inside secure
DRIVING TRUST

DTCP TOOLKIT: SOFTWARE AND HARDWARE IP

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

¡: FEATURES

- Comprehensive support for the DTCP-IP standard
  - DLNA compliant
  - Supports all four layers of copy protection
- Fully portable architecture
- Broad platform support: ARM, MIPS, x86 (32 and 64 bit), PPC, Tensilica
- Implementation for designs using a Trusted Execution Environment
- 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 Defi nition 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 DLNA and the newly introduced Miracast standard 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

Digital Transmission Content Protection (DTCP) is a method of protecting digital entertainment content such as high-defi nition movies, pay-perview television or music on home and personal networks including devices such as PCs, tablets, smartphones and gaming devices. It has been widely adopted across the globe in consumer electronics products from set top boxes and digital TVs to Blu-Ray and DVD recorders; with a spectrum of cable, satellite, and media services; and over a variety of wireless and wired interfaces.
Now referred to as DTCP-IP (Digital Transmission Content Protection — Internet Protocol), the standard provides a framework for the protection of Internet-based premium content. DTCP-IP support is a mandatory for DLNA devices that support protected streaming and applies to many Digital Rights Management (DRM) and content protection solutions. DTCP-IP combines managing and performing advanced cryptographic functions, incorporating authentication, digital signature algorithms, key storage and management all in accordance with the standard. The development of this type of encryption engine and management software requires expertise in cryptography, digital rights authentication, verifi cation against the DTLA standards, hardware and software design, a level of specialization best handled by experts and which can lead to long development cycles for those looking to implement DTCP-IP internally without the required expertise.

Inside Secure offers alternative methods for implementing a DTCP Toolkit :

- Designs using a Trusted Execution Environment (TEE): Inside Secure provides a software solution, easily integrated with a TEE, which implements all the functions of the HDCP protocol.
- Designs without a TEE: the HDCP Toolkit can be implemented simply with OS interfaces or, optionally, Inside Secure delivers a solution with all the HDCP content protection functions implemented in a secure hardware IP module.

Both approaches significantly reduce the cost and complexity of bringing to market server and client DLNA-certifi ed media devices.

Memberships and partnerships

Server and player support for protected streaming and move/copy

DTCP Toolkit can be used for streaming media and deployed for both transmission (server-side) and receiving (client-side). When deployed server-side it encrypts premium content files saved on a content serving device using DTCP-IP and streams the encrypted files to a client player device. DTCP-IP prevents contents from being leaked illegally by performing interactive device authentication between server and player devices before initiating the encrypted communications. To copy or move content data requiring copyright protection between devices, DTCP-IP move/copy must be supported by both content data's transmitter and receiver. A device that is capable of recording digital broadcasting programs encrypts and transmits the recorded data, and a receiver displays it. If a receiver device has a server feature, it can also stream and distribute moved/copied content. DTCP-IP also supports the ability to enforce copy rules regarding whether copies may be made and the number of copies allowed under license.

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. DTCP Toolkit is optimized to reduce power consumption and also offers the ability to off-load processing to hardware thus greatly reducing the power used in the DTCPIP media consumption.

Technology Overview

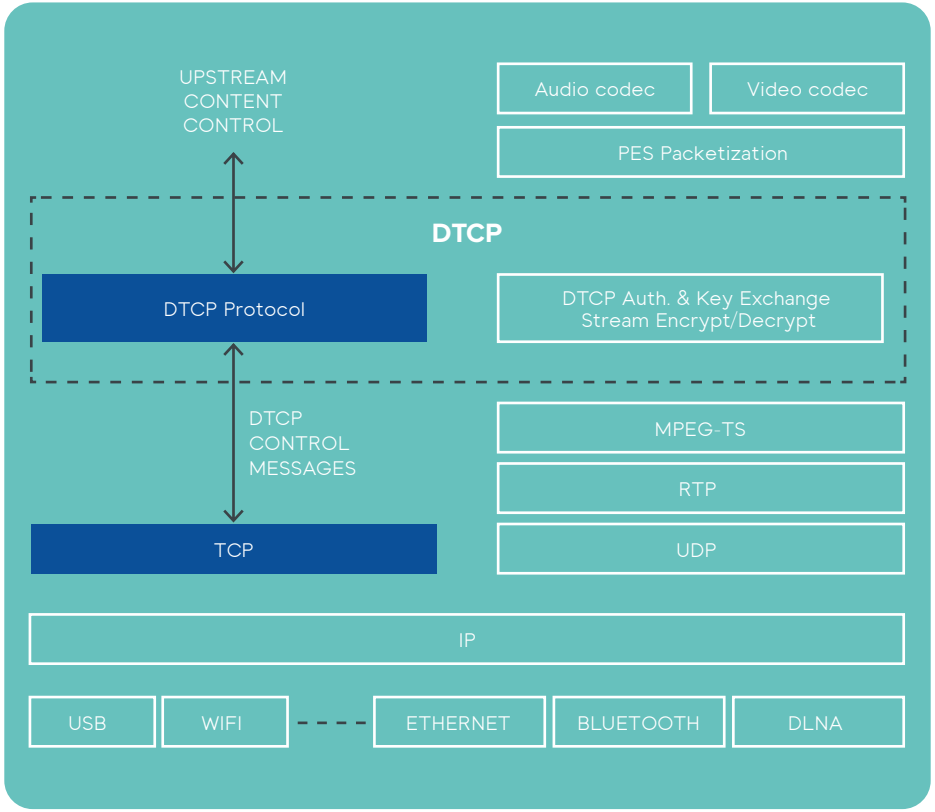
In a system where high value, premium content is available and which requires copy protection, the digital content and the technology that provides the secure communication between two devices must be protected. The secure part of the content protection system can be implemented in hardware-protected software by using a Trusted Execution Environment (TEE). Inside Secure provides complete software solutions for implementing DTCP-IP to ensure the protection of the device secret keys, the encryption of high-value content, key exchange mechanisms, mutual authentication and repudiation of devices that have been compromised. Our DTCP Toolkit supports all four layers of copy protection: copy control information, device authentication and key exchange, content encryption, and system renewability. In addition, a highly secure and optimized hardware module (DTCP Authentication Engine) is available to provide maximum security, easy system integration, optimal performance and lowest power dissipation in applications where no TEE is required or available. The DTCP Authentication Engine forms the hardware-based security boundary wherein all secure parameters and cryptographic computations are managed during all the DTCP-IP protocol phases from authentication of the connected devices up to and including the generation of the key stream.

dlna

The Digital Living Network Alliance (DLNA) is responsible for defining interoperability guidelines to enable sharing of digital media such as music, photos and videos between consumer devices such as computers, TVs, printers, cameras, cell phones, and other multimedia devices. Over 17,000 different devices have obtained "DLNA Certified" status, indicated by a logo on their packaging and confirming their interoperability with other devices.
More than 440 million DLNA-certified devices, from digital cameras to game consoles and TVs, have been installed in users' homes.

DTCP Toolkit

Inside Secure's DTCP Toolkit provides all the required features for a complete content protection solution comprised of all content control and management capabilities for the DTCP-IP standard. Besides the cryptographic functions and secure computations module the software includes the implementation of the state diagrams as defined by the DTCP-IP standard and supports the TCP/IP based communications between a transmitter, receiver and repeater (bridge).



SOFTWARE FEATURES AND FUNCTION

- Fully Tested and Verified
- DTLA Compliant
- Copy control information
- Full device authentication and key exchange
- Content encryption
- System renewability
- Small footprint
- Compliant with the latest standards (DTCP-E Rev 1.7 ED2 and DTCP Rev 1.4 ED3.)
- Option for security offload
  - TEE support
  - DTCP Authentication Engine Security Module
- GPL-free code
- Fully portable architecture
- Platforms – ARM, MIPS, x86 (32 and 64 bit), PPC, Tensilica
- OS Support – Linux, Android, Windows
- Interface Support:
  - Firewire
  - WiFi
  - MOST
  - WirelessHD
  - USB
  - Ethernet
  - Bluetooth

THE DTCP AUTHENTICATION ENGINE HARDWARE SECURITY MODULE

Hardware Configurations and gate count

• **DTCP Authentication Engine (b) High performance configuration**
- 81k gates in TSMC 40nm at 150MHz
- AES-128 performance up to 23Gbps at 600MHz

Interfaces

• **The DTCP 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**
- NVM Data Format Application Note
- NVM Image Tool User Guide

High Performance Security Module

The DTCP Authentication Engine Hardware Security Module can be used seamlessly with Inside Secure's DTCP Toolkit by replacing the content protection requirement in the protocol. The DTCP Authentication Engine module includes API's for DRM that can be used with Content Protection Client to implement an endend content protection solution. It provides all the required technology for implementing secure content protection including: secure key storage, cryptographic computations and ciphering as defined by DTCP V1.7 specifications. This module not only generates the session keys and input vectors for the AES-128 based cipher engine used to encrypt and decrypt the content stream but also provides all the cryptographic functions for authentication, key exchange, locality check and certificate verification.

In addition to providing the highest level of security the DTCP Authentication Engine provides hardware-based acceleration that exceeds the capabilities of software to perform power optimized cryptographic operations. The module also includes a secure interface to Non-Volatile Memory for retrieving the device unique keys that must be programmed as part of the manufacturing process.

The DTCP Authentication Engine is designed to be used in source and sink devices or in combination with both (bridge/repeater devices). It can be integrated into Application Processors, Multimedia Processors, SOCs for Set-top boxes and Graphics Processors. The DTCP Authentication Engine generates session keys and input vectors which are used by the AES-128 based cipher module and it supports the use of multiple commonly used interfaces such as USB, Ethernet, WiFi and Bluetooth as well as Media Oriented Systems Transport (MOST) and WirelessHD.

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

inside secure
DRIVING TRUST