

N32S0XX 系列安全芯片中间件及固件方案

简介

NSTurnkey-SmartToken 由 NSTurnkey-SmartToken COS 与 NSTurnkey-SmartToken API 组成。NSTurnkey-SmartToken COS 运行于 N32S0XX 系列安全芯片，将硬件安全设备的安全要素抽象化，形成通用的安全应用接口。在业务应用集成时无需关注硬件安全设备的具体实现。NSTurnkey-SmartToken API 是基于 N32S0XX 系列安全芯片（内含 NSTurnkey-SmartToken COS）的中间件，NSTurnkey-SmartToken API 包含了多种安全功能，接口丰富且易用，适配多种用户应用。

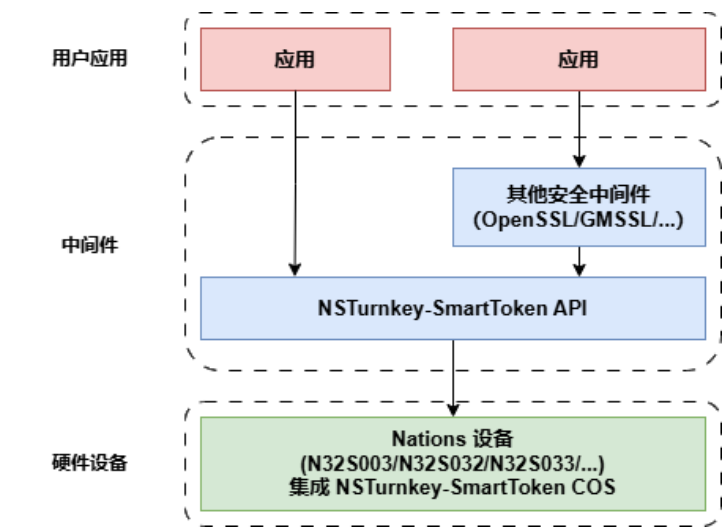


Figure 1 应用调用层次

即用的 SE 构建

- 芯片端零改造，无需二次开发
- 中间件易集成，极大降低导入工作量
- 成熟的硬件 API 接口，健全的方案，适配多种业务场景
- 支持接入 OpenSSL，GMSSL 等常见协议

完整的生态与技术支持

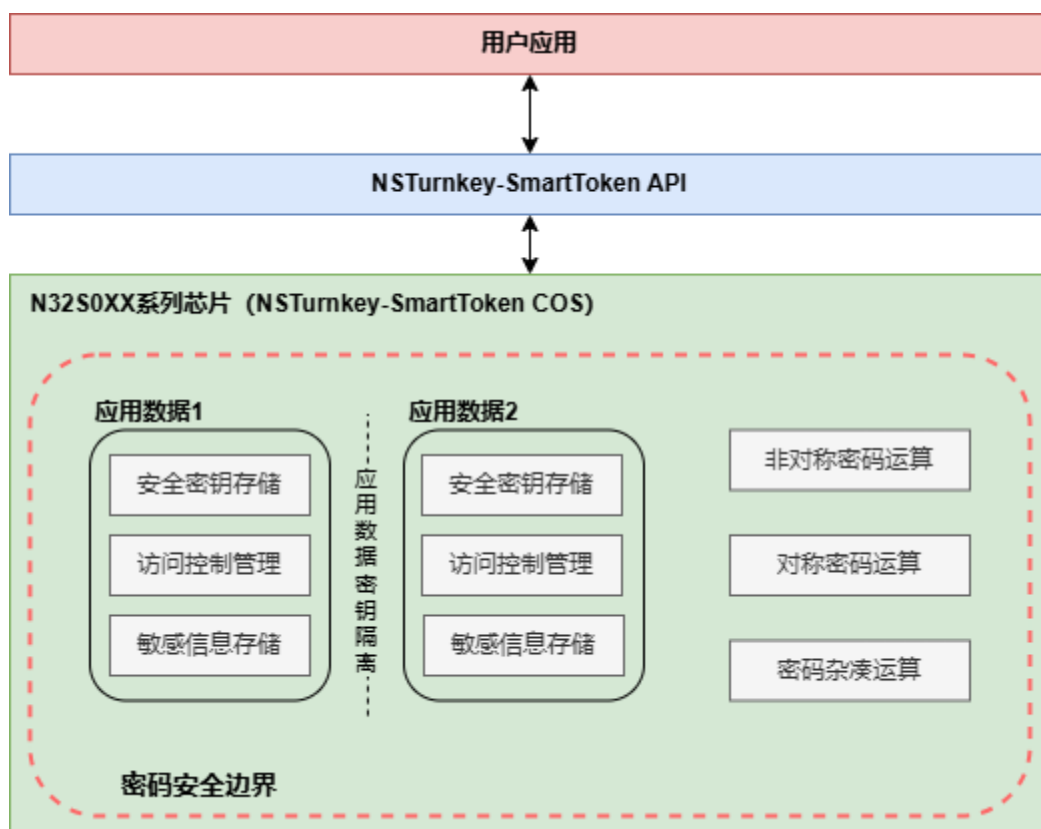
- 一站式的安全解决方案，直接对接业务侧
- 跨平台与互操作性，支持多种操作系统、设备与应用程序
- 提供丰富的产品选择，包括存储资源、通信接口、封装形态等
- 安全领域的合规性分析及咨询
- 提供产品、方案的安全分析与评估

标准化及高安全认证

- 支持 GM/T 0016 SKF 接口服务，国内通用的密码应用接口
- 符合 EAL4+ 安全评估
- 符合安全芯片二级、密码模块二级要求

整体框架

NSTurnkey-SmartToken 支持用户受控制管理和支配 N32S0XX 系列安全芯片的安全特性与功能。



安全特性

- 真随机数发生器
- 密钥生成/导入/导出/更新/删除等功能
- 数字签名与验证
- 非对称密码算法加密与解密
- 分组密码算法加密与解密
- 杂凑算法运算
- 密钥协商
- 权限控制
- 敏感信息与证书管理

声明：国民技术股份有限公司（以下简称国民技术）保有在不事先通知而修改这份文档的权利。国民技术认为提供的信息是准确可信的。尽管这样，国民技术对文档中可能出现的错误不承担任何责任。在购买前请联系国民技术获取该器件说明的最新版本。对于使用该器件引起的专利纠纷及第三方侵权国民技术不承担任何责任。另外，国民技术的产品不建议应用于生命相关的设备和系统，在使用该器件中因为设备或系统运转失灵而导致的损失国民技术不承担任何责任。国民技术对本手册拥有版权等知识产权，受法律保护。未经国民技术许可，任何单位及个人不得以任何方式或理由对本手册进行使用、复制、修改、抄录、传播等。