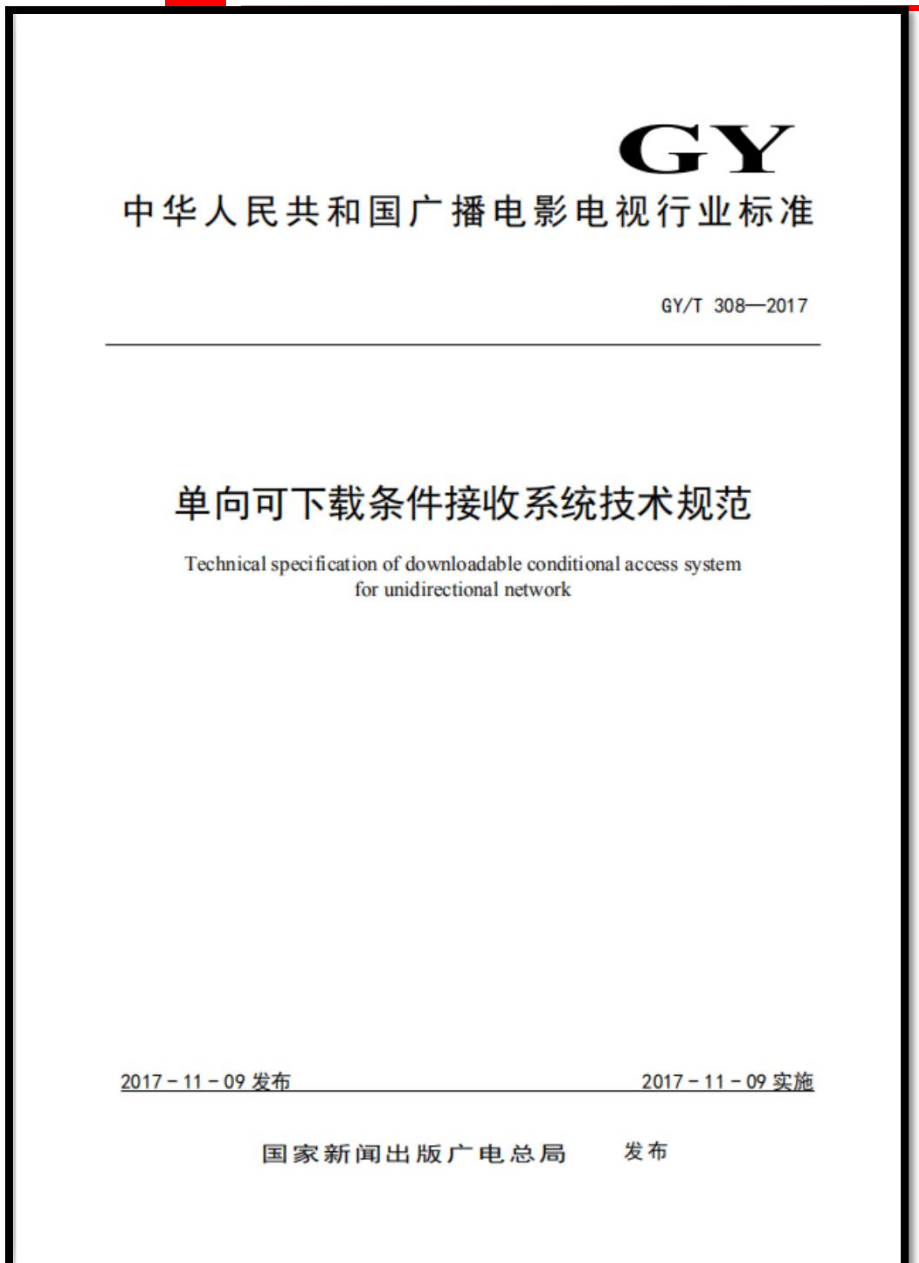
新一代卫星直播广播电视系统
安全数据管理平台业务介绍

卫星直播中心

2019年12月

目录

一、安全数据管理平台业务概述



GY

中华人民共和国广播电影电视行业标准

GY/T 308—2017

单向可下载条件接收系统技术规范

Technical specification of downloadable conditional access system for unidirectional network

2017－11－09 发布　　2017－11－09 实施

国家新闻出版广电总局　发布

按照《单向可下载条件接收系统技术规范标准》【GYT 308】的要求，DCAS安全数据管理平台（以下简称“TA”）是DCAS系统的安全基础设施，是支撑DCAS系统运行的不可或缺的环节。

一、安全数据管理平台业务概述

TA主要功能包括：

- 完成加密密钥的生成、植入、传递、维护等密钥管理工作
- 完成与解码芯片厂商、条件接收厂商、硬件安全模块厂商、运营商等相关方的业务交互
- 完成对终端软件和系统安全的数字签名能力支撑
- 完成DCAS系统中用于身份认证所需的数字证书的生命周期管理

一、安全数据管理平台业务概述

TA的主要业务包括：

01

解码芯片管理

对接解码芯片企业：芯片集成、密钥生成、芯片序列化。

02

条件接收系统管理

对接DCAS企业：Vendor_sysID分配、中间密钥生成、DCAS企业证书签名。

03

HSM管理

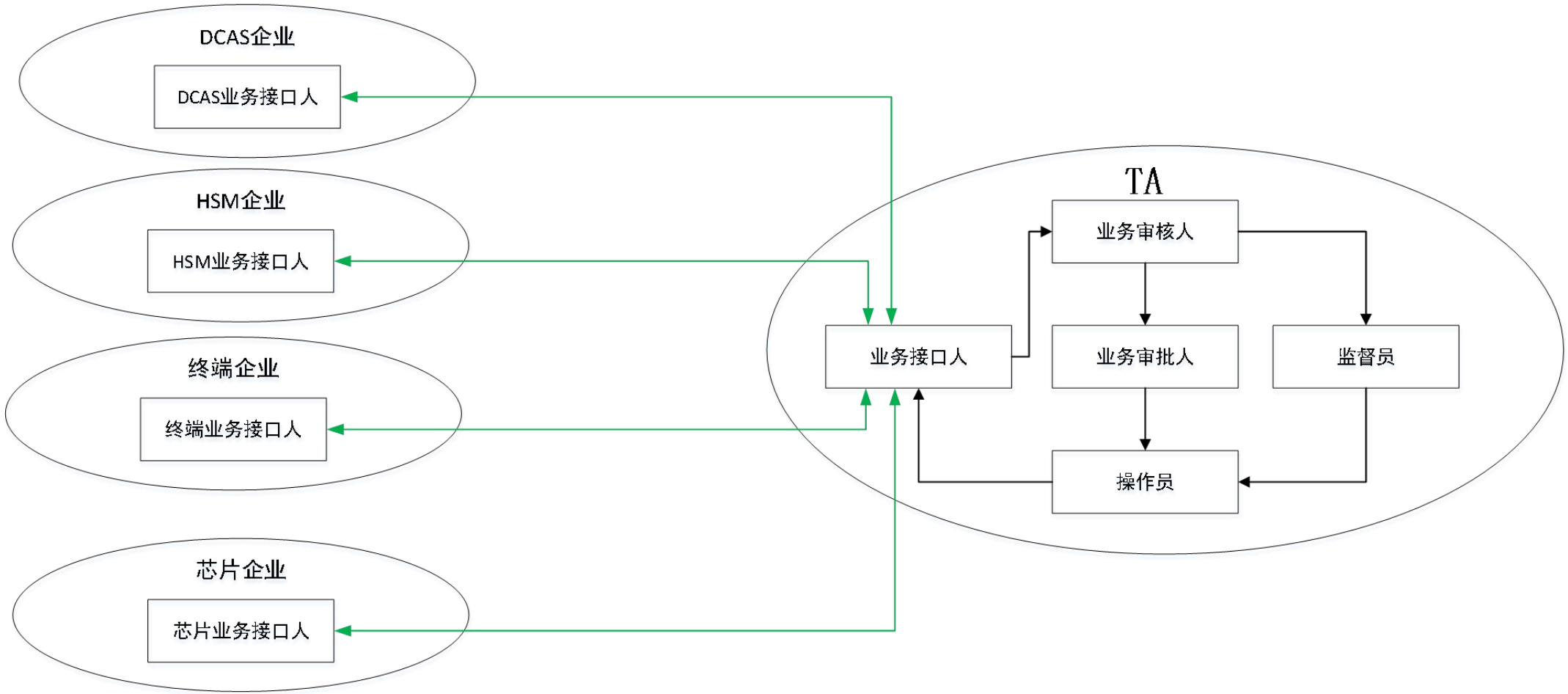
对接HSM企业：HSM ID分配、HSM企业证书签名。

04

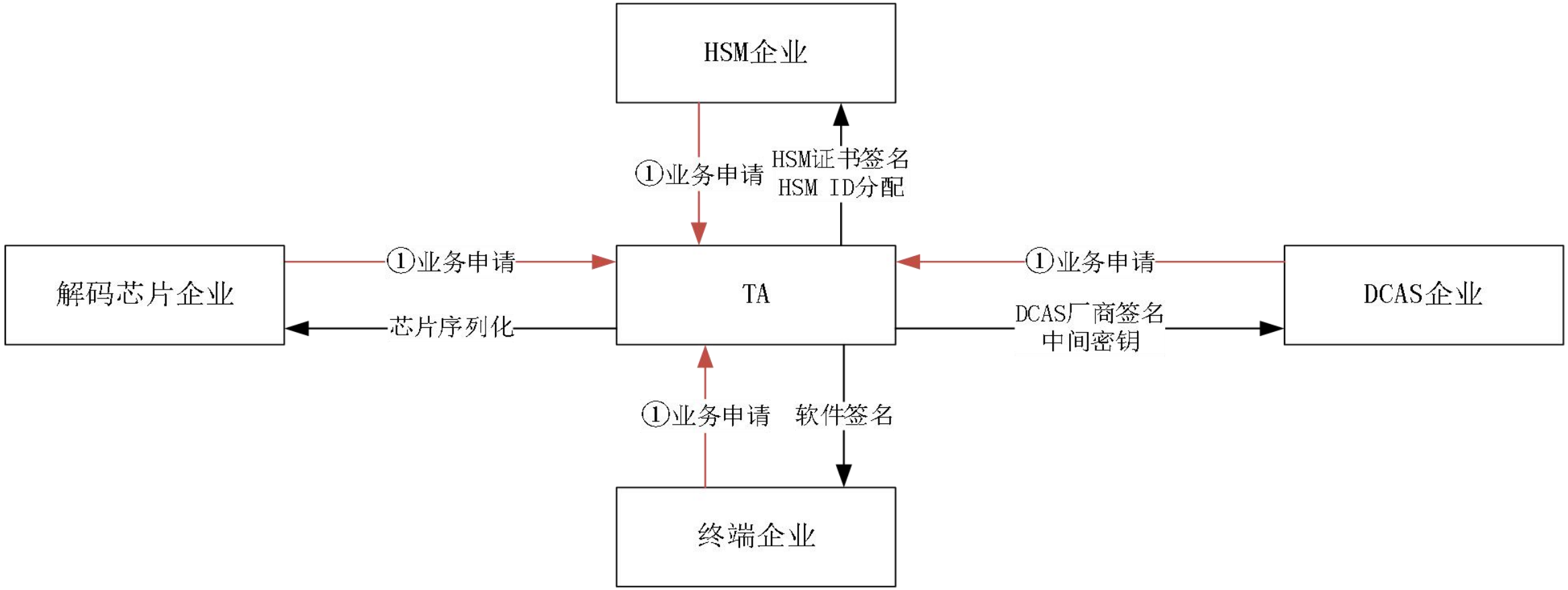
终端管理

对接终端企业：终端软件签名。

一、安全数据管理平台业务概述

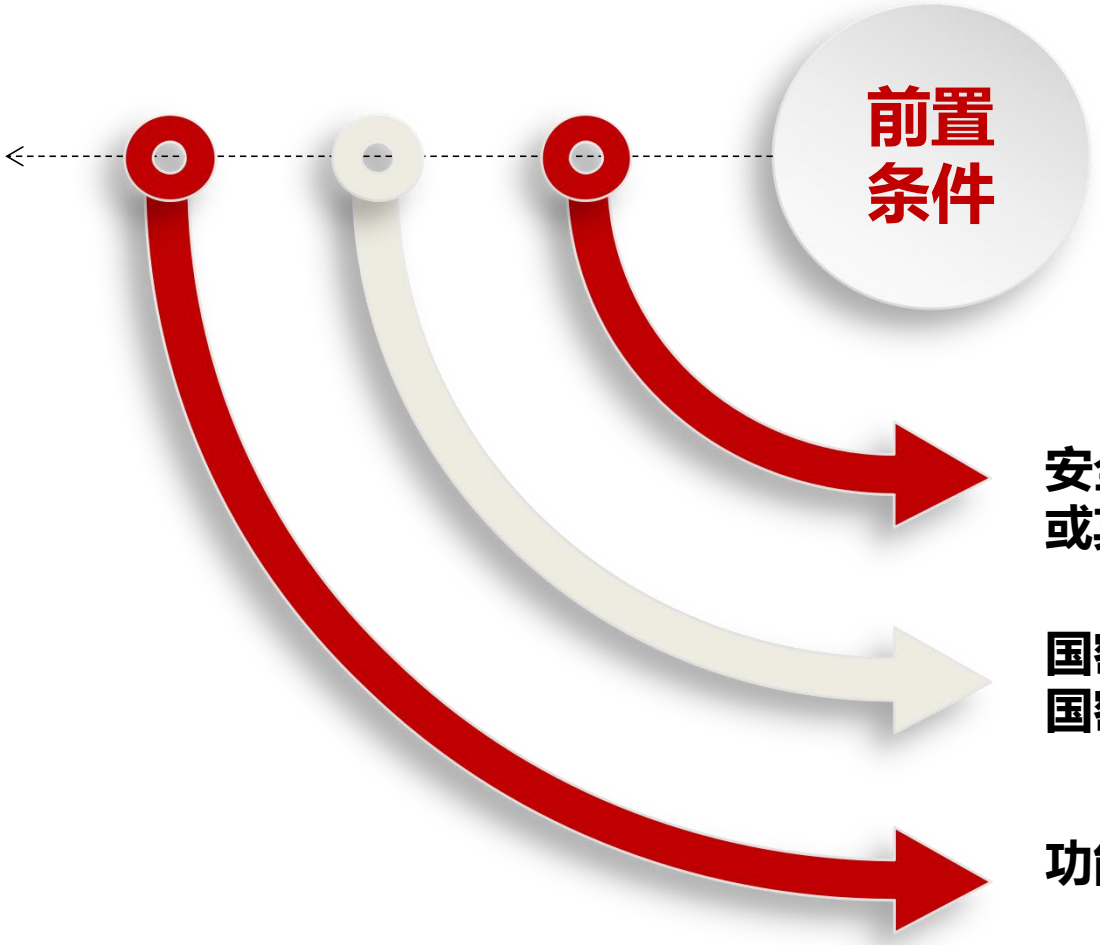


一、安全数据管理平台业务概述



目录

二、解码芯片业务流程



安全测试：解码芯片通过中国信息安全评测中心EAL3或以上等级，或其它获得认可评测机构的同等安全级别测试

国密测试：解码芯片通过商用密码检测中心的国密测试，取得国密型号。

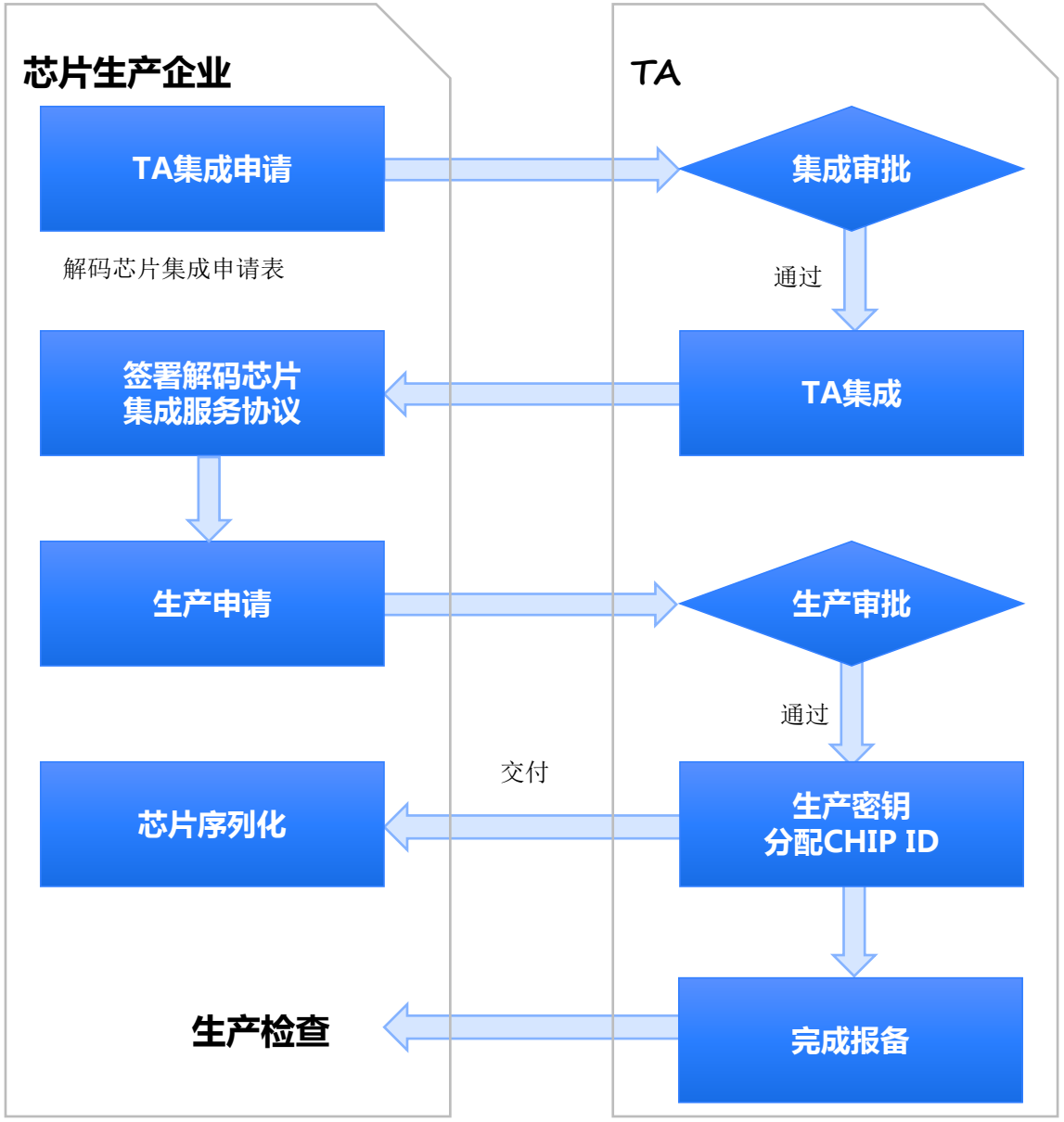
功能和集成测试：解码芯片通过广科院的DCAS功能和集成测试。

包含解调功能的解码芯片安全要求

符合总局科技司发布《直播卫星传输技术保密管理办法》

符合总局科技司下发的《直播卫星涉密人员、设备、文档保密要求》

二、解码芯片业务流程



明确解码芯片企业授权代表、联系人。
明确解码芯片CHIP ID规则，测试ID范围。
明确双方用于传输加密和验证的PGP公钥。
明确出厂OTP安全配置要求。
SCKv密钥生成的函数集成。
密钥数据部署和测试。
BLK0、ESCK、JTAGKEY、CHIPID等密钥及数据生成。

二、解码芯片安全要求

封装要求

解码芯片须与北斗芯片合封为一颗芯片，采用BGA形式封装，二者间的数据通信总线不应暴露于合封芯片之外。

北斗芯片

北斗芯片的固件不可更改。

二、解码芯片生产控制规范–公钥管理

预埋公钥	BL_KEY0须预埋在解码芯片OTP区解码芯片出厂前应确保OTP区已设置写保护，即不再允许对其进行修改。
设备环境要求	烧写设备须安置在一个隔离的物理空间内并配备监视设备。任何时候，监视设备都应启动并对其进行全程监控，监控录像保存90天以上。
人员要求	应指定专人负责操作相关设备，并在生产控制实施方案明确操作规程及信息安全责任，提交安全数据管理平台备案。
操作要求	不得以明文形式将BL_KEY0保存在硬盘或任何移动存储设备上。在使用完毕后，应立即将BL_KEY0从内存中删除。

二、解码芯片生产控制规范–安全数据管理

数据唯一性

同一型号下的每个解码芯片的芯片序列号(CHIPID)须保证是唯一的，即每个芯片只有一个序列号，且各芯片的序列号不能相同。

设备环境要求

须通过直播卫星安全数据管理平台提供设备或软件(即：黑盒子Black-box)获取芯片密钥和序列号。

人员要求

应指定专人负责操作相关设备，并在生产控制实施方案明确操作规程及信息安全责任，提交安全数据管理平台备案。

操作要求

不得以明文形式将芯片密钥保存在硬盘或任何移动存储设备上。应采取有效的手段避免将相同的芯片密钥写入不同的芯片。

二、解码芯片生产控制规范– JTAG保护

密码保护模式

解码芯片出厂时，JTAG端口应至少设定为密码保护模式。

永久关闭模式

解码芯片的JTAG端口须可以通过配置从密码保护模式进入永久关闭模式，但这个过程须是不可逆的。

二、生产控制规范– SEEDv、SMK及密钥函数

SEEDv仅能提供给指定的DCAS企业。SMK必须自行妥善保管、使用。SCK 初步处理函数仅能提供给TA。根密钥最终派生函数仅能提供给指定的DCAS企业。

对于上述数据及函数须妥善保管、使用，制定相关的保密措施并在生产控制实施方案明确，报TA备案。

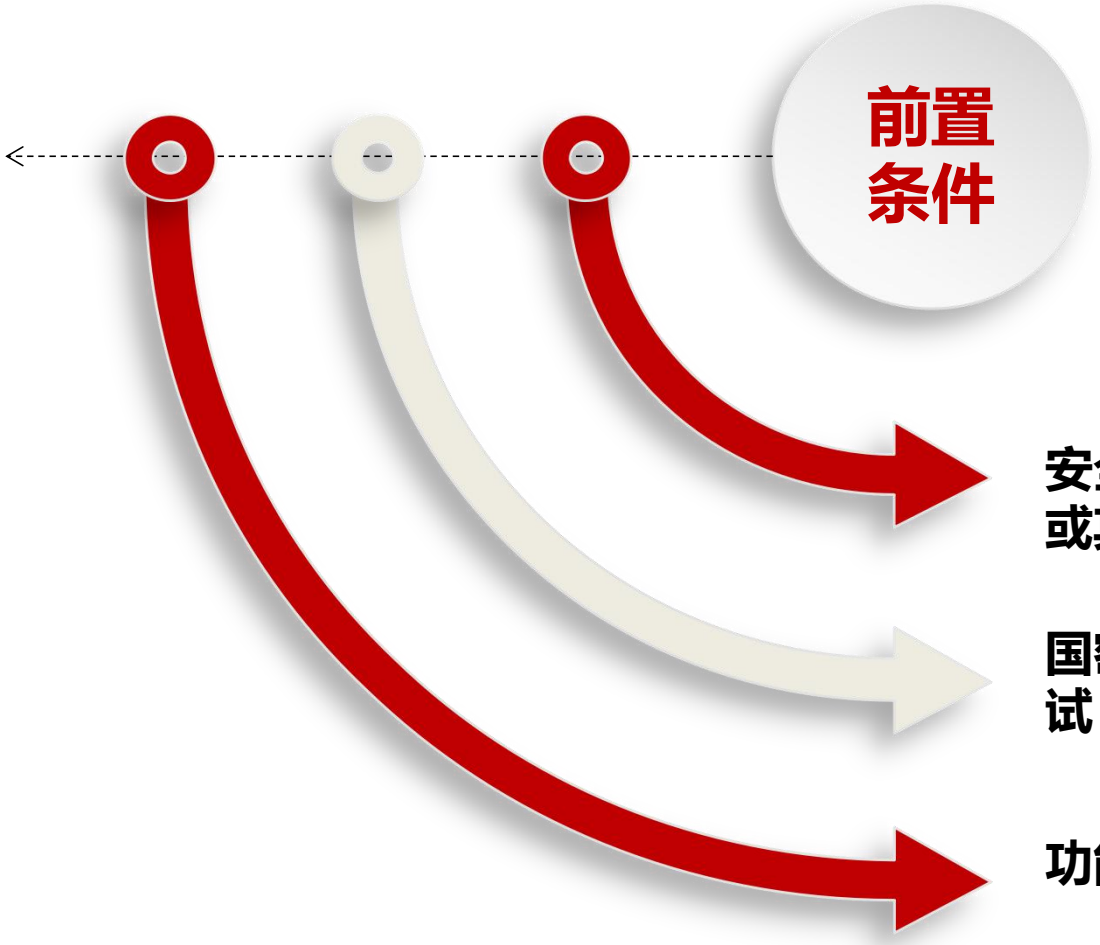
二、生产检查

解码芯片企业负责将TA发布的密钥文件导入产线黑盒系统并进行生产。TA将对解码芯片企业开展不定期检查，检查内容包括不限于：生产系统、生产环境、系统管理等。

检查依据为《新一代直播卫星解码芯片安全要求及生产控制规范》。

目录

四、DCAS业务流程

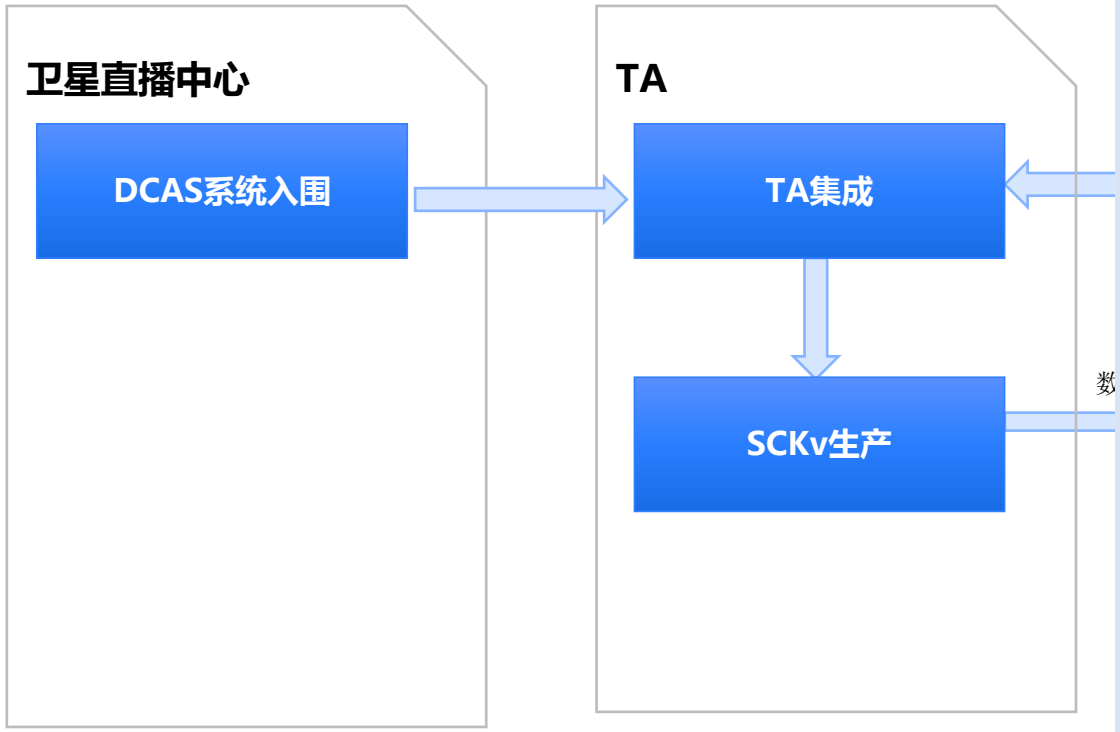


安全测试：前端系统通过中国信息安全评测中心EAL3或以上等级，或其它获得认可评测机构的同等安全级别测试

国密测试：前端系统和加密机通过商用密码检测中心的国密测试，取得国密型号。

功能和集成测试：通过相关检测机构的功能测试。

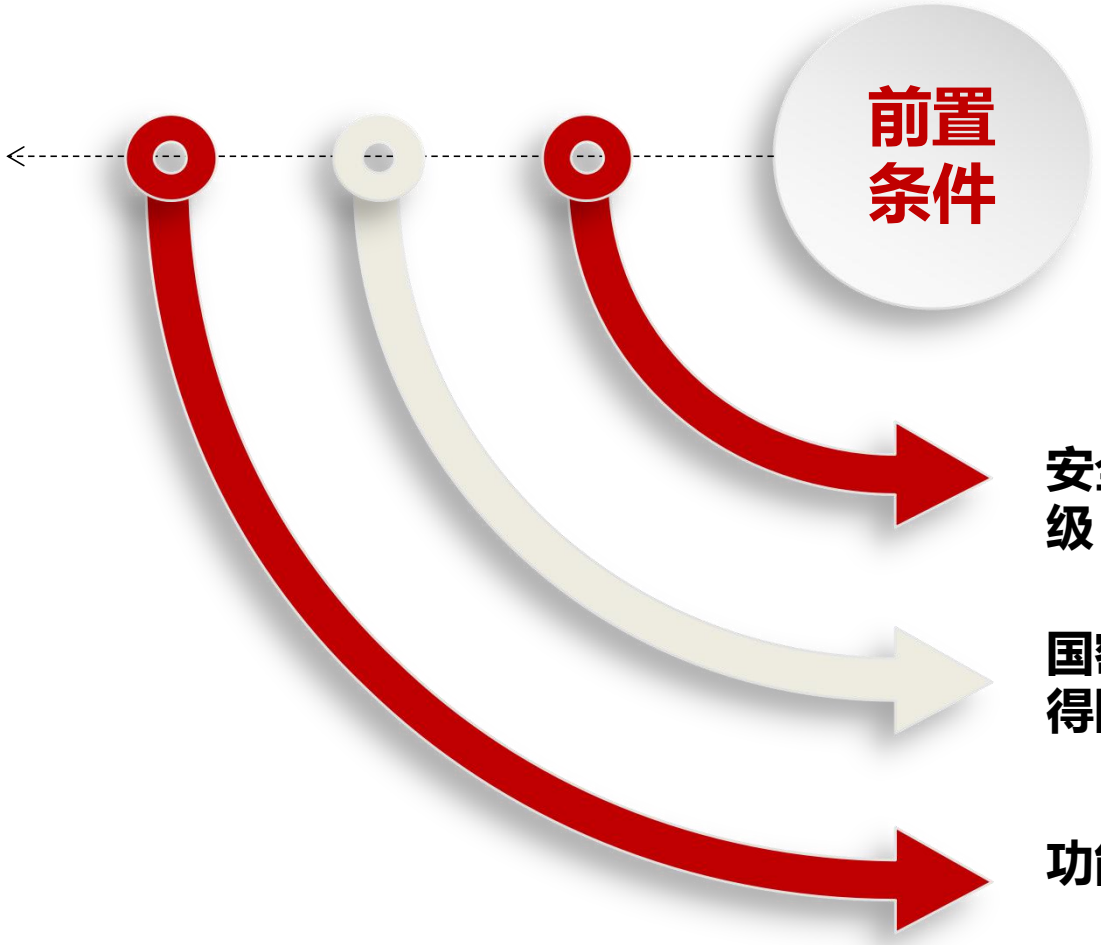
三、 DCAS业务流程



TA为DCAS企业分配一个Vendor_SysID。
TA向DCAS企业提供SCKv数据。
TA向DCAS企业提供解码芯片CHIPID。
TA用TA根证书为DCAS企业证书签名。
明确双方用于传输加密和验证的PGP公钥。

目录

四、HSM业务流程

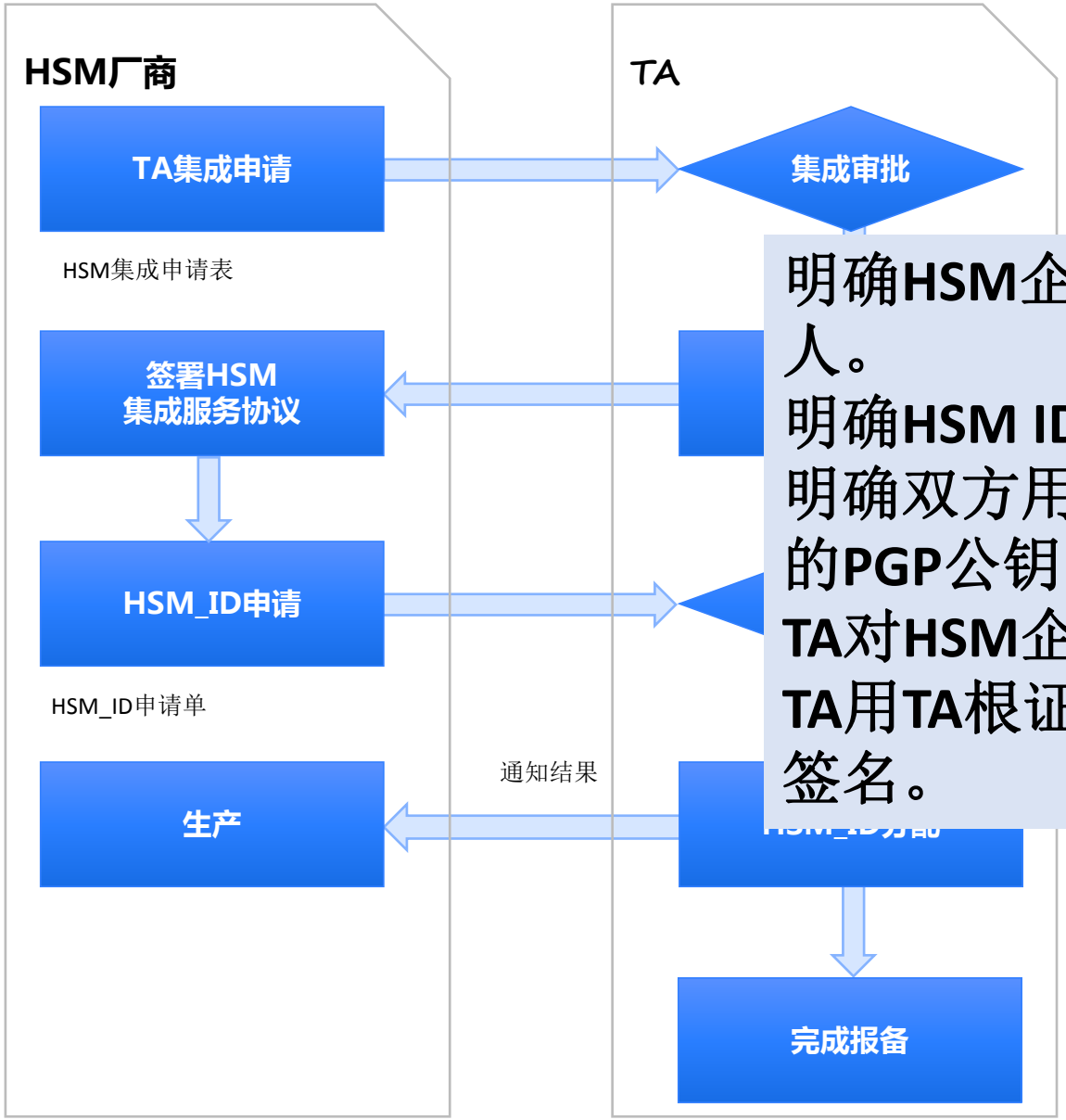


安全测试：HSM芯片通过中国信息安全评测中心EAL3或以上等级，或其它获得认可评测机构的同等安全级别测试

国密测试：HSM芯片通过商用密码检测中心的国密测试，取得国密型号。

功能和集成测试：HSM芯片通过广科院的DCAS功能和集成测试。

四、HSM业务流程



明确HSM企业授权代表、联系人。
明确HSM ID规则，测试ID范围。
明确双方用于传输加密和验证的PGP公钥。
TA对HSM企业分配HSM_ID。
TA用TA根证书对HSM企业证书签名。

谢 谢!