I/O伴侣的DTCP协议栈

Microchip I/O伴侣的完整数字传输内容保护（DTCP）实现方案

摘要

Microchip的I/O伴侣系列采用协处理器芯片，通过利用硬件加密加速和流密码处理可实现高效DTCP。

I/O伴侣的DTCP协议栈提供实现完整DTCP解决方案所需的所有较高软件层。DTCP协议栈完全可扩展，同时支持多种身份验证和密钥交换（AKE）进程。它具有高级密钥管理，允许同时验证多台设备。此外，还可以对它进行调节，以满足特定于供货商的要求。每个软件层均具有完整的记录和调试功能，可轻松实现系统分析和互操作性调试。该DTCP协议栈附带所有相关的规范和标准，可确保与其他DTCP设备兼容，从而最大程度节省成本，加快上市。

特性

- 协议栈各层完全实现了所有必需的规范，包括：
  - MOST® Cooperation的MOST内容保护机制—— DTCP实现方案
  - MOST Cooperation的通用FBlock的DTCP函数
  - DTLA/5C的DTCP卷1，补充协议B和补充协议H
  - Microchip的I/O伴侣DTCP协处理器
- 完整的AKE过程
- 完整的内容密钥交换（CKE）过程
- M6和AES-128流加密
- 支持同步和A/V分组等时流传输类
- 支持所有加密模式：copy-never（禁止复制）、copy-one-generation（复制一代）和no-more-copies（不再复制）
- 为不受保护的内容提供copy-free（自由复制）模式
- 标准化DTCP环境，以避免互操作性问题
- 显著降低成本，加快上市

图1：*I/O伴侣的DTCP协议栈*

- 针对与Microchip的MOST NetService配合使用而设计
- 针对与Microchip的IOC配置工具配合使用专门设计
- 标准C语言库
- 在主循环驱动的外部主机控制器（EHC）架构中工作；无需多线程操作系统
- 完整的应用程序编程接口（API），适用于AKE/CKE和加密通道设置和控制
- 快速而易用的系统设置
- 完全可扩展的架构：
  - 可调节并行的AKE进程数
  - 可调节经验证设备的密钥管理
  - 最多8个加密通道
  - 优化的RAM和CPU资源利用
- 支持Microchip的I/O伴侣系列

MICROCHIP

说明

实现DTCP应用是一项富有挑战而复杂的任务。Microchip的I/O伴侣系列包含协处理器，工程师可借此开发DTCP解决方案而无需对加密数学充分了解。有了它，外部主机控制器可不必执行耗费大量资源的算法。

但是，实现软件的上层也是一项复杂的工作。需要考虑几种不同标准组合的规范。不仅涵盖DTLA/5C规范及其补充协议B和H（针对内核算法、密钥管理、系统更新和超时），而且还涵盖补充标准化MOST API所需的MOST Cooperation FBlock定义。

I/O伴侣的DTCP协议栈是用可移植的纯C语言代码编写的完整而易用的分层解决方案。针对在采用主循环驱动架构的标准单片机上使用而设计，无需多线程操作系统或外部存储器管理单元。虽然I/O伴侣的DTCP协议栈代码短小，且经过优化，占用资源较少，然而其仍然能够充分扩展，可同时支持多个AKE进程，并具有高级密钥管理，允许同时验证多台设备。它附带了所有相关的规范和标准，可确保与其他DTCP设备兼容，将上市时间缩至最短。

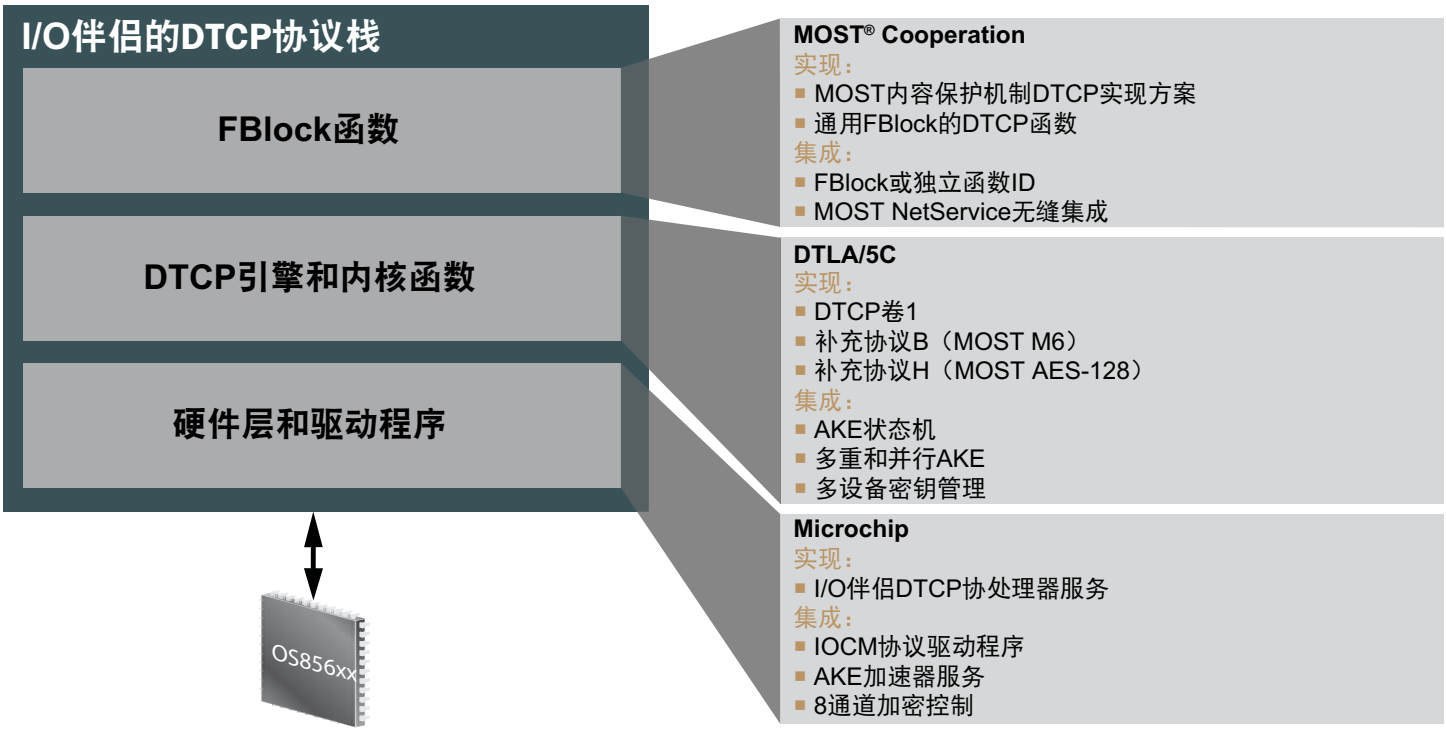

图2： *I/O伴侣的DTCP协议栈及其实现的功能*

www.microchip.com/DTCP-Stack

更多产品信息和各地销售办事处地址，请访问我公司网站。

Microchip Technology Inc. · 2355 W. Chandler Blvd. · Chandler, AZ 85224-6199

Microcontrollers • Digital Signal Controllers • Analog • Memory • Wireless

信息可能变更，恕不另行通知。Microchip的名称和徽标组合、Microchip徽标以及MOST均为Microchip Technology Incorporated在美国和其他国家或地区的注册商标。在此提及的所有其他商标均为各持有公司所有。© 2014，Microchip Technology Incorporated。版权所有。7/14
DS00001740A_CN