密码应用方案编制和实施

主讲人：胡双喜

天津市商用密码行业协会

目录

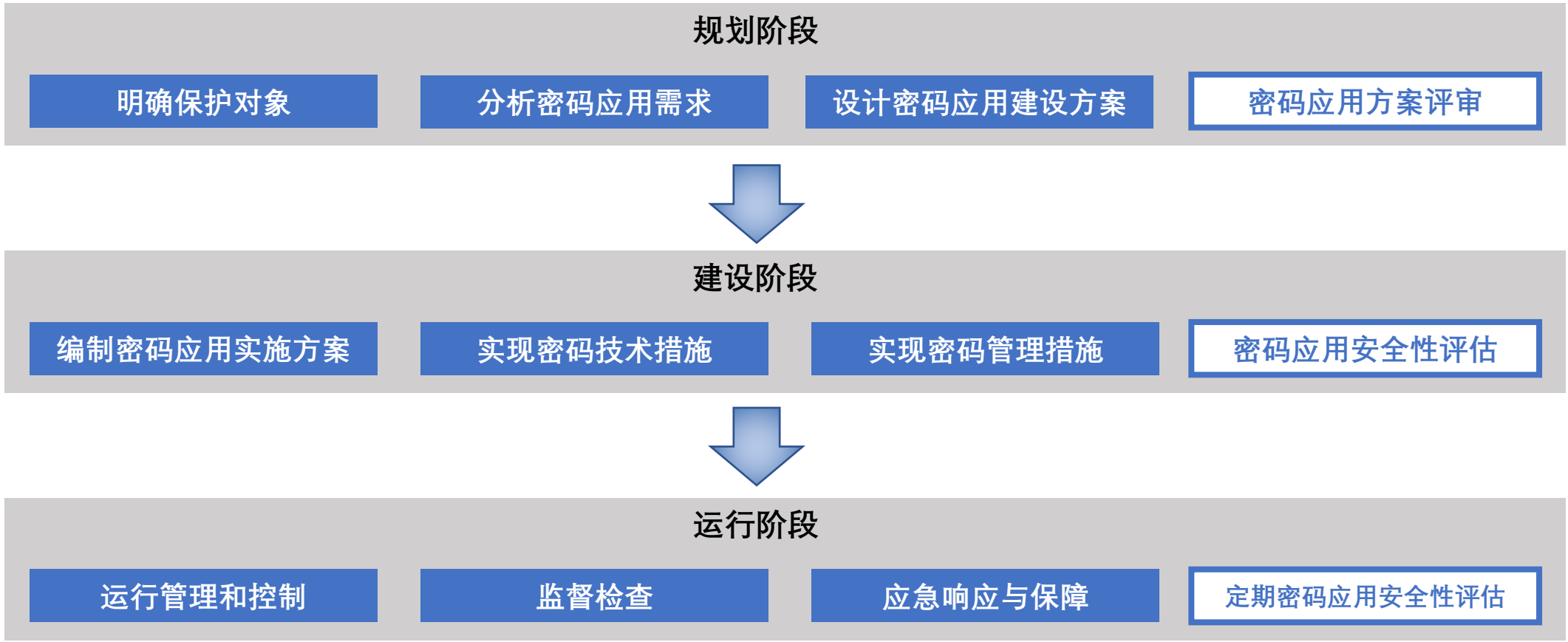
CONTENTS

密码应用系统建设

PART. 01

密码保障系统建设的总体思路

“三同步，一评估”原则：项目建设单位应当同步规划、同步建设、同步运行密码保障系统并定期进行评估



不同角色的职责分工

厂商和集成单位

编写方案、建设实施
配合密评、运行维护

测评单位

密码应用方案评估、
密码应用安全性评估

主管单位

完成方案合规性审核
完成密评报告备案
完成密评后监督检查

三者角色法律规定不可重叠

规划阶段的核心是密码应用方案的编制与评审

- 核心输出——符合业务需求和业务特点的“密码应用方案”（必备项）

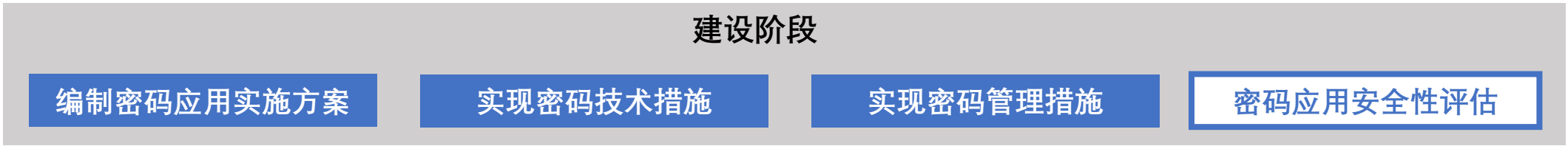
  是密码方案建设的前提和基础（新建系统和已建系统都需具备）

◆ 脱离业务特点谈论密码应用建设方案、对照密评指标逐项罗列密码产品，可能导致的后果是：

◆ 方案无法落地（例如：业务系统网络通道为单向传输，方案要求架设VPN安全通道）

◆ 方案重复建设（例如：用户原有密码机给业务系统调用，方案要求再采购密码机与日志服务器对接，保护设备日志完整性）

建设阶段的核心是密码技术、管理措施的实现



技术措施的实现通常包括：

- 密码产品或服务的采购
- 密码功能的开发
- 密码应用的集成

管理措施的实现通常包括：

- 密码管理制度的建设和修订
- 密码管理机构和人员的设置
- 建设过程管理

密码保障系统的建设是否合规、正确、有效，最终由“密码应用安全性评估”决定

运行阶段的核心是运营、监管和定期评估

运行阶段

运行管理和控制 | 监督检查 | 应急响应与保障 | 定期密码应用安全性评估

- 密码保障系统的正确运行直接关系到安全防护效果，需要系统运营方、监管方、测评方充分合作

系统监管方

□ 按照国家、行业相关密码应用监督检查要求及标准对密码应用活动开展监督检查工作

系统测评方

□ 定期开展商用密码应用安全性评估，确保信息系统的密码应用措施符合相应的安全要求

系统运营方

□ 按照职责划分和规章制度，正确执行运行管理和控制
□ 正确执行应急响应制度的要求，进行应急响应处理
□ 监测密码保障系统的运行状况
□ 定期实施安全自查

密码应用方案模板结构

■ 信息系统密码应用方案模板

- ① 背景
- ② 系统概述
- ③ 密码应用需求分析
- ④ 设计目标及原则
- ⑤ 密码应用方案
- ⑥ 安全管理方案
- ⑦ 实施保障方案
- ⑧ 密码应用建设投资概算

■ 系统概述
- ✓ 系统调研分析

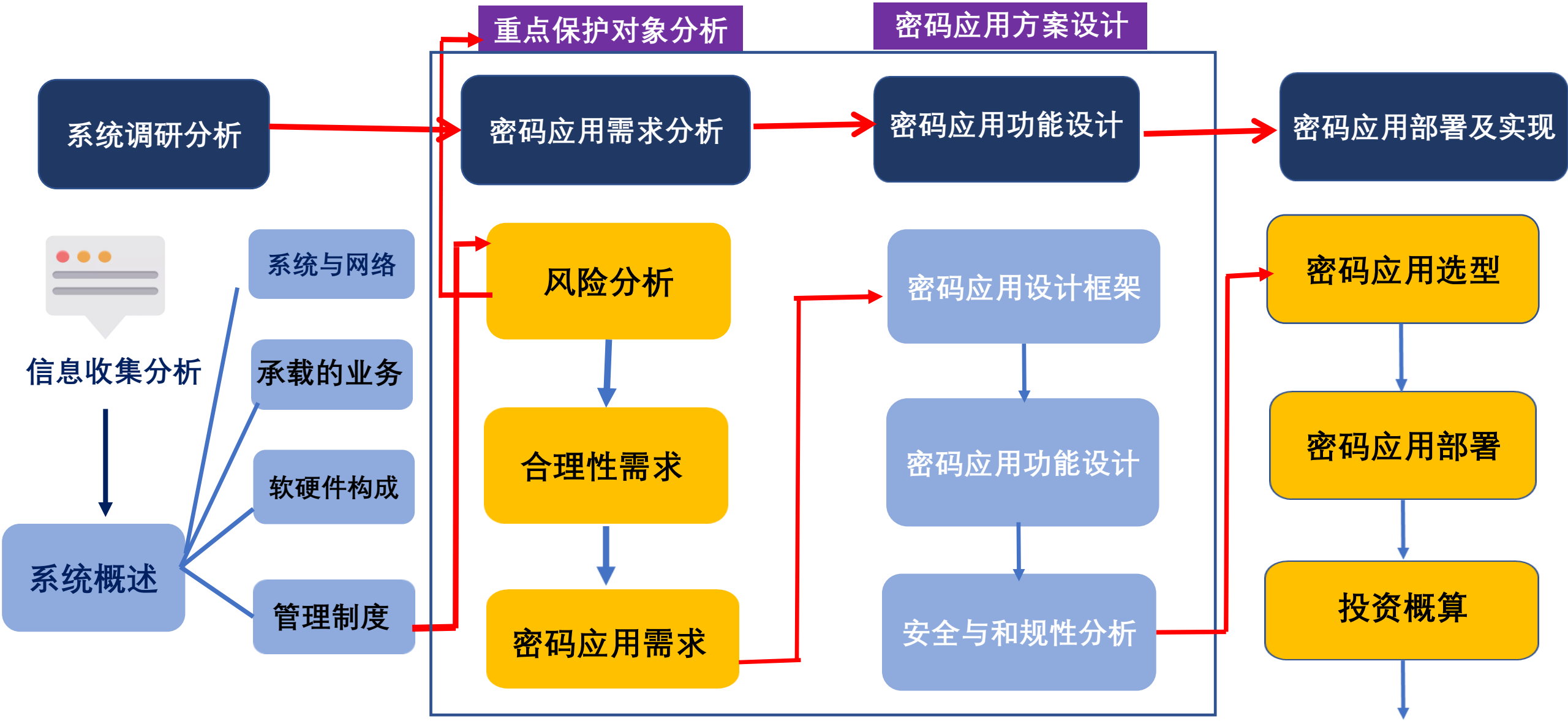
■ 密码应用需求分析
- ✓ 安全风险分析（重点保护对象分析）
- ✓ 密码应用需求

■ 密码应用设计
- ✓ 密码应用技术框架
- ✓ 密码应用功能设计
- ✓ 密码应用部署及实现
- ✓ 安全与合规性分析

■ 投资概算

目 录

密码应用方案设计流程


重点保护对象分析
密码应用方案设计
系统调研分析
密码应用需求分析
密码应用功能设计
密码应用部署及实现
信息收集分析
系统与网络
承载的业务
软硬件构成
管理制度
系统概述
风险分析
合理性需求
密码应用需求
密码应用设计框架
密码应用功能设计
安全与和规性分析
密码应用选型
密码应用部署
投资概算

应用系统调研分析

PART. 02

1 系统调研分析

■ 系统网络拓扑

- ✓ 体系架构：传统IT架构、云计算、…
- ✓ 网络所在**机房**情况：本地、运营商云机房、…
- ✓ 网络边界划分：**网络接入及其网络类型**
- ✓ 设备组成及实现功能：系统分区及其功能
- ✓ 所采取的**安全防护措施**：电子门禁系统、视频监控系统
- ✓ 给出系统网络拓扑图

分类	信息调研
物理和环境	**本地机房情况**；本地，IDC机房，运营商云机房，…；电子门禁系统、视频监控系统
网络和通信	**网络类型**：互联网、政务外网、专线…… **网络接入**：互联网访问应用系统通信信道，政务外网远程运维通信信道，…
设备和计算	
应用和数据	

1 系统调研分析

■ 承载的业务

✓ 承载的业务情况包含系统承载的**业务应用**、业务功能、信息种类、**关键数据**类型等。

■ 软硬件构成

✓ 包含**服务器**、用户终端、网络设备、存储、安全防护设备、**密码设备**等硬件资源和**操作系统**、**数据库**、应用中间件等软件设备资源。

分类	信息调研
物理和环境	**本地机房情况**；本地，IDC机房，运营商云机房，…；电子门禁系统、视频监控系统
网络和通信	**网络类型**：互联网、政务外网、专线…… **网络接入**：互联网访问应用系统通信信道，政务外网远程运维通信信道，…
设备和计算	信息系统中的设备，包括**服务器**、**密码设备** **操作系统**、**数据库**、**堡垒机**……
应用和数据	**业务应用**、**关键数据**、……

1 系统调研分析

- 配合梳理资产和网络非常必要
- 如果经费有限哪些可以考虑利旧

物理和环境安全：门禁系统部分设备、视频监控部分设备

其他层面安全：VPN安全网关、服务器密码机等密码设备

是否配置问题（合理、正确、有效使用）

设备是否过期（看采购设备时候是否证书有效期内）

- 国家鼓励使用密码技术

重点保护对象分析

PART. 03

2 重点保护对象分析

■ 物理和环境安全

- ✓ 本地机房情况；本地，IDC机房，运营商云机房，…；电子门禁系统、视频监控系统

■ 网络和通信安全

- ✓ 网络类型：互联网、政务外网、……
- ✓ 网络接入：互联网访问应用系统通信信道，政务外网远程运维通信信道，…

■ 设备和计算安全

- ✓ 信息系统中的设备，包括服务器、密码设备、操作系统、数据库、……

分类	重点保护对象
物理和环境	机房电子门禁系统及其数据、机房视频监控数据
网络和通信	互联网访问应用系统通信信道、政务外网访问应用通信信道、远程运维通信信道、数据灾备通信信道 通信双方、通信数据、网络边界访问控制
设备和计算	服务器、数据库、堡垒机、密码设备、重要可执行程序和文件

2 重点保护对象分析

■ 应用和数据安全

✓ 业务应用、关键数据、……

① 梳理用户类型

✓ 互联网用户、政务外网用户、管理员用户、……

✓ 不包括设备运维的管理员

② 梳理重要数据

✓ 鉴别数据：用户名/口令、证书

✓ 关键业务数据：例如电子公文

✓ 其他重要数据：访问控制信息、审计日志

分类	重点保护对象
应用和数据	1. **应用用户**：互联网用户、政务外网用户、管理员用户等的真实性 2. **重要数据**：鉴别数据、关键业务数据、访问控制信息、重要审计日志 3. **操作行为**：原发或接收行为的不可否认性

③ 重要操作行为

✓ 原发行为的不可否认性：例如，电子公文加盖电子印章

✓ 接受行为的不可否认性：客户取款数字签名

2 重点保护对象分析

■ 重点保护对象

- ✓ 需要分析准确，避免后续增项或是重来
- ✓ 选取必须的以及最合适的保护对象进行安全防护

■ 合理提供建议

- ✓ **哪些为不适用项（根据项目实际灵活考虑）**

  比如：托管到IDC机房；无远程运维；纯局域网环境；无敏感标记；无需不可否认性等

- ✓ **哪些风险较低，可以在合理经费情况下分布实施改造**

  比如：哪些分值高；哪些风险低；哪些改造代价小；哪些是必须的

- ✓ **哪些是高风险项，提供合理建议**

  根据密评等级确定高风险项，确定是否能够关闭或是缓解

2 重点保护对象分析

指标要求		一级	二级	三级	四级
物理和环境安全	身份鉴别 ★	可	宜	宜	应
	电子门禁记录数据存储完整性	可	可	宜	应
	视频监控记录数据存储完整性	--	--	宜	应
	密码产品	--	一	二	三
	密码服务	应	应	应	应
网络和通信安全	身份鉴别 ★	可	宜	应	应
	通信数据完整性	可	可	宜	应
	通信过程中重要数据机密性 ★	可	宜	应	应
	网络边界访问控制信息完整性	可	可	宜	应
	安全接入认证 ★	--	--	可	宜
	密码产品	--	一	二	三
	密码服务	应	应	应	应
设备和计算安全	身份鉴别 ★	可	宜	应	应
	远程管理通道安全 ★	--	--	应	应
	系统资源访问控制信息完整性	可	可	宜	应
	重要信息资源安全标记完整性	--	--	宜	应
	日志记录完整性	可	可	宜	应
	重要程序或文件完整性	--	--	宜	应
	密码产品	--	一	二	三
	密码服务	应	应	应	应
应用和数据安全	身份鉴别 ★	可	宜	应	应
	访问控制	可	可	宜	应
	重要信息资源安全标记完整性	--	--	宜	应
	重要数据传输机密性 ★	可	宜	应	应
	重要数据存储机密性 ★	可	宜	应	应
	重要数据传输完整性	可	宜	宜	应
	重要数据存储完整性 ★	可	宜	宜	应
	不可否认性 ★	可	可	宜	应
	密码产品	--	一	二	三
	密码服务	应	应	应	应

指标要求		一级	二级	三级	四级
管理制度	具备密码应用安全管理制度 ★	应	应	应	应
	密钥管理规则	应	应	应	应
	建立操作规程	--	应	应	应
	定期修订安全管理制度	--	--	应	应
	明确管理制度发布流程	--	--	应	应
	制度执行过程记录留存	--	--	应	应
人员管理	了解并遵守密码相关法律法规和密码管理制度	应	应	应	应
	建立密码应用岗位责任制度	--	应	应	应
	建立上岗人员培训制度	--	应	应	应
	定期进行安全岗位人员考核	--	--	应	应
	建立关键岗位人员保密制度和调离制度	应	应	应	应
建设运行	制定密码应用方案 ★	应	应	应	应
	制定密钥安全管理策略	应	应	应	应
	制定实施方案	应	应	应	应
	投入运行前进行密码应用安全性评估	可	宜	应	应
	定期开展密码应用安全性评估及攻防对抗演习	--	--	应	应
应急处置	应急预案	可	应	应	应
	事件处置	--	--	应	应
	向有关主管部门上报处置情况	--	--	应	应

密码应用方案设计

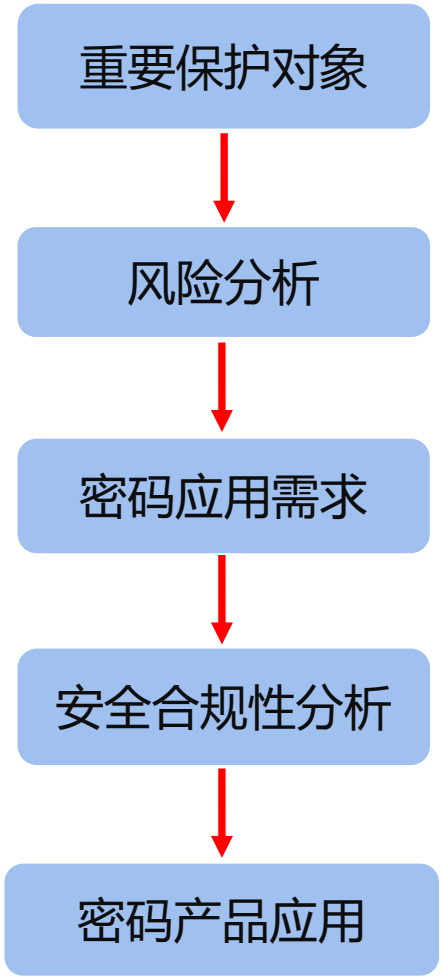
PART. 04

密码应用方案设计

PART. 01

物理和环境安全

设计流程



物理和环境			
	1风险分析	2密码应用需求	
	使用ID/IC卡/生物特征身份鉴别 — 存在非授权人员进入物理环境风险	确定进入机房人员的真实性，	
	进出机房记录未使用密码技术进行保护 — 存在数据非授权篡改的风险	保护电子门禁系统进入记录的完整性，防止被非授权篡改	
	视频监控音像数据未使用密码技术进行保护 — 存在数据非篡改的风险	保护视频监控音像记录完整性，防止被非授权篡改	
	3密码应用方案设计	4安全合规性分析	5密码产品应用
	部署合规的电子门禁系统，实现对人员的身份鉴别	电子门禁系统有认证证书，符合GM/T0028-2014二级要求•GM/T0036-2014技术要求	国密门禁系统
	使用HMAC-SM3技术对电子门禁系统进出记录数据进行完整性保护	电子门禁系统有认证证书，符合GM/T0028-2014二级要求和HMAC计算要求	门禁进出记录完整性模块
	使用HMAC-SM3技术视频监控音像数据进行完整性保护	安全音视频系统有认证证书，符合GM/T0028-2014二级要求和HMAC要求	视频监控记录完整性模块

3.1 物理和环境安全

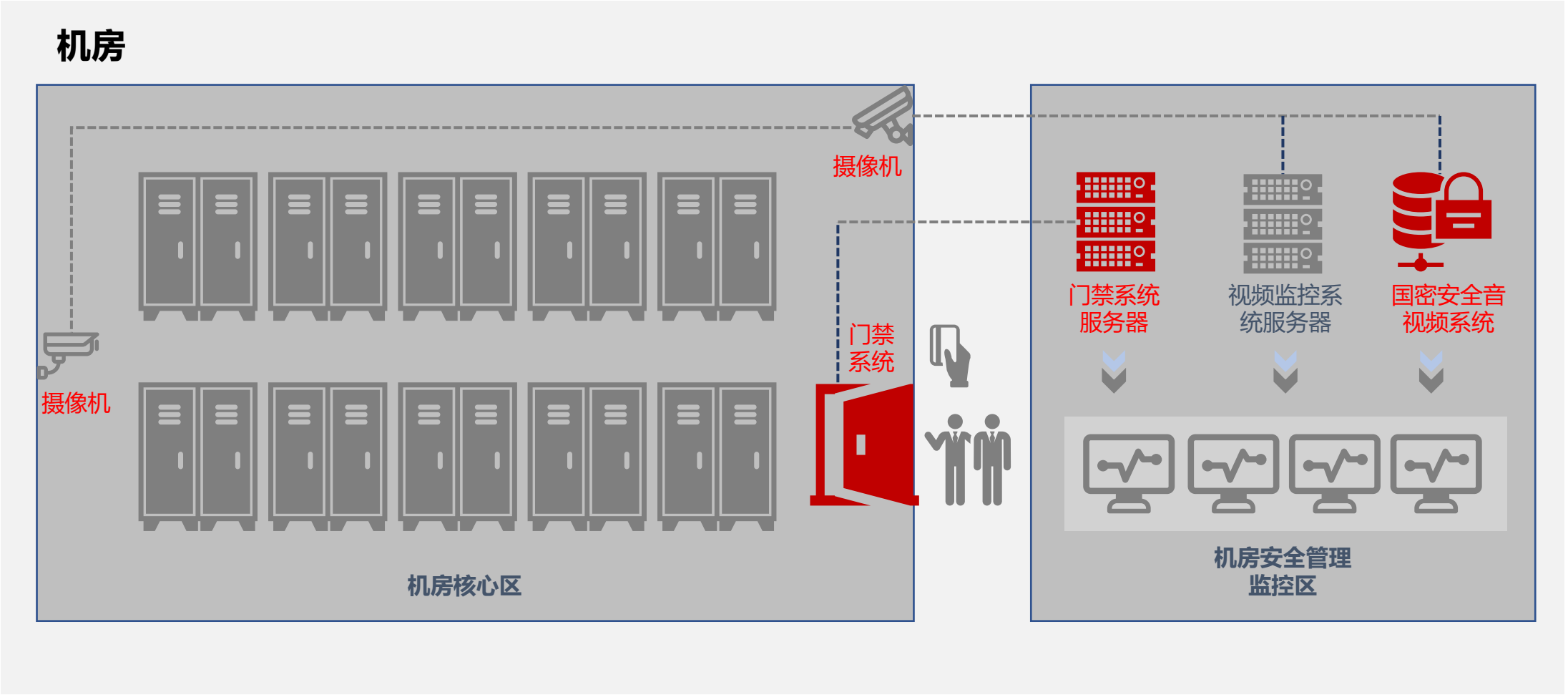
- **重要保护对象**
  - ✓ 机房电子门禁系统及其数据、机房视频监控数据
- **安全风险分析**
  - ✓ **电子门禁系统**使用**ID/IC卡/生物特征进行身份鉴别**，存在**非授权人员**进入物理环境的**风险**
  - ✓ **机房进出记录、视频监控数据未使用密码技术**进行完整性保护，存在数据**非授权篡改**的**风险**
- **密码应用需求**
  - ✓ 确认进入机房**人员身份的真实性**，**防止假冒人员进入**
  - ✓ 保护**机房进出记录的完整性**，**防止被非授权篡改**
  - ✓ 保护**视频监控影像数据的完整性**，**防止被非授权篡改**

3.1 物理和环境安全

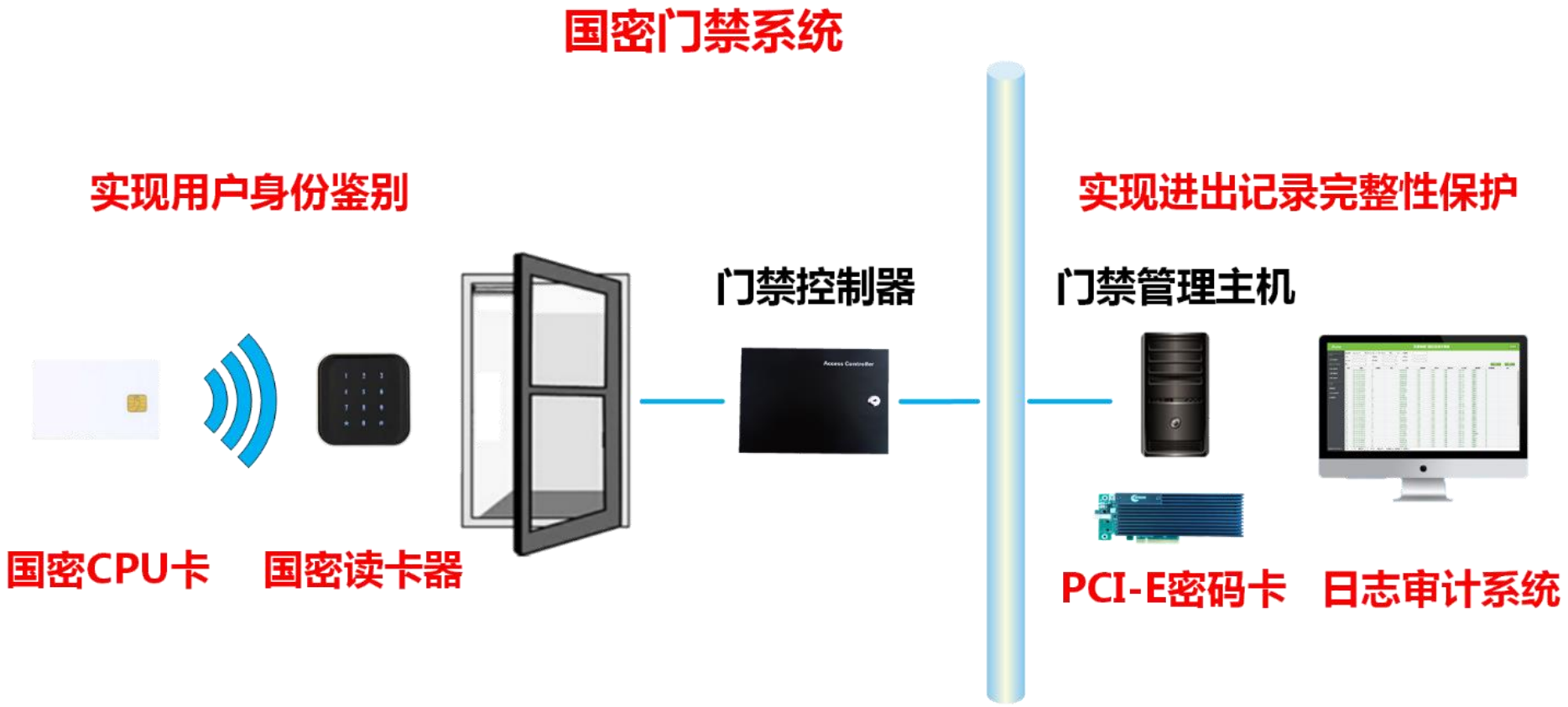
- **密码产品和技术**
  - ✓ 进出机房发身份鉴别：**电子门禁系统；**符合GM/T 0036-2014
  - ✓ 机房进出记录、视频监控影像数据：**安全音视频系统**；**HMAC-SM3技术**；
  - ✓ 密码模块符合**GM/T 0028-2014二级**要求
- **安全与合规性分析**
  - ✓ 身份鉴别：符合
  - ✓ 机房进出记录、视频监控影像数据的完整性：符合

网络和通信安全	测评对象	密码应用方案设计	量化指标			
			D	A	K	符合性
身份鉴别	电子门禁系统	部署合规的电子门禁系统，实现对人员的身份鉴别	√	√	√	符合
电子门禁记录数据完整性	电子门禁记录数据	使用HMAC-SM3密码技术和功能对物理机房进出记录数据进行完 整性保护	√	√	√	符合
视频记录数据完整性	视频音像记录数据	使用音视频加密系统的HMAC-SM3密码功能对视频监控音像数据进行完整性 保护	√	√	√	符合

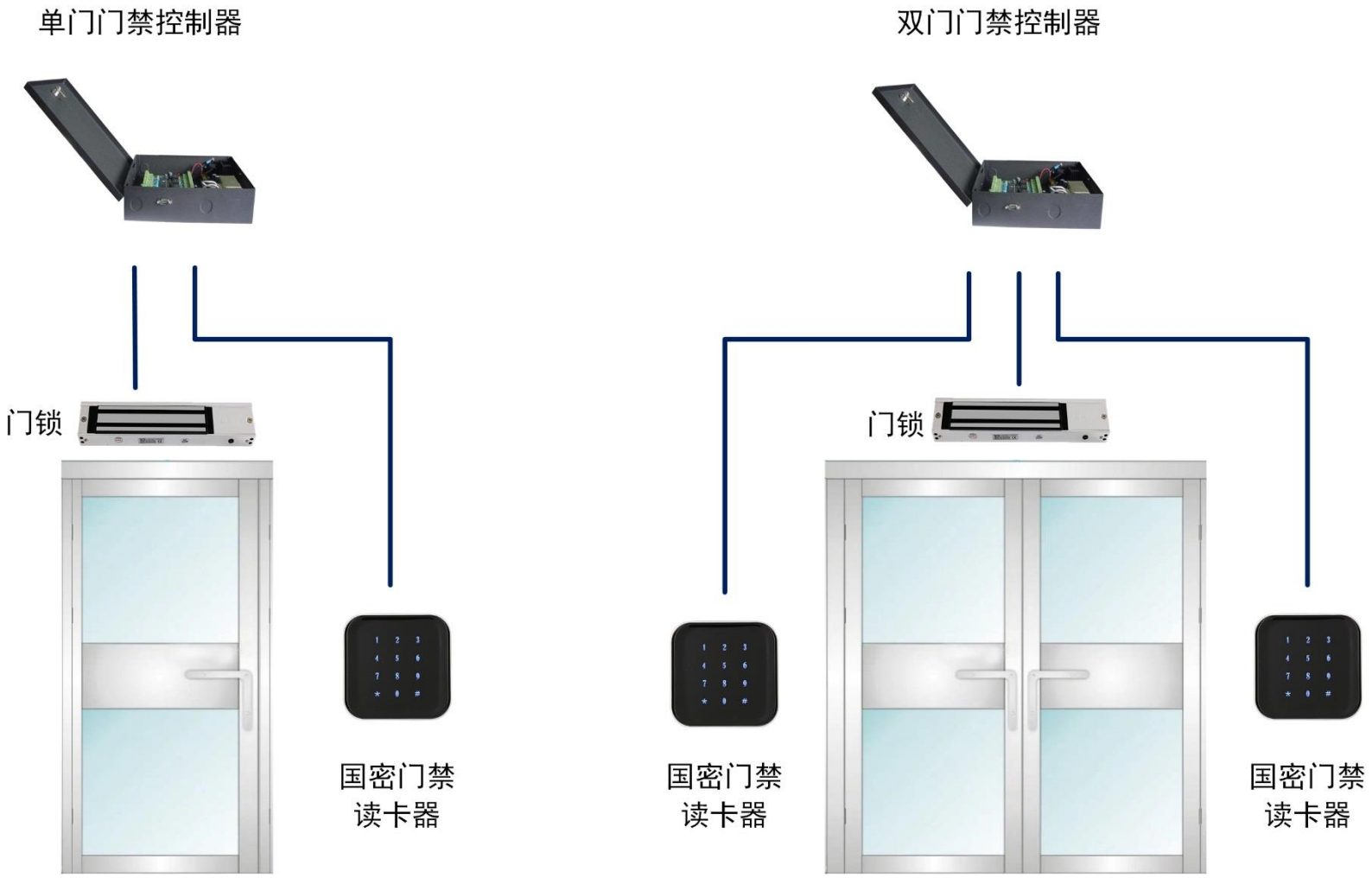
3.1 物理和环境安全


机房
摄像机
摄像机
门禁
系统
机房核心区
门禁系统
服务器
视频监控系
统服务器
国密安全音
视频系统
机房安全管理
监控区

国密门禁系统改造


国密门禁系统
实现用户身份鉴别
门禁控制器
实现进出记录完整性保护
门禁管理主机
国密CPU卡
国密读卡器
PCI-E密码卡
日志审计系统

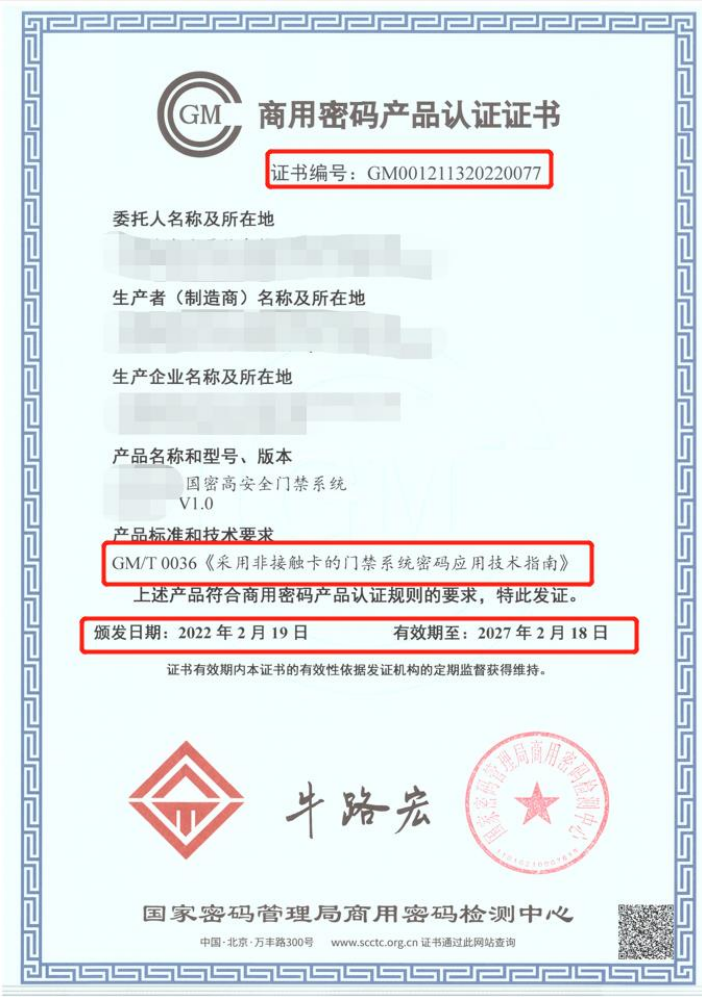
门禁改造利旧配置



国密监控系统改造配置

密码证书相关要求

齐套、合规、有效



商用密码产品认证证书

证书编号：GM001211320220077

委托人名称及所在地

生产者（制造商）名称及所在地

生产企业名称及所在地

产品名称和型号、版本

国密高安全门禁系统
V1.0

产品标准和技术要求

GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》

上述产品符合商用密码产品认证规则的要求，特此发证。

颁发日期：2022 年 2 月 19 日　　有效期至：2027 年 2 月 18 日

证书有效期内本证书的有效性依据发证机构的定期监督获得维持。

牛路宏

国家密码管理局商用密码检测中心

中国·北京·万丰路300号　www.scctc.org.cn 证书通过此网站查询

门禁系统

商用密码产品认证证书

证书编号：GM001210220230476

委托人名称及所在地

生产者（制造商）名称及所在地

生产企业名称及所在地

产品名称和型号、版本

智能 IC 卡
C-01 V1.0

产品标准和技术要求

GM/T 0041《智能 IC 卡密码检测规范》
GM/T 0028《密码模块安全技术要求》第二级要求

上述产品符合商用密码产品认证规则的要求，特此发证。

颁发日期：2023 年 5 月 29 日　　有效期至：2028 年 5 月 28 日

证书有效期内本证书的有效性依据发证机构的定期监督获得维持。

牛路宏

国家密码管理局商用密码检测中心

中国·北京·万丰路300号　www.scctc.org.cn 证书通过此网站查询

配件：CPU卡

商用密码产品认证证书

证书编号：GM001212220230342

委托人名称及所在地

生产者（制造商）名称及所在地

生产企业名称及所在地

产品名称和型号、版本

读卡模块（密码模块）
CR-01　V1.0

产品标准和技术要求

GM/T 0028《密码模块安全技术要求》第二级要求

上述产品符合商用密码产品认证规则的要求，特此发证。

颁发日期：2023 年 4 月 27 日　　有效期至：2028 年 4 月 26 日

证书有效期内本证书的有效性依据发证机构的定期监督获得维持。

牛路宏

国家密码管理局商用密码检测中心

中国·北京·万丰路300号　www.scctc.org.cn 证书通过此网站查询

配件：读卡模块

密码应用方案设计

PART. 02

网络和通信安全

3.2 网络和通信安全

- **重要保护对象**
  - ✓ 互联网访问应用系统通信信道、政务外网访问应用通信信道、远程运维通信信道、数据灾备通信信道
- **安全风险分析**
  - ✓ **业务通信信道**和**远程运维通信信道**使用不合规的HTTPS协议通信，**数据灾备通信信道**未使用密码技术
  - ✓ 通信双方**身份被假冒**，通信数据在信息系统外部被**非授权截取**、**非授权篡改风险**
- **密码应用需求**
  - ✓ 确保互联网和政务外网用户访问网络接入区、运维人员访问统一管理区、业务服务区和数据灾备区交互时通信**实体身份的真实性**，**防止与假冒实体进行通信**
  - ✓ 保护通信过程中业务数据、运维数据、灾备**数据的完整性**和**机密性**，**防止数据被非授权篡改**，**防止敏感数据泄露**
  - ✓ 保护互联网和政务外网用户访问网络接入区、管理员访问统一管理区、业务服务区和数据灾备区交互的网络边界设备中**访问控制信息的完整性**，**防止被非授权篡改**

3.2 网络和通信安全

- **密码产品和技术**
  - ✓ 互联网访问应用系统通信信道、政务外网访问应用通信信道：**安全认证网关**、**安全浏览器**；**HTTPS通信**
  - ✓ 数据灾备通信信道：**IPSec VPN**；**IPSec通信**
- **安全与合规性分析**
  - ✓ 身份鉴别：符合
  - ✓ 通信数据机密性、通信数据完整性：符合
  - ✓ 网络边界访问控制信息完整性：符合

网络和通信安全	测评对象	密码应用方案设计	量化指标			
			D	A	K	符合性
身份鉴别	通信信道通信双方（可单向）	使用数字证书进行身份鉴别，业务站点证书由合规的CA机构签发；通信信道使用SSL VPN和IPSec VPN保护，（GB/T 36968-2018《信息安全技术 IPSec VPN技术规范》、GM/T 0025-2014《SSL VPN网关产品规范》、GM/T 0026-2014《安全认证网关产品规范》）	√	√	√	符合
通信数据机密性、完整性	所有通信信道，包括业务信道、运维信道、数据灾备信道		√	√	√	符合
网络边界访问控制信息完整性	所有通信信道的网络边界信息	合规密码产品（安全认证网关、IPSec VPN）的自身安全机制实现	√	√	√	符合

3.2 网络和通信安全


用户侧
网络边界
运维或业务人员
国密浏览器
USB KEY
国密数字证书
互联网或运维网
防火墙
WAF
SSL VPN安全网关
云计算节点群
行政审批系统服务器
公文交换服务器
数据加密存储
网络办公系统
云服务器密码机
电子签章系统
签名验签服务器
协同签名系统
时间戳服务器
数字证书管理系统
密码应用支撑—密码资源池（密码服务平台）

网络和通信层面改造

改造方式

- ✓ VPN和浏览器设备合理部署、正确配置、有效应用就可以实现
- ✓ 移动端设备需要手机盾和SSL国密组件来实现

改造难点

- ✓ **移动端网络通信信道**
- ✓ **公众用户网络访问通道**
- ✓ **吞吐量巨大的网络通信信道**

产品名称	VPN安全网关(非信创)	VPN安全网关(信创)
IPSec密文吞吐率	15Gbps	800Mbps
IPSec最大隧道数	2500	300
IPSec每秒新建连接数	200	100
SSL密文吞吐率	7Gbps	550Mbps
SSL每秒新建连接数	1000	400
SSL最大并发连接数	20000	20000
SSL最大并发用户数	3000	2000

面向大规模公众服务只能使用SSL应用网关（反向代理模式）

网络和通信层面改造

	认证模式方案 （VPN网关采用认证模式）	反向代理方案 （VPN网关采用反向代理模式）
PC端	1）需要VPN网关与业务系统实现单点登录； 2）需要业务系统对接 UKey；	1）只需业务系统对接 UKey； 2）对接工作量较小；
移动端	1）需要VPN 客户端SDK与手机盾SDK整合，再提供给App厂商整合； 2）一个App/操作系统的**对接工作量较大；**	1）无需VPN厂商SDK； 2）一个App/操作系统的**对接工作量较小；**
对VPN网关厂商要求	**需要VPN网关厂商动用研发，**做大量技术支持	只需VPN网关配置成反向代理，**零技术支持**
结论	1）需要VPN网关厂商、业务系统开发商、手机盾厂商、UKey厂商做多家的应用对接； 2）**协调工作量较大；**	1）减少业务系统开发商的对接工作量，且基本上无需VPN网关厂商做技术支持； 2）可保证快速上线；

密码应用方案设计

PART. 03

设备和计算安全

3.3 设备和计算安全

- **重要保护对象**
  - ✓ 服务器、数据库、堡垒机、密码设备、重要可执行程序和文件
- **安全风险分析**
  - ✓ **服务器**、**数据库**、**堡垒机**采用基于**用户名/口令**的身份鉴别机制，并基于**HTTPS**（**密码技术不合规**）协议与堡垒机之间建立安全连接，存在设备被**非授权人员登录**、通信数据被**非授权截取**、**非授权篡改风险**
  - ✓ **重要可执行程序和文件未使用密码技术**进行**完整性**和**真实性保护**，使用或读取这些程序和文件时，未对其进行**完整性校验**，存在重要可执行程序或文件被**非授权篡改**、**来源不可信风险**
  - ✓ **服务器**、**数据库**、**堡垒机**等设备日志和访问控制信息均**明文存储**，**未使用密码技术**进行**完整性保护**，存在设备日志记录和访问控制信息**被非授权篡改风险**

3.3 设备和计算安全

密码应用需求

- ✓ 管理员通过远程运维管理终端访问**服务器**、**数据库**、**堡垒机**、**密码设备**时，对其**身份真实性**进行识别和确认，**防止假冒人员登录**
- ✓ 在远程运维管理时，对**运维管理通道**进行保护，**防止鉴别信息泄漏**
- ✓ 保护系统中**服务器**、**数据库**、**堡垒机**、**密码产品**等**设备日志**和**访问控制信息**的**完整性**，**防止被非授权篡改**
- ✓ 保护应用服务器等设备中**重要可执行程序**的**完整性**和**来源真实性**，**防止被非授权加载和篡改**

密码产品和技术

- ✓ 智能密码钥匙：**基于数字证书的身份鉴别**，GM/T 0027-2014《智能密码钥匙技术规范》
- ✓ 服务器密码机：**HMAC技术**，GM/T 0030-2014《服务器密码机技术规范》
- ✓ 密码模块符合**GM/T 0028-2014二级**要求

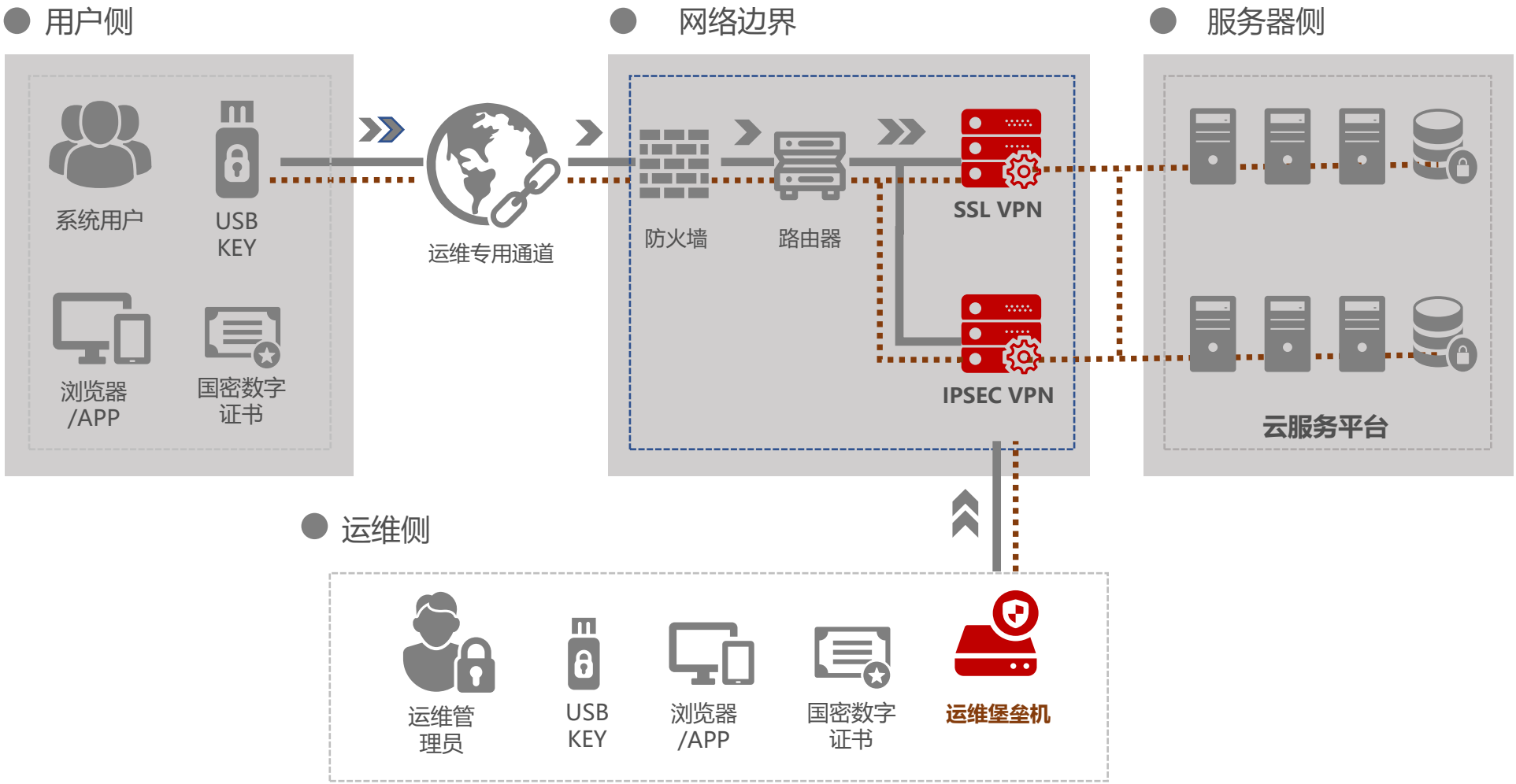
3.3 设备和计算安全

安全与合规性分析

- ✓ 身份鉴别、安全管理通道：部分符合
- ✓ 访问控制信息、日志记录的完整性：部分符合
- ✓ 重要可执行程序完整性、来源真实性：部分符合

设备和计算安全	测评对象	密码应用方案设计	量化指标			
			D	A	K	符合性
身份鉴别	服务器、数据库、堡垒机、密码设备	1．密码设备采用自带的智能密码钥匙实现身份鉴别； 2．堡垒机采用自带的智能密码钥匙实现身份鉴别； 3．服务器、数据库使用用户名/口令，通过国密堡垒机使用降风险	√ √ ×	√ √ ×	√ √ ×	部分符合
管理通道安全		使用不合规的SSH协议通信实现管理通道安全，通过国密堡垒机降风险	√	×	×	部分符合
访问控制信息完整性	服务器、数据库、堡垒机、密码设备	堡垒机、密码设备有认证证书，符合访问控制完整性要求 服务器、数据库设备暂时受限于技术原因，无法进行相关密码改造。	√ ×	√ ×	√ ×	部分符合
日志记录完整性		堡垒机、密码设备有认证证书，符合日志记录完整性要求 服务器、数据库设备暂时受限于技术原因，无法进行相关密码改造。	√ ×	√ ×	√ ×	部分符合
重要可执行程序完整性、来源真实性	重要可执行程序和文件	堡垒机、密码设备有认证证书，符合程序完整，来源真实要求 服务器、数据库设备暂时受限于技术原因，无法进行相关密码改造。	√ ×	√ ×	√ ×	部分符合

3.3 设备和计算安全


用户侧
网络边界
服务器侧
系统用户
USB KEY
浏览器 /APP
国密数字证书
运维专用通道
防火墙
路由器
SSL VPN
IPSEC VPN
云服务平台
运维侧
运维管理员
USB KEY
浏览器 /APP
国密数字证书
运维堡垒机

密码应用方案设计

PART. 04

应用和数据安全

3.4 应用和数据安全

- **重要保护对象**

1. 应用用户：互联网用户、政务外网用户、管理员用户等的真实性
2. 重要数据：鉴别数据、关键业务数据、访问控制信息、重要审计日志
3. 操作行为：原发或接收行为的不可否认性

- **安全风险分析**

✓ 互联网、政务外网用户均通过**用户名口令**进行登录，**未使用密码技术**进行身份鉴别，存在应用被**非授权人员登录风险**

✓ **未使用密码技术**对数据传输和存储进行**机密性**、**完整性保护**，存在重要数据**被窃取**和**非授权篡改风险**

✓ 访问控制信息、审计日志等重要数据均**明文存储**，**未使用密码技术**进行**完整性保护**，存在应用访问控制信息、审计日志数据被**非授权篡改风险**

✓ **未使用密码技术**对操作行为进行**不可否认性保护**，存在数据发送者或接收者**不承认**发送或接收到数据，或者**否认其操作行为**的**风险**

3.4 应用和数据安全

- **密码应用需求**
  - ✓ 确认应用系统**用户身份的真实性**，**防止假冒人员登录**
  - ✓ 对应用系统的**访问权限控制列表**、**审计数据**进行**完整性保护**，**防止被非授权篡改**
  - ✓ 保护政务外网、互联网客户端与服务端之间**传输和存储**的重要数据**机密性**和**完整性**，**防止数据泄露**、**被非授权篡改**
  - ✓ 保护系统中发送和接收**操作行为的不可否认性**，确保发送方和接收方对已经发生的**操作行为无法否认**
- **密码产品和技术**
  - ✓ 签名验签服务器、智能密码钥匙：**签名验签技术**，一起实现身份鉴别，签名验签服务器实现完整性密码功能
  - ✓ （云）服务器密码机：**加解密技术**、**HMAC技术**
  - ✓ 时间戳服务器、电子印章系统：**签名验签技术**，时间戳、电子印章一起实现不可否认性密码功能
  - ✓ 密码产品具有**商用密码产品认证证书（2级）**

3.4 应用和数据安全

安全与合规性分析

- ✓ 身份鉴别：符合或部分符合（根据实现方式）
- ✓ 访问控制信息：符合
- ✓ 重要数据的传输、存储：不符合、符合
- ✓ 不可否认性：符合

应用和数据安全	测评对象	密码应用方案设计	量化指标			
			D	A	K	符合性
身份鉴别	互联网用户、政务外网用户、管理员用户等	1.部署签名验签服务器、智能密码钥匙实现身份鉴别 2.通过身份认证网关与智能密码钥匙实现身份鉴别（看实现情况）	√ -	√ -	√ -	符合 部分符合
访问控制信息完整性	业务应用访问控制信息	部署签名验签服务器，使用数字签名验签技术对系统应用用户访问权限控制列表进行完整性保护	√	√	√	符合
重要数据传输	鉴别数据、关键业务数据	未使用密码技术，实现重要数据传输的安全保护；通过网络层弥补	-	-	-	不符合
重要数据存储	鉴别数据、关键业务数据、重要审计日志	部署服务器密码机或是数据库加密系统，使用加解密技术（SM4）和HMAC-SM3实现重要数 据的机密性和完整性保护	√	√	√	符合
不可否认性	原发或接收行为的不可否认性	部署电子签章系统、时间戳服务器，使用密码技术对系统重要操作行为数据进行签名，并加盖时间戳，实现操作行为的不可否认性	√	√	√	符合

3.4 应用和数据安全

- 密码技术保护的【重要数据】梳理，最终形成重要数据列表和数据分级

影响范围 影响程度	轻微	普通	严重
个人	公开	一般	重要
机构、组织（业务）	公开	一般	重要
国家、社会、公众	一般	重要	非商密范围

公开

网站公开信息、已公开发布的标准、政策、指导文件等

一般

一般业务信息，不敏感的个人信息（如角色、职务等）

重要

重要业务信息，敏感个人信息（如身份证号、联系方式等）

- 业务底稿、原始记录、日志记录——侧重完整性保护
- 业务结论、重要产出——机密性+完整性保护
- 敏感个人信息——侧重机密性保护

类似采集的音视频类文件建议进行完整性保护即可

应用和数据层面改造

产品名称	服务器密码机(非信创)	服务器密码机(信创)
SM2 密钥对生成（对/秒）	210000	18000
SM2 签名/验签（次/秒）	210000/60000	18000/16000
SM2 加密/解密（次/秒）	20000/70000	12000/16000
SM1 算法加解密（Mbps）	8000	800
SM4 算法加解密（Mbps）	8000	800
SM3 杂凑算法（Mbps）	6000	800
最大并发	10000	5000

产品名称	云服务器密码机（非信创）	云服务器密码机（信创）
虚机数量	64	32
SM2 密钥对生成（对/秒）	300000	100000
SM2 签名速度（Tps）	400000	100000
SM2 验签速度（Tps）	200000	90000
SM2 加密速度	2.5Gbps	13Mbps
SM2 解密速度	2.5Gbps	18Mbps
SM3	8Gbps	8Gbps
SM1	8Gbps	3.5Gbps
SM4	8Gbps	4Gbps

100MB数据文件为例计算加密损耗时间

100*8 = 800Mb

按正规计算
高性能8Gbps的加密速率仅需0.1秒
低性能800Mbps的加密速率仅需1秒

按实现效率50%计算
高性能8Gbps的加密速率仅需0.2秒
低性能800Mbps的加密速率仅需2秒

1天1台低性能设备可以加密文件:
100*24*60*60/2/1000 = 4320TB

应用和数据层面改造

产品名称	签名验签服务器（非信创）	签名验签服务器（信创）
SM2 签名/验签（次/秒）	**180000/65000**	30000/24000
SM2 数字信封加解密	**25000/40000**	12000/20000
SM2 带签名的数字信封封装解	**18000/26000**	8000/11000
最大并发	10000	5000

按正规计算

高性能1次签名/验签时间仅需几微妙级别

低性能1次签名/验签时间仅需几十微妙级别

1天1台低性能设备可以签名和验签次数（50%计算）：

签名：24*60*60*30000/2 = 12.96亿次

验签：24*60*60*24000/2 = 10.368亿次

另一种模式：数据库加密网关或是管理系统

数据库加密改造优势：

- ✓ 原有应用无需改造或是较少改造
- ✓ 业务系统只需配合测试
- ✓ 可灵活配置加密表、加密列
- ✓ 部署实施所需工作量少，人员密码专业技术要求低

数据库加密改造限制：

- ✓ 在业务SQL比较复杂的情况下，性能影响较大
- ✓ 在每个表3-5列进行机密性和完整性保护情况下，使用比较合适，过多会影响性能
- ✓ 需要进行存量数据的切换

总结

① 使用典型的密码应用技术

② 每个环节保持一致性，环环相扣

- **符合性**
  - ✓ 使用合规的**密码算法**
  - ✓ 使用合规的**密码技术**
  - ✓ 使用合规的**密码产品**
  - ✓ 使用合规的**密码服务**

- **高风险判定**和经验
  - ✓ **不能出现高风险**
  - ✓ **优先网络通信**
  - ✓ **考虑物理环境**
  - ✓ **重点应用数据**

方案实施及注意问题

PART. 05

4.1注意的问题

方案选择	需求的取舍	适用场景
全面应用	考虑全部风险项	预算充足、项目周期允许且所有责任主体都可以配合建设
部分应用	考虑全部高风险项及部分可改造的中、低风险项	在自身职责范围内尽可能解决服务平台面临的安全风险 同时确保其他责任主体能以较小的代价配合改造，规避高风险项
最小化应用	只考虑高风险项	用户方的预算和项目周期都非常紧张，需要以最小的代价完成服务平台的密码应用建设，尽可能回避高风险项 也适用于分期规划系统建设的第一阶段

4.1注意的问题

- **设计不要求都是符合**
  - ✓ 可以是**不适用**
  - ✓ 可以是**部分符合**
  - ✓ 甚至可以是**不符合**
  - ✓ **不符合**或**部分符合**的要进行**风险分析**

- **不适用**
  - ✓ 等级要求：“可”
  - ✓ 无密码应用需求等
- **部分符合**
  - ✓ 同一个指标
  - ✓ 重点保护对象有“符合”和“不符合”

4.2密评改造评语

1、密评合规并非盲目求大求全，而是基于信息系统实际需求建立密码合规矩阵，**按需选择、分布实施、合理建设**；

2、密评合规是各层面密码防护的有机结合体，**安全性与易用性**的有效结合是重点；**做好备份**运行再实施切换。

3、密码建设需要不断优化和提升，**从用户信息系统实际出发，做最适合用户现状的解决方案**。

4、密码建设中应用系统必须进行改造，**系统厂商和密码厂商全力配合，改造评估工作量更准，会节省大量成本和时间**。

总结

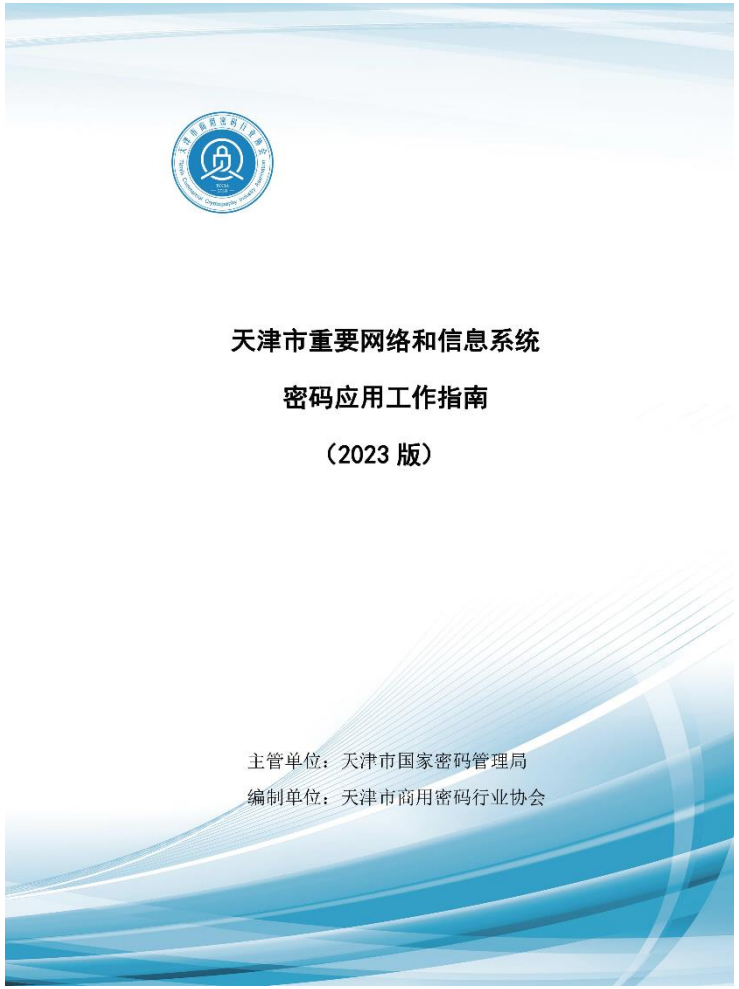
分析与总结：保障安全管理；优先网络通信；重点应用数据；关注性价优势

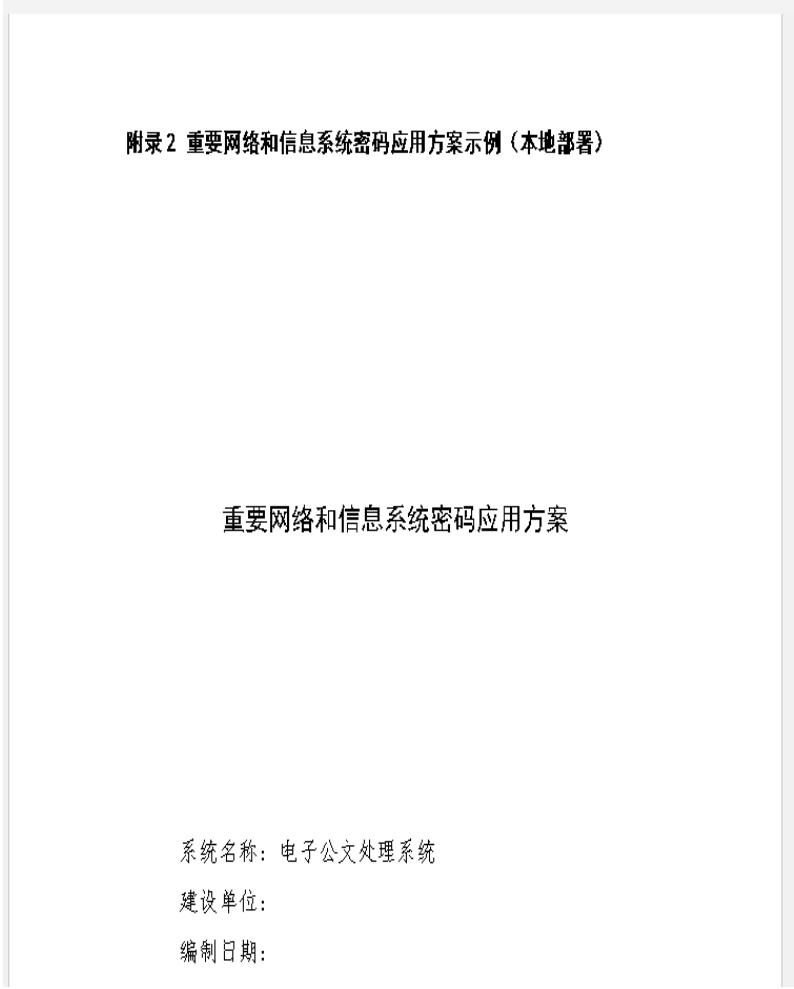
	物理和环境安全	网络和通信安全	设备和计算机安全	应用和数据安全	安全管理要求
	总分：10分	总分：20分	总分：10分	总分：30分	总分：30分
	指标：身份鉴别	**指标：1.身份鉴别 2.通信机密性**	**指标：1.身份鉴别 2.远程管理通道**	**指标：1.身份鉴别2.传输机密性3.存储安全4.不可否认**	**指标：安全管理制度 密码应用方案**
	实现性价比：高	**实现性价比：中高**	**实现性价比：低**	**实现性价比：中**	**实现性价比：高**
	实现难度：易	实现难度：中	实现难度：难	实现难度：难	实现难度：易
	高风险弥补：易	高风险弥补：难	高风险弥补：难	高风险弥补：难	高风险弥补：易

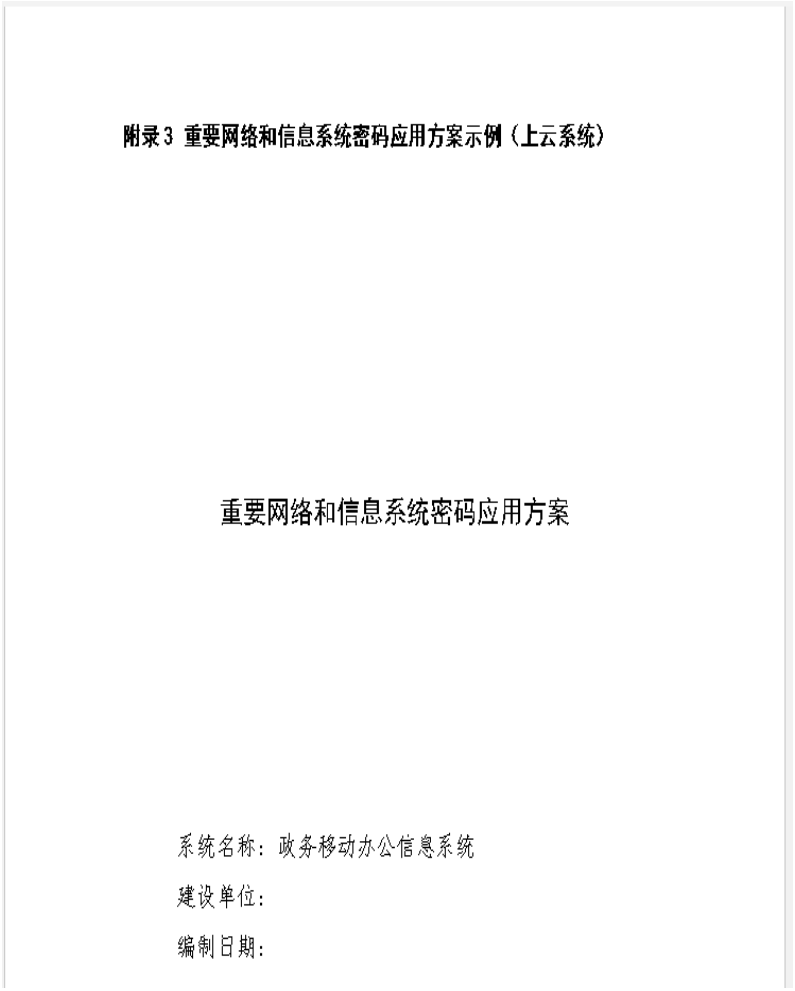
协会宣传推广平台

PART. 06

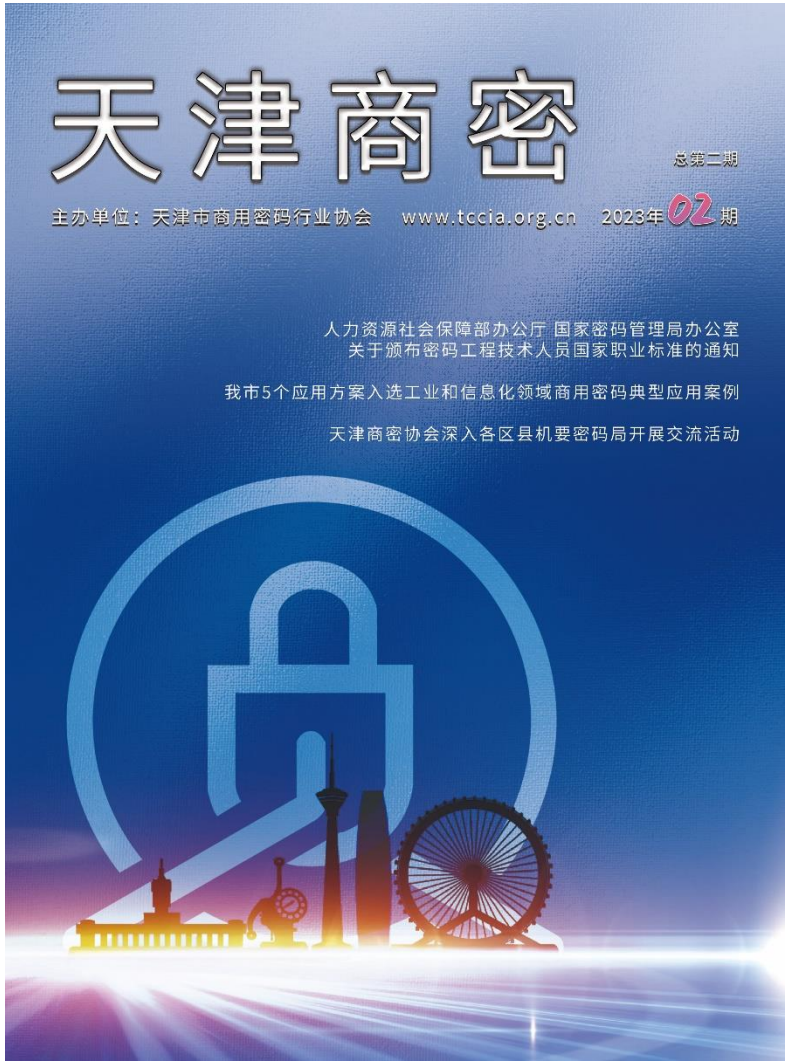
密码应用工作指南


天津市重要网络和信息系统
密码应用工作指南
（2023 版）
主管单位：天津市国家密码管理局
编制单位：天津市商用密码行业协会


附录 2 重要网络和信息系统密码应用方案示例（本地部署）
重要网络和信息系统密码应用方案
系统名称：电子公文处理系统
建设单位：
编制日期：


附录 3 重要网络和信息系统密码应用方案示例（上云系统）
重要网络和信息系统密码应用方案
系统名称：政务移动办公信息系统
建设单位：
编制日期：

协会专业期刊和厂商



会员单位

会长单位
天津光电通信技术有限公司

监事长单位
南开大学

常务副会长单位
天津灵创智恒软件技术有限公司

监事单位
天津英信科技有限公司
天津光电聚能专用通信设备有限公司

副会长单位
麒麟软件有限公司
飞腾信息技术有限公司
天津国芯科技有限公司
天津赢达信科技有限公司
恒银金融科技股份有限公司
天津长城计算机系统有限公司
天津市中环认证服务有限公司
中汽研软件测评(天津)有限公司

秘书长单位
天津光电安辰信息技术股份有限公司

理事单位
中互金认证有限公司
兴唐通信科技有限公司
道普信息技术有限公司
天津航天信息有限公司
中星电子股份有限公司
天津恒御科技有限公司
惠尔丰信息系统有限公司
北京数字认证股份有限公司
曙光信息产业股份有限公司
天津云安科技发展有限公司
天津国科量子科技有限公司
天津百望金赋科技有限公司
天津市滨海数字认证有限公司
天津联信达软件技术有限公司
天津七所精密机电技术有限公司
天津市中环系统工程有限责任公司
安云印(天津)大数据科技有限公司
天津南大通用数据技术股份有限公司
天津中网基业智能系统工程有限公司
江西智慧云测安全检测中心股份有限公司

会员单位
天津戎行技术有限公司
北京永中软件有限公司
浪潮软件集团有限公司
中孚信息股份有限公司
天翼安全科技有限公司
润成安全技术有限公司
天津优扬科技有限公司
宝牧科技(天津)有限公司
天地融科技股份有限公司
天津市海益电子有限公司
深信服科技股份有限公司
中汽数据(天津)有限公司
渔翁信息技术股份有限公司
恒利德(天津)科技有限公司
天津鲲鹏信息科技有限公司
天津鲲奥世达科技有限公司
天津市兴先道科技有限公司
天津安恒数据安全有限公司
北京国泰网信科技有限公司
北京江南天安科技有限公司
三未信安科技股份有限公司
天津市康恒信息科技有限公司
流光(天津)量子科技有限公司
中保网盾(天津)科技有限公司
天津安华易科技发展有限公司
天津华安保信息技术有限公司
北京海泰方圆科技股份有限公司
天津华汇工程建筑设计有限公司
北京卓识网安技术股份有限公司
北京安盟信息技术股份有限公司
宏信旺(天津)科技发展有限公司
佰运俐(天津)科技发展有限公司
天津睿信康达科技发展有限公司
中科问天量子科技(天津)有限公司
北京航天七零六信息科技有限公司
成都卫士通信息产业股份有限公司
威尔创新(天津)科技发展有限公司
中国电信集团有限公司天津分公司
中安云科科技发展(山东)有限公司
长春吉大正元信息技术股份有限公司
天津市国瑞数码安全系统股份有限公司
天津大学建筑设计规划研究总院有限公司
北京海量数据技术股份有限公司天津分公司
……

每期动态和网站更新

天津市商用密码应用
工 作 动 态

第11期

天津市商用密码行业协会　　2023年6月15日

特 别 报 道

1. 李强签署国务院令 公布修订后的《商用密码管理条例》

新华社北京5月24日电 国务院总理李强日前签署国务院令，公布修订后的《商用密码管理条例》（以下简称《条例》），自2023年7月1日起施行。

党中央、国务院高度重视商用密码工作。近年来，随着商用密码在网络与信息系统中广泛应用，其维护国家主权、安全和发展利益的作用越来越凸显。党的十八大以来，党中央、国务院对商用密码创新发展和行政审批制度改革提出了一系列要求，2020年施行的密码法对商用密码管理制度进行了结构性重塑。为了贯彻落实行政审批制度改革精神，细化密码法相关制度，对1999年公布的《条例》进行了全面修订。

详情可登录国家密码管理局官方网站、天津市国家密码管理局官方网站、天津市商用密码行业协会官方网站及公众号进行查阅。

天津方案和产品

天津市公安局和平分局智慧平安社区密码保障体系解决方案

为落实好天津市智慧平安社区建设要求，天津市公安局和平区分局联合北京数字认证股份有限公司、天津中网基业智能系统工程有限公司、联通数字科技有限公司天津市分公司开展2022年和平区智慧平安社区建设项目，该建设项目融合了密码技术与视频技术，通过数字签名、加解密等基于国产密码算法的密码技术从根本上解决了视频监控的安全性问题，同时构建了密码应用安全管理制度，有助于保障智慧平安社区重要数据安全，近而保障广大人民群众的生命和财产安全。

基本信息

1.项目简介

天津市公安局和平区分局建设的和平区智慧平安社区系统包含公安视频图像信息应用平台和社区人车聚类分析平台两个应用，方案按照本系统的网络安全保护等级三级，依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》和《公安机关商用密码应用指南（2020年版）》，遵循“三同步一评估”的要求，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等4个层面，以及管理制度、人员管理、建设运行和应急处置等4个方面，全面设计了和平区智慧平安社区系统密码应用建设方案。

本方案严格遵循商用密码应用安全性评估相关标准规范，在满足总体性、科学性、完备性、可行性原则的基础上，从身份鉴别、数据传输机密性与完整性保护、数据存储机密性与完整性保护、密钥安全管理等层面出发，采用SM1/2/3/4系列密码算法和安全合规的VPN安全网关、服务器密码机、签名验签服务器、智能密码钥匙（USBKey）、数字证书等密码产品和密码技术，保证符合GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中对于等保三级信息系统的密码应用要求。

2.方案背景、目的意义

智慧平安社区建设，事关巩固党的执政根基，事关基层社会治理体系和治理能力现代化，事关广大人民群众的切身利益。《国民经济和社会发展十四个五年规划和2035年远景目标纲要》就推进智慧平安社区建设提出明确要求。科技部、住建部、公安部等部委也发布相应政策规划及标准建设，明确提出要在2022年实现全国城镇地区智慧平安社区全覆盖的目标。

为落实好天津市智慧平安社区的建设要求，天津市公安局和平区分局开展2022年和平区智慧平安社区建设项目，对和平区大部分小区进行智慧平安社区建设。在智慧平安社区建设过程中，为响应国家对于公共安全视频监控建设联网应用工作的要求，依据GB/T 39786-2021《信息安全技术　信息系统密码应用基本要求》，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等4个层面，以及密钥管理、安全管理等方面，开展了智慧平安社区密码保障体系建设工作。

3.方案解决难点、堵点问题

1）智慧终端数量多、种类杂，身份真实性如何保障？

和平区智慧社区平台主要包括前端点位建设、后端存储及各类系统扩容，前端点位包括人脸抓拍相机、车辆抓拍相机、人车抓拍相机、一体化人车抓拍相机及其配套设施建设，后端存储主要是前端接入授权，结构化数据存储系统，云存储系统，解析系统，后端聚类系

天津商密产品明细表

序号	产品名称	产品型号	安全等级	证书编码	单位名称	联系人	联系方式
1	IPSec/SSL VPN综合安全网关 V1.0	AC-IPSEC/SSL VPN-01	安全二级	GM001210620230348	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
2	光电安晨读卡模块（密码模块）V1.0	AC-GMACR-01	安全二级	GM001212220230342	天津光电安晨信息技术股份有限公司	胡双喜	13821024385
3	密码卡 V1.0	CCUPN2001	安全二级	GM001210420230274	天津国芯科技有限公司	张斌	13820262575
4	Mini PCI-E密码卡 V1.0	CCUPM2005	安全二级	GM001210420230264	天津国芯科技有限公司	张斌	13820262575
5	PCI-E密码卡 V1.0	CCUPH2Q01	安全二级	GM001210420230257	天津国芯科技有限公司	张斌	13820262575
6	密码卡 V1.0	CCUPN2002	安全二级	GM001210420230248	天津国芯科技有限公司	张斌	13820262575
7	安全芯片 V1.0	CUni360S	安全二级	GM001212020230220	天津国芯科技有限公司	张斌	13820262575
8	数字证书认证系统 V1.0	ADC-CA	不涉及	GM001111820230160	中汽数据（天津）有限公司	张旺	15922090958
9	灵创智恒安全认证网关 V2.0	CIST-SAG	安全二级	GM001210720230148	天津灵创智恒软件技术有限公司	王城	13752238978
10	IPSec VPN安全通信网关 V7.6.10	BSAFE 6000	安全二级	GM001210520230121	宝牧科技（天津）有限公司	刘夏	18920325310
11	数字物理噪声源芯片 V1.0	CWNG10	安全一级	GM001212020230110	天津国芯科技有限公司	张斌	13820262575
12	国密SSL组件密码模块 V1.0	GMSSL	安全二级	GM001212220230112	天津赢达信科技有限公司	彭竹	18601092821
13	腾锐D2000 TCM可信密码模块 v1.1.0	D2000/GM/T0012-2020)	安全二级	GM001212320230070	飞腾信息技术有限公司	冯彦朝	13102232653
14	IPSec VPN安全通信网关 V7.6.10	BSAFE-1000	安全二级	GM001210520230002	宝牧科技（天津）有限公司	刘夏	18920325310
15	IPSec VPN安全通信终端 V3.1.8	BSAFE-300	安全二级	GM001210520230003	宝牧科技（天津）有限公司	刘夏	18920325310
16	IPSec VPN安全通信网关 V7.6.10	BSAFE-600	安全二级	GM001210520230001	宝牧科技（天津）有限公司	刘夏	18920325310
17	鹏瑞E2000通用安全处理器 B705	E2000	安全一级	GM001212020220798	飞鹤信息技术有限公司	冯彦朝	13102232653
18	飞腾S2500密码模块 V1.0	SMK001	安全二级	GM001212220220799	飞腾信息技术有限公司	冯彦朝	13102232653
19	手机盾认证系统服务端（密码模块）V1.0	AC-GMMD-S01	安全二级	GM001212220220786	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
20	手机盾认证系统客户端（密码模块）V1.0	AC-GMMD-C01	安全二级	GM001212220220787	天津光电安辰信息技术股份有限公司	胡双喜	13821024385
21	神通数据库管理系统密码运算模块 V7	HDEncrypt	安全二级	GM001212220220723	天津神舟通用数据技术有限公司		

天津方案（工信入围）

荣誉证书

HONORARY CREDENTIAL

中汽研软件测评（天津）有限公司

在2022年工业和信息化部、国家密码管理局开展的工业和信息化领域商用密码典型应用方案征集活动中，贵单位申报的汽车5GIPV6商用密码应用示范入选了工业和信息化领域商用密码典型应用方案名单，希望贵单位继续挖掘商用密码应用潜力，助力商用密码产业高质量发展。

特发此证，以资鼓励。

工业和信息化部商用密码产业促进联盟

2023年3月23日

荣誉证书

HONORARY CREDENTIAL

中国汽车技术研究中心有限公司

在2022年工业和信息化部、国家密码管理局开展的工业和信息化领域商用密码典型应用方案征集活动中，贵单位申报的汽车数据安全与个人信息保护密码标准化与应用检测平台建设入选了工业和信息化领域商用密码典型应用方案名单，希望贵单位继续挖掘商用密码应用潜力，助力商用密码产业高质量发展。

特发此证，以资鼓励。

工业和信息化部商用密码产业促进联盟

2023年3月23日

荣誉证书

HONORARY CREDENTIAL

曙光云计算集团有限公司

在2022年工业和信息化部、国家密码管理局开展的工业和信息化领域商用密码典型应用方案征集活动中，贵单位联合申报的天津市曙光政务云平台密码应用方案入选了工业和信息化领域商用密码典型应用方案名单，希望贵单位继续挖掘商用密码应用潜力，助力商用密码产业高质量发展。

特发此证，以资鼓励。

工业和信息化部商用密码产业促进联盟

2023年3月23日

荣誉证书

HONORARY CREDENTIAL

天津市公安局和平分局

在2022年工业和信息化部、国家密码管理局开展的工业和信息化领域商用密码典型应用方案征集活动中，贵单位申报的天津市公安局和平分局智慧平安社区密码保障体系建设方案入选了工业和信息化领域商用密码典型应用方案名单，希望贵单位继续挖掘商用密码应用潜力，助力商用密码产业高质量发展。

特发此证，以资鼓励。

工业和信息化部商用密码产业促进联盟

2023年3月23日

荣誉证书

HONORARY CREDENTIAL

天津市公安局

在2022年工业和信息化部、国家密码管理局开展的工业和信息化领域商用密码典型应用方案征集活动中，贵单位申报的天津市公安局新一代移动警务密码应用入选了工业和信息化领域商用密码典型应用方案名单，希望贵单位继续挖掘商用密码应用潜力，助力商用密码产业高质量发展。

特发此证，以资鼓励。

工业和信息化部商用密码产业促进联盟

2023年3月23日

感谢聆听

天津市商用密码行业协会