摩石观察

密码是保障网络安全的核心技术和基础支撑，在维护国家安全、促进经济社会发展、保护人民群众利益中发挥着不可替代的重要作用。“云物移大智”的蓬勃发展，5G、智慧城市、互联网＋政务服务的全力推进，离不开用密码技术来保障网络安全、保护数据安全、保证网上诚信。实现网络安全需要密码学与其他学科深入合作，需要密码产业与其他产业的深度融合，需要产学研管用的真诚协作，更需要全社会共同传播密码知识与政策、研究密码应用技术、推进密码应用方案。

为激浊扬清，构建以密码技术为核心、多种技术相互融合的新网络安全体系，推进密码技术科学规范应用，长期深耕于信息安全一线的卫士通公司凝聚了一批国内顶尖的密码专家于2016年建立了摩石实验室。依托密码基础理论，探索密码创新实践，解决密码应用难题，培养密码专业人才，摩石实验室致力于让密码技术更好地服务于网络强国、数字中国和智慧社会。

本着共同的愿景，《信息安全与通信保密》杂志社与摩石实验室精诚合作，专门开辟《摩石观察》栏目。立足于密码本真，反思密码实践，《摩石观察》将以密码人的细致严谨叩问密码创新的真理之门，为广大读者了解、认识、掌握、使用密码技术提供准确规范的参考依据；同时我们期望以密码会友，与理想作伴，热忱邀请有志之士共同探索密码理论与应用的最佳实践，为推动金融等重要领域密码应用与创新发展而奋斗。

构建智慧城市密码保障体系 推动密码在智慧城市中的应用发展

张远云[1]，董贵山[2]
（1. 卫士通信息产业股份有限公司，北京 100070
2. 中国电子科技集团，北京 100102）

[摘要] 面对国内如火如荼的智慧城市建设过程中普遍存在的“重业务、轻安全”的问题，本文认为网络安全和智慧城市的信息化建设应是“一体之两翼，驱动之双轮”，在智慧城市建设中，必须同步规划、同步建设、同步实施、同步运行，才能实现智慧城市的健康发展。基于此，智慧城市的网络和信息安全迫切的需要商用密码发挥更大的作用。本文首先分析了国内智慧城市密码应用的现状和发展的主要问题，并提出打造以密码为基石，以智能安全中枢为引擎的智慧城市安全体系，保障智慧城市整体安全。

[关键词] 智慧城市安全；密码；商用密码
[中图分类号] TP309　　[文献标识码] A　　[文章编号] 1009-8054（2019）05-0056-07

0 引言

当前，智慧城市建设工作如火如荼地全面铺开，国内已经有超过500个城市在《政府工作报告》或“十三五”规划中提出或正在建设，随着传统网络和信息安全威胁逐步渗透入智慧城市的建设过程中，网络和信息安全工作亟待全面跟进。

智慧城市建设发展离不开信息化发展，现有的智慧城市建设“重业务、轻安全”的做法普遍存在。习总书记指出“没有网络安全就没有国家安全，没有信息化就没有现代化”。我们应该认识到：没有网络安全，智慧城市建设发展越快，造成的危害可能就越大；没有智慧城市和信息化的发展，经济社会发展将滞后，网络安全也难以获得发展，因此，网络安全和智慧城市的信息化建设是相辅相成的，是“一体之两翼，驱动之双轮”,在智慧城市建设中，必须同步规划、同步建设、同步实施、同步运行，才能实现智慧城市的健康发展。

1 国内智慧城市密码应用现状

智慧城市是一个复杂的巨型系统，包含了物联感知、数据汇聚与共享、政务协同、惠民服务、城市公共设施管理、城市监管与科学决策等方方面面的应用，其安全保障需求也更加复杂。当前密码技术在智慧城市局部的一些网络信息系统发挥了数据保护、实体认证、签名验签等作用，同时国家也出台了部分密码标准规范，但总体来说，智慧城市密码保障依旧缺乏完整、规范的体系规划，密码应用广度和深度亟待提升。

为此，国家密码管理局于2017年对广东、四川、云南等7个省市推进政务云密码应用示范的要求，期望形成密码应用的范例，对以政务云为基础的智慧城市实施全面的网络和数据安全保护，以改变智慧城市建设中商用密码应用不足且缺乏规范指导的问题。

在物联感知方面，智慧城市需要海量的物联传感器和终端，实现城市感知功能，特别是5G技术进一步促进万物互联，需要实现实体可信、行为可控、数据可管等新型智慧城市的安全目标，迫切需要商用密码发挥更大的作用。

2 国内智慧城市密码应用发展的主要问题

当前，国内智慧城市密码应用推进过程中存在很多问题。具体主要表现在以下几个方面。

2.1 智慧城市密码应用和测评相关规范缺乏

国家下发了智慧城市建设的相关要求以及信息系统等级保护等通用规范，但在智慧城市依托的云计算、大数据、物联网和城市公共设施的安全和密码应用、系统测评等方面缺乏相关的标准规范指南。

2.2 智慧城市安全和密码应用顶层设计不足

在国内一线及部分二线城市、省会城市都对智慧城市的建设进行了顶层规划和方案设计，主要集中在物联感知、城市公共设施智能化和政务惠民应用方面，但对密码应用没有体系化的顶层设计牵引。

2.3 智慧城市密码应用产业支撑能力不强

现有密码技术和产品不能完全支撑智慧城市的安全需求，在物端的轻量级密码应用、城市公共基础设施的密码应用、城市高带宽融合

通信网络的密码应用、跨领域数据安全汇聚和共享交换等方面的需求尤其突出。

2.4 智慧城市密码管理保障和推进措施不力

国内智慧城市建设尚未严格按照“同步规划、同步建设、同步实施、同步运行” 制定强有力的管理保障和密码应用推进措施，建设方主要按照等级保护的基本要求和管理要求进行安全管理和建设推进，未能结合智慧城市的复杂情况制定针对性的保障措施，并强化多部门、多实体的协同联动。

2.5 智慧城市建设领域主动应用密码意识不够

城市建设方对智慧城市业务建设非常重视，从顶设到建设到运营，对业务投入了大量的资源，但对安全重视不足，通常将通过等级保护这一基本要求作为安全的最终要求，尤其是在海量异构的城市网络空间实体可信、数据全生命周期安全保护、数据隐私保护和安全共享交换、密码应用的态势监管等方面，对智慧城市复杂网络情况下的体系化密码应用主动使用意识不够。

3 构建以密码为基础的智慧城市安全保障体系

智慧城市的健康发展，需要网络安全的保驾护航，在智慧城市的建设过程中，要注意以下几点：

3.1 做好智慧城市安全的顶层设计和整体规划

智慧城市建设是“一把手”工程，要重视安全在智慧城市建设中的作用，在进行智慧城市顶层规划时做好安全的顶层设计和整体规划，避免头痛医头、脚痛医脚以及打补丁式的安全建设模式，强化对智慧城市安全的战略认知，从整体上统筹智慧城市安全需求和资源，总体规划功能完善、结构清晰的智慧城市安全基本框架，通过法律法规、标准规范、组织管理、安全技术、安全基础支撑及服务、人才培养、城市安全综合治理等方面的综合性保障建设，为智慧城市的发展保驾护航。

3.2 防患于未然，重视智慧城市安全建设的合规性

智慧城市建设要从顶层规划开始，相应的顶层规划、设计等必须通过专家评审才能实施。如果没有对安全的细致严格审查、审核，极有可能使智慧城市建设存在安全漏洞，带来极大的安全隐患。所以，在建设前要对智慧城市建设的各种方案进行安全性把关，确保不出差错再进入下一环节。

智慧城市建设完成后，能不能投入运行，要遵循国家相关标准，对智慧城市信息系统进行全面测评和审核认证，特别是智慧城市建设中的“云大物移智”等新技术的应用带来多种多样的安全隐患。只有经过适合智慧城市信息系统的评测技术（如等保、商用密码在智慧城市应用等）与方法，由具有资质的单位进行评测，才能评得客观、评得到位，只有通过这些机构的评测并颁发证书后，系统才可以投入运行，如果没有通过评测就不能投入运行，这是智慧城市建设的底线。

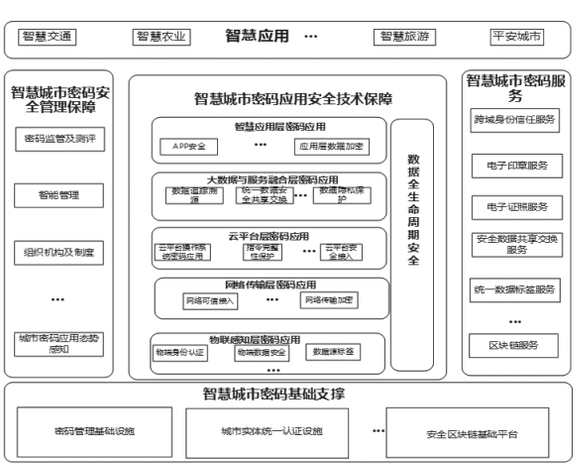
3.3 打造以密码为基石，以智能安全中枢为引擎的智慧城市安全体系，保障智慧城市整体安全

智慧城市是一个体系复杂、应用多样、不断演化的综合性系统，具有复杂、开放、互联的属性。密码技术与安全措施的缺失会导致诸如公共安全和公众隐私等信息受到损害，甚至引起不良社会影响。当前，新型智慧城市建设已上升为国家战略，需要建立健全新型智慧城

市网络安全保障体系，提升自主可控和安全防护能力。而密码是智慧城市安全的核心技术，在智慧城市安全中发挥保底作用，是最基础的防线，是智慧城市安全的基石。

在智慧城市建设中要以密码技术为基础支撑、以数据安全为核心目标，构建整体安全体系；以密码服务为牵引，数据价值为驱动，构建密码安全生态；以可信泛在接入、数据全生命周期保护和密码应用监管为抓手，构建安全秩序。

围绕智慧城市全方位、多层次、多维度的安全保障需求，构建智慧城市密码应用保障体系，通过“统”、“保”、“服”、“管”四个维度实现。



智慧城市密码应用体系

3.3.1 统：即统基础，打通道，建设统一的智慧城市密码基础支撑平台，提供对智慧城市对称 / 非对称密钥、统一身份的管理

建设密码管理基础设施，实现对密钥的统一管理；实现对入网密码设备的状态管理和合规性、有效性监管；实现对密码设备的在线监测、密码设备状态信息和告警等功能。

建设城市实体统一认证设施，提供对城市人、机、物的互信互认、互操作，实现对异构身份的统一识别，形成网络可信身份服务能力；推进“互联网 + 政务服务”密码应用，基于电子认证技术，利用城市实体统一认证设施，实现个人 / 企业 / 法人等的身份认证凭证之间的互通互认，推进标准统一、安全可靠、互联互通、应用方便、高度融合的电子政务密码应用。

建设安全区块链基础平台，提供基于国产密码的区块链安全组件，为城市区块链应用的跨链互操作互认证和监管审计提供支持，为国产密码在区块链领域的应用发展提供支撑。

3.3.2 保：即密码应用技术保障

保障基于商用密码的数据全生命周期的安全，保障智慧城市中关键信息基础设施的安全，从感、传、知（城市大脑的云平台、大数据）、用（各类智慧业务应用、各类用户）几个层次形成一体化的密码应用技术保障体系。

依托轻量级密码技术，提供对物联网多层次的安全防护能力。保证感知数据从感知端到执行端的全通信链路的隐蔽性和安全性。在感知层，重点保护感知终端的物理安全以及数据通信的机密性、完整性和实时性；在网络层，重点实现网络的安全接入，确保不同物联网络间的安全互联、互通和有效隔离；在应用层，重点保护物联网各类应用及业务的安全。

利用基于密码技术的身份认证、访问控制、授权管理、数据加解密、可信计算、密态计算、密文检索、数据脱敏、数据分级分类、数据标签等技术措施，构建数据产生、采集、存储、传输、分析、应用、安全交换共享、数据隐私保护等安全为一体的智慧城市密码应用安全技术体系，解决隐私泄露、数据源不可信、身份仿冒、可用不可见、数据无法追踪溯源、身份

不统一等风险下的身份识别、使用处理权出让下的数据保护、数据安全共享交换、数据滥用等问题，满足智慧城市下的数据基础资源防护、组织和共享防护、计算和分析防护、应用和服务防护等安全需求。

3.3.3 服：为智慧城市提供统一的密码服务

基于区块链、弹性密码防护技术，在城市公共基础设施、天地一体融合通信网络、计算设施、数据服务以及各类业务应用等多层次多领域提供基础的密码、安全及信任服务，将密码应用安全体系融入整个智慧城市的网络安全保障体系之中，通过密码支撑能力服务化，打造数据全生命周期保障能力、网络传输保障能力、数据安全感知能力、统一身份识别能力、数据防泄漏能力，为智慧城市的长远发展提供安全保障。

基于密码基础设施，建设统一信任服务平台，为智慧城市的用户、设备、应用、组织等实体提供分级认证授权、责任认定、电子印章、可信时间等可信安全服务。在智慧城市的人、设备、应用、组织等海量实体间建立信任传递关系，对实体进行身份管理，明确主客体之间的身份，对网络资源的访问和使用进行身份认证和权限管理，实现资源的受控访问和授权管理，对主体行为进行全程取证，确保身份可识别、行为可追溯、责任可界定，解决智慧城市中跨域和跨平台应用带来的用户复杂多样、权限模糊，物联网海量设备接入带来的数字身份管理困难、节点身份不可信、大数据环境中数据权责难以界定的问题。

打造城市密码资源服务平台，面向金融及重要行业领域为核心的业务在传输加密、存储加密、隐私保护、签名验签等方面的迫切需求，提供资源池化的密码运算服务，为智慧城市提供按需获取各种密码应用服务，以此筑牢智慧城市的业务安全底线。

建设统一密码应用监管平台，以智慧城市密码设备的合规使用、密码应用情况的有效掌控、密码服务的安全可靠为核心，对城市信息系统中应用的密码设备、密码系统以及密码模块的统一监管，包括密码应用总体策略、密码算法的有效性、密钥使用状态、密钥过期以及密钥异常情况等内容的监管，实现对密码应用态势的掌控，保证密码应用的合规性、有效性，使得密码设备、密码系统以及密码模块的使用满足国家密码主管部门的相关要求。

建设数据安全共享交换平台，基于密码技术对数据进行标识，记录所有人、使用人、各实体的数据分级分类等数据属性，利用数据指纹、数据水印等数据特征，并引入区块链，确定数据的权属和流转过程。以数据分类分级安全标签为核心，结合区块链技术的分布式权责界定和访问控制决策，对数据交换共享的全过程实施灵活的安全保护和管控，包括追溯数据的申请、审批、交互、流转等，为数据共享各方提供分级管控、确权确责、数据溯源等功能，确定安全责任人，明确安全责任。

利用基础设施提供的密码支撑服务，面向政务、企业、法人、个人的数据提供脱敏和机密性保护，通过对敏感数据的事前、事中、事后完整保护，实现数据的合规使用，防止主动或意外的数据泄露。由中国电科网络空间安全研究院负责创新或制定数据隐私保护的标准和技术手段；加强智慧城市信息系统开发、部署

等环节的密码安全保障，要从源头开始进行隐私保护，综合采用基于密码的访问控制、匿名化、数据脱敏、去标识化、差分隐私保护、数据挖掘、数据变换、推理控制、安全多方计算、盲签名、身份匿名、K 匿名、数据混淆等技术，对城市的信息系统提供脱敏、密文处理的密码服务能力。

3.3.4 管：即做好智慧城市的密码使用管理、监管和应用安全性评估工作

以网络安全、可靠、稳定运行为出发点，以保障业务应用数据安全为核心，以人工智能 / 深度学习、大数据融合分析、基因图谱分析等技术为基础，打造数据驱动、智能化的城市网络安全管理和指挥中枢，构建数据驱动的智能化城市网络信息安全大脑，统一管理和运营城市网络安全密码系统、平台和应用，形成贯通城市的全网、全维、全方位安全态势感知能力；通过城市网络安全大脑的建设，融合人工智能的主动化、持续化网络安全运营和密码服务保障，构建智慧城市网络安全和密码管理的 " 信息优势、认知优势、决策优势以及行动优势 "，支撑构筑一体化的智慧城市网络安全防线。

成立智慧城市密码应用相关领导小组和工作小组，负责智慧城市密码应用的规划、建设和管理，制定密码应用总体方针政策，检查智慧城市建设中密码技术和产品的使用情况，安全管理制度落实情况，协调处理智慧城市密码应用过程中的重大问题；制定密码应用完整的安全策略与制度体系，包括内外部人员安全管理策略与制度、密码设备及介质安全管理策略与制度、密码安全事件和应急管理策略和制度等策略等，从而明确智慧城市密码应用各个机构、人员的岗位职责，制定密码及其设备的使用管理办法，推进密码应用风险管理机制的建立，使得智慧城市的密码应用管理规范有序、稳步推进。

建立密码监督检查机制，督促规划和重点任务落实，定期检查密码应用和密码安全情况；建立密码安全监测预警和应急处置机制，确保密码安全管理的协同联动和有序高效；构建统一密码监管平台，推进密码管理部门对智慧城市中密码设备、密码资源、服务应用情况的统一监管和态势感知；加强密码应用安全性评估工作，制定信息系统密码应用评估审查制度，完善密码应用评估审查办法；加强密码应用安全性评估及测评工作，将评估结果作为项目规划立项、申报财政性资金、建设验收的必备材料；强化密码使用人员的安全教育，加强安全意识培训，树立正确的网络安全观，提高密码人员的密码使用规范意识和网络安全风险意识，减少违规违法行为的发生。

推进网络安全通报机制、应急响应机制、应急演练机制建设，提升应急管理安全突发事件的制度化响应和规范化处置水平。立足全局、统一规划，以城市关键信息基础设施为依托，通过泛在物联感知技术对虚实环境进行全数据镜像，汇聚城市全域海量异构数据，构建城市规模的物联数据感知平台和大数据汇聚平台，建立城市现实空间与网络空间相互影响、相关渗透、相互映射的整体视图控制机制。

制定并进出立足于本地城市的地方性法律法规、管理规范，约束数据提供方在数据隐私保护的职责，约束数据开发商按照规范进行开发，约束数据使用方依据隐私保护的规范不得乱用、滥用数据，明确各方在智慧城市中对政府、

企业、个人等数据信息的隐私保护，明确对数据泄漏造成严重后果的，按照国家相关法律法规进行处理

4 结语

要加强和规范智慧城市安全保障体系的建设，须以安全技术为手段，以安全管理作保障，以建设和运营为着力点，以合规性为底线，以密码为基石，并由安全基础平台和服务提供支撑，通过智能安全中枢统领智慧城市的安全保障体系，保障智慧城市的整体安全。

智慧城市安全建设不仅要处理好智慧城市安全各维度之间的关系，也要做好公众的安全意识培养，立法规定对公民个人的隐私保护也是重中之重，如何通过智慧城市建设拉动本地信息化、网络安全产业化的发展，智慧城市建设对数据的分级分类如何做、数据如何安全共享交换、对数据的确权确责和追踪也都是要注意的地方，智慧城市既要智慧，也要安全。只有这样，才能保障我国智慧城市建设的繁荣发展，不受制于人，才能满足我国信息化发展的需求。

作者简介

张远云，卫士通总体部副总经理，国家信息中心国信卫士网络空间安全研究院高级研究员，承担信息安全和密码领域的部分国家标准规范的编制工作，长期承担国家部委、省级电子政务网络、智慧城市、政务云等国家重点项目的系统建设方案设计工作。

董贵山，中国电科（CETC）网络安全领域首席专家，国务院特殊津贴专家，中国网安副总工程师，长期承担国家党政信息安全和密码应用领域的装备与系统研制，技术标准制定，系统建设方案设计等工作。

Build Smart City Password Security System, Promote the Application and Development of Passwords in Smart Cities

ZHANG Yuan-yun,DONG Gui-shan

（China Electronics Technology Group Corporation，Bejing 100102，China；
Westone Information Industry INC，Bejing 100070，China）

[Abstract] Facing the widespread problem of "emphasizing business and neglecting security " existing in the process of domestic smart city construction, this article holds that network security and smart city informatization construction should be a strategy of "One Body Two Wings and Two-wheel-drive".During the smart city construction, in order to realize the healthy development of a smart city, it is necessary to synchronize planning, construction, implementation and operation. Meanwhile, the network and information security of smart city urgently need the commercial cypher to play a greater role. This article will analyze the status quo of cypher application in the domestic smart city, as well as the main problems in cypher development, and gives out a proposal of how to ensure the overall security of smart city by creating a smart city security system based on the cypher and intelligent security hub.

[Keywords] Security of the Smart City; Cypher; Commercial Cypher