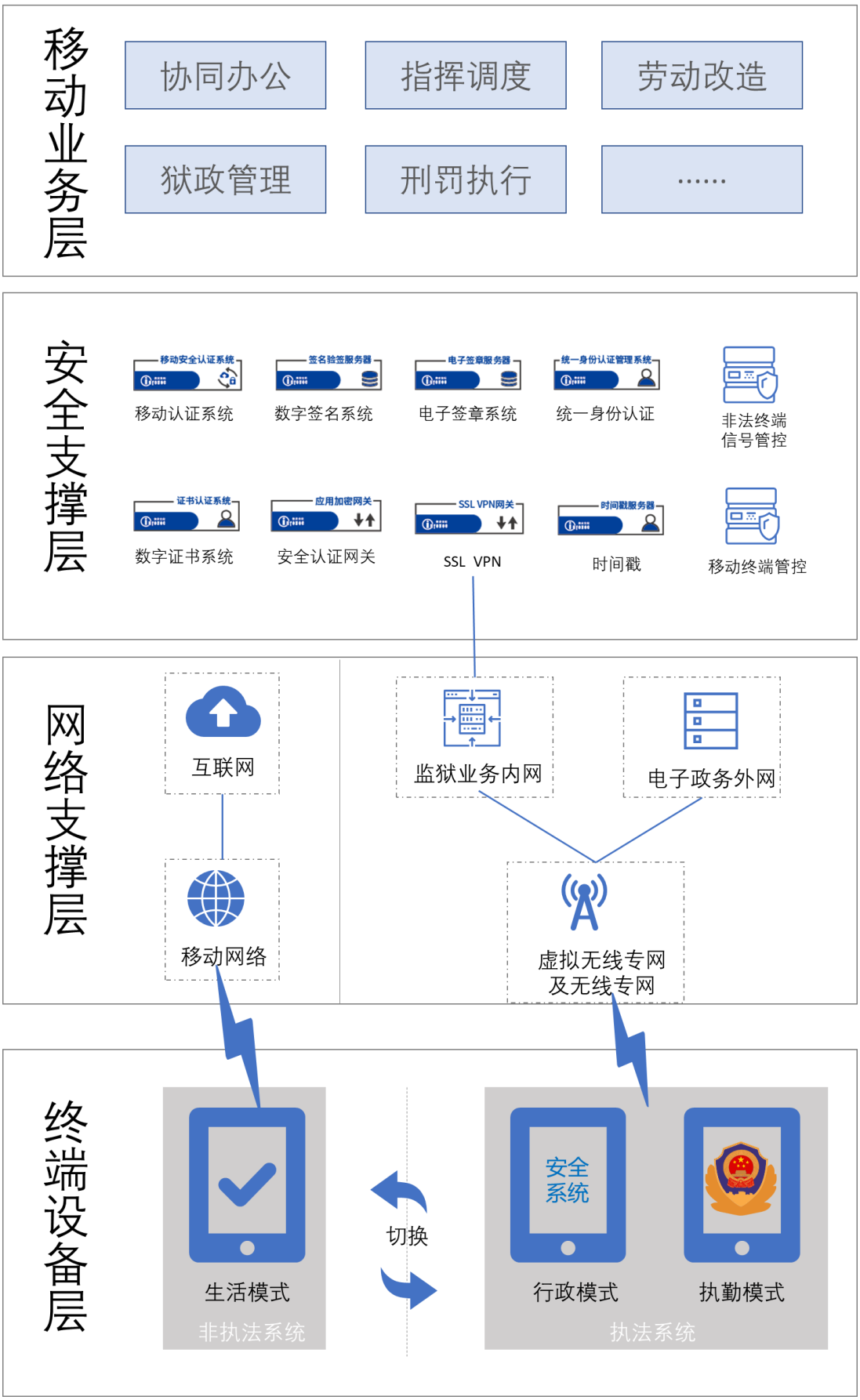
某省监狱管理局智慧监狱移动执法安全解决方案

北京信安世纪科技股份有限公司

随着以 5G、人工智能、工业互联网、物联网为代表的新基建的发展，某省监狱管理局不断深化智慧监狱建设，司法移动警务的信息化应用在不断深入，依托大数据、云计算、物联网、国产密码、移动互联等现代化新型技术，与监狱业务的深度融合，不断推动监狱信息化建设更趋科学化、精细化、智慧化，信息化技术积极进行智慧化转型升级，解决了诸如移动端办公无法统一管理，传统执法执勤模式效率低，整体指挥调度难等问题，大幅提高了监管系统智慧化办公的效率。

1.1 移动执法安全方案


移动业务层
协同办公
指挥调度
劳动改造
狱政管理
刑罚执行
……
安全支撑层
移动安全认证系统
移动认证系统
签名验签服务器
数字签名系统
电子签章服务器
电子签章系统
统一身份认证管理系统
统一身份认证
非法终端
信号管控
证书认证系统
数字证书系统
应用加密网关
安全认证网关
SSL VPN网关
SSL VPN
时间戳服务器
时间戳
移动终端管控
网络支撑层
互联网
移动网络
监狱业务内网
电子政务外网
虚拟无线专网
及无线专网
终端设备层
生活模式
非执法系统
切换
安全
系统
行政模式
执勤模式
执法系统

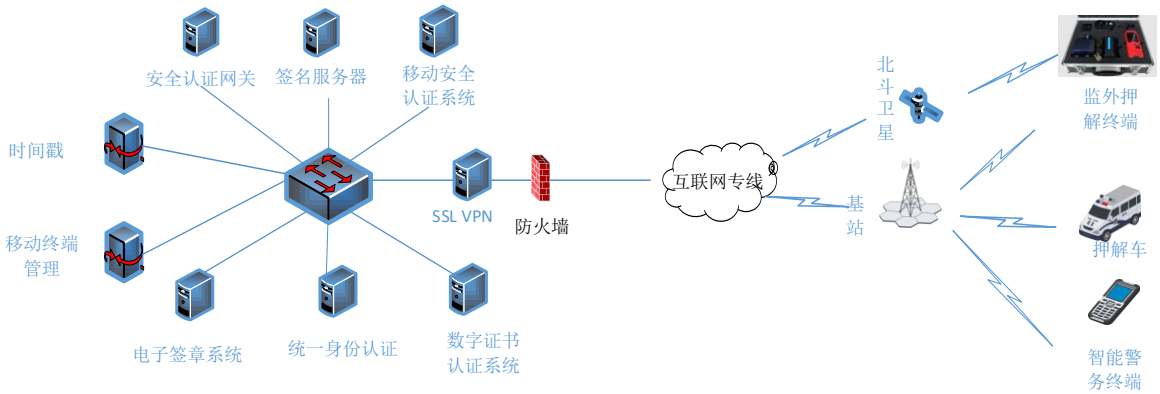
为保障信息安全该省监狱管理局智慧监狱移动执法系统，主要通过以下四个层面来实现：一是移动终端系统的安全，基于安卓系统深度定制的安全系统，设置双操作系统，包含执法系统和非执法系统，非执法系统即生活模式，可以连接互联网，用于生活娱乐等，非执法模式无法访问到监狱内网系统后台。执法系统包含行政模式及执勤模式，上班期间切换至“行政模式”连接专网工作，进入监区时，通过刷监区入口门禁切换至“执勤模式”，配合电话白名单保证通话安全，通过应用管理及其他管控功能确保监区内终端的安全使用。双系统保证业务数据与个人数据安全隔离，一个独立的安全工作系统，将应用、文件等数据全部存放在受保护的安全区域内，实现与个人数据的完全隔离，杜绝外部恶意入侵和非法读取。

二是网络的安全，执法系统依靠运营商的网络链路，提供 APN/VPDN 专用传输信道，来实现移动执法终端的接入。同时在业务层使用 SSLVPN 拨号接入，使用 TEE 数字证书认证，以此来进一步保障网络的安全。

三是数据的安全，终端硬件搭载了我国自主研发设计的密码产品国密 TEE 芯片，通过监狱管理局自建的数字证书认证系统，签发国密算法的数字证书，用于业务登录的身份认证、传输加密、存储加密、数字签名、电子印章等功能。采用高强度的国产自主商用密码算法，对工作数据进行加密，外界无法识别和读取数据，进一步减少信息泄漏风险。此外，安全系统切换后系统内的敏感数据自动清除，本地数据不留痕，从根本上杜绝设备泄露信息的可能性。

四是应用安全，移动终端配备有终端管理系统，安全系统内禁止私自安装应用，由后台管控平台统一下发安装。移动设备管控功能，提供了强大的集中管控能力，针对移动设备、应用、文件等资源进行有效的管控，轻松应对设备丢失带来的数据泄漏风险。通过移动终端管理系统对安全接入的移动终端进行远程管理和审计，提供工作人员的设备管理、用户管理、应用管理、内容管理、策略管理、统计分析及合规管理等安全服务保障，实现移动终端全生命周期的安全管理。

1.2 移动执法数字证书设计



某省监狱管理局移动执法安全方案由 SSLVPN 设备、数字证书认证系统、安全认证网关、安全 APP、移动执法终端、移动认证系统、统一身份认证系统、电子签章系统、时间戳系统、移动终端管理系统组成。

通过移动认证系统与监狱管理局建设的 CA 系统进行无缝对接，为执法用户在线发放移动数字证书，数字证书将与执法设备、用户进

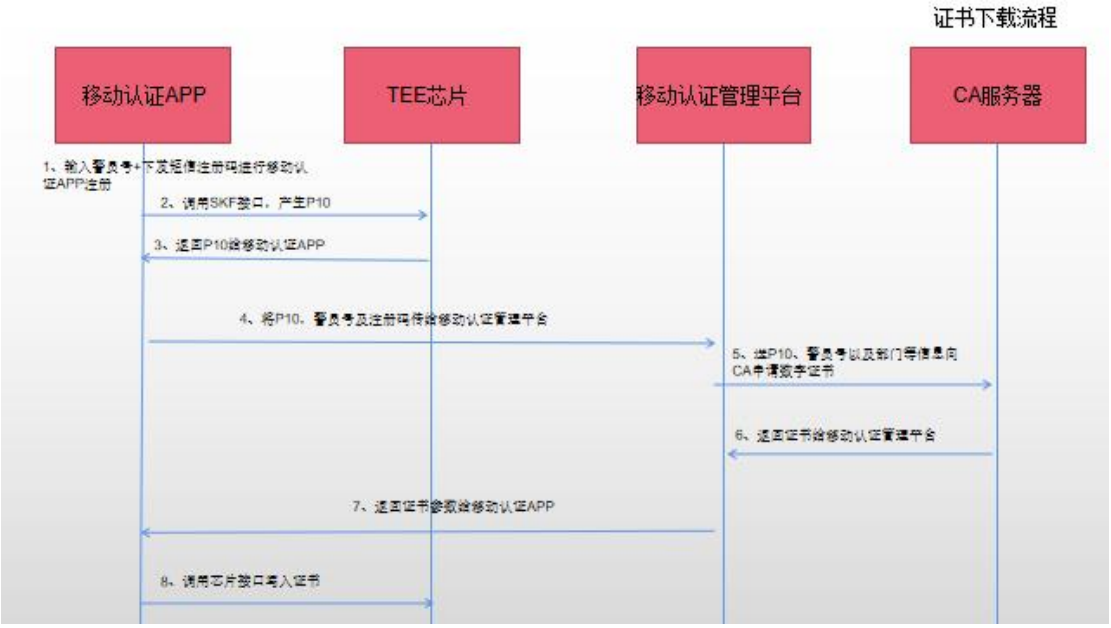
行一一绑定，并作为网络上唯一的身份凭证，确保只有授权的执法终端、执法人员才能安全访问后台执法系统，“人、机、卡、数字证书“捆绑”管理。

为最大化减少后期维护工作量，移动证书的注册、申请、更新、作废、冻结等全生命周期采用在线模式进行管理，证书的注册在执法人员首次账号注册时自动完成下载，对执法人员无感知，系统具有自动判断证书有效期，在证书有效期剩下 1 个月内自动完成证书更新，无需人工干预，当证书不再使用时，可以在后台对数字证书进行作废操作。

为提高执法人员数字证书密钥安全性，证书密钥将在执法终端 TEE 芯片内产生、存储、使用、销毁，整个密钥全生命周期不出芯片，确保密钥安全性。

移动执法终端只有通过 SSLVPN 设备认证通过后才能访问后台执法系统，移动执法终端与 SSLVPN 关间基于数字证书实现强身份认证，认证通过后将建立一条可信安全传输通道，所有执法数据将在隧道中采用加密方式传输，确保执法数据全程端到端的加密，从终端到数据中心，数据不落地。防止执法数据在传输过程中被非法窃听和篡改，身份验证通过后，SSLVPN 将根据执法人员身份进行授权，执法人员只能访问权限范围内的业务系统。

- **数字证书注册、下载**



1）将全省所有用户信息收集，通过批量方式导入移动认证系统，并通过手机短信方式将用户的注册码下发给用户。

2）用户输入警员号+下发短信注册码进行移动认证 APP 注册。

3）移动认证 APP 调用芯片 SKF 接口，产生 P10

4）芯片返回 P10 给移动认证 APP。

5）移动认证 APP 将 P10，警员号及注册码传给移动认证系统。

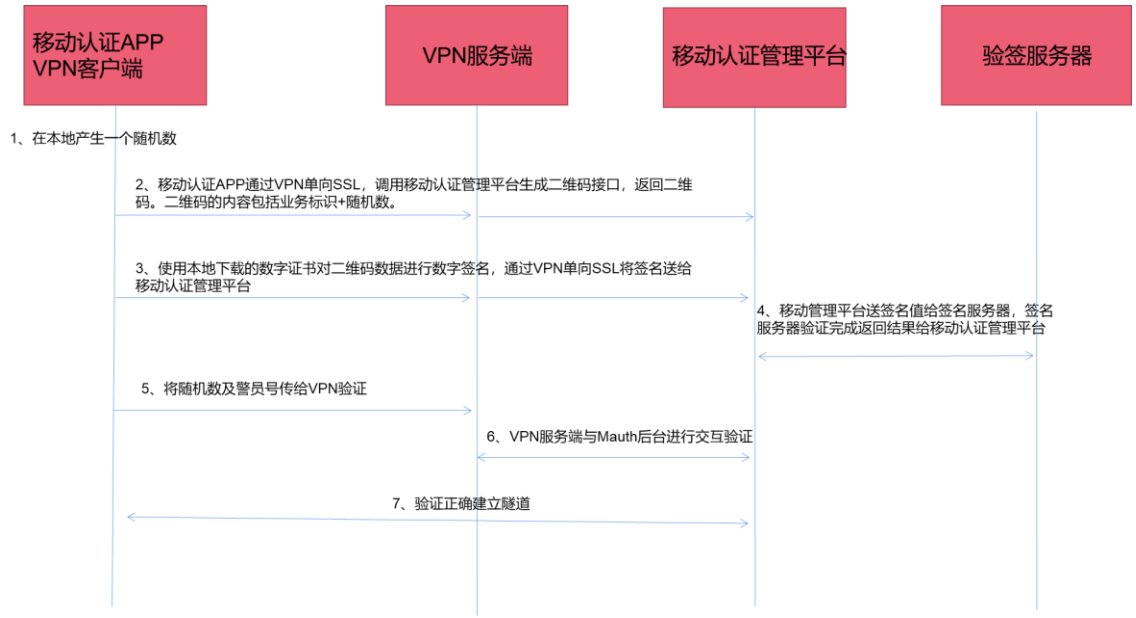
6）移动认证系统送 P10、警员号以及部门等信息向 CA 服务器申请数字证书

7）CA 服务器返回证书给移动认证系统。

8）移动认证系统将证书参数返回给移动认证 APP。

9）移动认证 APP 调用芯片 SKF 接口写入证书。

- **执法终端 VPN 接入基于数字证书认证**



1）移动认证 APP 在本地产生一个随机数。

2）移动认证 APP 调用移动认证系统产生二维码接口。（二维码数据包含业务标识+随机数+时间戳）

3）使用本地下载好的数字证书对二维码数据进行数字签名。

4）将数字签名发送给移动认证系统。

5）移动认证系统调用签名服务器对签名进行验证，返回验证结果。

6）移动认证 APP 将第一步产生的随机数送给可信网关进行验证。

7）可信网关向移动认证系统查询验证结果。

8）验证通过建立安全传输隧道，并对执法人员和终端进行授权。

- **移动执法数据安全加密**

移动执法设备现场取证数据通过该终端设备数字证书完成数据加密操作后上传执法平台系统，平台系统通过数字签名系统解密该证据数据，并验证数据数字签名有效性后进行归档存储，从而实现对现场取证数据机密性、完整性及合规性的保障。

执法人员使用移动执法终端进行现场处置、信息录入等关键执法业务操作时，执法数据均通过执法人员数字证书完成，此类执法数据上传平台系统后，平台系统通过数字签名验证系统核验执法操作合法性后，现场执法操作才能完成。事后通过恢复验证执法数据数字签名，可完成对执法人员执法操作的责任认定。

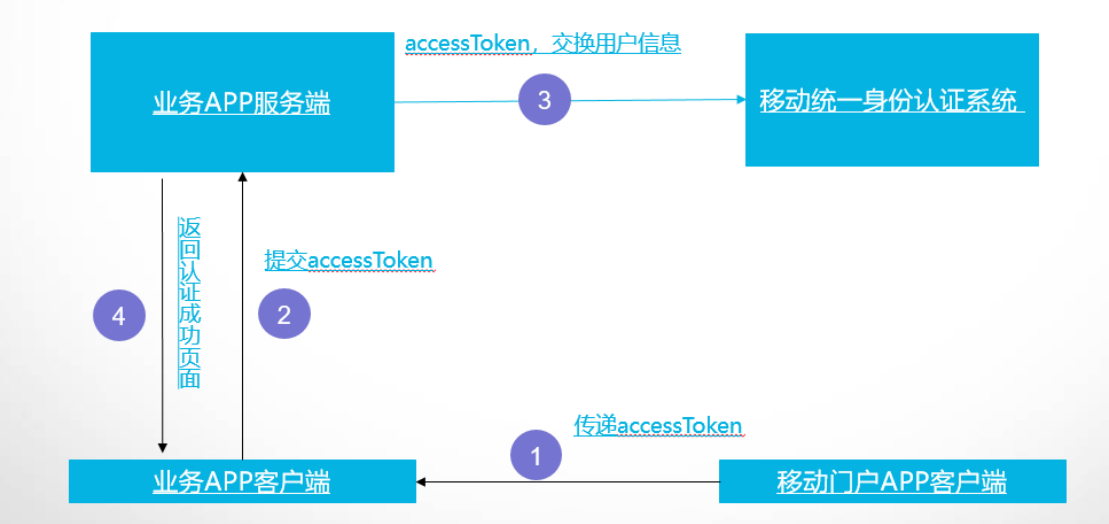
监狱工作人员在行政模式中需完成协同办公的流程审批，通过移动端电子签章技术确保了流程审批的身份认证、文件完整性、法律合规性等。

1.3 移动业务单点登录

统一身份认证系统提供移动 APP，其可以向执法人员展示当前权限所能看到的业务系统 App 的列表,并且提示用户哪些应用需要下载，下载过程中可以向用户展示当前的下载进度及下载完成之后帮助客户安装业务系统。平台提供的移动 APP 通过 OAuth 协议来支持移动 APP 的统一认证，即移动 APP 登录时，其需要通过 OAuth 协议来调用统一身份认证平台的移动 APP 实现统一认证，从而形成桌面移动一体化认证体系，对执法终端上多个 APP 实现一个入口、一个门户、一次认证、全网漫游，避免重复注册、重复认证、重复授权现象，最大化

提高操作便利性。

移动端单点登录流程：



在移动门户 APP 完成上述的认证之后，则获取到统一认证单点登录系统的 Access Token。现需要在移动门户 APP 上调用其它移动 APP 客户端，并且实现对其它移动 APP 客户端的单点登录。

1.4 建设意义

移动执法终端是替代传统办公的一种新的办公模式，移动执法利用现代移动终端技术、移动通讯技术、GIS 技术、GPS 技术等过与现有的业务系统有机结合构建智慧移动执法平台系统，办公可以在任意时间任意地点完成。

- 对执法终端的接入认证，确保授权的执法终端可以才可以接入，对非法接入的设备可以剔除注销。
- 与某省监狱管理局行业 CA 进行无缝对接，为执法人员发放移动数字证书，采用数字证书方式对执法人员、执法终端进行

绑定，保障授权的警务人员才能安全接入及身份认证。

- 对执法用户进行集中的认证、审计、授权、账户管理平台。
- 对执法数据全程端到端的加密，从终端到数据中心，数据不落地，保证安全性。
- 操作透明化，对用户无感知；
- 与应用的兼容好，与现有系统进行集成极少开发工作。
- 对执法终端上多个 APP 实现一个入口、一个门户、一次认证、全网漫游，避免重复注册、重复认证、重复授权现象，最大化提高操作便利性。

信安世纪智慧监狱移动执法安全解决方案为某省监狱管理局移动执法工作提供了合法有效的数字证书，在提升执法部门的工作效率和服务水平的同时，保障了移动执法过程的合法性，完美的解决了“安全”和“移动信息化”的矛盾，在提供良好应用体验的同时也保证了移动执法工作的安全，彻底的解决了移动执法“最后一公里”的数据、应用的安全问题。