

说明书

一种带低频磁通信的射频通信接入方法

技术领域

本发明涉及通信领域，尤其涉及一种带低频磁通信的射频通信接入方法。

背景技术

随着电子支付技术的发展，支付手段的电子化和移动化是不可避免的必然趋势。移动支付将移动的便携性和电子支付的自主性相结合，庞大的移动用户数量为移动支付的发展提供了良好的基础，因此移动支付所蕴藏的市场潜力巨大。其中，由带低频磁通信的射频 SIM 卡及其读卡器所组成的近距离通信系统属于一种典型的移动支付应用方式。在由带低频磁通信的射频 SIM 卡及其读卡器所组成的近距离通信系统中，采用低频磁通信进行距离控制，采用射频通信完成交易过程。

当带低频磁通信的射频 SIM 卡作为公交乘车卡、门禁通信卡、信用卡、小额支付卡、考勤卡等智能卡使用时，射频 SIM 卡作为一种身份识别或小额支付的工具，为增加其应用的便捷性，通常需要在极短的时间内完成射频 SIM 卡的接入认证和整个交易过程。

现有的带低频磁通信的射频 SIM 卡近距离通信系统中，由于低频通道的引入，低频通道物理特性决定了其数据传输速率不可能很高，造成接入速率较低。所以带低频磁通信的整个接入速度要低于纯射频通信的接入速度，在一定程度上加大了接入的时间开销，从而加大了整个交易的时间开销，在一定程度上影响了某些应用场合的用户体验满意度。同时，现有的带低频磁通信的射频 SIM 卡近距离通信系统接入过程没有考虑请求方和被请求方之间的

认证，且在后续通信过程中数据没有经过加密，在数据安全性上存在一定的隐患。

发明内容

本发明所要解决的技术问题是提供一种带低频磁通信的射频通信接入方法，加快带低频磁通信的近距离通信系统的射频通信接入速度，提高用户体验满意度。

为解决上述技术问题，本发明提出了一种带低频磁通信的射频通信接入方法，包括：

步骤 a，请求方通过低频通道发送激活请求，即低频特征码，所述低频特征码中包含请求方生成的第一随机数；

步骤 b，被请求方通过低频通道接收所述激活请求，产生激活响应信息，并通过射频通道在第一射频通信地址上发送所述激活响应信息，所述激活响应信息中包含被请求方生成的第二随机数和被请求方的身份标识；

步骤 c，请求方通过射频通道在第一射频通信地址上接收所述激活响应信息，并进行验证，若验证通过，则产生连接请求，并通过射频通道在第二射频通信地址上发送所述连接请求，所述连接请求中包含请求方生成的第三随机数；

步骤 d，被请求方通过射频通道在第二射频通信地址上接收到所述连接请求，并进行验证，若验证通过，则产生连接响应信息，并通过射频通道在第二射频通信地址上发送所述连接响应信息；

步骤 e，请求方通过射频通道在第二射频通信地址上接收所述连接响应信息并验证是否接入成功，若是则通过射频通道在第二射频通信地址上与被请求方进行交易。

进一步地，上述方法还可具有以下特点，所述低频特征码的长度小于等

于 2 字节。

进一步地，上述方法还可具有以下特点，所述低频特征码中只包含所述第一随机数，且所述第一随机数的长度为 1 字节。

进一步地，上述方法还可具有以下特点，所述步骤 b 包括：

步骤 b1，被请求方低频通道接收所述激活请求；

步骤 b2，被请求方生成第二随机数；

步骤 b3，被请求方根据所述激活请求中的第一随机数和射频通道支持的最大频点数，按照双方预设的频率计算方法算出射频通信频率；

步骤 b4，被请求方根据所述第一随机数，按照双方预设的地址计算方法

计算出所述第一射频通信地址；

步骤 b5，被请求方生成第一加密标识，所述第一加密标识中包含被请求

方选择的交易会话加密方式和支持的加密算法；

步骤 b6，被请求方以所述第二随机数、被请求方的身份标识和所述第一

加密标识为加密输入，以所述第一随机数和第二随机数为加密密钥，采用预

设的加密算法进行加密运算，并取加密结果的前 4 字节作为第一验证码；

步骤 b7，被请求方生成激活响应信息，所述激活响应信息包括所述第二

随机数、被请求方的身份标识、第一加密标识和第一验证码；

步骤 b8，被请求方通过射频通道在第一射频通信地址上用计算出的射频

通信频率发送所述激活响应信息。

进一步地，上述方法还可具有以下特点，所述步骤 b2 中，所述第二随机

数的长度为 4 字节。

进一步地，上述方法还可具有以下特点，所述步骤 b3 中，所述预设的

频率计算方法为：以所述射频通道支持的最大频点数为模，对所述第一随机

数进行求余运算，得到的余数与射频通信所用频率的编号相对应，由该编号

索引出所述射频通信频率。

进一步地，上述方法还可具有以下特点，所述步骤 b5 中，所述第一加密标识等于 0 则表示不加密，所述第一加密标识不等于 0 则表示加密，且采用第一加密标识所标识的算法加密。

进一步地，上述方法还可具有以下特点，所述步骤 b6 中，加密输入为 RN2||ID2||ALG1，加密密钥为 RN1||RN2，其中 “||” 表示拼接运算。

进一步地，上述方法还可具有以下特点，所述步骤 c 包括：

步骤 c1，请求方根据所述第一随机数和射频通道支持的最大频点数，按照双方预设的频率计算方法算出射频通信频率；

步骤 c2，请求方根据所述第一随机数，按照双方预设的地址计算方法算出所述第一射频通信地址；

步骤 c3，请求方通过射频通信通道在第一射频通信地址上采用计算出的射频通信频率接收所述激活响应信息；

步骤 c4，请求方以所述激活响应信息中的第二随机数、被请求方的身份标识和所述第一加密标识为加密输入，以所述第一随机数和第二随机数为加密密钥，采用预设的算法进行加密运算，并取加密结果的前 4 字节作为第一验证码，然后将该第一验证码与所述激活响应信息中包含的第一验证码比较，若两者相同，则验证通过，执行步骤 c5，否则接入错误，结束本次接入过程；

步骤 c5，请求方产生第三随机数；

步骤 c6，请求方生成第二加密标识，所述第二加密标识中包含请求方选择的交易会话加密方式和支持的加密算法；

步骤 c7，请求方以所述第三随机数、请求方的身份标识和所述第二加密标识为加密输入，以所述第一随机数、第二随机数和第三随机数为加密密钥，采用预设的加密算法进行加密运算，并取加密结果的前 4 字节作为第二验证码；

步骤 c8, 请求方生成连接请求, 所述连接请求中包含所述第三随机数、请求方的身份标识、第二加密标识和第二验证码;

步骤 c9, 请求方根据所述第一随机数和第二随机数, 按照双方预设的地址计算方法计算出第二射频通信地址;

步骤 c10, 请求方通过射频通道在第二射频通信地址上采用所述射频通信频率发送所述连接请求。

进一步地, 上述方法还可具有以下特点, 所述步骤 c5 中, 所述第三随机数的长度为 3 字节。

进一步地, 上述方法还可具有以下特点, 所述步骤 c7 中, 加密输入为 $RN3||ID1||ALG2$, 加密密钥为 $RN1||RN2||RN3$, 其中 “||” 表示拼接运算。

进一步地, 上述方法还可具有以下特点, 所述步骤 c9 中, 所述第二射频通信地址的计算方法为: 以所述第一随机数和第二随机数为输入, 进行预设的单向函数运算, 并将得到的运算结果的全部或部分内容作为所述第二射频通信地址。

进一步地, 上述方法还可具有以下特点, 所述步骤 c9 中, 所述第二射频通信地址的计算方法为: 取 $RN1||RN2$ 的全部或部分内容作为第二射频通信地址, 其中 “||” 表示拼接运算。

进一步地, 上述方法还可具有以下特点, 所述步骤 d 包括:

步骤 d1, 被请求方根据所述第一随机数和第二随机数, 按照双方预设的地址计算方法计算出第二射频通信地址;

步骤 d2, 被请求方通过射频通道在第二射频通信地址上采用所述射频通信频率接收所述连接请求;

步骤 d3, 被请求方以所述连接请求中的第三随机数、请求方的身份标识和所述第二加密标识为加密输入, 以所述第一随机数、第二随机数和第三随机数为加密密钥, 采用预设的加密算法进行加密运算, 并取加密结果的前 4

字节作为第二验证码，并将该第二验证码与所述连接请求中包含的第二验证码进行比较，若两者相同则验证通过，否则验证失败；

步骤 d4，被请求方根据第二验证码的验证结果，设置连接成功/失败的状态标识，若第二验证码验证通过，则将所述连接成功/失败的状态标识设置为连接成功标志，执行步骤 d5，否则将所述连接成功/失败的状态标识设置为连接失败标志，执行步骤 d6；

步骤 d5，被请求方生成第三加密标识，所述第三加密标识中包含被请求方最终选择的交易会话加密方式和支持的加密算法；

步骤 d6，被请求方以所述第三随机数、连接成功/失败的状态标识、第三加密标识为加密输入，以所述第一随机数、第二随机数和第三随机数为加密密钥，采用预设的加密算法进行加密运算，并取加密结果的前 4 字节作为第三验证码；

步骤 d7，被请求方生成连接响应信息，所述连接响应信息中包含连接成功/失败的状态标识、第三加密标识和第三验证码；

步骤 d8，被请求方通过射频通道在第二射频通信地址上发送所述连接响应信息。

进一步地，上述方法还可具有以下特点，所述步骤 d6 中，加密输入为 RN3||SFF||ALG3，加密密钥为 RN1||RN2||RN3，其中 “||” 表示拼接运算。

进一步地，上述方法还可具有以下特点，所述步骤 e 包括：

步骤 e1，请求方通过射频通道在第二射频通信地址上接收所述连接响应信息；

步骤 e2，请求方以所述连接响应信息中的第三随机数、连接成功/失败的状态标识、第三加密标识为加密输入，以所述第一随机数、第二随机数和第三随机数为加密密钥，采用预设的加密算法进行加密运算，并取加密结果的前 4 字节作为第三验证码，并将该第三验证码与所述连接响应信息中的第

三验证码进行比较，若两者相同则验证通过，执行步骤 e3；否则验证失败，结束本次接入过程；

步骤 e3，请求方根据所述连接响应信息中的连接成功/失败的状态标识判断被请求方接入是否成功，若接入失败，则结束本次接入过程，否则执行步骤 e4；

步骤 e4，请求方与被请求方通过射频通道在第二射频通信地址上进行交易。

进一步地，上述方法还可具有以下特点，所述步骤 e4 中，所述交易中采用会话密钥。

进一步地，上述方法还可具有以下特点，所述会话密钥为 8 字节 $RN1||RN2||RN3$ 或 16 字节 $RN1||RN2||RN3||\underline{RN1||RN2||RN3}$ ，其中“||”表示拼接运算， $\underline{RN1||RN2||RN3}$ 为 $RN1||RN2||RN3$ 的按位取反。

本发明所提供的带低频磁通信的射频通信接入方法，能够加快带低频磁通信的近距离通信系统的射频通信接入速度，提高用户体验满意度。

附图说明

图 1 为请求方的结构框图；

图 2 为被请求方的结构框图；

图 3 为本发明实施例中带低频磁通信的射频通信接入方法流程图。

具体实施方式

以下结合附图对本发明的原理和特征进行描述，所举实例只用于解释本发明，并非用于限定本发明的范围。

首先对本发明提供的带低频磁通信的射频通信接入方法所应用的系统中请求方和被请求方的结构作一介绍。图 1 为请求方的结构框图，如图 1 所

示,请求方 100 包含至少一第一控制模块 101,至少一第一射频通信模块 102,至少一第一低频磁通信模块 103。第一控制模块 101 至少与一个第一射频通信模块 102 和至少一个第一低频磁通信模块 103 连接。图 2 为被请求方的结构框图,如图 2 所示,被请求方 200 包含至少一第二控制模块 201,至少一第二射频通信模块 202,至少一第二低频磁通信模块 203。第二控制模块 201 至少与一个第二射频通信模块 202 和至少一个第二低频磁通信模块 203 连接。当然,这里只是给出了请求方和被请求方的典型结构,在其他的示例中,请求方或被请求方中的多个模块可以合并为一个大的模块,也可以将一个模块拆分为多个小的模块。

图 3 为本发明实施例中带低频磁通信的射频通信接入方法流程图。如图 3 所示,本实施例中,带低频磁通信的射频通信接入方法包括如下步骤:

步骤 301,请求方生成和发送激活请求,即低频特征码;

这里,激活请求是通过低频通道发送的,激活请求也即低频特征码,该低频特征码中包含请求方生成的第一随机数 RN1。较佳的,低频特征码的长度小于等于 2 字节。更佳的,为加快接入速度,低频特征码中可以只包含第一随机数 RN1,且第一随机数 RN1 的长度为 1 个字节。由于低频特征码中包含随机数,而随机数是不断变化的,因此可以保证低频特征码在每次接入认证过程中都不相同。

请求方不断发出激活请求,当被请求方进入允许的接入范围内,被请求方就开始响应。

步骤 302,被请求方接收激活请求;

被请求方通过低频通道接收请求方发送的激活请求。

步骤 303,被请求方生成和发送激活响应信息;

被请求方通过射频通道在第一射频通信地址 add1 上发送激活响应信息,该激活响应信息中包含被请求方生成的第二随机数 RN2 和被请求方的身份标

识 ID2。

具体地，步骤 303 可以包括如下子步骤：

步骤 31，被请求方生成第二随机数 RN2；

优选地，第二随机数 RN2 的长度可以取为 4 字节。

步骤 32，被请求方根据激活请求中的第一随机数 RN1 和射频通道支持的最大频点数，按照双方预设的频率计算方法计算出射频通信频率；

较佳的，频率计算方法可以为：以射频通道支持的最大频点数为模，对第一随机数 RN1 进行求余运算，得到的余数与射频通信所用频率的编号相对应，由该编号索引出所述射频通信频率。

步骤 33，被请求方根据第一随机数 RN1，按照双方预设的地址计算方法计算出第一射频通信地址 add1；

较佳的，第一射频通信地址 add1 的计算可以方法为：以第一随机数 RN1 为输入，进行预设的单向函数运算，并将得到的运算结果的全部或部分内容作为第一射频通信地址 add1。进一步地，第一射频通信地址 add1 的计算方法中可以采用 SHA-1 算法，并取结果前 5 字节作为第一射频通信地址 add1。

步骤 34，被请求方生成第一加密标识 ALG1，第一加密标识 ALG1 中包含被请求方选择的交易会话加密方式（即是否加密）和支持的加密算法；

较佳的，若 $ALG1=0$ ，则表示不加密；若 $ALG1 \neq 0$ ，则表示选择 ALG1 所标识的算法进行加密。

步骤 35，被请求方以第二随机数 RN2、被请求方的身份标识 ID2 和第一加密标识 ALG1 为加密输入，以第一随机数 RN1 和第二随机数 RN2 为加密密钥，采用预设的加密算法进行加密运算，并取加密结果的前 4 字节作为第一验证码 MAC1；

较佳的，加密输入为 $(RN2 || ID2 || ALG1)$ ，加密密钥为 $(RN1 || RN2)$ ，其中 “||” 表示拼接运算。

步骤 36, 被请求方生成激活响应信息, 该激活响应信息中包含第二随机数 RN2、被请求方的身份标识 ID2、第一加密标识 ALG1 和第一验证码 MAC1;

步骤 37, 被请求方通过射频通道在第一射频通信地址 add1 上用所述射频通信频率发送激活响应信息。

步骤 304, 请求方接收和验证激活响应信息;

请求方通过射频通道在第一射频通信地址 add1 上接收被请求方发送的激活响应信息, 并进行验证, 若验证通过, 则执行步骤 305, 否则结束本次接入过程。

具体地, 步骤 304 可以包括如下子步骤:

步骤 41, 请求方根据第一随机数 RN1 和射频通道支持的最大频点数, 按照双方预设的频率计算方法算出射频通信频率, 此处的频率计算方法与步骤 32 中的频率计算方法算一致;

步骤 42, 请求方根据第一随机数 RN1, 按照双方预设的地址计算方法计算出第一射频通信地址 add1;

步骤 43, 请求方通过射频通信通道在第一射频通信地址 add1 上采用所述射频通信频率接收被请求方发送的激活响应信息;

步骤 44, 请求方以激活响应信息中的第二随机数 RN2、被请求方的身份标识 ID2 和第一加密标识 ALG1 为加密输入, 以第一随机数 RN1 和第二随机数 RN2 为加密密钥, 采用预设的算法进行加密运算, 并取加密结果的前 4 字节作为第一验证码 MAC1, 然后将该第一验证码 MAC1 与激活响应信息中包含的第一验证码 MAC1 比较, 若两者相同, 则验证通过, 执行步骤 305, 否则接入错误, 结束本次接入过程。

步骤 305, 请求方生成和发送连接请求;

请求方通过射频通道在第二射频通信地址 add2 上发送连接请求, 连接请求中包含请求方生成的第三随机数 RN3。

具体地，步骤 305 可以包括如下子步骤：

步骤 51，请求方产生第三随机数 RN3；

步骤 52，请求方生成第二加密标识 ALG2，第二加密标识 ALG2 中包含请求方选择的交易会话加密方式和支持的加密算法；

第二加密标识 ALG2 优先选择与第一加密标识 ALG1 相同的加密方式和算法，若无法保持一致则另行选择一种新的加密方式和算法。如果请求方同意被请求方的加密选择，则设置 $ALG2=ALG1$ 。此种情况下，若 $ALG2=0$ ，则表示请求方同样选择不加密；若 $ALG2 \neq 0$ ，则表示请求方选择与被请求方同样的算法加密。如果请求方不支持被请求方的加密选择，则可另选 ALG2 ($ALG2 \neq ALG1$)。此种情况下，若 $ALG2=0$ ，则表示请求方选择不加密；若 $ALG2 \neq 0$ ，则表示请求方选择与被请求方不同的算法加密。

步骤 53，请求方以第三随机数 RN3、请求方的身份标识 ID1 和第二加密标识 ALG2 为加密输入，以第一随机数 RN1、第二随机数 RN2 和第三随机数 RN3 为加密密钥，采用预设的加密算法进行加密运算，并取加密结果的前 4 字节作为第二验证码 MAC2；

较佳的，加密输入为 $(RN3||ID1||ALG2)$ ，加密密钥为 $(RN1||RN2||RN3)$ 。其中 “||” 表示拼接运算。

步骤 54，请求方生成连接请求，连接请求中包含第三随机数 RN3、请求方的身份标识 ID1、第二加密标识 ALG2 和第二验证码 MAC2；

步骤 55，请求方根据第一随机数 RN1 和第二随机数 RN2，按照双方预设的地址计算方法计算出第二射频通信地址 add2；

第二射频通信地址 add2 的计算方法可以为：以第一随机数 RN1 和所述第二随机数 RN2 为输入，进行预设的单向函数运算，并将得到的运算结果的全部或部分内容作为第二射频通信地址 add2。较佳的，第二射频通信地址 add2 计算方法中可以采用 SHA-1 算法，输入为 $(RN1||RN2)$ ，并取结果前 5

字节作为第二射频通信地址 add2。或者，第二射频通信地址 add2 的计算方法也可以为：截取 $(RN1 || RN2)$ 的全部或部分内容作为第二射频通信地址 add2。最佳的， $(RN1 || RN2)$ 为 5 字节，直接作为 add2。

步骤 56，请求方通过射频频道在第二射频通信地址上 add2 采用所述射频频通信频率发送连接请求。

步骤 306，被请求方接收和验证连接请求；

被请求方通过射频频道在第二射频通信地址 add2 上接收到请求方发送的连接请求，并进行验证，若验证通过，则执行步骤 307，否则结束本次接入过程。

具体地，步骤 306 可以包括如下子步骤：

步骤 61，被请求方根据第一随机数 RN1 和第二随机数 RN2，按照双方预设的地址计算方法计算出第二射频通信地址 add2；步骤 61 中的地址计算方法与步骤 55 中的地址计算方法一致。

步骤 62，被请求方通过射频频道在第二射频通信地址 add2 上采用所述射频频通信频率接收连接请求；

步骤 63，被请求方以连接请求中的第三随机数 RN3、请求方的身份标识

ID1 和第二加密标识 ALG2 为加密输入，以第一随机数 RN1、第二随机数 RN2 和第三随机数 RN3 为加密密钥，采用预设的加密算法进行加密运算，并取加密结果的前 4 字节作为第二验证码 MAC2，并将该第二验证码 MAC2 与连接请求中包含的第二验证码 MAC2 进行比较，若两者相同则验证通过，否则验证失败。

步骤 307，被请求方生成和发送连接响应信息；

被请求方通过射频频道在第二射频通信地址 add2 上发送连接响应信息。具体地，步骤 307 可以包括如下子步骤：

步骤 71，被请求方根据第二验证码的验证结果 MAC2，设置连接成功/失

败的状态标识 SFF, 若第二验证码验证 MAC2 通过, 则将连接成功/失败的状态标识 SFF 设置为连接成功标志, 执行步骤 72, 否则将连接成功/失败的状态标识 SFF 设置为连接失败标志, 执行步骤 73;

步骤 72, 被请求方生成第三加密标识 ALG3, 第三加密标识 ALG3 中包含被请求方最终选择的交易会话加密方式和支持的加密算法;

第三加密标识 ALG3 可以与请求方在连接请求中选择的第二加密标识 ALG2 一致, 也可以不一致。如果被请求方同意请求方的加密选择, 则设置 $ALG3=ALG2$ 。此种情况下, 若 $ALG3=0$, 则表示被请求方最终选择与请求方一样不加密; 若 $ALG3 \neq 0$, 则表示被请求方最终选择与请求方在连接请求中选择的 ALG2 所指定的同样的算法加密。如果被请求方不同意请求方的加密选择, 则只能设置 $ALG3=0$, 表示被请求方最终选择不加密。由上可见, 在本发明中, 会话加密算法协商过程中采用被请求方优先的策略。

步骤 73, 被请求方以第三随机数 RN3、连接成功/失败的状态标识 SFF、第三加密标识 ALG3 为加密输入, 以第一随机数 RN1、第二随机数 RN2 和第三随机数 RN3 为加密密钥, 采用预设的加密算法进行加密运算, 并取加密结果的前 4 字节作为第三验证码 MAC3;

较佳的, 加密输入为 $(RN3 || SFF || ALG3)$, 加密密钥为 $(RN1 || RN2 || RN3)$ 。其中 “||” 表示拼接运算。

步骤 74, 被请求方生成连接响应信息, 连接响应信息中包含连接成功/失败的状态标识 SFF、第三加密标识 ALG3 和第三验证码 MAC3;

步骤 75, 被请求方在通过射频通道在第二射频通信地址 add2 上发送连接响应信息。

步骤 308, 请求方接收和验证连接响应消息;

请求方通过射频通道在第二射频通信地址 add2 上接收连接响应信息并验证是否接入成功, 若是则执行步骤 309, 否则结束本次接入过程。

具体地，步骤 308 可以包括如下子步骤：

步骤 81，请求方通过射频通道在第二射频通信地址 add2 上接收连接响应信息；

步骤 82，请求方以连接响应信息中的第三随机数 RN3、连接成功/失败的状态标识 SFF、第三加密标识 ALG3 为加密输入，以第一随机数 RN1、第二随机数 RN2 和第三随机数 RN3 为加密密钥，采用预设的加密算法进行加密运算，并取加密结果的前 4 字节作为第三验证码 MAC3，并将该第三验证码 MAC3 与连接响应信息中的第三验证码 MAC3 进行比较，若两者相同则验证通过，执行步骤 83；否则验证失败，结束本次接入过程；

步骤 83，请求方根据所述连接响应信息中的连接成功/失败的状态标识判断被请求方接入是否成功，若接入失败，则结束本次接入过程，否则执行步骤 309。

至此，请求方和被请求方双方都完成了快速和安全的接入认证以及加密算法与会话密钥的协商过程，进入后续交易处理流程。

步骤 309，进入抗冲突交易流程；

请求方与被请求方通过射频通道在第二射频通信地址 add2 上进行交易。交易会话若需要加密，则可以利用在接入认证阶段双方交换的随机数（RN1、RN2、RN3）使用某种方式生成会话密钥。较佳的，交易会话密钥为 8 字节（RN1||RN2||RN3）或 16 字节（RN1||RN2||RN3|| RN1||RN2||RN3），其中（RN1||RN2||RN3）为（RN1||RN2||RN3）的按位取反。

步骤 310，交易完成；

步骤 311，断开连接，退出。

由上可见，本发明既充分利用低频磁通信控制距离的优势，同时又尽量加快接入速度，进而提高整个交易的响应速度，提高用户体验满意度，并且保证接入的安全性和交易会话数据传输的机密性。

以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1. 一种带低频磁通信的射频通信接入方法,其特征在于,包括:

步骤 a,请求方通过低频通道发送激活请求,即低频特征码,所述低频特征码中包含请求方生成的第一随机数;

步骤 b,被请求方通过低频通道接收所述激活请求,产生激活响应信息,并通过射频通道在第一射频通信地址上发送所述激活响应信息,所述激活响应信息中包含被请求方生成的第二随机数和被请求方的身份标识;

步骤 c,请求方通过射频通道在第一射频通信地址上接收所述激活响应信息,并进行验证,若验证通过,则产生连接请求,并通过射频通道在第二射频通信地址上发送所述连接请求,所述连接请求中包含请求方生成的第三随机数;

步骤 d,被请求方通过射频通道在第二射频通信地址上接收到所述连接请求,并进行验证,若验证通过,则产生连接响应信息,并通过射频通道在第二射频通信地址上发送所述连接响应信息;

步骤 e,请求方通过射频通道在第二射频通信地址上接收所述连接响应信息并验证是否接入成功,若是则通过射频通道在第二射频通信地址上与被请求方进行交易。

2. 根据权利要求1所述的带低频磁通信的射频通信接入方法,其特征在于,所述低频特征码的长度小于等于2字节。

3. 根据权利要求2所述的带低频磁通信的射频通信接入方法,其特征在于,所述低频特征码中只包含所述第一随机数,且所述第一随机数的长度为1字节。

4. 根据权利要求1所述的带低频磁通信的射频通信接入方法,其特征在于,所述步骤b包括:

步骤 b1, 被请求方低频通道接收所述激活请求;

步骤 b2, 被请求方生成第二随机数;

步骤 b3, 被请求方根据所述激活请求中的第一随机数和射频通道支持的最大频点数, 按照双方预设的频率计算方法算出射频通信频率;

步骤 b4, 被请求方根据所述第一随机数, 按照双方预设的地址计算方法计算出所述第一射频通信地址;

步骤 b5, 被请求方生成第一加密标识, 所述第一加密标识中包含被请求方选择的交易会话加密方式和支持的加密算法;

步骤 b6, 被请求方以所述第二随机数、被请求方的身份标识和所述第一加密标识为加密输入, 以所述第一随机数和第二随机数为加密密钥, 采用预设的加密算法进行加密运算, 并取加密结果的前 4 字节作为第一验证码;

步骤 b7, 被请求方生成激活响应信息, 所述激活响应信息包括所述第二随机数、被请求方的身份标识、第一加密标识和第一验证码;

步骤 b8, 被请求方通过射频通道在第一射频通信地址上用计算出的射频通信频率发送所述激活响应信息。

5. 根据权利要求 4 所述的带低频磁通信的射频通信接入方法, 其特征在于, 所述步骤 b2 中, 所述第二随机数的长度为 4 字节。

6. 根据权利要求 4 所述的带低频磁通信的射频通信接入方法, 其特征在于, 所述步骤 b3 中, 所述预设的频率计算方法为: 以所述射频通道支持的最大频点数为模, 对所述第一随机数进行求余运算, 得到的余数与射频通信所用频率的编号相对应, 由该编号索引出所述射频通信频率。

7. 根据权利要求 4 所述的带低频磁通信的射频通信接入方法, 其特征在于, 所述步骤 b5 中, 所述第一加密标识等于 0 则表示不加密, 所述第一加密标识不等于 0 则表示加密, 且采用第一加密标识所标识的算法加密。

8. 根据权利要求 4 所述的带低频磁通信的射频通信接入方法, 其特征在

于, 所述步骤 b6 中, 加密输入为 RN2||ID2||ALG1, 加密密钥为 RN1||RN2, 其中 “||” 表示拼接运算。

9. 根据权利要求 1 所述的带低频磁通信的射频通信接入方法, 其特征在于, 所述步骤 c 包括:

步骤 c1, 请求方根据所述第一随机数和射频通道支持的最大频点数, 按照双方预设的频率计算方法算出射频通信频率;

步骤 c2, 请求方根据所述第一随机数, 按照双方预设的地址计算方法计算出所述第一射频通信地址;

步骤 c3, 请求方通过射频通信通道在第一射频通信地址上采用计算出的射频通信频率接收所述激活响应信息;

步骤 c4, 请求方以所述激活响应信息中的第二随机数、被请求方的身份标识和所述第一加密标识为加密输入, 以所述第一随机数和第二随机数为加密密钥, 采用预设的算法进行加密运算, 并取加密结果的前 4 字节作为第一验证码, 然后将该第一验证码与所述激活响应信息中包含的第一验证码比较, 若两者相同, 则验证通过, 执行步骤 c5, 否则接入错误, 结束本次接入过程;

步骤 c5, 请求方产生第三随机数;

步骤 c6, 请求方生成第二加密标识, 所述第二加密标识中包含请求方选择的交易会话加密方式和支持的加密算法;

步骤 c7, 请求方以所述第三随机数、请求方的身份标识和所述第二加密标识为加密输入, 以所述第一随机数、第二随机数和第三随机数为加密密钥, 采用预设的加密算法进行加密运算, 并取加密结果的前 4 字节作为第二验证码;

步骤 c8, 请求方生成连接请求, 所述连接请求中包含所述第三随机数、请求方的身份标识、第二加密标识和第二验证码;

步骤 c9, 请求方根据所述第一随机数和第二随机数, 按照双方预设的地址计算方法计算出第二射频通信地址;

步骤 c10, 请求方通过射频通道在第二射频通信地址上采用所述射频通信频率发送所述连接请求。

10. 根据权利要求 9 所述的带低频磁通信的射频通信接入方法, 其特征在于, 所述步骤 c5 中, 所述第三随机数的长度为 3 字节。

11. 根据权利要求 9 所述的带低频磁通信的射频通信接入方法, 其特征在于, 所述步骤 c7 中, 加密输入为 $RN3||ID1||ALG2$, 加密密钥为 $RN1||RN2||RN3$, 其中 “||” 表示拼接运算。

12. 根据权利要求 9 所述的带低频磁通信的射频通信接入方法, 其特征在于, 所述步骤 c9 中, 所述第二射频通信地址的计算方法为: 以所述第一随机数和第二随机数为输入, 进行预设的单向函数运算, 并将得到的运算结果的全部或部分内容作为所述第二射频通信地址。

13. 根据权利要求 9 所述的带低频磁通信的射频通信接入方法, 其特征在于, 所述步骤 c9 中, 所述第二射频通信地址的计算方法为: 取 $RN1||RN2$ 的全部或部分内容作为第二射频通信地址, 其中 “||” 表示拼接运算。

14. 根据权利要求 1 所述的带低频磁通信的射频通信接入方法, 其特征在于, 所述步骤 d 包括:

步骤 d1, 被请求方根据所述第一随机数和第二随机数, 按照双方预设的地址计算方法计算出第二射频通信地址;

步骤 d2, 被请求方通过射频通道在第二射频通信地址上采用所述射频通信频率接收所述连接请求;

步骤 d3, 被请求方以所述连接请求中的第三随机数、请求方的身份标识和所述第二加密标识为加密输入, 以所述第一随机数、第二随机数和第三随机数为加密密钥, 采用预设的加密算法进行加密运算, 并取加密结果的前 4

字节作为第二验证码，并将该第二验证码与所述连接请求中包含的第二验证码进行比较，若两者相同则验证通过，否则验证失败；

步骤 d4，被请求方根据第二验证码的验证结果，设置连接成功/失败的状态标识，若第二验证码验证通过，则将所述连接成功/失败的状态标识设置为连接成功标志，执行步骤 d5，否则将所述连接成功/失败的状态标识设置为连接失败标志，执行步骤 d6；

步骤 d5，被请求方生成第三加密标识，所述第三加密标识中包含被请求方最终选择的交易会话加密方式和支持的加密算法；

步骤 d6，被请求方以所述第三随机数、连接成功/失败的状态标识、第三加密标识为加密输入，以所述第一随机数、第二随机数和第三随机数为加密密钥，采用预设的加密算法进行加密运算，并取加密结果的前 4 字节作为第三验证码；

步骤 d7，被请求方生成连接响应信息，所述连接响应信息中包含连接成功/失败的状态标识、第三加密标识和第三验证码；

步骤 d8，被请求方通过射频通道在第二射频通信地址上发送所述连接响应信息。

15. 根据权利要求 14 所述的带低频磁通信的射频通信接入方法，其特征在于，所述步骤 d6 中，加密输入为 RN3||SFF||ALG3，加密密钥为 RN1||RN2||RN3，其中 “||” 表示拼接运算。

16. 根据权利要求 1 所述的带低频磁通信的射频通信接入方法，其特征在于，所述步骤 e 包括：

步骤 e1，请求方通过射频通道在第二射频通信地址上接收所述连接响应信息；

步骤 e2，请求方以所述连接响应信息中的第三随机数、连接成功/失败的状态标识、第三加密标识为加密输入，以所述第一随机数、第二随机数和

第三随机数为加密密钥，采用预设的加密算法进行加密运算，并取加密结果的前 4 字节作为第三验证码，并将该第三验证码与所述连接响应信息中的第三验证码进行比较，若两者相同则验证通过，执行步骤 e3；否则验证失败，结束本次接入过程；

步骤 e3，请求方根据所述连接响应信息中的连接成功/失败的状态标识判断被请求方接入是否成功，若接入失败，则结束本次接入过程，否则执行步骤 e4；

步骤 e4，请求方与被请求方通过射频通道在第二射频通信地址上进行交易。

17. 根据权利要求 1 所述的带低频磁通信的射频通信接入方法，其特征在于，所述步骤 e4 中，所述交易中采用会话密钥。

18. 根据权利要求 17 所述的带低频磁通信的射频通信接入方法，其特征在于，所述会话密钥为 8 字节 RN1||RN2||RN3 或 16 字节 RN1||RN2||RN3||RN1||RN2||RN3，其中“||”表示拼接运算，RN1||RN2||RN3为 RN1||RN2||RN3 的按位取反。