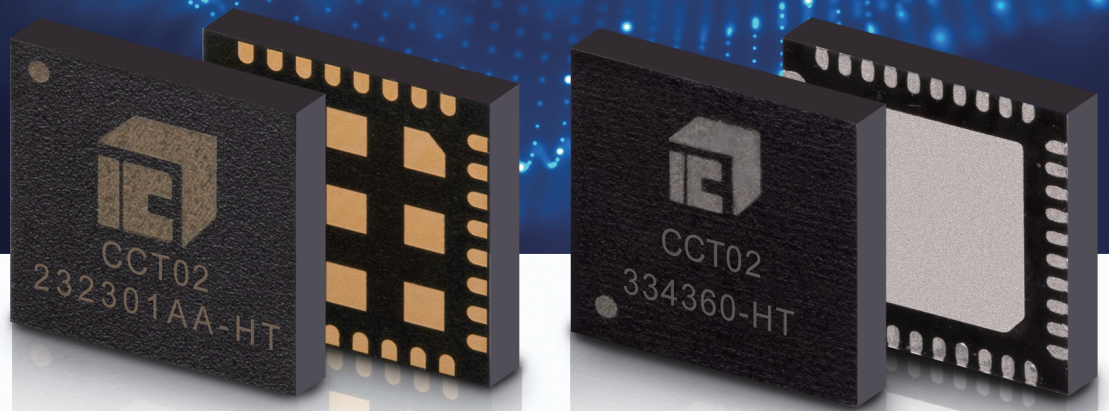
可信华泰



可信TCM密码模块

产品介绍
Product Introduction

可信 TCM 密码模块符合 GM/T 0012-2020《可信计算可信密码模块接口规范》、GM/T 0028-2014《密码模块安全技术要求》和 GM/T0008-2012《安全芯片密码检测准则》的检测规范。可信 TCM 密码模块可作为防护部件核心组件，为可信平台控制模块（TPCM）提供可信密码服务；也可作为独立模块，支撑可信计算密码支撑平台实现安全功能。产品具有低功耗、高性能、多功能及高安全性等特点。产品内置高等级安全特性的硬件算法协处理器，支持国家商用密码算法及国际标准算法。支持工业级温度范围（-40℃～ 85℃），可用于苛刻的工业环境。

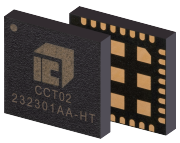
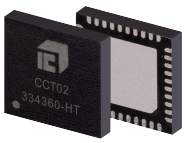
产品功能 Product Function

- 密码服务：支持国密算法；支持数字信封、数据封装、数据加解密三种加密方式；支持签名功能；支持密钥安全的生成、存储、使用、更新和销毁。
- 数据保护：可以抵御物理攻击和逻辑攻击，为敏感数据的存储和操作提供保护。
- 完整性校验：在TCM服务模块(TSM)调用下，实现对计算机的硬件、固件、操作系统和软件进行完整性校验。
- 身份认证：通过存储的唯一标识、密码、指纹等生物特征信息或数字证书，可实现多因子认证，完成用户身份认证、平台身份认证。

客户价值 Customer Value

- 数据安全：对敏感数据做数据保护和完整性校验，确保数据存储和传输的安全，通过身份认证和授权管理，可防止数据被未经授权的访问。
- 系统安全增强：通过完整性校验功能，阻挡恶意代码威胁。
- 标准规范：结合可信计算3.0技术，可以满足等保2.0、关键基础设施条例中对可信相关功能的要求。

产品规格 Product Specification

产品型号	CCT02-LGA32	CCT02-QFN40
CPU	C*CORE C0	
主频	100MHz	
尺寸	5*5MM	
工作温度	-40°C～85°C	
工作电压	1.8V~3.3V	
典型功耗	25mA@100MHz	
低功耗	2uA	
ESD	2KV	
接口	SPI	
存储保护机制	存储加密，总线加扰	
物理防攻击	支持	
安全检测与防护单元	TD/VD/FD/AD等	
随机数	GM/T 0005-2012真随机数标准	
	FIPS 140-S标准	
算法性能	SM2签名：6.6ms/次	
	SM3：46.5MB/S	
	SM4加密（ECB）：24.3MB/S	
密码资质	国家商用密码可信模块产品认证证书	
封装		

应用场景 Application Scenario

- VPN/安全网关等安全设备
- 可信服务器/PC
- 工程师站/操作员站等工控机
- PLC等嵌入式工控设备

立即了解更多内容：
公司网站：www.httc.com.cn
联系方式：010-88894990

印刷日期：2024.10

可信华泰