ICS 33.040.70
M 39

中华人民共和国国家标准

GB/T 17788—1999
eqv ITU-T T.36:1997

三类传真终端的安全能力

Security capabilities for use with group 3 facsimile terminals

1999-07-13 发布　　2000-01-01 实施

国家质量技术监督局　发布

目　　次

前　言

本标准等效采用ITU-T 建议 T.36《三类传真终端的安全能力》(1997 年版本)和 ITU-T 建议 T.36 增补 1(1999 年版本)。

本标准规定了两个独立的可用于传真文件安全传送的技术解决方案。这两个方案分别基于 HKM/HFX40 算法和 RSA 算法。使用此两种算法可为三类文件传真的安全传送提供如下能力:

——通信双方身份的相互认证,保证正确地将传真报文传送到指定接收终端;

——接收确认,接收终端向发送终端认可已接收到传真报文;

——报文完整性证实,接收终端在查证所接收到报文的完整性的基础上向发送终端返送报文完整性确认或否认信息;

——报文加密,使用秘密密钥对传真报文加密以防止报文内容的丢失。

在本标准的起草过程中,纠正了 ITU-T 建议 T.36(1997 年版本)中的一些编辑上的错误,同时增加了 ITU-T 建议 T.36 增补 1(1999 年版本)中有关人控模式的相关内容。

本标准的附录 A、B、C、D、E 均为标准的附录。

本标准由中华人民共和国邮电部提出。

本标准由邮电部电信科学研究规划院归口。

本标准起草单位:电信传输研究所。

本标准起草人:聂秀英、林海、胡毅红、崔进水。

ITU-T 前言

本建议规定了两个独立的可用于传真文件安全传送的技术解决方案。这两个技术方案分别基于HKM/HFX40 算法和 RSA 算法。

附件 A 包含与 HKM/HFX40 算法相关的信息。

附件 B 包含于 RSA 算法相关的信息。

附件 C 描述为传真终端提供秘密秘钥管理能力的 HKM 系统的使用。使用两个主要的规程来描述能力规定：

——在实体 X 和 Y 之间单向注册的规程(procREGxy)；和

——在实体 X 和 Y 之间秘密传送秘钥的规程(procSTKxy)。

附件 D 包括使用 HFK40 加密系统提供传真终端报文安全的规程。

为提供传送的传真报文的完整性，作为报文加密的替代以选择的或预编程的形式，附件 E 以其使用的方式描述 HFX-40 散列算法、必要的计算和在传真终端之间的互换信息。

附件 E 描述 HFX40-1 散列算法的使用，需要的计算，为发送的传真信息提供完整性在两个传真终端之间的信息的交换，作为加密信息的选择或预置项。

ITU-T 建议 T.36 由 ITU-T 第 8 研究组(1997—2000)起草并于 1997 年 7 月 2 日按照 WTSC 第 1 号决议的程序批准。

中华人民共和国国家标准

三类传真终端的安全能力

GB/T 17788—1999
eqv ITU-T T.36:1997

Security capabilities for use with group 3 facsimile terminals

1 范围

本标准规定了两个独立的可用于传真文件安全传送的技术解决方案：

在ITU-T建议T.30和T.30增补1(1997年版)附录A和附录G中描述的基于HKM/HFX40算法的解决方案；

在ITU-T建议T.30和T.30增补1(1997年版)附录B和附录H中描述的基于RSA算法的解决方案。

本标准可为安全传真终端的研究、设计、生产和使用提供参考和技术依据。

2 引用标准

下列标准所包含的条文，通过在本标准中引用而构成本标准的条文。在本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

ITU-T建议T.30(1996)和T.30增补1(1997) 公用电话交换网上文件传真传输规程

3 缩略语

本标准使用下列缩略语：

ASCII	信息互换用美国标准码
B(n)	基值(n)
ESH	经加密和扰码的均匀散列(24位十进制数)
ESIM	经加密和扰码后的完整性消息(12位十进制数)
ESSC	经加密和扰码后的秘密询问密钥
ESSK	经加密和扰码后的秘密密钥(12位十进制数)
ESSR	经加密和扰码后的秘密响应密钥
ESSS	经加密和扰码后的秘密会话密钥
HKM	HKM算法
HKM+1	HKM加密算法
HKM−1	HKM解密算法
HKMD+1	用HKM算法双重加密
HKMD−1	用HKM算法双重解密
IDx	X的传真标识码(传真电话号码)的最后6位数
IDy	Y的传真标识码(传真电话号码)的最后6位数
IM	用于确认或否认接收报文完整性的完整性信息(12位十进制数)

国家质量技术监督局1999-07-13批准　　2000-01-01实施