HDCP TOOLKIT: SOFTWARE AND HARDWARE IP

inside secure

Reducing the cost and complexity of protecting the use of digital media anytime, anywhere

Key features

- Comprehensive support for the HDCP standard
    - Efficient solutions for both compressed and uncompressed data streams
    - Support for HDCP 2.X
    - Backward compatibility with HDCP 1.3, 1.4
- Configurable for designs using a Trusted Execution Environment (TEE)
- Hardware IP-based content protection for designs without a TEE

Exploding demand for anywhere, any device access to digital media

Digital media is fast becoming the preferred consumer entertainment choice. Whether in the home or on-the-go, the amount of premium High Definition audio/video and the number of devices that can be used to distribute and use it is growing exponentially. Formerly stand-alone devices are now networked and repurposed as consumers are using storage drives and gaming consoles to store and serve content; while phones and tablets are augmenting television screens making multi-screen capabilities a must have feature. To improve the user experience standards such as HDCP have been put in place to ensure the interoperability of these devices and to protect the content being purchased and consumed.

Accelerating the development of interoperable media devices both, wired and wireless

High-bandwidth Digital Content Protection (HDCP) is a method of protecting digital entertainment content such as high-definition movies, pay-per-view television or music on home and personal networks including devices such as PCs, tablets, smartphones and gaming devices. Licensed to device manufacturers by Digital Content Protection LLC (DCP), the initial 1.x versions of HDCP were mainly used over HDMI wired connections with great success, achieving over 3 billion implementations. As content distribution has moved to phones and tablets and key leakage vulnerabilities were found, the HDCP standard has evolved to keep pace, with 2.x versions that protect TCP/ IP based connections across an array of wired and wireless interfaces and provide greater key protection. HDCP combines the need for managing and performing advanced cryptographic functions, incorporating authentication, digital signature algorithms, key storage and management all in accordance with the specified standard. The development of this type of encryption engine and management software requires expertise in cryptography, digital rights management, hardware and software design, a level of security specialization best handled by experts and which can lead to long development cycles for those looking to implement HDCP internally without the required expertise.

- **Inside Secure's solutions offer alternative methods for implementing an HDCP solution:**

○ **Designs using a Trusted Execution Environment** (**TEE**): As part of the HDCP license, an integrator agrees to certain rules, including the use of hardware protection for storing secret keys and for implementing the cryptographic functions. A TEE is considered to provide hardware based protection; Inside Secure provides a software solution, operating within the TEE, which implements all the functions of the HDCP protocol. Hardware acceleration options are also available to enhance the TEE-based solution in cases where higher performance or more CPU offloading are required.

○ **Designs without a TEE:** When a TEE is not part of the system design, Inside Secure delivers a solution with all the HDCP content protection functions implemented in a highly secure hardware IP module.

○ **Designs with Whitebox Cryptography:** When there is already a large install-base or hardware has already been developed Software-only HDCP allows you to add HDCP via a software update. Inside Secure's Whitebox paired with code protection allows you application to protect the HDCP secrets.

Memberships and partnerships

DCP GlobalPlatform SOLACIA TrustZone System Security by ARM VESA TRUSTONIC

All approaches significantly reduce the cost and complexity of security solutions while helping designers get to market quickly with HDCP compliant, robust cryptographic content protection across a range of architectures and use cases.

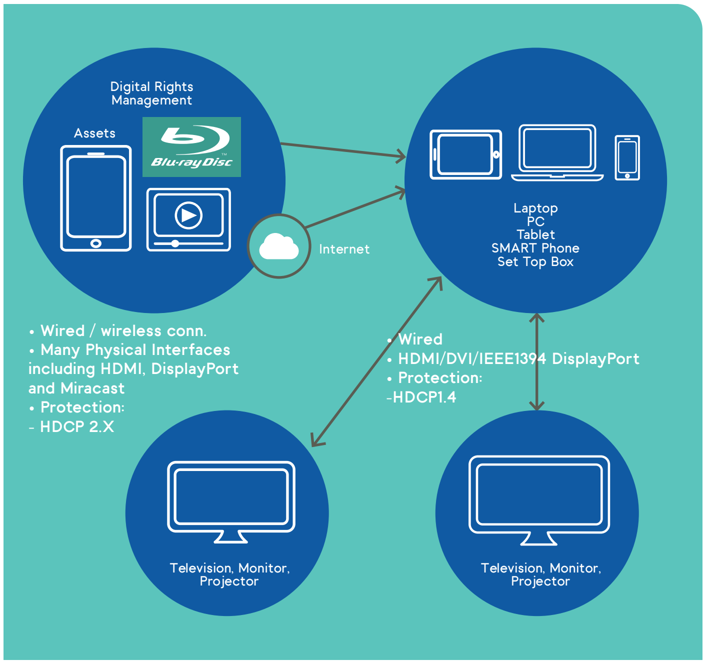
Optimized for mobile to support the growing number and type of mobile devices

Multi-screen viewing and the ability to view premium content on a mobile device has become the expected standard rather than the exception. Given this expectation and the need to protect content, which invariably relies on encryption, device manufactures are faced with a challenge of meeting the requirements of content providers and delivering a positive consumer experience. This challenge arises because power consumption on mobile devices is at a premium and encryption typically is power intensive, as a consequence deploying an optimized solution is key. Inside Secure's HDCP Toolkit are optimized to reduce power consumption and also offers the ability to off-load processing to hardware thus greatly reducing the power used in the HDCP media consumption.

Inside Secure's HDCP Toolkit - Software Solution with TEE

The Inside Secure HDCP Toolkit High-bandwidth Digital Content Protection software solution provides all the required features for a complete content protection solution and includes all control and management software for the HDCP2.3 specification. It is fully backwards compatible with the earlier versions: HDCP2.2, HDCP2.1 and HDPC2.0. The HDCP software, without hardware acceleration, is sufficient in cases where a TEE is available and the content is in a compressed data stream. In this situation, very high performance is not a requirement. For situations where a TEE is available but using an uncompressed video protocol (for example, HDMI or DisplayPort), the HDCP software needs to access the HDCP Datapath Engine, an AES cypher IP core which delivers the required level of high-bandwidth performance. This module implements the HDCP 1.4

and HDCP 2.x data plane in hardware. It is designed for integration with a TEE and must be located within the security boundary of the processor. The HDCP software also includes specific API's for signaling the HDCP protection status to a higher level content control function like DRM, and can be used in combination with Inside Secure's DRM PlayReady and Widevine software solutions to implement a complete end-to-end content protection solution.


Digital Rights Management
Assets
Blu-ray Disc
Internet
Laptop
PC
Tablet
SMART Phone
Set Top Box
• Wired / wireless conn.
• Many Physical Interfaces including HDMI, DisplayPort and Miracast
• Protection:
- HDCP 2.X
• Wired
• HDMI/DVI/IEEE1394 DisplayPort
• Protection:
-HDCP1.4
Television, Monitor, Projector
Television, Monitor, Projector

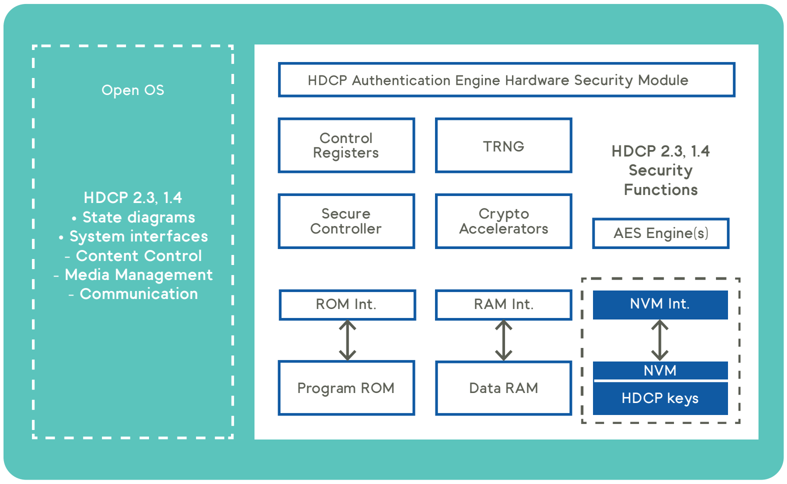
Inside Secure's HDCP Toolkit - Hardware IP Solution

For implementations that do not include a TEE, the HDCP Authentication Engine Hardware Security Module is available. This security module provides all the required technology for implementing a secure HDCP2.2 content protection solution. It includes functions like Secure Key Storage, all cryptographic computations and AES based ciphering as defined in the HDCP2.2 specifications. The HDCP Datapath Engine IP module is offered for systems with at TEE that need to support uncompressed content with HDCP1.4/2.x protection. The HDCP Datapath Engine module includes a data plane only implementation, where the HDCP Authentication Engine implements both the HDCP control plane and the data plane for compressed streaming interfaces like DLNA and Miracast.

Both the HDCP Datapath Engine and the HDCP Authentication Engine modules include an AES-128 based cipher engine for encrypting or decrypting the content stream. The HDCP Authentication Engine also provides all the cryptographic functions for Authentication, Key Exchange, Locality Check and certificate verification. In addition to a very high level of security the HDCP Authentication Engine module offers significant performance improvements and reduced power consumption compared to a software only implementation.

The HDCP Authentication Engine module includes a secure interface to Non-Volatile Memory (NVM) for storing and retrieving the HDCP2.2 secure keys which must be programmed during the manufacturing of the device. The HDCP Authentication Engine hardware security module can be integrated into a wide range of semiconductors, including Application Processors, Multimedia Processors, SOC's for Settop Boxes and Graphics Processors. The HDCP Authentication Engine generates session keys and input vectors which are then used by the AES-128 based cipher core within the module. HDCP Authentication Engine supports a variety of interfaces, including USB, WiFi and Ethernet for streaming compressed video. In addition, for systems without a TEE HDCP Authentication Engine can be used as both the control plane and data plane security module for the protection of streaming un-compressed video over HDMI and DisplayPort.

	HDCP 1.4	HDCP 2.3
Symmetric Crypto Algorithms	HDCP Block Cipher	AES
Asymmetric Crypto Algorithms	RSASSA-PKCS1v5	RSASSA-PKCS1v5
Hash and HMAC Algorithms	SHA1	SHA2-256 / HMAC-SHA256



Interface	Wired/Wireless	HDCP version
HDMI/DVI/HDBASE-T	Wired	HDCP 1.4/2.3
MHL	Wired	HDCP 1.4/2.2
DisplayPort	Wired	HDCP 1.4/2.2
USB	Wired	HDCP 2.2
Ethernet	Wired	HDCP 2.2
Diiva	Wired	HDCP 2.0
Miracast (WiFi Display)	Wireless	HDCP 2.3
Bluetooth	Wireless	HDCP 2.2
WiFi	Wireless	HDCP 2.2
WiDi	Wireless	HDCP 2.3
WiGig	Wireless	HDCP 2.0
WHDI	Wireless	HDCP 2.3
WirelessHD	Wireless	HDCP 2.2

Inside Secure’s HDCP Toolkit – Software-only Solution

When the stream is in compressed format the software-only solution allows you to easily add HDCP to a pre-existing device. A firmware update to your device is sufficient since the complying with robustness rules is done by using a whitebox. The complete software binary and therefore also the whitebox is protected using Inside Secure’s Code Protection which protects itself from external attacks. Available as a binary for a set of architectures you will just have to integrate it in your current SDK.

Backward Compatibility

Inside Secure’s HDCP Toolkit, both software and hardware, support HDCP2.X. They also support the older HCDP 1.4, often used with Display Port or HDMI. However, the ciphers and protocol definitions are totally different between HDCP 1.4 and HDCP 2.x.

HARDWARE IP SPECIFICATIONS

The HDCP Datapath Engine v1.4. & v2.3

- **Description**

The HDCP Datapath Engine provides all the highperformance hardware encryption required for providing HDCP1.4 and HDCP2.3 streaming content protection for high-speed uncompressed interfaces like DisplayPort and HDMI. This module works

seamlessly together with the Inside Secure HDCP protocol software running on a Trusted Execution Environment or in combination with the HDCP Authentication Engine Hardware Security Module

Hardware Configurations and gate count

The HDCP Hardware based Datapath engine is available in one configuration for integration with 1-4 lane Displayport interface

- 94k gates with TCM interface in TSMC 65nm : 28.8 Gb/s at 450MHz max frequency

- 97k gates with TCM interface in TSMC 40nm : 35.2 Gb/s at 550MHz max frequency

- 95k gates with TCM interface in TSMC 28nm : 32.4 Gb/s at 600MHz max frequency

The HDCP Authentication Engine Hardware Security Module

- **Description**

The HDCP Authentication Engine Security Module includes all the secure components like AKE, LC, SRM, SKE, Key Storage, required for implementing the HDCP protocol as specified by DCP, LLC. This module is an ideal solution to be integrated into SoC's that do not include a Trusted Execution Environment

- HDCP Authentication Engine (b) High performance configuration: 81k gates in TSMC 40nm at 150MHz and with an AES-128 performance of-up to 23Gbps at 600MHz

Performance (HDCP2.3)

- **Authentication protocol – Transmitter** (@150MHz) :

- Verify certrx <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:

- HDCP Authentication Engine (b) 38.4 bits/clock

Interfaces

- **The HDCP Authentication Engine 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**
- **Hardware Documentation Set** :

- Hardware Reference Manual
- Programmer Manual
- Verification Specification
- Integration Manual

- **NVM Image Tool for NVM content management** :

- NV M Image Tool User Guide

HDCP Toolkit

Security Functions

Inside Secure's HDCP module (implemented in software or hardware) supports the security functions as defined in the HDCP 2.3 protocol, including :

• **Master key, session key and nonce generation**
- NIST SP-800-90 compliant random number generation

• **Authentication and Key Exchange**
- Generation of random numbers for rtx and rrx
- Signature verification of certrx using kpubdcp
- 3072-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'
- Computation and verification of V and V'
- Pairing support (optional)

• **System Renewability** (SRM)
- 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 2.3 key stream generation

Secure access to confidential material

• **Protected access for 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 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

• **Hash and HMAC algorithms**
- SHA-256
- HMAC-SHA-256

• **True Random Number Generator**
- Hardware-based, Non-deterministic Random Number Generator
- Full digital implementation so no specific analog de sign is required
- NIST SP 800-90 compliant

For further details on all of Inside's security solutions, visit www.insidesecure.com

Information in this document is not intended to be legally binding. Inside Secure products are sold subject to Inside Secure Terms & Conditions of Sale or the provisions of any agreements entered into and executed by Inside Secure and the customer. Inside Secure,® Inside Secure logo and combinations thereof, and others are registered ® trademarks or tradenames of Inside Secure or its subsidiaries. Other terms and product names may be trademarks of others. The products described herein may be protected by one or more of the patents and/or patent applications listed in related datasheets, such document being available on request under specific conditions. Additional patents or patent applications may also apply depending on geographic regions.

inside secure