

Komise pro informační technologie (KIT) AV ČR schválila dne 27.9.2006 následující doporučení ústavům AV ČR pro zajištění legálního užívání softwaru podléhajícího ochraně podle autorského práva

A. Zásady a výchozí předpoklady stanoviska KIT

A1. Právní aspekty odpovědnosti za nelegální užívání softwaru

(1) Odpovědnost fyzických a právnických osob za takové užívání softwaru, které je v rozporu se zákonem č. 121/2000 Sb. o právu autorském v platném znění (dále jen autorský zákon) a které lze kvalifikovat jako neoprávněný zásah do autorských práv, lze rozlišit na:

- a) přestupkovou odpovědnost podle autorského zákona, zejména §40, dále podle §105a (přestupek fyzické osoby), §105b (správní delikt právnických a podnikajících fyzických osob) a podle zákona č. 200/1990 Sb. o přestupcích v platném znění, §32 (přestupek na úseku kultury)
- b) trestní odpovědnost ve smyslu §152 trestního zákona č. 140/1961 Sb. v platném znění
- c) hmotnou odpovědnost za škodu podle občanského zákoníku č. 40/1964 Sb. v platném znění a obchodního zákoníku č. 513/1991 Sb. v platném znění, způsobenou nositeli autorských práv tím, že nelegálně užívaný software nebyl zakoupen a používán v souladu s autorským právem.

(2) Užitím softwarového produktu jakožto díla ve smyslu autorského zákona a tedy zásahem do autorských práv dle §§12-14 zák.č.121/2000 Sb. je provozování produktu i jeho nainstalování.

(3) Trestní odpovědnost je vždy individuální odpovědností fyzické osoby, která software instaluje nebo používá. Neoprávněné zasahování do autorských práv může být trestným činem podle §152 tr. zák. bez ohledu na hodnotu autorského díla nebo výši způsobené škody.

(4) Plnění hmotné odpovědnosti za škodu způsobenou nelegálním užíváním softwaru v souvislosti s pracovní činností v pracovním poměru může být vymáháno na zaměstnavateli, stejně jako pokuta za spáchání takového přestupku. Pokud zaměstnavatel uhradil vlastníku nebo oprávněnému držiteli licence k softwaru škodu způsobenou nelegálním užitím softwaru, nebo zaplatil pokutu za nelegální užití softwaru, může požadovat na svém zaměstnanci, který je za vzniklou situaci a škodu odpovědný, aby ji uhradil v rozsahu a za podmínek upravených v zákoníku práce. Odpovědnost konkrétních osob může být upravena vnitřními směrnici instituce stanovenými statutárním zástupcem.

(5) Jsou-li splněny právní předpoklady pro to, aby licenční podmínky softwaru měly právní charakter dohody mezi osobou užívající software jakožto autorské dílo a nositelem autorských práv, platí tyto podmínky v tom rozsahu, v jakém zákony ČR poskytují prostor pro upřesnění takového právního vztahu formou dohody. Ustanovení licenčních podmínek, které by byly v rozporu se zákony ČR, jsou irelevantní. To nemusí platit v plném rozsahu v těch případech, kdy smluvními stranami nejsou výhradně české právnické nebo fyzické osoby a platná smlouva explicitně stanoví, že licenční podmínky se řídí právními předpisy jiného státu. Taková smlouva pak podléhá právní úpravě příslušného státu a platným relevantním mezinárodním dohodám, pokud takové existují.

A2. Základní požadavky a cíle vytvoření vnitřní směrnice instituce o legálním užívání softwaru

(1) Účelem vnitřní směrnice instituce ve věci užívání softwaru by mělo být stanovení konkrétní a trvalé odpovědnosti jednotlivých osob za užívání softwaru na jednotlivých počítačích v souladu s autorským právem, a to tak, aby nejen trestní odpovědnost, ale i odpovědnost za škodu vzniklou držiteli autorských práv v souvislosti s případným neoprávněným zásahem do těchto práv byla jednoznačně přiřazena konkrétním osobám, fyzickým nebo právnickým, které jsou ve smluvním vztahu k instituci.

(2) Směrnicí je vhodné upravit pravidla užívání softwaru (včetně instalace), jakož i kompetence osob, které

software užívají, a to pro ty druhy softwaru, které jsou autorským dílem ve smyslu autorského zákona a u nichž konkrétně přichází v úvahu možnost neoprávněného zasahování do autorských práv v souvislosti s pracovní činností. V praxi postačuje směrnicí vymezit užívání takového softwaru, jehož užití pro pracovní činnost v dané instituci vyžaduje zakoupení placené licence, tj. jehož užití bez zakoupení takové licence by bylo neoprávněným zasahováním do autorských práv. Směrnice může explicitně vynechat software užívaný v souladu se smlouvou typu Microsoft Campus Agreement a software, u něhož je oprávněnost užití zajištěna licenčním serverem nebo jinými technickými prostředky.

(3) Směrnice by měla respektovat potřeby vědecké práce a specifické podmínky v jednotlivých ústavech tak, aby omezení a administrativní zátěž vyplývající ze směrnice byla minimální při splnění hlavního účelu směrnice (část A2, odst. (1)) a zajištění její právní validity a konsistence.

(4) Aby odpovědnost konkrétních osob za legální užívání softwaru na jednotlivých počítačích mohla být jednoznačná a trvalá a představovala minimální dodatečnou administrativní zátěž, je nezbytné, aby

- a) vymezení odpovědnosti každé osoby za užívání softwaru korespondovalo se skutečným rozsahem jejich uživatelských a administrátorských činností, kompetencí, povinností a přístupových práv,
- b) těmto osobám byly pro zajištění uvedené odpovědnosti vytvořeny přiměřené podmínky.

A3. Evidence softwaru

(1) Zákon neukládá povinnost vést zvláštní evidenci softwaru, předpokládá však schopnost fyzické i právnické osoby užívající dílo ve smyslu autorského zákona prokázat oprávněnost užití. Nejsnazší způsob prokázání oprávněnosti užití je nalezení a předložení nabývacího dokladu. Z toho vyplývá, že pro každý počítač by měla existovat nějaká forma evidence softwarových produktů, jejichž legální užití v instituci vyžaduje zakoupení licence.

(2) Každá forma evidence by měla splňovat následující požadavky:

- a) měla by pro každou instalaci takového softwarového produktu na konkrétním počítači obsahovat informaci potřebnou pro snadné vyhledání nabývacího dokladu v archivu instituce, a tím se snadno vypořádat s případným podezřením nebo obviněním z neoprávněného zasahování do autorských práv,
- b) pro osobu odpovědnou za legální užívání softwaru na daném počítači by měla poskytovat jednoznačný doklad oprávněnosti užití,
- c) měla by pomoci snadno udržet přehled a zajistit, aby nebyl nedopatřením užíván software v rozporu s autorským právem.

(3) Není účelné kombinovat evidenci softwaru s evidencí hardwaru. Pro evidenci hardwaru postačuje běžná forma evidence majetku.

(4) Evidence softwaru, má-li sloužit pro prokázání oprávněnosti užití, vyžaduje evidenci od nulové hodnoty a dlouhodobou archivaci nabývacích dokladů. V těch případech, kdy je užití softwaru vázáno na konkrétní hardware (tzv. OEM software), je zapotřebí, aby software byl explicitně uveden na nabývacím dokladu příslušného hardwaru (např. dodacím listu) a aby originál tohoto dokladu byl dlouhodobě archivován a evidován jako nabývací doklad softwaru. Pro účely evidence hmotného majetku lze tento doklad nahradit kopií s poznámkou o umístění originálu.

B. Doporučené kroky k zajištění legálního užívání softwaru, doporučený obsah vnitřní směrnice

B1. Poučení zaměstnanců, vymezení softwaru podléhajícího směrnici, stanovení způsobu archivace nabývacích dokladů pořizovaného softwaru

(1) Zaměstnanci by měli být poučeni o charakteru právní odpovědnosti ve smyslu části A1 odst. (1) a (2)

a o nutnosti brát v omezeném rozsahu podle části A1 odst. (4) v úvahu licenční podmínky distribuované nositelem autorských práv.

(2) Software podléhající směrnici může být obecně vymezen podle části A2 odst. (2), tj. jako software, jehož legální užití pro účely související s pracovní činností v instituci vyžaduje zakoupení licence.

(3) Způsob archivace nabývacích dokladů softwarových produktů by měl být takový, aby nedocházelo k jejich skartování a aby umožňoval vyhledávání, např. podle interního čísla faktury.

B2. Stanovení odpovědných osob, jejich práv, povinností a podmínek vykonávání

(1) Pro každý jednotlivý počítač by měla být stanovena *odpovědná osoba*, případně více takových osob s jasně rozlišenou odpovědností podle odst. A2 odst. (4). Aby vymezení odpovědnosti těchto osob mohlo být reálné a trvalé, je nezbytné, aby korespondovalo se skutečným rozsahem jejich uživatelských a administrátorských činností, kompetencí, povinností a přístupových práv. Konkrétně, odpovědnost by měla v případě každého počítače nést ta osoba (fyzická osoba - zaměstnanec instituce, nebo právnická osoba vázaná smlouvou o poskytování softwarových služeb – outsourcingu), která ve skutečnosti daný počítač softwarově administruje, nebo rozhoduje o administrátorských úkonech, a může za legalitu softwaru trvale ručit. V případech, kdy více osob užívá a v nějaké míře i administruje jeden počítač, je vhodné využít technických prostředků, zejména přístupových práv v rámci vhodně zvolených operačních systémů, k oddělení oblastí kompetencí a tím i odpovědnosti.

(2) Nevhodné a nebezpečné je takové vymezení odpovědnosti, které je buď pouze formálního charakteru, tj. odpovědnými činí osoby, které o užívání daného počítače fakticky nemají přehled, nebo je reálné pouze v okamžiku nějaké – vždy technicky pochybné – kontroly, příp. nějaké formy auditu. Právní následky takového stavu jsou naznačeny v části C.

(3) Pro zajištění právní validity vymezení odpovědnosti konkrétní osoby musí být zajištěno:

- a) aby nikdo bez jejího vědomí neprováděl instalace softwaru podléhajícího směrnici, a to nejlépe současně zahrnutím této podmínky (tj. zákazu instalace softwaru bez souhlasu *odpovědné osoby*) do vnitřní směrnice a – je-li možno – využitím přístupových/administrátorských práv,
- b) aby *odpovědná osoba* měla kdykoli možnost jednoznačně zjistit, a v případě potřeby doložit, zda určitý software podléhající směrnici byl řádně zakoupen a zda licence potřebná k legálnímu nainstalování už nebyla použita pro jiný počítač. K tomu by měl sloužit systém evidence softwaru.

(4) Využívá-li *odpovědná osoba* přístupových práv administrátora k datovým oblastem jiných osob (uživatelů), má povinnost dbát na ochranu osobních údajů, ochranu osobnosti, respektování obsahu e-mailových zpráv a ochranu duševního vlastnictví podle zák. č. 101/2000 Sb. v platném znění, §§11-17 zák. č. 40/1964 Sb. v platném znění, Listiny základních práv a svobod, zák. 121/2000 Sb. v platném znění a souvisejících zákonů.

(5) *Odpovědná osoba* má povinnost dbát na bezpečnost svěřeného počítače minimálně v rozsahu stanoveném správcí sítě, do níž je daný počítač zapojen.

(6) Vnitřní směrnice by měla stanovit, kdo rozhoduje o přiřazení *odpovědných osob* jednotlivým počítačům (zejména v nejasných případech) a jakým způsobem a na jaké administrativní úrovni bude vedena evidence o *odpovědných osobách* pro jednotlivé počítače.

B3. Stanovení formy evidence softwaru

(1) Systém evidence by měl splňovat požadavky části A3 a části B2 odst. (3b).

Ve skutečnosti přichází v úvahu systém evidenčního listu u každého počítače, nebo systém certifikátů pro každou licenci softwarového produktu. V případě systému evidenčních listů je však obtížné zajistit jednoduché ověření počtu instalací v případě multilicencí a rovněž je obtížné zajistit, aby systém poskytoval právní jistotu

a ověřitelnost legality instalací *odpovědným osobám* pro jednotlivé počítače. V praxi by si *odpovědná osoba* musela po každé instalaci a zapsání instalace do evidenčního listu vyžádat podpis příslušné k tomu zmocněné osoby z oddělení nákupu, která by sama musela mít evidenci o provedených instalacích, zejména v případě multilicencí.

(2) Jako jednoduchý systém splňující uvedené nároky a zajišťující právní validitu vymezení odpovědnosti lze doporučit systém certifikátů vydávaných oddělením nákupu v okamžiku zaevidování softwaru. Certifikátem může být např. kopie dodacího listu nebo faktury a navíc musí obsahovat:

- a) interní evidenční číslo faktury podle něhož lze v archivu dohledat originál nabývacího dokladu
- b) pořadové číslo v případě multilicencí, kdy je certifikátů na jeden nabývací doklad vydáno právě tolik, kolik bylo zakoupeno licencí,
- c) podpis osoby zmocněné k vydávání těchto certifikátů.

(3) *Odpovědná osoba* uchovává certifikáty instalovaného softwaru pro každý počítač ve složce na bezpečném místě a na požádání nadřízených nebo statutárního zástupce pomocí certifikátů prokáže legalitu softwaru užívaného na daném počítači.

(4) Při přenesení licence z jednoho počítače na druhý, je-li takový postup v daném případě v souladu se zákonem a relevantními částmi licenční smlouvy, je softwarový produkt na původním počítači vymazán, certifikát vyřazen ze složky původního počítače a zařazen do složky druhého počítače, kde je software znovu nainstalován.

(5) Vzhledem k právní validitě vymezení odpovědnosti konkrétních *odpovědných osob* za užívání softwaru v souladu s autorským právem není nutná centrální registrace instalovaného softwaru. Jestliže taková registrace je přesto vyžadována, je možné ji realizovat tak, že *odpovědná osoba* při instalaci softwarového produktu pořídí kopii certifikátu a tuto kopii opatřenou datem, evidenčním číslem počítače a svým podpisem (v případě přenesení licence z jednoho počítače na jiný navíc evidenčním číslem původního počítače a podpisem jeho *odpovědné osoby*) pošle do centrální evidence.

C. Stanovisko k ověřování souladu instalovaného a evidovaného softwaru z rozhodnutí statutárního orgánu instituce, tzv. auditů

(1) Statutární zástupce má právo dle vlastní úvahy a v mezích zákona kontrolovat dodržování směrnice, kterou vydal (příp. prostřednictvím k tomu pověřených pracovníků), tedy např. zda evidence softwaru je řádně vedena, případně zda instalovaný software na počítačích odpovídá evidenci. Přínosem auditu je získání informace o aktuálním stavu dodržování autorského zákona v instituci. Ze zákona však povinnost jakékoli formy takové kontroly (auditů) nevyplyvá.

(2) Audit může být proveden pracovníky instituce (interní audit) nebo auditorskou firmou na základě smlouvy (externí audit). Za účelem zjištění instalovaného softwaru je zpravidla používán komerční softwarový produkt, který musí být na posuzovaném počítači spuštěn jednorázově v okamžiku provádění auditu (jednorázový audit), nebo trvale jako auditní agent (trvalý audit).

(3) Při rozhodování o provádění auditu je zapotřebí vzít v úvahu řadu rizik a problémů, které může takový krok přinést po stránce technické i právní:

- a) Spuštění auditovacího softwaru představuje zásah do počítače, který může narušit funkčnost programů i operačního systému, jak dokládá řada zkušeností. Zejména u složitějších a méně obvyklých instalací a konfigurací, které jsou nezbytné pro vědeckou práci svými nároky převyšující běžné kancelářské aplikace a u počítačů užívajících alternativně nebo i současně více operačních systémů (jak je běžné zejména v matematicky a technicky orientovaných ústavech, kde neexistuje žádná "standardní instalace"), by byl audit na každém počítači spojen s nutností nestandardních úkonů s vysokou pravděpodobností narušení funkčnosti. Spuštění auditovacího softwaru, zejména v těch případech, kdy tento software realizuje jakoukoli síťovou komunikaci, může též vést k narušení bezpečnosti operačního systému a/nebo negativnímu ovlivnění bezpečnostní politiky sítě.

b) Zásah do počítače auditovacím softwarem nebo osobou provádějící audit může znamenat ohrožení informací v počítači uložených, a to i informací podléhajících ochraně podle zákona. To se týká zejména ustanovení na ochranu osobnosti (§§11-17 zák.č. 40/1964 Sb.), osobních údajů (zák.č. 101/2000 Sb., ve znění zák.č. 227/2000, 177/2001, 450/2001, 107/2002, 310/2002, 517/2002, 439/2004, 480/2004, 626/2004, 309/2005, 413/2005, 444/2005), zákona o elektronických komunikacích (zák.č. 127/2005 ve znění zák. 290/2005, 361/2005), ochrany obsahu e-mailových zpráv (Ústava ČR, Listina základních práv a svobod, články 7, 10, 13) a ochrany duševního vlastnictví, zejména se zřetelem k dílům dosud nezveřejněným (§§2-14 zák. č. 121/2000 Sb. a související zákony, např. o patentech 206/2000 Sb., 207/2000 Sb.).

(4) Důvodem k provedení auditu může být nepřehledná situace v oblasti užívání softwaru, kterou není instituce schopna řešit vymezením odpovědnosti konkrétních osob za jednotlivé počítače, případně jiným způsobem, ve spojení s důvodným podezřením z užívání softwaru v rozporu s autorským právem.

(5) Důvodem k provedení auditu pro jednotlivý počítač může být nepřehledné množství instalovaného softwaru na tomto počítači v situaci, kdy není možné nebo vhodné provést kompletní přeinstalování operačního systému a všech aplikací, které je možno legálně užívat pro daný počítač.

(6) Při jednoznačném stanovení konkrétní odpovědnosti jednotlivých osob za jednotlivé počítače má audit smysl pouze v případě, že jej vyžaduje pro daný počítač sama *odpovědná osoba*. Jinak může dojít ke zpochybnění plné odpovědnosti *odpovědné osoby* za daný počítač zasahováním do jejích kompetencí. Nežádoucími důsledky takového kroku pak může být víceméně formální a nárazové (jednorázové nebo opakované) přenášení nepřesně definované části odpovědnosti na osobu zajišťující audit, rozmělnění odpovědnosti konkrétních osob v závislosti na technických parametrech a nedostacích softwarových a dalších technických prostředků pro audit používaných a v konečném důsledku pak implicitní přenesení nedostatečně definované části odpovědnosti na statutárního zástupce. Vedle zpochybnění plné odpovědnosti *odpovědné osoby* za legalitu softwaru dochází i ke zpochybnění odpovědnosti za bezpečnost systému.

(7) Při případném rozhodování o provedení a formě auditu je zapotřebí dále brát v úvahu zejména:

- a) jaký software může být při auditu použit a kdo ručí za škody a případné ohrožení informací podléhajících ochraně podle zákona tímto softwarem způsobené,
- b) jaké osoby mohou během auditu přijít do styku s informacemi podléhajících ochraně podle zákona a zda tyto osoby mají prověrku NBÚ, případně jakého stupně,
- c) zda případný externí smluvní partner, který má provádět audit, je pojištěn pro případ způsobení škody a na jakou částku,
- d) zda v případě opakovaného nebo trvalého auditu není v rozhodnutí obsažen budoucí konflikt se zákonem o veřejných zakázkách,
- e) zda informace získané případným externím smluvním partnerem nemohou být později zneužívány pro získávání dalších zakázek,
- f) zda psychologickým důsledkem provedení auditu nebude postavení instituce do role nepřítele vlastních zaměstnanců,
- g) zda existují dostatečné důvody pro audit, které ospravedlňují vynaložené prostředky a rizika, a zda stejného výsledku nelze dosáhnout jiným způsobem.

(8) Dojde-li v souvislosti s prováděním auditu k porušení zákona, příp. ke vzniku škody, s výjimkou případů, kdy škoda byla způsobena nedodržením smlouvy smluvním partnerem resp. nedodržením pokynů nebo porušením povinnosti pracovníkem instituce, který byl pověřen zajištěním auditu, nese odpovědnost za škody vzniklé v souvislosti s prováděním auditu statutární zástupce.

(9) Tím není dotčena individuální trestní odpovědnost jednotlivých osob. V této souvislosti je na místě upozornit zejména na dva trestné činy, k nimž může dojít v souvislosti s prováděním auditu a které patří mezi závažné trestné činy podléhající oznamovací povinnosti podle trestního zákona č. 140/1961 Sb. v aktuálním znění: trestný čin neoprávněného nakládání s osobními údaji podle §178 odst. 3 tr. zák. a trestný čin ohrožení utajované informace podle §§106-107 tr. zák. Podle §168 tr. zák. se dopouští trestného činu každý, kdo se hodnověrným způsobem dozví, že jiný spáchal některý z těchto trestných činů a takový trestný čin oznámí bez odkladu státnímu zástupci nebo policejnímu orgánu.

D. Příklad vnitřní směrnice instituce o užívání softwaru v souladu s autorským právem

Tato směrnice stanovuje pravidla pro evidenci a užívání softwaru, jehož užívání představuje zásah do autorských práv podle zák. č. 121/2000 Sb. v platném znění a je vázáno na zakoupení licence. Tato směrnice se nevztahuje na software užívaný v souladu se smlouvou Microsoft Campus Agreement a na software, u něhož je oprávněnost užití zajištěna licenčním serverem nebo jinými technickými prostředky. V dalším bude pojmem software míněn pouze ten software, na nějž se vztahuje tato směrnice.

Vedoucí oddělení zajistí, aby zaměstnanci byli seznámeni s právními aspekty užívání softwaru minimálně v rozsahu doporučení KIT, části A1.

Vedoucí administrativního úseku zajistí, aby nabývací doklady obsahující práva k užití softwaru, tj. nabývací doklady k softwarovým produktům a nabývací doklady k hardwaru, který je prodáván včetně softwaru, byly archivovány odděleně od ostatních dokladů a nepodléhaly skartaci.

Budou stanoveny odpovědné osoby pro každý počítač v souladu se zásadami danými doporučením KIT, částí B2. Implicitně je odpovědnou osobou pracovník, který je uživatelem daného počítače podle evidence majetku. Pokud je to zapotřebí pro dosažení souladu s uvedenými zásadami, stanoví jinou odpovědnou osobu (jiné odpovědné osoby) vedoucí oddělení.

Odpovědná osoba trvale ručí za to, že instalace a používání softwaru na daném počítači v rozsahu jejich kompetencí nebude v rozporu se zákonem o právu autorském č. 121/2000 v platném znění. Instalace softwaru podléhajícího této směrnici smí na daném počítači provádět pouze odpovědná osoba v rozsahu svých kompetencí, a to buď sama nebo s pomocí jiné osoby, kterou pověří.

V případě počítačů používaných více pracovníky by měl být vždy používán operační systém, který odděluje uživatelská a administrátorská oprávnění. Pokud je zapotřebí, aby na daném počítači byly prováděny i administrátorské úkony více osobami, měly by být tyto osoby stanoveny jako odpovědné s jednoznačně definovanými kompetencemi a rozsahy odpovědnosti pokud možno v souladu s jejich přístupovými právy.

Vedoucí oddělení zajistí, aby odpovědné osoby byly poučeny o svých právech, povinnostech a právních aspektech vykonávání softwarové administrace minimálně v rozsahu doporučení KIT, části B2 a části C, odst. (3b) a dále o svých povinnostech souvisejících se systémem evidence softwaru.

Interním dokladem legality softwaru bude certifikát vydávaný úsekem administrativy. Ke každému nabývacímu dokladu bude vydáno tolik certifikátů, kolik danému dokladu odpovídá licencí. Certifikát musí obsahovat:

- informace umožňující vyhledání nabývacího dokladu (např. číslo faktury)
- celkový počet licencí vázaných k nabývacímu dokladu a pořadové číslo certifikátu
- podpis osoby oprávněné k vydávání certifikátů

Vedoucí administrativního úseku pověří pracovníka/pracovníky oprávněné k vydávání certifikátů a určí způsob evidence vydaných certifikátů u nabývacích dokladů tak, aby k nabývacímu dokladu nebylo vydáno více certifikátů než odpovídá počtu licencí. Pověřený pracovník vydá vždy příslušný počet certifikátů k nově nakupovanému softwaru a pošle certifikáty objednateli. Objednatel rozdělí certifikáty odpovědným osobám jednotlivých počítačů podle určení jednotlivých licencí. Pracovník pověřený k vydávání certifikátů rovněž vydá příslušný počet certifikátů k archivním nabývacím dokladům, nebyly-li dosud vydány, na žádost osoby oprávněné disponovat prostředky, z nichž byl software zakoupen. Žádost o zpětné vydání certifikátů musí obsahovat číslo faktury nebo jinou identifikaci umožňující snadné nalezení nabývacího dokladu.

Certifikát je pro odpovědnou osobu dokladem legality užití instalovaného softwarového produktu na daném počítači. Odpovědná osoba uchovává certifikáty na bezpečném místě. Při instalaci softwarového produktu vyznačí na kopii certifikátu evidenční číslo počítače, kde byl produkt instalován a tuto kopii certifikátu opatřenou svým podpisem a datem uloží do centrální evidence. Pokud byla licence k užití softwaru přenesena z jiného počítače, je-li takový postup v daném případě v souladu se zákonem, tato skutečnost se rovněž vyznačí na kopii certifikátu zakládané do centrální evidence, opatřené navíc podpisem odpovědné osoby počítače, z něhož byla

licence přenesena (tj. pro standardní případ, kde byl software odinstalován).

Certifikáty mohou být i v elektronické podobě, jsou-li opatřeny potřebnými elektronickými podpisy.

Vedoucí administrativního úseku určí pracovníka pověřeného zakládáním kopií certifikátů do centrální evidence (příp. vedoucí oddělení, je-li evidence vedena na úrovni oddělení).

V případě počítačů, kde je nepřehledné množství instalovaného softwaru, příp. kde existuje důvodné podezření na přítomnost nežádoucího softwaru (viry, worms, spyware) nebo kde existuje podezření, že se na nich nachází nebo v minulosti nacházel software, jehož legalitu nelze prokázat a který technicky nebylo možné kompletně odinstalovat (typicky počítače se všemi verzemi operačních systémů Microsoft Windows), je nejvhodnějším řešením kompletní nová instalace operačního systému a aplikačního softwaru na základě sady certifikátů pro daný počítač. Alternativně lze uvažovat o vhodné formě auditu takového počítače, při dodržení podmínek doporučení KIT, části C.