重要门禁系统
密码应用指南

国家密码管理局
2009 年 11 月

目 录

前　言

本指南由国家密码管理局提出。

本指南起草单位：上海复旦微电子股份有限公司，上海华虹集成电路有限责任公司，兴唐通信科技有限公司，北京中电华大电子设计有限责任公司，上海华申智能卡应用系统有限公司，同方微电子有限公司，航天信息股份有限公司，复旦大学。

本指南由国家密码管理局负责解释。

1. 范围

本指南规定了采用非接触式 IC 卡的重要门禁系统中采用密码安全技术时，系统中使用的密码设备、密码算法、密码协议和对密钥管理的相关要求。

本指南适用于以下两种情况：

1）新建重要门禁系统的设计与实现；

2）按照国家密码管理部门要求实施的重要门禁系统密码子系统的改造。

2. 密码系统概述

2.1 系统构成

基于非接触式 IC 卡的重要门禁系统的密码应用涉及应用系统、密钥管理及发卡系统，如图 1 所示。

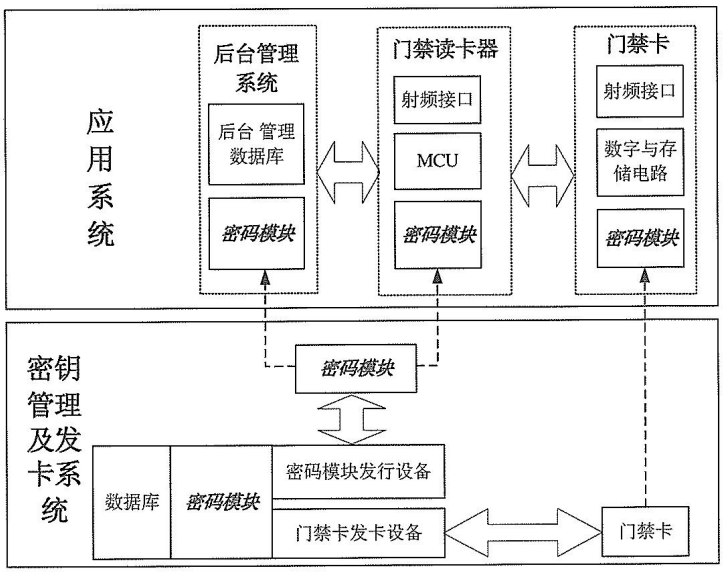

图 1 重要门禁系统中密码应用结构图

2.2 应用系统

在应用系统中，一般由门禁卡、门禁读卡器和后台管理系统构成，通过各设备内的密码模块对系统提供密码安全保护。其中，

1）门禁卡内的密码模块：用于门禁读卡器或后台管理系统对门禁卡进行身份鉴别时（鉴别门禁卡是否合法）提供密码服务（如计算鉴别码）；

2）门禁读卡器/后台管理系统内的密码模块：用于对门禁卡进行身份鉴别时提供密码服务（如密钥分散、验证鉴别码等）。在重要门禁系统的具体方案设计时，可选择在门禁读卡器或后台管理系统内配用密码模块。

2.3 密钥管理及发卡系统

密钥管理及发卡系统的功能是为重要门禁系统的密码应用生成密钥，并通过密码模块发行设备发行（初始化和注入密钥）密码模块，通过发卡设备对门禁卡发卡（初始化、注入密钥和写入应用信息）。

密钥管理及发卡系统中的密码设备提供密钥生成、密钥分散以及对门禁卡发卡时的身份鉴别等密码服务。

3. 与密码相关的安全技术要求

3.1 密码应用安全技术要求

基于非接触式 IC 卡的重要门禁系统中的密码应用方案要通过国家密码管理部门论证。

3.2 密码设备安全技术要求

基于非接触式 IC 卡的重要门禁系统中的密码设备包括：应用系统密码模块、密钥管理及发卡系统密码模块，具体密码设备的配用见图 1。

在重要门禁系统中使用的所有密码设备要通过国家密码管理局审批。

在重要门禁系统中使用的所有密码设备应具有必要的物理防护措施，以保证

密码安全。

3.3 密码算法安全技术要求

在重要门禁系统中所配用的密码算法必须符合国家密码管理局的要求，密码算法应用方案必须通过国家密码管理局的审批。

3.4 密码协议安全技术要求

在重要门禁系统中，须实现门禁读卡器或后台管理设备对门禁卡的身份鉴别，在身份鉴别过程中所使用的认证协议要通过国家密码管理局的审批。

3.5 密钥管理安全技术要求

3.5.1 密钥生成

密钥应由符合国家密码管理要求的随机数产生，应保证所生成密钥的机密性和随机性。要确保密钥生成过程不可预测，要确保在密钥空间内所生成的任意两个密钥具有相同的概率。

3.5.2 密钥注入

门禁卡发卡和密码模块发行时的密钥注入应注意以下两点：

1）密钥注入过程中不得泄露明文密钥的任何组成部分；

2）在密码设备、接口和传输信道未受到任何可能导致密钥或敏感数据泄露、篡改的状况下，才可以将密钥加载到密码设备中。

3.5.3 其他要求

在密钥生成、注入、更新及存储等的整个使用过程中，应保证密钥不被泄漏。

4. 密码应用参考方案

本指南给出了以下密码应用方案作为参考：

1）基于国产密码算法 SM7 的非接触逻辑加密卡方案，参见附录 A；

2）基于国产密码算法 SM1 的非接触 CPU 卡方案（包括方式 1 和方式 2 两种实现方式），参见附录 B。

5. 其他应考虑的安全因素

在本指南中只强调了对密码应用的安全要求，从系统整体的安全性出发，以下因素在具体系统实现时应加以考虑。

1）后台管理系统的管理要求；

2）门禁读卡器与后台管理系统的安全保障；

3）其他与密码安全机制无关的管理及技术措施，如口令识别、生物特征识别、人员值守等。

在系统方案设计及应用时，需针对具体应用情况在密码安全保障的基础上采取其他适当的管理和技术措施，以增强重要门禁系统的安全性。

附录 A 基于 SM7 算法的非接触式逻辑加密卡方案

A.1. 系统构成

本方案采用基于 SM7 算法的非接触逻辑加密卡作为门禁卡。系统构成示意图如图 A-1 所示。

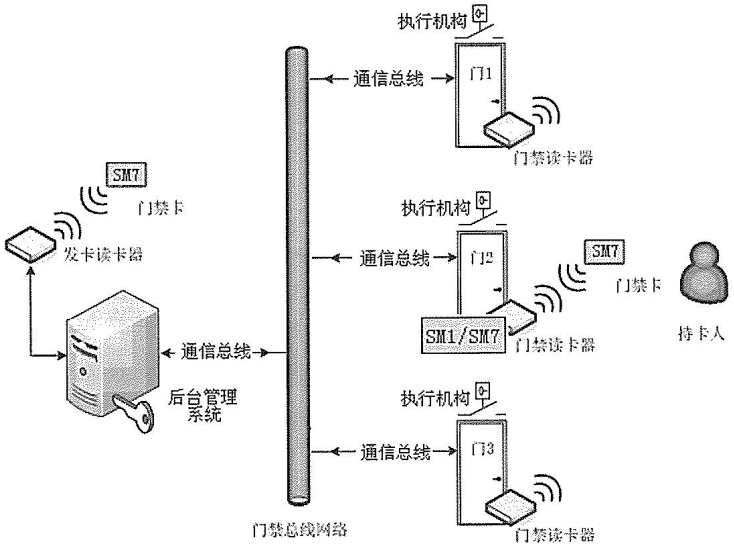

图 A-1 采用基于 SM7 算法的非接触逻辑加密卡作为门禁卡的系统示意图

A.2. 方案原理

本方案采用国家密码管理局指定的 SM1 分组加密算法进行密钥分散，实现一卡一密；采用国家密码管理局指定的 SM7 分组加密算法进行门禁卡与门禁读卡器之间的身份鉴别。本方案原理框图如图 A-2 所示。

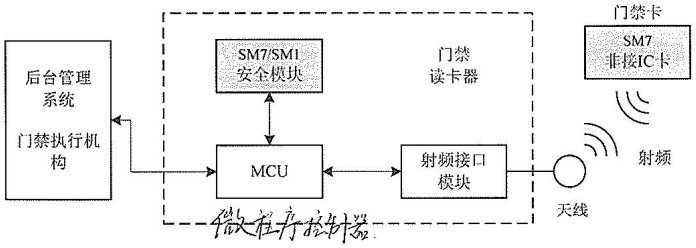

图 A-2 基于 SM7 的非接触逻辑加密卡门禁系统原理框图

门禁卡采用 128 位 SM7 分组密码算法，卡内存放发行信息及卡片密钥。

在门禁读卡器中，射频接口模块负责读卡器与门禁卡间的射频通信；MCU 负责读卡器内部的数据交换，与后台管理系统及门禁执行机构的数据通信。SM7/SM1 安全模块负责读卡器中的安全密码运算，鉴别门禁卡的合法性，存放系统根密钥。

方案中，门禁读卡器上传鉴别结果给后台管理系统，后台管理系统进行实时或非实时门禁权限及审计管理，门禁执行机构具体执行完成门禁操作。

A.3. 密码安全应用流程

A.3.1. 发卡系统

1) 安全模块发行

后台管理系统使用发卡系统密码设备生成门禁系统根密钥。门禁系统根密钥必须被安全地导入安全模块。

2) 门禁卡发卡

后台管理系统使用 SM1 算法对系统根密钥进行密钥分散，实现一卡一密；通过发卡读卡器对卡片进行数据结构的初始化、卡片密钥的下载、发行信息的写入；发卡过程使用 SM7 算法保证数据交换的机密性。

A.3.2. 门禁控制

门禁读卡器上传门禁卡身份鉴别的结果给后台管理系统，用于控制门禁功能

的执行。在该过程中，门禁读卡器使用安全模块的SM1算法对安全模块内预存的系统根密钥进行分散，得到与当前门禁卡对应的卡片密钥，然后使用安全模块的SM7算法和该卡片密钥对门禁卡进行身份鉴别。

A.4. 密码产品现状

本方案中的关键产品是支持SM7分组密码算法的非接触逻辑加密卡和读卡器中的SM7/SM1安全模块。

国家密码管理局商用密码产品定点单位能够提供支持SM7分组密码算法的非接触逻辑加密卡产品和SM7/SM1安全模块。

本方案所需关键产品已经具备批量供货条件。

A.5. 改造内容

对现有不符合本指南要求的门禁系统，如采用该方案，应进行如下改造：

1) 采用支持SM7分组密码算法的非接触逻辑加密卡作为门禁卡。
2) 对门禁读卡器进行升级或替换，采用SM7/SM1安全模块作为密码运算部件。
3) 对后台管理系统进行改造，采用发卡系统密码设备，进行安全模块发行。
4) 对后台管理系统进行改造，增加SM1安全模块进行密钥分散，使用带SM7安全模块的读写器进行发卡操作。

A.6. 方案特点

本方案采用经国家密码管理局认可的商用密码算法产品：支持SM7分组密码算法的非接触逻辑加密卡、SM7/SM1安全模块，安全性具有可靠保证。

使用逻辑加密卡的系统开发简便，具有升级改造周期短的特点。

本方案实现所需的相关商用密码产品已经具备批量供货能力。

附录 B 基于 SM1 算法的非接触式 CPU 卡方案

B.1. 系统构成

本方案采用基于 SM1 算法的非接触 CPU 卡，可采用两种方式实现，即方式 1 和方式 2。系统构成示意图如 B-1 所示。

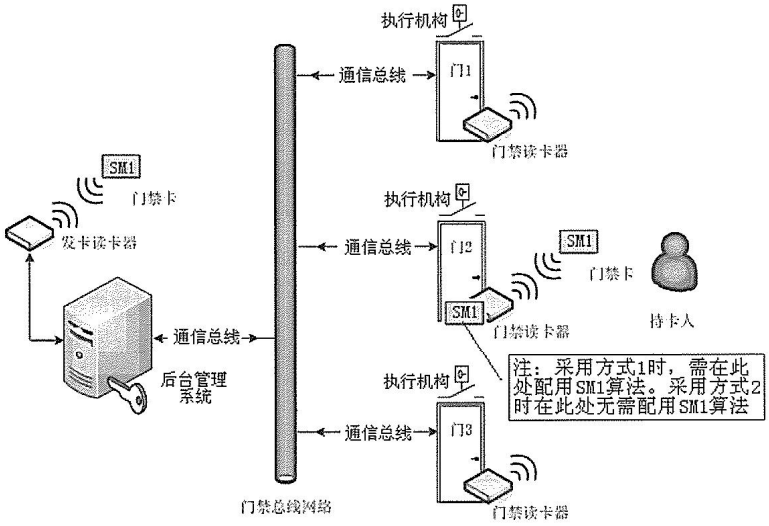

图 B-2 采用基于 SM1 算法的非接触 CPU 卡作为门禁卡的系统示意图

B.2. 方案原理

该方案中门禁卡采用由国家密码管理局指定的 SM1 算法的 CPU 卡，卡内存放发行信息和卡片密钥，并具有符合相关标准的片上操作系统（COS）；门禁卡与非接读卡器之间采用 SM1 算法进行身份鉴别和数据加密通讯；在发卡系统中和读写器中的安全模块中同样采用 SM1 算法进行门禁卡的密钥分散，实现一卡一密。

方式 1，与基于 SM7 算法的非接触式逻辑加密卡所采用的方案类似，主要不同点在于安全模块只需支持 SM1 算法。

其原理框图如图 B-2 所示。

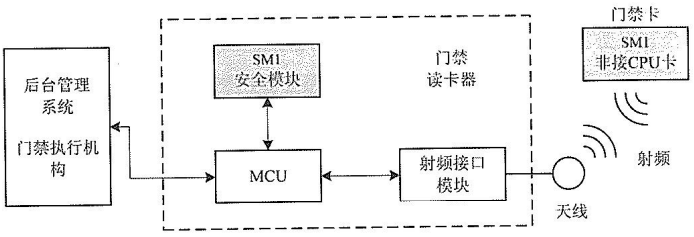

图 B-2 基于 SM1 的非接触 CPU 卡系统方式 1 原理框图

方式 2，适用于门禁读卡器实时在线操作的情况，门禁读卡器中不需包含带有 SM1 算法的安全模块，其原理框图如图 B-3 所示。

该方案中，读卡器不负责鉴别门禁卡的合法性，而是在获得门禁卡产生的身份鉴别信息后，将该需要鉴别的信息反馈给门禁控制后台管理系统。并由后台管理系统（如带有 SM1 算法的安全模块）或与其联网的后台管理系统（带有 SM1 算法的安全模块）鉴别门禁读卡器上传的鉴别信息，判断产生该鉴别信息的门禁卡是否合法，并控制门禁执行机构完成门禁操作，同时门禁服务器还负责门禁读卡器的管理工作。

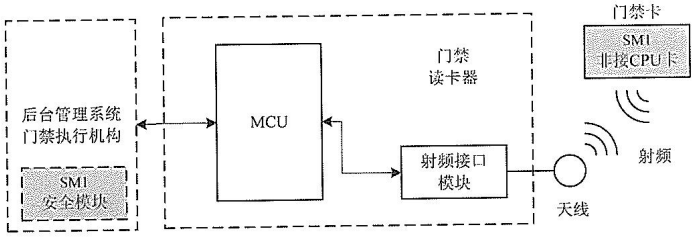

图 B-3 基于 SM1 的非接触 CPU 卡系统方式 2 原理框图

在该方案中，射频接口模块负责读卡器与门禁卡间的射频通信；MCU 控制射频接口模块与门禁卡的通讯，负责实现读卡器内部的数据传送及与后台管理系统的通信功能。

B.3. 密码安全应用流程

B.3.1. 发卡系统

分为门禁卡发卡和门禁读写器安全模块发行/SAM 发卡，上述两个方式一致。

1）安全模块发行

门禁后台管理系统使用发卡系统密码设备生成门禁系统根密钥，安全导入安全模块。

2）门禁卡发卡

后台管理系统使用 SM1 算法对系统根密钥进行密钥分散，实现一卡一密；通过发卡读卡器对卡片利用过程密钥采用 SM1 算法进行卡片身份鉴别，应用目录，文件系统等数据结构初始化并完成卡片密钥 Keyc 的下载，以及对卡片进行持卡人信息与签发单位信息的写入，该过程使用 CPU 卡的发卡流程保证信息写入的安全性、数据的机密性。

B.3.2. 门禁卡控制

针对上述两种方式，实现方式不同，分别论述如下。

1）方式 1 实现方法

方式 1 中，门禁读卡器直接对门禁卡作身份鉴别，并根据结果来控制门禁功能的执行。在该过程与采用 SM7 算法的逻辑加密卡类似，在此不作论述。不同的是身份鉴别时，采用用 CPU 卡的内部认证命令完成对 CPU 门禁卡的身份鉴别而不是逻辑加密卡的专用命令。

2）方式 2 实现方法

方式 2 中，门禁读卡器不直接对门禁卡作身份鉴别，而是由后台管理系统（通过 SM1 算法安全模块）对卡片进行身份鉴别，并根据鉴别结果来控制门禁功能的执行。

具体方法如下：

- 门禁读卡器读取门禁卡的卡片惟一识别号（UID），用于卡片一卡一密密码发散用的特定发行信息 Ci（如有）；
- 门禁读卡器发送一个内部认证命令给门禁卡，即发送随机数 R_n（随机数

的产生由下文论述）给门禁卡，门禁卡内部用存在卡片中的一卡一密密码 Keyc 对该随机数用 SM1 算法做加密运算，得到 R_a' =Enk（Keyc，R_a）并回发给门禁读卡器；

- 门禁读卡器传送该 Ra（也可以不上传），Ra'，UID，Ci（如有）到后台管理系统；
- 后台管理系统在得到第 3 步上传得信息后，即可以进行门禁卡的身份鉴别工作，首先利用门禁卡的 UID，Ci（如有）等分散因子，利用保存在安全模块中的系统根密钥 Keyr，用 SM1 算法分散得到门禁卡的一卡一密密钥 Keyc，即 Keyc=Enk（Keyr，UID，Ci）再用此一卡一密密钥对 Ra（记录在后台管理系统中或由读卡器上传）采用 SM1 算法做加密运算，即 Ra"=Enk(Keyc，Ra)，如果 Ra' ==Ra"，则卡片的身份鉴别正确，否则鉴别不通过；
- 后台管理系统对比卡片唯一性识别号是否为黑名单，如不是，则卡片为系统内合法门禁卡，发出开门信息到门禁执行机构开门。同时使用安全模块产生下一次读写器用于身份鉴别的随机数 Ra+1，并同本次鉴别结果（无论本次身份鉴别结果是否合法）发送至门禁读卡器。门禁读卡器接收并存储该随机数用于下一次门禁的内部认证命令的身份鉴别过程。

身份鉴别过程如图 B-4 所示。

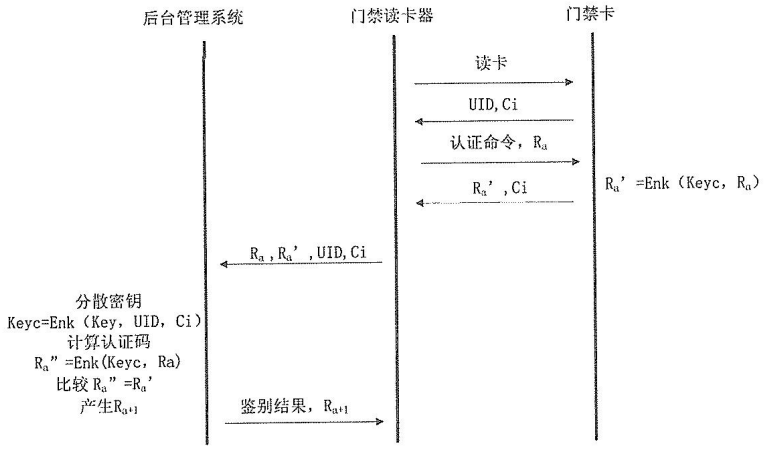

图 B-4　基于后台管理系统 SAM 的身份鉴别过程

由上述过程可以看到，门禁读卡器在身份鉴别中使用的随机数对安全性的影响很大，为了保证该随机数发生器的真随机性，其随机数产生需要由具有真随机数发生器的的安全模块产生，而本方案中推荐由 SM1 安全模块产生该随机数，MCU 利用该随机数进行门禁的身份鉴别过程。门禁读卡器在每次上电后（或规定一定时间）必须在门禁后台管理系统做一个在线注册的工作，表明其上线，与此同时，具有 SM1 算法安全模块后台管理系统利用 SM1 算法安全模块产生一个真随机数并传送给门禁读卡器，门禁读卡器收到该真随机数后存储，以此用于下一次门禁卡的身份鉴别。在一次完整地身份鉴别后，无论鉴别结果如何，后台管理系统均会利用安全模块产生新的随机数，并同鉴别结果一起发送给读写器，读写器存储该新的随机数用于下一次的门禁卡的身份鉴别。

B.4. 密码产品现状

本方案中的关键产品是支持 SM1 算法的非接触 CPU 卡和支持 SM1 算法的安全模块。

目前，已有定点等单位已开发支持 SM1 算法的 CPU 卡，并获得国家密码管理局审批，可以提供批量产品。

支持 SM1 算法的安全模块，已有定点等单位可以提供该产品。目前这些产品均可以批量供货。

B.5. 改造内容

对现有不符合本指南要求的门禁系统，如采用该方案，应进行如下改造：

1) 采用支持 SM1 算法的非接触 CPU 卡作为门禁卡。
2) 对门禁读卡器进行改造，如采用上述方式 1，则读卡器软硬件均需要改造，硬件上增加采用 SM1 算法安全模块（一般为 SAM 卡模式）作为密码运算部件。如果采用方式 2，则读写器软件需要改造，但硬件不需要更改。
3) 对发卡系统进行改造，增加使用 SM1 算法进行密钥分散，硬件上需要增加 SM1 安全模块，发卡程序需要根据应用需求作相应改变。发卡系统增加发卡系统密码设备用于安全模块/SAM 卡的发行。

B.6. 方案特点

本方案采用经国家密码管理局认可的商用密码算法产品：支持 SM1 算法的非接触 CPU 卡、SM1 安全模块，密码安全具有可靠保证。

使用 CPU 卡，具有更高安全性，灵活性好，应用可靠性高，数据交易完整性保障，扩展余地大，适用于具有多应用的场合。如果采用方式 2 进行改造，读卡器硬件无需改造，只需要软件升级，具有升级改造周期短，费用低的特点。