Cypherbridge® Systems
uHDCP™ Interface Independent HDCP 2.1 SDK

Overview

Portable ANSI C SDK implementing the DCP LLC HDCP 2.1 features and specifications.

HDCP 2.1 builds on the vast installed base of HD receivers, mobile phones and tablets in the market today, adding digital content protection for a variety of media and applications including wired and wireless LAN, WHDI, compressed and uncompressed content, and more. Based on proven cryptographic algorithms including RSA and AES, it combines the pervasive market acceptance of HDCP, together with the proven strength of PKI security standards, a solution for today and into the future.

The uHDCP SDK is designed from the ground up with a flexible structure and API to support current and new applications. It can be used for security plane processing on a range of processors and operating systems.

The HDCP 2.1 standard is backward compatible with HDCP/HDMI 1.x devices. The uHDMI 1.x SDK provides compatibility and converter support to interoperate HDCP 2.1 and 1.x applications.

Security Model

The uHDCP SDK is architected with triple-layer security demarcation. The top-most obfuscation layer protects the control core from user mode probes. Next, the kernel/trust-zone crossing layer can be used to execute security algorithms, authentication and session key updates in elevated security state. Finally, the uHDCP SDK is integrated with an industry leading security acceleration core and software library. The core stores and protects factory provisioned, AKE and SKE key material, and executes TRNG, AES and hash algorithms.

The software library can be deployed today, and set the stage for the integration of IP core on SOC for the ultimate in performance, low gate count and power savings.

DRM

The uHDCP SDK supports interface and HDCP event notification to local DRM client, providing seamless digital content protection from entitlement server to device.

Discovery and Pairing

The uHDCP SDK has in-box support for transmitter/receiver pairing over TCP, and can be adapted to other media such as USB.

Authentication and Key Exchange

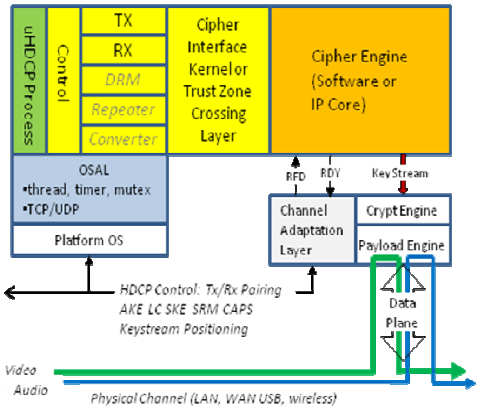
All aspects of the HDCP 2.1 specification are supported including AKE, Locality Check, and Session Key Exchange. The transmitter supports stored Km for fast re-establishment of session keys. SRM is implemented for device revocation.

Key Stream Processing

The cipher key stream is generated on-request and pipelined for low latency output. Key stream blocks are latched by the ciphering core, then used by the content engine to crypt or decrypt the content block. This flexible model can be used with a variety of multiplex containers and packet schemes including MPEG PES packetization defined by the HDCP 2.1 specification.

The uHDCP API includes StreamCtr and InputCtr control for sequential or random key output, and can be used for protected content trick-play for streaming or DVR stored content.

The uHDCP SDK is shown in the following diagram:



Features

- ✓ *Standards based interoperates with HDCP 2.1 devices*
- ✓ *Implements HDCP application process, Transmit and Receive roles and TCP control plane pairing.*
- ✓ *Integrated with HDCP hardware acceleration IP core and software library to securely store NVM and session key material*
- ✓ *Implements obfuscation layer to harden core processing*
- ✓ *Supports kernel driver or trust zone boundary layer crossing*
- ✓ *Portable ANSI-C SDK compact footprint. OS portability layer support for Android, Linux, and Windows.*
- ✓ *Developer and support features include INI configuration, memory management layer and session trace diagnostic log.*
- ✓ *Simple implementation can run as foreground application or detached service*

Options

- ✓ *Optional repeater function*
- ✓ *Optional uHDCP 1.x converter function*

For Pricing and Availability Contact:

Cypherbridge Systems, LLC
7040 Avenida Encinas #104211 Carlsbad, CA 92011
www.cypherbridge.com
sales@cypherbridge.com
Tel: (760) 814-1575

About Cypherbridge Systems:

Established in 2005 to offer software, server, security, device and system level products, our portfolio includes software stacks to enable a broad range of connected device applications integrating embedded device, communications networks, and back office servers in a system solution.