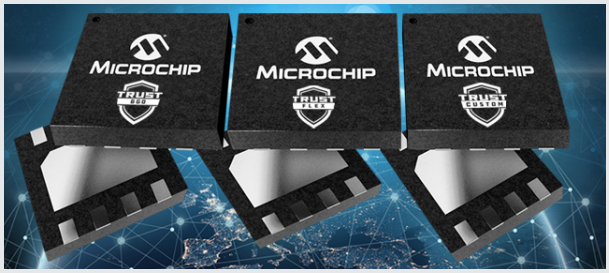
Microchip的可信平台

利用Microchip的安全制造基础架构在产品中安全置备凭证

摘要

对于少至十个部件，多至成千上万个设备的部署，可信平台都是一种经济高效的灵活解决方案，它不仅将Microchip的安全元件集成到您的设计中，还可缩短产品的上市时间。可信平台由一系列预置备、预配置或完全可自定义的安全元件组成。利用我们在工厂中安装的Microchip硬件安全模块（Hardware Secure Module，HSM），可在每个安全元件的边界内生成凭证。这些器件还配有硬件和软件开发工具，能够简化原型开发并快速跟踪您的开发进度。可信平台提供三层安全元件Trust&GO、TrustFLEX和TrustCUSTOM，为您满足公司的安全模型要求提供了多种选项，同时带来灵活性。



TRUST&GO

- 预配置和预置备器件
- 包括用于指纹验证的密钥和通用证书
- 最小起订量为10个，包括置备
- 提供完整的协议栈代码示例

TRUST FLEX

- 预配置和预置备器件
- 升级默认凭证以使用您自己的证书链
- 最小起订量为2,000个，包括置备
- 提供最常见的用例

TRUST CUSTOM

- 空白器件
- 完全可定制的器件
- 最小起订量为4,000个，包括置备
- 签署保密协议（NDA）后提供完整的数据手册和配置工具

主要亮点

- 通过预定义配置和预配轻松实现嵌入式安全
- 适用于TLS网络的Trust&GO
  - 利用“多帐户注册”的AWS IoT和Greengrass
  - 利用“令牌验证”的Google Cloud Platform
  - 第三方TLS身份验证
- 适用于LoRaWAN™网络的Trust&GO
  - The Things Industry（TTI）连接服务器
  - Actility连接服务器
- 通过Trust&GO的预定义配置和置备，轻松实现嵌入式安全
  - 任意云、任意PKI和任意证书颁发机构
  - 基于证书/令牌的身份验证
  - 固件验证/OTA验证/安全启动验证
  - 固件IP保护
  - 消息加密
  - I/O保护密钥
  - 配件身份验证
  - 密钥轮换
- 适合最小起订量（包括置备和Microchip证书）较低的大众市场
- 架构可适用于任何控制器和任何连接方式
- 利用可信平台设计套件（用例选择器、基于Python的笔记本、C代码以及用于密钥交换的配置程序）可实现快速开发

开发工具

- **可信平台设计套件**——软件工具，可帮助选择所需的预定义用例，利用python可执行教程测试安全元件设置，使用C代码示例加速嵌入式原型设计，以及在交换秘密信息期间保持自主
- **可信平台USB工具包（DM320118）**—具有USB端口的基础开发工具包，集成了ATECC608A Trust&GO、TrustFLEX和TrustCUSTOM
- **ATECC608A可信工具包（DT100104）**—DM320118的附加开发板，可充分利用焊接在PCB上的其他ATECC608A可信平台器件。
- 来自mikroe.com：**Secure click（uDFN: MIKROE-3746/SOIC: MIKROE-3788）**—DM320118的插座式扩展板，可借助ATECC608A可信平台扩展您的测试能力。

Trust&GO	说明
ATECC608A-TNGTLSS-B	Trust&GO TLS、置备原型设计、8-SOIC和I²C（10个起订）
ATECC608A-TNGTLSU-B	Trust&GO TLS、置备原型设计、8-UDFN和I²C（10个起订）
ATECC608A-TNGTLSS-C	Trust&GO TLS、置备、8-SOIC和I²C（100的倍数起订）
ATECC608A-TNGTLSU-C	Trust&GO TLS、置备、8-UDFN和I²C（100的倍数起订）
ATECC608A-TNGTLSS-G	Trust&GO TLS、置备、8-SOIC和I²C（2000的倍数起订）
ATECC608A-TNGTLSU-G	Trust&GO TLS、置备、8-UDFN和I²C（2000的倍数起订）
TrustFLEX	**说明**
ATECC608A-TFLXTLSS-Proto	TrustFLEX TLS、置备原型设计和8-SOIC（10个起订）
ATECC608A-TFLXTLSU-Proto	TrustFLEX TLS、置备原型设计、8-UDFN和I²C（10个起订）
ATECC608A-TFLXTLSS	TrustFLEX TLS、置备和8-SOIC，2000个起订
ATECC608A-TFLXTLSU	TrustFLEX TLS、置备和8-UDFN，2000个起订
TrustCUSTOM	**说明**
ATECC608A-TCSMS	TrustCUSTOM、置备和8-SOIC，4000个起订
ATECC608A-TCSMU	TrustCUSTOM、置备和8-UDFN，4000个起订
适用于The Things Industries的Trust&GO	**说明**
ATECC608A-TNGLORAS-B	Trust&GO LORAWAN™、置备原型设计、8-SOIC和I²C（10个起订）
ATECC608A-TNGLORAU-B	Trust&GO LORAWAN、置备原型设计、8-UDFN和I²C（10个起订）
ATECC608A-TNGLORAS-C	Trust&GO LORAWAN、置备、8-SOIC和I²C（100的倍数起订）
ATECC608A-TNGLORAU-C	Trust&GO LORAWAN、置备、8-UDFN和I²C（100的倍数起订）
ATECC608A-TNGLORAS-G	Trust&GO LORAWAN、置备、8-SOIC和I²C（2000的倍数起订）
ATECC608A-TNGLORAU-G	Trust&GO LORAWAN、置备、8-UDFN和I²C（2000的倍数起订）
适用于The Things Industries的TrustFLEX	**说明**
ATECC608A-TFLXLORAS-Proto	TrustFLEX LORAWAN、置备原型设计和8-SOIC（10个起订）
ATECC608A-TFLXLORAU-Proto	TrustFLEX LORAWAN、置备原型设计、8-UDFN和I²C（10个起订）
ATECC608A-TFLXLORAS	TrustFLEX LORAWAN、置备和8-SOIC，2000个起订
ATECC608A-TFLXLORAU	TrustFLEX LORAWAN、置备和8-UDFN，2000个起订
适用于Actility的Trust&GO	**说明**
ATECC608A-TNGACTS-B	Trust&GO Actility LORAWAN、置备原型设计、8-SOIC和I²C（10个起订）
ATECC608A-TNGACTU-B	Trust&GO Actility LORAWAN、置备原型设计、8-UDFN和I²C（10个起订）
ATECC608A-TNGACTS-C	Trust&GO Actility LORAWAN、置备、8-SOIC和I²C（100的倍数起订）
ATECC608A-TNGACTU-C	Trust&GO Actility LORAWAN、置备、8-UDFN和I²C（100的倍数起订）
ATECC608A-TNGACTS-G	Trust&GO Actility LORAWAN、置备、8-SOIC和I²C（2000的倍数起订）
ATECC608A-TNGACTU-G	Trust&GO Actility LORAWAN、置备、8-UDFN和I²C（2000的倍数起订）
适用于Actility的TrustFLEX	**说明**
ATECC608A-TFLXACTS-Proto	TrustFLEX Actility LoraWan、置备原型设计和8-SOIC（10个起订）
ATECC608A-TFLXACTU-Proto	TrustFLEX Actility LORAWAN、置备原型设计、8-UDFN和I²C（10个起订）
ATECC608A-TFLXACTS	TrustFLEX Actility LORAWAN、置备和8-SOIC，2000个起订
ATECC608A-TFLXACTU	TrustFLEX Actility LORAWAN、置备和8-UDFN，2000个起订

DS00003278B_CN