密九联

基于国密算法的物联网安全解决方案

技术白皮书

OLYM奥联
民族密码 奥联智造

深圳奥联信息安全技术有限公司

名词解释

IBC：IBC（Identity-BasedCryptograph）即基于标识的密码技术，是基于传统的 PKI(公开密钥基础设施)基础上发展而来，用户标识（如邮件地址）即是公钥，无需证书交互和验证过程，使安全应用易于部署和使用。

SM9：国家密码管理局发布的关于标识密码算法的商用密码算法。

SM4：国家密码管理局发布的关于对称算法的商用密码算法。

SM3：国家密码管理局发布的关于摘要算法的商用密码算法。

SM2：国家密码管理局发布的关于椭圆曲线公钥密码算法的商用密码算法。

文档版本：SIOT1901

发布日期：2019 年 4 月

目录

第 1 章　背景概述

1.1　物联网安全概述

在国家政策大力扶持下，中国物联网行业迅速兴起，目前连网的终端设备数量已经过亿，海量的终端接入形成了繁复交错的节点，同时也引入了各类的安全风险，物联网正在面临着严重的安全挑战。而面对接入设备的新型智能化、新兴恶意攻击手段不断提升，传统的网络安全、平台安全等防护措施已无法适应新安全形势的要求，各类物联网安全事件层出不穷。2016 年 9 月 20 日，Mirai（一种僵尸网络病毒，主要借助设备弱口令传播）针对法国网站中级 OVH 的攻击打破了 DDoS 攻击记录，最大达到了 1.5Tbit/s；2016 年 10 月，美国域名服务商 Dyn 同样遭受了大规模的 DDoS 攻击，使美工东海岸地区网络大面积瘫痪，终端设备停止服务；此外，2017 年 9 月，新出现了另一种 IoT_reaper 病毒，其不再依赖于破解设备弱口令，而是对物联网的漏洞进行攻击，存在更大的安全威胁。构建涵盖身份认证、数据保护等安全问题的防护体系是目前势必要解决的现实问题。

密码技术来作为信息安全的最关键防线，具备可靠性、安全性，国家密码管理局也已经发布了 SM9、SM4、SM3、SM2 等自主可靠的算法标准规范，基于算法的加密、签名可为物联网服务端、设备端、用户端提供安全支撑，快速、经济地解决敏感数据保护的问题。

本方案提供支持基于 SM9 算法的标识密码体系（IBC），结合密码技术和各软、硬组件，构建物联网安全保护体系，形成物联网安全解决方案，可实现身份认证、传输通道加密、数据安全保护、数据加密存储等功能，满足物联网平台现在及未来各项业务应用的安全需求。

1.2　物联网风险分析

1.2.1　身份认证风险

在物联网系统中，身份认证包括设备之间的认证、设备与用户、设备与平台之间的认证。传统的身份认证方式中，普通的用户名和密码认证方式，无法避免弱口令、撞库攻击、字典攻击等问题，大多数用户也没有定期更改密码的习惯；而采用数字证书认证虽然安全，但使用繁琐，在终端设备上安装控件或 KEY 驱动和管理程序等，使用极其不便。下图是现行的各种身份认证方式存在的弊端分析。

认证方式	弊端
普通口令认证	弱口令、口令截获、字典攻击、撞库、拖库
手机短信认证	认证费用高、伪基站、短信劫持、手机病毒
数字证书认证	部署成本高、必须安装插件、易用性不高
动态令牌	成本高、用户认证依赖独立设备、易用性不高、服务端密钥存在安全风险
指纹、虹膜等生物识别认证	部署成本高、终端适配要求高、实现难度大、易用性不高

表 1 各类身份认证方式分析

综上，要解决这些问题，需要一种兼顾易用性、安全性与兼容性的身份认证技术。

1.2.2 数据传输风险

物联网系统中数据传输过程中，一般都是明文形式传输，尽管有些采取了密钥加密的安全措施，但通常采用的是对称算法，加密解密为同一把密钥，一旦密钥被破解或被内部人员泄露，灾难将是延续性的，存在巨大的安全隐患；若是使用低强度密钥进行加密，依靠目前发达的计算条件，通过穷举等方式存在破解的可能，例如 DES 算法已经证明被破解。

在物联网系统中的智能摄像头、智能家居等应用环境中，海量终端设备，网络环境复杂，安全漏洞较多，在业务交互过程中，一旦网络被监听，数据即被窃取或篡改，造成敏感或重要数据泄露，将带来巨大的灾难。

1.2.3 数据存储风险

物联网数据存储风险主要表现在云服务端和终端设备两个方面。在物联网云服务端，数据集中和新技术的采用是产生云存储安全问题的根据，由于云计算的技术特性，多租户、资源共享、分布式存储等这些因素加大了数据保护的难度，增大了数据被滥用和受攻击的可能，因此云端数据安全保护是必须解决的问题；在终端设备，由于大量的感知设备暴露在复杂的社会环境中，受攻击的风险大大增加，遭到暴力的攻击和破解，终端设备上存储的采集数据、用户数据、业务数据一旦被窃取，将造成用户隐私数据泄露，带来严重影响。

1.3 传统解决方案面临的问题

1.3.1 基于口令和对称密钥等的方案

传统的身份认证方式中，通常是普通的用户名和密码，设备或用户使用默认密码或弱口令，无法避免撞库攻击、字典攻击等问题，存在身份认证的安全漏洞，比如僵尸病毒就是基于弱口令的漏洞进行攻击的，故引入基于对称算法的密码机技术，增强安全性。

在基于对称算法的解决方案中，加密解密均是同一把密钥，在物联网应用中，在终端设备中预置相同的密钥，通过加密随机数实现身份认证和加密数据实现信息安全的方式，但此种方式存在密钥被内部人员泄露、低强度加密易破解、密钥分发和更新困难等的的问题。

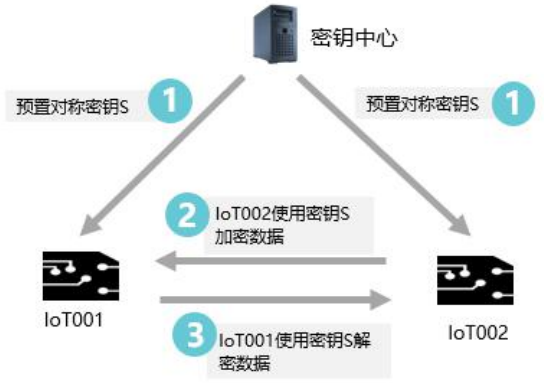


图 对称密钥加密过程

在物联网系统中，尽管对称算法的速度快、资源消耗低，但密钥分发和更新难、密钥和数据安全性低是基于对称算法的解决方案的硬伤，目前难以有效的解决，一旦密钥或数据被窃取和泄露，特别是物联网系统中存在海量的终端，将会造成大面积的瘫痪。单纯的使用对称算法不具备物联网对安全性的要求。

1.3.2 基于 PKI（Public Key Infrastructure）的密钥体系

基于对称算法的安全方案存在密钥分发困难、密文可被破解等问题，引入对称算法与非对称算法相结合的密钥体系，即 PKI（公开密钥基础建设）体系，相较于对称算法，用户端可自己生成密钥，保证了密钥的安全性和唯一性，非对称算法运算复杂，加密强度更大，通过交换数字证书的方式更轻易的实现两个陌生实体之间的身份认证。

在物联网应用 PKI，即是将各个设备作为主体，在设备发行使用之前需要申请和预置设备自身的设备证书，在与外界交互过程中通过证书完成身份认证、非对称加密签名等过程。

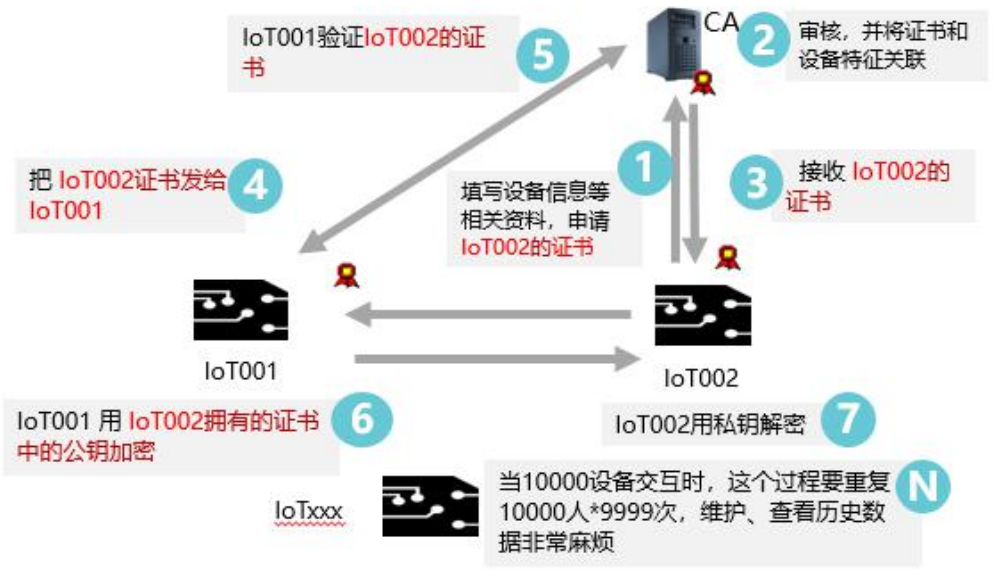


图 PKI 体系中加密过程

虽然该体系具备完善的密钥管理体系，但在物联网应用时存在以下问题：

- **证书管理和维护复杂。**目前物联网设计的终端数量一般是千万级，千万个设备就要创建和维护千万张证书，与这些证书相关的密钥要不断更新，旧密钥还要保存起来。持有证书的设备销毁后，就要撤销相关证书，因此，撤销列表也要维护、发布及不断更新。增加了数字证书管理的复杂度和维护成本；
- **通信和存储开销增加。**当设备之间进行身份认证、密钥协商时，双方需要先交换数字证书，降低了通信效率，且证书还要存储在本地，占用了存储资源。

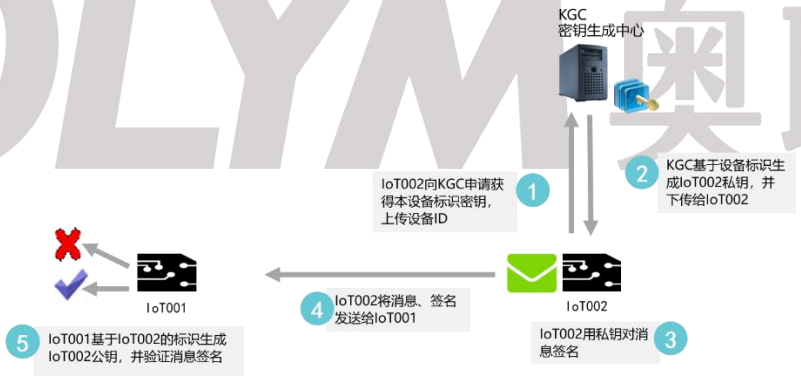
因此，在终端数量众多的物联网中，该体系不满足高性能、经济性、易用性的安全要求。

第 2 章　技术路线

2.1　基于身份标识的密钥体系

为解决 PKI 密钥体系的证书管理复杂、通信和存储开销增加等问题，本方案使用了基于 SM9 算法的标识密码技术（IBC,Identity-Based Cryptograph），该体系通过使用芯片、设备等特征值（如 ID 号等）作为标识公钥，不需要繁杂的证书管理和交换、验证等环节，可实现基于标识进行身份认证和加密等各种安全应用，特别适合物联网这种用户数巨大、点对交互频繁而随机的使用场景。

相较于 PKI 体系证书管理的复杂性，IBC 体系中只需托管一套私钥和公共参数即可，设备等实体凭标识从 KGC（密钥生成中心）申请密钥，无需申请和存储证书，减低了维护难度；在设备之间、设备与物联网平台之间进行身份认证、数据加密、数据签名时，不用交换数字证书，只需交换双方标识即可，减少了通信开销；且物联网平台部署在云端，IBC 体系的安全服务也可在云端开展，向设备分发密钥，符合物联网的技术特点。



图：采用 SM9 算法实现签名/验签流程示意图

IBC 在物联网中的优点总结如下：

- 设备标识可作为公钥，节省了数字证书发放成本，方便了端点之间的交互；
- 节省了 PKI 中繁琐的证书链验证时间，提高了通信效率；
- 基于非对称算法的加密和签名运算，保证了数据传输的安全性；
- 使用方便，易用、可操作性好；
- 基于标识，可提供灵活的安全策略控制；
- 成本低，设备管理和用户管理简单，适用于设备数量级较大的系统，契合当前物联网需求。

1.1. 体系比较

综合 PKI 和 IBC 密钥体系，进行比较，结果如下表：

对比内容/密钥体系	PKI 密钥体系	IBC 密钥体系
密钥预置复杂度	密钥由芯片自身生成，但还需预置证书，复杂度高	只需预置密钥和公共参数，复杂度低
密钥更新复杂度	密钥与证书绑定状态，复杂度高	改变标识即可，复杂度低
密钥管理复杂度	证书管理复杂	基于用户自身标识，管理简单
运算资源消耗	基于非对称算法和证书交互，资源消耗最大	基于非对称算法，但较之 PKI 消耗低
身份认证复杂度	需交换证书，复杂度高	标识即公钥，效率高
加密传输安全	非对称算法加密，安全性高	非对称算法加密，安全性高
签名抗抵赖	强抗抵赖性	密钥由信任中心分发，抗抵赖性较弱
存储安全实现	易于实现	易于实现
策略控制实现	基于证书，实现较复杂	基于标识，易于实现
系统规模	适应于小型物联网	适用于任何规模物联

第 3 章　解决方案

3.1　方案概述

本方案基于 SM9/SM3/SM4 国密算法及标识密码密码体制，结合包括物联网安全管理平台、密钥基础设施、安全中间件的软、硬系统或设备，贯穿物联网云管端用多个方面，提供基于电子签名的挑战应答、 数字信封等安全机制，可以快速实现身份认证、传输加密、存储加密、数字签名等功能，解决物联网系统中身份认证、数据安全等安全问题，构建物联网安全防护体系。

在物联网应用中，以芯片标识、IoT 设备标识、用户标识、标识、业务标识等信息作为公钥，利用可信赖的密钥管理中心安全分发和管理密钥，不需要申请和交换证书，从而降低密码系统应用的复杂性。通过 SM9 算法和 SM3 算法相结合完成数据签名过程，实现数据完整性和不可抵赖性；SM9 算法和 SM4 算法相结合基于数字信封或密钥协商技术完成数据加密传输和安全存储，实现数据私密性和安全性。

3.2　总体架构

依据物联网安全需求和标识密码技术特点，本方案总体架构如下：

物联网由应用系统、物联网运营平台、设备/芯片生产系统、终端应用组成，贯穿云—管—端三个层面，提供全部物联网服务。在防护体系中，由安全管理平台、密钥基础设施、安全中间件组成，提供用户、终端、平台、系统的全方位的安全支撑，实现密钥安全分发、身份认证、数据加密/签名等安全服务。且当业务、芯片、设备客户规模较大时，一般的物联网运营平台托管模式无法适用于其大量的密码服务和资源需求，本方案支持客户 VIP 模式，可单独管理和使用自己的密钥基础设施；且同时直接在客户系统端直接部署密钥基础设施，独享全部资源，实现灵活的基础设施建设。

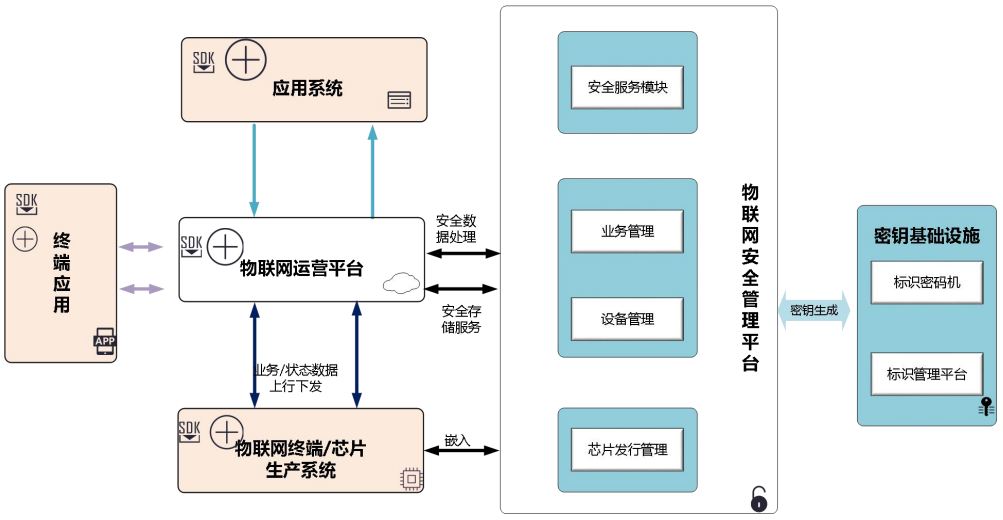


图 总体架构

密钥基础设施：包括密码机和安全管理平台。密码机可集群部署，提供 SM9、SM4 等密钥的生成和管理服务；标识管理平台提供用户、芯片、终端、业务系统服务端的标识管理、身份鉴别等服务。

安全管理平台：由芯片发行管理、终端管理、业务管理、日志审计等组成，基于身份安全、数据加密传输、数据安全存储、数据签名验签技术手段为物联网平台提供初次发行、二次发行、终端激活、业务管理、数据传输和存储等过程中的安全支撑。

安全中间件：安全中间件符合国家商密算法 SM9 技术标准，支持 SM9/SM3/SM4/SM2/RSA 等算法，支持 object-c、C/C++，C#等多种开发语言，支持 Linux、Android、iOS 等多系统，可实现快速集成，为平台、终端、终端应用提供身份认证、数据加密、数据签名等安全服务接口，实现密码服务。

终端应用：包括模组、安全芯片、智能网关等各种支持 SM9 算法的终端设备或应用。

3.3 相关产品介绍

3.3.1 SM9 密钥基础设施

3.3.1.1 简介

密钥基础设施包括标识密码机和标识管理平台，为物联网提供基础的密码服务，可部署在安全管理平台端，托管客户系统（业务系统、设备/芯片生产系统）的密钥，也可部署在客户系统客户系统服务端，由客户直接管理。

标识管理平台分为前端和后台管理，提供用户标识管理、密钥管理、数据库管理、划分企业组织、日志管理等功能。

标识密码机除了支持各类传统的密码算法如 SM2、SM3、SM4 国家标准密码算法和 AES、DES、3DES、SHA 系列、RSA 等国际算法外，特别支持 SM9 标识密码算法。提供包括 SM9/ SM4 等密钥生成、数据的非对称加解密、消息的签名验签、数据的对称加解密等功能。

3.3.1.2 主要功能

标识管理平台是基于 IBC 技术的集中管理平台，通过和标识密码机（KGC 密码机）的配合使用，可完成系统初始化、主密钥与公钥参数生成和保存、用户私钥的申请审核、生成、下载/分发、恢复、撤消等功能。提供以下服务：

- 系统管理：标识管理平台的初始化及设置，主私钥与系统参数管理、系统用户标识的管理；
- 安全管理：平台自身的管理，包括中心用户管理，口令修改、安全审计和认证与授权；
- 标识管理：提供用户标识管理，包括增加、删除、查询统计等；
- 用户管理：提供平台下所有企业用户和个人用户账户信息的审核、增加、更新和删除等功能；
- 密钥管理：提供标识密钥的整个生命周期和密钥相关安全属性的管理，包括密钥的申请、分发、更新、撤销等；
- 组织管理：提供对企业用户及其下级组织的管理功能；
- 日志管理：提供用户操作日志和业务管理日志的查询管理功能。

标识密码机可实现密钥生成—分发—启用—禁用—销毁的全生命周期管理、设备管理、访问控制等功能。支持各类密钥运算服务，如数据的非对称加解密、消息的签名验签、数据的对称加解密、消息认证码的计算、消息摘要的计算、PKCS7 和 S/MIME 数据格式的封装和解封装以及如短签名、格式保留加密等。密码机为应用程序提供了 API 编程接口，提供 Windows、Linux 系统的 API 开发接口文档和相关库文件。支持密钥导入、导出时,密钥均处于加密状态，支持密钥备份，支持双机热备。

密码机还可通过专用管理终端进行密码管理，可完成：

- 密钥管理：提供对密码机进行密钥生成、密钥查询、销毁等管理功能；
- 访问控制：基于 IP、口令等多方式控制对密码机的安全访问；
- 设备管理：提供对密码机进行日志管理、事件管理等
- 此外还提供，系统管理、系统裁剪等功能，简化密码管理流程。

3.3.2 SM9 安全管理平台

3.3.2.1 简介

安全管理平台系统架构如下图：

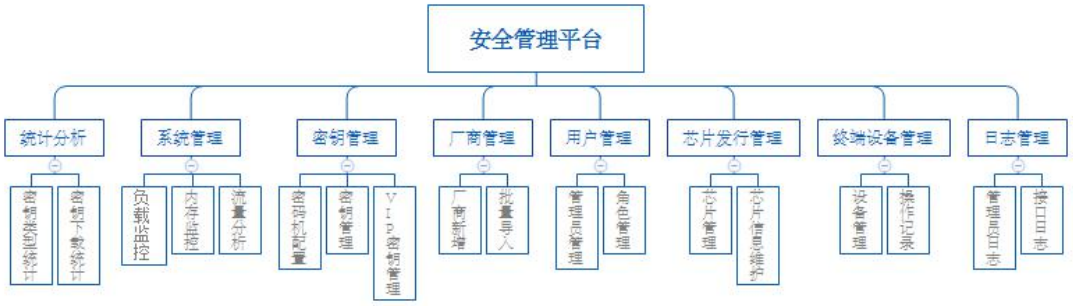


图 系统架构

安全管理平台架构由密钥管理、厂商管理、用户管理、芯片发行管理、终端设备管理、系统管理、统计分析、日志管理功能模块组成，涵盖了物联网安全管理中的芯片注册发行、二次发行、业务管理，支持 IBC 密码体系。

3.3.2.2 主要功能

1） 密钥管理

安全管理平台提供密钥管理功能，支持生成和管理 SM9 标识密钥、SM4 对称密钥，SM4 对称密钥用于生成 API KEY，完成厂商业务平台（芯片厂商、设备厂商、业务厂商）等的安全接入，支持生成和管理芯片、设备、厂商服务端的 SM9 标识密钥，实现密钥加密下发、数据加密、数据签名等安全服务，另外，支持 VIP 模式，提供包括 VIP 芯片、VIP 设备、VIP 服务端等密钥生成和管理。该模式旨在解决大规模的应用厂商需求，因其终端设备、业务规模、业务并发数量庞大，托管的共用的密码机无法支撑业务量，则可选择 VIP 模式，即可拥有专属的密码机。独享全部的密码机资源，实现高性能、高可用。

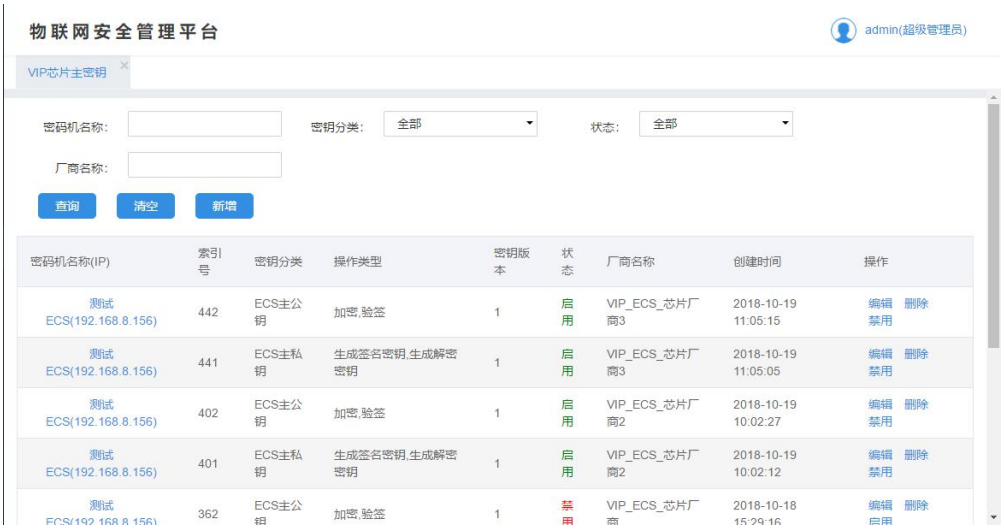


图 VIP 芯片主密钥

2） 厂商管理

安全管理平台提供厂商管理。本平台所指的厂商包括芯片厂商、设备厂商和业务厂商， 芯片厂商指负责芯片灌装的厂商；设备厂商指负责设备生产的厂商；业务厂商指物联网应用类的厂商。对厂商均支持基本的新增、清空、综合查询、导入等操作，便于用户操作。

3） 芯片发行管理

安全管理平台支持芯片密钥的离线发行和管理，实现芯片密钥的初始的灌装。支持基本的新增、清空、综合查询、导入等操作，同时在主界面上，支持添加芯片类型和显示芯片列表，包括了该芯片的厂商、标识、启用/禁用状态等属性。

4） 终端管理

支持终端设备管理，可添加和维护终端设备。支持终端激活，提供二次发行过程中设备密钥的生成和分发功能；支持终端的分类管理，同时支持日志记录功能，实现数据可回溯性。

5） 用户管理

安全管理平台支持平台角色管理和管理员管理，具备基本的增、删、改、查等管理功能。

6） 其他管理

安全管理平台还支持日志管理，实现操作可回溯，便于之后的安全审计；支持密钥统计，便于用户做行为分析；支持系统管理，实时监控系统运行状态、网络流量等。

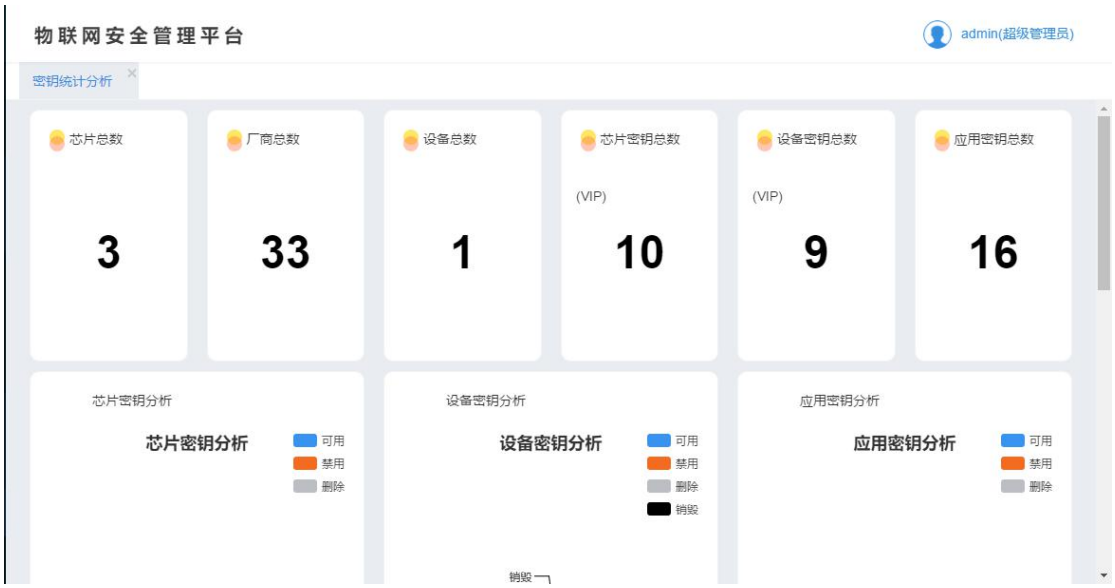


图 密钥统计

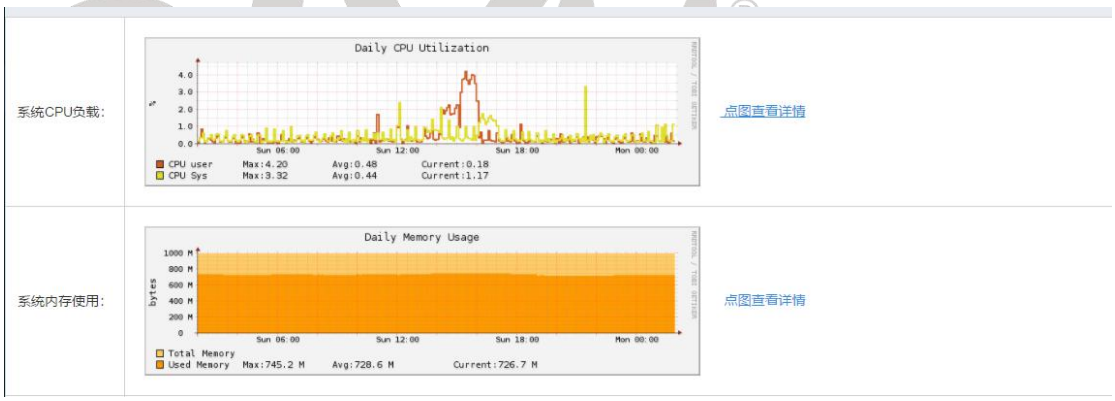


图 系统监控

3.3.3 SM9 安全中间件

安全中间件可应用于客户端和服务端，可集成在客户业务系统和生成系统、物联网平台、终端应用系统、终端应用上，支持 SM9/SM3/SM4/SM2/RSA 等算法，集成到应用系统能快速实现安全服务功能，数据格式符合业界标准，且可兼容已有的业务，通过对大量接口封装，简化开发和使用过程，适应性强。通过 SDK 和密钥基础设施结合，即可实现安全应用升级。让各种应用系统实现身份认证、数字签名、数据加密等功能。主要特点有：

1） 内置常用功能接口

安全中间件提供对文件、字符串、流媒体等用户数据的加解密、签名验签接口。向上提供了统一的应用层接口，该接口需具有不变性、可扩展性、易用性特点，客户可以在不同的开发平台通过应用程序接口作二次开发，向下支持各种 USB 设备、SD/TF 设备以及硬件加密卡。接口支持 RPC、SOAP、EJB/JMS 和 SOCKET 四种方式与密码中间件进行通讯

2） 多种开发语言支持

支持 object-c， C/C++, C#, DELPHI, JAVA，PASCAL, PHP，脚本(com 组件)等开发语言，其它的语言可以使用提供的 CLI 来扩展使用。

3） 多种系统支持

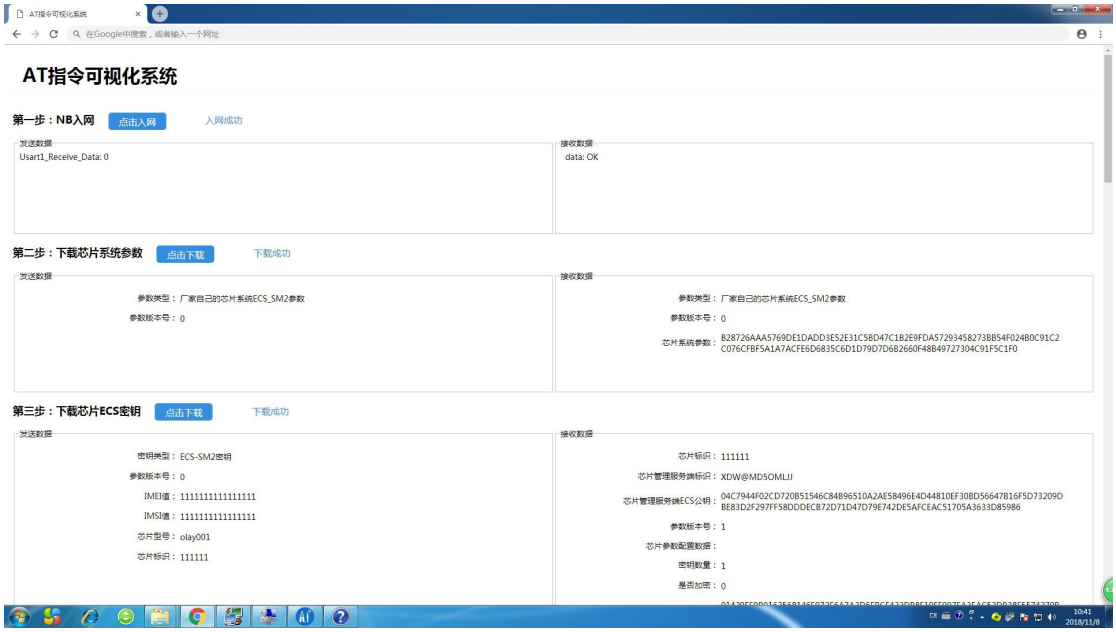
- WINDOWS：WINDOWS 2000, WINDOWS 2008, XP，VISTA, WIN7/8/10
- LINUX：FreeBSD, Red Hat, Ubuntu 等
- ANDROID：Android 8.0 以上
- IOS：iOS12.0 以上

3.3.4 SM9_NB 模组

我公司设计的 NB-IoT 模组，基于国产芯片组开发的窄带物联网无线通信模块，符合 3GPP 标准中的频段要求，具有体积小、功耗低、传输距离远、抗干扰能力强、随时在线、通讯成本低等特点。内置 SM9 密码算法，可为智能门锁、各种传感器等提供低成本的安全通讯通道。

3.3.5 SM9 物联网开发套件

我公司提供的基于 SM9 算法的物联网开发套件，可实现 SM9 密钥的申请、下发、身份鉴别、数字签名等等功能。提供详细的范例代码，支持主流的开发环境。



3.3.6 其他相关产品

本方案可根据需求，支持不同的模式，如：模组可集成 SIM 和 SE 模块、芯片使用 eSIM 技术等，可应用于 NB-IOT 等多种应用场景。随着产业界对 SM9 的认知程度越来越高，支持 SM9 算法的其他产品越来越多。

3.3.6.1 安全芯片

本方案支持市场上主流厂商的 GSM/GPRS/NB-IOT 等多种通信制式芯片，可完成密钥写入、加密、解密、签名、验签等，可完美对接 OneNET、天翼物联等主流的物联网平台，可应用于车规级、工业级、消费级物联网。

我司已完成多款 MCU、安全芯片的算法移植和测试。包括紫光同芯微电子有限公司 THD89、上海复旦微电子集团股份有限公司 FM1280、天津国芯科技有限公司 CCM3310S-T、意法半导体 STM32F407VET6、意法半导体 ST NUCLEO-L476RG、杭州晟元芯片技术有限公司 AS56、上海爱信诺航芯电子科技有限公司 ACH512、北京中电华大电子设计有限责任公司 CIU98320B、上海庆科信息技术有限公司 MK3080B 等。

3.3.6.2 模组支持

本方案支持主流的 NB-IOT 模组、工业级模组等类型，经测试，可实现安全服务功能并有着优良的性能，模组测试支持中国电信、中国联通、中国移动运营

商 2G/3G/4GSIM 卡，可实现与物联网平台的无缝对接。可应用于智能门锁、智能摄像头、智能燃气表、智能井盖、智能家居、智能停车等诸多应用场景。

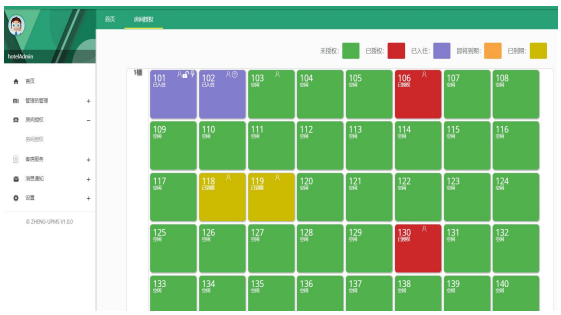
3.4 典型应用

以上解决方案还可以和其他应用结合，形成多种安全解决方案。

3.4.1 密九锁

我公司自研的密九锁，内置 SM9_NB 模组，采用基于国密 SM9/SM3/SM4/系列算法，结合 CHAP 挑战应答等机制，可以提供身份认证、安全存储、数据加密、数字签名等功能，实现 APP 到平台和锁的强身份认证、门锁权限定向分享、门锁状态查看等功能，服务端可实现门锁权限管理、门锁报警管理等管理功能。解决联网智能锁系统中身份认证、数据安全、传输安全、访问控制等多种安全问题，构建完善的智能门锁保护体系。

在整个通讯过程中均使用了国产密码算法，无用户名密码，所以不用担心黑客的口令、字典等攻击。所有数据在传输和存储中均是密文，密钥管理遵循国家相关技术规范。



3.4.2 加密摄像头

传统摄像头面临身份认证脆弱、视频数据明文传输等安全问题，因此导致的摄像头泄密事件频发。本方案以 SM9 算法为核心，使用下一代传输安全协议 NTLS，以摄像头设备 ID 或手机号等唯一的标识作为公钥，无需管理、验证、维护数字证书，实现网络摄像头访问的增强身份认证、视频传输加密和存储、监控定向分享等安全功能，且提供用户端、设备端、服务 SDK，可实现快速开发。

3.4.3 工控安全

当前工业领域的智能化、网联化程度越来越高，但是在工控安全领域仍没有得到长足的发展，多数工业系统在设计之初是封闭的“单机系统”，很多工控系统和设备没有防护措施，越来越多的安全风险暴露了出来。

可采用基于 SM9 算法的标识密钥体系，以设备 ID 为标识公钥，写入设备私钥，在工业控制元件中集成本方案软件开发包，基于标识实现设备识别与访问控制，可以实现设备身份认证、权限控制、数据加密等功能，构建工业控制系统信息安全体系。

3.4.4 智能家居安全

智能家居的出现给用户带来便利，用户很方便地通过智能手机、平板电脑和网络门户来控制，但家居联网生成的关于我们生活的数据会被储存到某家公司的服务器上，成为黑客、恶意软件和非授权用户攻击的目标，进行数据入侵，盗取用户隐私，甚至造成更严重的破坏。

智能家居场景中，可部署基础密钥设施，为用户分发 SM9 标识密钥，并将家庭路由器升级为智能安全网关，网关密钥可托管在密码机中，用户通过网关控制设备时，可基于密码技术实现用户强身份认证、安全接入、访问控制等安全功能。用户通过客户端应用程序，认证身份后，建立加密传输通道，可以访问指定的家庭网络中的其他家具设备，包括 IP-TV、摄像头、空调、冰箱等一系列基于网络访问的设备。

3.4.5 充电桩安全

电动汽车的发展迎合低碳经济的趋势，正在逐渐兴起，市场上出现了物联网的智能充电桩，用户可以通过手机应用在线支付使用充电桩，但目前通过无线或有线的网络传输没有加密措施，一旦遭受攻击，将会造成用户隐私数据泄露。

建设基于 SM9 算法物联网安全方案，可为用户端、设备端、接入平台端分发密钥，使用充电桩时，可实现用户身份认证、数据加密传输，且用户数据和平台数据可基于 SM4 对称算法进行加密存储，全过程保护数据安全和用户隐私。

3.4.6 智能井盖安全

基于物联网信息技术的“智能井盖”，可对周围环境进行数据采集，上报给远程监管平台，实现统一的数据处理，但在复杂的物联网环境中，缺乏有效的实时监控及管理手段，存在着身份认证、数据安全等安全问题。

可采用基于国密 SM9 标识密码技术为智能井盖提供安全支撑，通过硬件智能化、连接网络化、数字可视化，为用户提供安全身份认证、数据加密传输等服务，在井盖智能化的同时，实现控制和防护安全。

第 4 章　方案优势

4.1　安全功能

4.1.1　强身份认证

采用基于 SM9 算法的强身份认证技术，以设备 ID 或者用户手机号为标识公钥，分发专属私钥，无需证书认证等繁琐的过程，无用户名密码传递，杜绝了弱口令、暴力破解、撞库攻击等安全问题，使用私钥签名、公钥验签的方式，再结合 CHAP 挑战应答机制，实现终端与终端、终端与平台、平台与平台、用户与平台之间的强身份认证。

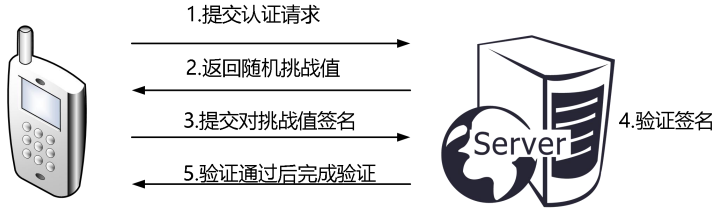


图 挑战应答机制

4.1.2　数据安全传输

在复杂的物联网环境中，要求数据网络传输的私密性，防止被窃取。在实体双方通信过程中，那个对称密钥加密、数字信封技术，数据在网络中均是密文的状态，保障物联网平台数据传输安全。

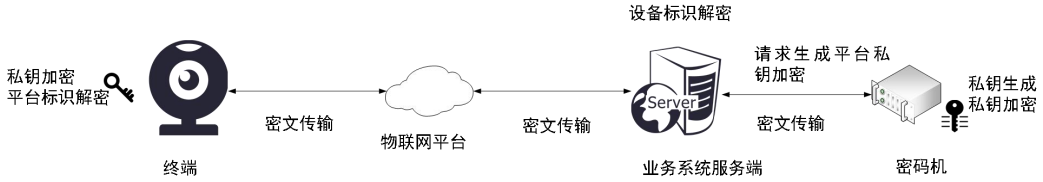


图 数字信封加密

4.1.3　数据加密存储

在物联网终端设备、各类平台，采用数据加密存储机制，支持基于国密 SM4 算法对本地存储数据进行加密，从根本上实现安全防护，即使数据被监听、窃取、非法访问，因为数据已经为密文状态，不会造成重要的、隐私的信息泄露，保证数据机密性和私密性。

4.1.4　签名抗抵赖

数据电子签名验签保证数据在传输、存储过程中不会被篡改，保证了数据完整性，同时也认证了数据发送方的真实身份。在终端设备这些物联网末端节点与

平台进行通信时，可利用电子签名、数字时间戳等机制进行业务认证，防止未授权的设备和应用接入物联网、下载密钥、使用未授权或未定制的业务，保证通信各方对自己行为及行为发生时间的不可抵赖性。

4.2 方案特点

4.2.1 安全性

综合使用国密算法 SM9/SM3/SM4，支持基于 SM9 算法的标识密钥体制，采用挑战应答、数字信封多种安全技术，实现身份和业务认证、数据安全传输、数据加密存储、数据签名与验签等多种安全功能，构建了全方位的安全保护体系。

4.2.2 标准性

采用中国国家密码管理局《SM9 标识密码算法》，接口设计符合《密码设备应用接口规范》，设施环境建设符合国家登报三级等要求，系统各模块遵从统一接口要求、机制要求、策略要求等，构建标准化的物联网安全防护体系。

4.2.3 灵活性

在物联网应用中，对于应用规模较大业务客户，可在客户业务系统服务端直接部署密钥基础设施和加密机，实现密钥直接管理，独享计算资源，灵活满足厂商用户的管理要求。

安全管理平台设计灵活，耦合性低而内聚性高，各系统模块之间接口设计合理完善，能够适应不同的物联网类型，可根据客户需求进行优化；采用多样的模式设计，比如 VIP 模式等，能够适应各类应用规模，经济而便捷。

4.2.4 海量用户支持

标识即公钥，无需数字证书交换，更易于使用，节省了业务开销和服务资源，提高了系统性能，能够支撑海量的用户；同时密码机支持集群方式部署，增加了系统并发量和流畅度，且根据用户需求，还可部署加密机，用于业务系统、生成系统服务端端的签名和解密，节省数据交换时间，提升安全服务效率。

方案设计支持冗余、扩展、备份等功能，可实现无限扩展升级运营级的管理架构，易于构建运营服务模式。

4.2.5 易于开发

硬件要求低，能支持多种类型的芯片，从而能够支持多种类的新接入终端，具备良好的扩展性；可提供客户端和服务端 SDK，支持多种开发语言和操作系统，通过身份认证、加密/解密、签名/验签等服务接口，实现不同类型的终端/服务端开发对接。

（以下无正文）