宽带无线 IP 标准工作组标准

《证书格式范例》

编　制　说　明

（征求意见稿）

2011 年 **12** 月

宽带无线 IP 标准工作组 WAPI 证书管理标准项目组

WAPI 产业联盟 WAPI 证书管理产品方案组

一、任务来源

根据工业和信息化部宽带无线 IP 标准工作组 2010 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 2010040-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 证书管理标准项目组”、WAPI 产业联盟“WAPI 证书管理产品方案组”。

三、目的意义

WLAN 网络具备移动性、高宽带特点，可满足用户有限移动下的高速接入需求。近年来，WLAN 产品日益丰富，3G 发牌后，手机与 WLAN 融合已经成为必然趋势。3G+WAPI 的业务可以在家庭、热点、专网等各种区域使用，在笔记本、PDA(掌上电脑)、上网本、MID(移动互联网设备)、数据卡、手持电子设备等设备中产生各种应用，结合互联网特点，可以为运营商应用增值服务提供广阔的发展空间。

随着 WLAN 网络和业务规模的不断扩大，以及 WLAN 用户终端的不断丰富，网络和信息安全成为必须考虑和解决的问题。

目前解决公众 WLAN 安全问题的方法中，WAPI 是中国提出的具有自主知识产权的安全技术标准。WAPI 主要采用了认证服务器、WLAN 接入设备、用户终端各自独立的“三元架构”，通过独立的认证服务器实现了用户终端与 WLAN 接入设备的双向鉴别，有效地规避了 WLAN 网络的安全隐患；同时使用强度较高的椭圆曲线密码算法进行证书签发、证书鉴别、密钥协商，用分组密码算法对传输数据进行加解密。

WAPI 体系中定义的证书标准，目前没有其它基础标准提供依托，是一个不太完备的标准框架，在具体运营时没有找不到依据。X509 系列标准定义了证书通用的一些操作，没有兼顾到目前 WAPI 体系中的设备的差异性。由于认证服务器和 WLAN 接入设备的密钥运算能力不同，各个厂商的实现差异化也很大，移动终端方面的差

异性更大。因此迫切的需要一套完整的规范来指导 WAPI 运营中的证书服务。本指导性技术文件针对证书格式进行了规范。

四、编制原则

本标准内容同国家已发布的标准保持一致性。本标准中所涉及到的 X.509 数字证书内容与中华人民共和国国家标准 GB/T 20518-2006 的关系如下:

a) 本标准中涉及的 X.509 数字证书的定义、结构和描述同 GB/T 20518-2006 完全一致;

b) 本标准为基于 GB/T 20518-2006 中所定义的 X.509 数字证书而列举的应用在 WAPI 协议中的具体格式范例。

本标准中未明确指明为可选要素的部分均为必备要素。

本标准实施过程中，涉及到密码技术的具体应用时，按照国家密码管理局的有关规定和相关规范执行。

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 11 月开始项目准备工作
2010 年 9 月完成项目编制工作大纲
2010 年 10 月完成编目立项建议书
2011 年 5 月完成草案稿
2011 年 7 月项目组重庆会议就草案稿的内容征求大会意见
2011 年 8 月项目组根据重庆会议要求就草案稿的内容征求运营商意见
2011 年 9 月项目组深圳会议就草案稿的内容再次征求大会意见
2011 年 12 月形成并提交征求意见稿

六、主要内容

本标准根据 GB/T 20518-2006 所规定的 X.509 数字证书的基本结构，进一步描述了符合 WAPI 协议产品所使用的 X.509 数字证书中应包含的数据项及其定义，并且列举了具体的数字证书编码范例。

本标准适用于采用 WAPI 协议的设备生产商、运营商以及检测机构。主要目录结构如下：

七、国际、国外同类标准情况

X509 系列标准规范了互联网领域证书相关的格式、申请、更新、撤销等相关服务，具有参考意义。鉴于 WAPI 是中国提出的具有自主知识产权的安全技术标准，将证书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完备的技术标准。

本项目以 GB 15629.11 系列无线局域网有关标准为基础，研究无线局域网中证书格式范例，属于这些标准的增强技术。

八、与有关的现行法律、法规和强制性国家标准的关系

本工作组标准文件《WAPI 证书管理 第 5 部分：证书格式范例》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

本标准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 证书管理标准项目组

WAPI 产业联盟 WAPI 证书管理产品方案组

2011 年 12 月