HIKVISION

AIOT智能物联时代下的商用密码技术应用

网络安全部

海康威视网络安全部

2026.11

目录

CONTENTS

01 政策背景痛点

02 整体解决方案

03 海康能力介绍



PART 01

政策背景和痛点

法律法规标准

2017年~2023年（试点建设期）： 大范围开展密评测试（强制）和整改（建议）

2023年~2027年（正式建设期）：新建项目必须通过密码测评（规划、验收重点）

商用密码政策情况

2017

启动密码改造试点工作

《关于开展密码应用安全性评估试点工作的通知》

2018

明确金融等领域密改要求

中办和国办印发《金融和重要领域密码应用与创新发展工作规划》

2019

明确政务信息化密码应用要求

【2019】57号文

2020

确立商用密码法律制度

颁布《中华人民共和国密码法》

2021

明确密评规范准则

《信息安全技术信息系统密码应用基本要求》

2022

商密金融行业标准发布

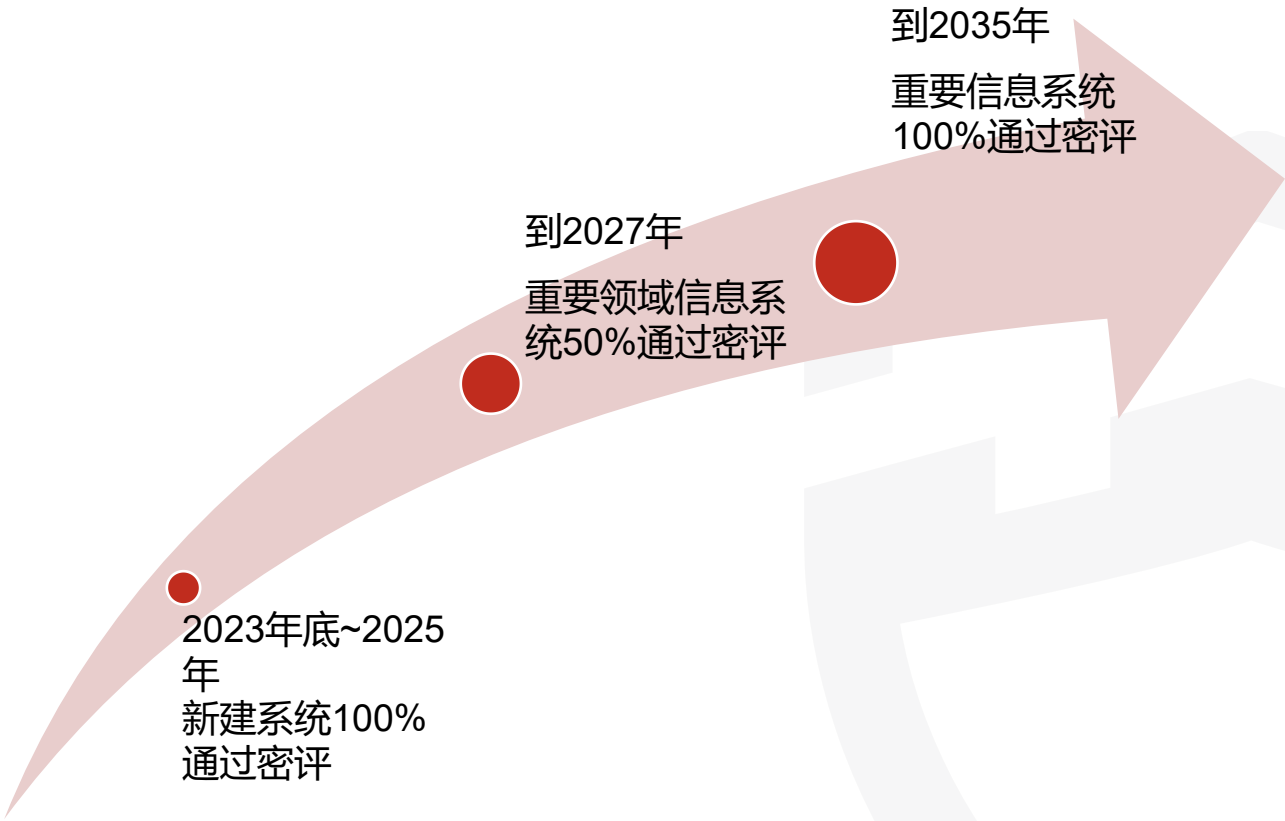
央行发布《金融行业信息系统商用密码应用》系列标准

2023

明确监督管理机制与法律责任

《商用密码管理条例》

政策趋势


到2035年
重要信息系统100%通过密评
到2027年
重要领域信息系统50%通过密评
2023年底~2025年
新建系统100%通过密评

近期重大政策及影响

2023年~2027年（正式建设期）：新建项目必须通过密码测评（整改）


中华人民共和国中央人民政府

中华人民共和国国务院令

第760号

《商用密码管理条例》已经2023年4月14日国务院第4次常务会议修订通过，现予公布，自2023年7月1日起施行。

总理 李强

2023年4月27日

商用密码管理条例

2023年5月24日，《商用密码管理条例》正式发布，7月1日起施行

01 明确《密码法》为立法宗旨

从国家法律法规层面明确商用密码应用的合理性和必要性

02 密评从“推荐”到“强制”

若未开展测评或测评验收不通过，将无法进行项目验收

03 明确监督管理机制与法律责任

各级密码管理局将加强监管，不符合密评将面临一百万罚款等

✦ 运营商机房

运营商机房**若未通过密评，则无法承接政府、金融项目**

1：内部发文要求3年内完成所有IDC机房国密改造

2：各省运营商划拨专门的建设预算，完成机房改造

3：内部发文要求新建机房必须符合密评要求

✦ 金融机房/数据中心

落实中央和行业政策，**新建或者维护项目中机房密评均作为重点建设内容**

1：2025年，自有数据中心100%完成改造

2：2035年，核心数据中心100%完成改造

✦ 所有机关(政府、司法、公安等)项目

政府财政支出关联的**新建项目，必须通过密评，否则项目验收不通过**

1：所有新建系统类项目密评机房部分，均是必选项

2：基本所有升级类项目，密评机房部分，也可纳入项目升级范畴，重点建设！

✦ 能源、医疗、教育等数据中心/机房

各行业政策要求，**新建或者维护项目中机房密评均作为重点建设内容**

1：所有数据中心、机房至少满足密评三级

2：行业十四五规划建设指导意见要求落实密码应用

密码应用痛点解读

密评不是“加分项”，而是项目闭环、经营资质与安全底线的“必答题”——每一处缺失都会在验收、投标、监管或事故中被放大。

01 验收卡口

密评未通过

项目无法竣工验收、无法上线运行，财政资金不予支付，工期与回款双双停滞。

02 法律红线

处罚已明确

《密码法》《商用密码管理条例》明确：拒不整改可处 1 万–100 万元罚款，并追究责任。

03 市场准入

投标资格受限

政府、金融、运营商等项目把密评作为门槛项，无测评报告直接失去投标与承接资格。

04 安全裸奔

数据明文流转

视频、图像、数据库明文存储传输，身份仅靠弱口令，密钥无统一管理，泄露即失控。

05 整改代价

返工成本翻倍

事后补改需重构网络与业务架构，业务中断、重复投资，周期与预算普遍上浮 50% 以上。

06 管理缺位

制度体系空白

管理制度、人员管理、建设运行、应急处置四类文档缺失，测评现场直接扣分。

密码应用痛点解读

HIKVISION

依据 GB/T 39786《信息安全技术 信息系统密码应用基本要求》，密评按四层面 + 三管理逐项核查，不留“补丁空间”。

物理和环境安全

常见缺失表现

机房出入仅凭门禁卡/密码，无基于商密的身份鉴别与记录完整性保护

直接后果

人员进出可被冒用、记录可被篡改，物理侧证据链断裂

网络和通信安全

常见缺失表现

远程运维、跨网传输走明文或国际算法，未使用国密 SSL/IPSec 通道

直接后果

链路被旁路监听即可获取全部业务数据

设备和计算安全

常见缺失表现

设备默认口令、日志可删改，无商密堡垒机做运维管控与抗抵赖

直接后果

内部越权操作无迹可查，事后无法定责

应用和数据安全

常见缺失表现

视频、图片、数据库明文存储，密钥散落在配置文件与运维手中

直接后果

一次拖库或设备丢失即造成批量数据泄露

密评采用“木桶原则”：四个层面 + 管理制度、人员管理、建设运行、应急处置，任一项不符合即整体不通过，需整改后重新测评——返工不是局部修补，而是全量复核。

PART 02

整体解决方案

HIKVISION

商用密码应用 安全性评估

概念

商用密码应用安全性评估（简称“**密评**”）对采用商用密码技术、产品和服务集成建设的网络和信息系统密码应用的合规性、正确性、有效性按照《信息系统密码应用基本要求GB/T 39786》进行**评估。**

对象

基础信息网络、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、面向社会服务的政务信息系统、**关键信息基础设施**、**网络安全等级保护第三级及以上信息系统**

评估内容

分别针对信息系统的物理机房、网络通信、设备计算、应用数据进行检测，评估**是否正确有效采用具备资质的密码产品**

评估结论

60分及以上（满分100分）且系统不涉及高风险，即“基本符合”，视为系统通过密评；**三级系统，每年测评一次**

密评解读


ICS 35.040
L 80

GB

中华人民共和国国家标准

GB/T 39786—2021

信息安全技术
信息系统密码应用基本要求

Information security technology—
Baseline for information system cryptography application

2021-03-09 发布　　2021-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

通用要求

规定了**密码算法、密码技术、密码产品和密码服务**应符合相关国家标准、行业标准的有关要求。

密码应用基本要求

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**

附录A　列出了不同级别密码应用基本要求**“应”、“宜”、“可”**的汇总表。

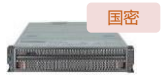
附录B　提出了**密钥生存周期管理**的建议，包括密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节。

整体建设内容

HIKVISION

物理环境安全 (10分)	网络通信安全 (20分)	设备计算安全 (10分)	应用数据安全 (30分)	安全管理 (30分)

商密安防产品系列



视频安全门禁系统



商密摄像机



商密存储设备



商密门禁设备

传输加密产品系列



IPSec VPN网关



SSL VPN网关

运维安全产品系列



SSL VPN网关



商密堡垒机

通用密码产品系列



服务器密码机



密钥管理系统

...

模块化加固系列



数据库加密网关



存储加密网关



数据保护系统
(终端应用)



文件加密网关

密码应用管理制度

- 《XXX单位密码管理制度汇编》
- 《XXX单位商用密码产品密钥管理指南》
- 《XXX单位商用密码产品操作规程》
- 《XXX单位密码管理制度修订记录台账》
- 《XXX单位管理文件评审及发布制度》
- 《XXX单位密码管理制度发布记录台账》
- 《XXX单位密码应用岗位责任制度》
- 《XXX单位密码应用人员培训制度》
- 《XXX单位XXX年度密码安全培训计划》
- 《XXX单位XXX年度密码应用安全考核试卷》
- 《XXX单位密码关键岗位人员保密和调离制度》
- 《XXX单位人员管理离职保密协议书》
- 《XXX单位XXX信息系统密码应用方案》
- 《XXX单位XXX信息系统密码应用实施方案》
- 《<XXX单位XXX信息系统密码应用方案>商用密码应用安全性评估报告》
- 《XXX单位XXX年度密码安全攻防对抗演习计划》
- 《XXX单位密码安全应急处置指南》
- 其他相关记录材料

✓ 安防品牌龙头信誉 ✓ 产品严格合规，不作伪 ✓ 形态、功能最全（多款唯一）	✓ 具备网络层应用级数据加密能力，支持跨网加密传输	✓ 业内首批获得资质厂商	✓ 完全自研的通用密码产品，具备三级密码自研能力 ✓ **为不具备开发条件的系统，提供驱动级模块加固能力**	✓ 专业安全服务，协助责任单位搭建密码应用管理体系

物理和环境安全

HIKVISION

商密摄像机



1-国密二级证书
2-形态涵盖枪机、半球

国密资质，稳定性好

商密存储设备



1-覆盖NVR/CVR/云存储
2-可满足密评三/四级要求

形态丰富，云存资质业内领先

商密门禁设备



1-全产品国密资质
2-质量较友商稳定

质量稳定、形态业内最多

视频安全门禁系统



1-适配各种适用场景
2-业务功能全支持

产品形态多样，业务灵活扩展

方案优势

- **产品体系最全：**海康有全系列多形态产品资质
- **产品严格合规：**一型号一证书，完全符合测评要求
- **业务功能全面：**在保证合规的同时，保证业务全面性和系统稳定性
- **项目案例最多：**覆盖所有省份、行业，累计案例2000+

小型机房解决方案

适用对象：小型机房或低预算用户

方案优势：机房密评三级满分；成本较低

推广优势：市场侧采购最多的方案，可在行业或区域大范围复制

密评四级解决方案

适用对象：有高安全建设要求的用户

方案优势：可最高分过测评；业内性能领先，业务功能全面，稳定性强

推广优势：项目体量庞大，典型案例众多，业内认可度高

利旧机房改造方案

适用对象：已建系统改造

方案优势：利旧原视频设备，性能业内领先

推广优势：低实施成本改造，不改变系统架构和使用习惯

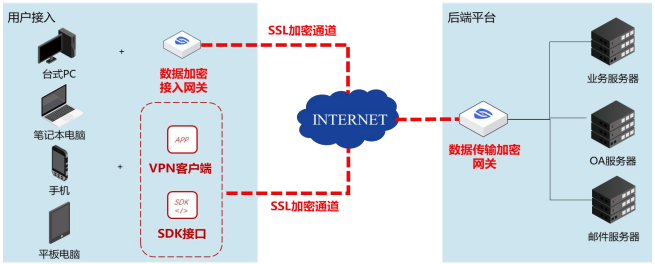
HIKVISION

产品优势

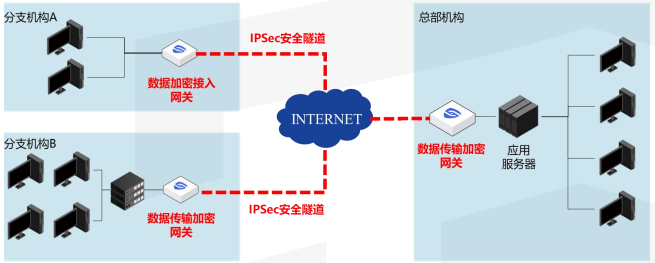
■ 国密通道加密

✓ 支持全通道加密，保障端到站、站到站安全
✓ 兼容主流网关设备，扩建升级项目利旧互通

■ SSL VPN（端到站）

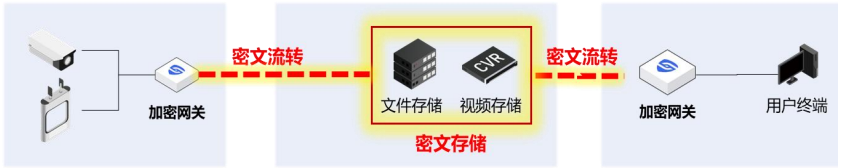


■ IPSec VPN（站到站）



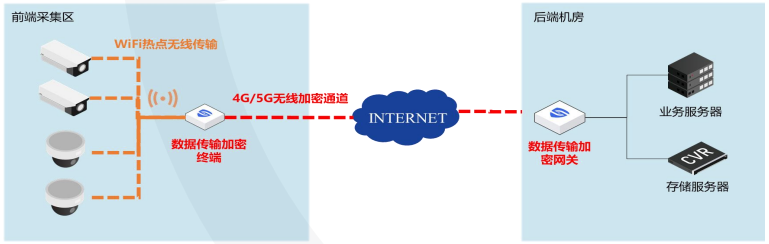
■ 应用数据加密

✓ 支持视频/图片/文件等最小化灵活加密
✓ 支持密文跨网流转，有效节省用户开支



■ 无线传输

✓ 多种无线加密技术（WiFi/5G/4G），适用于户外/线缆不通/远距离传输等场景
✓ 支持单/双向无线加密传输，适配IPC/电围/手持终端等无线设备



HIKVISION

集商密合规与安全运维于一体的堡垒机产品

产品定位



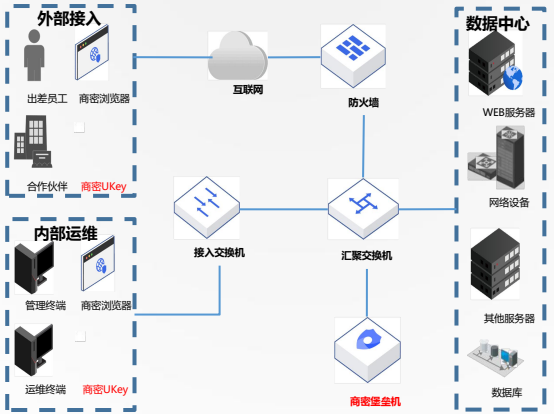
商密堡垒机，符合GM/T 0028《密码模块安全技术要求》安全等级第二级要求，基于商密算法及认证硬件模块，提供身份认证、安全通道、抗抵赖及完整性校验功能，确保数据机密性与完整性，同时支持运维审计与核心资产保护。

产品优势

- ✓ **满足多项合规要求：密评合规，国产化合规、等保合规**
- ✓ **跨平台兼容：基于B/S架构实现浏览器端统一管理，支持所有主流浏览器与操作系统**
- ✓ **架构灵活：兼容C/S菜单与直连模式，支持本地资源调用，兼顾传统客户端的高性能需求**
- ✓ **精细的权限管理：支持工单申请，协同操作、访问控制策略制定等功能，实现权限最小化管理，预防高危操作发生**
- ✓ **自动化运维：实现对Linux\Unix、Windows服务器、网络设备的密码定期自动修改，无需安装Agent**

业务设计

产品部署在汇聚交换机处，不更改原有网络的拓扑结构、不影响设备的业务数据流，支持集群部署、分级部署。



- ✓ 旁路部署，逻辑串联
- ✓ 不安装任何插件
- ✓ 不安装任何服务端引擎
- ✓ 不影响现有拓扑结构
- ✓ 不影响现有业务数据流

HIKVISION

适用标准密评应用数据安全建设，合规性强，安全性高

服务器密码机



1-国密三级/二级证书
2-便捷封装接口易改造

稳定性好，易用性强

签名验签服务器



1-多种签名格式支持
2-多种证书验证策略

高并发签名，满足不可否认性要求

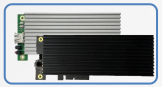
密钥管理系统



1-高稳定海量密钥分发场景
2-云环境/大数据场景可用

多场景密钥统一管理

密码卡系列



1-国密三级/二级证书
2-提供丰富的易集成接口/工具

高易用，高稳定，高性价比

产品优势

✓**高易用：提供便捷封装接口及工具，有效降低实施成本，实现密评快速改造**

✓**高稳定：提供密钥/业务/整机等多种健壮性保障机制，实现无忧部署接入**

场景定位

新建系统：新建信息系统时一步到位，同步考虑密码应用需求

高安全合规需求：实现全面的密码应用安全防护，可满足以较高分数通过测评

典型案例

- **全量密评：**
  四川仁寿医共体项目 — 多应用平台改造
- **全量密评：**
  绍兴交管平台项目 — 三方信息系统

应用和数据安全| 模块化加固产品系列

HIKVISION

适应密评应用数据安全定制场景，为不具备开发条件的系统提供模块化安全加固方案，实现免改造合规

数据存储安全网关



1-视频存储机密性完整性
2-兼容IPC/CVR/NVR/流媒体

稳定性好，性能业内领先

数据库透明加密系统



1-兼容主流通用/国产数据库
2-业务平台免集成免改造

纯透明加密，具备高可扩展性

文件系统加密网关



1-适配Linux、Windows环境
2-兼容结构化/非结构化数据存储安全场景

一机实现多场景数据存储合规

数据安全保护服务器



1-数据应用生命周期风险应对
2-应用效果具备用户高接受度

现有业务免改，合规改造

产品优势

✓**资质品牌一致性：产品全系列具备商密资质**

✓**部署即合规：现有业务免集成免改造，快速符合密评合规要求**

✓**场景覆盖全面：能够兼容数据复杂应用场景，同时具备较强可扩展性**

场景定位

- **海康系统：**①现有设备/系统不具备改造条件、②项目无法提供相应定制费用，免改加固方案可**同时应对合规和费用问题**
- **第三方系统：**免改加固方案，**快速实现密评合规，避免多方对接拉扯**等不可控因素

典型案例

- **机房密评：**
- 河南移动IT云机房　运营商机房
- **全量密评：**

昆明长水机场　三方通用信息系统

PART 03

海康能力介绍

海康威视商密业务发展历程

HIKVISION

海康威视于2015年开展商用密码技术研究，从技术内供到赋能产业，不断积累和沉淀，结合自身物联领域先驱优势，为用户提供业务应用级密码应用能力。

2016年

完成全链路国产密码加密系统研制

密码技术普及应用

设计商密视频监控方案，研制产品

《商用密码产品生产定点单位证书》

2017年

首批商密产品检测通过

SYT1703 密钥管理系统

SRM1707 安全门禁读卡器

《商用密码产品销售许可证》

2018年

整套视频监控系统检测通过

SHT1810 视频监控安全管理系统

SJT1809 视频采集加解密系统

FIPS 140-2 认证

2019年

确定商密技术为安全基石

基于安全芯片的内生安全架构

多类产品中支持商密技术

牵头制订密码行业标准（GM/T）

2020年

对外输出商密技术能力

成立产品业务部，着力密码产品研发

视频密钥系统，获**GM+AK证书**

商密方案，获世界物联网博览会金奖

2021年

形成全体系的密码能力

工信部 商密联盟 常务理事单位

软件密码模块（二级）

P3010密码卡（二级）

首批机房密评*满分通过*

首批安防系统密评三级通过

2022年

筑牢密码基石赋能产业

中国多媒体企业创新技术

首届全球数贸会先锋奖

产品系列化获得商密证书，构建全方位安全能力

2023年

构建多元化方案体系

工信部商密典型应用方案

工信部网络安全类示范项目

多行业密码专项方案

基于商密技术的数据安全方案

2024年

密码能力突破

三级密码卡（完全自研）

三级密码机（完全自研）

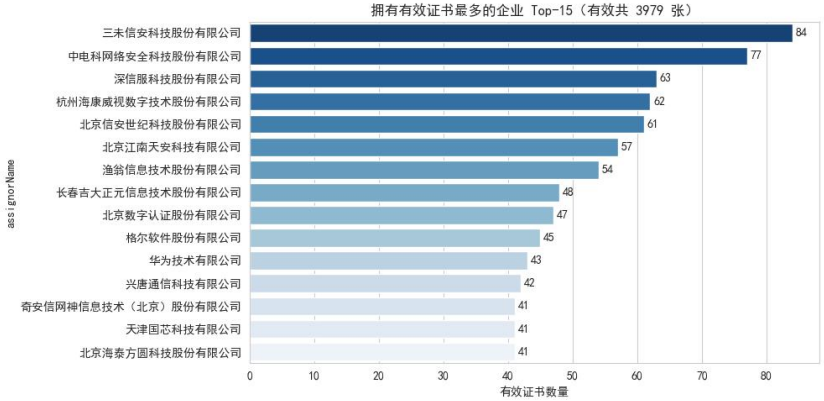
密评业务模块化中间件（业内独家）

四级机房密评案例大面积落地

产业链内情况说明

HIKVISION

海康威视聚焦密码应用，以夯实的技术基础和海量项目建设经验为基础，为用户提供真正解决问题的应用安全类产品&服务





- ✓ **截止8月10日，商密产品证书数68(位列第3），商密三级产品证书4张(位列第4)**. *预计到年底可达80款。*
- ✓ 海康威视属于**唯一非传统密码专业厂商拥有三级密码能力**的企业，同时具备密码与业务融合的天然优势。

海康威视已形成覆盖“芯片、模块、设备、系统、应用”全链条的商用密码技术创新和服务能力；并形成特色鲜明的“安防+密码”、“物联网+密码”方案体系。

物联密码成果积累

海康威视在物联网安全应用领域持续投入，在高性能密码加速、物联设备密钥管理、非结构化数据加密等领域申请物联安全相关专利300余项，研制安全物联产品100余种，落地安全物联系统项目超3000个







海康数据安全案例集

HIKVISION

公安

杭州市“TWGC”项目
哈尔滨市公安局全量密评项目
诸暨市公安局网络安全建设项目

交通

昆明长水国际机场
鄂尔多斯空港物流园区
温州市中心城区绿色停车

政府

吴川智慧城市项目
南开区新型智慧城市
郑州市新型智慧城市视联网









检法司

云南省监狱管理局项目
泉州市看守所“智慧看守”项目
福建省女子监狱

教育

闽江学院智慧校园项目
皖西学院智慧校园项目
徐州市教育局校园网建设项目

医疗

仁寿县公共卫生服务管理平台
瑞金医院
浙大二附院

HIKVISION

网络安全部