Współczesne systemy DRM

Podstawy, przyszłość i wyzwania

Aneta Zwierko

VOD prepaid system for Japanese Hospitals

IPTV/VOD system for based on HD Motorola STB for Japanese market (SO-Net)

VOD system via public Internet deployed in USA

IPTV/VOD available on the Russian market.

Surveillance system for Tokyo town hall

VOD (progressive download system) platform for Japanese content provider in Tokyo

DRM - podstawy

- DRM ang. *Digital Rights Management*, czyli **cyfrowe zarządzanie prawami**
- *Oparty o mechanizmy kryptograficzne lub inne metody ukrywania treści system zabezpieczeń mający przeciwdziałać używaniu danych w formacie elektronicznym w sposób sprzeczny z wolą ich wydawcy (źródło: wikipedia)*
- *Cel: ochrona praw autorskich twórców*
  - *umożliwia zdefiniowany dowolnych zasad wykorzystania kontentu*
- *Conditional Access Systems*

- Szyfrowanie symetryczne
  - ochrona danych
  - dystrybucja kluczy
- Uwierzytelnienie
  - uwierzytelnienie pochodzenia danych (pliku)
    - watermarking, fingerprinting
  - Uwierzytelnienie urządzenia
    - PKI, smartcards
  - Uwierzytelnienie użytkownika
    - metody biometryczne, tokeny

- Zaufane środowisko wykonania (ang. *secure execution environment*)
  - Rozwiązania hardwarowe
    - urządzenia z dodatkowymi procesorami i wydzieloną „bezpieczną” pamięcią
  - Rozwiązania softwarowe
    - „Zaufane środowisko wykonania” na PC/urządzeniu

- *Forensic DRM*
- *Zapobieganie kradzieży treści lub usługi*
  - *DVD's , IPTV*
- *Zapobieganie nieautoryzowanemu kopiowaniu*
  - *Macrovision, SCMS*
- *Zapobieganie nieautoryzowanemu użytkowaniu*
  - *FairPlay, IPTV*

DRM – aspekty prawne i kontrowersje

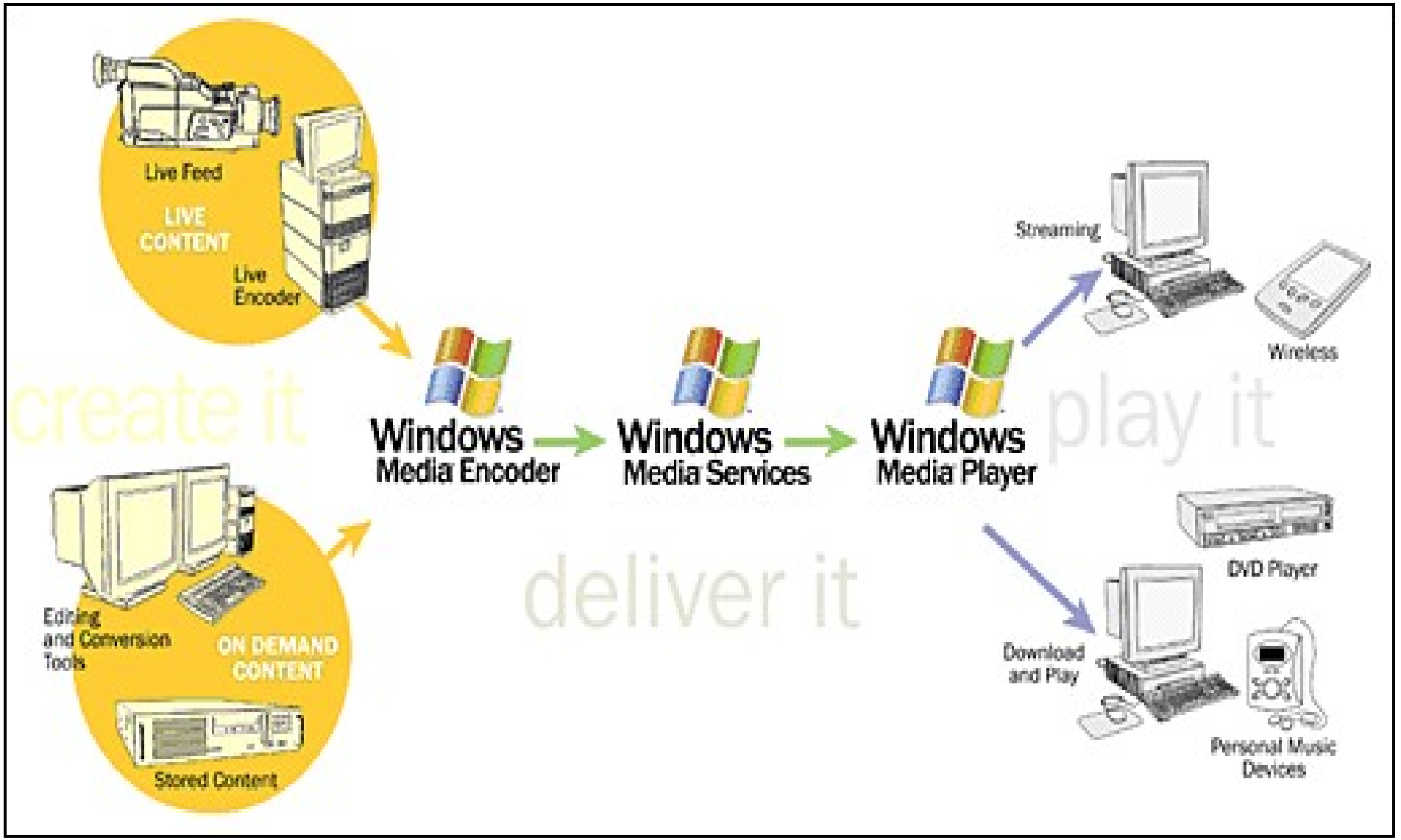
- DRM ang. *Digital Restrictions Management*, czyli cyfrowe zarządzanie ograniczeniami
- Prawa autorskie a systemy DRM
- Zasada prywatnego użytku
- Metoda arbitralnego, potencjalnie bezprawnego ograniczenia przywilejów konsumenckich
  - uniemożliwienie wykonywania prywatnych kopii zakupionych utworów
  - utrudnienie korzystania z utworów w określonych rejonach geograficznych, uniemożliwienie przewinięcia reklam i obwieszczeń poprzedzających film

- USA
  - Digital Millennium Copyright Act (DMCA) z 1998 r.
- Europa/Polska
  - EUCD (EUCD (2001/29) wprowadza samo zarządzanie prawami autorskimi (DRM). DRM jest elementem sprzętowym lub programem instalowanym przez dysponenta prawa autorskiego w komputerze lub innym programowalnym sprzęcie odbiorcy.
  - IPRED1 (2004/48)
  - IPRED2

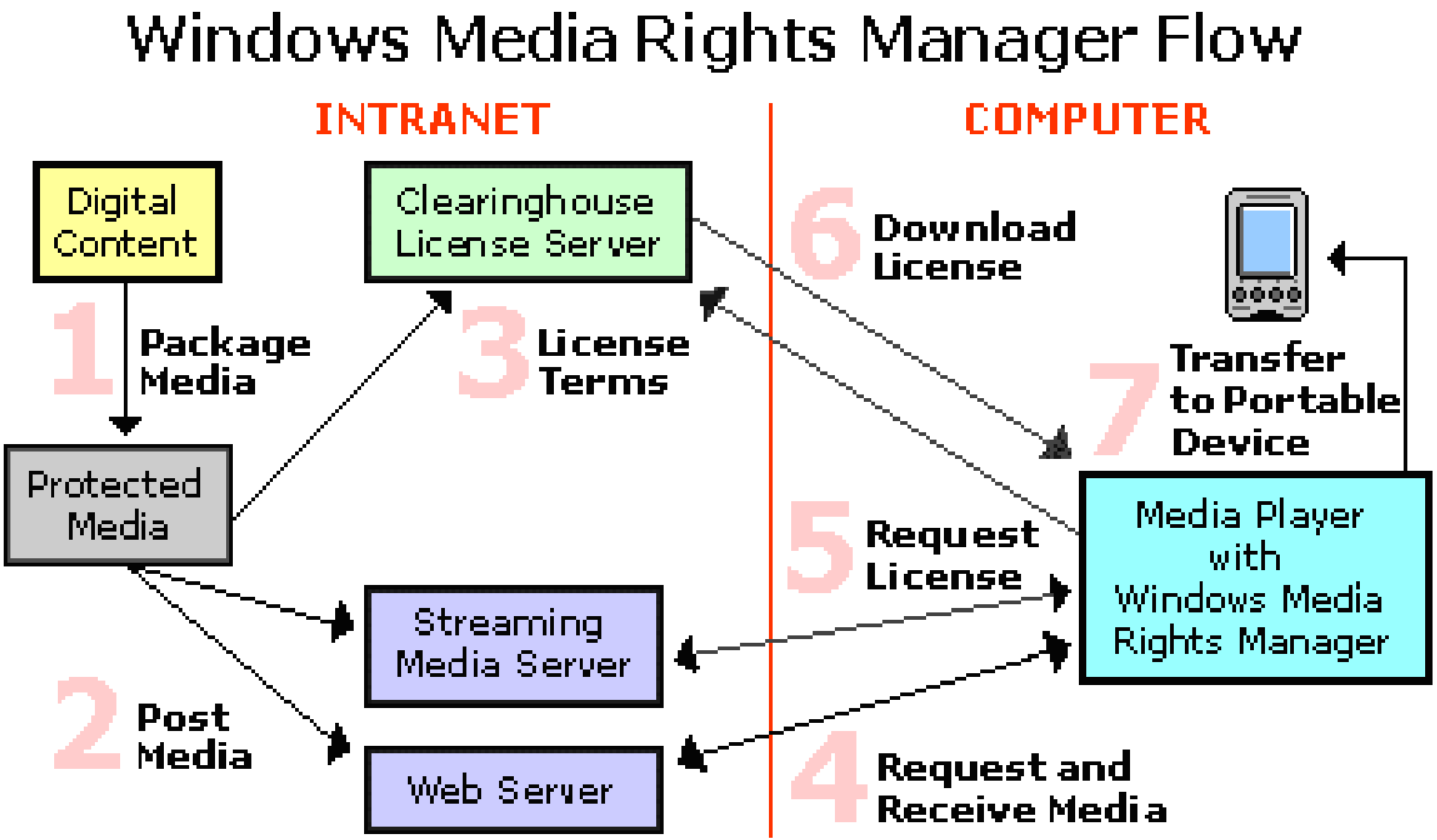
Współczesne systemy DRM

- Systemy DRM dla IPTV
  - Microsoft WindowsMedia
  - Marlin DRM
  - Verimatrix
  - DTCP
- Inne
  - FairPlay

Systemy DRM dla IPTV



Źródło: Microsoft



Źródło: Microsoft

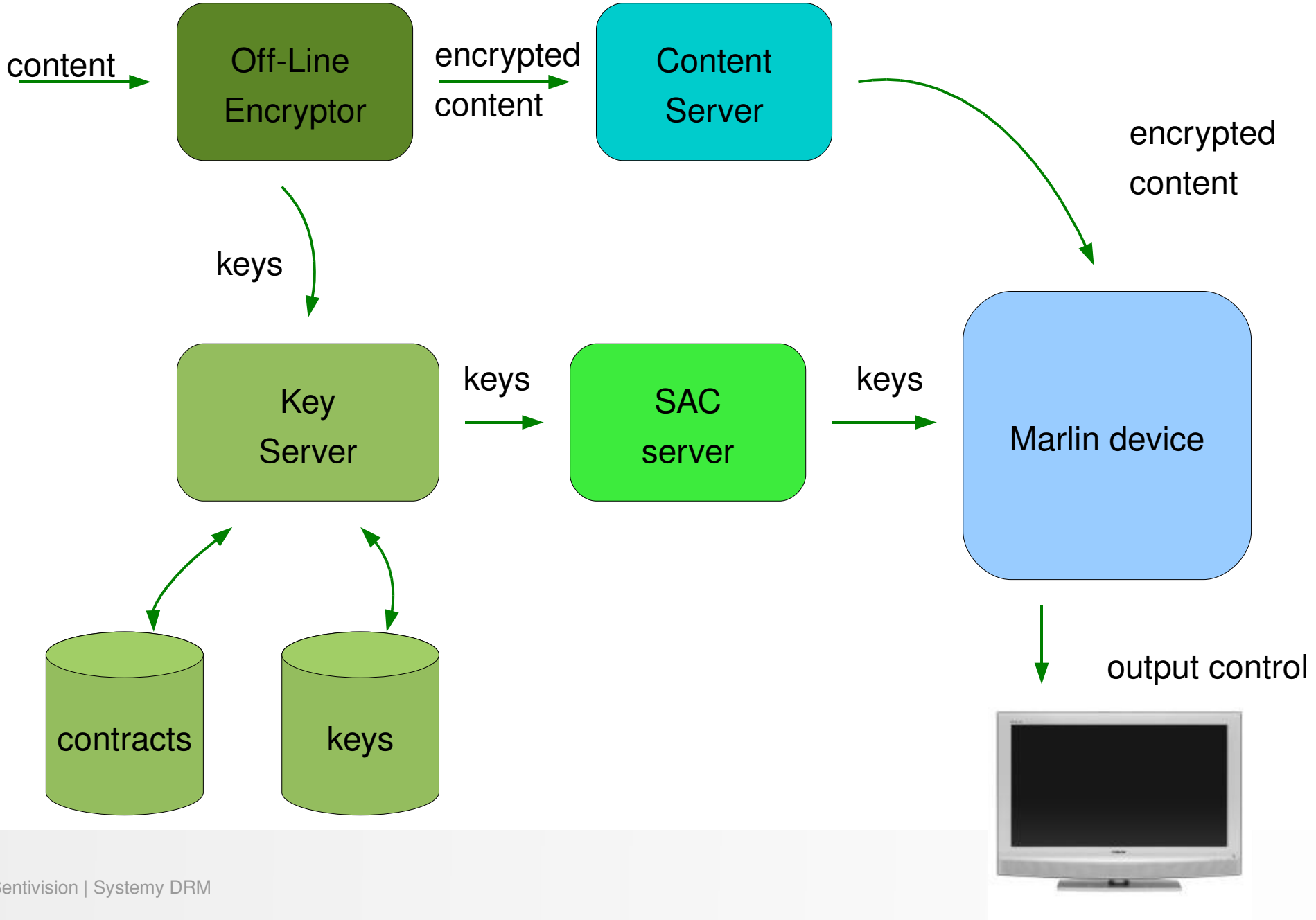
- Scenariusze wykorzystania
  - Bezpośrednie pobieranie licencji
  - Pośrednie pobieranie licencji
  - Usługi subskrypcji
  - Zakup i pobieranie pojedynczych utworów
  - Usługi wypożyczania
  - Wideo na żądanie i usługi typu pay per view
- Pliki ASF
- System zamknięty

- Urządzenia sieciowe
  - *ang. network devices*
  - przystawki cyfrowe, odtwarzacze DVD, odbiorniki multimediów cyfrowych i odbiorniki cyfrowego audio.
  - przesyłają zawartość w lokalnej sieci
  - nie przechowują zawartości
  - odtwarzanie zawartości w formie chronionej w sieci domowej bez jej lokalnego magazynowania
  - wykrywanie bliskości

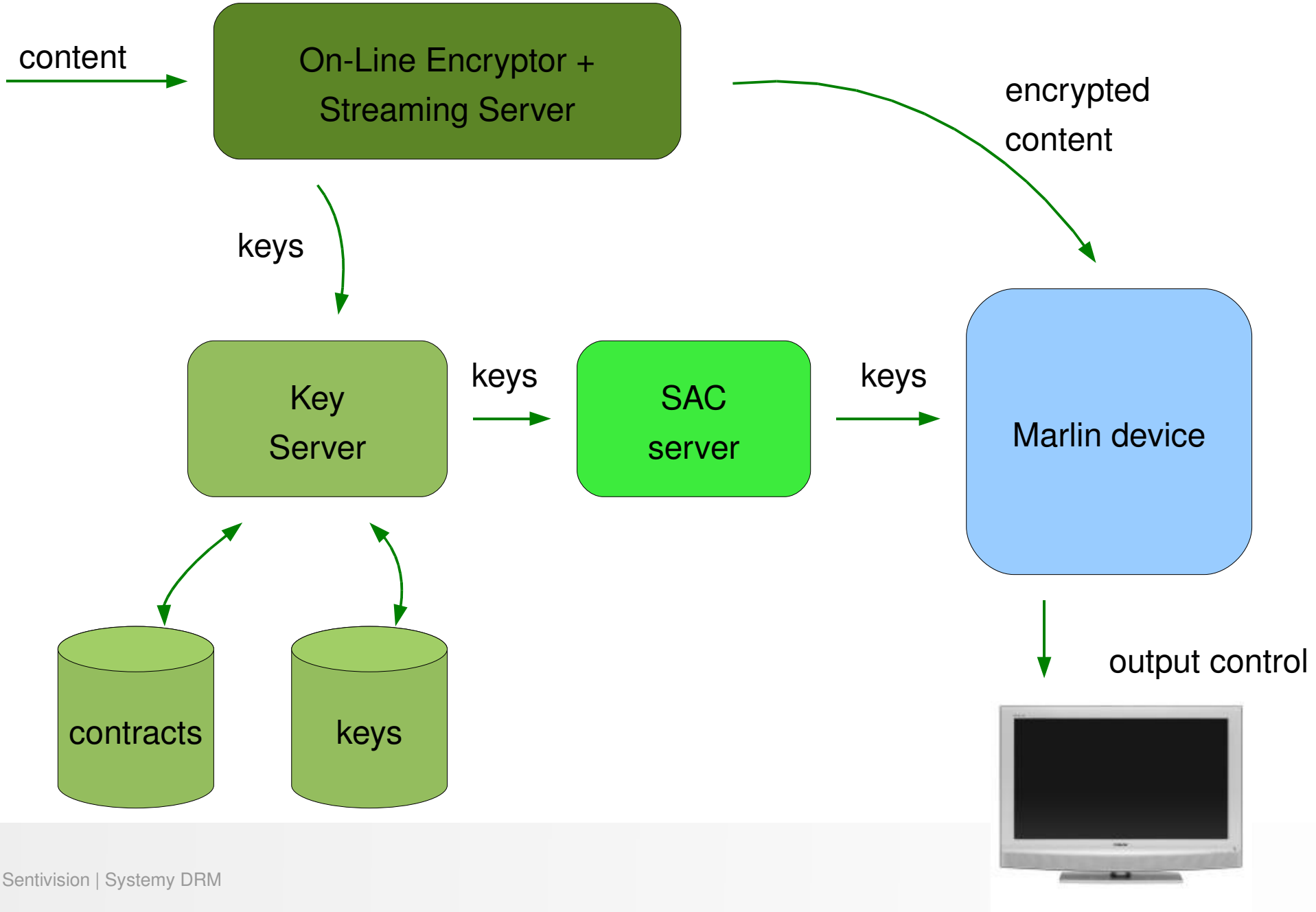
- Urządzenia przenośne
  - *ang. portable devices*
  - Przenośne odtwarzacze audio i wideo
  - Odtwarzanie z lokalnego dysku twardego
  - Obsługa VOD w sieci prywatnej

- Otwarty standard DRM
- Inicjatywa konsorcjum tworzonego przez
  - Intertrust Technologies, Matsushita Electric Industrial (Panasonic), Royal Philips Electronics, Samsung Electronics, Sony Corporation
- Wersje
  - Japońska (IPTV-ES)
  - Europa/Ameryka (Broadband)
- NEMO, Octopus
- Zgodny z OMA

Marlin DRM – architektura dla VOD

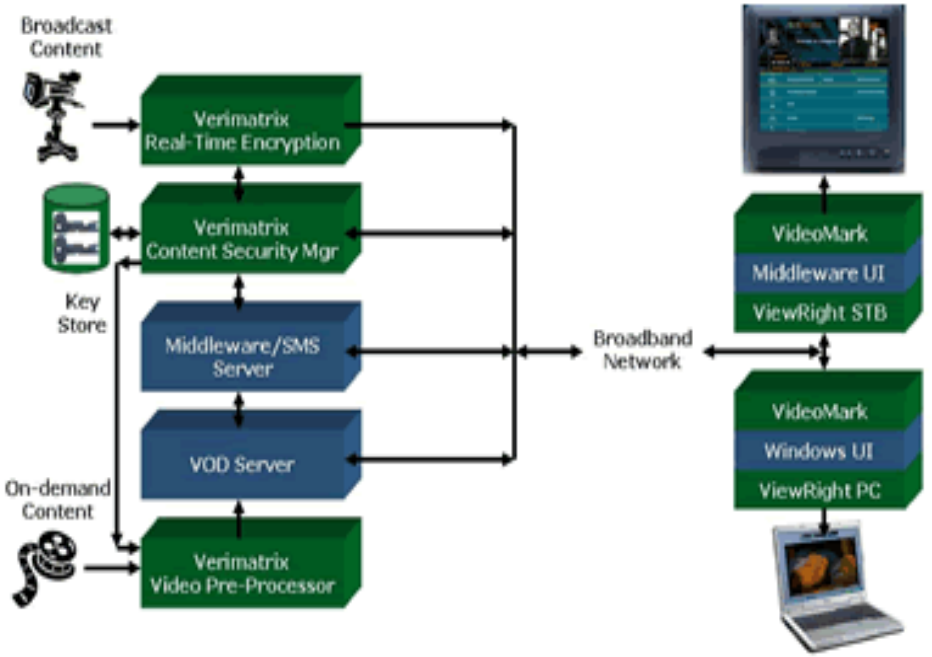


Marlin DRM – architektura dla TV



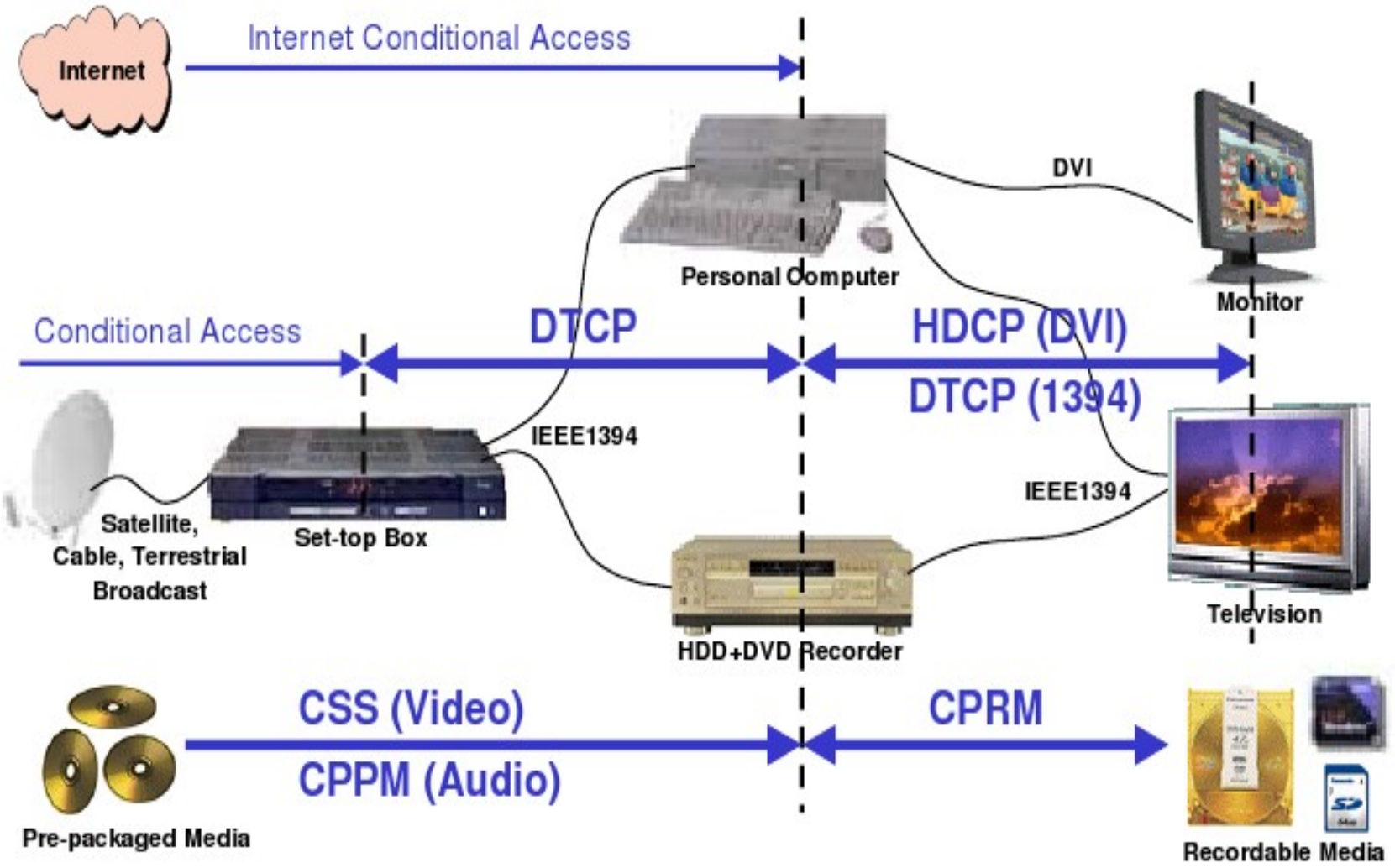
- Uwierzytelnienie
  - SAC: Secure Authenticated Channel
  - Oparty o krzywe eliptyczne
  - Każde urządzenie posiada certyfikat i klucze
- Treść (MPEG-TS/TTS) szyfrowana AESem
- Licencje
  - pojedyncza dla VOD
  - hierarchiczna dla TV (IPMC)
    - Klucz dla grupy kanałów

- Verimatrix Video Content Authority System (VCAS™)
- PKI i certyfikaty X509
- Watermarking
- Wykrywanie klonowania
- Rozwiązanie dla DVB, IPTV, IPTV over cable oraz Mobile



Źródło: Verimatrix

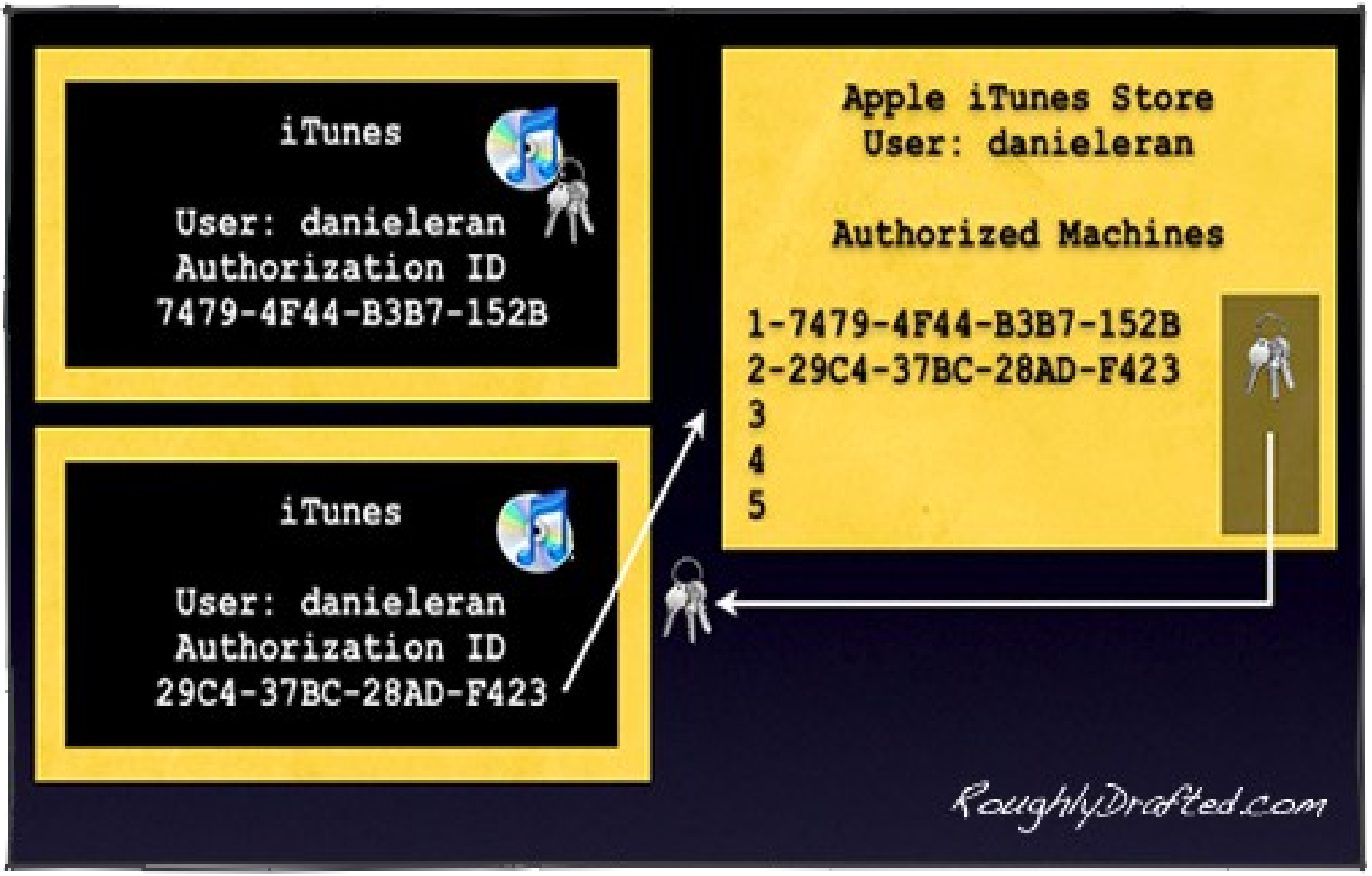
- Digital Transmission Content Protection
  - stworzony w 1998 przez Hitachi, Intel, Matsushita, Sony i Toshibę
- Umożliwia bezpieczną transmisję w ramach „cyfrowego domu”
- Wspiera USB, IP, WiFi, Bluetooth i MOST
- Wykorzystuje krzywe eliptyczne oraz PKI



Źródło: Intel

Inne systemy DRM

- FairPlay
  - Apple Computer
    - iPodach, iTunes, oraz iTunes Store
  - Szyfrowane są pliki muzyczne AAC
  - Ochrona przed nieatoryzowanym użyciem


iTunes
User: danieleran
Authorization ID
7479-4F44-B3B7-152B
iTunes
User: danieleran
Authorization ID
29C4-37BC-28AD-F423
Apple iTunes Store
User: danieleran
Authorized Machines
1-7479-4F44-B3B7-152B
2-29C4-37BC-28AD-F423
3
4
5
RoughlyDrafted.com

- Open Mobile Alliance
  - OMA 2.0, OMA BCAST
- DVB-CBMS (Convergence Broadcast and Mobile Services)
  - 18Crypt
  - Open Security Framework

Przyszłość

Dziękuję za uwagę

aneta.zwierko@sentivision.com

Sentivision POLAND

Phone +48 22 640 0860

http://www.sentivision.com