Adeas

HDCP

High-bandwidth Digital Content Protection

Introduction

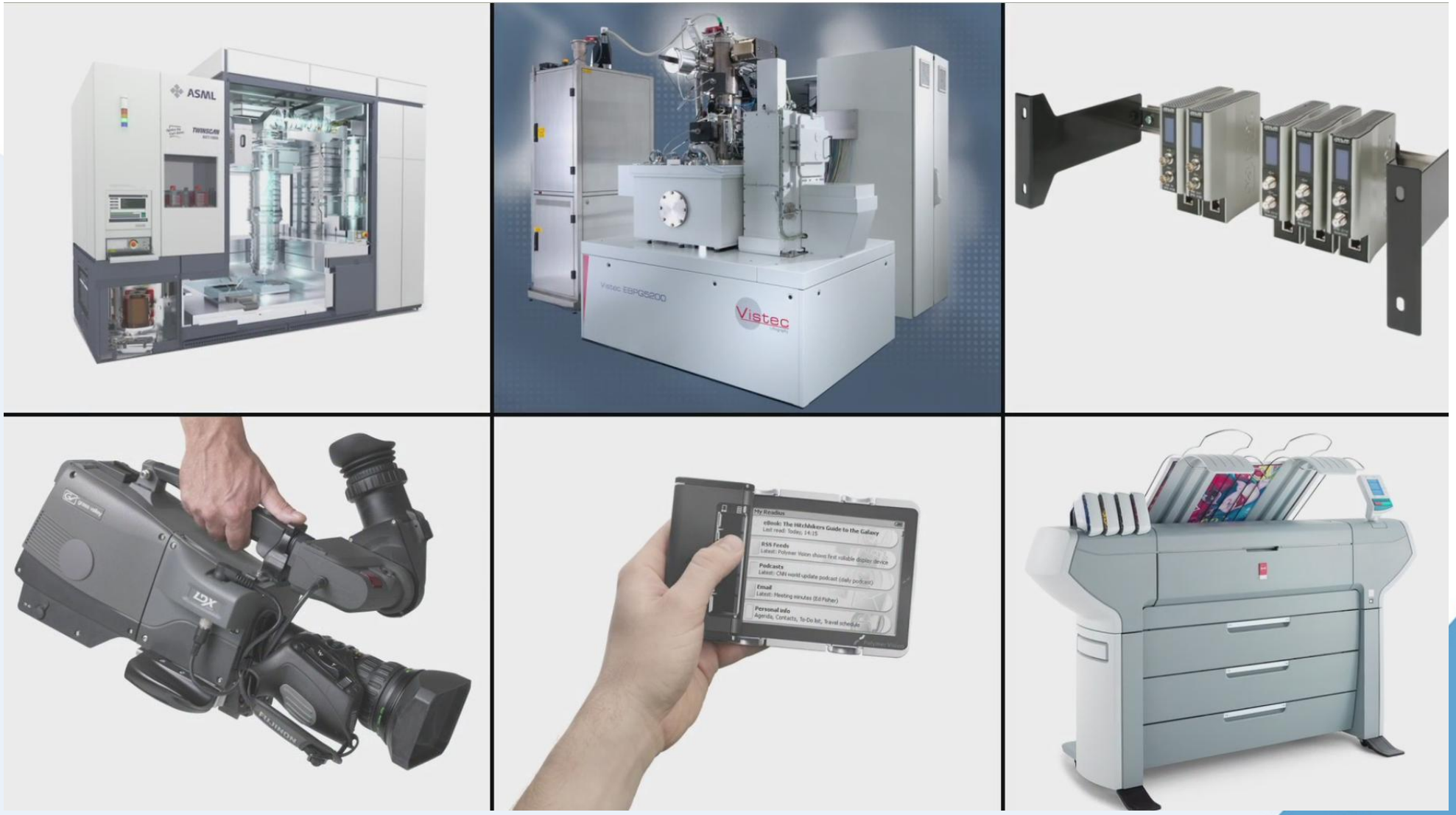
Who are we?

- Antoine Hermans, CTO
- Raymond Hermans, Designer

Who is Adeas?

- Independent Design House located in Eindhoven.
- Developers of customer specific electronic products, embedded systems and IP.
- Active in professional and industrial markets such as Broadcast, pro AV, printing, semiconductor and high tech machinery
- **Adeas specializes in FPGA and SoC solutions on advanced digital and mixed signal boards**
- Design Partner of both Altera and Xilinx

Introduction

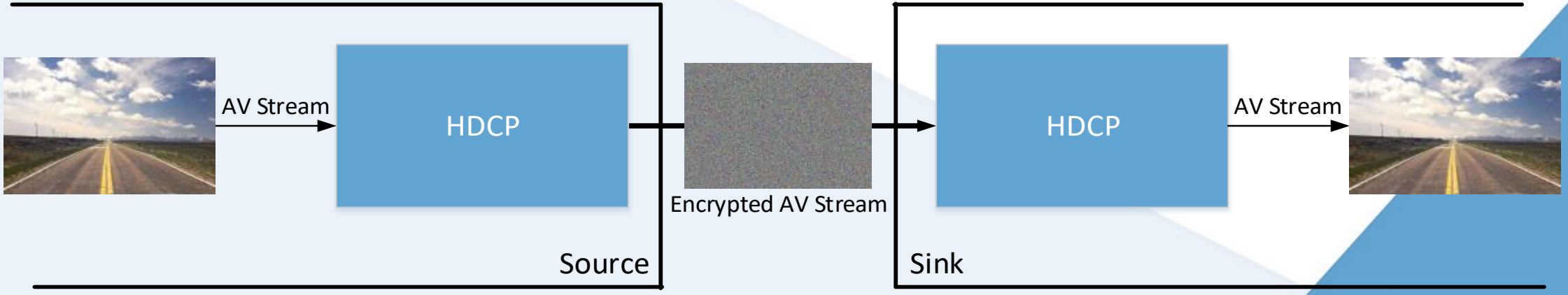


Agenda

- What is HDCP?
- HDCP2.2 main components
  - Authentication protocol
  - AV Encryption
  - System Renewability Message
- Reference design
  - HDMI pass-through reference design
  - Challenges
  - Testing
- Conclusion

What is HDCP?

- High-bandwidth Digital Content Protection
- Developed by Intel, licensed by DCP LLC
- Specification is open
- Used with i.e. HDMI, DisplayPort
- Source, Sink, Repeater

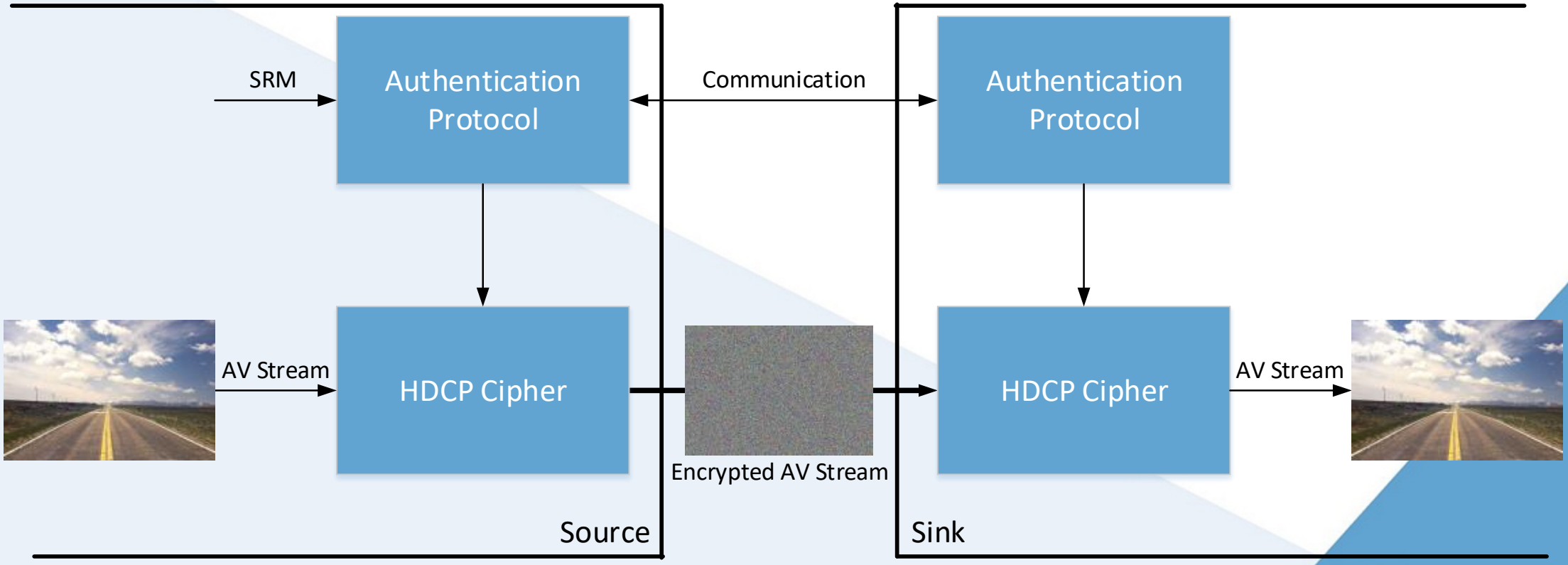


Agenda

- What is HDCP?
- **HDCP2.2 main components**
  - Authentication protocol
  - AV Encryption
  - System Renewability Message
- Reference design
  - HDMI pass-through reference design
  - Challenges
  - Testing
- Conclusion

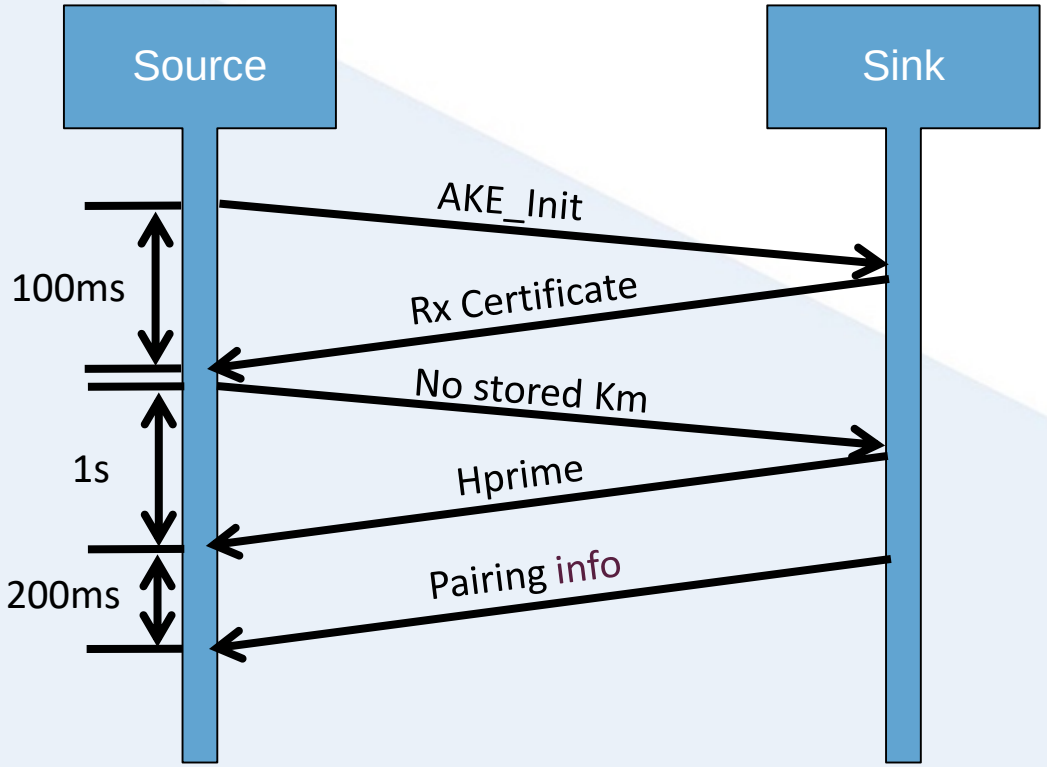
HDCP2.2 main components

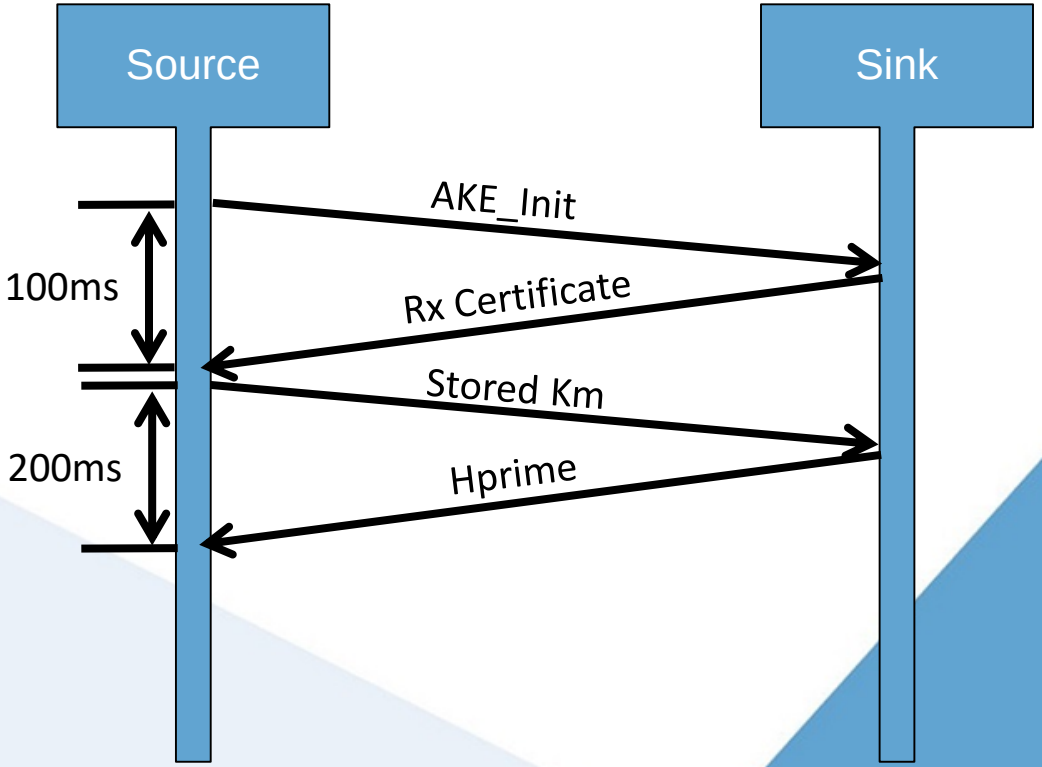
- Authentication protocol
- AV Encryption
- System Renewability Message (SRM)



Auth. protocol ; AKE phase

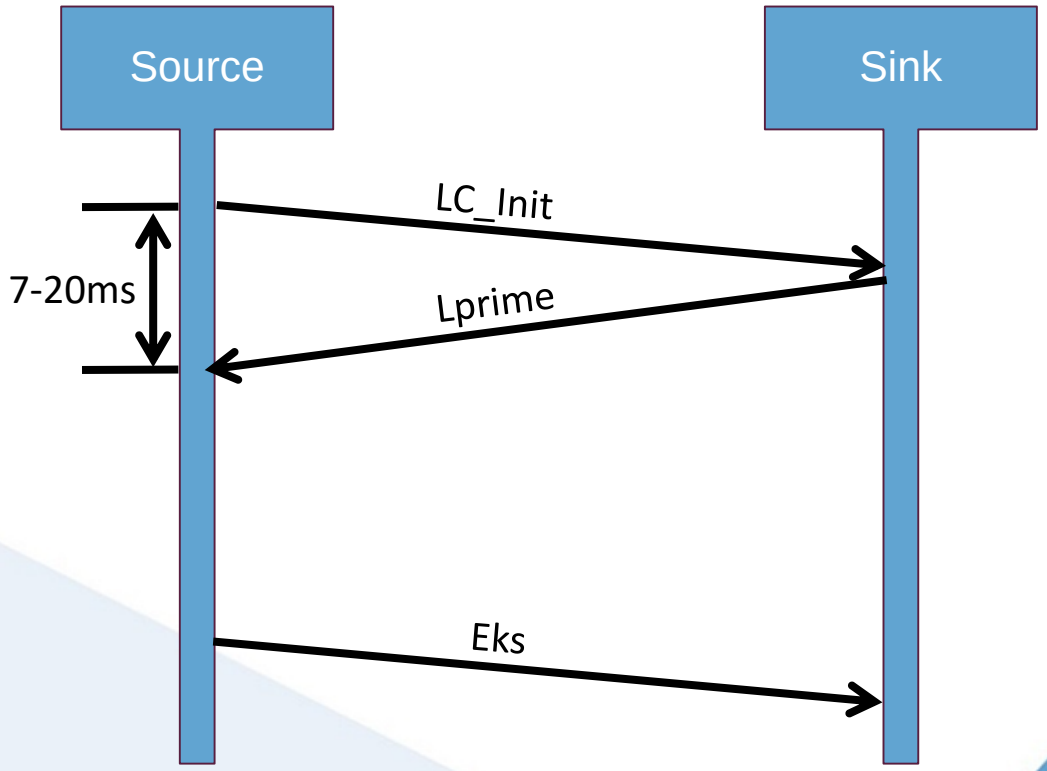
- Validate HDCP sink
- Exchange master key (Km)





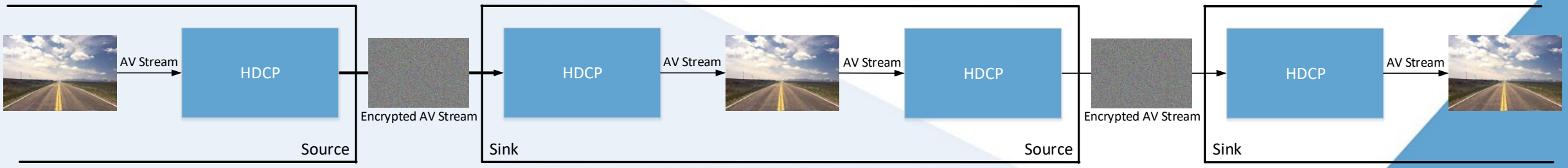
Auth. protocol ; Continued

- Locality check:
  - Verify locality HDCP sink
  - 7 ms (HDMI: 20 ms)
- SKE phase:
  - Transfer session key
    - Used during encryption



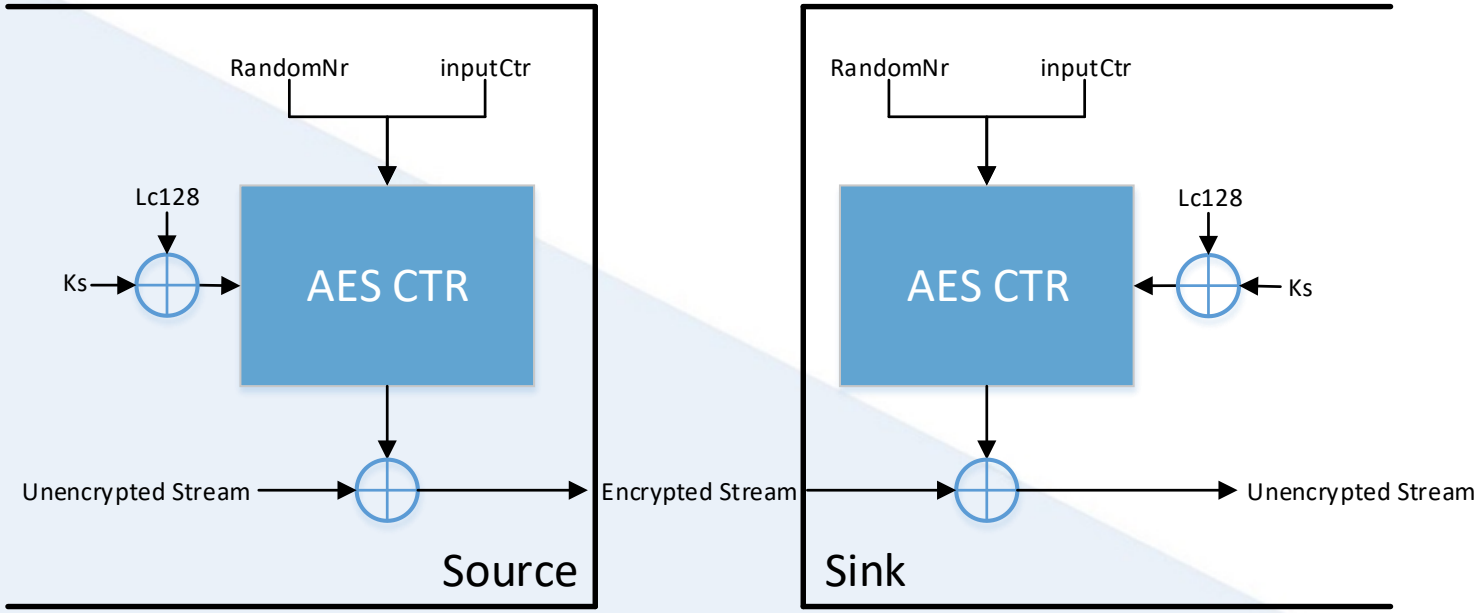
Auth. protocol ; Repeaters

- Extend the link (cable extender or splitter)
- Protocol converter (HDCP 2.2 <-> HDCP 1.4)
- Receiver ID list from all devices
- Max devices 32, max depth 4
- Content stream management



Encryption of audio and video

- 128 bit AES block cipher in counter mode
- Session key Ks
- Global constant Lc128



System Renewability Message

- List containing revoked receiver IDs.
- Stored in non-volatile memory
- Protected with signature
- Must be updated when new version is available / received

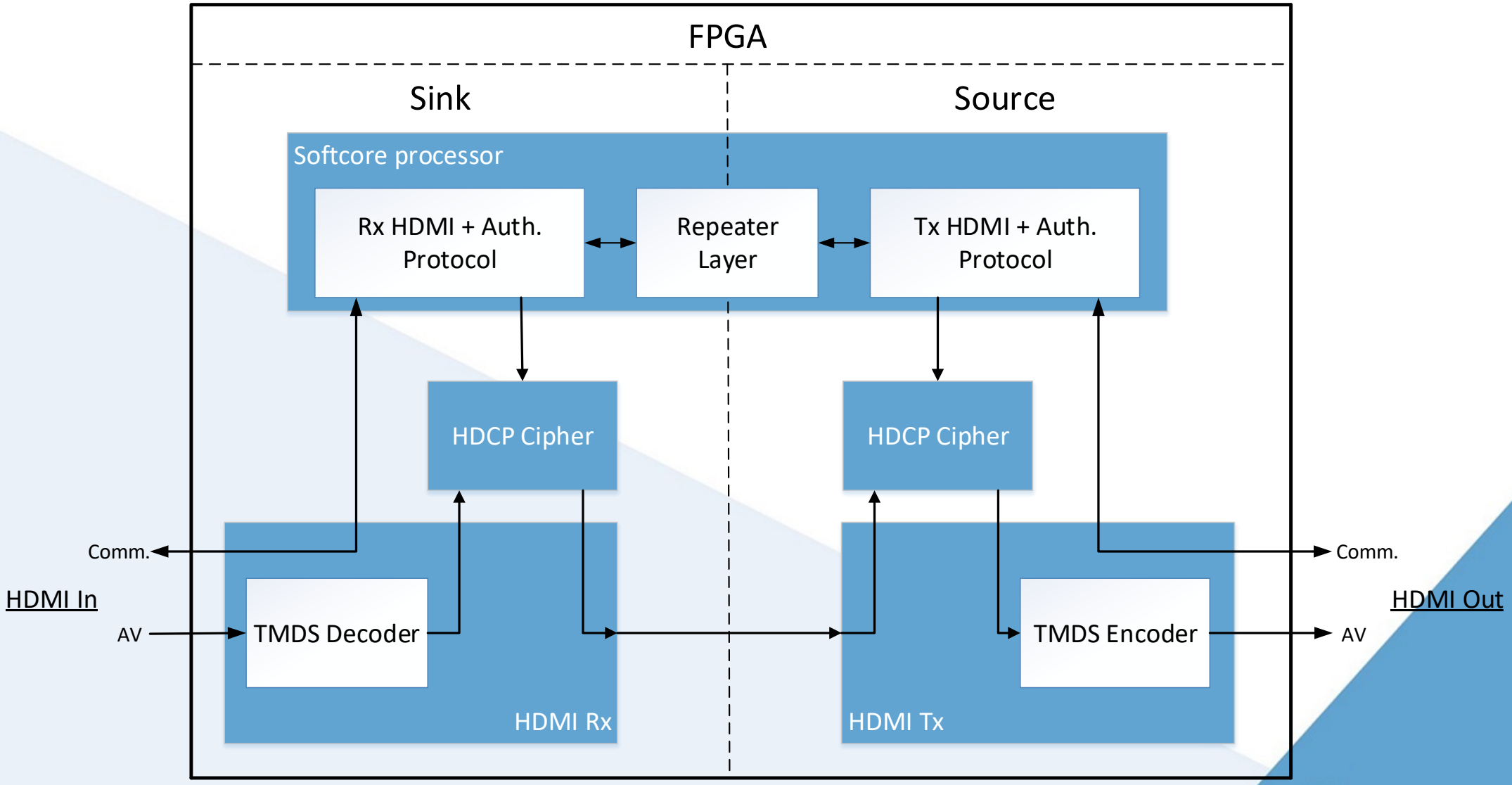
Agenda

- What is HDCP?
- HDCP2.2 main components
  - Authentication protocol
  - AV Encryption
  - System Renewability Message
- **Reference design**
  - HDMI pass-through reference design
  - Challenges
  - Testing
- Conclusion

HDMI pass-through reference design

- Why?
  - To be able to test and certify HDCP functionality
  - To enable customers to try out functionality
  - To give customers a head-start to integrate HDCP into their own design
- What?
  - HDMI input to HDMI output, including HDCP and repeater functionality
  - FPGA design running on a standard development kit
  - I/O realisation using an FMC extender board

HDMI pass-through reference design



Reference design

- Challenges
  - Debugging hash algorithms
  - Authentication protocol prone to errors
    - Started with SW only implementation
      - ➢ Enabling emulation of automated random topologies
  - @100MHz SW only approach did not meet timing
    - Acceleration in FPGA fabric
  - Testing (incl. interoperability)
    - Testequipment contained bugs
    - Commercial HDMI2.0 / HDCP2.2 devices not readily available
    - Commercial equipment erroneous HDMI / HDCP implementation
  - Key management
    - Must be securely stored

Agenda

- What is HDCP?
- HDCP2.2 main components
  - Authentication protocol
  - AV Encryption
  - System Renewability Message
- Reference design
  - HDMI pass-through reference design
  - Challenges
  - Testing
- **Conclusion**

Conclusion

- It is possible to implement a fully functional HDCP core (for source, sink and repeater) in an FPGA
- FPGA needed for encryption of A/V, and very handy for combining software control approach with strict timing requirements.
- Confirmation to the specification is a matter of system design, not only IP-core design
  - Copy protection
  - Key management
- (Interoperability) testing is difficult when technology is new

- QUESTIONS ?