ICS 35.240.15
A 11

中华人民共和国国家标准

GB/T 23695—2009

银行业务　安全文件传输(零售)

Banking—Secure file transfer(retail)

(ISO 15668:1999,MOD)

2009-05-06 发布　　2009-10-01 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

本标准修改采用 ISO 15668:1999《银行业务　安全文件传输(零售)》(英文版)。

本标准根据 ISO 15668:1999 重新起草,与 ISO 15668:1999 的技术性差异及原因为:

——删除“2　规范性引用文件”中对此文件的引用:ISO 8731-1:1987《银行业务　核准的报文鉴别算法　第1部分:DEA》,因为此标准中的算法不符合我国密码管理部门的有关规定,且该标准已于2005年被ISO废止。

——删除“2　规范性引用文件”中对此文件的引用:ISO 11568(所有部分)《银行业务　密钥管理(零售)》,因为此标准中的算法不符合我国密码管理部门的有关规定。

——删除“图1　终端软件的表示(示意图)”中的标号8,因为图1注释中未给出标号8的说明,且根据原文可知标号8是指引导程序(标号7)的运行环境或其他支持程序,而标准中提到引导程序(即层a)的安全性不在本标准的讨论范围之内,它的运行环境和支持程序被标为了灰色。在不影响理解的情况下,删除图中未给出解释的标号8。

——5.1.2.3中“密钥管理技术应符合ISO 11568的要求”,改为:“密钥管理技术应遵循我国密码管理部门的有关规定”。

——“6　鉴别机制”和“A.1　鉴别机制”中,“已核准的算法参考ISO 11568”改为:“已核准的算法应遵循国家的相关规定”。

——删去A.3中最后一句:“ISO 9807给出了已经核准的用于计算MAC的算法列表,其中在ISO 8731-1中说明的算法,以操作的密码分组链模式使用DEA,它是当 $n=64$, $m=32$, ISO/IEC 9797的一个特殊情况”。因为ISO 8731中的算法不符合我国密码管理部门的有关规定。

——删去A.2最后一句:“——ISO/IEC 10118-2,附录A,说明一种使用 $n=64$,哈希长度=56的DES方法”。

——删去A.2.3所举的例子,因为其中引用了DSA、RSA,不符合我国密码管理部门的规定。

——删去资料性附录B,因为其中引用了DEA,不符合我国密码管理部门的规定。

——C.4.3.3中“MAC密钥应遵循ISO 11568”,改为“MAC密钥应遵循我国密码管理部门的有关规定”。

为便于使用,本标准做了下列编辑性修改:

——用“本标准”代替“本国际标准”;

——删除国际标准前言;

——修改图1、图2中的印刷错误。

本标准的附录A、附录B、附录C和附录D为资料性附录。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会归口。

本标准负责起草单位:中国金融电子化公司、泛太领时科技(北京)有限公司。

本标准参加起草单位:中国人民银行、中国工商银行、中国农业银行、中国建设银行、交通银行、中国银联股份有限公司、华北计算技术研究所、北京工商大学。

本标准主要起草人:王平娃、李曙光、吕毅、杨颖莉、鲍乐群、万良君、林中、张启瑞、仲志晖、景芸、刘运、钱湘隆、赵金波、曹文中、李劲松、刘先、周亦鹏、王威。

引　言

本标准说明在零售银行业务环境下如何保护文件传输。使用该类文件传输的典型例子是在卡的接收设备和收单机构之间，或在收单机构和发卡方之间的文件传输。

银行业务　安全文件传输(零售)

1　范围

批发银行业务的文件传输是在安全性相对高的主机之间进行大量的信息交换(大宗文件传输);与此相比,零售银行业务文件传输以量少、下载设备操作环境的可信赖程度较低为特点。这类设备可以是(但不仅限于)电子销售点终端(EPOS)、自动售卖机(AVM)、自动柜员机(ATM)或与支付网关通信的商户服务器。

假设参与安全文件传输的实体之间预先建立的关系已经存在,尤其是涉及与文件传输责任相关的法律和商业等方面。

本标准适用于零售银行业务中不同类型的文件传输,但不包括 ISO 8583 中涉及的交易报文。

文件传输必须要求时效性,并且至少需要符合下列安全服务要求之一:

——报文源鉴别;

——接收方鉴别;

——完整性;

——机密性;

——信息源的不可否认性;

——接收的不可否认性;

——可审计性。

假设在传输前发起方传送的全部数据的合法性和正确性已经确认。

不同类型的传输文件可包括:

——软件;

——已经执行和注册的零售交易(上载);

——与收单机构相关的技术数据(存取参数)(下载);

——与收单机构相关的应用数据(BIN 列表、黑名单)(下载)。

该类文件传输的特点:

a)　传输的数据类型可以是:

——非保密数据(零售交易、技术类数据和应用数据的集合);

——保密数据。

b)　可以接收数据的实体数量:

——一个;

——多于一个(甚至向数千的接收者广播)。

c)　通讯通路可以包括以下一个或全部:

——电信:公用网络、专用网络。

d)　该类传输的方式是:

——直接连接、实时传输(电路交换);

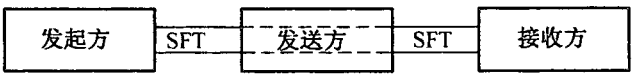
——存储转发传送(报文交换)。

注:本标准考虑到了传输过程中的安全服务要求。确保文件传输完成之后不被更改的要求不在本标准的范围之内。

安全文件传输的许可形式

安全文件传输

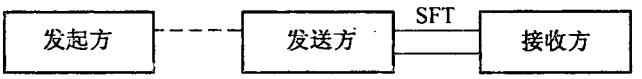
传输功能除了通信服务以外，不提供任何安全服务，在这种情况下文件应在传输之前被保护。安全性由发起方和接收方自己管理。他们不信赖底层的传输机制。在通信层（发送方和接收方）上，没有附加的安全性。



SFT＝Secure File Transfer

文件的安全传输

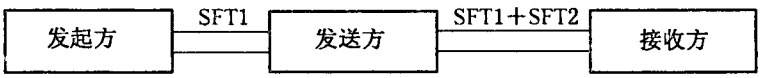
在这种情况下，仅当从发送方到接收方的过程中才考虑安全性，发起方完全信任发送方。例如，当发起方是发送方且安全性由传输层保证，由于发起方没有附加安全性，因此它不是端对端的安全性。在这种情况下，传输功能完全包括安全服务。文件无需在安全传输之前被保护。



安全文件的安全传输

安全功能在安全功能和传输功能之间分离。例如，发起方生成一文件，利用签名私钥对该文件签名，并且用仅由终端用户（接收者）知道的密钥对该文件加密。

所举的例子可以避免发送方组织中的人看到发起方文件的内容。而且发起方信赖它的代理来处理文件传输以及考虑发送方与接收方之间的鉴别、完整性。



2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。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标准，然而，鼓励根据本标准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标准。

GB 15851—1995 信息技术 安全技术 带消息恢复的数字签名方案(idt ISO/IEC 9796:1991)

GB/T 15852.1—2008 信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制(ISO/IEC 9797-1:1999,IDT)

GB/T 17903.2—2008 信息技术 安全技术 抗抵赖 第2部分：采用对称技术的机制(ISO/IEC 13888-2:1998,IDT)

GB/T 17903.3—2008 信息技术 安全技术 抗抵赖 第3部分：采用非对称技术的机制(ISO/IEC 13888-3:1997,IDT)

ISO 8372:1987 信息处理 64位分组密码算法的操作模式

ISO 8583:1993 产生报文的金融交易卡 交换报文规范

ISO 9564-1:1991 银行业务 个人识别码的管理与安全 第1部分：PIN保护原则和方法

ISO/IEC 9796-2:1997 信息技术 安全技术 带消息恢复的数字签名方案 第2部分：使用哈希函数的机制

ISO/IEC 9798-1:1991 信息技术 安全技术 实体鉴别机制 第1部分：一般模型

ISO/IEC 9798-2:1994 信息技术 安全技术 实体鉴别 第2部分：对称加密算法机制

ISO/IEC 9798-3:1993 信息技术 安全技术 实体鉴别机制 第3部分：公钥算法实体鉴别

ISO/IEC 9798-4:1995 信息技术 安全技术 实体鉴别 第4部分：使用密码校验功能机制

ISO 9807:1991 银行业务和相关金融服务 报文鉴别要求(零售)

ISO/IEC 10116:1993 信息技术 n 位分组密码算法的操作模式

ISO/IEC 10118-1:1994 信息技术 安全技术 哈希函数 第1部分:概述

ISO/IEC 10118-2:1994 信息技术 安全技术 哈希函数 第2部分:使用 n 位分组密码算法的哈希函数

3 术语和定义

下列术语和定义适用于本标准。

3.1

黑名单 hot list

发卡商或其代理商排列并在交易中无效的主账户号码(PAN)列表。

3.2

数字签名 digital signature

附加于数据单元之后的数据或者是数据单元加密后的某种形式,以使数据单元允许它的接受者检验数据单元的来源和完整性,及防止接受者的伪造。

3.3

文件校验值 file validation value

FVV

用于文件校验的派生值。

3.4

哈希值 hash code

对数据哈希后的结果。

3.5

哈希函数 hash function

将位串映射为定长位串的函数,在本标准中它具有以下两个特性:

——对于一个给定的输出不可能推导出与之相对应的输入;

——对于一个给定的输入不可能推导出第2个具有同一输出的输入。

3.6

应用管理器 application manager

终端软件的一部分,负责预期可执行对象安全下载的验证。

3.7

报文鉴别码 message authentication code

MAC

发送方和接收方传递报文包含的代码,用于证实报文来源及部分或全部报文文本的有效性。

注:代码是双方协定的计算结果。

3.8

发起方 originator

生成传输到接收方的文件并且对其安全性负责的实体。

3.9

接收方 receiver

接收文件的实体。

3.10

发送方 sender

发送文件的实体。

3.11

主办方 sponsor

评估文件传输风险的实体。

4 原则

4.1 报文源鉴别

报文源鉴别的目的是保证向接收方声称的发起方是真正的发起方。当被授权的接收方从授权的发起方子集中接收特定文件时，报文源鉴别可以向接收方保证所传输的文件是真实的。

报文源鉴别可以与文件传输同时发生，在直连模式下也可以先于传输过程发生。如果使用存储和转发传输，报文源鉴别应在传输完成后，接收方得到这个文件时进行(安全文件的传输属于该模式)。

鉴别报文内容的技术可以提供报文源鉴别，但这些技术要求整个文件的传输在鉴别可以确认前完成。也许有要求在发起传输之前需要进行报文源鉴别的情况。例如，尽管非法的发起方最终会被检测到，传输的文件也会被拒绝，但还是有防止冒名顶替者伪装成合法的文件提供方并且在传输大文件延时占用通信信道的要求。

4.2 接收方鉴别

该项安全服务在传输过程之前鉴别接收方的身份，因此，只有当接收方的身份被确认时，传输才会进行。

一些接收方(POS 终端)只允许接收某些类型的文件。部分鉴别过程由发起方控制，发起方有控制接收方接收某种类型文件的权利。

进行接收方鉴别的另一个目的是防止未授权方伪装成合法的接收方并防止发起方传输一冗长文件给伪装者占用发起方的通信资源。

接收方鉴别不能防止未授权方探知文件内容(通过“侦听”)。没有该项安全服务以及机密性安全服务，任何人都可轻易地伪装成合法的接收者获取文件。如果要保证仅使文件的授权接收方接收到文件，那么必须使用机密性安全服务。只有通过该方法才能确保未授权方不在通信信道上“侦听”并获取文件内容。

注：相关安全服务，接收的不可否认性可以确保在传输完成之后，授权方成功地接收到该文件。

4.3 完整性

对传输文件或者传输文件一部分的意外的或未授权的变更，应在传输时或传输之后被检测到。完整性服务在单个传输过程中可以控制整个文件，或能够分别控制文件的几个部分。

4.4 机密性

在需要时传输文件的机密性应得到保证并应用到整个文件或文件需要保密的部分中。

4.5 信息源的不可否认性

该项安全服务提供了这样的证据：声称的发起方实际生成了传输的文件(如果没有该证明，发起方可能错误地声称文件是接收方生成的，或接收方可能生成了该文件但错误地声称该文件来自发起方)。

4.6 接收的不可否认性

该项安全服务提供这样的证据：声称的接收方实际收到了传输的文件。没有该证据，接收方可能声称没有收到该文件。该项服务由附录 A 说明的机制实现。接收方发给发起方不可否认的标记报文，如果：

a) 目的接收方收到了该文件；

b) 文件内容没有被更改。

注：不可否认性的范围可由国内的法律、规章规定。

4.7 可审计性

如果应用需要可审计性，发送方/发起方和(或)接收方有必要适当记录传输过程的细节(时间和日

期、文件种类、文件容量、版本编号等)。这些记录包括传输失败的数据尝试,也包括成功传输数据的尝试。如果发生欺诈的尝试,失败的传输记录可以帮助识别尝试的来源。

5 应用

5.1 软件下载

5.1.1 定义

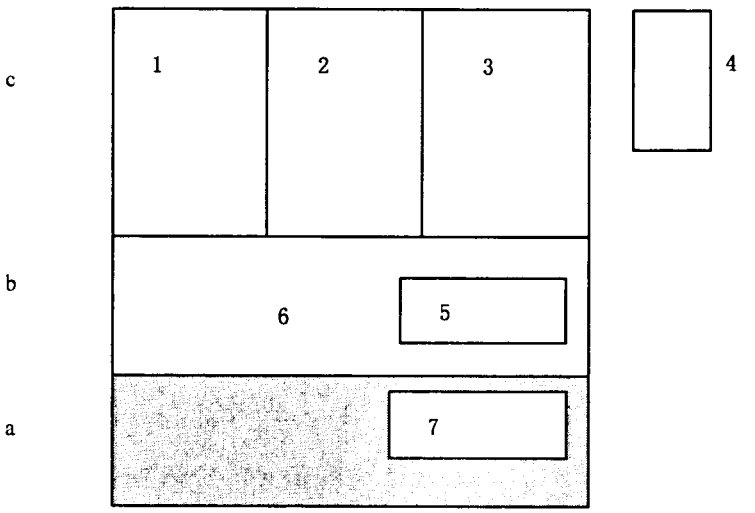
终端软件包括下列不同的功能层次(见图 1):

a) 可信赖的、固定的软件,在安全文件传输之前被预先加载,负责执行应用管理器的下载和安全运行的安全性机制;

b) 应用管理器负责执行不同应用程序的下载和安全运行的安全性机制;

c) 不同的应用,由可执行实体或解释性实体组成。

注:以上所述是加载和驱动终端设备程序过程中具有代表性的功能层次。只有层 b 和层 c 是可下载的。层 a 的安全性不在本标准范围之内。



1——应用 1;

2——应用 2;

3——应用 3;

4——可执行对象或解释性对象;

5——密钥;

6——应用管理器;

7——信赖的、固定的、预先加载的软件(引导程序 bootstrap)。

图 1 终端软件的表示(示意图)

软件下载所要求的安全性服务:

——互相鉴别或发起方/发送方的单方鉴别;

——传输文件的完整性确认。

在适当时敏感数据可以要求机密性(例如密钥)。

当下载功能在特定的缓存区中处理,并且在软件接收前已经执行了完整性检验时,可以不要求对发送方通过设备事先鉴别,只完成发送方的固有鉴别。

每个层面的操作顺序应是:相互鉴别、软件传输、完整性确认。如果相互鉴别失败,不应进行软件传输。如果完整性确认失败,接收设备不接收软件,并且所有操作步骤应重新执行。

注:对接收方不必总进行鉴别。对接收方来说,下载软件时进行报文源鉴别已经足够。

5.1.2 相互鉴别

5.1.2.1 实施

无论软件下载的发起方是哪个实体，在任何层面上，相互鉴别的成功执行应先于任何文件传输。

——当下载应用管理器时，应通过预先加载的可信赖的、固定的软件所提供的相互鉴别安全服务进行保护；

——应用下载本身应通过相互鉴别服务保护，在应用管理器中实施，并且对每一个授权的应用均使用专用密钥。

通常，发送方可管理几个应用，每个应用可传输到设备上。相互鉴别过程包括发送方对每个接收设备及其接收每个应用程序的权限的验证，它包括：

——每个设备应由唯一的识别码标识；

——发送方将授权应用的列表和每个设备识别码关联。

5.1.2.2 机制

相互鉴别机制要求 2 次或 3 次报文交换并且可以通过对称或非对称算法实现。ISO/IEC 9798 详细说明了该安全机制。

当使用对称算法时，ISO/IEC 9798-2:1997 和 ISO/IEC 9798-4:1995 适用。当使用非对称算法时，ISO/IEC 9798-3:1993 适用。

相互鉴别并不涉及可信赖第三方，可以使用序列号（或时间戳）进行两次鉴别或使用随机数进行三次鉴别。

详见附录 A。

5.1.2.3 密钥管理

密钥管理技术应遵循我国密码管理部门的有关规定。

对称算法

在所有下载之前应安全地安装初始密钥。同一个密钥可用于两个设备，但建议相互鉴别的每个设备使用唯一密钥，防止一个设备通过改变它的标识伪装为另一个设备，并且防止生成一个错误的发送方损害设备的密钥。

每个层面下载之前，用于相互鉴别的密钥可以不同。

非对称算法

非对称算法的使用要求接收方与发送方具有信赖关系，用于相互鉴别的密钥是：

——私钥驻留在设备中，并将与之关联的公钥传给发送方用以鉴别终端；

——所有设备每一层面具有一个唯一的公/私密钥对。

即使发送方不同，但对 b 和 c 两个层面而言，设备的私钥可以相同。

用于鉴别应用管理器的发送方的公钥应驻留在每一设备中，并防止被替代。用于鉴别应用管理器的公钥应与应用管理器同时安全下载或者预先安全加载。

5.1.3 完整性

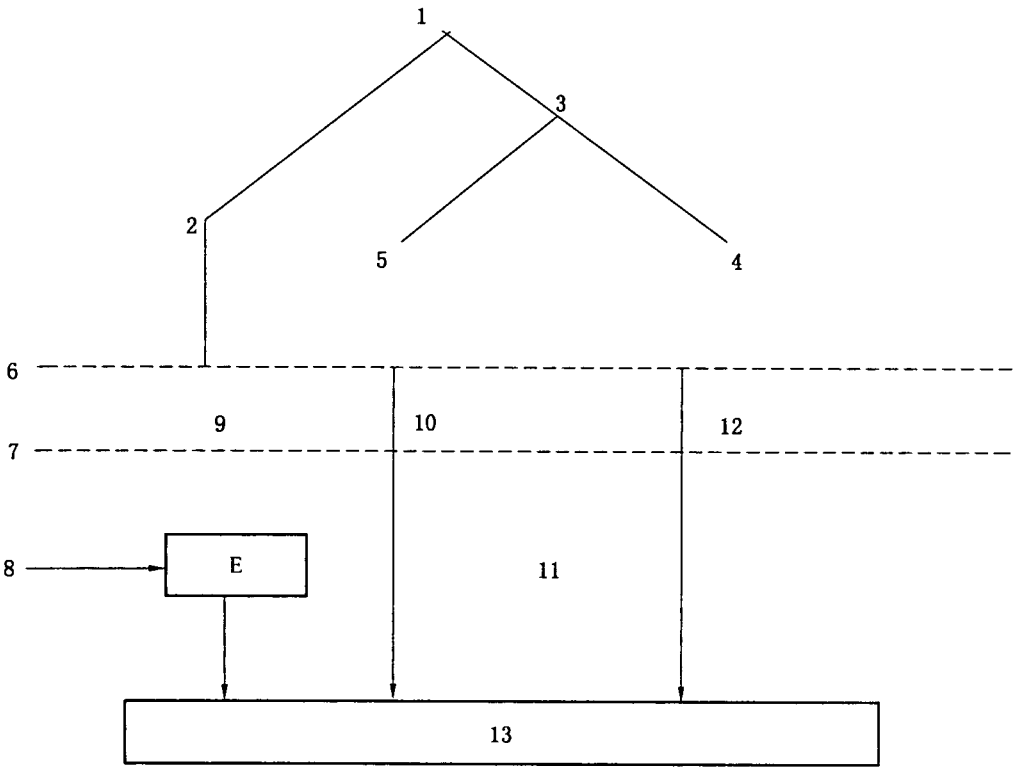
5.1.3.1 实施

应通过向文件内容添加 FVV 确保传输文件的完整性。文件的 FVV 只需计算一次，因为它不需依赖下载操作和接收设备的标识。

设备中一层软件下载后和在将其激活之前，该设备应确认下载文件的 FVV。

5.1.3.2 机制

依照所使用的算法，需要一步或多步生成 FVV，详见图 2 和附录 A。



1——文件；
2——不包含密钥的算法；
3——包含密钥的算法；
4——非对称算法；
5——对称算法；
6——步骤 1；
7——步骤 2；
8——密钥；
9——哈希值；
10——报文鉴别码(MAC)；
11——不做进一步处理；
12——数字签名；
13——文件校验值(FVV)。

图 2　FVV 的生成

5.1.3.3　密钥管理

FVV 需要使用密钥(对称算法)或私钥(非对称算法)或不使用密钥的值(哈希值)。基于密钥的 FVV 的操作由加密设备进行。

对称算法

用于每一层完整性的密钥应不同。

用于确认下载的应用管理器完整性的密钥应在设备交付使用之前安全地安装。

用于确认下载的应用完整性的密钥应是：

——在设备交付使用之前安全安装；或

——与应用管理器同时安全下载。

这些密钥的完整性和机密性应使用一系列预先安装的密钥保护。

非对称算法

每一层面有唯一的公/私密钥对，发送方保留私钥，所有接收方的公钥相同。

用于确认下载的应用管理器完整性的公钥应在每一个设备中，并防止被替换。用于确认下载的应用完整性的公钥应与应用管理器同时下载或预先加载。

加密哈希技术

哈希函数有两个阶段的操作。

生成 FVV 的第一步是，对整个传输文件进行哈希计算，使用哈希算法，不使用任何密钥(保密或其他的)。

第二步，包括应用对称或非对称的哈希算法，附加数据与合适的填充生成 FVV。

5.1.4 机密性

软件下载可以不需要机密性。当机密性服务被要求用于密钥和数据时，从发送方下载密钥或私钥，而且该密钥应经过加密保护。

5.1.5 接收的不可否认性

接收并确认了软件的完整性之后，设备应向发送方发送一安全确认，确认接收的完成(成功或失败)以及完整性验证结果。

——安全确认应包括肯定或否定的结果，以及在相互鉴别阶段由设备使用相同的密钥发给发送方的鉴别报文；

——时间戳。

安全确认应符合 GB/T 17903.2—2008 或 GB/T 17903.3—2008 的要求。

接收到安全确认时发送方应确认和记录。

5.1.6 发起的不可否认性

不可否认性应被用于确保服务的完整性。

当非对称算法用于确保完整性服务的同时也提供发起的不可否认性，因为只有发起方知道计算签名所需要的私钥。在这种情况下，设备应记录签名。

注：如果签名的数据不包括时间戳，不能完全达到发起不可否认性的目的。

5.1.7 可审计性

为了确保不可否认性服务，5.1.5 和 5.1.6 中所描述的信息应记录日志。

5.2 参数下载

5.2.1 定义

参数下载包括应用数据(例如 BIN 列表、最低限度)、黑名单文件、传输和更新发送方访问参数。

接收方的应用软件应发起这样一类传输，它可能包括与先前用于下载应用软件完全不同的协议和发送方。

用于参数传输的安全服务由发起方或发送方控制。通常，应用软件提供商通过应用服务器提供应用，参数由发起方通过参数服务器提供，两方实体可以相同。在该情况下，安全机制和密钥应由应用提供者通过应用软件依照主办方说明实施。

参数下载要求的安全服务有：

——互相鉴别或发起方/发送方的单方鉴别；

——完整性确认；

——适当的机密性；

——依据参数类型接收的不可否认性。

当需要上述参数时，操作的顺序应是相互鉴别，参数传输，完整性确认和接收的不可否认性。

在相互鉴别失败的情况下，不应执行参数传递。如果完整性确认失败，设备不应保留参数，整个操作应重新执行。

注：没有必要总是鉴别接收方。对接收方而言，对下载的参数报文源鉴别已足够。

5.2.2 相互鉴别

应用软件下载的相互鉴别要求适用于此。这种文件传输可看作是应用下载操作的附加层。

5.2.3 完整性

应用软件下载的完整性要求适用于此。这种文件传输可看作是应用下载操作的附加层。

5.2.4 机密性

根据网络种类,机密性服务可以被要求用于传输活动表,最低限度等参数。

当需要时,机密性服务的执行应满足本地规则。

5.2.5 接收的不可否认性

如果主办方要求,应用软件下载的接收不可否认性要求适用于此。

5.2.6 发起的不可否认性

如果主办方要求,应用软件下载的发起的不可否认性要求适用于此。

5.2.7 可审计性

为了确保不可否认性服务,应记录 5.1.5 和 5.1.6 中所描述的信息日志。

5.3 零售交易上载

5.3.1 定义

对于这种环境,发起方/发送方是终端或商户服务器。

零售交易上载包括,向收单机构服务器发送的该时期金融交易文件和附加的相关数据,例如金融交易笔数和交易总额。

零售交易上载需要的安全服务有:

——相互鉴别;

——交易文件传输的完整性确认。

操作的顺序应是:相互鉴别、交易文件传输、服务器进行完整性确认、服务器发送接收的证据。如果相互鉴别失败,应不执行文件传输。如果完整性确认失败,服务器应拒绝交易,相互鉴别应重新执行。

5.3.2 相互鉴别

5.3.2.1 实施

零售交易上载应通过应用层实施的相互鉴别进行保护。

5.3.2.2 机制

如同软件下载,ISO/IEC 9798 适用于此。

因为同一个收单机构可从不同生产商提供的设备中收集交易,所以该机制应独立于设备。

5.3.2.3 密钥管理

对称算法

因零售交易上载操作在收单机构的控制之下,用于相互鉴别的密钥由收单机构确定,它们应在设备中的保护区域,例如,ISO 10202-4:1996《金融交易卡 使用集成电路卡的金融交易系统的安全保障体系 第 4 部分:安全应用模块中所定义的安全应用模块(SAM)》。

同一密钥可以用于发送和接收,但每个设备应使用唯一的密钥。密钥可以作为参数下载的一部分被安全传输。

非对称算法

用于相互鉴别的密钥是:

——私钥驻留在设备中,与之关联的公钥传输给发送方用以鉴别终端;

——服务器中的唯一的私钥及所有设备共用的相关公钥。

用于鉴别服务器的公钥作为参数下载的一部分被安全传输,并防止被替换。

5.3.3 完整性

5.3.3.1 实施

通过向文件内容添加校验值来确保零售交易文件的完整性。校验值应在传输前计算。

5.3.3.2 机制

5.1.3.2 中定义的要求适用于此，适合的机制参考附录 A。

5.3.3.3 密钥管理

对称算法

因为零售交易上载操作在收单机构的控制之下，所以用于完整性确认的密钥由收单机构确定，它们应在设备中的保护区域，例如，ISO 10202-4:1996 中定义的 SAM。

建议每个设备的完整性确认过程使用唯一密钥。密钥可作为参数下载过程的一部分被安全传输。

非对称算法

用于完整性确认的密钥应是设备中保护区域的唯一私钥，传输给服务器的与之关联的公钥用于验证签名。

5.3.4 机密性

如果需要，该服务的实施应符合国内法规。

如果上载的零售交易包括 PIN，PIN 应按照 ISO 9564-1:1991 的要求加密。

5.3.5 接收的不可否认性

不作要求。

5.3.6 发起的不可否认性

不作要求。

5.3.7 可审计性

不作要求。

每个应用安全服务的详细介绍，详见附录 D。

6 鉴别机制

鉴别值整合在文件传输协议中或和服务文件一起单独传输，该传输与数据文件的传输分离。

不整合到安全参数的协议中，应在文件传输前进行鉴别交换。

在文件传输前如果没有建立通信会话，而且鉴别值没有整合在文件传输协议中，这时每一文件传输应同一个优先的鉴别关系关联。例如，建立该关联的一个加密方法是在鉴别过程中交换密钥，并使用该密钥保护传输。

当正式的会话在向两方提供可信的连接完整性之前建立，则该要求不存在。当正式的协议在传输前建立，如果鉴别值没有集成到文件传输协议中，当几个连续的文件在单一交易中传输，就没有必要在新的传输前重复鉴别交换。

集成安全参数的协议中，应使用下列的技术之一鉴别文件的发送方：

——该文件由发送方签名，文件添加数字签名；

——该文件通过对称算法加密；

——向该文件添加 MAC。

已核准的算法应遵循国家的相关规定。

附 录 A
（资料性附录）
机 制 示 例

A.1 鉴别机制

ISO/IEC 9798-1:1991 至 ISO/IEC 9798-4:1995 详细说明了应用于安全文件传输的实体鉴别机制。

已核准的算法应遵循国家的相关规定。

A.1.1 使用对称加密算法、不引入可信赖第三方的鉴别机制

ISO/IEC 9798-2:1994 详细说明了使用对称加密算法的实体鉴别机制。详细说明提供单方鉴别和相互鉴别的报文的交换。

ISO/IEC 9798-2:1994 基于共享一个公有的保密鉴别密钥，一个实体通过证明它对保密鉴别密钥的了解来确证它的身份。没有提及参与方了解密钥的方法。

详细说明的机制要求使用时间变量参数，例如，时间戳、序列数或随机数。它们用以防止重发。使用随机数鉴别的轮数要比使用时间戳或序列数鉴别的轮数多一轮。

文本域的使用是可选择的并依赖于应用。

单方鉴别模型

单方鉴别用于从终端向主机传输零售支付数据。主机鉴别终端。

一次鉴别

在该鉴别机制下，声明方 A 发起该过程，并由检验者 B 鉴别。通过生成、确认一时间戳或序列数的方式控制唯一性/时效性。详见 ISO/IEC 9798-2:1994。

A 向 B 发送以下标记：text1//eKAB(TA 或 NA// B//text2)；

KAB：由 AB 共享的公共保密鉴别密钥；

eKAB(X)：用密钥 KAB，通过对称加密算法生成的 X 的加密数据；

X//Y：数据项 X 和 Y 的串联；

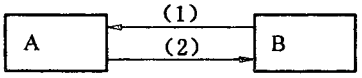
TA：时间戳；

NA：序列数；

B：B 的标识符(内容为可选项)。

两次鉴别

在该鉴别机制下，声明方 A 由发起该过程检验方 B 鉴别。通过生成、确认一随机数的方式控制随机数唯一性/时效性。详见 ISO/IEC 9798-2:1994。



B 向 A 发送一随机数：RB，可选的文本域 text1；

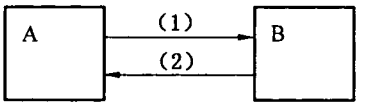
A 向 B 发送以下标记：text2//eKAB(RB// B//text3)(B 包含的内容是可选的)。

相互鉴别模型

相互鉴别用于终端和主机间的软件应用和保密数据文件的传输。

两次鉴别

在该鉴别机制下，通过生成、确认时间戳或序列数的方式控制唯一性/时效性。详见ISO/IEC 9798-2:1994。



(1)：A 向 B 发送以下标记：text1//eKAB(TA 或 NA// B//text2)；

(2)：B 向 A 发送以下标记：text3//eKAB(TB 或 NB// A//text4)；

TA、TB：时间戳；

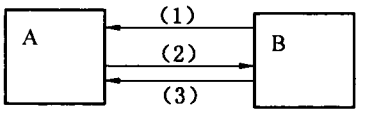
NA、NB：序列数；

B：B 的标识符(包含的内容是可选的)；

A：A 的标识符(包含的内容是可选的)。

三次鉴别

在该鉴别机制下，通过生成、确认一随机数的方式控制随机数唯一性/时效性。详见ISO/IEC 9798-2：1994。



(1)：B 向 A 发送一随机数：RB，可选的文本域 text1；

(2)：A 向 B 发送以下标记：text2//eKAB(RA//RB// B//text3)(B 包含的内容是可选的)；

(3)：B 向 A 发送以下标记：text4//eKAB(RB//RA//text5)；

RA、RB：随机数。

A.1.2 应用 ISO/IEC 9798-2：1994 保护文件传输

依赖带标记的文本域的使用：

——如果加密文本域为空，该机制用于文件传输之前的鉴别；

——如果加密文本域和传输的文件相同，则相当于发送加密文件；

——如果加密文本域是对称的密钥，则密钥分发与鉴别相结合。

同一功能使用几个密钥时，明文文本域包括用于加密数据的密钥标识符或交换密钥标识符或两者都包括。

A.1.3 使用非对称加密算法和不引入可信赖第三方的鉴别机制

ISO/IEC 9798-3：1993 详细说明使用非对称加密算法的鉴别机制。它说明了提供单方鉴别和相互鉴别的报文交换。

数字签名用于确认实体的身份：通过使用密钥在特殊数据上签名的方式鉴别实体的身份，以此表明它已获知保密签名密钥。鉴别实体拥有相应有效的公共密钥。

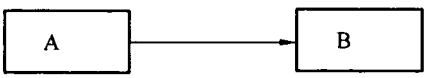
被说明的机制需要使用时间变量参数，例如时间戳、序列数或随机数。使用随机数鉴别的轮数要比使用时间戳或序列数鉴别的轮数多一轮。

单方鉴别模型

单方鉴别用于从终端向主机传输零售支付数据。由主机鉴别终端。

一次鉴别

在该鉴别机制下，声明方 A 发起该过程，并由检验方 B 鉴别。通过生成和确认时间戳或序列数控制唯一性/时效性。详见 ISO/IEC 9798-3：1993。



A 向 B 发送以下标记：CertA//TA 或 NA//B//Text1//sSA(TA 或 NA//B//Text2)；

CertA：证书(可选)；

TA：时间戳；

NA:序列数;

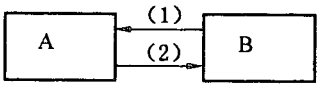
B:B 的标识符;

sSA:使用 A 的密钥的数字签名;

X//Y:数据项 X、Y 的串联。

两次鉴别

在该鉴别机制下,声明方 A 由发起该过程检验方 B 鉴别。通过生成和确认随机数控制唯一性/时效性。详见 ISO/IEC 9798-3:1993。



(1):B 向 A 发送一随机数:RB 和可选的文本域 Text1;

(2):A 向 B 发送以下标记:CertA//RA//RB//B//Text2//sSA(RA//RB//B//Text3);

RA,RB:随机数;

CertA:A 的证书(可选);

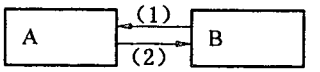
B:B 的标识符。

相互鉴别模型

相互鉴别用于终端和主机间的软件应用,保密数据文件传输。

两次鉴别

在该鉴别机制下,通过生成和确认时间戳或序列数控制唯一性/时效性。详见 ISO/IEC 9798-3:1993。



(1):A 向 B 发送以下标记:CertA//TA 或 NA//B//Text1//sSA(TA 或 NA//B//Text2);

(2):B 向 A 发送以下标记:CertB//TB 或 NB//A//Text3//sSB(TB 或 NB//A//Text4);

CertA:A 的证书(可选);

CertB:B 的证书(可选);

TA、TB:时间戳;

NA、NB:序列数;

B:B 的标识符;

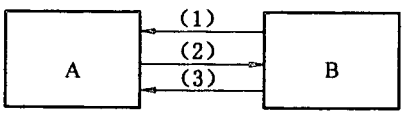
A:A 的标识符;

sSA:使用 A 的密钥的数字签名;

sSB:使用 B 的密钥的数字签名。

三次鉴别

在该鉴别机制下,通过生成和确认随机数控制唯一性/时效性。详见 ISO/IEC 9798-3:1993。



(1):B 向 A 发送随机数 RB 和可选的文本域 Text1;

(2):A 向 B 发送以下标记:CertA//RA//RB//B//Text2//sSA(RA//RB//B//Text3)(B 包含的内容是可选的);

(3):B 向 A 发送以下标记:CertB//RB//RA//A//Text4//sSB(RB//RA//A//Text5)(A 包含的内容是可选的);

RA、RB:随机数。

A.1.4 应用 ISO/IEC 9798-3:1993 保护文件传输

依赖带以下标记的文本域：

——如果加密的文本域为空，则该机制用于文件传输前的鉴别；

——如果加密的文本域和传输的文件相同，且数字签名允许报文恢复(见数字签名条款)，则它相当于发送加密文件；

——如果加密的文本域和传输的文件相同，且数字签名不允许报文恢复(见数字签名条款)，则该文件同它的签名一起传输；

——如果加密的文本域是对称密钥，如果数据签名允许报文恢复(数字签名条款)，密钥分发结合着鉴别过程。

当相同的功能使用几个密钥时，明文文本域包括用于数据签名的密钥标识符或交换密钥的标识符，或两者都包括。

A.1.5 引入可信赖第三方的鉴别机制

当使用 TTP 时 ISO/IEC 9798-2:1994 和 ISO/IEC 9798-3:1993 中说明的机制可采用。原则是结合密钥交换进行鉴别。当使用对称加密算法时，不需要有双方实体共享的通用保密鉴别密钥，而是每个实体拥有一个和 TTP 共享的保密密钥，实体要求从 TTP 获得交易密钥。

A.1.6 使用密码检验函数的鉴别机制

ISO/IEC 9798-4:1995 详细说明使用密码检验函数的实体鉴别机制。详细说明提供单方鉴别和相互鉴别的报文交换。

ISO/IEC 9798-4:1995 基于共享一共同保密鉴别密钥，通过证明它对保密鉴别密钥的了解来确证实体的身份。

没有说明参与方了解密钥的方法。

详细说明的机制要使用时间变量参数，例如时间戳，序列数或随机数等。使用随机数鉴别的轮数要比使用时间戳或序列数鉴别的轮数多一轮。

注：原则与 ISO/IEC 9798-2:1994 一致，密码检验函数替换对称加密算法。ISO/IEC 9798-4:1995 提供该函数的例子。

A.2 数字签名

文件可以用下列方式签名：

——用对称密码系统；

——用非对称密码系统。

A.2.1 使用包括可信赖第三方的对称密码系统

该条款说明适于数字签名(见数字签名的定义)预期结果的方案，数字签名使用对称密码系统。

发送方和接收方通过可信赖第三方通信。发送方与可信赖第三方共享一密钥 Ks，接收方与可信赖第三方共享另一个不同的密钥 Kr。这些密钥建立的方式不在本标准范围之内。

a) 发送方用 Ks 加密该文件，发送给可信赖第三方；

b) 可信赖第三方用 Ks 解密文件；

c) 可信赖第三方增加“已接收到来自发送方的报文”声明，并用 Kr 加密；

d) 可信赖第三方发送加密的文件给接收方；

e) 接收方用 Kr 解密文件。

A.2.2 使用非对称密码系统

多数的数字签名方案基于公钥密码系统。

原则如下：发送方用私钥加密文件，对文件签名；接收方用发送方的公钥解密，验证签名。

为防止发送方重用相同签名发送相同文件两次，数字签名应包括时间戳。日期和时间附于文件上，

和文件的剩余部分一同签名。

为确保不可否认性，密钥存放在安全的密码设备内或由可信赖的第三方保存。

当把数字签名和公钥加密结合在一起时，签名操作在加密操作前执行：

a) 发送方用它的私钥签名；

b) 发送方用接收方的公钥加密已签名的文件，发给接收方；

c) 接收方用它的私钥解密该文件；

d) 接收方用发送方的公钥确认该签名。

数字签名方案存在的两种类型：

——提供报文恢复：当验证过程解密了报文信息；

——不提供报文恢复：当验证过程需要提供报文信息时。

GB 15851—1995 详细说明向有限长度报文的数字签名提供报文恢复和使用公钥密码系统的方案。它不涉及哈希函数的使用。本标准在文件长度有限时可用于安全文件传输，该机制等同于加密，因该文件无需传输，它的签名单独传输，接收方可通过数字签名恢复该文件。

注：ISO/IEC 9796-2:1994 说明数字签名方案，该方案提供使用哈希函数的报文恢复。

A.2.3 允许数字签名的算法例子

DSA

数字签名算法(DSA)由美国国家标准和技术协会(NIST)提出，用于他们的数字签名标准(DSS)。它详细说明了公钥数字签名算法。DSA 不允许报文恢复。

RSA(Rivest，Shamir，Adleman)

RSA 允许报文恢复。

A.2.4 哈希函数

在实际的实施过程中，公钥算法效率太低，不用于对大文件的签名。哈希函数可将文件缩短为概要输入数字签名机制。原则如下：发送方将文件缩短为报文摘要，叫做哈希，并用自己的私钥加密哈希，然后把文件和签名的哈希发给接收方。接收方生成一已接收文件的哈希，用发送方的公钥解密已签名的哈希。如果两结果匹配，签名是合法的。档案系统可把文件的哈希和时间戳一同存储(传输的时间戳或提交到档案系统的时间戳，或两者兼有)。接收方存储已收到的数字签名，如果对签名有异议，可以重新确认。

哈希函数的例子：

——SHA-1 可作为任意长度的报文输入，生成 160 位的哈希。

——使用对称分组算法的哈希函数：

- ISO/IEC 10118-1《信息技术　安全技术　哈希函数　第 1 部分：概述》；ISO/IEC 10118.2《信息技术　安全技术　哈希函数　第 2 部分：使用 n 位分组密码算法的哈希函数》。
- ISO/IEC 10118-2:1994，详细说明使用 n 位分组密码算法的哈希函数(拥有 n 位分组长度的明文块和密文块)。不对 n 位分组密码算法详细说明。详细说明了两类哈希函数。第一类提供小于或等于 n 位长度的哈希值，第二类提供小于或等于长度为 $2n$ 的哈希值。
- ISO/IEC 10118-3，标准的 SHA-1，RIPEMD-128 和 RIPEMD-160。

A.3 报文鉴别码

报文鉴别码可用于鉴别文件的来源和保护从发送方到接收方文件的完整性。它由文件发送方生成，并和文件一同传输。

报文鉴别码可应用于整个文件或文件的一部分。

GB/T 15852.1—2008 详细说明了数据完整性机制：该方法使用密钥和 n 位分组密码算法来计算 m 位密码校验值。密码校验值作为报文鉴别码(MAC)。

A.4 密码算法

A.4.1 对称密码

ISO/IEC 10116:1993 的标题为《信息技术 n 位分组密码算法的操作模式》，说明了 n 位分组密码算法的 4 种操作模式(它并不对 n 位分组密码算法进行说明)：

——电子编码本模式(ECB)；

——密码块链接模式(CBC)；

——密码反馈模式(CFB)；

——输出反馈模式(OFB)。

和每种模式各属性的注释。

注：当 $n=64$ 时，ISO 8372:1987 与 ISO/IEC 10116:1993 一致。

A.4.2 非对称密码

RSA 是非对称密码的例子。

附 录 B
（资料性附录）
实施的例子

B.1 系统的说明

该例子涉及的 POS 终端构成如下：

——软件：

- 操作系统的安全应用管理器部分；
- 若干零售银行业务应用；
- 每种应用的参数文件，包括 BIN 列表，活动表，最低限度……

——硬件：

- 终端(CPU，ROM，RAM，……)；
- 安全密码处理器；
- 可移动的 IC 卡，收单机构用于识别和鉴别商户。

设备连接的不同服务器如下：

——生产商服务器，用于下载应用管理器；

——应用提供商服务器，用于下载应用软件；

——参数服务器，收单机构控制，用于下载参数；

——收单机构服务器，接收金融交易文件。

B.2 终端的密码函数

注解：

——A＝eK(B)：使用对称密钥 K 生成的 B 的加密数据；

——B＝dK(A)：使用密钥 K 解密密文 A，恢复为明文 B。

B.2.1 软件下载

B.2.1.1 完整性确认：非对称算法

非对称算法用于软件下载的完整性确认。

这种方法将公钥保留在终端。该密钥不要求机密性保护，但要防止被替换。

该方法防止生成虚假签名，甚至于在已经成功攻击终端的安全设备的情况下，也可防止生成虚假签名。

B.2.1.2 相互鉴别：对称算法

对称算法用于相互鉴别。

不管使用何种算法，相互鉴别都要求使用存放在终端的密钥。

为防止使用从泄密的终端获取的密钥来伪造终端，下载应用管理器需要衍生鉴别密钥。

实施衍生密钥系统，尽管对称算法可同唯一主密钥和衍生算法一起实施，仍将要求通过非对称算法保留所有终端的全部密钥表。

B.2.1.3 应用管理器实施的密钥管理

B.2.1.3.1 相互鉴别

DEA1 作为对称算法用于相互鉴别。

KAM：用于衍生的相互鉴别主密钥，由生产商生成，安装于生产商服务器之上。

KATi：由生产商生成相互鉴别衍生密钥，在交付之前安装于终端的安全密码处理器之上。

TID:终端标识符。

KATi=eKAM(TID);TID=dKAM(KATi)。

B.2.1.3.2 完整性

RSA 作为非对称算法用于完整性鉴别。

SKKI:生产商使用的私钥,用于签名软件(当签名不包括时间戳或序列数时,无需安装在生产商服务器上)。

PKKI:生产商生成的公钥,在交付之前安装在终端的安全密码处理器上。

B.2.1.4 应用实施的密钥管理

B.2.1.4.1 相互鉴别

DEA1 作为对称算法用于鉴别终端。

KAAn:应用 n 的相互鉴别密钥,由应用提供商生成,安装在应用服务器之上。必须安全地发送给终端,在安全密码处理器上进行保护。为达到此目的,生产商应生成非对称密钥对:SKAAn、PKAAn。生产商向所有应用提供商公布公钥,以便于他们可加密 KAAn。每个应用提供商返回密码 ePKAAn(KAAn)给生产商。私有传输密钥 SKAAn 在交付之前,由生产商安装在终端的安全密码处理器之上。

应用管理器软件保留安装在终端上的应用列表和用于相互鉴别的相关密码 ePKAAn(KAAn)。在应用管理器下载操作过程中,应用列表和相关密码传输给终端。

B.2.1.4.2 完整性

RSA 作为非对称算法用于确认应用软件的完整性。

应用提供商 n 生成非对称密钥对:SKAnI、PKAnI。它发布公钥给生产商。

SKAnI:应用提供商 n 使用的私钥,用于签名它的应用软件(当签名不包括时间戳或序列数时,无需安装在服务器上)。

PKAnI:终端已下载的应用管理器中包含的关联密钥。

安装在终端上的终端软件维护应用列表和用于完整性确认的关联公钥。

B.2.2 参数下载

与收单机构相关的密钥,可以保存在可移动的安全加密设备中,由收单机构用于标识和鉴别商户。

B.2.2.1 相互鉴别

DEA1 作为对称算法用于终端的鉴别。

KAQM:收单机构和终端的相互鉴别的主密钥,由收单机构生成,安装在参数服务器上。

KAQRk:相互鉴别的衍生密钥,由收单机构生成,安装在零售商 k 的终端上,例如通过商户的 IC 卡进行安装。

RID:零售商标识符。

KAQRk=eKAQM(RID)。

B.2.2.2 完整性确认

RSA 作为非对称密钥用于确认应用参数的完整性。

SKPI:收单机构使用的私钥,用于签名它的应用参数(需作为签名安装在服务器之上,须包括时间戳或序列数)。

PKPI:由终端使用的包含在商户 IC 卡中关联公钥。

B.2.3 交易上载

B.2.3.1 相互鉴别

当完整性服务和接收不可否认性服务按照本标准实施时,在传输交易文件之前,本标准不再明确提出其他的鉴别的安全要求。

本例实现了这两种服务。

B.2.3.2 完整性确认:对称算法

对称算法用于交易文件的完整性确认。

完整性确认使用基于衍生密钥的方法,该项服务由收单机构服务器提供终端的鉴别服务。

DEA1 作为对称算法用于交易文件的完整性确认。

KTQM:收单机构的主密钥,由收单机构生成,安装在收单机构服务器上。

KTQRk:完整性确认衍生密钥,由收单机构生成,加载于商户 IC 卡上。

KTQRk=eKTQM(RID)。

使用衍生密钥可防止生成虚假签名,甚至于在已经成功攻击终端安全设备的情况下,也可防止生成虚假签名。

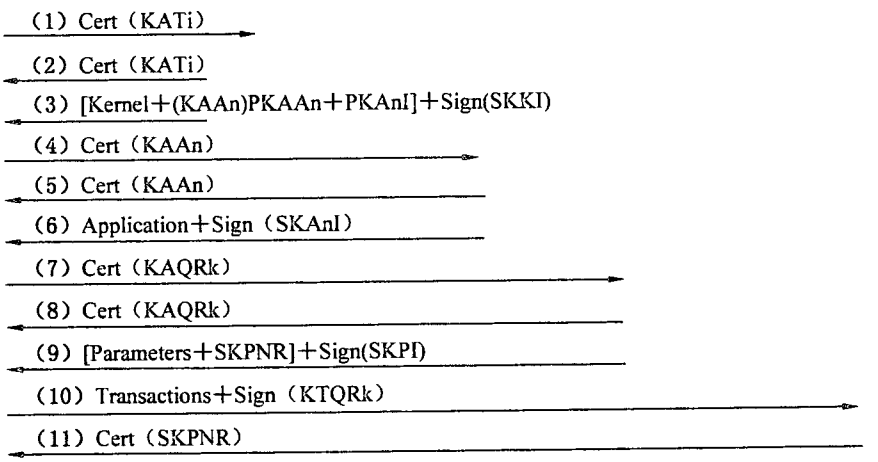
B.2.3.3 接收的不可否认性:非对称算法

该服务使用非对称算法,私钥 SKPNR 由收单机构生成并驻留在收单机构服务器中,当成功接收交易文件和确认完整性时,私钥 SKPNR 用于生成实时证书。

保护防止替换的公钥 PKPNR 包含在由收单机构发送的参数文件中并保护其完整性。

终端使用该证书鉴别接收金融交易文件的收单机构服务器,在成功确认证书之后,立即清除该文件。

商户 IC 卡	终端 i	生产商服务器	应用服务器 n	参数服务器	收单机构服务器
KAQRk	KATi	KAM	KAAn	KAQM	KTQM
PKPI	PKKI	(SKKI)	PKAAn	(SKPI)	SKPNR
KTQRk	SKAAn	PKAnI	(SKAnI)		



注:(K)表示密钥 K 无需安装在服务器之上。

(1)(2)应用管理器的下载:终端和使用对称衍生密钥 KATi 的生产商服务器之间的相互鉴别。

(3)下载应用服务器+在应用下载中使用的密钥:生产商服务器使用非对称密钥 SKKI 签名。

(4)(5)应用下载:终端和使用对称密钥 KAAn 的应用服务器相互鉴别。

(6)应用下载:应用服务器使用非对称密钥 SKAnI 签名。

(7)(8)参数下载:终端和使用对称衍生密钥 KAQRk 的参数服务器相互鉴别。

(9)参数下载+交易上载过程使用的密钥:参数服务器使用非对称密钥 SKPI 签名。

(10)交易文件上载:终端使用对称衍生密钥 KTQRk 签名。

(11)交易文件上载:收单机构服务器使用非对称密钥 SKPNR 认证。

图 B.1

附 录 C
（资料性附录）
保证文件传输完整性确认的示例

该示例来自澳大利亚的国家标准 AS 2805-10。

C.1 范围

该示例不包括文件传输处理机制的任何规则，仅限于数据校验方式。该示例详细说明了两个通信实体传输期间确保文件完整性的方法：

a） 直接从文件计算出来完整性校验值；

b） 用文件的哈希结果计算出完整性校验值。

完整性校验值称为文件校验值(FVV)，参见 4.3。

该示例不包括确保文件机密性或文件传输的技术。

注：发送 FVV 管理文件的报文示例参见附录 A 和附录 B 中的图 B.1。

C.2 定义

以下定义适用于本示例。

C.2.1 数据密钥

用于数据加密或解密的密码密钥。

C.2.2 文件校验值(FVV)

用于文件校验的导出值。

C.2.3 中间节点

向安全密码设备(SCD)提供数据转发服务的计算机系统或设备。

C.2.4 MAC 密钥(KMAC)

用于计算、校验或既计算又校验报文鉴别代码的密钥。

C.2.5 安全密码设备(SCD)

提供安全密码服务的作为系统一部分的接收方；终端密码单元(TCU)是一种安全密码设备(SCD)。

C.2.6 安全机制

相互认可的实体进行手工交付时用以确保物理安全的方法。

C.2.7 主办方

负责文件内容合法性和完整性的实体。

C.3 综述

C.3.1 概述

文件传输完整性确认是独立于文件传输的功能，验证被加载或更新到 SCD 中的文件是否与发送方的一致。通过使用该技术，可以在非安全的网络上发送完整的文件或文件更新，并且在被载入到 SCD 并检验之前，将其存储在中间节点上，因此该方法为网络传输提供了更多的选择性。

这仅仅是对 SCD 中的文件进行 FVV 交换和验证，并且是在安全报文交换中进行的。

这一节提供了使用的原则的概述。

管理文件传输完整性确认的步骤如下：

a） 报文鉴别；

b) 对文件进行哈希；

c) FVV 加密。

C.3.2 原则

强调文件传输完整性确认的原则如下：

——在任何情况下，整个文件应使用 FVV；

——FVV 应通过安全机制、加密或 MAC 方式从发起方到接收方进行传输；

——只有在 FVV 确认之后才能使用文件；

——如果接收到的是更新文件，那么在更新被应用前应使用 FVV 验证该文件的正确性；

——主办方应负责文件的准确性和 FVV 的生成；

——文件接收方应通过 FVV 检验文件的完整性；

——接收方应使用 SCD 安全地计算出 FVV。

C.4 功能元的说明

C.4.1 文件确认值

FVV 衍生于文件的内容，目的是确认文件的完整性。

当进行修正时，应使用 FVV 检验文件的完整性。文件被修正时，修正后的文件的完整性应使用 FVV 进行检验。这可确保修正被正确地应用。

C.4.2 FVV 衍生

C.4.2.1 概述

当 SCD 能支持基于密钥的技术，FVV 应通过基于密钥的模式衍生。当基于密钥的技术不适合，例如，由于接收方数量过多的原因，可使用基于哈希的技术，不要求使用密钥进行计算。

FVV 应基于完整的物理文件进行计算。

基于密钥的技术将只使用 ISO 9807:1991 上所说明的算法。

除了不使用密钥之外，非基于密钥技术在操作上和基于密钥的技术相似。尽管使用 ISO 9807:1991 中的单倍和双倍长度的哈希函数会简单一些，但哈希函数并不仅限于某种特定的方法。

C.4.2.2 基于密钥的 FVV

FVV 通过使用 SCD 中指定的特定密钥，通过 MAC 方式进行计算。

C.4.2.3 非基于密钥 FVV

使用哈希算法计算文件 FVV。

C.4.3 安全 FVV 传输

C.4.3.1 概述

FVV 加密或进行 MAC 计算用于保护 FVV 在主办方和 SCD 间传输。

C.4.3.2 基于密钥的 FVV

因 FVV 是对文件进行报文鉴别的结果，所以不需要额外的工作。

C.4.3.3 非基于密钥的 FVV

非基于密钥的 FVV 应使用 MAC 密钥(MAC 密钥应遵循我国密码管理部门的有关规定)或使用适当的数据保护方式进行传输。FVV 可以通过使用 KD 进行加密或使用 KMAC 进行 MAC 计算。

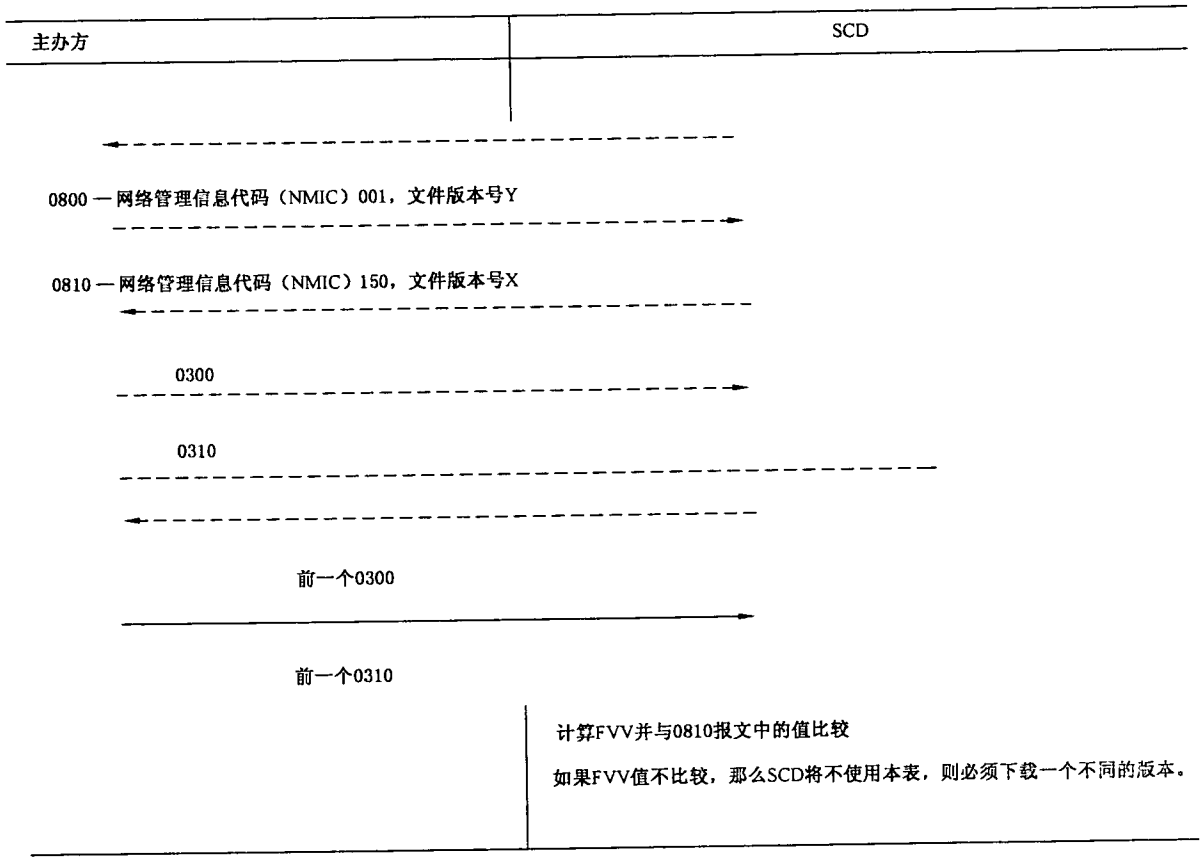
推荐使用 MAC 密钥方式。

C.5 操作

主办方使用基于密钥或非基于密钥的模式衍生文件的 FVV。一旦衍生，FVV 由主办方进行 MAC 计算或加密，并安全地传送到目的地。接收方对接收或更新的文件用相同的方法衍生 FVV，并与接收到的 FVV 值进行比较。FVV 中的差异表明文件不同于预期或文件没有正确更新。

注：本示例说明需要同时保存当前的活动文件和替换文件。

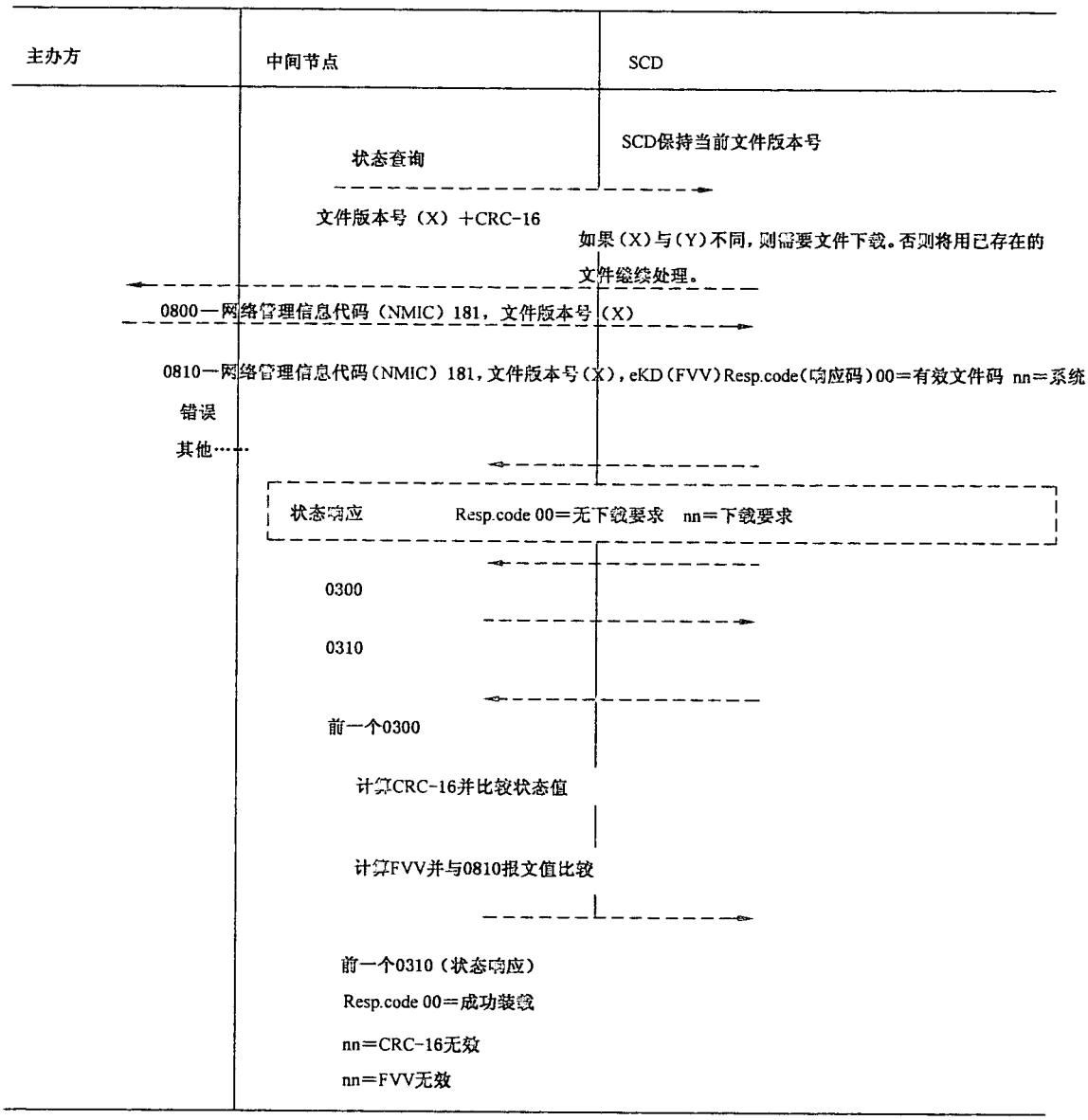
直接发送 FVV 管理文件到 SCD 的报文流例子



注：上述报文类型遵循 AS 2805-2。

图 C.1　报文顺序——直接发送 FVV 管理文件到 SCD 的报文流例子

通过中间节点发送 FVV 管理文件到 SCD 的报文流例子

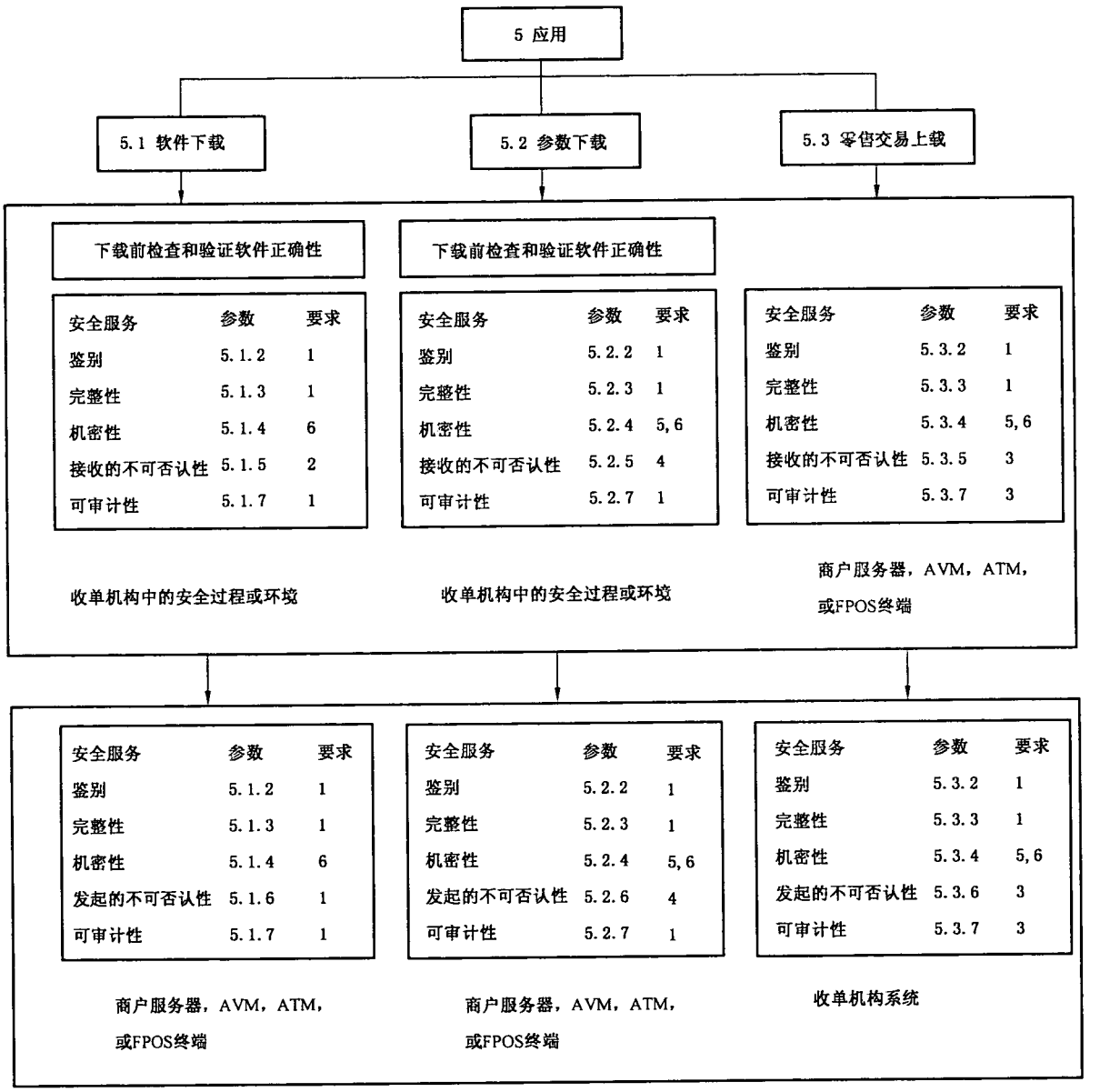


注 1："nn"是用于私有使用的保留码。

注 2：上述报文类型遵循 AS 2805-2。

图 C.2　报文顺序——通过中间节点发送 FVV 管理文件到 SCD 的报文流例子

附 录 D
（资料性附录）
安全服务的图形概要参考



图例(要求)	
1＝应	4＝如果被主办方要求则需要
2＝宜	5＝当要求满足当地法规时需要
3＝不要求	6＝对敏感数据需要

中 华 人 民 共 和 国
国 家 标 准
银行业务 安全文件传输(零售)
GB/T 23695—2009
*
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.spc.net.cn
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 2 字数 49 千字
2009年8月第一版 2009年8月第一次印刷
*
书号:155066·1-38453 定价 30.00 元

GB/T 23695-2009

打印日期:2009年9月7日