基于 Arm 上的安全启动和安全固件更新概述® TrustZone® STM32L5 系列微控制器

引言

本应用笔记描述如何在基于 Arm® Cortex®-M33 处理器的 Arm® TrustZone® STM32 微控制器上获得安全启动和安全固件更新解决方案。该应用笔记还提供此解决方案与 X-CUBE-SBSFU 解决方案的顶层比较结果，后者适用于基于 Arm® Cortex®-M0、Cortex®-M3、Cortex®-M4、或 Cortex®-M7 处理器的非 TrustZone®STM32 微控制器。它还为安全启动和安全固件更新解决方案提供顶层集成指南。

对于 Arm® TrustZone® STM32 微控制器，安全启动和安全固件更新解决方案在相应的 STM32Cube MCU 包中提供。与 X-CUBE-SBSFU STM32Cube 扩展包中提出的解决方案不同，该解决方案基于开源 TF-M（面向 Arm® Cortex®-M 的可信固件）参考实现。

本应用笔记适用于所有 TrustZone® STM32 微控制器。然而，本文档中仅将 STM32L5 系列作为示例。

如需关于开源 TF-M 参考实现的详细信息，请参见[TF-M]。

1 概述

在本应用笔记中，术语 *X-CUBE-SBSFU* 指的是 X-CUBE-SBSFU STM32Cube 扩展包中可用的安全启动和安全固件更新解决方案，而术语 *SBSFU* 指的是 STM32Cube MCU 包中可用的安全启动和安全固件更新解决方案（STM32CubeL5 用作示例）。

表 1 给出了相关的缩略语定义，帮助您更好地理解本文档。

表 1. 缩略语列表

缩略语	定义
AEAD	带关联数据的认证加密。
AES	高级加密标准。
CBC	AES 密码块链接。
EAT	实体认证令牌。
ECDSA	椭圆曲线数字签名算法。
GCM	AES Galois/计数器模式。
HDP	隐藏保护。
HUK	硬件唯一密钥。
ITS	内部可信存储。
KMS	密钥管理服务。
MAC	消息认证码。
MPU	存储器保护单元。
OEM	原始设备制造商。
OTFDEC	实时解密。
PKCS	公钥加密标准。
PSA	平台安全架构。设备安全框架。
RDP	读保护。
RoT	信任根。
RSA	Rivest–Shamir–Adleman 算法。
SBSFU	安全启动和安全固件更新.
SESIP	物联网平台安全评估标准。
SST	安全存储。
TBSA-M	面向 Arm® Cortex®-M 的可信基础系统架构。
TF-M	面向 M-级 Arm®处理器的可信固件。 TF-M 为 Armv8-M 提供安全世界软件的参考实现。
TZ	TrustZone®.
WRP	写保护。

提示 *Arm 和 TrustZone 是 Arm Limited（或其子公司）在美国和或其他地区的注册商标。*

2 参考

下面的表 2 和表 3 中提供的资源是公开的，可以从意法半导体的网站 *www.st.com* 或第三方网站上获得。

表 2. 参考文档

参考	文档
[AN5156]	应用笔记(1)： *STM32 微控制器安全简介.*
[UM2262]	用户手册(1)： *X-CUBE-SBSFU STM32Cube 扩展包入门.*
[UM2671]	用户手册(1)： *STM32CubeL5 TFM 应用程序入门.*
[TFM 用户指南]	TF-M 用户指南面向 v1.0-RC2： https://ci.trustedfirmware.org/job/tf-m-build-test-nightly/lastSuccessfulBuild/artifact/build-docs/tf-m_documents/install/doc/user_guide/html/index.html(2)
[PSA_API]	PSA 开发人员 API： //developer.arm.com/architectures/security-architectures/platform-security-architecture#implement(2)

1. *在 www.st.com 上提供。如需详细信息，请与意法半导体联系。*
2. *该 URL 属于第三方。它在文档发布时处于活动状态，但意法半导体对 URL 或参考材料的任何变更、转移或停用不承担责任。*

表 3. 开源软件资源

参考	开源软件资源
[TF-M]	TF-M （可信固件-M）Arm Limited 驱动开源软件框架： www.trustedfirmware.org/(1)
[MCUboot]	MCUboot 开源软件： juullabs-oss.github.io/mcuboot/(1)
[MbedCrypto]	MbedCrypto 开源软件： github.com/ARMmbed/mbed-crypto(1)
[Mbed TLS]	Mbed™ TLS 开源网站： tls.mbed.org/(1)
[PSA]	PSA 认证网站： www.psacertified.org(1)

1. *该 URL 属于第三方。它在文档发布时处于活动状态，但意法半导体对 URL 或参考材料的任何变更、转移或停用不承担责任。*

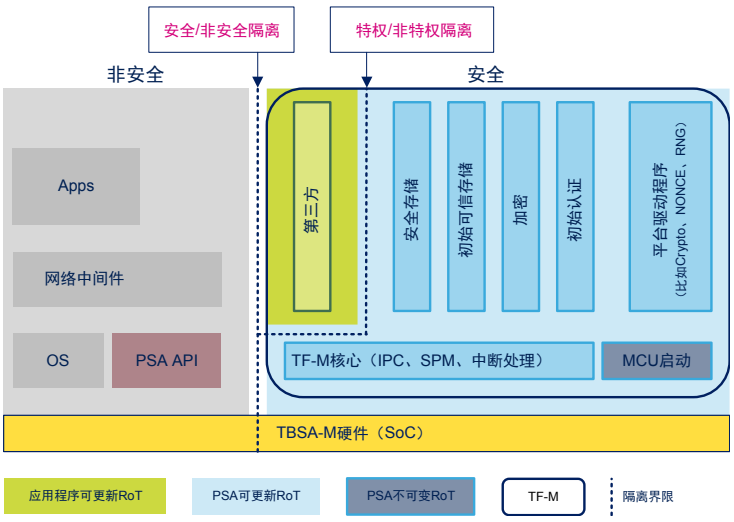
提示 *Mbed 是 Arm Limited（或其子公司）在美国和或其他地区的商标。*

3 Arm® 可信固件-M （TF-M）简介

TF-M （参照[TF-M]）是 Arm Limited 驱动的开源软件框架，在 Arm® Cortex®-M33 (TrustZone®)处理器上提供了 PSA 标准的参考实现：

- PSA 不可变 RoT（信任根）：在任何复位后执行的不可变“*安全启动和安全固件更新*”应用程序。该应用程序基于 MCUboot 开源软件（参照[MCUboot]）。
- PSA 可更新 RoT：“*安全*”应用程序实现了一组隔离在安全/特权环境中的安全服务，非安全应用程序可以通过 PSA API 在非安全应用程序运行时期中调用这些服务（参照[PSA_API]）：
  - 安全存储服务：TF-M 安全存储（SST）服务实现 PSA 保护的存储 API，允许数据加密并将结果写入可能不可信的存储中。SST 服务采用基于 AEAD 加密策略的 AES-GCM 作为参考，保护数据的完整性和真实性。
  - 内部可信存储服务：TF-M 内部可信存储（ITS）服务实现 PSA 内部可信存储 API，允许在微控制器内置的闪存区域中写入数据，该区域将通过硬件安全保护机制与非安全或非特权应用程序隔离。
  - 加密服务：TF-M 加密服务实现了 PSA 加密 API，允许应用程序使用加密原语，如对称和非对称密码、散列、信息验证码（MAC）和带关联数据的认证加密（AEAD）。它基于 MbedCrypto 开源软件（参照[MbedCrypto]）。
  - 初始认证服务：TF-M 初始认证服务允许应用程序在验证过程中向验证实体证明设备身份。初始认证服务可以根据请求创建一个令牌，其中包含特定于设备的固定数据集。
- 应用程序可更新 RoT：隔离在安全/非特权环境中的第三方安全服务，可以由非安全应用程序在非安全应用程序运行时期中调用。

图 1. TF-M 概述



4 X-CUBE-SBSFU vs. TF-M 对比

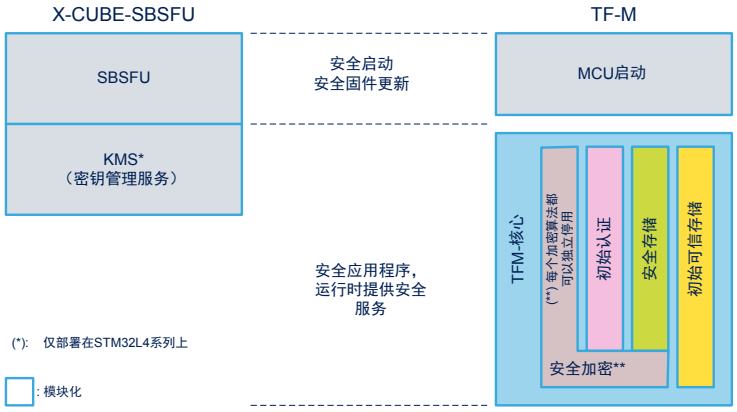
4.1 概述

X-CUBE-SBSFU 提供意法半导体的安全启动和安全固件更新实现，以及（仅有选择地面向部分 STM32 系列）应用程序在运行时期可用的安全 KMS（密钥管理服务）服务。

TF-M 参考实现提供基于开源 MCU 启动的安全启动和安全固件更新服务，以及应用程序在运行时期可用的一组安全服务。

X-CUBE-SBSFU 和 TF-M 之间的高层比较请参见图 2

图 2. *X-CUBE-SBSFU* vs. TF-M 概述



TF-M 的 MCU 启动部分好比 *X-CUBE-SBSFU*（无 KMS）：提供类似的服务。

X-CUBE-SBSFU KMS 支持的服务类似于 TF-M 安全加密服务，但是加密算法或特性不一样；即使两者都基于不透明密钥 API 概念，API 也是不同的。请参考相关用户手册（[UM2262]和[UM2671]）中引用的 X-CUBE-SBSFU 和 TF-M API 文档，获取与所支持的特性有关的详细信息。

4.2 顶层特性

即使 *X-CUBE-SBSFU* 和 TF-M 提出类似的服务，两种解决方案的特性也不完全相同。 表 4 总结了 X-CUBE-SBSFUV2.3.0 中的 *X-CUBE-SBSFU* 和 STM32CubeL5 V1.2.0 中基于 TF-M 的应用程序之间的不同。

表 4. *X-CUBE-SBSFU* vs. TF-M 顶层特性

安全话题	X-CUBE-SBSFU V2.3.0 中的 *X-CUBE-SBSFU* (1)	STM32CubeL5 V1.2.0 中的 TF-M(1)
SBSFU	1 个或 2 个镜像插槽。 新镜像通过本地加载器或 USER APP。	仅 2 个镜像插槽。 新镜像通过 USER APP。
	单一固件映像。 完全或部分更新。	单一固件镜像或多个(2)固件镜像（安全与非安全）。 仅完全更新。
	对称加密方案。 非对称加密方案，带或不带固件加密。	非对称加密方案，不带固件加密。
运行时期 安全服务	安全服务 • 1 层隔离 • 中断不受管理 • 主加密服务（仅限 STM32L4 系列）	安全服务 • 2 层隔离 • 非安全中断受管理 • 完整加密服务（纯软件或软件与硬件混合） • 初始认证 • 安全存储（数据加密/完整性） • 内部可信存储（数据完整性） • 架构已准备好集成非特权应用服务
验证	安全评估。	PSA L2 认证。

1. *不同之处用粗体突出显示。*

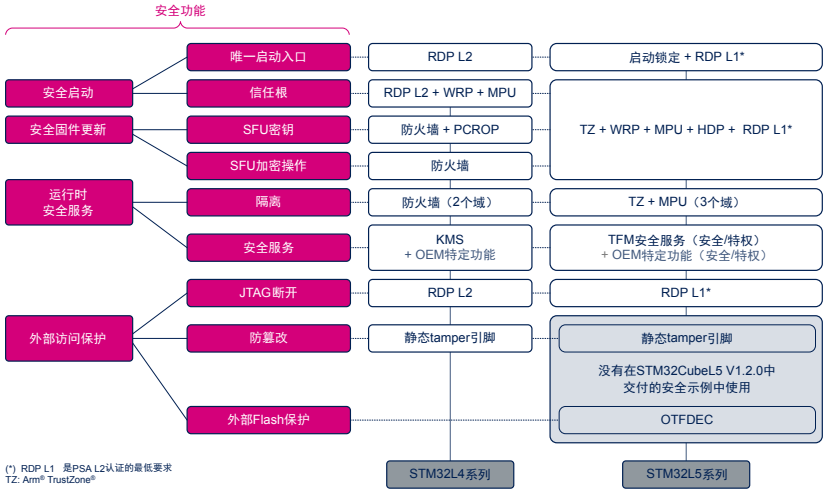
要了解最新的特性差异，请参照最新版本的 X-CUBE-SBSFU 扩展包和 STM32CubeL5 MCU 软件包（ 可从 *www.st.com* 上的各自产品页面获得）。

有关 TF-M 特性的更多信息，请参见[UM2671]。

4.3 硬件安全

STM32CubeL5 中基于 TF-M 的应用程序的安全策略依赖 TrustZone®和 STM32L5 系列硬件安全特性。图 3 显示该安全策略与 X-CUBE-SBSFU 中 *X-CUBE-SBSFU* 安全策略的对比（以 STM32L4 系列为例）。

图 3. *X-CUBE-SBSFU*（STM32L4 系列）和 TF-M（STM32L5 系列）安全策略概述



关于带 TF-M 的安全策略的更多细节，请参阅[UM2671]。

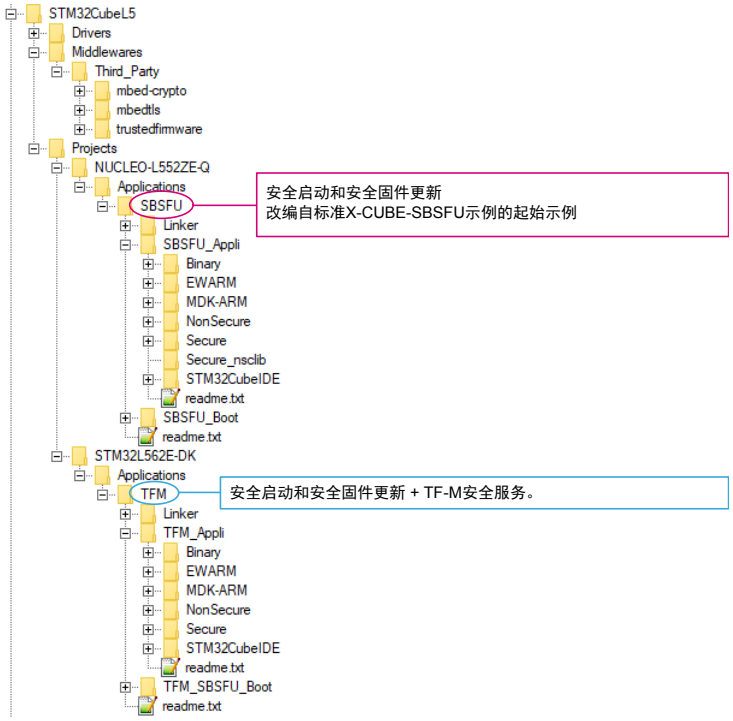
5 STM32CubeL5 基于 TF-M 的应用

STM32CubeL5 MCU 软件包基于 TF-M 参考实现提出两种不同应用，可移植到 STM32L5 系列以利用硬件安全特性的好处。

- *SBSFU*：它包括“*安全启动和安全固件更新*”应用程序（名为 `SBSFU_Boot`）简单用户应用程序示例（名为 `SBSFU_Appli`）。
- TFM：它包括“*安全启动和安全固件更新*”应用程序（`TFM_SBSFU_Boot`）和在运行时期提供 TFM 安全服务的用户应用程序（名为 `TFM_Appli`）。

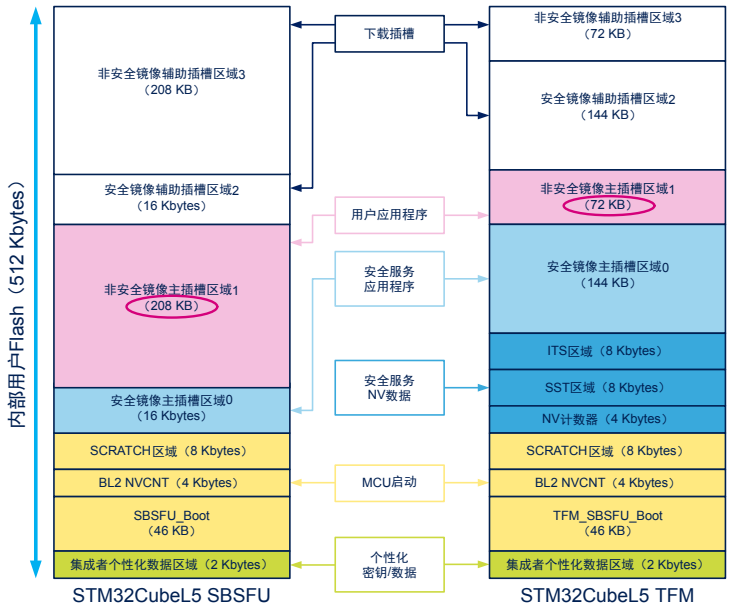
建议使用不带 KMS 的 *X-CUBE-SBSFU* 的用户考虑迁移到 STM32L5 系列并使用 STM32CubeL5 *SBSFU* 应用程序。建议使用带 KMS 的 *X-CUBE-SBSFU* 的用户考虑迁移到 STM32L5 系列 并使用 STM32CubeL5 TFM 应用程序（可能会删除一些安全服务或加密算法以满足应用程序需要）。

图 4. STM32CubeL5 基于 TF-M 的应用



通过移除运行时期的 TF-M 安全服务，STM32CubeL5 *SBSFU* 应用程序为可用于用户应用程序的闪存容量最大化，如图 5 中所示。

图 5. STM32CubeL5 基于 TF-M 的应用内存占用



如需关于内存映射的详细信息，请参阅[UM2671]中的*内存布局*一节。

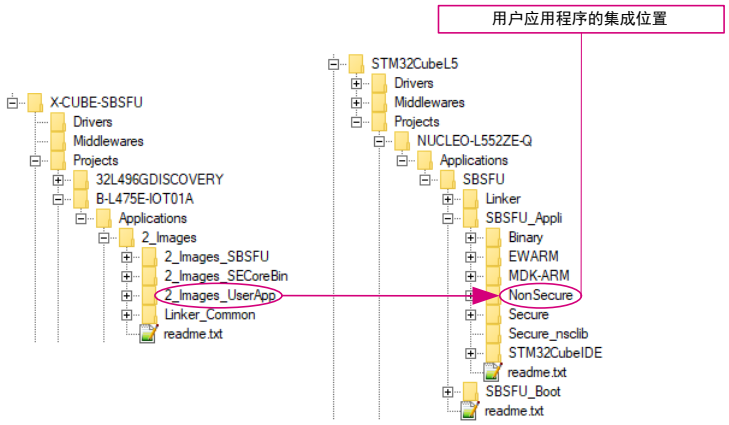
6 STM32CubeL5 *SBSFU* 应用

6.1 用户应用程序集成

当将 *X-CUBE-SBSFU* 应用程序移植到 STM32CubeL5 *SBSFU* 时， 用户应用程序必须集成到 `SBSFU/SBSFU_Appli/NonSecure` 文件夹中，如图 6 中所示。

此文件夹包含一个简单的用户应用程序示例。

图 6. 用户应用程序集成

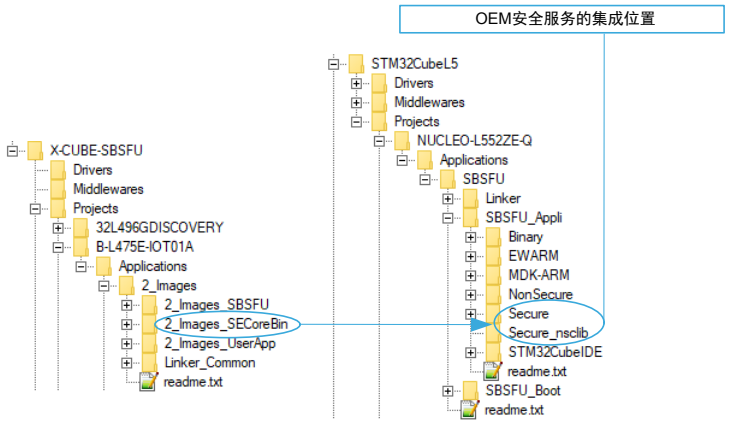


6.2 OEM 安全服务集成

如果 OEM 自己的安全服务也在 X-CUBE-SBSFU 中实现，这些 OEM 安全服务必须集成到 `SBSFU/SBSFU_Appli/Secure` 和 `SBSFU/SBSFU_Appli/Secure_nsclib` 文件夹中， 参照图 7 中所示的 STM32CubeL5 TrustZone® HAL 示例。

这些文件夹包含一个简单的 OEM 安全服务示例：*“安全 GPIO 翻转”*。

图 7. OEM 安全服务集成（*SBSFU*）



6.3 密钥个性化

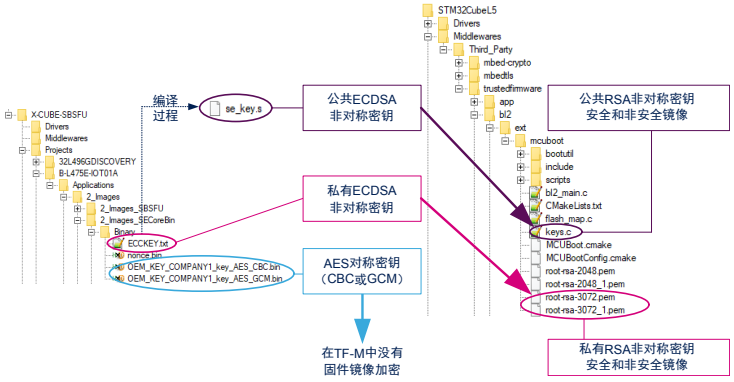
在 *X-CUBE-SBSFU* 中，个性化数据是加密密钥：

- AES 对称密钥（CBC 或 GCM）：用于固件镜像加密
- ECDSA 非对称密钥：用于固件镜像签名

SBSFU STM32CubeL5 V1.2.0 中不支持固件加密。没有可个性化的 AES 对称密钥。

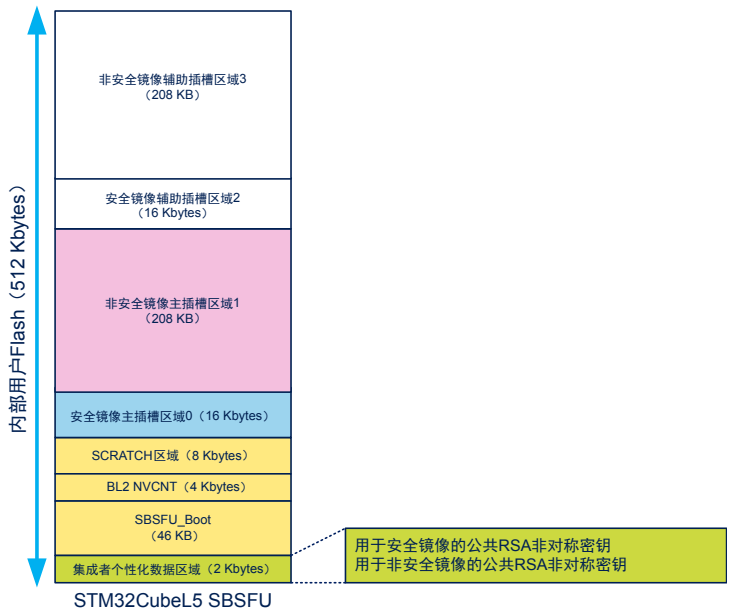
关于固件镜像签名，*SBSFU* 示例中有两个 RSA 非对称密钥（一个用于安全镜像，一个用于非安全镜像）可进行个性化，而 *X-CUBE-SBSFU* 中只有一个 ECDSA 非对称密钥。必须注意的是，与 *X-CUBE-SBSFU* 相反，公共非对称密钥不是在 STM32CubeL5 *SBSFU* 编译过程中自动生成的，而是需要由用户将其与私有非对称密钥一起提供（参见图 8）。

图 8. 固件镜像密钥个性化



这两个私有 RSA 非对称密钥用于对安全和非安全固件镜像进行签名；它们没有内嵌在闪存中，而两个公共 RSA 非对称密钥存在于 `SBSFU_Boot` 项目的编译输出中。它们内嵌在专用的不可变 Flash 区域（个性化数据区域）中，如图 9 中所示。

图 9. 在 STM32CubeL5 *SBSFU* 中的集成者个性化数据区域



7 STM32CubeL5 TFM 应用

第 6 节 STM32CubeL5 SBSFU 应用中提供的顶层集成指南适用于 STM32CubeL5 TFM 应用。本节中提供特定于 STM32CubeL5 TFM 应用的额外顶层集成指南。

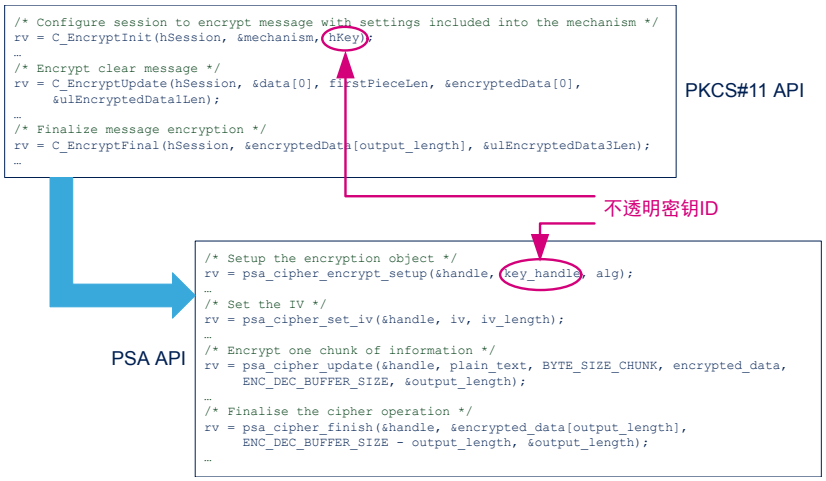
如需关于 STM32CubeL5 TFM 应用的更多信息，请参见[UM2671]。

7.1 运行时期的加密安全服务

在 *X-CUBE-SBSFU* 中，通过 PKCS#11 API 为用户应用程序提供 KMS 服务。在 STM32CubeL5 TFM 应用中，通过 PSA 加密 API 为用户应用程序提供安全加密服务。两者都基于不透明密钥 API 概念。

图 10 举例说明关于面向 AES 加密的 API 使用差异。

图 10. PSA API 迁移示例

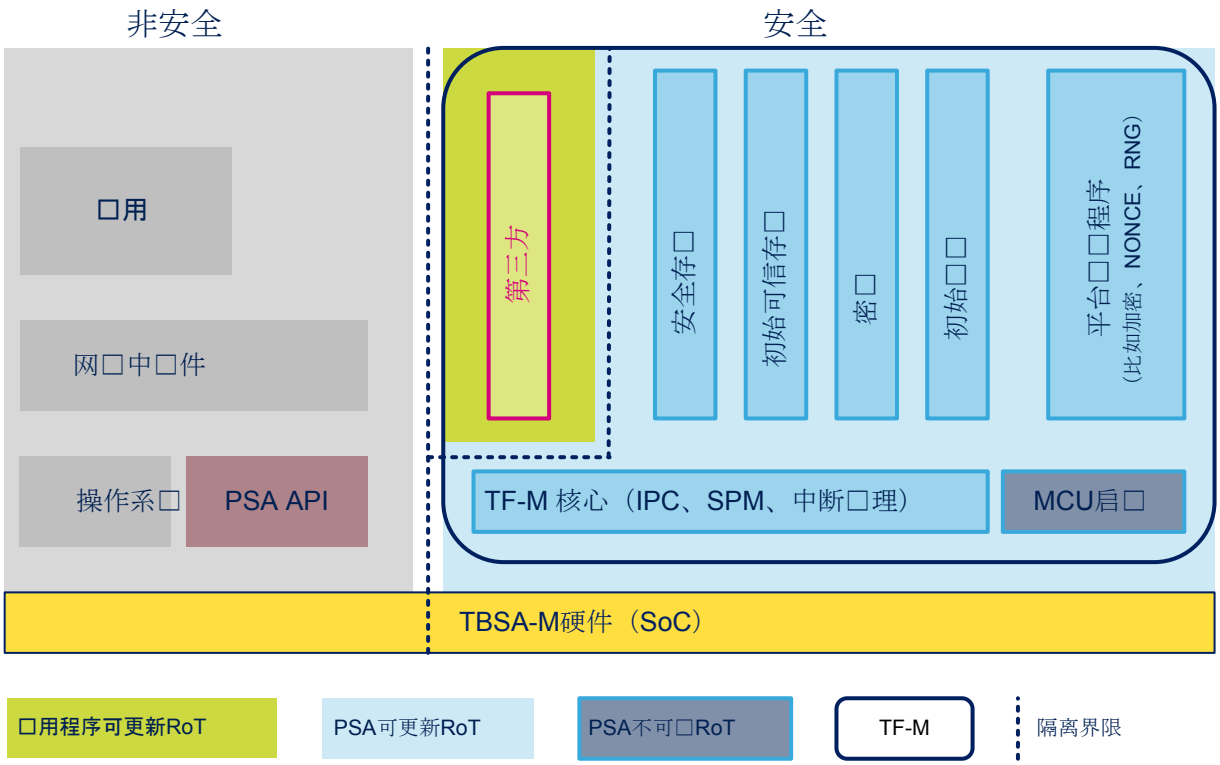


关于 PSA API 的更多信息，请参阅 TFM 用户应用程序示例和[PSA_API]。

7.2 OEM 安全服务集成

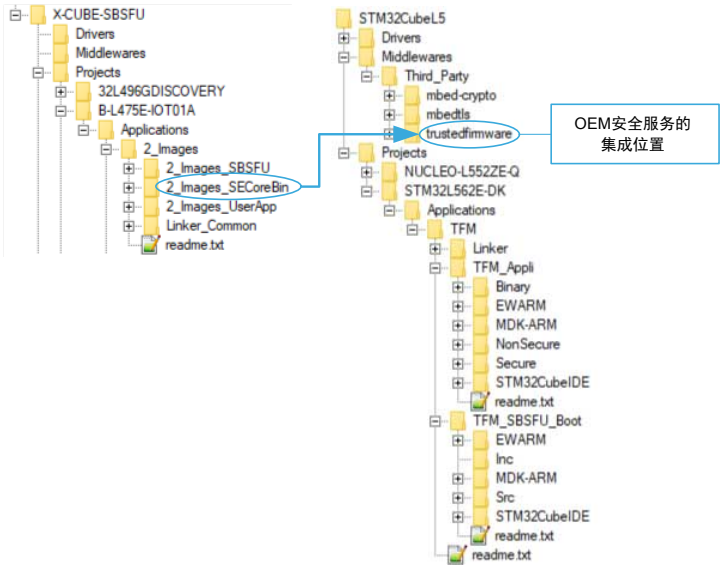
如图 11 中所示，OEM 安全服务必须集成为安全应用程序的安全/非特权部分中的第三方安全服务（称为“*来自 TFM 框架的应用程序 RoT*”）。关于“*来自 TFM 框架的应用程序 RoT*”，请参照[UM2671]。

图 11. TF-M 中的第三方安全服务



如图 12 中所示，这些服务必须集成在 `Middlewares/trustedfirmware` 文件夹中。关于更多信息，请参见[TFM 用户指南]。

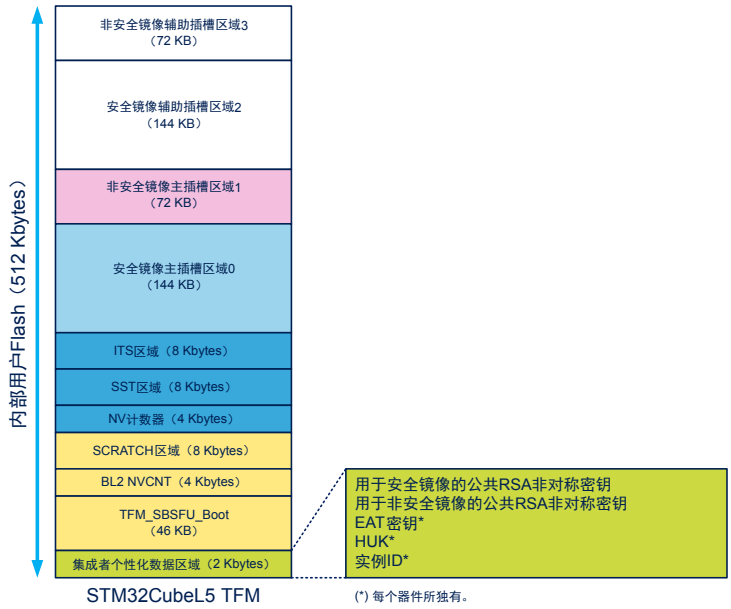
图 12. OEM 安全服务集成（TFM）



7.3 数据个性化

除了固件镜像身份验证密钥，TFM 应用程序的个性化还需要额外数据：EAT 密钥、HUK 和实例 ID。TF-M 初始认证服务需要这些数据。它们是特定于产品的（每个器件所独有的）。这些数据与公共 RSA 非对称密钥一起被分组在专用的不可变 Flash 区域（个性化数据区域）中，在激活最终安全配置之前，必须针对生产中的每个器件对该区域进行个性化设置。

图 13. 个性化数据区域



如需关于个性化数据的更多细节，请参阅[UM2671]中的*集成者角色描述*一节。

版本历史

表 5. 文档版本历史

日期	版本	变更
2020 年 2 月 20 日	1	初始版本。

目录

表一览

图一览