



# MCARD Overview

March 19, 2015



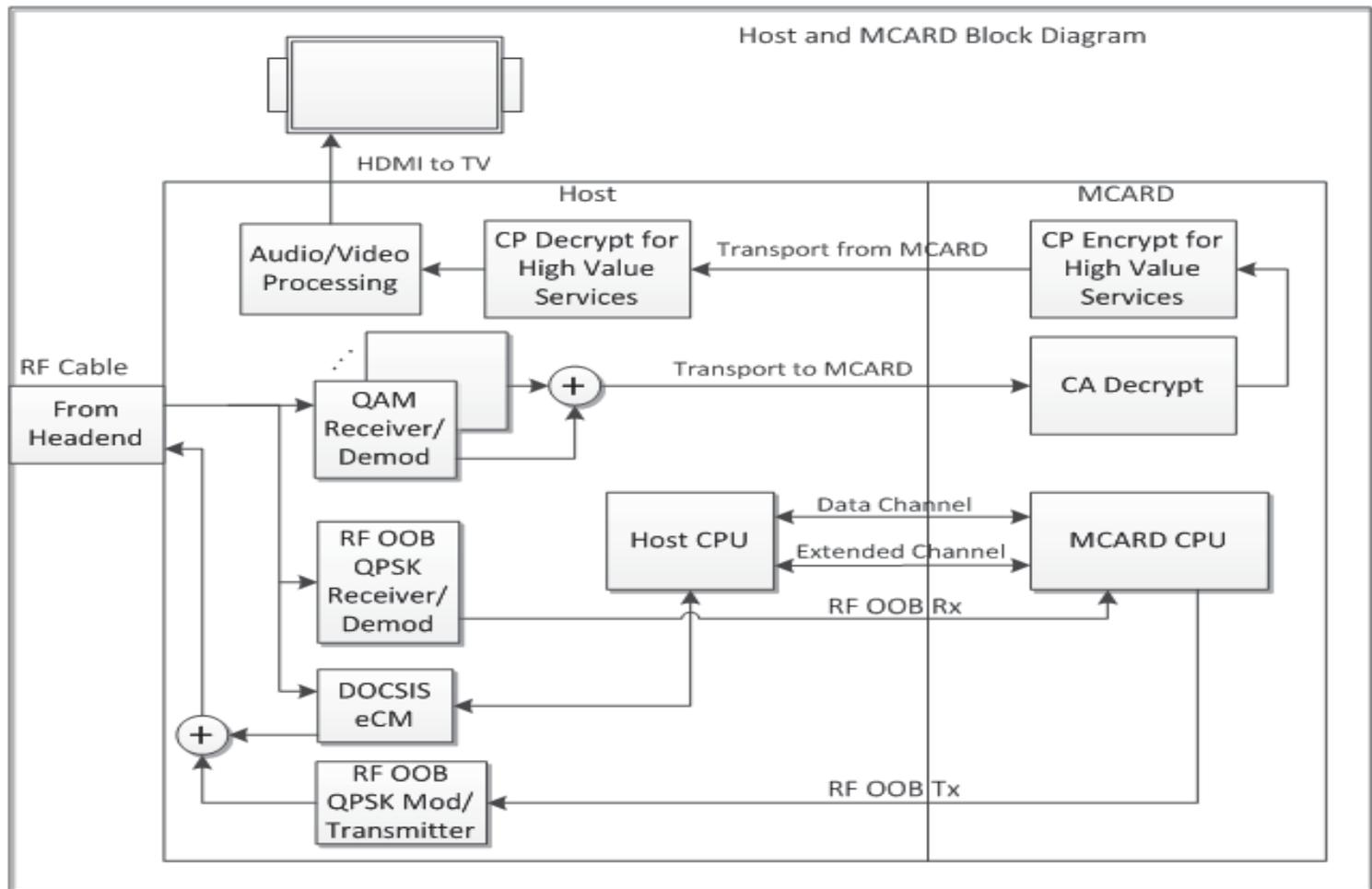
Copyright © 2015 CCAD, LLC  
All Rights Reserved

# MCARD Overview

---

- ❑ CableCARDS provide a standardized way to separate security and network specific functions from generic set top box (STB) functions.
    - At the time, SA and GI systems. Tried to capture differences that existed at the time between the systems at the “plumbing level”.
    - As the systems evolved, various changes and augmentations needed to be made to account for innovations going on in the systems. Examples are DOCSIS, SDV, and Multi Tuner DVR.
  
  - ❑ The device that a CableCARD plugs into is called a Host.
  
  - ❑ The Single-stream CableCARD (SCARD) had limited deployment and was replaced with the Multi-stream CableCARD (MCARD).
    - Had to have 2 cards for watch & record DVR support
    - Also had to later create an SVD tuning resolver to hide SDV implementation details, which varied widely across systems.
  
  - ❑ MCARD supports at least four services, and is thus used in multi-tuner Hosts.
-

# Host and MCARD Block Diagram



# MCARD Overview – Head end

---

- ❑ For in-band data the cable system head end:
  - Encrypts the audio/video packets.
  - Inserts ECMs.
  - Assembles services into QAM streams.
  - Assigns QAM streams to RF frequencies.
  
- ❑ Out-of-band (OOB) data, such as EMMs, are sent to the Host/MCARD via either RF OOB (QPSK) or DOCSIS.
  - The diagram shows the extended channel as the conduit for supporting DOCSIS
  
- ❑ Two way Hosts can return data from the MCARD to the head end, via either RF OOB, or DOCSIS.

# MCARD Overview – Host and MCARD Partitioning

---

- ❑ The Host contains all receivers/demods, plus any modulators/transmitters, for data from and to the head end, whether in-band or out-of-band.
- ❑ In band transport data, the encrypted audio and video MPEG packets, are routed from the Host to the MCARD for conditional access decryption.
- ❑ The MCARD adds copy protection encryption for high value services, and returns the transport data to the Host.
- ❑ The Host performs copy protection decryption for high value services and then audio and video processing for presentation to the user.

# MediaCipher – Local Host/MCARD Threat Analysis

Threat	Mitigation
Unplug OOB receiver to miss EMMs.	Periodically change EMM keys.
Unplug OOB transmitter to avoid reporting PPV purchase.	MCARD security subsystem enforces a credit limit, to limit the number of PPV purchases that can be made before reporting is required.
Attempts to read or clone keys.	A robust hardware/firmware design protects keys from being read.
Attempts to change STB/MCARD code to weaken or remove security features	STB/MCARD only accept signed code.

# MediaCipher – System Threat Analysis

---

Threat	Mitigation
Brute force cryptographic attack using plaintext and ciphertext to deduce decryption key.	Use small key change intervals for content decryption keys.
Compromised keylist.	A hardware based key is required to uncover sensitive data on the keylist.
Rent multiple STB/MCARDs on a single account, and redistribute.	Monitor STB/MCARD response pattern versus network topology.