Application Note

SimpleLink™ Wi-Fi® CC3x20、CC3x3x 内置安全功能

摘要

CC3120/CC3130/CC3135 和 CC3220/CC3230/CC3235x 器件均是 SimpleLink™ 微控制器 (MCU) 平台的一部分，而该平台由 Wi-Fi®、低功耗 ***Bluetooth***®、Sub-1GHz 和主机 MCU 构成。它们均共用一个简单易用的通用开发环境，其中包含单核软件开发套件 (SDK) 和丰富的工具集。只需进行一次 SimpleLink 平台集成，便可将配置文件中的任意器件组合添加到设计中。 SimpleLink 平台的最终目标是确保设计要求变更时，完全重复使用代码。如需了解更多相关信息，请访问 www.ti.com.cn/simplelink/cn。

SimpleLink MCU 产品系列提供的单一开发环境包含灵活的硬件、软件和工具选项，便于客户开发有线和无线应用。为了最终能够在主机 MCU、Wi-Fi、Bluetooth 低功耗、Sub-1 GHz 器件等平台中完全重复使用代码，可根据客户的设计选择 MCU 或连接标准。只需一次性投资 SimpleLink 软件开发套件 (SDK) 便可重复使用，从而开启创建无限应用的大门。如需了解更多相关信息，请访问 www.ti.com.cn/simplelink/cn。

内容

1 引言 3
- 1.1 术语 3
- 1.2 物联网 (IoT) 产品和安全性 3
- 1.3 主要特性 6

2 网络层安全 9
- 2.1 Wi-Fi 安全 9
- 2.2 安全套接字层 10

3 文件系统安全 17
- 3.1 概述 17
- 3.2 文件系统安全功能描述 18
- 3.3 文件创建属性 22

4 对器件进行编程 22
- 4.1 开发阶段 23
- 4.2 生产阶段 23

5 现场软件更新 24
- 5.1 文件捆绑包保护 24
- 5.2 安全内容交付 24

6 应用层安全性 27
- 6.1 安全密钥存储 27
- 6.2 硬件加密引擎 (仅限 CC3220/CC3230/CC3235x 器件) 27

7 运行时二进制保护 29
- 7.1 CC3220S/CC3230S/CC3235S 器件 29
- 7.2 CC3220SF/CC3230SF/CC3235SF 器件 29

8 安全性设计 31
- 8.1 结束语 31

修订历史记录 32

商标

1 引言

物联网 (IoT) 产品和系统可能包含较为敏感和私密的信息，因此强调了保护数据安全的重要性。此类数据可能包括密码、密钥、凭证、配置、个人信息、供应商知识产权 (IP) 等。即使数据看起来不敏感或者非机密，也可能泄露会威胁到敏感数据的信息。

德州仪器 (TI)™ 的 SimpleLink Wi-FiInternet-on-a chip™ 器件系列提供广泛的内置安全功能，以便帮助开发人员满足各种安全需求，同时不增加主 MCU 的处理负担。本文档介绍了这些安全相关的功能，并就每种功能在实际系统实施中的应用提供相关建议。

CC3x20 和 CC3x3x 器件的设计可确保网络安全软件在器件上的专用子系统内运行。该子系统是一种配备硬件加密引擎的片上网络处理器，可形成一种独立的执行环境，减轻系统主 MCU 的负担。这些安全功能覆盖整个产品生命周期中的各种典型活动，包括联网活动、数据存储、IP 保护、防克隆保护和生产期间的安全配置。这些安全功能通过一个包含简洁 API、工具和文档的生态系统向供应商提供。

1.1 术语

表 1-1 简要介绍了理解安全方法和功能所需的关键术语。

表 1-1. 术语

术语	说明
资产	资产是指对其所有者有价值的任何信息（安全相关元素）。因此，必须通过目标系统的各种措施进行保护（机密性、完整性、真实性相关）。资产可以是专有信息、个人数据或知识产权。
非对称密钥	非对称密钥对在算法中使用，其中一方使用密钥执行加密操作，另一方则使用另一密钥执行相反操作。密钥对可定义为公共和私有密钥，最常用于数字签名和对称密钥分配。
攻击向量	用于破坏系统安全防护措施，从而获得单个或多个资产控制权的一组动作。
真实性	确保资产或实体是真实的，且已获得执行某一任务的授权，或者可按预期使用。验证过程通常涉及加密算法，该算法用于检查实体的真实身份与宣称的身份是否相符。某些预定义的信任机制始终属于验证机制的一部分。
证书	证书是标准格式文件。其中通常包含使用者公共密钥，以及头文件和公共密钥的 CA 签名。可提供 CA 公共密钥（若是证书链，则为子 CA）的任何人都能够验证使用者的身份。
证书颁发机构 (CA)	受信任的实体，颁发用于验证身份的证书。
证书链， 信任链	证书链包含形成层级结构的多个证书，支持任何人验证一直到根证书的任何证书颁发者的身份。
密码套件	密码套件是一种已命名的算法组合，用于身份验证、密钥交换、数据加密和消息验证代码。这组算法用于 SSL 握手和会话。
机密性	机密性可确保资产不会供未获授权的实体使用，也不会向此类实体披露。在大多数情况下，机密性表现为进行加密，而在其他情况下，则使用混淆技术来保持机密性
暴露点	识别出的进入系统的入口点，可启动一次或多次安全攻击（攻击向量）。
完整性	用于描述对象与原始版本相比在整体上保持不变的属性。
密钥	密钥用于数据加密、密钥建立和数字签名。密钥长度和类型取决于所使用的算法、具体用途和安全级别。
PKI	公钥基础设施。
吊销的证书	颁发者不再授权使用和不再认为有效的证书。
根 CA	证书颁发机构对照最终验证的证书链提供的最高级别的证书。它始终自签名且公开可用。
安全措施	旨在为某些资产提供预期保护以抵御某些威胁的措施。
对称密钥	在算法中使用的密钥，其中双方使用相同密钥执行加密操作。

1.2 物联网 (IoT) 产品和安全性

物联网设备本质上是一种联网设备，因此可充当网关，对监控视频等敏感数据进行恶意访问或控制门锁等执行器。

为确保支持互联网的产品实现良好的安全性，必须对具体产品及其系统级要求执行安全评估。这种评估应确定涉及的资产，并分析环境以及产品可能按预期和未按预期使用的情况，从而检测产品可能存在的漏洞。

这种评估可帮助开发人员使用可用的安全功能制定最佳保护机制。

每种产品的环境、资产和工艺都各不相同，但 IoT 设备通常都有一些相同的暴露点：

- 因特网（或内联网）连接
- 局域网连接
- 物理访问（无论是否能够操作硬件接口）

图 1-1 所示为连入 IoT 的产品通常具有的暴露点。

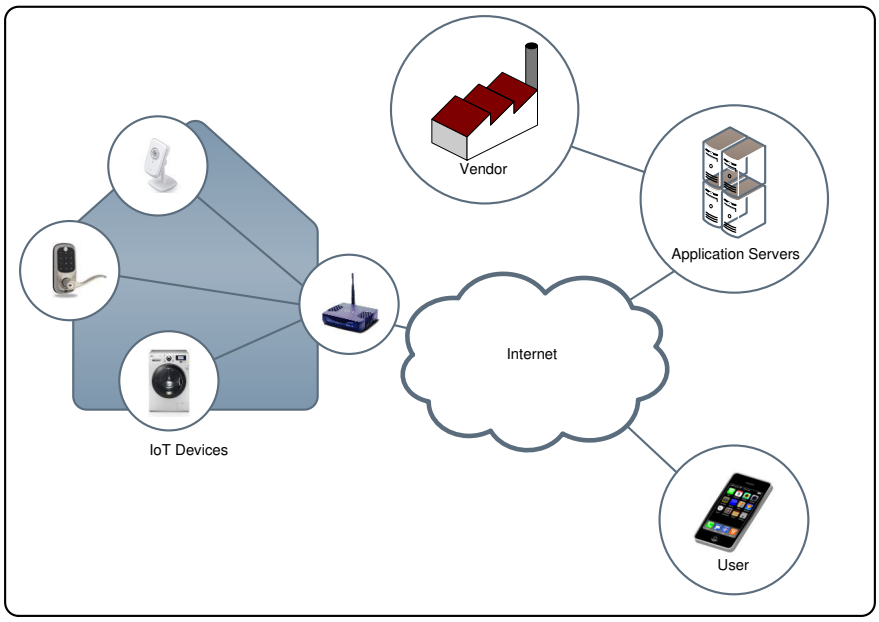

图 1-1. IoT 设备常见的暴露点

1.2.1 因特网连接

此暴露点与来自互联网连接的所有可能攻击通道相关。此向量中的漏洞可能来自所有通信通道（比如套接字）和使用的协议。通常，这些攻击的潜在目标是通过这些通道的所有资源和信息。不过，要意识到攻击方会尝试使用这些资源来增加暴露点，因此，必须仔细检查这些通道上的任何资源或信息。

SimpleLink Wi-Fi 器件集成了各种各样的功能，包括符合标准的安全传输层（SSL/TLS，也被称为安全套接字）、域名验证、安全内容交付以及器件唯一标识符，从而保障网络层通信安全。

这些功能不仅支持数据加密，还可通过信任验证程序的标准链对数据来源进行身份验证。

1.2.2 局域网连接

此暴露点类似于互联网连接暴露点。局域网的一般性质使其容易受到一组特定的攻击向量攻击。例如，监视无线网络，或者在 WLAN 或 LAN 上注入恶意或滥用流量。

其中一个向量基于攻击者未连接无线网络时对无线网络通信的被动监视。无线网络可能会遭到被动监视，因为即便在安全无线网络中，其中一些通信数据包标头也不会进行加密。这些标头可能会泄露该网络中设备的 MAC 地址以及这些设备所生成流量的时间特性等信息。

Wi-Fi Alliance® 在其相关标准中规定了安全和合规性测试。SimpleLink Wi-Fi 器件已获得 Wi-Fi Alliance 认证，符合所有相关安全要求。

另一攻击向量与来自局域网 (LAN) 中其他设备的攻击相关。这为执行涉及网络访问的攻击向量提供了额外的机会，导致能够为网络通信合理注入流量，滥用目标设备上的端口和可用协议。因特网通常会阻止访问这些端口和协议，但 LAN 会允许访问。

SimpleLink Wi-Fi 器件包括 HTTPS 服务器和 RX 滤波器等功能，因此支持为局域网开发附加安全层。

1.2.3 物理访问

若遇到物理访问攻击，暴露点位于产品级，因此需要考虑多种因素。物理访问可能会引发产品级篡改和印刷电路板 (PCB) 篡改等攻击向量。产品级篡改攻击向量是指在攻击过程中，攻击者可使用最终产品的外部接口（比如电力线、按钮等）来控制设备的运行方式。另一个攻击向量与攻击者能够接触实际电路板 (PCB) 并监听线路或硬件接口相关。在更为严重的情况下，攻击者甚至可能尝试篡改导线，替换 PCB 上的器件，连接到主控制器，以及注入信号来触发某些操作。

为了帮助抵御这类攻击，SimpleLink Wi-Fi 提供了 IP 保护、通过加密确保文件系统安全、文件完整性检查、克隆保护等功能。

1.3 主要特性

SimpleLink Wi-Fi Internet-on-a chip 系列器件提供广泛的内置安全功能。这些安全功能可支持并帮助设计人员解决各种安全需求，降低目标应用中的安全风险。图 1-2 简要展示了 SimpleLink Wi-Fi Internet-on-a chip™ 系列器件中提供的主要安全功能。图中按照这些功能通常所适用的暴露水平对其进行了组织整理。

表 1-2 列出了主要安全功能的概要说明。

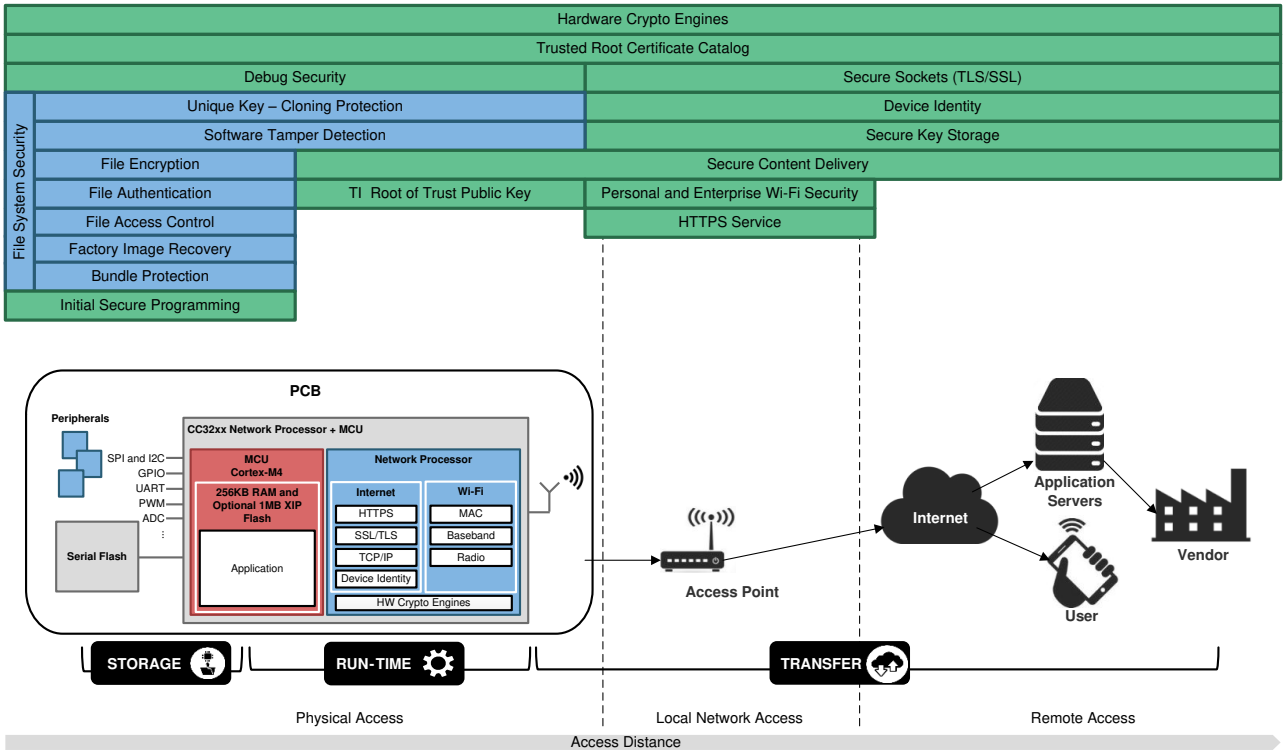

图 1-2. 安全措施

表 1-2. 主要安全功能

功能	描述	CC3120/CC3220	CC3135/ CC3235x	CC3130/ CC3230x
个人和企业 Wi-Fi 安全	符合 802.11 标准的安全支持 (WPA/WPA2-PSK/WPA2-EAP/ WPA2+PMF/WPA3)	+	+	+
安全套接字	符合 SSLv3、TLS1.0/1.1/1.2 标准的传输层安全。	可同时打开 6 个套接字	可同时打开 16 个套接字	可同时打开 16 个套接字
OCSP TLS 扩展	OCSP 是 TLS 协议的扩展，在 TLS 握手期间运行以检查证书链是否有已撤销的证书。支持 OCSP、OCSP Stapling 和 Stapling v2。	-	+	+
HTTPS 服务器	在 TLS 套接字顶层运行的内部 HTTPS 服务器，支持客户端身份验证。	+	+	+
器件身份	不可修改的唯一 128 位码，由 TI 在生产过程中存储在器件内。它可用作器件唯一标识 (UDID)。	+	+	+
安全密钥存储	外部闪存上的非对称密钥对存储，由从器件唯一密钥得出的密钥进行加密。	+	+	+
受信任根证书目录	内置安全机制，确保 CA 为受信任的证书链根，可用于 TLS 和文件签名。	+	+	+
TI 信任根公开密钥	基于硬件的机制，支持使用非对称密钥验证 TI 为特定内容（如软件服务包、受信任根证书目录等）的真正来源。	+	+	+
文件系统安全性	文件系统安全性可确保数据机密性和完整性。	+	+	+
安全引导	在启动期间验证运行时二进制文件的完整性和真实性（仅限 CC3220S、CC3220SF、CC3235S 和 CC3235SF）。	+	+	+

表 1-2. 主要安全功能 (continued)

功能	描述	CC3120/CC3220	CC3135/ CC3235x	CC3130/ CC3230x
安全内容交付	提供独立于传输层安全性的以端到端方式向系统交付机密信息的能力。	+	+	+
初始安全编程	编程期间的映像完整性检查和映像机密性，包括系统配置和用户文件等。	+	+	+
调试安全	阻止对调试功能的访问，如通过外部工具对 JTAG 接口进行的访问以及逐文件访问。	+	+	+
软件篡改检测	检测可能对安全文件内容进行的未授权操作并发出警告。	+	+	+
克隆保护	文件系统会使用器件独有的密钥对进行加密。	+	+	+
符合 FIPS 140-2 第 1 级标准(1)	FIPS 140-2 是一项用于批准加密模块的美国政府计算机安全标准。SimpleLink Wi-Fi 器件中有两个芯片模块受到 FIPS 140-2 第 1 级约束。	-	+	-

(1) 目前正在进行 FIPS 认证，如需了解最新状态，请参阅 https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules。

CC3220 和 CC323x 器件具有独特的架构，采用两个物理上独立的 MCU 和内存执行环境。图 1-3 展示了 CC3220/CC3230/CC3235x 器件的简化框图并标示了它们提供的安全功能。

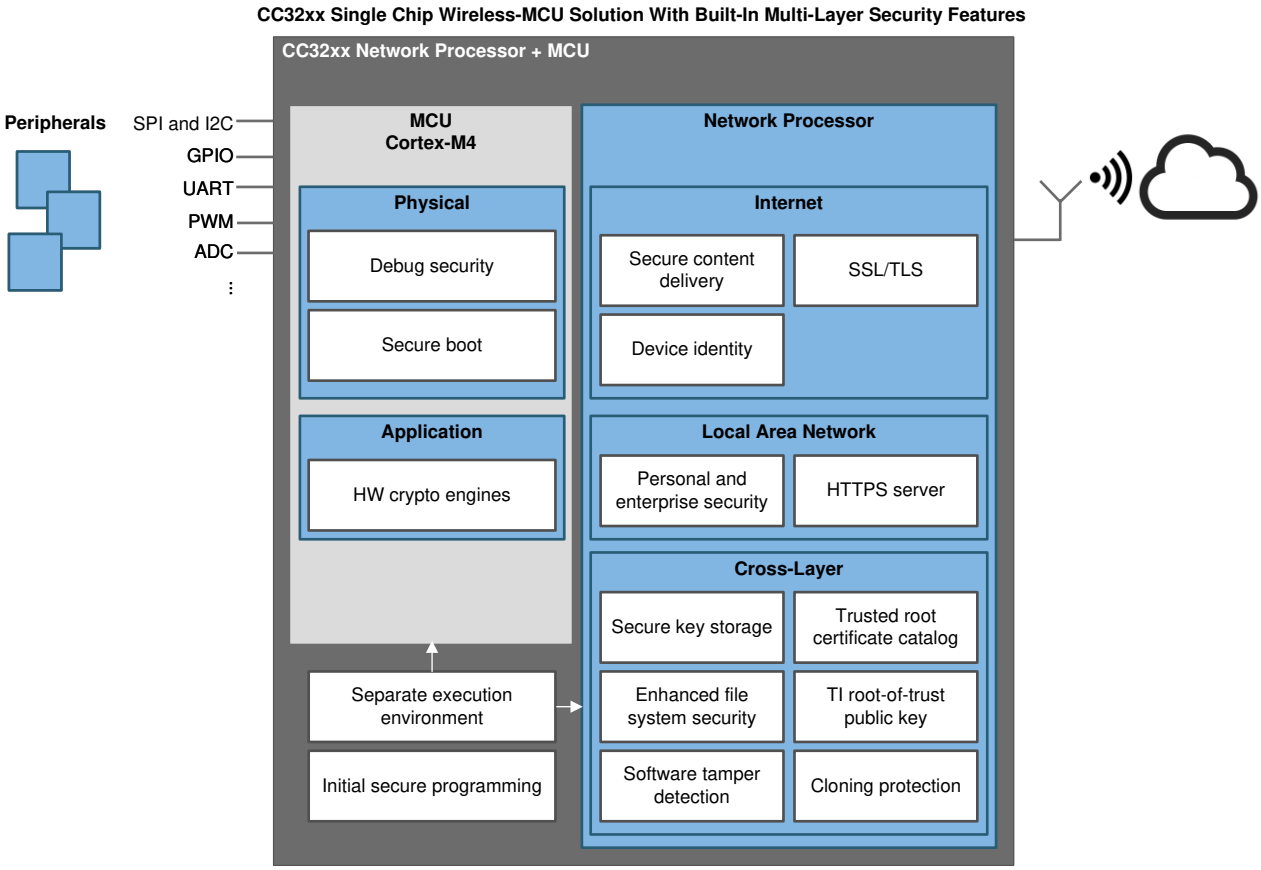

图 1-3. CC3220/CC3230/CC3235x 器件安全功能

图 1-4 展示了 CC3120/CC3130/CC3135 器件具备的安全功能的框图。

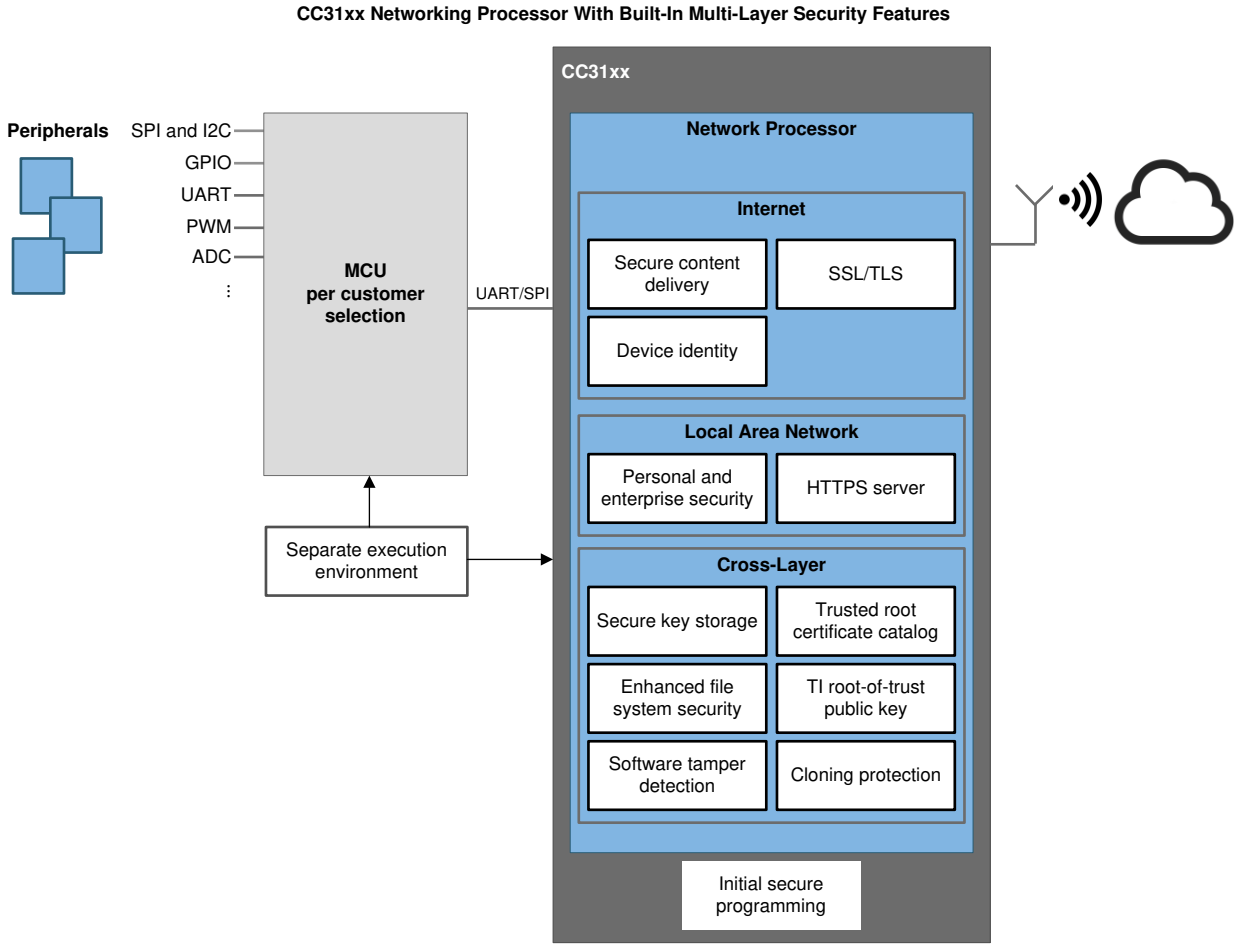

图 1-4. CC3120/CC3130/CC3135 器件安全功能

2 网络层安全

SimpleLink 器件是一款基于 Wi-Fi 的器件，支持局域网段（在节点与 AP 之间）的 802.11 安全协议，在使用 TCP/IP 进行节点之间的通信时，支持传输层的 TLS/SSL。TLS/SSL 可确保网络节点之间的机密性、数据完整性和真实性。

图 2-1 所示为常见的安全通信层。

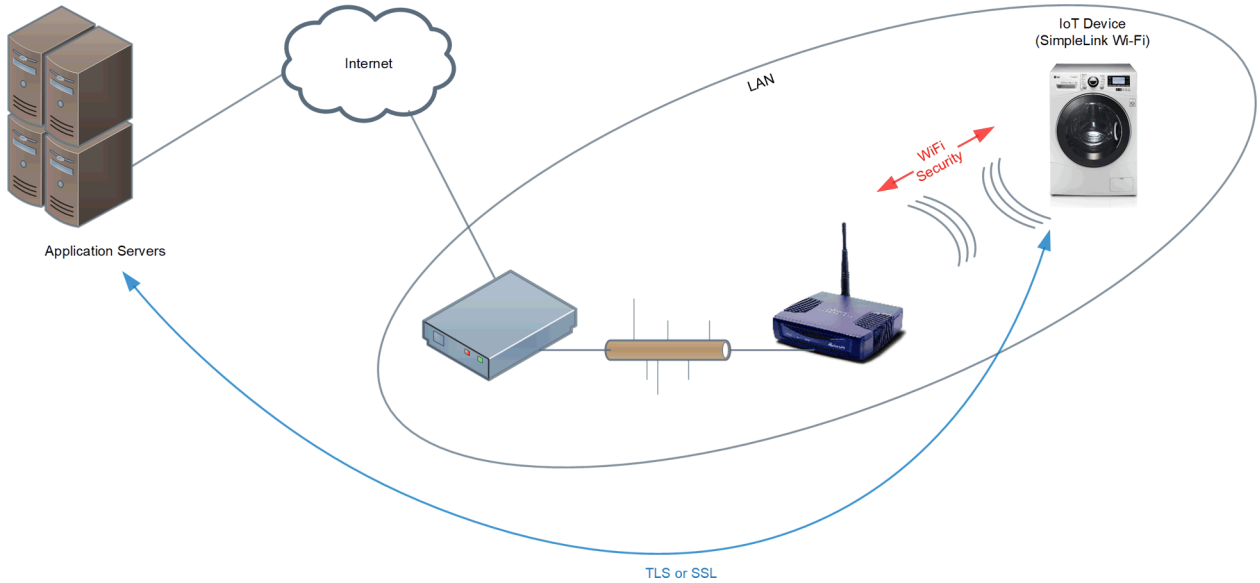

图 2-1. 网络安全拓扑

2.1 Wi-Fi 安全

SimpleLink 器件的 Wi-Fi 层符合 802.11 安全标准，可确保 AP 与 STA 之间或 Wi-Fi 直连模式下的两个对等器件间事务中的帧（L2 数据单元）的完整性和机密性。IEEE 802.11 规范及其扩展内容中介绍了相关安全协议。

SimpleLink 器件的 Wi-Fi 子系统支持个人或企业安全设置，包括基于 RADIUS 的身份验证 (802.1X)。

SimpleLink 器件属于 Wi-Fi-CERTIFIED™ 器件，符合相关的 Wi-Fi Alliance (WFA) 安全标准和测试套件要求。表 2-1 列出了支持的 Wi-Fi 安全相关功能。

表 2-1. Wi-Fi 安全

类型	Wi-Fi 安全
个人	AES (WPA2-PSK/WPA2+PMK/WPA3-PSK) TKIP (WPA-PSK) WEP
企业	EAP Fast EAP PEAPv0 MSCHAPv2 EAP PEAPv0 TLS EAP PEAPv1 TLS EAP TLS EAP TTLS TLS EAP TTLS MSCHAPv2

所有无线密码均以加密格式存储在串行闪存上。这些密码仅供网络处理器 (NWP) 使用，不可通过 API 或任何调试通道用于主机。

备注

WEP 安全性在设计上存在缺陷和不足。TI 强烈建议不要使用。仅出于旧版兼容原因，SimpleLink 产品才支持这种安全性。

2.2 安全套接字层

SimpleLink 器件基于按标准实施的 SSL 和 TLS 协议提供安全传输层（安全套接字），这些网络协议涉及专用于实现 TCP/IP 连接通信安全的加密方式。在大多数系统中，SSL/TLS 以传输层之上的层的形式实施。在 SimpleLink 器件中，SSL/TLS 已嵌入 BSD 套接字层，支持无缝访问安全套接字层。API 扩展让用户可以对 SSL/TLS 行为和配置进行一定程度的控制。

SSL/TLS 在网络处理器子系统上运行。通过设计，器件架构可确保网络处理器是一个物理上独立的处理子系统，从而形成独立的执行环境。硬件加速器可用于减少加密算法中涉及的密集算术计算。

表 2-2 简要介绍了 SimpleLink 器件中受支持的 SSL/TLS 规范。

表 2-2. 支持的 SSL 规范

协议版本	SSL v3、TLS 1.0、TLS 1.1、TLS 1.2
密码套件	SL_SEC_MASK_SSL_RSA_WITH_RC4_128_SHA SL_SEC_MASK_SSL_RSA_WITH_RC4_128_MD5 SL_SEC_MASK_TLS_RSA_WITH_AES_256_CBC_SHA SL_SEC_MASK_TLS_DHE_RSA_WITH_AES_256_CBC_SHA SL_SEC_MASK_TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA SL_SEC_MASK_TLS_ECDHE_RSA_WITH_RC4_128_SHA SL_SEC_MASK_TLS_RSA_WITH_AES_128_CBC_SHA256 SL_SEC_MASK_TLS_RSA_WITH_AES_256_CBC_SHA256 SL_SEC_MASK_TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 SL_SEC_MASK_TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 SL_SEC_MASK_TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA SL_SEC_MASK_TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA SL_SEC_MASK_TLS_RSA_WITH_AES_128_GCM_SHA256 SL_SEC_MASK_TLS_RSA_WITH_AES_256_GCM_SHA384 SL_SEC_MASK_TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 SL_SEC_MASK_TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 SL_SEC_MASK_TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 SL_SEC_MASK_TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 SL_SEC_MASK_TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 SL_SEC_MASK_TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 SL_SEC_MASK_TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 SL_SEC_MASK_TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 SL_SEC_MASK_TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
最大安全套接字数	16 (CC3x3x)、6 (CC3x20x)
其他	服务器身份验证 客户端身份验证 域名验证 独立的执行环境 OCSP（仅限 CC3x3x 上）

2.2.1 SSL/TLS 证书处理和其他安全文件

证书文件、DH (Diffie-Hellman) 参数和密钥必须存储在器件的文件系统中，以根据所选的密码套件执行某些 SSL/TLS 功能（请参见表 2-3）。

证书为标准格式文件，其中包含非对称密钥对的公共密钥，因此在本质上为非机密信息。另一方面，私有密钥是机密信息，需要保持加密。应对这些文件进行访问控制限制，限制对合法所有者的读访问（请参见节 3.2.4）。

密钥和证书由 SSL 套接字在执行握手时在内部使用。主机必须使用 API 仅将相关文件与 SSL/TLS 套接字绑定。

表 2-3 列出了 SimpleLink SSL/TLS 套接字支持的文件。

表 2-3. SSL/TLS 文件

文件	客户端如何使用	服务器如何使用
根 CA 文件： 自签名证书，用于对远程对等器件链进行签名	验证受信任的服务器链。 如果未安装，则返回 ESECSNOVERIFY 警告，但连接不会隐式终止。 格式：PEM/DER	安装后支持客户端验证。 如果客户端无法提供与已安装 CA 证书相匹配的相应信任链，器件会发出 ESEC_NO_PEER_CERT 事件。 格式：PEM/DER
证书文件： 颁发给该实体的证书	此证书文件在服务器需要执行客户端身份验证时用作客户端证书。 如果该文件不存在且服务器需要执行客户端身份验证，则服务器会返回 ALERT，提示对等器件验证错误。 私有密钥必须使用此文件进行编程，否则连接会失败并显示 ESECBADPRIVATEFILE。 格式：PEM/DER	此证书文件用作服务器证书或证书链。 该证书应为列表中的第一个证书。 该文件必须进行配置。如果未配置，则会生成错误 EBADCERTFILE。 格式：PEM
私钥文件： RSA 或 ECDSA 密钥	如果服务器需要执行客户端身份验证，则用作客户端私有密钥。 如果未随此文件安装匹配的公用证书文件，则会显示 ESECBADCERTFILE。 格式：PEM/DER	用作服务器的私有密钥。必须编程为使用 SSL/TLS 连接服务器。 如果不可用，则返回 EBADCERTFILE。 格式：PEM/DER
PEER 证书、 DH Param（客户端、服务器）	若对此文件进行编程，则会通过完整的服务器证书对比来实现域验证。 此证书会与 SSL/TLS 握手过程中服务器证书提供的证书进行比较，防止发生中间人 (MITM) 攻击。它用于验证此服务器为尝试连接的目标服务器。 格式：PEM/DER	用作 DH 参数文件，支持使用基于 DH 的密码。 格式：PEM/DER

2.2.2 SSL/TLS 握手概述

在两个对等器件间建立 TCP 连接后，在协商会话安全参数及验证对等器件时会应用 SSL 协议。

此握手过程可以简要描述为：此握手操作由 SimpleLink 器件执行，并对用户保持透明：

1. 客户端问候消息随下列参数发送：
   - 要使用的协议版本 - SSLv3、TLS1.0、TLS1.1、TLS1.2
   - 客户端支持的密码套件
   - 扩展，用于不同的 SSL 应用
2. 服务器从客户端问候密码列表中选择协议版本和密码套件，并向客户端发送 ServerHello 消息。
3. 服务器向客户端发送证书链（根 CA 除外）。
4. 客户端会从客户端持有的根 CA 开始，检查证书链中每个证书的签名，以此验证证书链。服务器可能会向客户端请求证书，用于执行客户端身份验证。
5. 客户端和服务器建立会话（对称）密钥，然后开始传输加密数据。

图 2-2 展示了 SSL/TLS 握手过程。

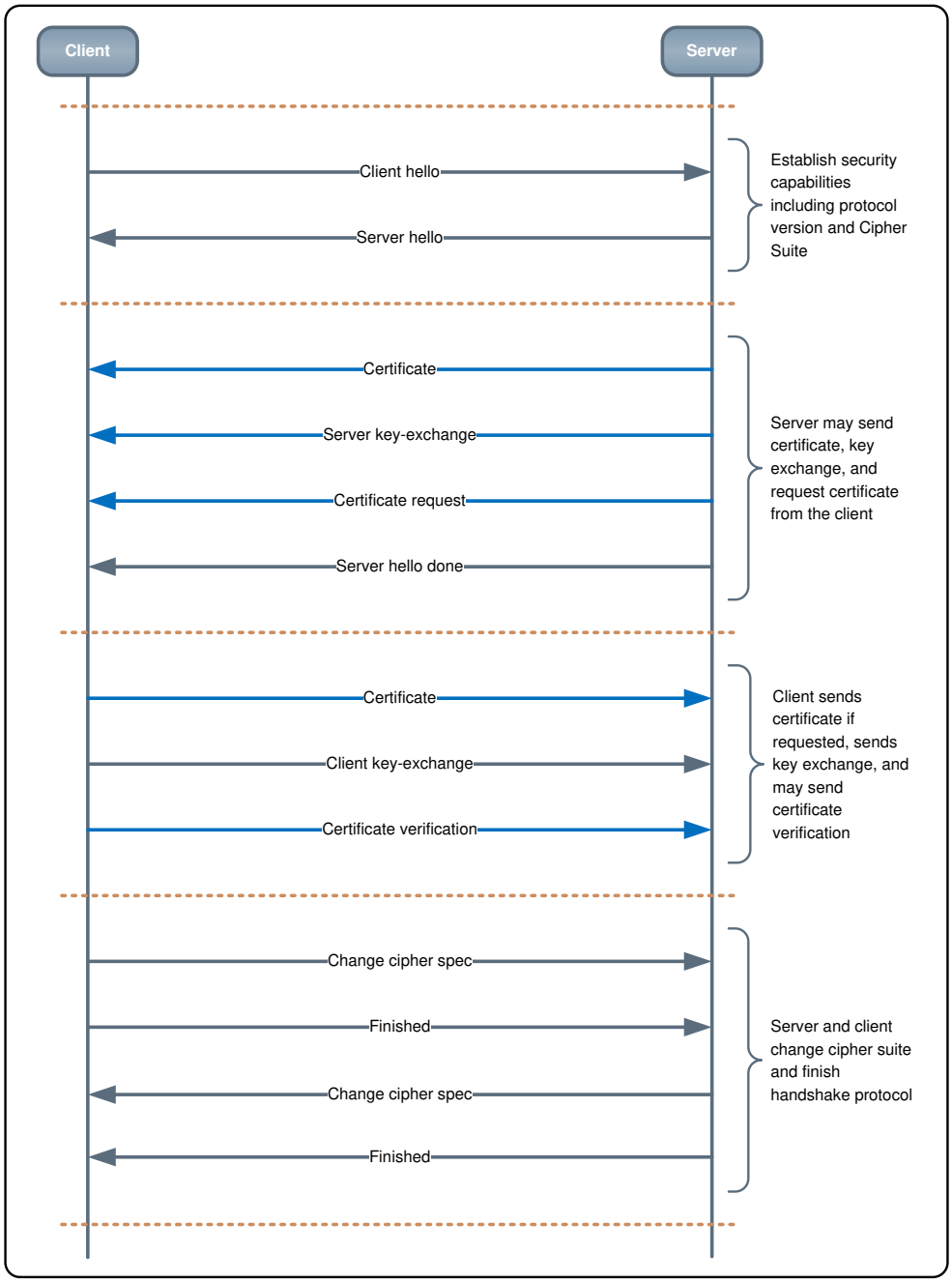

图 2-2. SSL/TLS 握手

2.2.3 SimpleLink 器件的 SSL/TLS 握手

SSL/TLS 协议是 SimpleLink 器件网络协议栈不可分割的一部分，在网络子系统中运行，从而形成独立的执行环境。该层的唯一接口是通过来自应用程序处理器的 API 调用。

2.2.3.1 SSL/TLS 握手支持的功能

表 2-4 列出了 SSL/TLS 握手功能。

表 2-4. SSL/TLS 主要握手功能

操作	客户端	服务器
验证对等器件	√	√
STARTTLS	√	√
服务器域验证	√	不适用
受信任根证书目录	√	不适用
时间和日期验证	√	不适用
OCSP	√	不适用

2.2.3.2 基本 SSL/TLS 连接

在大多数系统中，SSL/TLS 协议在 TCP 层之上实施。在 SimpleLink 器件中，SSL/TLS 套接字已嵌入 TCP 层，同时保留标准 TCP 套接字的感观。整个 SSL/TLS 握手是在连接会话期间自动触发的（当调用 connect() 或 accept() API 时）。此方法简化了使用安全套接字的工作。若使用协议参数中的安全参数打开套接字，然后调用连接或接受命令，则可与其他对等器件建立安全连接。

在服务器模式下，必须提供服务器证书或证书链以及私有密钥。此证书链在握手过程中发送。若缺失这些文件，调用 sl_Accept 时会生成错误。

在客户端模式下，如果远程服务器策略需要执行客户端身份验证，则可提供客户端证书及其私有密钥。

2.2.3.3 错误和警告

BSD 命令会返回有关任何故障的详细错误，包括安全套接字握手。

有些错误代码会反映安全相关的警告，但不会阻止进程。强烈建议开发人员注意以下警告，因为这些警告指示潜在的安全问题：

- SL_ERROR_BSD_ESECSNOVERIFY – 已连接，但未进行服务器验证
- SL_ERROR_BSD_ESECDATEERROR – 已连接，但证书日期验证出错
- SL_ERROR_BSD_ESECUNKNOWNROOTCA – 已连接，但根 CA 不受信任

2.2.3.4 验证对等器件

与服务器的基本连接导致 sl_Connect 命令收到错误 – SL_ERROR_BSD_ESECSNOVERIFY。这意味着数据流从此时开始加密，但 SimpleLink 器件并未验证远端是否为真正的服务器。

在这种情况下，数据已加密并且现在偷听者无法窃听数据，但服务器身份未经验证。如果不对服务器身份进行验证，则仍可能受到中间人 (MITM) 攻击或网络钓鱼攻击。

设定一个对服务器证书签名的根 CA 会触发对服务器信任链进行签名检查，这也被称为*完整信任链验证*。如果验证失败，连接就会终止。

如果 SimpleLink 器件处于服务器模式，则可以通过设定对客户端证书进行签名的根 CA 来验证客户端。如果验证失败，连接就会终止。

2.2.3.5 域名验证

信任链评估可确保由受信任的实体执行通信。不过，仍然不能保证它的身份是通信目标对象。

通过域名验证可以确保这一点。域名验证可用于确认实际通信对象的身份是否就是通信目标对象。通过对比服务器提供的证书和预期预存储证书的内容即可确认这一点。

如果对比失败，则会触发安全警告，但仍保持连接。警告的处理方式由开发人员决定。

2.2.3.6 受信任根证书目录

受信任根证书目录是一种由 TI 提供并签发的文件，其中包含一系列已知的受信任根 CA（TI SDK 和相关材料中提供完整列表）。该目录中包含来自常见受信任 CA（例如 VeriSign®、GoDaddy® 或 GeoTrust® 等）的受信任根证书。受信任根证书目录还保存了 TI 已知的吊销证书清单。受信任根证书目录仅用于客户端模式。用作服务器时，允许使用自签名根 CA 对客户端进行身份验证。

如果根 CA 对受信任根证书目录而言是未知的，sl_Connect 命令会返回警告 SL_ERROR_BSD_ESECUNKNOWNROOTCA，这表示已成功建立连接，但用于验证服务器信任链的根 CA 是未知的。在这种情况下，开发人员应选择是以显式方式终止连接还是自行冒险继续处理。

若在 SSL/TLS 连接期间收到吊销的证书（已检查所有证书链），或者由用户设定的根 CA 已被吊销，握手会终止，sl_Connect 命令返回 SL_ERROR_BSD_ESECCERTIFICATEREVOKED。

受信任根证书目录以文件形式存储在文件系统中，而且只能更新为更新的版本。

图 2-3 显示了证书文件和受信任根证书目录之间的关系。TI 批准的根 CA 列表已在 SDK 中提供，也可在 SimpleLink CC3120/CC3220 根证书目录中找到。

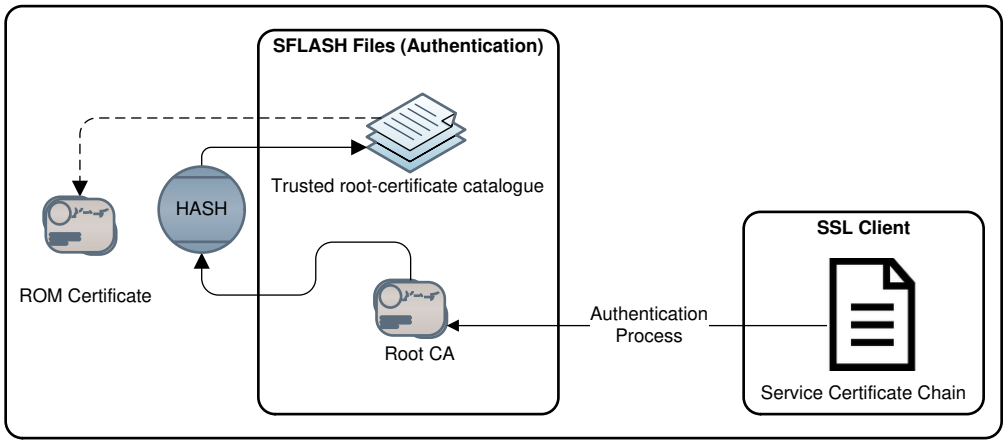

图 2-3. 证书文件及其与受信任根证书目录之间的关系

2.2.3.7 验证服务器的日期

每个证书都有到期日期。当以客户端模式连接服务器时，如果已设定根 CA，则会进行服务器时间验证。如果时间验证失败，sl_connect 命令会返回错误 SL_ERROR_BSD_ESECDATEERROR，表示“已连接，但时间和日期验证出错”(connected with time and date validation error)。用户可以设定器件的时间和日期，用于执行证书时间和日期验证。日期和时间在休眠模式下保持不变。

设定日期和时间时，会对串行闪存执行写操作，因此在考虑闪存耐用性时应考虑此因素。

2.2.3.8 OCSP

OCSP 是 TLS 协议的扩展，在 TLS 握手期间运行以检查证书链是否有已撤销的证书。SimpleLink Wi-Fi 器件 (CC3x3x) 支持 OCSP、OCSP Stapling 和 OCSP Stapling v2。器件会自动根据服务器能力选择这些模式。此功能启用后，器件会检查整个证书链是否有已撤销的证书。此功能默认为禁用。

2.2.4 SSL/TLS 连接的最大数

CC3120、CC3220R、CC3220S 和 CC3220SF 器件最多具有 6 个并发连接的 SSL/TLS 客户端套接字。对于服务器套接字，接受套接字 (服务器用于侦听新连接的套接字) 不计算在内。

在 CC3130、CC3230S、CC3230SF、CC3135、CC3235S 和 CC3235SF 器件中，所有 16 个套接字都可以是安全套接字。

2.2.5 选择 SSL 参数

可以设置允许使用的 SSL 版本，以针对不同的实现方式使用特定的密码列表。一些密码算法由硬件运行，而另一些则由软件运行。借助 Simpelink 接口，可以轻松地仅选择硬件加速算法。

2.2.6 套接字安全性变更 (STARTTLS)

常规的 TCP 套接字可以升级为 SSL/TLS 套接字。若要进行升级，用户必须以显式方式触发 SSL/TLS 握手，而与套接字连接 (由 sl_connect 或 sl_accept API 触发) 无关。此实现通常在采用 STARTTLS 的应用内使用，用于将连接的会话升级为安全连接。

此类应用的示例为端口 587 上的简单邮件传输协议 (SMTP)。只有在从对等器件接收到 SSL/TLS 关断警告时，才能将安全套接字降级为非安全 TCP 套接字。SimpleLink 器件用户无法在安全连接上发起 SSL/TLS 关断操作。如果套接字已升级或降级，则会向主机下发异步事件，指示进入新状态。

3 文件系统安全

3.1 概述

SimpleLink 解决方案具有外部非易失性存储器 (NVM)，该存储器采用串行闪存器件的形式。SFLASH 上的数据有序地存储在文件系统中，而且器件提供用于对其进行访问的 API。文件系统可供主机应用程序使用，用于创建、写入和读取文件。文件系统也可供网络子系统使用，用于存储配置文件和临时文件。

系统文件在编程过程中创建或由器件创建，用于在循环通电时保存器件状态和配置。这些文件无法通过主机访问。

文件系统设计为具有内置的内容保护功能。其中的一些功能会在内部应用，而其他功能则由用户控制。

以下功能构成了器件文件系统安全功能集：

- 加密 - 使用标准 AES-128 加密算法对文件进行存储和加密。
- 克隆保护 – 整个文件系统内容，包括应用程序二进制映像，都会使用器件独有密钥进行加密。
- 文件系统完整性验证 - 验证文件系统结构完整性的目的是检查文件系统是否被篡改。
- 软件篡改检测 - 内容完整性可通过文件系统进行验证，如果检测到对文件的恶意访问，则会触发警报。
- 访问控制 - 可按访问类型将文件访问限制为仅合法所有者能够访问。
- 来源验证 - 文件可定义为仅限提供有效的证书时才具备更新资格。
- 恢复机制 - 文件系统可恢复为初始编程配置。

服务包和受信任根证书目录均为系统文件，它们必须以安全文件的形式进行创建。这些文件只能由器件读取。对于包含 SSL/TLS 连接密钥等机密数据的文件，也应采用安全文件的形式进行创建。

3.2 文件系统安全功能描述

3.2.1 加密

通过数据加密可实现机密性。在这种情况下，只有经过加密的文件版本才能保存在串行闪存上。AES-128-CTR 是选定的加密方法。密钥由器件使用真随机数发生器 (TRNG) 硬件引擎在内部生成。解密是器件固有的特性，并会在读取文件时动态执行。

3.2.2 克隆保护

文件系统元数据会使用器件密钥进行加密，每个器件具有唯一的密钥。该密钥对于每个器件而言都具有唯一性，因此无法将某一器件上创建的文件系统移至另一器件。这样做会导致在执行启动序列期间检测到安全违例，器件会进入锁定状态。

3.2.3 完整性验证

对于创建时带有 *安全认证*标志的安全文件，需要执行完整性检查。完整性检查由 SimpleLink 器件执行。每次文件发生更改时，都会执行新的哈希算法，并得到文件签名。当打开文件执行读操作时，需对照此签名对文件内容进行验证。

系统文件和文件系统结构也受到保护，其完整性由器件进行测试。系统文件的完整性验证使用 HMAC-SHA-256 算法执行。

如果器件确认验证失败，则会触发系统安全警报。

如果器件确认文件系统结构或系统文件的验证失败，则会将其状态更改为锁定状态。

3.2.4 访问控制

每个安全文件都有几种访问级别；访问级别就文件的使用方式进行了限制。令牌用于控制对安全文件的访问。

创建安全文件后，会生成四个不同的令牌（32 位数）。每个令牌都为文件提供一个不同的访问级别，如表 3-1 所述。

表 3-1. 令牌

类型	说明
主机令牌	支持对文件的完全访问。安全文件只能使用主机令牌删除。只要文件存在，主机令牌就不可更改。
读/写令牌	支持读写访问。此令牌在文件发生更改后自动生成。
只写令牌	仅支持写访问。用于面向生产者的文件，如私有密钥等。此令牌在文件发生更改后自动生成。
只读令牌	仅支持读访问。用于面向消费方的文件，如公共密钥等。此令牌在文件发生更改后自动生成。

网络处理器会自动生成安全文件的令牌。主机令牌为文件创建函数的输出参数，并由主机接收。

通过提供有效文件令牌作为输入，Get Info 功能支持主机检索所有可访问文件令牌。只能检索出优先级低于输入令牌的令牌。

每当打开文件执行写操作时，系统的默认行为将是重新生成所有文件令牌，但主机令牌除外。这种默认行为可使用文件创建标志进行更改。文件创建标志可覆盖令牌创建的默认行为。节 3.3 对文件创建进行了说明。

当打开安全文件执行写操作时，打开-写入函数会返回新生成的令牌。返回的令牌与输入令牌具有相同的访问级别。

例如，对于在将写令牌作为输入的情况下打开以执行写操作的文件，则会返回新的文件写令牌。

3.2.5 受信任源验证

文件系统可确保文件签名来源被公共根 CA 信任，以此提供另一层保护。该程序默认应用于安全文件。

用于此过程的身份验证方法遵循 PKI，密钥大小可为 128 或 256。文件签名用于验证文件完整性以及用于对该文件进行签名的信任链。

若要创建身份验证过程的数字签名，供应商必须拥有 RSA 密钥对。持有公共密钥的证书必须经由链接到已知根证书颁发机构 (CA) 的证书进行签署。该证书的整个信任链由器件验证，并将根 CA 的签名与使用受信任根证书目录的预期哈希算法进行对比。

备注

该文件验证过程中不会验证证书到期日期，因为不存在绝对的方法可以确保本地日期和时间的有效性在所有情况下都适用。

在创建新的安全文件时，可以选择跳过文件验证的默认行为。这通过使用以下专用创建标志来实现：SL_FS_CREATE_NOSIGNATURE。

图 3-1 显示了文件验证过程。

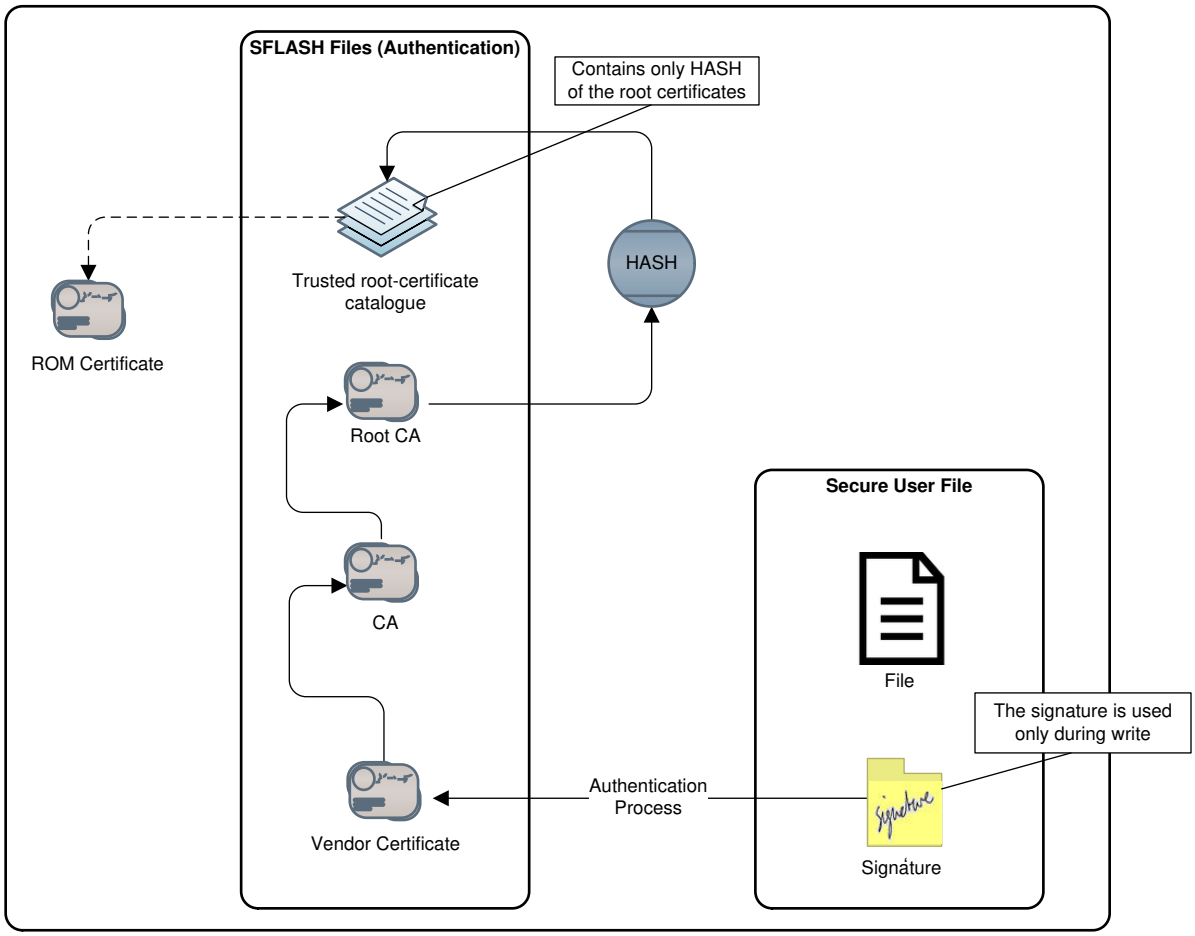

图 3-1. 验证文件签名

3.2.5.1 服务包和受信任根证书目录来源验证

服务包和受信任根证书目录均为仅限 TI 提供并签名的文件。

对服务包和证书存储文件执行写操作需要签名；这些文件的签名由 TI 提供。证书材料预先安装在器件上。

受信任根证书目录包含吊销证书清单。如果在 SSL/TLS 连接的过程中出现此清单中的某一证书，连接就会终止并且器件会向主机触发事件。

3.2.6 恢复机制

SimpleLink 器件中嵌入了内部恢复机制，支持文件系统在生产过程中恢复为编程的预定义映像。

恢复映像是串行闪存中保存的系统文件。该文件以安全文件的形式存储。恢复映像文件已列入文件列表，但无法通过主机进行访问。

可使用以下方法触发恢复程序：

- 设置 SOP
- 通过主机调用函数 sl_DeviceSet

恢复机制支持多种模式；器件恢复模式在创建文件系统映像的过程中进行配置。

支持的恢复模式包括：

- 无 - 无恢复设置，在这种情况下，不保存恢复映像文件。
- 支持恢复出厂默认设置。
- 支持恢复出厂映像和出厂默认设置。

恢复出厂映像 - 出厂映像文件包含编程设定的映像文件，其中包括服务包、主机应用程序（限 CC3220/CC3230/CC3235x）、配置文件和用户文件。调用后，器件会执行格式化，然后重新编程。所有文件的内容都会替换为出厂映像文件。原始映像中不存在的文件都会被删除。恢复出厂映像操作可通过主机命令或设置 SOP 来调用。

恢复出厂默认设置 - 恢复出厂默认设置与恢复出厂映像类似。区别在于，不会恢复服务包和主机应用程序（限 CC3220/CC3230/CC3235x），因此会使用最新的服务包和最新的主机应用程序。使用这种方法时，主机应用程序可能使用的任何文件都会恢复为编程设定的内容。

恢复出厂默认设置过程具备故障安全特性，即使在操作过程中断电也会继续执行。

3.2.7 篡改警报

SimpleLink 器件具备数据篡改程序和安全警报计数器。该程序会在访问文件系统时检查系统文件和以*安全和认证*形式创建的文件是否存在完整性违规。

访问违规（如尝试访问令牌无效或不正确的文件）也会被视为尝试篡改操作而进行监视和检测。

当系统达到预定义的安全警报限制时，器件会锁定并触发异步事件。

若要从锁定状态恢复，必须对器件进行重新编程或使其恢复出厂映像。

安全警报计数器将始终保持运行，其值在编程过程中或仅在恢复出厂设置功能中设为 0。

安全警报阈值可以在映像创建过程中配置（使用映像生成器工具）。

主机可以使用 sl_deviceGet API 检索系统中当前的安全警报数。

表 3-2 列出了不同的安全警报。

表 3-2. 安全警报

类型	说明
显式警报（严重）	无论警报计数器阈值如何，器件都会立即锁定。 在检测到以下篡改事件时会创建显式警报： • 文件系统结构完整性错误 • 系统文件完整性错误 • 克隆 SFLASH
隐式警报	当警报计数器达到警报阈值时，器件锁定。 在检测到以下篡改事件时创建隐式警报： • 访问令牌无效或不正确 • 以*安全和认证*形式创建的文件，在打开以执行读操作时出现完整性违规 • 在升级*安全和认证*文件内容时设置的签名或证书无效

3.2.8 特殊系统文件

表 3-3 列出了由 SimpleLink 器件特殊处理的文件。

表 3-3. 特殊处理文件

类型	说明
服务包	服务包创建为安全签名的公共写文件。 该文件的签名由 TI 提供，并且由器件使用基于硬件的信任根进行验证。
受信任根证书目录	受信任根证书创建为采用安全签名的公共写文件。该文件的签名由 TI 提供，并且由器件使用基于硬件的信任根进行验证。 该文件还具备防降级保护；主机无法写入版本低于已安装版本的文件。
运行时二进制文件（主机应用程序）	运行时二进制文件必须创建为安全签名文件。 供应商负责创建主机签名并提供签名证书。

3.2.9 文件安全级别

主机可以在 SimpleLink 器件文件系统中创建文件，并设置所创建文件的安全级别。

表 3-4 列出了可能的安全级别。

表 3-4. 文件安全级别

类型	说明
无	数据以纯文本形式存储。 系统不会对数据进行验证。
安全文件	该文件内容以加密形式存储。 访问该文件需要令牌。
安全和认证文件	该文件内容以加密形式存储。 访问该文件需要令牌。 每次打开文件执行读操作时，系统都会测试文件的完整性。 每次文件发生更改后都会执行文件身份验证来源和文件完整性检查。

3.3 文件创建属性

文件属性在创建过程中定义，其中包括文件的安全属性。这设定了文件与安全相关的处理方式。文件属性基于创建标志且无法更改。

表 3-5 列出了创建标志。

表 3-5. 创建标志

类型	说明
SL_FS_CREATE_FAILSAFE	通过失效防护功能打开文件时，文件系统中会为文件分配空间以创建两份副本，但一次只有一份副本有效。每次打开文件执行写操作时，无效的位置会被擦除。如果系统在对支持故障安全的文件执行写操作时断电，原有实例就会保留有效的副本。
SL_FS_CREATE_SECURE	作为安全文件创建的文件会在 SFLASH 上对其内容进行加密。该文件的访问受限，需要使用文件令牌。
SL_FS_CREATE_NOSIGNATURE	该标志仅与安全文件相关。默认情况下，在对安全文件执行写操作时需要使用签名。此签名用于对文件来源执行身份验证。该标志支持用户在写操作期间跳过身份验证。
SL_FS_CREATE_STATIC_TOKEN	仅与安全文件相关。该标志会更改默认的文件令牌创建行为：借助该标志，在每次打开文件执行写操作时，文件令牌不会更改。
SL_FS_CREATE_VENDOR_TOKEN	仅与安全文件相关。该标志会更改默认的文件令牌创建行为：借助该标志，文件主令牌由主机设定。
SL_FS_CREATE_PUBLIC_WRITE	仅与安全文件相关。该标志会更改默认的文件令牌创建行为：借助该标志，可对文件执行写操作而无需令牌。
SL_FS_CREATE_PUBLIC_READ	仅与安全文件相关。该标志会更改默认的文件令牌创建行为：借助该标志，可对文件执行读操作而无需令牌。

表 3-6 列出了属于非创建标志的标志。这些非创建标志可在每次打开文件执行写操作时设定。

表 3-6. 非创建标志

类型	说明
SL_FS_WRITE_BUNDLE_FILE	用于捆绑提交功能。
SL_FS_WRITE_ENCRYPTED	用于安全内容交付。

4 对器件进行编程

对器件进行编程的过程会对系统完整性产生重大影响。为确保系统完整性，SimpleLink 器件应用基于映像的编程方法。器件编程过程使用单个映像文件，其中包含所有器件配置、运行时二进制文件以及其他互补数据文件。所有这些内容都能够打包到单个文件中，然后用于编程，确保不会发生器件被部分配置的情况。

映像创建由 TI 提供的跨平台外部工具处理。该工具将构成映像的所有材料作为输入，并输出映像二进制文件，该文件可刷写到器件所连的串行闪存中。

实际烧录过程与映像结构无关。因此，该过程可由该工具执行，或由其他标准闪存工具执行。

此映像用作恢复操作时的出厂默认映像（如果使用该选项），具体如节 3.2.6 所述。

4.1 开发阶段

为了便于使用 SimpleLink 器件进行开发，同时又不损害安全功能，SimpleLink 器件支持独立的开发方法（调试安全性）。

在开发模式下，所有安全功能均可使用，但为确保调试环境适合，所有调试接口均可用，而且可以逐个文件修改文件系统内容（为了避免针对每次更改重新生成并编程新映像）。

为避免泄露器件唯一的密钥材料，在此模式下使用一组单独的密钥。

器件根据映像类型切换为开发模式，而映像类型在映像创建过程中确定。每个器件的开发映像都是唯一的。映像与编程目标器件紧密相关（根据其硬件定义的 MAC 地址）。这有助于阻止开发映像广泛用于生产。

在开发模式下，支持以下功能：

- 允许通过映像创建工具来访问文件（逐文件访问）。
- 可通过映像创建工具来访问文件列表。
- 启用了 JTAG 接口（仅限 CC3220/CC3230/CC3235x 器件）。

4.2 生产阶段

生产映像适用于大规模生产，并可同时编程到多个器件。此映像在器件首次启动时被压缩，并转换为器件唯一的映像。JTAG 接口会被阻止。

4.2.1 编程方法

SimpleLink 器件支持以下编程方法：

- 映像创建工具（使用 UART 传输）
- 主机编程（使用主机 API）
- 外部编程（比如“Gang”编程）

4.2.1.1 外部编程（Gang 编程）详情

若要使用此方法进行操作：

1. 未在目标 PCB 上组装串行闪存时，使用第三方编程器对其进行编程。第三方编程工具需要支持标准文件格式（Intel HEX 文件或二进制原始文件）。
2. 将编程后的串行闪存装在目标 PCB 上。
3. 首次上电过程中，SimpleLink 器件会检测该映像，确保其完整性，然后开始压缩。

可对该映像进行加密，使其对处理 Gang 编程的第三方保密。在这种情况下，映像创建过程中会提供密钥，而输出映像则使用该密钥进行加密。在生产过程中，进行映像检测时，器件会通过 UART 线路提供对映像进行解密的密钥，等待从 OEM 激活。映像经过认证后，会立即开始进行压缩。

备注

CC32xx LaunchPad™ 开发套件配备一个连接器，用于连接外部编程器来测试此方法。

5 现场软件更新

SimpleLink 器件支持多种现场软件更新方法，同时可保持系统完整性，并支持使用基于 CA 的信任链来验证软件更新来源。

5.1 文件捆绑包保护

文件捆绑包保护是由 SimpleLink 器件提供的方法，用于在更新文件集合（也被称为文件捆绑包）时保持系统完整性。捆绑包支持对整个集合进行更新，也支持回滚到之前的版本。因此，避免中间发生混淆。

5.1.1 文件捆绑包更新流程

捆绑包中的所有文件必须创建为 FAILSAFE。任何特定时间点都只能更新单个捆绑包。

1. 在设有捆绑包标志的捆绑包中写入每个文件的新版本，即可启动更新程序。
2. 重启器件。
3. 发生故障时，捆绑包可回滚到之前的版本，以示其拒绝更新。在这种情况下，所有文件都恢复为之前的内容。

捆绑包文件的更新过程具有故障安全特性，如果在此过程中发生意外重置，则视为捆绑包更新程序中止。因此，会触发自动回滚，捆绑包所有文件都会恢复为其之前的副本。

文件捆绑包更新过程中可创建新文件。如果捆绑包回滚，新文件会被删除。

5.2 安全内容交付

安全内容交付功能可在应用层提供另一级别的安全性，支持将机密内容交换给器件。该内容由器件解密，并且在此过程中并没有任何实体提供解密方法。此功能在无线 (OTA) 更新等情况下非常实用。安全内容交付方便用户对由远程器件加密并在 NWP 内快速解密的内容进行编程，而用于此过程的私有密钥保持在 SimpleLink 网络子系统中不可访问，并且不可通过主机访问。如果在应用层应用该功能，则支持通过非安全通道将文件传输到系统中。

5.2.1 过程描述

安全内容交付功能的过程描述如下：

1. 使用 NetUtils API 生成密钥对。
2. 检索临时的 ECC 公共密钥。
3. 将公共密钥发送至应用远程服务器。
4. 接收经过加密的文件。
5. 打开具有特殊标志的新文件，该标志指示将写入安全内容交付。
6. 随后写入经过加密的文件内容。
7. 关闭文件。

在此过程结束时，将文件保存到 SFLASH 中，然后使用不同于接收过程的密钥和方法来将文件加密为常规安全文件。

图 5-1 显示了安全内容交付过程。

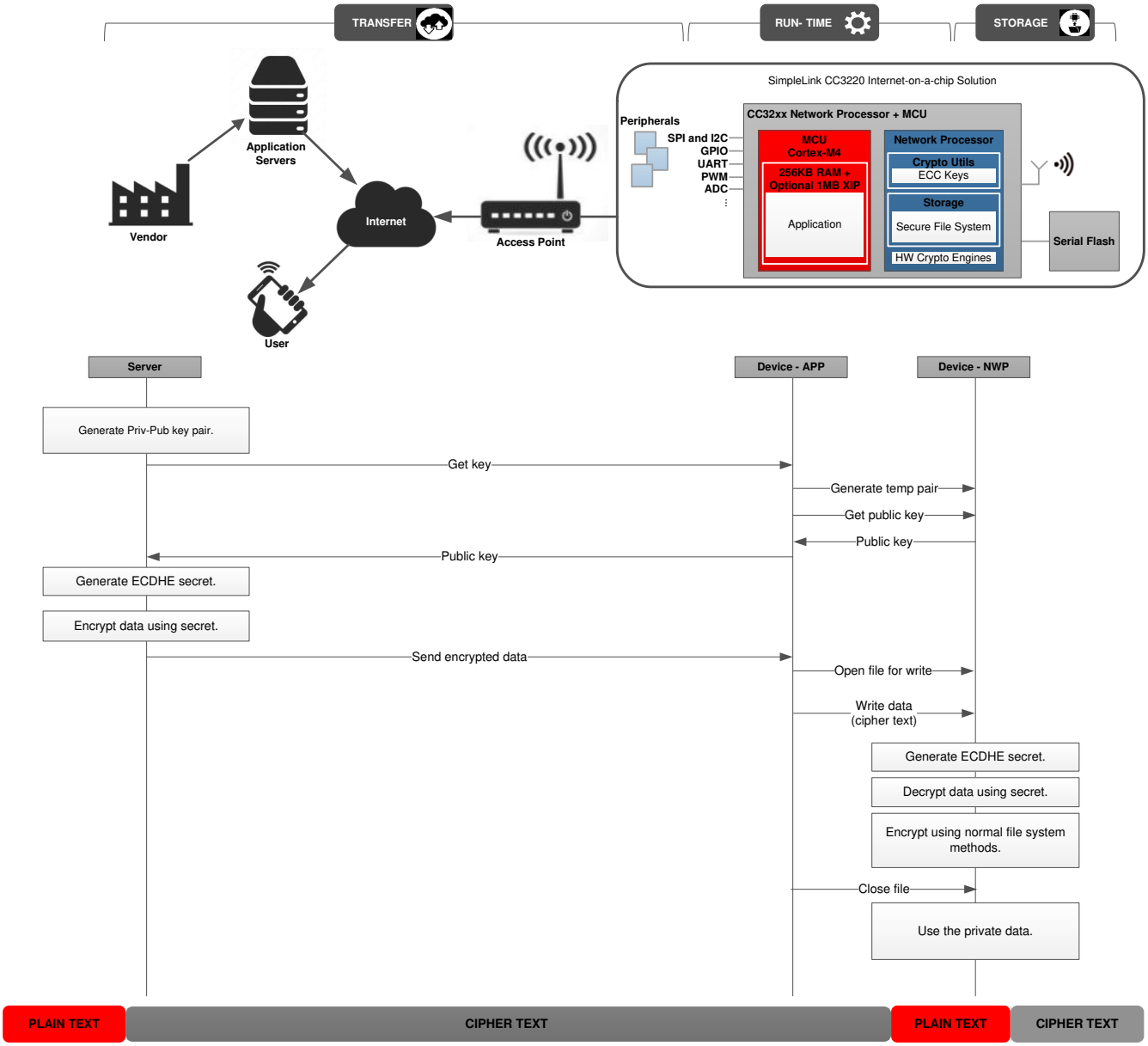

图 5-1. 安全内容交付 - 过程描述

5.2.2 经过加密的文件格式

此流程交付的文件应具有特殊格式。图 5-2 显示了此格式。

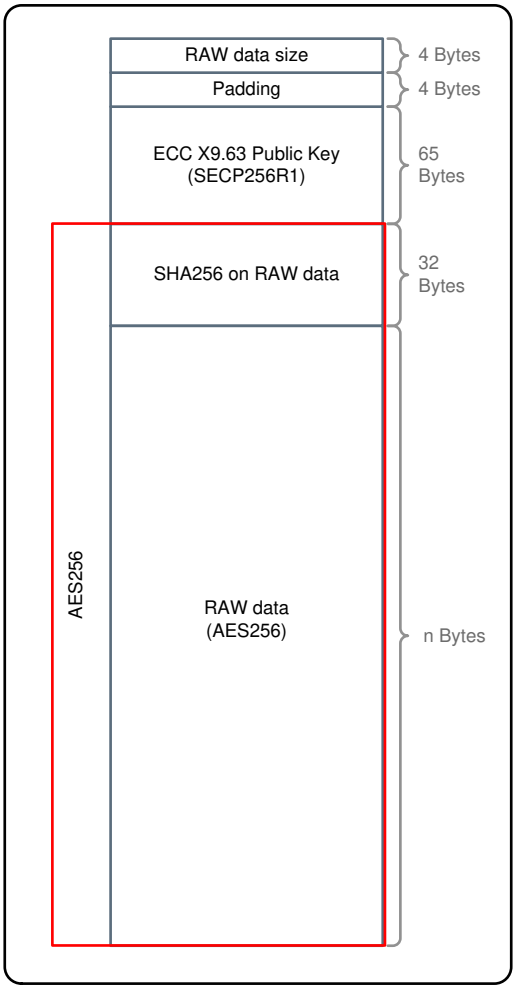

图 5-2. 安全内容交付 - 文件格式

5.2.3 更多详细信息

- 来自网络子系统的临时 ECC 密钥并非持久有效。启动新的过程时，当前临时密钥就会失效，SimpleLink 器件随即重新启动，或者主机会请求新的密钥。密钥被清除后，就无法恢复，并且不允许使用该密钥的内容。
- ECC 密钥遵循 SECP256R1 命名曲线。
- AES 密钥使用 ECDHE 算法通过 NWP 公共密钥和编码器私有密钥生成。
- 加密后的文件应按顺序执行写操作，不会出现写入偏移（写 API 中的偏移字段会被忽略）。

6 应用层安全性

6.1 安全密钥存储

SimpleLink 器件支持外部闪存上的非对称密钥对存储，同时内置加密加速和加密服务，以帮助执行一些与加密相关的常规操作。

这些加密服务提供的机制最多可管理八个 ECC 密钥对，并使用它们对数据缓冲区进行签名或验证。与其他功能相同，该功能也可用于认证器件身份。

受支持的密钥对有三种类型：

- 器件独有密钥对：器件的单个 256 位唯一密钥，嵌入在硬件中
- 临时密钥对：在请求时使用内部 TRNG 引擎创建
- 已安装的密钥对：由供应商安装和维护

系统密钥存储包含八个带索引的密钥对。

索引 0 被保留用于基于硬件的器件唯一密钥对。索引 1 至 7 根据应用需求用于临时或已安装的密钥对。

所有密钥均为遵循 SECP256R1 命名曲线的 ECC 密钥。

对于所有密钥对，私有密钥都不公开，只能在用于签名和解密操作时才能间接使用。公共密钥可由主机应用程序检索。

6.2 硬件加密引擎（仅限 CC3220/CC3230/CC3235x 器件）

SimpleLink CC3220/CC3230/CC3235x MCU 包含一组硬件加密引擎，可提高需要自定义或应用层面安全性的应用性能。这些引擎使得 Arm® Cortex®-M4 MCU 无需处理加密算法中所涉及的复杂耗时算术运算。

器件包括以下硬件加密引擎：

- 高级加密标准 (AES)
- 数据加密标准 (DES)
- 安全哈希算法/消息摘要算法 (SHA/MD5)
- 循环冗余校验 (CRC)
- 真随机数发生器 (TRNG)

有关硬件加密引擎的更多信息，请参阅 CC3220 SimpleLink™ Wi-Fi 和物联网技术参考手册或 SimpleLink Wi-Fi CC323x 技术参考手册。

6.2.1 高级加密标准 (AES)

AES 模块可基于二进制密钥提供硬件加速加密和解密操作。AES 是一种用于加密和解密的分组密码模块，支持 128 位、192 位和 256 位密钥。

该模块支持以下 AES 功能：

- 基本 AES 加密和解密操作
- 密钥大小：128、192 和 256 位
- 硬件中的密钥调度
- 反馈模式：
  - 电子源码书模式 (ECB)
  - 密码块链接 (CBC)
  - 计数器模式 (CTR)
  - 密码反馈模式 (CFB)，128 位
  - F8 模式
- AES-XTS
- AES-GCM（使用 AES-CTR 模式和 GHASH）
- AES-CCM（使用 AES-CTR 模式和 AES-CBC-MAC）
- 仅身份验证模式 CBC-MAC，f9
- 基本 GHASH 操作（选择不加密）

6.2.2 数据加密标准 (DES)

DES 模块可提供硬件加速的数据加密和解密功能。DES 可运行单一 DES 算法或三重 DES（TDES 或 3DES）算法。

DES 算法可生成基于纯文本块和加密文本块工作的分组密码。DES 的块大小为 8 字节（64 位）。DES 密钥包含 64 位二进制数字，但实际只有 56 位直接用于算法。其他 8 位可用于错误检测。

三重 DES 是指 DES 连续使用三次，使用三个密钥，因此密钥长度实际上为 168 位。每个三重 DES 加密或解密操作都是由一组 DES 加密和解密操作构成。

DES 加速器包括以下主要特性：

- DES 加密和解密
- 三重 DES（即 3DES）加密和解密
- 反馈模式：ECB、CBC、CFB

6.2.3 安全哈希算法/消息摘要算法 (SHA/MD5)

SHA/MD5 是一款用于哈希和消息认证的硬件加密加速器。

此模块可运行以下算法：

- MD5 消息摘要算法
- SHA-1 算法
- SHA-2（SHA-224 和 SHA-256）
- 使用 MD5、SHA-1 和 SHA-2 的哈希运算消息认证码 (HMAC) 操作

该算法生成消息或数据文件的精简集，即摘要或签名，可将其用于验证消息完整性。

- MD5 哈希算法
- SHA-1、SHA-224 或 SHA-256 哈希算法
- 对不超过 64 字节的 HMAC 密钥，执行自动 HMAC 密钥预处理
- 对超过 64 字节的 HMAC 密钥，在主机辅助下执行 HMAC 密钥预处理

6.2.4 循环冗余校验 (CRC)

CRC 是常用于数据传输和安全系统检查的错误检测码，同样还可以与 AES 和 DES 结合使用。

CRC 模块支持以下功能：

- 支持主要的 CRC 多项式
  - CRC-16-IBM
  - CRC-16-CCITT
  - CRC-32
  - CRC-32C
  - TCP 校验和
- 支持半字和字节交换
- 允许字节和字馈入

6.2.5 真随机数生成器

TRNG 是一款物理随机数生成器，用于生成真正的随机数。它可由主机使用以生成密钥，也可由需要真正随机数的任何其他应用程序使用。

7 运行时二进制保护

SimpleLink CC3220S、CC3220SF、CC3230S、CC3230SF、CC3235S 和 CC3235SF 器件提供多种措施，通过利用文件系统的安全功能来实现主机应用程序运行时二进制保护。

7.1 CC3220S/CC3230S/CC3235S 器件

在 SimpleLink CC3220S/CC3230S/CC3235S 器件上，应用程序运行时二进制文件存储在外部串行闪存上。该文件在启动时加载至内部 SRAM 并从此处执行。

该文件在文件系统中作为安全文件存储，具有公共写权限和失效防护属性集。因此，安全文件的所有属性对该文件均适用。其中包括加密和真实性检查。

真实性是基于受信任根证书目录来实现的，并在编程过程中进行验证。如果映像的签名无效，则表示编程失败。

7.2 CC3220SF/CC3230SF/CC3235SF 器件

在 SimpleLink CC3220SF/CC3230SF/CC3235SF 器件上，应用程序运行时二进制文件可存储在片上闪存上并直接从此处执行（与 XIP 相同）。该器件在内部管理片上闪存，并禁止外部直接访问，除非应用开发模式。

在编程过程中，首先会将映像下载到串行闪存中（以预定义文件名另存为 /sys/mcuflashimg.bin），并在此处对其进行签名和加密。首次启动时，启动加载程序会从串行闪存读取加密后的映像，然后对其解密并写入片上闪存。

为确保整个映像的完整性，会生成散列的应用程序二进制文件并将其存储在文件系统中（以安全系统文件形式）。该散列在启动期间使用，用于验证存储在片上闪存中的映像是否对应于正确编程的映像。该散列可将片上闪存中的映像与串行闪存内容链接起来。将映像复制到片上闪存后，对串行闪存的更改可基于该散列进行检测，并视为篡改尝试。在这种情况下，会擦除片上闪存。

该器件支持最大 1022KB 的运行时二进制文件。必须将应用程序二进制文件连同签名一同提供给映像创建工具。真实性基于证书存储功能实现，并在编程过程中进行验证。如果映像的签名无效，则表示编程失败。

图 7-1 简要介绍了在 CC3220SF/CC3230SF/CC3235SF 器件中将映像从串行闪存传输到片上闪存的过程。

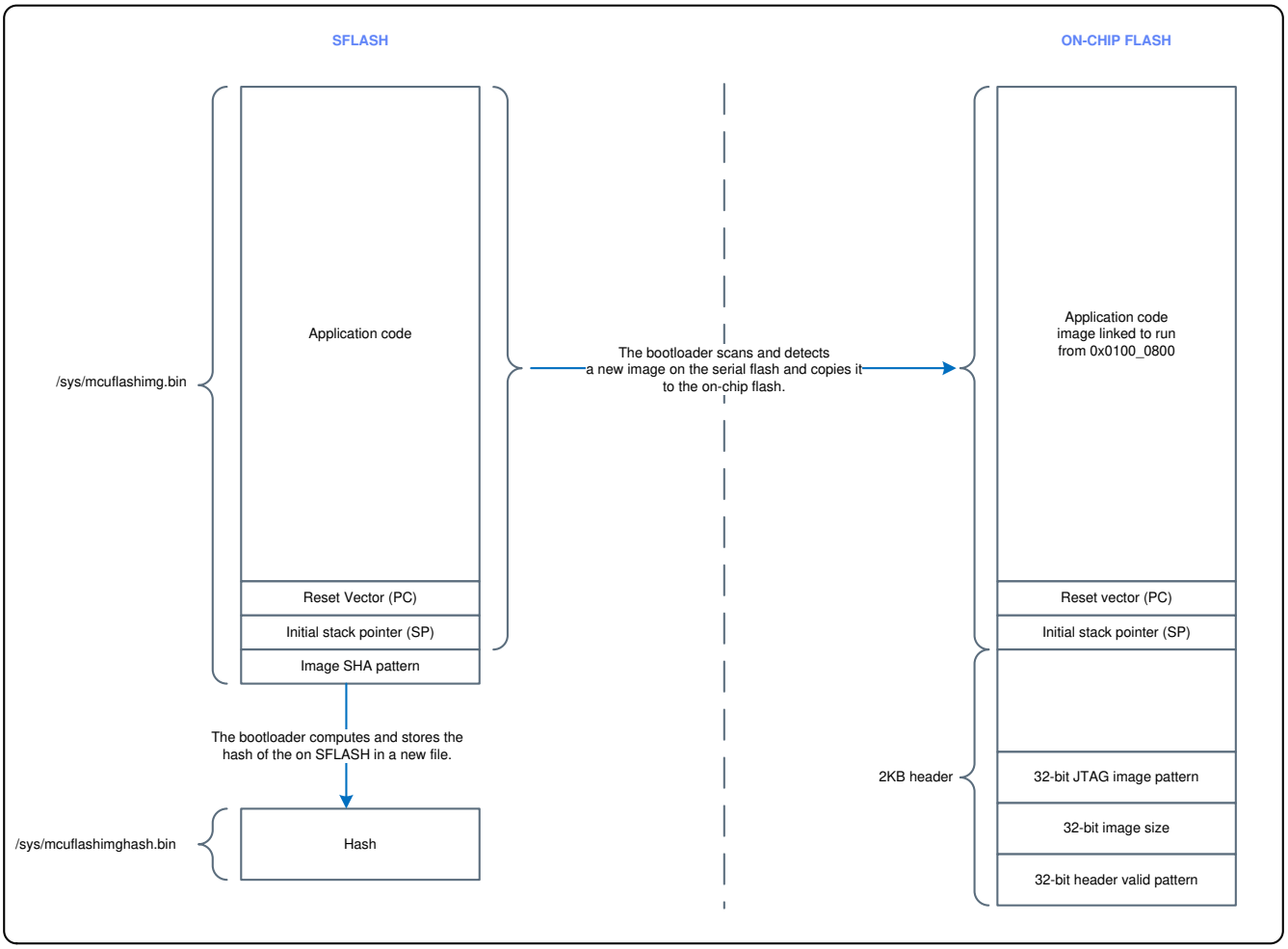

图 7-1. 片上闪存编程和更新

8 安全性设计

8.1 结束语

因特网连接通常只有在使用正确的网络配置或防火墙时才视为受到保护。这种假设是错误的，并且与现实不符。问题在于，即使网络配置或防火墙阻止访问网络级的器件，或者封锁某些协议和端口，因特网连接仍然面临一些应用级缺陷（例如，通过探查穿过防火墙和配置页面的通信流量等手段）。

如果指令不够清晰明确，或者网络中的其他器件需要较为宽松的安全设置，仅靠基于防火墙或安装策略进行保护会导致出现安全漏洞。

在物联网领域，仅基于这些策略进行保护时，保护效果更差，因为大多数设备都是由非专业的终端用户执行安装。这并不意味着该网络不需要配置，但确实不能仅依靠这种保护策略，还必须在其他层进行其他设计。

最近几年，情况变得日益严峻，因为这类设备大多数都支持远程软件更新（通用术语：OTA 更新）。这种更新不仅威胁到要更新的特定设备，还会造成恶意用户接入局域网。当攻击者成功更换支持因特网的设备中的软件时（即使该设备的隐私性和安全性看起来并不关键），攻击者还能够接入局域网，进而访问局域网中的其他设备。我们应将这种攻击视为局域网安全性评估的一部分。

人们普遍认为局域网连接是安全的：只有许可设备或用户才能连入网络，并且与因特网之间存在网络边界。实际上，LAN 的主要缺陷就是网络安全配置不佳。Wi-Fi 网络在家庭用户和企业用户间广泛使用，更恶化了网络安全配置不佳的局面，因为它们允许任何人接入局域网，并且无需与家中或办公室内的网络插口建立物理连接。对恶意用户而言，唯一要求是与此网络区域保持合理的距离（数十米）。

LAN 可提供对所连设备、端口和协议的访问（这通常都是 WAN 或因特网所阻止的），从而提供更多暴露点。安全的网络应用应考虑所有这些缺陷，并通过其他层的安全性缓解这些风险。

一般而言，OTA 应用的整个固件更新过程不包括在此文档范围内，必须由 OEM 定义。不过，TI 强烈建议主机应用支持以下功能，从而验证软件更新来源：

- 验证 OTA 服务器的域名。
- 对 OTA 服务器进行身份验证。
- 使用安全通道（如 SSL/TLS 等）进行内容交付。

总之，TI 建议执行以下安全性最佳设计实践：

1. 识别资产。
2. 识别可能的缺陷。
3. 保护必须保护的内容。
4. 仅使用众所周知的安全实践。
5. 禁用所有未使用的服务和功能（例如，HTTP 服务器）

修订历史记录

注：以前版本的页码可能与当前版本的页码不同

Changes from Revision B (May 2018) to Revision C (September 2020) **Page**

- 更改了文档标题和整个文档以包括 CC3230 器件 3
- 更改了表 1-2 *主要安全功能* 中“个人和企业 Wi-Fi 安全性”和“克隆保护”这几行的描述 6
- 更改了表 2-1 “*Wi-Fi 安全性*”中“个人”一行中的 AES 条目 9
- 更改了 节 3.1 “*概述*”中的“克隆保护”列表项 17
- 更改了 节 3.2.2 “*克隆保护*”中的第一句话 18

重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265