物联网安全芯片需求和应用白皮书

中国移动通信集团有限公司

中国移动物联网联盟

2018 年 12 月

前　言

近年来，随着物联网的迅速发展，物联网安全事件频发。一方面，物联网设备被利用于攻击互联网基础设施，如利用了大量摄像头的 Mirai 僵尸网络攻击事件导致大规模断网；另一方面，网络安全事件也深刻影响了物联网领域，如勒索病毒对物联网关键基础设施的攻击导致电网、工业控制系统、水处理设备等物联网关键基础设施失效。物联网设备一旦出现安全问题，除了带来财产损失，还可能造成人身伤害和公共基础设施被破坏，甚至危害生命安全和社会安定。

物联网终端形态和功能丰富多样，终端的软硬件能力和物联网业务系统的安全需求也千差万别，这些都为物联网终端和物联网业务的安全保障带来巨大的挑战。

安全芯片具有多种物理防御措施，能提供独立的数据存储和安全运行环境，具备出色的密码计算能力，可为物联网终端和物联网业务系统提供基于硬件的安全基础，构建安全应用环境，是满足物联网终端和业务系统安全需求的主要手段之一。

本册白皮书由中国移动通信集团有限公司研究院和中移物联网有限公司联合提出，旨在分析物联网终端的安全特性，剖析物联网终端的网络接入安全需求、数据安全需求和物联网业务安全需求，结合安全芯片的基础安全能力和性能特点，探讨安全芯片在物联网业务领域的应用和性能要求，指导物联网终端厂商和系统服务商合理选用安全芯片，提高整体物联网业务系统的安全。

目　录

1 安全芯片产业现状

1.1 安全芯片简介

安全芯片是在单一芯片上提供微型计算环境（包括 CPU，ROM，EEPROM，RAM 和 I/O 接口，以及密码算法协处理器和物理噪声源等），为上层软件提供安全存储、安全运算、密码算法计算等安全服务的硬件元器件，主要功能包括：

- 提供安全存储环境
- 提供安全运行环境
- 提供密码算法计算能力
- 提供随机数生成能力
- 自身安全防护能力

1.2 安全芯片类型

安全芯片的应用形态、接口多样，根据集成形式不同，可以分为以下三种类型：

- 可插拔独立安全模块形态：

通过标准外置接口与终端集成，例如:TF 密码卡和 UKey 等，市场有大量的相关产品，是使用最广泛的安全芯片产品。同时，也有通过自定义接插件集成的非标准硬件接口形态，主要应用于定制终端。

- 嵌入式独立安全模块形态：

通过贴片、焊接、合封等方式集成在终端主板上，由于集成难度相对较大，主要应用于定制终端。

- 内置非独立安全模块形态（inSE）：

在终端芯片中实现全部或部分安全芯片功能，通常由独立的 CPU 核实现，使其运行环境独立于终端芯片的硬件环境。

不同形态安全芯片的特性分析如下表所示：

	独立安全模块（可插拔）	独立安全模块（嵌入式）	集成安全芯片
性能	由安全芯片自身器件性能和接口类型决定		受接口限制目前较低
功耗	高	高	低
成本	高	低	无额外成本
集成稳定性	低	高	高
集成难度	低	高	低
适用终端	通用终端	专用终端	通用终端
主要应用场景	个人通信、移动办公、金融支付	个人通信、金融支付	金融支付

表 1. 安全芯片特性分析

安全芯片的性能主要取决于自身硬件处理能力和接口速率，自身硬件处理能力由 CPU、ROM、时钟频率等硬件决定安全芯片使用的主流接口情况如下表所示：

接口类型	速率
7816	230Kbps（USIM）
SD	10Mbps左右
SPI	数Mbps
I2C	100Kbps-3.4Mbps
USB1.1	12Mbps
USB2.0	480Mbps
USB3.0	理论4.8Gbps
UART RS232	20Kbps
UART RS422/RS485	10Mbps

表 2. 安全芯片主流接口

1.3 安全芯片分级

基于物联网业务的不同安全需求，在物联网场景下选择安全芯片时，除了考虑芯片的物理形态，内核、主频、存储空间等性能指标，接口、算法等功能指标，工作温度、存储可靠性、环境适应性等可靠性指标外，国家密码管理局定义的《密码模块安全技术要求》[7]也是对安全芯片密码安全能力判断的一个重要依据。该要求对密码模块的安全能力判定分为四级，对物理安全机制和访问控制机制的要求逐级增强。

- 安全一级规定了最基础的安全要求，例如：软件或固件模块可以运行在不可修改的、受限的或可修改的运行环境中，模块应当使用至少一个核准的安全功能或敏感安全参数建立方法。对物理安全机制、权限管控没有特殊要求。

- 安全二级提出了物理安全机制的要求，例如：增加了拆卸证据的要求，同时要求基于角色的鉴别机制，对权限控制进行了约束。
- 安全三级进一步提高了物理安全机制要求，能够以很高的概率检测到直接物理访问、安全模块的试用或修改、物理探测等行为，同时要求基于身份的鉴别机制。
- 安全四级是该评价体系中的最高安全标准，除包括较低等级中规定的安全要求外，还要求具备能够检测到物理破坏时自动清除敏感安全数据、多因素身份鉴别等安全能力。

1.4 主流安全芯片产品

TF 密码卡、eSAM 和 eSIM 是目前使用最为广泛的安全芯片类型，适用于不同的终端和业务场景，目前主流产品的基本信息如下：

- TF 密码卡

TF 卡形态安全芯片，通过 SD memory 方式与终端通信，功耗 100mW 左右，部分产品同时支持大容量存储。支持国际主流密码算法和国产商用密码算法，广泛应用于保密通信、移动办公等安全领域，一般都具有国产商用密码产品型号。

- eSAM（Embedded Secure Access Module）

eSAM 是将一颗具有操作系统（COS）的安全芯片封装在 DIP8 或 SOP8 模块中，做成一个安全模块，可以完成数据的加密解密、双向身份认证、访问权限控制、通信线路保护、临时密钥导出、数据文件存储等多种功能。支持国产商用密码算法和国际主流密码算法，目前广泛应用于智能电表、水电、燃气表、热力表和机顶盒等终端设备。

- eSIM（Embedded-SIM）

eUICC 是由 GSMA 组织联合运营商、终端厂商、卡商共同提出的下一代 SIM 卡技术标准。eSIM 的核心思想是将 SIM 卡硬件 eUICC 的生产与运营商签约数据的生产分离，eUICC 预先置入终端设备，其中不包含运营商签约数据；用户在开始使用终端设备后，以空中写卡方式从网络平台下载运营商签约数据，安装到 eUICC 中。

eSIM 的出现主要是作为下一代 SIM 卡技术，替代现有 SIM 卡，由于 eSIM 的载体安全芯片在处理能力、安全能力等方面的增强，也可以同时对外提供密码算法计算等安全能力，供系统或应用调用，实现通用安全芯片的数据加解密、身份认证等安全功能，达到只使用一颗安全芯片，可同时提供 eSIM 应用和通用安全芯片两种功能。

除以上三种安全芯片的产品形态外，内置安全芯片（inSE）是一种近年出现的安全芯片新形态，具有性能高、功耗低、成本低等优点，物联网是其未来应用的重要场景。inSE 内置于通用终端芯片，占用独立 CPU 核，RAM 和 ROM 空间一般为 128KB-256KB，共用外部通用存储空间，与独立的安全芯片相比，不带来额外的功耗。产品多遵循 JAVA CARD[13]和 GP[12]等标准，主要支持 RSA、AES、SHA256、ECC 等国际主流密码算法和国产商用密码算法，部分产品通过国家密码管理局密码模块的密码检测。目前最主要的应用场景为基于生物特征的身份认证和金融支付。

2 安全芯片相关政策

2.1 国家法律

2016 年 11 月国家发布《中华人民共和国网络安全法》[1]，指出对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度[11]的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。网络安全等级保护制度[11]要求四级及以上的系统使用硬件密码产品进行信息安全保护。

2.2 行业规范

金融行业领域中，2011 年 3 月中国人民银行发布《中国人民银行关于推进金融 IC 卡应用工作的意见》[9]，指出 2013 年 1 月 1 日起全国性商业银

行均应开始发行金融 IC 卡，2015 年 1 月 1 日起在经济发达地区和重点合作行业领域，商业银行发行的、以人民币为结算账户的银行卡均应为金融 IC 卡。

卫生行业领域中，2012 年 2 月卫生部发布《居民健康卡管理办法（试行）》[8]推动实现居民在各级各类医疗卫生机构就诊“一卡通”。居民健康卡可用于居民身份识别、个人基本健康信息存储、实现跨区域跨机构就医数据交换和费用结算等。

金融 IC 卡与一卡通的核心部件均为安全芯片。通过内置的安全芯片，金融 IC 卡与一卡通可以实现敏感数据的安全存储、身份信息的安全存储和识别以及金融数据的交易保护。

2.3 技术标准

国家密码管理局密标委发布的 GM/T0054-2018《信息系统密码应用基本要求》[6]，规定三级和四级等保信息系统[3]应该使用密码技术保障应用和数据安全；对于四级等保信息系统[3]要求采用符合 GM/T 0028[7]的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

在公共安全视频监控领域，由公安部提出的国家标准 GB 35114-2017《公共安全视频监控联网信息安全技术要求》[5]于 2018 年 11 月 1 日正式实施。该标准规定了公共安全领域视频监控联网视频信息以及控制信令信息安全保护的技术要求，适用于公共安全领域视频监控系统的信息安全方案设计、系统检测及与之相关的设备研发与检测。该标准将安全前端(摄像机)的安全能力由弱到强分为 A、B、C 三级。A 级可以使用软件密码模块实现安全能力，更高等级的安全能力需使用硬件实现。

在个人信息保护方面，信息安全测评机构、知名大学、公安研究所及阿里、腾讯等互联网公司共同起草的国家标准 GB/T 35273-2017《信息安全技术 个人信息安全规范》[4]对个人敏感信息的传输和存储提出要求，包括传输和存储个人敏感信息时，应采用加密等安全措施；存储个人生物识别信息时，应采用摘要等技术措施处理后再进行存储。

在智能锁方面，中国泰尔实验室联合中国电信、中移物联网有限公司及相关企业在电信终端产业协会（TAF）制订了《智能门锁信息安全技术要求与测试方法》[10]，该标准同时也得到了公安部的高度认可与支持，公安部也曾派出技术专家参与标准制定与讨论。

3 安全芯片应用现状

目前，安全芯片在智能手机中的应用已经十分普及。

智能手机被广泛用于移动办公、移动金融和移动娱乐等各个方面，面临着非法访问、假冒窃听，病毒木马等多种安全威胁。在日常生活中，智能手机的安全问题导致信息泄露、财产受损的事例层出不穷。在智能手机中，身份认证和数据保护的基础依赖于密码体系的密钥安全。由于智能手机操作系统复杂、应用繁多，密钥直接存储在手机的通用硬件中无法保证其存储和使用的安全。

目前，在智能手机中，为解决密钥存储和运行环境的安全，广泛使用可信执行环境（TEE）、安全芯片或两者相结合的方法对密钥进行安全保护，应用于移动金融、数字版权保护、生物特征认证、安全启动和固件升级等多个领域。

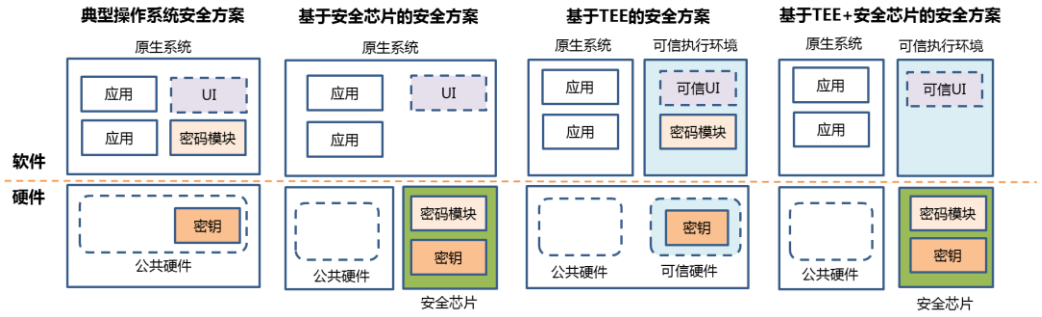

图 1. 智能手机中的安全方案

- 基于安全芯片的安全方案

安全芯片硬件元器件相对较少，容易建立物理防护措施和实施安全保障。安全芯片自身软件系统简单，相比于智能终端复杂或是开放的操作系统，具有更高的安全性，解决了复杂软件不可控易有漏洞的安全风险。

将密钥存储在独立的安全芯片硬件中，密钥在运行过程中始终不出安全

芯片，大大提升了密钥和密钥运行环境的安全。

- 基于可信执行环境（TEE）的安全方案

基于 TEE 的安全方案是一种介于纯软件实现密码模块和安全芯片作为密码模块之间的中间方案。TEE 访问的软硬件资源与普通操作系统隔离，TEE 提供授权安全软件（可信应用）的安全执行环境，同时也保护可信应用和数据的保密性、完整性和访问权限。普通操作系统及其上的应用程序无法直接访问 TEE 中的软硬件资源，需通过安全的 API 与 TEE 交互。

基于 TEE 的安全方案将密钥存储在由 TEE 隔离的可信硬件资源中，密码模块运行在 TEE 中，在 TEE 内还可提供可信的 UI 供用户进行敏感数据的安全操作。

基于 TEE 的安全方案解决了纯硬件密码模块在移动终端上部署不便的问题，提供了介于软件密码模块和基于硬件密码模块之间的一种适度安全。

- 基于 TEE＋安全芯片的安全方案

基于 TEE＋安全芯片的安全方案将密钥的存储和运算运行于安全芯片中，通过 TEE 提供可信的 UI 进行交互。该方案的特点是仅可以通过 TEE 访问安全芯片，为安全芯片的访问提供了安全防护，同时还可以为安全芯片的操作提供了可信的交互界面，从而全面保障了应用的运行安全。

除智能手机外，目前安全芯片还广泛应用于金融卡、交通卡等移动支付领域，确保支付过程的安全。安全芯片还用于移动通信模组，在传统的移动通信模组内加入安全芯片，利用安全芯片的密码模块，为通信模组提供加/解密功能，将普通的通信模组变为加密通信模组。

4 物联网安全芯片需求

4.1 物联网终端安全特性

4.1.1 终端类型繁多

物联网终端形态功能差异很大，既有通用智能终端，也有简单功能终端。

通用智能终端如智能手机、无人机、机器人等，设计复杂，具备智能操作系统，能满足多种功能应用。这种设备通常硬件配置高，外部接口较多，

支持多种网络接入方式，空间相对较大，成本较高。这类终端可参考安全芯片在智能手机领域的应用现状，保障系统、数据、传输、业务的安全。

简单功能终端如温湿度传感器、水电气表计等，设计简单，配备嵌入式或专有操作系统，仅满足单一功能应用。这种设备通常硬件配置不高，系统主频和存储受限，支持有限的网络接入方式。然而，在物联网应用领域，有些简单功能终端也需要承担高安全性要求的业务，还需兼顾性能、功耗的要求。这类终端需根据业务安全等级要求和软硬件资源的限制，选择合适的安全防护措施。

4.1.2 接入方式多样

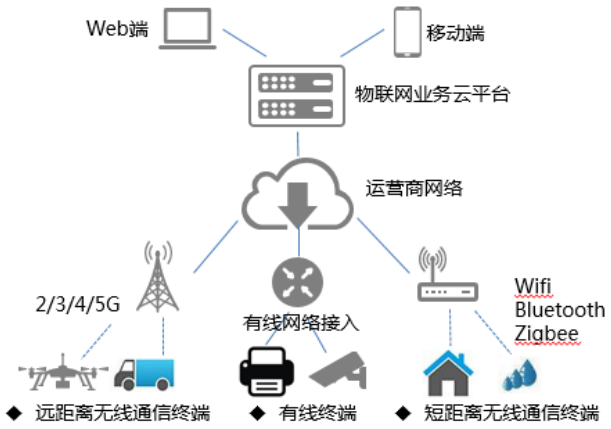

图 2. 物联网终端分类

物联网终端有多种网络接入方式，如有线终端、远距离无线通信终端和近距离无线通信终端等。

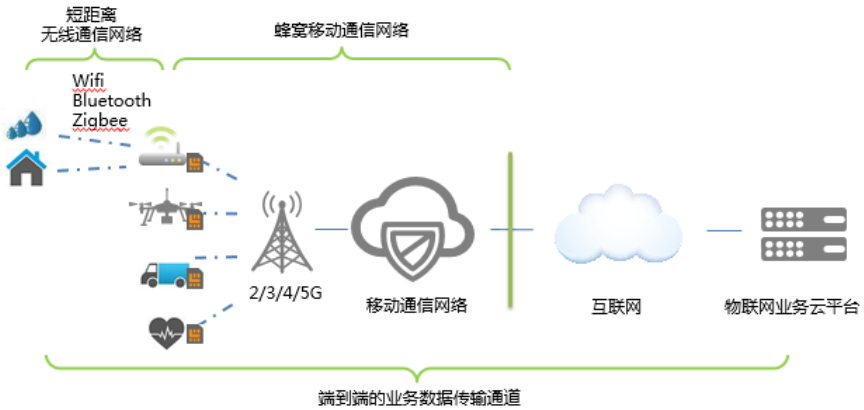

图 3. 物联网终端无线网络接入

远距离无线通信终端内置(U)SIM、eSIM 等，接入 2/3/4/5G 等蜂窝移动通信网络，与物联网业务云平台进行交互。典型的远距离无线通信终端如：

车联网终端、无人机、网关设备等。

终端接入移动通信网络需进行认证。通过认证后，移动通信网络为终端的数据传输提供安全的网络层传输。目前，接入移动运营商网络的身份认证模块，如(U)SIM、eSIM 等，通常置于安全芯片中，并在安全芯片内运行，用户的身份信息存储和相关的密码计算均在同一颗安全芯片中。安全芯片为物联网终端接入移动通信网络的身份认证提供安全的存储环境和计算环境，确保了身份认证过程的安全和基于身份信息的数据网络传输安全。

短距离无线通信终端通过 WiFi，Zigbee，Bluetooth 等短距离无线通信网络接入网关设备，网关接入蜂窝移动通信网络。典型的短距离无线通信终端如：智能家电、工业传感器等。短距离无线通信协议通常由特定的短距离无线通信芯片实现，在通信芯片中，提供短距离无线通信网络内的身份认证和传输数据的加解密功能。

除了上述通信网络提供的安全传输，物联网终端和业务平台之间还需考虑端到端的业务安全传输通道。

4.1.3 业务场景丰富

物联网终端支持的业务场景丰富多样，物联网设备不但应用于个人使用场景，还广泛应用于家庭和多种行业领域。物联网技术与行业信息化技术相结合，应用于智能制造、智能家居、智能电网、智能医疗和车联网等多个领域。

行业业务系统不同于个人应用场景，行业业务系统涉及面广、影响力大。有些系统涉及用户个人隐私和商业机密，数据一旦泄露，将危害个人生命财产安全或带来巨大的商业损失。有些系统涉及公共安全和国计民生，一旦遭到破坏，影响巨大，将危及公共利益和国家安全。

涉及面广、影响大的业务系统需要充分考虑端到端的安全设计，采取终端与业务平台的身份认证、数据的安全存储和安全传输等多种安全措施。

4.1.4 应用环境复杂

物联网终端的应用环境远比智能手机复杂，智能手机由个人进行保管和使用。物联网终端应用的环境更加多样，有些终端具有移动性的特点，活动范围大，移动速度快；有些终端无人机交互界面；有些终端部署在偏远地区，

无人值守，更新维护困难。

因此，物联网终端更易遭受物理攻击和人为破坏，导致终端失效、被仿冒、被控制和业务数据泄露，危害业务系统的正常运行。针对以上特点，需考虑对物联网终端配备不可复制的唯一标识和抗高强度物理攻击的安全部件。

4.2 接入安全需求

如图 4 所示，终端接入移动通信网络后，除利用现有移动通信网络安全措施保证网络层传输安全外，在应用层仍需要考虑从终端到业务平台的端到端业务安全。物联网终端与业务平台之间需要相互认证对方身份并且通过安全的通信通道传输应用数据。目前，较为普遍的方法是在终端部署安全模块，安全模块通常部署在安全芯片中，在云平台部署具有安全芯片的安全网关，物联网终端和业务云平台之间利用安全芯片的安全存储能力和密码计算能力，构建一个安全通道，解决端到端业务的传输安全。

图 4. 端到端业务安全

随着移动通信网络安全能力的不断增强和丰富，移动通信网络在基于终端已有的（U）SIM/eSIM 等安全模块进行网络接入的双向认证和安全传输的同时，也可为上层应用提供开放的认证能力和安全的会话密钥。

3GPP 在 Release 6 已经提出将运营商网络认证能力提供给上层应用的标准，即 GBA（Generic Bootstrapping Architecture）[14]。GBA 利用网络层认证和密钥协商的结果，为应用提供身份认证及应用会话密钥。3GPP 在 Release 15 针对轻量级物联网设备提出了 BEST（Battery Efficient Security for very low Throughout Machine Type Communication devices）[15]。BEST 着重强调低功耗和非 IP 协议的支持方案，并在会话密钥协商的基础上提供用户数据完整性和机密性保护。目前，针对 5G 网络的新架构特点，3GPP Release 16 正在研究基于 3GPP 凭证的应用层认证和密钥管理方案，即

AKMA（Authentication and Key Management for Applications based on 3GPP credential in 5G）[16]。AKMA 以 5G 网络中海量设备的接入认证需求及其应用的加密通信需求为切入点，研究 5G 网络中基于卡的业务认证和密钥分发方案，旨在向更多领域和行业应用提供运营商特有的安全保障。

4.3 业务安全需求

4.3.1 唯一标识需求

与用户使用智能手机登陆 QQ、博客、淘宝等应用不同，医疗设备、车载通信设备、传感器设备等物联网终端很多不具备人机交互界面，无法通过提供用户的身份信息来进行认证。

目前，物联网终端与业务系统的认证基于业务系统按一定约定为其分配的标识，且通常为软件实现。当业务系统不同时，标识也会随之不同。软件实现的标识容易被拷贝复制或篡改。安全芯片可生成具有唯一性、不可预测的真随机数，且具有关键数据不可被导出、不可篡改的特点，可用于唯一标识物联网终端。唯一标识可以是安全芯片产生的一串随机数，可以是从外部写入的一串随机数，还可以是基于某个随机数推演出来的 ID。

将唯一标识与使用者及归属企业进行关联，可以将使用者、物联网终端和归属企业建立有效绑定连接。实现企业对物联网终端的身份管理的同时，也可实现管理机构对物联网终端的监管。

4.3.2 数据源认证需求

传统终端使用业务场景通常是用户登录业务系统，业务系统验证用户身份并为用户提供服务。与传统终端的业务场景不同，物联网终端大多是直接连接业务云平台，上报业务数据和接受控制指令。

车载设备、智能摄像头、无人机等物联网通用智能终端与业务云平台进行数据交互，一旦接收到伪造的控制指令，会导致终端被远程操控，不能正常工作，甚至造成更严重的危害。因此，物联网终端不但需要进行身份认证，还应在每次消息交互时，对消息进行数据源认证。

安全芯片可以生成公私钥对，且私钥不可导出、不可篡改。物联网终端与云平台交互关键消息时，可以使用私钥对交互的消息进行签名，使用公钥

对交互的消息进行验签，以保证消息是由真实的物联网终端或云平台发送，保证数据来源安全。

4.3.3 业务传输机密性保护

涉及公共安全或对国计民生有重大影响的物联网业务系统，如：消防监控、电力监控、冷链设备监控、工业控制系统、车辆信息远程监控、车联网中的物联分析等，终端发送控制数据和业务应用数据如未经加密，在明文传输的情况下，业务数据可能被未授权获知，会对社会秩序、公共利益甚至国家安全造成损害。

业务传输机密性可以通过对传输的数据进行加密的方法来保证。物联网终端向业务平台发送数据时，它对数据进行加密，业务平台接收到数据后，对数据进行解密；反之，业务平台向物联网终端下发控制指令时，对数据进行加密，物联网终端对数据进行解密。

安全芯片可以产生唯一、不可预测的随机数、具备安全的密钥存储环境、安全的运行环境和密码计算能力，能保证终端加解密处理过程中密钥不被非授权获取，攻击者不能非授权获取到明文数据。实现业务数据在终端与业务云平台间的端到端加密传输。

4.3.4 业务传输完整性保护

涉及公共利益的物联网业务系统，如：环境监测、智能抄表等，终端发送的业务应用数据如被篡改，会对社会秩序、公共利益造成损害。

如果终端为单一功能终端，通常软硬件配置不高，很少具备安全防护措施。终端大多被部署在室外无人值守的环境，终端可能被恶意刷机或物理攻击。通过配置独立的安全芯片，可提供独立的密钥存储和运行环境，不需额外占用系统资源。安全芯片具有防物理攻击能力，可保证设备在无人值守的情况下的完整性运算不被破坏。

如果终端是无人机等通用智能终端，可采用和智能手机类似的安全芯片解决方案，实现业务数据在终端与业务云平台间的端到端完整性传输。

4.4 数据安全需求

终端本地数据的安全主要包括终端固件安全和关键数据安全。

物联网终端相比较于智能手机，通常人机交互较少，有些甚至是处在无人值守的环境中，终端系统和系统内的关键数据更易受到物理攻击和人为破坏。同时，海量连接的设备难于实时监控并进行及时的系统修复和升级，需要系统自身具备较强的抗攻击能力。

在物联网设备的启动过程中，可以利用安全芯片内置系统的可信根，对系统的启动过程进行逐级度量和载入，安全芯片中的可信根先于系统其他部分启动，并在完成对系统的可信度量后再将控制权交给原系统，确保系统固件未被篡改，保证系统初始状态的可信。

在物联网终端进行系统升级的过程中，利用安全芯片的身份认证能力和密码计算能力，对升级包的来源进行认证，对升级包的内容进行完整性校验，可以弥补物联网终端升级过程中人为监控过少或无法进行人为监控带来的安全风险，避免固件在升级过程中遭到篡改。

在终端内，可以将关键数据存储于安全芯片内，安全芯片提供了加/解密算法实现和专用的安全存储单元，存储用户的关键数据和加解密参数，实现对数据的加密保护和访问控制，防止数据泄露。或者使用安全芯片中的密码模块，对关键数据进行加密后存储在终端本地，加密保护使得数据在没有密钥的情况下不能被明文读取，防止对终端本地数据的非法访问。

5 安全芯片应用建议

5.1 保密通信

5.1.1 保密通信安全需求

随着移动通信市场的日益成熟和发展，安全问题已成为人们关注的焦点。在公众应用领域，我国已拥有全球最大的移动终端用户规模，据工信部统计，截至 2018 年 6 月末，我国移动互联网用户总数达到 13.4 亿户。在行业应用领域，随着行业信息化水平的不断提高，移动办公、移动商务、移动政务发展迅速。公众个人隐私、商业秘密、行业信息、甚至国家秘密都在公共移动通信网络传输，对保密通信提出了较高的安全需求。

5.1.2 安全芯片在保密通信的应用

鉴于安全芯片功能丰富、性能适中、体积小巧和功耗极低等方面的特点，能够与移动终端进行有效的集成，是解决保密通信安全需求的可行手段。更重要的是安全芯片以独立硬件形态提供安全的运算和存储环境，能够与移动终端的软硬件环境做到安全隔离，因此相较于纯软件密码模块具有更高的安全性。

在 VoLTE 加密电话应用中，安全芯片提供国产商用密码算法运算、证书私钥等密码资源安全存储、关键密码协议处理，以及随机数生成等安全能力。对于 AMR 12.2kbps、AMR-WB 23.85kbps 等编解码速率，对称算法处理性能小于 100kbps 的安全芯片即可满足需求。对于 VoLTE 视频加密电话应用，为了支持 VGA（分辨率 640*480dpi，帧率 15-30fps）和 720P（分辨率 1280*720dpi，帧率 30fps）的图像格式，安全芯片的对称算法处理性能则要提高到数 mbps。

在分组数据加密应用中，安全芯片支撑数据加密通道的建立，为移动办公、视频会议等上层应用的数据传输提供安全保护。为了适应上层应用对速率和时延等性能的较高要求，这就对安全芯片的对称算法处理能力提出了较高要求，对于视频会议、移动办公等高速业务，对称算法处理性能要求至少为数 mbps。

在本地安全存储应用中，安全芯片可以提供独立的存储空间供用户存储数据，也可以对用户数据进行加密后存储于移动终端的通用存储空间。如果提供独立空间存储，则根据具体业务需求由安全芯片提供数 GB 的存储空间。如果加密存储存储于通用存储空间，则需要安全芯片具备高速的对称算法处理性能，考虑到用户体验，至少需要 10mbps 级别。

信息安全作为一种隐形的能力，对于保密通信用户来说，不能以降低用户体验为代价来提高安全性，因此在保密通信领域应用安全芯片，要尽量减少其对终端和应用的影响。随着保密通信应用的持续发展和业务的不断丰富，对信息安全的需求将不断提高，这将对安全芯片在算法引擎功能、性能、功耗等方面提出更高的要求。

5.2 车联网通信

5.2.1 车联网通信安全需求

车联网是以车内网、车际网和车载移动互联网为基础，按照约定的通信协议和数据交互标准，在车与车（V2V）、车与路边设施（V2I）、车与行人（V2P）以及车与网络（V2N）之间进行无线通信和数据交换与共享的网络系统。它通过人—车—路—网之间的实时感知与协同来实现智能交通管理、智能动态信息服务和智能车辆控制的一体化，向用户提供道路安全、交通效率提升和信息娱乐等各类服务，满足人们交通信息消费的需要。

基于 PC5 接口进行直连通信是车联网典型的业务特征。在此场景下，车联网终端设备在工信部规划的 5905—5925 MHz 以及未来新增的专用工作频段上通过直通链路进行短距离信息交换，满足提高交通效率及道路交通安全、自动化驾驶等 V2V/I/P 车联网业务的需要。直连通信采用广播方式进行，在没有安全保护的情况下，车联网系统面临着虚假信息、假冒终端、信息篡改/重放、隐私泄露的安全风险，需要采取密码学方法来实现对终端身份、消息源、消息机密性、完整性等方面的保护。车联网业务中有关驾驶安全类业务的主要特征是低时延、高可靠。在时延需求上，辅助驾驶阶段要求 20~100ms，而自动驾驶阶段要求时延可低至 3ms。这对终端的安全实现提出了较高的要求。

5.2.2 安全芯片在车联网通信的应用

安全芯片功能丰富、不占用额外系统资源，是满足车联网安全需求的有效手段。更重要的是安全芯片以独立硬件形态提供安全的运算和存储环境，能够与车联网终端、系统设备的软硬件环境做到安全隔离，具有更高的安全性。

在车联网应用中，安全芯片提供国产商用密码算法运算、证书私钥等密码资源安全存储、关键密码协议处理，以及随机数生成等安全功能。对于 I2V 业务应用每秒 10 次的信息发送速率，车载终端非对称算法处理性能达到每秒 10 次的安全芯片即可满足要求。对于 V2V 应用，考虑车的快速移动性和实时响应的需求，安全芯片的非对称算法处理性能需达到每秒数千次。

在本地安全存储应用中，安全芯片可以提供独立的存储空间供用户存储关键数据，如：证书的安全存储等。由于证书大小通常可控制在数百字节，因此支持数 GB 存储空间的安全芯片能满足这方面的安全需求。

信息安全是车联网业务发展的重要保障，对于车联网系统及应用而言，需要兼顾低时延、高可靠的业务处理特点和车联网系统的安全性，因此在车联网领域应用安全芯片，其处理性能需要满足车联网系统的整体业务性能要求。随着车联网业务的深入开展和不断丰富，还会对安全保障提出更多要求，这需要对安全芯片在算法引擎功能、性能、功耗等方面的不断提高，以保障未来车联网业务的顺利开展。

5.3 智能家电

智能家电主要应用智能控制、传感器、RFID、网络通信和大数据云平台等技术，使家用电器从传统的机械式变成智能设备。智能家电联网的主流通信方式为：WiFi、Zigbee、蓝牙，NB-IOT，LoRa 等。智能家电和人们的生活息息相关，联网后一旦出现设备被攻击、被破解，被劫持控制等安全问题，会造成个人财产损失，严重的可能危及到家庭和人身安全。

智能家电除了考虑联网后自身的安全，还需考虑遵守国内外相关的数据保护法规，保护个人隐私。如：欧盟出台的一般数据保护条例[2]（General Data Protection Regulation，GDPR）和我国的网络安全法[1]。在 GDPR 中，要求考虑个人数据的匿名化和加密，确保处理系统和服务的保密性、完整性、可用性和可恢复性。我国的网络安全法[1]强调了网络运营者包括网络服务提供者需合法的搜集和使用个人信息，并且是个人信息保护的责任主体。

目前，主流家电厂家已使用或正在考虑使用安全芯片来保障智能家电的使用安全。随着 GDPR 的出台，出口的智能家电短期内有望将安全芯片作为产品标配。在国内市场，随着个人信息保护法律框架和国家标准的逐步形成，家电行业对信息安全的重视程度逐渐提高，对智能家电的安全保护措施也会愈加完善。

使用安全芯片进行设备身份认证和传输加密是安全芯片在智能家电领域的主要应用方式。在智能家里领域应用的安全芯片，需具备真随机数发生能

力和一定容量的安全存储。目前在智能家电行业中，通常的业务系统对算法的性能要求不高，根据业务系统的需求，需支持主流的对称、非对称算法或国密算法。由于家电行业出货量很大，安全芯片在智能家电领域的应用将会有广阔的市场前景。

6 总结

随着物联网终端设备的高度网络化，物联网业务的蓬勃发展，物联网终端的安全问题日益凸显，业务安全保护的需求也会越来越强烈。

安全芯片自身具备物理安全措施，提供硬件隔离的安全存储环境和运行环境、具备密码计算等安全能力，为物联网终端和终端接入业务系统提供基于硬件的信任根。以安全芯片为基础，可为终端构建安全的系统运行环境，进一步保障业务数据、业务应用的安全。在公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及一些终端或业务一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，建议发展物联网业务的同时，同步考虑以安全芯片为基础的硬件安全解决方案，确保业务获得较高安全的保障。安全芯片的形态多样，物理接口和性能也差别很大，面对物联网终端功能形态各异、业务应用丰富多样的现状，应合理利用安全芯片的基础安全能力，选择集成业务所需的安全芯片，为终端和业务云平台构建安全的业务应用环境，提高整个物联网业务系统的安全。

参考资料：

[1]《中华人民共和国网络安全法》

[2]《一般数据保护条例》 (General Data Protection Regulation，GDPR)

[3] GB/T 22239： 《信息安全技术 信息系统安全等级保护基本要求》

[4] GB/T 35273： 《信息安全技术 个人信息安全规范》

[5] GB 35114： 《公共安全视频监控联网信息安全技术要求》

[6] GM/T 0054： 《信息系统密码应用基本要求》

[7] GM/T 0028：《密码模块安全技术要求》

[8]《居民健康卡管理办法（试行）》

[9]《中国人民银行关于推进金融 IC 卡应用工作的意见》

[10]《智能门锁信息安全技术要求与测试方法》

[11]《网络安全等级保护条例（征求意见稿）》

[12] GlobalPlatform Card Specification

[13] Java Card Classic Platform Specification

[14] 3GPP TS 33.220: “Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA).”

[15] 3GPP TS 33.163: “Battery Efficient Security for very low Throughput Machine Type Communication (MTC) devices (BEST).”

[16] 3GPP TR 33.835：“ Study on authentication and key management for applications based on 3GPP credential in 5G.”