life.augmented

安全解决方案
确保您
高枕无忧

目录

安全解决方案
简介

凭借其STSECURE产品组合，意法半导体提供广泛的安全微控制器和交钥匙解决方案，以满足市场对高级安全性的需求。

随着互联设备数目的不断增多，犯罪分子通过植入恶意软件或盗版软件来控制/危害互联网络、进而控制特定资产的机会越来越多。受到这些威胁的频率很高，并且这经常发生在私有和专业环境中。

STSECURE，确保您高枕无忧

致力于安全的完整产品组合

在快速发展的数字世界中，STSECURE产品和解决方案通过确保其机密性、完整性以及在需要的地方和时间对授权请求者的可用性来保护您的隐私和资产。我们提供经过硬件和软件认证的解决方案以及与安全功能的无缝集成，并且我们是加密和设备架构方面的专家。

欲了解更多信息，请访问：**www.st.com/stsecure**

超过30年的安全经验

超过
80亿
安全微控制器
目前已发出

密码学与架构专业知识

大力参与安全社区

内部技术

经过硬件和软件认证的解决方案

安全环境
（开发、测试、个性化）

安全解决方案
我们的价值链

我们价值链的主要活动

供应商

我们从供应商采购硅锭、原材料、设备、能源、气体、化学品和服务。

研发理念与设计

新产品通过多步骤工艺制造，以产生用于在硅中蚀刻设计的掩模。

前端制造

芯片生产经历大约400道单独工序的工艺，从平面硅晶圆开始，到最后屏蔽成百上千个晶片。

电子晶圆分类、安全密钥和数据加载

安全微控制器需要使用硬件安全模块(HSM)将嵌入式软件、密钥和数据预先载入安全环境中。

装配线和最终后端

封装之前，将晶片从硅晶圆上切割下来。然后在交付前对这些芯片进行测试。

安全预个性化

安全微控制器包括必须在安全环境中加载的客户密钥和数据。

可持续性技术

我们在产品设计过程中系统地考虑了设备在整个生命周期中对环境的影响。

标准

意法半导体在其供应链中遵守责任商业联盟（RBA）行为准则，该准则要求通过ISO和OHSAS认证来应对道德、社会、环境、健康和安全风险。我们是责任矿产倡议（RMI）的成员。

我们设计、制造产品并提供个性化服务，以确保设备符合质量、环境、安全和保安标准与认证：

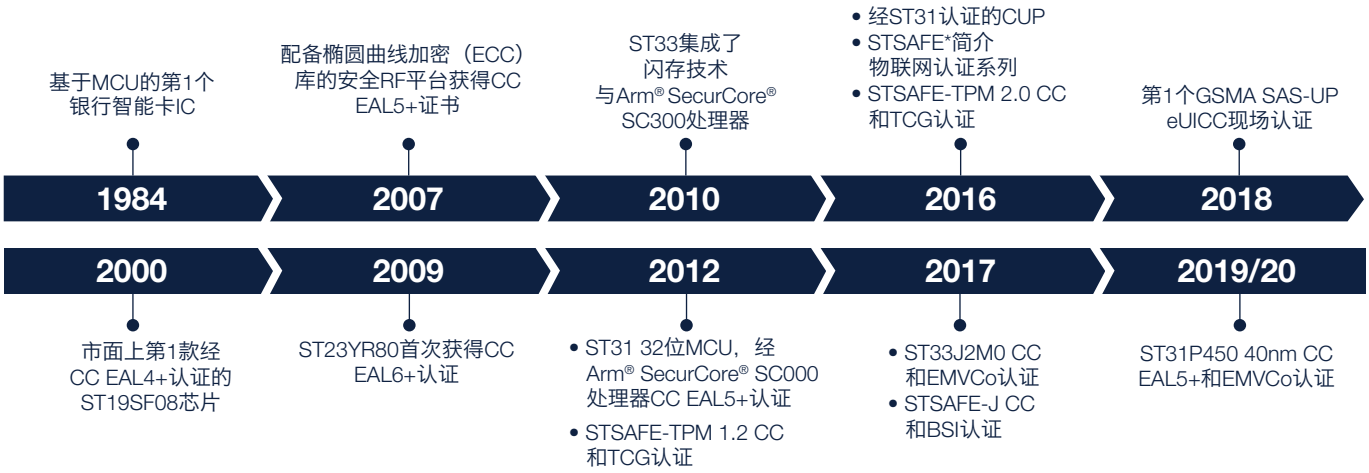
- 管理系统的连续性
- ISO/TS 16949质量管理体系
- 万事达卡质量管理（CQM）认证
- ISO 50001和ISO 14064环境管理标准
- 通用标准EAL5+/EAL6+和FIPS 140-2/3安全评估
- ISO/IEC 15408计算机安全认证
- OHSAS职业健康与安全管理系统
- 业务连续性管理
- ISO 22301业务连续性标准
- GSMA SAS-UP（UICC生产安全认证计划）eUICC个性化现场认证。

意法半导体根据最高安全生命周期提供端到端安全解决方案

安全解决方案
我们的产品

认证

EMVCo、Visa、Mastercard、NFC、MTPS、中国银联（CUP）、FIPS和Common Criteria（CC）等组织颁发的奖励和证书印证了意法半导体的成功。并且，意法半导体是第一家获得用于eSIM生产的“GSMA SAS-UP认证”电子元件制造商，这展示了其在这类器件所能达到的最高水平的安全性以及满足所有市场需求的灵活性。



技术

安全市场朝物联网、安全汽车、M2M、工业和5G应用的演进促进了先进技术的发展，以便设计符合最新要求的解决方案。这些应用需要具有可扩展eNVM单元以及在宽温度范围上具有高循环能力、良好的保留能力和低功耗的高性价比产品。

40nm eSTM*，同类最佳的40nm浮栅技术

40nm eSTM（沟槽存储器中的嵌入式选择）是意法半导体为嵌入式应用中的通用和安全微控制器设计、开发和工业化的新型嵌入式非易失性存储器。凭借其独特的架构，40nm eSTM单元在比典型闪存单元更小的区域内提供了传统分离栅NVM单元的优势，并具有非常好的可扩展性与可靠的性能。

- 小单元面积，具有很好的可扩展性，可生产高性价比产品
- 业界最高的耐用性之一，可提高最终产品的可靠性
- 针对低功耗和超低功耗应用的低电流泄漏技术
- 适用于许多应用：汽车、工业、消费、移动交易。

注释
*STMicroelectronics International NV或其附属公司在欧盟和/或其他地区的注册和/或未注册商标。

安全解决方案
如何联系我们

保护您的所有应用

完全微控制器技术由基于智能卡技术、移动交易和互联世界的动力学系统驱动。因此，意法半导体现在可保护您的所有应用，无论是SIM、银行业和ID，还是包括非接触式交易和物联网连接在内的最新应用。

借助STSECURE产品组合，意法半导体可使工业、城市、家庭、汽车和日常用品变得更智能，并能以更安全的方式建立联系。

个人电子产品

银行业、ID和运输

ST31
STPay

安全的可穿戴设备

ST31
ST54

移动安全消费者

ST33 eSIM, eSE
ST21NFC
ST54

计算机和外设

STSAFE-A
STSAFE-J
STSAFE-TPM

工业

M2M连接

ST32, ST32-M
ST33-M
ST4SIM-S / -M

汽车

安全汽车

ST33-A
ST33GTPMA
ST4SIM-A

安全解决方案
我们的系列

智能卡封装

借助遍布全球和本地的广泛合作伙伴网络，能以多种封装解决方案交付银行业、ID和运输产品。

意法半导体的产品使您可以从其广泛的模块中选择一种设备，或通过意法半导体与合作伙伴（可以提供嵌体和/或双接口模块）合作，使您也可以从一站式解决方案中受益。

面向银行业、ID和运输业的产品系列

面向智能卡应用的ST31

ST31硬件平台专为支持智能卡应用而设计，如银行业、身份识别、付费电视和运输。

- **基于40nm eSTM技术的ST31P450**可实现更快的交易和更出色的用户体验
- **面向生物识别系统卡的ST31**支持用于支付和ID的高级身份验证技术

STPay，意法半导体的安全支付解决方案

STPay系列基于ST31硬件，是面向银行业、运输智能卡和可穿戴支付的独立产品。它使卡制造商可快速应对各种市场需求，同时节省软件开发工作量和时间。

- **STPay双接口**解决方案
- **STPay接触式**解决方案
- **用于生物统计的STPay**

我们的移动安全系列

ST33、ST21NFC和ST54移动融合

意法半导体提供齐全的NFC、eSE和GSMA认证eSIM产品与解决方案，适用于安全移动交易应用。这些产品与解决方案以前单独提供，现在可作为将NFC控制器、eSE和eSIM相结合的全集成解决方案提供，从而带来了新的设计机会。

- **ST33 SIM、eSIM和eSE**
- **ST21NFC** NFC控制器
- 集成eSIM、eSE和NFC的**ST54**

我们的汽车产品系列

ST33-A和ST4SIM-A，汽车级产品系列

随着汽车的互联程度越来越高，它们更容易受到攻击，确保安全性也越来越具有挑战性。因此，基于ST33硬件，意法半导体提供了可扩展的汽车级安全元件和eSIM解决方案组合，这些解决方案专用于汽车生态系统中的安全性和连接性。

- **ST33G1M2A**硬件
- 适用于eSE的**ST33GTPMA** SoC
- 适用于eSIM的**ST4SIM-A** SoC

ST33，多用途系列

ST33是我们主要的历史安全硬件平台之一，可在多种应用中找到其身影。借助最新的32位Arm® SecurCore® SC300，它可以提供大存储容量、多个通信接口以及各种外形（晶圆、SIM模块、DFN、WLCSP）的认证加密库。

- 移动安全：SIM、eSIM和eSE
- 工业和物联网：M2M eSIM & eSE
- 汽车：eSE和eSIM
- 可信计算：TPM解决方案

我们的品牌保护、工业和物联网系列

用于身份验证的STSAFE

STSAFE系列通过构建安全且可信的嵌入式系统来保护业务。STSAFE安全元件适用于从嵌入式平台到网关和服务器的物联网生态系统产品。

- **STSAFE-A**，用于嵌入式系统和品牌保护
- **STSAFE-J**，用于网关和物联网设备
- **STSAFE-TPM**，用于标准化和成熟的TPM服务

面向蜂窝网络连接的ST4SIM

从可移除SIM到GSMA认证的eSIM，ST4SIM是灵活的可扩展产品，可用于在各种环境中建立蜂窝网络连接。优质且可靠的ST4SIM产品是完整生态系统的一部分，该生态系统由专注于连接和订阅管理平台的合作伙伴构建。

- **ST4SIM-S**用于物联网
- **ST4SIM-M**用于工业
- **ST4SIM-A**用于汽车

智能卡应用
ST31

意法半导体在全球出售了400多万件用于银行业、ID和运输的STSECURE微控制器，在智能卡行业具有深厚的专业知识和丰富的参考资料。

从传统智能卡到创新的可穿戴设备和生物识别解决方案，意法半导体提供完整的接触式和双接口安全微控制器产品组合。

借助40nm eSTM技术和先进的非接触式IP，最新的ST31产品可通过制造超小型晶粒来应对非接触应用的挑战。

超过
4亿
STSECURE微控制器嵌入在智能卡中

ST31，高度安全的微控制器
适用于智能卡应用的硬件平台

ST31硬件平台可确保可靠的安全水平，因为该平台采用最高的安全标准与认证。有了齐全的接触式和多协议通信接口，您一定能找到完美适合广泛智能卡应用的选择。

产品系列

ST31P450

- 最新的40nm eSTM技术
- 一流的RF性能和低功耗设计
- 符合MIFARE®和Calypso®，适用于运输应用

用于生物统计的ST31

- 生物识别系统卡解决方案
- 为支付和ID卡开发带嵌入式电源管理系统的高级身份验证技术。

欲了解更多信息，请访问：**www.st.com/st31**

主要特性

- 32位Arm® SecurCore® SC000 CPU
- 增强硬件安全功能
- 多协议（ISO7816、ISO14443 A/B、ISO18092、VHBR）
- EMVCo、CC至EAL6+和CUP认证
- MIFARE Plus®、MIFARE Classic®和MIFARE® DESFire®库

智能卡应用
STPay

对可信支付交易的日益增长的需求已推动银行卡市场转向EMV芯片密码解决方案。

双接口卡已占全球芯片密码产品年发行量的大约一半左右。创新的外形使得非接触式支付功能可包含在生物识别卡和可穿戴对象中，以最大限度地提高易用性和用户体验。

STPay系列提供基于Java OS的全系银行业务解决方案，这些解决方案涵盖了广泛的支付应用。

即用型
适用于银行和运输应用

STPAY，意法半导体的安全支付解决方案

面向支付和运输应用的最具扩展性的产品

STPay安全支付产品组合是业内最佳的即用型独立解决方案之一，包括所有主要的国际和区域支付方案。

产品系列

STPay双接口

- 经基于参考天线的支付方案认证
- 带Java平台的STPay-Topaz-1，用于灵活地实现小程序

STPay接触式

- 国际白标支付方案（CPA、ELO）

用于生物测定的STPay

- 生物识别系统卡支付解决方案。

欲了解更多信息，请访问：**www.st.com/stpay**

主要特性

- 多种国际和区域支付方案（Visa、MasterCard、JCB、American Express、Discover、Interac Flash、CUP、Rupay...）
- 硬件认证，EMVCo、CC EAL5+）取决于操作系统和应用软件
- 接触式和双接口（ISO7816、ISO14443 A/B）
- 符合CPS标准（通用个性化标准）
- 数据卡EMV芯片供应商计划
- 以多种外形（晶片、微模块）交付

移动安全

ST33, ST21NFC, ST54

移动安全已从手机中大量采用的SIM技术扩展到智能手机、平板电脑、可穿戴设备和笔记本电脑设备中不断增长的NFC、嵌入式安全元件（eSE）和嵌入式SIM（eSIM）技术。

从最先进的ST21NFC到集成了广泛部署的ST33的ST54，意法半导体为安全移动交易应用（安全连接、支付、无线充电、数字汽车钥匙）提供全面的NFC和eSE/eSIM产品。

ST54，NFC、ST33 eSE和eSIM

面向移动设备的集成解决方案

移动融合，保护您的应用

构建最有效、最安全的移动解决方案

ST54系统级封装集成了NFC控制器和eSE解决方案，并通过将NFC、eSE和eSIM技术融合到ST54J中而迈出了新的一步，从而在小型WLCSP封装中实现了单晶粒解决方案（晶圆级芯片规模封装）。

可实现更好的非接触式交易的增强型NFC

意法半导体的增强型NFC技术非常适合需要卡仿真功能的空间受限应用。先进的模拟前端，采用有源负载调制技术，可确保可靠性在充满挑战的环境中或在需要非常小的天线的应用中进行NFC和非接触式交易。

意法半导体的eSIM领导能力

凭借更小、更薄的WLCSP以及符合GSMA标准的个性化晶圆工业流，ST33成为了主要OEM部署基于eSIM的新器件的行业标准，迄今为止，其销售量已达到数亿件。

意法半导体在2018年成为第一家获得GSMA SAS-UP认证的芯片制造商，从而能够为移动设备和连接的设备个性化定制ST33 eSIM，以使OEM实现无缝的硬件和软件集成。

欲了解更多信息，请访问：**www.st.com/sim-esim**和**www.st.com/secure-nfc**

独立解决方案

适用于eSIM和eSE应用的ST33

ST33安全微控制器满足安全应用的高级安全与性能要求，这些应用包括具有大用户闪存功能的嵌入式SIM和嵌入式NFC安全元件。

eSIM是直接焊接在PCB上的表面安装器件，它使OEM能够设计更小、更薄的移动设备，并使最终用户能够订阅他们选择的移动网络运营商。符合GSMA远程SIM配置规范的订阅管理系统可确保eSIM器件内部的SIM应用的远程配置。

适用于NFC控制器的ST21NFC

非接触式移动交易的增长推动了NFC和eSE解决方案在智能手机和可穿戴设备等消费移动设备中的采用。平板电脑、游戏机、笔记本电脑和超级本还集成了NFC技术，这使其可以读取标签，以便与智能物联网对象交互或接受支付卡。

ST21NFCD是意法半导体的第四代NFC控制器，它具有高性能的射频增强器，可实现最佳用户体验，并确保高水平的互操作性，从而简化了OEM的集成和认证工作。

主要特性

ST33
- 高达2 MB Flash
- 以多种封装交付（WLCSP、MFF2、DFN8）
- GSMA SAS-UP认证流程
- EMVCo、CC EAL5+、MTPS认证

ST21NFC
- 适用于微小的金属盖天线的增强型NFC
- 减少BOM
- 低功耗模式
- 卡模拟、读写器和P2P

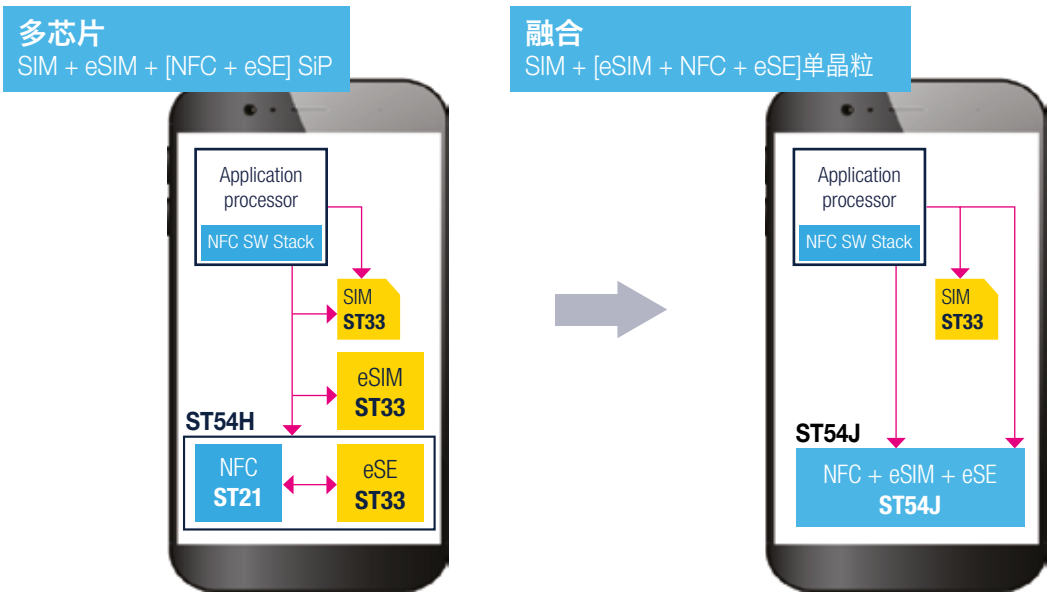
ST54
- ST33 eSE、eSIM和ST21NFC
- BGA系统级封装和WLCSP单晶粒
- GSMA SAS-UP认证流程
- EMVCo、CC EAL5+、MTPS认证
- MIFARE®和FeliCa®

集成解决方案

ST54H & ST54J

为管理未来的安全移动交易，意法半导体提供大量的ST54集成解决方案。第一代产品为以BGA封装形式提供的系统级封装（ST54H），而为解决融合问题而优化的新型ST54J系统芯片(SoC)则以采用薄WLCSP封装的单晶粒形式提供。

ST54J不仅为移动和物联网设备提供可增强性能的集成，而且具有意法半导体软件合作伙伴生态系统的附加优势，可在移动支付和电子票务交易中提供更流畅的用户体验，同时还支持人性化的远程移动配置，以支持多个运营商订阅。



身份验证
STSAFE

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安全元件符合最严苛的安全认证，并通过具有预先配置的密钥和证书的可信供应链以交钥匙解决方案的形式提供，其中包括用于安全无缝集成的一组软件库和驱动程序。

可扩展的安全产品

适用于品牌保护和嵌入式系统

STSAFE，支持端到端安全

构建安全可靠的系统

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。

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与数据机密性。

产品系列

为嵌入式系统而优化的STSAFE-A

STSAFE-A是一种经过优化的解决方案，该解决方案可针对遭受欺诈和伪造的应用进行强大的验证，确保安全的通道建立和存储。对于希望围绕其品牌建立生态系统的公司，这些产品是关键的推动者。

带Java平台的灵活STSAFE-J

STSAFE-J是基于GlobalPlatform®、Java Card™和专用小程序的灵活解决方案。它提供满足自定义应用要求的各种安全服务。

STSAFE-TPM标准化计算服务

STSAFE-TPM是一种可提供标准化可信计算服务的成熟解决方案(ISO / IEC 11889)，非常适合基于Windows或Linux的平台。该系列适用于消费、工业和汽车认证。

欲了解更多信息，请访问：
www.st.com/stsafe

细分市场中的STSAFE映射

消费电子
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

基础设施
网关、基站、实用程序

优化的**STSAFE-A**
为品牌保护和安全连接而调优

灵活的**STSAFE-J**
带可选默认小程序的灵活Java™平台

规范的**STSAFE-TPM**
适用于可信计算与加密服务的TCG标准化平台

可实现无缝安全性的STSAFE-A110生态系统

STSAFE-A110是最新的STSAFE-A安全元件，它具有最先进的安全功能，可防止假冒正品外设和IoT设备。其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）

- 用于安全密钥配置的预个性化STSAFE-A110
- Arduino™接口、驱动程序和源代码示例。

在线订购X-NUCLEO-SAFEA1：**www.st.com/stsafe-a110**

主要特性

- 可安全地建立TLS会话
- 采用基于CC EAL5+硬件的先进安全功能
- 符合USB Type-C标准和LPWAN身份验证要求
- 可根据客户需求安全地实施个性化

STSAFE-A110 封装

X-NUCLEO-SAFEA1

STPM4RasPI TPM扩展板

主要特性

- 经过测量的启动和平台完整性
- 身份验证和安全存储
- 密码工具箱
- 固件可升级
- Linux生态系统可用性
- CC EAL4+、TCG和FIPS 140-2认证
- 提供多种封装（QFN32、WLCSP、TSSOP20）

STSAFE-TPM可信解决方案环境

STSAFE-TPM是经过TPM认证的产品系列，可在扩展温度范围内运行。完整的开发套件可提供轻松集成。

- 可用于SPI和I²C接口的Raspberry PI®和STM32MP1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）
- 借助开源TPM软件栈和意法半导体合作伙伴网络，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**

M2M连接
ST4SIM

蜂窝网络连接是联网设备的关键赋能因素。它带来了更多样化的智能对象，并为新市场机会开辟了道路。

为满足市场需求，意法半导体提供采用ST4SIM解决方案的多样化量身定制连接产品组合，以及与物联网、工业和汽车级应用兼容的各种SIM和eSIM。

ST4SIM产品系列是完整生态系统的一部分，该生态系统由提供和运行设备车载和服务配置平台的可信赖合作伙伴构建。

SIM & eSIM

面向蜂窝网络连接工业和汽车应用

ST4SIM，随时随地建立连接

通过SIM和eSIM始终保持连接并始终处于控制之下

ST4SIM SIM和eSIM产品组基于基本型、加密型和GSMA SGP.02配置。我们的解决方案允许设备随时随地联网，同时确保资产安全。它们简化了远程状态监测和预测性维护等用例以及紧急援助等联网驾驶服务。

产品系列

ST4SIM-S用于物联网
- 基本型SIM/eSIM与加密型SIM/eSIM
- 可配置且可定制用于工业的ST4SIM-M

ST4SIM-M用于工业应用
- 基本型SIM/eSIM、加密型SIM/eSIM和GSMA SIM/eSIM
- 工业级（JEDEC JESD47）

ST4SIM-A用于汽车
- 加密型eSIM与GSMA eSIM
- 汽车级（AEC-Q100 2级）

主要特性
- 从可移除SIM到GSMA认证eSIM的可扩展产品
- 兼容Java Card OS / Global Platform
- 诸多可信合作伙伴提供的连接和平台
- 优质可靠的即用型解决方案
- 以多种外形交付（卡插件、FF2、WLCSP、TSSOP20）

欲了解更多信息，请访问：**www.st.com/st4sim**

安全汽车

ST33-A, ST4SIM-A

今天汽车行业约80%的创新都是直接或间接通过电子设备实现的。

随着互联汽车的增长以及汽车行业朝自动驾驶的发展，安全微控制器已被嵌入到车辆远程信息处理系统、网关和ECU（电子控制单元）中。

意法半导体将安全性作为这些趋势的核心，并致力于开发安全解决方案，以满足新数字技术时代的要求。

保护网关和远程信息处理系统

确保安全驾驶

ST33-A和ST4SIM-A，连接并保护汽车

嵌入在汽车生态系统中的安全解决方案

开发了互联车辆和汽车应用中的安全元件和嵌入式SIM，可防止服务和网络访问故障、设备克隆、伪造和数据窃听和损坏问题。它们涵盖了主要的V2X和车载功能（软件升级、ADAS、平台完整性、安全数据存储等），以确保乘客安全、车辆行为和数据隐私。

产品系列

适用于eSE和eSIM的ST33G1M2A硬件

- 在网关、防盗控制系统和远程信息处理系统中确保车载安全性
- AEC-Q100和CC EAL5+认证

适用于eSE的ST33GTPMA SoC

- 确保平台完整性
- 基于最新的TPM 2.0固件
- 通过FIPS 140-2和CC EAL4+认证

主要特性

- 从硬件到即用型解决方案的可扩展产品
- 汽车级解决方案
- 稳定可靠的产品

适用于eSIM的ST4SIM-A SoC

- 基于符合GSMA SGP.02规范的ST33G1M2A硬件
- 完整的车载连接解决方案
- 非常适合紧急呼叫设备（紧急呼叫）。

欲了解更多信息，请访问**www.st.com/secure-auto**

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：BRSMCU0620