面向强监管行业的5G三重安全防护技术研究

Research on 5G Triple Security Protection Technology for Strong Regulatory Industries

李雯雯[1],吴　博[2],陈　丹[3],肖　羽[3],刘宏伟[1](1. 联通数字科技有限公司,北京 100031;2. 中国移动通信研究院,北京 100045;3. 中国联合网络通信集团有限公司,北京 100033)

Li Wenwen[1], Wu Bo[2], Chen Dan[3], Xiao Yu[3], Liu Hongwei[1](1. China Unicom Digital Technology Company Limited, Beijing 100031, China; 2. China Mobile Research Institution, Beijing 100045, China; 3. China United Network Communications Group Co., Ltd., Beijing, 100033, China)

摘　要:

针对公检法司监等政务行业、涉密军工企业对移动办公的需求,从网络、隧道、数据3个层面为5G专网构建三重安全防护体系,使5G专网更加灵活、便捷、安全、可靠。同时,针对不同办公区域弱、中、强的管控需求,提出一种全面、普适的融合组网方案及终端切换方案,解决了移动警务网络部署及手机管控的难点,消除政企客户对5G专网安全性的顾虑,满足国家对于5G电子政务外网的建设要求。

关键词:

5G;专网;移动办公;安全;管控

doi:10.12045/j.issn.1007-3043.2025.02.014

文章编号:1007-3043(2025)02-0077-06

中图分类号:TN915

文献标识码:A

开放科学(资源服务)标识码(OSID):

Abstract:

In response to the demand for mobile office in government industries such as public security, procuratorial, judicial, supervisory, and classified military enterprises, it constructs a triple security protection system for 5G private networks from three levels: network, tunnel, and data, making 5G private networks more flexible, convenient, secure, and reliable. At the same time, aiming at the weak, medium, and strong control needs of different office areas, it proposes a comprehensive and universal integrated networking solution and terminal switching solution, which solves the difficulties of mobile network deployment and mobile phone control, eliminates the concerns of government and enterprise customers about the security of 5G private networks, and meets the national requirements for the construction of 5G e-government external networks.

Keywords:

5G; Private network; Mobile office; Security; Control and management

引用格式:李雯雯,吴博,陈丹,等. 面向强监管行业的5G三重安全防护技术研究[J]. 邮电设计技术,2025(2):77-82.

0 引言

随着移动终端的普及和移动通信技术的不断发展,便捷、灵活的移动办公成为政企行业不可或缺的工作方式之一。但移动办公的开放性和无线连接的脆弱性增加了安全风险,手机系统后门、重要数据采集、通话及信息监听成为了信息窃密的主要手段。网络安全形势日趋严峻,网络攻击威胁上升,事故隐患易发,亟需从网络承载、传输通道、终端数据等方面全方位加强防范。

为了响应国家的政策要求以及满足政务外网新兴场景的业务需求,2022年6月,国务院发布了关于加强数字政府建设的指导意见,这是国家层面第一个关于数字政府建设的纲领性文件,其中明确要求“强化电子政务外网服务功能,提高电子政务外网移动接入能力”。国家发改委在《“十四五”推进国家政务信息

收稿日期:2025-01-06

化规划》[1]中也明确提出,要“提高电子政务外网移动接入能力,探索5G、区块链等新技术在政务外网领域的应用”。2024年3月6日,国家电子政务外网管理中心发布了《国家电子政务外网5G专用网络接入规范与安全要求》[2]标准的征求意见稿,基于运营商的5G网络基础设施,为国家电子政务外网构建5G专用网络,可显著提高政务外网的泛在接入能力和移动接入能力,延伸政务外网的覆盖范围,满足移动办公、移动执法、应急通信、偏远接入、物联感知、专网融合等场景下的网络接入。

有了国家层面的明确要求,地方上迅速跟进,广东、江苏、四川、福建等都将“依托5G等信息基础设施,规划建设无线政务专网”纳入《十四五规划》,提出要将5G技术应用在政务外网中,提高政务外网移动接入能力。由此可见,“提高电子政务外网移动接入能力”是普遍的政策要求,而将5G技术应用在电子政务外网领域是普遍的技术趋势。

针对公检法司监、军工等特殊行业强监管客户,5G网络不仅旨在提升政务外网的移动性和便捷性,更重要的是不能降低现有电子政务移动办公系统的安全等级。在《国家电子政务外网5G专用网络接入规范与安全要求》标准中,5G政务外网的安全技术框架涉及3个方面:终端、5G专用网络和安全接入区(见图1)。

图1 5G政务外网安全技术框架

1 三重安全防护体系

基于5G政务外网安全技术框架,本文从网络层面、隧道层面、数据层面阐述5G专网三重防护体系(见图2),满足政企客户对移动终端和物联网设备统一接入、管理和控制的需求,为5G专网建设一套健康、有序、安全、灵活的保障机制,消除政企客户对5G专网安全性的顾虑。

1.1 网络安全

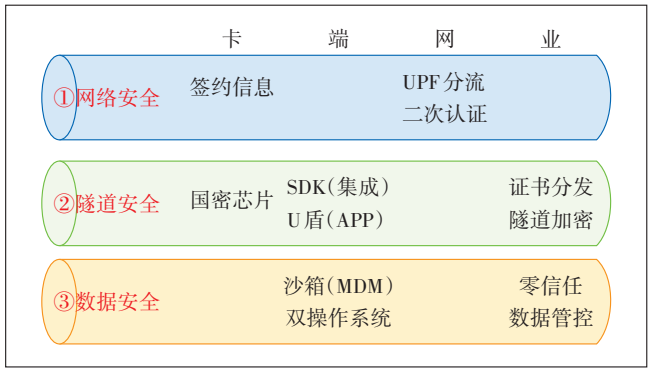

图2 三重安全防护体系

与普通2C公众业务相比,2B业务具有更高的安全保密、自主可控需求。5G终端通过大网AKA主认证后并不能直接与企业内网业务系统建立连接,而是通过业务相关的信任状对5G终端进行二次认证,并在认证通过的情况下才允许5G专网为用户建立与企业内网业务系统间的通信链路,从而提升对企业内网业务系统的保护[3]。

DN-AAA是3GPP标准中定义的网元设备,主要基于EAP框架实现5G专网接入认证。SMF网元在建立用户面数据通道时,将根据专用DNN签约信息决定是否发起二次认证。SMF网元向DN-AAA设备发出认证消息,并建立5G终端与DN-AAA设备之间的认证通道。5G终端和DN-AAA设备之间经过若干次EAP-Request/EAP-Response消息交互,最后由DN-AAA设备向5G终端发送认证结果。二次认证通过之后,5G核心网将为终端建立到企业内网的连接[4]。5G网络二次认证示意如图3所示。

1.2 隧道安全

5G终端完成专网接入二次认证后,为了确保网络

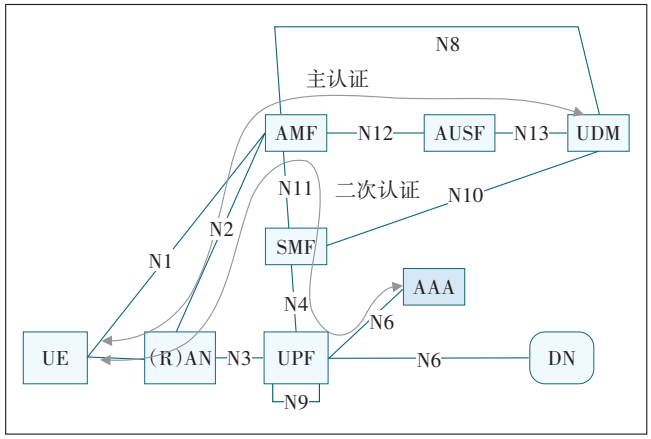

图3 5G网络二次认证示意

传输通道的安全性及完整性，在5G终端中使用带安全芯片的国密SIM卡，以SIM卡安全芯片为载体和可信任根[5]，通过调用移动通信网络特有的通用认证机制（General Boot strapping Architecture，GBA）能力[6]，将企业所需的数字证书通过空口安全可信地分发至SIM卡安全芯片内，从而对5G终端的用户身份进行双向认证。证书认证通过后，在5G终端与安全接入网关之间建立国密TLS隧道，对所有在隧道中传输的数据进行端到端加解密，从而为企业员工个人手机、便携机（笔记本电脑、PAD等）提供身份认证、行为确权、安全存储、传输加密等安全应用服务。国密传输安全架构如图4所示。

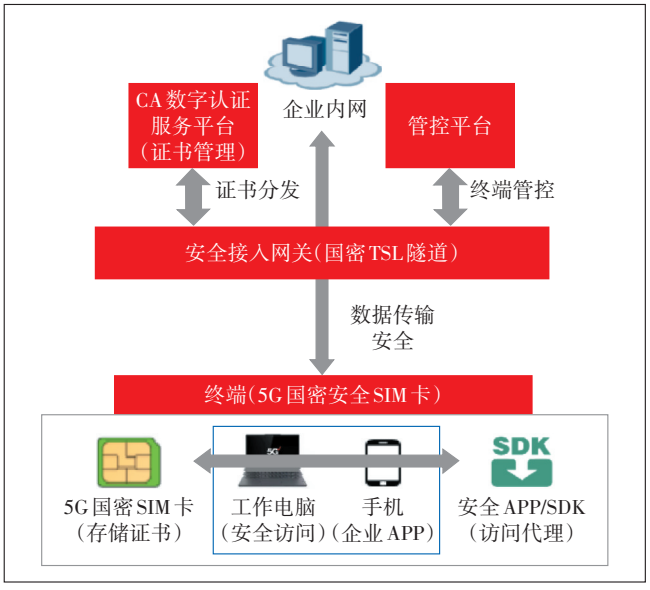

图4　国密传输安全架构

根据不同的应用场景，国密SIM卡集成了多类型CA数字证书（如X509、C-V2X、UID等），以满足不同行业不同类型终端的认证需求[7]。国密SIM卡支持2种证书分发方式。

a）通用认证安全。以软件SDK形式适配不同类型终端，通过互联网通道将证书分发至终端。

b）GBA认证安全。调用5G网络GBA能力，通过空口按需在线分发证书或关键数据。

1.3 数据安全

在5G终端完成二次认证、建立国密传输隧道后，由于终端自身普遍安全防御水平较低，特别是企业员工个人手机既处理办公，又连接互联网，企业数据中心的防护设备很难抵御VPN远程接入隧道中的威胁，也很难防范员工个人上网行为可能导致的违规访问、企业数据泄露、内网病毒攻击等风险。

为了补齐端侧安全管控能力，需要从移动设备、网络接入、身份管理、移动应用、硬件外设多个方面进行全方位的安全保障，并采用不同的空间隔离技术，将个人域与工作域区分开[8]。

a）针对自带设备办公（BYOD）场景，在终端上安装沙箱APP，在沙箱中运行的应用程序只能访问自己的本地内容，而不能访问其他应用程序的文件目录结构[9]。这种逻辑隔离机制可以有效防止应用程序之间的数据泄露和恶意攻击，从而提高手机系统的安全性。

b）针对公检法司监、军工等特殊行业强监管客户，定制主流终端支持双操作系统，允许用户在工作系统中处理工作事务，而在个人系统中处理个人事务，从而实现个人域、工作域的物理隔离，隔离程度更高，并提供政企工作域内运行环境的安全防护。

2 强监管安全方案

2.1 融合组网模式

根据网络资源的部署方式，5G专网一般可分为5G虚拟专网、5G混合专网、5G独享专网3种。不同行业对5G专网的部署模式需求不同，以公安、监狱等移动执法专网为例，根据5G终端使用场景，可划分为个人区、办公区、监管区3类（见图5），相关安全要求如下。

a）个人区。为非监管区、非办公区（如在家或出差途中）建设5G虚拟专网，5G终端签约通用DNN（如3gnet），业务数据通过运营商公用基站接入Internet，访问微信、百度等互联网应用。

b）办公区。为监管区外的办公区（如园区、办公楼等）建设5G混合专网，下沉专享UPF。5G终端签约专用DNN，通过UL CL、DNN等技术将访问政务外网的数据分流至专享UPF[10]，根据专用DNN签约信息，先后通过DN-AAA二次认证、国密证书认证后，访问政务外网相关应用。

c）监管区。为监管区内（如看守所、狱所等）建设5G独享专网，部署专用基站、专用承载，下沉轻量核心网（包括用户面和控制面），在专用基站上配置特定用户白名单，只有通过二次认证的移动执法终端可接入，其他公众移动通信用户无法接入专网。同时，为禁止监管区内服刑人员违规携带手机与外界通信，需部署信号屏蔽系统，屏蔽监管区域内所有违规手机信

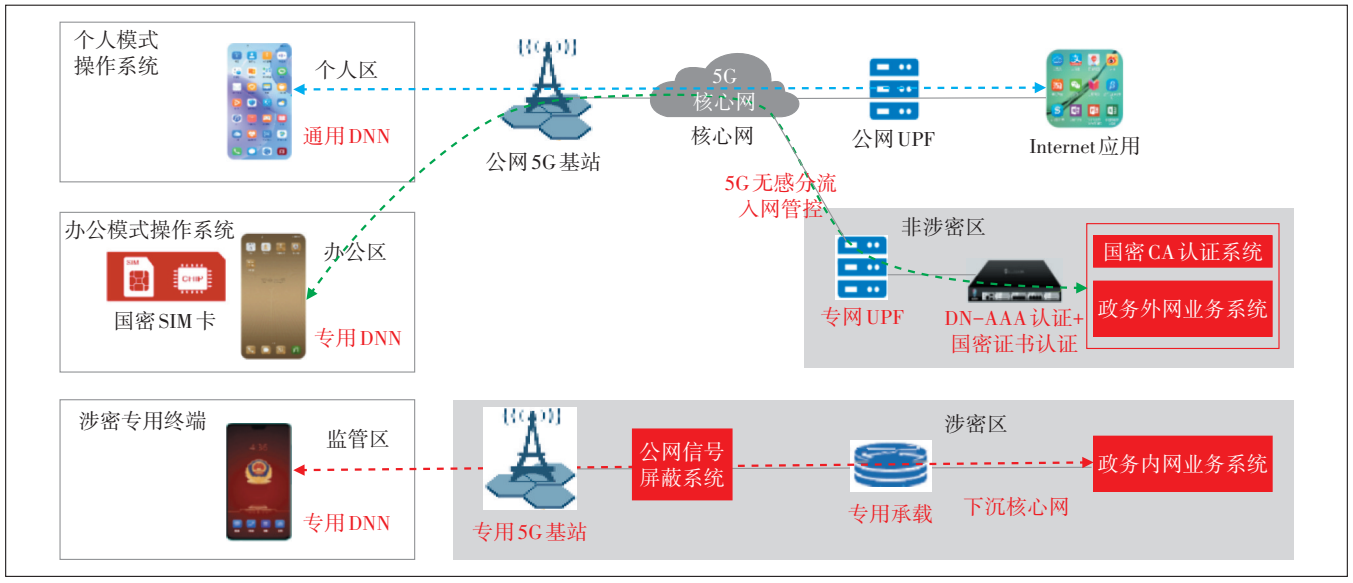

图5　不同区域的融合组网架构

号，并对监管区内所有违规手机进行行为及信息侦测[11]，从而满足监管区内高安全、强隔离、严管控等定制化建网需求。

2.2 终端状态切换

移动执法专网分区建设后，还需要根据5G终端使用场景，设置个人模式、办公模式、监管模式3种模式，并根据场景自动进行状态切换。

a）个人模式。为个人正常使用、弱管控模式，不改变个人原有使用习惯，用户可自行安装互联网应用市场下的合法软件，电话通信、其他终端功能均可正常使用。后台管控平台不对私人数据进行任何控制，仅推送办公消息，禁止用户私自升级、刷机，并按需对终端进行远程定位。

b）办公模式。为移动办公的中等管控模式，通过沙箱访问专有应用市场，移动办公类APP由后台管控平台通过专有应用市场推送安装，用户仅可访问指定已发布应用，仅可通过安全浏览器访问指定链接，并对即时通信、浏览器、输入法等应用程序进行网址黑名单、关键字词过滤等。

c）监管模式。为特定业务开启的强管控模式，一旦进入监管区，自动强制终端锁定至安全桌面状态，仅可访问专用应用市场推送安装的专用APP，同时根据策略限制终端通信能力、禁止调取系统设置、屏蔽硬件外设等。如仅允许与全局移动执法终端、局内固话通信，不能主动拨打外部电话，不能连接除监管区移动执法专网外的其他任何网络。屏蔽Wi-Fi、蓝牙、热点等通信能力。禁止调取照相机、录音机、投屏等系统自带应用进行拍照、录像、录音、截屏、录屏、投影等。

上述3种模式需匹配3类场景实现手动或自动切换，一般有如下3种切换方案。

a）手动切换。手机桌面有“一键切换”按钮，由用户自行判断，在政府办公园区外切换至个人模式，在政府办公园区内切换至办公模式[12]。若要强制切换，需有对应的纪律手段保障。

b）NFC技术。在政府办公楼入口放置NFC门禁刷卡机，并与后台管控平台打通[13]。用户进入办公楼时，需用手机刷开门禁，通过身份验证后，后台管控平台推送指令，强制由个人模式或办公模式切换至监管区模式。安全桌面一旦触发无法强制退出，即使通过强制关机方式关机，重启后仍然恢复至安全桌面。

c）时间地理围栏。基于GPS或TAC[14]、Cell_ID[15]等运营商网络参数创建时间或地理位置的管理策略，并与后台管控平台打通。当移动终端处于某段时间或某个地理位置范围时，自动开启控制策略，触发安全桌面。运营商网络参数真实可靠，可避免GPS定位信息被篡改。

3 典型案例分析

某地方政府的“X政通”APP应用，面向全省5万多台移动终端（手机、PAD等），提供轻应用、大平台、富生态的统一政务协同门户。“X政通”工作场景复杂，涉

及公网区（Internet）、非涉密办公区（政务外网）以及涉密办公区（政务内网）3类场景的多次切换。当前该局工作人员配备2台手机，1台仅处理涉密业务，一般通过纪律手段对涉密手机进行严格管控（如仅允许在涉密区使用涉密手机，不允许外带），另外1台在公网区、非涉密办公区混用，安全防护不足，易被从公网区攻破。同时，非涉密办公区基于公网VPN拨号不安全、不便捷、体验差，运维工单中1/5为VPN相关问题，如VPN登录不上、VPN频繁重复连接或断开连接、VPN开视频会议卡顿、VPN密码忘记等。

当该局工作人员在公网区、非涉密办公区访问“X政通”APP应用时，首先需要在移动终端上安装VPN客户端，再通过拨号的方式在Internet上建立VPN隧道，经过VPN网关进行负载均衡，最后访问非涉密数据中心（见图6）。现有使用模式下，“X政通”APP应用与Internet应用无差别，存在一定安全隐患。

根据目前纪律要求，不允许携带个人终端进入涉密区，也不允许涉密终端带出涉密区。因此，当该局工作人员进入办公楼5层涉密区时只能处理涉密业务，无法接收办公业务推送消息、处理办公业务，进入一种“失联”状态，影响工作效率。

在非涉密机房部署下沉式专享UPF和三重安全管控系统（包括DN-AAA系统、国密认证加密系统、MDM终端管控系统），将网络升级为5G随行专网（见图7）。当该局工作人员在省外出差时，无需在移动终端上安装VPN客户端，可直接通过专用DNN、通用DNN手动切换的方式分别访问“X政通”APP应用、Internet应用。当该局工作人员位于省内时，网络侧开启UL CL分流策略，可实现“X政通”APP应用、Internet应用的无感分流。改进的使用模式通过双DNN、UL CL等技术实现了“X政通”APP应用与Internet应用的逻辑隔离，同时针对“X政通”APP应用，通过专网二次认证、国密认证及数据加密确保了内网访问安全。

当该局工作人员进入办公楼5层涉密区时，在一定程度上放宽纪律要求，允许携带个人终端进入涉密区。MDM终端管控系统结合NFC、时间地理围栏等技术，强制禁用个人模式、使能涉密相关应用权限，工作人员可通过“一键切换”按钮，在办公模式与监管模式之间进行切换。因此，工作人员在涉密区既能处理涉密业务，又可以接收办公业务推送消息、处理办公业务，提升了工作效率。

4 结束语

随着移动办公需求的日益增长，传统Wi-Fi/VPN/4G VPDN通信方式，已无法满足不同行业、不同场景连接易、体验优、高可靠的内网访问诉求。5G专网可

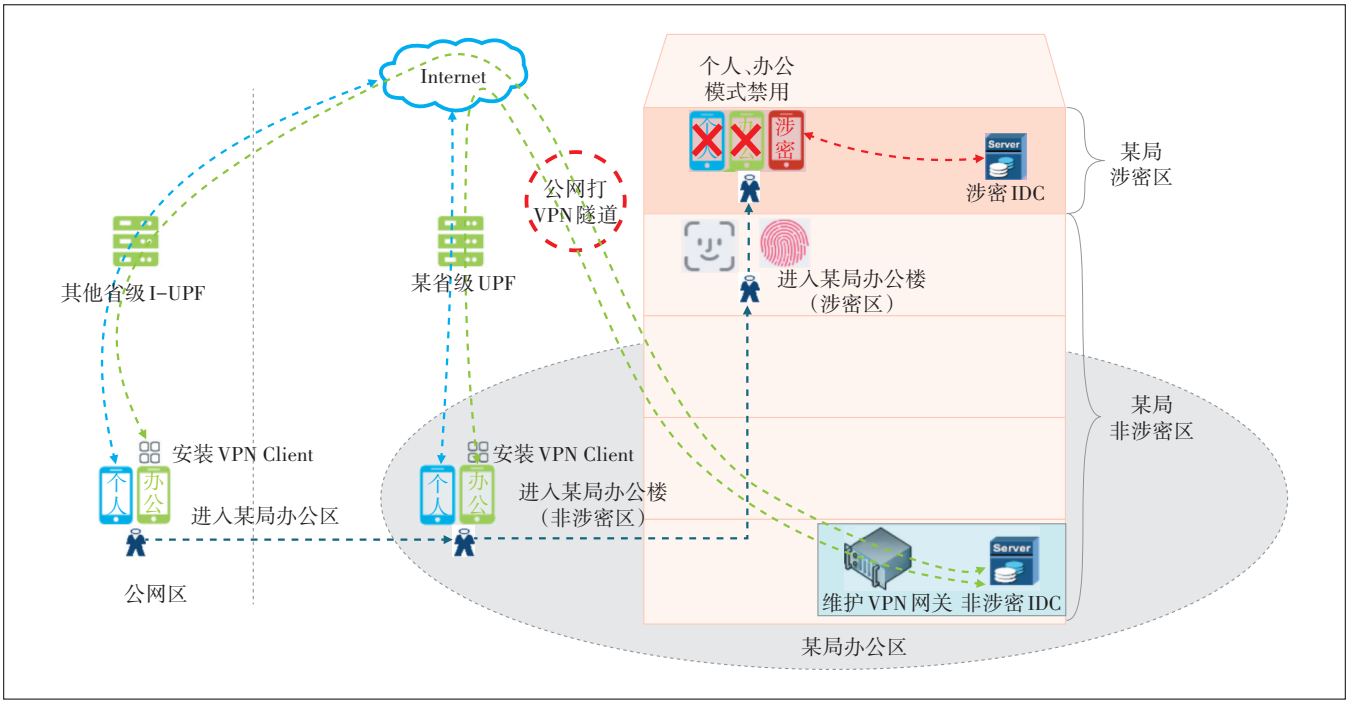

图6　“X政通”APP使用模式现状

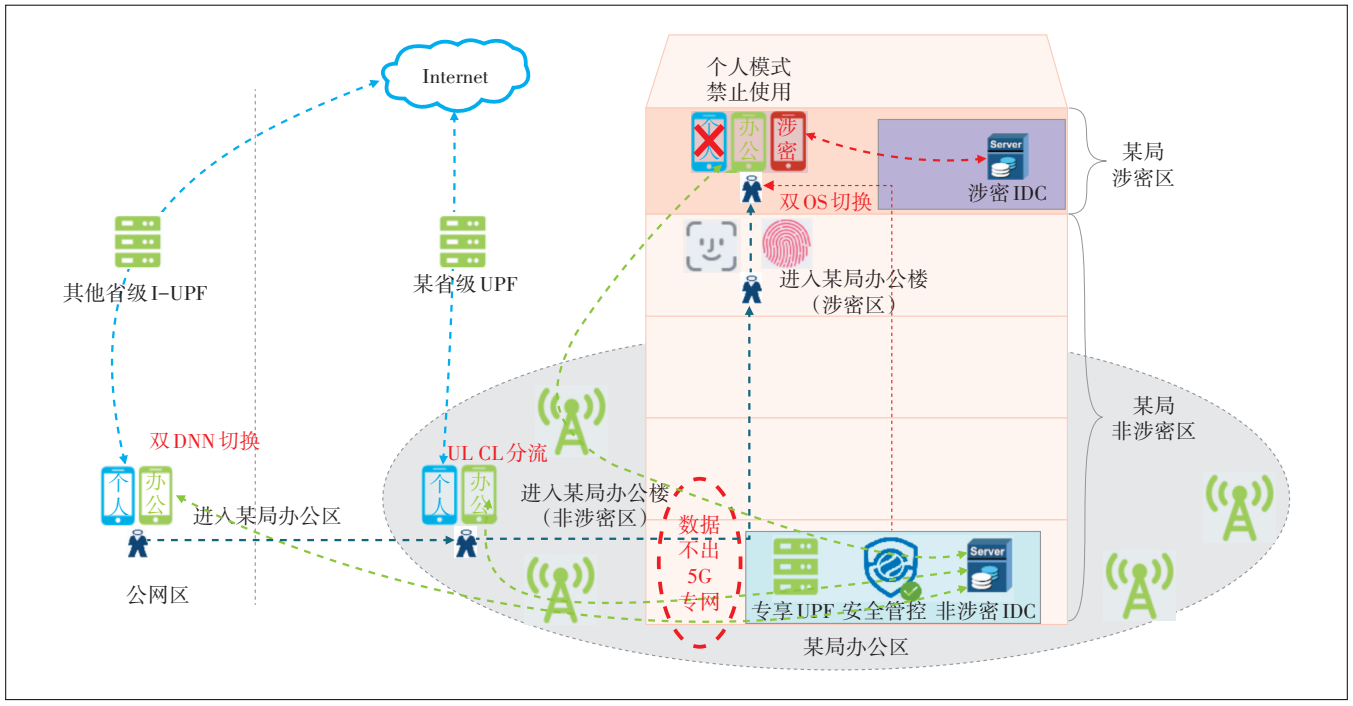

图7　改进的“X政通”APP使用模式

显著提升终端泛在接入能力、移动接入能力、便捷访问能力，本文通过构建三重安全防护体系，从网络、隧道、数据3个层面加强终端安全管控能力，满足政企客户对移动终端和物联网设备统一接入、管理和控制的需求。同时，本文针对公检法司监、军工等特殊行业强监管客户，提出了个人区、办公区、监管区融合组网方案，以及终端个人、办公、监管3种模式特征及状态切换方案，对公安、监狱等移动执法专网的建设及警务定制终端的管控有实际指导意义。

参考文献：

[1] 国家发展改革委. 国家发展改革委关于印发《“十四五”推进国家政务信息化规划》的通知[EB/OL]. [2024-06-30]. https://www.gov.cn/zhengce/zhengceku/2022-01/06/content_5666746.htm.
[2] 国家电子政务外网管理中心. 国家电子政务外网5G专用网络接入规范与安全要求[Z]. 2024:10-13.
[3] 王建英,吕俟林,许建明. 可应用于5G网络的垂直行业二次认证方法浅析[J]. 通信技术,2020,53(10):2538-2542.
[4] 董芸,何余锋,王菲,等. 基于DN-AAA的5G专网接入安全管控方案研究及应用[J]. 信息安全研究,2023,9(8):784-791.
[5] 陈凤. 基于5G国密NFC卡的数字身份认证体系构建及应用研究[J]. 百科论坛电子杂志,2022(3):233-235.
[6] 李佩源,刘建伟. 基于超级SIM的5G端云安全体系架构与关键技术[J]. 中兴通讯技术,2023,29(1):13-19.
[7] 任亚梅,李炜. 基于GBA的认证鉴权流程的设计与实现[Z]. 中国科技论文在线,2010.
[8] 赵思岩,邹智. 移动终端管理(MDM)浅析[J]. 黑龙江科学,2014,5(9):254.
[9] 李彬. 基于Android沙箱的软件行为分析系统的设计与实现[D]. 北京:北京邮电大学,2012.
[10] 李雯雯,蔡庆宇,赵元,等. 基于5G专网的跨域漫游分流技术研究[J]. 邮电设计技术,2023(3):27-34.
[11] 郑志超. 无线电信号屏蔽工作原理及发展[J]. 科技展望,2016(25):116.
[12] 田斌,张小娟,周倩倩,等. 基于NFC技术的门禁系统设计[J]. 电子世界,2014(22):21-22,23.
[13] 梁怡兰. 无线通信基站定位技术研究与应用[J]. 大众科技,2018,20(3):5-7.
[14] LI W W,YAN M,CHAN C A,et al. An area restriction scheme based on TAC control policy for 5G private network[C]//2023 IEEE 11th International Conference on Computer Science and Network Technology (ICCSNT). Dalian:IEEE,2023:85-89.
[15] 朱时清. 公安移动警务应用研究[D]. 成都:电子科技大学,2011.

作者简介：
李雯雯,高级工程师,硕士,主要从事5G核心网安全技术研究工作;吴博,高级工程师,硕士,主要从事Android系统开发及大数据研究工作;陈丹,高级工程师,博士,主要从事5G随行专网分流技术研究工作;肖羽,高级工程师,硕士,主要从事5G政务专网认证技术研究工作;刘宏伟,高级工程师,硕士,主要从事5G智能运维技术研究工作。