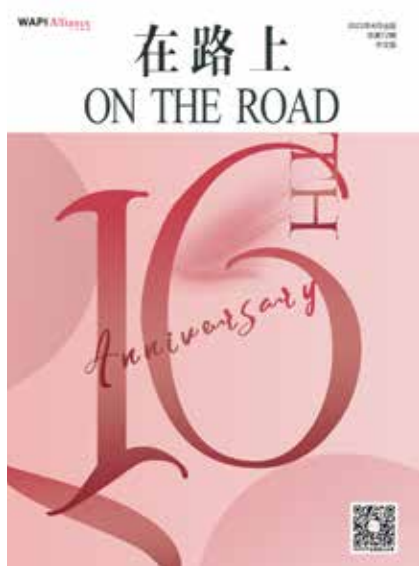


在路上 ON THE ROAD





理事成员：

中国移动通信集团公司
中国电信集团有限公司
中国联合网络通信集团有限公司
国家密码管理局商用密码检测中心
国家无线电监测中心检测中心
北大方正集团有限公司
北京中电华大电子设计有限责任公司
北京六合万通微电子科技股份有限公司
广州杰赛科技股份有限公司
西电捷通公司
深圳市明华澳汉智能卡有限公司

WAPI产业联盟

理 事 长： 曹 军
秘 书 长： 张璐璐

《在路上 On The Road》编辑部

主 编： 张璐璐
编 辑： 周 园 简 练 米 东
王立华 刘剑昕

美术编辑： 周 园

WAPI产业联盟秘书处

会员服务部 标 准 化 部 市场与产业部
测试实验室 综合管理部

联络单位

ISO/IEC JTC1/SC6中国对口委员会
工业和信息化部宽带无线IP标准工作组

联系方式

地 址： 北京海淀区知春路27号量子芯座1608室
邮 编： 100191
电 话： 010-82351181
传 真： 010-82351181 ext.1901
邮 箱： wapi@wapia.org zhouy@wapia.org
网 站： <http://www.wapia.org.cn>
公众号：



庆 Celebration

- 05 庆 WAPI产业联盟成立16周年

媒体聚焦 Media Focus

- 07 通信世界等：
服务安全无线局域网建设 WAPI产业联盟推出终端实体证书管理（CMEE）检测服务
- 08 产业技术创新战略联盟协同发展网：
《2020-2021年度产业技术创新战略联盟活跃度评价报告》在京发布

联盟关注 Alliance Concerns

- 10 WAPI产业联盟被评为A级活跃度联盟
- 11 十部委联合制定产业促进措施 商密行业发展机遇报告
- 19 关于商用密码应用安全性评估的“十问十答”

特别报道 Special Report

- 23 习近平总书记谈标准化工作（摘要）

政经要闻 Policy News

- 26 习近平：加强数字政府建设，完善科技激励机制
- 26 《政府工作报告》：数字化建设要强化网络安全
- 26 中办、国办：发挥社会组织平台作用，促进社会信用体系建设高质量发展
- 27 中央财经委员会中央财经委员会：
要适度超前布局有利于引领产业发展和维护国家安全的基础设施
- 28 两会委员为强化网络安全建言献策
- 28 交通部、科技部：加速新一代信息技术与交通运输融合
- 29 国资委成立科技创新局、社会责任局：
推动中央企业科技创新和社会责任工作高标准高质量开展
- 29 市场监管总局、工信部：建设国家级质量标准实验室 推进产业基础高级化和产业链现代化
- 30 工信部：构建车联网网络安全和数据安全标准体系 支撑车联网产业安全健康发展
- 30 田玉龙：三方面发力 确保工业互联网安全有序健康发展
- 31 国标委：发布2022年全国标准化工作要点 构建高质量标准体系支撑和着力点
- 31 海南省：部署开展商用密码应用示范工作
- 31 蔡奇：推进中关村新一轮先行先试改革，聚焦重点任务

联盟工作 Alliance Work

- 33 联盟永远跟党走把握历史主动 明确“开创”深意
- 35 WAPI产业联盟参加中共北京市中关村社团第二联合党委第二流动党员联合支部委员会组织生活会
- 36 WAPI产业联盟参加“党建红 园林绿”公益植树和红色教育活动
- 37 以实际行动服务中关村世界领先科技园区建设之WAPI产业联盟参加中关村产业技术联盟业务工作会议
- 38 以实际行动助力中关村世界领先科技园区建设之WAPI产业联盟参加“园区行”活动——走进未来科学城
- 39 WAPI产业联盟召开 2022年第一次标准工作及项目组会议（总第121次）
- 42 WAPI产业联盟启动63项团体标准复审工作
- 43 WAPI产业联盟发布《无线局域网产品工程化实现指南》系列 4项团体标准修改单
- 44 WAPI产业联盟《无线局域网系统》系列团体标准 进入报批阶段
- 44 《WAPI规模组网技术规范》团体标准立项
- 45 WAPI产业联盟团体标准《无线网络安全 术语》即将进入征求意见阶段
- 46 华为无线接入点系列产品通过联盟测试
- 46 山东思极无线接入点系列产品通过联盟测试
- 47 南京才华科技UHF智能手持终端通过联盟测试

新成员 New Member

- 48 山东思极科技有限公司加入WAPI产业联盟 协力推动国家电网WAPI建设
- 49 深圳市国电科技通信有限公司加入WAPI产业联盟

成员与市场 Member & Marketing

- 50 数字认证：大众“免费Wi-Fi”暗藏陷阱 民生行业无线应用WAPI才是标配
- 52 MTK发布天玑8000 全线支持WAPI
- 52 新华三连续13年WLAN市场份额第一
- 53 信锐技术助力广西医科大学完成数字化转型升级
- 53 中兴“新支点”国产操作系统 用户均免费使用
- 54 北京科创资源辐射津冀 京津冀实现地区生产总值9.6万亿

产业技术论坛 Industry & Technology Forum

- 55 浅谈《原子密钥建立与实体鉴别》系列团体标准



WAPI产业联盟成立16周年

尊敬的专家、领导和业界同仁，亲爱的联盟成员：

2022年3月7日，WAPI产业联盟迎来崭新的一岁。16岁，你好！

在这个伟大的时代，有一种理想让我们魂牵梦萦，有一种信仰让我们坚如磐石，有一种力量让我们勇往直前……这种理想、信仰和力量，叫做自主可控网络安全。

16年，春华秋实，岁物丰成！WAPI产业联盟既有干劲，也有韧劲，组织百余家成员单位协同创新，WAPI产业链、创新链、供应链扎实壮大。152项国际国家团体标准、190亿芯片产品和多厂商供货环境、成熟的物联网标准化接口和集成化模组、系统完备的测试工具、定制化的联盟公共服务平台，发挥出“既有自主可控技术标准、又有成熟产业和好用产品”的优势，为各行各业开展安全无线网络和信息化建设提供了高效保障。

我们深知，凡是过去，皆为序章。

我们深知，新征程路上，有雪山草地，有星辰大海，有大漠孤烟，有小桥流水……路上皆是风景，脚下充满力量。

而最荣幸是，能继续和您一起，不忘初心，一步一个脚印向前走，一年接着一年干，一起向未来！

WAPI产业联盟

（中关村网络安全产业联盟）

2022年3月

郑海 简练 张 周 米东 张国强 刘剑昕 王华 申富彬

通信世界等：

服务安全无线局域网建设 WAPI产业联盟推出终端实体证书管理（CMEE）检测服务

【编者按】为解决WAPI安全无线局域网规模建设中的数字证书高效集中管理问题，WAPI产业联盟推出了终端实体证书管理（CMEE）检测服务。该服务依据联盟2项团体标准CMEE技术规范和CMEE测试规范开展，已正式纳入《无线局域网鉴别与保密基础结构（WAPI）功能测试项目》扩展功能测试项目中。此事引起了业界和媒体广泛关注。2022年3月31日，通信世界、中国电子报、电子信息产业网、飞象网等媒体对此进行了报道。

以下是通信世界的报道。



日前，WAPI产业联盟测试实验室推出终端实体证书管理（CMEE）检测服务，解决WAPI安全无线局域网规模建设中的数字证书高效集中管理问题。

伴随WAPI安全无线局域网规模建设和应用，需要对大量设备进行管理、运营和维护，这对数字证书管理提出了更高的要求。证书如何便捷的申请和发放，如何安全的传输和使用，成为大规模组网下迫切需要提升和优化的要素。对此，WAPI产业联盟组织西电捷通公司、北京数字认证股份有限公司、无线网络安全技术国家工程研究中心等单位研发了终端实体证书管理（CMEE）技术。

CMEE定义了证书认证系统中实体证书管理的安全操作，包括证书的申请、更新、恢复、撤销、查询、获取等等。通过CMEE可实现用户实时在线申请数字证书，可以通过安全传输通道获取证书，让市场用户更便捷、更安全、更低成本地管理和使用证书。

为服务市场需求，保证不同厂商产品间的证书管理能够互联互通，WAPI产业联盟迅速组织制定并发布了CMEE技术规范 and CMEE测试规范2项团体标准。其中，CMEE技术规范为实体安全连接的建立和数据传输提供了保障，CMEE测试规范为证书管理的工程化实现提供了测试验证依据。更值得一提的是，上述2项团体标准不仅适用于无线局域网，也同样适用于以太网、IP安全网络等等。

在团体标准创制同期，WAPI产业联盟测试实验室开展了CMEE配套测试工具开发和测试能力建设。目前，CMEE测试已纳入到联盟《无线局域网鉴别与保密基础结构（WAPI）功能测试项目》扩展功能测试项目中，随时为产业和市场用户提供测试验证服务。

作为无线网络安全公共技术服务平台，WAPI产业联盟始终坚持技术规范与测试规范协同发展，以技术规范引导和服务市场，以测试规范检验验证产品功能、保障互联互通。因联盟平台的专业性、开放性、中立性，市场用户在WAPI网络建设中，大多采用“委托联盟开展测试”、“采信联盟测试报告”等方式完成设备选型和采购。对有自建WAPI检测能力需求的用户单位，联盟也提供必要的支撑和服务。

部分媒体新闻链接：

通信世界：<http://www.cww.net.cn/article?id=560148>

中国电子报/电子信息产业网：<http://www.cena.com.cn/infocom/20220401/115704.html>

飞象网：<http://www.cctime.com/html/2022-3-31/1614002.htm>



图：WAPI产业联盟团体标准CMEE技术规范与CMEE测试规范

产业技术创新战略联盟协同发展网： 《2020-2021年度产业技术创新战略联盟活跃度评价报告》 在京发布

协发网秘书处 产业技术创新战略联盟协同发展网

2022年4月15日，《2020-2021年度产业技术创新战略联盟活跃度评价报告》发布会在北京召开。科技部成果转化与区域创新司副司长吴家喜，科技部试点联盟联络组秘书长、产业技术创新战略联盟协同发展网理事长单位负责人李新男，中关村国联产业协同创新发展促进中心理事长阮军，产业技术创新战略联盟协同发展网秘书长程学忠和自律机制建设部负责人仲继寿，以及科技日报、光明网、中国网、搜狐科技等新闻媒体代表应邀参加会议。会议由程学忠主持。

产业技术创新战略联盟协同发展网自律机制建设部部长仲继寿报告了《2020-2021年度产业技术创新战略联盟活跃度评价报告》主要内容，本次评价共有107家试点联盟录入了动态数据库信息，其中86家联盟达到评价要求，将各试点联盟活跃度划分为活跃度高、活跃度较高、活跃度一般、不活跃等四个等级，经过综合评价，活跃度高和较高的联盟有57家，达到参评联盟的66.28%，这些联盟在围绕产业链构建创新链、带动产业发展成效、联盟组织机构建设与运行等方面都开展了大量有实效的工作。评价结果显示，活跃度高联盟共35家，占参评联盟的40.69%、活跃度较高的联盟共22家，占参评联盟的25.58%、活跃度一般的联盟共18家，占参评联盟的20.93%、不活跃的联盟共11家，占参评联盟的12.79%。并对2018-2021年连续三个评价期活跃度评价结果进行了综合分析评价，24家联盟连续三年保持高活跃度，表明这些联盟在组织机构建设与运行、产学研深度融合协同创新、引领或支撑产业创新发展等方面取得了突出成效，对全国产业技术创新战略联盟的构建与发展起到了示范带动作用，特评为“A级活跃度产业技术创新战略联盟”。从活跃度评价综合结果可以看出，联盟秘书处运行规范是联盟健康发展的前提和保证；部分联盟在组织协同创新活动方面有待加强；联盟还需通过宣传和示范活动发挥更大作用。

会上，与会领导为获得“A级活跃度产业技术创新战略联盟”代表颁发了荣誉证书。并分别围绕联盟在围绕产业链构建产业技术创新链方面的做法和经验；联盟是如何立足市场需求，建立科技创新、标准研制与产业发展协同机制，探索以科技研发提升技术标准水平、以技术标准促进科技成果转化，服务产业发展模式；联盟在推进产业关键核心技术攻关，解决“卡脖子”技术问题和跨行业跨领域合作方面等新闻媒体关心的问题进行了权威解答。

据李新男介绍，产业技术创新战略联盟作为我国新型产学研协同创新组织形态和国家技术创新工程三大载体之一，是创新共同体的重要组成部分，已列入《“十四五”国家科技创新规划》和新修订的《中华人民共和国科学技术进步法》，将为产业技术创新战略联盟规范发展提供法律保障。

据了解，这是自2013年以来，科技部试点联盟联络组、产业技术创新战略联盟协同发展网对试点联盟开展的第8次活跃度评价。联盟活跃度评价报告为协助政府有关部门了解联盟实际情况、研究制定联盟相关政策，以及科技计划择优支持等方面提供了重要依据和参考；同时也发挥了对联盟的引导和示范作用。本次联盟活跃度评价工作根据科技部成果转化与区域创新司的意见，以联盟动态信息数据库信息为主要依据，综合了各联盟所在行业专家、媒体报道等各渠道反馈情况，经初评、复评、复核会评三个程序形成《2020—2021年度产业技术创新战略联盟活跃度评价报告》。在指标设计方面，主要考虑体现国家政策导向，强化联盟在创新驱动战略中的功能；基于各联盟发展不平衡，兼顾成熟联盟和发展中联盟的实际状态；兼顾开展联盟工作的共性要求和各联盟所属产业的特点和差异性；基于对联盟诚信度的信任，以及信息的可采集性、可比较性。活跃度评价内容主要侧重考核联盟组织机构建设与运行、联盟协同创新活动和联盟带动产业发展成效。

序号	联盟名称	批次
1	新一代煤（能源）化工产业技术创新战略联盟	102
2	农业装备产业技术创新战略联盟	104
3	TD产业技术创新战略联盟	105
4	汽车轻量化产业技术创新战略联盟	107
5	半导体照明产业技术创新战略联盟	110
6	WAPI产业技术创新战略联盟	114
7	闪联产业技术创新战略联盟	115
8	化纤产业技术创新战略联盟	118
9	存储产业技术创新战略联盟	119
10	新一代纺织设备产业技术创新战略联盟	124
11	太阳能光热产业技术创新战略联盟	125
12	木竹产业技术创新战略联盟	129
13	集成电路封测产业技术创新战略联盟	138
14	再生资源产业技术创新战略联盟	154
15	电动汽车产业技术创新战略联盟	212
16	光纤材料产业技术创新战略联盟	215
17	住宅科技产业技术创新战略联盟	233
18	烟气污染治理产业技术创新战略联盟	235
19	航天制造装备产业技术创新战略联盟	304
20	科研用试剂产业技术创新战略联盟	307
21	粉末冶金产业技术创新战略联盟	320
22	花卉产业技术创新战略联盟	341
23	建筑信息模型（BIM）产业技术创新战略联盟	354
24	第三代半导体产业技术创新战略联盟	D106

WAPI产业联盟被评为A级活跃度联盟

日前中国产业技术创新战略联盟协同发展网公布了《2020—2021年度产业技术创新战略联盟活跃度评价报告》，WAPI产业技术创新战略联盟获评为“A级活跃度产业技术创新战略联盟”，并作为典型案例入选《产业技术创新战略联盟典型案例选编（2021）》。案例从自律建设、协同创新、标准制定、平台建设、专利共享、人才培养、国际合作、行业带动等方面，介绍了联盟的经验做法。



当前产业技术创新战略联盟作为我国新型产学研协同创新组织形态和国家技术创新工程三大载体之一，是创新共同体的重要组成部分，已列入《“十四五”国家科技创新规划》和新修订的《中华人民共和国科学技术进步法》。自2013年以来，科技部试点联盟联络组、中国产业技术创新战略联盟协同发展网对试点联盟开展活跃度评价。联盟活跃度评价报告为协助政府有关部门了解联盟实际情况、研究制定联盟相关政策，以及科技计划择优支持等方面提供了重要依据和参考；同时也发挥了对联盟的引导和示范作用。

WAPI Alliance
产业联盟

WAPI 产业联盟

WAPI产业联盟于2006年3月7日经国务院批准成立，是国内首家专注于网络安全且目前最具规模的产业联盟，是国内首家自成立之日起秘书处采用专职人员、不依托任何单位独立运作的新型社会组织和协同创新载体，法人名称为“中关村网络安全产业联盟”。目前，联盟是5A级中国社会组织，国家首批A类产业技术创新战略联盟，国家首批团体标准试点单位，也是国家网络安全防御产业技术基础设施——无线网络安全技术国家工程研究中心的发起单位。

联盟的宗旨是：整合协调产业和社会资源，提升联盟会员在无线网络和网络安全相关领域的研究、开发、制造、服务水平，促进产业健康发展；以国际领先的基础共性技术Tetra和WAPI，带动无线网络和网络安全健康高效发展；发挥联盟的“政、产、学、研、用”链条作用，促进产业群体协同创新、提升综合竞争力。

16年来，WAPI产业联盟立足网络安全和标准化等国家战略，基于市场需求，在无线网络和网络安全领域，组织开展标准化、产业化、商用化、国际化等方面工作，成效显著：在标准化方面，已开展了180余项标准的制修订，为构建最基础最共性的网络安全架构体系提供有效支撑，其中发布（获发布）国际标准（ISO/IEC）14项、欧洲标准3项、国家标准41项、国家军用标准4项、行业标准7项、团体标准87项。在产业化方面，WAPI已经成为全球无线局域网芯片的标准配置，支持WAPI的芯片已达500多个型号，全球累计出货量已超过190亿颗；支持WAPI的移动终端和网络制设备已超过18000款。在服务市场应用方面，除电信运营商公共无线局域网之外，WAPI已广泛服务海关、能源、政务、公安、交通等行业，在这些应用实践中形成了WAPI物联网、WAPI移动互联网、WAPI社会化网络等综合解决方案，有效保护了各行各业的网络安全和数据资产不受侵害，深受市场用户好评。

联盟官网：<http://www.wapia.org.cn>

十部委联合制定产业促进措施 商密行业发展机遇报告

北京商用密码行业协会

【编者按】2022年1月，国家密码管理局联合中央网信办、国家发改委、科技部、工信部、公安部、财政部、国资委、市场监管总局、证监会等十部委联合发布《促进商用密码产业高质量发展的若干措施》（以下简称《若干措施》），文件明确提出，将通过深化需求牵引、创新驱动提升全链条、支持平台建设和完善发展环境四个方面，加快推进商用密码产业高质量发展，切实提升网络空间密码保障能力。本期，节选北京商用密码行业协会发布的《商用密码行业发展机遇报告（2022）》以飨读者。

一、密码产业概况和现状分析

（一）密码产业的构成

1. 密码产业的定义与范畴

按照《密码法》有关规定，密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。

密码产业是指为了保障信息安全，提供加密保护、安全认证相关技术、产品和服务的相关行业总称，主要包含算法与协议的研制、基础算力的软硬件产品生产、与信息化业务场景结合的产品和服务、检测认证、应用安全性评估等各类经济活动。

a) 按照产品功能分类

类别	解释	典型产品
密码算法类	构成密码应用基础的能提供密码运算功能的产品	密码算法实现软件、密码算法芯片等产品
数据加解密类	提供数据加解密功能的产品	加密机、加密卡等产品
认证鉴别类	提供身份鉴别、消息鉴别等功能的产品	动态密码口令、身份认证系统、电子签章等产品
证书管理类	提供数字证书的产生、分发、管理功能的产品	数字证书管理系统产品
密钥管理类	提供密钥的产生、分发、管理功能的产品	密钥管理系统等产品
密码防伪类	提供密码防伪验证功能的产品	电子印章系统、支付密码器、数字水印等产品
综合类	提供上述两种或两种以上功能的产品	统一密服平台等产品

b) 按照产品形态分类

类别	解释	典型产品
密码软件类	指以纯软件形态出现的产品	信息加密软件、密码算法实现软件等产品
密码芯片类	指以集成电路芯片形态出现的密码产品	密码算法芯片、密码SOC芯片等产品
密码模块类	指以多芯片组装的背板形态出现，具备专用密码功能，但本身不能完成完整的密码功能的产品	加解密模块、安全控制模块等产品
密码板卡类	指以板卡形态出现，具备完整密码功能的产品	USB密码钥匙、PCI密码卡等产品
密码整机类	指以整机形态出现，具备完整密码功能的产品	VPN、网络密码机、服务器密码机、签名验签服务器等产品
密码系统类	指以密码形态出现，有密码功能支撑的产品	安全认证系统、密钥管理系统等产品

2. 产业技术链的上中下游

密码产业的茁壮发展，离不开信息技术生态的支撑，密码技术链总体分为上、中、下游环节。上游包括密码算法标准、网络协议及规范等；中游包括网络协议栈实现、软件开发工具链、硬件密码模块和驱动、CPU密码指令集支持等；下游包括基础应用软件与行业应用软件等。

从产业链发展的角度分析，目前居于密码产业链上游的主要为核心元器件和操作系统、核心高端芯片的研发设计；中游主要为整机及终端领域，主要体现在生产自主可控整机和服务器方面；下游主要是软件、系统集成及应用领域，以国密算法支持应用领域，其客户主要为政府、电信、金融、能源、交通、军工等企业级客户和新兴起的个人用户市场。根据需求驱动，关键领域加大了信息安全包括密码相关产品及服务的采购力度，政府、电信、金融、能源、军队等重点行业，教育、电商、交通等新兴行业对信息安全产品、服务的需求强劲，拉动了密码安全市场的整体需求。

3. 国内外密码行业差异

从全球区域分析来看，以美国为主导的北美市场仍然占据全球最大的市场份额。在排名前10的网络安全公司中，美国公司占据了7个席位，表现出强大的国际竞争力。以中国、日本和印度为代表的亚太地区，受益于近期国家安全战略的发布以及日益增长的信息安全需求，市场也呈现出高速发展的态势。

根据全球商用密码产品的分布情况，根据网络联盟安全研究机构NAI Labs的调查统计结果，其标定的1598种密码产品，由全球多家公司生产和经营（美国479家，其他国家543家），分布在至少73个国家。其中，美国国内生产或经营的密码产品有868种，美国以外的39个国家和地区生产或经营的密码产品为730种。

我国密码早先以国家政府部门使用为主，所以是以顶层设计、国家意识为主导。近年来，随着网络空间安全意识增强，我国逐步向商用领域拓展。自2017年至今，我国自主研发的SM2、SM3、SM4、SM9、ZUC等商用密码标准算法已体系化推进成为ISO/IEC国际标准。

（二）我国密码产业初具生态

密码产业已呈现创新发展能力。密码领域的主要科研单位：科学院、北京电子科技学院、三零所、数据所、山东大学、西安电子科技大学、北京邮电大学、武汉大学、上海交大等。密码理论百花齐放，序列密码、分组密码、公钥密码、散列函数、同态加密、多方安全计算等密码算法大量涌现，基于密码技术的身份鉴别、电子签名、访问控制、数据加密、可信计算、密文计算、去标识化等，被用来解决信息的真实性、机密性、完整性、不可否认性等安全问题。

密码法律标准实现体系化发展。截至2021年3月15日，累计发布密码国家标准39项，密码行业标准115项。如今，从顶层设计到法律法规，从行业标准到产业政策的密集颁布，商用密码法律标准已实现自上而下的体系化发展。尤其是《密码法》颁布以来，商用密码检测认证体系建立完善、商用密码应用安全性评估、商用密码进出口管理得以进一步规范和完善，为拓宽密码应用市场提供了有力保障。

关键领域的实战化应用。商用密码产业正处高速发展期，全国电子认证服务机构签发的数字证书，广泛应用于金融、税务、教育、电信、电子商务等领域，产生了重大的社会效益和经济效益。诸如金融、政府、央企、军工、能源等关键领域用户，也都在大幅有序推进基于密码技术的安全服务实战化应用，为国家安全整体建设添砖加瓦。

产业生态体系建设蓬勃健康有序。站在“十四五”新起点，在相关法规政策推动下，各地密码协会纷纷设立，密码应用与创新示范基地、行业密码应用研究中心和产业园区建设蓬勃开展；检测认证体系不断健全，为推动密码科学化规范化管理，促进产业健康有序发展提供了坚实支撑。这必将助推密码技术、产品、应用加速成熟，使其竞争力达到国际领先水平，实现密码“走出去”。

配套支撑体系建设未雨绸缪。产业规模的跨步式快增长，伴随而来的是对支撑体系的需求激增。国家市

场监督管理总局与国家密码管理局联合发布一系列规范性文件，进一步明确商用密码检测认证工作原则、工作机制和实施要求；组织开展商用密码应用安全性评估试点，推进评估标准、技术、机构、人才支撑体系建设。

（三）密码产业的市场分析

1. 市场规模不断扩大

党的十八大以来，商用密码产业进入创新发展、协同发展、高质量发展的快车道，产业规模不断扩大，呈现强势增长劲头。

据赛迪网安所发布的统计数据来看，2018年市场规模总量为283亿元，较上一年增长18.21%；2019年市场规模总量为350亿元，较上一年增长23.67%；2020年市场规模总量为466亿元，较上一年增长33.14%。

随着《密码法》、《金融和重要领域密码应用与创新发展工作规划（2018—2022年）》等相关政策发布，特别是国务院颁布的《“十四五”数字经济发展规划》，提出了数字经济安全体系概念，其中要求加强密码应用安全性评估，要求促进数据加密技术，可见在在实战与合规双重驱动下，密码需求被充分激活，预计2025年我国商用密码规模将超千亿元。

未来，随着国家“十四五”规划等一系列数字化发展战略的实施落地，对商用密码的刚性需求将逐步持续释放，以商用密码产业为代表的网络安全相关产业具有巨大市场潜力和发展空间。

2. 密码行业竞争格局

“放管服”改革进一步深化，商用密码技术推陈出新，密码从业单位数量和规模不断增加。截至2019年底，全国具备商用密码型号证书产品的企业有547家。2020年，《商用密码产品认证目录》颁布后，全国拥有认证商密产品的企业共551家，北京地区企业达到182家，占比超过30%，同期深圳66家、上海41家、杭州17家、天津13家，武汉11家。

从地域分布来看，北京、广州、浙江、上海的企业数量之和占据行业半数以上，北京和广东的商用密码企业最多。从规模体量来看，目前商用密码行业多为中小型企业，营收体量相对较小，行业较为碎片化，每家公司业务集中于少数区域或个别优势行业。未来，随着的行业的发展，商用密码企业正在逐步成长，更加专业化、专精化，并呈现整合趋势。

3. 驱动因素与发展态势

1) 供给侧高质量升级释放产业活力

技术融合催生新的应用空间。随着新基建等基础设施的加速构建，将有数以万亿计的新设备接入网络，5G、人工智能、边缘计算、区块链等新技术进一步与传统产业融合。为了满足我国新基建发展的安全新需求，密码技术、产品和服务都需要前瞻性思考、全局性谋划，加快关键核心技术自主创新，打造高性能密码产

品提速运算效率，落实专业化、平台化的密码服务，实现质量升级、效率提高、服务完善，强化密码安全保障能力。

服务形态不断升级形成良性互动。当前在强劲需求拉动下，密码供给形态正从“以产品为主”演化为“产品+服务”。整个密码产业的供给质量不断提升，让密码能用、好用、用好，形成需求牵引供给、供给创造需求的更高水平动态平衡。

2) 监管侧政策红利推动跨越式发展

从合规需求看，以商用密码应用安全性评估为主要抓手，结合信创的系统化合规将会持续深入。《网络安全法》、《数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》等环环相扣的“法规链”和层层压实的“责任链”，也在持续带动使用密码技术的新需求。在不同角度需求的共同驱动下，实战与合规叠加的需求成为产业发展的关键动力，推动新密码市场加速形成。

结合《中华人民共和国密码法》、《商用密码管理条例（修订草案征求意见稿）》、《促进商用密码产业高质量发展的若干措施》等法律法规，密码新监管可以概括为“一收一放”。“一收”是指在《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知》（国办发〔2019〕57号）、《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（公网安〔2020〕1960号）等制度的推动下，政务、网络安全等级保护、关键信息基础设施安全保护等头部市场明确了密码合规建设风向标。这些政策“收”紧监管力度，拉动合规需求规模，提升合规供给质量；“一放”是指对商业市场落实“放管服”，“放”宽市场准入，充分唤醒密码需求。差异化的市场监管营造了更加公平开放的密码商业环境，有效激活国内密码市场潜力，并鼓励密码产业“走出去”，构建国内大循环为主体、国内国际双循环相互促进的新格局。

二、密码产业挑战与机遇并存，在我国数字经济中发挥重要作用

（一）在数字经济中的作用和意义

“十四五”时期，我国进入数字化发展、建设数字中国的快车道，开启了全面建设社会主义现代化国家新征程。密码作为数字时代的安全基因，在维护国家安全和社会公共利益、保障人民合法权益等方面具有重要战略意义。在新发展格局下，密码产业正面临着复杂挑战，但也迎来了重大机遇。

（二）变中求进，密码产业高质量发展正当时

密码产业正面临深刻变化

当今世界正经历百年未有之大变局，密码产业同样面临着复杂变化。随着数字产业化和产业数字化的加速推进，我国出现密码安全需求滞后、产业链供应链创新不足、高质量发展平台建设欠缺、密码产业发展环境不完善等问题。这要求密码产业立足高质量要求，夯实安全性底座，筑牢产业级防线。密码市场的内涵从过去单一的“国密合规”变得更加丰富和细化，并呈现出分层次叠加的多样化需求，即“实战防护、密评合规、信

创合规”。从实战需求看，日趋严峻的网络安全威胁使得数字产业迫切需要密码技术这个“压舱石”，以有效抵御外部黑客攻击、防止内部人员窃取，而且产业数字化转型又对密码产业提出新的需求。相对日益增长的数字经济，密码产业还需迎头赶上。

密码安全保障需求不足。重要网络和信息系统运营者在密码保障方面投入比例较少、安全建设滞后于业务功能建设；针对商用密码应用安全性评估有待完善、企业安全制度建设亟需健全、商用密码应用示范作用还需提升；跨境数据承载介质多样、形态各异、应用广泛，所在国政策和法律存在差异，均增加应用密码技术保障数据开发利用安全难度。密码产业应因时而变、谋势而动，不断深化需求牵引的发展路径。

产业链供应链创新薄弱。当前和未来一段时期，我国基于密码的安全防护能力、防护方式仍有更多提升空间。其中，主要矛盾体现为产品使用不规范、应用范围不广、创新性不足，产品品种和供给质量难以适应需求变化，密码领域工程研究中心、重点实验室等创新载体不足，关键核心技术受制于人的局面尚未根本改变，密码应用随时面临“卡脖子”风险。产业应始终保持“如履薄冰、如临深渊”的状态，着力补短板、强弱项，加速自主创新、实现产业升级。

高质量发展平台建设不足。商用密码产业链供应链优质资源分散，缺乏产业级创新发展基地，打造聚合效应。密码产业正处于“最初阶段”，出现众多以创新密码技术为主导的中小型创业企业，而行业领军企业和大型综合性企业缺乏在密码领域重点布局，引领性后劲不足。此外，密码行业间交流协作仍需提高，政府投资基金引导作用和人才培养建设等方面，同样需要进一步升级。

密码产业发展环境不完善。目前，我国自主研制和参与国际标准的实践经验不足，相较于国外企业密码标准体系输出能力较弱；商用密码产品检测认证体系和应用安全性评估体系需要优化，中小微企业融资担保政策也需进一步加强。

密码产业处于升级窗口期

我国密码产业已转向提质增效的发展阶段，高质量成为密码产业发展的鲜明标识和强劲动力。随着市场需求升级，创新能力提升，制度优势显现，密码产业迎来重要机遇期，发展韧性强劲、长期向好。

从产业市场来看，《密码法》的施行吹响了密码产业发展“冲锋号”，造就发展黄金窗口期，密码建设从国家层面迎来最好时机，SM系列算法将加速在上中下游的全面融合和推广应用。新技术、新业态成就密码产业发展新机遇，云计算、物联网、5G等信息技术演进促进算法协议以更低成本完成升级。从产业融合来看，密码技术正在以前所未有的广度和深度与信息技术相互促进、融合发展，为网络空间的云计算、大数据、物联网等应用保驾护航。

信创产业发展为密码行业壮大带来历史契机，密码既是信创的重要组成部分，又为信创产业拧紧“安全阀”。而且，信创相关产业充沛的技术人才保障，以及“一带一路”巨大市场潜力，也为密码产业发展奠定重

要基础。

（三）乘势而上，适宜资本运作的新兴产业

从商业发展角度来看，目前我国密码产业前景广阔、大有作为，正处于欣欣向荣的蓝海阶段。聚焦密码领域的创业企业正在蓄力发展，需要有资本市场的助力、整合资源，在相关领军企业中打造行业龙头企业。商用密码产业目前产品类别较多，行业较为分散，而预计该行业将继续以创新为主导，频繁的收购和战略联盟将成为参与者增强行业存在感的关键战略。同时，资本对头部企业的偏好和集中以及行业内小规模兼并收购事件预示着行业逐渐走向集中，马太效应初步显现。目前的商用密码产业具有“小而多”的特点，从行业发展的角度来讲，这个行业正处于“最初阶段”，正是布局重大机会的关键时期。

三、《若干措施》为商用密码产业营造高质量发展环境

近期，十部委联合发布的《促进商用密码产业高质量发展的若干措施》，恰值《密码法》颁布两周年，为商用密码产业的发展按下了“加速键”。《若干措施》坚持深化需求牵引、坚持创新驱动、坚持构建生态、坚持优化环境，不编“花篮子”，不搭“花架子”，扎实推动商用密码产业发展进入“快车道”。

（一）《若干措施》强调要走持续深化需求牵引的发展路径。依法督促推进密码应用“三同步”，强化密码评估执法检查。“三同步”是指在网络和信息系統建设时，按照同步规划、同步建设、同步运行的方式建设密码保障系统，并定期评估。同时通过商用密码应用示范，促进网络身份互信互任和数据信息协同共享。密码技术本身具有低成本、易使用等特性，可保护数据要素在跨越层级、地域、系统之间的安全有序流动，从而实现部门、业务网络直接的高效互认，进而达到个业务单位之间进行数据信息协同共享的效果。

（二）《若干措施》强调坚持创新驱动、提升产业链供应链安全稳定水平。当前，新一代信息网络、量子信息、人工智能等新兴行业正在成为我国新经济的增长点，亟需与密码技术深度融合创新以构建数据安全防护建设。《若干措施》支持密码科技创新，鼓励商用密码单位、企业研发创新型商用密码产品，有利于提升密码技术的高质量供给。

（三）《若干措施》强调搭建产业发展平台。密码产业需要优化要素资源配置，集聚商用密码产业链、供应链、人才链等领域的优质资源，同时支持规范商用密码应用与创新发展基地建设，打造区域性密码创新中心，形成商用密码新技术、新企业的优质“孵化器”，发挥产业链供应链的聚集效应。同时鼓励引导有关领军企业和大型综合性企业积极布局商用密码创新与产业发展，打造商用密码创新策源地、产业链生态链“链长”，助力商用密码领域龙头骨干企业或其细分方向“独角兽”企业的塑造。鼓励运用市场规则设立密码基金和创新发展基金，综合运用股权投资、创业投资、风险投资等方式，从产业孵化角度赋能符合条件的商用密码企业，为商用密码企业发展打入“强心剂”。

（四）《若干措施》强调持续优化完善商用密码产业发展环境。完善商用密码国家标准和重点行业领域商用密码应用标准体系，充分调动企业积极性，积极发挥密码企业创新主导作用，让技术创新空间更为广阔，促进产业蓬勃发展。持续完善商用密码产品检测认证体系，强化商用密码应用安全性评估体系建设。通过优化融资担保业务政策，从金融角度赋能符合条件的商用密码企业，为中小微企业发展营造良好的融资环境。此外，还将从资本市场角度支持商用密码企业发展，强化企业兼并重组、融资、上市服务体系。从而建立起产融结合、相互促进的发展环境，有利于商用密码产业长期、快速、全面的高质量发展。

四、《若干措施》为密码产业带来的新机遇

在政策方面，《措施》中重点指出鼓励企业、金融机构和社会资本以产业基金形式对合适的密码企业进行支持，并且由央行、银保监会和证监会负责优化中小微密码企业融资政策，强化密码企业兼并重组、融资和上市服务体系。可以预见，密码行业相关企业将获得上市发行的支持，对于支持密码企业发展的社会资本，其投资循环通道将更加顺畅，有利于提升投资效率和产业孵化速度。

根据《若干措施》，支持领军企业、产业链生态链“链长”成长为龙头骨干企业。密码前沿技术与应用的引领企业，是信息安全领域的“执牛耳者”，应抓住时代机遇窗口，加速布局密码业务，深化技术创新研究，扎实推进我国商用密码产业建设及发展。

按照《若干措施》规划，还将促进商用密码与新一代信息网络、量子信息、人工智能、物联网、先进制造、工业控制、区块链、智能网联汽车、数字货币等融合创新。预计在这些领域取得先机的密码企业将会率先从中受益、放量增长。

关于商用密码应用安全性评估的“十问十答”

【商密君】

近年来，网络空间安全一直是经济社会关注的焦点，2022年网络信息安全更是成为315晚会关注重点。密码为保护信息安全而生，是网络安全的核心要件，是数字经济基础支撑。下面，我们就来介绍一下日常工作生活中融入的商用密码应用及其安全性评估。

一、什么是商用密码，为什么要使用商用密码？

密码分为核心密码、普通密码和商用密码，我们日常工作生活中接触到的多是商用密码。工作中，网上办公、缴税纳税等过程都有商用密码在起作用。生活中，第二代居民身份证就通过商用密码技术保证认证一致，购买火车票、网络购物等在线支付全过程都有商用密码的保护。

商用密码，是指对不涉及国家秘密内容的信息进行加密保护或安全认证所使用的密码技术和密码产品。其中，商用密码技术，是保障信息安全的核心技术。从功能上看，主要包括加密保护技术和安全认证技术；从内容上看，主要包括密码算法、密钥管理和密码协议。商用密码产品，是指采用密码技术对不涉及国家秘密内容的信息进行加密保护或安全认证的产品，即承载密码技术、实现密码功能的实体。按照形态划分，商用密码产品分为六类，即软件、芯片、模块、板卡、整机、系统；按照功能划分，商用密码产品分为七类，即密码算法类、数据加解密类、认证鉴别类、证书管理类、密钥管理类、密码防伪类和综合类。

密码是网络信任体系的重要基石，是目前世界上公认的，保障网络与信息安全最有效、最可靠、最经济的关键核心技术。《网络安全法》《密码法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等法律法规均不同程度地提到要使用商用密码。在信息互联时代，密码除传统加密外，主要体现在身份认证、权限管理、访问控制等。数字经济时代，密码的作用不断扩展到数据流通、数据共享等新维度，密码技术自身也需要持续革新。

二、商用密码应用安全性评估（简称“密评”）是什么，哪些单位需要开展密评工作？

“密评”是指在采用商用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性进行评估。

国家网络安全和密码相关法律法规明确要求非涉密的关键信息基础设施、等保三级及以上系统、国家政务等重要信息系统要开展密评工作。



并且，密评管理办法也明确规定：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，需要每年至少评估一次。



工业和信息化部下发的基础电信企业及其专业公司网络与信息安全工作评分标准中支出，参与商用密码应用试点，有突出表现的，视情予以加分。

三、不做密评或测试结果不合格会有哪些影响呢？

相关影响已经有文件加以明确：

● 首先，是《密码法》第三十七条第一款指出：关键信息基础设施的运营者未按照要求使用商用密码，或者未按照要求开展密评的，由密码管理部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，将处十万元以上一百万元以下罚款。

● 《国家政务信息化项目建设管理办法》第二十八条第三款也有提到：对于不符合密码应用和网络安全要求，或者存在重大安全隐患的政务信息系统，不安排运行维护经费，项目建设单位不得新建、改建、扩建政务信息系统。

此外，全国各地也在不断将密码应用要求纳入行业管理规范、工作计划。如近两年印发的《广东省政务信息化项目建设管理办法》《河北省省级政务信息化项目建设管理办法》《河南省政务云管理办法》《江西省政务信息化项目建设管理办法》《吉林省政务信息化项目建设管理办法》《广西政务信息化项目建设管理办法》，均提到了要按要求采用密码技术和定期开展密评。

四、密评在密码应用部署过程中所处的位置，全过程涉及的参与方有哪些？

项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，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。



五、密评主要由哪些机构开展？

从事密评活动的机构，应当经国家密码管理部门认定，依法取得商用密码检测机构资质。

六、开展密评工作主要参考哪些标准规范？

参考的标准主要分为两类：

● 第一类是基本要求

就是我们通常说的“信息系统密码应用基本要求”，主要依据国家标准GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，此标准于2021年10月1日正式实施。



● 第二类是评估方法

目前主要参考的文件是2021年发布的GM/T 0115-2021《信息系统密码应用测评要求》、GM/T 0116-2021《信息系统密码应用测评过程指南》，中国密码学会密评联委会修订形成的《信息系统密码应用高风险判定指引》《商用密码应用安全性评估量化评估规则》。

密评量化评估满分100分，得分大于等于60分且没有高风险项为基本合格。

七、密评的服务内容主要有哪些？

密评工作主要包括两部分内容：一是信息系统规划阶段的密码应用方案评估，这一环节主要用于保证建设方案的安全性；二是信息系统建设完成后针对该系统开展现场测试。

● 方案评估阶段

主要针对新建或改造信息系统，密码应用改造方案一般由用户单位组织编写，用户单位编写密码应用建设方案/



改造方案后，应委托专家对方案进行评估或委托密评机构出具方案密评报告。

● 系统评估阶段

主要依据国标GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》，从物理和环境、网络和通信、设备和计算、应用和数据、安全管理等方面开展评估。

注：密评系统的定级参照网络安全等级保护的系统定级。

八、密评过程主要包括哪些环节？

密评过程（如图）分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动；测评双方之间的沟通与洽谈贯穿整个密码应用安全性评估过程。其中，测评对象包括安全人员、管理



员、密码产品、网络设备、服务器、数据库、安全设备、操作系统、应用系统、业务系统、技术文档、管理制度文档等；测评工具涉及协议分析工具、端口扫描工具、渗透测试工具、算法和随机性检测工具、密码应用检测工具、密码安全协议检测工具等。

九、密评过程中有哪些常见问题？

用户单位在密码实际应用改造过程中，会遇到诸多问题，如租用外部机房如何满足物理和环境安全项的要求、自建CA的合规性、云平台 and 云上应用的测评等问题，通用解答可参见2021年底已发布的《商用密码应用安全性评估FAQ》（<https://ht.cacnet.org.cn/upload/file/20211217/1639751669666037.pdf>），针对具体问题还需要结合用户单位实际情况进行详细解答。

十、取得密评报告后应如何去管理部门备案？

按照《密码法》确定的属地管理原则，应由运营者所在地的密码管理部门作为备案部门，由省级密码管理部门作为一般备案部门，国家密码管理局作为特殊备案部门。自密评报告出具之日起30日内，填写《网络与信息系统密评备案信息表》，并按备案表要求，附上密评合同和密评报告，邮寄到所属地密码管理局。

备案编号：CASE-

网络与信息系统密评备案信息表

单位名称	填写规范名称（加盖公章）		
统一社会信用代码			
单位地址			
所属地区		备案密码管理部门	
单位负责人	姓 名		职务/职称
	联系电话		电子邮箱
责任部门			

习近平总书记谈标准化工作（摘要）

【编者按】编者按：标准是人类文明进步的成果，是世界的“通用语言”。尤其在网络空间命运共同体时代，标准对开放和安全的网络信息空间协同发展起到了至关重要的作用。党的十八大以来，习近平总书记在公开发表的讲话和活动中多次对标准化工作做出了重要指示。系统学习并深刻理解习总书记这些指示精神，将让我们在立足网络安全本职、持续开展标准化创新和成果转化时，更有目标、更有底气、更有信心。

我们相信促进和参与和平、安全和开放的网络信息空间十分重要，强调通过全球认可的规范、标准和实践实现信息通信技术的安全使用至关重要。

（二〇一三年三月二十七日金砖国家领导人第五次会晤发表的《金砖国家领导人第五次会晤德班宣言》）

在信息领域没有双重标准，各国都有权维护自己的信息安全，不能一个国家安全而其他国家不安全，一部分国家安全而另一部分国家不安全，更不能牺牲别国安全谋求自身所谓绝对安全。

（二〇一四年七月十六日在巴西国会的演讲）

抓紧修改完善相关法律法规，尽快完成促进科技成果转化法的修订，加快标准化法、反垄断法、公司法以及知识产权保护等方面的法律法规修订工作。要在采取国际最高安全标准、确保安全的前提下抓紧启动东部沿海地区新的核电项目建设。

（二〇一四年八月十八日在中央财经领导小组第七次会议上的讲话）

支持非洲国家提高海关、质检、税务等执法能力，开展标准化和认证认可、电子商务等领域合作。

（二〇一五年十二月四日在中非合作论坛约翰内斯堡峰会开幕式上的致辞）

实施“一带一路”建设、京津冀协同发展、长江经济带发展三大战略，带来了许多难得的重大机遇，民营企业完全可以深度参与其中，推动装备、技术、标准、服务的联合重组，实现产业优化升级。

（二〇一六年三月四日参加全国政协十二届第四次会议民建、工商联界委员联组会时的讲话）

组建“互联网+”联盟、高端芯片联盟等，加强战略、技术、标准、市场等沟通协作，协同创新攻关。要落实网络安全责任制，制定网络安全标准，明确保护对象、保护层级、保护措施。加强战略、技术、标准、市场等沟通协作、协同创新攻关。落实网络安全责任制，制定网络安全标准，明确保护对象、保护层级、保护措施。

（二〇一六年四月十九日在网络安全和信息化工作座谈会上的讲话）

要健全安全生产法律法规和标准体系，统筹做好涉及安全生产的法律法规和标准的制定修订工作。

(二〇一六年七月二十日对加强安全生产和汛期安全防范工作的重要指示)

我们应该加强政策规则的联动，一方面通过宏观经济政策协调放大正面外溢效应，减少负面外部影响，另一方面倡导交流互鉴，解决制度、政策、标准不对称问题。

(二〇一六年九月三日在G20峰会开幕式上的主旨演讲)

标准是人类文明进步的成果。标准已成为世界“通用语言”。世界需要标准协同发展，标准促进世界互联互通。

标准是人类文明进步的成果。从中国古代的“车同轨、书同文”，到现代工业规模化生产，都是标准化的生动实践。伴随着经济全球化深入发展，标准化在便利经贸往来、支撑产业发展、促进科技进步、规范社会治理中的作用日益凸显。标准已成为世界“通用语言”。世界需要标准协同发展，标准促进世界互联互通。

中国将积极实施标准化战略，以标准助力创新发展、协调发展、绿色发展、开放发展、共享发展。我们愿同世界各国一道，深化标准合作，加强交流互鉴，共同完善国际标准体系。

标准助推创新发展，标准引领时代进步。国际标准是全球治理体系和经贸合作发展的重要技术基础。国际标准化组织作为最权威的综合性国际标准机构，制定的标准在全球得到广泛应用。希望与会嘉宾集思广益、凝聚共识，共同探索标准化在完善全球治理、促进可持续发展中的积极作用，为创造人类更加美好的未来作出贡献。

(二〇一六年九月九日致第39届国际标准化组织大会的贺信)

我们同意践行高标准、惠民生、可持续理念，积极对接普遍接受的国际规则标准，坚持以人民为中心的发展思想，走经济、社会、环境协调发展之路。我们将推进建设经济走廊，发展经贸产业合作园区，继续加强市场、规制、标准等方面软联通，以及数字基础设施建设。

(二〇一九年四月二十七日在第二届“一带一路”国际合作高峰论坛记者会上的讲话)

当前，绿色低碳循环发展成为人类共同目标，人工智能、大数据、5G等新技术与新能源发电、电动汽车等深度融合发展，迫切需要制定和应用相关领域国际标准，加强标准领域国际合作。

中国高度重视标准化工作，积极推广应用国际标准以高标准助力高技术创新，促进高水平开放，引领高质量发展。中国将继续积极支持和参与国际标准化活动愿同各国一道，不断完善国际标准体系和治理结构，更好发挥标准在国际贸易和全球治理中的作用。

(二〇一九年十月二十一日致第83届国际电工委员会大会的贺信)

要推动协同攻关，加快推进核心技术突破，为区块链应用发展提供安全可控的技术支撑。要加强区块链标准化研究，提升国际话语权和规则制定权。

(二〇一九年十月二十四日在中共中央政治局第十八次集体学习上的讲话)

建立以企业为主体、市场为导向、产学研深度融合的技术创新体系，支持大中小企业和各类主体融通创新，创新促进科技成果转化机制，积极发展新动能，强化标准引领，提升产业基础能力和产业链现代化水平。建设更高水平开放型经济新体制。

(二〇一九年十月三十一日《中共中央关于坚持和完善中国特色社会主义制度 推进国家治理体系和治理能力现代化若干重大问题的决定》)

全面构建政务数据共享安全制度体系、管理体系、技术防护体系，打破部门信息壁垒，推动数据共享对接更加精准顺畅，提升法治化、制度化、标准化水平。

(二〇二〇年十二月三十一日在中央全面深化改革委员会第十七次会议上的讲话)

要建设开放型世界经济，坚定维护多边贸易体制，不搞歧视性、排他性标准、规则、体系，不搞割裂贸易、投资、技术的高墙壁垒。中国将着力推动规则、规制、管理、标准等制度型开放，持续打造市场化、法治化、国际化营商环境，发挥超大市场优势和内需潜力，为各国合作提供更多机遇，为世界经济复苏和增长注入更多动力。

(二〇二一年一月二十五日在世界经济论坛“达沃斯议程”对话会上的特别致辞)

我们遵循普遍接受的国际规则，符合市场原则，尊重欧盟标准，欢迎其他国家和国际组织积极参与，实现共赢、多赢。中国将继续扩大开放，着力推动规则、规制、管理、标准等制度型开放，持续营造市场化、法治化、国际化营商环境。

(二〇二一年二月九日在中国-中东欧国家领导人峰会上的主旨讲话)

习近平：

加强数字政府建设，完善科技激励机制

中共中央总书记、国家主席、中央军委主席、中央全面深化改革委员会主任习近平4月19日下午主持召开中央全面深化改革委员会第二十五次会议，审议通过了《关于加强数字政府建设的指导意见》、《关于完善科技激励机制的若干意见》等。习近平强调，要全面贯彻网络强国战略，把数字技术广泛应用于政府管理服务，推动政府数字化、智能化运行，为推进国家治理体系和治理能力现代化提供有力支撑。要坚持面向世界科技前沿、面向经济主战场、面向国家重大需求、面向人民生命健康，树立勇担使命、潜心研究、创造价值的激励导向，营造有利于原创成果不断涌现、科技成果有效转化的创新生态，激励广大科技人员各展其能、各尽其才。

《政府工作报告》：

数字化建设要强化网络安全

3月5日，国务院总理李克强代表国务院向十三届全国人大五次会议作《政府工作报告》。总结了过去一年的工作成绩，对未来我国数字化如何建设，以及如何安全稳定发展，指明了方向。

《报告》总结了过去一年取得的重要成果。强化创新引领，稳定产业链供应链；加强国家实验室建设；推进重大科技项目实施；改革完善中央财政科研经费管理，提高间接费用比例，扩大科研自主权；延续实施研发费用加计扣除政策，将制造业企业研发费用加计扣除比例提高到100%；强化知识产权保护，开展重点产业强链补链行动，传统产业数字化、智能化改造加快，新兴产业保持良好发展势头。

《报告》明确了2022年的政府工作任务。要促进数字经济发展，加强数字中国建设整体布局，建设数字信息基础设施，促进产业数字化转型；要加快发展工业互联网，培育壮大数字产业，提升关键软硬件技术创新和供给能力，完善数字经济治理，释放数据要素潜力。要推进国家安全体系和能力建设，强化网络安全、数据安全和个人信息保护。

中办、国办：

发挥社会组织平台作用，促进社会信用体系建设高质量发展

3月29日，中共中央办公厅、国务院办公厅印发《关于推进社会信用体系建设高质量发展促进形成新发展格局的意见》，意见指出，要统筹推进公共信用信息系统建设，充分发挥社会组织信用信息公示平台的信息公开作用。要强化标准、检验检测等方面诚信要求，扩大国内市场优质产品和服务供给，提升产业链供应链安全可控水平。

中央财经委员会中央财经委员会： 要适度超前布局有利于引领产业发展和维护国家安全的基础设施

2022年4月26日，习近平主持召开了中央财经委员会第十一次会议，会议强调，要适度超前，布局有利于引领产业发展和维护国家安全的基础设施，同时把握好超前建设的度。要科学规划，贯彻新发展理念，立足全生命周期，统筹各类基础设施布局，实现互联互通、共建共享、协调联动。要多轮驱动，发挥政府和市场、中央和地方、国有资本和社会资本多方面作用，分层分类加强基础设施建设。要注重效益，既要算经济账，又要算综合账，提高基础设施全生命周期综合效益。

在引导好市场预期、稳定市场信心方面，强调要统筹发展和安全两件大事，牢固树立底线思维，切实加强重大风险预测预警能力，有切实管用的应对预案及具体可操作的举措。

在全面加强基础设施建设、保障国家安全方面，强调我国基础设施同国家发展和安全保障需要相比还不适应，全面加强基础设施建设，对保障国家安全，畅通国内大循环、促进国内国际双循环，扩大内需，推动高质量发展，都具有重大意义。

在强化基础设施建设支撑保障方面，强调要在党中央统一领导下，建立重大基础设施建设协调机制，统筹协调各领域、各地区基础设施规划和建设，强化用地、用海、用能等资源要素保障。要适应基础设施建设融资需求，拓宽长期资金筹措渠道，加大财政投入，更好集中保障国家重大基础设施建设的资金需求。要坚持创新驱动，加大关键核心技术研发，提升基础设施技术自主可控水平。

在适度超前、布局有利于引领产业发展和维护国家安全的基础设施方面，强调要科学规划，贯彻新发展理念，立足全生命周期，统筹各类基础设施布局，实现互联互通、共建共享、协调联动。要多轮驱动，发挥政府和市场、中央和地方、国有资本和社会资本多方面作用，分层分类加强基础设施建设。要注重效益，既要算经济账，又要算综合账，提高基础设施全生命周期综合效益。

会议还指出，要加强交通、能源、水利等网络型基础设施建设，把联网、补网、强链作为建设的重点，着力提升网络效益。要加强信息、科技、物流等产业升级基础设施建设，布局建设新一代超算、云计算、人工智能平台、宽带基础网络等设施，推进重大科技基础设施布局建设，加强综合交通枢纽及集疏运体系建设，布局建设一批支线机场、通用机场和货运机场。

两会委员为强化网络安全建言献策

2022年两会期间，网络安全成为代表委员热点提案。

全国政协委员、中国工程院院士邓中翰建议，从标准、技术体系等方面出台顶层规划和实施细则，强化相关企业在信息安全技术和产品上加大研发投入，强化自主可控标准、技术的推广应用，建立起以自主可控技术和国产密码算法为核心的车载视音频数据安全体系；国家以标准化、通用化为纽带，以关键技术研发和产品设备生产为突破口，引导打造车载视音频数据安全创新产业链，逐步形成自主可控的产品体系；建议组织开展试点示范工作，结合国家车联网试点示范工程，开展关键技术验证，以利大规模推广使用。

全国政协委员、启明星辰集团首席执行官严望佳建议，新型电力系统不再是一个单一封闭系统，而是开放、互联的网络，面临更多安全风险。应积极稳妥有序地推进新型电力系统与网络安全同步规划建设，要求电力行业企业适度提高在新型电力系统规划建设运维预算中的网络安全预算占比。应高度重视新型电力系统中的能源数据安全治理、数据智能自动化调度运营安全和能源数据安全保障体系的规划建设。鼓励针对新型电力系统关键核心技术的联合攻关、自主可控的网络安全专用设备研制和开展能源绿色低碳转型场景化的安全协同创新技术研究。

全国政协委员、安天科技股份有限公司创始人肖新光建议，当前中国应推动重点行业、重点领域、关键信息基础设施等关键部门要根据自身特点，开展敌情想定分析工作，叠加到地缘安全风险的背景下，分析可能发起攻击的威胁行为体。基于威胁行为体的动机、能力、作业风格等信息，完成想定构建；并形成阶段性更新机制，以及重大关联安全风险和事件背景下的紧急触发机制。

全国人大代表、中电工业互联网有限公司党委书记、董事长朱立锋建议，数据安全是国家安全的重要组成部分，是数字经济时代最紧迫和最基础的安全问题。我国的数据安全合规体系建设还存在一定的滞后性，亟须充分调动社会各界力量尽快解决。建议从完善制度规则体系、建立综合治理体系、建强基础设施体系、打造产业生态体系等四个方面提升我国数据安全治理能力。

交通部、科技部：

加速新一代信息技术与交通运输融合

3月25日，交通部、科技部印发《交通领域科技创新中长期发展规划纲要（2021—2035年）》。纲要提出，要构建形成数字化、网络化、智能化、绿色化的综合交通运输系统。要加快新一代信息技术在交通运输公共服务、交通运输监测预警、综合应急指挥和监管、交通运输舆情主动响应、驾驶培训等领域应用。

国资委成立科技创新局、社会责任局： 推动中央企业科技创新和社会责任工作高标准高质量开展

3月16日，国务院国资委网站公布成立科技创新局、社会责任局，并召开成立大会。会上，国资委领导要求两局要提高政治站位，把准职责定位，聚焦主责主业，抓紧抓实国资央企科技创新和社会责任重点工作任务。新成立的两局将组织指导中央企业深入实施创新驱动发展战略、积极履行社会责任，坚定不移做强做优做大国有资本和国有企业，加快打造世界一流企业。

原来国资委就已经有科技创新和社会责任局，科技创新和社会责任工作统一在一个局，现在将两项工作分别独立并成立独立的局，更加强化了中央企业落实竞争力、创新力、控制力、影响力、抗风险能力，特别是国有企业不仅定位为市场竞争主体需要盈利，更要考虑到承担创新发展和社会责任的责任。

目前，科技创新局要突出抓好重大科技专项任务落地，着力推动国有企业打造原创技术策源地；突出抓好强化企业创新主体地位，加快推动中央企业建设创新型领军企业；突出抓好科技生态优化，更好激发中央企业创新创造潜能；突出抓好中央企业两化融合和数字化转型，大力推进中央企业创新链产业链深度融合。社会责任局要突出抓好中央企业碳达峰碳中和有关工作；抓好安全环保工作，推动企业全过程、全链条完善风险防控体系；抓好中央企业乡村振兴和援疆援藏援青工作；抓好中央企业质量管理和品牌建设，打造一批国际知名高端品牌；抓好中央企业社会责任体系构建工作，指导推动企业积极践行ESG理念，主动适应、引领国际规则标准制定，更好推动可持续发展。

市场监管总局、工信部： 建设国家级质量标准实验室 推进产业基础高级化和产业链现代化

3月2日，市场监管总局和工信部发布《关于推进国家级质量标准实验室建设的指导意见》，意见指出，要围绕质量、安全等领域，开展标准（标准样品）实验验证、计量检测技术、方法和测试装备研究、产品安全评估和监管技术等研究。要在信息技术等领域，开展质量共性技术研究，解决技术、质量、标准协同的关键问题。

意见要求，到2025年力争在信息技术等重点领域建设若干国家级质量标准实验室；突破一批检验检测新技术和共性关键技术，研制一批智能化高端检测设备，形成一批重点产业标准及认证方法。到2035年基本建成同现代产业体系发展与安全保障相适应的国家级质量标准实验室体系。

工信部：

构建车联网网络安全和数据安全标准体系

支撑车联网产业安全健康发展

3月7日，工信部印发《车联网网络安全和数据安全标准体系建设指南》。提出到2023年底，初步构建起车联网网络安全和数据安全标准体系。重点研究基础共性、终端与设施网络安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等标准，完成50项以上急需标准的研制。到2025年，形成较为完善的车联网网络安全和数据安全标准体系。完成100项以上标准的研制，提升标准对细分领域的覆盖程度，加强标准服务能力，提高标准应用水平，支撑车联网产业安全健康发展。标准体系框架包括总体与基础共性、终端与设施网络安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等6部分。

田玉龙：

三方面发力 确保工业互联网安全有序健康发展

2月23日，工信部总工程师、新闻发言人田玉龙在国务院政策例行吹风会上表示，要健全完善工业互联网的平台安全政策体系和保障体系，推动建立工业互联网企业网络安全分类分级管理制度。下一步，工信部将在三个方面发力，确保工业互联网安全有序健康发展。

一是要推动建立工业互联网企业网络安全分类分级管理制度，在试点基础上进一步总结，扩大推广应用。加快研制发布平台企业网络安全标准。

二是要健全平台企业的监测预警，对网络安全平台企业要加强监测预警，信息通报和应急处置，确保安全。

三是要组织开展安全深度行活动，推动新技术、新产品、新标准应用，使工业互联网平台安全产品解决方案在各行各业中能够得到实际应用。

国标委：

发布2022年全国标准化工作要点 构建高质量标准体系支撑和着力点

2月15日，国家标准化管理委员会发布《2022年全国标准化工作要点》，以着力重点突破、深化改革创新、提升质量效益、加强标准国际化为指引，明确了2022年标准化工作的重点任务、工作路径等。工作要点指出：要加快关键信息基础设施安全保护、网络安全产品和服务等网络安全重点标准制修订；要研究建立推荐性国家标准采信团体标准机制；要发布实施促进团体标准规范优质发展的意见，实施团体标准培优计划，推动团体标准化建设，引导社会团体制定原创性、高质量标准；要推动团体标准组织开展自我评价和自我声明；要鼓励社会团体参与国际性专业标准组织活动；要大力发展标准化服务业，搭建标准服务平台，推动标准、检验检测、标准样品等融合发展。

海南省：

部署开展商用密码应用示范工作

为有效防范海南自由贸易港建设面临的网络和数据安全风险，加快推进商用密码应用，切实提升全省网络空间密码保障能力，近日，海南省国家密码管理局联合省发改委、省财政厅、省大数据管理局等部门印发《关于开展商用密码应用示范的通知》，选取海南省政务云密码服务平台、海易办平台、海南自贸港物码溯源管理系统等10个重要信息系统部署开展商用密码应用示范。

此次示范将按照“全省一盘棋，全岛同城化”集约化建设理念，在省级政务领域先行先试，统筹建设海南省电子政务云密码服务平台，统一为全省政务云业务应用系统提供云密码服务；通过应用示范逐步完善平台运营机制，形成一套全省适用政务云密码服务标准和模式，指导规范各级政务信息系统的密码应用建设及运行管理。金融、交通、电力、公共卫生以及商品流通等行业领域示范将按照“成熟一批总结一批”的模式及时总结和推广，以示范引领带动行业系统内商用密码应用，并逐步拓展应用的深度和广度。

在全省部署开展商用密码应用示范既是落实《密码法》和国家密码局等部门关于促进商用密码产业高质量发展若干措施的具体要求，也是主动做好自贸港全岛封关运作准备工作的实际行动，这将进一步规范促进海南省商用密码应用，夯实自贸港网络安全和数据安全风险防控基础。

蔡奇：

推进中关村新一轮先行先试改革，聚焦重点任务

3月18日，市委书记蔡奇在中关村新一轮先行先试改革动员部署会上强调，要深入学习贯彻习近平总书记关于建设科技强国的重要论述，坚定改革信心决心，把握战略主动，当好改革创新“试验田”，推进中关村新一轮先行先试改革，加快建设世界领先科技园区和创新高地。科技部部长王志刚，中国工程院院长李晓红，市委副书记、市长陈吉宁出席。

会议强调，开展中关村新一轮先行先试改革，要聚焦重点任务，扎实推动改革举措落地见效。

一要做强创新主体。支持企业牵头组建创新联合体，开展联合技术攻关。用好中小微企业使用科技成果的政策措施，培育“专精特新”企业和隐形冠军企业。支持高校、科研院所瞄准前沿科技和未来产业中的难题开展研发，推动产学研深度融合。

二要紧抓人才这个第一资源。推动高水平人才高地建设，完善战略人才发现、培养和激励机制，培养急需紧缺人才和重点产业人才，建立高水平专业化科技服务人才队伍。

三要畅通金融通道。推动投贷联动、投担联动、科技保险等金融服务模式和产品创新，建立企业研发创新全链条金融支持机制。抓好中关村科创金融试验区创建。

四要优化创新机制。落深落细促进科技成果转化条例、“科创30条”，完善科研任务“揭榜挂帅”机制。抓好科技成果评价综合改革试点，建立分类评价体系，加速科技成果产出和应用。

五要发挥政策叠加优势。做好政策统筹对接和集成利用。加紧推进国际信息产业和数字贸易港建设。

六要统筹发展与安全。牢固树立安全意识，健全与改革相匹配的风险防控机制，及时有效防范化解科技、金融、网络与信息安全等领域风险。

七要全力抓好政策落地。抓实抓细各项配套工作，做好服务保障，把政策落实到项目、园区、企业上来。市级部门优化调整完善相关措施，其他各区(分园)抓紧研究各自应用落地方案。

联盟永远跟党走 把握历史主动 明确“开创”深意

学习时报

具有历史性意义的党的十九届六中全会，审议通过了《中共中央关于党的百年奋斗重大成就和历史经验的决议》（以下简称《决议》），彰显了坚定的历史自信。《决议》分阶段对党在不同时期取得的重大成就进行了梳理，并用“开创中国特色社会主义新时代”为标题，重点介绍了党的十八大以来取得的历史性成就、发生的历史性变革。选取“开创”二字，饱含深刻意蕴。全会召开后，学界对会议精神、决议内容进行了多角度、深层次的解读阐释，但缺憾在于“开创”二字的解读付之阙如。

在《现代汉语词典》中，“开创”意指“开始建立；创建”。在改革开放以来党的重要文献中，“开创”一般用于理论创新出现巨大突破、新的道路得以成功开辟、事业取得非凡成就等。这从一些重要文献的命名上亦不难看出。比如，1982年党的十二大报告的题目是《全面开创社会主义现代化建设的新局面》，这是党代会报告的标题中第一次出现“开创”；1998年在纪念党的十一届三中全会召开20周年大会上的讲话中，江泽民同志指出，“没有毛泽东同志的领导，就没有新中国的成立；没有邓小平同志的领导，就没有建设有中国特色社会主义道路的开创”；2007年胡锦涛同志在党的十七大报告中指出，“改革开放伟大事业，是以邓小平同志为核心的党的第二代中央领导集体带领全党全国各族人民开创的”；2012年党的十八大报告指出，以邓小平同志为核心的党的第二代中央领导集体带领全党全国各族人民“成功开创了中国特色社会主义”；2018年，习近平总书记指出，以邓小平同志为主要代表的中国共产党人“成功开创了中国特色社会主义”。党的十九届

六中全会在决议第四部分标题“开创中国特色社会主义新时代”使用“开创”二字，主要是因为党的十八大以来，在以习近平同志为核心的党中央坚强领导下，我们创立了新思想、创造了新成就、创建了新制度、锻造了新精神，通过一系列变革性实践，取得重大突破性进展和标志性成果。

创立了新思想。这一思想就是习近平新时代中国特色社会主义思想，它坚持把马克思主义基本原理同中国具体实际相结合、同中华优秀传统文化相结合，科学回答了新时代坚持和发展什么样的中国特色社会主义、怎样坚持和发展中国特色社会主义，建设什么样的社会主义现代化强国、怎样建设社会主义现代化强国，建设什么样的长期执政的马克思主义政党、怎样建设长期执政的马克思主义政党等重大时代课题，进一步深化了对共产党执政规律、社会主义建设规律、人类社会发 展规律的认识，是对中国特色社会主义建设规律认识的新跃升，是当代中国马克思主义、二十一世纪马克思主义，是中华文化和中国精神的时代精华，实现了马克思主义中国化新的飞跃。从科学回答的系列重大时代课题到“十个明确”的核心内容，都表明十八大以来党的创新理论具有极强原创性，是马克思主义在中国发展的新阶段。习近平总书记是新思想的主要创立者。《决议》站在历史高度鲜明提出“两个确立”，即党确立习近平同志党中央的核心、全党的核心地位，确立习近平新时代中国特色社会主义思想的指导地位。这反映了全党全军全国各族人民共同心愿，对新时代党和国家事业发展、对推进中华民族伟大复兴历史进程具有决定性意义。

创造了新成就。在党的创新理论科学指引下，

党的十八大以来党和国家事业取得历史性成就、发生历史性变革，为开创新时代奠定坚实物质基础。《决议》从坚持党的全面领导、全面从严治党、经济建设、全面深化改革开放、政治建设、全面依法治国等13个方面，分领域总结了新时代取得的历史性成就。这些成就涵盖治党治国治军、内政外交国防、改革发展稳定，是全方位、开创性的，带有深层次、根本性的新特征。尤其是在全球经济增长放缓的情况下，在疫情持续肆虐的情况下，中国共产党精心组织、团结一致、上下合力，历史性消灭绝对贫困，全面建成了小康社会，成功开启了全面建设社会主义现代化国家新征程。在中国共产党成立100周年的历史性年份，国内生产总值突破114万亿元人民币，中国经济总量达到了历史新高。就此，《决议》简明概括为“自信自强、守正创新，创造了新时代中国特色社会主义的伟大成就”。这些前所未有的巨大成就足以让中国共产党和中国人民向世界宣告，中华民族迎来了从站起来、富起来到强起来的伟大飞跃。中国人民在中国共产党的领导下，坚持走中国式现代化新道路，创造了人类文明新形态，也为世界提供了中国智慧、中国方案，彰显了中国成就的世界历史意义。

创建了新制度。制度更带有根本性、全局性、稳定性和长期性。国家间竞争不仅有思想上的较量，更有制度层面的比拼。在创立新思想、创造新成就的过程中，中国共产党谋划长远，围绕坚持和发展中国特色社会主义创建了一系列新制度。习近平总书记鲜明指出，从形成更加成熟更加定型的制度看，我国社会主义实践前半程的主要历史任务是建立社会主义基本制度，并在这个基础上进行改革，现在已经有了很好的基础。我国社会主义实践后半程的主要历史任务是完善和发展中国特色社会主义制度，为党和国家事业发展、为人民幸福安康、社会和谐稳定、为国家长治久安提供一整套更完备、更稳定、更管用的制度体系。为完成这个“后半程的主要历史任务”，党的十八届三中全会明确全面深化改革总目标是完善和

发展中国特色社会主义制度、推进国家治理体系和治理能力现代化；党的十八届四中全会明确全面推进依法治国总目标是建设中国特色社会主义法治体系、建设社会主义法治国家；党的十九大明确提出，坚持依法治国和依规治党有机统一，加快形成覆盖党的领导和党的建设各方面的党内法规体系；党的十九届四中全会通过的《中共中央关于坚持和完善中国特色社会主义制度、推进国家治理体系和治理能力现代化若干重大问题的决定》，进一步就制度建设作出部署。习近平总书记在庆祝中国共产党成立100周年大会上宣布“形成比较完善的党内法规体系”。《决议》指出“中国特色社会主义制度更加成熟更加定型，国家治理体系和治理能力现代化水平不断提高”。在党的十八大以来以来的制度建设中，有很多是创新性制度安排，包括关于做到“两个维护”的制度、关于“不忘初心、牢记使命”的制度、关于社会主义核心价值观的制度等等。正是这些新创建的制度为我国经济社会健康发展进而取得非凡成就，提供了坚强制度保障。

锻造了新精神。一个时代有一个时代的独特精神标识。新民主主义革命时期的精神标识是“浴血奋战、百折不挠”；社会主义革命和建设时期的精神标识是“自力更生、发愤图强”；改革开放和社会主义现代化建设新时期的精神标识是“解放思想、锐意进取”。党的十八大以来，中国特色社会主义进入新时代。在这个新的历史方位，中国人民从全面建成小康社会向实现共同富裕进发，中国国力从经济大国向世界强国冲刺，中国正日益走近世界舞台中央。在中国共产党的坚强领导下，中国亿万儿女精准扶贫、合力抗疫，保持稳中有进的态势，展现出新时代中国精神的新风貌。这一新风貌就是充满自信、满怀豪情，既继承前人敬畏先辈又开拓进取、勇于创新，简言之就是“自信自强、守正创新”。这一新精神是伟大中国精神的重要组成部分，是全面建设社会主义现代化国家、实现中华民族伟大复兴的重要精神支撑。

有了新思想的科学指引、有了新成就的厚实基

础、有了新制度的坚强保障、有了新精神的活力支撑，中国特色社会主义新时代才得以成功开创。当然，开创了新时代，绝不意味着可以忘记前人的贡献。我们要始终铭记老一辈革命家的艰辛开拓，我们要始终铭记前辈们的奋力拼搏。正是他们的艰苦奋斗、努力奋斗、不懈奋斗，为我们开创新时代提供了宝贵经验、理论准备、物质基础、精神支撑。我们今天开创的新时代，是站在前人肩膀基础上的“百尺竿头、再进一步”。

踏上新征程，展望新百年。唯有在党的创新理论指引下，不断完善中国特色社会主义制度，不断创造新的更大奇迹，我们才能如期全面建成社会主义现代化强国、实现中华民族伟大复兴，才能让中国人民过上更加美好的幸福生活。

作者沈传亮，系中央党校（国家行政学院）研究室副主任、教授

WAPI产业联盟参加中共北京市中关村社团第二联合党委第二流动党员联合支部委员会组织生活会

WAPI产业联盟 周 园

2022年4月1日，中共北京市中关村社团第二联合党委第二流动党员联合支部委员会召开组织生活会。WAPI产业联盟积极分子周园参加了本次会议。

为更加紧密团结在党中央周围，WAPI产业联盟和4家社会组织于2021年8月30日共同组建了中共北京市中关村社团第二联合党委第二流动党员联合支部。

会上，贾连涛书记带领党支部同志深入学习、热烈讨论，结合基层党组织和党员思想学习工作实际，紧密围绕组织生活会主题，严格落实组织生活会和民主评议党员相关制度规定和任务要求，对照党章和《中国共产党组织工作条例》认真查摆存在问题和不足，并特出新的整改措施。

2022年，中共北京市中关村社团第二联合党委第二流动党员联合支部委员会将严格落实“三会一课”制度。流动党员支部更不能降低标准，要结合自身的

特点，做到精心组织、周密安排、抓好落实。学习习近平总书记在庆祝中国共产党成立100周年大会上的重要讲话和十九届各中全会精神。按要求做到每季度至少组织召开一次党员大会、完成党课学习、召开组织生活会等相关活动，真正把党建工作摆在与业务工作同等重要的位置。同时加强联合流动党支部所在联盟间资源优势，共同开展党建与业务紧密融合的主题党日活动，发挥好社会组织的桥梁与纽带作用。

会后，周园组织WAPI产业联盟秘书处全体工作人员学习了《中国共产党组织工作条例》和近期相关文件，并宣贯了本次会议精神。WAPI产业联盟秘书处将坚决贯彻落实新时代党建工作要求，打牢思想基础，提升政治能力。结合网络安全领域的实际情况和任务，积极运用新知识、新思维、新方法，发挥创新联合体作用。

WAPI产业联盟参加“党建红 园林绿” 公益植树和红色教育活动

WAPI产业联盟 周 园



2022年4月15日，WAPI产业联盟周园、刘剑昕两位同志参加了中关村产业技术联盟联合会组织的“党建红 园林绿”公益植树和红色教育基地参观主题党日活动。

当天上午，活动人员赴亿亩千田植树基地进行公益植树。大家热情洋溢，分工协作，配合默契。经过共同努力，50余株小树苗整齐排列，迎风向阳，所有人都为美化环境贡献一份力量而深感自豪。

下午，活动人员赴慕田峪长城精神传承馆参观学习。展馆一层的守望和平长城历史区，通过拓印匾

额、地理图示等长城展品，展示了古代中国长城抵御侵略的重要作用和形成中华民族强大凝聚力的伟大意义。在展馆二层，大家参观了百年辉煌、红色记忆、不忘初心、扬帆起航等七个板块，身临其境地体会中国共产党的百年奋斗之路和光辉历程，领会中国共产党在长期奋斗中铸就的伟大精神。此外，大家还参观了党建教育区“新中国的和平主张、北京市在新时代的重要使命和发展成就、慕田峪长城的发展历程和愿景”等。



以实际行动服务中关村世界领先科技园区建设之 WAPI产业联盟参加中关村产业技术联盟业务工作会议

WAPI产业联盟 刘剑昕

2022年4月1日，WAPI产业联盟参加了中关村产业技术联盟业务工作会议。市科委、中关村管委会科技服务业处二级调研员李建玲、中关村产业技术联盟联合会副秘书长杨一图等领导出席会议并讲话。

李建玲围绕“十四五”时期北京加快推进国际科技创新中心和世界领先科技园区建设的目标、部署和要求，对联盟工作提出了四点希望：一是通过参与“联合护航行动”、“园区行”、“科创大赛”等品牌活动，持续强化自身建设，创新打造服务于园区发展的贴心服务；二是推动产业标准创制国际化，增加产业技术联盟国际影响力和话语权；三是扩展联盟国际合作新路径和国际视野，将以联盟为核心的服务队伍打造成为“懂科技、敢创新、爱奋斗”具有创新发展战斗力的新生力；四是重视联盟党建工作，持续加强党建引领，促进党建业务融合发展。

杨一图表示，长期以来，在科技创新和产业发展方面，产业技术联盟起着不可忽视的协同促进作用，是支持区域升级产业结构、提升专业化服务水平的重要助力。各联盟在组织机构建设与运行、协同创新活动、带动产业发展等方面具备各自的特点和亮点，在优化共性技术研发体系、标准创制和推广、引导产业发展战略、推动产学研用深度融合等方面，具有显著的行业引领和产业促进作用。在新的历史时期，联盟需要围绕国际合作交流、各类标准的创制和推广、协同推进技术创新、服务园区建设、搭建服务平台等方面继续发挥更加重要的作用，实现联盟的高质量和创

新发展。

会上，还从“党建工作体系、2022年党建工作要点、党建工作建议要求”几个方面分享了党建工作开展的经验和探索，并对联盟信息报送、诚信建设、“联合护航行动”的开展要求和实施情况做了详细介绍与培训。

在WAPI产业联盟发展的16年间，始终坚决拥护中国共产党的领导，坚持以党的政治路线、中心工作和方针政策指导联盟日常工作，持续强化联盟自身建设。以“标准创新”、“检验检测”、“公共服务平台”为抓手，打造“市场需求→制定标准→规范产品→形成解决方案→市场广泛采信标准→服务市场”的融合创新链条，解决协同技术创新中的“小精专卡脖子难题”。在发挥社会组织外交作用、解决网络安全卡脖子、改变领域受制于人、推动科技创新和成果转化、提升中国标准国际话语权、服务关键信息基础设施建设等诸多方面成果显著。

2022年，WAPI产业联盟已结合北京市科委、中关村管委会在服务园区方面的核心关注，提出了服务一区十六园的“自主可控无线局域网检测能力建设和提升计划”，并将配合各园区的产业重点，聚焦“国防安全、能源安全、金融安全、公安安全、交通安全”等民生行业，落地重大示范项目。新的历史时期，WAPI产业联盟将充分发挥社会组织独特作用，以实际行动助力北京国际科技创新中心和中关村世界领先科技园区建设！

以实际行动助力中关村世界领先科技园区建设之 WAPI产业联盟参加“园区行”活动——走进未来科学城

WAPI产业联盟 刘剑昕

3月23日，WAPI产业联盟参加了中关村产业技术联盟“园区行”之走进未来科学城活动。北京未来科学城管委会科技创新处处长张卫军、昌平区投资促进服务中心副主任张冰、中关村产业技术联盟联合会副秘书长杨一图、北京未来科学城发展集团有限公司副总经理/北京未来科学城产业发展有限公司董事长周榕等领导出席活动。

“园区行”活动的目的是贯彻党中央国务院和市委市政府部署要求，不断加强中关村产业技术联盟对创新驱动发展战略、京津冀协同战略、“一带一路”倡议等重大战略和北京市委市政府“十四五”时期推进北京国际科技创新中心建设，中关村世界领先科技园区建设等决策部署的响应落实。

在周榕副总经理的带领下，WAPI产业联盟等单位代表一行先后参观了未来科学城展厅、科学城能源谷、未来中心项目及沙盘，对未来科学城整体建设情况和周边配套设施、产业发展情况等做了了解，并在未来中心开展座谈。

周榕副总经理介绍了未来科学城的基本情况、配套优势、地理优势、服务政策等内容。张冰主任介绍了昌平区投资环境和支持政策，并在会上同步发布了昌平区中介奖励政策，希望能通过走进园区活动寻求双方进一步的合作机会，发挥创新型社会组织的资源优势。张卫军处长围绕未来科学城发展的沿革、技术创新的优势等情况进行了介绍，并希望同中关村产业联盟和企业形成良好的互动，共同助力未来科学城

资源和中关村资源的衔接和交流。联盟联合会杨一图副秘书长，围绕产业联盟和联盟联合会的成立背景、成长情况、功能定位、工作内容等进行了介绍。兴创空间联盟盖帅秘书长对兴创空间联盟基本情况、工作内容、政策制定和研究方面工作经验等情况进行了介绍。随后联盟和企业代表围绕先进能源、先进制造等行业发展趋势、项目合作、活动后续服务支撑等方面进行了深入沟通交流。

多年来，WAPI产业联盟一直积极响应并支持配合北京市科委、中关村管委会工作，立足无线网络和网络安全领域，开展技术创新和成果转化。近三年，已通过搭建无线网络安全有关共性技术服务平台，为一区十六园200多家企业提供服务，已完成150多款型号的产品测试服务，辐射30亿件产品，已完成“便携式网络运维检查工具”、“WLAN快速切换CPE”等共性关键技术开发和成果转移10余项等等。

2022年，WAPI产业联盟结合北京市科委、中关村管委会服务一区十六园方面的核心关注，提出了服务一区十六园的“自主可控无线局域网检测能力建设和提升计划”，并将配合各园区的产业重点，聚焦“国防安全、能源安全、金融安全、公安安全、交通安全”等民生行业，落地重大示范项目。我们希望，能够发挥出产业联盟这类社会组织的独特作用，以实际行动助力北京国际科技创新中心和中关村世界领先科技园区建设。

WAPI产业联盟召开 2022年第一次标准工作及项目组会议（总第121次）

WAPI产业联盟 米 东



2022年3月17日，WAPI产业联盟组织召开2022年第一次标准工作及项目组会议。会议包括：2022年第一季度技术标准产业工作报告、技术产业最新动态分享、最新联盟团体标准宣贯、在研标准项目讨论和审议、标准国际化专题讨论、标准化知识交流与培训等。来自无线网络安全技术国家工程研究中心、国家无线电监测中心检测中心、江苏省电子信息产品质量监督检验研究院、广州广电计量检测股份有限公司、中国电信研究院、华为技术有限公司、西电捷通公司、北京数字认证股份有限公司、高通无线通信技术（中国）有限公司、山东华辰泰尔信息科技股份有限公司、展讯半导体、西安芯语慧联信息科技有限公司、北京华信傲天网络技术有限公司、上海麓慧科技有限公司、新华三技术有限公司、广州杰赛科技股份有限公司、深圳市智开科技有限公司、北京紫光展锐通信技术有限公司、瑞晟微电子（苏州）有限公司、

巷子科技(北京)有限公司、重庆源盾科技集团有限公司、桂林电子科技大学、南京博丰通讯科技有限公司、四川岁月文明科技有限公司、北京比邻科技有限公司等单位代表，无线网络安全标准化委员会专家委员，ISO/IEC JTC 1/SC 6国内技术对口单位、工业和信息化部宽带无线IP标准工作组等标准组织代表参加会议。

WAPI产业联盟秘书长、无线网络安全标准化委员会副主任委员张璐璐在会议致辞中表示，结合国内外环境变化和产业市场需求，联盟2022年标准化工作重点包括“固平台、提质量、定需求、促应用、优生态、抓机遇”六部分。今年第一季度，联盟秘书处已落实如下工作：第一、加强联盟标准化部专职化人员建设，为产业链上下游做好高质量标准组织和协同创新服务。第二、结合工作具体情况和变化，修订了《WAPI产业联盟标准化工作管理办法》、《WAPI产

业联盟无线网络安全标准化委员会导则》、《WAPI产业联盟团体标准制修订工作程序》。第三、进一步明确技术协调层（WG）和编制层（PE）是联盟标准化工作的基础和核心力量，并组织召开2022年无线网络安全标委会工作组组长和项目编辑协同工作促进会，统一了认识和思路，明确了工作协同机制。第四、讨论并确定了2022年联盟标准制修订计划和团体标准复审计划。计划推进并发布国际标准1项，国家标准1项，团体标准6项。今年上半年将启动并完成63项联盟团体标准的复审。张璐璐表示，2022年，WAPI产业联盟将重点围绕服务国家网络安全总体目标、服务民生行业需求等，组织成员开展技术标准产业的协同创新，服务重要项目的落地。这其中，标准化工作仍将是重要的和必要的抓手。希望联盟标委会委员、各工作组和项目组以及所有成员单位发挥作用，坚持问题导向、效果导向，加快研制市场急需的关键标准，提升标准实施应用效果。

工信部宽带无线IP标准工作组秘书长、无线网络安全标准化委员会副主任委员黄振海分享了近期无线网络安全及标准化相关政策，其中，建议关注如下：第一、《国家标准化发展纲要》提出的实现四个转变，包括：推动实现标准供给由政府主导向政府与市场并重转变，标准运用由产业与贸易为主向经济社会全域转变，标准化工作由国内驱动向国内国际相互促进转变，标准化发展由数量规模型向质量效益型转变。第二、《关于促进团体标准规范优质发展的意见》提出的“制定原创性、高质量的团体标准，填补标准空白”“鼓励团体标准组织建立标准制定、检验、检测、认证一体化工作机制，推动团体标准在招投标、合同履行等市场活动中实施应用，提高社会对团体标准的认知度和认可度”，“提升团体标准组织的诚信和影响”。第三、2022年《政府工作报告》提出的要“围绕打造市场化法治化国际化营商环境，持续推进‘放管服’改革”，要“强化网络安全、数

据安全和个人信息保护，加强国家安全保障能力建设”。黄振海表示，当前政策和国家规划，为WAPI标准产业共同体的组织发展、标准开发、市场应用、产业配套指明了发展方向和实施路径。WAPI标准产业共同体要抓住机遇，联盟要继续充当好政产学研用的桥梁纽带，发挥好无线网络安全标准产业的联通和支撑作用。

黄振海还向与会人员报告了第一季度团体标准和国际标准工作情况：在团体标准方面，发布了团体标准9项、团体标准修改单4项、完成送审稿审查3项。在标准国际化方面，SC6国内技术对口工作稳步推进，第一季度共对内流通国际提案文件34份，向国际上反馈投票/意见7份；我国主导/参与的“无线局域网接入控制”、“未来网络—基于代理模型的服务质量”、“OID解析系统（ORS）结构”、“对象标识符解析系统（ORS）运营机构规程”等多项国际标准提案获推进；在其他TC和SC中，成员单位多项提案也获进展；ISO/IEC JTC 1/SC 6/WG 1（系统间远程通信和信息交换）第39次工作组会议，11位中国专家均来自我们共同体的成员单位，无线网络安全标委会副主任委员黄振海作为SC 6/WG 1召集人主持会议。

WAPI产业联盟市场总监简练报告了2022年第一季度标准产业市场应用阶段性进展，重点包括：芯语慧联公司、西电捷通公司、三凯威公司联合技术攻关并推出了首套全国产化、高安全、低功耗的WAPI MCU物联网终端模组，填补了产业空白。联盟发布的《无线局域网安全技术规范》《信息安全技术 证书管理测试规范》《信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别》等9项团体标准和《无线局域网产品工程化实现指南》4项团体标准修改单，为无线网络安全技术的持续创新演进和快速服务市场需求，提供了支撑和保障。对上述工作，业内多家媒体进行了报道。

在技术产业新动态分享环节，北京华信傲天网

络技术有限公司产品管理总监范小伟和西安芯语慧联信息科技有限公司总经理童伟刚，做《国产FEM在华信傲天企业级AP的选型及应用实践》和《首款全国产高安全低功耗WAPI MCU可信模组——TH6160》报告。其中，华信傲天携手麓慧科技，完成了无线局域网高性能AP的国产FEM器件pin-to-pin替代，让量产产品实现了高品质无缝替代，解决了供应链安全问题。西安芯语慧联信息科技有限公司的WAPI MCU可信模组，有效满足了当前“低功耗物联网设备快速实现安全无线局域网连接”的市场需求，解决了此前“普通模块功耗偏高、低功耗模块需要二次开发”产业难题，保障了各行各业用户实施WAPI安全方案时的高效率、系统性和完整性，适用于更多行业的细分场景。

T/WAPIA 046—2021《无线局域网安全技术规范》的项目编辑、无线网络安全技术国家工程研究中心张变玲对该团体标准进行了宣贯。当前，全球网络安全面临“量子计算攻击威胁、字典攻击”等新的安

全风险和挑战，我国《密码法》、《数据安全法》、《个人信息保护法》等法律法规，对加强用户身份保护提出了明确的要求。结合产业市场的需求，WAPI产业联盟迅速组织开展了《无线局域网安全技术规范》的标准创新工作，本团体标准使用了安全性更高的原子密钥建立与实体鉴别（AKEA）机制，适配了国密算法SM2和SM3，增强了主动身份保护、抗字典攻击和缓解量子计算暴力攻击等安全性。

在已立项项目讨论阶段，与会人员对《无线局域网系统 第1部分：工程设计规范》（送审稿）、《无线局域网系统 第2部分：工程施工规范》（送审稿）、《无线局域网系统 第3部分：验收测试方法》（送审稿）、《无线网络安全技术术语》（草案稿）进行了集中讨论，经会上协商一致，形成了相关意见和决议。

会上，还进行了标准国际化专题讨论和标准化知识交流与培训。



WAPI产业联盟启动63项团体标准复审工作

WAPI产业联盟 米 东

为规范WAPI产业联盟团体标准管理，掌握标准的技术状态及实施应用情况，提升联盟团体标准的适用性，根据联盟标准化管理制度的有关要求，以及无线网络安全标准化委员会的工作安排，WAPI产业联盟于2022年4月1日启动团体标准复审工作。

标准复审范围为截至2022年6月底实施满3年的WAPI产业联盟团体标准，本次纳入复审范围的共计63项。按工作组技术领域分类，涉及总体工作组（WG1）、网络安全工作组（WG2）、无线网络工作组（WG3）、产品与解决方案工作组（WG4）、互操作测试工作组（WG5）等五个工作组。

本次标准复审工作将围绕标准的技术内容、标准实施应用情况、标准的协调性、标准文本质量等方面展开评价，并根据复审结论对相关标准进行修订完善。通过标准复审，进一步提升WAPI产业联盟团体标准的适用性、规范性、时效性和协调性，使之高质量地为市场与产业服务。

复审程序分三个阶段，包括工作组复审阶段、总体组审议阶段、标委会审议及报批阶段。计划2022年上半年完成上述WAPI产业联盟团体标准复审工作，并通过联盟公共服务平台向社会通告标准复审结论。

WAPI产业联盟发布 《无线局域网产品工程化实现指南》系列 4项团体标准修改单

WAPI产业联盟 简 练

日前，WAPI产业联盟发布了《无线局域网产品工程化实现指南》系列4项团体标准修改单，以保障不同厂商的无线局域网产品之间在启用服务质量（QoS）等扩展功能时仍具有良好的WAPI安全协议互通性。

近年来，随着WAPI技术的发展和IEEE 802.11n/e/p/ad/ac/ax等技术的演进，两者在技术上的融合为无线局域网提供了安全、高速率的解决方案，越来越多的设备生产厂商开始关注这些融合技术的应用。《无线局域网产品工程化实现指南》系列团体标准详细规范了WAPI与IEEE 802.11 n/e/p/ad/ac/ax等技术融合过程中需要特别注意的技术细节，用于指导更高速率WAPI产品的创新和生产制造。

本次这4项修改单是对T/WAPIA 007.1—2010《无线局域网产品工程化实现指南 第1部分 WAPI

与IEEE 802.11n》、T/WAPIA 007.8—2016《无线局域网产品工程化实现指南 第8部分 WAPI与IEEE 802.11ac》、T/WAPIA 007.9—2016《无线局域网产品工程化实现指南 第9部分 WAPI与IEEE 802.11ad》、T/WAPIA 007.10—2020《无线局域网产品工程化实现指南 第10部分：WAPI与IEEE 802.11ax》4项团体标准的补充和扩展，使其更加适用于基础通信模块的扩展规范，确保无线局域网产品能够提供鉴别和保密通信，并且能与其他厂商的无线局域网产品之间具有良好的WAPI安全协议互通性。

修改单内容主要包括WPI完整性校验数据的组成方法和数据分组序号（PN）的使用规则。WPI完整性校验数据中，细化了帧头QoS控制字段校验规则，最大限度地保障帧头字段内容的完整性；PN部分扩展了在QoS模式下发送端和接受端PN使用和重放攻击检测策略，更好地支持QoS模式下的数据完整性。

WAPI产业联盟《无线局域网系统》系列团体标准 进入报批阶段

WAPI产业联盟 米 东

2022年3月31日，WAPI产业联盟组织召开无线网络安全标准化委员会临时扩大会议，审议《无线局域网系统 第一部分：工程设计规范》《无线局域网系统 第二部分：工程施工规范》《无线局域网系统 第三部分：验收测试方法》3项系列团体标准的送审意见处理情况。为使问题得到充分探讨，特别邀请了对三项标准规范有积极建设性意见的委员和业内专家，经过充分讨论，达成一致意见，三项系列团体标准已进入报批阶段，目前编制组正在完善报批稿及相关材料。

十三五以来，我国无线局域网系统工程等新型基础设施建设明显提速，为进一步促进无线局域网的发展，规范无线局域网系统工程施工，由无线网络安全技术国家工程研究中心申请，WAPI产业联盟下达了《无线局域网系统》系列团体标准的立项计划，组织有关单位，开展标准研制工作。

本系列标准依据 GB 15629.11系列、GB/T 32420—2015无线局域网测试规范等国家标准，结合无线局域网在各行业领域的实际需求，规范了相应的工程设计原则及要求、施工过程管理、施工规范等内容。同时在GB/T 32420—2015基础上，分析研究不同行业针对WAPI无线局域网系统的需求，编制了无线局域网系统验收测试方法，该方法覆盖了无线局域网系统功能、网络安全、网络性能等方面的验收测试，规范了无线局域网系统的工程验收测试工作。

《无线局域网系统》系列团体标准的制定和发布，将为行业内无线局域网络建设单位、施工单位、监管部门等提供技术支撑，为无线局域网系统建设中工程设计、工程施工、验收测试提供专业依据，从而保障各行业安全无线局域网建设质量。

《WAPI规模组网技术规范》团体标准立项

WAPI产业联盟 简 练

2021年12月15日，无线网络安全标准化委员会依据WAPI产业联盟《团体标准制修订工作程序》的有关规定，对团体标准《WAPI规模组网技术规范》完成立项评审，批准立项。

对于WAPI技术的规模应用，特别是大规模多区域运营，需要部署多个鉴别服务器（AS）。AS之间的相互关系、WAPI用户如何实现便捷的漫游，还缺少

相应的组网和业务规范流程，有必要研究多AS部署的WAPI组网技术，并制定相应的组网规范。

本项目拟要解决的主要问题有：多AS组网架构，WLAN网络与WAPI证书签发系统接口，WAPI用户本地接入鉴别流程，WAPI用户跨AS域漫游接入鉴别流程等。

WAPI产业联盟团体标准《无线网络安全 术语》

即将进入征求意见阶段

WAPI产业联盟 米 东

随着无线局域网（WLAN）、射频识别（RFID）、近场通信（NFC）、移动通信4G/5G等无线网络的普及和广泛应用，在为日常生活工作带来便利的同时，网络安全威胁也伴随左右。因此，世界各国持续加大网络安全投入，不断推动网络安全产业发展，相应的技术创新、标准研制、产业合作交流日益增多。在此过程中WAPI产业联盟发现，在无线网络安全领域，尚存在很多基础概念不准、业界认识不清、用户理解不一致等问题，导致许多概念术语使用混乱，影响行业管理、企业、科研机构、用户的交流和融通。例如无线局域网，英文规范简称为WLAN，但目前部分场合使用Wi-Fi代替，在技术和应用方面均不规范。实际上，Wi-Fi是美国发起的无线局域网领域产业联盟（Wi-Fi联盟）的商标，指代Wi-Fi联盟自身，以及通过Wi-Fi联盟认证的产品所采用的WLAN技术和标准，在全球无线局域网领域，Wi-Fi代表一种特定的技术和标准实现。用“Wi-Fi”指代无线局域网（WLAN），相当于用美国职业篮球联赛（NBA）指代整个篮球运动，不符合《中华人民共和国国家通用语言文字法》规定的需要使用外国语言文字的、应当用国家通用语言文字作必要注释的规定，

也一定程度上将因错误概念的误导和固化而导致我国无线局域网产业发展受到限制，丧失独立自主性和创新发展空间。类似这样的概念和术语，亟需制定相应的标准予以规范。

术语是在特定学科领域用于表示概念的称谓的集合，是通过文字来表达或限定科学概念的约定性语言符号，是思想和认识交流的工具，也是产业交流和演进的基础支撑。为统一无线网络安全领域的术语和定义，消除不同行业、组织之间技术交流的屏障，为网络信息安全领域基础性认识和理解提供依据，WAPI产业联盟启动《无线网络安全 术语》团体标准制定工作，该团体标准将界定无线网络安全技术领域中基本或通用概念的术语和定义，并对其进行分类，适用于对无线网络安全技术概念的理解、其他无线网络安全技术标准的制定以及无线网络安全标准化委员会和WAPI标准产业共同体内交流。该项目于2020年5月正式立项。

2022年4月，标准项目组召开项目组会议，与会专家就《无线网络安全 术语》草案稿内容及编制说明进行了充分研讨并达成一致意见。根据联盟团体标准制修订程序，目前该团体标准正在完善草案稿，即将进入征求意见阶段。

华为无线接入点系列产品通过联盟测试

WAPI产业联盟 王立华

2022年3月，华为技术有限公司（以下简称华为）的无线接入点系列产品通过了WAPI产业联盟无线局域网鉴别与保密基础结构（WAPI）互通性、完整性及性能测试。联盟为上述产品出具了测试报告。

本次测试通过的无线接入点型号为：AP7060DN、AirEngine5700、AirEngine6700。其中，AirEngine6700通过了802.11ax模式下的WAPI协议互通性测试，具有速度快、覆盖广、漫游稳、体验好等特点。上述产品能够满足企业、教育、金融、医疗、政府、制造、商业等领域和场景的数字化、无线化、物

联化办公与生产作业需求。

联盟测试实验室依据GB/T 32420-2015《无线局域网测试规范》和T/WAPIA 037.2-2021《无线局域网测试 第2部分：设备测试规范》，对上述设备进行了协议互通性、完整性及功能测试。针对产品测试过程的问题，联盟测试实验室和华为通过积极沟通和协同分析研究，顺利地完成了产品整改工作。

上述通过测试的产品，将服务电力行业等基于WAPI的可信WLAN规模建设。

山东思极无线接入点系列产品通过联盟测试

WAPI产业联盟 王立华

2022年3月，华为技术有限公司（以下简称华为）的无线接入点系列产品通过了WAPI产业联盟无线局域网鉴别与保密基础结构（WAPI）互通性、完整性及性能测试。联盟为上述产品出具了测试报告。

本次测试通过的无线接入点型号为：AP7060DN、AirEngine5700、AirEngine6700。其中，AirEngine6700通过了802.11ax模式下的WAPI协议互通性测试，具有速度快、覆盖广、漫游稳、体验好等特点。上述产品能够满足企业、教育、金融、医疗、政府、制造、商业等领域和场景的数字化、无线化、物

联化办公与生产作业需求。

联盟测试实验室依据GB/T 32420-2015《无线局域网测试规范》和T/WAPIA 037.2-2021《无线局域网测试 第2部分：设备测试规范》，对上述设备进行了协议互通性、完整性及功能测试。针对产品测试过程的问题，联盟测试实验室和华为通过积极沟通和协同分析研究，顺利地完成了产品整改工作。

上述通过测试的产品，将服务电力行业等基于WAPI的可信WLAN规模建设。

南京才华科技UHF智能手持终端通过联盟测试

WAPI产业联盟 王立华



南京才华科技UHF智能手持终端

日前，南京才华科技集团有限公司（以下简称南京才华科技）的资产管理专用机具——UHF智能手持终端通过了WAPI产业联盟无线局域网鉴别与保密基础结构（WAPI）互通性、完整性及性能测试。联盟为上述产品出具了测试报告。

由于Wi-Fi的安全缺陷问题，无法满足各行各业关键信息基础设施无线局域网建设和数据安全传输的要求，因此各行业纷纷选择自主可控的WAPI技术产品。

南京才华科技的UHF智能手持终端采用了手持式设计，小巧便捷。设备同时具备了识别RFID电子标签、条形码、二维码、军用GM码的功能，支持2.4/5GHz双频接入，可通过WAPI安全无线局域网，将采集的信息实时传输至后台管理系统。

联盟测试实验室依据GB/T 32420-2015《无线局域网测试规范》和T/WAPIA 037.2-2021《无线局域网测试 第2部分：设备测试规范》，对上述设备进行了协议互通性、完整性及功能测试。测试过程中，联盟测试实验室和设备厂商克服当前突发的疫情困难，通过远程联调形式互动，顺利完成了产品测试工作。

当前，安全无线局域网（WAPI）正广泛服务政务、海关、能源、金融、交通等建设需求，有效保护了我国重要行业/领域的网络安全和数据资产不受侵害。多厂商多种类的WAPI业务终端和专用机具在现场巡检、仓储物流、物资管理、安防监控等场景中表现突出。

山东思极科技有限公司加入WAPI产业联盟 协力推动国家电网WAPI建设

WAPI产业联盟 周 园

2022年3月15日，经联盟理事会批准，山东思极科技有限公司正式加入WAPI产业联盟，联盟会员单位增至110家。

山东思极科技公司（以下简称“山东思极”）成立于2020年，由国网山东省电力公司和国网信通产业集团合资成立，是国家电网有限公司的全资子公司。作为国家电网战略性新兴产业的重要载体，山东思极肩负着国家电网落实“碳达峰、碳中和”、“数字新基建”、“大数据”等重要战略责任，是山东省域电力大数据、电力基础设施、数字基础设施、电力无线通信等核心资源的运营主体。



据山东思极介绍，根据国网山东省调的安排，山东思极正有序推进无线局域网WAPI系统的试点应用工作，目前已与主流厂商展开合作，在济南、烟台、东营等地市变电站，德州、济宁、济南市莱芜区等地区分布式光伏厂站开展了WAPI试点应用。下一步将总结试点单位建设经验，在山东省域全面推动变电站、整县光伏无线局域网WAPI系统的部署。

近年来，山东思极秉承“资源共享、互利共赢”的理念，立足“为数字新基建充电，为能源互联网赋能”的重要使命，积极布局撬动山东省数字化新兴产业发展，致力于建设成为“具有国网品质的一流数字化综合服务商”。期间，山东思极充分发挥电网、数据、品牌和技术优势，以服务国家战略大局、解决企业数字化发展痛点难点为价值体现，创新打造“融、云、海、网、新、维”6大业务板块，规划“基础资源商业运营、云边协同算力服务、大数据增值变现、公网通信集约运营、5G专网建设与应用、北斗及地理信息服务、新能源服务、智慧化运维”8类核心业务，完善产业链、打造创新链、整合资源链、实现价值链，深化实施数字赋能行动，支撑构建以新能源为主体的新型电力系统，助力实现“双碳”目标，积极打造数字化新兴产业的形象窗口、文化名片和宣传阵地，助力高品质、智慧化、现代化“数字山东”建设。

目前，山东思极探索并走出了一条创新发展之路，建成了全国首套省域5G电力示范网，构建了国内首个电力行业5G专网运营平台，创新实现了全省720余万张电力物联网卡的精益化集约管控，获批山东省能源互联网大数据发展创新实验室的数字化企业，全省共享配电杆路1.7万公里、电力杆塔867基，助力节碳达20余万吨；签约了“电力基础资源共建共享”、“5G电力专网切片战略合作”数字化项目；公司的“双碳背景下智能电网5G规模化应用”获得第四届5G“绽放杯”能源赛道一等奖、“智慧化5G模组切片安全项目”获工业互联网赛道三等奖。此外，山东思极还荣获了2021年度“国网山东省电力公司先进单位”、“经营创新一等奖”等荣誉。

深圳市国电科技通信有限公司加入WAPI产业联盟

WAPI产业联盟 周 园



日前经联盟理事会批准，深圳市国电科技通信有限公司正式加入WAPI产业联盟，联盟会员单位增至111家。

深圳市国电科技通信有限公司（以下简称“深国电”），是国家电网有限公司下属企业，也是国家和深圳市高新技术企业。深国电成立于2003年，注册资本3.25亿元，总部位于深圳市龙华区，另在深圳福田、北京、银川、武汉、兰州等地设有办公区，现有员工580余人。

据深国电介绍，目前正在紧锣密鼓地开展电力行业WAPI工业级产品研发工作，计划今年完成WAPI工业路由器、室内AP、室外AP、CPE、证书鉴别服务器等产品的开发和测试。

值得关注的是，深国电致力于支持母公司（智芯公司）建设成为中国特色国际领先的工业芯片企业，坚持“芯片平台+业务应用”布局，聚焦“物联”及数字化、智能化趋势，持续深耕电力物联业务，加快同源技术向工业物联领域突破应用，构建起芯片器件、物联感知、智能终端、平台数据、智能制造、集成运维六大产品线，推动工业领域核心芯片国产化替代。其高速载波系列产品在国网市场占有率多年保持第一，并已广泛应用于南方电网、地方电力、澳门电力以及其他工业领域。低压配用电终端、智能断路器、物联设备管理组件等核心产品和解决方案已在多个网省公司实现规模化应用。



数字认证：

大众“免费Wi-Fi”暗藏陷阱
民生行业无线应用WAPI才是标配

数字认证

2022年央视315晚会爆料：在大众手机上的应用商店里，有很多“免费Wi-Fi连接”服务的APP。经过315信息安全实验室实际测试，用户不但无法通过APP免费连接Wi-Fi网络，反而在不知情的情况下，被APP频频访问隐私数据，下载未经授权许可的应用程序，甚至连广告弹窗都无法关闭。



315晚会曝光截图

事实上，Wi-Fi应用不安全的话题早已经是老生常谈了。这些年更是动辄爆出黑客冒充公共Wi-Fi“钓鱼”、Wi-Fi密码被破解、通过会话拦截入侵企业Wi-Fi网络等新闻事件。与广大消费市场Wi-Fi应用“水深火热”相反的是，在国家重要行业，尤其是关系到国计民生的基础设施行业，却很少被爆出“无线应用不安全”的新闻。

行业青睐WAPI

这很大一部分功劳要归结于我国政府布局深远——早在2003年，我国就发布了国家强制标准GB 15629.11/1102-2003批准，即WAPI标准，这也是我国唯一的无线局域网安全国家标准。与Wi-Fi相比，WAPI规避了Wi-Fi自身在技术架构上的重大安全缺陷，技术可控更有保障。

由于国家基础设施事关千家万户、社会稳定和国家安全，其网络安全的重要性和紧迫性不言而喻，所以从那时起，WAPI就陆续被部署在海关、金融、能源、政务、公安、交通、医疗、教育等重要行业的信息网络

基础设施中，应用场景也开始涉及到工业互联网、物联网、车联网等。

近年来，随着国家连续出台了《网络安全法》、《密码法》、等保2.0、《数据安全法》等法律法规，国内重要行业对于安全可控的无线网络需求愈发明确。WAPI因其产业成熟度高、不增加采购成本、建设配套条件丰富、有效保护信息通道安全和数据资产安全等优势，也受到越来越多行业用户的青睐。

北京数字认证股份有限公司（以下简称“数字认证”）是我国WAPI产业联盟的重要成员单位，也一直在积极推进WAPI的落地实践。

经过自主研发，数字认证推出无线统一认证管理系统WUAS。WUAS产品是WAPI无线接入协议三元架构中的认证元，是一款基于国密算法的WAPI无线协议安全接入的安全认证类产品，可以实现数字凭证签发、数字身份管理、终端设备的综合管理，并可以通过策略配置实现终端设备及数字身份的身份鉴别及访问控制，目前已在国内多项重大行业项目中广泛应用：

某大型国际机场

2019年，某大型国际机场作为WAPI技术在国家重大工程中落地并产生实际效益的标杆项目，航站楼业务区域实现了WAPI网络全覆盖，为机场内日常办公和开展海关、边检、运维等业务提供支撑保障。

随着WAPI无线网络运营不断深入，各重大项目中涉及业务机具形态各异、种类繁多，需要以统一规制安装WAPI证书。数字认证作为项目组重要成员，牵头开发了数字证书一键申请下载安装应用技术，解决了数字证书大批量安装的问题。同时，数字认证还参与发布了团体标准《GB/T 32420实施指南 第2部分：无线局域网设备测试》，指导精细化产品测试，提升检测效率，保障了项目高质量按期完成。

某能源国有企业

该企业开发了新兴业务，包括视频监控、巡检机器人、移动作业和传感器业务等，需要建设WAPI作为现有光纤通信的延伸，满足各类业务安全的、泛在的、灵活的“最后一公里”无线接入需求。

数字认证公司WUAS产品，提供了WAPI证书的签发，以及业务端的身份认证与授权，充分保障了数据传输的安全和用户信息的完整。

某国家部级单位

在该单位的WAPI无线局域网规划建设项目中，为了满足总部及全国分支机构内部建设无线局域网的需求，数字认证公司WUAS产品在总部和3个分支机构内进行了部署，发挥可管可控可追溯的作用，也达到了无线局域网建设要求。

如今，不同行业的应用场景对WAPI证书管理方案提出了差异化的需求，数字认证也在不断完善WAPI证书管理服务，为行业用户精心打造了企业级、平台级、互联网运营级等多种WAPI证书管理解决方案，适用于各类WAPI证书在不同应用场景下的颁发。

2022年，WAPI产业群体仍在不断壮大，为保障国家安全、推动经济高质量发展贡献更磅礴的力量。数字认证也将一如既往，为行业用户提供高质量的技术服务支撑。

MTK发布天玑8000 全线支持WAPI

天极网

2022年3月1日,MediaTek发布天玑8000系列5G移动平台,包括天玑8100和天玑8000,为高端智能手机带来先进的网络连接、显示、游戏、多媒体和影像技术。

天玑8100与天玑8000 5G移动平台均支持WAPI,均采用台积电5nm制程,拥有出色的性能和能效表现。两款平台采用了八核CPU架构设计,天玑8100搭载4个主频高达2.85GHz的Arm Cortex-A78核心和4个ArmCortex-A55能效核心,天玑8000的Cortex-A78核心主频则为2.75GHz。两个平台采用了Arm Mali-G610六核GPU,搭载MediaTek HyperEngine5.0游戏引擎,支持四通道LPDDR5内存与UFS3.1闪存,可提供高速数据传输。天玑8000系列通过平台的全局能效优化,为用户带来流畅且稳定的高帧率游戏体验,其低功耗特性为终端的持久续航和温控奠定了扎实基础。

上述产品预计2022年第一季度至第二季度陆续上市。

新华三连续13年WLAN市场份额第一

新华三

近日,全球权威数据公司IDC发布《中国WLAN市场季度跟踪报告,2021Q4》:紫光股份旗下新华三集团以28.4%的市场份额排名第一。2009年至2021年,新华三已连续13年稳居中国企业级WLAN市场第一。

结合未来建设智能园区网需要兼具“无线优先、业务保障、一网承载、智能运维”四大特点,新华三提出了以“智快体验”的产品理念。目前能够为30+行业专属场景提供定制化解决方案,在建网、用网、护网3个方面,实现端到端的全方位保障,同时自主研发了无线iRadio、iStation、iHeal、iEdge技术,在射频优化、漫游接入、网络自动化和边缘保障等方面不断优化无线网络,为行业用户提供高速稳定无线网络的同时,切实推动其业务转型创新,提升百行百业场景化用户体验。

2021年,新华三在冬奥会、中南大学、深圳地铁等项目中均获得良好评价。

信锐技术助力广西医科大学完成数字化转型升级

通信世界

日前在信锐助力下，广西医科大学教育信息化转型升级已取得初步成效。目前已为学校部署了近3600台AP提升用网体验，并联动物联网拓展，在满足全校区无线网络覆盖的同时完成学校智慧化建设需求。

全场景无线覆盖 实现全校室内外高质量无线网络全覆盖，满足校园师生的日常学习和办公需求。	认证划分更安全 无线网络具备独立的访客信号以及能给来访人员进行上网权限管控和校园文化信息推送。
统一运维管理 新旧校区规模较大，设备数量多，需要能够实现统一运维管理，降低运维人员工作压力。	物联网扩展 管理平台支持进行物联网扩展为智慧校园物联网建设做好准备。

中兴“新支点”国产操作系统 用户均免费使用

网 易

2022年3月，据中兴新支点官方信息，新支点操作系统进行升级更新，将桌面模式里的个人版和企业版合并升级为专业版，并宣布无论是个人用户、企业用户，还是政府单位，全部都免费正版授权使用新支点操作系统里的桌面模式，定制或技术服务除外。

据中兴新支点官方说法，此次将桌面模式向个人和企业都免费开放使用，是希望无论是个人还是企业都一起参与进来，以开放的心态，推动国产操作系统的快速发展。

北京科创资源辐射津冀

京津冀实现地区生产总值9.6万亿

创新创业中关村

日前，北京市统计局发布数据显示，2021年，京津冀实现地区生产总值9.6万亿元。与2019年相比，京津冀三地GDP两年平均分别增长4.7%、3.9%和5.1%。

生产领域中，北京规模以上工业增加值比上年增长31%，其中医药行业、电子行业贡献突出；津冀规模以上工业增加值分别增长8.2%和4.9%，采矿业，制造业，电力、热力、燃气及水生产和供应业三大门类生产全面增长。服务业运行稳定，三地服务业增加值比上年分别增长5.7%、6.7%和7.7%，其中信息服务业均实现两位数增长。

在京津冀三地，高精尖产业加快成长，三地创新能力不断提升。据统计，2021年，北京高技术产业和战略性新兴产业增加值占GDP的比重均在2成以上，智能化产品生产加速，工业机器人产量在上年两位数增长的基础上，同比增长达到56%。天津高技术产业和战略性新兴产业增加值两年平均分别增长9.9%和7.3%，明显快于全市工业平均水平，服务机器人、新能源汽车、集成电路产量分别增长1.7倍、54.3%和53.2%。河北规模以上工业高新技术产业增加值增速比上年加快5.4个百分点，占规模以上工业增加值比重比上年提高2.1个百分点，高端装备制造产业八大行业实现全面增长。

浅谈《原子密钥建立与实体鉴别》系列团体标准

无线网络安全技术国家工程研究中心，西电捷通公司

赵晓荣，李琴，铁满霞，黄振海

1. 《原子密钥建立与实体鉴别系列》团体标准概述

2021年12月，中关村无线网络安全产业联盟（WAPI产业联盟）发布了T/WAPIA 045《信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别》系列7项团体标准，首次提出原子密钥建立与实体鉴别（Atomic Key Establishment and entity Authentication, AKEA）的概念，并制定了多种具体的AKEA机制。该系列团体标准的起草单位主要包括西安西电捷通无线网络通信股份有限公司、无线网络安全技术国家工程研究中心、WAPI产业联盟、国家密码管理局商用密码检测中心、国家无线电监测中心检测中心、北京数字认证股份有限公司、中国网络安全审查技术与认证中心、中国通用技术研究院、国家信息技术安全研究中心等。

T/WAPIA 045系列 原子密钥建立与实体鉴别

1	T/WAPIA 045.1	信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别 第1部分：服务和协议
2	T/WAPIA 045.2	信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别 第2部分：轻量级原子密钥建立与实体鉴别
3	T/WAPIA 045.3	信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别 第3部分：采用证书的原子密钥建立与实体鉴别
4	T/WAPIA 045.4	信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别 第4部分：采用预共享密钥的原子密钥建立与实体鉴别
5	T/WAPIA 045.5	信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别 第5部分：采用预共享密钥与证书组合的原子密钥建立与实体鉴别
6	T/WAPIA 045.6	信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别 第6部分：三元移动通信系统安全-基于对称密钥的原子密钥建立与实体鉴别
7	T/WAPIA 045.7	信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别 第7部分：三元移动通信系统安全-基于非对称密钥的原子密钥建立与实体鉴别

图1 T/WAPIA 045系列团体标准

2. 相关术语概念

T/WAPIA 045系列团体标准首次提出原子密钥建立与实体鉴别（AKEA）的概念，为便于理解AKEA概念以及该系列标准，首先给出如下两个术语概念：

（1）实体鉴别（entity authentication）：实体鉴别指证实一个实体就是所声称实体的过程（ISO/IEC 9798-1:2010），也即某一实体确信与之关联的实体正是所需要的实体的过程。在实体鉴别过程中，身份由某次通信连接或者会话的参与者提供，实体鉴别在连接建立或在数据传送阶段的某些时刻发生；

(2) 密钥建立 (key establishment) : 密钥建立指为一个或多个实体产生一个可用的共享的秘密密钥的过程, 包括密钥协商、密钥传送 (ISO/IEC 11770-1:2010) ; 通过该过程创建的密钥通常用于实体建立连接后的保密通信过程, 用于实现数据的机密性和完整性。

从上述定义可以看出, 实体鉴别与密钥建立是两个独立的术语概念。T/WAPIA 045系列团体标准在前述两个术语概念基础上首次提出了原子密钥建立与实体鉴别AKEA。

原子是化学元素的最小单位, 在化学反应中不可再分割。原子性则指事务的不可分割性, 一个事务的所有操作要么不间断地全部被执行, 要么任何操作也没有被执行。

T/WAPIA 045中首次提出的原子机制, 指一种向两个对等实体提供一项或多项服务的机制。首先, 两个实体均无法在接收到最后一条消息之前完成任何服务; 其次, 每个实体均可以检测到交换的所有消息的内容和顺序的任何更改, 包括接收到的最后一条消息。

T/WAPIA 045中首次提出的AKEA, 指一种原子机制, 使用不可还原且不可分割的消息交换序列, 为两个对等实体提供实体身份鉴别和密钥建立, 任何实体在收到最后一条消息之前均无法完成对其对等实体的身份鉴别或密钥建立。

AKEA的提出, 标志着在基础网络安全协议技术演进中实体鉴别和密钥建立两个概念的融合。AKEA的原子性意味着以下特性:

(1) 隐式密钥确认: 确保那些通过身份鉴别的实体都持有已建立的密钥。注意, 不可能发生这样的情况: 首先由实体A和B进行身份验证, 然后由实体A和C进行密钥建立, 以至于最终C拥有密钥, 而A以为是B拥有密钥;

(2) 整体性: 两个实体均不能在收到最后一条消息之前验证其对等实体或建立密钥;

(3) 完整性: 每个实体均可以检测交换的所有消息的内容和顺序的任何更改, 包括最后收到的消息;

(4) 不可分割性: 防止接力攻击的组合机制。机制执行结束后, 两个实体将获得相同的结果 (成功或失败), 并且在成功的情况下, 将获得对端身份证明和拥有相同密钥。

3. 相关标准情况

3.1 国际标准

全球技术标准体系历经演进, 与实体鉴别及密钥建立相关的信息安全基础共性技术标准化工作主要集中在国际标准化组织/国际电工委员会第一联合技术委员会信息安全分委会 (ISO/IEC JTC 1/SC 27), 实体鉴别系列国际标准对应ISO/IEC 9798系列, 密钥建立系列国际标准对应ISO/IEC 11770系列。

ISO/IEC 9798系列现行有效标准有6项: 第1部分是总则, 规范了使用安全技术的实体鉴别机制的模型、一般要求和约束条件; 第2部分是采用对称加密算法的机制; 第3部分是采用数字签名技术的机制; 第4部分是采用密码校验函数的机制; 第5部分是采用零知识技术的机制; 第6部分是采用人工数据传递的机制。其中ISO/IEC 9798-3自1998年后20多年间仅有的两次技术标准演进均由我国推动, 该部分标准中所有在线实体

鉴别技术均由中国贡献。ISO/IEC 9798-3:1998/Amd.1:2010中纳入了我国自主研发的2项三元对等实体鉴别（双向鉴别）技术；ISO/IEC 9798-3:2019中进一步丰富了实体鉴别国际标准技术体系，增加了单向鉴别、多在线可信第三方等3项三元对等实体鉴别机制。这五项自主研发的鉴别机制有效防范了信息未经授权使用、误用等网络信息安全隐患。



图2 ISO/IEC 9798系列标准

ISO/IEC 11770系列现行有效标准有7项（第1至第7部分），第8部分正在制定中。第1部分是框架，规范了建立密钥管理机制所基于的通用模型，给出了ISO/IEC 11770所有部分通用的密钥管理基本概念，规范了密钥管理服务的特征，建立密钥材料生命周期管理的一般原则以及建立密钥分配的概念模型；第2部分是采用对称技术的机制；第3部分是采用非对称技术的机制；第4部分是基于弱秘密的机制；第5部分是群组密钥管理；第6部分是密钥派生；第7部分是基于口令的跨域鉴别密钥交换；第8部分是基于口令的密钥派生（制定中）。



图3 ISO/IEC 11770系列标准

3.2 国家标准

国家标准体系中，与实体鉴别及密钥建立相关的信息安全基础共性技术标准化工作主要集中在全国信息安全标准化技术委员会（TC 260），实体鉴别系列国家标准对应GB/T 15843系列，密钥建立系列国家标准对应GB/T 17901系列。



图4 GB/T 15843系列标准

GB/T 15843系列国家标准对应ISO/IEC 9798系列国际标准，也划分为6个部分，分别等同采用国际标准ISO/IEC 9798的对应部分。随着我国参与制定的国际标准ISO/IEC 9798-3:2019的发布，目前GB/T 15843.3正在推动相应的修订，已进入报批阶段。



图5 GB/T 17901系列标准

GB/T 17901系列国家标准对应ISO/IEC 11770系列国际标准，拟包含上述6部分，目前第1和第3部分已发布。GB/T 17901.1—2020修改采用国际标准ISO/IEC 11770-1:2010，GB/T 17901.3—2021修改采用国际标准ISO/IEC 11770-3:2015，这两部分和国际标准的区别主要是适应我国密码算法使用等相关要求。

3.3 技术标准演进需求

随着安全需求的不断发展，在实际的通信环境中，仅需要身份鉴别或仅需要实体之间保密通信（需首先完成密钥建立）的场景非常少见，若要在一个完整的通信过程中既实现实体鉴别又实现保密通信，则需要实体鉴别机制和密钥建立机制二者结合。目前业界通常的做法是将上述两个标准体系中分别规范的实体鉴别和密钥建立机制简单叠加、组合，这种做法在流程上交互消息会比较多，在叠加的过程中还需要考虑安全衔接等技术细节。因此，亟需一种原子机制的概念及标准，以对同时实现实体身份鉴别和密钥建立两个功能的新机制进行规范。

T/WAPIA 045 AKEA系列7项团体标准，就是在上述需求背景下首次提出了原子机制、AKEA的术语概念，并规范了一系列具体的AKEA机制。

4. 原子密钥建立与实体鉴别系列团体标准

4.1 T/WAPIA 045.1—2021

T/WAPIA 045.1—2021是AKEA系列第1部分：服务和协议，本部分规范了AKEA的服务和协议，用以支持实体间安全的通信和信息交换，还规范了AKEA可扩展的封装协议（EEP）。

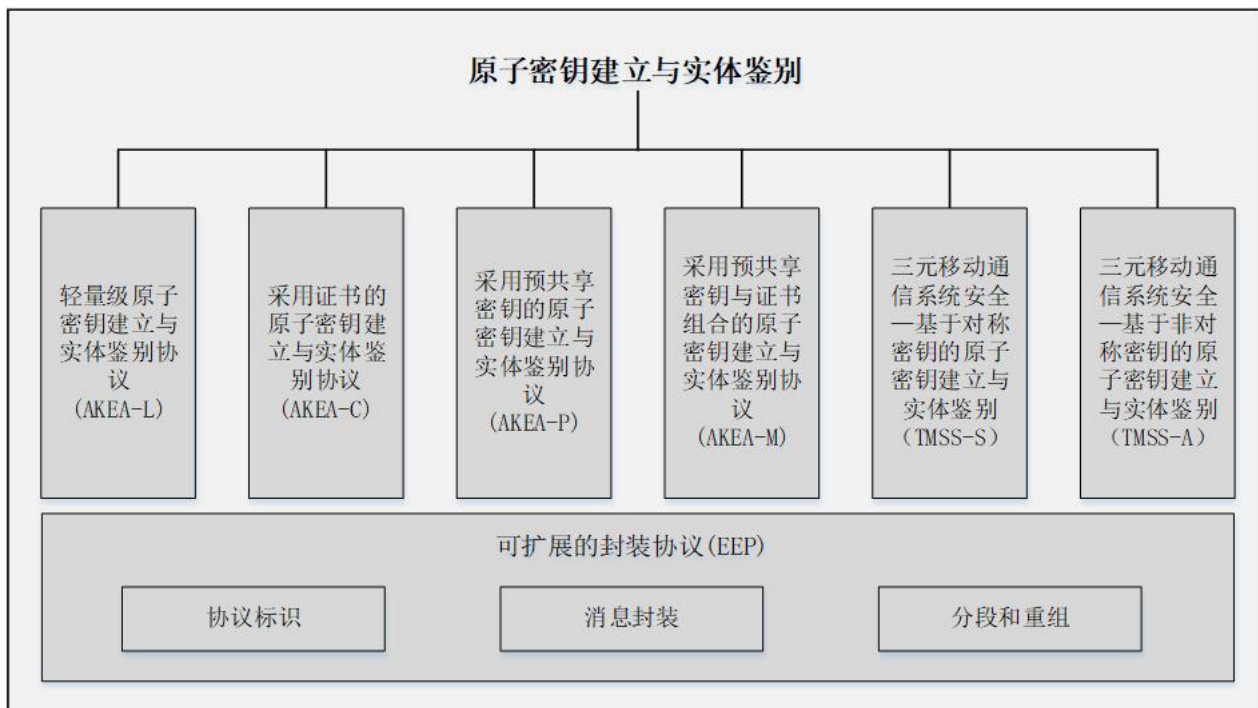


图6 AKEA标准体系框架

本部分第5章规范了AKEA系列标准各协议使用到的数据元素及格式，是AKEA系统标准后6部分的基础。本部分第6章规范了AKEA架构、实体、协议构成及各协议关系。本部分第7章规范了AKEA提供的6种鉴别服务

及密钥建立服务，明确了对无鉴别的支持，但从安全的角度不建议使用无鉴别机制。本部分第8章规范了AKEA协议，其中EEP协议将需要传输的消息、分片数据按照可管理的分组进行处理，可选地进行压缩、数据完整性计算、加密处理，然后传送；而接收到的数据首先进行解密处理、数据完整性校验、解压缩，重组后发送给更高一层的客户端。EEP协议可用于封装AKEA系列后面几部分规范的具体的AKEA机制，是AKEA系列标准的公共基础技术组件，通过在消息封装头部携带前序消息的杂凑值，形成一个杂凑链，同步保证了协议执行的效率和安全性。本部分第9章规范了EEP协议对快速鉴别的支持，第10章规范了密钥上报过程。

4.2 T/WAPIA 045.2—2021

T/WAPIA 045.2—2021是AKEA系列第2部分：轻量级原子实体鉴别与密钥建立，本部分规范了轻量级原子实体鉴别与密钥建立（AKEA-L），可封装在EEP协议中实现实体间原子实体鉴别与密钥建立。

本部分第5章规范了AKEA-L架构，使用AKEA-L协议协商的密钥建立算法和参数，通过密钥交换协议或随机数交换算法，请求者REQ和鉴别接入控制器AAC基于预共享密钥协商建立一个共享的主鉴别密钥MAK，通过MAK建立用于安全通信的会话密钥体系。

本部分第6章规范了AKEA-L格式和数据元素，明确了与EEP协议的接口。AKEA-L协议不仅实现初始鉴别功能和实现密钥更新功能，还可用于实现快速密钥更新。

AKEA-L支持两种密钥建立体系：第7.2章节中规范的基于基密钥BK的实体鉴别与密钥建立体系，以及第7.3章节中规范的基于预共享密钥PSK的实体鉴别与密钥建立体系。

本部分第8章规范了AKEA-L握手消息交互流程，包括带鉴别、无鉴别、随机数密钥交换情况下实体鉴别和密钥建立过程，以及用于切换网络接入点时的快速鉴别或者在同（跨）域情况下的快速密钥更新。

AKEA-L协议不仅支持实现初始鉴别，还支持实现密钥更新以及快速密钥更新等能力。

4.3 T/WAPIA 045.3—2021

T/WAPIA 045.3—2021是AKEA系列第3部分：采用证书的原子密钥建立与实体鉴别，该部分规范了采用证书的原子密钥建立与实体鉴别协议(AKEA-C)，可封装在EEP协议中实现实体间原子实体鉴别与密钥建立。

AKEA-C中实体采用证书作为身份凭证，实现实体之间单向或双向鉴别，包括全网络隐私信息保护、鉴别实体之间隐私信息的保护以及漫游情况下的实体鉴别和密钥建立等。

本部分第5章规范了AKEA-C协议的握手交互过程，在安全通信前，AKEA-C在请求端和接入端实体之间提供鉴别，并进行密钥协商和确认，采用数字证书作为实体间的凭证。在鉴别和密钥管理协议、压缩和鉴别服务使用的密码套件的算法和参数协商后，AKEA-C成功完成，建立共享基密钥BK，基于BK建立整个密钥体系。

本部分第6章规范了AKEA-C格式和相关的数据元素及其定义，其中的数据元素是在第1部分的基础上完善了证书验证结果和涉及AS时需要接入端向其发送的指定信息等。

本部分第7章规范了AKEA-C的协议握手消息交互，包括两个实体之间分别相互的单向和双向的实体鉴别与密钥建立过程，以及网络中存在可信第三方时实体利用第三方实现单向或者双向的身份鉴别与密钥建立的过程。

程。AKEA-C协议中，还支持主动身份保护，在协议执行过程中，当请求端获得接入端的身份鉴别结果并确定其是自己想要接入的网络时，才将自己的身份信息发送至接入端让其验证。

4.4 T/WAPIA 045.4—2021

T/WAPIA 045.4—2021是AKEA系列第4部分：采用预共享密钥的原子密钥建立与实体鉴别，该部分规范了采用预共享密钥的原子密钥建立与实体鉴别（AKEA-P），可封装在EEP协议中实现实体间原子实体鉴别与密钥建立。

该标准规范了采用预共享密钥作为身份凭证，实现实体之间单向或双向鉴别的机制，其中包括了全网络隐私信息保护、鉴别实体之间隐私信息的保护情况下的原子密钥建立与实体鉴别，并且可以实现抵御字典攻击和降低量子计算攻击的功能。

本部分第5章规范了AKEA-P的过程和协议，第6章规范了AKEA-P格式和相关的数据元素，第7章规范了AKEA-P握手消息交互的具体实现，包括不存在可信第三方的两元实体架构下的两个单向和一个双向的实体鉴别与密钥建立机制；以及存在可信第三方的情况下（漫游与非漫游）实体利用第三方实现双向的身份鉴别与密钥建立。

4.5 T/WAPIA 045.5—2021

T/WAPIA 045.5—2021是AKEA系列第5部分：采用预共享密钥与证书组合的原子密钥建立与实体鉴别，该部分规范了采用预共享密钥与证书组合的原子密钥建立与实体鉴别（AKEA-M），即实体一端采用数字证书、一端采用预共享密钥的密钥建立与实体鉴别，可封装在EEP协议中实现实体间原子实体鉴别与密钥建立。

本部分主要规范了非对等网络环境下，实体一端采用预共享密钥一端采用证书作为身份凭证，实现实体之间单向或双向鉴别的机制，其中包括了全网络保护、鉴别实体之间网络信息的保护情况下的原子密钥建立与实体鉴别等，解决了实体申请证书难的问题。

AKEA-M握手消息交互中需要可信第三方的参与；在AKEA-M中持证书的实体和鉴别服务器分别持有数字证书及其对应的私钥；持证书的实体知晓其所信任的鉴别服务器的数字证书或者数字证书中的公钥；鉴别服务器具有验证实体数字证书合法性的能力以及验证持有PSK实体的身份合法性的能力；持有PSK的实体和鉴别服务器之间具有有效的预共享密钥，并使用预先约定的校验算法。

当实体需要身份主动保护（隐私信息全局网络保护）时，鉴别服务器应同时持有用于加密的证书及其对应的私钥，且实体持有鉴别服务器加密证书或者加密证书中的公钥。

本部分在7.1章节中规范了请求端采用预共享密钥、接入端采用数字证书作为身份凭证，在7.2章节中规范了请求端采用数字证书、接入端采用预共享密钥作为身份凭证，在存在可信第三方的情况下（漫游与非漫游）实体利用可信第三方实现双向的身份鉴别与密钥建立。

特别说明的是，此过程中持有证书的实体使用AKEA-L中基于BK的密钥建立层次建立密钥体系，持有PSK的实体使用AKEA-L中基于PSK的密钥建立层次建立密钥体系，在整个原子机制的执行过程中，实现了密钥的确认，即，对方均持有与自己相同的会话密钥。

4.6 T/WAPIA 045.6—2021和T/WAPIA 045.7—2021

T/WAPIA 045.6—2021和T/WAPIA 045.7—2021分别是AKEA系列第6部分和第7部分，是AKEA在三元移动通信系统安全中的具体应用，分别是基于对称密钥的原子密钥建立与实体鉴别，和基于非对称密钥的原子密钥建立与实体鉴别。

第6部分规范了在移动通信系统中，基于对称密钥的原理，保护申请访问网络的实体身份不被泄露（正常情况下使用临时身份或者临时身份失效或者首次执行本次协议时加密身份）并实现实体之间漫游（非漫游）情况下的双向鉴别以及密钥建立，并且同步执行请求对端实体临时身份更新以保证其安全性。

第7部分规范了在移动通信系统中，基于非对称密钥的原理实现实体之间漫游和非漫游情况下的双向鉴别以及密钥建立过程。

5. 标准应用建议

WAPI产业联盟发布的T/WAPIA 045系列团体标准，基于三元对等安全架构，具备身份保护能力、抗字典攻击、抗量子计算攻击等能力，充分考虑了区块链等新技术应用中的技术特性，提供了传统非对称密码算法向后量子密码算法演进阶段协议的安全能力提升。同时，在安全性方面，该系列标准充分考虑了已知和预测的各种应用技术需求，提出了通用的技术组件以供调用；多种技术机制完备且设计合理，满足了各种应用场景；在协议设计过程中，使用多种密码机制保证消息传递过程中的保密性和完整性；在同步实现密钥建立与实体鉴别过程中，利用哈希链、身份保护、完整性校验以及签名验签等方式，保证了协议设计的原子性。

T/WAPIA 045系列团体标准所规范的AKEA架构及协议，是信息安全技术领域基础共性技术，可与IP、WLAN等多种网络通信协议相结合，增强其网络安全性。AKEA技术体系中提出了安全通道建立机制，可被采纳并应用于WLAN、LAN、IP层以及应用层等，满足网络安全访问和保密通信等需求。AKEA使用不可还原且不可分割的消息交换序列，为两个对等实体提供实体身份鉴别和密钥建立，任何实体在收到最后一条消息之前都无法完成对其对等实体的身份鉴别或密钥建立，可满足目前和未来网络通信领域中合法客户端访问合法网络以及保密通信的安全需求。该标准在实际应用中可结合不同需求，通过配置相关安全能力参数，在完成实体鉴别和密钥建立功能时为全网络或局部网络提供多安全级别的差异化保障能力。该系列技术标准还提供了一种量子安全中期演进架构，以融合运用经典公钥密码与分组密码体制的方式，为网络空间提供抗量子计算攻击的纵深防御能力。

WAPI 产业联盟成员单位名录

中国移动通信集团公司	京信通信技术（广州）有限公司	福建星网锐捷网络有限公司
中国电信集团公司	北京城市热点资讯有限公司	北京新岸线移动多媒体技术有限公司
中国联合网络通信集团有限公司	优比无线技术（深圳）有限公司	广东欧珀移动通信有限公司
国家密码管理局商用密码检测中心	南京智达康无线通信科技股份有限公司	上海贝尔股份有限公司
国家无线电监测中心检测中心	上海欣民通信技术有限公司	成都鼎桥通信技术有限公司
北大方正集团有限公司	福建三元达通讯股份有限公司	飞天联合（北京）系统技术有限公司
西安西电捷通无线网络通信股份有限公司	新华三技术有限公司	中国电力科学研究院
北京中电华大电子设计有限责任公司	北京傲天动联技术股份有限公司	锐迪科微电子（上海）有限公司
北京六合万通微电子技术股份有限公司	中兴通讯股份有限公司	苏州汉明科技有限公司
广州杰赛科技股份有限公司	武汉虹信通信技术有限责任公司	神州数码网络(北京)有限公司
深圳市明华澳汉智能卡有限公司	广州市卓纪思网络科技有限公司	北京必虎科技股份有限公司
无锡中太数据通信有限公司	赛芯电子技术（上海）有限公司	北京市政务网络管理中心
青岛海尔科技有限公司	雷凌科技股份有限公司	天津赞普科技股份有限公司
海信集团有限公司	瑞晟微电子（苏州）有限公司	北京数字认证股份有限公司
联想（北京）有限公司	联发博动科技（北京）有限公司	上海连尚网络科技有限公司
华为技术有限公司	四川天邑信息科技股份有限公司	深圳市瑞科慧联科技有限公司
大唐移动通信设备有限公司	湖南城市热点无线通信有限公司	深圳市信锐网科技术有限公司
北京朗波芯微技术有限公司	珠海市魅族科技有限公司	福建新大陆通信科技股份有限公司
大唐微电子技术有限公司	深圳市雄脉科技有限公司	北京比邻科技有限公司
上海鼎芯科技有限公司	奥泰尔科技（深圳）有限公司	天津市电子机电产品检测中心
北京天一集成科技有限公司	北京网贝合创科技有限公司	高通无线通信技术（中国）有限公司
北京联信永益信息技术有限公司	网件（北京）网络技术有限公司	中科开创（广州）智能科技发展有限公司
深圳鑫金浪电子有限公司	上海市数字证书认证中心有限公司	北京华信傲天网络技术有限公司
深圳市普天宜通科技有限公司	北京创原天地科技有限公司	南京博洛米通信技术有限公司
北京汉铭信通科技有限公司	阿德利亚科技（北京）有限责任公司	广西新海通信科技有限公司
西安大唐电信有限公司	深圳市华讯方舟软件信息有限公司	上海麓慧科技有限公司
深圳共进电子股份有限公司	迈创智慧供应链股份有限公司	深圳市智开科技有限公司
北京华安广通科技发展有限公司	科通宽带技术(深圳)有限公司	南方电网数字电网研究院有限公司
深圳国人通信有限公司	邦讯技术股份有限公司	深圳航天科创实业有限公司
东蓝数码有限公司	惠州市宝丰信息科技有限公司	南方电网深圳数字电网研究院有限公司
美国安移通网络公司北京代表处	晨星软件研发（深圳）有限公司	广西电力线路器材厂有限责任公司
北京五龙电信技术公司	卓望数码技术（深圳）有限公司	广西通量能源技术有限公司
北京同耀通电科技有限公司	迈普通信技术股份有限公司	恩智浦（中国）管理有限公司
北京登合科技有限公司	北京汇通融业科技发展有限公司	南方电网科学研究院有限责任公司
宇龙计算机通信科技（深圳）有限公司	上海寰创通信科技有限公司	山东华辰泰尔信息科技股份有限公司
上海润欣科技有限公司	吉翁电子（深圳）有限公司	山东思极科技有限公司
弘浩明传科技股份有限公司	北京汇为永兴科技有限公司	深圳市国电科技通信有限公司

【注：截至2022年4月，联盟正式成员已达111家，以加入联盟的时间先后排序。】

WAPI Alliance
产业联盟



地 址：北京市海淀区知春路27号量子芯座1608室

邮 编：100191

电 话：010-82351181

传 真：010-82351181 ext. 1901

邮 箱：wapi@wapia.org

网 址：<http://www.wapia.org.cn>