CBWIPS

宽带无线IP标准工作组标准化指导性技术文件

CBWIPS/Z 022—2010

无线局域网证书鉴别漫游规范

Wireless Local Area Network Roaming of Certificate

Authentication Specification

2010-12 -03 发布　　2010-12-03 实施

工业和信息化部宽带无线 IP 标准工作组　发 布

目　　次

版权声明

CBWIPS

前　言

本指导性技术文件由工业和信息化部宽带无线 IP 标准工作组和 WAPI 产业联盟(中国计算机行业协会无线网络和网络安全接入技术专业委员会）共同提出，由工业和信息化部宽带无线 IP 标准工作组归口。

本指导性技术文件主要起草单位：工业和信息化部宽带无线 IP 标准工作组“无线局域网证书鉴别漫游标准项目组” 暨 WAPI 产业联盟“无线局域网证书鉴别漫游产品方案组”(中国电信集团股份有限公司上海研究院、西安西电捷通无线网络通信股份有限公司、北京大学深圳研究生院、WAPI 测试实验室、无锡中太数据通信有限公司、北京网贝合创科技有限公司、广州杰赛科技股份有限公司、上海市数字证书认证中心有限公司、北京中电华大电子设计有限责任公司、北京创原天地科技有限公司、中国电子技术标准化研究所、北京五龙电信技术公司、重庆邮电大学、中国泰尔实验室、国家密码管理局商用密码检测中心、北京北大方正集团公司、弘浩明传科技（北京）有限公司、迈普通信技术股份有限公司、西安邮电学院等)。

本指导性技术文件主要起草人：高波、张变玲、潘毅明、赖晓龙、朱跃生、铁满霞、秦志强、胡亚楠、李琳、张龙、张永强、王天华、兰天、奚红梅、卓兰、高宏、龙昭华、赵强、罗鹏、韩康、申晖、康震、朱志祥、黄振海、郭晓东、李少锋、罗先林、李明亮、林凡、陈荦琪、周涛、王旭、高强、葛莉、雷霆、王胜男、冯晔、黄金玉、杨宏、余乃平、温蕾、李玉静、董涌潮等。

引　言

无线局域网鉴别与保密基础结构 WAPI（wireless local area network authentication and privacy infrastructure）为无线局域网中的数据链路层提供了安全解决方案，包括身份鉴别、密钥管理、数据加密、数据鉴别和重放保护等功能。在无线局域网中，由于无线通信的特点，用户随时会发生漫游移动，为实现用户移动接入网络的便捷性，需要设计无需用户的参与而实现无缝的漫游协议，满足大规模应用的需要。

本工作组标准化指导性技术文件详细说明了在漫游接入情况下的 WAPI 证书鉴别的协议流程、协议处理和帧格式等技术内容，适用于指导符合 GB15629.11 系列国家标准的无线局域网产品的开发。

CBWIPS

无线局域网证书鉴别漫游规范

1　范围

本指导性技术文件规定了WAPI证书漫游鉴别的协议流程、协议处理和帧格式等技术内容。

本指导性技术文件适用于指导符合GB15629.11系列国家标准的无线局域网产品开发。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 15629.11-2003　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

GB 15629.11-2003/XG1-2006　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　第1号修改单

CBWIPS/Z 010-2009　WAPI多信任证书实施技术

3　网络拓扑和协议流程

3.1　综述

无线局域网国家标准中采用了WAPI安全接入机制。WAPI提供了基于证书和预共享密钥的安全机制，其中证书机制适合于运营应用的环境。本方案在国家标准的基础上进行扩展，解决WAPI安全机制的证书漫游鉴别问题，提供一种安全性高、运行性能高的基于WAPI证书的漫游鉴别协议。

本方案实际物理网络部署时可用以下方式，AS之间直接建立信任关系互联或由中心（集团）AS负责中转AS之间的漫游鉴别消息，见图1。

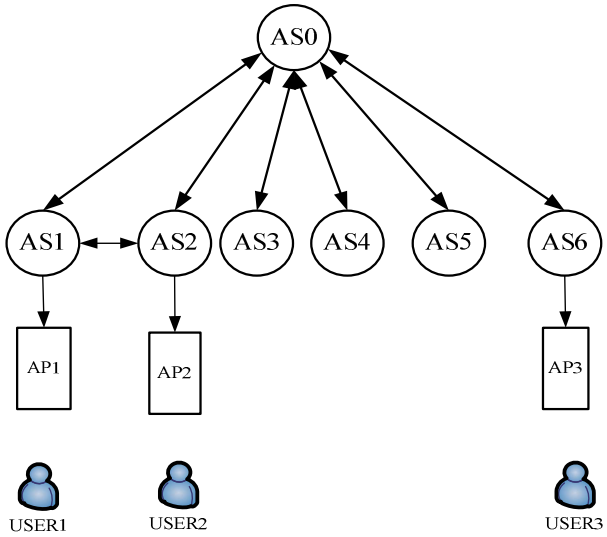

图1　漫游网络拓扑图

3.2 协议设计

本方案基于 GB 15629.11-2003/XG1-2006 中的 WAPI 鉴别协议进行扩展，在用户漫游时，对终端证书的鉴别返回到归属地进行。在鉴别协议设计时考虑了同一运营商内部和不同运营商之间的漫游问题。

3.2.1 AS 之间有直接信任关系

证书鉴别过程见图2。

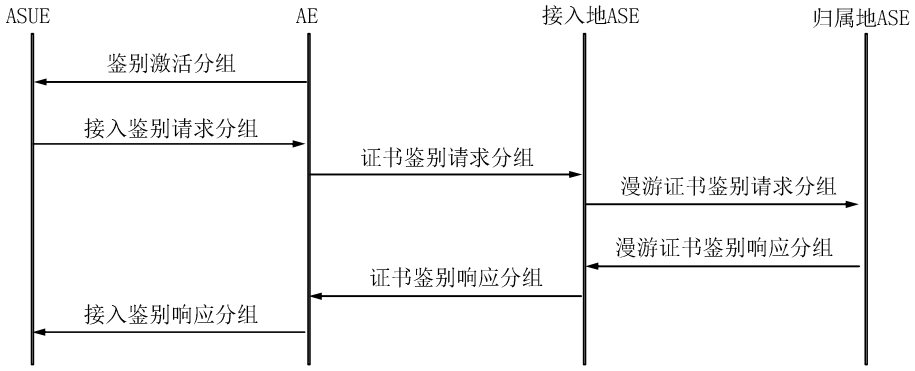

图2 证书漫游鉴别过程

3.2.2 AS 之间无直接信任关系

证书鉴别过程见图3。

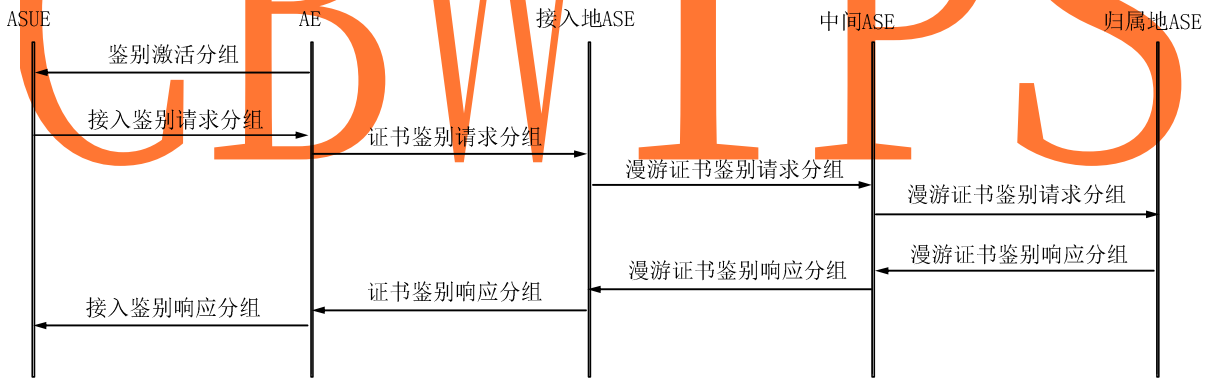

图3 证书漫游鉴别过程（中心转发）

相邻 AS 可互相交换存储证书，或预置共享密钥来建立信任关系。接入地 AS 如果没有找到直接信任的归属地 AS，则把漫游证书鉴别请求发往中心 AS（每个运营网络一个中心 AS，各地区 AS 和中心 AS 互相交换存储证书或预置共享密钥建立信任关系），接入地 AS 负责把该漫游认证请求发往中心 AS，中心 AS 再把漫游证书鉴别请求发给归属地 AS 进行证书认证。

若用户跨运营商漫游，接入地 AS 把漫游证书鉴别请求发往中心 AS（每个运营商一个中心 AS，各地区 AS 和中心 AS 互相交换存储证书或预置共享密钥），中心 AS 负责把该漫游认证请求发往归属地运营商中心 AS，归属地运营商中心 AS 再把漫游证书鉴别请求发给归属地 AS 进行证书认证。

4 协议分组格式

4.1 漫游证书鉴别请求

由接入地 ASU 发往归属地 ASU，漫游证书鉴别请求分组数据字段定义见图 4。

终端信任的 AS 证书持有者名称	ADDID	AE 询问	ASUE 询问	STA_{ASUE} 的证书	STA_{AE} 的证书	STA_{AE} 的证书鉴别结果	接入地 ASU 的证书	扩展属性个数	扩展属性	消息鉴别
可变	12	32	32	可变	可变	1	可变	1	可变	可变

图4　漫游证书鉴别请求分组数据字段格式（单位：八位位组）

其中：

——终端信任的 AS 证书持有者名称定义见图 5。

标识	长度	内容
2	2	可变

图5　终端信任的 AS 证书持有者名称定义（单位：八位位组）

其中：

- 标识字段用于表示持有者名称类型：

  1　表示内容字段为采用 DER 编码格式的终端信任的 AS 证书持有者名称；

  其他值保留。

- 长度字段值表示内容字段的八位位组数；
- 内容字段：标识字段值为 1 时，表示采用 DER 编码格式的终端信任的 AS 证书持有者名称。

——ADDID，AE 询问，STA_{ASUE} 的证书，STA_{AE} 的证书，字段格式见 GB 15629.11-2003/XG1-2006 中的定义。

——STA_{AE} 的证书鉴别结果，长度为一个八位位组。值的定义见 GB 15629.11-2003/XG1-2006 中 8.1.4.2.4。

——扩展属性个数字段标识后面包含的扩展属性个数。

——扩展属性字段采用 TLV 格式。

——消息鉴别字段采用 TLV 格式，见图 6。

类型	长度	内容
1	2	可变

图6　TLV 格式（单位：八位位组）

当类型字段值为 1 时，表示内容字段为证书和签名信息，见图 7。

证书	签名
可变	可变

图7　证书和签名信息格式（单位：八位位组）

签名字段属性定义见 GB 15629.11-2003/XG1-2006 中 8.1.4.1.2，表示对本分组中除消息鉴别字段外其他分组内容信息计算签名。

此处的证书为接入地鉴别服务器 AS 或中转（中心）AS 的证书，签名为用该证书对应的私钥计算的签名。

当类型字段值为 2 时，表示内容字段为共享密钥计算得出的消息鉴别码，见图 8。

消息鉴别码
20

图8　消息鉴别码格式（单位：八位位组）

消息鉴别码字段长度为20个八位位组，表示用HMAC-SHA256算法对本分组中除消息鉴别字段外其他分组内容信息计算得到，算法的具体信息见GB15629.11-2003/XG1-2006附录E。

AS接收到AP发送的证书鉴别请求后，首先根据证书鉴别请求分组中终端的证书颁发者和ASUE信任的ASU列表判断是否可在本地鉴别，即判断终端是否信任本地的AS，若不信任则需要构造漫游证书鉴别请求分组并发到合适的AS进行漫游鉴别。构造漫游证书鉴别请求时，选择合适的终端信任的AS证书持有者名称时优先选择ASUE信任的ASU列表中信任的AS，若选择的AS无响应或收到的漫游证书鉴别响应中终端的证书鉴别结果为“颁发者不明确”，选择其他信任的AS构造漫游证书鉴别请求，发送漫游证书鉴别请求分组，若用可选的终端信任的AS构造的漫游证书鉴别请求均无响应或收到的响应中终端证书的鉴别结果为“颁发者不明确”，则AS向AP返回证书鉴别响应分组，其中终端的证书鉴别结果为“颁发者不明确”。

AS收到漫游证书鉴别请求后，首先验证消息鉴别字段的有效性，若验证失败丢弃该分组，然后验证分组中的终端信任的AS证书持有者名称，判断自己是否能验证终端的证书有效性，若能验证，则验证终端证书的合法性，构造漫游证书鉴别响应分组返回给发送漫游证书鉴别请求的AS；若不能验证则根据本地存贮的信任AS信息列表构造漫游证书鉴别请求发给适合的AS，若在本地存贮的信任AS信息列表中找不到适合的AS，则构造漫游证书鉴别响应分组返回给发送漫游证书鉴别请求的AS，其中终端的证书鉴别结果设置为“颁发者不明确”，且分组中的ASUE信任的服务器签名字段由本AS私钥计算填充。

漫游证书鉴别请求分组格式中每经过一个中间ASE，替换分组中的消息鉴别字段（漫游证书鉴别请求和响应分组在ASE之间进行中转传输时的格式保持不变）。

4.2　漫游证书鉴别响应

由归属地ASU发往接入地ASU，漫游证书鉴别响应分组数据字段定义见图9。

接入地 AS 证书持有者名称	ADDID	证书的验证结果	ASUE 信任的服务器签名 1	接入地 ASU 的证书	ASUE 信任的服务器签名 2	扩展属性个数	扩展属性	消息鉴别
可变	12	可变	可变	可变	可变	1	可变	可变

图9　漫游证书鉴别响应分组数据字段格式（单位：八位位组）

其中：

——接入地 AS 证书持有者名称字段格式定义同漫游证书鉴别请求分组中的终端信任的 AS 证书持有者名称；

——ADDID，证书的验证结果，接入地 ASU 的证书，ASUE 信任的服务器签名 1，ASUE 信任的服务器签名 2 字段格式见 GB 15629.11-2003/XG1-2006 中的定义；

——扩展属性个数字段标识后面包含的扩展属性个数；

——扩展属性字段采用 TLV 格式，见图 10。

目前的扩展属性有业务鉴权属性。

类型	长度	内容
2	2	可变

图10　TLV 格式（单位：八位位组）

当类型字段值为6时，表示内容字段为用户的业务鉴权属性。

——消息鉴别字段定义同前。

ASUE 信任的服务器签名 1 是由 ASUE 信任的服务器的证书对证书的验证结果字段进行的签名。

ASUE 信任的服务器签名 2 是由 ASUE 信任的服务器的证书对接入地 ASU 证书字段进行的签名。

消息鉴别字段采用 TLV 格式，见图 11。

类型	长度	内容
1	2	可变

图11　TLV 格式（单位：八位位组）

当类型字段值为 1 时，表示内容字段为证书和签名信息，见图 12。

证书	签名
可变	可变

图12　证书和签名信息（单位：八位位组）

此处的证书为 ASUE 信任的归属地服务器 AS 或中转（中心）AS 证书，签名为用该证书对应的私钥计算的签名。

当类型字段值为 2 时，表示内容字段为共享密钥计算得出的消息鉴别码，见图 13。

消息鉴别码
20

图13　消息鉴别码（单位：八位位组）

证书、签名和消息鉴别码定义见 4.1。

AS 收到漫游证书鉴别响应后，首先验证消息鉴别字段的有效性，若验证失败丢弃该分组，然后验证分组中的接入地 AS 证书持有者名称，若与自身的证书持有者名称不符合则根据本地存贮的信任 AS 信息列表构造漫游证书鉴别响应发给适合的 AS，若与自身的证书持有者名称相符，则构造证书鉴别响应分组返回给 AP。

其他涉及到的分组格式定义见 GB 15629.11-2003/XG1-2006。

5　协议类型字段定义

在 GB 15629.11-2003/XG1-2006 中 8.1.4.1 的基础上扩展定义 WAI 协议分组头中的子类型字段：

——AS 之间的漫游鉴别分组利用 UDP 端口 3810 进行通信；

——128：表示漫游证书鉴别请求分组；

——129：表示漫游证书鉴别响应分组。