# IOT系统二期需求

## 概述

一期总结：完成5个基本页面，完成了demo原型开发，包括设备管理和安全管理中心的事件管理部分、完成了前端和后端开发框架。周期：8月7~9月20.

二期来源：和nxp的接触之后，对方在本阶段明确4个主要需求：ota、kms（产线密钥）、设备认证、安全通信。周期，9.17~10月底，M需要能够演示，云端尽量配合完成必要集成。

本文描述对象ISEE-C。

简称：

C：ISEE-C，云端

M：ISEE-M，终端系统

P：ISEE-P，产线

## 需求列表

本阶段规划ISEE-C的基本功能要求如下：

简言之“kaote”：

kms

auth

ota

transmission

edr

二期不考虑edr。

### KMS

ISEE-P简称P。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **需求项** | **附加描述** | **责任人** | **时间要求** |
|  | 设备公钥存储 | 来自P端的设备公钥列表的导入。 |  | 1 |
|  | 设备对称密钥管理 | 来自P端的或者，由C端提供给P端的对称密钥的根。  补充说明：  C端提供派生方法，以供业务层使用设备密钥。 |  | 1 |
|  | 密钥保护 | 确保所有私钥和对称密钥的安全，即，不允许在正式环境出现明文。  补充说明:  C端本期采用软Keystore方式实现。分离出的签名服务端的HSM也采用软实现。  采用Java的KeystoreAPI实现，这一层API将与真实的硬件HSM对接。 |  | 1 |
|  | 云端密钥 | 云端主密钥，RSA2048，ECDSA256，对称根256。 |  | 1 |
|  | 接口 | 产线设备数据导入接口。  对称根密钥导出到P或者由P导入到C的接口。  提供基础密码算法服务接口。  定义导入文件格式。 |  | 1 |
|  | 产线通道安全 | C和P之间需有密钥协商机制，双向身份认证机制。 |  | 1 |
|  | P端加密机管理 | C端提供P加密机的生命周期管理，以及密钥管理，例如公钥、ID、配置、厂商、生产时间等。 |  | 1 |
|  |  |  |  |  |

### Auth

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **需求项** | **附加描述** | **责任人** | **时间要求** |
|  | 设备认证 | 【可选】证明设备可信。流程：设备发起请求，外部发起挑战，设备做签名。  设备需要确保签名密钥的安全。外部节点应有该设备对应的公钥或者证书。 |  |  |
|  | 云端（外部）认证 | 【可选】验证设备外部节点是否合法。  流程：外部发起请求，设备反馈挑战，外部对挑战做签名，设备验证签名和挑战。  需要设备中在出厂前植入不可篡改的公钥或者公钥hash，或者一个对称密钥。 |  |  |
|  | 证明 | 【可选】设备端keystore中产生的二级业务密钥，其公钥以及当前系统安全状态打包成自签名证书，证书签名密钥为设备的根密钥（产线部署）。  用途：外部可验证该证书来自可信区域。 |  |  |
|  | 模块接口 | 【可选】提供签名、验证、导出公钥、导出证书、导入公钥、导入证书。加密导出或者导入私钥及对称密钥。  【必选】设备认证用的签名接口 |  |  |
|  |  |  |  |  |

### Ota

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **需求项** | **附加描述** | **责任人** | **时间要求** |
|  | 安全通信 | 基于GNP保护 |  | 1 |
|  | 防降级 | 【可选】  终端构造类似RPMB的计数器。  验证签名后需要校验counter是否回退。  C端签名时输入Counter值。  C端应能监控到当前M端的Counter值。 |  |  |
|  | 签名服务安全性 | 【可选】  IP白名单。  签名服务和在线OTA服务分离。  签名服务与签名HSM一并部署在公司内网。  签名服务主动链接ota在线服务，并将签名结果推送至ota服务器。 |  |  |
|  | 对外服务web接口安全 | 1. IP白名单，限定内网访问。 2. 【可选】usbdongle 3. 【可选】手机security Key |  |  |
|  | 签名前的审核 | 【可选】  签名操作需提示是否对镜像做过严格审核。  提醒管理员审核方式选一种确认：   1. 人工代码review并确保该代码编译出的镜像为待签名镜像。 2. 可信二进制与待签二进制做二进制比对，或逆向后比对后认为无主观恶意代码。 3. 有承担能力的人对文件的hash手工签字画押后，备案。 |  |  |
|  | ota管理页面的镜像列表 | 包含镜像类型、文件名、功能特性说明、Counter值、推送策略、升级策略 |  |  |
|  | 推送策略 | 【可选】可定义推送时间段。  x月x号x时，xxx分钟后，立即。  支持某时间段内随机下载、按顺序下载以降低带宽占用。  可定义推送目标设备类型。  可定义特定版本推送。 |  |  |
|  | 安装策略 | 【可选】可定义安装时间段。  允许故障后自动重置。  支持随机时间升级、固定时间升级，以适配各种业务情况。如，业务不可停，不可同时大规模故障。  试点安装：选择小范围试点，已检验真实环境可靠性。 |  |  |
|  | 重置 | 【可选】允许手工重置某一设备、某一型号。  ota不应影响系统recover区域，以免发生灾难。 |  |  |
|  | 设备联动 | 【可选】ota业务应有设备管理服务配合。  实现针对特定设备的状态监控、维护以及特定型号、批次的维护。  设备管理应包含芯片信息和设备信息。 |  |  |
|  | 固件整体ota | 芯片中所有软件的整体打包更新。 |  | 1 |
|  | 模块化升级 | 【可选】ta、ca以及各种服务模块的单独升级。  各种配置文件的单独更新。  各种密钥的更新。 |  |  |
|  | 差分包 | 【可选】因IOT场景整体包不大，但在设计时应尽量做到编译结果的细粒度模块化。以便于后期实现本功能。 |  |  |
|  | 断点续传 | 【可选】确保传输可靠性。断网恢复，断电恢复。 |  |  |
|  | 故障恢复 | 【可选】传输过程、安装过程断电，重启，应能够回退或者继续安装过程。  如果可以，选择继续完成ota操作。 |  |  |
|  | 版本控制 | ota服务器实现各文件的版本管理。 |  | 1 |
|  | ota服务和签名服务的分工 | 签名服务实现审核、counter配置、签名、推送。  其余功能由ota服务实现。 |  | 1 |
|  | ota基本功能 | 【可选】满足对软件、配置、密钥等数据的更新。  更新可以是增加、修改也可以是删除。  【必选】软件的修改 |  | 1 |
|  | 状态与监控 | 【可选】ota分为下载和安装2个环节。  每个环节应至少有4个状态：开始、进行中、完成、失败。最少共8个状态。  尽可能的上报当前的状态到C端。C端实时显示（单个设备的状态，各种状态的设备数） |  |  |
|  | 镜像加密 | 可运行的二进制镜像，采用nxp的加密方式加密。  其它数据采用自定义方式，或者统一打包到镜像中。 |  | 1 |

### Transmission

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **需求项** | **附加描述** | **责任人** | **时间要求** |
|  | 实现应用层保护协议GNP | GNP的根密钥由云端HSM保护。  保护链路数据的机密性、完整性、防伪性、防中间人。  符合GNPv3的设计要求。  需要适配终端支持的算法。  为应用层提供的接口：协商、编码、解码。  模块应有明确的状态反馈。  补充说明：GNP视作ssl安全功能的最小集，不兼容传输层，与安全域无缝接入，适用于无rsa的终端，宜适用于保护业务，如ota。  关于算法：v3中指定了  ECDH p256r1+rsa2048 pss oaep + sha256 + HMAC-SHA256 +AES256-CBC-nopadding。  问题：rsa2048性能？  产生密钥：产线由加密机产生后加密灌入芯片？还是采用1024位？  签名：？  在产线C-P设计中明确termID，检查GNP中的是否符合，尽可能沿用GNP设计。  产线用的DevID={FactoryCrypterID(2),OEMID(2),ChipManufacturerID(2),SeManufacturerID(2),ISEEVersion(2),hash(HWUID,”tid”)(8),DevSN(8),SeSN(8)}；  GNP中的TerminalID=trunc16(sha256（DevID） ) |  | 1 |
|  | 实现传输层SSL协议支持 | 【可选】，二期nxp没提，我们自行考虑。  设备端的keymaster和云端的keymaster为ssl提供密钥保护，可以通过pkcs11也可以通过类似xp项目的方式，确保身份认证密钥不泄露。  云端构建CA体系，需要为设备端以及客户云颁发子证书，以及预置CA根证书。  为客户云颁发子证书应考虑服务附加值问题，否则应链接到豆荚云。 |  |  |
|  | mqtt。。。。 |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### 其它要求

ISEE-C简称C。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **需求项** | **附加描述** | **责任人** | **时间要求** |
|  | C-M基础接口设计文档 | 基础网络数据格式描述，交互流程描述，文件格式描述 等。 |  | 1 |
|  | C-P接口设计文档 | 产线相关文件格式描述， 网络接口描述等。 |  | 1 |
|  | OTA之C-M接口设计 | 网络数据格式描述，交互流程描述，文件格式描述 等。 |  | 1 |
|  | 密钥表文档 | 罗列系统中所有的密钥，明确：名称、用途、如何产生、如何保护、如何销毁。 |  | 1 |
|  |  |  |  |  |

## 项目要求

时间要求

9.23~10.30

人员计划

C:李东季、许成鹏

里程碑deadline：

需求 ：

设计完成：

ISEE-C开发编码：

与ISEE-P集成：

与ISEE-M集成：

整体测试：

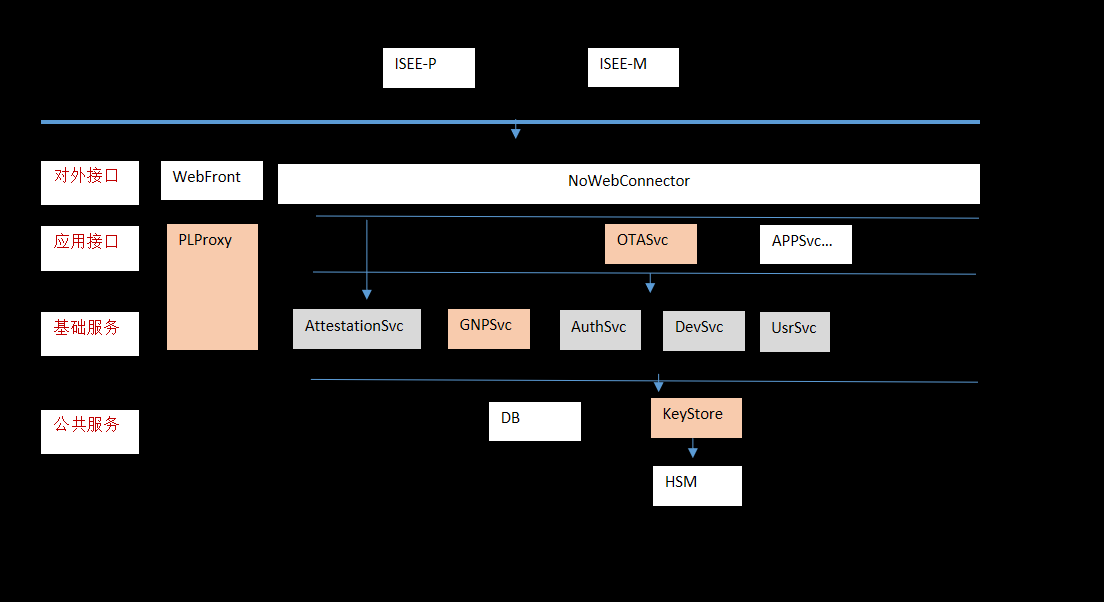
# 附录

## 系统建议简图

GNP：传输保护。

KeyStore：提供基础密码服务。

原版见pptx图，截图：



对于M端，Keystore和其它svc之间也建议这样的层次结构，即最底下是基础“加密机”，是公共基础服务，它不理解密钥的用途，不理解业务。