Arm® TrustZone® STM32 微控制器的安全启动和安全固件更新解决方案概述

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流程解决方案。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流程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流程解决方案在相应的 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（可信固件面向 Arm® Cortex®-M）参考实现。

本应用笔记适用于所有 TrustZone® STM32 微控制器（参考表 1）。然而，本文档中将 STM32L5 系列作为示例。

STM32Cube MCU 包中可用的基于 TF-M 的应用可能会不同，具体取决于 TrustZone®STM32 微控制器。参照公认的 Arm® TrustZone® STM32 微控制器（参见第 2 节 参考）的 TFM 应用（TF-M 的完整实现）的用户手册，获取对解决方案的精确描述。

如需关于开源 TF-M 参考实现的详细信息，请参见[TF-M]。

表 1. 适用产品

类型	产品系列
微控制器	STM32L5 系列, STM32U5 系列

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流程解决方案，而术语 *SBSFU* 指的是 Arm®TrustZone®STM32 微控制器 STM32Cube MCU 软件包中可用的安全启动和安全固件更新流程解决方案（STM32CubeL5 用作示例）。

表 2 给出了相关的缩略语定义，帮助您更好地理解本文档。

表 2. 缩略语列表

缩略语	定义
AEAD	关联数据的认证加密
AES	高级加密标准
CBC	AES 密码块链接
CTR	AES 计数器模式
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	动态解密
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	可信根
RSA	Rivest–Shamir–Adleman 算法
SBSFU	安全启动和安全固件更新流程
SST	安全存储服务。安全存储服务由 TBSA-M 提供 TF-M
TBSA-M	面向 Arm® Cortex®-M 的可信基础系统架构
TF-M	可信固件 面向 M-级 Arm®处理器。 TF-M 为 Armv8-M 提供安全世界软件的参考实现
TFM	基于 TF-M 的应用程序的名称，该程序具有以下完整功能 STM32Cube MCU 包
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 3 和表 4 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 3. 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.*
[UM2851]	用户手册(1)： *STM32CubeU5 TFM 应用程序入门.*
[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激活状态，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 4. 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 驱动的开源软件框架： www.trustedfirmware.org/(1)
[MCUboot]	MCUboot 开源 软件： mcuboot.com(1)
[mbed-crypto]	mbed-crypto 开源软件： github.com/ARMmbed/mbed-crypto(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激活状态，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。*

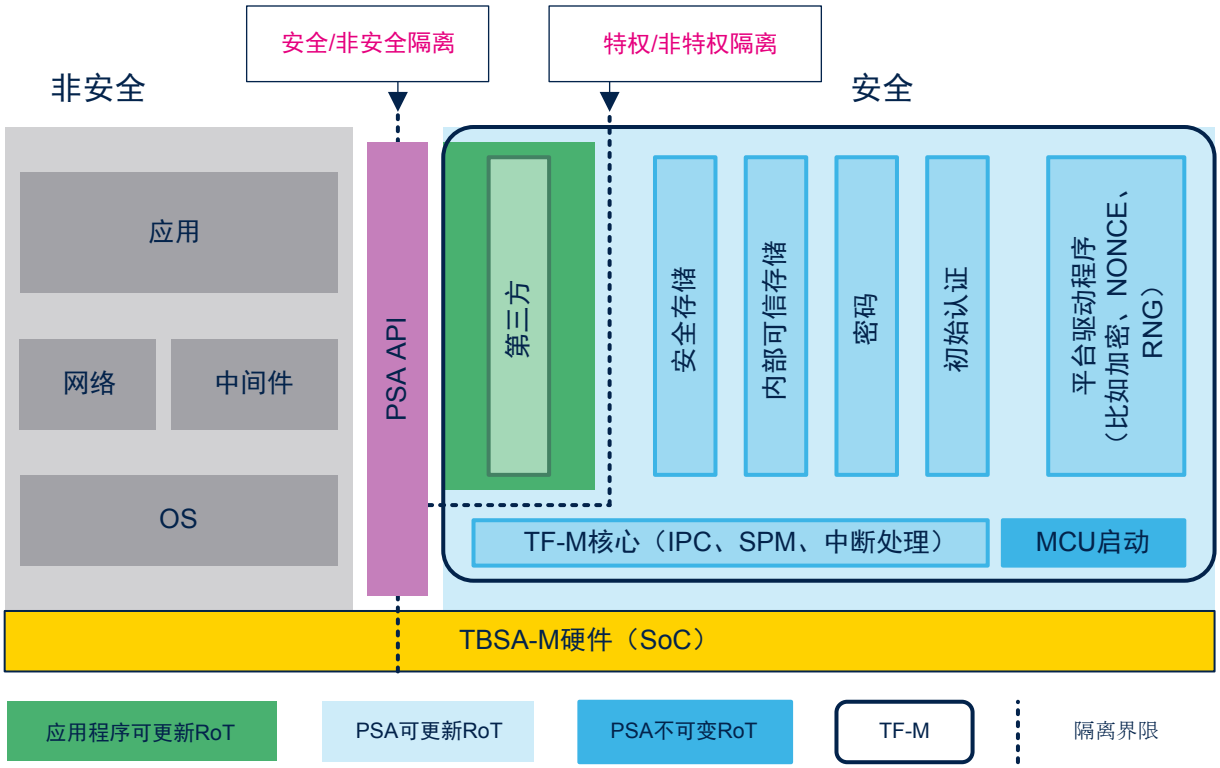
提示 *Mbed 是 Arm Limited（或其子公司）在美国和或其他地区的商标。*

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流程*”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，允许应用程序使用密码学原语，如对称和非对称密码、哈希、信息验证码（MAC）和带关联数据的认证加密（AEAD）。它基于 mbed-crypto 开源软件（参照[mbed-crypto]）。
  - 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

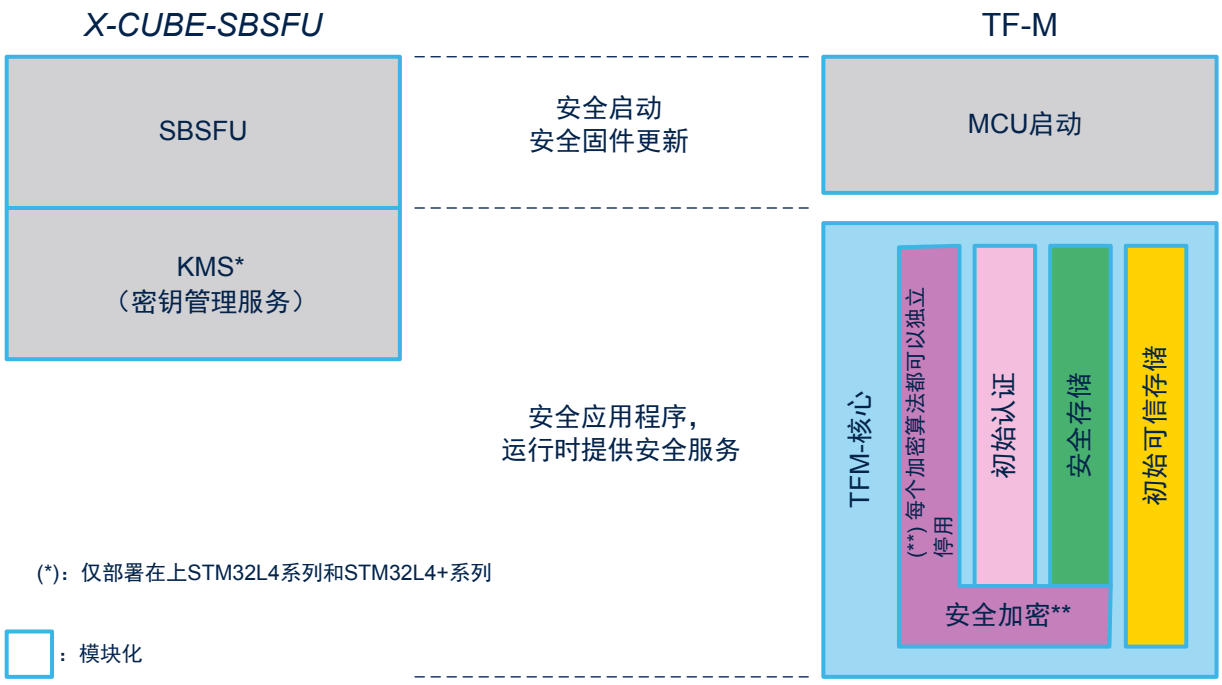
4.1 概述

X-CUBE-SBSFU 提供意法半导体的安全启动和安全固件更新流程实现，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流程服务，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 之间的上层比较请参见图 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。参考相关用户手册（相关 Arm® TrustZone® STM32Cube MCU 包的[UM2262] 和 TFM 用户手册；参见第 2 节 参考）中引用的 X-CUBE-SBSFU 和 TF-M API 文档，获取关于受支持特性的更多详细信息。

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 5 总结了 X-CUBE-SBSFUV2.4.0 中的 *X-CUBE-SBSFU* 和基于 TF-M 的应用程序之间的不同，详见 STM32CubeL5 V1.4.0.

表 5. *X-CUBE-SBSFU* vs. TF-M 顶层特性

安全话题	*X-CUBE-SBSFU* 在 X-CUBE-SBSFU V2.4.0 中，(1)	TF-M in STM32CubeL5 V1.4.0(1)
SBSFU	1 或 2 个插槽/镜像。 新镜像通过本地加载器或 USER APP。 外部 Flash 存储器中的加密镜像执行。	1 或 2 个插槽/镜像。 新镜像通过本地加载器或 USER APP。 外部 Flash 存储器中的加密镜像执行。
	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（ECDSA）**或对称加密方案**，有/无固件加密。	非对称加密方案（**RSA** 或 ECDSA），有/无固件加密。
运行时期 安全服务	安全服务 • 1 层隔离 • 非安全中断受管理（仅 STM32L4+系列） • 主加密服务（仅 STM32L4 系列和 STM32L4+ 系列）	安全服务 • **2 层隔离** • 非安全中断不受管理 • **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**

1. *不同之处用粗体突出显示。*

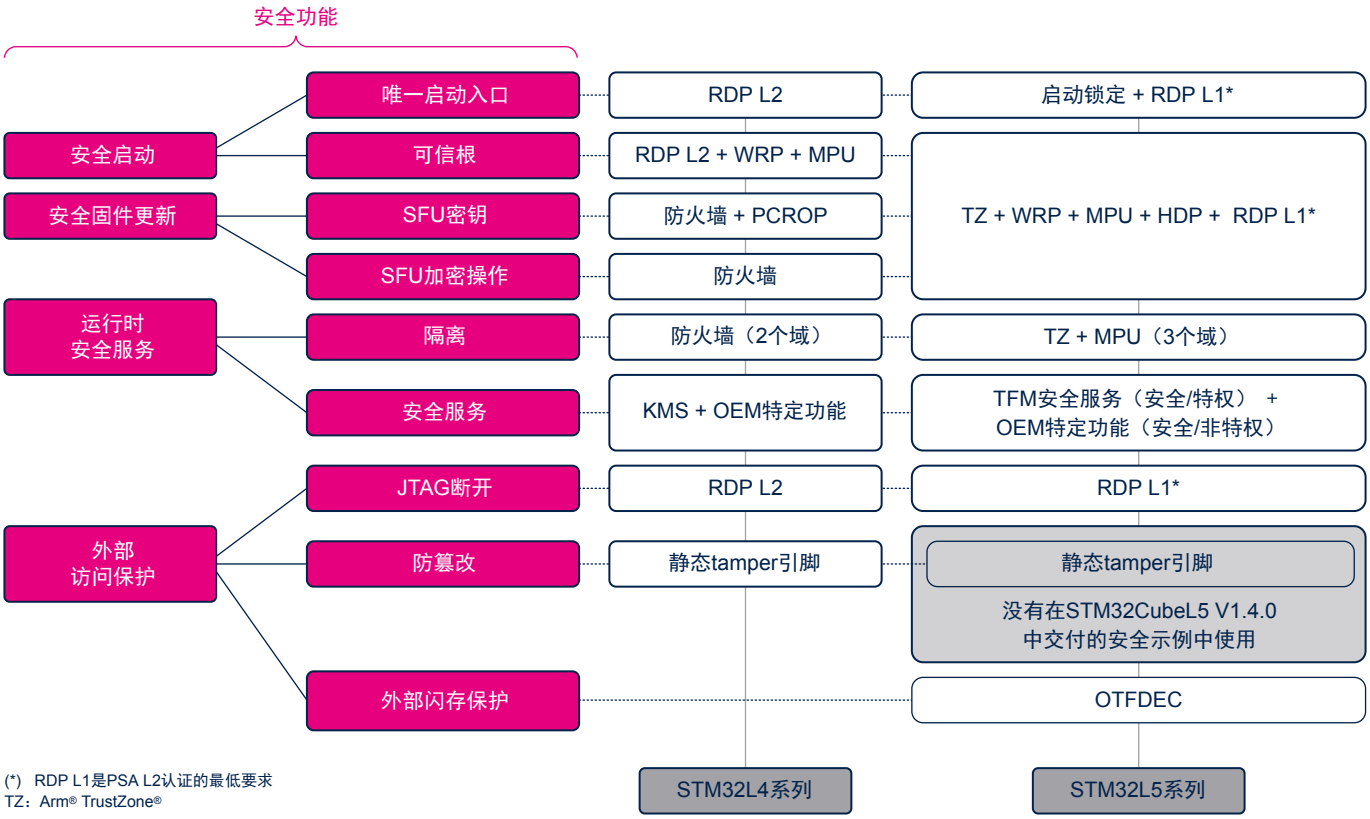
要了解面向基于 *X-CUBE-SBSFU* 和 TF-M 的应用（面向 Arm® TrustZone® STM32 微控制器）之间的最新特性差异，请参阅相关[UM2262]和 TFM 用户手册的最新版本 Arm® TrustZone® STM32Cube MCU 包（参见第 2 节 参考）。

4.3 硬件安全

基于 TF-M 的应用程序的安全策略是依赖 TrustZone®和 STM32 微控制器安全特性。

图 3 显示该安全策略（以 STM32L5 系列为例）与 X-CUBE-SBSFU 中 SBSFU 安全策略（以 STM32L4 系列为例）的对比。

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



如需详细了解安全策略（带 TF-M）有关信息，请参照相关 Arm® TrustZone® STM32Cube MCU 包的 TFM 用户手册（参见第 2 节 参考）。

5 TF-M 基于...的应用

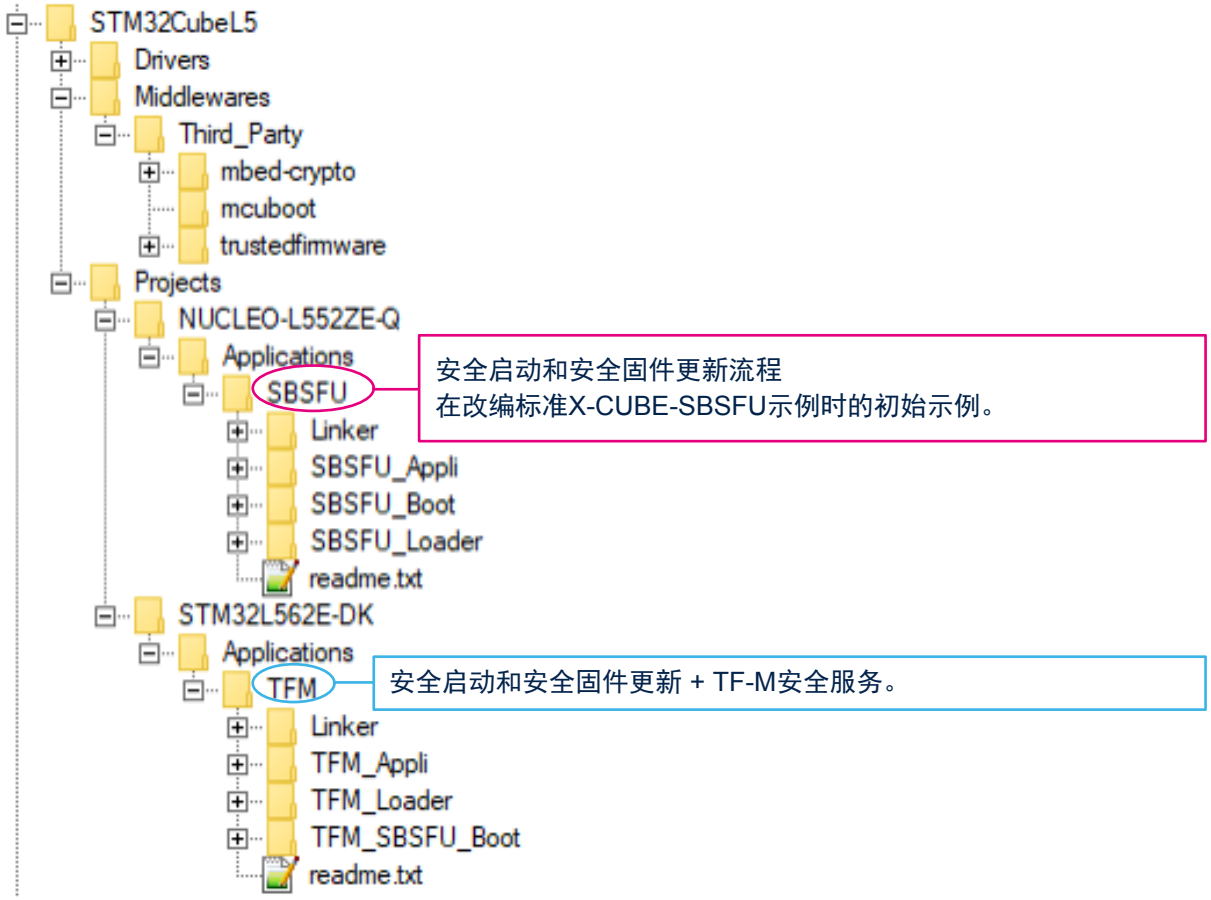
本章介绍基于 TF-M 的应用（在 Arm® TrustZone® STM32 微控制器的 STM32Cube MCU 软件包中）。

Arm® TrustZone® STM32Cube MCU 软件包基于 TF-M 参考实现提出两种不同应用，可移植到 Arm®TrustZone®STM32 微控制器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流程*"应用程序（名为 `SBSFU_Boot`）简单用户应用程序示例（名为 `SBSFU_Appli`）。此外还包含了本地加载程序应用示例（名为 `SBSFU_Loader`）。
- TFM：它包括"*安全启动和安全固件更新流程*"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`）。此外还包含了本地加载程序应用示例（名为 `TFM_Loader`）。

建议使用 *X-CUBE-SBSFU*（不带 KMS）的用户考虑迁移到 Arm® TrustZone® STM32Cube MCU 包中感兴趣的 *SBSFU* 应用程序。建议使用 *X-CUBE-SBSFU*（带 KMS）的用户考虑迁移到 Arm® TrustZone® STM32Cube MCU 包中感兴趣的 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）。

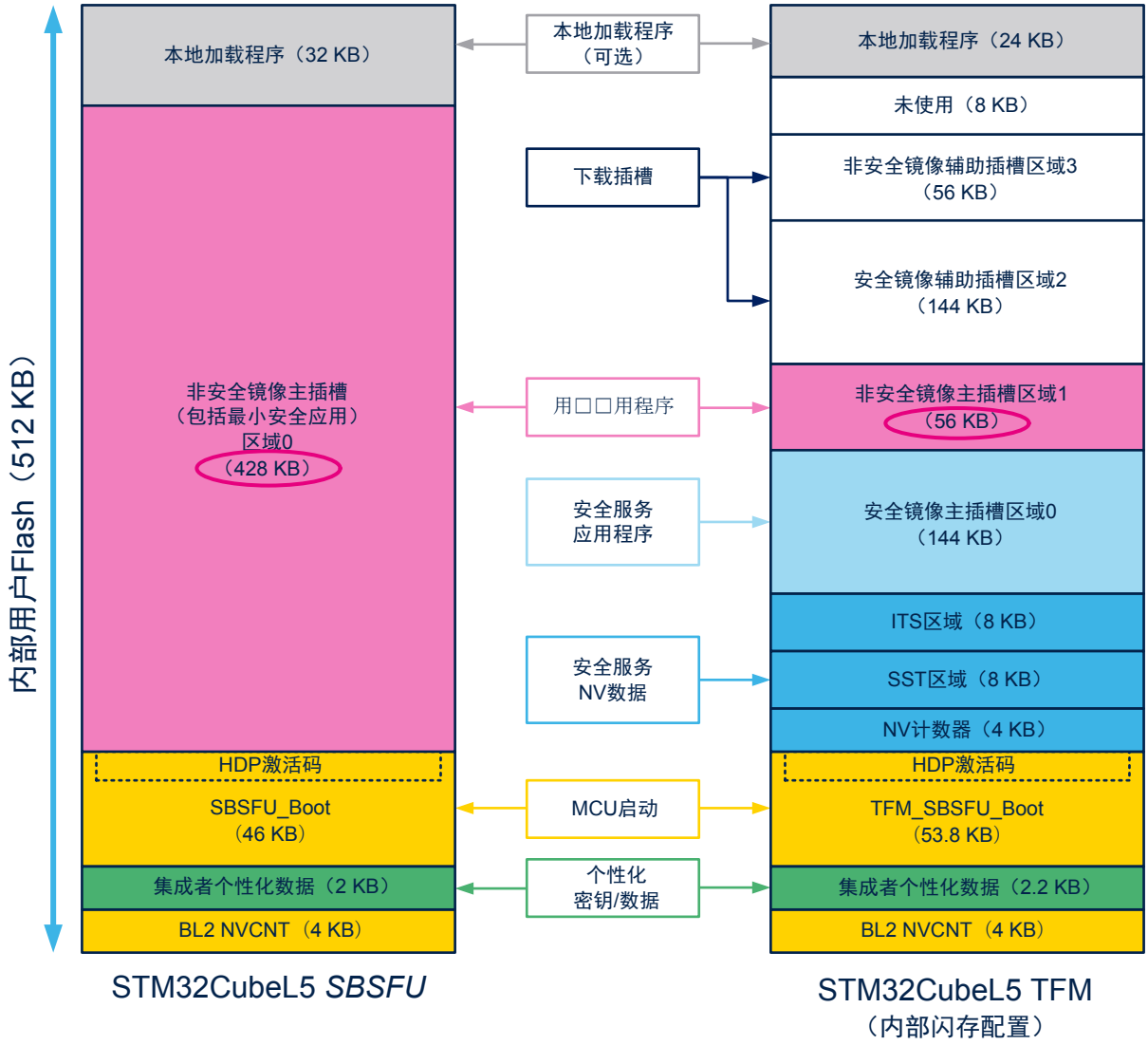
图 4. STM32CubeL5 基于 TF-M



对于每个应用程序，其内存占用取决于配置（参考相关 Arm® TrustZone® STM32Cube MCU 包的 TFM 用户手册中的*内存布局*一节；参见第 2 节 参考）。

通过移除运行时期的 TF-M 安全服务并建议一个固件镜像配置仅与主插槽配置相结合，相关 Arm® TrustZone® STM32Cube MCU 包中的 *SBSFU* 应用程序将用户应用程序可用的内部闪存数量最大化，见图 5。

图 5. 基于的 STM32CubeL5 应用程序的内存占用示例 TF-M



如需详细了解内存映射有关信息，请参考相关 Arm® TrustZone® STM32Cube MCU 包的 TFM 用户手册中的*内存布局*一节（参见第 2 节 参考）。

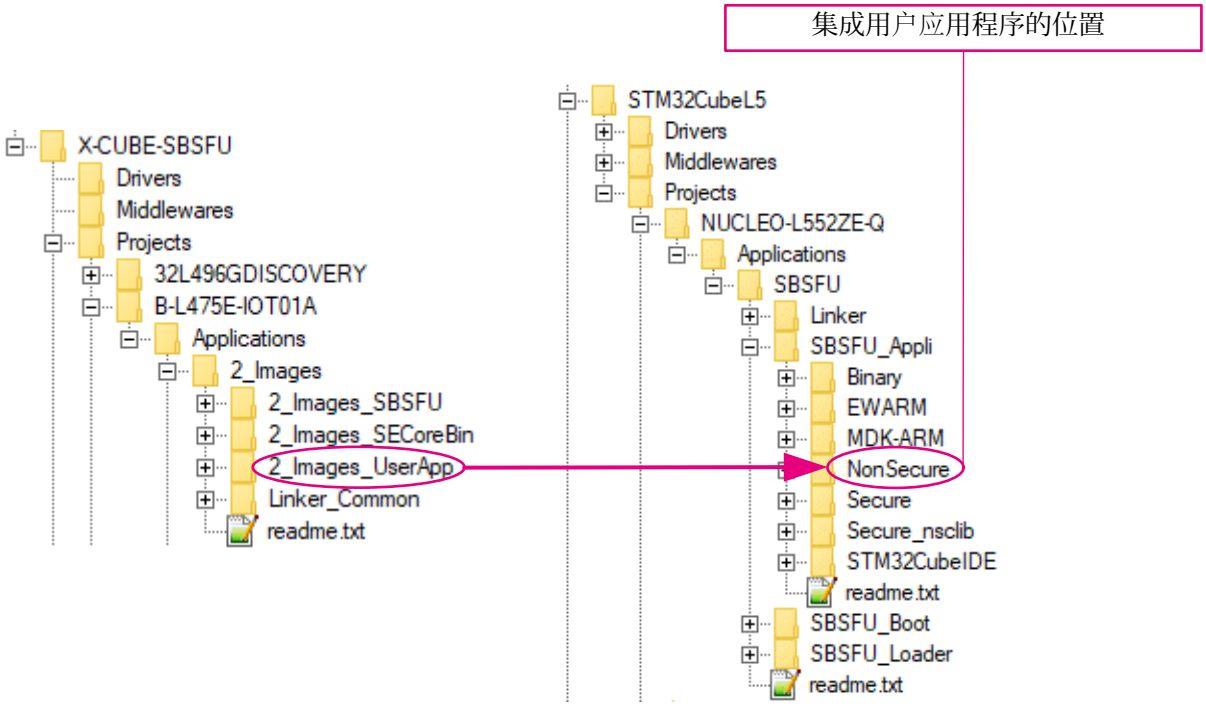
6 *SBSFU* 应用

本章介绍 Arm® TrustZone® STM32 微控制器的 STM32Cube MCU 软件包的 *SBSFU* 应用程序。

6.1 用户应用程序集成

当从 *X-CUBE-SBSFU* 应用程序迁移到 Arm® TrustZone® STM32Cube MCU 包中的 *SBSFU* 应用程序后，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

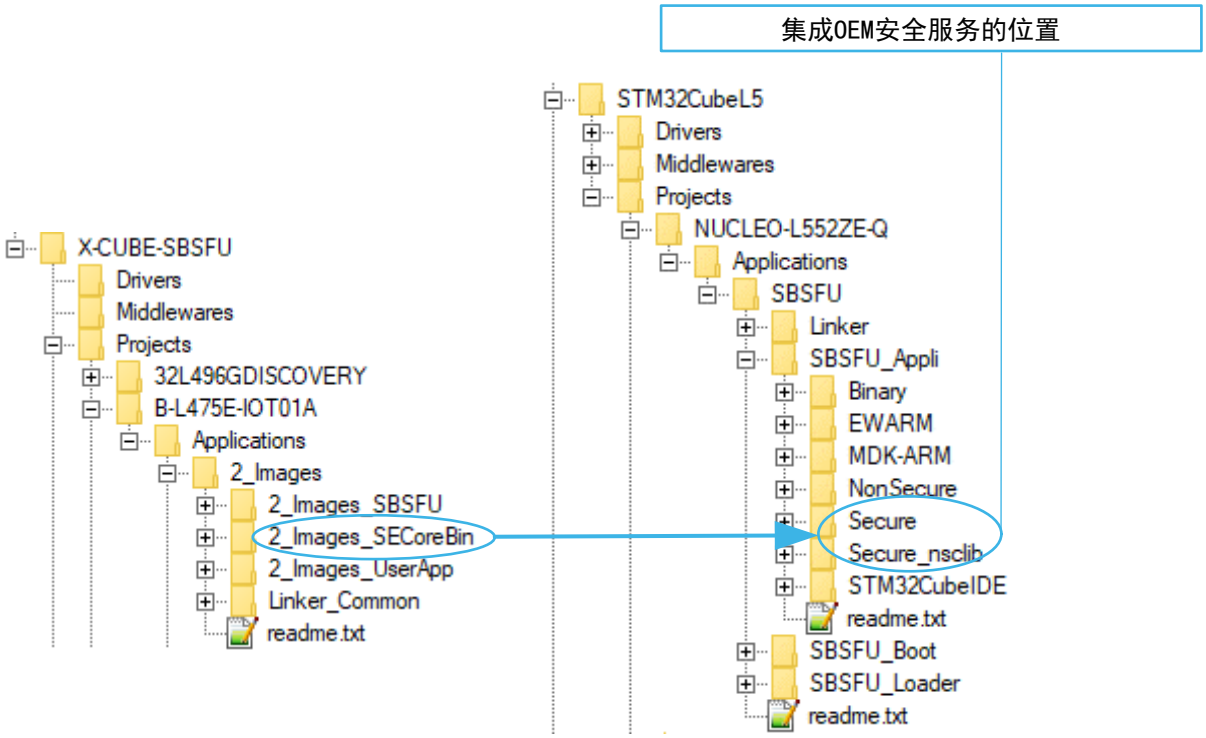


6.2 OEM 安全服务集成

如果 OEM 自己的安全服务也在 X-CUBE-SBSFU 中实现，则这些 OEM 安全服务必须集成到 `SBSFU/SBSFU_Appli/Secure` 和 `SBSFU/SBSFU_Appli/Secure_ncslib` 文件夹中， 参照 STM32Cube MCU 软件包中的 TrustZone®HAL 示例，如图 7 所示。

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

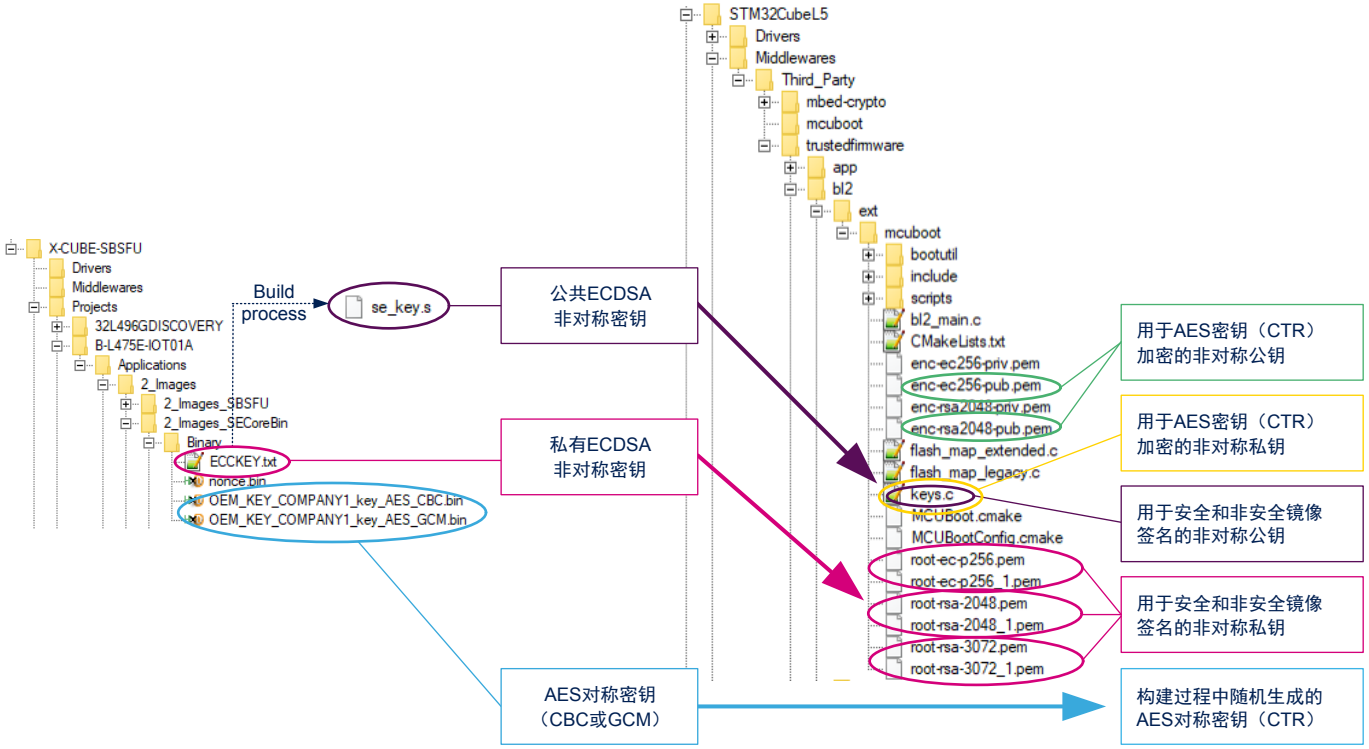
在 *X-CUBE-SBSFU* 中，个性化数据是加密密钥：

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

关于固件镜像签名，STM32CubeL5 V1.4.0 的 *SBSFU* 中有两个 RSA 或 ECDSA 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）。

SBSFU 在 STM32CubeL5 V1.4.0 中，通过 AES-CTR 加密法支持固件加密。相比 *X-CUBE-SBSFU*，AES-CTR 密钥不存在于个性化数据中，而是在每个构建过程中随机生成的，然后被加密（RSA-OAEP 或 ecees - p256）并在固件映像中提供。用于加密 AES-CTR 密钥的非对称密钥（RSA 或 ECDSA）与非对称签名密钥不同。用于 AES-CTR 密钥加密的非对称公钥和私钥必须由用户提供（参照图 8）。

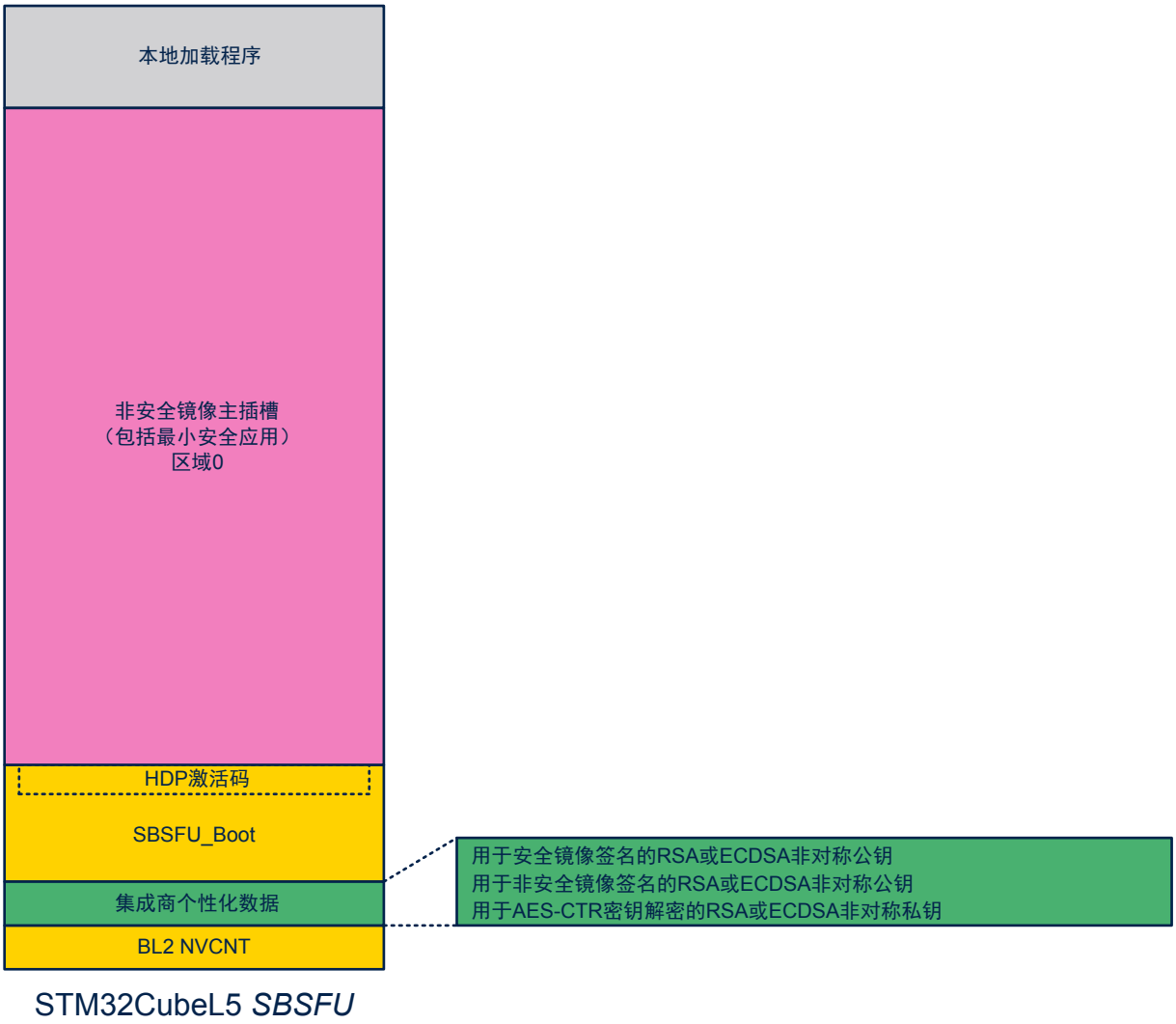
图 8. 固件镜像密钥个性化



这两个私有 RSA 或 ECDSA 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，而两个相关的公共 RSA 或 ECDSA 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。

用于加密 AES-CTR 密钥的 RSA 或 ECDSA 非对称公钥不是内嵌在 Flash 存储器中，而相关的 RSA 或 ECDSA 非对称私钥存在于 SBSFU_Boot 项目的构建输出和个性化数据区域中，如图 9 中所示。

图 9. 集成者个性化数据区域在 STM32CubeL5 *SBSFU*



7 TFM 应用

本章介绍 Arm® TrustZone® STM32 微控制器的 STM32Cube MCU 软件包中的 TFM 应用程序。

第 6 节 SBSFU 应用中提供的顶层集成指南适用于 TFM STM32Cube MCU 软件包应用。本节中提供特定于 TFM STM32Cube MCU 软件包应用的额外顶层集成指南。

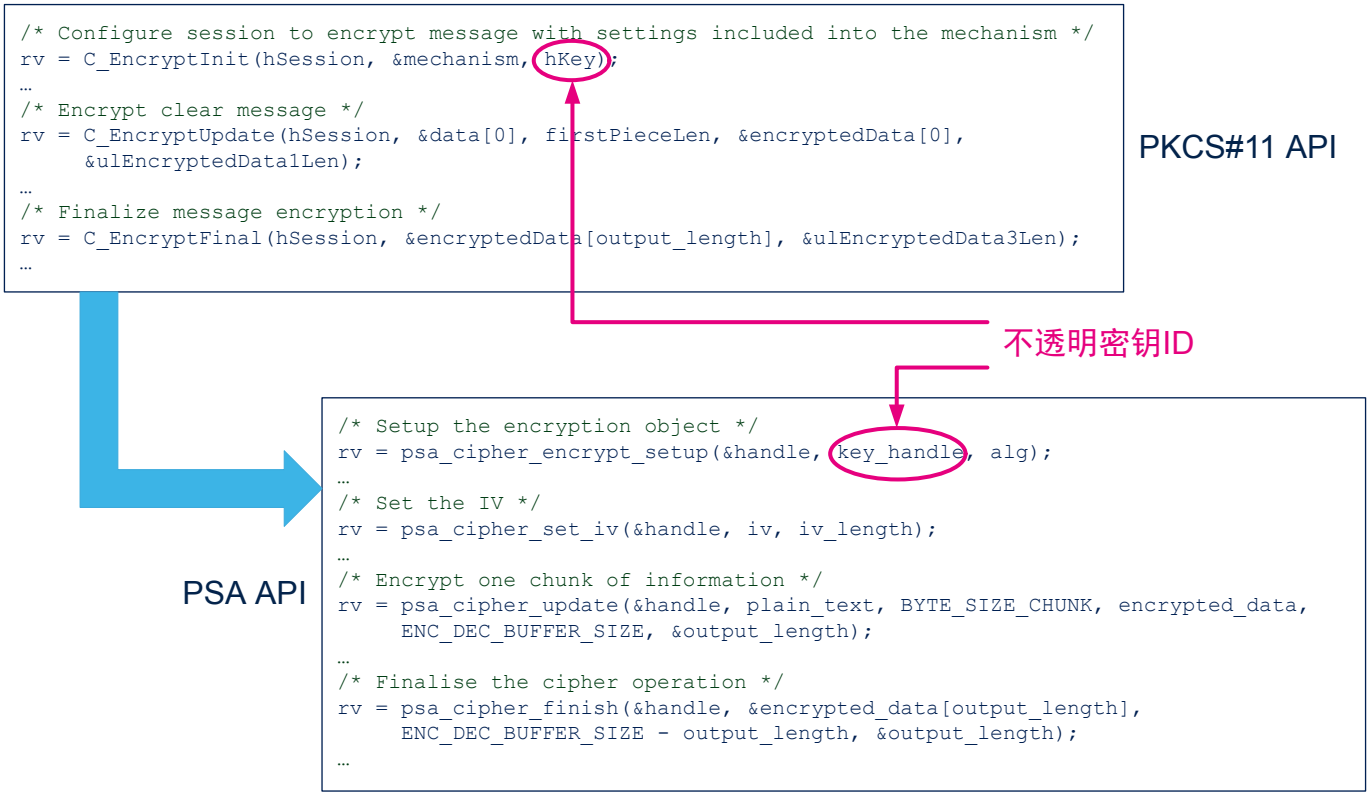
如需详细了解 STM32Cube MCU 软件包中的 TFM 应用程序，请参照相关 Arm® TrustZone® STM32Cube MCU 包的 TFM 用户手册（参见第 2 节 参考）。

7.1 运行时期的加密安全服务 运行时期

在 *X-CUBE-SBSFU* 中，通过 PKCS#11 API 为用户应用程序提供 KMS 服务。在 STM32Cube MCU 软件包 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

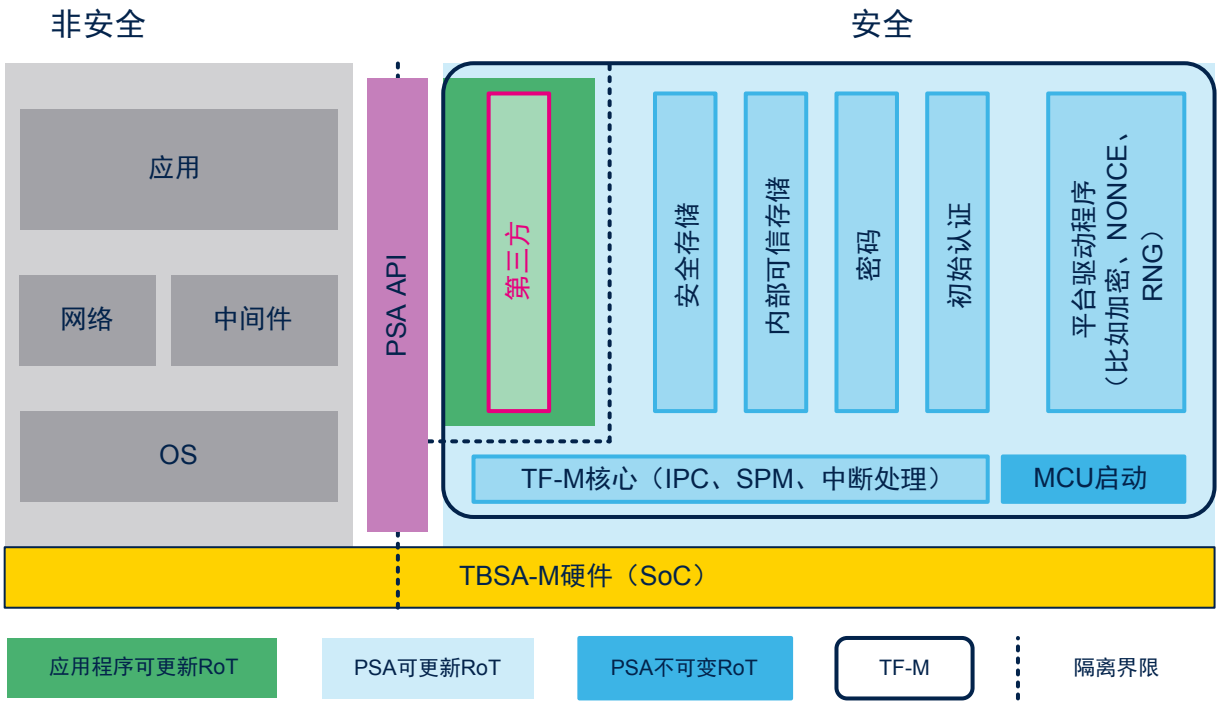


关于 PSA API 的更多信息，请参阅 TFM 用户应用程序示例和[PSA_API]。

7.2 OEM 安全服务集成

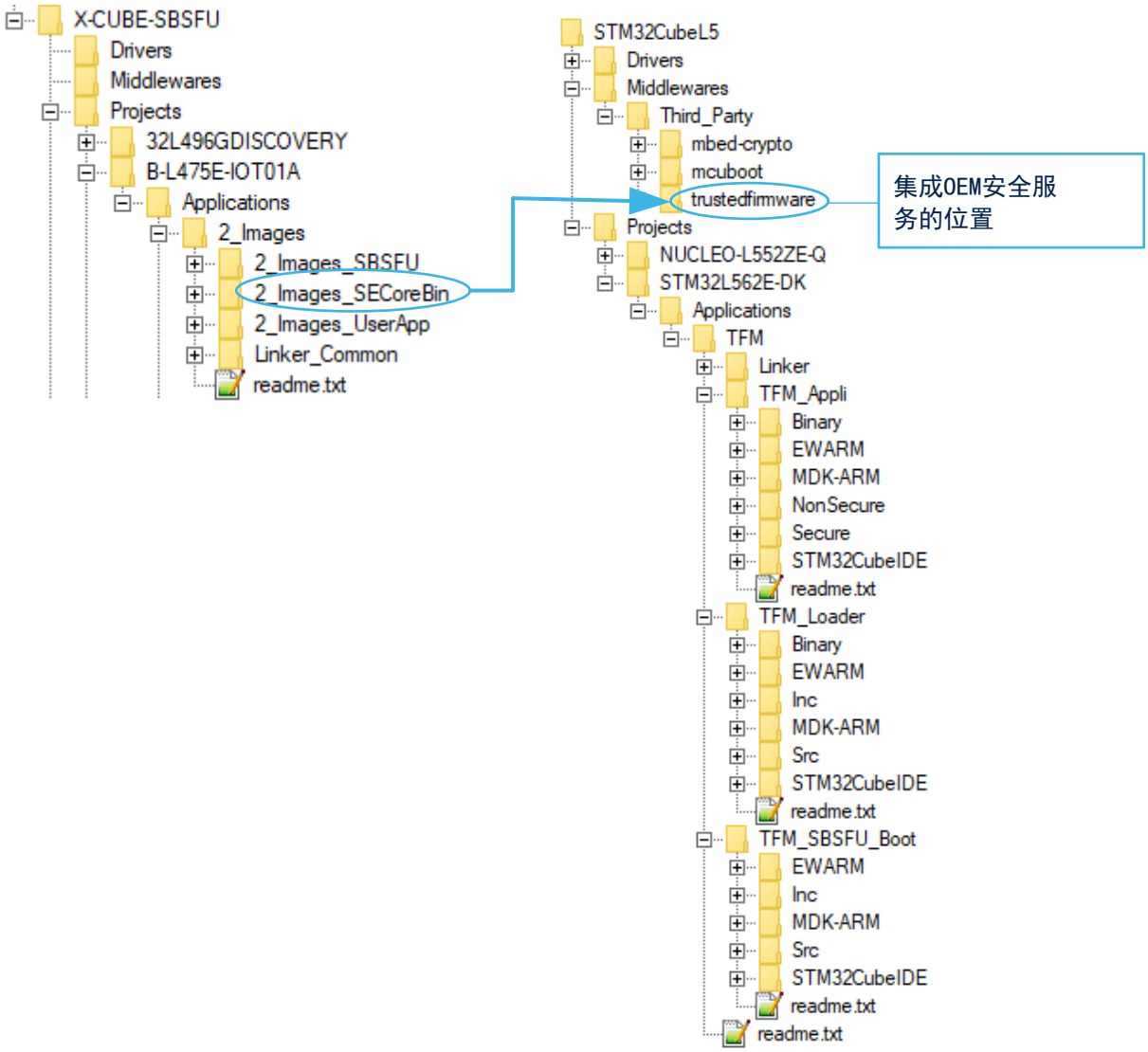
如图 11 中所示，OEM 安全服务必须集成为安全应用程序的安全/非特权部分中的第三方安全服务（称为*"来自 TFM 框架的应用程序 RoT"*）。如需详细了解*"来自 TFM 框架的应用程序 RoT"*有关信息，请参照相关 Arm® TrustZone® STM32Cube MCU 包的 TFM 用户手册（参见第 2 节 参考）。

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。有关详细信息，请参见 [TF-M]。

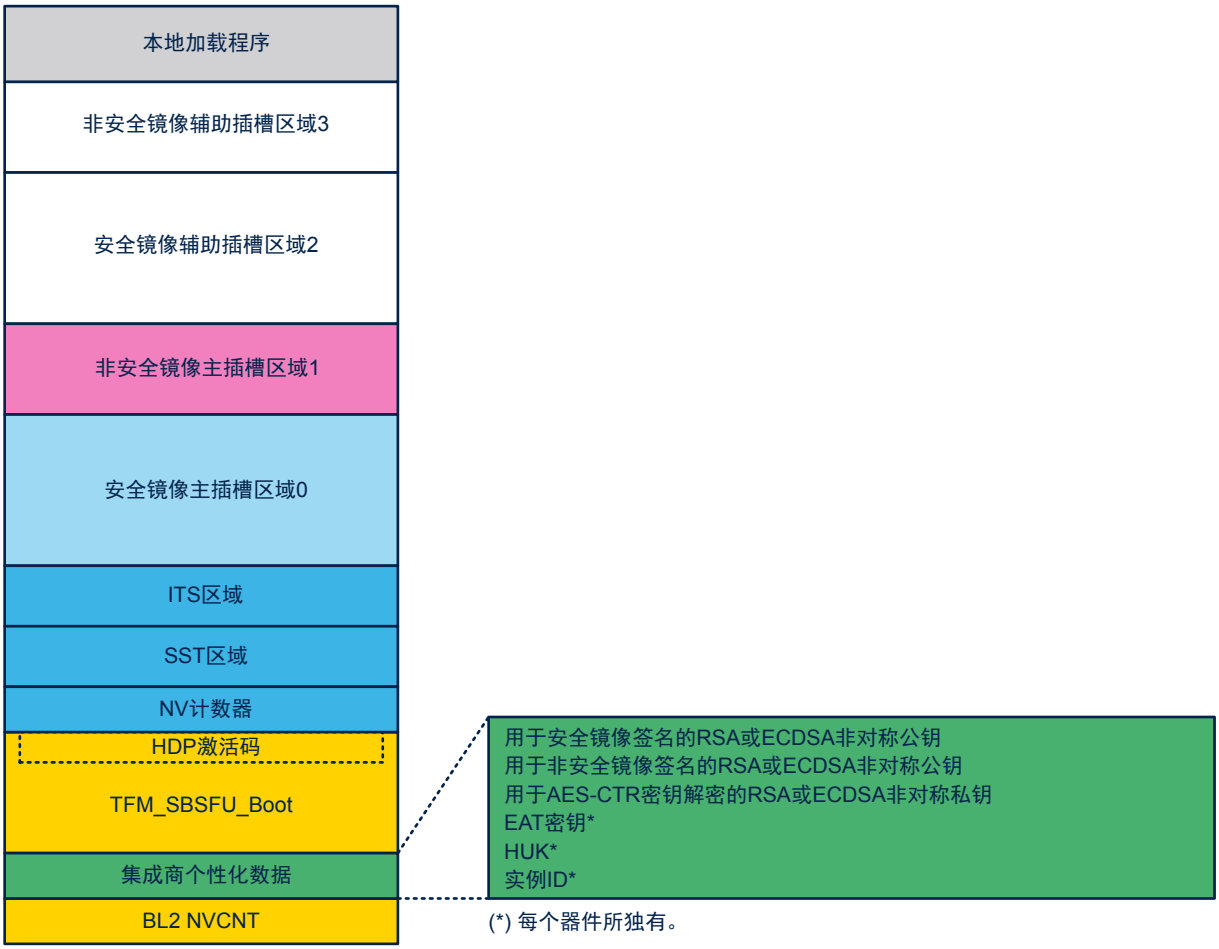
图 12. OEM 安全服务集成（TFM）



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）。这些数据与用于镜像签名和 AES CTR 密钥解密（参照第 6.3 节 密钥个性化）的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



如需详细了解个性化数据有关信息，请参考相关 Arm® TrustZone® STM32Cube MCU 包的 TFM 用户手册中的*集成商角色描述*一节（参见第 2 节 参考）。

版本历史

表 6. 文档版本历史

日期	版本	变更
2020 年 2 月 20 日	1	初始版本。
2020 年 7 月 24 日	2	更新了 STM32CubeL5 固件 V1.3.0 版本的整个文档。SBSFU_Boot 中的新特性：镜像加密，外部 Flash 存储支持 OTFDEC，可配置加密方案，可配置镜像数量模式，可配置插槽模式，以及 RSA 硬件加速器。引进了本地加载程序。
2021 年 8 月 16 日	3	使文档可通用于所有适用的 Arm® TrustZone® STM32 微控制器和相关 STM32Cube MCU 软件包，以 STM32CubeL5 MCU 软件包为例： • 更新了文档标题 • 增加了表 1. 适用产品，并进行了更新 表 3. 参考文档 • 更新了第 4.2 节 顶层特性和 第 6.3 节 密钥个性化

目录

表一览

图一览