

具有基于硬件的密钥存储的CryptoAuthentication™加密元件

评估、开发和生产工具包选择指南

用于每个阶段的工具包

Microchip提供多种工具包和软件，可帮助评估人员和开发人员完成从评估到生产的整个设计过程。所有加密工具包都通过运行CryptoAuthentication评估系统软件来配置CryptoAuthentication器件。人性化的软硬件组合可为用户提供评估、开发与生产过程中所需的工具。

从评估工具包入手

AT88CK590评估工具包中包含三个器件：ATSHA204A、ATECC508A和ATAES132A。此工具包可通过运行CryptoAuthentication软件来配置和评估工具包中所含的三个加密器件的操作。在了解器件的操作与性能后，就可轻松使用流程中的下一个工具。

下一步——CryptoAuthentication SOIC入门工具包 (DM320109) 或Xplained Pro开发工具包

CryptoAuthentication入门工具包中包含SAM D21-XPRO开发板、SOIC插座板和多个CryptoAuthentication器件样片。此外，此开发板还可与UDFN插座板、CryptoAuth-XPRO或CryptoAuth-XPRO-B板配合使用。在初次评估之后，可使用附加扩展板配合SAM D21单片机板或其他与XPRO兼容的单片机板进行开发。

针对PIC®单片机，可从MikroElektronika获取适用于ATSHA204A、ATECC508A、ATECC608A和ATAES132A安全器件的Secure click板。

软件支持和工具

为支持硬件开发工具包，Microchip提供了软件工具，帮助对CryptoAuthentication器件进行评估和开发。这些工具包括用于探索器件特性与功能的评估软件、命令库、应用示例和配置支持工具等。

互连的IoT世界

在这个日益互联化的世界中，始终都应确保连接到IoT云的安全性。Microchip正与多个供应商展开合作，帮助用户方便、轻松地连接到云。AT88CKECC-AWS-XSTK-B工具包使客户能够快速轻松地连接到Amazon IoT服务。ATAFERO-MOD2-XPRO是与Afero联合开发的产品，能够通过Wi-Fi®和/或Bluetooth®连接到云或边缘节点，提供近似无缝的IoT体验。Afero提供完整的系统解决方案体验，具备云和软件开发工具，可为快速进行IoT解决方案的原型设计与开发提供支持。Google Cloud IoT Core 身份验证工具包可确保身份验证和Google Cloud硬件的安全性。

资源预置工具包

想要建立自己的信任链？Microchip提供Root（AT88CKECCROOT）与Signer（AT88CKECCSIGNER）模块和关联固件，可安全地生成生产器件签名所需的信任根和Signer模块。这两个工具包每个都配有3个USB加密狗，用于生成主要与备用器件。为方便起见，这两个工具包已在AT88CKECCPROVISION工具包中合二为一。

生产解决方案

安全性取决于最薄弱环节。Microchip提供安全的生产方法，不会泄漏只有您知悉的专有信息。通过使用片上传输密钥、加密机密信息交换和使用高度安全的HSM，Microchip或其他安全合作伙伴可提供满足您需求的生产解决方案。

CryptoAuthentication™评估和开发工具包		
工具包类型	订购代码	支持的器件
AT88CK590评估工具包	AT88CK590	ATECC508A、ATSHA204A和ATAES132A
CryptoAuthentication SOIC入门工具包	DM320109	ATECC608A、ATECC508A、ATSHA204A和ATAES132A
CryptoAuth Xplained Pro扩展工具包	ATCRYPTOAUTH-XPRO	ATECC508A、ATSHA204A和ATAES132A
CryptoAuth XPRO-B扩展工具包	ATCRYPTOAUTH-XPRO-B	ATECC608A、ATECC508A、ATSHA204A和ATAES132A
CryptoAuthentication SOIC插座工具包	AT88CKSCKTSOIC-XPRO	ATECC608A、ATECC508A、ATECC108A、ATSHA204A和ATAES132A
CryptoAuthentication UDFN插座工具包	AT88CKSCKTUDFN-XPRO	ATECC608A、ATECC508A、ATECC108A、ATSHA204A和ATAES132A
用于ATECC508A的Secure click ⁽¹⁾	MIKROE-2522	ATECC508A I ² C模式
用于ATAES132A的Secure 2 click ⁽¹⁾	MIKROE-2760	ATAES132A I ² C模式
用于ATSHA204A的Secure 3 click ⁽¹⁾	MIKROE-2761	ATSHA204A I ² C模式
用于ATECC608A的Secure 4 click ⁽¹⁾	MIKROE-2829	ATECC608A I ² C模式
资源预置支持工具包		
工具包类型	订购代码	备注
信任根模块	AT88CKECCROOT	用于支持安全生成信任根
Signer模块	AT88CKECCSIGNER	用于支持安全生成由信任根签名的Signer
具有Root和Signer的资源预置工具包	AT88CKECCPROVISION	包含Root和Signer模块
IoT支持工具包		
工具包类型	订购代码	支持的器件
支持Wi-Fi®的Amazon IoT工具包	AT88CKECC-AWS-XSTK-B	ATECC508A、ATECC608A、ATSAMG55和ATWINC1500
支持Wi-Fi和蓝牙的Afero IoT	ATAFERO-MOD2-XPRO	ATECC508A、ATSAMG55和ATWINC3400
用于Cortex®-M0+、Cortex-M4和Raspberry Pi®的Google Cloud IoT身份验证	microchip.com/ATECC608aGCPiotCore	ATECC608A、ATSAMD21、ATSAMG55和ATWINC1500

⁽¹⁾ Secure click板可从MikroElektronika获取。有关更多信息，请访问www.Mikroe.com/click。

软件工具	说明
CryptoAuthLib	支持SHA和ECC器件的功能扩展库。此库随时可以通过硬件抽象层适应新的单片机
CryptoAuthentication™示例	使用SAM D21-XPRO评估板和CryptoAuthLib了解安全身份验证的基础知识
CryptoAuthLib-Python	当前正在开发中的一个工具系列，可以通过使用Python模拟主机应用程序加快开发速度。有关更多信息，请联系Microchip。
ACES	Microchip的Crypto Evaluation Studio。基于GUI的工具，可用于探索CryptoAuthentication器件。ACES可与CryptoAuthentication入门工具包和AT88CK101工具包配合使用。

技术支持类型	说明
技术咨询	访问Microchip的知识库，并联系技术支持人员 www.microchip.com/support
设计合作伙伴	需要安全方面的设计帮助？请查看我们的设计合作伙伴、安全顾问和云服务提供商列表。 www.microchip.com/design-centers/security-ics/design-partners/partner-list

Microchip的名称和徽标组合、Microchip徽标及PIC均为Microchip Technology Incorporated在美国和其他国家或地区的注册商标。CryptoAuthentication为Microchip Technology Incorporated在美国和其他国家或地区的商标。Cortex是Arm Limited（或其子公司）在美国和/或其他国家/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。
© 2019, Microchip Technology Incorporated版权所有。 7/19

DS00002219B_CN