

ICS 35.100.70  
L 79



# 中华人民共和国国家标准

GB/T 19714—2005

GB/T 19714—2005

## 信息技术 安全技术 公钥基础设施 证书管理协议

Information technology—Security technology—Internet public key  
infrastructure—Certificate management protocol

中华人民共和国  
国家标准  
信息技术 安全技术 公钥基础设施  
证书管理协议  
GB/T 19714—2005

\*

中国标准出版社出版发行  
北京复兴门外三里河北街16号  
邮政编码:100045

网址 www.bzcs.com

电话:68523946 68517548

中国标准出版社秦皇岛印刷厂印刷

各地新华书店经销

\*

开本 880×1230 1/16 印张 4 字数 119 千字

2005年8月第一版 2005年8月第一次印刷

\*

书号:155066·1-23067 定价 24.00 元

如有印装差错 由本社发行中心调换

版权专有 侵权必究

举报电话:(010)68533533



GB/T 19714-2005

2005-04-19 发布

2005-10-01 实施

中华人民共和国国家质量监督检验检疫总局  
中国国家标准化管理委员会 发布

附录 G  
(资料性附录)

用于 E-MAIL 或者 HTTP 的 MIME 类型

MIME 类型

MIME 媒体类型名字: application

MIME 图标子类型名字: pkixcmp

编码注意事项:

内容会包含任意的八位字节值(对 PKI 消息的 ASN.1 DER 编码,与在 IETF PKIX Working Group specifications 中定义的一样)。采用 MIME e-mail 时需要 base64 编码;采用 HTTP 时不需要编码。

安全注意事项:

本 MIME 类型用于在 PKI 实体中传输 Public-Key Infrastructure(PKI) 消息。消息由 IETF PKIX 工作组来定义,用于建立和维护互联网 X.509 PKI。如果 PKI 消息本身得到了 PKIX 规范中所定义的保护,那么在这一级别中不要求采用特定的安全机制。

使用本媒体类型的应用软件:

应用使用证书管理、操作或者辅助的协议(IETF PKIX 工作组定义的),通过 E-Mail 或者 HTTP 来发送 PKI 消息的应用软件。

目 次

前言 ..... III

引言 ..... IV

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 3

5 PKI 管理概述 ..... 3

5.1 PKI 管理模型 ..... 3

5.2 PKI 实体的定义 ..... 3

5.3 PKI 管理要求 ..... 5

5.4 PKI 管理操作 ..... 5

6 前提与限制 ..... 7

6.1 终端实体初始化 ..... 7

6.2 初始注册/认证 ..... 7

6.3 私钥拥有证明 ..... 9

6.4 根 CA 的更新 ..... 10

7 数据结构 ..... 12

7.1 PKI 消息综述 ..... 12

7.2 公共数据结构 ..... 16

7.3 与操作相关的数据结构 ..... 20

8 必需的 PKI 管理功能 ..... 24

8.1 根 CA 初始化 ..... 24

8.2 根 CA 密钥更新 ..... 24

8.3 下级 CA 初始化 ..... 24

8.4 CRL 产生 ..... 24

8.5 PKI 信息请求 ..... 24

8.6 交叉认证 ..... 24

8.7 终端实体初始化 ..... 25

8.8 证书请求 ..... 26

8.9 密钥更新 ..... 26

9 传输 ..... 26

9.1 基于文件的协议 ..... 26

9.2 直接基于 TCP 的管理协议 ..... 26

9.3 基于 E-mail 的管理协议 ..... 27

9.4 基于 HTTP 的管理协议 ..... 27

附录 A(资料性附录) RA 存在的原因 ..... 28

附录 B(规范性附录) 必选的 PKI 管理消息结构 ..... 29

附录 C(规范性附录) 可选的 PKI 管理消息结构 ..... 36

附录 D(资料性附录) 请求消息行为说明 ..... 42  
 附录 E(资料性附录) 使用“口令短语” ..... 43  
 附录 F(规范性附录) “可编译”的 ASN.1 模块..... 45  
 附录 G(资料性附录) 用于 E-MAIL 或者 HTTP 的 MIME 类型 ..... 56  
 参考文献 ..... 57

```

    checkAfter      INTEGER,
-- 以秒为单位的时间
    reason          PKIFreeText OPTIONAL
  }

```

END