资源代价与安全算力

商用密码应用建设解决方案

GO TECH 国泰网信 闫彦

CONTENTS

目 录

01 密评概述

密评定义、密评标准、密评工作流程

什么是密码

- 密码是指使用特定变换对数据等信息进行**加密保护**或者**安全认证**的**物项**和**技术**。

加密保护	使用特定变换将原来可读的信息变成不能识别的符合序列
安全认证	使用特定变换确认信息是否被篡改、是否来自可靠信息源以及确认行为是否真实等
物项	实现加密保护或安全认证功能的设备与系统
技术	实现加密保护或安全认证功能的方法或手段

密码是保障网络与信息安全的基石

机密性

保证信息不被泄露给非授权的个人、计算机等实体。

真实性

保证信息来源可靠、没有被伪造和篡改。

完整性

保证数据没有受到非授权的篡改或破坏。

不可否认性

保证一个已经发生的操作行为无法否认。

商用密码应用现状

商用密码应用形势不乐观

- 密码应用**不广泛**
- 密码应用**不规范**
- 密码应用**不安全**

解决商用密码应用中存在的突出问题，为重要网络和信息系统的安全提供科学评价方法

- **以评促建**
- **以评促改**
- **以评促用**
- 逐步**规范**商用密码的使用和管理

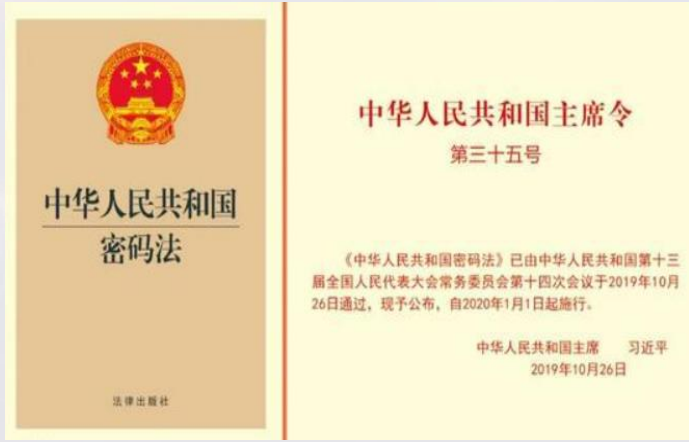
密评定义

- 《密码法》第二十七条规定

➢ 法律、行政法规和国家有关规定要求使用商用密码进行保护的**关键信息基础设施**，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展**商用密码应用安全性评估**(以下简称“密评”）。

➢ **定义：密评**是指对**采用商用密码技术、产品和服务**集成建设的**网络与信息系统**密码应用的**合规性、正确性、有效性**进行评估。

合规性：密码算法、密码技术、密码产品、密码模块和密码服务使用合规;
正确性：密码算法、密码协议、密钥管理、密码产品和服务使用正确;
有效性：密码协议、密钥管理系统、密码应用子系统和密码安全防护机制不仅设计合理，在系统运行过程中能够发挥密码作用。



- 密评意义

开展密评，是为了解决商用密码应用中存在的突出问题，为网络和信息系统的安全提供科学评价方法，逐步规范商用密码的使用和管理。从根本上改变商用密码应用**不广泛、不规范、不安全**的现状，确保商用密码在网络和信息系统中有效使用，切实构建起坚实可靠的网络安全密码屏障。

密评对象

- **基础信息网络**：电信网、广播电视网、互联网
- **重要信息系统**：能源、教育、公安、测绘地理信息、社保、交通、 卫生计生、金融等涉及国计民生和基础信息资源的重要信息系统
- **重要工业控制系统**：核设施、航空航天、先进制造、石油石化、油气管网、电力系统、交通运输、水利枢纽、城市设施等重要工业控制系统
- **面向社会服务的政务信息系统**：党政机关和使用财政性资金的事业单位和团体组织使用的面向社会服务的信息系统

密评相关角色及工作简介

密评角色

系统责任单位

系统规划、建设实施
运行验收、应急预案

- **规划阶段**：责任单位依据商用密码技术标准，制定商用密码应用建设方案，组织专家或委托具有相关资质的测评机构进行方案评估
- **建设阶段**：系统建设完成后，责任单位应当委托测评机构开展密评（对照密码应用方案）
- **运行阶段**：责任单位应当委托测评机构定期开展密评（对照密码应用方案），若评估未通过，责任单位应当期限整改并重新组织评估

密码服务提供商

科研能力、产品供给
解决方案、系统集成
密码服务

- **规划阶段**：配合系统责任单位设计密码应用解决方案、实施方案、应急处置方案，配合密码应用安全性评估
- **建设阶段**：提供密码产品、密码集成、密码运维服务，配合密码应用安全性评估
- **运行阶段**：提供密码运维服务，配合密码应用安全性评估

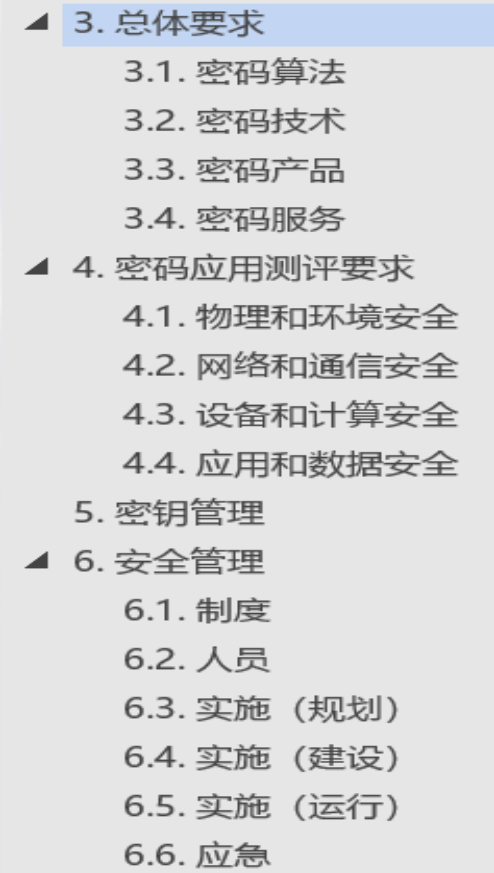
测评单位

密码技术基本测评
密码技术应用测评

- **规划阶段**：**制定系统测评方案与实施方案-测评备案-开展测评-形成测评报告**
- **建设阶段**：**针对密码应用技术**（物理和环境安全、网络和通信安全、设备和主机安全、应用和数据安全）、**密钥管理、安全管理开展测评。**
- **运行阶段**：**合规性评估：** 按照《商用密码管理条例》等密码法规和行业相关的密码使用要求，是否使用符合国家密码法规和标准规定的商用密码算法，是否使用经过国家密码管理局审批的密码产品或服务
正确性评估： 系统中采用的标准密码算法、协议和密钥管理机制是否按照相应的密码国家和行业标准进行正确的设计和实现。自定义密码协议、密钥管理机制的设计和实现是否正确，是否符合相关标准要求；密码保障系统建设或改造过程中密码产品和服务的部署和应用是否正确。
有效性评估： 密码应用安全是否立足系统安全、体系安全、动态安全、纵深防御、体系建设的思想，环境+设备+网络+应用

测评标准及依据

- 依据标准
  - GB/T 39786-2021《信息系统密码应用基本要求》
  - 《信息系统密码测评要求》（试行）
  - 《信息系统密码测评过程指南》
  - 《商用密码应用安全性评估管理办法》（试行）
  - 《商用密码应用安全性评估作业指导书》
  - 《商用密码应用安全性评估测评工具使用需求说明》
- 参照标准
  - 13个GB标准，53个GM
  - 《GB/T 22239-2018 信息安全技术 信息系统安全等级保护基本要求》
  - 《GB/T 20984-2007 信息安全技术 信息安全风险评估规范》
- 关键点
  - 相关密码产品需具有国密局相关资质认证
  - 定制化的密码组件原则上单独取证（密码模块）
  - 密码服务体系设计安全合规（密钥安全）



密评工作流程-被测单位


新建系统
规划
建设
运行
应急
网络运营者
制定密码应用方案
建设实施
定期评估（关基、等保三每年一次）
事件、调整特殊情况通报
密评机构
评估密码应用方案
密码应用安全性评估
密码管理部门
指导-监督-检查
已建系统
差距评估
改造规划
改造实施
运行阶段
应急响应
网络运营者
组织评估
制定密码应用方案
改造实施
定期评估
事件、调整特殊情况通报
密评机构
密码应用安全性评估
评估密码应用方案
密码应用安全性评估
密码管理部门
指导-监督-检查

密评工作流程-测评机构


① 前期调研组
② 现场测评组
③ 报告审批组
调研
方案编制
测评准备
现场测评
分析与
报告编制
报告审核
出具报告
信息系统资产
信息安全等级
安全防护现状
测评对象与指标确定
测评工具接入点确定
测评内容确定
测评工具和表单准备
现场测评准备
现场测评和结果记录
问题整改与回归测评
结果确认与资料归还
单项测评结果判定
单元测评结果判定
整体测评与风险分析
测评结论与报告编制
密码应用安全性
测评报告

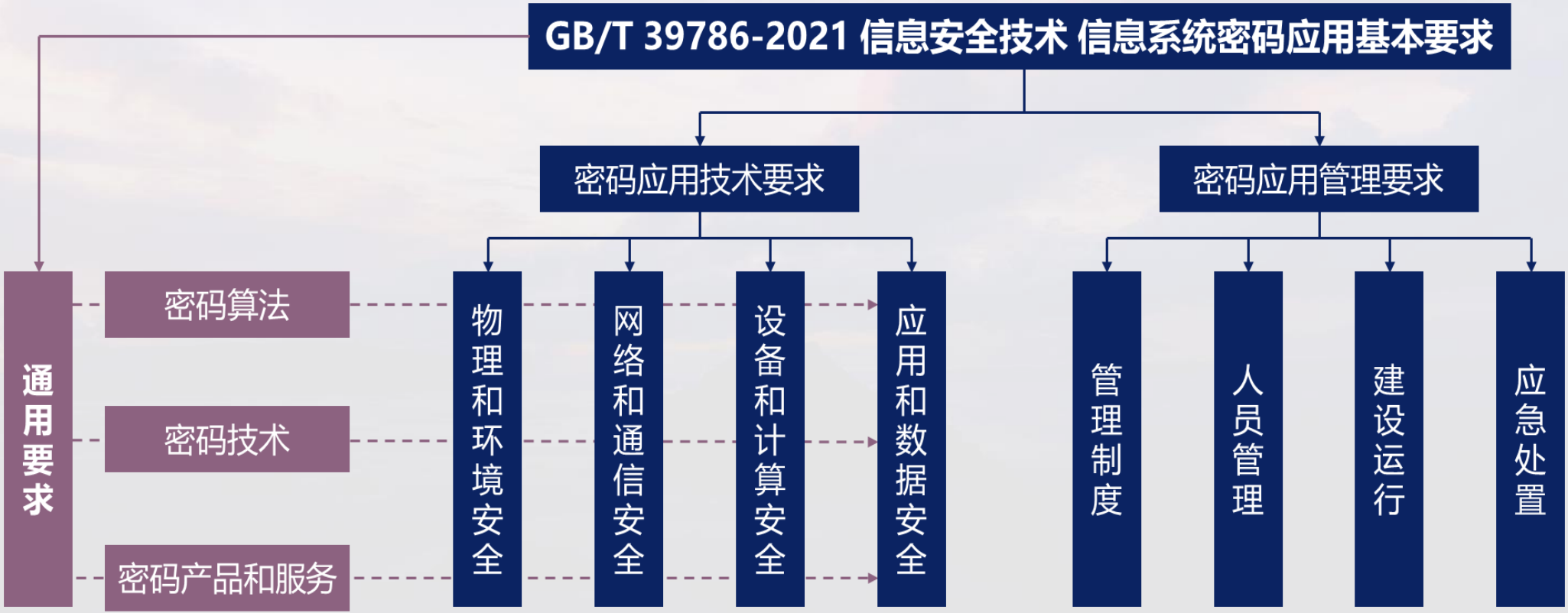
密评工作流程-测评机构

	量化评估		风险分析		评估结论
	100分	且	无风险	=	符合
目前阈值为60分	≥阈值	且	无高风险	=	基本符合
	<阈值	或者	有高风险	=	不符合

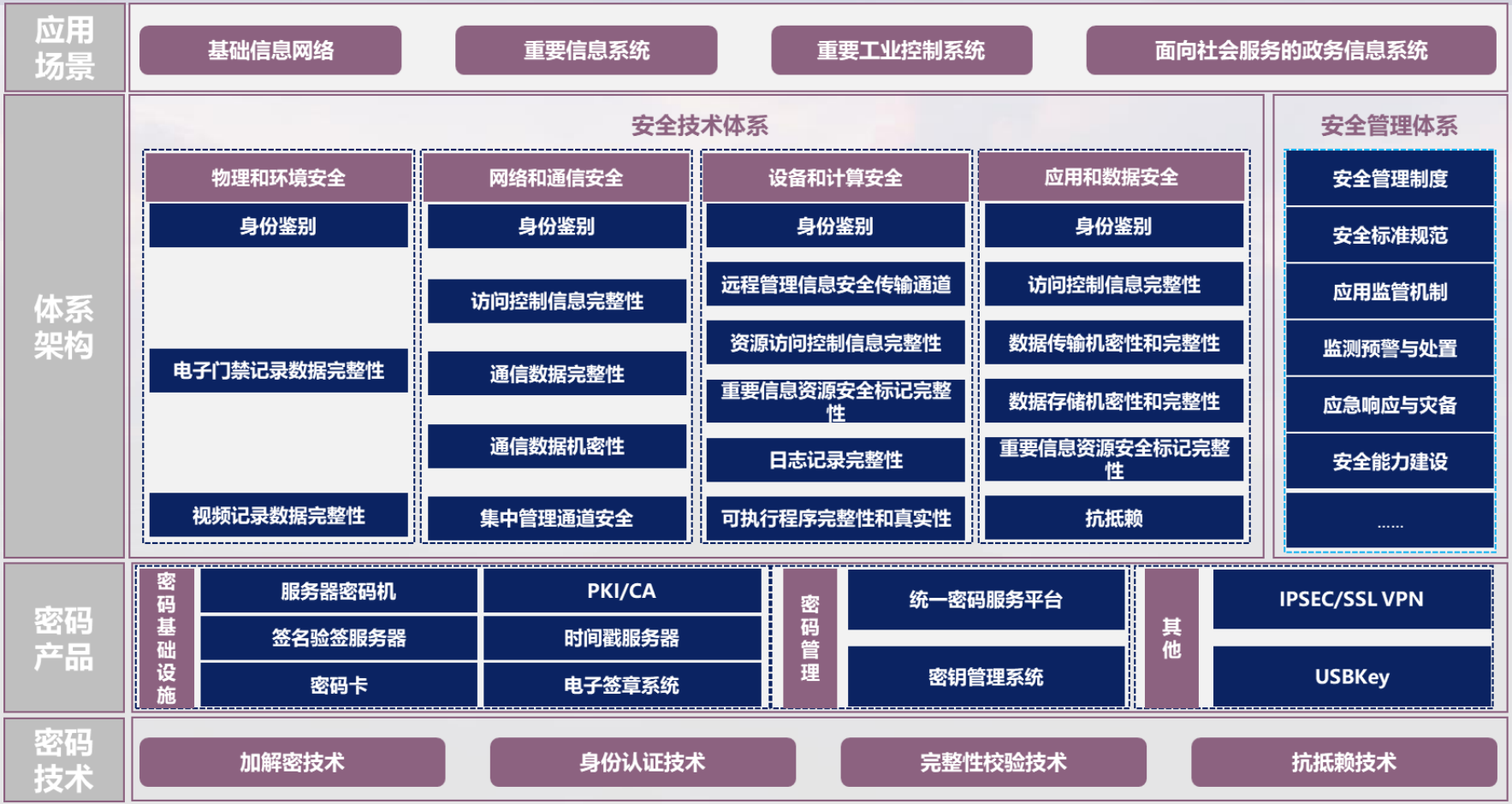
02 密码应用合规方案设计

方案架构、技术原理、合规方案设计

密码应用建设需求


GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求
密码应用技术要求
密码应用管理要求
通用要求
密码算法
密码技术
密码产品和服务
物理和环境安全
网络和通信安全
设备和计算安全
应用和数据安全
管理制度
人员管理
建设运行
应急处置

密码应用合规方案架构

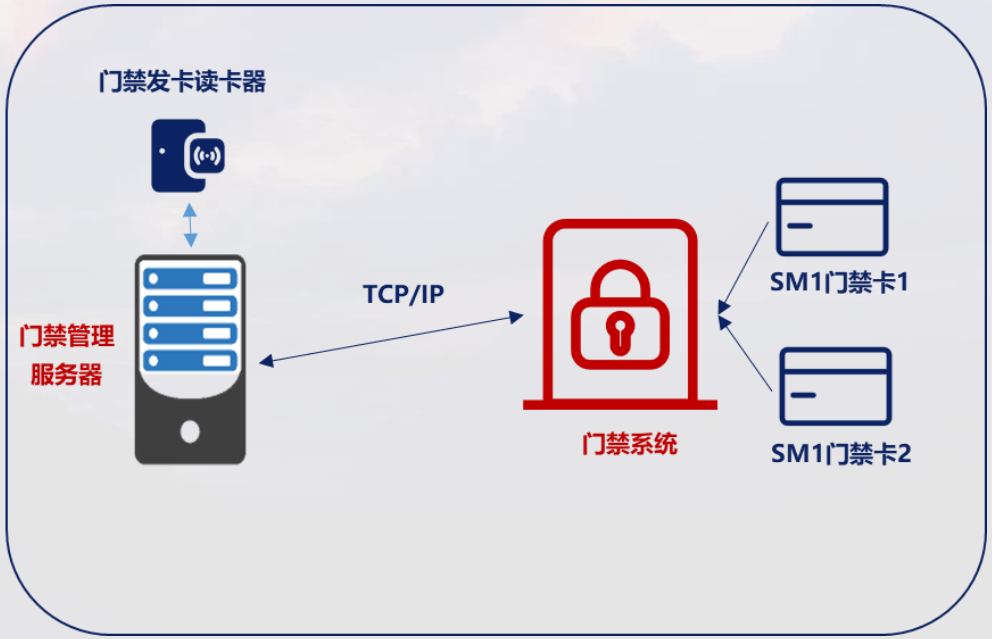

应用场景
基础信息网络
重要信息系统
重要工业控制系统
面向社会服务的政务信息系统
体系架构
安全技术体系
物理和环境安全
身份鉴别
电子门禁记录数据完整性
视频记录数据完整性
网络和通信安全
身份鉴别
访问控制信息完整性
通信数据完整性
通信数据机密性
集中管理通道安全
设备和计算安全
身份鉴别
远程管理信息安全传输通道
资源访问控制信息完整性
重要信息资源安全标记完整性
日志记录完整性
可执行程序完整性和真实性
应用和数据安全
身份鉴别
访问控制信息完整性
数据传输机密性和完整性
数据存储机密性和完整性
重要信息资源安全标记完整性
抗抵赖
安全管理体系
安全管理制度
安全标准规范
应用监管机制
监测预警与处置
应急响应与灾备
安全能力建设
.....
密码产品
密码基础设施
服务器密码机
PKI/CA
签名验签服务器
时间戳服务器
密码卡
电子签章系统
密码管理
统一密码服务平台
密钥管理系统
其他
IPSEC/SSL VPN
USBKey
密码技术
加解密技术
身份认证技术
完整性校验技术
抗抵赖技术

密码建设-物理和环境安全

- 门禁系统改造

➢ 更换符合GM/T 0036-2014《采用非接触卡的门禁系统密码应用指南》标准要求，并取得**商用密码产品型号证书**的门禁系统，使用国密算法进行密钥分散，实现门禁卡的“一卡一密”，并基于国密算法对人员身份进行鉴别；

➢ 门禁管理服务器需支持对进出记录的完整性保护，通过门禁系统厂家配合整改完成人员出入记录的完整性保护。



- 可选措施

➢ 基于生物识别技术（如指纹等）对进出入人员进行身份鉴别；

➢ 重要区域出入口配备专人值守并进行登记，且采用视频监控系统进行实时监控等。

密码建设-网络和通信安全

- 站到站的密码建设

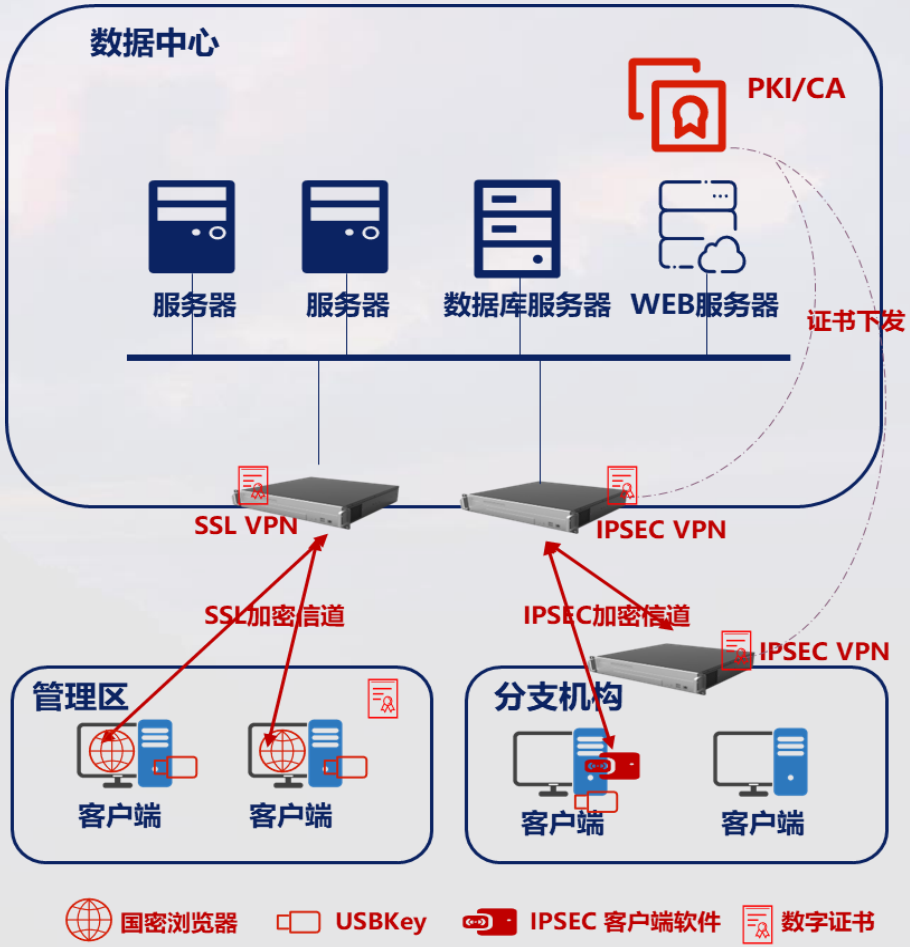
在分支机构网络出口处和企业内网网络出口处成对部署IPSEC VPN，进行站到站的网络链路安全防护，完成传输链路的数据机密性和完整性以及身份真实性校验。

- 端到站的密码建设

在网络边界部署符合国密标准的SSL VPN设备，通过VPN设备保障通信过程中数据的机密性和完整性。SSL VPN 在客户端测需使用国密浏览器，或者浏览器进行国密改造，安装国密浏览器插件。

- 可选措施

在“应用和数据安全”层面针对重要数据传输采用服务器密码机进行重要数据加密传输，完成机密性保护；



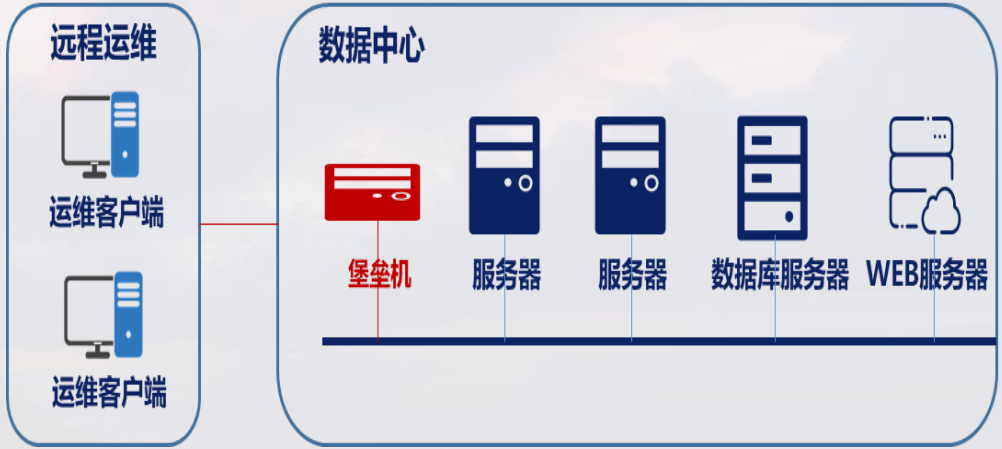
密码建设-设备和计算安全

- 身份鉴别

关闭设备的本地登录，远程运维人员通过具有密码功能的堡垒机，使用堡垒机的人员身份鉴别功能，实现设备的远程安全管理及登录用户身份鉴别。

- 完整性校验

设备厂家对设备进行升级改造，添加密码模块和设备数字证书，在日志生成时进行数字签名。后续查看调用日志时进行签名验签，完成设备日志的完整性校验。



- 缓解措施
  - 在“网络与通信层”/“应用与数据层”建立身份认证机制。
  - 在“网络和通信安全”层面采用SSL/IPSEC VPN保证重要数据在传输过程中的机密性；
  - 应用系统通过服务器密码机/签名验签服务器进行身份鉴别，保证只有授权人员才能访问应用系统的重要数据，且定期对重要数据进行备份；

密码建设-应用和数据安全

- 身份鉴别

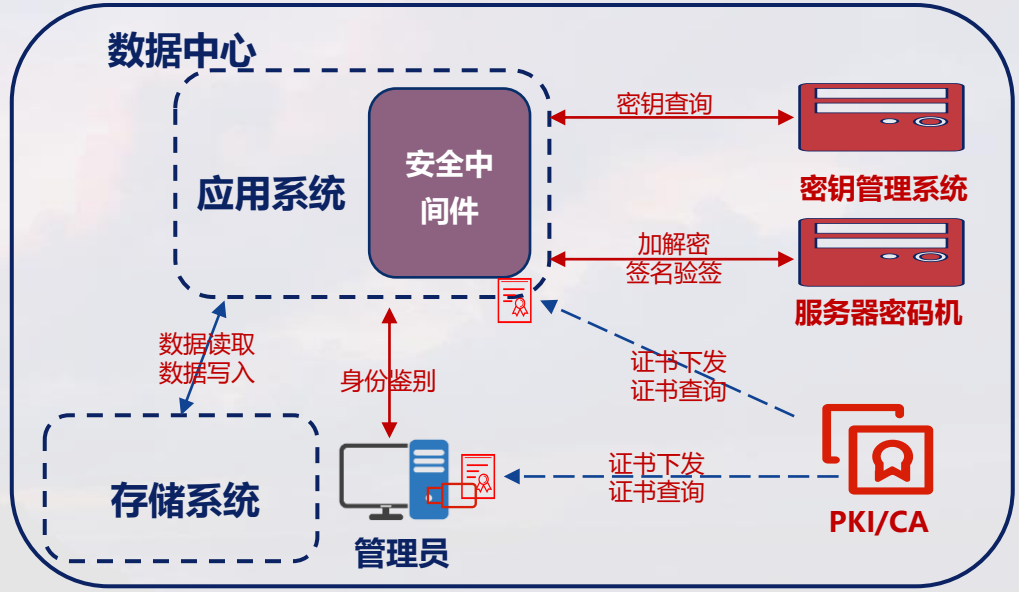
数据中心部署服务器密码机，通过应用系统配合整改，在系统管理员登录时，安全中间件调用服务器密码机生成签名挑战，与管理员交换挑战值后签名验签，完成身份鉴别。

- 数据传输加密

安全中间件调用密码机接口，提交原始数据及密钥，通过服务器密码机加密后传输至管理员客户端，客户端通过调用USBKey进行解密，完成数据传输加密。

- 数据存储加密

应用系统通过密钥管理系统进行加密密钥查询，安全中间件调用密码机接口，提交原始数据及密钥，通过服务器密码机加密后写入到存储系统，完成数据存储加密。

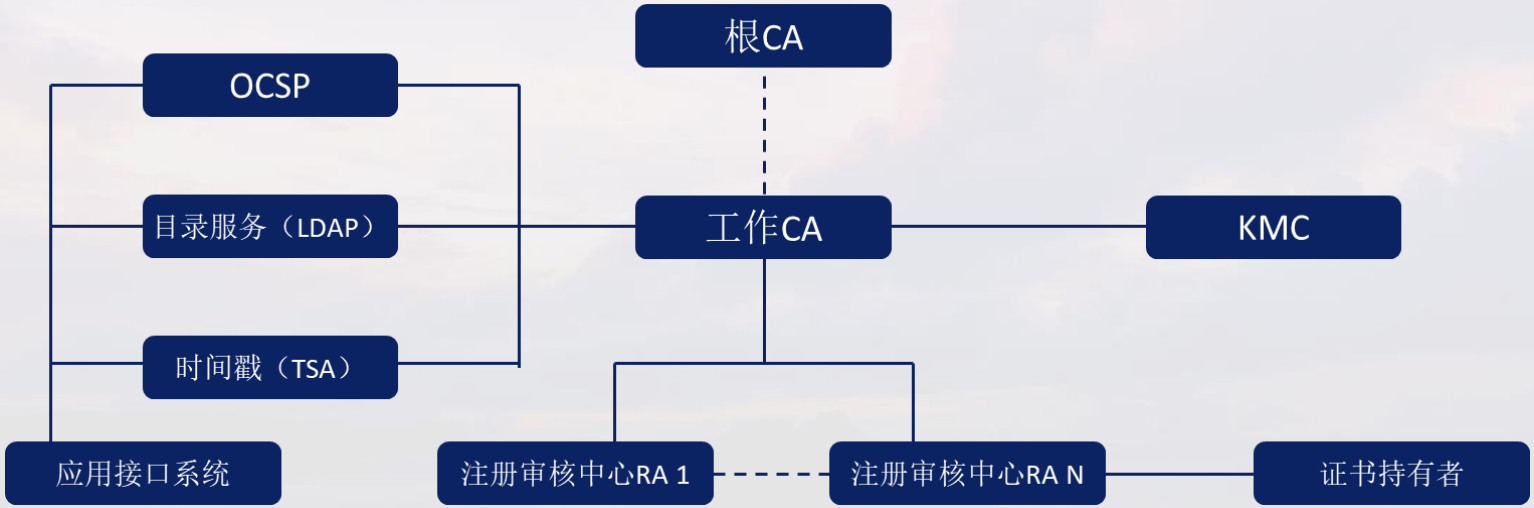


- 可选措施

- 基于特定设备（如手机短信验证）或生物识别技术（如指纹）保证用户身份的真实性；
- 在“网络和通信安全”层面使用SSL /IPSec VPN网关等建立集中管理通道。

密码建设-密码管理建设

- 证书认证体系



- 改造要点

  - 重要性：密码应用体系建立的核心环节，身份认证、完整性校验、抗抵赖等机制均需要数字证书进行支撑；
  - 利旧问题：一个信任体系通常只保留一套CA系统，也可采用证书租用方式实现；
  - 密钥管理问题：证书系统可以全面支撑非对称密钥的管理过程。

密码建设-密码管理建设

- 密钥管理体系

- 改造要点

➢ **密钥管理维度问题**

CA系统无法管理的密钥类型均需要通过密钥管理系统实现，一般常见情况是存在数据加密存储需求时，与服务器密码机配套使用。

➢ **密管系统建设问题**

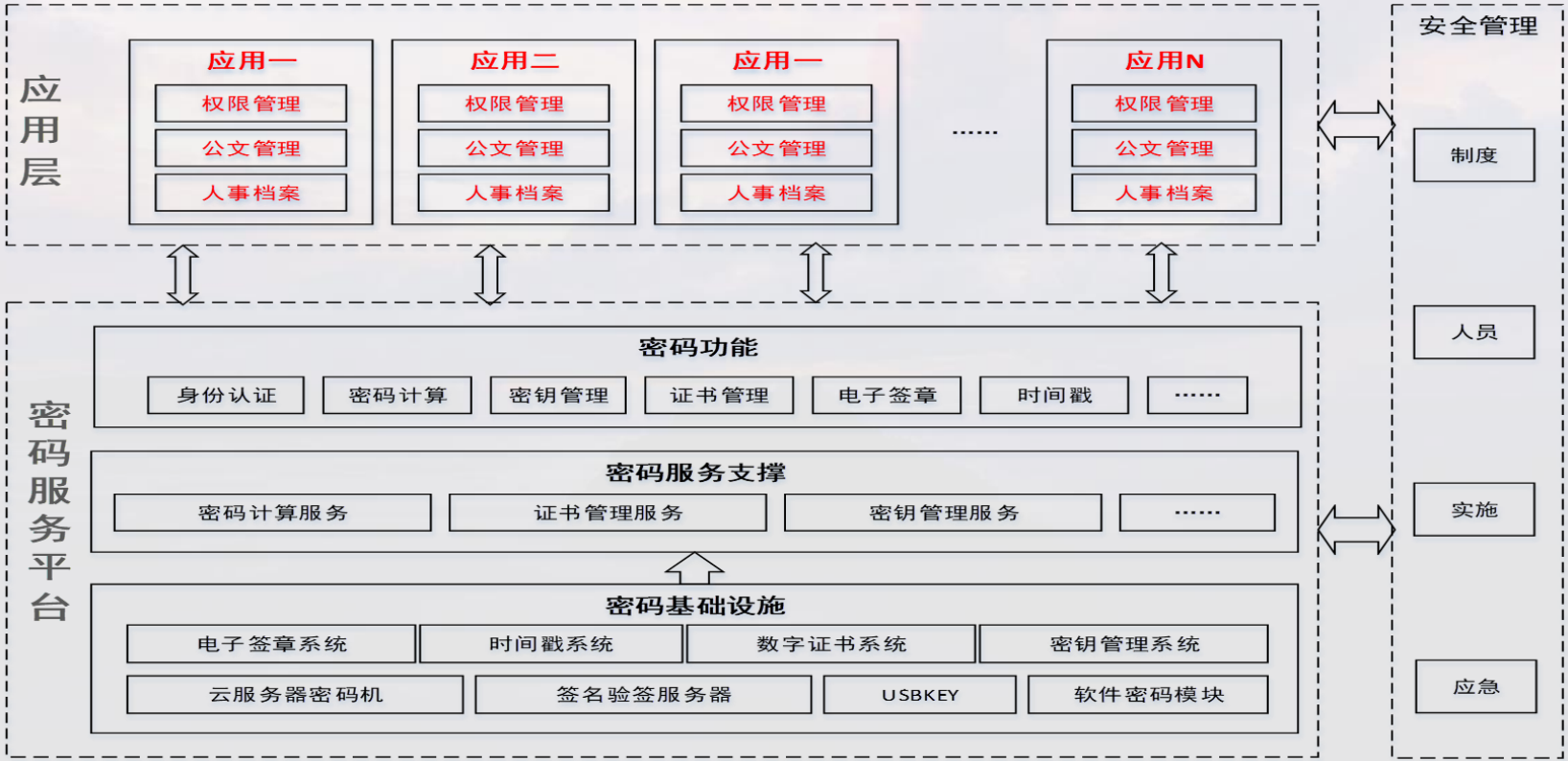
需要了解具体业务逻辑进行定制和接口适配，简单场景可由业务应用根据密钥管理体系自实现。

➢ **配套密码机问题**

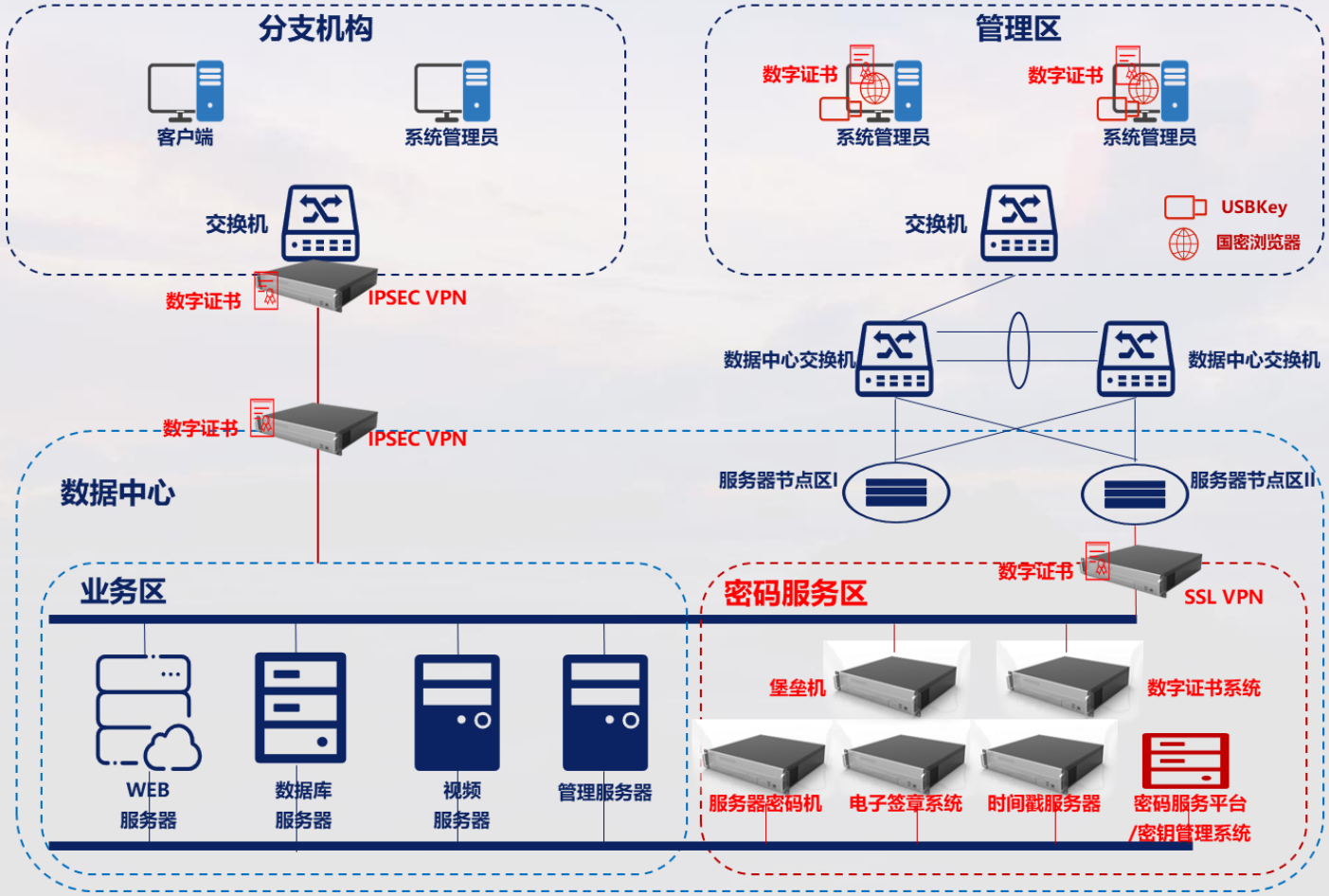
密钥管理系统配套的密码机为专用密码机，不可以同业务系统共用。

密码建设-密码管理建设

- 密码服务平台

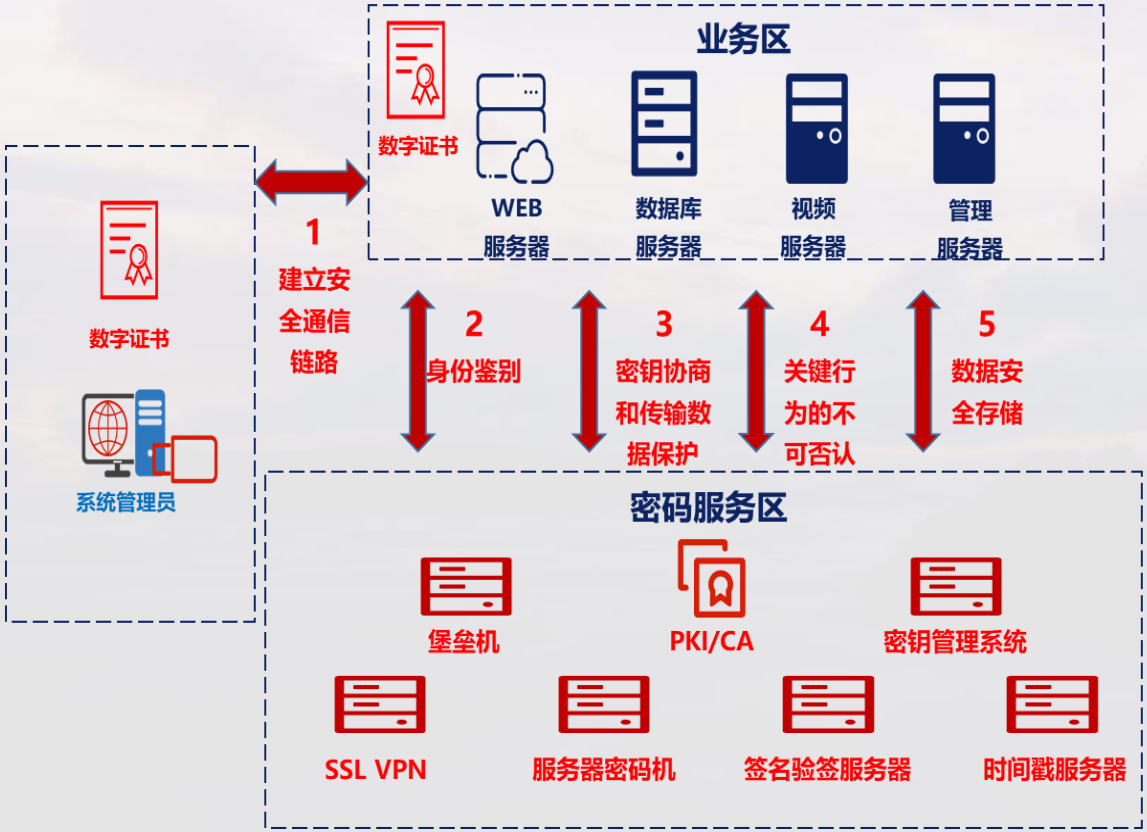


密码建设-整体部署方案



- 服务器密码机/签名验签服务器
- 密码服务平台/密钥管理系统
- 数字证书系统
- SSL/IPSec VPN网关
- 国密浏览器
- USBKey
- 门禁系统
- 时间戳系统/电子签章系统
- 国密堡垒机
- 日志审计服务器
- 根据业务需求配置

密码建设-密码应用工作流程



1、建立安全通信链路：系统管理员调用USBKey，使用国密浏览器与SSL VPN建立安全通信链路；

2、身份鉴别：系统管理员利用用户名/口令和USBKey的方式，通过PKI/CA，登录服务器短的后台管理系统；

3、密钥协商和传输数据保护：第一步中安全链路只保护了国密浏览器与SSL VPN网关之间的交互数据。考虑应用系统中存在个分系统，为了实现各系统间数据隔离，系统管理员和各个分系统之间的敏感数据也需要单独安全保护，防护方式主要通过分系统与对应的系统管理员通过各自的密钥对利用SM2密钥协商算法协商临时的保密性和完整性保护密钥，完成系统管理员访问应用时敏感数据的安全传输；

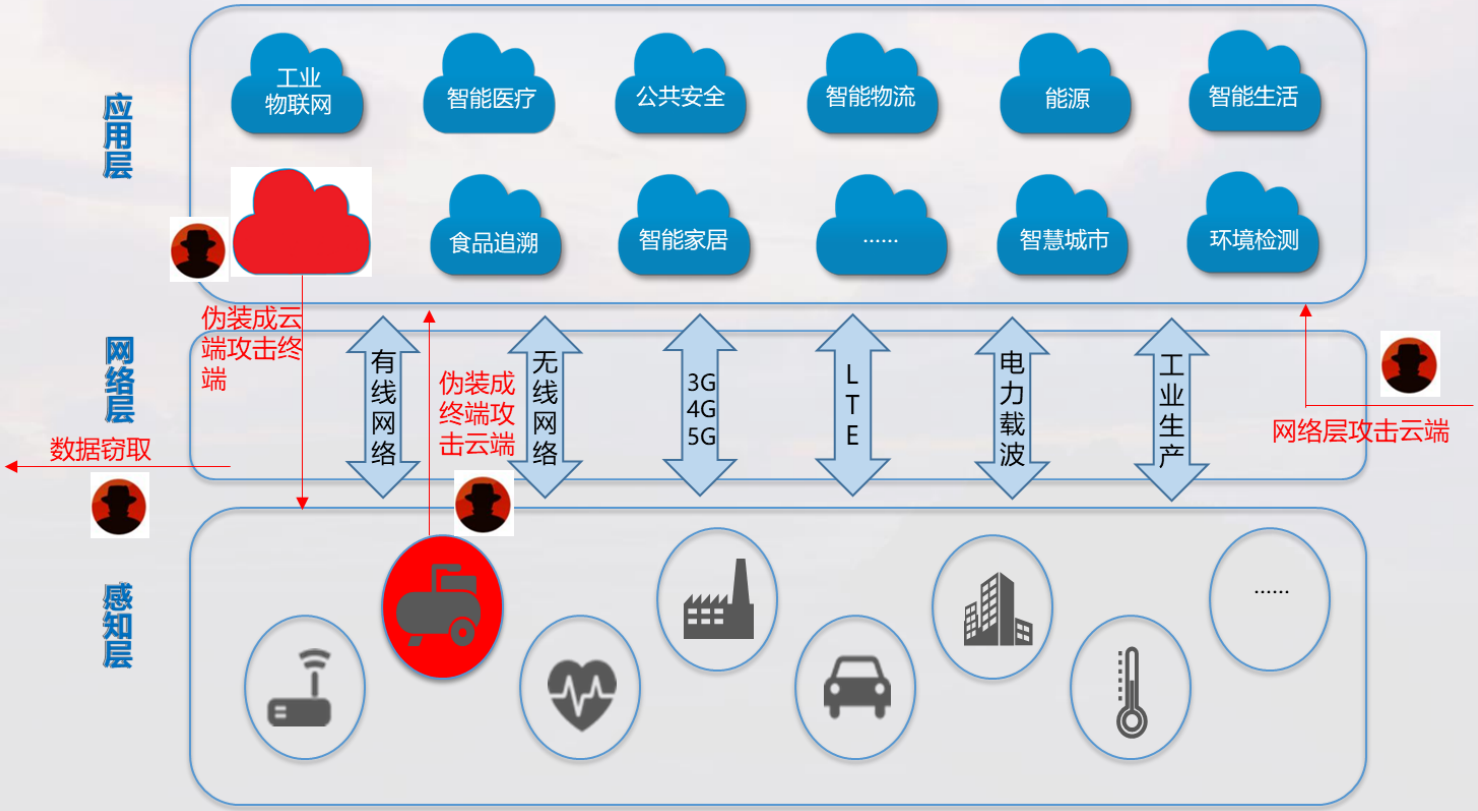
4、关键操作的不可否认性：对于系统管理员的关键操作，需要系统管理员使用USBKey进行数字签名，并由系统调用服务器密码机进行验签，以验证该操作确实由系统管理员完成，确保关键操作的不可否认性；

5、数据安全存储：服务器收到系统管理员编辑确认的关键数据后，调用服务器密码机，利用自己的加密密钥和HMAC密钥对重要数据进行保密性和完整性保护，之后服务器将其存储到数据库服务器中。

03 特殊场景密码建设方案

物联网、工业控制、移动办公、视频监控

物联网场景-物联网安全风险



物联网安全风险主要集中在应用层和感知层

应用层风险：

- 来自网络的攻击
- 伪装的感知终端攻击
- 数据窃取

感知层风险：

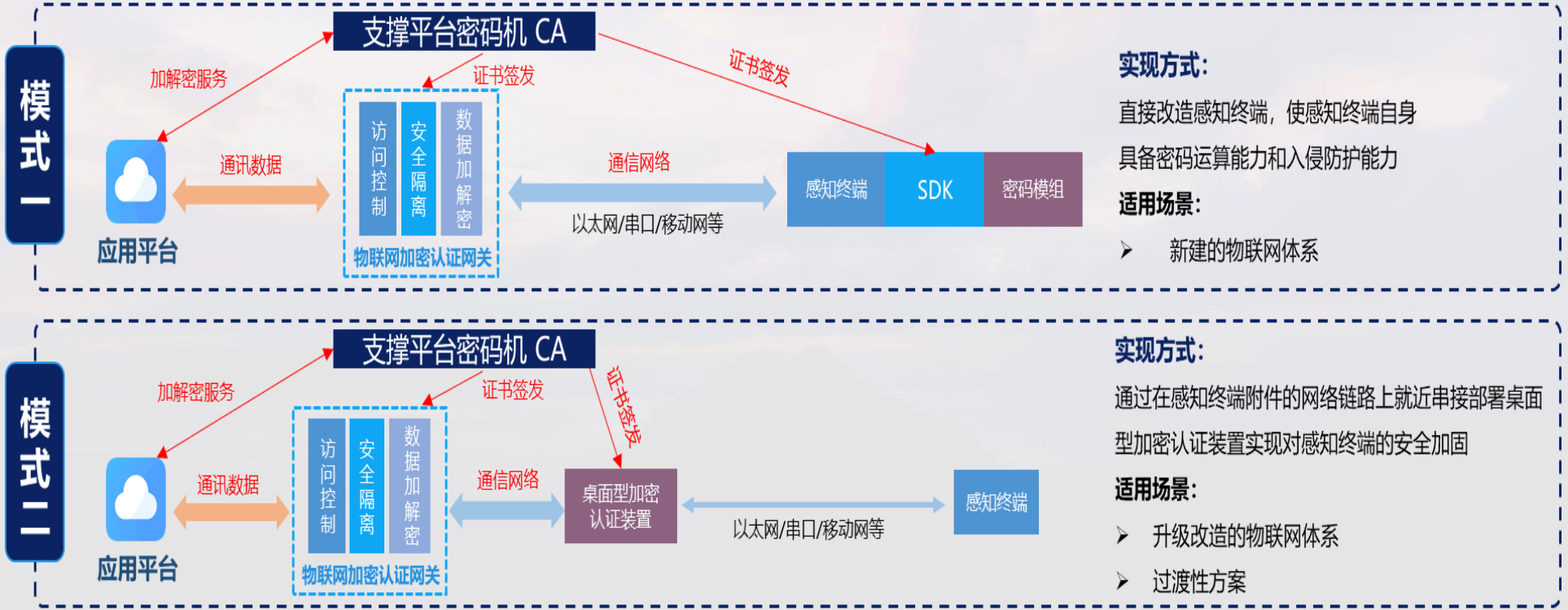
- 来自网络的控制指令和攻击
- 伪装的云端应用异常指令和攻击
- 数据窃取

物联网场景-安全防护思路

技术路线

- 应用层入侵防护：网络隔离技术
- 感知层入侵防护：协议白名单
- 身份认证：基于PKI/CA体系
- 数据加密：VPN技术/应用层加密
- 态势感知平台：提供数据采集装置和边缘计算能力

物联网场景-物联网安全密码技术实现



工业场景-密码建设方案

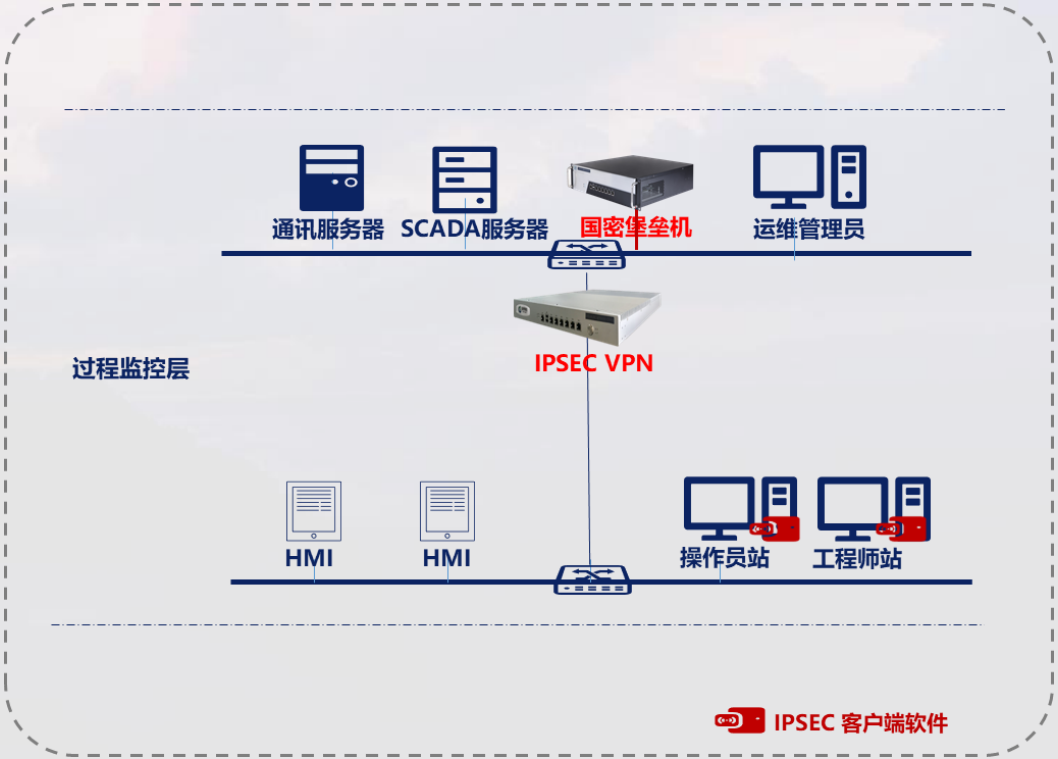
- 工业控制系统特点

- 密码应用需求

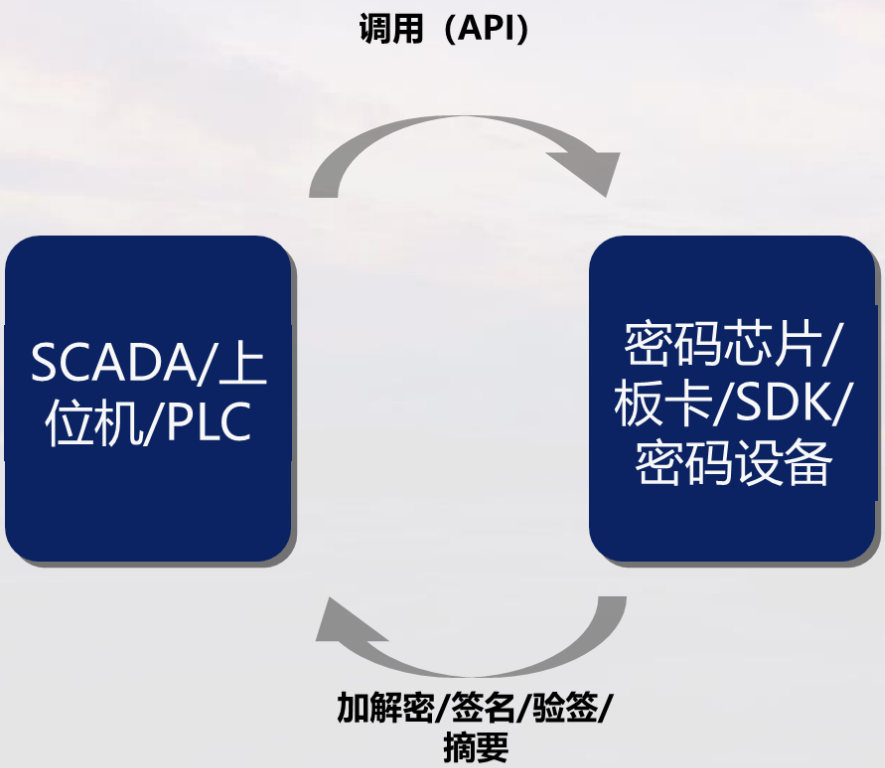
➢ 网络层传输重要指令加密；

➢ 操作人员及运维人员的身份鉴别。

- 密码建设方案



工业场景-工业控制系统与密码的技术融合机制



安全可靠的密码运算与密钥存储机制

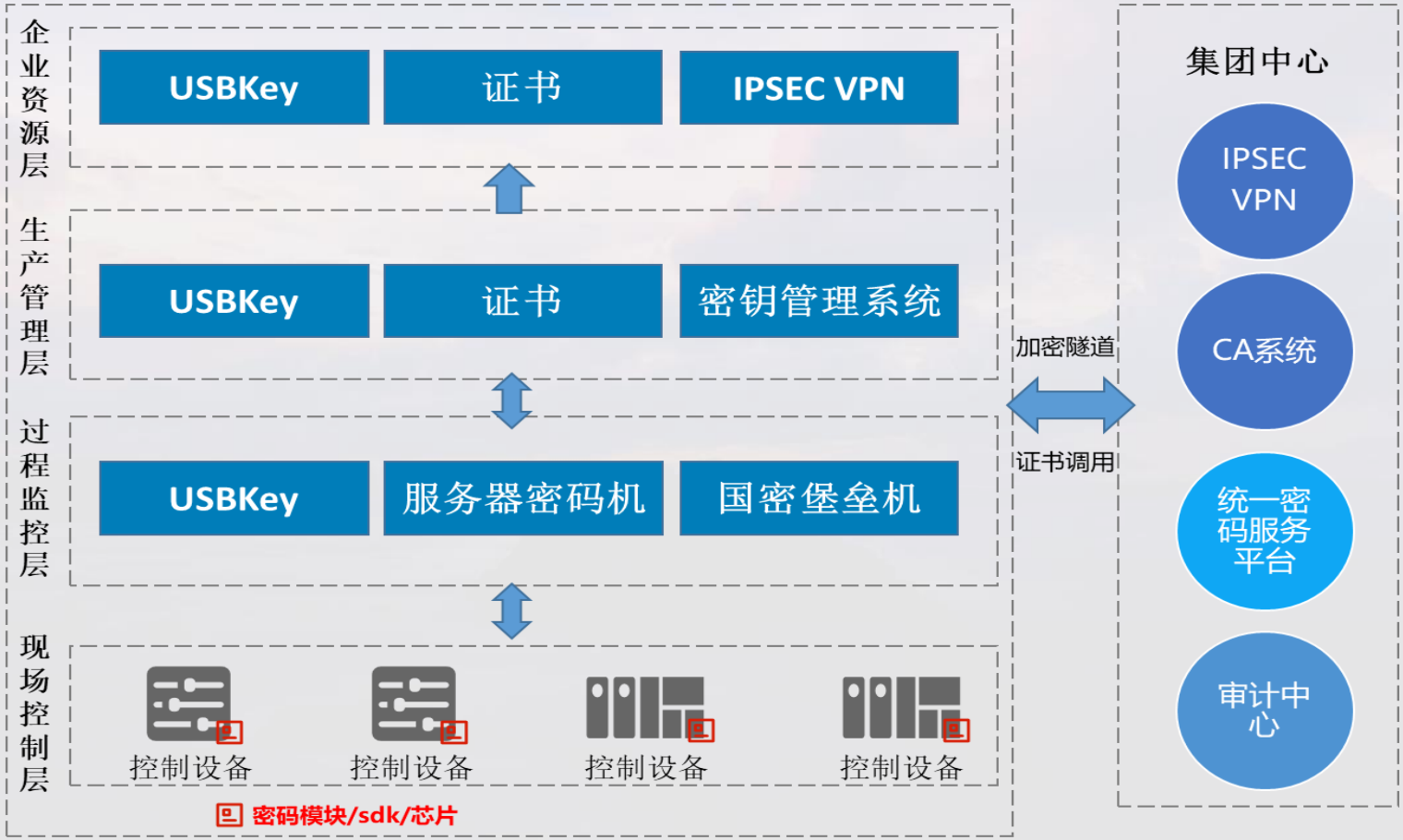
- 技术融合机制

  - 密码组件的形态选择
  - 工业协议的适配和改造
  - 密码应用机制的选择
  - 系统可用性要求、密码性能与成本之间的平衡

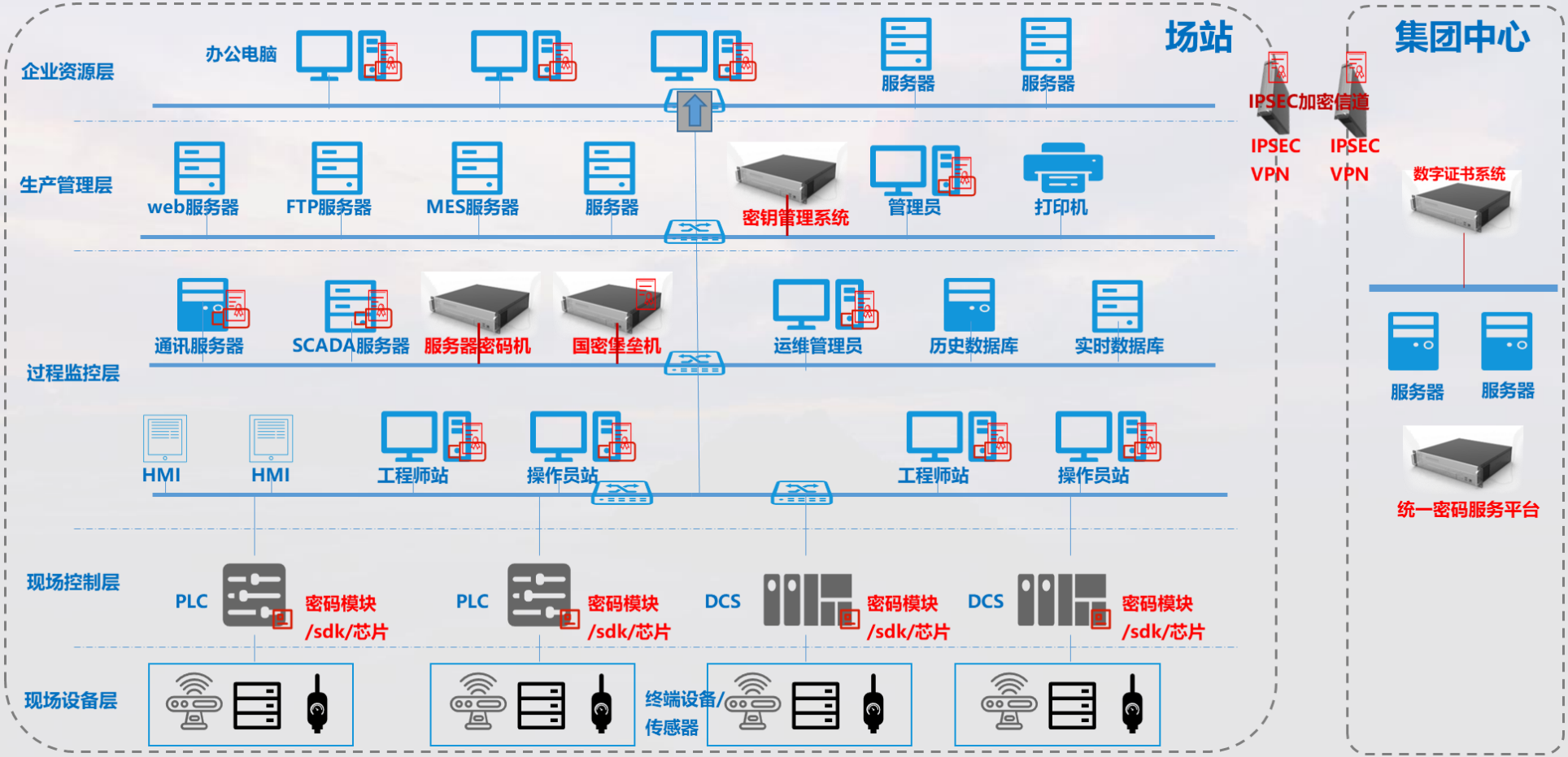
工业场景-工业控制系统与密码的技术融合机制

安全与业务高度融合，使网络安全机制成为业务系统内生安全基因，不受攻防水平差距影响，不依赖网络结构，不存在传统意义上的边界概念

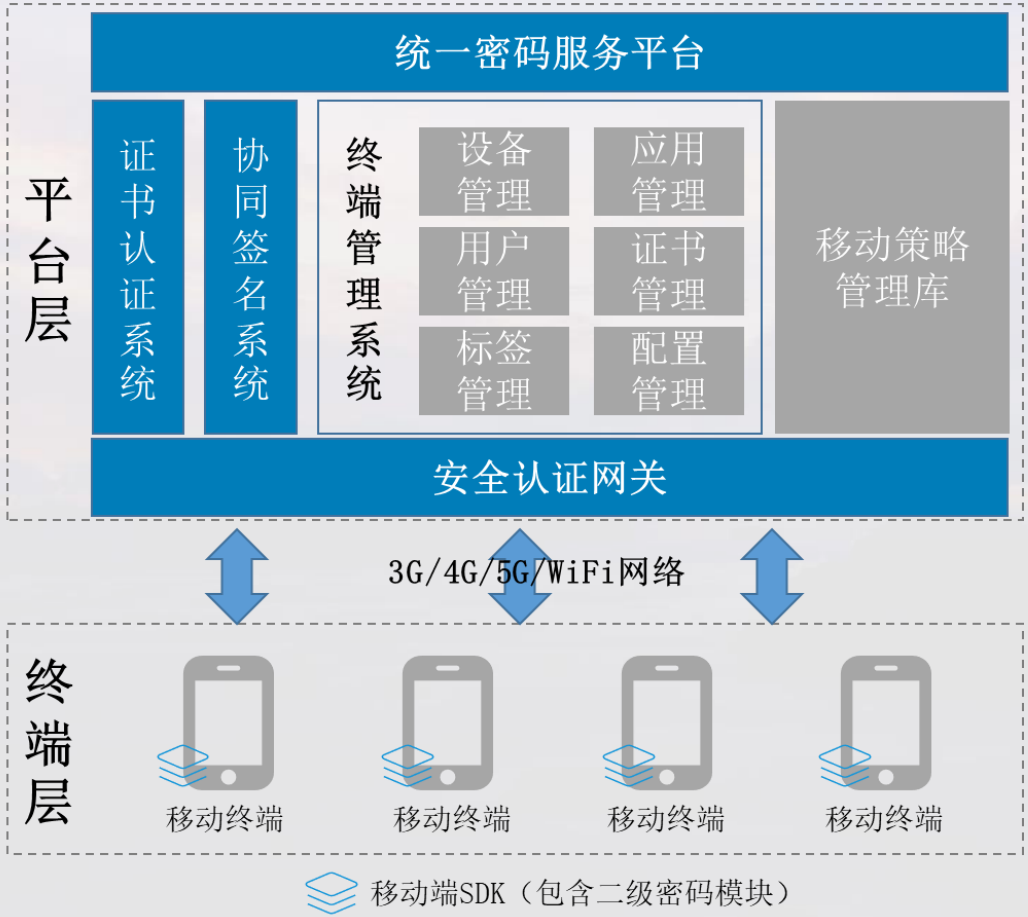
工业场景-安全防护思路


企业资源层
USBKey
证书
IPSEC VPN
生产管理层
USBKey
证书
密钥管理系统
过程监控层
USBKey
服务器密码机
国密堡垒机
现场控制层
控制设备
控制设备
控制设备
控制设备
密码模块/sdk/芯片
加密隧道
证书调用
集团中心
IPSEC VPN
CA系统
统一密码服务平台
审计中心

工业场景-密码应用部署图



移动办公场景-安全防护思路



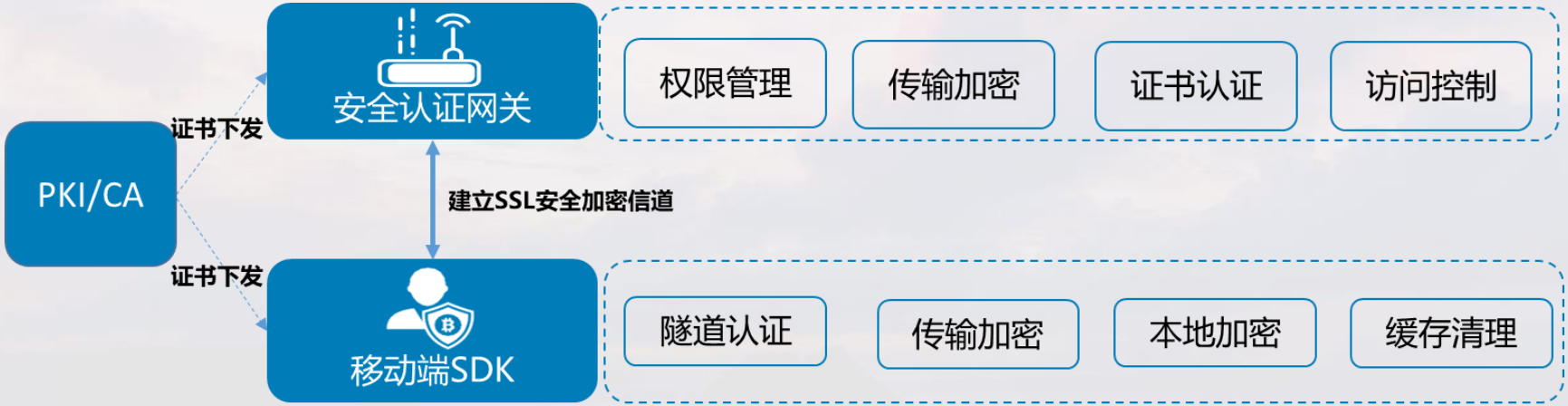
技术防护思路

针对移动办公系统网络层、设备层和应用层安的全防护通过身份认证、数据加密、完整性校验技术实现。主要通过移动端SDK、安全认证网关、证书认证系统和统一密码服务平台等密码产品来实现。移动终端侧密码模块一般以SDK形式嵌入在移动端APP中。

- 身份认证：基于PKI/CA体系
- 数据加密：VPN技术/应用层加密
- 完整性校验：APP数字签名技术
- 密钥保护：门限密码/协同签名/密钥白盒

移动办公场景-网络和通信

- 身份鉴别、数据传输机密性、完整性校验



- 网络层安全防护

➢ PKI/CA系统对安全认证网关和移动终端发送数字证书；

➢ 通过移动端安全软件（安全SDK）与安全认证网关建立SSL安全加密信道；

➢ 通过安全加密信道完成用户身份认证和传输数据加解密及访问控制等功能。

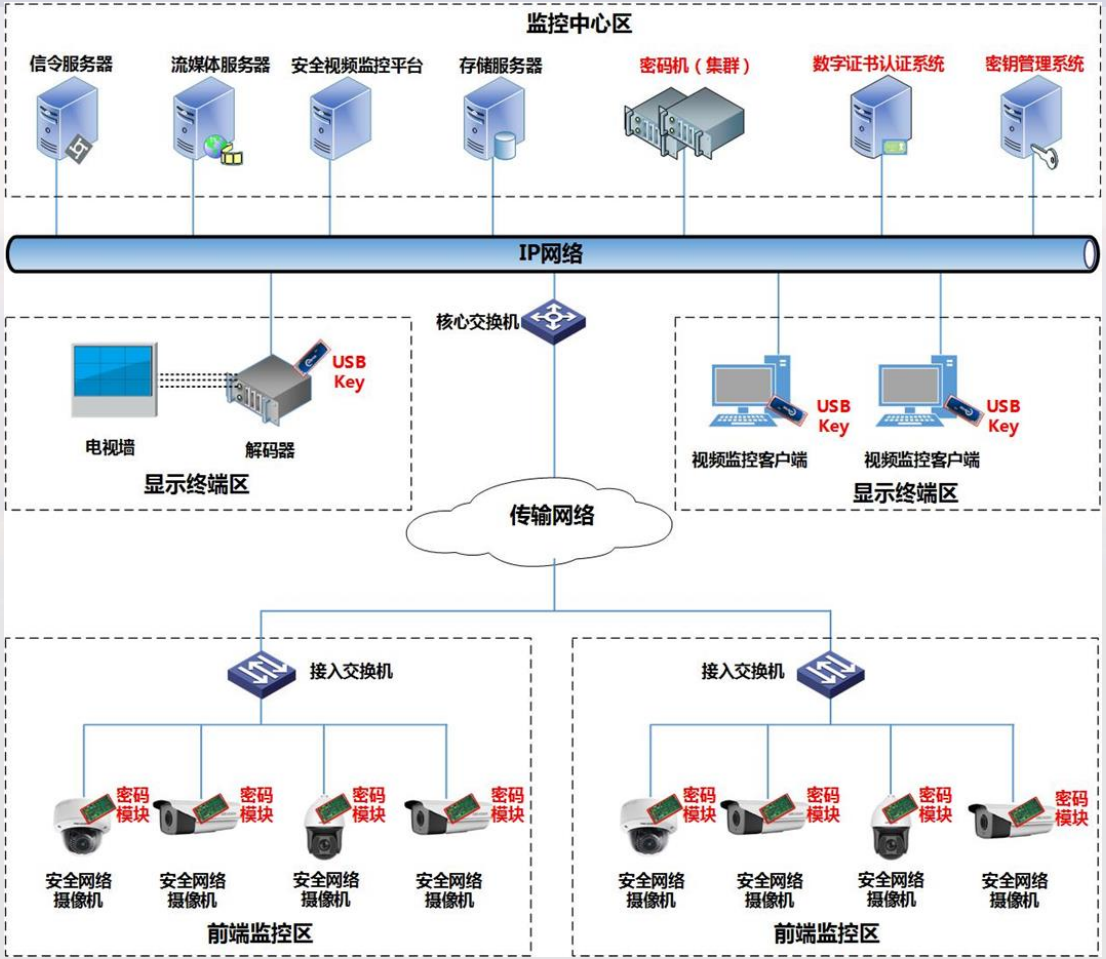
移动办公场景-密码应用部署图

视频监控场景-视频改造方案概述

通过提供一整套包含安全功能在内的完整的视频监控系统的方式，实现视频监控系统安全合规。方案全面符合GB/T 35114等相关标准要求。

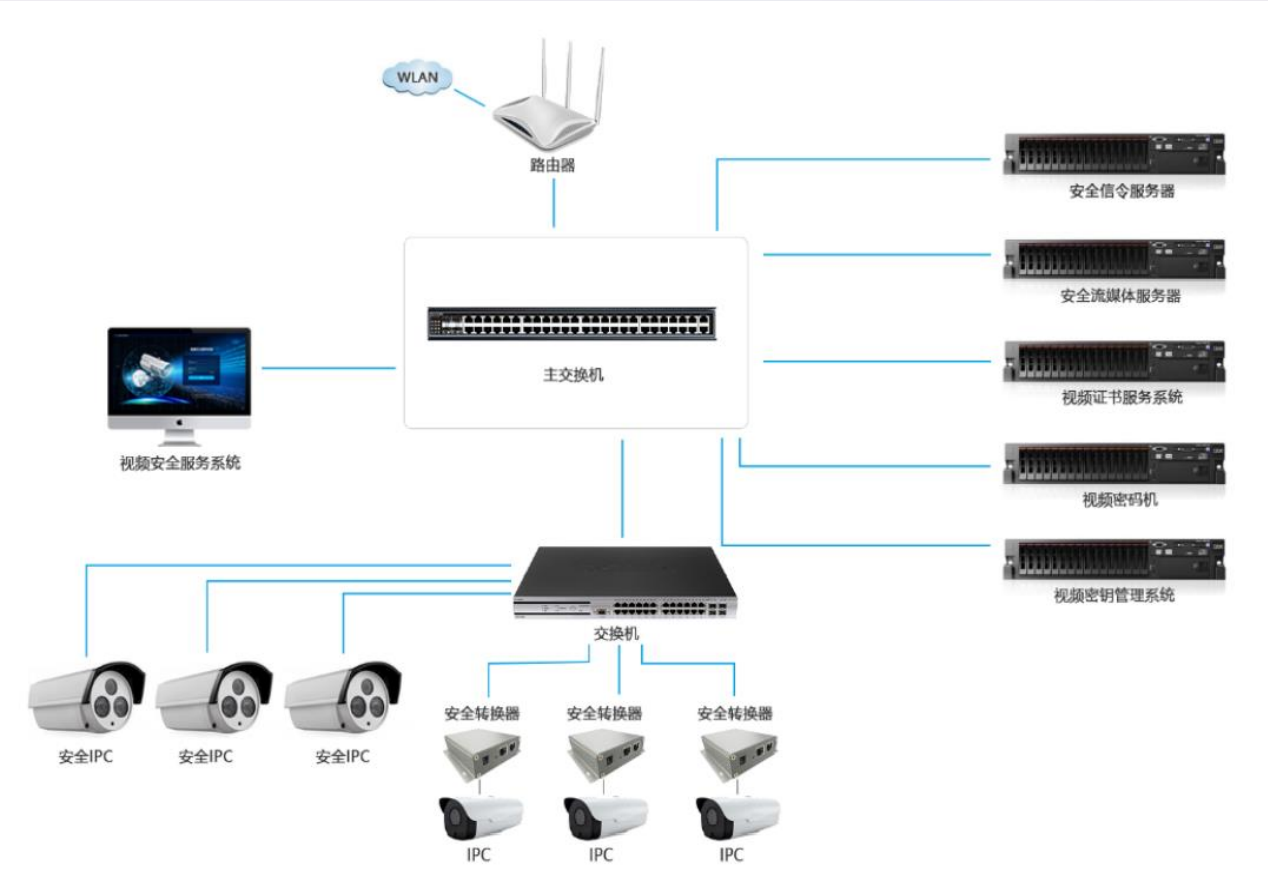
在已建成的视频监控系统的基础上，通过额外部署相关密码产品，重点保障摄像头与视频监控业务系统之间的身份认证及视频通信传输加密，满足部分GB/T 35114标准要求，其他部分还需视频监控系统应用自身进行改造。

视频监控场景-新建视频监控方案



- 前端监控区
  - 集成密码模块的安全网络枪型/半球/筒型/球型摄像机
- 监控中心区
  - 信令服务器、流媒体服务器、安全视频监控平台
  - **密码机（集群）**
  - **密钥管理系统**
  - **数字证书认证系统**
  - 存储服务器
- 显示终端区
  - 电视墙+解码器（含USBKey）
  - 视频监控客户端（含USBKey）

视频监控场景-已建视频改造方案



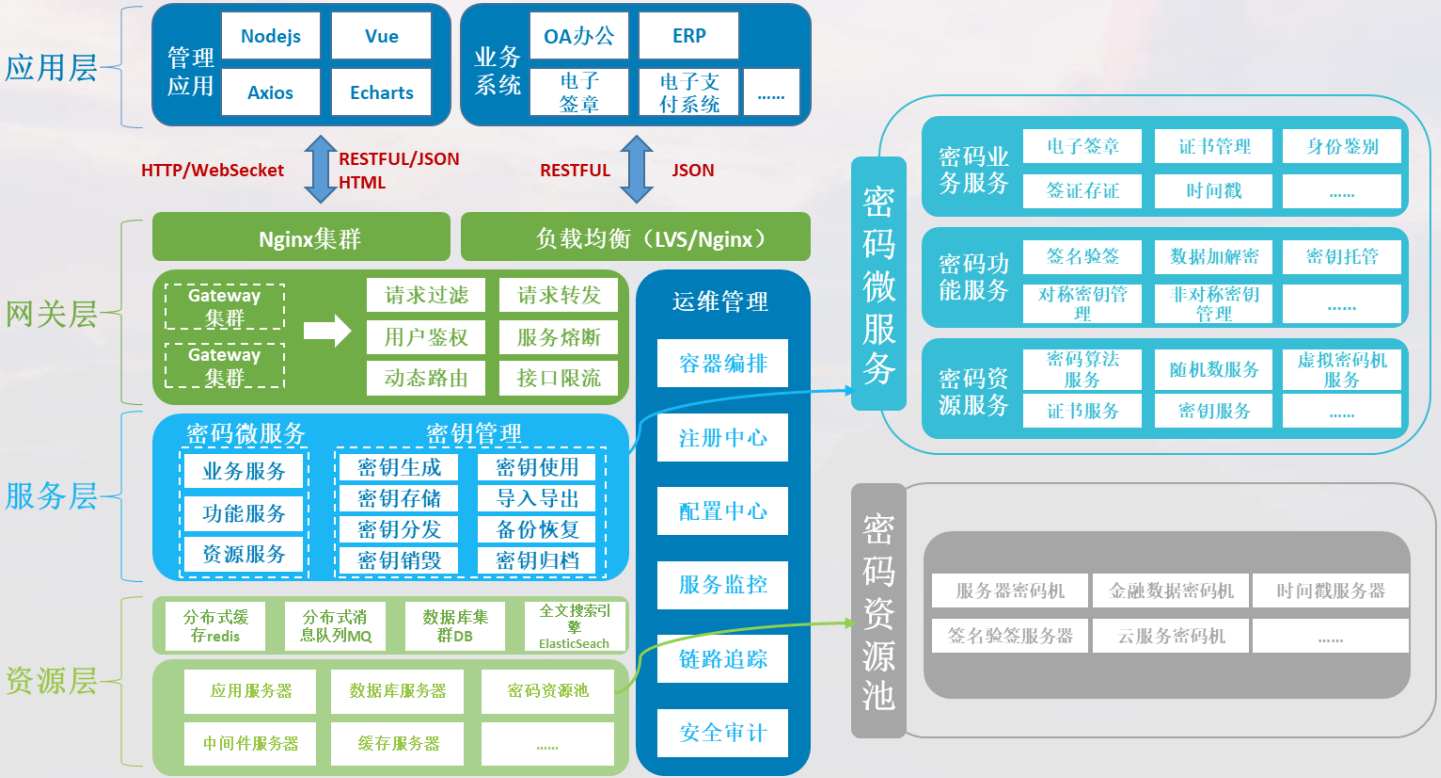
- 视频监控安全解决方案从产品架构上可分为三部分，分别是**前端安全设备、视频安全服务系统、视频安全密码服务支撑平台**。前端安全设备为安全转换器。视频安全密码服务支撑平台包括安全信令服务器、安全流媒体服务器、视频证书服务系统、视频密码机、视频密钥管理系统。
- 系统以国产商用密码算法为基础，利用公钥基础设施以及安全芯片、智能密码钥匙、密码机、密钥管理系统等密码运算、管理设备，可以实现视频监控联网系统内各类设备、平台、用户的统一身份认证信令完整性验证等安全防护功能。

04 密码相关产品简介

常见密码产品、服务简介

重点密码类产品介绍

- 统一密码服务平台

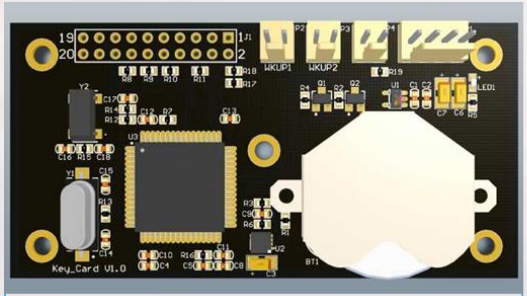


- 功能特点

- 高度集成化的一站式服务平台，基于统一的服务接口为信息系统提供密码服务
- 整合全部密码资源，形成密码资源池降低建设成本
- 对密码资源进行统一监管，便于统一维护

重点密码类产品介绍

- 定制化的密码板卡/模组

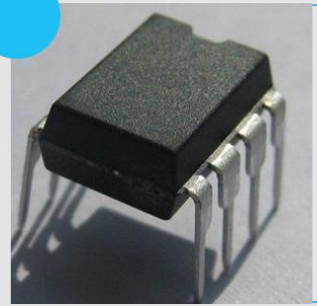


低功耗密钥服务板

家庭互联网安全网关

网络加密模块，FPGA及高速并行密码运算。

带国密算法传感器节点，SM1-2-3和ZUC接入，图为气体传感器



国密算法支持，SPI、UART等不同嵌入式接口支持，应用于智能传感器

其他密码产品简介

序号	产品名称	功能简介
1	国密门禁系统	符合GM/T 0036-2014标准，提供人员的身份鉴别和出入记录的完整性保护
2	国密浏览器	国密浏览器与SSL VPN建立SLL加密信道
3	密码机（服务器密码机/金融数据密码机/签名验签服务器）	提供密码运算及密钥保护能力
4	密码卡	提供密码运算能力及基本密钥保护能力
5	VPN网关	提供通信链路双向的数据加密和身份认证保证通信链路的安全性
6	密钥管理系统	为用户业务系统提供各种密钥的生成、存储、导出、恢复、更新、销毁等全周期管理
7	PKI/CA系统	为用户提供数字证书申请、审核、签发、发布、注销、更新、下载等全生命周期管理
8	时间戳服务器	为用户的电子数据签发权威可信时间戳
9	电子签章系统	利用图像处理技术将电子签名操作转化保障电子信息的真实性和完整性以及签名人的不可否认性
10	物联网安全接入网关	实现物联网系统网络边界安全防护，具有网络隔离、数据加密、身份认证等功能
11	桌面型加密认证装置	具有数据加密、身份认证、协议识别及过滤等功能
12	物联网边缘计算安全装置	支持身份认证、数据加解密、网络隔离等功能，基于可信操作系统的数据采集、分析
13	协同签名系统	提供移动端手机证书的协同密钥运算，实现移动手机证书的身份鉴别
14	APP加固系统	对APP应用的每个文件分配唯一识别指纹，程序执行时进行签名验签，完成可执行程序的完整性保护

谢谢大家

安天冬训营 wtc.antiy.cn