ICS 35.030
CCS L 80

团　　体　　标　　准

T/ZSA 218-2024

无线局域网密码应用基本要求

Basic requirements for wireless local area network

cryptography application

2024-02-02 发布　　2024-02-03 实施

中关村标准化协会　　发布

目　　次

前　言

本文件按照 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》的规则起草。

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。

本文件由中关村标准化协会技术委员会提出并归口。

本文件起草单位：中关村无线网络安全产业联盟、北京联盛德微电子有限责任公司、北京三凯威科技有限公司、北京数字认证股份有限公司、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、中国电力科学研究院有限公司、广西电网电力调度控制中心、华为技术有限公司、陕西省网络与信息安全测评中心、北京紫光展锐科技有限公司、西安芯语慧联信息科技有限公司、广西通量能源技术有限公司、北京兴汉网际股份有限公司、工业和信息化部宽带无线 IP 标准工作组。

本文件主要起草人：潘琪、王立华、张璐璐、侯鹏亮、简练、黄振海、张国强、张变玲、刘婷、刘剑昕、李庆、李锐、匡俊华、郑亚杰、童伟刚、范小伟、李琴、颜湘、杜志强、林凡、肖龙、米东、郑骊、周涛、周园、张志海、林和昀、阳佑敏、马卓元、曹永峰、胡霄亮、季晨荷、周晓萌、李丛蓉、韦利娜、贺燚。

引　言

GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》适用于指导、规范信息系统密码应用的规划、建设、运行及测评，并提出了各领域与行业可结合该领域与行业的密码应用需求来指导、规范信息系统密码应用的原则。本文件在上述原则基础上，充分研究分析密码应用规范性要素，结合信息系统建设机构、运营机构对无线局域网（WLAN）的密码应用需求，以及WLAN产品开发商、生产商、技术研究机构等的密码应用能力，从技术要求和管理要求的多个层面，规定了信息系统中WLAN密码应用的基本要求。

本文件可为应用了WLAN网络的信息系统的建设机构、运营机构进行WLAN网络的建设运营，为WLAN产品开发商依法进行WLAN产品的设计研发提供准确、完整的指导，确保相关产品密码应用环节的合规性、一致性和互通性，为信息系统提供安全保障。

无线局域网密码应用基本要求

1 范围

本文件规定了信息系统中无线局域网（WLAN）密码应用的通则、第一级密码应用要求、第二级密码应用要求、第三级密码应用要求和第四级密码应用要求。

本文件适用于应用了WLAN网络的信息系统的规划、建设、运行及测评。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 15629.11（所有部分） 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范

GB/T 37092—2018 信息安全技术 密码模块安全要求

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

T/WAPIA 046 无线局域网安全技术规范

T/WAPIA 038 信息安全技术 终端实体证书管理

3 术语和定义

GB/T 39786—2021界定的以及下列术语和定义适用于本文件。

3.1

密码模块 cryptography module

实现密码运算功能，相对独立的软件、硬件、固件或这三者组合。

[来源：GB/T 25069—2022，3.379]

3.2

设备密钥 device key pair

存储在设备内部的用于设备管理的非对称密钥对，包含签名密钥对和加密密钥对。

[来源：GB/T 36322—2018，3.4]

3.3

WAPI标准体系 WAPI standard system

规范、引用和采用WAPI的国家标准、行业标准、团体标准及国际标准等的集合。

3.4

无线局域网鉴别基础结构 WLAN authentication infrastructure

用于无线局域网接入控制的身份鉴别和密钥管理安全方案。

[来源：T/WAPIA 046—2021，3.21]

3.5

无线局域网鉴别与保密基础结构 WLAN authentication and privacy infrastructure

由无线局域网鉴别基础结构（WAI）和无线局域网保密基础结构（WPI）组成，为无线局域网接入点、终端提供对等身份鉴别和数据机密性服务。

[来源：T/WAPIA 046—2021，3.22]

3.6

无线局域网保密基础结构 WLAN privacy infrastructure

用于无线局域网中数据传输保护的安全方案，包括数据加密、数据鉴别和重放保护等功能。

[来源：T/WAPIA 046—2021，3.27]

3.7

WAPI标准体系　WAPI standard system

规范、引用和采用WAPI的国家标准、行业标准、团体标准及国际标准等的集合。

4　缩略语

下列缩略语适用于本文件。

AC：接入点控制器（AP Controller）

AP：无线接入点（Access Point）

AS：鉴别服务器（Authentication Server）

CIS：证书签发服务器（Certificate Issue Server）

PDU：协议数据单元（Protocol Data Unit）

STA：站（点）（Station）

WAI：无线局域网鉴别基础结构（WLAN Authentication Infrastructure）

WAPI：无线局域网鉴别与保密基础结构（WLAN Authentication and Privacy Infrastructure）

WLAN：无线局域网（Wireless Local Area Network）

WPI：无线局域网保密基础结构（WLAN Privacy Infrastructure）

5　通则

5.1　信息系统无线局域网

GB/T 39786—2021中将信息系统密码应用要求划分为若干安全层面，每个安全层面对应的信息系统要素和组成见图1。

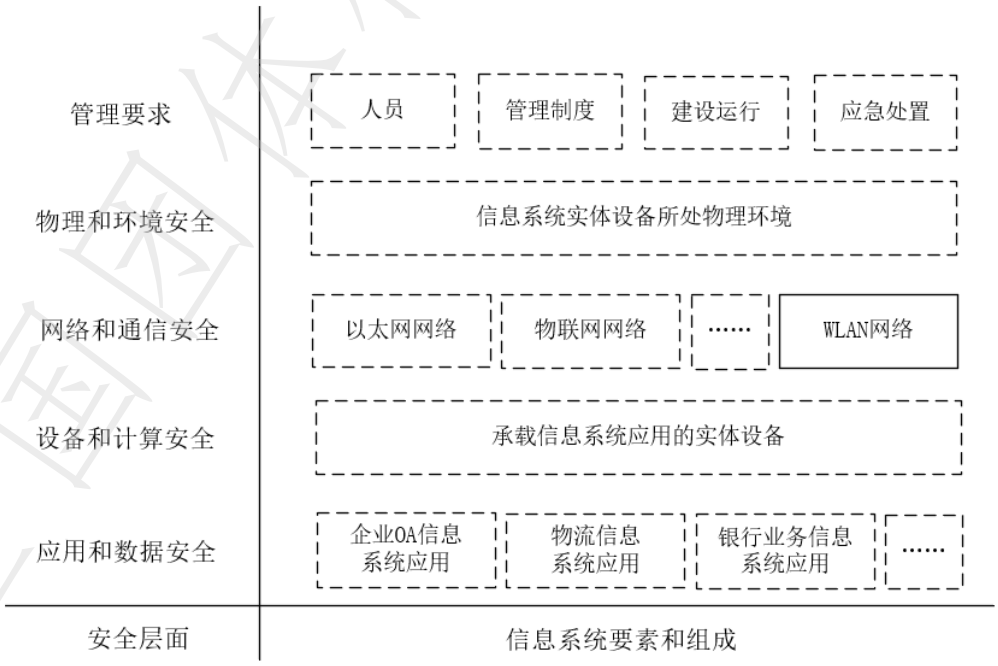

图 1 信息系统要素和组成图

本文件是针对信息系统网络和通信安全层面中的WLAN网络提出的密码应用技术要求，对于涉及WLAN网络的其它安全层面要求，应符合GB/T 39786—2021中对应安全层面的要求，建设运行层面中的无线局域网密钥生存周期管理见附录A。

5.2 无线局域网网络通信要素

信息系统无线局域网网络通信要素包括三个方面：网络通信主体、网络通信信道，和其它提供安全保护功能的设备和服务。WLAN网络通信要素示意见图2。

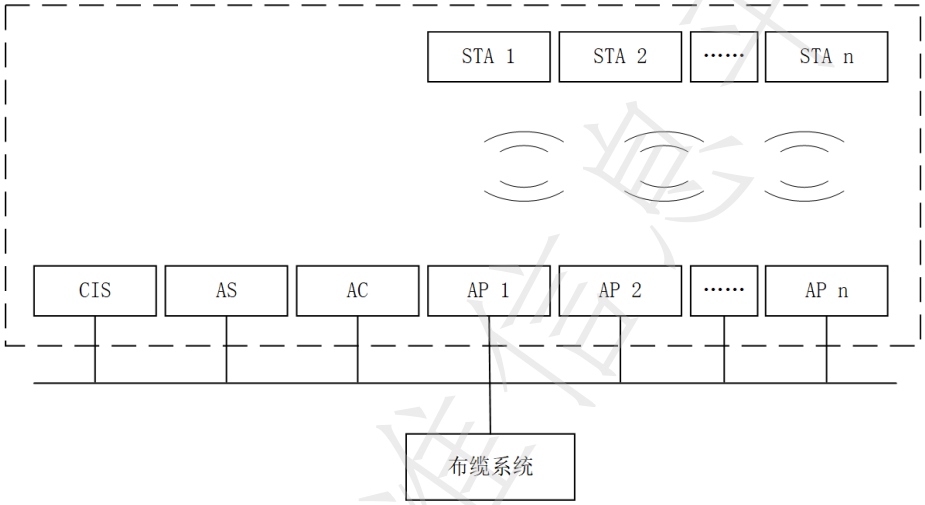

图 2 WLAN 网络通信要素示意

a) 网络通信主体

1) 独立的无线局域网设备，如 STA、AP；

2) 集成或内置了无线局域网模块的设备，如智能移动通信终端、平板式计算机、智能家电等。

注：本文件中以 STA、AP 表示网络通信主体。

b) 网络通信信道

在 WLAN 通信主体之间实现安全传输 PDU 的媒体。

c) 其它提供安全保护功能的设备和服务

包括无线局域网特有的网络设备，如 AS、CIS、AC，以及提供无线局域网密码服务的密码产品，例如密码模块等。此类设备和服务不具备独立完成无线局域网功能的能力，但能够协同网络通信主体完成无线局域网功能，并协同提供安全保护能力。

5.3 等级划分和通用要求

5.3.1 等级划分

GB 15629.11（所有部分）和T/WAPIA 046中规定了无线局域网的安全机制，包括WAI鉴别和密钥管理、WPI数据保密等，这些安全机制使用相应的密码技术，从机密性、完整性、真实性、不可否认性四个密码安全功能维度来保护具体的应用对象。

依据不同的安全机制和密码技术，信息系统无线局域网密码应用划分为自低向高的四个等级，用一、二、三、四表示，该等级与GB/T 39786—2021中的等级对应关系如下：

a) 若信息系统符合 GB/T 39786—2021 中规定的第一级密码应用基本要求，则其 WLAN 部分应符合本文件中规定的第一级密码应用基本要求；

b) 若信息系统符合 GB/T 39786—2021 中规定的第二级密码应用基本要求，则其 WLAN 部分应符合本文件中规定的第二级密码应用基本要求；

c） 若信息系统符合 GB/T 39786—2021 中规定的第三级密码应用基本要求，则其 WLAN 部分应符合本文件中规定的第三级密码应用基本要求；
d） 若信息系统符合 GB/T 39786—2021 中规定的第四级密码应用基本要求，则其 WLAN 部分应符合本文件中规定的第四级密码应用基本要求。

5.3.2 通用要求

第一级到第四级的无线局域网密码应用应符合GB/T 39786—2021第5章中规定的要求和以下要求：
a） WLAN 网络通信主体，以及使用的安全机制和密码技术应符合 WAPI 标准体系的要求；
b） WLAN 中使用的提供安全保护功能的设备，应符合 WAPI 标准体系的要求和相关国家标准、行业标准、团体标准的要求；
c） WLAN 中使用的密码服务，应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。

6 第一级密码应用基本要求

第一级密码应用基本要求包括：
a） 应采用密码技术对STA和AP进行身份鉴别。该密码技术应采用国家密码管理部门批准的密码算法，应采用GB 15629.11（所有部分）或T/WAPIA 046中规定的无线局域网鉴别机制；
b） 应采用密码技术保证STA与AP间通信过程中数据的完整性和机密性。该密码技术应采用国家密码管理部门批准的密码算法，应采用GB 15629.11（所有部分）或T/WAPIA 046中规定的WPI数据保密机制。

注：无线局域网鉴别机制见附录B。

7 第二级密码应用基本要求

第二级密码应用基本要求包括：
a） 应采用密码技术对STA和AP进行身份鉴别。该密码技术应采用国家密码管理部门批准的密码算法，应采用GB 15629.11（所有部分）或T/WAPIA 046中规定的无线局域网鉴别机制；
b） 应采用密码技术保证STA与AP间通信过程中数据的完整性和机密性。该密码技术应采用国家密码管理部门批准的密码算法，应采用GB 15629.11（所有部分）或T/WAPIA 046中规定的WPI数据保密机制；
c） 以上如采用密码产品，该密码产品应达到GB/T 37092—2018中规定的一级或一级以上安全要求。

8 第三级密码应用基本要求

第三级密码应用基本要求包括：
a） 应采用密码技术对STA和AP进行身份鉴别。该密码技术应采用国家密码管理部门批准的密码算法，应采用GB 15629.11（所有部分）或T/WAPIA 046标中规定的基于证书的无线局域网鉴别机制，并且采用AS提供的鉴别服务；
b） 应采用密码技术保证STA与AP间通信过程中数据的完整性和机密性。该密码技术应采用国家密码管理部门批准的密码算法，应采用GB 15629.11（所有部分）或T/WAPIA 046中规定的WPI数据保密机制；
c） 宜采用密码技术保证AP与AC间通信过程中的数据的完整性；
d） 宜采用密码技术对STA、AP通信实体证书的分发过程进行保护，保证证书的安全传输和安全管理；

e） 以上如采用密码产品，该密码产品应达到GB/T 37092—2018中规定的二级或二级以上安全要求。

9 第四级密码应用基本要求

第四级密码应用基本要求包括：

a） 应采用密码技术对STA和AP进行身份鉴别。该密码技术应采用国家密码管理部门批准的密码算法，应采用T/WAPIA 046中规定的增强证书鉴别机制，并且采用AS提供的鉴别服务；

b） 应采用密码技术保证STA与AP间通信过程中数据的完整性和机密性。该密码技术应采用国家密码管理部门批准的密码算法，应采用T/WAPIA 046中规定的WPI数据保密机制；

c） 宜采用密码技术保证AP与AC间通信过程中的数据的完整性；

d） 宜采用 T/WAPIA 038 中规定的协议和密码技术对 STA、AP 通信实体证书的分发过程进行保护，保证证书的安全传输和安全管理；

e） 宜采用密码技术（例如 GM/T 0014—2012 中 5.3～5.6 规定的相关协议）保证 AS 与 CIS 间通信过程中的数据的完整性和机密性；

f） 宜采用 T/WAPIA 046 中规定的带有身份保护功能的身份鉴别协议，保证 STA、AP 通信实体身份隐私信息不被泄露；

g） 以上如采用密码产品，该密码产品应达到 GB/T 37092—2018 中规定的三级或三级以上安全要求。

附 录 A
（资料性）
无线局域网密钥生存周期管理

A.1 设备密钥

本文件中设备密钥指WLAN设备在GB 15629.11（所有部分）或T/WAPIA 046中规定的基于证书的鉴别机制场景下，进行WAPI安全鉴别所使用的密钥。需要进行密钥管理的WLAN设备包括网络通信主体设备（如STA、AP），以及其它提供安全保护功能的部分设备（如AS、CIS）。

信息系统中WLAN密码应用的密钥体系由业务系统根据密码应用需求在密码应用方案中明确，并在密码应用实施中落实，并对WLAN设备密钥的全生命周期进行管理，保证私钥不被非授权的访问、使用、泄露、修改和替换，保证公钥不被非授权的修改和替换。WLAN设备密钥管理包括密钥的产生、存储、分发、导入与导出、使用、备份与恢复、归档、销毁等环节。

a） 密钥产生

WLAN设备密钥在符合GB/T 37092—2018中规定的密码模块内部产生是十分必要的。

b） 密钥存储

WLAN设备私钥不以明文方式存储在密码模块外；WLAN设备公钥可以以数字证书的形式在密码模块外存储。

c） 密钥分发

WLAN设备私钥不进行分发；WLAN设备公钥可以以数字证书的形式分发。

d） 密钥导入与导出

WLAN设备私钥不进行导入与导出；WLAN设备公钥可以以数字证书的形式导入与导出。

e） 密钥使用

WLAN设备密钥明确用途后按用途正确使用；在使用WLAN设备公钥前对其进行验证。

f） 密钥备份与恢复

WLAN设备密钥如果有密码备份和恢复需求，有必要制定明确的密钥备份恢复策略，利用密码模块的密钥备份恢复机制对密钥进行备份或恢复；密钥的备份与恢复有必要生成审计信息，审计信息包括备份或恢复的主体、备份或恢复的时间等。

g） 密钥归档

WLAN设备密钥如果有归档需求，有必要采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息。密钥的归档有必要生成审计信息，审计信息包括归档的密钥、归档的时间等。

h） 密钥销毁

对于CIS等密钥颁发设备，具有在紧急情况下销毁密钥的措施是十分必要的。

A.2 其他密钥

信息系统WLAN其他密钥（非设备密钥）的密钥生存周期管理要求见GB/T 39786—2021附录B。

附 录 B
（资料性）
无线局域网鉴别机制

GB 15629.11（所有部分）和T/WAPIA 046中规定了四种WLAN鉴别机制，包括：

a） WAI预共享密钥鉴别和密钥管理；

b） WAI增强预共享密钥鉴别和密钥管理；

c） WAI证书鉴别和密钥管理；

d） WAI增强证书鉴别和密钥管理。

其中a）和b）为基于预共享密钥的鉴别机制，c）和d）为基于证书的鉴别机制。

参 考 文 献

[1] GB/T 25069—2022 信息安全技术 术语
[2] GB/T 36322—2018 信息安全技术 密码设备应用接口规范
[3] GM/T 0014—2012 数字证书认证系统密码协议规范
[4] T/WAPIA 038—2019 信息安全技术 终端实体证书管理