



电力可信 WAPI 系统

产品说明书

2023

使用本产品前请仔细阅读本说明书

目录

1、 电力可信 WAPI 简介	2
2、 WAPI 系统基本概念	2
3、 WAPI 的工作过程	3
4、 WAPI 系统典型组网	4
5、 WAPI 证书鉴别方式	4
6、 WAPI 预共享密钥鉴别方式	5
7、 WAPI 的密钥管理	5
8、 联系方式	6
9、 免责声明	6
10、 更新历史	7

1、电力可信 WAPI 简介

WAPI 是 WLAN Authentication and Privacy Infrastructure（无线局域网鉴别与保密基础结构）的简称，是中国提出的、以 802.11 无线协议为基础的无线安全标准。

WAPI 协议由以下两部分构成：

（1）**WAI**：是 WLAN Authentication Infrastructure（无线局域网鉴别基础结构）的简称，是用于无线局域网中身份鉴别和密钥管理的安全方案；

（2）**WPI**：是 WLAN Privacy Infrastructure（无线局域网保密基础结构）的简称，是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。

2、WAPI 系统基本概念

（1）**AC（Access Controller，接入控制器）**：用于对 WLAN 中与之关联的 FIT AP 进行控制和管理的设备。

（2）**AP（Access Point，接入点）**：是指任何一个能通过无线介质为无线终端提供分布式访问服务的实体。

（3）**AS（Authentication Server，鉴别服务器）**：用于对用户和设备证书进行身份鉴别等，是基于公钥密码技术的 WAI 中重要的组成部分。

（4）**BK（Base Key，基密钥）**：用于导出单播会话密钥，由证书鉴别过程协商得到或者由预共享密钥导出。

（5）**FAT AP（FAT Access Point，胖 AP）**：传统 AP，除了提供基本的无线连接功能外，还能提供安全、管理和性能增强功能。FAT AP 不能与 AC 关联使用。

（5）**FIT AP（FIT Access Point，瘦 AP）**：区别于传统的 FAT AP，只提供可

靠、高性能的无线连接功能，而剥离了其它功能。FIT AP 必须与 AC 关联使用，本文中的 AP 均指 FIT AP。

(6) **MSK (Multicast Session Key, 组播会话密钥)**: 用于保护站点发送的组播 MPDU 的随机值，由组播主密钥导出，包括组播加密密钥和组播完整性校验密钥。

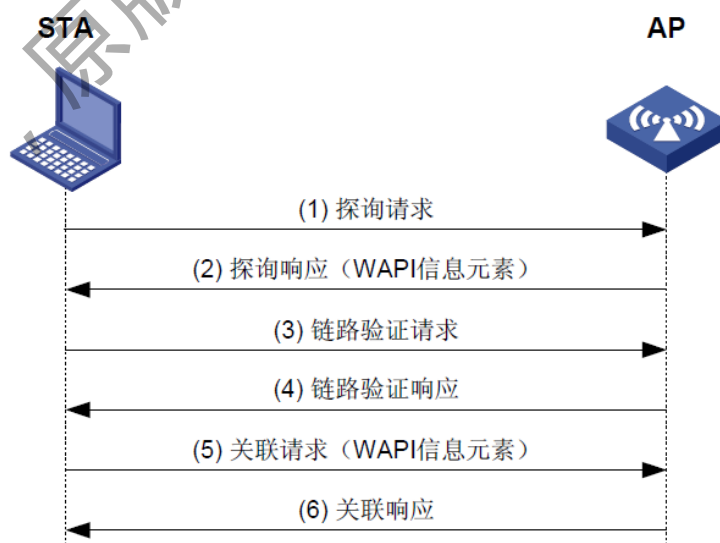
(7) **PSK (Preshared Key, 预共享密钥)**: 是发布给 STA 的静态密钥。

(8) **STA (Station, 站点)**: 即无线终端，本文中是指带有支持 WAPI 协议无线网卡的 PC、便携式笔记本电脑等无线终端。

(9) **USK (Unicast Session Key, 单播会话密钥)**: 是由 BK 通过伪随机函数导出的随机值，分为四个部分：单播加密密钥、单播完整性校验密钥、消息鉴别密钥和密钥加密密钥。

(10) **WAPI user (WAPI 用户)**: 是指使用 WAPI 安全模式进行认证的用户，系统所支持的最大 WAPI 用户数量为 1024 个。本文中也称为 STA。

3、WAPI 的工作过程



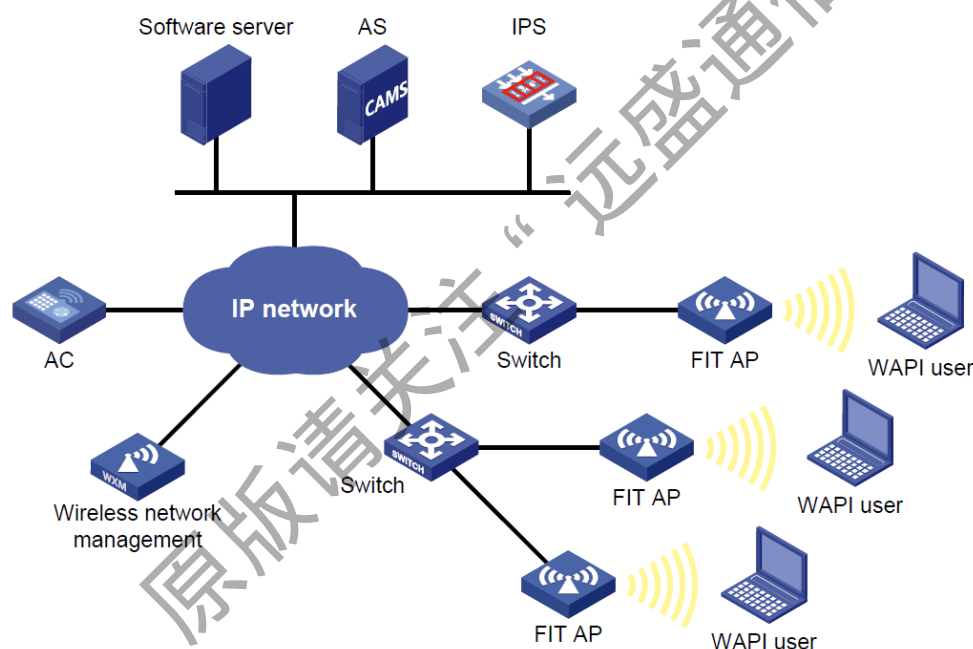
在一个采用了 WAPI 安全关联机制的 WLAN 中，当 STA 需要访问该 WLAN

时，通过被动侦听 AP 的信标（Beacon）帧或主动发送探测帧（主动探测）以识别 AP 所采用的安全策略：

（1）若 AP 采用证书鉴别方式，AP 将发送鉴别激活分组启动证书鉴别过程，当证书鉴别过程成功结束后，AP 和 STA 再进行单播密钥协商和组播密钥通告；

（2）若 AP 采用预共享密钥鉴别方式，AP 将与 STA 直接进行单播密钥协商和组播密钥通告。

4、WAPI 系统典型组网



在一个典型的 WAPI 系统中，WAPI 用户通过 AP 接入有线 IP 网络。首先，WAPI 用户与 AP 进行 802.11 链路协商，之后 AP 为该用户触发 WAI 鉴别过程，配合 AS 完成与用户的双向认证。当认证通过后，AP 会发起对该用户的密钥协商，并使用协商出的密钥通过 WPI 向该 WAPI 用户提供加、解密服务。

5、WAPI 证书鉴别方式

数字证书是一种经 PKI（Public Key Infrastructure，公钥基础设施）证书授权

中心签名的、包含公开密钥及用户相关信息的文件，是网络用户的数字身份凭证。WAPI 系统中所使用的用户证书为数字证书，通过 AS 对用户证书进行验证，可以唯一确定 WAPI 用户的身份及其合法性。

证书鉴别是基于 STA 和 AP 双方的证书所进行的鉴别。鉴别前 STA 和 AP 必须预先拥有各自的证书，然后通过 AS 对双方的身份进行鉴别，根据双方产生的临时公钥和临时私钥生成 BK，并为随后的单播密钥协商和组播密钥通告做好准备。

6、WAPI 预共享密钥鉴别方式

预共享密钥鉴别是基于 STA 和 AP 双方的密钥所进行的鉴别。鉴别前 STA 和 AP 必须预先配置有相同的密钥，即预共享密钥。鉴别时直接将预共享密钥转换为 BK，然后进行单播密钥协商和组播密钥通告。

7、WAPI 的密钥管理

STA 与 AP 之间交互的单播数据利用单播密钥协商过程所协商出的单播加密密钥和单播完整性校验密钥进行保护；AP 利用自己通告的、由组播主密钥导出的组播加密密钥和组播完整性校验密钥对其发送的广播/组播数据进行保护，而 STA 则采用 AP 通告的、由组播主密钥导出的组播加密密钥和组播完整性校验密钥对收到的广播/组播数据进行解密。

8、联系方式

公司名称：山东远盛通信科技有限公司

公司地址：山东省济南市历城区银丰新能源产业园 1 号楼 17 层

售前咨询：13864080101

售后电话：0531-59723816

网址：www.sdyuansheng.cn

9、免责声明

本文档提供有关 电力可信 WAPI 系统 系列产品的信息，本文档未授予任何知识产权的许可，并未以明示或暗示，或以禁止发言或其它方式授予任何知识产权许可。除在其产品的销售条款和条件声明的责任之外，我公司概不承担任何其它责任。

我公司对本产品的销售和/或使用不作任何明示或暗示的担保，包括对产品的特定用途适用性，适销性或对任何专利权，版权或其它知识产权的侵权责任等均不作担保。本公司可能随时对产品规格及产品描述做出修改，恕不另行通知。

相关配置软件可进入我公司官网进行下载，或关注企业公众号“远盛通信”进行资料下载。



10、更新历史

版本号	修订内容	修订时间
V1.0	初始版本	2023 年 3 月

声明

本手册所描述的内容可能与您现使用的版本有区别，如果您按照本手册使用时遇到有无法解决的问题，请与本公司技术支持部或产品供应商联系。本手册内容将不定期更新，公司有保留不另行通知的权利。