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

GB/Z 19717—2005

中华人民共和国
国家标准化指导性技术文件
基于多用途互联网邮件扩展(MIME)的
安全报文交换
GB/Z 19717—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.bzcbs.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 1.5　字数 37 千字
2005年7月第一版　2005年7月第一次印刷
*
书号:155066·1-23060　定价 14.00 元

GB/Z 19717-2005

```
MLData ::= SEQUENCE {
  mailListIdentifier EntityIdentifier,
  expansionTime GeneralizedTime,
  mlReceiptPolicy MLReceiptPolicy OPTIONAL }

EntityIdentifier ::= CHOICE {
  issuerAndSerialNumber IssuerAndSerialNumber,
  subjectKeyIdentifier SubjectKeyIdentifier }

MLReceiptPolicy ::= CHOICE {
  none [0] NULL,
  insteadOf [1] SEQUENCE SIZE (1..MAX) OF GeneralNames,
  inAdditionTo [2] SEQUENCE SIZE (1..MAX) OF GeneralNames }
```

——签字证书属性定义(Signing Certificate Attribute Definition)

```
SigningCertificate ::=   SEQUENCE {
    certs          SEQUENCE OF ESSCertID,
    policies       SEQUENCE OF PolicyInformation OPTIONAL
}

id-aa-signingCertificate OBJECT IDENTIFIER ::= { iso(1)
    member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
    smime(16) id-aa(2) 12 }

ESSCertID ::=   SEQUENCE {
    certHash                 Hash,
    issuerSerial             IssuerSerial OPTIONAL
}

Hash ::= OCTET STRING -- SHA1 hash of entire certificate

IssuerSerial ::= SEQUENCE {
    issuer                   GeneralNames,
    serialNumber             CertificateSerialNumber
}

END -- of ExtendedSecurityServices
```


目　　次

```
id-aa-msgSigDigest OBJECT IDENTIFIER ::= { iso(1) member-body(2)
    us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 5}
```

——签字内容参考属性(Signed Content Reference Attribute)

```
ContentReference ::= SEQUENCE {
  contentType ContentType,
  signedContentIdentifier ContentIdentifier,
  originatorSignatureValue OCTET STRING }

id-aa-contentReference    OBJECT IDENTIFIER ::= { iso(1) member-body(2)
    us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 10 }
```

——eSSSecurityLabel 语法(Syntax of eSSSecurityLabel)

```
ESSSecurityLabel ::= SET {
  security-policy-identifier SecurityPolicyIdentifier,
  security-classification SecurityClassification OPTIONAL,
  privacy-mark ESSPrivacyMark OPTIONAL,
  security-categories SecurityCategories OPTIONAL }

id-aa-securityLabel OBJECT IDENTIFIER ::= { iso(1) member-body(2)
    us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 2}

SecurityPolicyIdentifier ::= OBJECT IDENTIFIER

SecurityClassification ::= INTEGER {
  unmarked (0),
  unclassified (1),
  restricted (2),
  confidential (3),
  secret (4),
  top-secret (5) } (0..ub-integer-options)

ub-integer-options INTEGER ::= 256

ESSPrivacyMark ::= CHOICE {
    pString        PrintableString (SIZE (1..ub-privacy-mark-length)),
    utf8String     UTF8String (SIZE (1..MAX))
}
```


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。