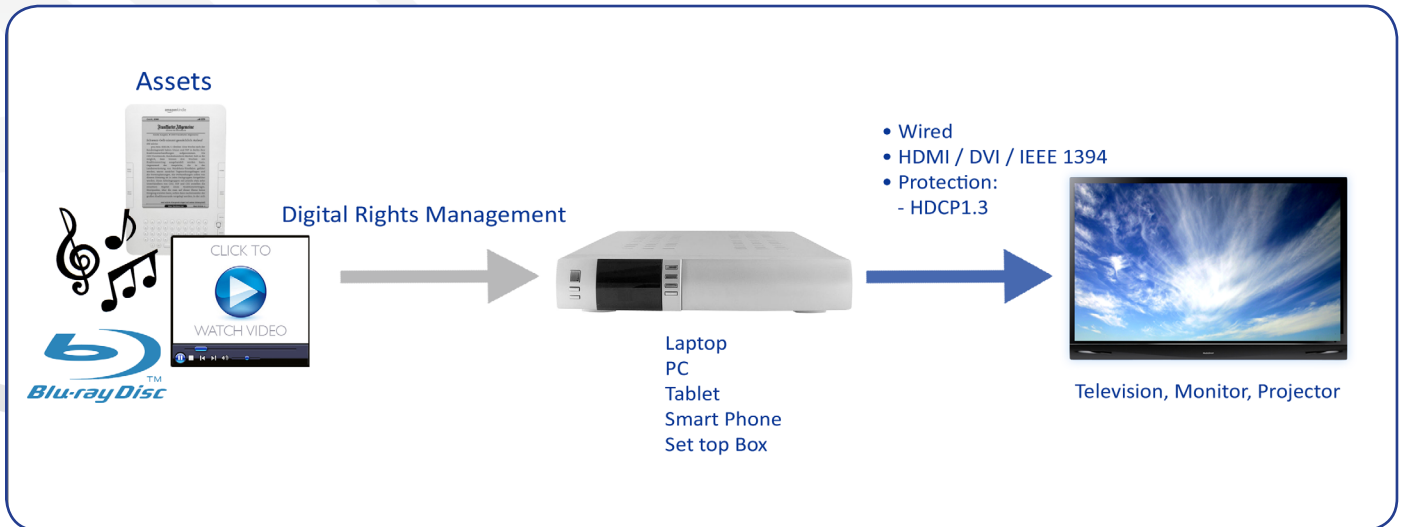


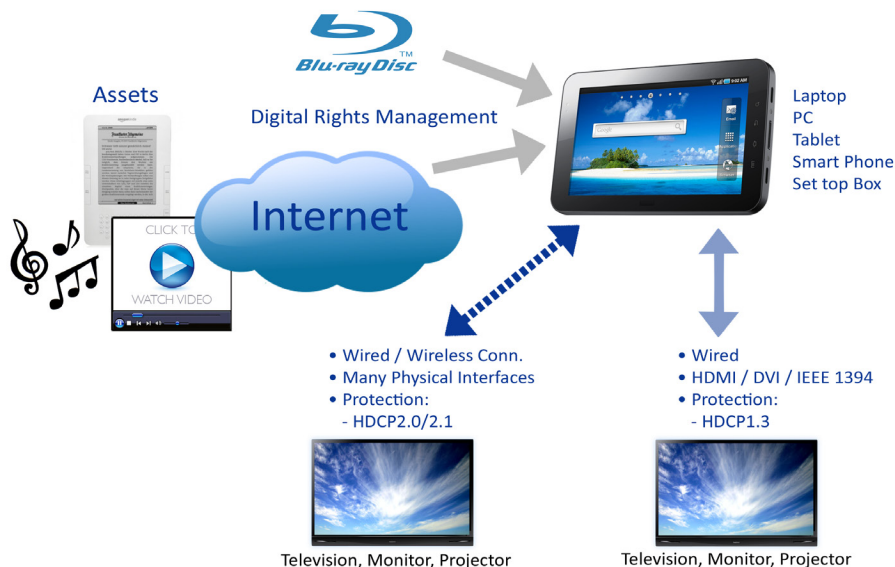
# High-bandwidth Digital Content Protection (HDCP)



## Introduction

For distributing High-value digital content generally Digital Rights Management (DRM) technology is used. Once the content is available inside a device like a Settop Box, Notebook or PC the content must be kept secret and may only be forwarded to another device unless it is encrypted. The most commonly used technology today for transferring HD content is an HDMI connection which includes HDCP1.3 protection. Besides the traditional devices (Notebook, Laptop, PC) other devices like Tablets and Smart-phones are being used for viewing HD content and in addition high value digital content

is more and more distributed via the Internet. In addition to these market changes many other wired and wireless interfaces are being used besides e.g. HDMI. All the above changes have created an increasing need for high-end content protection. The HDCP2.1 content protection standards are developed and adopted for protecting commonly used TCP/IP based connections like WiFi, USB, Ethernet and for uncompressed and high-bandwidth interfaces like DiiVA, WiGig, WHDI, WirelessHD.



## High-bandwidth Digital Content Protection

In a system where high value content is available and which requires copy protection, the digital content and the technology that provides the secure communication between two devices must be protected. The secure part of the content protection system can be implemented in hardware protected software by using e.g. Trustzone. AuthenTec provides complete solutions for implementing the HDCP2.0/2.1 standards.

In addition a highly secure and optimized hardware module is available by which the highest level of security can be achieved, provides easy system integration, optimal performance and lowest power dissipation. The EIP-115 forms the hardware-based security boundary wherein all secure parameters and cryptographic computations are managed during all the HDCP2.1 protocol phases from authentication of the connected devices up to and including the generation of the key stream. The EIP-115 is defined for being used in source and sink devices or in a combination of both (bridge/repeater devices).

The EIP-115 hardware security module can be integrated into Application Processors, Multimedia Processors, SOC's for Settop Boxes, Graphics Processors, etc. As the output of the EIP-115 are the generated session keys and input vectors to be used in the AES-128 based cipher module, multiple commonly used interfaces can be used like USB, WiFi and Ethernet. Newly introduced wireless and wired interfaces like WiGig, WirelessHD, WHDI, DiiVA, etc. are also supported by the same module although some of these interfaces require an additional interface specific cipher engine.

### SOFTWARE

The HDCP2.1 High-bandwidth Digital Content Protection software provides all required features for a complete content protection solution which also includes all control and management software for the HDCP standards. Besides the cryptographic functions and secure computations module the software includes the implementation of the state diagrams as defined by the HDCP2.1 standards and supports the TCP/IP based communication between a transmitter, receiver and repeater (bridge).

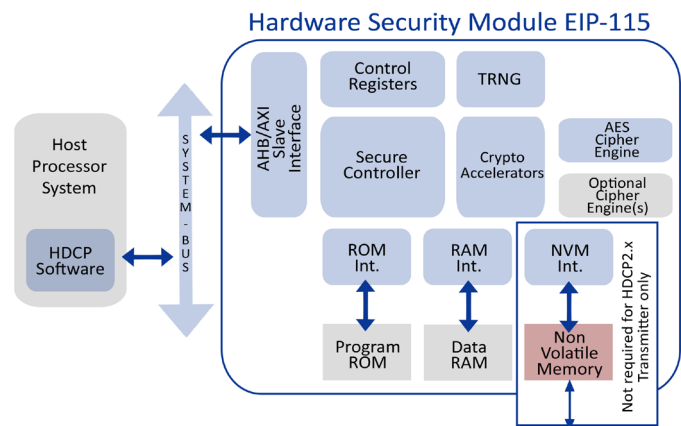
The EIP-115 hardware security module can be used seamlessly with this software, by replacing the security required part of

the protocol, for the highest level of security and to comply with the latest HDCP content protection specifications. Since the software includes specific API's for DRM it can be used in combination with AuthenTec's DRM Fusion software to implement a complete end-to-end content protection solution.

### SECURITY MODULE

The security module provides all the required technology for implementing a secure content protection solution. It includes functions like secure storage, cryptographic computations and ciphering as defined in the HDCP2.0/2.1 specifications. This module not only generates the keys and input vectors for the AES-128 based cipher engine for encrypting or decrypting the content stream but also provides all the cryptographic functions for authentication, key exchange, locality check and certificate verification. In order to implement a secure solution specific precautions must be taken in order to protect a software only implementation against hacking like software obfuscation or integration into the secure world of a Trustzone based platform.

Besides a very high level of security the EIP-115 hardware-based acceleration offers significant advantages above a software only implementation for timing critical and performance and power optimized cryptographic operations. The module includes a secure interface to Non-Volatile Memory (NVM) for retrieving the device unique keys which must be programmed as part of the manufacturing process.



## Features

The security module (implemented in software or hardware) supports the security functions as defined in the HDCP 2.1 protocol. As an example the list below includes the details for the HDCP2.1 security functions such as:

- *Master key, session key and nonce generation*
  - NIST SP-800-90 compliant random number generation
- *Authentication and Key Exchange*
  - Generation of nonces rtx and rrx
  - Signature verification of certx using kpubdcp 072-bit RSASSA-PKCS#1 v1.5
  - RSAES-OAEP (PKCS#1 v2.1) encrypt/decrypt
  - Derivation of kd using AES Counter mode
  - Computation and verification of H and H'
  - Pairing support (optional)
- *System Renewability*
  - SRM signature verification using kpubdcp 3072-bit RSASSA-PKCS#1 v1.5
- *Session Key Exchange*
  - Generation and computation of ks and riv
  - Derivation of dkey2 using AES Counter mode
- *Locality Check*
  - Computation and verification of L and L'
  - Generation of nonce rn
- *Stream Management*
  - AES Counter mode based HDCP 2.1 key stream generation

### Secure access of confidential material

- Protected access of confidential parameters and key material such as private keys and session keys, as required by the robustness rules.

## Cryptographic functions

### Symmetric crypto algorithms

- AES CTR and CBC mode with a key length of 128 bits

### Asymmetric crypto algorithms

- RSA-CRT - with a modulus length of 512 bits
- RSA - with modulus lengths of 1024 and 3072 bits
- ECC - using the signature algorithms DLSP/DLVP-DSA – EMSA-SHA1 and ECSVDP-DH

### Hash and HMAC algorithms

- SHA-1
- SHA-256
- HMAC-SHA-256

### True Random Number Generator

- Hardware-based, Non-deterministic Random Number Generator
- Full digital implementation so no specific analog design is required
- NIST SP 800-90 compliant

## EIP-115 - Hardware Configurations and gate count

The EIP-115 Hardware based security module is available in two different configurations:

- *EIP-115a Low gate count configuration:*
  - 35k gates TCM in TSMC 40nm at 150MHz
  - AES-128 performance up to 2.4Gbps at 600MHz
- *EIP-115b High performance configuration:*
  - 81k gates in TSMC 40nm at 150MHz
  - AES-128 performance up to 23Gbps at 600MHz

## PERFORMANCE (HDCP2.1)

- *Authentication protocol – Transmitter (@150MHz):*
  - Verify certx <3ms
  - RSAES-OAEP encrypt <2ms
  - Verify SRM Signature <11ms
  - Compute H <0.4ms
  - Compute L <0.4ms
- *Authentication protocol – Receiver (@150MHz):*
  - RSAES-OAEP decrypt <27ms
  - Compute H' <0.4ms
  - Compute L' <0.4ms
- *Pairing:*
  - Encrypt km <0.6ms
  - Decrypt km <0.6ms
- *Key stream generation:*
  - EIP-115a 4 bits/clock
  - EIP-115b 38.4 bits/clock

## INTERFACES

- *Host Interface*

The EIP-115 has a single 32-bit Host slave interface, available with the following bus interface types:

  - TCM interface
  - AHB interface
  - AXI interface
- *NVM Interface*
  - Generic memory interface for easy integration of Non-Volatile Memories.

## TOOLS

- NVM Image Tool for NVM content management

## HARDWARE DOCUMENTATION SET

- Hardware Reference Manual
- Programmer Manual
- Verification Specification
- Integration Manual
- NVM Data Format Application Note
- NVM Image Tool User Guide