

## Overview

Aizyc HDCP IP core (High-bandwidth Digital Content Protection (HDCP) IP is a key security technology that addresses all content protection needs for high-value digital content.

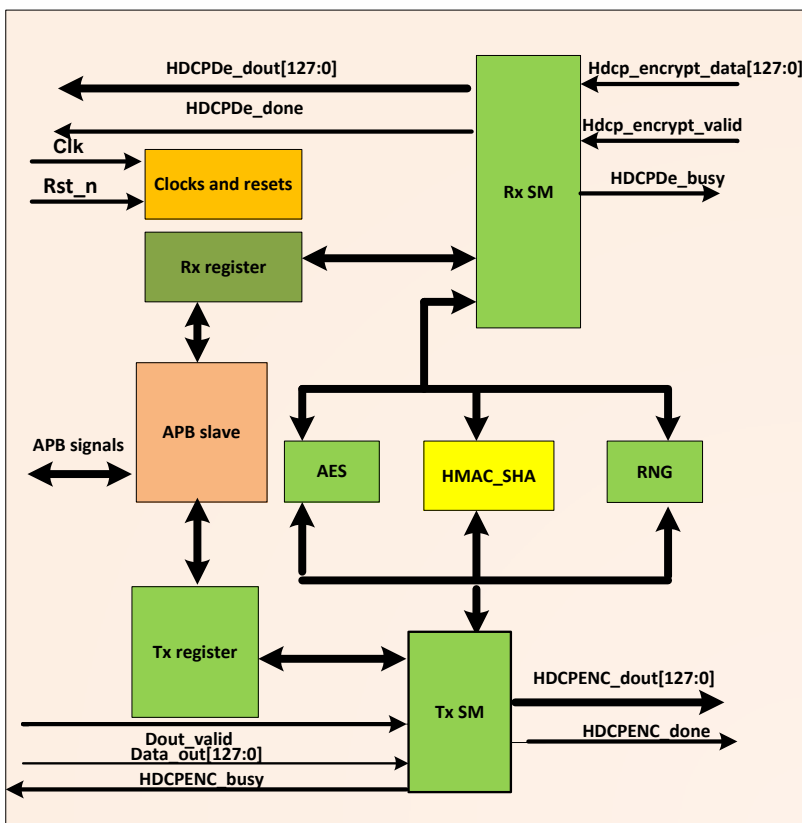
The HDCP IP Core offers out of the box solution for SoC designers to integrate itself with minimal tweaking. The IP comes with supporting firmware in Linux.

**Authentication:** A HDCP transmitter and receiver pair performs authentication before it does AV data transfer. Authentication involves a series of control messages to be exchanged among transmitter and receiver. As two things are established (1) receiver is authentic (2) a secret key that will be used for encrypting AV data.

Hardware and Software together play a role in authentication process. Software detects receiver when it is connected and directs the HW to start authentication. HW generates control messages and associated data for authentication, writes the data to registers and interrupts SW to let it transfer messages to Receiver. Control messages received from the other end are written to register set by SW thereby HW reads and performs authentication checks.

The IP core is portable to an ASIC or a FPGA. Along with the IP core, we will provide complete test environment with constraint randomized test cases and our full support during integration.

## Functional Block Diagram



## HDCP 2.0 IP Core

### Features

- Compliant to HDCP Rev 2.0
- Performs Authentication and Session management
- Performs encryption and decryption
- Supports repeaters.
- Supports 32-bit APB slave interface for register configuration.
- Linux based software is provided.
- AES-128 in CTR mode
- SHA-256 in HMAC mode
- Random Number Generator compliant to NIST-SP 800 90
- Gate count - 120K
- Platforms- ThreadX, Linux, Ucos-ii RTOs

## Functional Block Description

### HMAC\_SHA

**HMAC** (Hash-based Message Authentication Code) block is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret key. SHA-2 is used in HMAC mode. In HDCP authentication HMAC is used in three of the processes.

- (1) to compute H/H' using Kd, (2) to compute V and V' for authentication with devices connected across repeaters and (3) to compute L/L' for locality check.

### Tx/Rx registers

Registers are used for HW/SW interface. SW accesses registers over APB interface. HW uses registers to set the message and data for control messages and raises an interrupt to SW to let it transfer the message to receiver. The messages received at system are written to receive set of registers and flagged using control bits to let the HW process them.

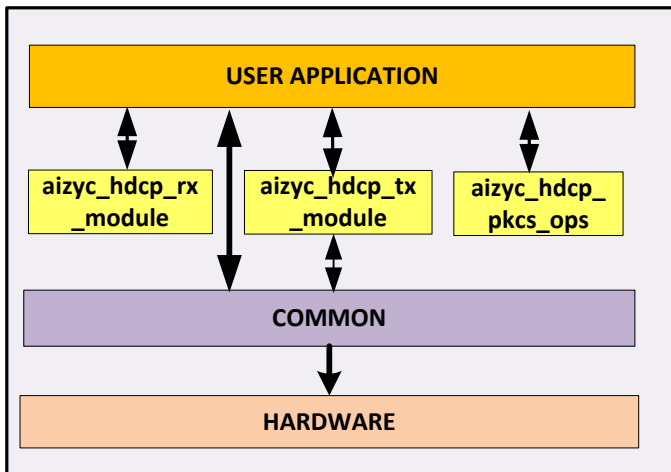
### AES

128-bit AES is used in CTR Mode. AES is used in authentication for RNG, master key generation, key derivation and also in data transfer

### RNG

Deterministic Random Number Generator used in both HDCP Transmitter and HDCP Receiver. Counter based DRBG using AES-128 Block cipher specified in NIST SP 800-90 is used. It generates random values for secret key material  $r_{tx}$ ,  $r_{rx}$ ,  $r_{iv}$ ,  $r_n$ ,  $k_m$ ,  $k_s$ .

### Sample Driver



### Software Operations

**MASTERKEY encryption:** Master key encryption is done using RSHE-SOAEP encryption scheme defined by PKCS #1V.2.1 RSA cryptography standard.

**MASTERKEY decryption:** Master key decryption is done using RSHE-SOAEP encryption scheme defined by PKCS #1V.2.1 RSA cryptography standard.

**SRM and signature verification:** Receiver certificate's signature and SRM are verified using RSASSA-PKCS1-V1.5 scheme as defined in PKCS#1 V.2.1 RSA cryptography standard.

### Clocks and Resets

HDCP2.0 works on a single clock, clk. Clock frequency is not governed by HDCP specification. Based on implementation we expect to achieve 135 MHz.

### Contact Information

Aizyc Technology Private Limited  
6th Floor, Plot No: 488 & 489,  
Ayyappa Society, Madhapur  
Hyderabad - 500081, AP, India , Phone: +91 40 6459 -9771

USA Branch: 228 Hamilton ave,  
3rd Floor, Palo Alto, CA 94301  
Phone: +1 (408) 338 - 69291

### Design Attributes

- Fully Synchronous Design
- Technology independent design
- Highly modular design
- Platforms : Solaris and Linux
- Verilog Simulators : Cadence IUS

### Aizyc Advantage

- Scalable IP Core
- Compact Design
- Cost-effective
- Portability : ASIC, FPGA
- Validation on Xilinx Spartan 3
- Continuous support during integration, design and verification

### Deliverables

- Synthesizable Verilog RTL
- Test bench and exhaustive Test cases
- Synthesis constraints and script files
- Sample AHB Slave Driver
- Documentation – User Manual, Verification plan , Validation Report, Synthesis, DFT and Integration Guidelines