宽带无线 IP 标准工作组标准化指导性技术文件

《WAPI 私钥/证书本地存储及使用技术规范》

编　制　说　明

（第二次征求意见稿）

2010 年 **12** 月

一、任务来源

根据工业和信息化部宽带无线 IP 标准工作组 2009 年制修订标准项目计划，由工业和信息化部宽带无线 IP 标准工作组和 WAPI 产业联盟共同负责起草，工业和信息化部宽带无线 IP 标准工作组归口，其项目计划代号为 2010013-Z-CBWIPS。

二、起草单位

起草单位：工业和信息化部宽带无线 IP 标准工作组“WAPI 私钥/证书本地存储及使用技术标准项目组”、WAPI 产业联盟“WAPI 私钥/证书本地存储及使用技术产品方案组”。

三、目的意义

我国已经于 2003 年至 2006 年分别颁布了无线局域网相关国家标准 GB 5629.11-2003 、 GB 15629.11-2003/XG1-2006 、 GB 15629.1101-2006 、 GB 15629.1102-2003、GB/T15629.1103-2006 和 GB 15629.1104-2006，初步形成了无线局域网国家标准体系。其中国家标准 GB 15629.11-2003《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》是无线局域网领域的基础性规范，规定了局部区域范围内用于固定式、便携式与移动式站（点）无线连通性的媒体访问控制(MAC)和物理层(PHY)规范。

随着技术的发展，WLAN 网络应用日益广泛，承载的业务种类日益复杂，已经从热点接入扩展为可运营网络，在此情况下， WLAN 网络的安全、可运营、可管理已经成为必然需求。由于 WAPI 证书是整个应用 WAPI 技术系统的安全起点，研究和制定“证书本地存储及应用技术规范”,用于指导厂商进行相关进行研发和生产，已经势在必行。

四、编制原则

本标准从系统结构、技术要求等方面规范了 WAPI 证书本地存储及应用技术。

本标准的制定完成将填补 WAPI 证书本地存储及应用方面的技术空白，为采用 WAPI 证书本地存储及应用的架构和系统等提供标准依据，完善 WAPI 国家标准体系。

本标准的编制主要按照符合国际标准，同时结合我国国内实际情况的原则进行。随着技术的发展、设备的进步以及标准制定工作的深入开展，还将对该标准的范围和内容作进一步的扩充和完善。

五、编制过程

2009 年 10 月开始项目准备工作

2009 年 11 月完成项目编制工作大纲

2009 年 11 月完成编目立项建议书

2009 年 12 月项目组武夷山会议就草案稿的内容征求大会意见

2010 年 04 月完成征求意见稿

2010 年 10 月形成并提交征求意见稿

2010 年 10 月至 11 月处理搜集到的意见,形成新版本文档

2010 年 12 月参加工作组举行的项目组集中会议, 对征求到的意见处理情况进行了汇报,会议决定 12 月 31 日前提交第二次征求意见稿到工作组秘书处。

2010 年 12 月 31 日，根据工作组 12 月会议决议和征求到的意见，形成第二次征求意见稿并提交至工作组秘书处开展第二次征求意见工作

六、主要内容

本规范规定了 WAPI 私钥/证书的本地存储及应用技术规范，目前 WAPI 私钥/证书的存储介质包括独立安全介质和开放介质两大类。本规范只定义独立安全介质的安全存取、文件管理和安全使用相关内容：

私钥/证书的安全存取技术，包括文件格式、存取控制条件、存取操作命令。

私钥/证书的安全分发技术，包括私钥/证书文件的申请、生成、更新、吊销流程中，独立安全介质和证书颁发设备的交互接口。

私钥/证书的安全应用技术，包括 WAI 功能在独立安全介质和终端之间的划分，WAI 执行过程中，终端和独立安全介质的交互接口。

本规范适用于 WAPI 技术架构，依据中国国家标准 GB 15629.11，此标准是国际标准 ISO/IEC 8802-11 在中国的采纳版本，源自 IEEE 802.11 标准，主要目录结构如下：

七、国际、国外同类标准情况

本规范适用于 WAPI 技术架构，依据中国国家标准 GB 15629.11，此标准是国际标准 ISO/IEC 8802-11 在中国的采纳版本，源自 IEEE 802.11 标准，本规范也是 RFC5416 的延伸和扩展。鉴于中国国家标准 GB 15629.11 中的 WAPI 技术是中国提出的具有自主知识产权的安全技术标准，将 WAPI 证书本地存储及应用技术应用于中国自主知识产权的无线局域网安全服务，目前国内外都还没有类似技术标准。

八、与有关的现行法律、法规和强制性国家标准的关系

本工作组标准化指导性技术文件《WAPI 私钥/证书本地存储及使用技术规范》与有关的现行法律、法规和强制性国家标准不发生抵触。

九、标准类型建议

本指导性技术文件建议以指导性技术文件发布，且没有保密的要求。

宽带无线 IP 标准工作组 WAPI 私钥/证书本地存储及使用技术标准项目组

WAPI 产业联盟 WAPI 私钥/证书本地存储及使用技术产品方案组

2010 年 12 月