Requirements on reconfigurable platform for DRM implementation

Martin Šimka, Sentivision Polska

martin@sentivision.com

sentivision

Contents

- DRM – Digital Rights Management
- Typical DRM application
- Requirements on a target platform
- DRM on reconfigurable HW

Digital Rights Management 1/2

- Access control
  - Authentication
- Content protection
  - Encryption, Watermarking
- Usage control
  - Metering, Output limitations

Digital Rights Management 2/2

- Well known applications
  - Copy protection for CD, DVD, ...
  - DRMs for mp3 players (e.g. iPod)
- Other areas
  - IPTV and VoD (Video on Demand) systems
  - Maps for GPS
  - ...

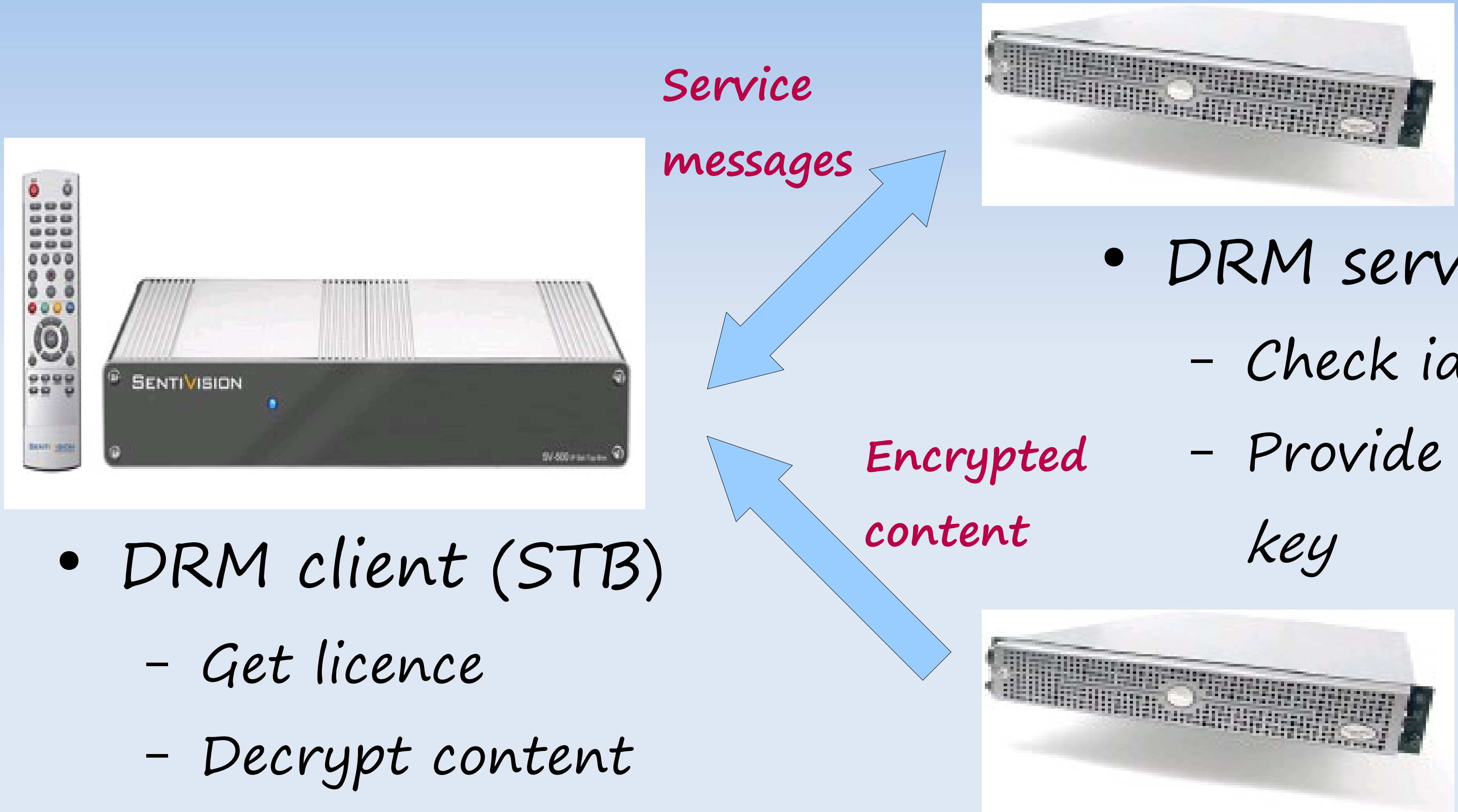
Typical DRM application 1/3

- In VoD system
  - Based on chip-cards or public-key certificates
  - Communication over an insecure channel (internet)
  - Several DRM standards (Verimatrix, Windows Media, Marlin, Secure Media, ...)

Typical DRM application 2/3

- Public-key cryptography
  - Parties authentication
  - Purchase of license
- Symmetric cryptography
  - Content encryption

Typical DRM application 3/3



- DRM server
  - Check identity
  - Provide content key

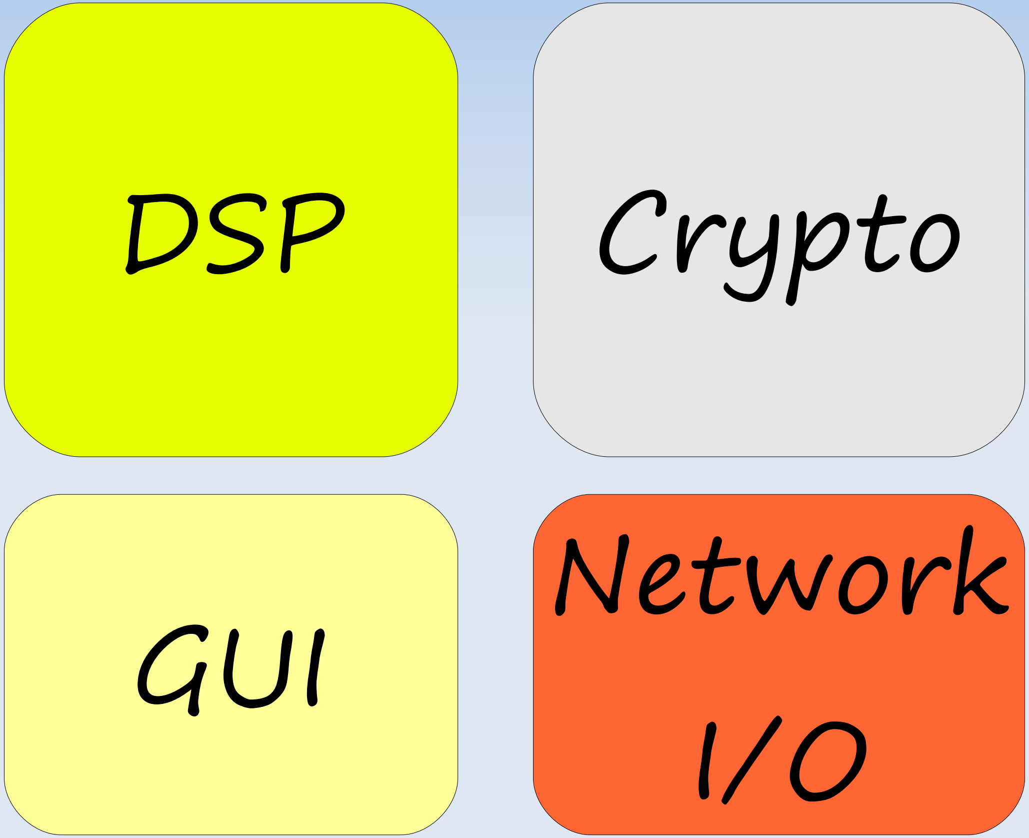
- DRM client (STB)
  - Get licence
  - Decrypt content

- Content server

Requirements for platform

- DRM is just one part of the VoD system
- Heavy use of resources:
  - Content decoding – digital signal processing (DSP)
  - Content decryption, signature generation/verification

Main parts of the system



DSP

Crypto

GUI

Network I/O

Performance of the system

- DSP
  - H.264 / WM / MP4 decoding
- Crypto
  - RSA/ECC, RC4/AES/DES, TRNG, SHA
- Hardware acceleration
  - Coprocessor, special instruction set

Security of the system

- Requirements
  - Code and platform trust
  - Secure memory operations
  - Secure storage
  - Reliable source of randomness
  - Secure clock

How suitable is FPGA for DRM?

- Support for HW operations
  - IP blocks, instruction sets
  - For crypto and DSP operations
- Dynamic reprogramming
  - For various standards

How suitable is FPGA for DRM?

- One chip solution
  - Throughput of the on-the-fly decryption and decoding
- DSP & FPGA (separated chips) solution
  - Platform trust, bus&memory encryption/data integrity

How suitable is FPGA for DRM?

- FPGA – a secure platform?
  - Secure storage memory, TRNG, Secure clock
  - Still open issues
- Price
  - Expensive chips, complicated development

Conclusions 1/2

- VoD system with DRM requires hardware support for:
  - Cryptographic operations
  - DSP operations
- Several algorithms system is suitable for implementation on reconfigurable platform

Conclusions 2/2

- Problematic areas:
  - performance (decoding + decryption)
  - security of the platform
  - price

Questions?

Thank you for your attention!