ICS 35.040
CCS L 80

团　体　标　准

T/WAPIA 013.4—2025

信息安全技术 数字证书管理 第4部分：证书撤销

Information security technology - Digital certificate management - Part 4: Certificate revocation

2025-12-10 发布　　2025-12-10 实施

中关村无线网络安全产业联盟　发布

版权声明

目　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是T/WAPIA 013《信息安全技术 数字证书管理》的第4部分。T/WAPIA 013已经发布了以下部分：

— 第 2 部分：证书存储和使用；
— 第 3 部分：证书颁发；
— 第 4 部分：证书撤销；
— 第 5 部分：证书格式。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中关村无线网络安全产业联盟与工业和信息化部宽带无线IP标准工作组联合提出。

本文件由中关村无线网络安全产业联盟无线网络安全标准化工作委员会归口。

本文件起草单位：北京数字认证股份有限公司、中关村无线网络安全产业联盟、南方电网数字电网科技（广东）有限公司、广州莲雾科技有限公司、深圳市智开科技有限公司、西安芯语慧联信息科技有限公司、西安西电捷通无线网络通信股份有限公司、无线网络安全技术国家工程研究中心、工业和信息化部宽带无线IP标准工作组、北京华信傲天网络技术有限公司、中能融合智慧科技有限公司。

本文件主要起草人：侯鹏亮、于双双、辛文、李忠、黄振海、张璐璐、刘婷、郑骊、简练、刘剑昕、周园、王立华、李仲斌、林加毅、韩曦、吴泽雄、刘高锦、童伟刚、张国强、潘琪、刘图、任亮、齐飞、鲍树楠、沙学松、张昊公。

引　言

在安全无线局域网中，可能会出现各种原因导致实体证书需要提前失效，如私钥泄露、身份信息变化等。为了确保数字证书在需要时能够及时失效，防止被恶意使用，证书撤销技术标准应运而生。本文件将详细介绍证书撤销的相关技术，包括证书撤销的流程、机制以及撤销信息的发布方式等，为网络安全领域的研究人员和从业者提供参考和指导。

T/WAPIA 013拟由五个部分构成：

— 第1部分：总则。目的在于确立数字证书管理总体原则和基本要求等相关内容。

— 第2部分：证书存储和使用。目的在于规范数字证书及私钥在独立安全媒体中的安全存储、安全分发和安全使用相关内容。

— 第3部分：证书颁发。目的在于规范数字证书申请、审核、签发、验证等相关内容。

— 第4部分：证书撤销。目的在于规范数字证书撤销流程等相关内容。

— 第5部分：证书格式。目的在于规范数字证书基本结构及各数据项内容。

本文件实施过程中，涉及到密码技术的具体应用时，适用密码算法相关国家标准、行业标准，以及国家密码管理主管部门的有关规定。

信息安全技术 数字证书管理 第4部分：证书撤销

1 范围

本文件确立了证书撤销的条件与过程，规定了终端实体证书撤销的状态发布与更新要求、CRL格式要求和撤销后的处理要求。

本文件适用于终端设备STA和无线接入点AP场景下的证书撤销管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

T/WAPIA 013.5—2024 信息安全技术 数字证书管理 第5部分：证书格式

3 术语和定义

本文件没有需要界定的术语和定义。

4 缩略语

AC：接入点控制器（ap controller）
AP：接入点（access point）
AS：鉴别服务器（authentication server）
CIS：证书签发服务器（certificate issuing server）
CRL：证书撤销列表（certificate revocation list）
DER：可分辨编码规则（distinguished encoding rules）
HTTPS：安全超文本传输协议（hyper text transfer protocol secure）
JSON：javascript对象表示法（javascript object notation）
MAC：媒体访问控制（medium access control）
POST：持久化覆盖式状态传输（persistent overwrite transfer state）
STA：站点（station）
UTF-8：UCS变换形式8（UCS transformation format 8）

5 撤销条件与过程

5.1 撤销条件

符合下列情形之一的，管理员应将证书撤销：

a) 用户身份信息发生改变；
b) 私钥不慎遗失或被非法泄露；
c) 未经授权擅自将证书用于非许可的用途；
d) 证书被标记为无效。

5.2 撤销过程

证书撤销流程见图1。

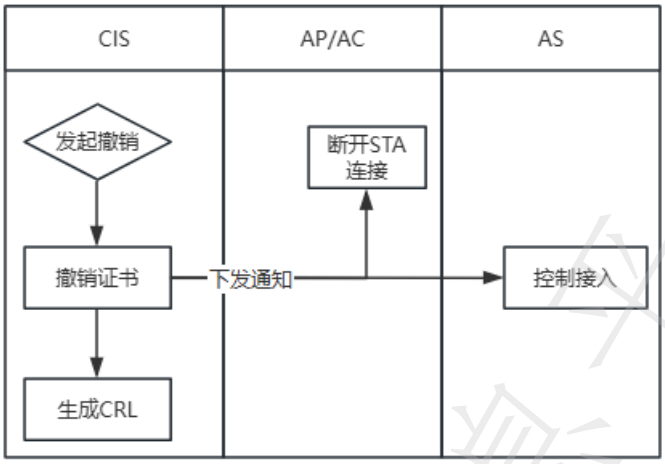

图1 证书撤销流程

证书撤销步骤如下。

a）发起撤销：某个STA（或AP）的证书需撤销时，管理员发起撤销流程。

b）撤销证书：CIS将证书状态置为无效。

c）下发通知：CIS向与被撤销证书的STA（或AP）关联的AP（或AC）及AS下发证书撤销通知。

d）断开STA连接：AP（或AC）收到撤销通知后，应断开STA（或AP）相关的网络连接及通信会话。

e）控制接入：被撤销的证书不能接入网络。

f）生成CRL：将撤销的证书信息更新至CRL中。

5.3 撤销通知接口

5.3.1 接口详情

接口详情如下。

a）传输协议：HTTPS。

b）端口：3830。

c）接口地址：/ap/offline。

d）请求方式：POST。

e）请求格式：JSON。

f）编码方式：UTF-8。

5.3.2 请求参数

撤销通知接口请求参数描述见表 1。

表 1 撤销通知接口请求参数描述

参数名称	参数类型	长度	是否必填	备注
type	int	1	是	1：AP； 2：STA
snum	String	30	否	撤销的证书序列号（AP 设备证书被撤销时此项必填）
mac	String	17	否	撤销证书的 MAC 地址（STA 设备证书被撤销时此项必填）

表 1 撤销通知接口请求参数描述（续）

参数名称	参数类型	长度	是否必填	备注
sign	String	256	是	采用 CIS 证书的私钥对 type、snum、mac 字段拼接值（type+snum+mac）进行签名，本字段为签名值 DER 的 base64 编码

5.3.3 请求示例

示例：

```
{
    "type ": "2",
    "snum": "4563434",
    "mac": "00:0B:C0:03:5F:8F",
    "sign": ""
}
```

5.3.4 接口响应

撤销通知接口响应参数描述见表 2。

表 2 撤销通知接口响应参数描述

参数名称	参数类型	长度	备注
code	String	10	状态码： 200：成功； 201：失败
msg	String	100	状态说明信息

5.3.5 响应示例

示例：

```
{
    "code": 201,
    "msg": "通知失败"
}
```

6 撤销状态发布与更新要求

证书撤销后 CIS 应更新证书状态为无效，并在 1 h 内将撤销的证书信息更新至 CRL 中，CIS 应支持 CRL 的下载，必要时应支持 CRL 的网络发布。

7 CRL 格式要求

CRL格式应符合T/WAPIA 013.5—2024第7章。

8 撤销后的处理要求

当证书被执行撤销，该证书即失效，不应再使用。

证书撤销后应采取以下处理措施：

a）在1 h内更新CRL；

b）设备断开网络；

c）限制使用已撤销状态的证书进行鉴别；

d）CIS应记录证书撤销日志。