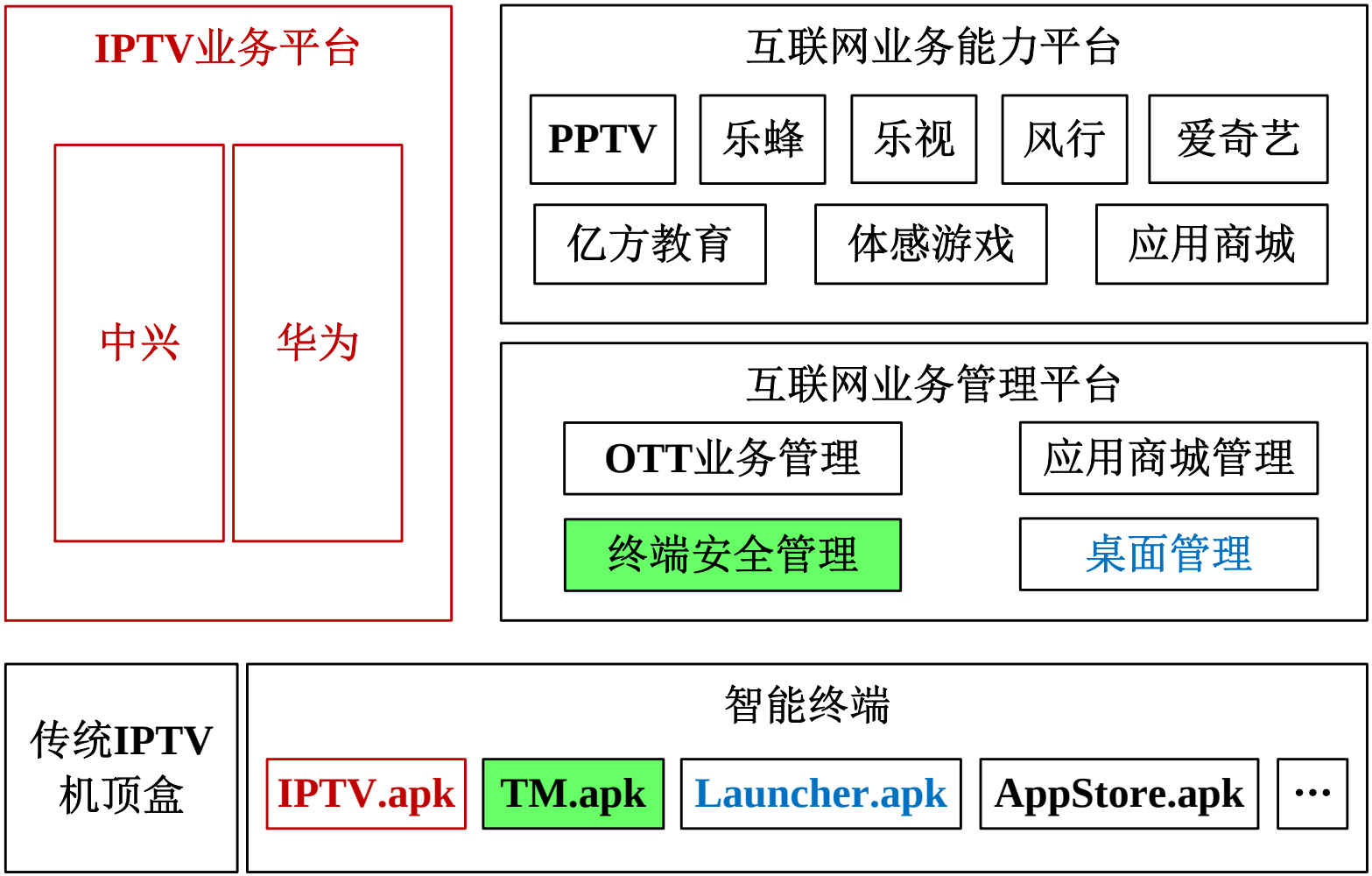
上卡网络
Shanghai Alcatel Network Support System

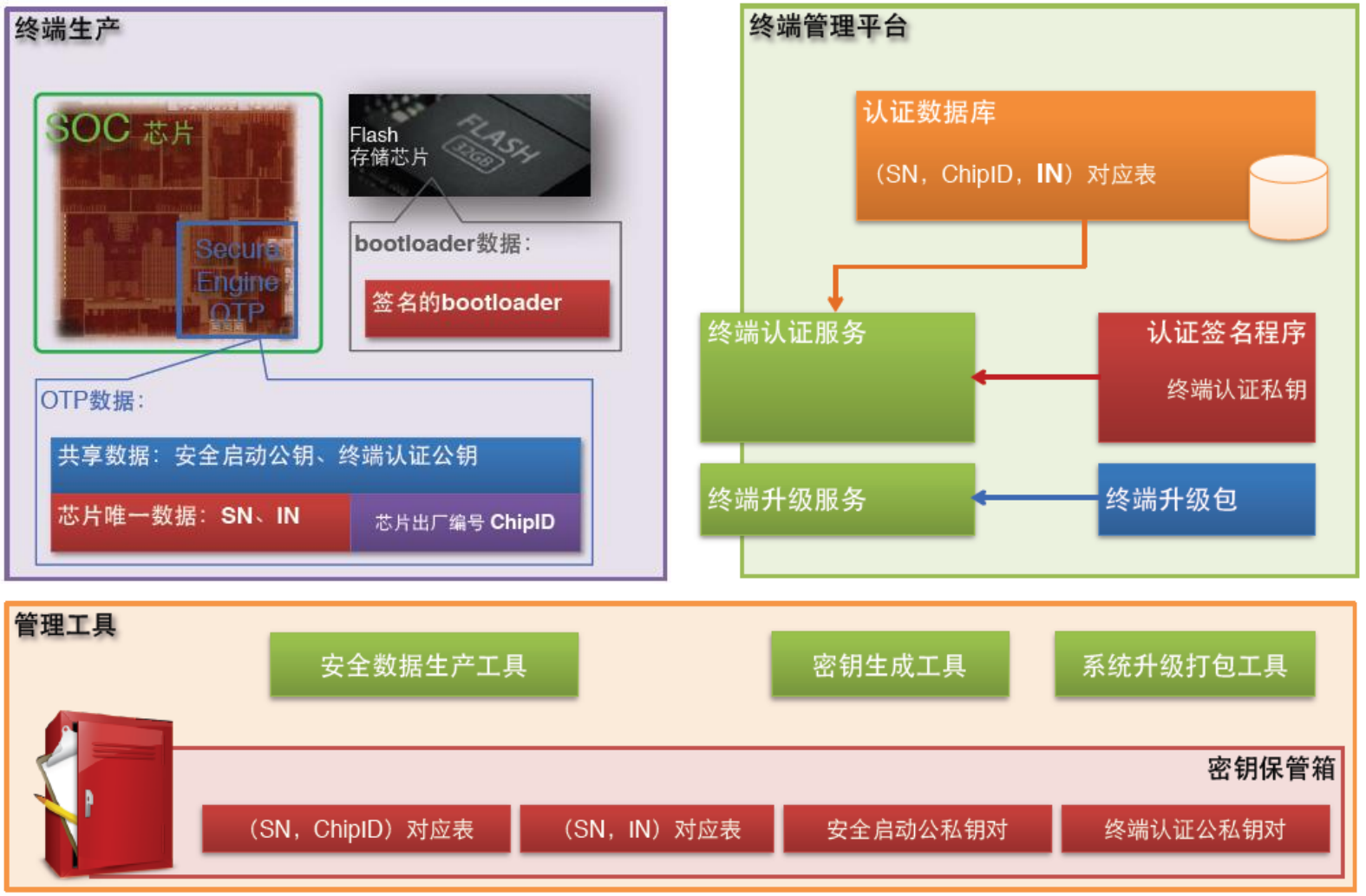
智能终端安全管理方案

2013.05.30

智能终端安全管理总体架构



安全机制 - 安全系统的构成



智能终端安全机制

- 基于OTP的防刷机机制和对操作系统核心文件进行只读保护
  - ✓ 只读数据
    - SN、ChipID、安全启动公钥、终端认证公钥
  - ✓ 不可读数据
    - IN，只能通过H函数给出计算结果
  - ✓ 防刷机机制
    - 根据安全启动公钥检查系统内核签名
    - 根据安全启动公钥检查Bootloader签名
    - 根据安全启动公钥检查系统文件分区
    - 根据安全启动公钥检查系统恢复分区
- 基于主芯片的终端唯一性识别
  - ✓ 芯片唯一数据：SN、IN
  - ✓ 芯片出厂编号：ChipID

提纲

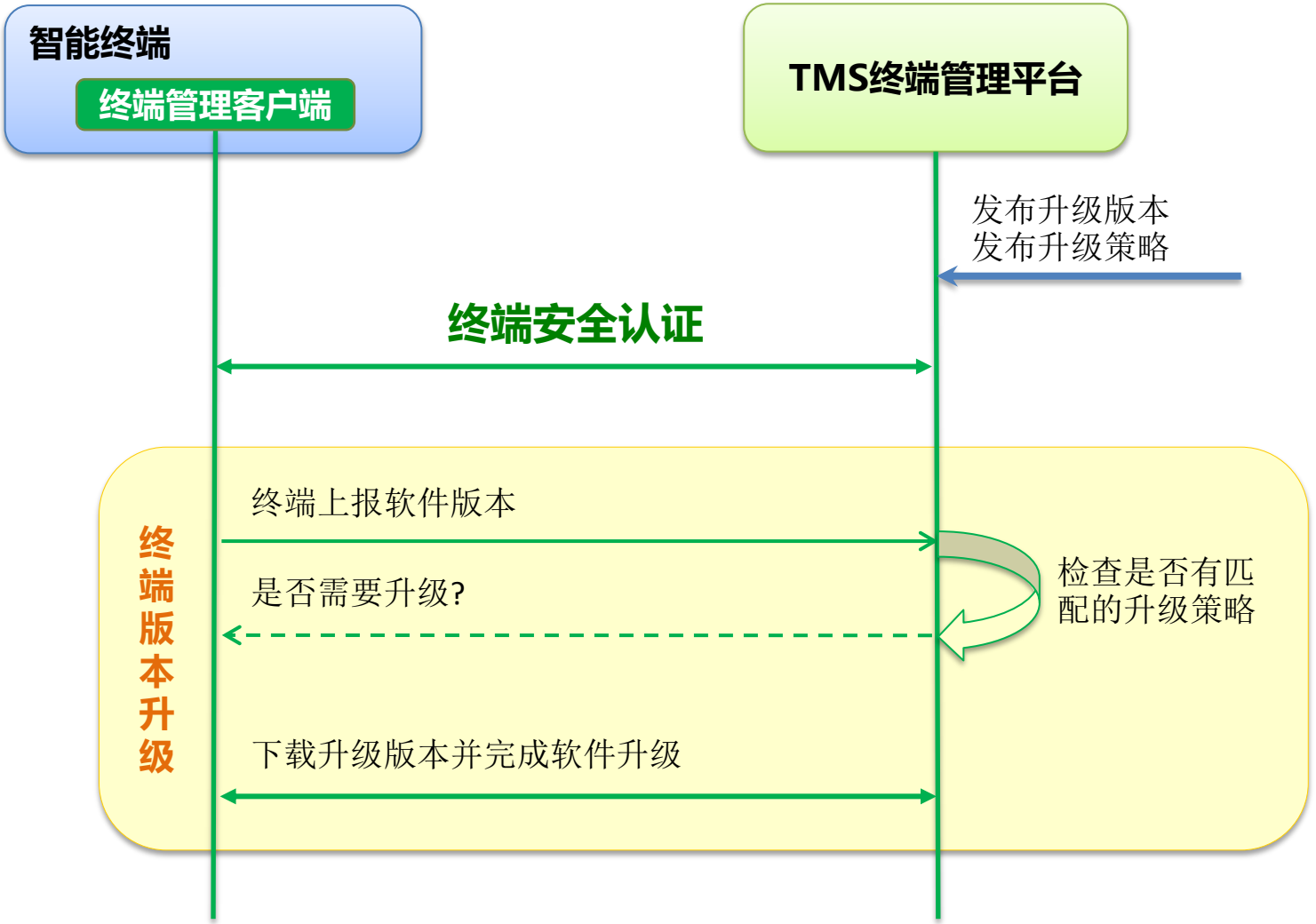
- 终端安全认证
- 终端安全升级
- 桌面管理应用的安全接入认证
- 终端安全生产
- 网络拓扑和设备需求

终端安全认证流程

SN	终端序列号，公开可读，不可改写
R1	终端产生的随机数
T1	终端产生的时间戳
M	魔术字，用来识别解密后的明文
R2	服务端产生的随机数
T2	服务端产生的时间戳
Kpri	服务端保存的RSA认证私钥
Kpub	终端上保存的不可改写的RSA认证公钥，与Kpri为一对
IN	终端上机密保存，不可读取的内部唯一序列号
ChipID	芯片序列号，公开可读，不可改写

- AES-CBC，PKCS5Padding
- 明文：SessionToken+路由表服务器地址(O)+应用签名服务器地址(M)+魔术字(M)）
- 初始化向量IV：R1
- 密钥：R2

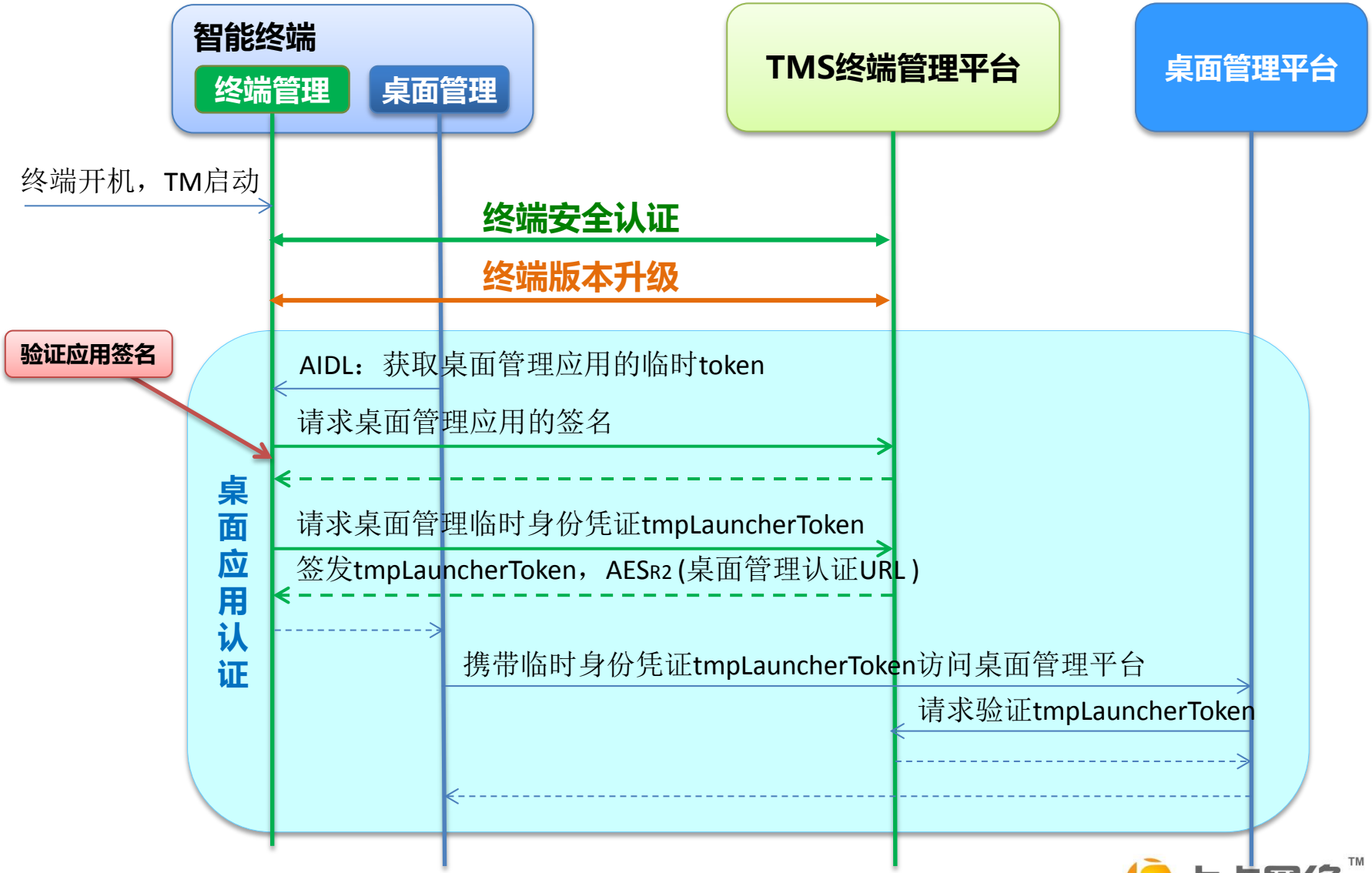
终端升级流程


智能终端
终端管理客户端
TMS终端管理平台
发布升级版本
发布升级策略
终端安全认证
终端版本升级
终端上报软件版本
是否需要升级?
检查是否有匹配的升级策略
下载升级版本并完成软件升级

终端升级管理

- **终端软件升级流程**
  - ✓ 准备：软件版本+安全启动私钥签名；上传到下载服务器；发布升级策略
  - ✓ 升级：终端开机通过安全认证后，上报软件版本，TMS引导终端下载新的软件版本完成升级
- **终端软件升级管理功能**
  - ✓ 负责操作系统的版本升级（TM客户端只能跟随操作系统一起升级）
  - ✓ （可选）支持应用升级：如IPTV客户端升级等应用升级等
- **终端软件升级策略管理**
  - ✓ 指定终端序列号的版本升级策略：指定SN的OS/应用升级到特定版本
  - ✓ 组合条件的OS/应用版本升级策略
    - 终端型号：指定型号的终端无条件升级到特定版本
    - 终端型号 + IP范围：指定区域的某款终端升级到特定版本
    - 终端型号 + 软件版本：指定软件版本的某款终端升级到特定版本
    - 终端型号 + IP范围 + 软件版本：指定区域、软件版本的终端升级到特定版本

终端桌面管理应用的安全接入认证



提纲

- 终端安全认证
- 终端版本升级
- **终端安全生产**
  - 安全数据
  - 手工烧写安全数据
  - 正式烧写安全数据

安全生产数据

- 终端生产涉及的安全数据包括：
  - ✓ **启动公私密钥对：**公钥写入安全芯片，用于安全启动和安全升级；私钥由平台运维人员保管，用于系统升级包的签名
  - ✓ **认证公私密钥对：**公钥写入安全芯片，私钥存放于平台，用于安全认证
  - ✓ 关键数据：**SN、 ChipID、 IN**
- 启动公钥和认证公钥的烧写
  - ✓ 每一个批次的所有终端共享同一个启动公钥和认证公钥
  - ✓ 可以在关键数据SN、ChipID、IN烧写之前一次性烧写到终端
- 关键数据烧写
  - ✓ 临时方案：针对调试阶段的、零星数量的终端，可采取手工临时烧写的方案，电信人员现场监督电信安全数据烧写过程
  - ✓ 正式方案：针对终端批量生产，采用远程正式烧写方案

安全生产工具

- 安全生产工具

工具名称	终端厂商提供	阿网提供
启动公私密钥对生成工具	●	
认证公私密钥对生成工具		●
TM签名打包工具（用于系统升级）	●	
临时烧写方案：关键数据生成工具		●
临时烧写方案：终端烧写apk	●	
正式烧写方案：云端烧写工具		●
正式烧写方案：PC端烧写工具		●
正式烧写方案：终端烧写apk	●	

临时烧写方案和工具

- 数据临时烧写流程
  - ✓ 电信生成/确定安全启动密钥对，安全认证密钥对，并将安全启动公钥、安全认证公钥提供给芯片厂商，芯片厂商将两个公钥写入芯片
  - ✓ 电信分配终端SN，并使用“临时烧写关键数据生成工具”生成关键数据
  - ✓ 电信将关键数据提供给终端厂商，并监护终端厂商将关键数据写入终端/芯片、销毁关键数据的过程
  - ✓ 终端厂商将SN对应的mac地址、ChipID提供给电信
  - ✓ 电信将关键数据、mac、chipID等数据导入生产环境
- 临时烧写关键数据生成工具
  - ✓ 关键数据：sn+na+nb+na
  - ✓ sn = “SN” + SN，共26个ASCII字符
  - ✓ na，nb：原始IN采用AES加密转换成Byte数组，再转换成16进制，结果为64字符的文本，一拆为二，分别附加“NA”和“NB”前缀，生成34个ASCII字符的na和34个ASCII字符的nb
  - ✓ ha = “HA” +MD5(sha256(24位SN+ChipsetType+IN+T+R))，共34个ASCII字符

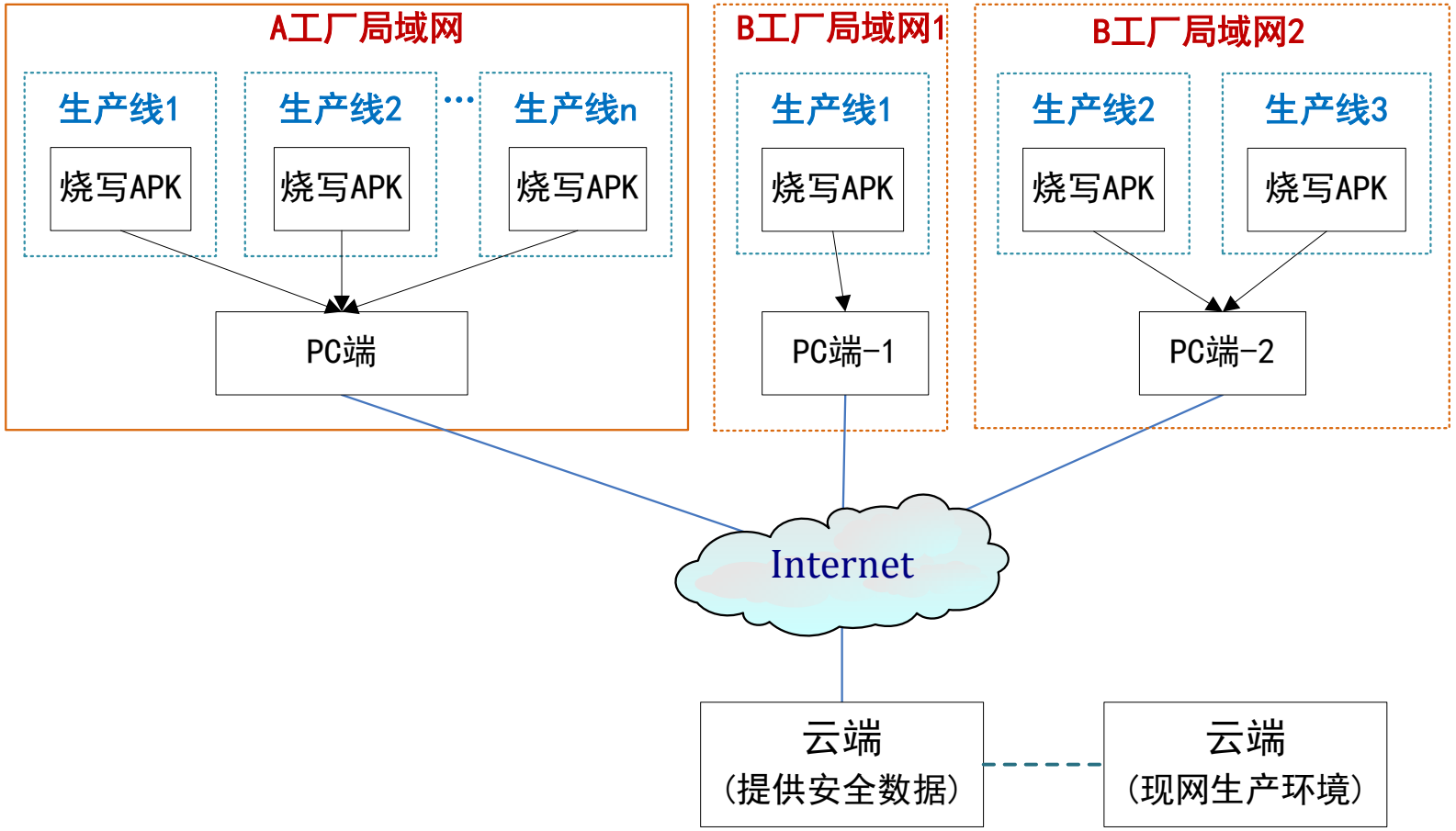
  其中，ChipsetType，T和R为事先约定的值

正式烧写方案和工具

- 关键数据正式烧写方案和工具
  - ✓ 烧写系统由三部分组成
    - ✓ 云端烧写服务器：负责安全数据的生产与输出
    - ✓ 工厂烧写PC：作为云端和机顶盒之间交换、验证安全数据的桥梁
    - ✓ 机顶盒烧写apk：负责获取安全数据后写入芯片的OTP区域
  - ✓ 安全控制：
    - ✓ 关键数据IN采用认证私钥加密后传送给烧写apk，由芯片解密后写入
    - ✓ 每个生产批次，云端为每个PC端分配一个用户名密码，只在一次生产中有效

正式烧写方案网络架构

烧写系统架构



安全生产流程

安全生产流程

- **准备阶段**
  - ✓ 使用“密钥生成工具”生成启动公私钥对和认证公私钥对，公钥提供给芯片生产厂商
  - ✓ 确定本次量产数量，电信分配相应数量的SN（根据损耗率，提供一定余量），终端厂商提供相应数量的mac地址
  - ✓ 安全数据初始化：为每个SN分配一个mac地址，以及创建关键安全数据IN
  - ✓ 导出SN与mac对应表，提供给终端生产厂商，用于打印SN和mac标签
  - ✓ 为工厂每台烧写PC分配一对烧写用户名和密码，用于工厂PC登录烧写云端服务器
  - ✓ 烧写apk准备：终端厂商/芯片商提供烧写APK，交终端生产线

安全生产流程

安全生产流程（续）

- **数据烧写**
  - ✓ 工厂烧写PC使用云端分配的烧写用户名和密码登录到云端服务器
  - ✓ 扫描枪连接机顶盒，扫描SN条码，烧写apk向烧写PC请求SN的安全数据，并上传ChipID参数
  - ✓ PC端携带token、SN、ChipID向云端请求安全数据
  - ✓ 云端确认该SN为 “待生产”状态，下发关键数据sn，mac，in和ha，并将该SN标记为“生产中”状态
    - sn：明文，24个ascii字符
    - mac：明文，12个ascii字符
    - in：Rsa1024PrivKey（IN+T+R），使用认证私钥进行加密，得到一串256字节的十六进制字符串；
    - ha：MD5(SHA256(SN+ChipID+IN+T+R)+mac)，共32个ascii字符（T/R为约定值)
    - sn+mac+in+ha共24+12+256+32=324个ascii字符
  - ✓ 烧写apk通过hash验证数据有效后，烧写数据

安全生产流程

安全生产流程（续）

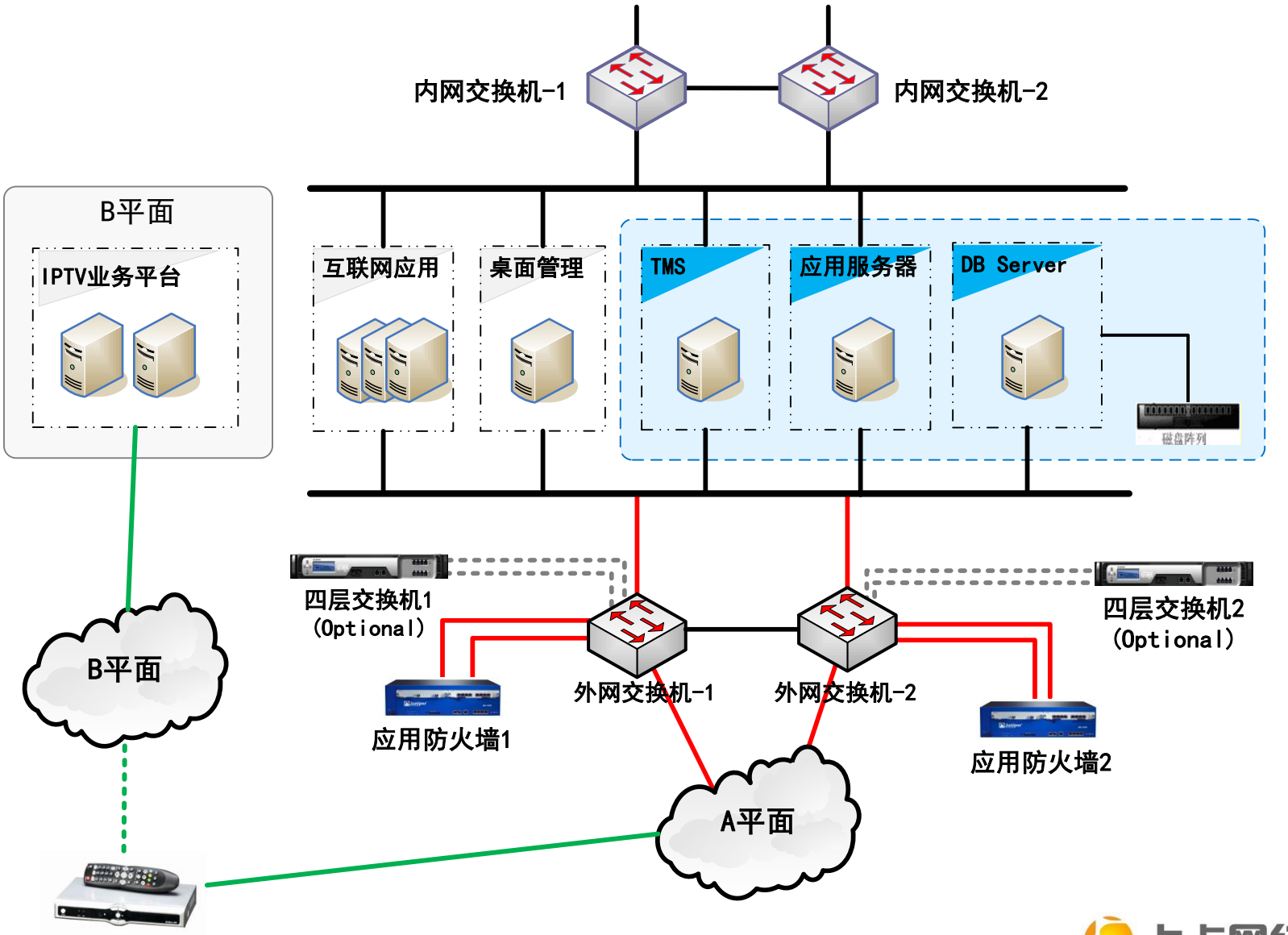
- **数据验证**
  - ✓ 终端向云端（由工厂PC代理）请求挑战字
  - ✓ 云端下发用认证私钥加密的挑战字ChallengeCode = RSA1024(“CTIT”+T1+R1+T2+R2)
  - ✓ 终端用认证公钥解密挑战字，上传Authenticator=SHA256(SN+ChipID+IN+T2+R2)
  - ✓ 云端验证Authenticator有效性，将SN的烧写状态为“烧写成功”或“烧写失败”，，并下发烧写结果
  - ✓ 如果在“验证数据”时遇到异常，工人可通过烧写apk重新发起“验证数据”过程

  数据验证过程基本模拟终端的安全认证过程，验证终端SN、ChipID、IN和认证公钥的正确性。
- **数据导出**
  - ✓ 生产完成后，将烧写成功的终端安全数据从烧写库导出到生产库

提纲

- 终端安全认证
- 终端版本升级
- 终端安全生产
- **网络拓扑和设备需求**

网络拓扑示意


内网交换机-1
内网交换机-2
B平面
IPTV业务平台
互联网应用
桌面管理
TMS
应用服务器
DB Server
磁盘阵列
四层交换机1
(Optional)
四层交换机2
(Optional)
外网交换机-1
外网交换机-2
应用防火墙1
应用防火墙2
B平面
A平面

网络和设备需求

- **服务器和存储设备需求**
  - ✓ **磁盘阵列×1**：双控制器，12个600GB 15krpm SAS硬盘，2个SFP收发器
  - ✓ **数据库服务器×1：** 4×八核CPU，32GB内存，2×300GB SAS硬盘，2个单口光纤HBA卡，4个千兆网口，RAID卡，远程管理卡，DVD-ROM，4个热插拔冗余电源模块，Redhat v6.1
  - ✓ **TMS应用服务器×1：**2×四核CPU，8GB内存，5×900GB SAS硬盘，6个千兆网口，RAID卡，远程管理卡，DVD-ROM，2个热插拔冗余电源模块

    参照上海的业务模型，单台TMS应用服务器可以为20w智能终端用户提供服务
  - ✓ **其他应用服务器：**
    - 管理服务器×1：部署配置管理应用
    - 下载服务器×1：部署智能终端系统升级版本下载服务
    - 烧写服务器×1：部署云端烧写工具
    - 最简配置：以上三个应用可以部署在同一台物理服务器上

网络和设备需求

- **第三方软件需求**

服务器	操作系统	应用软件
数据库服务器	Redhat5.1+, 4 socket	Oracle 11g
TMS应用服务器	Redhat5.1+, 2 socket	Weblogic 10MP1+
其他应用服务器	Redhat5.1+, 2 socket	tomcat 6.0, java1.6

分工与合作

芯片/终端厂商

- 工厂烧写PC服务器设备
- 零星生产－关键数据烧写apk
- 批量生产－关键数据烧写apk
- 启动key生成工具
- 系统升级包签名工具

TMS平台开发商

- TMS平台软件：TMS、配置管理
- 认证key生成工具
- 零星生产：数据生成工具
- 批量生产：云端烧写工具，PC端烧写工具
- 协助四川电信部署、测试和运维支撑

电信运营商

- 终端安全生产：
  - 分配SN（厂商代码、终端型号、批次、起始序号、数量）
  - 零星生产
    - ✓ 生成关键数据
    - ✓ 烧写过程安全监护
  - 批量生产：
    - ✓ 为烧写PC分配烧写帐号密码
  - 将关键数据导入到现网
- 系统部署环境
- 平台运行维护

敬请指导！