WAPI Alliance
产业联盟

在路上
ON THE ROAD

2022年12月出版
总第76期
中文版

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 JTC 1/SC 6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：

WAPI产业联盟公众号

媒体聚焦
Media Focus

WAPI 问答
WAPI FAQ

联盟关注
Alliance Concerns

产经要闻
Industrial & Economic News

联盟工作
Alliance Work

成员与市场
Member & Marketing

产业技术论坛
Industry & Technology Forum

新华社、中国政府网：

我国又一项物联网安全关键技术成为国际标准

【编者按】日前，WAPI产业联盟牵头组织成员单位自主研发的物联网安全协议关键技术（TRAIS），被国际标准化组织/国际电工委员会（ISO/IEC）发布成为国际标准，标准号为：ISO/IEC 29167-16:2022。这是我国在物联网关键核心技术领域又一项拥有自主知识产权的国际标准，也是联盟践行网络强国战略和创新驱动发展战略的又一成功实践。TRAIS国际标准的发布与应用，标志着我国提出的物联网安全协议技术已形成相对完整的国际标准体系，有助于实现全球物联网的互联互通和共享共治，巩固我国物联网安全群体创新成果。

此事引起国内外广泛关注。新华社、中国政府网、学习强国、国家标准化管理委员会、中国知识产权报、中国政协网、中国网、人民网、央广网、中国日报、中国军网、光明网等数十家官方机构和权威媒体发布相关报道。

以下是新华社和中国政府网的报道:

新华社北京12月14日电（记者刘羽佳）记者日前从WAPI产业联盟获悉，我国自主研发的物联网安全协议关键技术（TRAIS）被国际标准化组织/国际电工委员会（ISO/IEC）发布成为国际标准。这是我国在物联网关键核心技术领域又一项拥有自主知识产权的国际标准。

据介绍，该标准规范了有源射频识别（RFID）系统的空中接口安全防护方法，能够提供实体鉴别、安全

通信等高等级安全服务，可有效防范针对RFID系统的身份伪造、数据窃听与篡改等安全威胁。RFID是一种先进的非接触式自动识别技术，通过射频信号自动识别目标对象并获取相关数据，广泛应用于物流仓储、零售、制造业、医疗、交通、电子支付等领域。

此前，我国在RFID、NFC安全技术领域已发布6项国际标准。加上TRAIS技术，7项国际标准共同构成了物联网安全关键技术标准体系，有助于实现全球物联网系统的互联互通和共享共治。

西电捷通公司、无线网络安全技术国家工程研究中心是7项国际标准的主要技术贡献者，并遵循规则就持有的标准必要专利，向全球做出合理和非歧视许可使用的声明。WAPI产业联盟、国家商用密码检测中心、国家无线电监测中心检测中心、国家信息技术安全研究中心等10余家单位参与标准开发工作。

“二十多年来，我们在技术研发和标准制修订方面持续投入，以适应不断演进的全球网络安全需求。”西电捷通公司董事长曹军说。

WAPI产业联盟秘书长张璐璐表示，该标准的应用，将让全球RFID产品和系统更安全、更可信赖，让用户更放心地享受物联网带来的便利。

部分媒体新闻链接：

国务院 中国政府网：http://www.gov.cn/xinwen/2022-12/14/content_5732049.htm

新华社：https://h.xinhuaxmt.com/vh512/share/11266285?d=1348d1e&channel=weixin

学习强国：https://www.xuexi.cn/lgpage/detail/index.html?id=3532453238100525726&item_id=3532453238100525726

国家标准化管理委员会：http://www.sac.gov.cn/xw/bzhdt/202212/t20221220_350351.html

中国知识产权报：http://epaper.iprchn.com/zscqb/html/2022-12/21/content_27586_7124645.htm

中国政协网：http://www.rmzxb.com.cn/c/2022-12-15/3258852.shtml

人民网：http://finance.people.com.cn/n1/2022/1214/c1004-32587239.html

新华网：http://m.news.cn/2022-12/14/c_1129208175.htm

新华每日电讯：http://www.news.cn/mrdx/2022-12/15/c_1310684176.htm

中国网：http://ydyl.china.com.cn/2022-12/15/content_85013976.htm

中国日报网：https://cn.chinadaily.com.cn/a/202212/14/WS6399db50a3102ada8b226b5a.html

中国经济网：http://bgimg.ce.cn/cysc/yy/hydt/202212/14/t20221214_38288948.shtml

中国科技网：http://www.stdaily.com/index/kejixinwen/202212/f6c227e06f8a4a6b9ec7c59930752473.shtml

央广网：https://tech.cnr.cn/techyw/kan/20221215/t20221215_526095386.shtml

光明网：https://m.gmw.cn/baijia/2022-12/14/1303224509.html

中国军网：http://www.81.cn/jfjbmap/content/2022-12/15/content_329900.htm

中国政务：http://zw.china.com.cn/2022-12/15/content_85012907.html

中国邮电报：https://paper.cnii.com.cn/article/rmydb_16294_314340.html

通信世界：http://www.cww.net.cn/article?id=572412

中国金融信息网：https://www.cnfin.com/hg-lb/detail/20221214/3766153_1.html

中国证券网：https://news.cnstock.com/news,bwkx-202212-4993720.htm

中国工信产业网：https://www.cnii.com.cn/gxxww/rmydb/202212/t20221219_435065.html

RFID世界网：http://news.rfidworld.com.cn/2022_12/1dc9f350d559d29c.html

创头条：https://www.ctoutiao.com/3106480.html

新浪网：https://finance.sina.com.cn/tech/roll/2022-12-19/doc-imxxepne3838306.shtml

搜狐网：https://it.sohu.com/a/617308490_121609529

腾讯网：https://view.inews.qq.com/wxn/20221214A05T4V00?web_channel=detail

欧美同学会：http://www.wrsa.net/content_42205531.htm

团结网：http://www.tuanjiewang.cn/2022-12/14/content_8945859.htm

中国西藏网：http://www.tibet.cn/cn/politics/202212/t20221215_7327708.html

网信天津：https://baijiahao.baidu.com/s?id=1752232065359498718&wfr=spider&for=pc

安徽省科技厅：http://kjt.ah.gov.cn/kjzx/kjyw/121346931.html

扬子晚报：http://www.yzwb.net/zncontent/2611171.html

青海羚网：https://www.qhlingwang.com/xinwen/guonei/2022-12-15/580233.html

阜阳市科技局：https://kjj.fy.gov.cn/content/detail/639fa8e088668897178b4571.html

邯郸新闻网：https://www.handannews.com.cn/news/content/2022-12/15/content_20063349.html

阿克苏市人民政府：https://www.akss.gov.cn/zwgk/sjzt/20221215/i867240.html

三明日报：http://smrb.smnet.com.cn/pc/layout/content/202212/15/content_131385.html

南报网：http://www.njdaily.cn/news/2022/1215/4965615856610777677.html

舜网：http://news.e23.cn/guonei/2022-12-15/2022C1500005.html

兰州新闻网：http://www.lzbs.com.cn/gnnews/2022-12/15/content_504350735.htm

贵阳网：http://www.gywb.cn/system/2022/12/14/055591066.shtml

胡杨网：http://www.huyangnet.cn/content/2022-12/14/content_1712207.html

六安新闻网：http://news.luaninfo.com/laxw/gnxw/content_157081

全保定网：http://www.bdall.com/content/2022-12/15/content_86018.html

茂名网：https://www.mm111.net/2022/12/15/991284933.html

延伸阅读

1、标准信息

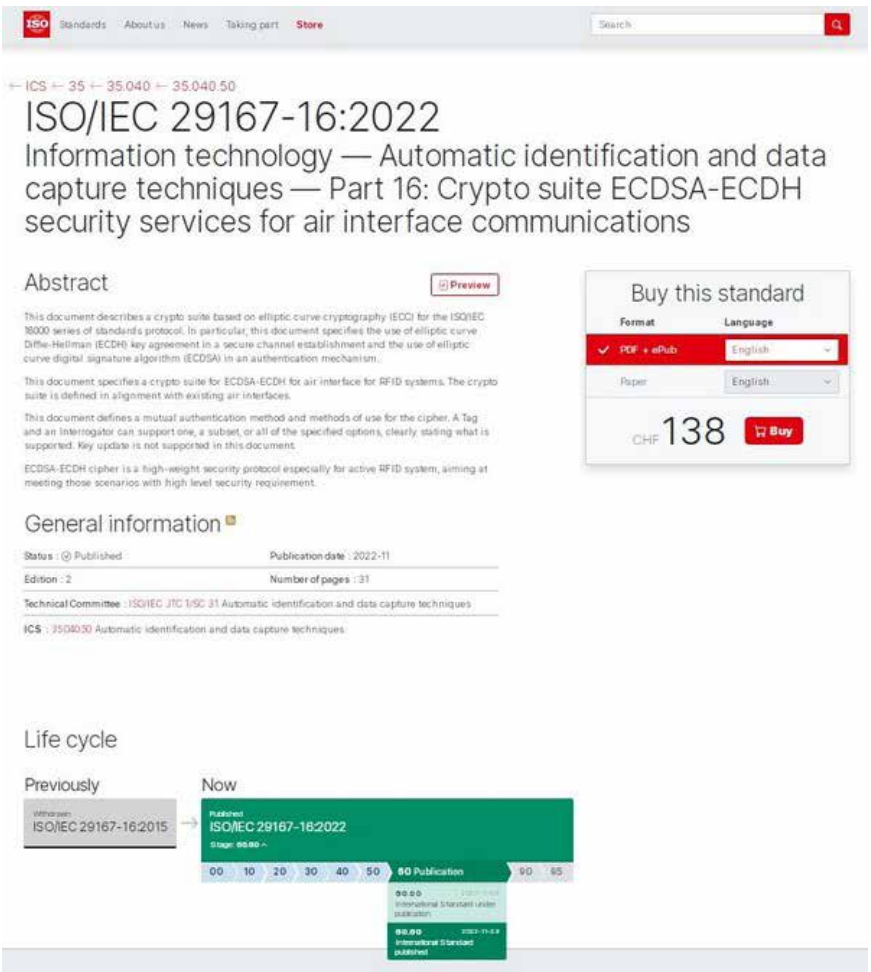
标准号：ISO/IEC 29167-16:2022

名称：Information technology — Automatic identification and data capture techniques — Part 16: Crypto suite ECDSA-ECDH security services for air interface communications《信息技术 自动识别与数据获取技术 第16部分：用于空中接口通信的ECDSA-ECDH密码套件安全服务》

发布日期：2022年11月29日

所属技术委员会：国际标准化组织和国际电工委员会信息技术联合技术委员会第31分技术委员会（ISO/IEC JTC 1/SC 31，标准化领域为自动识别和数据采集）

ISO标准发布网址：https://www.iso.org/standard/81524.html



图：ISO网站截图—ISO/IEC 29167-16:2022发布

2、标准推进过程

一项技术提案从提出到发布为国际标准，通常要经过NP→WD→CD→DIS→FDIS→IS等六个阶段，如果技术成熟度高，可跳过中间某些阶段。本标准情况如下：

2021年1月21日，通过新工作项目（NP）投票，正式立项；

2021年3月30日，注册为委员会草案（CD）,启动CD投票；

2021年9月6日，通过CD投票，注册为国际标准草案（DIS）；

2021年11月25日，为期12周的DIS投票启动；

2022年2月26日，全票通过DIS投票，由于没有技术问题和意见，项目直接进入发布阶段；

2022年11月29日，完成标准审查流程，由ISO/IEC正式发布为国际标准。

3、七项物联网安全国际标准体系情况

序号	技术领域	标准编号	标准名称	对应的中文名称	标准必要专利	发布时间
1.	RFID	ISO/IEC 29167-16：2015	Information technology — Automatic identification and data capture techniques — Part 16: Crypto suite ECDSA-ECDH security services for air interface communications	《信息技术 自动识别与数据获取技术 第 16 部分：用于空中接口通信的 ECDSA-ECDH 密码套件安全服务》	ISO 网站可查专利声明	2015/11/18
2.	NFC	ISO/IEC 13157-4：2016	Information technology -- Telecommunications and information exchange between systems -- NFC Security -- Part 4: NFC-SEC entity authentication and key agreement using asymmetric cryptography	《信息技术 系统间远程通信和信息交换 第 4 部分：使用非对称密码技术的 NFC-SEC 实体鉴别与密钥协商》	ISO 网站可查专利声明	2016/6/10

序号	技术领域	标准编号	标准名称	对应的中文名称	标准必要专利	发布时间
3.	NFC	ISO/IEC 13157-5：2016	Information technology -- Telecommunications and information exchange between systems -- NFC Security -- Part 5: NFC-SEC entity authentication and key agreement using symmetric cryptography	《信息技术 系统间远程通信和信息交换 第 5 部分：使用对称密码技术的 NFC-SEC 实体鉴别与密钥协商》	ISO 网站可查专利声明	2016/6/10
4.	RFID	ISO/IEC TS 29167-15:2017	Information technology -- Automatic identification and data capture techniques -- Part 15: Crypto suite XOR security services for air interface communications	《信息技术 自动识别与数据获取技术 第 15 部分：用于空中接口通信的密码套件 XOR 安全服务》	ISO 网站可查专利声明	2017/10/2
5.	NFC	ISO/IEC 22425:2017	Information technology -- Telecommunications and information exchange between systems -- NFC-SEC Test Methods	《信息技术 系统间远程通信和信息交换 NFC 安全测试方法》	ISO 网站可查专利声明	2017/11/15
6.	RFID	ISO/IEC 19823-16:2020	Information technology -- Conformance test methods for security service crypto suites -- Part 16: Crypto suite ECDSA-ECDH security services for air interface communications	信息技术 安全服务密码套件一致性测试方法 第 16 部分：用于空中接口通信的 ECDSA-ECDH 密码套件安全服务	ISO 网站可查专利声明	2020/10/26
7.	RFID	ISO/IEC 29167-16：2022	Information technology — Automatic identification and data capture techniques — Part 16: Crypto suite ECDSA-ECDH security services for air interface communications	信息技术 自动识别与数据获取技术 第 16 部分：用于空中接口通信的 ECDSA-ECDH 密码套件安全服务	ISO 网站可查专利声明	2022/11/29

注:

1. ISO/IEC 29167-16:2015（TRAIS-P，基于公钥密码算法的标签和读写器空中接口安全），规范了有源RFID系统的空中接口安全防护方法，能够提供实体鉴别、安全通信等高等级安全服务，可有效防范针对RFID系统的身份伪造、数据窃听与篡改等安全威胁。

2. ISO/IEC 13157-4:2016（NEAU-A，NFC非对称实体鉴别），采用非对称密码技术提供底层的安全保障，防止伪造、窃听和篡改等攻击，以应对NFC多种应用场景的安全挑战。NEAU定义了密钥协商和确认协议，提供了设备之间的对等双向鉴别，其突出特点是定义了独立于具体NFC应用的通用空口通信安全，可防止近距离空口窃听、设备伪造、数据篡改等欺诈攻击，更为端到端模式下开展高价值交易提供了鉴别保障，可取得与高端智能卡比拟的高安全等级。

3. ISO/IEC 13157-5:2016（NEAU-S，NFC对称实体鉴别），采用对称密码技术提供底层的安全保障，防止伪造、窃听和篡改等攻击，以应对NFC多种应用场景的安全挑战。

4. ISO/IEC TS 29167-15:2017（TRAIS-X，基于异或运算的标签和读写器空中接口安全），主要用于保护无源RFID产品和系统安全，其特点是能够在运算资源开销很小的情况下提供基础安全保障。

5. ISO/IEC 22425:2017（NEAU-Test），本标准是NEAU（ISO/IEC 13157-4:2016、ISO/IEC 13157-5:2016）对应的测试标准，它规范了NFC空中接口通信安全协议的符合性测试方法。

6. ISO/IEC 19823-16:2020（TRAIS-Test），本标准是TRAIS-P（ISO/IEC 29167-16:2015）对应的测试标准，它规范了RFID安全密码套件一致性测试方法。

7. ISO/IEC 29167-16:2022，规范了有源RFID系统的空中接口安全防护方法，能够提供实体鉴别、安全通信等高等级安全服务，可有效防范针对RFID系统的身份伪造、数据窃听与篡改等安全威胁。本标准是TRAIS技术自2015年之后再次被国际标准修订发布，以适应不断发展演进的全球物联网安全需求。

中国标准化、中国电子报等：

北京市市场监管局发布《高质量团体标准评价规范》

WAPI产业联盟是主要起草单位

【编者按】2022年9月29日，北京市地方标准DB11/T 2020—2022《高质量团体标准评价规范》获正式发布，WAPI产业联盟（中关村无线网络安全产业联盟）是标准主要编制单位。该标准规定了高质量团体标准的评价原则、评价条件、评价内容、评价程序及结果等内容，适用于团体标准的高质量效果评价。中国标准化、中国电子报/电子信息产业网、通信世界、飞象网等媒体对此进行了报道。

以下是中国标准化、中国电子报等媒体报道：

2022年9月29日，北京市地方标准DB11/T 2020—2022《高质量团体标准评价规范》获正式发布，WAPI产业联盟（中关村无线网络安全产业联盟）是标准主要起草单位。该标准规定了高质量团体标准的评价原则、评价条件、评价内容、评价程序及结果等内容，适用于团体标准的高质量效果评价。

团体标准是国家标准体系的重要组成部分，发展团体标准对于充分释放市场主体标准化活力，优化标准供给结构，提高产品和服务竞争力，助推高质量发展具有重要意义。为贯彻《国家标准化发展纲要》，实施首都标准化战略纲要，助力首都高质量发展标准体系建设，促进团体标准高质量发展，北京市市场监督管理局启动了《高质量团体标准评价规范》的制定工作。

图： DB11/T 2020—2022《高质量团体标准评价规范》

该标准于2021年3月立项，于2023年1月1日起正式实施，由北京市标准化研究院、中关村半导体照明工程研发及产业联盟、中关村无线网络安全产业联盟、中关村乐家智慧居住区产业技术联盟、中关村材料试验技术联盟、中关村天合宽禁带半导体技术创新联盟、中关村企业信用促进会、北京市闪联信息产业协会、北京市安全生产联合会、北京第三代半导体产业技术创新战略联盟、北京标准化协会、中关村车载信息服务产业应用联盟、北京电信技术发展产业协会、中关村标准化协会、中关村中交国通智能交通产业联盟等单位共同编制。该标准是评价北京市团体标准水平的重要依据，将规范和引导团体标准的高质量发展。

WAPI产业联盟是国家标准委首批团体标准试点单位、中关村国家自主创新示范区标准化示范单位，在团体标准协同创新和成果转化方面走在前列。目前，联盟已发布了90项团体标准，其中21项团体标准获发布成为国家标准，6项团体标准获发布成为国际标准；2017年2项团体标准入选工信部百项团体标准应用示范项目，2019年1项团体标准入选工信部百项团体标准应用示范项目；2020年荣获中国标准创新贡献三等奖，2022年7月通过了中国标准创新贡献一等奖建议名单公示。

部分媒体新闻链接：

中国标准化：https://mp.weixin.qq.com/s/itL1SqVRVcb_wz63tDqhjQ

中国电子报：http://www.cena.com.cn/infocom/20221027/118017.html

通信世界：http://www.cww.net.cn/article?id=569855

飞象网：http://www.cctime.com/html/2022-10-27/1633601.htm

中国日报网、通信世界等：
联盛德微电子WAPI系列产品通过联盟测试

【编者按】日前，联盛德微电子无线局域网系列产品通过了联盟WAPI互通性、完整性及功能测试。其中WAPI终端DTU设备和WAPI MCU无线终端模组，具有全国产化、高安全、低功耗、小尺寸、免驱动、高可靠、易扩展特点，可广泛服务传感器远程监测、工业自动化、智能电网、智慧交通、可穿戴设备、智能语音设备、智能安防设备、智慧仓储无线系统、智能开关、无线继电器、仪器仪表监测等物联网应用场景。中国日报网、中国政协网、中国电子报/电子信息产业网、中国电力网、通信世界、飞象网、新浪网、网易、搜狐网、腾讯网、凤凰网、产业发展研究网等媒体对此进行了报道。

中国电子报、通信世界等媒体报道如下：

日前，北京联盛德微电子有限责任公司（以下简称联盛德微电子）的无线局域网系列产品通过了WAPI产业联盟无线局域网鉴别与保密基础结构（WAPI）互通性、完整性及功能测试。联盟为上述产品出具了测试报告。

本次通过测试设备包括WAPI鉴别服务器（AS）、WAPI企业级室内/室外用无线接入点（AP）、WAPI终端DTU设备和WAPI MCU无线终端模组。其中AS设备具备证书签发、鉴别、漫游、管理功能；AP设备支持

2.4/5GHz双频接入，通信速率支持802.11ac协议；终端设备具备体积小、功耗低、接口丰富特点，能够满足传感器类应用场景以及电池供电设备低功耗的应用需求。

图：联盟为联盛德WAPI系列产品出具测试报告

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、功能及性能测试，针对首轮测试中AP设备在WAPI协议完整性存在的部分未通过项，联盟实验室进行了精准定位并提出整改建议，联盛德微电子依据联盟建议完成了整改。

当前，通过WAPI CPE（客户端前置设备）、WAPI DTU（数据传输单元）、WAPI MCU（微处理单元）模组，能够便捷地在行业机具中实现安全无线局域网功能，帮助行业用户实现在业务中使用无线通信技术进行数据安全传输的需求。

据联盛德微电子介绍，本次与WAPI产业联盟协同研发并推出的WAPI终端DTU设备和WAPI MCU无线终端模组值得业界关注。其中，WAPI终端DTU设备是基于全国产WAPI芯片模组的行业专用 DTU设备，具有RS232/RS485工业总线转WAPI网络数据收发的能力，即插即用，无需对现有设备做任何修改、无需传统的串口线缆布线即可实现数据的无线收发，帮行业用户实现了RS232/RS485设备使用WAPI开展业务的需求，保障了行业设备网络通信的安全性、便捷性、合规性。WAPI MCU无线终端模组，基于嵌入式MCU系统架构，内置联盛德微电子自主研发的全国产无线局域网 SoC主控芯片，具有全国产化、高安全、低功耗、小尺寸、免驱动、高可靠、易扩展等特点。这两款设备，可广泛服务传感器远程监测、工业自动化、智能电网、智慧交通、可穿戴设备、智能语音设备、智能安防设备、智慧仓储无线系统、智能开关、无线继电器、仪器仪表监测等物联网应用场景。

联盛德微电子表示，作为国内本土集成电路设计企业，我们始终致力于设计开发自主可控的无线通信芯片、模组及应用方案。我们也将和WAPI产业联盟一起，开展技术协同创新和产品研发方面的深度合作，关注能源、仓储、安防等领域需求，推出更多品类的产品，提供从芯片到整机产品、从终端到网络的完整解决方案。

图：协同研发并推出的全国产WAPI终端DTU设备

图：协同研发并推出的全国产WAPI MCU无线终端模组

中国日报网、中国政协网等媒体报道如下:

日前,北京联盛德微电子有限责任公司(Winner Micro)全系列WAPI产品通过了WAPI产业联盟认证,并取得了联盟认证证书。

此次通过WAPI联盟认证的产品设备包括网络端的WAPI鉴别服务器(AS)、WAPI企业级室内/室外用AP;也包括WAPI终端DTU设备和WAPI MCU无线终端模组。至此,联盛德微电子从终端侧到网络侧全线产品已全部满足WAPI产业联盟无线局域网鉴别与保密基础结构(WAPI)互通性、完整性及性能要求。可为客户提供完整安全的系统级解决方案和一条龙服务。

图:联盟为联盛德WAPI系列产品出具测试报告

WAPI 鉴别服务器 WMAS5000

WMAS5000 作为一款WAPI鉴别服务器(AS)产品,支持ASU和CISU实体功能,具有WAPI证书签发、导入、吊销、查询、更新、CRL签发,以及WAPI证书鉴别、漫游证书鉴别、双因子鉴别等协议能力,并具备服务器数据备份与恢复、设备证书分组、多级日志、安全审计、用户管理等丰富的设备管理功能,同时支持大量用户并发认证,可有效保障行业用户使用WAPI网络时的规模性、安全性、合规性、稳定性、以及可朔源性。

WAPI企业级AP:

室内型 WMAP3609C / 室外型 WMAP2409C

全千兆网络接口,2.4G 802.11ac 400Mbps + 5G 802.11ac 867Mbps的无线接入速度,无线处理速度最高可达1.267Gbps。即插即用,具有高性能、高增益、高接收灵敏度、高带宽、高接入数等特点,覆盖范围更大,并提供更高的无线传输性能及稳定性。

WAPI终端DTU设备 WMD180-485

业界首款基于全国产WAPI芯片模组的行业专用 DTU(数据传输单元)设备,具有 RS232/RS485工业总线转WAPI无线网络数据收发的能力,即插即用,无需对现网设备做任何修改、无需传统的串口线缆布线即可实现数据的无线收发,帮助行业用户轻松搞定RS232/RS485设备使用WAPI无线技术进行数据安全传输的需求,保障行业设备网络通信的便捷性、安全性与合规性。

全国产、高安全、低功耗WAPI MCU无线通信模组 WM6180

新一代旗舰版WAPI MCU(微控制单元)物联网无线终端模组,具有全国产化、高安全、低功耗、小尺寸、免驱动、高可靠、易扩展等特点。WM6180模组内置联盛德微电子自主研发的全国产WLAN SoC主控芯片。芯片支持硬件WAPI安全协议;全国产CPU内核,最高主频240MHz;支持嵌入式操作系统的SDK软件平台;支持多种网络通信协议;支持丰富的数字接口。

WM6180创新点：区别于WAPI CPE类型产品,WM6180基于嵌入式MCU系统架构,体积更小、功耗更低、性价比更高。非常适合终端传感器类产品应用,尤其能够满足电池供电设备的WAPI无线化需求。

WM6180模组可广泛服务于传感器远程监测、工业自动化、智能电网、智慧交通、可穿戴设备、智能语音设备、智能安防设备、智慧仓储无线系统、智能开关、无线继电器、仪器仪表监测等物联网应用场景,帮助用户高效、便捷地实现“WAPI+”安全应用解决方案的部署实施。

联盛德微电子作为国内本土集成电路设计企业,始终立志于设计开发自主可控的无线通信芯片、模组及应用方案。公司相继推出多款支持WAPI无线安全协议的芯片、模组、网络端设备等相关产品和解决方案。联盛德微电子将在WAPI领域不断创新,继续推出更多产品品类,面向电力、能源等多领域提供从芯片到整机产品,从终端到网络端的完整解决方案。

部分媒体新闻链接:

中国日报网: https://cn.chinadaily.com.cn/a/202211/17/WS6375fdd9a3109bd995a508f3.html

中国政协网: http://www.rmzxb.com.cn/c/2022-11-18/3243052.shtml

中国电力网: http://www.chinapower.com.cn/biznews/xiaofei/20221117/62450.html

通信世界: http://www.cww.net.cn/article?id=571312

飞象网: http://www.cctime.com/html/2022-11-22/1636270.htm

电子信息产业网: http://www.cena.com.cn/infocom/20221122/118240.html

凤凰网: http://baby.ifeng.com/c/8L0f3wIxJ3S

腾讯网: https://new.qq.com/rain/a/20221117A0321L00

网易: https://www.163.com/dy/article/HMCFAPRF0553Q79E.html

搜狐: https://www.sohu.com/a/607487405_120891316

新浪网: https://news.sina.com.cn/sx/2022-11-17/detail-imqmmthc4943575.shtml

产业发展研究网: http://www.chinaidr.com/tradenews/2022-11/216127.html

飞象网：

WAPI产业联盟召开2022年第四次标准工作及项目组会议（总第124次）

【编者按】12月21日，WAPI产业联盟克服疫情困难，成功召开2022年第四次标准工作及项目组会议（总第124次）。2022年世界标准日的中国主题是“数字时代的标准化”，强调标准让数字时代的信息更安全，标准让数字时代的联通更高效，标准让数字时代的质量更可靠，标准让数字时代的发展环境更优化。WAPI标准产业共同体所开发的标准体系正务于上述目标。作为新型产业标准开发平台，联盟将继续在新的技术和产业演进中，充当好行业管理、企业、科研机构、用户的桥梁纽带，发挥好无线网络安全标准的联通和支撑作用。飞象网等媒体发布相关报道。

以下是飞象网报道：

12月21日，WAPI产业联盟组织召开2022年第四次标准工作及项目组会议（总第124次）。会议包括：2022年第四季度标委会主任委员会议情况通报、2022年第四季度技术标准产业工作报告、技术产业最新动态分享、在研标准项目讨论和审议、2022年度技术标准工作总结、SC6国内技术对口工作报告、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、中国电信股份有限公司研究院、中国电力科学研究院、中电科普天科技股份有限公司、华为技术有限公司、西电捷通公司、深圳市国电科技通信有限公司、国网重庆市电力公司、北京铁路通信技术中心、北京市政务信息安全保障中心、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、紫光展锐科技有限公司、北京联盛德微电子有限责任公司、新华三技术有限公司、北京

佰才邦技术股份有限公司、北京华信傲天网络技术有限公司、锐捷网络股份有限公司、迈普通信技术股份有限公司、深圳市智开科技有限公司、北京兴汉网际股份有限公司、南京博丰通信科技有限公司、瑞晟微电子（苏州）有限公司、西安芯语慧联信息科技有限公司、巷子科技(北京)有限公司、南京博洛米通信技术有限公司、北京比邻科技有限公司、重庆华联众智科技有限公司、重庆源盾科技集团有限公司、四川岁月文明科技有限公司、北京邮电大学、北京工业大学重庆研究院、重庆大学、重庆邮电大学、湖北经济学院、西安工业大学等单位，以及无线网络安全标准化委员会、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的80余位代表参会。

图：会议合影（部分）

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，第四季度标准产业共同体克服疫情困难，取得了高效扎实的工作成果。一是稳步推进标准化工作， 9项国际标准、1项国家标准、15项团体标准、1项北京地方标准、1项中关村标准的制修订工作正按计划推进。其中：又一项物联网安全关键技术成为国际标准（标准号：ISO/IEC 29167-16:2022），它与之前发布的6项RFID、NFC安全技术领域国际标准，共同构成了物联网安全关键技术标准体系，有助于实现全球物联网系统的互联互通和共享共治。新华社、中国政府网、学习强国、国家标准委、中国知识产权报等数十家官方机构和权威媒体对此进行了报道。另一项北京市地方标准DB11/T 2020—2022《高质量团体标准评价规范》也获正式发布，WAPI产业联盟是标准主要编制单位。该标准规定了高质量团体标准的评价原则、评价条件、评价内容、评价程序及结果等内容，适用于团体标准的高质量效果评价。中国标准化、中国电子报/电子信息产业网、通信世界、飞象网等媒体对此进行了报道。二是无线网络安全标准化委员会力量再度壮大，下半年七位委员的加入，为标委会注入了新的标准专家力量。三是着力开展WLAN领域概念辨析及宣贯，通过组织编写《WLAN领域关键概念辨析说明》，在联盟公众号、网站、《在路上》开设 “WAPI问答（系列连载）” 专栏等方式，去着力解决当前行业对WLAN、WAPI、Wi-Fi概念混淆不清等问题，解答用户单位在WAPI建设过程中的各种疑问。四是大力推进标准成果转化和实施应用。围绕用户单位“全国产、机具易用性”等需求，联盛德、至周科技、博洛米等会员单位发布了模组、鉴别服务器、无线接入点、终端等多款WAPI产品，目前已经上市。五是强化WAPI标准实施（被引用）工作推进，积极建立并增进了与相关标准化组织

之间的联系，促进技术融合和WAPI标准体系的引用。六是针对市场用户反馈的“WAPI精细化检测服务供给不足、WAPI物联网和工业互联网典型应用和解决方案尚不充分”等卡脖子难题，给予重点关注。结合南瑞集团等行业用户的具体需求，进行了点对点培训。

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在致辞中表示，10月14日是世界标准日，国际主题是美好世界的共同愿景，中国主题是数字时代的标准化，充分说明标准化对于全球未来发展的重要性。中国主题强调标准让数字时代的信息更安全，标准让数字时代的联通更高效，标准让数字时代的质量更可靠，标准让数字时代的发展环境更优化。WAPI标准产业共同体所开发的标准体系正服务于上述目标。作为新型产业标准开发平台，联盟将继续在新的技术和产业演进中，充当好行业管理、企业、科研机构、用户的桥梁作用，发挥好无线网络安全标准的联通和支撑作用。在过去的一年，WAPI产业在重要行业应用的步伐不断加快，关键基础技术、产品、测评技术、网络系统建设、密评等新的标准需求不断涌现，关键信息基础设施落地取得新的进展；技术标准和法律、行政法规、部门规章、政策文件等构成的产业合规性体系，其基础性指导性作用也越来越明显。希望大家齐心协力，通过所有利益相关方的技术洞察和实现经验反馈，将标准化工作推向新的高度。

黄振海还报告了第四季度团体标准和国际标准工作情况：在团体标准方面，完成2项团体标准立项投票工作，组织8项草案稿编制工作，形成征求意见稿3项、研究报告1份。在标准国际化方面，SC6国内技术对口工作稳步推进，第二季度共对内流通国际提案文件125份，向国际上反馈投票/意见18份；拥有我国自主知识产权的1项射频识别空中接口安全（TRAIS）国际标准获发布；我国主导的2项“无线局域网接入控制”进入国际标准草案（DIS）阶段，2项“未来网络—基于代理模型的服务质量”进入发布阶段；参与的4项“无人机区域网络（LADAN/UAAN）”标准进入FDIS阶段。在国际标准工作支撑方面，组织参加国家标准化活动，涉及ISO/IEC JTC1/SC27、SC6/WG1、SC6/AG4等分技术委员会或工作组，即将参加2023年1月召开的SC6/WG7中期会议。

WAPI产业联盟标准化部总监米东报告了2022年12月8日召开的无线网络安全标准化委员会2022年第四季度主任委员会议情况以及与会主任委员、副主任委员相关指导意见。

WAPI产业联盟市场总监简练报告了2022年第四季度标准产业市场应用阶段性进展。联盟标准化工作再传喜报，因标准化成果突出，WAPI产业联盟被授予“海淀区标准创新单位”；组织至周科技、博洛米、联盛德等多家厂商推出鉴别服务器、无线接入点、终端等多款全系列WAPI产品，联盟测试实验室给予高效和精细化检测支持。

联盟新成员北京佰才邦技术股份有限公司科技部总监兼标准总监云翔介绍了本单位情况和产品解决方案。佰才邦是3GPP、GTI等标准制定的积极参与者，拥有全硬件平台开发能力。佰才邦无线宽带产品可提供高品质的宽带接入业务，目前室内室外型CPE均集成WLAN模块。加入联盟后，佰才邦计划为行

业提供5G与WAPI全面融合解决方案，让随时随地的安全无线柔性办公成为可能。同时还将推出变电站WAPI可信解决方案，推动构建立体安全防护机制，杜绝非法接入、仿冒、入侵等安全隐患。

会议对已立项标准《无线网络安全 术语》《信息系统无线局域网密码应用基本要求》《无线局域网证书鉴别漫游应用扩展技术规范》《无线局域网设备技术要求与测试方法》（所有部分）、《信息安全技术 证书管理 第2部分：证书/私钥存储和使用技术》《信息安全技术 证书管理 第5部分：证书格式》《信息安全技术 三元鉴别可扩展协议消息封装扩展要求》《信息技术 无线局域网媒体访问控制和物理层规范 信息元素扩展要求》《传感器类设备专用WLAN通信模块技术要求与测试方法》《工业串口类设备专用WLAN通信模块技术要求与测试方法》进行了集中讨论并协商一致，形成了相关决议。

会议对2022年度技术标准工作进行了总结，盘点了“制度建设与完善，国际、国家、团体、地方等多层面的标准制修订工作，标准推广实施，标准国际化”等方面重要成果。此外，还从“继续落实固平台、提质量、定需求、促应用、优生态、抓机遇”等维度，介绍了2023年标准化工作计划重点。

SC6国内技术对口单位秘书处郑骊对SC6国内技术对口工作进行了总结报告，并鼓励更多专家积极参与国际标准工作。会议期间还开展了《国际标准组织常备文件体系分析》等标准化知识交流与培训。

媒体新闻链接：

飞象网：http://www.cctime.com/html/2022-12-23/1639026.htm

WAPI 问答（系列连载）

在WAPI服务各行各业关键信息基础设施建设过程中，联盟总结了一些市场用户的常见问题，并结合百度百科、搜狗百科、互动百科、维基百科中文版等对WAPI的解释存在一定不准确乃至错误之处，开辟WAPI问答（系列连载）栏目，帮助大家更加客观准确地了解WAPI。

欢迎您随时和我们交流探讨。

联系方式：010-82351181，staff@wapia.org

第二部分（PART 2）

1. 问：业界一些场景习惯把“无线局域网（WLAN）”称为“Wi-Fi”，是不是无伤大雅，只要理解意思就行?

答：不是。把“无线局域网（WLAN）= Wi-Fi”，相当于把 “篮球 = NBA”，把“卫星导航系统 = GPS”，形式上看是以偏概全，实质上是抹杀 / 忽视中国的自主技术成果，不正确且危害巨大。

一是错误使用导致违法。违反了《中华人民共和国国家通用语言文字法》中“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的注释”的规定。

二是可能未授权使用了美国Wi-Fi产业联盟组织的商标名称。使用“Wi-Fi”标记意味着产品符合美国Wi-Fi联盟标准（美IEEE标准+Wi-Fi联盟互操作标准），并通过了Wi-Fi联盟收费的产品认证。

三是以Wi-Fi取代WLAN，将导致技术/标准/产业被深度“绑架”。即：以偏概全符号固化 → 技术发展路径绑定 → 产业发展受制于人，危害巨大。

目前国内存在一些典型错误表达，包括政府或行业在公开会议/下发文件/采购要求中，把无线局域网（WLAN）称为“Wi-Fi”；一些WLAN覆盖（包括支持WAPI服务）的区域，标记为Wi-Fi等，这种错误做法需要纠正以传递正确信息，建议：规范使用正确中英文学名，在描述“无线局域网”这种网络形态时，使用正确表述——“无线局域网”或者“WLAN”；在描述“符合中国标准的无线局域网”时，使用正确表述——“符合GB 15629.11系列标准和相关行业/团体标准的无线局域网”或者“采用WAPI技术的无线局域网”。

2. 问：WAPI 比Wi-Fi更加安全，是因为用了国产密码算法么？

答：Wi-Fi自诞生起，业界就不断披露存在各种安全漏洞，最近的包括针对WPA2的KRACK攻击，以及针对WPA3的dragonblood等攻击，相对而言，WAPI迄今未被业界提出有安全漏洞。技术角度，主要是因为：

（1）WAPI安全架构更优。WAPI采用三元对等安全架构（对应全球安全架构演进的第三阶段），Wi-Fi采用二转三元过渡架构（对应全球安全架构演进的第二阶段）。在不同架构下，核心区别是无线接入点（AP）有没有独立身份，这决定了无线局域网终端和接入点的双向鉴别是直接还是间接（三元是直接，二转三元是间接），也导致Wi-Fi容易遭受中间人攻击（假基站）。

（2）WAPI安全协议设计更完备。WAPI采用具备原子性的五次传递过程确保安全，Wi-Fi采用的安全协议设计，已被全球业界揭示出容易遭受KRACK、dragonblood等攻击。

（3）WAPI采用国产密码算法。国产SM系列密码算法是经过我国密码学界长期研究提出的，目前已被发布成为国家标准和ISO/IEC国际标准，采用国产密码算法是WAPI高安全性的基础。

3. 问：现有的国家标准体系是2003年和2006年发布的，十几年过去了，WAPI是否还具有先进性？

答：WLAN标准是模块化演进的，2006年的标准最高通信速率是54Mbps，现在最新的ISO/IEC标准已经超过1Gbps，但标准均是后向兼容的，所以54Mbps的速率选项仍在最新标准中，也就是说，过去的标准并非失效了，仍然在使用中。另外，就安全部分而言，国际上普遍的规律是安全协议发展相对稳定、时间上迭代较慢，IEEE标准体系自2006年之后也只产生了一种新的机制（WPA3），并且架构同前。

因此，2006年发布的WAPI安全协议现在仍然适用，是符合技术发展和产业演进规律的，WAPI迄今没有发现安全漏洞，可提供无线局域网的安全连接能力。并且，基于WAPI安全协议，WAPI标准体系不断演进发展，数十项国家标准、行业标准、团体标准得到发布，现实中不同利益相关方的技术洞察和实现经验反馈到标准体系制定过程中，符合产业的发展需求。

4. 问：WAPI 所采用的三元对等（TePA）网络安全技术架构是什么，先进性在哪里？

答：三元对等架构（TePA）是引入在线可信第三方，实现两个实体对等鉴别的架构。以三元对等安全架构为核心，包括网络空间可信身份连接不可或缺的基础安全机制（实体鉴别、群签名、密钥管理等）；和网络基础连接所需的网络通信安全协议，如无线局域网安全（WAPI）、光/电以太网安全（TLSec）、射频识别空中接口安全（TRAIS）、近场通信安全（NEAU）等，形成了三元对等网络安全技术体系，为网络连接提供可一体化实现的原子性基础安全能力。

“信任”是通信中必不可少的，也是三元对等架构（TePA）的核心所在，该架构基于提出的独一无二的理念和创新：引入在线可信第三方的对等实体鉴别，“信任”在TePA中是天然融入的。

比如：当你遇到了一个人，不确认他/她是不是值得信赖，但是如果这个人是由你完全信赖的伙伴介绍给你认识的，那么他/她是可以信赖的。而且，在很多交流场景中，你无法直接联系到你完全信赖的伙伴，而只能联系到所遇到的那个人；而那个人可以直接联系到你完全信赖的伙伴，在这种情况下，如何判断他/她是否值得信赖？这就是TePA如何将“信任”集成到数据通信中的方式：为了验证对方的身份和可信度，实体之间需要一个在线可信第三方提供服务。

为了核实某人的身份，你或许可以通过查验他/她的护照、身份证或者名片。但是，你无法判定这些凭证本身的真伪，也无法判定这些凭证的拥有者是否应该被信任。

数据通信中往往会使用各种各样的凭证，最常见的是共享的密钥或者口令。但是，这些凭证无法用于防止黑客，而且仅仅适用于一个预先假设存在的信任关系条件下，而通常环境下这种信任关系又无法产生。

TePA优先选用的是最安全的凭证类型：公钥数字证书。如果两个实体试图建立一个通信会话，那么他们会交换数字凭证，然后提交给在线可信第三方进行验证——数字凭证的真实性、有效性，数字凭证是否适用于特定会话，数字凭证的拥有者在特定会话中是可以被信赖的。

TePA加强了可信实体的参与，确保了正确而全面的验证，TePA已经是ISO、IEC等国际安全标准中的一个组成部分，同时已经被国际标准化组织ISO/IEC、欧洲标准化组织ECMA以及中国国家标准的许多主要数据通信协议所采纳。

5. 问：除WAPI外，基于三元对等（TePA）安全架构的网络安全协议技术还有哪些？

答：三元对等架构（TePA）应用于有线、无线、近距离通信、IP网络等多种网络，已形成了二十多项网络安全协议技术，并已被国际标准（ISO/IEC）、欧洲标准、中国国家标准、行业标准、团体标准采纳，构建了新一代网络四层安全协议，为TCP/IP四层互联网协议提供基础安全架构。这些协议技术及标准已在能源、通信、金融、交通枢纽工程等关键基础设施，及国防、公用事业等多行业和领域应用。

除WAPI外，典型的网络安全协议技术及标准包括：

（1）以太网安全——TLSec：GB/T 15629.3；

（2）射频识别安全——TRAIS：ISO/IEC 29167-16，ISO/IEC TS 29167-15，ISO/IEC 19823-16，GB/T 28925，GB/T 28926，GB/T 29768，GB/T 35102，GJB 7377.1，GJB 7377.2等；

（3）近场通信安全——NEAU：ISO/IEC 13157-4，ISO/IEC 13157-5，ISO/IEC 22425，ECMA 410，

ECMA 411，ECMA 415，GB/T 33746，GB/T 30001.1，GM/T 0101等；

（4）IP安全可信——TISec：GB/T 25068.5等。

6. 问：WAPI基础标准发布已经近20年，并且标准体系在不断演进，目前应用的情况如何？

答：WAPI已经得到了广泛的应用，成为全球无线局域网芯片的标准配置，并且其安全能力已经在为关键信息基础设施提供安全保障。

截至2022年9月，支持WAPI的无线局域网芯片已超过500款型号、全球累计出货量超过220亿颗，移动终端和网络侧设备等已超过19000款，并为电信运营商集采网络设备提供了安全能力，除公共WLAN网络外，WAPI已广泛部署于海关、金融、能源、政务、公安、交通、医疗、教育等行业，成为行业物联网的关键组成部分。

目前，集成和支持WAPI功能的产品形态越来越丰富、产品体系越来越完善。包括但不限于：芯片、模组、个人电脑、智能手机、平板电脑、应用软件/APP、无线局域网接入点/路由器、无线局域网控制器、鉴别管理服务器、办公机具、各类行业专用机具等等。

7. 问：笔记本电脑如何升级支持并启用WAPI？

答：主流WLAN芯片均已具备WAPI安全能力，笔记本电脑厂商可以通过软件升级支持和让用户选择使用WAPI功能。具体方式是：笔记本厂商发布对应机型的支持WAPI的安装包，用户进行安装后，即可以使笔记本具备WAPI安全服务能力，无需更换硬件。

据不完全统计，戴尔、惠普等笔记本厂商均发布过此类安装包。

8. 问：对于一个AP/AC厂商来说，将AP/AC升级至支持WAPI，需要投入几名研发人员，多长时间？

答：WAPI的标准和相关算法都是公开的，任何厂商均可按照标准开发产品，也可以选择与有开发经验的厂商合作。据了解，在成熟的AP/AC产品上增加WAPI功能，投入2-3人约1-3个月可完成升级。

9. 部分WAPI产品取得了型号核准证书，在行业实际应用中却发现安全功能不完整，这是什么原因？

答：伴随着WAPI广泛服务国防、政务、能源、交通、金融等重要行业，WAPI常规互通性测试项目，已不能完全满足行业WAPI规模建设和业务运行的发展需求。有必要在WAPI协议互通性测试、WAPI协议完整性

测试等若干方面，依据最新标准增加精细化测试项目。

其次，市场用户对实施WAPI测评的要求，大多已贯穿了“产品采购前、网络建设中、运行管理时”全阶段。随着各阶段的不同、检测场景的不同，对测评工具的要求也不同，之前传统形态和功能的WAPI合规性检测系统并不能满足。所以一方面要对WAPI产品进行更加精细化的测试，另一方面还要对WAPI网络的功能性能进行测试。

10. 问：WAPI产业联盟测试实验室是政府机构么，通过了工信部相关检测后，是否需要再到联盟实验室通过检测，两者有什么区别?

答：WAPI产业联盟测试实验室是为联盟群体服务的自设机构，所提供的检测能力服务是对国家相关检测的良好补充。具体情况是：

（1）目前针对产品的WAPI能力，除了常规的符合性、互通性项目以外，还需要进行负面测试，目的是发现这些产品在WAPI协议实现上潜在的不完整。负面测试也称为协议完整性测试，可以检查产品在一些特殊极端情况下的表现。打个比方来说，对于一辆汽车，踩油门前进，踩刹车停止，这是正常的测试项目，但如果同时踩下刹车和油门，会发生什么情况？这个测试就属于负面测试范畴。WAPI产业联盟会定期对外发布WAPI测试项目，详情可咨询：010-82351181。

（2）WAPI产业联盟测试实验室提供协议完整性检测(负面测试)服务。检测无线局域网产品是否满足WAPI协议完整性的要求。无线局域网WAPI安全协议检测系统除了严格按照协议约定格式、字段属性构造、数据报文，对待测设备进行正确性，一致性检测、检验之外，增补设计了7大类协议完整性检测项目，分为异常WAI子类型、异常WAI头部字段、异常指定字段、异常完整性校验字段、异常WPI数据、异常组播密钥更新、异常AE签名属性字段；每一类分为若干项，每一项有一至两个测试用例。

此功能旨在设计一簇“错误”的WAPI协议程序库，并通过发送这类异常的WAPI数据报文与待测设备进行WAPI鉴别和加解密处理的过程，从而甄别设备是否能正确处理异常情况的过程。

负面测试服务有助于设备厂商和行业网络建设方尽快定位设备的安全风险，并指导设备的开发优化。

医院要严格落实商用密码应用
《“十四五”全民健康信息化规划》
全面推广商用密码应用

国家卫生健康委

近日，为推动“十四五”期间全民健康信息化发展，国家卫生健康委、国家中医药局、国家疾控局制定了《“十四五”全民健康信息化规划》。

《规划》要求在严格落实网络安全等级保护制度及商用密码应用等基础安全保障制度的基础上，以关键信息基础设施安全为重点，落实数据出境安全管理制度，加强医疗设备相关网络和数据安全监管，全面落实网络安全管理要求。

《规划》要求构建卫生健康行业网络可信体系。建设一批医疗卫生机构商用密码应用示范，全面推广商用密码应用，完善卫生健康行业商用密码应用体系。

《规划》提出8个方面主要任务。一是集约建设信息化基础设施支撑体系。二是健全全民健康信息化标准体系。三是深化“互联网+医疗健康”服务体系。四是完善健康医疗大数据资源要素体系。五是推进数字健康融合创新发展体系。六是拓展基层信息化保障服务体系。七是强化卫生健康统计调查分析应用体系。八是夯实网络与数据安全保障体系。

《“十四五”全民健康信息化规划》明确了如下：

夯实网络与数据安全保障体系坚持发展与安全并重，完善网络安全和数据安全制度，围绕网络与数据安全全链条、全要素、全周期加强教育培训和宣贯，加大网络安全投入，切实防范化解风险，提高安全防护能力，不断完善网络安全和数据安全综合防范体系。

全面落实网络安全和数据安全相关法规标准。贯彻落实《网络安全法》《数据安全法》《个人信息保护法》《密码法》《关键信息基础设施安全保护条例》及配套标准规范要求，履行好法律赋予的网络安全、数据安全监管权和行政执法权。在严格落实网络安全等级保护制度及商用密码应用等基础安全保障制度的基础上，以关键信息基础设施安全为重点，落实数据出境安全管理制度，加强医疗设备相关网络和数据安全监管，全面落实网络安全管理要求。研究制定卫生健康信息管理办法和相应的标准规范，对合理使用数据提供合规指南，对违规行为及时予以纠正。

完善网络安全和数据安全责任体系和管理制度。落实党委（党组）网络安全和数据安全责任制，压实主体责任，落实网络安全审查办法，强化绩效考核和评价机制。加强技术支撑机构建设，完善行业网络安全和数据安全监测、检查和通报机制，增强网络安全和数据安全应急响应能力，完善人防、物防、技防、制防、时防相关制度和措施，全面提升网络安全和数据安全管理能力。探索信息技术应用创新试点示范，提升供应链安全管理能力。

构建卫生健康行业网络可信体系。建设一批医疗卫生机构商用密码应用示范，全面推广商用密码应用，完善卫生健康行业商用密码应用体系。建设各类医疗卫生机构、人员和患者可信数字身份管理系统，实现医患可信身份电子认证和电子签名，保证访问、处理数据的用户身份真实，确保网络行为可管、可控、可溯源。完善卫生健康行业电子认证服务体系，实现电子认证服务跨区域互信互认。

中共中央 国务院：

构建数据基础制度 保障安全发展

2022年12月19日，中共中央、国务院印发《关于构建数据基础制度更好发挥数据要素作用的意见》，提出五项工作原则：

一是遵循发展规律，创新制度安排。探索有利于数据安全保护、有效利用、合规流通的产权制度和市场体系。

二是坚持共享共用，释放价值红利。强化反垄断和反不正当竞争，形成依法规范、共同参与、各取所需、共享红利的发展模式。

三是强化优质供给，促进合规流通。增强数据的可用、可信、可流通、可追溯水平。实现数据流通全过程动态管理，在合规流通使用中激活数据价值。

四是完善治理体系，保障安全发展。统筹发展和安全，贯彻总体国家安全观，强化数据安全保障体系建设，把安全贯穿数据供给、流通、使用全过程，划定监管底线和红线。加强数据分类分级管理，把该管的管住、该放的放开，积极有效防范和化解各种数据风险，形成政府监管与市场自律、法治与行业自治协同、国内与国际统筹的数据要素治理结构。

五是深化开放合作，实现互利共赢。

国务院：

携手构建网络空间命运共同体

2022年11月7日，国务院发布《携手构建网络空间命运共同体》白皮书。介绍了新时代中国互联网发展和治理理念与实践，分享中国推动构建网络空间命运共同体的积极成果，展望网络空间国际合作前景。

白皮书指出，随着新一轮科技革命和产业变革加速推进，互联网让世界变成了“地球村”，国际社会越来越成为你中有我、我中有你的命运共同体。发展好、运用好、治理好互联网，让互联网更好造福人类，是国际社会的共同责任。白皮书介绍，作为全球最大的发展中国家和网民数量最多的国家，中国顺应信息时代发展趋势，坚持以人民为中心的发展思想，秉持共商共建共享的全球治理观，推动构建网络空间命运共同体。

中国立足新发展阶段、贯彻新发展理念、构建新发展格局，建设网络强国、数字中国，在激发数字经济活力、推进数字生态建设、营造清朗网络空间、防范网络安全风险等方面不断取得新的成效，为高质量发展提供了有力服务、支撑和保障，为构建网络空间命运共同体提供了坚实基础。

中国不断深化网络空间国际交流合作，拓展数字经济合作，共同维护网络空间安全，积极参与全球互联网治理体系改革和建设，促进互联网普惠包容发展，与国际社会携手推动构建网络空间命运共同体。白皮书指出，互联网是人类的共同家园，让这个家园更繁荣、更干净、更安全，是国际社会的共同责任。中国愿同世界各国一道，共同构建更加公平合理、开放包容、安全稳定、富有生机活力的网络空间，携手构建网络空间命运共同体，开创人类更加美好的未来。

国家发改委：

全面加强网络安全保护，筑牢数字安全屏障

2022年10月28日，国家发展改革委发布《关于数字经济发展情况的报告》指出，要全面加强网络安全和数据安全保护，筑牢数字安全屏障。要贯彻国家网络安全、数据安全等法律法规，落实网络安全等级保护、关键信息基础设施安全保护等制度要求，强化网络、数据等安全保障体系建设，健全网络应急事件预警通报和应急处置机制，强化网络安全技术措施同步规划、同步建设、同步使用要求，推动网络安全产业高质量发展，增强网络安全防护能力。

科技部等九部门发文：

中关村示范区核心区的中央单位适用

《北京市促进科技成果转化条例》

2022年10月28日，科技部、发改委、教育部、财政部、国务院国资委等九部门联合印发《关于允许在中关村国家自主创新示范区核心区（海淀园）的中央高等院校、科研机构及企事业单位等适用<北京市促进科技成果转化条例>的通知》，允许注册在海淀园的中央单位适用《北京市促进科技成果转化条例》。政策的出台不仅可激发在园中央单位开展科技成果转化的内生动力、充分释放《条例》的制度红利，而且对于促进央地协同，推动北京市全面落实创新驱动发展战略具有重要意义。

国标委：

发布国家标准《信息安全技术 关键信息基础设施安全保护要求》助力关键信息基础设施安全保障体系建设

2022年10月12日，国家标准化管理委员会发布《信息安全技术 关键信息基础设施安全保护要求》（GB/T 39204-2022）国家标准。该标准是关键信息基础设施安全保护标准体系的构建基础，标准提出了以关键业务为核心的整体防控、以风险管理为导向的动态防护、以信息共享为基础的协同联防的关键信息基础设施安全保护3项基本原则，从分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等6个方面提出了111条安全要求，为运营者开展关键信息基础设施保护工作需求提供了强有力的标准保障。标准将于2023年5月1日正式实施。

国家卫健委：

夯实网络安全保障体系，全面推广商用密码应用

2022年11月9日，国家卫生健康委、国家中医药局、国家疾控局发布《“十四五”全民健康信息化规划》要求，要夯实网络安全保障体系，完善网络安全制度，围绕网络安全全链条、全要素、全周期加强教育培训和宣贯，加大网络安全投入，切实防范化解风险，提高安全防护能力，不断完善网络安全综合防范体系。要全面落实网络安全和数据安全相关法规标准，贯彻落实《网络安全法》《数据安全法》《个人信息保护法》《密码法》《关键信息基础设施安全保护条例》及配套标准规范要求。要在严格落实网络安全等级保护制度及商用密码应用等基础安全保障制度的基础上，以关键信息基础设施安全为重点，加强医疗设备相关网络安全监管，全面落实网络安全管理要求。要构建卫生健康行业网络可信体系，建设一批医疗卫生机构商用密码应用示范，全面推广商用密码应用，完善卫生健康行业商用密码应用体系。

北京市人大常委会：

重点保护关键信息基础设施，建立健全安全保障体系和产业生态

2022年11月25日，北京市人大常委会表决通过了《北京市数字经济促进条例》，自2023年1月1日起施行。条例规定，要对关键信息基础设施实行重点保护，建立关键信息基础设施网络安全保障体系，构建跨领域、跨部门、政企合作的安全风险联防联控机制，采取措施监测、防御、处置网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治危害关键信息基础设施安全的违法犯罪活动。要支持网络安全和软硬件产品的研发应用，鼓励安全评估、检测认证等数据安全服务业发展。支持农业、制造业、建筑、能源、金融、医疗、教育、流通等产业领域互联网发展，推进产业数字化转型升级，建立健全安全保障体系和产业生态。

工信部商密应用推进标准工作组：

要发挥密码在工业互联网安全中的核心保障和基础支撑作用

2022年11月，工业和信息化部商用密码应用推进标准工作组发布《工业互联网密码支撑标准体系建设指南》。指南明确了工业互联网密码支撑标准体系建设思路及目标，提出密码应用共性、设备密码应用、控制系统密码应用、网络密码应用、边缘计算密码应用、平台密码应用、数据密码应用、密码行业应用、密码应用管理与支撑等九个方面的标准建设内容。这对加快指导研制工业互联网密码应用标准，强化工业互联网安全防护能力，推动工业互联网产业高质量发展具有重要支撑作用。

WAPI产业联盟组织全员系统学习贯彻党的二十大精神

WAPI产业联盟　周　园

2022年10月，中国共产党第二十次全国代表大会胜利召开。为与党中央保持高度一致，并将党的方针政策与联盟工作密切联系起来，WAPI产业联盟组织秘书处全体工作人员展开了一系列党的二十大专题学习研讨活动。

10月16日，联盟统一组织秘书处全体工作人员在线观看了中国共产党第二十次全国代表大会开幕直播，同志们一边认真聆听习总书记的《高举中国特色社会主义伟大旗帜为全面建设社会主义现代化国家而团结奋斗》报告，一边做好要点记录，为后续深化理解吃透党的二十大精神并落实到工作中打好基础。

10月28日至30日，联盟在秘书处工作人员在自行学习领会基础上，连续 3天组织开展了党的二十大报告文件精读、理解和研讨活动。活动中，全体工作人员精读和理解了《党的二十大报告全文》，研读了“五个牢牢把握”、“三个务必”等要求，在对比新旧《中国共产党章程》基础上，重点学习领会了新党章修改的六方面内容。秘书处同志学习热情高涨，积极分享学习感悟，大家表示：集中系统学习令我们受益匪浅，对党中央的精神、目标、战

略有了更加清晰全面的认识。在今后的工作，联盟秘书处要自觉用党的二十大精神武装头脑，保持学思践悟，将党的二十大精神落实到“自主可控安全技术创新、产业链创新链供应链聚力合作、服务市场需求”等工作中，化为生动实践。

11月4日至23日，联盟组织秘书处工作人员和成员单位参加了4场北京市中关村社团第二联合党委、中关村产业技术联盟联合会主办的“学习贯彻党的二十大精神·名家宣讲解读”系列活动，线上学习了《以中国式现代化不断推进中华民族伟大复兴——党的二十大报告精神解读》、《认真学习贯彻二十大精神，全面推进网络安全产业新发展》、《学习贯彻党的二十大精神》、《关于认真开展学习宣传贯彻党的二十大精神活动的通知》。上述工作，获得了北京市中关村社团第二联合党委的肯定和段恒副书记的现场表扬。

11月28日，WAPI产业联盟组织秘书处全体工作人员参加北京市民政局综合党委系统学习宣传贯彻党的二十大精神宣讲报告会。认真聆听了北京市社会组织管理中心温育梁主任的报告，并在会后进行了会议精神分享与研讨。

通过系列学习，WAPI产业联盟秘书处全体同志更加坚定了永远跟党走的恒心，坚定了通过自身奋斗去加快实施创新驱动发展战略、加快实现高水平科技自立自强的决心。新的历史时期，我们要在党的二十大精神指引下，保持并进一步发扬我国在无线网络和网络安全领域的技术产业领先优势，发挥联盟社会组织在新一轮科技革命和产业变革中的驱动作用，以更昂扬的斗志、更坚定的信念、更强烈的担当、更有力的举措，组织产学研用聚力创新，为我国实现科技自立自强贡献力量！

北京市中关村社团第二联合党委开展“在路上·京西红色文化行” 党的主题活动

WAPI产业联盟　周　园

2022年10月25日，北京市中关村社团第二联合党委与WAPI产业联盟，组织所属社会组织及会员单位的党员、积极分子代表走进京西门头沟,联合开展“在路上·京西红色文化行”党的主题活动。

当天上午，活动人员赴京西门头沟的爨底下村，学习红色村庄的红色历史：爨底下村是我国保留比较完整的山村古建筑群，1942年日军烧毁爨底下村房屋228间，在抗日战争和解放战争时期，爨底下村年青人前赴后继，参军、参政、参战，80%的农户为军属、干属、烈属，有34名烈士为国捐躯。活动人员参观了抗日战争时期被日军烧毁的房屋遗址、记载革命历史的红色文化展室和红色宣传墙，听取了讲解人员的详细介绍。

下午，大家赴京西山区中共第一党支部所在地雁翅镇开展徒步活动，相继走访了崔显芳烈士纪念馆、田庄高小党支部旧址、崔显芳故居、雁翅镇革命英雄纪念碑等，领会红色星星之火可以燎原的革命奋进精神。

在一天充实的红色学习活动中，所有同志的思想觉悟得到进一步提升。大家深刻体会到当前和平、富足生活来之不易。老一辈革命家和全体军民的精神，激励了现场所有党员、积极分子和同志们，大家表示，要学习继承老一辈的大无畏、不屈不挠、艰苦斗争精神，并通过自身奋斗，将其发扬光大。

WAPI产业联盟秘书长张璐璐表示，联盟要坚定不移跟党走，坚决贯彻新时代党建工作要求，打牢全员思想基础，提升政治能力。具体工作中，我们要认真学习和落实党的二十大会议精神，在党的指引下，以无线网络安全技术产业创新为核心，以专业标准制定和促进科技成果转化为重点，以探索和建立无线网络和网络安全发展规律和科学运行模式为目标，为我国无线网络和网络安全产业健康快速发展做出新的更大贡献!

中关村无线网络安全产业联盟
第二届第一次会员大会暨换届大会成功召开

WAPI产业联盟　米 东

2022年11月9日，中关村无线网络安全产业联盟（以下简称WAPI产业联盟）在北京召开第二届第一次会员大会暨换届大会。会员听取并表决通过了联盟第一届理事会工作报告和财务工作报告、联盟第一届监事会工作报告、联盟《章程》和《会费收取和管理办法》，选举了联盟新一届理事和监事。

大会由联盟秘书长张璐璐主持。

联盟第一届理事长曹军做届内理事会工作报告和财务报告。2016年至2022年，WAPI产业联盟所开展的工作与国家战略高度一致，联盟基础条件优秀、内部治理科学有效、财务运行稳健、具高自律诚信主动性和社会组织探索性，凭借扎实的工作和显著的成果，获政府主管部门和会员单位肯定。这期间，

联盟标准产业共同体队伍持续壮大，已发布(获发布) 160项标准，包括国际标准、欧洲标准、国家标准、军用标准、行业标准、地方标准、团体标准等，形成了覆盖技术、产品、测试、应用等方面的完备标准体系；WAPI产业链、创新链、供应链完备，WAPI自主安全协议已被全球220亿颗芯片所集成，广泛服务政务、国防、海关、能源、交通、金融、医疗、教育等关基建设，有效保护了网络安全和数据资产不受侵害；结合对WAPI的深刻理解和专职化专业化的秘书处团队，持续开展了公共技术支撑平台建设和服务，解决了企业和市场“不想做、做不了，但又希望有人做”的技术产业难题。

联盟第一届监事长夏翔做届内监事会工作报告，报告了第一届监事会对联盟方方面面的监督情况。本届监事会认为，2016年至2022年联盟的日常工作、重大事件均做到了充分听取联盟会员意见，联盟的重大决策均通报了全体会员。联盟大会、理事会、秘书处各项工作，符合联盟《章程》中关于联盟工作范围的规定，各项决议规范有效。

会上，集体表决通过了联盟第一届理事会工作报告和财务工作报告、联盟第一届监事会工作报告、新一届联盟《章程》和《会费收取和管理办法》；选举西电捷通公司曹军、中关村无线网络安全产业联盟张璐璐、中国电信股份有限公司高波、中国联合网络通信集团有限公司邱勇、国家密码管理局商用密码检测中心张众、国家无线电监测中心检测中心尹玉昂、北京数字认证股份有限公司侯鹏亮、中电科普天科技股份有限公司林凡、北京中电华大电子设计有限责任公司兰天、深圳市明华澳汉智能卡有限公司李翔、北大方正集团有限公司陈实如为新一届理事会成员；选举北京柴傅律师事务所夏翔、北京登合科技有限公司单丹、迈创智慧供应链股份有限公司丁思海为新一届监事会成员。

同日召开了中关村无线网络安全产业联盟第二届第一次理事会和监事会。会上，选举曹军同志为联盟新一任理事长、夏翔同志为联盟新一任监事长、张璐璐同志为联盟新一任秘书长，集体表决通过了联盟内部管理制度。

新一任理事长曹军在发言中表示，本届会员大会是联盟新的开篇，新的理事会和领导班子的建成，标志着联盟将迈向一个新的高度。我们会牢记联盟初心和使命，脚踏实地做工作，真正地为党和政府、为产业市场、为社会做实事。当前WAPI等网络安全市场需求大、质量要求更高，联盟这5年的工作重点是：第一、致力与生态伙伴协同打造高效协作的无线网络安全标准产业共同体，进一步丰富WAPI产业链、创新链、供应链；第二、通过标准、方案、检测等抓手，服务市场用户的安全自主可控无线网络建设和应用需求；第三、持续联盟公共平台建设，为产业市场提供精准服务，解决“企业想做、做不了、但必须有人做的卡脖子难题”。通过这些扎扎实实的工作，发挥出产业联盟社会组织的独特作用，聚力创新，服务市场需求，让企业获得实实在在的收益。

作为开放的、国际化的协同创新平台，我们欢迎所有致力于此的单位加入WAPI产业联盟，携手同行，为推动无线网络安全产业健康持续高效发展作出新的更大贡献！

2022年无线网络安全标准化委员会第四季度主任委员会议顺利召开

WAPI产业联盟　米 东

2022年12月8日，WAPI产业联盟无线网络安全标准化委员会（以下简称“标委会”）副主任委员黄振海主持召开第四季度主任委员会议。副主任委员王立建、张璐璐、陶洪波、王宏，及联盟秘书处标准化部、市场与产业部负责同志参加了会议。

联盟标准化部总监米东从2022年第二次主任委员会议精神落实情况、第四季度标准化工作成效、机遇与挑战等方面汇报了第四季度联盟标准化重点工作。结合今年第二次主任委员会议精神，联盟标准化部组织开展如下工作：第一、WLAN领域概念辨析及宣贯，组织编写了《WLAN领域关键概念辨析说明》，《在路上》期刊也开设了 “WAPI问答（系列连载）” 专栏，解决行业对WLAN、WAPI、Wi-Fi概念混淆不清等问题，解答各行各业关基建设中对WAPI的关注。第二、稳步推进标准化工作， 9项国际标准、1项国家标准、15项团体标准、1项北京地方标准、1项中关村标准的制修订正按计划推进，其中1项国际标准、1项北京市地方标准获发布。第三、推进标准成果转化和实施应用。联盛德、至周科技、博洛米等联盟会员发布了鉴别服务器、无线接入点、终端等多款WAPI系列产品。

标委会副主任委员、总体工作组组长黄振海做《强化WAPI标准实施（被引用）情况汇报》。为进一步推进WAPI标准的应用，标委会总体工作组制定了相应方案，积极建立并增进与相关标准化组织之间的联系，促进对彼此标准体系的了解，从组织角度促进技术融合和WAPI标准体系的引用。目前已与国标委相关专业技术委员会、行业标准化协会、团标组织建立联系。

联盟市场总监简练重点汇报当前WAPI产业应用和网络部署中遇到的问题和瓶颈，针对市场用户对WAPI精细化检测服务供给不足、WAPI物联网和工业互联网典型应用和解决方案等重点关注，与会专家充分讨论并给予了详实建议。

会上，审议通过了2022年无线网络安全标准化委员会全体会议方案，审议通过了2022年度标委会优秀委员和优秀项目编辑提名，围绕2023年标委会工作重点和规划进行了研讨，并将要点共识列入年度工作计划。

儒安物联安全无线局域网系列产品通过联盟测试

WAPI产业联盟　王立华

图：联盟为儒安物联安全无线局域网系列产品出具测试报告

日前，儒安物联科技集团有限公司（以下简称儒安物联）的安全无线局域网系列产品通过了WAPI产业联盟无线局域网鉴别与保密基础结构（WAPI）互通性、完整性及功能测试。联盟为上述产品出具了测试报告。

本次受测设备包含无线接入点（AP）、终端（STA）、鉴别服务器（AS）。其中，AP、STA设备均支持2.4/5GHz双频工作，通信速率支持802.11ac协议；AS设备具备漫游功能，能满足行业大宽带、移动性、大连接等应用需求。

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。测试过程中，联盟实验室和设备厂商积极克服疫情困难，通过远程联调等方式，高效地完成了此次测试。

随着安全无线局域网广泛应用，越来越多厂商均在大规模生产制造WAPI产品，并力争为行业用户提供从接入到鉴别的整体解决方案，满足用户设备选型和采购需求。

WAPI产业联盟发布最新版《WAPI标准产业应用及环境监测报告》

WAPI产业联盟　简 练

2022年12月20日，WAPI产业联盟发布最新版《WAPI标准产业应用及环境监测报告》。

本期《报告》，重点对报告的第一部分“无线局域网涉及国家政策和法规信息索引”进行了修编，将一些发布时间较早的政策进行了删减，重点聚焦现行有效的、具有持续性的政策和法律法规，提升阅读效率。

《WAPI标准产业应用及环境监测报告》是WAPI产业联盟帮助政府、厂商、市场用户深入了解安全无线局域网（WAPI）的产业和市场全貌，服务市场建设和示范，提升WAPI技术产业成果转化效率，加强产业链上下游企业-企业、企业-市场之间的对接合作的重要工具。主要内容包括：无线局域网及WAPI政策及配套监管、国家标准符合依据、全产业链厂商及其产品统计分析、市场应用示范案例、公共关键技术和解决方案、技术标准体系介绍等，以电子文档或印刷品形式面向政府、产业、公众公开。《报告》中涉及的产品数据与信息，均源自公开媒体或厂商。其中，产业数据统计、应用情况统计、WAPI等网络安全技术标准情况统计，均截至2022年12月20日。鉴于产业特性和技术迭代，存在一定动态变化的可能。

《报告》全文可通过扫描下方二维码下载：

博洛米B0882型WAPI鉴权服务器AS通过权威测试认证

博洛米

南京博洛米通信技术有限公司B0882型WAPI鉴权服务器AS通过WAPI测试实验室/WAPI产业联盟测试认证。

博洛米是一家可信通信整体解决方案供应商。作为最重要的产品线之一，近年来公司不断加大WAPI可信无线局域网系统的研发投入，目前已经陆续推出了二十多款产品，通过了相关测试和认证，并成功应用于仓储、物流、能源、安保、运输等行业。下一步公司将继续丰富和完善产品线，提供涵盖中间件模组、终端、无线接入点、接入控制器和鉴别服务器等产品，并跟进用户需求进行国产化、自主可控、安全性、可靠性、兼容性定制，从而提供WAPI可信无线局域网高性能、全栈式整体解决方案。

MTK发布两款天玑移动芯片 支持WAPI

MediaTek

2022年11月8日，MediaTek发布天玑9200旗舰5G移动芯片，凭借在高性能、高能效、低功耗方面的创新突破。天玑9200支持高速5G网络以及即将到来的802.11be无线连接，支持WAPI，以先进科技赋能移动终端打造专业级影像、沉浸式游戏体验，推动全球移动体验升级。

天玑9200支持MediaTek HyperCoex超连接技术，当WLAN和蓝牙同时连接时，能提供更强的信号、更远的连接距离、更强的抗干扰能力，无论影音娱乐还是连接游戏外设，都让用户享受更低时延。

2022年12月8日，MediaTek发布天玑8200 5G移动芯片，赋能高端手机升级游戏、影像、显示与连接体验。天玑8200支持802.11ax连接速率，支持WAPI，采用先进的4nm制程，八核CPU架构包含4个Cortex-A78大核，主频最高达到3.1GHz，搭载Mali-G610六核 GPU，助力终端充分释放高性能、高能效优势。

据悉，搭载以上两款芯片的智能手机预计将于2022年底上市。

国务院发文强调多次的电子签章
如何为建设数字政府提速

数字认证

随着国家大力推进数字政府建设，数字基础设施逐渐从分散建设到共建共享，形成上下联动、纵横协作、共享顺畅的一体化、集约化数字政府平台支撑格局。6月国务院印发《国务院关于加强数字政府建设的指导意见》中，提出数字政府建设的七方面重点任务，其中明确提出要加强重点共性应用支撑能力，推进数字化共性应用集约建设。国务院办公厅多次在发文中提及电子印章应用，作为数字经济发展的重要一环，电子签章平台为各行业提供数字化改造升级支撑的同时，全面夯实数字政府建设根基，助力提升千行百业的数字化、智能化水平，优化营商环境，帮助实现省级市级政务服务“一网通办”从“网上可办、网上申办”向“全程网办、全网通办”超越。

数字认证基于多年政务服务经验，结合密码和云计算领域的技术积累，基于微服务架构，为企事业单位提供闭环的电子签章服务，覆盖电子签章制作、备案、授权、应用等全流程，能够与业务应用无缝集成，满足多终端、多场景、跨域互签互验的电子签章应用，充分满足企事业单位在各领域的各类签章需求。

在政务服务领域，满足各类数字政府业务在身份可信、行为可信、信任传递等方面的需求，赋能数字政府各个职能领域，实现“全程网办、全网通办”，优化营商环境，提高群众满意度，提升政府运行效率。在公共服务和商业服务领域，通过可信合法、安全可靠的电子签章平台，与业务应用无缝集成，切实推进集团各级组织机构印章的统一管控和使用日志审计，推动业务用章全流程电子化、业务办理无纸化，减轻企事业单位运营成本，提高企业运营效率。

电子签章接入政府内部办公系统后，省去公文人工邮寄、分发等线下工作，政务公文传输可实现在线化，推动政府公文流转、审批、联合发文等。

原先需要企业和个人到现场递交资料，办理如营业执照、运输许可证照、出入境证明等，如今通过电子签章服务，可实现“不见面办理”，经办人网上递交盖印电子签章的资料后，不出门不排队仅需短短几分钟即可完成资料提交，大大减少了时间和人力的投入。

让跨省市投标、医保社保转移、住房公积金提取等高频服务事项，实现跨省通办，互签互认，缩短办事周期、减少来回奔波，切实解决企业、群众异地办事的不便。

除政务服务外，在招投标业务、企业内部信息化平台建设、商业合同及劳动合同签署中、金融机构电子材料提交等场景下，实现业务用章全流程电子化、业务办理无纸化，推动更多业务移动端办理，进一步实现降本增效，全方位赋能企业运营。

锐捷网络成功上市 登陆深交所创业板

证券时报

2022年11月21日，锐捷网络股份有限公司（证券代码：301165，下称“锐捷网络”）在深圳证券交易所创业板上市。

锐捷于2010年加入WAPI产业联盟。在网络设备领域，锐捷网络持续实现高速增长。2019年至2021年，网络设备收入复合增长率达33.4%。锐捷网络始终引领数据中心网络创新升级，数据中心交换机市场近3年复合增长率达55.8%。此外，锐捷网络深耕无线网络用户场景，解决高复杂场景应用难题，在助力客户业务创新的同时赢得市场领先。

在网络安全领域，锐捷网络安全产品服务政府、金融、教育等行业客户超10,000家，并结合客户需求不断开发出有针对性、创新性的产品方案，满足各行业客户不断增长的信息化和数字化建设需求。

新华三助力85家上榜医院数字化转型

天极网

11月20日，复旦大学医院管理研究所正式发布《2021年度中国医院排行榜》百强名单，新华三集团连续12年领航医疗行业数字化，助力85家百强医院数字化转型。

“十四五”期间，全面推进健康中国建设处于国家优先发展的战略位置。智慧医院是“健康中国”建设总体战略的重要组成部分。面对新机遇，新华三集团陆续突破，依托“数字大脑”的全栈实力持续创新，打造了多场景下的智慧医院解决方案，并连续12年领航医疗行业数字化。此外，新华三集团联合10多类90+TOP医疗生态合作伙伴，共同打造智慧化联合解决方案，以“伙伴优先”原则落实“五个加速”，经过H3C DILab兼容性认证，为客户提供端到端方案落地保障。

五角大楼将公布零信任网络战略

金台资讯

据美国“防务新闻”网站报道，美国国防部零信任网络战略正在接受公共审查，相关文件将于近期公布。该战略将对五角大楼实现零信任的百余项行动进行阐述，涵盖应用程序、自动化和分析学。五角大楼试图通过构建各部门范围内零信任网络安全架构，确保国防部相关企业重要数据的安全。

五角大楼首席信息官约翰·谢尔曼近期表示，美国已不再是唯一拥有最先进网络与通信技术的国家，若不对本国网络进行防护，其他同样精通网络技术的国家可通过多种技术手段访问美国机密网站，窃取相关数据，威胁美国国家安全和社会稳定。因此，提高数据安全等级已成为美国当前十分重要的任务。

零信任是网络安全的一种新范式，假设网络始终处于危险之中，因此，需要对用户和设备进行持续验证。这种做法被称为“从不信任，总是核实”。此次零信任战略的提出是对拜登政府2021年颁布的《关于改善国家网络安全行政令》的进一步落实，旨在由传统的基于边界的网络防御转向持续验证，将政府安全架构迁移至零信任架构，加强抵御网络威胁的能力。

总体来说，五角大楼零信任战略行动措施包括：各机构工作人员使用特定身份访问应用程序，各机构对其网络环境中所有域名解析系统请求和超文本传输协议进行加密，联邦政府拥有运营和授权使用所有设备的完整清单，所有应用程序接入互联网并定期接受严格测试，利用云安全服务监控敏感数据的访问。

随着信息技术的迅猛发展，网络已成为现代军事斗争的重要战场。近年来，以美国为首的西方国家纷纷加大网络技术在军事领域的研究和投入。2009年，美军成立网络司令部，成为全球首个公开将战争机构引入互联网的国家。近年来，美国不断扩大网络部队规模，组织多场网络战演习。美军计划2024年前实现基于美国网络安全和基础设施安全局零信任成熟度模型的安全目标。

据介绍，此次零信任网络战略的出台，是美军加固其网络安全的重要举措。这一战略以新技术为核心，试图利用零信任这一新兴安全保障技术，达到提高网络安全水平的目的，体现出美军对网络安全的高度重视。有分析人士指出，作为世界头号军事强国，美国对网络安全的要求会越来越高。此次零信任网络战略也不可能是终点，有必要对美军网络战略的后续发展进行跟踪研究。

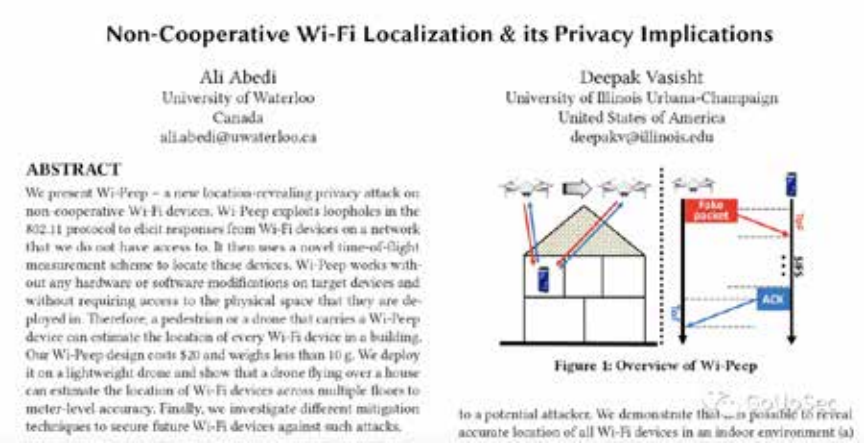
攻防最前线：

用无人机监控Wi-Fi网络中的设备和人员

节选自安全内参

近日，伊利诺伊大学的研究人员发表了一篇有趣的新论文，题为“非合作式Wi-Fi定位与隐私影响”，讨论如何用无人机Wi-Fi定位和跟踪室内设备及其使用者。

这项新的攻击技术被称为Wi-Peep，攻击者无需获取Wi-Fi网络的访问权限，即可通过802.11协议中的一个缺陷来跟踪Wi-Fi设备的踪迹：



Non-Cooperative Wi-Fi Localization & its Privacy Implications

Ali Abedi
University of Waterloo
Canada
ali.abedi@uwaterloo.ca

Deepak Vasisht
University of Illinois Urbana-Champaign
United States of America
deepakv@illinois.edu

ABSTRACT

We present Wi-Peep – a new location-revealing privacy attack on non-cooperative Wi-Fi devices. Wi-Peep exploits loopholes in the 802.11 protocol to elicit responses from Wi-Fi devices on a network that we do not have access to. It then uses a novel time-of-flight measurement scheme to locate these devices. Wi-Peep works without any hardware or software modifications on target devices and without requiring access to the physical space that they are deployed in. Therefore, a pedestrian or a drone that carries a Wi-Peep device can estimate the location of every Wi-Fi device in a building. Our Wi-Peep design costs $20 and weighs less than 10 g. We deploy it on a lightweight drone and show that a drone flying over a house can estimate the location of Wi-Fi devices across multiple floors to meter-level accuracy. Finally, we investigate different mitigation techniques to secure future Wi-Fi devices against such attacks.

Figure 1: Overview of Wi-Peep

to a potential attacker. We demonstrate that ... is possible to reveal accurate location of all Wi-Fi devices in an indoor environment (a)

图1：研究论文

根据论文，攻击者无需在目标设备上安装任何软件即可实施攻击（监控），系统可以移植到无人机上或携带到物理空间中。设备成本不到20美元，重量不到10克（小型无人机可以轻松携带）：

图2：Wi-Peep设备原型

该研究调查了安装在无人机上的Wi-Peep的使用情况。总体而言，攻击的第一阶段需要发现目标设备的MAC地址。这涉及到虚假信标的传输，以及设备MAC地址响应的位置（即使接入不同的Wi-Fi接入点）：

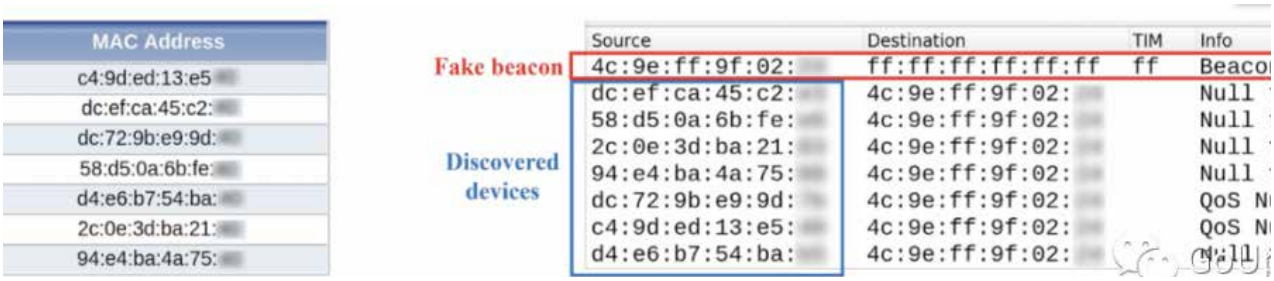


图3：通过信标请求发现设备

该攻击使用了ToF（飞行时间）方法来定位设备。攻击者测量接收确认所花费的时间，然后将其乘以光速值。接收确认信息中包含来自目标设备的时间戳，攻击者可以计算它们之间的延迟。然后，攻击者可以计算出往返飞行时间和SIFS（数据包接收和ACK传输之间的延迟）。有了这些数据，攻击者可以将设备定位在一定半径范围内。

之后，攻击者发送与目标所在Wi-Fi网络无关的虚假Wi-Fi数据包，也就是论文中提及的“礼貌的Wi-Fi技术”（编者：Wi-Fi通讯协议的一个不安全机制，会向未接入网络的陌生设备发送的任何数据包反馈确认数据包）：

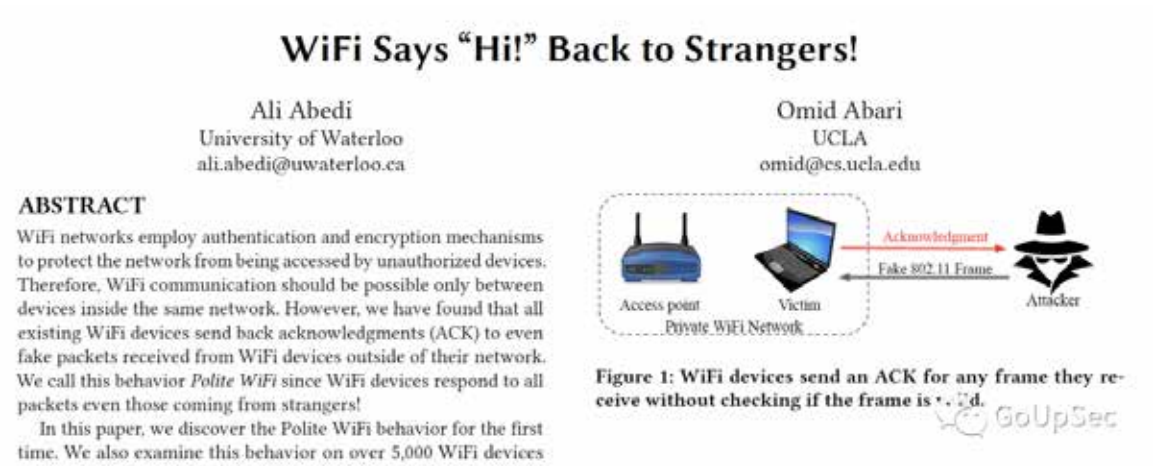


图4：“礼貌的Wi-Fi”

使用这种方法，研究人员之前发现许多设备都会响应“Wi-Fi礼仪”请求，并且反馈的MAC地址通常会暴露设备制造商名称：

WiFi Client Device		WiFi Access Point	
Vendor	# devices	Vendor	# devices
Apple,	143	Hitron	723
Google	102	Sagemcom	601
Intel	66	Technicolor	410
Hitron	65	eero	195
HP	63	Extreme N.	188
Samsung	56	Cisco	156
Espressif	47	HP	104
Hon Hai	46	TP-LINK	101
Amazon	41	Google	80
Sagemcom	38	D-Link	75
Liteon	33	NETGEAR	69
AzureWave	30	ASUSTek	51
Sonos	30	Aruba	46
Nest Labs	27	SmartRG,	44
Murata	24	Ubiquiti N.	35
Belkin	20	Zebra	35
TP-LINK	20	Pegatron	28
Cisco	16	Belkin	25
ecobee	13	Mitsumi	25
Microsoft	13	Apple	19
Others	630	Others	789
Total	1523	Total	3805

Table 2: List of WiFi devices and APs that respond to our fake 802.11 frames.

图5：设备供应商发现

通过发送“礼貌的Wi-Fi”请求，研究人员发现他们甚至可以监控目标是如何使用设备。根据下面这个图表，攻击者可以监控设备在地面上的活动——被用户拾起，打字，然后将设备放回地面：

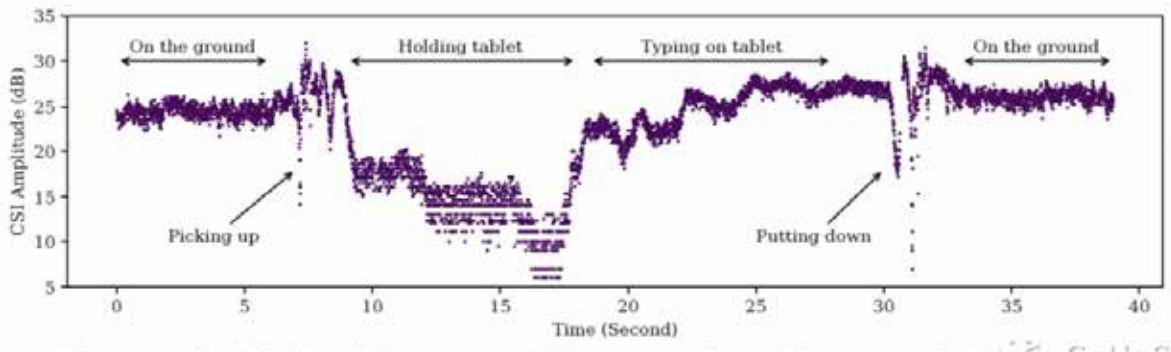


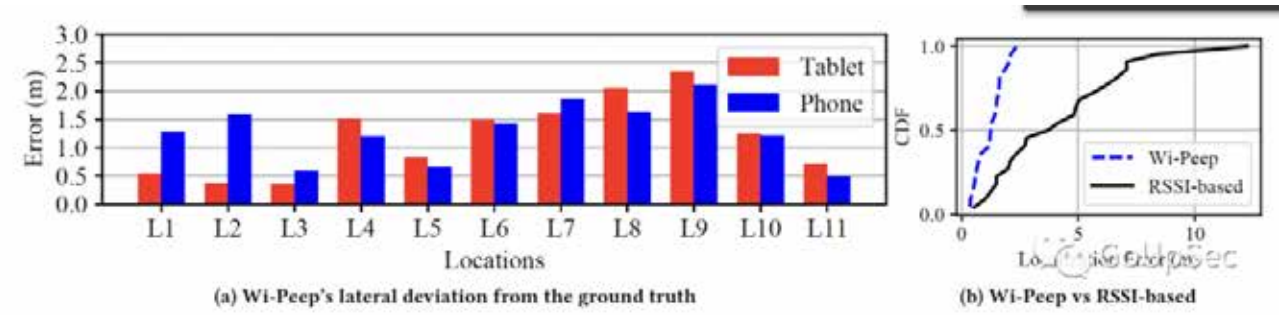
Figure 5: The measured CSI of acknowledgments received from a victim device. The variation of CSI can potentially reveal information such as activities and even the text typed on this device.

图6：设备的活动监控

研究团队设置了一个在地下室、主楼层和二楼的房子中定位11台设备的实验：

Figure 8: The floor plan of the target building.

结果表明，二楼的定位误差相当小（小于0.5m），但当设备放置在主楼层时误差增加（误差高达2m）。令人惊讶的是，地下室设备的定位误差通常低于楼上的设备：



(a) Wi-Peep's lateral deviation from the ground truth

(b) Wi-Peep vs RSSI-based

浅谈下一代无线局域网技术

本文由无线网络安全技术国家工程研究中心供稿

一、背景情况

无线局域网（WLAN）技术近20年来一直在不断演进，WLAN技术按功能可分为基础通信技术模块和安全技术模块，目前主流产品支持的最新基础通信技术为IEEE 802.11ax（注：Wi-Fi联盟把使用802.11ax的WLAN称作Wi-Fi 6）。802.11ax主要使用了OFDMA（正交频分多址）、MU-MIMO（多用户多入多出）等技术，MU-MIMO技术允许路由器同时与多个设备通信，而不是依次进行通信。MU-MIMO允许路由器一次与多达4个设备同时通信（演进版本最多支持8条数据流）。802.11ax还利用其他技术，如OFDMA和发射波束成形，两者的作用分别提高效率和网络容量。802.11ax理论最高速率可达9.6Gbps。近几年各种应用的发展，对WLAN的数据吞吐率和时延等方面提出了新的需求。

针对现有协议已无法完全满足日新月异需求场景的情况，IEEE于2019年成立了802.11be EHT(Extremely High Throughput)工作组来对下一代WLAN基础通信协议标准化，工作组的目标是在802.11ax基础上将吞吐率提高到30Gbps+，频谱在现有的标准下进一步扩充并进一步降低复杂环境下的无线网络延时和抖动。工作组已于2022年10月发布D2.0协议草案，计划至2023年10月发布D5.0，最终的协议标准D5.0-Pub预计将于2024年5月发布。

二、IEEE 802.11be支持的新特性：

更大数据容量

802.11be将信号的调制方式升级到了4096-QAM，以拥有更大的数据容量。无线技术当然会涉及到信号的调制方式，在802.11ax中，标准使用的是1024-QAM调制，而802.11be预计将继续升级调制方式，直接使用4096-QAM，进一步扩大传输数据容量，为最高的30Gbps吞吐率打好基础。

更低时延

延迟是指数据在进行传输时的时间长度，在无线传输中非常重要。802.11ax技术的延迟在10-20毫秒，演进版本在干扰较少的环境中可以实现更低的延迟。在802.11be的网络标准中，通过MLO、行波变换(TWT)和rTWT改进触发传输，以及最终集成的时间敏感网络(TSN)功能，使得802.11be延迟降低到低于10毫秒。

更多数据流（预计）

802.11be支持更多的数据流，引入了CMU-MIMO。802.11ax最多支持8条数据流，而引入MU-MIMO

是其一大升级之处，让多个设备可以同时使用多条数据流与接入点进行通信。802.11be会将这个数字扩大一倍，设备可以支持16条数据流，支持更多的数据流也将带来更强大的特性CMU-MIMO。其中，C代表Coordinated（协同），意为16条数据流可以不由一个接入点提供，而是由多个接入点同时提供。

CMU-MIMO是迎合无线网络多接入点发展方向的新特性。为了扩大WLAN网络的覆盖范围而常采用Mesh组网方式，这其实就是增加了接入点数量；而CMU-MIMO可以让用户充分利用多出来的接入点，将16条数据流分流到不同的接入点中，同时进行工作。

三频段同时工作

其次，802.11be还引入了新的6GHz频段，三频段同时工作。众所周知，802.11ax可同时使用2.4GHz和5GHz两个频段，而它的演进版本则引入了新的6GHz频段。802.11be将会继续使用这个新频段，并努力达成同时使用三个频段进行通信的目标，从而获得更大的通信带宽来增加自己的速率，并且还将扩大单信道的宽度，从802.11ax的160MHz倍增至320MHz。

引入Multi–Link多链路机制

为了实现所有可用频谱资源的高效利用，迫切需要在2.4 GHz、5 GHz和6 GHz上建立新的频谱管理、协调和传输机制。802.11be工作组定义了多链路聚合相关的技术，主要包括增强型多链路聚合的MAC架构、多链路信道接入和多链路传输等相关技术。

支持Multi–RU机制

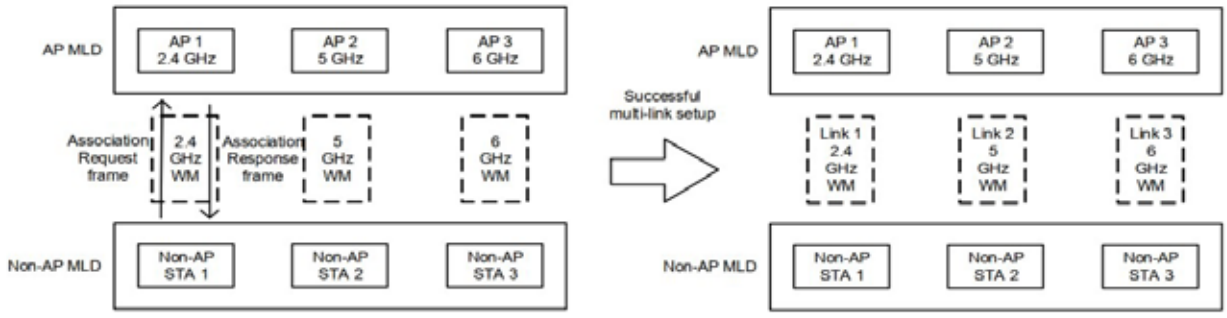
在802.11ax中，每个用户只能在分配到的特定RU上发送或接收帧，大大限制了频谱资源调度的灵活性。为解决该问题，进一步提升频谱效率，802.11be中定义了允许将多个RU分配给单用户的机制。当然，为了平衡实现的复杂度和频谱的利用率，协议中对RU的组合做了一定的限制，即：小规格RU（小于242-Tone的RU）只能与小规格RU合并，大规格RU（大于等于242-Tone的RU）只能与大规格RU合并，不允许小规格RU和大规格RU混合使用。

更舒适智能互联体验

就应用层面来说，届时如果802.11be的传输速度真能达到30Gbps，则可为用户带来更加流畅、快速的传输体验，因其拥有更大的覆盖范围并有效的减少了传输拥堵问题，将更有力的助推8K超高清视频产品的普及。从用户角度来看，802.11be让8K视频的在线播放不再是梦，用户也会因此获得更好的影音体验。此外，更快的传输速度也一定会延伸出更多的智能产品功能与体验，譬如人工智能互动、家居智能控制，解决当下消费者在这些领域的消费痛点，获得更加舒适的智能体验。

WLAN基础通信部分主要规范的是物理层PHY和MAC层技术，在802.11be中，PHY的一个主要变化就是MLD（多链路设备），即提供多链路物理层支持的硬件，MLD的MAC部分即为MLO。在MLD以前的IC（简

单理解为射频radio）虽然支持多个频段的连接，但是每次只能选择一个频段进行连接。对一个终端而言，一次只能和AP建立一个单独的WLAN连接，即不是连接在2.4GHz上，就是连接在5GHz上。而多个AP可以多个频段同时工作，但是其实现方法是通过多个IC的方式进行处理，即不同频段使用不同的IC进行隔离，从而允许多频段并行工作互不影响。



图：多频段链路建立

MLD指的是提供多个链路的设备，可以理解为AP1，AP2和AP3是同一个AP的中的一个或多个射频IC（Radio），这个射频IC包含了三个频段，对应2.4GHz，5GHz和6GHz频段。图中的下半部分中对应的是终端STA，STA和AP一样，也是一个射频IC对应三个频段。AP和STA之间可以建立多个连接，即图中链路1，2，3。802.11be的这种特性能够将频谱资源通过多条链路优化使用，带来如下优势：

- 吞吐量的增加：多条链路意味着可以同时进行数据传输，不考虑传输方式的情况下，吞吐量等价于各个链路之和。

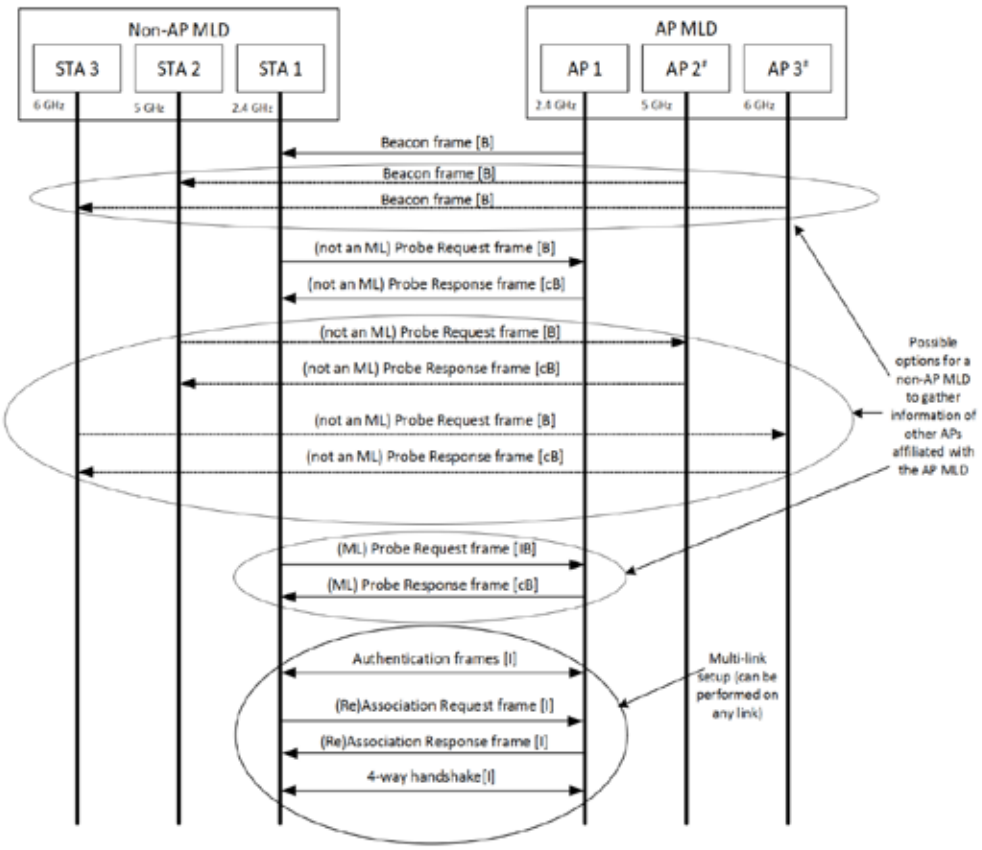
- 降低延时：因为多个不同频段链路的存在，相比之前单链路的信道竞争，多链路增加了设备获取信道通信的概率，从而降低了通信延时。同时终端接入时的选择性也大大提高。

- 增加数据传输可靠性：不同的链路可以传输相同的数据，链路间可以互补，减少数据帧的重传，提高数据传输可靠性。

- 传输分流和隔离：不同的链路工作在不同的频段上，同时多链路使用时支持同时双向传输，即链路1发送，链路2接收同时进行。

IEEE 802.11be与WAPI

802.11be所规范的技术属于基础通信模块，主要对PHY和MAC技术进行研究改进，完整的无线局域网技术还包括安全部分，中国自主研发的WAPI安全技术，近年来也在不断演进，已经形成了完备的安全保障技术体系。在下一代无线局域网产品中，需要研究802.11be与WAPI结合的接口定义及要求。



图：多链路建立过程

上图是在多链路模式下链路建立的过程，WAPI协议工作时，主要与MAC层协议协同实现安全关联及数据保密等安全功能，802.11be与之前版本协议的主要区别在于新增的多链路特性，所以与WAPI结合的接口研究重点是在多链路模式下如何实现WAPI安全机制的策略协商、策略选择、安全关联、身份鉴别及密钥体系的建立。在non-AP MLD和AP MLD之间的多链路(重)建立成功之后，基密钥安全关联和单播密钥安全关联在non-AP MLD和AP MLD之间建立，而对于建立的每个链路，在non-AP MLD和AP MLD之间建立组播密钥安全关联。如果启用管理帧保护则建立完整性组播安全关联。单播密钥安全关联用于在所有建立链路上对单独寻址的MPDU进行加密封装和解封装，链路的组播密钥安全关联用于对链路上的组寻址MPDU进行加密封装和解封装。启用管理帧保护时，链路的完整性组播安全关联用于为链路上的组寻址稳健管理帧提供完整性保护。在身份鉴别及密钥建立过程中需要扩展安全关联及相关密钥与每个链路的对应关系，需要在交互的消息中增加相关的信息内容。

在安全关联及密钥体系建立的基础上，基于多链路模式实现数据的保密通信。在数据通信过程中需要根据多链路通信的特点定义多链路地址和分组序号PN等信息的处理接口。

802.11be目前还是草案阶段，预计随着后续工作开展，协议还会做一定的完善和扩展，与WAPI协议的接口定义也会随之做进一步扩展。

WAPI 产业联盟成员单位名录

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

【注：截至2022年12月，联盟正式成员已达114家，以加入联盟的时间先后排序。】

WAPI Alliance

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