ICS 35.030
CCS L 78

团　体　标　准

T/WAPIA 046—2021/XG1—2025

无线局域网安全技术规范

第 1 号修改单

Security technical specification for wireless LAN

Amendment 1

2025-06-30 发布　　2025-06-30 实施

中关村无线网络安全产业联盟　发布

版权声明

前　言

本文件按GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是T/WAPIA 046《无线局域网安全技术规范》的第1号修改单。

本文件与T/WAPIA 046—2021相比，主要技术变化如下：

a) WAI2协议封装格式（见修改5，2021版的第6.2.1）；

b) 组播密钥通告过程协议封装（见修改10，2021版的6.2.3.2）。

其中，对T/WAPIA 046—2021修改时涉及到的有关章条的信息如下：

修改项号	T/WAPIA 046—021 章条号	修改说明
1	全文	T/WAPIA 046—2021 标准文本全文“WAI 增强”修改为“WAI2”
2	全文	T/WAPIA 046—2021 标准文本全文“WAPI 信息元素”修改为“WAPIE”
3	4	T/WAPIA 046—2021 4.2 缩略语增加内容
4	6.1.6.3	T/WAPIA 046—2021 6.1.6.3 内容替换
5	6.2.1	T/WAPIA 046—2021 6.2.1 内容替换
6	6.2.2.1	删除 T/WAPIA 046—2021 6.2.2.1 标题下的内容，保留章条号及标题
7	6.2.3.1.1	T/WAPIA 046—2021 6.2.3.1.1 内容替换
8	6.2.3.1.2	T/WAPIA 046—2021 6.2.3.1.2 表 3 替换
9	6.2.3.1.3	T/WAPIA 046—2021 6.2.3.1.3 表 4 替换
10	6.2.3.2	T/WAPIA 046—2021 6.2.3.2 内容替换
11	6.5.3.1	T/WAPIA 046—2021 6.5.3.1 内容替换
12	6.2.3.2.3	删除 T/WAPIA 046—2021 6.2.3.2.3
13	6.2.3.4	在 T/WAPIA 046—2021 6.2.3.3 内容之后增加 6.2.3.4
14	B.4.3	T/WAPIA 046—2021 附录 B.4.3 第 7.3 节管理帧帧体组成部分相关修改中 7.3.2.8.2 替换
15	B.4.3	T/WAPIA 046—2021 附录 B 7.3.2.9 内容替换

本文件由中关村无线网络安全产业联盟与工业和信息化部宽带无线 IP 标准工作组联合提出。

本文件由中关村无线网络安全产业联盟无线网络安全标准化工作委员会归口。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件起草单位：无线网络安全技术国家工程研究中心、西安西电捷通无线网络通信股份有限公司、中关村无线网络安全产业联盟、西安芯语慧联信息科技有限公司、深圳市智开科技有限公司、工信部宽带无线 IP 标准工作组、国家密码管理局商用密码检测中心、国家信息技术安全研究中心、国家无线电监测中心检测中心、中国移动通信集团有限公司、中能融合智慧科技有限公司、广西大学、广西诚新慧创科技有限公司、中国通用技术研究院、北京数字认证股份有限公司、北京计算机技术及应用研究所、广西通量能源技术有限公司、广州未来能源中心。

本文件主要起草人：张变玲、曹军、张国强、潘琪、刘高锦、童伟刚、简练、王月辉、李冬、铁满霞、李琴、黄振海、颜湘、王宏、陶洪波、陈宇、张阳、赵晓荣、沙学松、卢泉、韦利娜、刘科伟、侯鹏亮、赖晓龙、杜志强、孟伟、郑骊、张璐璐、刘剑昕、王立华、朱正美、韦昌才、贾嘉、于光明、陈维刚、肖龙、周涛、王锐、李国友、邓开勇、马丹丹、陈更、杨晓宇、田玉存、刘鸿运、张芝军、罗鹏、尹玉昂、于双双、赵万峰、李玉娇、周园、孙硕、陈晓龙、胡霄亮、赵慧、芦亮。

无线局域网安全技术规范

第 1 号修改单

1　T/WAPIA 046—2021 标准文本全文“WAI 增强”修改为“WAI2”

2　T/WAPIA 046—2021 标准文本全文“WAPI 信息元素”修改为“WAPIE”

3　T/WAPIA 046—2021 4.2 缩略语增加以下内容：

BIMK　信标帧完整性组播密钥（beacon integrity multicast key）
KeyID　密钥标识（key identifier）
LinkID　链路标识（link identifier）
MLO　多链路操作（multi-link operation）
WAPIE　WAPI信息元素（WAPI information element）

4　T/WAPIA 046—2021 6.1.6.3 内容替换为：

6.1.6.3 鉴别和密钥协商

如果STA与AP/STA关联时选择采用WAPI安全机制，双方应进行双向身份鉴别和密钥协商，过程如下：

a) 若采用基于WAI证书的方式，身份鉴别和密钥协商过程包括证书鉴别、单播密钥协商与组播密钥通告；若采用WAI预共享密钥的方式，身份鉴别和密钥协商过程为单播密钥协商与组播密钥通告。

STA与AP/STA之间的鉴别数据分组利用以太类型字段为0x88B4的WAI协议传送，AP/STA与ASU之间的鉴别数据报文通过UDP套接口传输，ASU的端口号为3810。

b) 若采用基于AKEA(AKEA-C和AKEA-P)的方式，身份鉴别和密钥协商过程包括原子密钥建立与实体鉴别，还可包含组播密钥通告。STA与AP/STA之间的AKEA鉴别数据分组利用EEP封装后用以太类型字段为0x88B4的WAI协议传送，AP与ASU之间的AKEA鉴别数据报文通过UDP套接口传输，ASU的端口号为5111。

WAPI鉴别和密钥管理完成的时间应小于MIB值gb15629dot11wapiConfigSATimeout，它开始于STA的站管理实体决定建立WAPI安全网络，到MLME-SETPROTECTION.request原语被激发结束。若在MIB值gb15629dot11wapiConfigSATimeout的时间内没有完成安全关联的建立，则两个STA将解除链路验证。

5　T/WAPIA 046—2021 6.2.1 内容替换为：

6.2.1 WAPI 安全机制概述

6.2.1.1 WAPI 安全机制

WAPI为系统提供安全保护。WAPI包含以下部分：

a) WAI 鉴别和密钥管理：

1) WAI证书鉴别和密钥管理,见6.2.2；

2) WAI预共享密钥鉴别和密钥管理,见6.2.2；

3) WAI2证书鉴别和密钥管理，采用证书的原子密钥建立与实体鉴别（AKEA-C），见6.2.3；

4）WAI2预共享密钥鉴别和密钥管理，采用预共享密钥的原子密钥建立与实体鉴别（AKEA-P），见6.2.3。

b）WPI 数据保密，包括二种工作模式：

1）WPI-SM4-OFB+CMAC-128，见6.5.3.2；

2）WPI-SM4-GCM-128，见6.5.3.3。

6.2.1.2 WAI 协议封装格式

WAI鉴别系统的WAI协议分组数据基本格式见图5。WAI协议分组中各字段如无特殊说明均按大数结尾顺序编码发送。

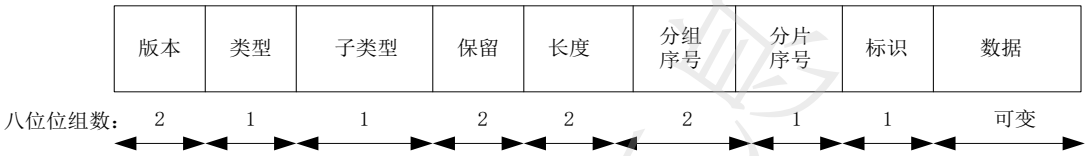


图5　WAI 鉴别系统的 WAI 协议分组数据基本格式

ASUE、AE 和 ASU 之间的 WAI 协议分组数据的字段定义如下。

——版本字段长度为 2 个八位位组，表示鉴别基础结构的版本号。版本号值为 1；

——类型字段长度为 1 个八位位组，表示协议类型，定义如下：

1　表示 WAI 协议分组；

2　表示 WAI2 协议分组；

其他值保留。

——子类型字段的长度为 1 个八位位组：

1）　当类型字段的值为 1 时，子类型字段值定义如下：

1 表示预鉴别开始分组；

2 表示站间密钥请求分组；

3 表示鉴别激活分组；

4 表示接入鉴别请求分组；

5 表示接入鉴别响应分组；

6 表示证书鉴别请求分组；

7 表示证书鉴别响应分组；

8 表示单播密钥协商请求分组；

9 表示单播密钥协商响应分组；

10 表示单播密钥协商确认分组；

11 表示组播密钥/站间密钥通告分组；

12 表示组播密钥/站间密钥响应分组；

其他值保留。

2）　当类型字段的值为 2 时，子类型字段值定义如下：

1 表示 EEP 分组；

其他值保留。

3）　当类型字段为其他值时，子类型字段值保留；

——保留字段长度为 2 个八位位组，默认值为 0；

——长度字段长度为 2 个八位位组，其值表示 WAI 协议分组所有字段的八位位组数；

——分组序号字段长度为 2 个八位位组，其值表示协议分组序号。第一个分组序号为 1，后序分组依次按 1 递增；

——分片序号字段长度为 1 个八位位组，其值表示分片的顺序编号，每一个分组的第一个分片序

号为0，后序分片依次按1递增；

——标识字段长度为1个八位位组，第0位表示后续是否有分片，值为0表示没有，值为1表示有。位1至位7保留；

——数据字段的内容根据类型和子类型的值而定，它除了包含固定的内容，还可包含可选的属性。

其中：分组序号字段、分片序号字段和标识字段仅在ASUE和AE之间的WAI协议分组中有效。定义WAI协议分组的最大长度为65535个八位位组。

6　删除T/WAPIA 046—2021 6.2.2.1标题下的悬置段。

7　T/WAPIA 046—2021 6.2.3.1.1内容替换为：

6.2.3.1.1 鉴别与密钥建立概述

WAI2采用AKEA协议，包括基于证书AKEA-C和预共享密钥AKEA-P两种鉴别与密钥建立方法，实现实体鉴别的同时，完成基密钥和单播密钥的建立。AKEA-C鉴别协议定义见T/WAPIA 045.3—2021，AKEA-P鉴别协议定义见T/WAPIA 045.4—2021。WAPI中的ASUE实体对应AKEA中的REQ，WAPI的AE实体对应AKEA中AAC,WAPI实体中的ASE实体对应AKEA中的AS。

协议中AKEA-C-AACauth和AKEA-P-AACauth负载中的EncData($Text_{AAC}$)字段，$Text_{AAC}$为Text类型的数据元素，数组元素值格式见图34a，包括AP在信标帧和探询响应帧中发送的WAPIE和若干个WAPI密钥数据信息元素，密钥数据内容为AP要通告的组播会话密钥、完整性组播密钥和信标帧完整性组播密钥。STA检查$Text_{AAC}$的元素字段中的WAPIE和自己收到的信标帧和探询响应帧的WAPIE是否相同，若不相同，解除与AE的链路验证。

WAPIE	WAPI-MSK	WAPI-IMK	WAPI-BIMK

图34a AKEA-C-AACauth和AKEA-P-AACauth中$Text_{AAC}$数据元素值格式

协议中AKEA-C-REQauth和AKEA-P-REQAuth负载中的EncData($Text_{REQ}$)字段，$Text_{REQ}$为Text类型的数据元素，数据元素值包含ASUE的WAPIE，在BSS模式下，该字段和ASUE在关联请求帧中发送的WAPIE相同；在IBSS模式下，该字段包含ASUE选择的单播密码算法、AE通告的组播密码算法和当前使用的鉴别和密钥管理套件列表。在BSS模式下，AP检查$Text_{REQ}$中的WAPIE字段和自己收到的关联请求帧的WAPIE是否相同，若不同，解除与STA的链路验证；在IBSS模式下，检查$Text_{REQ}$中WAPI元素字段选择的单播密钥算法是被支持的，如果不支持则解除与STA的链路验证。

注：EncData类型和Text类型的数据元素定义见T/WAPIA 045.1—2021第5章。

8　T/WAPIA 046—2021 6.2.3.1.2表3替换为：

表3 AKEA-C安全能力

编号	安全能力名称	安全能力取值
1	密钥协商机制	SM2密钥交换协议
2	KDF算法	SM4-XCBC-MAC-128
3	PRF算法	KD-HMAC-SM3
4	MAC/MIC算法	HMAC-SM3

编号	安全能力名称	安全能力取值
5	数据分组加密算法（用于 AKEA-C 协议字段加密及 EEP 安全数据通信加密）	SM4-GCM-128
6	身份鉴别机制	MIA
7	数字签名算法	无匿名 SM2 数字签名算法
8	匿名实体	不支持
9	是否包括 AS	身份鉴别机制需要包括 AS
10	主动身份保护	支持 REQ 和 AAC 主动身份保护
11	被动身份保护	不支持
12	安全信道密钥更新	必须采用安全信道进行密钥更新
13	HASH 算法	SM3
14	身份 ID	MAC 地址或证书信息或根据本地策略设置其他类型

9　T/WAPIA 046—2021 6.2.3.1.3 表 4 替换为：

表 4 AKEA-P 安全能力

编号	安全能力名称	安全能力取值
1	密钥协商机制	SM2 密钥交换协议
2	KDF 算法	SM4-XCBC-MAC-128
3	PRF 算法	KD-HMAC-SM3
4	MAC/MIC 算法	HMAC-SM3
5	数据分组加密算法(用于 AKEA-C 协议字段加密及 EEP 安全数据通信加密）	SM4-GCM-128
6	身份鉴别机制	MIA
7	是否包括 AS	身份鉴别机制不包括 AS
8	身份保护	支持
9	安全信道密钥更新	必须采用安全信道进行密钥更新
10	是否支持高强度的身份鉴别密钥	支持
11	是否支持秘密的密钥交换	支持
12	HASH 算法	SM3

编号	安全能力名称	安全能力取值
13	身份 ID	MAC 地址或根据本地策略设置其他类型身份 ID

10 T/WAPIA 046—2021 6.2.3.2 内容替换为：

6.2.3.2 WAI2 组播密钥建立

6.2.3.2.1 WAI2 组播密钥通告流程

WAI2组播密钥通告分组和WAI2组播密钥响应分组封装在EEP安全数据通信（组播密钥分发）的数据部分。EEP的规定见T/WAPIA 045.1—2021第8章。

WAI2组播密钥建立协议见图35。

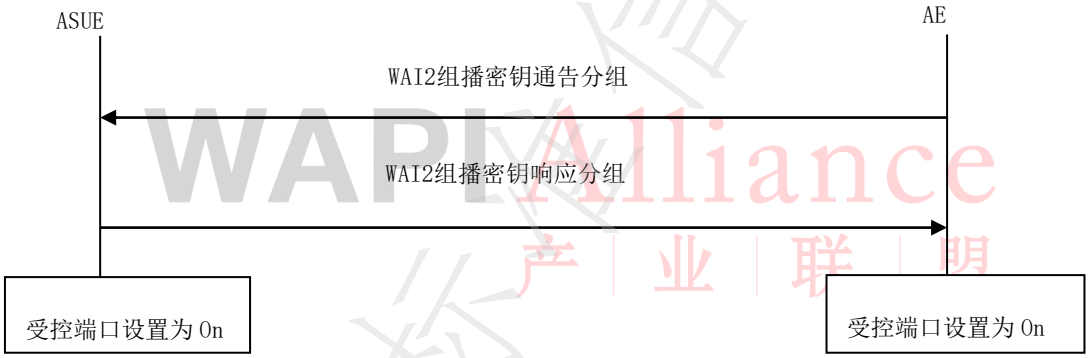


图35 WAI2 组播密钥通告过程

WAI2组播密钥通告分组和WAI2组播密钥响应分组封装在EEP安全数据通信的数据部分，其中EEP子类型值为254，安全数据通信类型值为2，标识组播密钥分发。EEP在传输时封装在WAI2协议中。EEP的规定见T/WAPIA 045.1—2021第8章。

EEP中封装的组播密钥分发数据格式见图36。

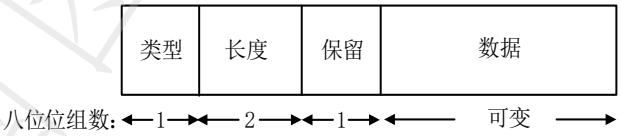


图36 WAI2 组播密钥分发数据格式

字段定义如下。

——类型字段长度为 1 个八位位组，标识消息类型，类型字段的值定义如下：

1 表示组播密钥通告分组；

2 表示组播密钥响应分组；

其他值保留。

——长度字段长度为 2 个八位位组，标识组播密钥分发数据所有字段的长度；

——保留字段长度为 1 个八位位组，默认值为 0；

——数据字段的内容根据类型字段的值而定。

6.2.3.2.2 WAI2 组播密钥通告分组

AE要更新组播密钥/完整性组播密钥/信标帧完整性组播密钥时，AE向ASUE发送组播密钥通告分组通告组播密钥/完整性组播密钥/信标帧完整性组播密钥。

WAI2组播密钥通告分组数据格式见图37。

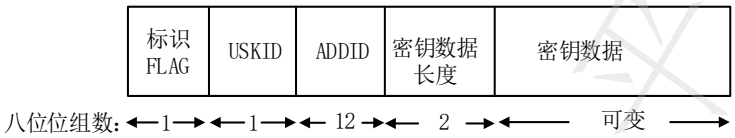


图37　WAI2 组播密钥通告分组数据字段格式

字段定义如下。

——标识 FLAG 字段长度为 1 个八位位组，为保留字段；

——USKID 字段长度为 1 个八位位组；

——ADDID 字段长度为 12 个八位位组。当通告的密钥是 STAKey 会话密钥时，该字段的值为发起方的 MAC 地址||对端的 MAC 地址；当通告的密钥为组播会话密钥或完整性组播密钥时，该字段的值为 MAC_{AE}||MAC_{ASUE}；

——密钥数据字段包含若干个密钥数据信息，其内容字段是 AE 通告的密钥，通告的密钥为 AE 生成的随机数。格式见图 37a。

图 37a 密钥数据字段格式

注：依据协商的密码套件，会话密钥可能包含加密密钥和完整性校验密钥，这种情况下密钥数据分为长度相等的两部分，第一部分为加密密钥，第二部分为完整性校验密钥。

ASUE接收到AE发送的组播密钥通告分组后，进行如下处理。

a) 生成组播密钥响应分组，发送给 AE。

b) 安装密钥。若密钥数据包含组播密钥或完整性组播密钥或信标帧完整性组播密钥，则利用原语 MLME-SETWPIKEYS.request 安装新的组播会话密钥或完整性组播密钥或信标帧完整性组播密钥，并调用原语 MLME-SETPROTECTION.request 启用其接收功能；一旦使用此新密钥正确解密或校验过数据时，删除旧的组播密钥或完整性组播密钥或信标帧完整性组播密钥。

若AE通告了新的组播密钥，ASUE保存组播密钥，在接收组播数据帧时根据KeyIdx字段选择组播解密密钥，当ASUE接收到AE用最新通告的组播密钥加密的组播数据帧，并且校验和解密均正确时，丢弃旧的组播密钥。

若AE通告了新的完整性组播密钥，ASUE保存完整性组播密钥，在接收组播管理帧时根据KeyIdx字段选择完整性组播密钥进行校验，当ASUE接收到AE用最新通告的完整性组播密钥保护的组播管理帧，并且校验正确时，丢弃旧的完整性组播密钥。

若AE通告了新的信标帧完整性组播密钥，ASUE保存信标帧完整性组播密钥，在接收信标帧时根据KeyIdx字段选择信标帧完整性组播密钥进行校验，当ASUE接收到AE用最新通告的信标帧完整性组播密钥保护的信标帧，并且校验正确时，丢弃旧的信标帧完整性组播密钥。

6.2.3.2.3 WAI2 组播密钥响应分组

WAI2组播密钥响应分组数据字段格式见图38。

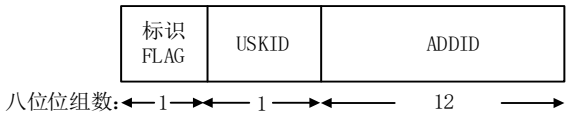


图38　WAI2 组播密钥响应分组数据字段格式

字段定义如下。

——标识字段长度为 1 个八位位组，定义如前，此字段值应与 AE 发送的 WAI2 组播密钥通告分组中的标识字段值相同；

——USKID 字段长度为 1 个八位位组，此字段值应与 AE 发送的 WAI2 组播密钥通告分组中的 USKID 字段值相同；

——ADDID 字段长度为 12 个八位位组，该字段的值和 WAI2 组播密钥通告分组中 ADDID 字段值相同。

ASUE向AE发送WAI2组播密钥响应分组，AE接收到ASUE发送的WAI2组播密钥响应分组后，进行如下处理。

a) 比较标识、USKID 字段和 ADDID 字段与发送的 WAI2 组播密钥通告分组中的相应字段值，若均相同，则本次组播密钥通告成功；否则，丢弃该分组。

b) 通告成功后，若 AE 已通告给所有已关联的 ASUE，则删除旧密钥。若此次通告的密钥尚未安装，则利用原语 MLME-SETWPIKEYS.request 安装新密钥，AE 调用原语 MLME-SETPROTECTION.request 启动新密钥的发送功能，即利用此密钥加密组播数据或计算组播管理帧完整性校验码或信标帧完整性校验码。AE 在更新组播密钥过程中，使用旧的组播密钥对组播数据帧进行加密发送，当对所有已关联到该 AP 的 STA 均组播密钥通告后，才启用最新通告的组播密钥用于组播数据帧的加密发送。AE 在更新完整性组播密钥或信标帧完整性组播密钥过程中，使用旧的完整性组播密钥或信标帧完整性组播密钥对组播管理帧或信标帧进行校验码计算发送，当对所有已关联到该 AP 的 STA 均完成完整性组播密钥或信标帧完整性组播密钥通告后，才启用最新通告的完整性组播密钥或信标帧完整性组播密钥用于计算组播管理帧完整性校验码或信标帧完整性校验码。

11　T/WAPIA 046—2021 6.5.3.1 内容替换为：

6.5.3.1 WPI-SM4 封装结构

WPI-SM4的MPDU封装结构见图41　。

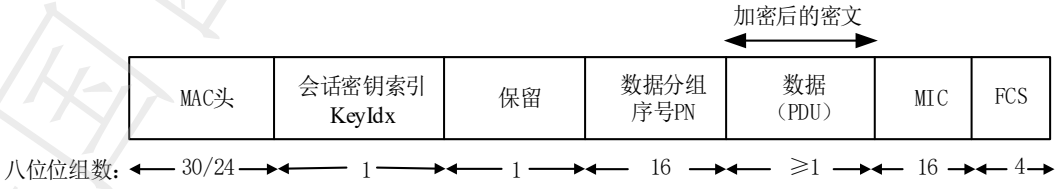


图41　WPI-SM4-OFB+CMAC-128 的 MPDU 封装结构

字段定义如下。

——MAC 头字段，当地址 4 存在时，长度为 30 个八位位组；当地址 4 不存在时，长度为 24 个八位位组；

——KeyIdx 字段长度为 1 个八位位组，表示 USKID 或 MSKID 或 STAKeyID 值；

——保留字段长度为 1 个八位位组，默认值为 0；

——PN 字段长度为 16 个八位位组，表示一个整数，标识数据分组序号，该数据分组序号作为数据加密和校验时所需的 IV。数据分组序号 PN 字段按小数结尾编码发送；

——PDU（数据）字段为 MPDU 数据，最大长度为 2278＝2312－18（WPI 头）－16（MIC）个八位位组；

——MIC 字段长度为 16 个八位位组；

——FCS 字段长度为 4 个八位位组，为 MAC 帧格式的帧校验序列；

——MIC 字段是利用完整性校验密钥对完整性校验数据计算得到，MIC 计算时完整完整性校验数据见图 42。

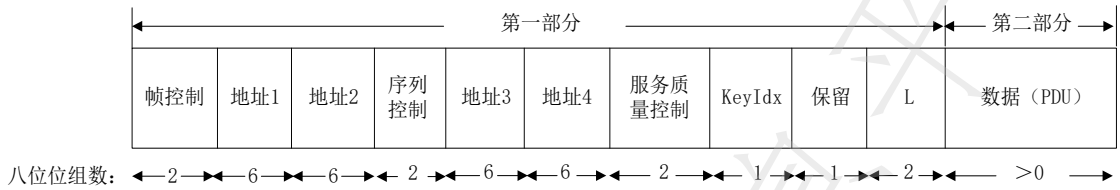


图42　完整性校验数据

完整性校验数据包含两部分内容，其中第一部分作为AAD使用。

第一部分：

——帧控制，2 个八位位组；

1） 位 4、5、6 在数据帧中置为 0；

2） 位 11、12、13 置为 0；

3） 位 14 置为 1；

4） 位 15：

- 当该分组时包含 QoS Control 字段的数据帧时置为 0；
- 其他情况保留原始值；

——地址 1，6 个八位位组；

——地址 2，6 个八位位组；

——序列控制字段（位 4～15 置为 0），2 个八位位组；

——地址 3，6 个八位位组；

——地址 4，6 个八位位组。若 MAC 帧头中不存在地址 4 时，则该字段的 6 个八位位组的值均置为 0；

——QC 如果出现，其是表示 MSDU 优先级的 2 个八位位组的 QoS Control 字段。QC TID 字段用于构建 AAD。如果在 non-DMG BSS 中里 STA 和对端的 SPP A-MSDU Capable 字段都为 1，那么 AAD 构建里使用位 7（the A-MSDU Present 字段）。当 STA 或对端的 SPP A-MSDU Capable 字段为 0，QC 字段的其余位设置为 0（位 4～6,8～15，位 7）。在 DMG BSS 中，位 7 和位 8（A-MSDU Type 字段）用于构建 AAD，其余位的值在构建 AAD 时设为 0（位 4～6，位 9～15）；

——KeyIdx 字段。1 个八位位组；

——保留字段。1 个八位位组；

——PDU 数据的长度 L。2 个八位位组。该字段按大数结尾编码计算。

第二部分：

——PDU 数据。大于 0 个八位位组。

在WPI-SM4-OFB+CMAC-128中使用CBC-MAC模式计算完整性校验码MIC时，应保证完整性检验数据的长度为16个八位位组的整数倍。若完整性校验数据第一部分的长度不足16个八位位组的整数倍，应将第一部分扩展为16个八位位组的最小整数倍，扩展采用第一部分后面补零的方法；若完整性校验数据第二部分的长度不足16个八位位组的整数倍，应将第二部分扩展为16个八位位组的最小整数倍，扩展采用第二部分后面补零的方法。接收方验证校验时采用相同的处理。

数据发送时，WPI-SM4-OFB+CMAC-128的MPDU封装过程如下：

a） 利用完整性校验密钥与数据分组序号 PN，通过工作在 CMAC 模式的校验算法对完整性校验数据进行计算，得到完整性校验码 MIC；

b) 利用加密密钥与数据分组序号 PN，通过工作在 OFB 模式的加密算法对 MPDU 数据||MIC 进行加密，得到 MPDU 数据||MIC 的密文；

c) 封装后再组帧发送。

数据接收时，WPI-SM4 的 MPDU 解封装过程如下：

a) 判断数据分组序号 PN 是否有效，若无效，则丢弃该数据，且将 MIB 值 gb15629dot11wapiStatsWPIReplayCounters 加 1；

b) 利用解密密钥与数据分组序号 PN,通过工作在 OFB 模式的解密算法对分组中的 MPDU 数据||MIC 密文进行解密，恢复出 MPDU 数据||MIC 明文。若此时没有有效的解密密钥，则丢弃该数据，且将 MIB 值 gb15629dot11wapiStatsWPIDecryptableErrors 加 1；

c) 利用完整性校验密钥与数据分组序号 PN，通过工作在 CMAC 模式的校验算法对完整性校验数据进行本地计算，若计算得到的值与分组中的完整性校验码 MIC 不同，则丢弃该数据，且将 MIB 值 gb15629dot11wapiStatsWPIMICErrors 加 1；

d) 解封装后将 MPDU 明文进行重组处理。

12 删除 T/WAPIA 046—2021 6.2.3.2.3。

13 在 T/WAPIA 046—2021 6.2.3.3 内容之后增加 6.2.3.4：

6.2.3.4 安全关联更新与密钥更新

采用WAI2协议建立安全关联后，根据本地策略设置安全关联更新时间，安全关联更新应对STA和AP的身份重新鉴别，在重新鉴别的基础上应对基密钥、单播会话密钥和组播密钥进行更新。

单播密钥更新采用AKEA-L带鉴别的密钥交换机制,其中涉及到的算法及参数与身份鉴别过程中协商的算法参数保持一致。BK和单播密钥更新完成后需要更新组播密钥。AKEA-L鉴别协议规定见T/WAPIA 045.2—2021。

单播密钥更新采用的AKEA-L协议，封装在加密的EEP安全数据通信协议中，其中EEP子类型值为254，安全数据通信类型值为1，标识密钥更新。EEP在传输时封装在WAI2协议中。EEP的详细规定见T/WAPIA 045.1—2021第8章。

14 T/WAPIA 046—2021 附录 B.4.3 第 7.3 节管理帧帧体组成部分相关修改中 7.3.2.8.2 替换为：

7.3.2.8.2 密码套件

密码套件选择格式见图41f。

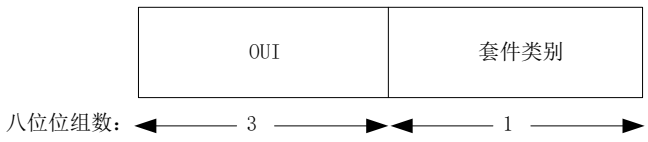


图41f 套件选择格式

表19b提供本文件定义的密码套件。

表 19b 密码套件

OUI	类型 1八位位组	含义
00-14-72	0	保留
00-14-72	1	WPI-SM4-OFB+CMAC-128
00-14-72	2	WPI-SM4-GCM-128
00-14-72	3	WPI-SM4-CMAC-128
00-14-72	4	WPI-SM4-GMAC-128
00-14-72	5	WPI-SMX-GCM-256
00-14-72	6～255	保留
其他	0～255	保留

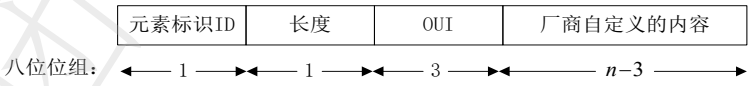
当选择的鉴别和密钥管理套件为1或2时，默认选择的单播密码套件为00-14-72:1（WPI-SM4-OFB+CMAC-128），当支持的鉴别和密钥管理套件为3、4、5、6时，默认选择的单播密码套件为00-14-72:2（WPI-SM4-GCM-128）。00-14-72:5（WPI-SMX-GCM-256）预留定义更高安全强度的密码套件。当支持的鉴别和密钥管理套件为1、2时，默认选择的组播密码套件为00-14-72:1（WPI-SM4-OFB+CMAC-128），组管理密码套件为00-14-72:3（WPI-SM4-CMAC-128）；当支持的鉴别和密钥管理套件为3、4、5、6时，默认选择的组播密码套件为00-14-72:2（WPI-SM4-GCM-128），组管理密码套件为00-14-72:4（WPI-SM4-GMAC-128）。

15 在T/WAPIA 046—2021 附录B 7.3.2.9内容替换为：

7.3.2.9 厂商自定义IE

7.3.2.9.1 WAPI能力IE

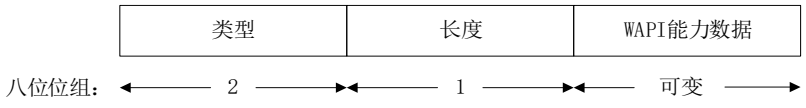
厂商自定义IE包含扩展IE信息，采用专用的IE号来标识。厂商自定义IE格式见0，信息字段中的前3个八位位组包含厂商特定的OUI。该IE的信息字段长度为n个八位位组，$3 \le n \le 255$。OUI字段是ISO授权组织分配的公开值，占3个八位位组。厂商自定义的内容字段长度为$n-3$个八位位组。



图B.12 厂商自定义的IE格式

一个帧体中可包含多个厂商自定义的IE。每个厂商自定义的IE可包含不同的OUI值。一个帧体可包含的厂商自定义的IE的个数只受帧体大小的限制。

OUI值为00-14-72，表示该厂商自定义IE为为WAPI能力IE。WAPI能力IE中厂商自定义内容包含2个八位位组的类型字段、1个八位位组的长度字段以及可变长度的能力数据字段，子IE字段格式见0。



图B.13 WAPI能力信息字段格式

——类型字段标识WAPI能力IE类型。

2 表示 MMIE；

3 表示 WAPIFTIE；

4 表示 WAPI 密钥数据 IE；

其他值保留。

——长度字段规定了能力数据字段中的八位位组数。

——能力数据为 WAPI 能力 IE 的能力数据信息。

在一个IE(ID=221,OUI=00-14-72)中,可包含多个不同的类型值的WAPI能力IE字段,标识多种WAPI能力IE类型。一个帧体中可包含多个IE，且多个IE的ID=221，OUI=00-14-72。

7.3.2.9.2 MMIE

MMIE提供消息完整性保护和防止组播管理帧被篡改和重放。0为MMIE格式，MMIE封装到厂商自定义IE中。MMIE应在所有帧体数据的最后，在FCS之前。

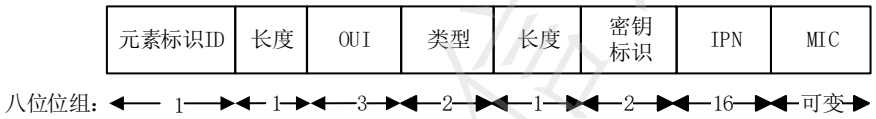


图 B.14 MMIE 格式

类型字段为2(十进制数)。

长度字段标识MMIE中除类型和长度字段以外其他所有字段的八位位组数。

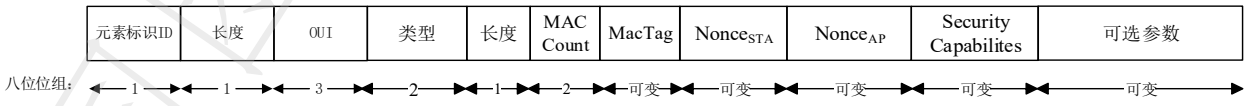
密钥标识字段KeyIdx标识用于计算MIC的组播完整性校验密钥。

IPN字段，长度为16个八位位组，表示一个整数，用于标识分组序号，该分组序号作为计算MIC字段的IV值。IPN按小数结尾编码发送。

MIC字段是利用组播完整性校验密钥采用组管理密码套件对管理协议数据单元计算得到的消息鉴别码，当采用WPI-SM4-CMAC-128和WPI-SM4-GMAC-128套件时，MIC字段长度为16。

7.3.2.9.3 WAPIFTIE

WAPIFTIE包含了快速切换时执行快速鉴别时所需要的信息，WAPIFTIE格式见0。



图B.15 WAPIFTIE格式

类型字段为3（十进制数）。

长度字段标识本IE能力数据的八位位组数。

MAC Count字段定义见0。

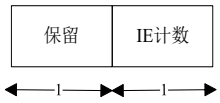


图 B.16 MAC Count 信息格式

保留字段长度为一个八位位组。

IE计数字段长度为一个八位位组，标识在计算MacTag时所包含的IE个数，取值0表示没有MacTag信息。

图 41j 中 MacTag、$Nonce_{REQ}$、$Nonce_{AP}$ 和 SecturityCapabilites 字段定义应符合 T/WAPIA 045.2—2021 中 6.2。$Nonce_{AP}$ 的定义与 $Nonce_{AAC}$ 一致。

可选参数子字段格式见0。

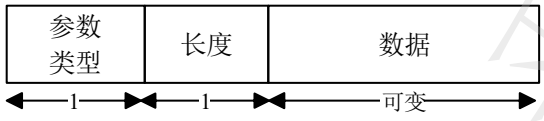


图 B.17 可选参数子字段格式

可选参数子字段类型格式见表B.1。

表B.18 可选参数子字段类型格式

参数类型值	数据字段内容	备注
0	保留	
1	ID_{STA}	（ID_{STA} 定义同 ID_{REQ}）
2	ID_{InitAP}	（ID_{InitAP} 定义同 ID_{AAC}）
3	ID_{newAP}	（ID_{newAP} 定义同 ID_{AAC}）
4	$KEYname_{STA}$	（$KEYname_{STA}$ 定义同 $KEYname_{REQ}$）
5	$EncData_{AP}$(NMK，$Nonce_{SN}$)	（$EncData_{AP}$ 定义同 $EncData_{AAC}$）
6～255	保留	

7.3.2.9.4 WAPI 密钥数据 IE 字段

7.3.2.9.4.1 WAPI 密钥数据 IE 封装

WAPI密钥数据IE采用厂商自定义IE封装，包含了密钥建立时所需要的信息，WAPI密钥数据IE格式见0。

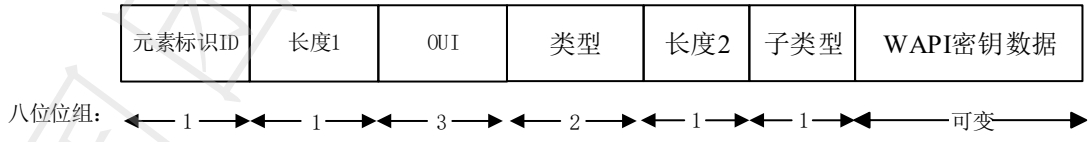


图 B.18 密钥数据 IE 格式

其中：

——元素标识 ID 字段值为 221，标识厂商自定义 IE；

——长度 1 字段本 IE 中除元素标识 ID 和长度以外其他字段的八位位组数；

——OUI 值为 00-14-72；

——类型字段标识 IE 类型。

4 表示该 IE 为 WAPI 密钥数据 IE；

——长度 2 字段标识标识子类型和 WAPI 密钥数据字段的八位位组数；

——子类型用于标识 WAPI 密钥数据类型，子类型对应的密钥数据内容见 0；

表 B.19 WAPI 密钥数据内容

子类型	WAPI 密钥数据内容
0	保留
1	WAPI-MSK 密钥数据
2	WAPI-IMK 密钥数据
3	WAPI-BIMK 密钥数据
4～10	保留
11	WAPI-MAC 地址密钥数据
12	WAPI-Key ID 密钥数据
13	MLO WAPI-MSK 密钥数据
14	MLO WAPI-IMK 密钥数据
15	MLO WAPI 链路信息密钥数据
16	MLO WAPI-BIMK 密钥数据
17～255	保留

——WAPI 密钥数据为子类型标识的密钥数据信息。

7.3.2.9.4.2 WAPI-MSK 密钥数据；

WAPI-MSK密钥数据格式见0。

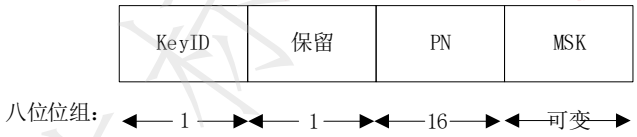


图 B.19 WAPI-MSK 密钥数据格式

其中：

——KeyID 字段长度为 1 个八位位组，其中位 0 标识当前通告的密钥标识，其他位保留（设置为 0）。本字段中位 0 初始值为 0，每次更新通告密钥时，该位在 0 和 1 之间翻转；

——保留字段长度为 1 个八位位组，默认值为 0；

——PN 字段长度为 2 个八位位组，表示一个整数，用于标识已经使用当前通告的密钥加密发送的数据分组序号（WPI 组播数据分组中的 PN），之后 STA 收到的数据帧序号应大于本字段值，否则丢弃 MSK；

——MSK 字段为通告的组播会话密钥。

7.3.2.9.4.3 WAPI-IMK 密钥数据

WAPI-IMK密钥数据格式见**错误!未找到引用源。**。

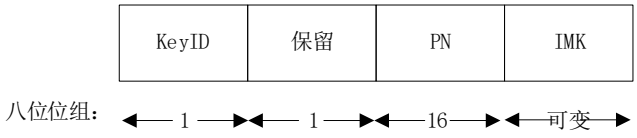


图 B.22 WAPI-IMK 密钥数据格式

其中：

——KeyID 字段长度为 1 个八位位组，其中位 0 标识当前通告的密钥标识，其他位保留（设置为 0）。本字段中位 0 初始值为 0，每次更新通告密钥时，该位在 0 和 1 之间翻转；
——保留字段，长度为 1 个八位位组；
——PN 字段长度为 2 个八位位组，表示一个整数，用于标识已经使用当前通告的密钥保护发送的数据分组序号，之后 STA 收到的帧序号应大于本字段值，否则丢弃；
——IMK 为通告的完整性组播密钥。

7.3.2.9.4.4 WAPI-BIMK 密钥数据

WAPI-IMK密钥数据格式见**错误!未找到引用源。**。

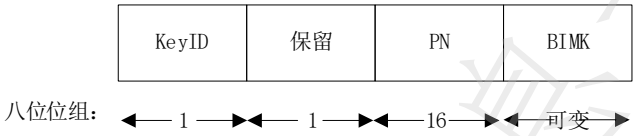


图 B.22 WAPI-IMK 密钥数据格式

其中：
——KeyID 字段长度为 1 个八位位组，其中位 0 标识当前通告的密钥标识，其他位保留（设置为 0）。本字段中位 0 初始值为 0，每次更新通告密钥时，该位在 0 和 1 之间翻转；
——保留字段，长度为 1 个八位位组；
——PN 字段长度为 2 个八位位组，表示一个整数，用于标识已经使用当前通告的密钥保护发送的数据分组序号，之后 STA 收到的帧序号应大于本字段值，否则丢弃；
——BIMK 为通告的信标帧完整性组播密钥。

7.3.2.9.4.5 WAPI-MAC 地址密钥数据

WAPI-MAC地址密钥数据格式见0。

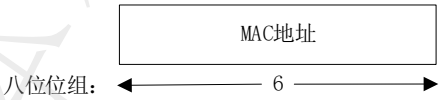


图 B.20 WAPI-MAC 地址密钥数据格式

其中MAC地址，长度为6个八位位组。

7.3.2.9.4.6 WAPI-KeyID 密钥数据

WAPI-KeyID密钥数据格式见0。

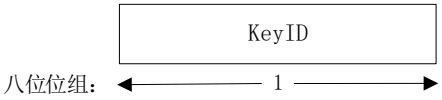


图 B.21 WAPI-KeyID 密钥数据格式

其中KeyID，长度为1个八位位组,其中位0标识当前通告的密钥，初始值为0，每次更新通告密钥时，该位在0和1之间翻转，其他位保留（设置为0）。

7.3.2.9.4.7 MLO WAPI-MSK 密钥数据

MLO WAPI-MSK密钥数据格式见0。

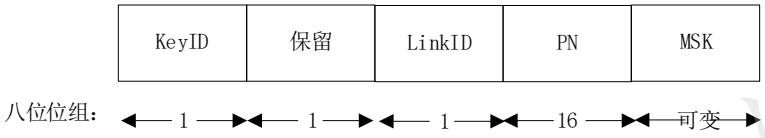


图 B.23 MLO WAPI-MSK 密钥数据格式

其中：

——KeyID 字段长度为 1 个八位位组，其中位 0 标识当前通告的密钥标识，其他位保留（设置为 0）。本字段中位 0 初始值为 0，每次更新通告密钥时，该位在 0 和 1 之间翻转；

——保留字段，长度为 1 个八位位组；

——LinkID，长度为 1 个八位位组，其中位 0 到位 3 用于标识通告 MSK 的链路；

——PN 字段长度为 2 个八位位组，表示一个整数，用于标识已经使用当前通告的密钥加密发送的数据分组序号（WPI 组播数据分组中的 PN），之后 STA 收到的数据帧序号应大于本字段值，否则丢弃；

——MSK 为通告的组播会话密钥。

7.3.2.9.4.8 MLO WAPI-IMK 密钥数据

MLO WAPI-IMK密钥数据格式见0。

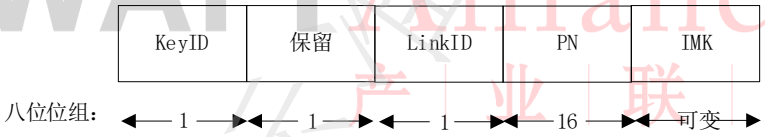


图 B.24 MLO WAPI-IMK 密钥数据格式

其中：

——KeyID 字段长度为 1 个八位位组，其中位 0 标识当前通告的密钥标识，其他位保留（设置为 0）。本字段中位 0 初始值为 0，每次更新通告密钥时，该位在 0 和 1 之间翻转；

——保留字段，长度为 1 个八位位组；

——LinkID，长度为 1 个八位位组，其中位 0 到位 3 用于标识通告 IMK 的链路；

——PN 字段长度为 2 个八位位组，表示一个整数，用于标识已经使用当前通告的密钥保护发送的分组序号，之后 STA 收到的帧序号应大于本字段值，否则丢弃；

——IMK 为通告的完整性组播密钥。

7.3.2.9.4.9 MLO WAPI 链路信息密钥数据

MLO WAPI链路信息密钥数据格式见0。

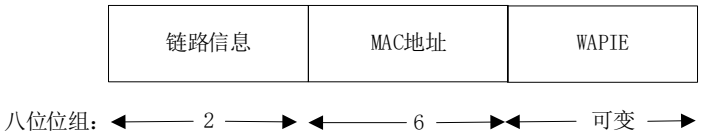


图 B.25 MLO WAPI 链路信息密钥数据格式

其中：

——链路信息字段包含 MLO WAPI 链路信息字段中子字段是否存在，格式见 0；

——MAC 地址字段包含链路信息字段指定的链路对应附属 STA 的 MAC 地址；

——WAPIE 字段包含链路信息字段指定的链路对应附属 STA 的 WAPIE。

图 B.26 链路信息格式

其中：

——LinkID，长度为 1 个八位位组，其中位 0 到位 3 用于标识附属链路信息，其他位保留；

——WAPIE 标识用于表示 WAPIE 字段是否存在，当值为 1 时表示 MLO WAPI 链路信息密钥数据信息包含 WAPIE 字段，值为 0 时标识不包含 WAPIE 字段；

——保留字段，长度为 7 位。

7.3.2.9.4.10 MLO WAPI-BIMK 密钥数据

MLO WAPI-IMK密钥数据格式见0。

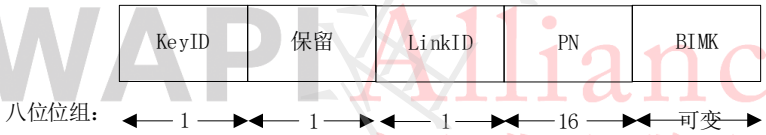


图 B.24 MLO WAPI-IMK 密钥数据格式

其中：

——KeyID 字段长度为 1 个八位位组，其中位 0 标识当前通告的密钥标识，其他位保留（设置为 0）。本字段中位 0 初始值为 0，每次更新通告密钥时，该位在 0 和 1 之间翻转；

——保留字段，长度为 1 个八位位组；

——LinkID，长度为 1 个八位位组，其中位 0 到位 3 用于标识通告 BIMK 的链路；

——PN 字段长度为 2 个八位位组，表示一个整数，用于标识已经使用当前通告的密钥保护发送的分组序号，之后 STA 收到的帧序号应大于本字段值，否则丢弃；

——BIMK 为通告的信标帧完整性组播密钥。