Elektronická identita a ochrana digitálních děl

Doc. Ing. Karel Burda, CSc.

FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH
TECHNOLOGIÍ

Program

Elektronická identita a ochrana digitálních děl

1. Úvod
2. Elektronické průkazy
3. Ochrana digitálních děl
4. Závěr

1. Úvod

Úvod

- Prvním tématem dnešní přednášky je elektronická identita. Identita je unikátní pojmenování osoby v rámci určitého systému. Tímto jménem, alias identifikátorem, je v daném systému každá osoba jednoznačně definována a na základě tohoto identifikátoru jsou osobě v systému přiřazena určitá práva. Pokud má systém elektronickou povahu, tak pak hovoříme o elektronické identitě.
- S elektronickou identitou jsme se již setkali u systémů elektronické kontroly vstupu. Identifikátorem osoby v nich bylo Wiegandovo slovo a právem byl vstup do určité oblasti.
- V dnešní přednášce nás budou zajímat elektronické systémy, v nichž se používají občanské identifikátory, jako jsou jména a příjmení. Právy pak jsou například práva na využívání pozemku, na překročení státní hranice, k využívání peněžních prostředků na účtu apod. Často se jedná o systémy státní správy. Seznámíme se dnes s problematikou biometrických pasů a elektronických občanských průkazů.
- Druhým tématem přednášky je ochrana autorských děl v datové podobě (např. filmy, hudba, počítačové hry apod.). Tento typ děl je cílem různých útoků, kdy se útočník typicky snaží dílo tzv. prezentovat (např. přehrát si film, zahrát si hru) bez toho, že by zaplatil autorské poplatky, nebo se útočník snaží neoprávněně obohatit prostřednictvím cizího díla.
- Ochrana datových alias digitálních autorských děl se řeší v rámci správy digitálních práv („Digital Rights Management“ - DRM).

2. Elektronické průkazy

Elektronický průkaz

- Elektronický průkaz je klasický listinný průkaz, do něhož je integrováno elektronické zařízení s identifikačními daty osoby a vhodným rozhraním. To dovoluje rychlé načtení identifikačních údajů osoby do elektronického systému.
- K lokální autentizaci držitele průkazu se obvykle využívá biometrická autentizace. K tomuto typu elektronických průkazů patří v ČR cestovní pas s biometrickými údaji (obr. vlevo).
- Pro vzdálenou autentizaci držitele průkazu se využívá hardwarová autentizace založená na kryptografii. K tomuto typu elektronických průkazů patří v ČR elektronický občanský průkaz (obr. vpravo).

Biometrický pas

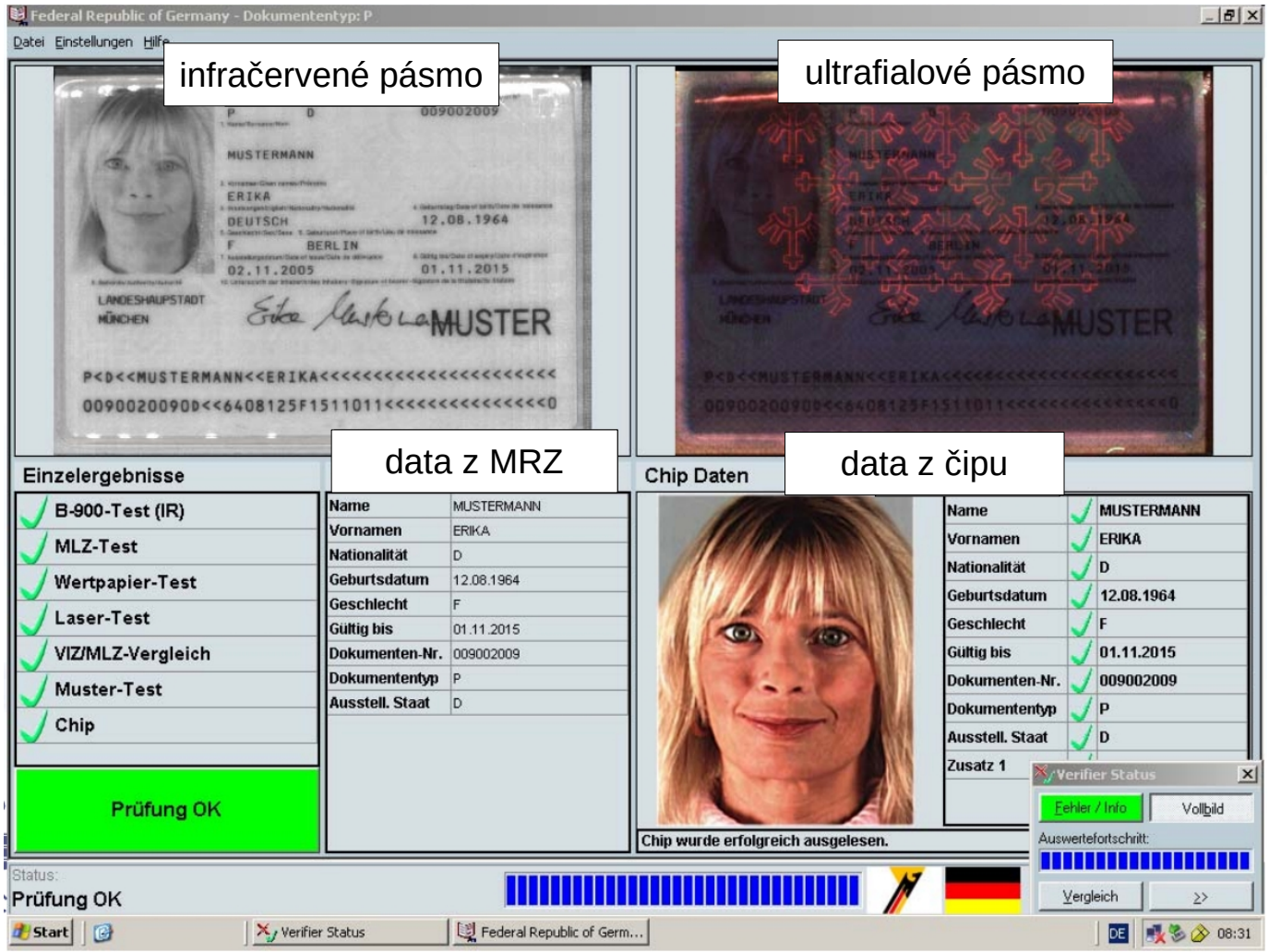
- Biometrický cestovní pas je klasická knížka, v níž je zalisován mikropočítač s NFC („Near field communication“) rozhraním.
- Mikropočítač slouží jako bezpečné paměťové úložiště identifikačních údajů osoby (jméno, příjmení apod.) a biometrických ověřovacích faktorů (typicky fotografie a otisk prstu). Autentičnost těchto dat je potvrzena digitálním podpisem příslušné autority.
- Ověřovací strana nejprve zkontroluje autentičnost listinné formy průkazu. K tomu slouží tiskařské ochranné prvky, jako jsou hologramové nálepky, mikroobrázky apod.
- Poté se z tzv. strojově čitelné zóny (viz dále) technikou optického rozpoznávání znaků (OCR) vyčtou základní identifikační údaje osoby.
- Následně se z mikropočítače vyčtou autoritou podepsané identifikační údaje a ověřovací biometrické údaje. Podpis autority se ověří a základní identifikační údaje se porovnají s údaji ze strojově čitelné zóny.
- V kladném případě se použijí ověřovací faktory k biometrické autentizaci osoby.
- Výhodou biometrického cestovního pasu je strojové zjištění a ověření identity osoby, čímž se zvyšuje propustnost kontrolního místa (např. přepážky na letišti). Navazující biometrickou autentizací se navíc zvyšuje i bezpečnost autentizace (vícefaktorová autentizace).

Tiskařské ochranné prvky

- Tiskařské ochranné prvky jsou tištěné nebo ražené struktury v papírovém nebo plastovém substrátu. K jejich vytvoření jsou zapotřebí speciální tiskařské stroje a případně i speciální substráty.
- Vysoká cena a regulace prodeje těchto substrátů a strojů je činí pro běžné útočníky nedostupnými, takže kvalitní padělky průkazů jsou prakticky nemožné.
- K obvyklým speciálním substrátům patří papír s vodoznakem (obr. vlevo) nebo s vlákny.
- V současné době se velice často používají tzv. opticky proměnné prvky. Opticky proměnný prvek („Optically variable device“ - OVD) je difrakční optická struktura vzniklá kombinací tisku a ražby. Pokud je takovýto prvek ozařován, tak v závislosti na intenzitě ozařování a v závislosti na úhlu pozorování vyhlíží různě (obr. vpravo).

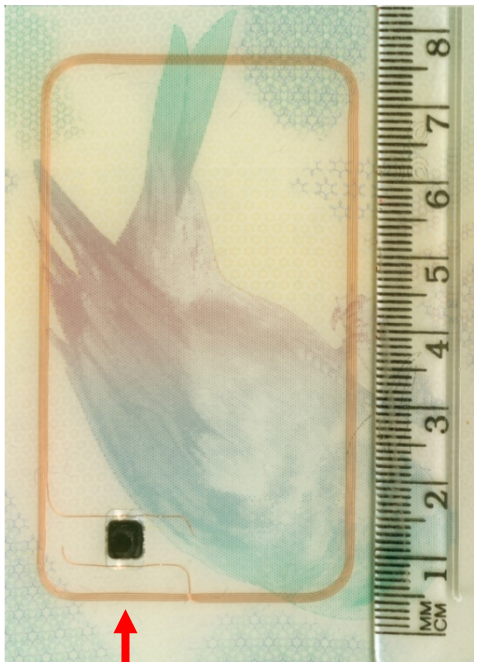
Kontrola tiskařských ochranných prvků

- Tiskařské ochranné prvky se kontrolují ve viditelném, infračerveném i ultrafialovém světle.
- Příklad toho, co na obrazovce svého terminálu vidí obsluha :



Biometrický pas a čtečka

Symbol biometrického pasu



Mikropočítač

Mobilní čtečka

Strojově čitelná zóna

- Strojově čitelná zóna („Machine Readable Zone“ = MRZ),
- MRZ umožňuje automatizované čtení údajů pomocí techniky optického rozpoznávání znaků („Optical Character Recognition“ = OCR).

MRZ →

Strojově čitelná zóna identifikačních dokladů

P<CZENOVAKOVA<<EMILIE<<<<<<<<<<<<<<<<<<<<<<<<
00000017<8CZE6805126F1606133685512151<<<<94

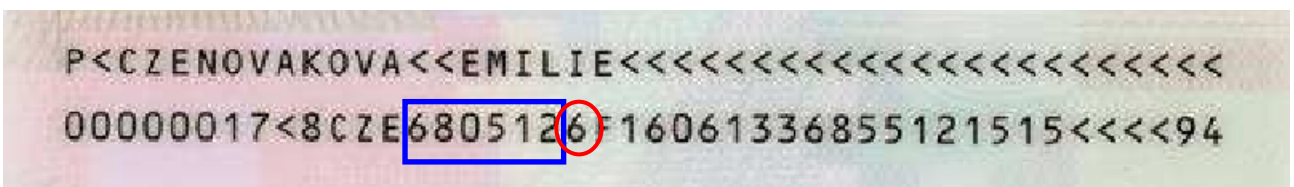
Pol.	Význam	Příklad	Pozn.
01	Typ dokumentu	P<	a) P = pas, I = OP, ... b) "<" = oddělovač/výplň
02	Stát, který dokument vydal	CZE	CZE = ČR
03	Příjmení a jméno/jména držitele	NOVAKOVA<< EMILIE<...	Diakritika se ignoruje
04	Číslo dokumentu. Když je delší než 9 číslic, tak se zbytek čísla uvede v položce 12.	00000017<	00000017
05	Kontrolní číslice položky 04.	8	Výpočet metodou "731".
06	Občanství držitele.	CZE	CZE = ČR
07	Datum narození držitele.	680512	12.května 1968
08	Kontrolní číslice položky 07.	6	Výpočet metodou "731".
09	Pohlaví.	F	M = muž, F = žena.
10	Poslední den platnosti dokumentu.	160613	13. června 2016
11	Kontrolní číslice položky 10.	3	Výpočet metodou "731".
12	Volitelné pole (zbytek čísla dokumentu, další identifikátory apod.)	6855121515<<<<	Zde je uvedeno rodné číslo
13	Kontrolní číslice položky 12.	9	Výpočet metodou "731".
14	Kontrolní číslice všech číslic ve 2. řádku (tj. řetězce položek 04, 05, 07, 08, 10, 11, 12 a 13).	4	Výpočet metodou "731".

Výpočet kontrolní číslice metodou "731"

- Výpočet kontrolní číslice C čísla $X_0X_1X_2X_3X_4X_5X_6 \ldots X_N$, kde X_i je i-tá číslice čísla.
- $C = (\sum S_i) \bmod 10$, kde $S_i = (X_i \cdot K_i) \bmod 10$, přičemž

$$K_i = \begin{cases} 7, \text{ pro } i \bmod 3 = 0, \\ 3, \text{ pro } i \bmod 3 = 1, \\ 1, \text{ pro } i \bmod 3 = 2. \end{cases}$$

- Příklad:



číslice X_i	6	8	0	5	1	2
koeficienty K_i	7	3	1	7	3	1
$S_i = (X_i \cdot K_i) \bmod 10$	2	4	0	5	3	2
$C = (\sum S_i) \bmod 10$	2	6	6	1	4	**6**

Data v čipu

- Paměť čipu je rozdělena na:
  - externě nedostupný segment: slouží k ukládání tajných klíčů,
  - externě dostupný segment: slouží k ukládání ostatních dat.
- Ostatní data jsou organizována do skupin („Data Group“ = DG):

Pol.	Význam	Pozn.
DG1	Data v MRZ	Povinné.
DG2	Biometrická data obličeje	V ČR ano.
DG3	Biometrická data otisků prstů	V ČR ano.
DG4	Biometrická data duhovky	V ČR pravděpodobně ne.
DG5	Fotografie držitele pasu	Povinné.
DG6	Rezervováno	-
DG7	Obrázek podpisu držitele	Povinné.
DG8-10	Bezpečnostní parametry pasu	Zatím nedefinováno.
DG11	Dodatečné údaje o držiteli (např. bydliště, tlf. apod.)	Nepovinné.
DG12	Dodatečné údaje o pasu (např. kým vydán)	Nepovinné.
DG13	Volitelná data	-
DG14	Rezervováno	-
DG15	Veřejný klíč pro autentizaci čipu	V ČR ano.
DG16	Adresy příbuzných držitele	Nepovinné.

Bezpečnost uložených dat

- K zajištění bezpečnosti dat uložených v čipu biometrického pasu se používají následující mechanismy.
- Povinný mechanismus:
  - ověření autentičnosti dat: data skupin DG1 až DG16 jsou digitálně podepsána vydavatelem pasu. Veřejné klíče vydavatelů pasů se mezi státy předávají diplomatickými službami.
- Volitelné mechanismy:
  - ověření autentičnosti čipu („Active Authentization“ = AA): čip má v externě nedostupném segmentu paměti svůj podepisovací klíč SK_C. Odpovídající veřejný klíč VK_C je uložen ve skupině DG15. Čtečka zašle náhodnou výzvu *N*, kterou čip podepíše pomocí svého SK_C a podpis zašle čtečce. Čtečka pomocí VK_C podpis ověří.
  - šifrovaný přenos mezi čtečkou a čipem („Basic access control“ = BAC): obě strany na základě údajů ve strojově čitelné zóně odvodí pomocný klíč *PK*, jímž si šifrovaně vymění náhodná čísla *N1* a *N2*. Z nich se pak odvozovací funkcí odvodí relační klíč *RK* pro šifrování dat přenášených z čipu ke čtečce.

Možné útoky na elektronický pas (1/3)

Získání uložených dat

- Přečtením dat z externě dostupného segmentu paměti lze získat citlivé údaje o držiteli pasu. Dále je možné vyrobit klon pasu.
- Čtení dat z pasu bez vědomí jeho držitele má znemožnit mechanismus BAC. K uskutečnění BAC (konkrétně ke konstrukci pomocného klíče *PK*) je totiž nutné znát data z MRZ, tj. pas musí být k přečtení MRZ otevřený. To však nemusí být pro útočníka problém z následujících důvodů.
- 1. důvod: z pasu budou číst např. hoteliéři. Mají tak přístup k DMZ a metodou BAC si mohou všechna uložená data přečíst.
- 2. důvod: při metodě BAC se pomocný klíč odvozuje z DMZ. Řada údajů v DMZ je predikovatelná a tak odposlechem šifrované relace mezi čtečkou a čipem a vyzkoušením možných klíčů (řádově hodiny) lze přenesená data zjistit.

Možné útoky na elektronický pas (2/3)

Sledování pohybu držitele

- Odposlechem a kryptoanalýzou relace BAC mohou monitorovat příchod/odchod držitele i jiné subjekty než hostitelský stát.
- Využitím metody AA může dokonce držitel pasu potvrzovat digitálním podpisem svoji přítomnost v dané lokalitě v daném čase. Průchodem v blízkosti falešné čtečky obdrží čip od této čtečky výzvu k autentizaci. Tato výzva však nebude náhodná, ale bude obsahovat kód lokality a času. Čip tuto výzvu podepíše, čímž prakticky stvrdí, že se držitel pasu pohyboval v blízkosti inkriminované čtečky.
- Pokud má navíc čip stálý identifikátor UID („Universal IDentifier“), tak lze sledovat rozmístěním čteček na vhodných místech pohyb držitele po celém státě. Např. čtečka zabudovaná do dveří obchodu bude generovat elektromagnetické pole. Tím dojde ke zprovoznění čipu a mikropočítač v pasu se čtečce identifikuje svým UID.

Možné útoky na elektronický pas (3/3)

Zneužití pasu

- Útočník s klonem pasu držitele může získat jeho identitu. Klon lze odhalit metodou AA, ale:
  1. metoda AA je nepovinná a v pasech řady států (např. Německo) je blokována.
  2. existuje možnost útoku mužem uprostřed. Útočník na hranici ve svém pasu předloží pouze komunikační rozhraní rádiového spoje končícího např. v hotelovém pokoji s pasem skutečného držitele. Čtečka na hranicích tak prakticky ověřuje pas stovky kilometrů vzdálený.
- Útočník může u nálože umístit čtečku, která na základě zjištění, že se v její blízkosti nachází např. držitel pasu USA, inicializuje výbuch. Tomu lze sice zabránit metodou BAC, ale ta je opět nepovinná.

Elektronický občanský průkaz

- Elektronický občanský průkaz (e-OP) je klasický občanský průkaz v podobě plastikové kartičky (obr. vlevo), ve které je zalisován mikropočítač s kontaktním rozhraním (obr. vpravo). Průkaz se vkládá do čtečky připojené k počítači uživatele.
- V průkazu je uložen soukromý klíč SK_U uživatele a certifikát CRT_U, který obsahuje základní identifikační údaje uživatele (jméno, příjmení atd.) spolu s veřejným klíčem VK_U.
- Autentizace probíhá tak, že se mezi autentizačním serverem AS a počítačem vybuduje TLS spojení. V něm AS zašle do průkazu náhodnou výzvu N. Po vložení identifikačního osobního kódu IOK uživatelem vypočítá mikropočítač k zaslané výzvě podpis $P = Q(N, SK_U)$, kde Q je podepisovací funkce. Podpis P spolu s certifikátem CRT_U je odeslán autentizačnímu serveru AS.
- Autentizační server ověří správnost certifikátu CRT_U a získá z něho veřejný klíč VK_U. S jeho pomocí pak ověří správnost podpisu P. Tím uživatel prokáže, že je osobou s identifikačními údaji uvedenými v CRT_U.

Centralizovaná autentizace

- Autentizace pomocí elektronického občanského průkazu je pro všechny státem provozované servery S centralizovaná. Společným autentizačním serverem AS pro tyto servery je server „eidentita.cz“, přičemž komunikace mezi počítačem uživatele U a všemi servery se uskutečňuje prostřednictvím TLS spojení.
- Pokud se uživatel chce přihlásit ke státnímu serveru S, tak ten jej nejprve kódem 302 přesměruje na server AS, kde je autentizován (viz předchozí snímek).
- Po autentizaci je počítač uživatele U přesměrován zpět k serveru S spolu s potvrzením o jeho identitě.
- Potvrzení o identitě jsou osobní údaje *OU* uživatele. Od serveru AS jsou přenášeny do serveru S jako kryptogram $C_1 = E(OU, K)$, přičemž klíč K se přenáší jako kryptogram $C_2 = E(K, VK_S)$.
- Servery S tedy spolu se serverem AS komunikují přes počítač uživatele U. Zprávy této komunikace jsou navíc podepisovány soukromými klíči serverů SK_S a SK_{AS}, přičemž veřejné klíče VK_S a VK_{AS} jsou přeneseny jako součást zmiňované komunikace v certifikátech CRT_S a CRT_{AS}. Tyto certifikáty jsou podepsány autoritou, jejímž veřejným klíčem zmiňované servery disponují.

Obecné problémy s elektronickými průkazy

- V současné době je celková počítačová bezpečnost na nízké úrovni. Je to dáno tím, že neexistují otevřené hardwarové platformy a prakticky ani bezpečné operační systémy.
- Hardwarové platformy obsahují nezdokumentované komponenty a firmware. Např. nové procesory Intel v sobě obsahují zcela autonomní mikroprocesor i s operačním systémem, kterým firma Intel teoreticky může ovládnout celý počítač – viz odkaz níže. https://cs.wikipedia.org/wiki/Intel_Management_Engine.
- Protože se nelze spolehnout na bezpečnost počítačů, mělo by se s elektronizací v rámci států (tzv. e-Government) postupovat velmi opatrně.
- Například v Estonsku a Slovensku došlo v roce 2017 k ohrožení hardwarové autentizace u e-OP (viz https://goo.gl/zuzjs2). Mikroprocesory od firmy Infineon generovaly prvočísla pro tvorbu RSA podepisovacího kryptosystému nedostatečně náhodně. To dovolilo ze znalosti veřejného klíče zjistit hodnotu soukromého klíče s náklady za cca 40 tis. amerických dolarů.

2. Ochrana digitálních děl

Základní pojmy

- Autorská data: data, v nichž jsou zakódována nějaká autorská díla, např. filmy, hudba, literatura, počítačové hry nebo software.
- Prezentace autorských dat: promítání filmu, poslech hudby, čtení literárního díla, hraní počítačové hry nebo využití služeb poskytovaných nějakým software.
- Data lze snadno kopírovat, což v případě autorských děl svádí k porušování autorských práv.
- Správa digitálních práv („Digital Rights Management“ - DRM): soubor technických metod, které jsou určeny k řízení kopírování a prezentací autorských dat v souladu s požadavky majitele práv k autorským datům.
- Přehrávač: elektronické zařízení, které je určeno k prezentaci autorských dat a k jejich kopírování.
- Autor: osoba, které stanovuje omezení týkající se prezentace a kopírování konkrétního autorského díla.
- Útočník: osoba, která usiluje o porušení zmíněných omezení.
- Zrádce: osoba nebo přehrávač, které jsou zdrojem neoprávněné kopie autorských dat.

Ochrany DRM

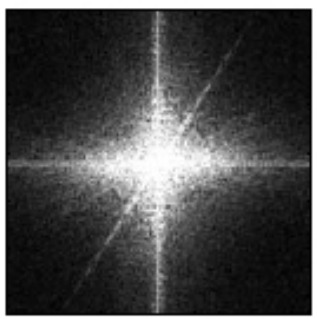
- Autorská data jsou uložena na nějakém elektronickém médiu (např. na DVD) a cílem ochran DRM je vynucovat kopírování a prezentaci autorských dat v souladu s omezeními, které stanovil autor těchto dat.
- Těmito omezeními jsou zpravidla maximální počet prezentací nebo maximální počet pořízených kopií.

- Ochrany DRM bývají založeny:
  - na metodách digitálního vodoznaku,
  - na metodách řízení přístupu,
  - na kryptografických metodách,
  - na kombinaci výše zmíněných metod.

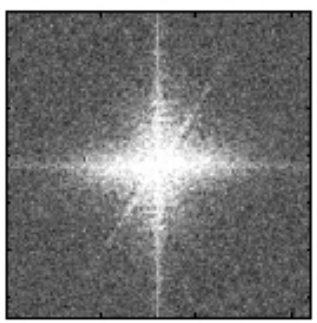
- Kryptografické metody a metody řízení přístupu známe z předchozích přednášek a tak si nyní podrobněji vysvětlíme digitální vodoznak.

Digitální vodoznak

- Digitální vodoznak: autorská data, která jsou vložena do chráněných dat takovým způsobem, že je prakticky nelze z těchto dat neoprávněně odstranit.
- Pomocí vodoznaku:
  - lze dokázat vlastnictví práv k chráněným datům (tzv. identifikační vodoznak),
  - lze řídit přístup k chráněným datům (tzv. zamítající vodoznak).

Autorská data (vlevo) a použitý vodoznak (vpravo).

Chráněná data (vlevo) a z nich extrahovaný vodoznak (vpravo).

Zjevné vodoznaky

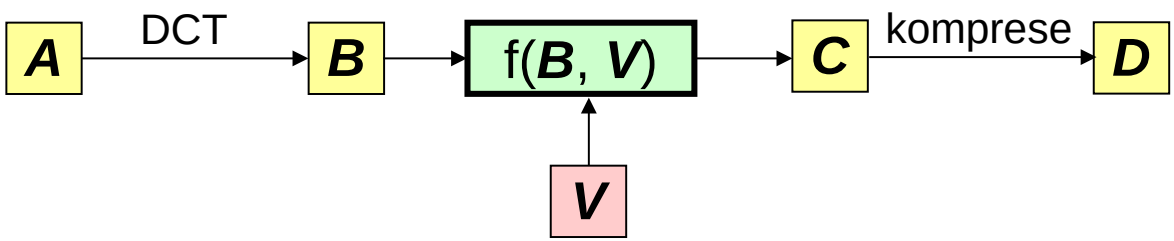
- Identifikační vodoznaky jsou zpravidla zjevnými vodoznaky.
- Zjevné digitální vodoznaky: pozorovatel je při prezentaci autorských dat může snadno detekovat.
- Zpravidla obsahují informace o autorovi dat a tak autorovi umožňují prokázat autorství.
- V případě obrázků se jedná o změnu jasu a barvy těch obrazových bodů, které tvoří vodoznak.
- V případě zvuků se jedná o mix původního zvuku se zvukem vodoznaku (např. komentář rozhlasového moderátora pronášený v úvodu hudební skladby).

Skryté vodoznaky

- Skryté vodoznaky slouží jak k identifikaci tak i k řízení přístupu.
- Data vodoznaku jsou do původních autorských dat vložena tak, aby nebyla detekovatelná ani odstranitelná.
- Využívá se redundance v autorských datech. Jako příklad si uvedeme DCT vodoznak.

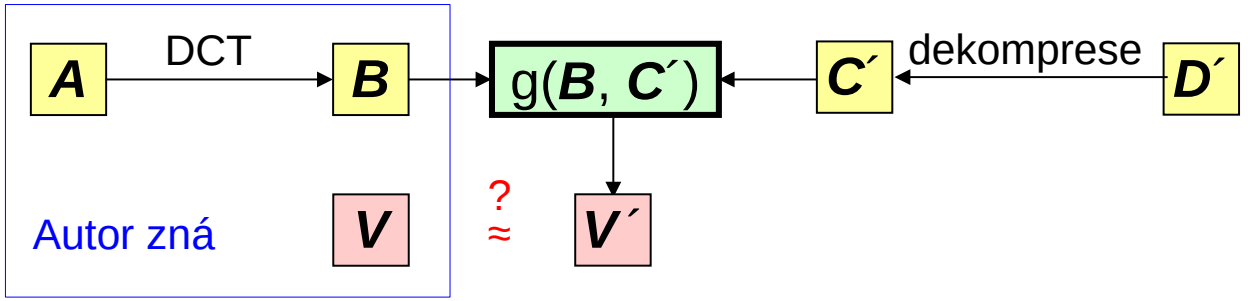
Skrytý vodoznak typu DCT - vložení

- DCT vodoznak je vodoznak vkládaný pomocí diskrétní kosínové transformace (DCT).
- Používá se často u obrázků formátu JPEG, kde už je DCT transformace využívána ke kompresi obrázků.
- Každý obrázek je rozdělen na bloky 8×8 pixelů. Tyto bloky lze reprezentovat jako matici ***A*** = $\{a_{ij}\}$ celých čísel formátu 8×8.
- Matice ***A*** se diskrétní kosínovou transformací převede na matici ***B*** = $\{b_{ij}\}$, která má také formát 8×8 čísel. Každý prvek b_{ij} přitom stanoveným způsobem závisí na všech prvcích a_{ij}.
- Vybrané prvky matice ***B*** se zkombinují s čísly vodoznaku ***V*** = $\{v_{ij}\}$, kde $v_{ij} \in \{-1, +1\}$. Možné přiřazení je například $c_{ij} = b_{ij} + g \cdot v_{ij}$, kde g je zvolená konstanta.
- Výsledná matice ***C*** se dále standardním způsobem komprimuje a uloží jako soubor ***D***.



Skrytý vodoznak typu DCT - kontrola

- Autor, který provádí kontrolu vodoznaku, samozřejmě zná hodnoty b_{ij} (originální obrázek), v_{ij} (vodoznak) a g (zvolená konstanta).
- Pokud útočník původní ***D*** zmodifikoval do podoby ***D´***, tak se dekompresí zmodifikované matice získá matice ***C´***, která je aproximací původní matice ***C***.
- Poté se provede extrakce vodoznaku – v našem příkladu výpočtem $v_{ij}' = (c_{ij}' - b_{ij})/g$.
- Získané hodnoty v'_{ij} se vhodným statistickým testem porovnají s hodnotami vloženého vodoznaku v_{ij}. V případě statistické shody veličin v_{ij}' a v_{ij} je existence vodoznaku prokázána.



- Odolnost DCT vodoznaku vůči útokům spočívá v tom, že útočník nemá k dispozici původní obrázek a obecně ani nezná způsob vložení vodoznaku.
- Při pokusu použít hrubou sílu a náhodně měnit hodnoty $c_{ij}´$ s cílem skrýt vodoznak v šumu narazí útočník na problém, že změna každé hodnoty $c_{ij}´$ má prostřednictvím inverzní kosínové transformace vliv na každý pixel příslušného bloku. Málo významné změny hodnot však vodoznak pod šum nedostanou a naopak významné změny obrázek nepřijatelným způsobem zkreslí.

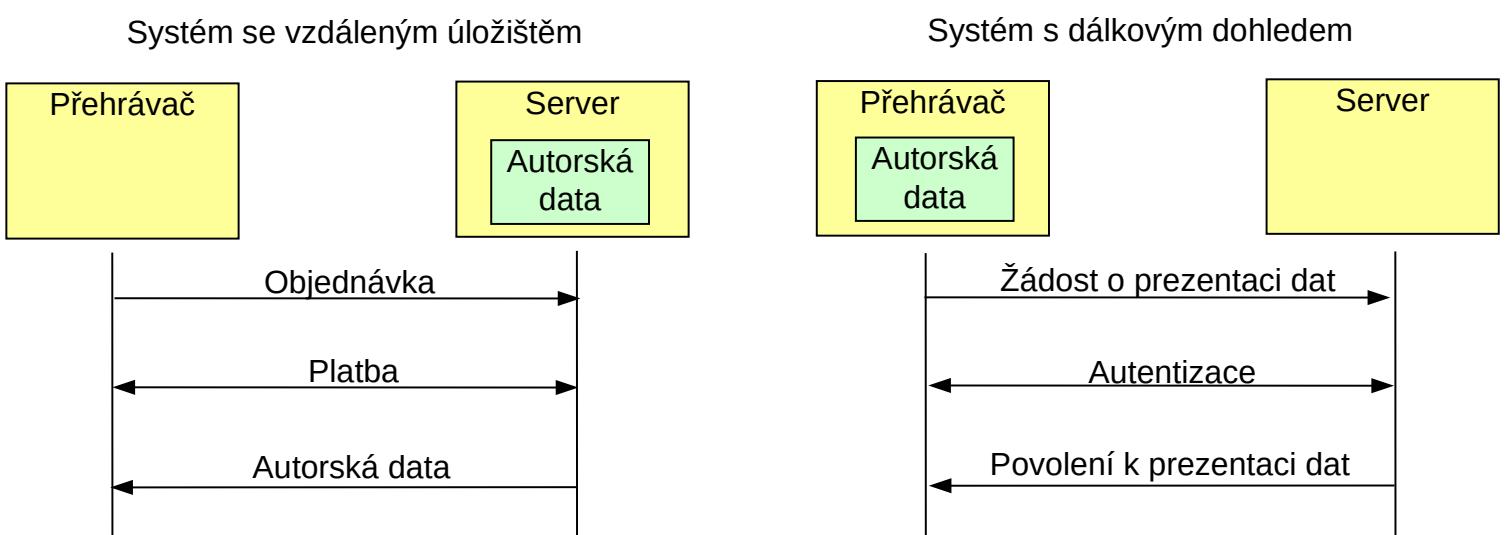
Klasifikace ochran DRM

- Ochrany DRM:
  1. vzdálené: vyžadují spojení mezi přehrávačem a centrálním serverem.
     - s prodejem: přehrávač dílo prezentuje po elektronické platbě serveru.
     - s povolením: přehrávač dílo prezentuje po povolení serverem.
  2. lokální: není nutný centrální prvek.
     - s identifikací vodoznakem: autora nebo kupce díla lze dohledat pomocí vodoznaku.
     - s řízením přístupu: přehrávač dílo prezentuje po splnění stanovených podmínek.
       – podmínkou jsou vlastnosti média,
       – podmínkou jsou vlastnosti přehrávače (stanovený typ nebo znalost tajného klíče),
       – podmínkou je znalost uživatele (obvykle znalost hesla).

- Výše uvedené ochrany lze různě kombinovat.

Vzdálené DRM ochrany

- Prezentaci autorských dat zajišťuje přehrávač a DRM ochranu zajišťuje vzdálený server.
- Vzdálený server může:
  - autorská data poskytovat (systém se vzdáleným úložištěm),
  - prezentaci autorských dat povolovat (systém dálkového dohledu).
- Systémy se vzdáleným úložištěm (obr. vlevo) využívají např. prodejci hudby. Uživatel si dílo objedná a zaplatí. Dílo je mu předáno a poté si je může přehrávat.
- Systémy s dálkovým dohledem (obr. vpravo) typicky využívají poskytovatelé licencovaného software. Přehrávač požádá u serveru o prezentaci dat a autentizuje se. Pokud jsou splněny licenční podmínky (např. že daný SW aktuálně běží na 48 počítačích VUT z 50 možných), tak server vydá přehrávači povolení k prezentaci dat.



Lokální DRM ochrany

- Správa digitálních práv založená na lokálních ochranách nevyžaduje síťové připojení uživatele.
- Ochrana práv je v tomto případě realizována výhradně přehrávačem.
- Lokální ochrany lze třídit podle kombinace typu média s chráněnými daty a přehrávače těchto médií:

  1) běžné médium
     - univerzální přehrávač,
     - speciální přehrávač,

  2) speciální médium a speciální přehrávač.

  (Pozn.: kombinace speciálního média a univerzálního přehrávače nemá smysl - běžný přehrávač není schopen se speciálním médiem pracovat).

Běžné médium - univerzální přehrávač

- Jediným způsobem ochrany dat u kombinace běžné médium - univerzální přehrávač je identifikační vodoznak.
- V tomto případě se do dat vkládají identifikační údaje buď vlastníka práv, nebo uživatele kupujícího daná data.
- Identifikační údaje jsou do dat vloženy některou z metod digitálního vodoznaku a tyto údaje tak lze odstranit pouze za cenu významného poškození původních dat.
- Pomocí identifikačního vodoznaku může vlastník práv dokázat pro každou kopii chráněných dat, že on je vlastníkem práv k těmto datům, nebo může zjistit, od kterého kupujícího byla data nelegálně zkopírována.

Běžné médium - speciální přehrávač (1/3)

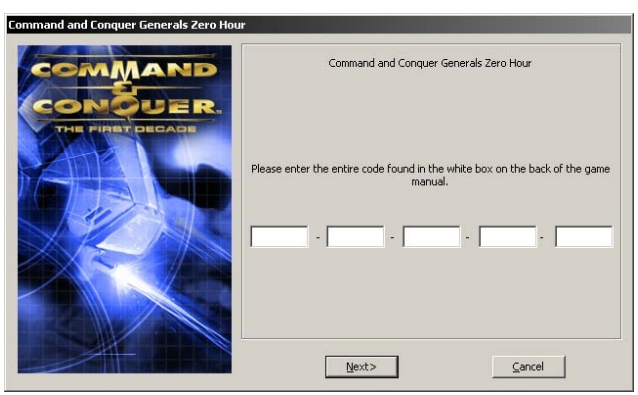
- V případě běžného média a speciálního přehrávače se využívá řízení přístupu, kde se jako kritérium využívá:
  - znalost uživatele,
  - vlastnost přehrávače (buď typ přehrávače nebo disponování tajným klíčem).

- V tomto případě má uživatel speciální přehrávač, který data přehraje pouze v případě, že jsou splněny určité podmínky.

- Speciální přehrávač může být:
  - speciální z výroby,
  - univerzální, který byl modifikován autorskými daty.

Běžné médium - speciální přehrávač (2/3)

- V případě autentizace znalostí musí uživatel před přehráním nebo instalací chráněných dat vložit do přehrávače nějaké heslo. V případě správného hesla přehrávač data z média prezentuje, resp. data z média dešifruje a následně prezentuje. Typicky se jedná o SW, k jehož instalaci autor poskytuje unikátní heslo (obr. vlevo).
- V případě požadavku splnění požadované vlastnosti přehrávače se často používá možnost, kdy autor s daty prodává i nějaký autentizační předmět (zpravidla nějaký typ hardwarového klíče), který se do přehrávače musí před přehráním chráněných dat vložit (obrázky vpravo). Tento způsob se často používá k ochraně specializovaného SW.

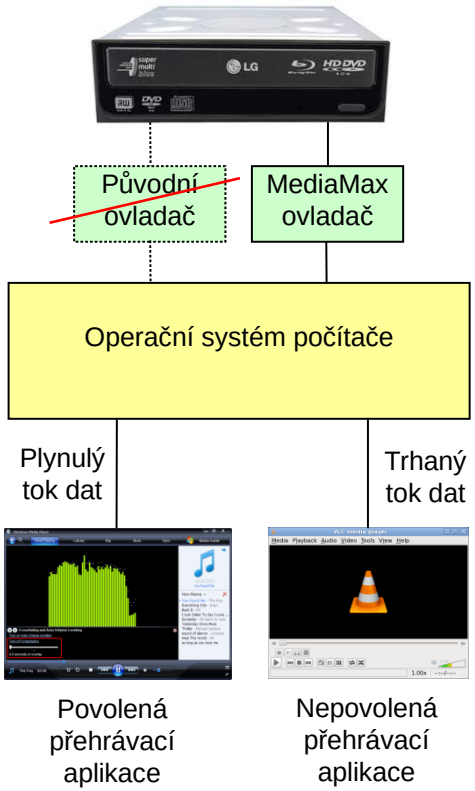


Běžné médium - speciální přehrávač (3/3)

- Další možnost kombinace běžné médium - speciální přehrávač je v současné době realizována tak, že běžné médium obsahuje program, který zmodifikuje standardní přehrávač (zpravidla PC) tak, aby se stal speciálním (např. CD Cops, nebo MediaMax – viz dále).
- V tomto případě je na médiu kromě autorských dat speciální program, který zajišťuje samotnou ochranu.
- Při vložení média do přehrávače se tento program aktivuje a určitým způsobem přehrávač modifikuje.
- Takto modifikovaný přehrávač pak přehrání dat z média povolí jen při splnění určitých vlastností média nebo uložených dat.
- Příkladem je například technika CD Cops, která vychází z toho, že čtení dat z lisovaného CD disku je mnohonásobně rychlejší než čtení dat z vypalovaného disku. Ochranný program nejprve otestuje rychlost čtení dat z média. Pokud zjistí, že CD disk není lisovaný, tak zabrání jeho dalšímu čtení.
- Dalším příkladem je vložení vodoznaku do prezentovaných dat (např. MediaMax). Pokud přehrávač detekuje, že přehrávaná data obsahují vodoznak, tak se začne chovat podle stanovené politiky (např. dovolí vytvořit jen stanovený počet kopií autorských dat).

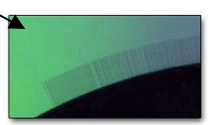
Příklad DRM MediaMax

- Před spuštěním CD na počítači se nainstaloval DRM software MediaMax (byl uložen v obvodové stopě CD). Tím došlo k modifikaci běžného přehrávače na speciální přehrávač, kdy původní ovladač CD mechaniky by nahrazen ovladačem MediaMax.
- Uvedený ovladač u každého CD kontroloval pomocí vodoznaku, zda se jedná ochráněné CD.
- Pokud se jednalo o chráněné CD a přehrávačem byl přehrávač Windows Media Player, tak přehrávání proběhlo bez problémů. Přehrávač Windows Media Player přitom umožnil uživateli využívat obsah CD jen v určeném rozsahu (např. maximální počet kopií CD, formát kopií skladeb jen WMA apod.).
- V případě jiného přehrávače ovladač data skladby náhodně zpožďoval, čímž došlo ke zkreslení přehrávaných dat.



Speciální médium - speciální přehrávač

- Další třídou lokální ochrany digitálních práv je kombinace speciálního média a speciálního přehrávače.
- Uvedená kombinace je málo používána. Asi nejznámějším představitelem je hrací konzola Nintendo GameCube.
- V tomto případě je použit standardní DVD disk, na který je vysoce výkonným laserem vypálen čárový kód (BAC = Burst Cutting Area).
- Tento kód nedokáží běžné vypalovací mechaniky vytvořit, takže na PC nelze vytvářet nelegální kopie.
- Přehrávač přítomnost kódu BAC testuje a pokud jej nenalezne, tak nedovolí načtení dat z disku.
- Starším reprezentantem speciálního média jsou tzv. cartridge (paměť typu ROM ve speciální kazetě).



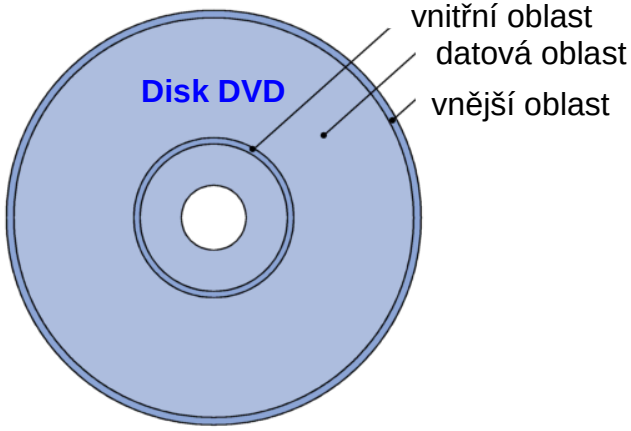
Ochrany DRM s šifrováním

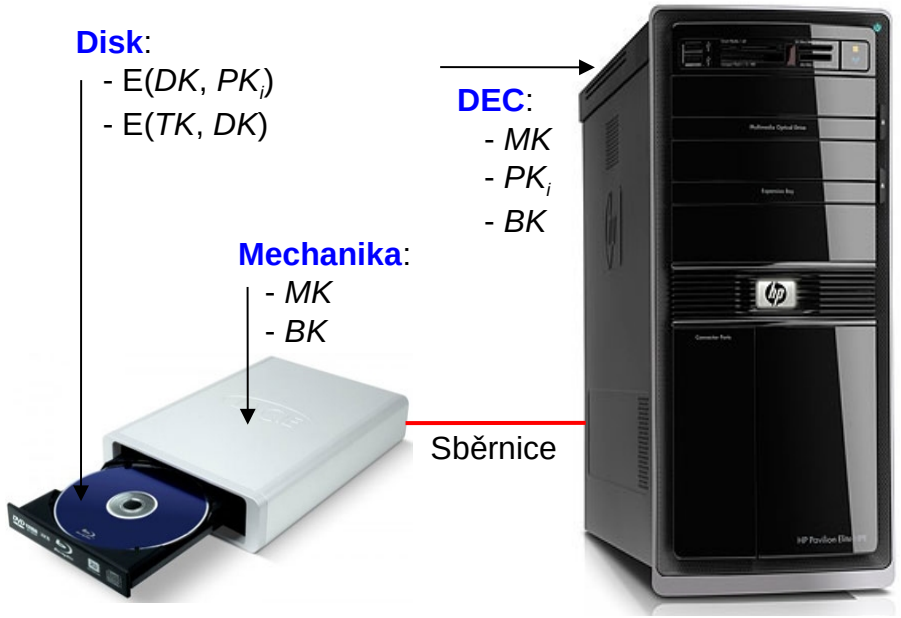
Technika CSS

- Perspektivní metodou ochrany práv k digitálním záznamům je šifrování.
- Asi nejznámějším reprezentantem této metody je technika CSS („Content-Scramble System“).Tato technika vznikla v roce 1996 a používá se na ochranu DVD filmů. Poměrně rychle však byla překonána.
- V roce 1999 byl publikován program DeCSS, který umožnil uživatelům operačního systému Linux sledovat filmy na DVD zabezpečených technikou CSS. Do té doby tuto možnost neměli.
- V CSS systému se k šifrování používá proudová šifra s délkou klíče 40 bitů.
- První slabinou CSS je krátký klíč. V té době totiž panovaly v USA zákony omezující export zařízení s větší délkou klíče. Potom složitost útoku hrubou silou (tj. vyzkoušení všech možných hodnot klíče) je $2^{40} \approx 10^{12}$ pokusů. Pro počítače z roku 1999 to byla záležitost 1 dne.
- Druhou slabinou byla správa klíčů. Existuje 409 klíčů přehrávače PK a každý licencovaný výrobce obdržel alespoň jeden takový klíč. Prozrazením jediného klíče PK je však kompromitován celý systém CSS!

Content-Scrambler System (CSS)

- Film je zašifrován na disku DVD.
- Na jeho dešifrování se podílí DVD mechanika přehrávače a specializované obvody přehrávače (dále zkráceně DEC). Mechanika a DEC jsou propojeny nechráněnou sběrnicí.
- Klíčová správa CSS systému definuje následující klíče:
  - hlavní klíč *MK* (Master Key): bezpečně uložen jak v mechanice, tak i v DEC,
  - klíč přehrávače PK_i (Player Key), jeden z $i = 1$ až 409: uložen v DEC,
  - klíč disku *DK* (Disc Key): zašifrován na DVD ve 409 kryptogramech každým ze 409 klíčů PK_i,
  - klíč titulu TK (Title Key): zašifrován na DVD pomocí *DK*,
  - klíč sběrnice *BK* (Bus Key): odvozen v průběhu vzájemné autentizace mezi mechanikou a DEC.





Autentizace Mechanika - DEC

- Nejprve se Mechanika (dále zkráceně MECH) a DEC navzájem autentizují metodou výzva - odpověď na základě znalosti klíče *MK* („Master Key“). Jak MECH, tak i DEC mají tento klíč bezpečně uložen v chráněné části své paměti.
- DEC vygeneruje náhodné číslo N_A (tzv. výzvu) a zašle jej po sběrnici do MECH. Ta výzvu zašifruje klíčem *MK* a tuto odpověď $C_A = E(N_A, MK)$ zašle do DEC. Spolu s tím odešle i vlastní výzvu N_B.
- DEC odpověď C_A dešifruje klíčem *MK* a měl by získat svoji výzvu, tj. $D(C_A, MK) = N_A$.
- DEC poté zašifruje výzvu od MECH a odešle odpověď $C_B = E(N_B, MK)$. MECH musí dešifrováním C_B získat N_B.
- Pokud odpovědi na výzvy souhlasily, tak DEC i MECH vědí, že protějšek zná klíč *MK* a tudíž je důvěryhodný.
- Další služební komunikace mezi MECH a DEC je na sběrnici již šifrovaná. K tomuto šifrování odvodí klíč sběrnice $BK = F(N_A, N_B, MK)$, kde F je funkce k odvozování klíčů („Key Derivation Function“).

Nalezení klíče disku

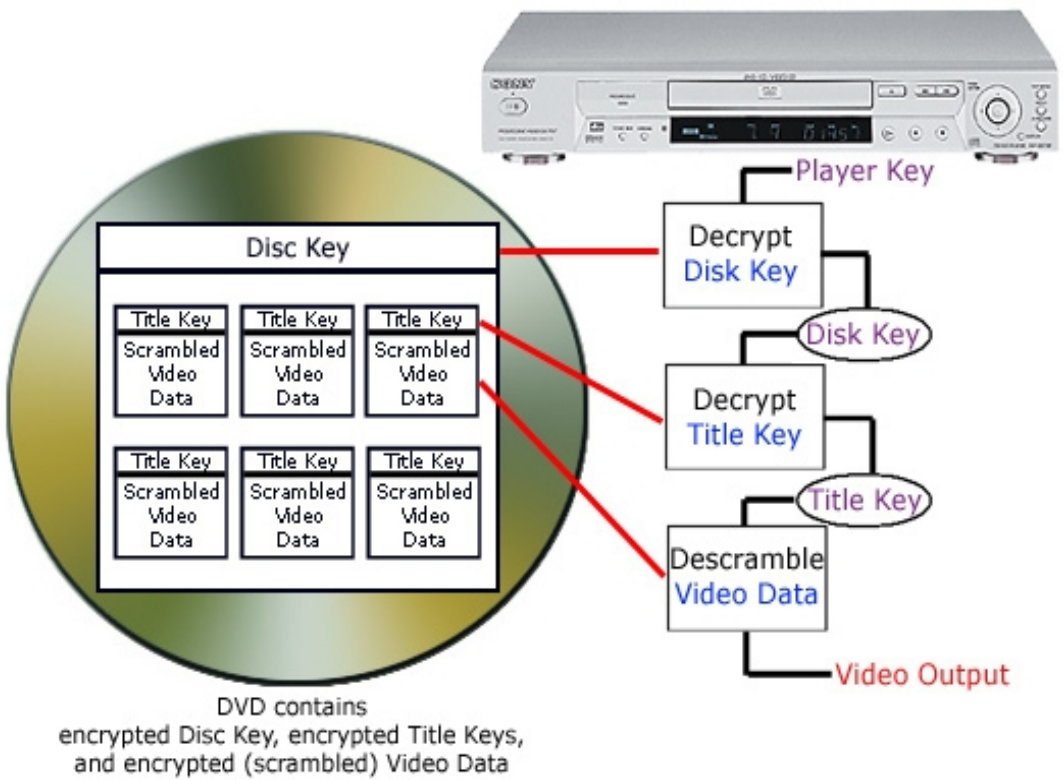
- Každý licencovaný výrobce přehrávačů dostal alespoň jeden klíč přehrávače PK_x, kde $x \in \{1, 2, ..., 409\}$. Tento klíč do svého výrobku bezpečně uloží.
- Nyní musí DEC zjistit klíč disku *DK*. Pro každý DVD je použit jiný klíč, který je v zašifrované podobě uložen na DVD. Klíč *DK* je na každém DVD zašifrován všemi 409 klíči přehrávačů PK_x.
- MECH přečte z disku a do DEC odešle hodnotu $C_{DK} = E(DK, DK)$ a 409 kryptogramů $C_i = E(DK, PK_i)$, kde $i = 1$ až 409.
- DEC neví, který z kryptogramů C_i je zašifrován jeho klíčem PK_x a tak postupně zkouší svým klíčem dešifrovat všechny C_i:

$$W_i = D(C_i, PK_x).$$

- Skutečnost, zda $W_i = DK$, se testuje na podmínce, zda $E(W_i, W_i) = C_{DK}$. Když tato shoda nastane, tak DEC zjistil správný klíč disku $DK = W_i$.

Dešifrování obsahu

- Na základě znalosti klíče disku *DK* („Disc Key“) může DEC zjistit klíč titulu *TK* („Title Key“).
- DEC od MECH dostane kryptogram $C_{TK} = E(TK, DK)$, ve kterém je zašifrován klíč titulu *TK*.
- Získaným klíčem disku *DK* dešifruje C_{TK} a tak zjistí *TK*.
- Klíčem *TK* pak už následně dešifruje datový obsah („Video Data“) z disku.



CSS - zhodnocení

- První slabinou CSS je nízká odolnost šifrovacího algoritmu. Klíč titulu *TK* lze získat metodou hrubé síly řádově v hodinách.
- Dešifrovaný film pak lze následně komprimovat a uveřejnit na Internetu, nebo šířit jako standardní DVD.

- Další slabinou CSS je klíčové hospodářství, kde kritickou položkou je klíč přehrávače *PK*. (Pozn.: Klíč *MK* útočník nepotřebuje, protože DVD mechanika přečte všechny údaje na disku bez potřeby autentizace.)
- V případě prozrazení jediného ze všech 409 klíčů *PK* je bezpečnost celého systému CSS zlikvidována. Útočník je v tomto případě legálním uživatelem - z disku si přečte všechny kryptogramy, klíčem *PK* je dešifruje, zjistí správný klíč disku a následně i klíč titulu.
- Jeden z klíčů *PK* byl získán zpětným inženýrstvím ze softwarového DVD přehrávače Xing.

Advanced Access Content System (AACS)

- Nástupcem systému CSS je Advanced Access Content System (AACS): systém pro ochranu obsahu DVD, HD DVD a Blue Ray disků.

- V AACS došlo k odstranění hlavních slabin CSS:
  - proudová šifra byla nahrazena kvalitním algoritmem blokové šifry AES („Advanced Encryption Standard“) s délkou klíče 128 bit,
  - ve správě klíčů byl klíč výrobce přehrávače PK nahrazen množinou klíčů výrobku podle konceptu dynamického skupinového klíče ("broadcast encryption").
- Na šifru AES není v současné době znám nějaký útok, který by měl smysl.

Princip správy klíčů v AACS

- Dynamická správa klíčů v AACS je založena na *n*-vrstvém stromě klíčů.
- Každý jednotlivý přehrávač zná unikátní sadu značek.
- Na disku je chráněný obsah zašifrován klíčem titulu *TK*. Zároveň je tento klíč zašifrován klíči, které dokáží ze známých značek odvodit pouze oprávněné přehrávače. Ty pak mohou klíč *TK* dešifrovat a chráněný obsah přehrát.
- Přehrávače, jejichž klíče byly v minulosti prozrazeny, jsou ze skupiny oprávněných přehrávačů vyloučeny. To znamená, že dokáží přehrávat pouze disky vydané v době před tím, než se dostaly na seznam vyloučených.
- Dynamická správa klíčů nechrání před hrozbou, že nějaký uživatel dešifruje vybraný titul a jeho kopii anonymně distribuuje například po Internetu, nebo na DVD.

4. Závěr

Shrnutí a závěr

- Elektronický průkaz je klasický listinný průkaz, do něhož je integrován mikropočítač s identifikačními údaji osoby. Mikropočítač může také obsahovat podepsané biometrické ověřovací faktory (např. biometrický pas) a kryptografické dokazovací faktory (např. e-OP).
- Identifikační údaje v datové podobě umožňují rychlé vyčtení těchto údajů. Biometrické ověřovací faktory pak umožňují kvalitnější lokální autentizaci osoby a kryptografické dokazovací faktory umožňují vzdálenou autentizaci osoby.

- Techniky ochrany digitálních děl slouží k vynucování podmínek pro prezentaci těchto děl, které stanovil autor díla.
- Techniky DRM jsou založeny na vodoznacích, autentizaci, šifrování a na specifických vlastnostech přehrávačů a médií.

- Otázka ke zkoušce:
  Ochrany digitálních děl:
  - Účel a klasifikace ochran.
  - Vzdálené DRM ochrany – typy, principy a vlastnosti.
  - Lokální DRM ochrany – typy, principy a vlastnosti.