life.augmented

STSAFE
用于验证和嵌入安全

目录

身份验证简介

身份验证产品为用于品牌保护、平台完整性、PC和IT安全、安全连接至云和远程服务器的安全元件。

身份验证产品具有出色的存储和处理机密信息能力，有助于保护公司形象、声誉和收入，防止克隆和窃取，并确保安全可信的服务。

保护业务与品牌

实施安全措施时的简单错误或数据测量不正确可能导致拒绝服务，从而影响最终用户的安全或隐私，并可能影响公司的品牌声誉。为帮助公司维护其声誉和保护其品牌，意法半导体提供了广泛的产品和解决方案组合，以及一整套的硬件和软件开发工具。

意法半导体的解决方案如何应对安全威胁

安全威胁

- 设备克隆或伪造
- 设备完整性或数据损坏
- 机密信息丢失

ST安全元件

安全服务

- 身份验证，唯一ID
- 安全通信
- 平台完整性
- 使用情况监控
- 安全存储
- 密钥配置

安全服务优势

- 收益保护
- 声誉
- 服务的连续性和可靠性
- 保护客户资产和隐私
- 遵守法规
- 避免额外的安全基础设施投资

STSECURE

80+亿件
安全微控制器
目前已发出

STSAFE产品组合与市场

用于品牌保护和嵌入式系统的可扩展安全产品

STSAFE是提供身份验证、机密性和平台完整性服务的安全元件产品系列，可使OEM免受克隆、伪造、恶意软件注入和未经授权的生产侵害。

STSAFE安全元件符合业界严苛的安全认证，是通过具有预先配置的密钥和证书的可信赖供应链开发的交钥匙解决方案，其中包括用于安全无缝集成的一组软件库和驱动程序。

STSAFE支持端到端安全

从嵌入式平台到网关和服务器，意法半导体提供适合多种应用的各种安全元件，以构建安全且可信的系统。

STSAFE安全元件集成到器件设计中并连接到其处理单元，可帮助验证设备和确保平台完整性、数据机密性以及端到端安全性。

产品系列

- 为嵌入式系统而优化的STSAFE-A
- 带Java平台的灵活STSAFE-J
- 适用于可信计算的标准化STSAFE-TPM

细分市场中的STSAFE映射

标准的STSAFE-TPM
适用于可信计算与加密服务的TCG标准化平台

灵活的STSAFE-J
带可选默认小程序的灵活Java™平台

优化的STSAFE-A
为品牌保护和安全连接而调优

耗材、配件、
打印机、计算机

工业
环境传感器、执行器、
工厂自动化

网关、基站、
实用程序

优化的 STSAFE-A

STSAFE-A在CC EAL5+平台上运行，是一个高度安全的身份验证解决方案，其安全特性通过独立第三方认证。

其命令集经过定制，以确保强大的设备身份验证、监控设备使用情况、协助附近的主机安全通道建立(TLS)并维护主机平台完整性。

为保护您的业务而优化的STSAFE-A

可实现无缝安全性的STSAFE-A110生态系统

STSAFE-A110是STSAFE-A安全元件，它具有领先的安全功能，可防止假冒正品外设和IoT设备。

主要特性

- 强大的身份验证（符合USB-C和QI）
- 安全通道建立(TLS)
- 签名验证
- 递减计数器
- 安全数据存储
- 符合LPWAN Lora与Sigfox

产业生态系统

STSAFE-A110生态系统包含一整套用于无缝集成的工具：

- ODE STM32扩展板（X-NUCLEO-SAFEA1）
- STM32 Cube开发生态系统（X-CUBE-SAFEA1软件包）
- 可用于快速评估的预个人化STSAFE-A110
- 在意法半导体工厂进行的个人化客户认证和配置服务无需额外费用

欲了解更多信息，请访问：www.st.com/stsafe-a

在线订购X-NUCLEO-SAFEA1：www.st.com/stsafe-A110

主要优势

- 为耗材和小型平台而优化
- 个人化服务
- 使用与STM32和其他通用MCU兼容的库进行无缝集成
- 通过电子分销提供
- CC EAL5+-认证

产品系列

产品名称	支持OS	接口	认证	封装选项	工作温度范围	NVM存储
STSAFE-A110	• 强大的身份验证 • 建立安全连接 • 使用情况监控 • 主机平台完整性 • 符合LoRa与Sigfox	I²C	CC EAL5+ HW	SO8N DFN 2x3	从-40至+105° C	6 KB
STSAFE-A1SX	• Sigfox身份验证 • Sigfox框架 • 加密/解密（可选）					

灵活的
STSAFE-J

STSAFE-J是基于Java Card操作系统的灵活解决方案，可供客户自由运行计划使用的小程序。

STSAFE-J也可以与小程序一起使用，以确保在主机平台上的安全：强大的身份验证、建立安全连接、使用情况监控和平台完整性。

主要优势

- 带有意法半导体通用或特定于客户的小程序的灵活Java解决方案
- 使用与标准MCU和MPU兼容的库无缝集成
- CC EAL5+认证

STSAFE-J，灵活的JAVA平台

具有认证保护配置文件的STSAFE-J100

主要特性

- CC EAL5+ 认证平台
- Java 3.0.4和GP 2.1.1认证平台
- 通用意法半导体小程序：
  - 身份验证
  - 安全连接
  - 安全数据存储
  - 个人化服务
- 客户特定小程序

开发工具和服务

- 扩展板兼容STM32 Nucleo和Arduino板
- 嵌入在应用微控制器中的示例代码和库（PKCS11软件包）
- 欲了解更多信息，请访问：www.st.com/stsafe-j

产品系列

产品名称	支持OS	接口	认证	封装选项	工作温度范围	NVM存储
STSAFE-J100	GP 2.1.1 / JC 3.0.4	接触式 ISO/IEC 7816、I²C	CC EAL5+	DFN8 VFQFPN32	-40至105° C	80 KB

标准的
STSAFE-TPM

STSAFE-TPM是一种广泛部署的标准化解决方案，是个人计算机和服务器安全性的基石。它非常适合基于Windows和Linux操作系统的生态系统。

所有STSAFE-TPM产品均通过CC和FIPS 140-2认证，并符合安全性和法规要求。该产品组合符合消费、工业和汽车应用要求。

主要优势
- 与Linux和TCG TPM软件堆栈集成
- FIPS和CC认证
- 使用寿命长
- 随附密钥和证书

适用于可信计算的标准化STSAFE-TPM

将信任从个人计算扩展到连接的设备

STSAFE-TPM是一种可提供标准化可信计算服务（ISO / IEC 11889）的成熟解决方案，非常适合基于Windows或Linux的平台。

主要特性
- 对长生命周期设备的扩展加密支持（ECC384、SHA2-384、SHA3、AES 256）
- 可通过默认的容错加载程序来升级TPM固件
- TPM固件和关键数据自我恢复(NIST SP800-193)
- 以CC保证等级(AVA_VAN.5)进行渗透测试
- 提供SPI或I²C接口
- 消费性/ AEC-Q100 / 工业认证
- 提供标准和小尺寸封装，如WLCSP

产业生态系统

完整的开发套件可提供轻松集成。
- 用于SPI和I²C接口的Raspberry PI®和STM32-MP1扩展板(STPM4RasPI)
- 带有驱动程序和实用程序的软件包（通信驱动程序和固件升级）
- 得益于Windows和Linux支持、TCG开源或第三方TPM栈，可实现顺利的系统集成

欲了解更多信息，请访问：www.st.com/stsafe-tpm

产品系列

产品名称	应用领域	支持OS	接口	认证	封装选项	工作温度范围
ST33TPHF20/2E	TPM PC /服务器、网络、打印机、物联网	TPM 1.2 / TPM 2.0	TCG SPI (33 MHz) TCG I²C (400 KHz)	CC EAL4+、TCG、FIPS 140-2	TSSOP28，VQFN32	-40至105° C
ST33TPHF2X		TPM 2.0		CC EAL4+（高攻击潜力）、TCG、FIPS 140-2	VQFN32	
ST33GTPMA	汽车		TCG SPI (18 MHz) TCG I²C (200 KHz)		TSSOP20	
ST33GTPMI	工业				WLCSP	

life.augmented

关于意法半导体产品和解决方案的更多信息，请访问www.st.com

订购代码：BRSTSAFE0820