ICS 35.100.70
L 79

中华人民共和国国家标准化指导性技术文件

GB/Z 19717—2005

基于多用途互联网邮件扩展(MIME)的安全报文交换

Secure message interchange based on Multipurpose Internet Mail Extensions

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

目　　次

前　言

本指导性技术文件主要参照 Internet 工程任务组提出的 RFC 2630 密码报文语法、RFC 2633 S/MIME 报文规范 第 3 版和 RFC 2634 增强的 S/MIME 安全服务制定的。

本指导性技术文件的附录 A 是资料性附录。

本指导性技术文件由中华人民共和国信息产业部提出。

本指导性技术文件由全国信息安全技术标准化技术委员会归口。

本指导性技术文件起草单位：中国电子技术标准化研究所。

本指导性技术文件主要起草人：吴志刚、赵菁华、王颜尊。

本指导性技术文件仅供参考。

引　言

Internet 的电子邮件在传输中广泛使用简单邮件传输协议(即 SMTP),而 SMTP 却未提供加密服务。攻击者可在邮件传输中截获数据,并能将邮件中的文本格式、非文本格式的二进制数据(如:.exe 文件)进行轻松地还原。Internet 电子邮件面临着各种安全威胁(如信息泄露、冒充身份等)。

安全电子邮件能够提供信息加密、身份鉴别、内容完整性、机密性及抗抵赖性等安全服务。目前,Internet 工程任务组研究制定的安全多用途互联网邮件扩展(S/MIME)规范已成为安全电子邮件的重要支撑标准。S/MIME 系列规范主要采用单向散列算法和公开密钥基础设施(PKI)来实现数据加密和数字签名,从而保证邮件的安全性。

本指导性技术文件给出了 S/MIME 系列规范的关键内容,便于对 S/MIME 系列规范的深入分析及相关产品的开发。

本指导性技术文件凡涉及密码相关内容,按国家有关法规实施。

本指导性技术文件中所引用的 MD5、SHA-1、DSS、RSA、DES、RC2、DH 密码算法等均为举例说明。

基于多用途互联网邮件扩展(MIME)的安全报文交换

1 范围

本指导性技术文件阐述了安全发送和接收多用途互联网邮件扩展(MIME)数据的基本方法(即安全多用途互联网邮件扩展,S/MIME)。该方法基于广泛使用的多用途互联网邮件扩展协议(MIME),向各种 Internet 报文应用提供鉴别、报文的完整性、抗抵赖性、机密性等多种安全服务。传统的邮件用户代理使用该方法可以向所发送的报文增加各种加密服务,并能够有效处理所收报文中的加密服务。本指导性技术文件还描述了 S/MIME 的增强安全服务。

本指导性技术文件不限于电子邮件,它还可以用于任何传输 MIME 数据的传输机制(如超文本传输协议,HTTP)。该规范利用了 MIME 面向对象的特点,使得在各种传输系统中能够交换安全报文。

2 规范性引用文件

下列文件中的条款通过本指导性技术文件的引用而成为本指导性技术文件的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本指导性技术文件,然而,鼓励根据本指导性技术文件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指导性技术文件。

RFC 2045 多用途 Internet 邮件扩展(MIME) 第 1 部分 Internet 报文体的格式

RFC 2630 密码报文语法

RFC 2633 S/MIME 报文规范 第 3 版

RFC 2634 增强的 S/MIME 安全服务

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本指导性技术文件。

3.1.1

证书 certificate

采用数字签名将实体的可辨别名与公开密钥捆绑起来的类型。

3.1.2

接收代理 receiving agent

一种软件,它解释并处理 S/MIME CMS 对象及含有 CMS 对象的 MIME 主体部分。

3.1.3

发送代理 sending agent

一种软件,它创建 S/MIME CMS 对象和创建含有 CMS 对象的 MIME 主体部分。

3.1.4

多用途互联网邮件扩展 Multipurpose Internet Mail Extensions(MIME)

MIME 容许以下格式文档作为报文:

a) 非 ASCII 码的字符集的文本报文体;

b) 非文本报文体的不同格式的扩展集;