卡管理方法、用户终端、服务器、系统及存储介质

相关申请的交叉引用

本申请要求享有于 2020 年 12 月 08 日提交的名称为“卡管理方法、用户终端、服务器、系统及存储介质”的中国专利申请 202011422479.X 的优先权，该申请的全部内容通过引用并入本文中。

技术领域

本申请属于数据处理领域，尤其涉及一种卡管理方法、用户终端、服务器、系统及存储介质。

背景技术

随着信息技术的不断发展，用户可通过安装有应用程序的用户终端完成支付交易。在进行支付交易前，用户需要将自己用于进行支付交易的资源卡如银行卡等在应用程序中进行绑定，使得在通过应用程序进行支付交易的过程中可使用该资源卡。

用户可根据需求的变化，对资源卡进行管理，例如增加应用程序中绑定的资源卡，或删除应用程序中绑定的资源卡等。为了便于对资源卡进行管理，会为每张资源卡设置程序数据包和个人化数据，并存储在用户终端中。在用户绑定多张卡的情况下，需要在用户终端中存储大量的个人化数据，增加了在用户终端中占用的存储资源。

发明内容

本申请实施例提供一种卡管理方法、用户终端、服务器、系统及存储介质，能够减少占用的用户终端的存储资源。

第一方面，本申请实施例一种卡管理方法，应用于用户终端，用户终端包括安全元件，安全元件存储有第一类通用个人化数据和第二类通用个

人化数据；

方法包括：向服务器发送卡绑定消息，卡绑定消息包括绑定卡的卡认证信息，以使服务器确定绑定卡的卡类型，并在绑定卡验证成功的情况下，为绑定卡分配专用卡信息，专用卡信息包括卡交易标识；接收服务器发送的绑定卡的卡类型和绑定卡的专用卡信息；将绑定卡的专用卡信息加载至安全元件，绑定卡的专用卡信息与匹配通用个人化数据用于进行绑定卡的交易验证，匹配通用个人化数据为与绑定卡的卡类型匹配的第一类通用个人化数据或第二类通用个人化数据。

第二方面，本申请实施例一种卡管理方法，应用于服务器，服务器存储有第一类通用个人化数据和第二类通用个人化数据；

方法包括：响应于接收的用户终端发送的卡绑定消息，确定绑定卡的卡类型，并对绑定卡进行验证，在验证成功的情况下，为绑定卡分配专用卡信息，卡绑定消息包括绑定卡的卡认证信息，专用卡信息包括卡交易标识，绑定卡的专用卡信息与匹配通用个人化数据用于进行绑定卡的交易验证，匹配通用个人化数据为与绑定卡的卡类型匹配的第一类通用个人化数据或第二类通用个人化数据；向服务器发送卡绑定应答消息，卡绑定应答消息包括绑定卡的卡类型和绑定卡的专用卡信息。

第三方面，本申请实施例一种用户终端，用户终端具有安全元件，安全元件存储有第一类通用个人化数据和第二类通用个人化数据；

用户终端包括：发送模块，用于向服务器发送卡绑定消息，卡绑定消息包括绑定卡的卡认证信息，以使服务器确定绑定卡的卡类型，并在绑定卡验证成功的情况下，为绑定卡分配专用卡信息，专用卡信息包括卡交易标识；接收模块，用于接收服务器发送的绑定卡的卡类型和绑定卡的专用卡信息；处理模块，用于将绑定卡的专用卡信息加载至安全元件，绑定卡的专用卡信息与匹配通用个人化数据用于进行绑定卡的交易验证，匹配通用个人化数据为与绑定卡的卡类型匹配的第一类通用个人化数据或第二类通用个人化数据。

第四方面，本申请实施例一种服务器，服务器存储有第一类通用个人化数据和第二类通用个人化数据；

服务器包括：接收模块，用于接收用户终端发送的卡绑定消息，卡绑定消息包括绑定卡的卡认证信息；处理模块，用于响应卡绑定消息，确定绑定卡的卡类型，并对绑定卡进行验证，在验证成功的情况下，为绑定卡分配专用卡信息，专用卡信息包括卡交易标识，绑定卡的专用卡信息与匹配通用个人化数据用于进行绑定卡的交易验证，匹配通用个人化数据为与绑定卡的卡类型匹配的第一类通用个人化数据或第二类通用个人化数据；发送模块，用于向服务器发送卡绑定应答消息，卡绑定应答消息包括绑定卡的卡类型和绑定卡的专用卡信息。

第五方面，本申请实施例提供一种用户终端，包括：处理器以及存储有计算机程序指令的存储器；处理器执行计算机程序指令时实现第一方面中的卡管理方法。

第六方面，本申请实施例提供本申请实施例提供一种服务器，包括：处理器以及存储有计算机程序指令的存储器；处理器执行计算机程序指令时实现第二方面中的卡管理方法。

第七方面，本申请实施例提供一种卡管理系统，包括第五方面的用户终端和第六方面的服务器。

第八方面，本申请实施例提供一种计算机存储介质，计算机存储介质上存储有计算机程序指令，计算机程序指令被处理器执行时实现第一方面中的卡管理方法或第二方面中的卡管理方法。

本申请实施例提供一种卡管理方法、用户终端、服务器、系统及存储介质，用户终端的安全元件中存储有第一类通用个人化数据和第二类通用个人化数据。在对卡进行绑定的过程中，用户终端通过卡绑定消息与服务器进行交互，以得到服务器为该卡分配的专用卡信息。将得到的专用卡信息加载至安全元件中。在卡绑定的过程中，不需要下载该卡进行交易验证所用的所有个人化数据，在利用该卡进行支付交易的情况下，用户终端和服务器可利用匹配通用个人化数据和该卡的专用卡信息实现交易验证。用户终端不需要重复存储各卡进行交易验证所需要的通用的个人化数据，从而减少了占用的用户终端的存储资源。

附图说明

为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例中所需要使用的附图作简单的介绍，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为本申请实施例提供的卡管理方法的应用场景的一示例的示意图；

图 2 为本申请实施例提供的用户终端的安全元件中存储内容的一示例的示意图；

图 3 为本申请第一方面提供的卡管理方法的一实施例的流程图；

图 4 为本申请第一方面提供的卡管理方法的另一实施例的流程图；

图 5 为本申请第一方面提供的卡管理方法的又一实施例的流程图；

图 6 为本申请第一方面提供的卡管理方法的再一实施例的流程图；

图 7 为本申请第一方面提供的卡管理流程的又再一实施例的流程图；

图 8 为本申请第二方面提供的卡管理方法的一实施例的流程图；

图 9 为本申请第二方面提供的卡管理方法的另一实施例的流程图；

图 10 为本申请第二方面提供的卡管理方法的又一实施例的流程图；

图 11 为本申请第二方面提供的卡管理方法的再一实施例的流程图；

图 12 为本申请第二方面提供的卡管理方法的又再一实施例的流程图；

图 13 为本申请实施例提供的卡绑定流程的一示例的流程图；

图 14 为本申请实施例提供的卡删除流程的一示例的流程图；

图 15 为本申请实施例提供的卡绑定流程的另一示例的流程图；

图 16 为本申请第三方面提供的用户终端的一实施例的结构示意图；

图 17 为本申请第三方面提供的用户终端的另一实施例的结构示意图；

图 18 为本申请第四方面提供的服务器的一实施例的结构示意图；

图 19 为本申请第四方面提供的服务器的另一实施例的结构示意图；

图 20 为本申请第五方面提供的用户终端的一实施例的结构示意图；

图 21 为本申请第六方面提供的服务器的一实施例的结构示意图。

具体实施方式

下面将详细描述本申请的各个方面的特征和示例性实施例，为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及具体实施例，对本申请进行进一步详细描述。应理解，此处所描述的具体实施例仅意在解释本申请，而不是限定本申请。对于本领域技术人员来说，本申请可以在不需要这些具体细节中的一些细节的情况下实施。下面对实施例的描述仅仅是为了通过示出本申请的示例来提供对本申请更好的理解。

随着信息技术的不断发展，用于可通过用户终端中安装的应用程序来完成支付交易。应用程序会与用户的卡如银行卡等绑定，在支付交易的过程中，支付交易过程中的资源从应用程序绑定的一张卡中转出。利用每张卡进行支付交易的过程中，需要进行交易验证。为了能够实现交易验证，会为每张卡分配一一对应的程序数据包和个人化数据，并存储在用户终端。每张卡都对应有专用的程序数据包和个人化数据。例如，用户终端的应用程序绑定有卡 C1、C2 和 C3，对应地，用户终端存储有卡 C1 对应的程序数据包 Cap 1 和个人化数据 Data C1、卡 C2 对应的程序数据包 Cap 2 和个人化数据 Data C2、卡 C3 对应的程序数据包 Cap 3 和个人化数据 Data C3。在应用程序绑定有多张卡的情况下，需要在用户终端存储多张卡各自对应的个人化数据，占用了用户终端较多的存储资源。

本申请实施例提供一种卡管理方法、用户终端、服务器、系统及存储介质，能够减少卡管理在用户终端中占用的存储资源。

图 1 为本申请实施例提供的卡管理方法的应用场景的一示例的示意图。如图 1 所示，本申请实施例提供的卡管理方法可涉及用户终端 11 和服务器 12，在此并不限定。

用户终端 11 可包括手机、平板电脑、可穿戴设备、各类异形卡等具有支付交易功能的终端设备，在此并不限定。用户终端 11 中可安装有用于进行支付交易的应用程序，可通过应用程序实现支付交易。对应地，用户终端 11 的应用程序可包括可穿戴类终端设备软件开发工具包（Software Development Kit，SDK）、其他类终端设备软件开发工具包和支付应用程

序软件开发工具包，在此并不限定。

在一些示例中，用户终端可包括支付终端和辅助终端。辅助终端可作为支付终端与服务器之间的交互中转设备，即支付终端可与服务器之间通过辅助终端进行交互。例如，支付终端可包括可穿戴设备，如智能手表、智能眼镜等设备，辅助终端可包括手机等设备，在此并不限定。

用户终端 11 可包括安全元件，安全元件为用户终端 11 中设置的安全保护元件，可包括具体的硬件电路，也可包括搭建的安全环境，在此并不限定。例如，安全元件可包括安全芯片（Secure Element，SE）、可信执行环境（Trusted Execution Environment，TEE）、SE+TEE、基于主机的卡模拟（Host-based Card Emulation，HCE）等。在本申请实施例中，安全元件中存储有第一类通用个人化数据和第二类通用个人化数据。具体的，可在初次进行卡绑定的过程中，将第一类通用个人化数据和第二类通用个人化数据下载至安全元件中；也可在用户终端 11 出厂前将第一类通用个人化数据和第二类通用个人化数据预置在安全元件中，在此并不限定。

第一类通用个人化数据和第二类通用个人化数据可与不同卡的卡专用信息共同作用，实现各卡在支付交易过程中的交易验证。具体地，第一类通用个人化数据可用于卡类型为第一类型的卡的交易验证。在卡的卡类型为第一类型的情况下，利用第一类通用个人化数据和该卡的专用卡信息对该卡进行交易验证。第二类通用个人化数据可用于卡类型为第二类型的卡的交易验证。卡的卡类型为第二类型的情况下，利用第二类通用个人化数据和该卡的专用卡信息对该卡进行交易验证。

例如，在卡为银行卡的情况下，第一类型的卡可为借记卡，第二类型的卡可为贷记卡，在此并不限定。

不同的卡的卡专用信息不同。在一些示例中，卡专用信息可包括卡的卡交易标识即 Token。不同的卡的卡交易标识不同。不同类型的卡的卡交易标识的格式也可不同。例如，第一类型的卡为借记卡，借记卡的卡交易标识可为 19 位标识；第二类型的卡为贷记卡，贷记卡的卡交易标识可为 16 位标识。

卡的专用卡信息、卡的卡类型和卡的生命状态的映射关系可存储于安

全元件中，也可存储于用户终端中的其他器件中，在此并不限定。该映射关系可采用表的形式进行存储和管理，在此并不限定。卡的生命状态用于表征卡的使用状态。在一些示例中，卡的使用状态可包括生效状态、失效状态和默认使用状态。卡的使用状态为生效状态，表示该卡已绑定，为可用状态。卡的使用状态为失效状态，表示该卡已删除，为不可用状态。卡的使用状态为默认使用状态，表示该卡已绑定，且支付交易使用该卡进行。

在一些示例中，用户的安全元件中可存储一个通用程序数据包。该通用程序数据包包括安全元件运行所需的程序，在此并不限定。该通用程序数据包具体可为 Cap 包形式。安全元件中对卡的相关信息、卡的专用卡信息、第一类通用个人化数据和第二类通用个人化数据等的内部操作可共用这一个程序数据包，且该通用程序数据包存储至安全元件后，不再删除，避免绑定卡过程和删除卡过程中对程序数据包频繁的下载和删除。具体地，该通用程序数据包可在初次进行卡绑定的过程中下载至安全元件中；也可在用户终端出厂前将该通用程序数据包预置在安全元件中，在此并不限定。

在一些示例中，专用卡信息还可包括专用个人化数据。不同的卡对应的专用个人化数据不同。对于一张卡类型为第一类型的卡而言，利用该卡的卡交易标识、该卡的专用个人化数据和第一类通用个人化数据即可实现该卡的交易验证计算。对于一张卡类型为第二类型的卡而言，利用该卡的卡交易标识、该卡的专用个人化数据和第二类通用个人化数据即可实现该卡的交易验证计算。第一类通用个人化数据为卡类型为第一类型的卡进行交易验证所需的相同的个人化数据。第二类通用个人化数据为卡类型为第二类型的卡进行交易验证所需的相同的个人化数据。专用个人化数据即为不同的卡进行交易验证所需的不同的个人化数据。

例如，图 2 为本申请实施例提供的用户终端的安全元件中存储内容的一示例的示意图。如图 2 所示，安全元件中存储有通用程序数据包即 Cap 包、第一类通用个人化数据、第二类通用个人化数据、绑定的各个银行卡的专用卡信息以及映射关系管理表。第一类型的卡为银行卡中的借记卡，

第一类通用个人化数据记为 Data A。第二类型的卡为银行卡中的贷记卡，第二类通用个人化数据记为 Data B。设应用程序绑定有银行卡 C1、C2、C3、C4、C5 和 C6。专用卡信息可包括卡交易标识和专用个人化数据。其中，银行卡 C1、C2 和 C3 为借记卡，银行卡 C1、C2 和 C3 各自的专用卡信息分别为信息 M1、信息 M2 和信息 M3。信息 M1 包括卡交易标识 Token 1 和专用个人化数据 Data 1；信息 M2 包括卡交易标识 Token 2 和专用个人化数据 Data 2；信息 M3 包括卡交易标识 Token 3 和专用个人化数据 Data 3。银行卡 C1、C2 和 C3 的专用卡信息均与第一类通用个人化数据对应（图 2 中以箭头表示对应关系）。银行卡 C4、C5 和 C6 为贷记卡，银行卡 C4、C5 和 C6 各自的专用卡信息分别为信息 M4、信息 M5 和信息 M6。信息 M4 包括卡交易标识 Token 4 和专用个人化数据 Data 4；信息 M5 包括卡交易标识 Token 5 和专用个人化数据 Data 5；信息 M6 包括卡交易标识 Token 6 和专用个人化数据 Data 6。银行卡 C4、C5 和 C6 的专用卡信息均与第二类通用个人化数据对应（图 2 中以箭头表示对应关系）。映射关系管理表包括各银行卡 C1、C2、C3、C4、C5 和 C6 各自的专用卡信息、卡类型和生命状态。如图 2 所示，银行卡 C1、C2、C3、C4、C5 和 C6 各自的生命状态分别为默认使用状态、生效状态、生效状态、生效状态、生效状态和失效状态。

需要说明的是，在此并不限定卡类型的数量，例如，在存在卡类型为第三类型的卡、卡类型为第四类型的卡等的情况下，安全元件中还可存储有第三类通用个人化数据、第四类通用个人化数据等，第三类通用个人化数据、第四类通用个人化数据等与第一通用个人化数据、第二通用个人化数据类似，作用和在卡管理流程中的使用可参考第一通用个人化数据、第二通用个人化数据，在此不再赘述。

服务器 12 可包括管理服务器 121 和应用程序的后台服务器 122，在此并不限定。在一些示例中，管理服务器 121 可包括可信服务管理平台（Trusted Service Manager，TSM）服务器 1211 和内容服务提供者（Telematics Service Provider，TSP）服务器 1212。管理服务器 121 和后台服务器 122 之间可进行交互。TSM 服务器 1211 与 TSP 服务器 1212 也可进

行交互。

服务器 12 中可存储有与服务器 12 进行交互的各个用户终端对应的第一类通用个人化数据和第二类通用个人化数据。用户终端的安全元件中的第一类通用个人化数据和第二类通用个人化数据与服务器中存储的第一类通用个人化数据和第二类通用个人化数据相同。需要说明的是，不同用户终端对应的第一类通用个人化数据和第二类通用个人化数据不同，可由服务器统一分配。

服务器 12 可与用户终端 11 同步卡的专用卡信息、卡类型和生命状态的映射关系，以使得用户终端 11 与服务器 12 中的信息同步，避免因信息不同步而造成的支付交易错误问题。

下面将具体说明本申请提供的卡管理方法、用户终端、服务器、系统及存储介质。

本申请第一方面提供一种卡管理方法，可应用于用户终端。图 3 为本申请第一方面提供的卡管理方法的一实施例的流程图。如图 3 所示，该卡管理方法可包括步骤 S201 至步骤 S203。

在步骤 S201 中，向服务器发送卡绑定消息，以使服务器确定绑定卡的卡类型，并在绑定卡验证成功的情况下，为绑定卡分配专用卡信息。

卡绑定消息包括绑定卡的卡认证信息。卡认证信息用于对卡进行验证。在一些示例中，卡认证信息可包括但不限于卡标识、卡类型验证信息和输入验证码。卡标识用于标识卡，例如，卡标识可为卡号。卡类型验证信息用于进行对某类型的卡的验证。卡类型不同，卡类型验证信息可不同。例如，第一类型的卡为借记卡，第一类型的卡对应的卡类型验证信息可包括取款密码；第二类型的卡为贷记卡，第二类型的卡对应的卡类型验证信息可包括贷记卡安全码即 CVN2 码和贷记卡有效期。输入验证码为用户终端接收的输入的验证码，具体可为用户输入的验证码，或者，通过用户终端授权从包括动态验证码的短消息中识别并输入的验证码，在此并不限定。

卡绑定消息可包括多个消息，多个消息可根据验证需求分次发送。多个消息中的每个消息包括的卡认证信息可不同，具体内容会在后文中详细

说明。

服务器接收到卡绑定消息，可根据卡绑定消息中的卡认证信息对卡进行验证，在验证成功的情况下，卡绑定消息指示的卡即绑定卡分配专用卡信息。专用卡信息包括卡交易标识。在使用该卡进行支付交易的情况下，用户终端向其他设备发送的是卡交易标识，以使其他设备通过卡交易标识确定进行支付交易的账户。卡交易标识由服务器分配，不同的卡的卡交易标识不同。在一些示例中，专用卡信息还可包括专用个人化数据，具体内容可参见上文中的相关说明，在此不再赘述。

在步骤 S202 中，接收服务器发送的绑定卡的卡类型和绑定卡的专用卡信息。

用户终端可分次接收绑定卡的卡类型和绑定卡的专用卡信息。在卡绑定消息包括多个消息的情况下，服务器可根据卡绑定消息中各消息，分次发送绑定卡的卡类型和绑定卡的专用卡信息。具体地，服务器可通过卡绑定应答消息发送绑定卡的卡类型和绑定卡的专用卡信息。

步骤 S201 和步骤 S202 之间的时序关系，可根据卡绑定消息和卡类型、专用卡信息之间的请求和应答关系确定，在此并不限定。

在步骤 S203 中，将绑定卡的专用卡信息加载至安全元件。

绑定卡的专用卡信息与匹配通用个人化数据用于进行绑定卡的交易验证。匹配通用个人化数据为与绑定卡的卡类型匹配的第一类通用个人化数据或第二类通用个人化数据。也就是说，绑定卡的卡类型为第一类型，匹配通用个人化数据为第一类通用个人化数据。绑定卡的卡类型为第二类型，匹配通用个人化数据为第二类通用个人化数据。

卡类型相同的不同卡的专用卡信息不同，但卡类型相同的不同卡的匹配通用个人化数据相同，即卡类型相同的不同卡共用相同的匹配通用个人化数据。

在一些示例中，在绑定卡包括卡类型相同的第一卡和第二卡的情况下，第一卡的专用卡信息与目标匹配通用个人化数据用于进行第一卡的交易验证，第二卡的专用卡信息与目标匹配通用个人化数据用于进行第二卡的交易验证。目标通用个人化数据为第一卡的卡类型匹配的第一类通用个

人化数据或第二类通用个人化数据。在卡类型相同的更多张卡的情况下，这更多张卡共用相同的目标匹配通用个人化数据。

例如，如图 2 所示，银行卡 C1 的专用卡信息 M1 和第一类通用个人化数据 Data A 用于进行银行卡 C1 的交易验证。银行卡 C2 的专用卡信息 M2 和第一类通用个人化数据 Data A 用于进行银行卡 C2 的交易验证。银行卡 C3 的专用卡信息 M3 和第一类通用个人化数据 Data A 用于进行银行卡 C3 的交易验证。银行卡 C1、C2 和 C3 各自的专用卡信息不同，但共用相同的第一类通用个人化数据。

而且，第一类通用个人化数据和第二类通用个人化数据具有通用性，在不同的用户终端、不同的应用程序中均可使用，具有更优的兼容性。

具体地，用户终端可通过控制指令，将绑定卡的专用卡信息加载至安全元件。控制指令可由服务器先发送给用户终端，再由用户终端发送给安全元件，以对安全元件进行控制。在一些示例中，控制指令可包括应用协议数据单元（Application Protocol Data Unit，APDU）指令，在此并不限定 APDU 指令的具体内容。

在一些示例中，在用户终端的应用程序初次进行卡绑定的情况下，服务器还可向用户终端发送通用程序数据包，用户终端接收该通用程序数据包，将该通用程序数据包加载至安全元件。具体地，用户终端可通过 APDU 指令将通用程序数据包加载至安全元件。其中可通过 APDU 指令将通用程序数据包分割成多个部分加载。在此并不限定 APDU 指令的具体内容。

在用户终端的应用程序还绑定有卡的情况下，该通用程序数据包在用户终端中不会删除。

在一些示例中，在用户终端的应用程序初次进行卡绑定的情况下，用户终端还可触发安装卡组织程序。具体地，用户终端可通过 APDU 指令将卡组织程序安装至安全元件，在此并不限定 APDU 指令的具体内容。

在本申请实施例中，用户终端的安全元件中存储有第一类通用个人化数据和第二类通用个人化数据。在对卡进行绑定的过程中，用户终端通过卡绑定消息与服务器进行交互，以得到服务器为该卡分配的专用卡信息。

将得到的专用卡信息加载至安全元件中。在卡绑定的过程中，不需要下载该卡进行交易验证所用的所有个人化数据，在利用该卡进行支付交易的情况下，用户终端和服务器可利用匹配通用个人化数据和该卡的专用卡信息实现交易验证。用户终端不需要重复存储各卡进行交易验证所需要的通用的个人化数据，从而减少了占用的用户终端的存储资源。

而且，在卡绑定过程中，除了用户终端的应用程序初次绑定卡的情况，用户终端需要下载的内容不包括通用的个人化数据，减少了用户终端下载数据花费的时间，从而加快了卡绑定的速度，使得卡绑定流程更加快捷、简单。

在另一些实施例中，卡绑定消息包括第一卡绑定消息、第二卡绑定消息和绑定验证消息。卡认证信息包括卡标识、卡类型验证信息和输入验证码。图 4 为本申请第一方面提供的卡管理方法的另一实施例的流程图。图 4 与图 3 的不同之处在于，图 3 中的步骤 S201 可具体细化为图 4 中的步骤 S2011 至步骤 S2013，图 3 中的步骤 S202 可具体细化为图 4 中的步骤 S2021 至步骤 S2023。

在步骤 S2011 中，向服务器发送第一卡绑定消息。

第一卡绑定消息包括绑定卡的卡标识。用户终端向服务器发送第一卡绑定消息，以使服务器根据绑定卡的卡标识，识别卡的卡类型，将卡的卡类型通过应答消息反馈给服务器。卡类型不同的卡的卡标识的格式不同，服务器可通过绑定卡的卡标识的格式，识别出绑定卡的卡类型。

在步骤 S2021 中，接收服务器发送的第一应答消息。

第一应答消息包括绑定卡的卡类型。服务器可通过第一应答消息将绑定卡的卡类型反馈给服务器。

在步骤 S2012 中，向服务器发送第二卡绑定消息。

第二卡绑定信息包括绑定卡的卡类型验证信息。卡类型不同，卡的卡类型验证信息也可不同。具体地，在绑定卡的卡类型为第一类型的情况下，卡类型验证信息包括第一类验证信息；在绑定卡的卡类型为第二类型的情况下，卡类型验证信息包括第二类验证信息。其中，第一类验证信息与第二类验证信息不同。例如，在第一类型的卡为借记卡的情况下，第一

类验证信息可包括取款密码；在第二类型的卡为贷记卡的情况下，第二类验证信息可包括贷记卡安全码和贷记卡有效期。

在接收到服务器发送第一应答消息的情况下，用户终端向服务器发送第二卡绑定消息，以使服务器根据第二卡绑定消息中的卡类型验证信息进行卡类型验证。卡类型验证即为针对该类型的卡的验证。例如，在第一类型的卡为借记卡的情况下，进行的是针对借记卡的验证；在第二类型的卡为贷记卡的情况下，进行的是针对贷记卡的验证。

在步骤 S2022 中，接收服务器发送的第二应答消息。

第二应答消息包括动态验证码。服务器在卡类型验证成功的情况下，可通过第二应答消息将动态验证码反馈给服务器。

在步骤 S2013 中，向服务器发送绑定验证消息。

绑定验证消息包括输入验证码。输入验证码可为用户终端接收的输入的验证码，具体可为用户输入的验证码，或者，通过用户终端授权从包括动态验证码的短消息中识别并输入的验证码，在此并不限定。

在接收到服务器发送的第二应答消息的情况下，向服务器发送绑定验证消息，以使服务器根据输入验证码和动态验证码，进行验证码验证。在上述卡类型验证成功且验证码验证成功的情况下，服务器确定对绑定卡的验证成功。

在步骤 S2023 中，接收服务器发送的第三应答消息。

第三应答消息包括绑定卡的专用卡信息。在对绑定卡的验证成功的情况下，服务器为用户终端分配该绑定卡的专用卡信息，并可通过第三应答消息向用户终端发送。

为了便于对卡的信息进行管理，可为绑定卡设置生命状态，还可在用户终端可与服务器之间进行数据同步，以保证用户终端与服务器之间的数据一致。图 5 为本申请第一方面提供的卡管理方法的又一实施例的流程图。图 5 与图 3 的不同之处在于，图 5 所示的卡管理方法还可包括步骤 S204 和步骤 S205。

在步骤 S204 中，通过安全元件将绑定卡的生命状态设置为生效状态，并生成或更新第一映射关系。

第一映射关系包括绑定卡的专用卡信息、绑定卡的卡类型和绑定卡的生命状态的映射关系。

在一些实施例中，绑定卡之前并未与该用户终端的应用程序绑定过，即本次绑定为该绑定卡与该用户终端的应用程序的第一次绑定。用户终端并未存储有该绑定卡的专用卡信息、绑定卡的卡类型和绑定卡的生命状态的映射关系。在这种情况下，用户终端生成第一映射关系。

在另一些实施例中，绑定卡之前曾与该用户终端的应用程序绑定过并被删除过，即本次绑定为该绑定卡与该用户终端的应用程序的第 N 次绑定，N 为大于 1 的整数。在一些情况下，用户终端在本次绑定之前已经删除了该绑定卡的专用卡信息、绑定卡的卡类型和绑定卡的生命状态的映射关系，对应地，本次用户终端需要生成第一映射关系。在另一些情况下，用户终端在本次绑定之前未删除该绑定卡的专用卡信息、绑定卡的卡类型和绑定卡的生命状态的映射关系，只是将绑定卡的生命状态更改为失效状态，对应地，本次用户终端不需要专门生成新的第一映射关系，只需更新第一映射关系，即将第一映射关系中绑定卡的生命状态更新为生效状态。

在步骤 S205 中，将设置后的绑定卡的生命状态和第一映射关系同步至服务器。

服务器需要与用户终端同步各个卡的专用卡信息、卡类型和生命状态的映射关系，以避免在支付交易过程中出现错误。在此并不限定用户终端与服务器的同步的方式。

用户终端的应用程序可能会绑定多张卡，在绑定多张卡的情况下，会在绑定的多张卡中设置一张默认卡。进行支付交易时会直接使用该默认卡。默认卡可更改。图 6 为本申请第一方面提供的卡管理方法的再一实施例的流程图。图 6 与图 5 的不同之处在于，图 6 所示的卡管理方法还可包括步骤 S206 至步骤 S209。

在步骤 S206 中，接收默认卡选取输入。

默认卡选取输入用于指示选定的默认卡。具体地，默认卡选取输入指示的是本次选定的默认卡。默认卡选取输入可为用户对用户终端进行输入。用户终端可根据默认卡选取输入，确定默认卡选取输入指示的默认卡

的卡交易标识。

在步骤 S207 中，将原始默认卡的生命状态更新为生效状态。

在将默认卡的生命状态更新为默认使用状态之前，用户终端的应用程序绑定的卡中存在一张生命状态为默认使用状态的卡，该卡即为上一次选定的默认卡。为了将上一次选定的默认卡与本次选定的默认卡区分，这里将上一次选定的默认卡称为原始默认卡。原始默认卡更新前的生命状态为默认使用状态。

响应于默认卡选取输入，用户终端可通过控制指令，将原始默认卡的生命状态更新为生效状态，即将原始默认卡的默认使用状态取消。具体地，将原始默认卡的生命状态由默认使用状态更改为生效状态。原始默认卡的卡类型在此并不限定，可与默认卡的卡类型相同，也可与默认卡的卡类型不同。

在一些示例中，用户终端可通过控制指令，控制安全元件取消原始默认卡的默认使用状态。控制指令可由服务器先发送给用户终端，再由用户终端发送给安全元件，以对安全元件进行控制。具体地，控制指令可包括 APDU 指令，在此并不限定 APDU 指令的具体内容。

原始默认卡的生命状态发生变化，对应地，原始默认卡的专用卡信息、原始默认卡的卡类型和原始默认卡的生命状态的映射关系也对应更新。具体地，可更新映射关系管理表中原始默认卡所对应的映射关系。

在步骤 S208 中，控制安全元件将默认卡的生命状态更新为默认使用状态。

响应于默认卡选取输入，用户终端将该默认卡的生命状态更新为默认使用状态。该默认卡是已与用户终端的应用程序绑定的卡，具体地，用户终端将该默认卡的生命状态由生效状态更改为默认使用状态。

在一些示例中，用户终端可通过控制指令，控制安全元件将默认卡的生命状态更新为默认使用状态。控制指令可由服务器先发送给用户终端，再由用户终端发送给安全元件，以对安全元件进行控制。具体地，控制指令可包括 APDU 指令，在此并不限定 APDU 指令的具体内容。

默认卡的生命状态发生变化，对应地，默认卡的专用卡信息、默认卡

的卡类型和默认卡的生命状态的映射关系也对应更新。具体地，可更新映射关系管理表中默认卡所对应的映射关系。

在步骤 S209 中，将更新后的默认卡的生命状态和更新后的原始默认卡的生命状态同步至服务器。

为了保证用户终端中的卡的相关信息与服务器中的卡的相关信息保持一致，在用户终端中的卡的相关信息发生变化的情况下，用户终端与服务器同步。

在本实施例中，默认卡的设置可在用户终端本地进行，无需与服务器进行交互，即可更改默认卡，加快了默认卡设置的速度，使得默认卡设置流程更加快捷、简单。

在用户不需要利用某张卡进行支付交易的情况下，还可根据需求，将用户终端的应用程序中已绑定的卡删除，即执行卡删除流程。图 7 为本申请第一方面提供的卡管理流程的又再一实施例的流程图。图 7 与图 5 的不同之处在于，图 7 所示的卡管理方法还可包括步骤 S210 至步骤 S213。

在步骤 S210 中，向服务器发送卡删除请求消息，以使服务器反馈待删除卡的卡交易标识。

卡删除请求消息指示选定的待删除卡。服务器接收到卡删除请求消息，向用户终端反馈待删除卡的卡交易标识。

在步骤 S211 中，接收服务器反馈的待删除卡的卡交易标识。

在步骤 S212 中，控制安全元件将待删除卡的生命状态更新为失效状态。

删除卡即为将待删除卡与用户终端的应用程序解绑。在用户终端中可不删除该待删除卡的卡交易标识，由于待删除卡的生命状态已经更新为失效状态，即使保留该待删除卡的卡交易标识，待删除卡的卡交易标识也无法使用，对支付交易并不会造成影响。

在一些示例中，用户终端可通过控制指令，控制安全元件将待删除卡的生命状态更新为失效状态。控制指令可由服务器先发送给用户终端，再由用户终端发送给安全元件，以对安全元件进行控制。具体地，控制指令可包括 APDU 指令，在此并不限定 APDU 指令的具体内容。

在待删除卡为用户终端的应用程序绑定的最后一张卡的情况下，执行上述卡删除流程以外，还可将通用程序数据包删除，在此并不限定。

在一些示例中，用户终端可不删除第二映射关系，只更新第二映射关系中待删除卡的生命状态。第二映射关系包括待删除卡的专用卡信息、待删除卡的卡类型和待删除卡的生命状态的映射关系。用户终端不删除第二映射关系，在用户终端的应用程序再次绑定该待删除卡的情况下，可通过更新第二映射关系中待删除卡的生命状态，以达到快速恢复绑卡的效果。

在另一些示例中，用户终端可删除第二映射关系。在用户终端的应用程序再次绑定该待删除卡的情况下，可重新生成第二映射关系。

在一些情况下，卡删除流程也可触发默认卡设置流程。例如，待删除卡的生命状态在更新前为默认使用状态。则在卡删除过程中，还需执行默认卡设置流程，指定一张新的默认卡，并将指定的新的默认卡的生命状态更新为默认使用状态。

在步骤 S213 中，将更新后的待删除卡的生命状态同步至服务器。

为了保证用户终端中的卡的相关信息与服务器中的卡的相关信息保持一致，在用户终端中的卡的相关信息发生变化的情况下，用户终端与服务器同步。

在又一些实施例中，用户终端可能会绑定之前删除过的卡。由于卡删除流程中并未在用户终端中删除卡的卡交易标识，只是将删除的卡的生命状态更改为失效状态。因此，在用户终端中依然可查找到曾删除过的卡的卡交易标识，在服务器中也可查找到曾删除过的卡的专用卡信息、卡类型和生命状态的映射关系。对应地，在用户终端绑定之前删除过的卡的情况下，用户终端依旧可采用上述实施例中卡绑定流程中的方法，对该曾删除过的卡再次进行绑定。与未绑定过的卡的绑定相比，绑定曾删除过的卡，服务器为该卡分配的专用卡信息即为该卡曾经的专用卡信息，不需要重新生成专用卡信息。用户终端响应于服务器发送的该卡的专用卡信息，可将用户终端中该卡的生命状态从失效状态更新为生效状态。在该卡的专用卡信息、卡类型和生命状态的映射关系在删除卡时在用户终端未删除的情况下，更新该对应关系中的生命状态即可。在该卡的专用卡信息、卡类型和

生命状态的映射关系在删除卡时在用户终端删除的情况下，可重新生成该卡的专用卡信息、卡类型和生命状态的映射关系。

在用户对卡进行挂失的情况下，用户可通过卡组织、在任意一台用户终端登录应用程序或登录网页等方式，删除挂失的卡，减少了挂失卡所需的时间。

本申请第二方面提供了一种卡管理方法，该卡管理方法可应用于服务器。服务器可存储有第一类通用个人化数据和第二类通用个人化数据，且服务器存储的第一类通用个人化数据与用户终端存储的第一类通用个人化数据一致，服务器存储的第二类通用个人化数据与用户终端存储的第二类通用个人化数据一致。图 8 为本申请第二方面提供的卡管理方法的一实施例的流程图。如图 8 所示，该卡管理方法可包括步骤 S301 和步骤 S302。

在步骤 S301 中，响应于接收的用户终端发送的卡绑定消息，确定绑定卡的卡类型，并对绑定卡进行验证，在验证成功的情况下，为绑定卡分配专用卡信息。

卡绑定消息包括绑定卡的卡认证信息。卡绑定消息可包括多个消息，每个消息可包括不同的卡认证信息。用户终端可分多次发送卡绑定消息。对应地，服务器可分多次接收卡绑定消息，根据每次接收的消息，可确定绑定卡的卡类型，以及对绑定卡进行对应的验证，具体内容可参见上文以及后文中的详细说明。

在对绑定卡验证失败的情况下，服务器不会为绑定卡分配专用卡信息。

在一些示例中，卡认证信息可包括卡标识、卡类型验证信息和输入验证码。

专用卡信息包括卡交易标识。绑定卡的专用卡信息与匹配通用个人化数据用于进行绑定卡的交易验证。匹配通用个人化数据为与绑定卡的卡类型匹配的第一类通用个人化数据或第二类通用个人化数据。

服务器为卡类型相同的不同卡所分配的专用卡信息不同。但卡类型相同的不同卡的匹配通用个人化数据相同，即卡类型相同的不同卡共用相同的匹配通用个人化数据。

在一些示例中，在绑定卡包括卡类型相同的第一卡和第二卡的情况下，第一卡的专用卡信息与目标匹配通用个人化数据用于进行第一卡的交易验证，第二卡的专用卡信息与目标匹配通用个人化数据用于进行第二卡的交易验证。目标匹配通用个人化数据为与第一卡的卡类型匹配的第一类通用个人化数据或第二类通用个人化数据。

在一些示例中，专用卡信息还包括专用个人化数据。专用个人化数据的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在步骤 S302 中，向服务器发送卡绑定应答消息。

卡绑定应答消息包括绑定卡的卡类型和绑定卡的专用卡信息。卡绑定应答消息可包括多个消息，每个消息中包括的内容可不同，具体内容可参见上文以及后文中的详细说明。服务器可将这多个消息分次向用户终端发送，对应地，用户终端可分次接收这多个消息。

上述步骤 S301 和步骤 S302 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在本申请实施例中，服务器接收用户终端发送的卡绑定消息，响应于卡绑定消息，确定绑定卡的卡类型，并对绑定卡进行验证，在验证成功的情况下，为绑定卡分配专用卡信息，并向用户终端发送，以使用户终端接收绑定卡的专用卡信息，在利用该卡进行支付交易的情况下，用户终端和服务器可利用用户终端，通用个人化数据和该卡的专用卡信息实现交易验证。服务器不需要在每一次卡绑定过程中将绑定的卡进行交易验证所需的通用的个人化数据重复发送给用户终端，从而减少了占用的用户终端的存储资源，也能够减少下载过程中占用的下载资源。

而且，在卡绑定过程中，除了用户终端的应用程序初次绑定卡的情况，服务器需要向用户终端发送的内容不包括通用的个人化数据，减少了用户终端下载数据花费的时间，从而加快了卡绑定的速度，使得卡绑定流程更加快捷、简单。

在另一些示例中，卡绑定消息包括第一卡绑定消息、第二卡绑定消息和绑定验证消息。卡绑定应答消息包括第一应答消息和第二应答消息。卡认证信息包括卡标识、卡类型验证信息和输入验证码。图 9 为本申请第二

方面提供的卡管理方法的另一实施例的流程图。图 9 与图 8 的不同之处在于，图 8 中的步骤 S301 可细化为图 9 中的步骤 S3011 至步骤 S3013，图 8 中的步骤 S302 可细化为图 9 中的步骤 S3021 至步骤 S3023。

在步骤 S3011 中，响应于用户终端发送的第一卡绑定消息，根据第一卡绑定消息中绑定卡的卡标识，确定绑定卡的卡类型。

第一卡绑定消息包括绑定卡的卡标识。卡类型不同的卡的卡标识的格式不同。服务器可根据绑定卡的卡标识，识别绑定卡的卡类型。

在步骤 S3021 中，向用户终端发送第一应答消息。

在响应于用户终端发送的第一卡绑定消息确定绑定卡的卡类型的情况下，向用户终端发送第一应答消息。第一应答消息包括绑定卡的卡类型。

在步骤 S3012 中，响应于用户终端发送的第二卡绑定消息，利用第二卡绑定消息中绑定卡的卡类型验证信息，对绑定卡进行卡类型验证。

第二卡绑定消息包括与绑定卡的卡类型匹配的卡类型验证信息。

在一些示例中，在绑定卡的卡类型为第一类型的情况下，卡类型验证信息包括第一类验证信息；在绑定卡的卡类型为第二类型的情况下，卡类型验证信息包括第二类验证信息。其中，第一类验证信息与第二类验证信息不同。

在步骤 S3022 中，向用户终端发送第二应答消息。

在响应于用户终端发送的第二卡绑定消息对绑定卡的卡类型验证成功的情况下，向用户终端发送第二应答消息。第二应答消息包括动态验证码。

在步骤 S3013 中，响应于用户终端发送的绑定验证消息，在绑定验证消息中的输入验证码与动态验证码一致的情况下，为绑定卡分配专用卡信息。

绑定验证消息包括输入验证码。绑定验证消息中的输入验证码与冬天验证码一致，表示验证码验证成功。在验证码验证成功的情况下，服务器为绑定卡分配专用卡信息。

在步骤 S3023 中，向用户终端发送第三应答消息。

在响应于用户终端发送的绑定验证消息对绑定卡的验证码验证成功的

情况下，向用户终端发送第三应答消息。第三应答消息包括绑定卡的专用卡信息。

上述步骤 S3011 至步骤 S3013，以及步骤 S3021 至步骤 S3023 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在一些示例中，在用户终端初次进行卡绑定的情况下，服务器还可向用户终端发送通用程序数据包。

为了保证用户终端与服务器之间的数据保持一致，可在用户终端可与服务器之间进行数据同步。图 10 为本申请第二方面提供的卡管理方法的又一实施例的流程图。图 10 与图 8 的不同之处在于，图 10 所示的卡管理方法还可包括步骤 S303。

在步骤 S303 中，与用户终端同步设置后的绑定卡的生命状态和第一映射关系。

第一映射关系包括绑定卡的专用卡信息、绑定卡的卡类型和绑定卡的生命状态的映射关系。

步骤 S303 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

用户终端的应用程序可能会绑定多张卡，在绑定多张卡的情况下，会在绑定的多张卡中设置一张默认卡。进行支付交易时会直接使用该默认卡。默认卡可更改。图 11 为本申请第二方面提供的卡管理方法的再一实施例的流程图。图 11 与图 10 的不同之处在于，图 11 所示的卡管理方法还可包括步骤 S304。

在步骤 S304 中，与用户终端同步更新后的默认卡的生命状态和更新后的原始默认卡的生命状态。

原始默认卡更新前的生命状态为默认使用状态。

上述步骤 S304 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在用户不需要利用某张卡进行支付交易的情况下，还可根据需求，将用户终端的应用程序中已绑定的卡删除，即执行卡删除流程。图 12 为本申请第二方面提供的卡管理方法的又再一实施例的流程图。图 12 与图 10

的不同之处在于，图 12 所示的卡管理方法还可包括步骤 S305 和步骤 S306。

在步骤 S305 中，响应于用户终端发送的卡删除请求，向用户终端反馈待删除卡的卡交易标识。

卡删除请求消息指示选定的待删除卡。

在步骤 S306 中，与用户终端同步更新后的待删除卡的生命状态。

在一些示例中，服务器可更新第二映射关系中的待删除卡的生命状态，但不删除第二映射关系。在另一些示例中，可服务器也可对应删除第二映射关系，在此并不限定。

上述步骤 S305 和步骤 S306 的具体内容可参见上述实施例中的相关说明，在此不再赘述。

在上述实施例中，为了保证服务器中的卡的相关信息与用户终端中的卡的相关信息保持一致，在用户终端中的卡的相关信息发生变化的情况下，用户终端与服务器同步，以使服务器中卡的相关信息可与终端设备中的卡的相关信息保持一致。在此并不限定服务器与用户终端之间的同步方式。

为了进一步说明卡管理方法中涉及到的各个流程，下面以用户终端包括安全元件，用户终端安装有应用程序，服务器包括应用程序的后台服务器、TSM 服务器和 TSP 服务器为例进行说明。应用程序具体可为电子钱包应用程序。

图 13 为本申请实施例提供的卡绑定流程的一示例的流程图。其中的绑定卡之前未与用户终端的应用程序绑定过。如图 13 所示，卡绑定流程可包括步骤 S401 至步骤 S424。

在步骤 S401 中，应用程序接收卡绑定输入。

卡绑定输入可包括绑定卡的卡标识。

在步骤 S402 中，应用程序向后台服务器发送第一卡绑定消息。

第一卡绑定消息包括绑定卡的卡标识。

在步骤 S403 中，后台服务器根据绑定卡的卡标识，确定绑定卡的卡类型。

在步骤 S404 中，后台服务器向应用程序发送第一应答消息。

第一应答消息包括绑定卡的卡类型。

在步骤 S405 中，应用程序根据绑定卡的卡类型，发出提示消息，提示用户输入与绑定卡的卡类型对应的卡类型验证信息。

在步骤 S406 中，应用程序接收卡类型验证信息输入。

在步骤 S407 中，应用程序向后台服务器发送第二卡绑定消息。

第二卡绑定消息包括绑定卡的卡类型验证信息。

在步骤 S408 中，后台服务器根据绑定卡的卡类型验证信息，进行卡类型验证。

在步骤 S409 中，在卡类型验证成功的情况下，后台服务器向应用程序发送第二应答消息。

第二应答消息包括动态验证码。

在步骤 S410 中，应用程序接收验证码输入。

在步骤 S411 中，应用程序向后台服务器发送绑定验证消息。

绑定验证消息包括输入验证码。

在步骤 S412 中，后台服务器根据输入验证码，进行验证码验证。

在步骤 S413 中，在验证码验证成功的情况下，后台服务器向 TSM 服务器发送专用卡信息请求消息。

在步骤 S414 中，TSM 服务器向 TSP 服务器发送专用卡信息请求消息。

在步骤 S415 中，TSP 服务器为绑定卡生成专用卡信息。

在步骤 S416 中，TSP 服务器向 TSM 服务器发送绑定卡的专用卡信息。

在步骤 S417 中，TSM 服务器向后台服务器发送绑定卡的专用卡信息。

在步骤 S418 中，后台服务器向应用程序发送第三应答消息。

第三应答消息包括绑定卡的专用卡信息。

在步骤 S419 中，应用程序向安全元件传输绑定卡的专用卡信息。

在步骤 S420 中，安全元件存储绑定卡的专用卡信息，设置绑定卡的

生命状态，生成第一映射关系。

在步骤 S421 中，安全元件将绑定卡的生命状态传输至应用程序。

在步骤 S422 中，应用程序向后台服务器发送绑定卡的生命状态。

在步骤 S423 中，后台服务器向应用程序发送第一反馈消息。

第一反馈消息表征服务器中绑定卡的生命状态同步成功。

在步骤 S424，应用程序发出提示消息，提示用户卡绑定成功。

图 14 为本申请实施例提供的卡删除流程的一示例的流程图。如图 12 所示，卡删除流程可包括步骤 S501 至步骤 S509。

在步骤 S501 中，应用程序接收卡删除输入。

卡删除输入用于选定待删除卡。

在步骤 S502 中，应用程序向后台服务器发送卡删除请求消息。

卡删除请求消息指示选定的待删除卡。

在步骤 S503 中，后台服务器向应用程序反馈待删除卡的卡交易标识。

在步骤 S504 中，应用程序向安全元件传输待删除卡的卡交易标识。

在步骤 S505 中，安全元件根据待删除卡对应的映射关系，将待删除卡的生命状态更新为失效状态。

在步骤 S506 中，安全元件向应用程序传输待删除卡的生命状态。

在步骤 S507 中，应用程序向后台服务器发送待删除卡的生命状态。

在步骤 S508 中，后台服务器向应用程序发送第二反馈消息。

第二反馈消息用于表征服务器中待删除卡的生命状态同步成功。

在步骤 S509 中，应用程序发出提示消息，提示用户卡删除成功

图 15 为本申请实施例提供的卡绑定流程的另一示例的流程图。其中的绑定卡为曾与用户终端的应用程序绑定且被删除过的卡。如图 13 所示，卡绑定流程可包括步骤 S601 至步骤 S610。

在步骤 S601 中，应用程序接收卡绑定输入。

卡绑定输入可包括绑定卡的卡标识。

在步骤 S602 中，应用程序向后台服务器发送第一卡绑定消息。

第一卡绑定消息包括绑定卡的卡标识。

在步骤 S603 中，后台服务器根据卡标识，确定绑定卡曾被删除，获取曾为该绑定卡分配的专用卡信息，不需要为该绑定卡重新生成专用卡信息。

在步骤 S604 中，后台服务器向应用程序发送绑定卡的专用卡信息。

在步骤 S605 中，应用程序向安全元件传输绑定卡的专用卡信息。

在步骤 S606 中，安全元件存储绑定卡的专用卡信息，更新绑定卡的生命状态。

在步骤 S607 中，安全元件将绑定卡的生命状态传输至应用程序。

在步骤 S608 中，应用程序向后台服务器发送绑定卡的生命状态。

在步骤 S609 中，后台服务器向应用程序发送第三反馈消息。

第三反馈消息表征服务器中绑定卡的生命状态同步成功。

在步骤 S610，应用程序发出提示消息，提示用户卡绑定成功。

本申请第三方面提供一种用户终端。用户终端具有安全元件。安全元件存储有第一类通用个人化数据和第二类通用个人化数据。图 16 为本申请第三方面提供的用户终端的一实施例的结构示意图。如图 16 所示，该用户终端 700 可包括发送模块 701、接收模块 702 和处理模块 703。

发送模块 701 可用于向服务器发送卡绑定消息，以使服务器确定绑定卡的卡类型，并在绑定卡验证成功的情况下，为绑定卡分配专用卡信息。

卡绑定消息包括绑定卡的卡认证信息。专用卡信息包括卡交易标识。在一些示例中，专用卡信息还包括专用个人化数据。

接收模块 702 可用于接收服务器发送的绑定卡的卡类型和绑定卡的专用卡信息。

处理模块 703 可用于将绑定卡的专用卡信息加载至安全元件。

绑定卡的专用卡信息与匹配通用个人化数据用于进行绑定卡的交易验证。匹配通用个人化数据为与绑定卡的卡类型匹配的第一类通用个人化数据或第二类通用个人化数据。第一映射关系包括绑定卡的专用卡信息、绑定卡的卡类型和绑定卡的生命状态的映射关系。

在一些示例中，在绑定卡包括卡类型相同的第一卡和第二卡的情况下，第一卡的专用卡信息与目标匹配通用个人化数据用于进行第一卡的交

易验证，第二卡的专用卡信息与目标匹配通用个人化数据用于进行第二卡的交易验证。其中，目标匹配通用个人化数据为与第一卡的卡类型匹配的第一类通用个人化数据或第二类通用个人化数据。

在本申请实施例中，用户终端的安全元件中存储有第一类通用个人化数据和第二类通用个人化数据。在对卡进行绑定的过程中，用户终端通过卡绑定消息与服务器进行交互，以得到服务器为该卡分配的专用卡信息。将得到的专用卡信息加载至安全元件中。在卡绑定的过程中，不需要下载该卡进行交易验证所用的所有个人化数据，在利用该卡进行支付交易的情况下，用户终端和服务器可利用匹配通用个人化数据和该卡的专用卡信息实现交易验证。用户终端不需要重复存储各卡进行交易验证所需要的通用的个人化数据，从而减少了占用的用户终端的存储资源。

而且，在卡绑定过程中，除了用户终端的应用程序初次绑定卡的情况，用户终端需要下载的内容不包括通用的个人化数据，减少了用户终端下载数据花费的时间，从而加快了卡绑定的速度，使得卡绑定流程更加快捷、简单。

在一些示例中，卡绑定消息包括第一卡绑定消息、第二卡绑定消息和绑定验证消息。卡认证信息包括卡标识、卡类型验证信息和输入验证码。

上述发送模块 702 可用于：向服务器发送第一卡绑定消息，第一卡绑定消息包括绑定卡的卡标识；在接收到服务器发送第一应答消息的情况下，向服务器发送第二卡绑定消息，第一应答消息包括绑定卡的卡类型，第二卡绑定信息包括绑定卡的卡类型验证信息；在接收到服务器发送的第二应答消息的情况下，向服务器发送绑定验证消息，第二应答消息包括动态验证码，绑定验证消息包括输入验证码。

具体地，在绑定卡的卡类型为第一类型的情况下，卡类型验证信息包括第一类验证信息；在绑定卡的卡类型为第二类型的情况下，卡类型验证信息包括第二类验证信息。其中，第一类验证信息与第二类验证信息不同。

在一些示例中，上述接收模块 702 还可用于在用户终端初次进行卡绑定的情况下，接收服务器发送的通用程序数据包。

上述处理模块 703 还可用于将通用程序数据包加载至安全元件。

在一些示例中，上述处理模块 703 还可用于通过安全元件将绑定卡的生命状态设置为生效状态，并生成或更新第一映射关系。

图 17 为本申请第三方面提供的用户终端的另一实施例的结构示意图。图 17 与图 16 的不同之处在于，用户终端 700 还可包括同步模块 704。

同步模块 704 可用于将设置后的绑定卡的生命状态和第一映射关系同步至服务器。

在一些示例中，上述接收模块 702 还可用于接收默认卡选取输入。

默认卡选取输入用于指示选定的默认卡；

上述处理模块 703 还可用于控制安全元件将原始默认卡的生命状态更新为生效状态。

原始默认卡更新前的生命状态为默认使用状态；

上述处理模块 703 还可用于控制安全元件将默认卡的生命状态更新为默认使用状态。

上述同步模块 704 还可用于将更新后的默认卡的生命状态和更新后的原始默认卡的生命状态同步至服务器。

在一些示例中，上述发送模块 701 还可用于向服务器发送卡删除请求消息，以使服务器反馈待删除卡的卡交易标识。

卡删除请求消息指示选定的待删除卡。

上述接收模块 702 还可用于接收服务器反馈的待删除卡的卡交易标识。

上述处理模块 703 还可用于控制安全元件将待删除卡的生命状态更新为失效状态。

上述同步模块 704 还可用于将更新后的待删除卡的生命状态同步至服务器。

在一些示例中，上述处理模块 703 还可用于删除第二映射关系，第二映射关系包括待删除卡的专用卡信息、待删除卡的卡类型和待删除卡的生命状态的映射关系。

本申请第四方面提供一种服务器。服务器存储有第一类通用个人化数据和第二类通用个人化数据。图 18 为本申请第四方面提供的服务器的一实施例的结构示意图。如图 18 所示，服务器 800 可包括接收模块 801、处理模块 802 和发送模块 803。

接收模块 801 可用于接收用户终端发送的卡绑定消息。

卡绑定消息包括绑定卡的卡认证信息。

处理模块 802 可用于响应卡绑定消息，确定绑定卡的卡类型，并对绑定卡进行验证，在验证成功的情况下，为绑定卡分配专用卡信息。

专用卡信息包括卡交易标识。绑定卡的专用卡信息与匹配通用个人化数据用于进行绑定卡的交易验证。匹配通用个人化数据为与绑定卡的卡类型匹配的第一类通用个人化数据或第二类通用个人化数据。

在一些示例中，专用卡信息还包括专用个人化数据。

发送模块 803 可用于向服务器发送卡绑定应答消息。

卡绑定应答消息包括绑定卡的卡类型和绑定卡的专用卡信息。

在一些示例中，在绑定卡包括卡类型相同的第一卡和第二卡的情况下，第一卡的专用卡信息与目标匹配通用个人化数据用于进行第一卡的交易验证，第二卡的专用卡信息与目标匹配通用个人化数据用于进行第二卡的交易验证。其中，目标匹配通用个人化数据为与第一卡的卡类型匹配的第一类通用个人化数据或第二类通用个人化数据。

在本申请实施例中，服务器接收用户终端发送的卡绑定消息，响应于卡绑定消息，确定绑定卡的卡类型，并对绑定卡进行验证，在验证成功的情况下，为绑定卡分配专用卡信息，并向用户终端发送，以使用户终端接收绑定卡的专用卡信息。在利用该卡进行支付交易的情况下，用户终端和服务器可利用用户终端，通用个人化数据和该卡的专用卡信息实现交易验证。服务器不需要在每一次卡绑定过程中将绑定的卡进行交易验证所需的通用的个人化数据重复发送给用户终端，从而减少了占用的用户终端的存储资源，也能够减少下载过程中占用的下载资源。

而且，在卡绑定过程中，除了用户终端的应用程序初次绑定卡的情况，服务器需要向用户终端发送的内容不包括通用的个人化数据，减少了

用户终端下载数据花费的时间，从而加快了卡绑定的速度，使得卡绑定流程更加快捷、简单。

在一些示例中，卡绑定应答消息包括第一应答消息、第二应答消息和第三应答消息。卡认证信息包括卡标识、卡类型验证信息和输入验证码。

上述发送模块 803 可用于：在响应于用户终端发送的第一卡绑定消息确定绑定卡的卡类型的情况下，向用户终端发送第一应答消息，第一应答消息包括绑定卡的卡类型，第一卡绑定消息包括绑定卡的卡标识；在响应于用户终端发送的第二卡绑定消息对绑定卡的卡类型验证成功的情况下，向用户终端发送第二应答消息，第二卡绑定消息包括与绑定卡的卡类型匹配的卡类型验证信息，第二应答消息包括动态验证码；在响应于用户终端发送的绑定验证消息对绑定卡的验证码验证成功的情况下，向用户终端发送第三应答消息，绑定验证消息包括输入验证码，第三应答消息包括绑定卡的专用卡信息。

在一些示例中，卡绑定消息包括第一卡绑定消息、第二卡绑定消息和绑定验证消息。

上述处理模块 802 可用于：根据第一卡绑定消息中绑定卡的卡标识，确定绑定卡的卡类型；利用第二卡绑定消息中绑定卡的卡类型验证信息，对绑定卡进行卡类型验证；在绑定验证消息中的输入验证码与动态验证码一致的情况下，为绑定卡分配专用卡信息。

具体地，在绑定卡的卡类型为第一类型的情况下，卡类型验证信息包括第一类验证信息；在绑定卡的卡类型为第二类型的情况下，卡类型验证信息包括第二类验证信息。其中，第一类验证信息与第二类验证信息不同。

在一些示例中，上述发送模块 803 还可用于在用户终端初次进行卡绑定的情况下，向用户终端发送通用程序数据包。

图 19 为本申请第四方面提供的服务器的另一实施例的结构示意图。图 19 与图 18 的不同之处在于，图 19 所示的服务器 800 还可包括同步模块 804。

同步模块 804 用于与用户终端同步设置后的绑定卡的生命状态和第一

映射关系。

第一映射关系包括绑定卡的专用卡信息、绑定卡的卡类型和绑定卡的生命状态的映射关系。

在一些示例中，上述同步模块 804 还可用于与用户终端同步更新后的默认卡的生命状态和更新后的原始默认卡的生命状态，原始默认卡更新前的生命状态为默认使用状态。

在一些示例中，上述发送模块 803 还可用于响应于用户终端发送的卡删除请求，向用户终端反馈待删除卡的卡交易标识。

卡删除请求消息指示选定的待删除卡。

上述同步模块 804 还可用于与用户终端同步更新后的待删除卡的生命状态。

在一些示例中，上述处理模块 802 还可用于删除第二映射关系。

第二映射关系包括待删除卡的专用卡信息、待删除卡的卡类型和待删除卡的生命状态的映射关系。

本申请第五方面提供了一种用户终端。图 20 为本申请第五方面提供的用户终端的一实施例的结构示意图。如图 20 所示，用户终端 900 包括存储器 901、处理器 902 及存储在存储器 901 上并可在处理器 902 上运行的计算机程序。

在一个示例中，上述处理器 902 可以包括中央处理器（CPU），或者特定集成电路（Application Specific Integrated Circuit，ASIC），或者可以被配置成实施本申请实施例的一个或多个集成电路。

存储器 901 可包括只读存储器（Read-Only Memory，ROM），随机存取存储器（Random Access Memory，RAM），磁盘存储介质设备，光存储介质设备，闪存设备，电气、光学或其他物理/有形的存储器存储设备。因此，通常，存储器包括一个或多个编码有包括计算机可执行指令的软件的有形（非暂态）计算机可读存储介质（例如，存储器设备），并且当该软件被执行（例如，由一个或多个处理器）时，其可操作来执行参考根据本申请第一方面的卡管理方法所描述的操作。

处理器 902 通过读取存储器 901 中存储的可执行程序代码来运行与可执行程序代码对应的计算机程序，以用于实现上述实施例中第一方面的卡管理方法。

在一个示例中，用户终端 900 还可包括通信接口 903 和总线 904。其中，如图 20 所示，存储器 901、处理器 902、通信接口 903 通过总线 904 连接并完成相互间的通信。

通信接口 903，主要用于实现本申请实施例中各模块、装置、单元和/或设备之间的通信。也可通过通信接口 903 接入输入设备和/或输出设备。

总线 904 包括硬件、软件或两者，将用户终端 900 的部件彼此耦接在一起。举例来说而非限制，总线 904 可包括加速图形端口（Accelerated Graphics Port，AGP）或其他图形总线、增强工业标准架构（Enhanced Industry Standard Architecture，EISA）总线、前端总线（Front Side Bus，FSB）、超传输（Hyper Transport，HT）互连、工业标准架构（Industrial Standard Architecture，ISA）总线、无限带宽互连、低引脚数（Low pin count，LPC）总线、存储器总线、微信道架构（Micro Channel Architecture，MCA）总线、外围组件互连（Peripheral Component Interconnect，PCI）总线、PCI-Express（PCI-X）总线、串行高级技术附件（Serial Advanced Technology Attachment，SATA）总线、视频电子标准协会局部（Video Electronics Standards Association Local Bus，VLB）总线或其他合适的总线或者两个或更多个以上这些的组合。在合适的情况下，总线 904 可包括一个或多个总线。尽管本申请实施例描述和示出了特定的总线，但本申请考虑任何合适的总线或互连。

本申请第六方面提供了一种服务器。图 21 为本申请第六方面提供的服务器的一实施例的结构示意图。如图 21 所示，服务器 1000 包括存储器 1001、处理器 1002 及存储在存储器 1001 上并可在处理器 1002 上运行的计算机程序。

在一个示例中，上述处理器 1002 可以包括中央处理器（CPU），或者特定集成电路（Application Specific Integrated Circuit，ASIC），或者可以被配置成实施本申请实施例的一个或多个集成电路。

存储器 1001 可包括只读存储器（Read-Only Memory，ROM），随机存取存储器（Random Access Memory，RAM），磁盘存储介质设备，光存储介质设备，闪存设备，电气、光学或其他物理/有形的存储器存储设备。因此，通常，存储器包括一个或多个编码有包括计算机可执行指令的软件的有形（非暂态）计算机可读存储介质（例如，存储器设备），并且当该软件被执行（例如，由一个或多个处理器）时，其可操作来执行参考根据本申请第二方面的卡管理方法所描述的操作。

处理器 1002 通过读取存储器 1001 中存储的可执行程序代码来运行与可执行程序代码对应的计算机程序，以用于实现上述实施例中第二方面的卡管理方法。

在一个示例中，服务器 1000 还可包括通信接口 1003 和总线 1004。其中，如图 21 所示，存储器 1001、处理器 1002、通信接口 1003 通过总线 1004 连接并完成相互间的通信。

通信接口 1003，主要用于实现本申请实施例中各模块、装置、单元和/或设备之间的通信。也可通过通信接口 1003 接入输入设备和/或输出设备。

总线 1004 包括硬件、软件或两者，将服务器 1000 的部件彼此耦接在一起。举例来说而非限制，总线 1004 可包括加速图形端口（Accelerated Graphics Port，AGP）或其他图形总线、增强工业标准架构（Enhanced Industry Standard Architecture，EISA）总线、前端总线（Front Side Bus，FSB）、超传输（Hyper Transport，HT）互连、工业标准架构（Industrial Standard Architecture，ISA）总线、无限带宽互连、低引脚数（Low pin count，LPC）总线、存储器总线、微信道架构（Micro Channel Architecture，MCA）总线、外围组件互连（Peripheral Component Interconnect，PCI）总线、PCI-Express（PCI-X）总线、串行高级技术附件（Serial Advanced Technology Attachment，SATA）总线、视频电子标准协会局部（Video Electronics Standards Association Local Bus，VLB）总线或其他合适的总线或者两个或更多个以上这些的组合。在合适的情况下，总线 1004 可包括一个或多个总线。尽管本申请实施例描述和示出了特定的

总线，但本申请考虑任何合适的总线或互连。

本申请第七方面还提供了一种卡管理系统。该卡管理系统可包括上述实施例中的用户终端和服务器，具体内容可参见上述实施例中的相关说明，在此不再赘述。

本申请第八方面还提供一种计算机存储介质，该计算机存储介质上存储有计算机程序，该计算机程序被处理器执行时可实现上述实施例中的卡管理方法，且能达到相同的技术效果，为避免重复，这里不再赘述。其中，上述计算机存储介质可包括非暂态计算机可读存储介质，如只读存储器（Read-Only Memory，简称 ROM）、随机存取存储器（Random Access Memory，简称 RAM）、磁碟或者光盘等，在此并不限定。

需要明确的是，本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同或相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。对于用户终端实施例、服务器实施例、系统实施例、计算机存储介质实施例而言，相关之处可以参见方法实施例的说明部分。本申请并不局限于上文所描述并在图中示出的特定步骤和结构。本领域的技术人员可以在领会本申请的精神之后，作出各种改变、修改和添加，或者改变步骤之间的顺序。并且，为了简明起见，这里省略对已知方法技术的详细描述。

上面参考根据本申请的实施例的方法、装置（系统）和计算机程序产品的流程图和/或框图描述了本申请的各方面。应当理解，流程图和/或框图中的每个方框以及流程图和/或框图中各方框的组合可以由计算机程序指令实现。这些计算机程序指令可被提供给通用计算机、专用计算机、或其它可编程数据处理装置的处理器，以产生一种机器，使得经由计算机或其它可编程数据处理装置的处理器执行的这些指令使能对流程图和/或框图的一个或多个方框中指定的功能/动作的实现。这种处理器可以是但不限于是通用处理器、专用处理器、特殊应用处理器或者现场可编程逻辑电路。还可理解，框图和/或流程图中的每个方框以及框图和/或流程图中的方框的组合，也可以由执行指定的功能或动作的专用硬件来实现，或可由专用硬件和计算机指令的组合来实现。

本领域技术人员应能理解，上述实施例均是示例性而非限制性的。在不同实施例中出现的不同技术特征可以进行组合，以取得有益效果。本领域技术人员在研究附图、说明书及权利要求书的基础上，应能理解并实现所揭示的实施例的其他变化的实施例。在权利要求书中，术语“包括”并不排除其他装置或步骤；数量词“一个”不排除多个；术语“第一”、“第二”用于标示名称而非用于表示任何特定的顺序。权利要求中的任何附图标记均不应被理解为对保护范围的限制。权利要求中出现的多个部分的功能可以由一个单独的硬件或软件模块来实现。某些技术特征出现在不同的从属权利要求中并不意味着不能将这些技术特征进行组合以取得有益效果。