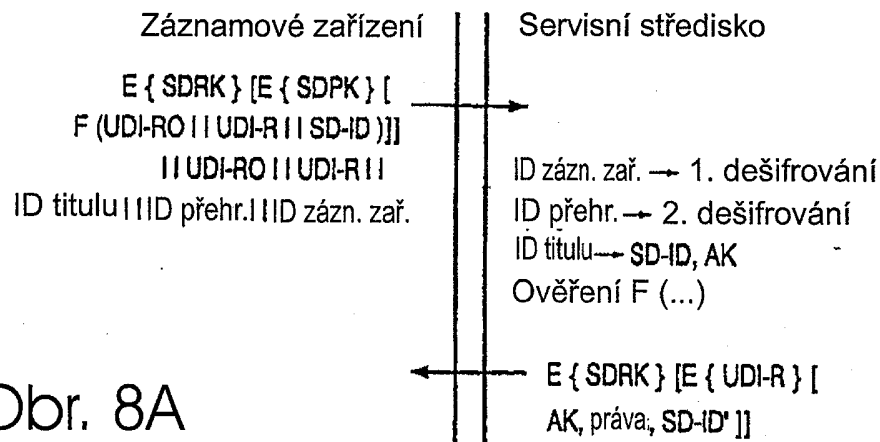
Obr. 6



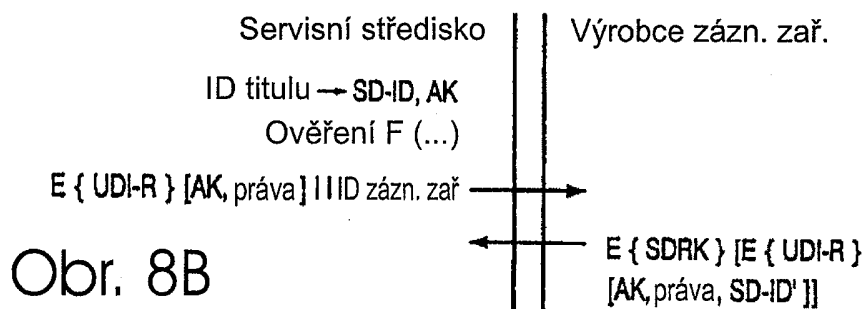
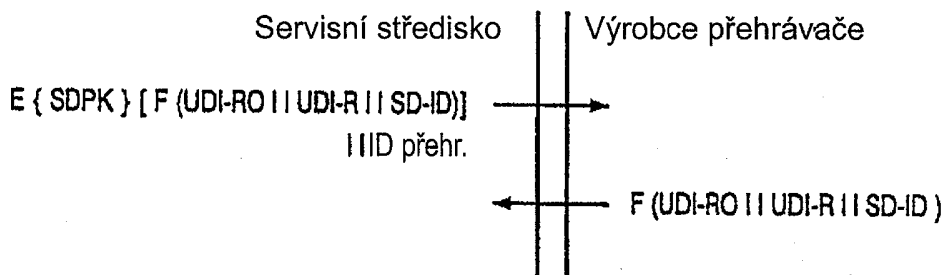
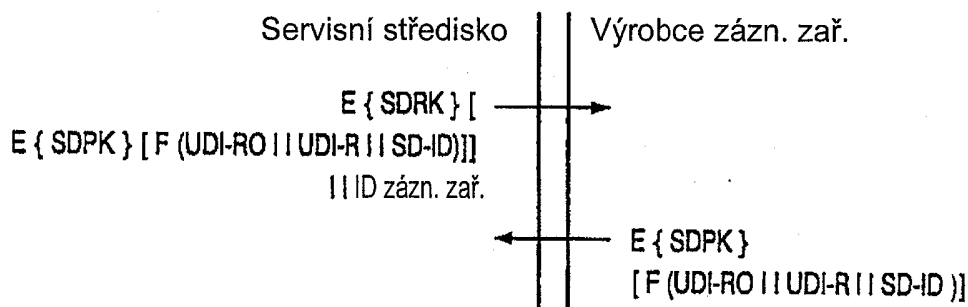
Obr. 7

5/6

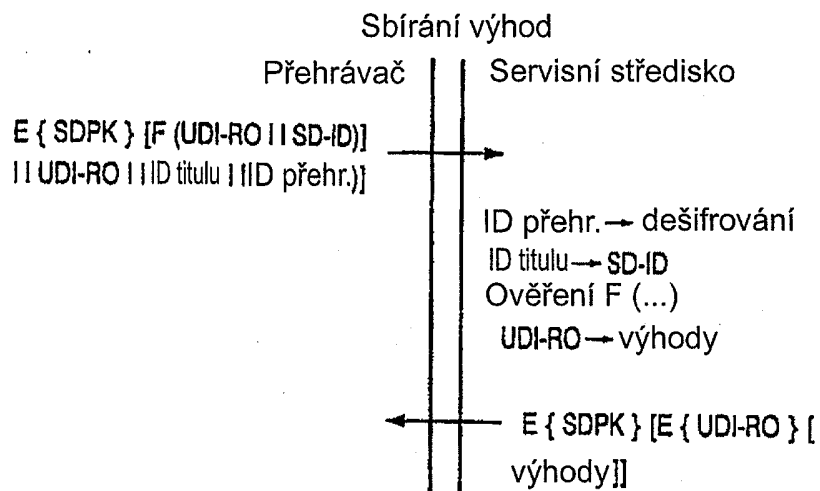
Povolování



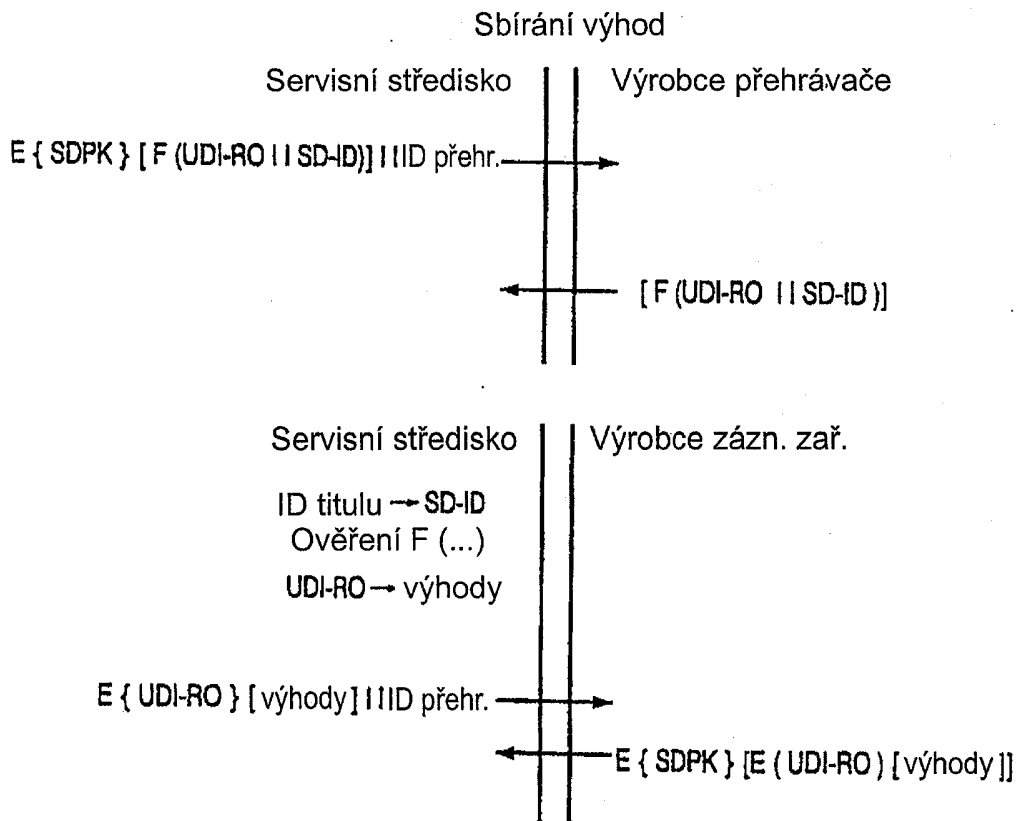
Povolování



6/6



Obr. 9A



Obr. 9B