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

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
*
中国标准出版社出版
北京复兴门外三里河北街16号
邮政编码:100045
电　　话:68522112
中国标准出版社秦皇岛印刷厂印刷
新华书店北京发行所发行　各地新华书店经售

*
开本 880×1230　1/16　印张 2½　字数 73 千字
1999年11月第一版　1999年11月第一次印刷
印数 1—1 000
*
书号:155066·1-16257　定价 18.00 元
*
标 目 391—27

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。

目　　次

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

IMy	由 Y 生成的完整性消息，用以确认或否认接收报文的完整性(12 位十进制数)
ITU-T	国际电信联盟—电信标准化部
mod n	模 n 运算
MPx	X 的互原语。16 位十进制数，只能由 X 生成。MPx 是由 X 使用 HKM 算法通过从 UINx、UCNx、IDx 和 IDy 形成的原语生成的。
MPy	Y 的互原语
OT	一次性密钥。由双方用户约定的 6 至 64 位十进制数
OTx	X 在 Y 处注册时 X 第一次使用的一次性密钥
OTy	Y 第一次使用的一次性密钥，当 Y 发起 Y 在 X 处注册以完成相互注册时，它可以与 OTx 相同或不同
PH	报文的均匀散列(24 位十进制数)
P(n)	相值(n)
Primitive（原语）	由 UIN 和 UCN 形成的 64 位数字的复合数
ProcREGxy	X 和 Y 之间注册的规程
ProcSTKxy	从 X 到 Y 安全传输秘密密钥的规程
PRS	伪随机序列
RCN	注册的密码数(16 位十进制数)
RNCn	与 SCn 相关联的非密随机数(4 位十进制数)
RNIM	与 IM 相关联的非密随机数(4 位十进制数)
RNK	当加密 SK 时，用来对 MPx 生成的原语提供变化的非密随机数(4 位十进制数)
RNSRn	与 SRn 相关联的非密随机数(4 位十进制数)
RNSSn	与 SSn 相关联的非密随机数(4 位十进制数)
SCn	第 n 个询问密钥(12 位十进制数)
SH	扰码的均匀散列(24 位十进制数)
SK	秘密密钥，它可以是 SCn、SRn、SSn 等(12 位十进制数)
SRn	第 n 个秘密响应密钥(12 位十进制数)
SS	用于 HFX40-I 完整性算法的秘密会话密钥(12 位十进制数)
SSK	扰码秘密密钥(12 位十进制数)
SSn	第 n 个秘密会话密钥。用于 HFX40 密码算法和/或散列(12 位十进制数)
SSx	由 X 生成的秘密会话密钥，用于 HFX40 密码算法(12 位十进制数)
TKx	传送密钥，由 X 生成的加密 MPx(16 位十进制数)
UCN	唯一加密数，例如，UCNx、UCNy。只有系统知道的 16 位十进制数
UIN	唯一标识码，例如，UINx、UINy。只有系统知道的 48 位十进制数
X	一个实体的名
x	标识拥有者身份或由 X 生成的后缀
XOR'd	异或
Y	第二个实体的名
y	标识拥有者身份或由 Y 生成的后缀

附 录 A
（标准的附录）
使用 HKM 和 HFX 体制的三类文件传真的安全传输规程

A1 引言

A1.1 本附录描述了三类文件传真终端使用 HKM 和 HFX 体制提供安全通信的规程。

A1.2 本附录的使用是选用的。

A1.3 ITU-T 建议 T.30 附录 A 或附录 G 中定义的误码纠错(适当的)是必备的。

A2 传真文件安全规程的概要

A2.1 HKM 和 HFX 体制为实体(终端或终端操作者)之间文件安全通信提供以下能力：

——实体间相互认证；

——建立秘密会话密钥；

——文件保密；

——接收确认；

——文件完整性确认或否认。

A2.2 功能

使用本标准附录 C 中定义的 HKM 体制来提供密钥管理。规定了三种规程：1) 注册模式(见 C4)；2) 安全模式(见 C5)；3) 人控模式(见 C7)。注册建立相互秘密并能为后续传输提供安全保障。在后续传输中，HKM 体制提供相互认证、用于文件保密和完整性的秘密会话密钥、接收确认和文件完整性确认或否认。

使用附录 D 中规定的 HFX40 密码算法提供文件保密。HFX40 密码算法使用 12 位十进制数字密钥，该密钥大约为 40 比特。

使用附录 E 中规定的体制提供文件完整性。附录 E 规定了包括相关联计算和报文交换的散列算法。

附 录 B
（标准的附录）
基于 RSA 算法的三类传真的安全方案

B1 引言

本附录基于 RSA 密码算法机制规定提供安全特征的机制。

本附录的使用是选用的。

B2 引用标准

——ISO/IEC 9796:1991 信息技术-安全技术-给出报文恢复的数字签名方案。

——RIVEST(R.L),SHAMIR(A),ADLEMAN(L):获得数字签名和公共密钥密码体制的方法，附录 A:RSA,CACM(ACM 的通信),21 卷，第 2 部分，120～126 页，1978。

——ISO/IEC CD10118-3(版本 2):1995,信息技术-安全技术-散列函数-第 3 部分:专用的散列函数。

——ISO/IEC JTC 1/SC 27 N1108：

· 在安全散列标准中描述的 SHA-1(安全散列算法)，FIPS(联邦信息处理标准)PUB 180-1，1995 年 4 月，来自美国 NIST(国家标准化研究院)的算法。

· MD-5(RFC 1321)。

——ISO/IEC 9979:1991 信息技术——安全技术——用于密码算法注册的规程。

B3 技术描述

本解决方案的完整描述见建议 T.30 的附录 H。

附 录 C
(标准的附录)
使用 HKM 密钥管理体制的文件传真安全传输规程

C1 范围

本附录规定用于传真终端的 HKM 密钥管理体制，以便能够安全地交换密钥。

HKM 密钥管理体制主要用于各种类型的专用传真终端，同样也可用于基于计算机的传真系统。

本附录描述使用 HKM 算法的两个主要规程，即 procREGxy 和 procSTKxy，可提供：

——相互认证(见 C5.3 和 C6)；

——使用 HFX40 密码算法提供报文保密(附录 D)；

——使用散列函数提供报文完整性(附录 E)；

——安全交换用于认证的询问密钥和响应密钥，以及用于报文保密或完整性的会话密钥(见 C5 和 C6)。

使用代数表示法帮助表示密钥管理协议和规程，见 C2。

HKM 体制基于使用 19 个系统质数。这些相同的 19 个质数也用于报文加密算法(在附录 D 中描述)和主要报文完整性散列算法(在附录 E 中描述)。但本附录不包括报文加密算法和主要报文完整性散列算法。

C6 中给出了计算举例，这些举例用于验证本附录的执行。

注：HKM 密钥管理体制受知识产权的保护；那些权利的所有者同意遵循 ITU-T 电信标准化局(TSB)的规章。细节可从 TSB 获得。

C2 约定

C2.1 概述

C2.2 中详述的代数表示法用于描述密钥管理协议和规程。

C2.2 符号

[]	将消息括以此括号
{}	将算法括以此括号
()	将原语括以此括号
⟨⟩	将要存储的信息括以此括号
><	将取出的存储信息括以此括号
&	无需改变其长度的融合或修改，例如 UCNx 和 IDx
RCNx>>>>>>	将 RCNx 送给 Y
>>>>>>RCNx	从 X 接收 RCNx

HKM+1	用 HKM 算法加密
HKM−1	用 HKM 算法解密
HKMD+1	用 HKM 算法双重加密
HKMD−1	用 HKM 算法双重解密

C3 用于传真终端的 HKM 算法描述

HKM 算法使用秘密的终端特定号码和其他的用户特定变量构成原语，此原语同加密密钥一起，使用模数运算为计算提供输入数据。秘密号码 UIN 和 UCN 由制造商或代理安全地存于传真终端中。不需要将它们与各种形式的系列号相互参照。

模数运算的模由存于终端中的 19 个特殊的质数集提供。

模数运算处理的输出是用于加密报文的长伪随机数序列(PRS)。

HKM 也可以用于不可逆模式，即，加密处理发生后不能执行其逆过程。

上面特性构成的密码基于两个规程，procREGxy 和 procSTKxy。

C6 中给出算法和特定质数的细节。

C4 注册模式

C4.1 在实体 X 和 Y 间注册的规程(procREGxy)

X 在 Y 处注册时，X 通过加密算法将 UINx 和 UCNx 与 IDx 和 IDy 组合起来生成不可逆的数。该形成的 16 位数为 MPx，使用 MPx 来加密和安全传送密钥，下面内容给出解释。

在注册传输之外的安全环境中，用户间协商一次性密钥(OT)。X 的用户选择注册模式，并输入 Y 的传真标识码(传真电话号码)。IDx 和 IDy 构成该算法使用的其他原语的基础。X 的用户还要输入 OTx。

X 通过 HKM+1 用 OTx 加密 MPx 以形成送给 Y 的 TKx。在 Y 处，输入 OTx，并使用 OTx 通过 HKM−1 解密 TKx 以恢复出 MPx。

Y 不存储 MPx，而是立即用经 IDx 和 IDy 修改的 UINy 和 UCNy 构成的原语，通过 HKM+1 算法加密 MPx 以形成 RCNy。Y 将 RCNy 送到 X 处存储。Y 不需要存储 RCNy，X 在下一次发起到 Y 的安全传输时将公开地把它送回给 Y。

两个终端可以隐式地验证它们自身的身份，因为 X 是唯一可生成与 Y 有关的 MPx 的终端，Y 是唯一可以从 RCNy 中恢复 MPx 的终端。

procREGxy 可用代数表示法表示：

X	Y
>UINx,UCNx<	>UINy,UCNy<
MPx=(UINx,UCNx & IDx & IDy){HKM+1}	
[UCNx & IDx & IDy]	
TKx=(OTx){HKM+1}[MPx]	
TKx>>>>>>	
	>>>>>>TKx
	MPx=(OTx){HKM−1}[TKx]
	RCNy=(UINy,UCNy & IDx & IDy){HKM+1}
	[MPx]
	RCNy>>>>>>
>>>>>>RCNy	
<RCNy>	

ProcREGxy 的描述和所有的计算举例在 C6.4 中给出。

C4.2 在实体 Y 和 X 间注册的规程(procREGyx)

为完成注册,Y 执行一个与 X 相同的规程 procREGyx,该规程建立 MPy 和 RCNx(Y 和 X 处的用户同意的 OTy 可以与在 procREGxy 期间使用的 OTx 相同或不同)。

ProcREGyx 可用代数表示法表示:

Y	X
	>UINx,UCNx<
>UINy,UCNy<	
MPy=(UINy,UCNy & IDy & IDx){HKM+1}	
[UCNy & IDy & IDx]	
TKy=(OTy){HKM+1}[MPy]	
TKy>>>>>>>	
	>>>>>>>TKy
	MPy=(OTy){HKM-1}[TKy]
	RCNx=(UINx,UCNx & IDy & IDx){HKM+1}[MPy]
	RCNx>>>>>>>
>>>>>>>RCNx	
<RCNx>	

C4.3 一次呼叫的注册规程

使用 ProcREGxy 和 ProcREGyx 的两个分离的注册过程可合并在一次呼叫中,以下用代数表示法示出,此例中该呼叫由 X 发起。

X	Y
>UINx,UCNx<	
	>UINy,UCNy<
MPx=(UINx,UCNx & IDx & IDy){HKM+1}	
[UCNx & IDx & IDy]	
TKx=(OTx){HKM+1}[MPx]	
TKx>>>>>>>	
	>>>>>>>TKx
	MPx=(OTx){HKM-1}[TKx]
	RCNy=(UINy,UCNy & IDx & IDy){HKM+1}[MPx]
	MPy=(UINy,UCNy & IDy & IDx){HKM+1}[UCNy & IDy & IDx]
	TKy=(OTy){HKM+1}[MPy]
	RCNy,TKy>>>>>>>
>>>>>>>RCNy,TKy	
<RCNy>	
MPy=(OTy){HKM-1}[TKy]	
RCNx=(UINx,UCNx & IDy & IDx){HKM+1}[MPy]	
RCNx>>>>>>>	
	>>>>>>>RCNx

<RCNx>

C4.4 注册认证

通过在X和Y之间提供询问/响应的交换，注册认证包括在X和Y之间注册的规程中。询问/响应使用在C5.1中描述的procSTKxy和procSTKyx。下例示出了使用代数表示法表示的一次呼叫中双向注册的规程。

X	Y
>UINx,UCNx<	>UINy,UCNy<
MPx=(UINx,UCNx & IDx & IDy){HKM+1} [UCNx & IDx & IDy]	
TKx=(OTx){HKM+1}{MPx}	
<SC0x> by procSTKxy=ESSC0x	
TKx,RNC0x,ESSC0x>>>>>>	
	>>>>>>TKx,RNC0x,ESSC0x
	MPx=(OTx){HKM−1}[TKx]
	RCNy=(UINy,UCNy & IDx & IDy){HKM+1} [MPx]
	MPy=(UINy,UCNy & IDy & IDx){HKM+1} [UCNy & IDy & IDx]
	TKy=(OTy){HKM+1}[MPy]
	ESSC0x by procSTKxy=SC0x
	SC0x=SR0y
	SR0y by procSTKyx=ESSR0y
	<SC0y> by procSTKyx=ESSC0y
	RCNy,TKy,RNSR0y,ESSR0y,RNC0y,ESSC0y >>>>>>
>>>>>>RCNy,TKy,RNSR0y,ESSR0y, RNC0y,ESSC0y	
<RCNy>	
MPy=(OTy){HKM−1}[TKy]	
RCNx=(UINx,UCNx & IDy & IDx){HKM+1} [MPy]	
ESSR0y by procSTKyx=SR0y	
Compare SR0y with <SC0y>	
ESSC0y by procSTKyx=SC0y	
SC0y=SR0x	
SR0x by procSTKxy=ESSR0x	
RCNx,RNSR0x,ESSP0x>>>>>>	
	>>>>>>RCNx,RNR0x,ESSR0x
	<RCNx>
	ESSR0x by procSTKxy=SR0x
	Compare SR0x with <SC0y>

若询问SC0x等于响应SR0y，并且询问SC0y等于响应SR0x，则完成了X和Y间的相互注册认证。

C5 安全模式

一旦建立了 MPx 和 MPy 的注册，HKM 算法即可用于提供在 X 和 Y 间秘密密钥的安全通信。该秘密密钥可能是 SC、SR 或 SS。这里使用的规程(procSTKxy)在以下章节中描述。

C5.1 SK 从 X 到 Y 安全传输规程(procSTKxy)

从 X 安全地传送到 Y 的秘密密钥 SKx，使用 HKMD+1 加密和扰码后形成 ESSKx。用于 HKMD+1 的原语是由 MPx 生成并用 RNKx 进行修改的。RNKx 同 RCNy 和 ESSKx 一起公开传送给 Y。

Y 用 RCNy 恢复 MPx，用 HKMD−1 解密并解扰 ESSKx 恢复出 SKx。用于 HKMD−1 的原语同在 X 处一样是经 RNKx 修改并由 MPx 演变形成。

ProcSTKxy 可用代数表示法表示：

X	Y
>UINx,UCNx,RCNy<	>UINy,UCNy,RCNx<
MPx=(UINx,UCNx & IDx & IDy){HKM+1}	
[UCNx & IDx & IDy]	
ESSKx=(MPx & RNKx){HKMD+1}[SKx]	
RCNy,RNKx,ESSKx>>>>>>	
	>>>>>>RCNy,RNKx,ESSKx
	MPx=(UINy,UCNy & IDx & IDy){HKM−1}
	[RCNy]
	SKx=(MPx & RNKx){HKMD−1}[ESSKx]

ProcSTKxy 所有计算的描述和例子在 C6.5 中给出。

C5.2 在安全模式下使用 procSTKxy 和 procSTKyx

一旦 X 和 Y 完成注册后，即可安全地完成所有的传输。在安全模式下使用 HKM 算法重新创建 MPx 和 MPy，以便能够使用 procSTKxy 和 procSTKyx 来安全传送密钥。

C5.3 X 与 Y 的相互认证

在本部分中，X 发起呼叫并发送加密报文给 Y。

在 X 侧：

——X 输入 Y 的传真电话号码；

——X 重新生成原来用于 X 和 Y 之间注册的 MPx；

——X 生成 SC1x 和 RNC1x 并存储 SC1x；

——X 通过 procSTKxy 规程，用 MPx、RNC1x 和 SC1x 来形成 ESSC1x；

——X 向 Y 发送 RCNy、RNC1x 和 ESSC1x。

在 Y 侧：

——Y 解密 RCNy 来形成 MPx；

——Y 通过 procSTKxy 规程用 MPx、RNC1x 和 ESSC1x 恢复 SC1x；

——Y 重新生成 MPy；

——Y 使用 SC1x 作为安全响应密钥 SR1y 并生成 RNSR1y；

——Y 通过 procSTKyx 规程用 MPy、RNSR1y 和 SR1y 形成 ESSR1y；

——Y 生成 SC1y 和 RNC1y 并存储 SC1y；

——Y 通过 procSTKyx 规程用 MPy、RNC1y 和 SC1y 形成 ESSC1y；

——Y 向 X 发送 RCNx、RNSR1y、ESSR1y、RNC1y 和 ESSC1y。

在 X 侧：

——X 解密 RCNx 形成 MPy；

——X 通过 procSTKyx 规程用 MPy、RNSR1y 和 ESSR1y 形成 SR1y；

——X 比较 SR1y 和 SC1x，假如一致则 Y 通过 X 的认证；

——X 通过 procSTKyx 规程用 MPy、RNC1y 和 ESSC1y 恢复 SC1y；

——X 用 SC1y 作为响应密钥 SR1x 并生成 RNSR1x；

——X 通过 procSTKxy 规程用 MPx、RNSR1x 和 SR1x 形成 ESSR1x；

——X 向 Y 发送 RNSR1x 和 ESSR1x。

在 Y 侧：

——Y 通过 procSTKxy 规程用 MPx、RNSR1x 和 ESSR1x 恢复 SR1x；

——Y 比较 SR1x 和 SC1y，假如一致则 X 通过 Y 的认证。

在此 X 和 Y 已经交换了 RCNx 和 RCNy 并完成相互/询问-响应交换。如果 SC1x 与 SR1y、SC1y 与 SR1x 相等，相互认证完成。

X 和 Y 相互认证的过程可用代数表示法表示：

X	Y
>UINx,UCNx,RCNy<	>UINy,UCNy,RCNx<
<SC1x> by procSTKxy=ESSC1x	
RCNy,RNC1x,ESSC1x>>>>>>	
	>>>>>>RCNy,RNC1x,ESSC1x
	<RCNy>
	ESSC1x by procSTKxy=SC1x
	SC1x=SR1y
	SR1y by procSTKyx=ESSR1y
	<SC1y> by procSTKyx=ESSC1y
	RCNx,RNSR1y,ESSR1y,RNC1y,ESSC1y>>
	>>>>
>>>>>>RCNx,RNSR1y,ESSR1y,RNC1y,	
ESSC1y	
<RCNx>	
ESSR1y by procSTKyx=SR1y	
Compare SR1y with <SC1x>	
ESSC1y by procSTKyx=SC1y	
SC1y=SR1x	
SR1x by procSTKxy=ESSR1x	
RNSR1x,ESSR1x>>>>>>	
	>>>>>>RNSR1x,ESSR1x
	ESSR1x by procSTKxy=SR1x
	Compare SR1x with <SC1y>

如果询问 SC1x 等于响应 SR1y 并且询问 SC1y 等于响应 SR1x，则相互认证完成。

C5.4 X 和 Y 之间建立秘密会话密钥

在本部分中，X 发起呼叫并向 Y 发送加密报文，此时已经成功地建立 C5.3 中描述的相互认证。

在 X 侧：

——X 重新生成原来用于 X 和 Y 之间注册的 MPx；

——X 生成 SS1x 和 RNSS1x；

——X 通过 procSTKxy 规程用 MPx、RNSS1x 和 SS1x 形成 ESSS1x；

——X 发送 RCNy、RNSS1x 和 ESSS1x 到 Y。

在 Y 侧：

——Y 解密 RCNy 恢复 MPx；

——Y 通过 procSTKxy 规程用 MPx、RNSS1x 和 ESSS1x 恢复 SS1x；

X 和 Y 建立秘密会话密钥的过程可用代数表示法表示如下：

X	Y
<RCNy>	<RCNx>
SS1x by procSTKxy=ESSS1x	
RCNy,RNSS1x,ESSS1x>>>>>>	
	>>>>>>RCNy,RNSS1x,ESSS1x
	ESSS1x by procSTKxy=SS1x

X 和 Y 使用 SS1x 和 HFX40 密码算法 HFX40 对主要报文进行加/解密来提供安全性(附录 D)，和/或使用散列算法 HFX40-I 在传输过程中提供报文的完整性(附录 E)。

C5.5 接收确认

在本部分中，X 发起呼叫并向 Y 发送加密报文，即已经建立 C5.3 中描述的相互认证、安全交换了 C5.4 中描述的 SS1x，并已经发送报文。在报文的结尾，X 向 Y 发送 SC2x，如果接收的报文是完整的，Y 将把 SC2x 作为 SR2y 使用。

在 X 侧：

——X 重新生成原用于 X 和 Y 之间注册的 MPx；

——X 生成 SC2x 和 RNC2x 并存储 SC2x；

——X 通过 procSTKxy 规程用 MPx、RNC2x 和 SC2x 形成 ESSC2x；

——X 向 Y 发送 RCNy、RNC2x 和 ESSC2x。

在 Y 侧：

——Y 解密 RCNy 形成 MPx；

——Y 通过 procSTKxy 规程用 MPx、RNC2x 和 ESSC2x 恢复 SC2x；

——Y 再生成 MPy；

——Y 使用 SC2x 作为 SR2y 并生成 RNSR2y；

——Y 通过 procSTKyx 规程用 MPy、RNSR2y 和 SR2y 形成 ESSR2y；

——Y 向 X 发送 RCNx、RNSR2y 和 ESSR2y。

在 X 侧：

——X 解密 RCNx 形成 MPy；

——X 通过 procSTKyx 规程用 MPy、RNSR2y 和 ESSR2y 恢复 SR2y；

——X 比较 SR2y 和 SC2x，如果相等，说明 Y 确认收到 X 的报文。

接收确认的过程可用代数表示法表示：

X	Y
>RCNy<	>RCNx<
<SC2x> by procSTKxy=ESSC2x	
RCNy,RNC2x,ESSC2x>>>>>>	
	>>>>>>RCNy,RNC2x,ESSC2x
	ESSC2x by procSTKxy=SC2x
	SC2x=SR2y
	SR2y by procSTKyx=ESSR2y
	RCNx,RNSR2y,ESSR2y>>>>>>

>>>>>>> RCNx,RNSR2y,ESSR2y

ESSR2y by procSTKyx=SR2y

Compare SR2y with <SC2x>

如果从Y来的SR2y等于存于X的SC2x,则X确认Y收到了报文。

C5.6 完整性的确认或否认

在本部分中,X发起呼叫并向Y发送已保护其完整性的报文,即已经满意地建立C5.3中描述的相互认证,安全地交换了C5.4中描述的SSx,并且报文通过了或未通过Y的完整性测试(附录E)。

Y生成IMy来确认或否认收到报文的完整性。IMy是由数字2至9中选择的12位随机数。在该12位数中随机选择一位数字进行替代,选择"1"表示确认完整性,选择"0"表示否认完整性。

在Y侧:

——Y生成由数字2至9组成的12位随机数;

——Y生成1至12之间的随机数作为上面随机数的替代点;

——Y将替代点的数字改变为"1"或"0",以形成IMy;

——Y生成RNIMy;

——Y通过procSTKyx用MPy、RNIMy和IMy形成ESIMy;

——Y向X发送RCNx、RNIMy和ESIMy。

在X侧:

——X解密RCNx形成MPy;

——X通过procSTKyx用MPy、RNIMy和ESIMy恢复IMy;

——X检查IMy包含的"1"或"0"来确认或否认完整性。

完整性确认的过程可用代数表示法表示:

X　　Y

>RCNx<

IMy by procSTKyx=ESIMy

RCNx,RNIMy,ESIMy>>>>>>>

>>>>>>> RCNx,RNIMy,ESIMy

ESIMy by procSTKyx=IMy

Check IMy for a "1" or a "0"

如果该秘密的完整性消息包含"1",则确认完整性;如果包含"0",则否认完整性。响应举例:

IMy=257795199982　　确认完整性

IMy=317736845378　　确认完整性

IMy=738543680892　　否认完整性

IMy=457745204639　　否认完整性

C6 HKM算法

C6.1 引言

本部分根据存储的数码和在注册过程(procREG)和安全传输密钥过程(procSTK)中使用这些数计算的规则,描述HKM算法。这些规则的最好解释是使用数字举例。使用测试值的计算可用于检验执行的正确性。

C6.2 存储信息

所有的终端都装备相同的19个系统取模质数。

32603　32507　32183　32003　31847　31607　31583　31547　31259　31139　30803　30539

30467　30347　30323　30203　29879　29759　29663

前 9 个数同 HKM 算法一起用于注册、认证和其他密钥管理功能。所有 19 个数都用于报文加密算法(附录 D)和报文完整性算法(附录 E)。

C6.3 秘密存储信息

每个终端都通过适当的过程装备两个随机生成的十进制数,这些数秘密地存储于终端中。它们是 48 位的 UIN 和 16 位的 UCN。UIN 和 UCN 同其他标识码一起形成 HKM 算法的原语。

X 和 Y 的测试举例是:

UINx=345092978336094172898029844342879120988727823781

UCNx=1333908734565521

UINy=9735576938377831483537091674367228734498197673 57

UCNy=7598247578649467

C6.4 注册模式

C6.4.1 使用代数表示法的 procREGxy

X	Y
>UINx,UCNx<	>UINy,UCNy<
MPx=(UINx,UCNx & IDx & IDy)	
{HKM+1}[UCNx & IDx & IDy]	
TKx=(OTx){HKM+1}[MPx]	
TKx>>>>>>	
	>>>>>>TKx
	MPx=(OTx){HKM−1}[TKx]
	RCNy=(UINy,UCNy & IDx & IDy){HKM+1}[MPx]
	RCNy>>>>>>
>>>>>>RCNy	
<RCNy>	

随后的部分使用测试值示出了 procREGxy 使用的所有计算。

C6.4.2 在 X 处导出 MPx 的计算

MPx=(UINx,UCNx & IDx & IDy){HKM+1}[UCNx & IDx & IDy]

C6.4.2.1 原语(UINx,UCNx & IDx & IDy)的初步计算

UINx=345092978336094172898029844342879120988727823781

UCNx=1333908734565521

IDx=642092

IDy=538249

由 UINx 和 UCNx 拼接形成一个 64 位的原语。

原语=3450929783360941728980298443428791209887278237811333908734565521

该原语分为两个 32 位数,9 个相原语值[P(0)到 P(8)]由第 1 个数得到,9 个基原语值[B(0)到 B(8)]由第二个数得到。把第 1 个数分为 7 组 4 位数和 2 组 2 位数可得到相值。基值是用完全相同的方法从第二个数得到的。

相原语值通过加上 101 的增积来修改,基原语通过加上 79 的增积来修改。用 101 和 79 来修改是为保证质数的模数运算尽可能快的开始。

使用原语=3450929783360941728980298443428791209887278237811333908734565521

相原语和基原语值如下所示:

P(0) 3450+(0*101)=3450 B(0) 9120+(0*79)=9120