ICS 33 040 40
L 78

YD

中华人民共和国通信行业标准

YD/T 1614-2007

公众IP网络安全要求
——基于数字证书的访问控制

Security Requirements for Public IP Network
——Access Control based Digital Certificate

2007-04-16 发布　　2007-10-01 实施

中华人民共和国信息产业部　发布

目　次

前　言

本标准是“公众IP网络安全”系列标准之一。该系列标准预计的结构及名称如下：

1. 公众IP网络安全要求——安全框架；
2. 公众IP网络安全要求——基于数字证书的访问控制；
3. 公众IP网络安全要求——基于远端接入用户验证服务协议（RADIUS）的访问控制；
4. 公众IP网络安全要求——基于Diameter的访问控制。

本标准的附录A、附录B、附录C和附录D均为资料性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：信息产业部电信研究院

中国电信集团公司

本标准主要起草人：聂秀英　魏　亮　唐永丽　彭　俊　余英泽　尹亚莉

公众 IP 网络安全要求
——基于数字证书的访问控制

1 范围

本标准规定了根据用户所持有的数字证书对普通用户访问网络资源及有偿信息资源的访问控制要求，同时规定了基于 IPsec 的 VPN 中对等体之间利用数字证书进行认证的技术要求。

本标准适用于基于数字证书进行访问控制的系统。

2 规范性引用文件

下列文件中的条款通过在本标准中的引用而构成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括斟误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

YD/T 1322.3-2004	电子商务技术要求 第三部分：证书及认证系统
YD/T 1615-2007	公众 IP 网络安全要求——基于远端接入用户验证服务协议（RADIUS）的访问控制要求
IEEE 802.1x	基于端口的网络接入控制
IETF RFC 2406（1998）	IP 封装安全载荷（ESP）
IETF RFC 2407（1998）	解释 ISAKMP 的 Internet IP 安全域
IETF RFC 2408（1998）	Internet 安全联盟及密钥管理协议（ISAKMP）
IETF RFC 2409（1998）	Internet 密钥互换（IKE）
IETF RFC 2560（1999）	Internet X.509 公共密钥基础设施在线证书状态协议
IETF RFC 2716（1999）	PPP EAP TLS 认证协议
IETF RFC 2863（2000）	远程拨入用户认证服务（RADIUS）
IETF RFC 3280（2002）	Internet X.509 公共基础设施 证书和 CRL 轮廓
IETF RFC 3281（2002）	用于认证的 Internet 属性证书轮廓
IETF RFC 3579（2003）	远程拨入用户认证服务（RADIUS）对可扩展的认证协议（EAP）的支持
IETF RFC 3580（2003）	IEEE 802.1X 远程拨入用户认证服务（RADIUS）使用指南
IETF RFC 3770（2004）	支持以点对点协议（PPP）和无线局域网（WLAN）认证的证书扩展和属性
IETF RFC 3748（2004）	可扩展的认证协议（EAP）
IETF RFC 4058（2005）	用于承载网络接入认证的协议需求

3 缩略语

下列缩略语适用于本标准。

AA	Attribute Authority	属性证书认证中心
AS	Authentication Server	认证服务器

CA	Certificate Authority	数字证书认证中心
DSL	Digital Subscriber Line	数字用户线
DSLAM	Digital Subscriber Line Access Multiplex	数字用户线接入复用器
EAP	Extensible Authentication Protocol	可扩展的认证协议
EAPOL	EAP over LAN	LAN 上的 EAP
EAPOR	EAP between RADIUS and Authentication entity	RADIUS 和认证实体之间的 EAP
RADIUS	Remote Authentication Dial Up Service	远程拨入用户认证服务
IKE	Internet Key Exchange	Internet 密钥互换
ID	Identifier	个人标识符
LAN	Local Area Network	局域网
LCP	Link Control Protocol	链路控制协议
KE	Key Exchange	密钥互换
NAS	Network Access Server	网络接入服务器
OCSP	Online Certificate Status Protocol	在线证书状态协议
PKC	Public Key Certificate	公共密钥证书
PKI	Public Key Infrastructures	公共密钥基础设施
PKIX	Public-Key Infrastructure（X.509）	公共密钥基础设施（X.509）
RA	Register Authority	注册中心
SSL	Secure Socket Layer	安全套接层
TLS	Transport Layer Security	传送层安全
VPN	Visual Private Network	虚拟专用网络
WLAN	Wireless Local Area Network	无线局域网

4 定义与符号

4.1 定义

下列定义适用于本标准。

4.1.1 证书

可以指属性证书或公共密钥证书。除非特别指出，证书可用于表示属性证书和公共密钥证书（PKC）。

4.1.2 数字证书认证中心（CA）

一个或多个用户信任的、生成和签署公共密钥证书的权威机构。该机构在证书的整个生存期内负责管理公共密钥证书。

4.1.3 属性证书认证中心（AA）

一个或多个用户信任的、生成和签署用户属性证书的权威机构。该机构在属性证书的整个生存期内负责管理属性证书。

4.1.4 公共密钥证书（PKC）

包含有关端实体的公共密钥和一些其他信息的数据结构。该证书具有签发该证书的 CA 的私有密钥数字签名。

4.1.5 基于 IPsec 的 VPN 中的对等体

指在它们之间需要建立 IPsec 隧道的两个实体。

4.2 符号

下列符号适用于本标准。

HDR：ISAKMP 头，其互换类型是模式。若写成 HDR*时，表示载荷加密。

SA：指一个或多个建议的 SA 协商。初始者可以提供多个建议，用于在协商时响应者必须仅返回一个。

KE：包含有在 Diffie-Hellman 互换中互换信息的密钥载荷。

Nx：临时载荷，x 可以是 i 或 r，分别表示 ISAKMP 的初始者和响应者。

IDx：x 的标识载荷，在过程 1 期间，x 可以是“ii”或“ir”，分别表示 ISAKMP 初始者和响应者。

SIG：签名载荷。签名的数据是互换特定的。

CERT：证书载荷。

HASH：hash 载荷。Hash 的内容对认证方法是特定的。

5 概述

5.1 基于数字证书认证的基本原理

基于数字证书的认证，包括对用户所提供的数字证书本身的确认以及对提交数字证书的用户是否为该数字证书合法持有者的确认。其基本原理为：

1. 对数字证书本身有效性的确认

a）确认数字证书本身包含信息的准确性

- 用户端软件（或受信 CA）创建一对密钥，其中一个是公开密钥，另外一个是私有密钥。客户准备一个包括用户 ID 和用户公开密钥的未签名证书，然后用一种安全的方式把它发送给一个 CA。
- CA 通过计算该未签名证书的散列值，并用 CA 的私有密钥加密该散列值后，产生一个签名（已加密的散列码）。CA 接着把它附在该未签名的证书上，并把现在已经签名的该证书返还给该客户。
- 客户可以把它的已经通过 CA 签名的证书发送给任何其他用户。收到证书的用户可以通过计算证书的散列值（不包括签名），并用 CA 的公开密钥解密该签名，把该散列值与已解密的签名进行比较，以验证其他用户的证书的准确性。

b）确认数字证书的有效性

- 收到证书的用户在确认用户本身的准确性后，到 CA 用户数据库中查找用户所提交的证书是否被列入到证书废弃表中，从而确认用户所提交的证书是否有效。

2. 确认提交数字证书的用户是否为所提交的数字证书的合法持有者

- 收到数字证书的一方生成一个随机数，利用所收到的数字证书中所包含的公开密钥加密随机数并将加密后的随机数发送给发出数字证书的一方。
- 接收到加密后的随机数的一方利用自身的秘密密钥将接收到的加密后随机数解密，并用对方的公开密钥加密返传给对方。
- 接收到返传回来的信息后，用户利用自身的私有密钥解密接收到的信息，并将解密后的内容与最初生成的随机数相比较，若两者相同，则可确认对方是该数字证书是合法持有者。

通过上面的两个过程完成基于数字证书对用户身份的认证。本标准中不规定用户如何获得证书以及与 CA 本身相关的技术规定。

5.2 基于数字证书进行访问控制的应用

访问控制通常是指进行通信的一方对与其通信的另一方的身份（或通信双方之间的身份）进行确认并根据某种策略对是否允许已经确认身份的通信方进行通信或访问。为此基于数字证书可以进行如下情况下的访问控制：

1）用户访问 IP 网络时，IP 网络对用户进行访问控制。

2）用户访问连接到 IP 网络上的有偿信息资源时，有偿信息资源对用户进行访问控制。

3）IPsec VPN 中的对等体之间相互确认彼此身份时基于各自已经拥有的数字证书进行访问控制。

6 基于数字证书的访问控制系统的组成及组成部分的功能

6.1 系统组成

6.1.1 基于数字证书访问 IP 网络的访问控制系统的组成

基于数字证书对用户接入网络进行访问控制的系统功能框图如图 1 所示。

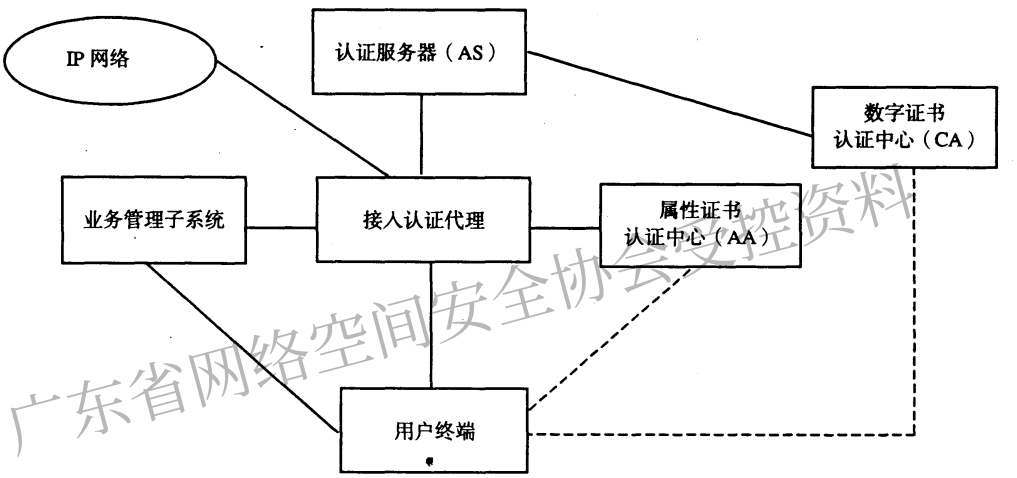


图 1 基于数字证书对用户接入网络进行访问控制的系统功能框图

如图 1 所示，基于数字证书的用户接入访问控制系统主要由接入认证代理、认证服务器、数字证书认证中心、属性证书认证中心和业务管理系统组成。图中所示的各组成部分是逻辑实体，在实际实施中不同的逻辑实体可能由同一个物理实体或位于同一地点的物理实体来实现。对已经拥有数字证书的用户接入网络时，用户首先与接入认证代理建立连接，用户接入代理与用户协商用户认证方式，用户选择采用数字证书的方式进行认证，接入代理向用户发送提交用户数字证书的申请，用户将可以证明其身份的数字证书提交给接入认证代理，用户接入认证代理将用户所提交的数字证书转发给认证服务器。认证服务器利用数字证书认证中心所提供的服务来验证数字证书的有效性，然后通过随机生成一随机数并利用用户数字证书中的用户公开密钥对随机数进行加密并发送到接入认证代理，由接入认证代理转发给用户，用户利用自己所拥有的私有密钥对所接收到的已加密的随机数进行解密并将解密后的随机数经过接入认证代理转发给认证服务器。认证服务器将接收到的随机数与原始随机数进行比较，若相同便向接入代理发送用户通过身份认证的证实消息。接入认证代理然后根据用户所提供的数字证书上的相关信息到属性认证中心中查找用户的属性证书确定用户所申请的业务种类结合在业务管理子系统所提供的该用户以往业务的使用情况（主要是缴费情况）决定是否允许用户访问网络或相关的资源。在具体实施时，根据网络提供者的具体情况确定在向用户终端授权接入时是否使用属性证书和业务管理系统所提供的信息。

6.1.2 基于数字证书访问有偿信息资源的访问控制系统的组成

基于数字证书对用户访问有偿信息资源的访问控制的功能框图如图 2 所示。

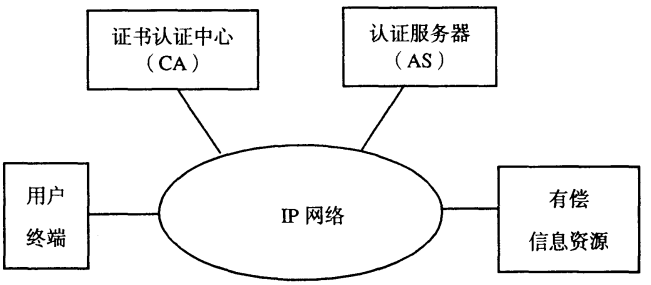


图 2 基于数字证书对用户访问有偿资源进行访问控制的系统功能框图

如图 2 所示，用户在访问有偿信息或进行电子商务等应用时，需要在进行交易的双方或信息提供者对用户进行身份认证。此时，认证过程是在用户已经连接到网络之后的二次认证，是在应用层上进行的，此时不需要网络接入认证代理。信息提供者是否设置用户访问接入认证代理由具体的实施者确定。

6.1.3 基于 IPsec 的 VPN 中对等体之间基于数字证书进行认证的系统组成

基于 IPsec 的 VPN 中对等体之间基于数字证书认证的系统功能框图如图 3 所示。

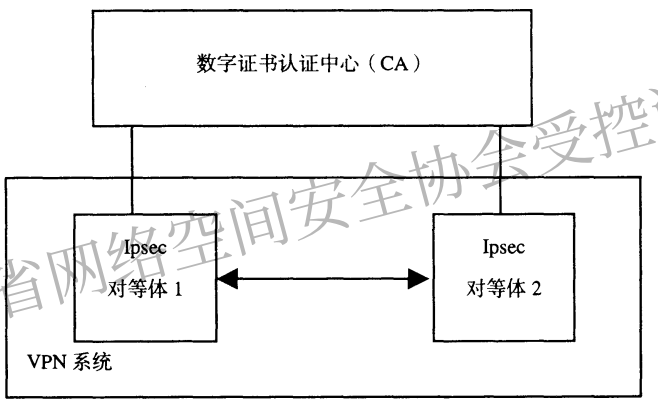


图 3 基于 IPsec 的 VPN 中对等体之间基于数字证书认证的系统功能框图

如图 3 所示，IPsec 对等体之间基于数字证书的认证系统由数字证书认证中心和 VPN 系统组成。其中数字证书认证中心负责数字证书的签发、撤消、证书签发和撤消的认证、数字证书的维护、更新、注册等功能。VPN 系统完成数字证书中非对称密钥对的生成以及 IPsec 对等体之间的通信。

6.2 各组成部分的功能要求

6.2.1 接入认证代理

在实际实现中接入认证代理可以是 NAS（用户采用 DSL 方式接入网络）、以太网交换机（以局域网方式接入时）、AP（以 WLAN 方式接入时）等。本标准中接入认证代理主要完成如下功能：

1）在用户连接到网络前，负责与用户终端建立用户与接入认证代理之间的连接通路。

2）向用户发送提交数字证书的请求。

3）接收用户提交的数字证书并将其转发给认证服务器。

4）转发认证服务器与用户之间所交换的信息。

5）在用户的身份被成功认证后，根据用户的数字证书的相关信息到属性证书认证中心查找用户的属性证书，并根据用户的属性证书以及业务管理中心所提供的信息，确定是否允许用户接入网络或访问有偿信息（选用）。

6）将用户认证结果通知用户，同时根据认证结果将用户连接到或不连接到网络。在将用户连接到网络时，为用户分配相应的网络资源（如 IP 地址及网络接入带宽等）（选用）。

7）负责根据用户的申请将用户从网络断开，同时通知业务管理系统。

6.2.2 数字证书认证中心（CA）

数字证书认证中心负责完成如下一些功能：

1）注册服务。

2）初始化服务。

3）认证服务。

4）密钥对恢复服务。

5）密钥生成服务。

6）密钥更新服务。

a）密钥作废；

b）密钥放弃。

7）注销服务。

8）证书和注销注释分发和公布。

6.2.3 属性证书认证中心（AA）

属性证书认证中心是生成和确定属性证书的第三方可信机构，其主要功能如下：

1）维护和制定授权模型，签发属性证书。

2）对属性证书进行有效的管理，及时发布证书的注销信息。

3）用户管理（用户注册，信息修改，注销）。

4）证书管理（各类证书的申请，证书的下载，注销，证书服务注册）。

5）角色管理（授权模型制订，授权模型查询，授权模型元素添加）。

6）审核管理（注册用户和申请证书的审核）。

7）操作员管理（操作员注册、注销、查询、信息权限修改）。

8）证书发布。

9）KeyNet 清理。

10）杂项管理（日志管理，审计管理，代码管理，综合查询，系统配置）。

6.2.4 业务管理子系统

业务管理子系统主要负责完成如下一些功能：

1）受理用户业务申请，协助用户申请数字证书和属性证书、存储用户的相关信息。

2）负责维护和管理用户信息，包括用户数字证书号码、用户业务开通情况、用户缴费信息。

3）向接入认证代理提供用户信息。

6.2.5 认证服务器（AS）

认证服务器主要完成如下一些功能（在具体实施时认证服务器可以是 Radius 服务器或 Diameter 服务器）：

1）确认用户所提交的数字证书的有效性。

2）验证提交数字证书的用户是否是该数字证书的合法持有者，此时需要通过数字证书认证中心协助完成对所提交的数字证书的认证。

3）将用户是否通过认证的结果通过接入认证代理发送给用户。

6.2.6 用户终端

用户终端是用户使用业务时接入到公众 IP 网络的实体。主要完成申请业务的注册并获得数字证书，并是用户接受业务的物理载体。本标准中的用户终端指用户终端设备，包括笔记本电脑、台式计算机、PDA、移动电话以及通过有线或无线方式连接到网络的路由器。

6.2.7 IPsec 对等体

IPsec 对等体或“对等体”是指为进行通信建立安全隧道利用 IKE 和 IPsec 与另一个对等体进行通信的 IPsec 系统。可以是传统的安全网关（具有两个网络接口，一个是受保护的网络，另一个是未受保护的网络）或者是 IPsec 客户端（具有一个网络接口）。在这两种情况下，IPsec 系统可以在没有 IPsec 保护的情况下通过流量，也可以对所选择的业务流施加 IPsec 保护。

7 用户与接入认证代理的连接方式

当用户通过 DSL、LAN 以及 WLAN 与接入认证代理相连时，可以采用基于数字证书的认证方式对用户进行访问控制。

7.1 用户通过 DSL 与接入认证代理相连

用户通过 DSL 与接入认证代理相连的框图如图 4（a）和 4（b）所示。图 4（a）中网络接入服务器完成接入认证代理的功能；图 4（b）中 DSLAM 完成接入认证代理的功能。

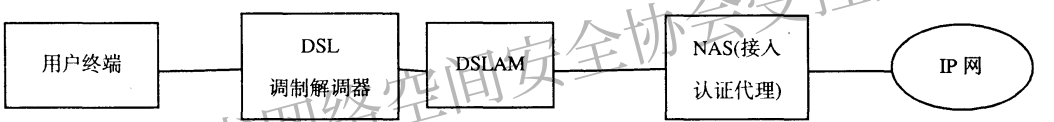


图 4（a）用户终端通过 DSL 与接入认证代理相连（NAS 作为接入认证代理）

图 4（b）用户终端通过 DSL 与接入认证代理相连（DSLAM 作为接入认证代理）

7.2 用户通过 LAN 与接入认证代理相连

用户通过 LAN 与接入认证代理相连的框图如图 5 所示。此时以太网交换机完成接入认证代理的功能。

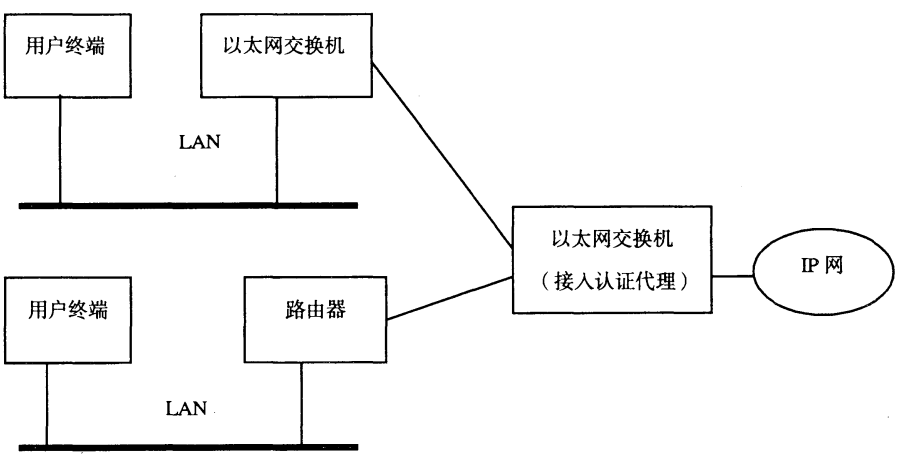


图 5 用户与接入认证代理通过 LAN 相连

7.3 用户通过 WLAN 与接入认证代理相连

用户通过 WLAN 与接入认证代理相连的框图如图 6 所示。此时 AP 完成接入认证代理的功能。

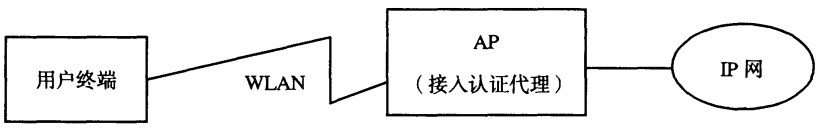


图 6　用户与接入认证代理通过 WLAN 相连

8　通信流程及协议

8.1　通信流程

8.1.1　基于数字证书接入网络的访问控制通信流程

8.1.1.1　用户终端和接入认证代理之间采用 PPP 协议基于数字证书的访问控制通信流程

用户终端和接入认证代理之间采用 PPP 协议基于数字证书的访问控制通信流程如图 7 所示。

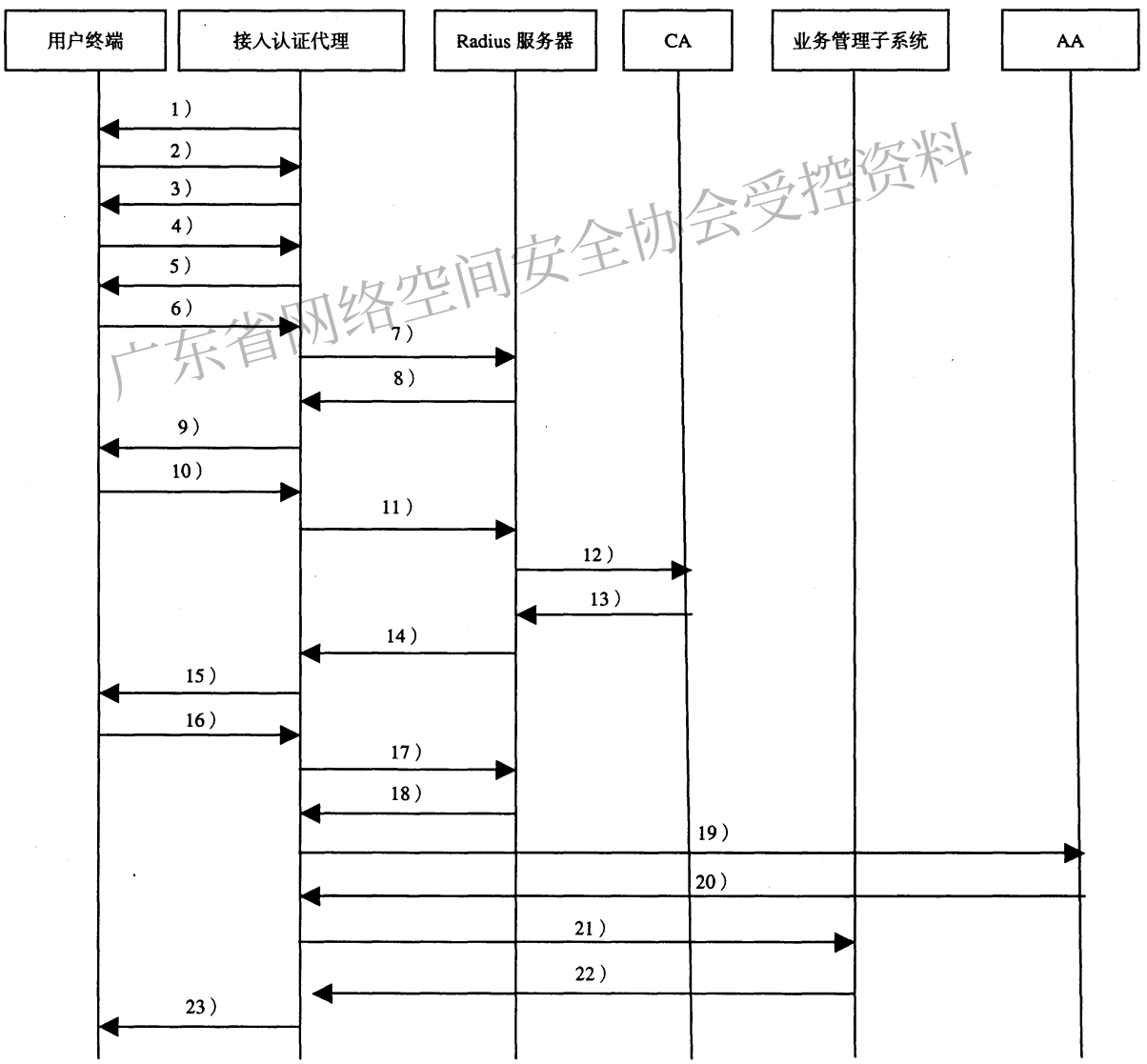


图 7　采用 PPP 协议基于数字证书的访问控制通信流程

本部分仅给出用户终端成功地认证并连接到网络的流程，同时认证服务器为 Radius 服务器。其他情况请参照 RFC 3579，RFC 2716 的相关规定。

流程说明：

1）接入认证代理向用户终端发送 PPP LCP Request-EAP auth 请求采用 EAP 认证。

2）用户终端向接入认证代理发送 PPP LCP ACK-EAP auth 证实采用 EAP 认证。

3）接入认证代理向用户终端发送 PPP EAP Request/ID 请求用户终端输入标识符。

4）用户终端向接入认证代理发送 PPP EAP-Response/ ID（MyID）将用户终端 ID 发送给接入认证代理。

5）接入认证代理向用户终端发送 PPP EAP-Request/EAP-Type=EAP-TLS（TLS Start，S bit set），开始 EAP TLS。

6）用户终端向接入认证代理发送 PPP EAP-Response/ EAP-Type=EAP-TLS（TLS client_hello）响应开始 EAP TLS。

7）接入认证代理向 Radius 服务器发送 RADIUS Access-Request/EAP-Message/ EAP-Response/EAP-Type=EAP-TLS 请求 Radius 服务器开始 EAP。

8）Radius 服务器向接入认证代理发送 RADIUS Access-Challenge/EAP-Message/EAP-Request/EAP-Type=EAP-TLS；EAP-Request/。

9）接入认证代理向用户终端发送 PPP EAP-Request/EAP-Type=EAP-TLS（TLS server_hello，TLS certificate，[TLS server_key_exchange，] [TLS certificate_request，] TLS server_hello_done）向用户终端请求发送数字证书。

10）用户终端向接入认证代理发送 PPP EAP-Response/EAP-Type=EAP-TLS（TLS certificate，TLS client_key_exchange，[TLS certificate_verify，] TLS change_cipher_spec，TLS finished）向接入认证代理发送数字证书。

11）接入认证代理向 Radius 服务器发送 RADIUS Access-Request/EAP-Message/EAP-Response/EAP-Type=EAP-TLS 转发用户终端发送来的用户终端数字证书。

12）Radius 服务器向数字证书认证中心发送 OCSPRequest 请求查询用户所提交的数字证书的有效性。

13）数字证书认证中心向 Radius 服务器发送 OCSPResponse 确认用户所提交的数字证书是有效的。

14）Radius 服务器向接入认证代理发送 RADIUS Access-Challenge/ EAP-Message/ EAP-Request/EAP-Type=EAP-TLS 将随机生成的随机数用用户的公开密钥加密后发送给接入认证代理。

15）接入认证代理向用户终端发送 EAP-Request/EAP-Type=EAP-TLS（TLS change_cipher_spec，TLS finished）将由 Radius 服务器接收到的信息转发给用户终端。

16）用户终端向接入认证代理发送 PPP EAP-Response/ EAP-Type=EAP-TLS，将使用其自身的私有密钥解码后的随机数用其私有密钥加密后发送给接入认证代理。

17）接入认证代理向 Radius 服务器发送 EAP-Message/EAP-Response/EAP-Type=EAP-TLS 将由用户终端处接收到的信息转发给 Radius 服务器。

18）Radius 服务器使用用户的公有密钥将接收到的信息解密，同时将解密后的随机数与其发送出去的随机数对比，若两者相同，则向接入认证代理发送 RADIUS Access-Accept/EAP-Message/EAP-Success（其他属性）说明认证成功。

19）接入认证代理到属性证书中心请求用户的属性证书。

20）属性证书中心向接入认证代理发送其所请求的用户属性证书。

21）接入认证代理向业务管理中心发送请求发送用户使用情况信息。

22）业务管理系统向接入认证代理发送用户使用情况信息。

23）接入认证代理根据接收到的属性证书中的内容及用户使用业务的情况信息，确定是否允许用户访问，将用户终端连接到网络中。

8.1.1.2 在用户终端和接入认证代理之间采用 IEEE 802.1x 的基于数字证书的访问控制通信流程

在用户终端和接入认证代理之间采用 IEEE 802.1x 的基于数字证书的访问控制通信流程的示例如图 8 所示，本标准中认证服务器以 Radius 服务器为例。同时仅给出用户认证成功并成功接入到网络的情况。具体规定见《公众 IP 网络安全要求——基于 802.1x 的访问控制》。

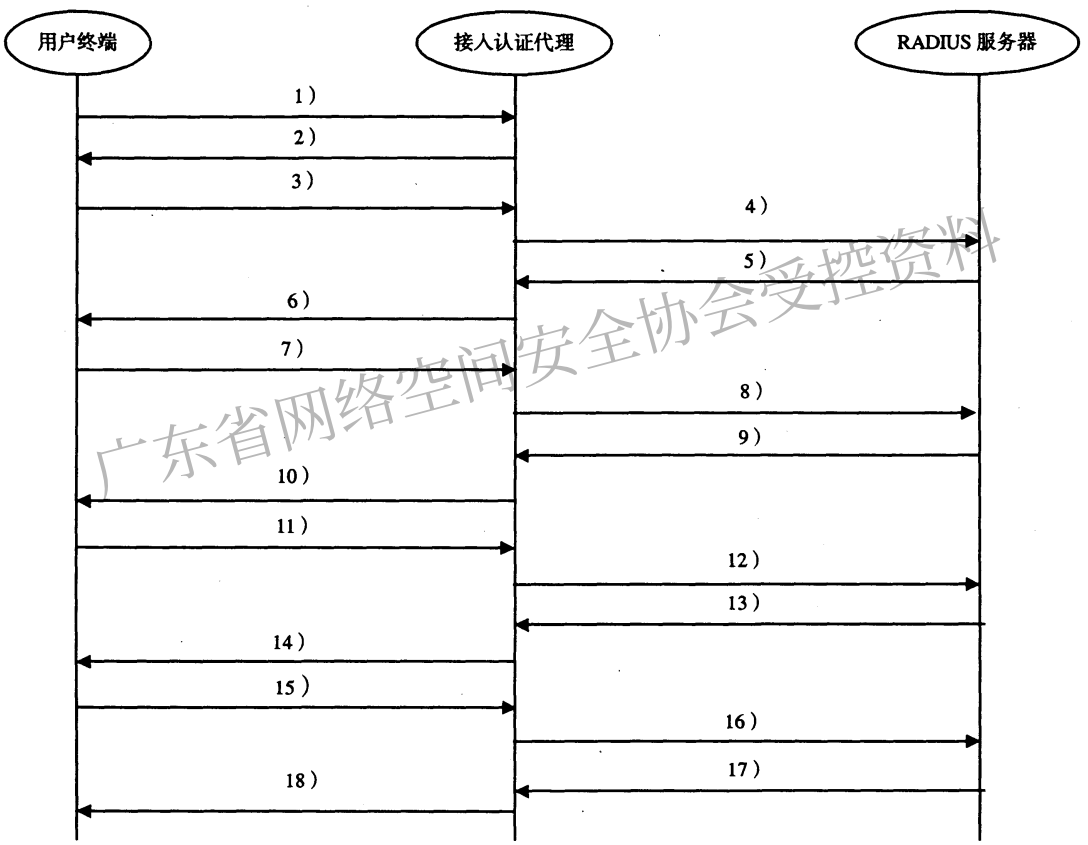


图 8 采用 IEEE 802.1x 基于数字证书访问控制通信流程

1）用户终端向接入认证代理发送一个EAPoL-Start报文，开始认证接入。

2）接入认证代理向用户终端发送EAP-Request/Identity报文，请求用户终端发送用户ID。

3）用户终端回应一个EAP-Response/Identity给接入认证代理的请求，其中包括用户ID。

4）接入认证代理将EAP-Response/Identity报文封装到RADIUS Access-Request报文中，发送给RADIUS，其中包含了客户ID属性、MAC地址；接入认证代理记录客户的MAC地址和状态。

5）RADIUS响应EAP-TLS/Start报文，通过RADIUS Access-Challenge报文发送到接入认证代理。

6）接入认证代理取出其中的EAP报文，即EAP-Request/TLS-Start报文发送给用户终端。

7）用户终端回应EAP-Response/TLS（client_hello）握手报文，其中包含用户终端支持的TLS版本、密码组给接入认证代理。

8）接入认证代理将EAP-Response/TLS(client_hello)握手报文封装到RADIUS Access-Request报文中，发送到认证服务器。

9）认证服务器以RADIUS Access-Challenge/EAP-Request报文进行响应，封装多个TLS记录，包含TLS server_hello握手、TLS certificate、server_key_exchange、certificate_request、server_hello_done等，其中TLS certificate包含验证RADIUS的证书信息，server_key_exchange包含RADIUS的公钥。

10）接入认证代理将RADIUS的EAP-Request报文发送到用户终端。

11）用户终端对RADIUS服务器进行认证，若认证成功则继续，若失败则终止认证。认证成功终端回应EAP-Response报文，对认证服务器的TLS记录进行响应，包含TLS certificate、client_key_exchange、certificate_verify、change_cipher_spec、finished等记录，其中TLS certificate包含验证用户终端的证书信息，client_key_exchange是使用RADIUS公钥加密后的定长随机串，也称为Pre Master Secret，Change_Cipher_Spec包含了用户终端能够支持的加密类型。

12）接入认证代理将EAP报文封装到RADIUS Access-Request报文中，发送到认证服务器。

13）认证服务器响应RADIUS Access-Challenge/EAP-Request报文，包含change_cipher_spec、finished记录，指定了使用的加密类型。

14）接入认证代理将EAP-Request报文发送给用户终端。

15）用户终端响应EAP-Response/EAP_type=EAP-TLS，表明TLS握手（Handshake）结束。

16）接入认证代理将该报文封装到RADIUS Access-Request报文中，发送到认证服务器。

17）认证服务器返回RADIUS Access-Accept/EAP_Success给接入认证代理。

18）接入认证代理将RADIUS Access-Accept/EAP_Success消息传递到用户终端。

8.1.2 基于数字证书访问有偿信息资源的通信流程

对于用户访问有偿信息资源，在大多数情况下，有偿信息资源需要对用户进行二次认证。该认证过程是在用户已经连接到网络上并准备访问有偿信息资源时开始的，其通信流程如图9所示。

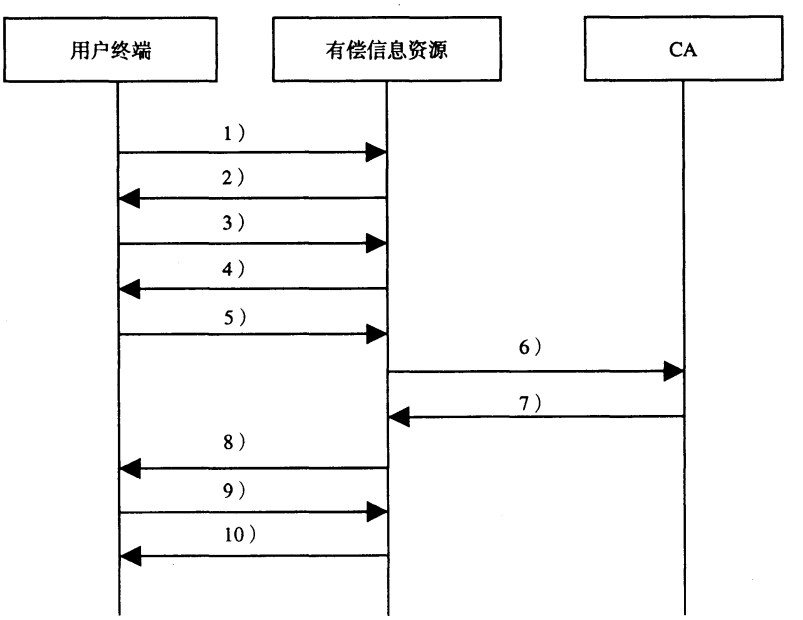


图9 用户访问有偿信息资源的通信流程

通信流程说明：

1）用户终端向信息提供者发送信息访问请求。

2）信息提供者向用户终端发送建立 SSL 的请求。

3）用户终端向信息提供者发送建立 SSL 的响应，与信息提供者之间建立一 SSL 通道。

4）信息提供者向用户终端发送数字证书请求。

5）用户终端向信息提供者提交数字证书。

6）信息提供者到 CA 在线查询用户数字证书的有效性。

7）CA 向信息提供者返回用户数字证书的有效性信息。

8）若用户数字证书有效，信息提供者向用户发送使用用户公钥加密的随机生成的随机数。

9）用户终端使用用户的私有密钥将接收到的信息解密，同时使用私有密钥加密解密后的随机数，并将加密后的信息发送到信息提供者。

10）信息提供者使用用户的公钥将接收到的加密信息解密并与原始的随机数比较，若两者相同，则向用户终端发送认证成功消息并允许用户访问信息提供者。

8.1.3 IPsec VPN 对等体之间基于数字证书的认证通信流程

IPsec VPN中在IKE的阶段1进行认证。IKE规定了4种认证方式：两种采用公开密钥加密的认证，另两种分别为采用数字签名的认证以及采用预共享密钥认证。除了采用预共享密钥认证外，其他认证方式都可能需要数字证书的支持。 在IKE阶段1的主模式是ISAKMP标识保护互换的一个示例：最初的两条消息协商策略，接下来的两条消息互换Diffie-Hellman 公开值和用于互换所需要的补充数据（例如随机数）；最后两条消息认证 Diffie-Hellman互换。作为初始ISAKMP互换的一部分协商的认证方法影响载荷的组成但不影响其目的。图10给出了使用签名的主模式的认证通信流程示例。图11给出了使用公开密钥加密的修订模式的主模式认证通信流程示例。有关符号的使用等详细细节参见RFC 2409中的相关规定。

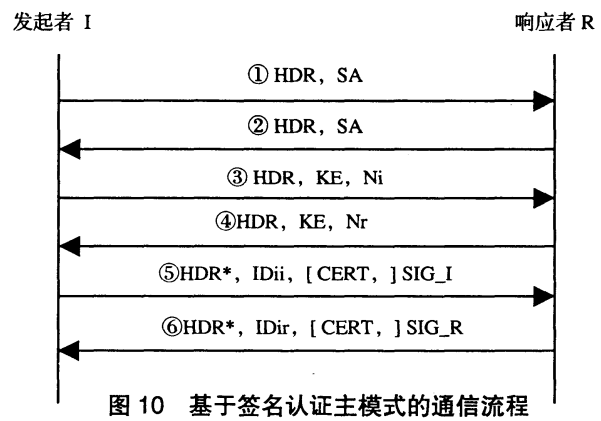


图 10　基于签名认证主模式的通信流程

通信流程说明：

1）发起者向响应者R发起安全联盟协商。在该协商中发起者I向响应者R发送其可支持的安全联盟协商列表并在消息头中携带自身的信息。

2）响应者R对发起者I发送的安全联盟协商进行响应。在响应消息中响应者R向发起者I返回其在由发起者发送过来的安全联盟协商列表中所选择的安全联盟策略以及包含其自身消息的头。若响应者R无法在从发起者I接收到的列表中选择到合适的安全联盟策略，将返回协商失败消息或将选择的自己所支持的安全联盟策略发送给发起者I。

3）发起者I向响应者R发送DH（Diffie-Hellman）公开值（KE）以及用于验证发起者I身份的由发起者I生成的随机数Ni以及数字证书请求。

4）响应者R向发起者I返回其计算的DH（Diffie-Hellman）公开值（KE）、用于验证响应者R身份的由响应者R生成的随机数Nr以及数字证书请求。

5）发起者I向响应者R发送利用前面4步交换的信息所计算出的共享DH值加密的发起者I的标识信息、数字证书、发起者的签名，以便响应者R获得确认发起者I身份的信息。

6）响应者R向发起者I返回前面4步交换的信息所计算出的共享DH值加密的响应者R的标识信息、数字证书、响应者的签名，以便发起者I获得确认响应者R身份的信息。

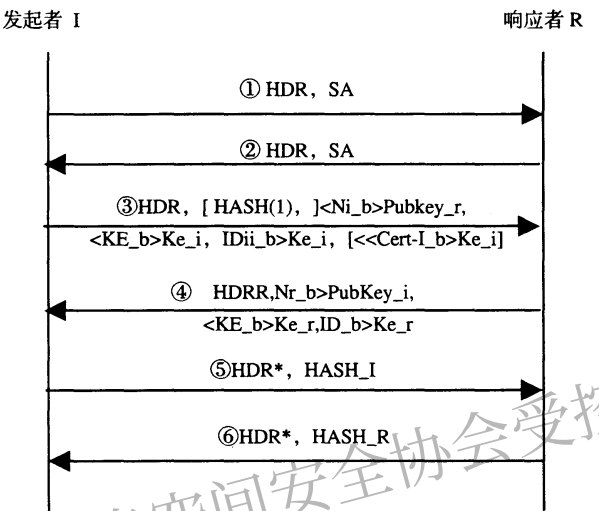


图 11 基于修订后的公开密钥认证的主模式的通信流程

通信流程说明：

1）发起者向响应者R发起安全联盟协商。在该协商中发起者I向响应者R发送其可支持的安全联盟协商列表，并在消息头中携带自身的信息。

2）响应者R对发起者I发送的安全联盟协商进行响应。在响应消息中，响应者R向发起者I返回其在由发起者发送过来的安全联盟协商列表中所选择的安全联盟策略以及包含其自身消息的头。若响应者R无法在从发起者I接收到的列表中选择到合适的安全联盟策略，则将返回协商失败消息或将选择的自己所支持的安全联盟策略发送给发起者I。

3）为确认响应者是否为其所提交的数字证书所声称的持有者，同时将其生成的 DH 公开值、数字证书等发送给响应者，发起者 I 向响应者发送利用响应者的公开密钥加密的由发起者生成的随机数 Ni-b、采用 ke-i 加密的 DH 公开值、数字证书以及身份信息等相关信息。

4）响应者R向发起者I返回利用发起者公开密钥加密的由响应者生成的随机机数Nr以及采用Ke-r加密的DH公开值、身份信息。

5）发起者I向响应者R发送利用自身的私有密钥解密从响应者接收到的随机数Nr等计算的散列值Hash-I，供响应者R确认发起者I的身份。

6）响应者R向发起者I发送利用自身的私有密钥解密从响应者接收的随机数Ni等计算的散列值Hash-R，供发起者I确认响应者R的身份。

8.2 通信协议

8.2.1 采用 PPP 协议进行基于数字证书的访问控制采用的通信协议

采用 PPP 协议进行基于数字证书的访问控制时，采用如下一些通信协议：

- 在用户终端和接入认证代理之间采用 RFC 2716 中规定的 PPP EAP TLS 认证协议。
- 在接入认证代理与认证服务器之间采用 RFC 3579《拨入用户服务的远程认证（RADIUS）对可扩展的认证协议（EAP）的支持》中规定的协议。
- 在认证服务器与 CA 之间采用 RFC 2560《Internet X.509 公共密钥基础设施在线证书状态协议》中规定的协议。

8.2.2 采用 IEEE 802.1x 进行基于数字证书的访问控制采用的通信协议

采用 IEEE 802.1x 进行基于数字证书的访问控制时，采用如下一些通信协议：

- 在用户终端和接入认证代理之间采用 IEEE 802.1x 中规定的 EAP overLAN 协议。
- 在接入认证代理和认证服务器之间采用 RFC 3579《拨入用户服务的远程认证（RADIUS）对可扩展的认证协议（EAP）的支持》中规定的协议。
- 在认证服务器与 CA 之间采用 RFC 2560《Internet X.509 公共密钥基础设施在线证书状态协议》中规定的协议。

8.2.3 应用层上进行基于数字证书的访问控制采用的通信协议

应用层上进行基于数字证书的访问控制可采用如下一些通信协议（也可以采用其他一些协议）：

- 在用户终端和有偿信息提供者之间采用 RFC 2068 中规定的 HTTP 协议 Post 方式或者其他协议。
- 在有偿信息提供者和 CA 之间采用 RFC 2560《Internet X.509 公共密钥基础设施在线证书状态协议》中规定的协议。

8.2.4 IPsec VPN 中使用数字证书进行认证的通信协议

IPsec VPN 中使用数字证书进行认证的通信协议应符合 RFC 2407、RFC 2408 和 RFC 2409 中的相关规定。在 IPsec VPN 中的对等体在确认对方发送来的数字证书的有效性时，与 CA 之间之间采用 RFC 2560《Internet X.509 公共密钥基础设施在线证书状态协议》中规定的协议。

9 数字证书格式

本标准中使用的数字证书格式应符合 IETF RFC 3280 及 RFC 3770 中的相应规定，同时根据实施者的具体情况选择使用。数字证书的基本项的 ASN.1 表示如下：

```
Certificate  ::=  SEQUENCE  {
        tbsCertificate          TBSCertificate,
        signatureAlgorithm      AlgorithmIdentifier,
        signatureValue          BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
        version             [0]  EXPLICIT Version DEFAULT v1,
        serialNumber             CertificateSerialNumber,
        signature                AlgorithmIdentifier,
        issuer                   Name,
```

```
        validity                Validity,
        subject                 Name,
        subjectPublicKeyInfo SubjectPublicKeyInfo,
        issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                                -- If present, version MUST be v2 or v3
        subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                                -- If present, version MUST be v2 or v3
        extensions      [3]  EXPLICIT Extensions OPTIONAL
                                -- If present, version MUST be v3
        }

    Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }

    CertificateSerialNumber  ::=  INTEGER

    Validity ::= SEQUENCE {
        notBefore       Time,
        notAfter        Time }

    Time ::= CHOICE {
        utcTime         UTCTime,
        generalTime     GeneralizedTime }

    UniqueIdentifier  ::=  BIT STRING

    SubjectPublicKeyInfo  ::=  SEQUENCE  {
        algorithm           AlgorithmIdentifier,
        subjectPublicKey    BIT STRING  }

    Extensions  ::=  SEQUENCE SIZE (1..MAX)  OF Extension
Extension  ::=  SEQUENCE  {
        extnID      OBJECT IDENTIFIER,
        critical    BOOLEAN DEFAULT FALSE,
        extnValue   OCTET STRING  }
```

证书的扩展项应符合 YD/T 1322.3-2004 的 8.2 和 RFC 3770 第二章和第三章中的规定。

10 属性证书格式

本标准中使用的数字证书格式应符合 IETF RFC 3281 及 RFC 3770 中的相应规定，同时根据实施者的具体情况选择使用。在 RFC 3281 中定义的属性证书基本项的 ASN.1 表示如下:

```
AttributeCertificate ::= SEQUENCE {
        acinfo                  AttributeCertificateInfo,
        signatureAlgorithm      AlgorithmIdentifier,
        signatureValue          BIT STRING
}

AttributeCertificateInfo ::= SEQUENCE {
        Version                 AttCertVersion -- version is v2,
        Holder                  Holder,
        Issuer                  AttCertIssuer,
        Signature               AlgorithmIdentifier,
        SerialNumber            CertificateSerialNumber,
        AttrCertValidityPeriod  AttCertValidityPeriod,
        Attributes              SEQUENCE OF Attribute,
        IssuerUniqueID          UniqueIdentifier OPTIONAL,
        Extensions              Extensions OPTIONAL
}

AttCertVersion ::= INTEGER { v2 ( 1 ) }
Holder ::= SEQUENCE {
        baseCertificateID   [0] IssuerSerial OPTIONAL,
                -- 签发者和持有者的公共密钥证书序列号
        entityName          [1] GeneralNames OPTIONAL,
                -- 提出者或角色名
        objectDigestInfo    [2] ObjectDigestInfo OPTIONAL
                -- 用于直接认证持有者，例如，可执行的
}

ObjectDigestInfo ::= SEQUENCE {
        digestedObjectType  ENUMERATED {
                publicKey           ( 0 ),
                publicKeyCert       ( 1 ),
                otherObjectTypes    ( 2 ) },
                        -- otherObjectTypes MUST NOT
```

```
                    -- be used in this profile
    otherObjectTypeID    OBJECT IDENTIFIER OPTIONAL,
    digestAlgorithm      AlgorithmIdentifier,
    objectDigest         BIT STRING
}

AttCertIssuer ::= CHOICE {
    v1Form    GeneralNames,  --在该轮廓中不必使用

    v2Form    [0] V2Form     -- 仅 v2
}

V2Form ::= SEQUENCE {
    issuerName              GeneralNames      OPTIONAL,
    baseCertificateID       [0] IssuerSerial  OPTIONAL,
    objectDigestInfo        [1] ObjectDigestInfo  OPTIONAL
      -- 在该轮廓中不必出现签发者名字
      -- 在该轮廓中不必出现 baseCertificateID 和 objectDigestInfo
}

  IssuerSerial  ::=  SEQUENCE {
    issuer          GeneralNames,
    serial          CertificateSerialNumber,
    issuerUID       UniqueIdentifier OPTIONAL
}

AttCertValidityPeriod  ::= SEQUENCE {
    notBeforeTime     GeneralizedTime,
    notAfterTime      GeneralizedTime
}

Attribute ::= SEQUENCE {
     type         AttributeType,
     values       SET OF AttributeValue
       -- 至少需要一个值
}
```

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType

11 设备要求

在利用通信网络进行通信时，为保证通信网络和通信本身的安全，网络设备之间以及终端与网络设备之间应存在相互信任关系。在本标准中采用基于数字证书的认证来实现这种信任关系。

11.1 接入认证代理

根据用户终端接入网络的接入方式的不同，接入认证代理可以采用不同的设备，如 NAS、以太网络交换机等。这些设备除具有其设备本身的相关的功能外，为支持基于数字证书的访问控制，还需要满足如下一些要求：

1）支持扩展的 EAP 和 AAA 协议，Radius 或 Diameter。

2）具有访问属性认证中心和业务管理系统的功能（选用）。

11.2 用户终端设备要求

用户终端除满足其自身应用的要求外，为支持基于数字证书的认证方式，需要满足如下要求：

1）支持 PKI 数字证书机制，本标准中规定的数字证书格式。

2）具有存放证书并根据证书进行认证的功能。

3）支持 EAP 协议。

11.3 认证服务器要求

认证服务器需满足如下要求：

1）支持基于数字证书的认证，支持 PKI 数字证书机制。

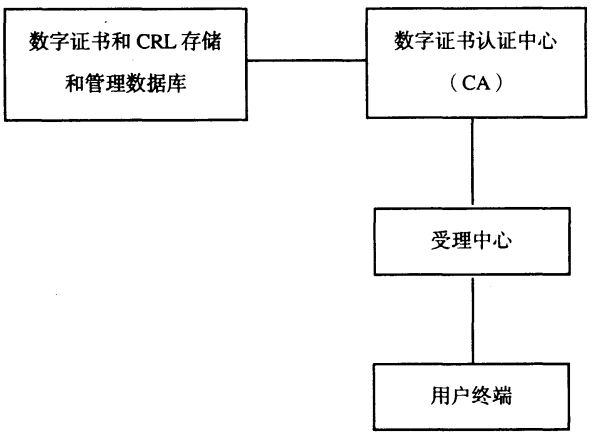
2）具有与 CA 的逻辑接口，可利用 CA 提供的服务确定用户所提交的数字证书的有效性。

3）支持 EAP 协议。

附 录 A
（资料性附录）
数字证书认证系统

A.1 数字证书认证系统的结构

数字证书认证系统主要由认证中心、受理中心、数字证书和CRL存储和管理数据库组成。其组成框图如图A.1所示。



图A.1 数字证书认证系统的结构

体系结构中各部分的功能：

1）终端实体：终端实体可以是用户或可以为其发布证书的其他类型实体。包括被签发证书并且可以签署数字文件和加密文件的公共密钥持有者和通过被信任的CA的已知公共密钥证实数字签名和它们的证书路径的客户机。

2）认证中心：负责发放、管理、认证和注销公共密钥证书的实体。

3）受理中心：负责确定公共密钥和证书持有者身份和其他属性之间的联系的机构。

4）证书和CRL存储和管理：负责存储已经签发的证书和已经废弃的证书列表并负责对证书和CRL进行增删改等管理操作。

A.2 基于数字证书的宽带用户访问控制系统与数字证书认证系统之间的对应关系

公众IP网络上基于数字证书的宽带用户接入认证系统，可以看作为某一职能认证系统的一个应用系统或是一个专门进行宽带用户接入认证的认证系统。图1中的终端实体可以是用户终端；受理中心可以是公众IP网络接入认证系统中的用户管理系统中的业务受理中心或用户注册服务中心；认证中心可以是设在某个省的一个专用认证中心或是利用其他认证中心代为完成认证中心的功能。在认证系统应用于公众IP网络的用户认证时，用户需要将其所持有的数字证书首先发送到其所连接到的接入认证代理。为此在组建基于数字证书对用户进行接入认证的公众IP网络时，需要对接入认证代理进行必要的功能扩展。

A.3 数字证书认证中心

数字证书认证中心是基于PKI技术的安全认证系统。在本标准中不具体规定组建数字证书认证中心的相关技术要求，本标准的实施者可选择采用由第三方组建的认证中心，也可以根据IETF工作组制定的一系列标准来建设专用的数字证书认证中心。

附 录 B
（资料性附录）
属性证书认证系统

B.1 属性证书认证系统的结构

属性证书认证系统是基于特权管理基础设施 PMI 的负责发布属性证书并对属性证书进行管理的系统。其结构如图 B.1 所示。

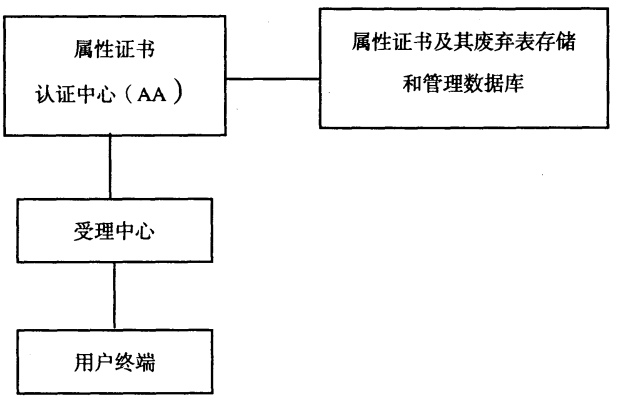


图 B.1 属性证书认证中心的构成

属性证书认证中心与数字证书认证中心一样由用户终端、受理中心和属性认证中心组成。主要完成如下一些功能：

1）根据受理中心所提供的用户有效数字证书的内容以及用户拟申请授权的业务信息为用户生成属性证书。

2）在认证服务器完成对用户数字证书有效性的认证后向认证服务器提供用户的属性证书，以便认证服务器确定是否向用户提供其所申请的业务。

B.2 本标准规定的系统与属性证书认证系统之间的关系

属性证书认证系统是遵循 PMI 技术而组建的认证体系，本标准中用户属性证书与网络可为用户提供的业务种类以及用户申请的业务直接相关。考虑到简化用户申请业务的手续和步骤，在本标准中业务管理系统的受理中心具有属性认证中心中受理中心的职能，同时作为属性认证系统的一部分。

B.3 属性证书认证系统的技术要求

组建属性认证系统时应遵循 ITU-T 建议 X.509 已经 IETF PKIX 工作组所指定的相关标准。

附 录 C
（资料性附录）
业务管理子系统

C.1 业务管理子系统的组成

业务管理子系统主要由业务受理中心、业务生成和管理部分、资源管理和分配部分以及管理部分组成。组成框图如图 C.1 所示。

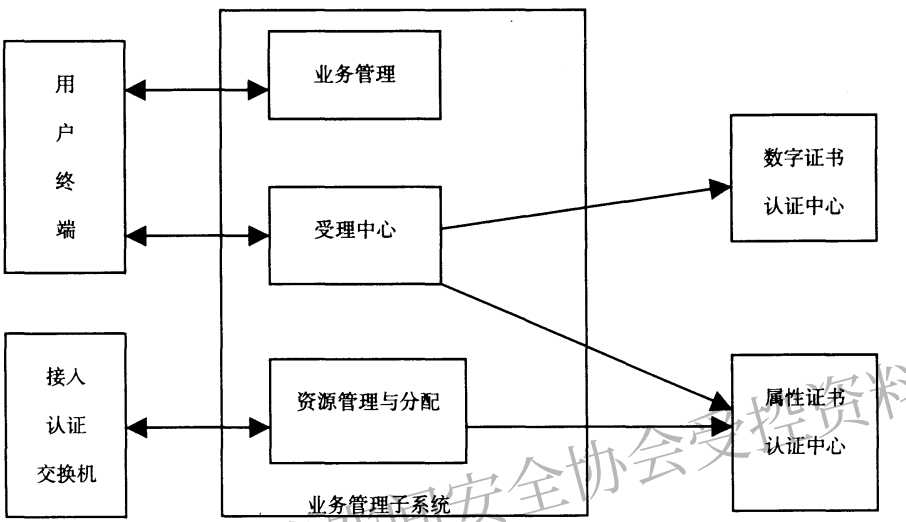


图 C.1 业务管理子系统组成框图

C.2 各组成模块的功能要求

C.2.1 受理中心

在具体实现时，受理中心可作为数字证书认证中心和属性证书认证中心的注册中心。受理中心主要完成如下一些功能：

1）接受用户申请的业务开通申请，并代替用户向数字认证中心和属性认证中心申请数字证书和属性证书。

2）将用户所提交的数字证书发送到业务管理部分，并将用户开通信息（包括用户的数字证书序列号、用户的属性证书等）存储到数据库中。

C.2.2 资源管理与分配

资源管理与分配主要完成以下一些功能：

1）对网络资源（网络带宽、IP 地址数、端口情况）进行管理包括网络所有资源、正在使用的资源情况。

2）若用户所提交的数字证书有效，根据用户的属性证书中用户所申请业务的情况以及用户以往使用情况（主要包括用户的缴费情况以及对该用户所实施的计费策略）为用户分配 IP 地址以及相应的网络资源，同时通知接入交换机扫描交换机端口，并完成与对应的用户 MAC 地址的端口的连接。

3）将用户接入信息（包括用户数字证书信息、用户的 MAC 地址以及用户的 IP 地址信息等）通知计费系统开始对用户实施计费。

C.2.3 业务管理部分

业务管理部分完成以下一些功能：

1）管理用户使用业务情况。

2）管理用户计费及缴费情况。

附 录 D
（资料性附录）
证书发放和存放要求

D.1 证书种类

证书包括数字证书和属性证书。

数字证书是由用户在进行业务申请时委托受理中心向数字证书认证中心申请代表用户身份，并在用户连接到网络使用网络业务时向接入认证交换机提交来证明自身身份。

属性证书是根据用户所申请的业务种类和缴费方式，由受理中心代表用户向属性证书认证中心申请，当用户接入网络时由用户交换机到属性证书认证中心查询并根据属性证书及网络目前所有的资源情况为用户建立连接。

D.2 证书的发放对象

数字证书的发放对象为用户终端设备。

属性证书的发放对象是用户终端或集团用户。

D.3 证书的发放方式

证书的发放可以采用在线方式和离线方式。

在线方式是指用户或受理中心通过网络向证书认证中心申请，证书认证中心通过网络将证书传送到用户。

离线方式是指根据用户的申请将所生成的证书直接存储到存储媒体（包括软盘、USB 等）来进行发放的方式。

D.4 证书的存放方式

用户申请并使用的数字证书可存储在软盘/USB 中或存储在用户终端中。

中华人民共和国
通信行业标准
公众IP网络安全要求
——基于数字证书的访问控制
YD/T 1614-2007
*
人民邮电出版社出版发行
北京市崇文区夕照寺街14号A座
邮政编码：100061
北京新瑞铭印刷有限公司

*
开本：880×1230　1/16　　2007年6月第1版
印张：2　　2007年6月北京第1次印刷
字数：52千字
ISBN 978-7-115-1410/07-73
定价：15元
本书如有印装质量问题，请与本社联系　电话：(010)67114922