(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 112232805 B
(45)授权公告日 2021.03.02

(21)申请号 202011469593.8
(22)申请日 2020.12.15
(65)同一申请的已公布的文献号
申请公布号 CN 112232805 A
(43)申请公布日 2021.01.15
(73)专利权人 中国银联股份有限公司
地址 200135 上海市浦东新区含笑路36号
(72)发明人 刘刚 彭程 孙权 邹震中
詹成初 才华
(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 贺琳
(51)Int.Cl.
G06Q 20/34(2012.01)
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)

(56)对比文件
CN 105719391 A,2016.06.29
CN 103186858 A,2013.07.03
CN 111932245 A,2020.11.13
CN 111932244 A,2020.11.13
CN 106600266 A,2017.04.26

审查员 黄旭光

权利要求书5页 说明书26页 附图13页

(54)发明名称

卡管理方法、用户终端、服务器、系统及存储介质

(57)摘要

本申请公开了一种卡管理方法、用户终端、服务器、系统及存储介质，属于数据处理领域。用户终端的安全元件存储有第一类通用卡实例和第二类通用卡实例，第一匹配通用卡实例用于绑定卡的交易验证，第一匹配通用卡实例包括第一匹配通用卡标识，第一匹配通用卡标识为与绑定卡的卡类型匹配的第一类通用卡标识或第二类通用卡标识。该方法包括：向服务器发送卡绑定消息，卡绑定消息包括安全元件标识和绑定卡认证信息，以使服务器为绑定卡分配卡交易标识，并建立第一映射关系；接收服务器发送的绑定卡的卡交易标识；将绑定卡的卡交易标识存储至安全元件。根据本申请实施例，能够降低卡管理流程的繁琐程度。

CN 112232805 B

1.一种卡管理方法,其特征在于,应用于用户终端,所述用户终端包括安全元件,所述安全元件存储有第一类通用卡实例和第二类通用卡实例,所述第一类通用卡实例包括第一类通用卡标识和第一类通用个人化数据,所述第二类通用卡实例包括第二类通用卡标识和第二类通用个人化数据,所述第一类通用卡实例用于所述用户终端进行卡类型为第一类型的卡的交易验证,所述第二类通用卡实例用于所述用户终端进行卡类型为第二类型的卡的交易验证;

所述方法包括:

向服务器发送卡绑定消息,所述卡绑定消息包括所述安全元件的安全元件标识和绑定卡的卡认证信息,以使所述服务器为所述绑定卡分配卡交易标识,并建立第一映射关系,所述第一映射关系包括所述安全元件标识、第一匹配通用卡标识和所述绑定卡的卡交易标识的映射关系,所述第一匹配通用卡标识为与所述绑定卡的卡类型匹配的所述第一类通用卡标识或所述第二类通用卡标识;

接收所述服务器发送的所述绑定卡的卡交易标识;

将所述绑定卡的卡交易标识存储至所述安全元件,第一匹配通用卡实例用于所述绑定卡的交易验证,所述第一匹配通用卡实例包括所述第一匹配通用卡标识,所述第一匹配通用卡实例为与所述绑定卡的卡类型匹配的所述第一类通用卡实例或所述第二类通用卡实例。

2.根据权利要求1所述的方法,其特征在于,还包括:

在利用所述绑定卡进行联网交易的情况下,利用所述第一匹配通用卡实例进行交易验证计算,向交易设备提供第一交易验证信息,所述第一交易验证信息包括所述绑定卡的卡交易标识,以通过所述交易设备使所述服务器根据所述第一映射关系,利用与所述绑定卡的卡交易标识对应的所述第一匹配通用卡实例进行交易验证计算。

3.根据权利要求1所述的方法,其特征在于,还包括:

在利用所述绑定卡进行脱机交易的情况下,利用所述第一匹配通用卡实例进行交易验证计算,向交易设备提供第二交易验证信息,所述第二交易验证信息包括所述第一匹配通用卡实例,以使所述交易设备利用所述第一匹配通用卡实例进行交易验证计算。

4.根据权利要求1所述的方法,其特征在于,在所述用户终端初次进行卡绑定的情况下,在所述向服务器发送卡绑定消息之前,还包括:

向所述服务器发送初始化请求消息;

与所述服务器建立所述安全元件与所述服务器之间的安全通道;

通过所述安全通道接收所述服务器下发的初始化信息,并将所述初始化信息存储至所述安全元件,所述初始化信息包括所述安全元件标识、加密公钥、所述第一类通用卡实例和所述第二类通用卡实例。

5.根据权利要求4所述的方法,其特征在于,在所述用户终端非初次进行卡绑定的情况下,接收的所述绑定卡的卡交易标识为利用与所述加密公钥成对的加密私钥加密的卡交易标识,

所述将所述绑定卡的卡交易标识存储至所述安全元件,包括:

在所述安全元件内利用所述加密公钥对所述绑定卡的卡交易标识解密,存储解密后的所述绑定卡的卡交易标识。

6.根据权利要求4所述的方法,其特征在于,

在所述安全元件未存储有程序数据包的情况下,所述初始化信息还包括程序数据包;

在所述安全元件中存储的程序数据包需要更新的情况下,所述初始化信息还包括升级后的程序数据包。

7.根据权利要求1所述的方法,其特征在于,还包括:

在所述安全元件中存储的程序数据包需要更新的情况下,向所述服务器发送更新请求消息,所述更新请求消息用于请求更新后的程序数据包。

8.根据权利要求1所述的方法,其特征在于,在所述将所述绑定卡的卡交易标识存储至所述安全元件之后,还包括:

向所述服务器发送验证码获取请求消息;

接收所述服务器响应于所述验证码获取请求消息反馈的第一动态验证码;

接收输入的第二动态验证码;

向所述服务器发送验证码请求消息,所述验证码请求消息包括所述第二动态验证码,以使所述服务器在所述第二动态验证码验证成功的情况下激活所述第一映射关系。

9.根据权利要求1所述的方法,其特征在于,还包括:

接收默认卡设置输入,所述默认卡设置输入用于选定默认卡;

在联网的情况下,向所述服务器发送默认卡设置消息,所述默认卡设置消息包括所述默认卡的卡交易标识,以使所述服务器将第二映射关系的使用状态设置为默认使用状态,所述第二映射关系包括所述安全元件标识、第二匹配通用卡标识和所述默认卡的卡交易标识的映射关系,所述第二匹配通用卡标识为与所述默认卡的卡类型匹配的所述第一类通用卡标识或所述第二类通用卡标识;

接收所述服务器发送的默认卡应答消息,所述默认卡应答消息用于表征所述第二映射关系的使用状态已设置为默认使用状态;

响应于所述默认卡应答消息,通过默认卡设置指令,将所述安全元件中所述默认卡的卡交易标识的使用状态设置为默认使用状态,将所述安全元件中与所述默认卡的卡交易标识对应的第二匹配通用卡实例的生命状态设置为生效状态,所述第二匹配通用卡实例为与所述默认卡的卡类型匹配的所述第一类通用卡实例或所述第二类通用卡实例。

10.根据权利要求1所述的方法,其特征在于,还包括:

响应于接收的卡删除消息,在所述安全元件中删除待删除卡的卡交易标识,或将所述待删除卡的卡交易标识的生命状态设置为失效状态,所述卡删除消息用于指示所述待删除卡。

11.一种卡管理方法,其特征在于,应用于服务器,所述服务器存储有用户终端的第一类通用卡实例和第二类通用卡实例,所述第一类通用卡实例包括第一类通用卡标识和第一类通用个人化数据,所述第二类通用卡实例包括第二类通用卡标识和第二类通用个人化数据,所述第一类通用卡实例用于所述用户终端进行卡类型为第一类型的卡的交易验证,所述第二类通用卡实例用于所述用户终端进行卡类型为第二类型的卡的交易验证;

所述方法包括:

接收所述用户终端发送的卡绑定消息,所述卡绑定消息包括安全元件标识和绑定卡认证信息,所述绑定卡认证信息包括绑定卡的卡认证信息;

响应于所述卡绑定消息，为所述绑定卡分配卡交易标识，并建立第一映射关系，所述第一映射关系包括所述安全元件标识、第一匹配通用卡标识和所述绑定卡的卡交易标识的映射关系，所述第一匹配通用卡标识为与所述绑定卡的卡类型匹配的所述第一类通用卡标识或所述第二类通用卡标识，第一匹配通用卡实例用于所述绑定卡的交易验证，所述第一匹配通用卡实例包括所述第一匹配通用卡标识，所述第一匹配通用卡实例为与所述绑定卡的卡类型匹配的所述第一类通用卡实例或所述第二类通用卡实例；

向所述用户终端发送所述绑定卡的卡交易标识。

12.根据权利要求11所述的方法，其特征在于，还包括：

在利用所述绑定卡进行联网交易的情况下，通过交易设备接收所述用户终端提供的第一交易验证信息，所述第一交易验证信息包括所述绑定卡的卡交易标识，根据所述第一映射关系，利用与所述绑定卡的卡交易标识对应的第一匹配通用卡实例进行交易验证计算。

13.根据权利要求11所述的方法，其特征在于，还包括：

在所述用户终端利用所述绑定卡与交易设备进行脱机交易后，在联网的情况下，获取所述第一匹配通用卡实例，利用所述第一匹配通用卡实例进行交易验证计算。

14.根据权利要求11所述的方法，其特征在于，在所述接收所述用户终端发送的卡绑定消息之前，还包括：

接收所述用户终端发送的初始化请求消息；

响应于所述初始化请求消息，与所述用户终端建立所述用户终端中安全元件与所述服务器之间的安全通道；

通过所述安全通道向所述安全元件下发初始化信息，所述初始化信息包括所述安全元件标识、加密公钥、所述第一类通用卡实例和所述第二类通用卡实例。

15.根据权利要求14所述的方法，其特征在于，在所述服务器非初次接收到所述卡绑定消息的情况下，所述向所述用户终端发送所述绑定卡的卡交易标识，包括：

利用与所述加密公钥成对的加密私钥对所述绑定卡的卡交易标识加密；

向所述用户终端发送加密后的所述绑定卡的卡交易标识。

16.根据权利要求14所述的方法，其特征在于，

在所述安全元件未存储有程序数据包的情况下，所述初始化信息还包括程序数据包；

在所述安全元件中存储的程序数据包需要更新的情况下，所述初始化信息还包括更新后的程序数据包。

17.根据权利要求11所述的方法，其特征在于，还包括：

在所述安全元件中存储的程序数据包需要更新的情况下，接收所述用户终端发送的更新请求消息；

响应所述更新请求消息，向所述用户终端下发更新后的程序数据包。

18.根据权利要求11所述的方法，其特征在于，在所述建立第一映射关系之后，还包括：

接收所述用户终端发送的验证码获取请求消息；

响应所述验证码获取请求消息，向所述用户终端反馈第一动态验证码；

接收所述用户终端发送的验证码请求消息，所述验证码请求消息包括第二动态验证码；

在所述第二动态验证码验证成功的情况下激活所述第一映射关系。

19.根据权利要求11所述的方法,其特征在于,还包括:

在联网的情况下,接收所述用户终端发送的默认卡设置消息,所述默认卡设置消息包括选定的默认卡的卡交易标识;

响应于所述默认卡设置消息,将第二映射关系的使用状态设置为默认使用状态,所述第二映射关系包括所述安全元件标识、第二匹配通用卡标识和所述默认卡的卡交易标识的映射关系;

向所述用户终端发送默认卡应答消息,所述默认卡应答消息用于表征所述第二映射关系的使用状态已设置为默认使用状态。

20.根据权利要求19所述的方法,其特征在于,还包括:

在所述用户终端与交易设备进行脱机交易后,在联网的情况下,确定使用状态为默认使用状态的所述第二映射关系;

利用所述第二映射关系中所述默认卡的卡交易标识进行结算。

21.根据权利要求11所述的方法,其特征在于,还包括:

接收卡删除请求消息,所述卡删除请求消息用于指示待删除卡;

响应于所述卡删除请求消息,删除第三映射关系,或者,将所述第三映射关系的生命状态设置为失效状态,所述第三映射关系包括所述安全元件标识、第三匹配通用卡标识与所述待删除卡的卡交易标识的对应关系,所述第三匹配通用卡标识为与所述待删除卡的卡类型匹配的所述第一类通用卡标识或所述第二类通用卡标识。

22.一种用户终端,其特征在于,所述用户终端具有安全元件,所述安全元件存储有第一类通用卡实例和第二类通用卡实例,所述第一类通用卡实例包括第一类通用卡标识和第一类通用个人化数据,所述第二类通用卡实例包括第二类通用卡标识和第二类通用个人化数据,所述第一类通用卡实例用于所述用户终端进行卡类型为第一类型的卡的交易验证,所述第二类通用卡实例用于所述用户终端进行卡类型为第二类型的卡的交易验证;

所述用户终端包括:

发送模块,用于向服务器发送卡绑定消息,所述卡绑定消息包括安全元件标识和绑定卡认证信息,所述绑定卡认证信息包括绑定卡的卡认证信息,以使所述服务器为所述绑定卡分配卡交易标识,并建立第一映射关系,所述第一映射关系包括所述安全元件标识、第一匹配通用卡标识和所述绑定卡的卡交易标识的映射关系,所述第一匹配通用卡标识为与所述绑定卡的卡类型匹配的所述第一类通用卡标识或所述第二类通用卡标识,第一匹配通用卡实例用于所述绑定卡的交易验证,所述第一匹配通用卡实例包括所述第一匹配通用卡标识,所述第一匹配通用卡实例为与所述绑定卡的卡类型匹配的所述第一类通用卡实例或所述第二类通用卡实例;

接收模块,用于接收所述服务器发送的所述绑定卡的卡交易标识;

处理模块,用于将所述绑定卡的卡交易标识存储至所述安全元件。

23.一种服务器,其特征在于,所述服务器存储有用户终端的第一类通用卡实例和第二类通用卡实例,所述第一类通用卡实例包括第一类通用卡标识和第一类通用个人化数据,所述第二类通用卡实例包括第二类通用卡标识和第二类通用个人化数据,所述第一类通用卡实例用于所述用户终端进行卡类型为第一类型的卡的交易验证,所述第二类通用卡实例用于所述用户终端进行卡类型为第二类型的卡的交易验证;

所述服务器包括：

接收模块，用于接收所述用户终端发送的卡绑定消息，所述卡绑定消息包括安全元件标识和绑定卡认证信息，所述绑定卡认证信息包括绑定卡的卡认证信息；

处理模块，用于响应于所述卡绑定消息，为所述绑定卡分配卡交易标识，并建立第一映射关系，所述第一映射关系包括所述安全元件标识、第一匹配通用卡标识和所述绑定卡的卡交易标识的映射关系，所述第一匹配通用卡标识为与所述绑定卡的卡类型匹配的所述第一类通用卡标识或所述第二类通用卡标识，第一匹配通用卡实例用于所述绑定卡的交易验证，所述第一匹配通用卡实例包括所述第一匹配通用卡标识，所述第一匹配通用卡实例为与所述绑定卡的卡类型匹配的所述第一类通用卡实例或所述第二类通用卡实例；

发送模块，用于向所述用户终端发送所述绑定卡的卡交易标识。

24.一种用户终端，其特征在于，包括：处理器以及存储有计算机程序指令的存储器；

所述处理器执行所述计算机程序指令时实现如权利要求1至10中任意一项所述的卡管理方法。

25.一种服务器，其特征在于，包括：处理器以及存储有计算机程序指令的存储器；

所述处理器执行所述计算机程序指令时实现如权利要求11至21中任意一项所述的卡管理方法。

26.一种卡管理系统，其特征在于，包括如权利要求24所述的用户终端和如权利要求25所述的服务器。

27.一种计算机存储介质，其特征在于，所述计算机存储介质上存储有计算机程序指令，所述计算机程序指令被处理器执行时实现如权利要求1至21中任意一项所述的卡管理方法。

卡管理方法、用户终端、服务器、系统及存储介质

技术领域

[0001] 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

[0002] 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卡。

[0003] 用户可根据需求的变化，对卡进行管理，例如增加应用程序中绑定的卡，或删除应用程序中绑定的卡等。为了使卡能够进行支付交易，在多次绑定卡的情况下，需要频繁地进行增加的绑定的卡对应的程序数据包和个人化数据的下载和存储，使卡管理流程更加繁琐。

发明内容

[0004] 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，能够降低卡管理流程的繁琐程度。

[0005] 第一方面，本申请实施例提供一种卡管理方法，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卡实例和第二类通用卡实例，第一类通用卡实例包括第一类通用卡标识和第一类通用个人化数据，第二类通用卡实例包括第二类通用卡标识和第二类通用个人化数据，第一类通用卡实例用于用户终端进行卡类型为第一类型的卡的交易验证，第二类通用卡实例用于用户终端进行卡类型为第二类型的卡的交易验证；

[0006] 方法包括：向服务器发送卡绑定消息，卡绑定消息包括安全元件的安全元件标识和绑定卡的卡认证信息，以使服务器为绑定卡分配卡交易标识，并建立第一映射关系，第一映射关系包括安全元件标识、第一匹配通用卡标识和绑定卡的卡交易标识的映射关系，第一匹配通用卡标识为与绑定卡的卡类型匹配的第一类通用卡标识或第二类通用卡标识；接收服务器发送的绑定卡的卡交易标识；将绑定卡的卡交易标识存储至安全元件，第一匹配通用卡实例用于绑定卡的交易验证，第一匹配通用卡实例包括第一匹配通用卡标识，第一匹配通用卡实例为与绑定卡的卡类型匹配的第一类通用卡实例或第二类通用卡实例。

[0007] 第二方面，本申请实施例提供一种卡管理方法，其特征在于，应用于服务器，服务器存储有用户终端的第一类通用卡实例和第二类通用卡实例，第一类通用卡实例包括第一类通用卡标识和第一类通用个人化数据，第二类通用卡实例包括第二类通用卡标识和第二类通用个人化数据，第一类通用卡实例用于用户终端进行卡类型为第一类型的卡的交易验证，第二类通用卡实例用于用户终端进行卡类型为第二类型的卡的交易验证；

[0008] 方法包括：接收用户终端发送的卡绑定消息，卡绑定消息包括安全元件标识和绑定卡认证信息，绑定卡认证信息包括绑定卡的卡认证信息；响应于卡绑定消息，为绑定卡分配卡交易标识，并建立第一映射关系，第一映射关系包括安全元件标识、第一匹配通用卡标

识和绑定卡的卡交易标识的映射关系，第一匹配通用卡标识为与绑定卡的卡类型匹配的第一类通用卡标识或第二类通用卡标识；向用户终端发送绑定卡的卡交易标识，第一匹配通用卡实例用于绑定卡的交易验证，第一匹配通用卡实例包括第一匹配通用卡标识，第一匹配通用卡实例为与绑定卡的卡类型匹配的第一类通用卡实例或第二类通用卡实例。

[0009] 第三方面，本申请实施例提供一种用户终端，其特征在于，用户终端具有安全元件，安全元件存储有第一类通用卡实例和第二类通用卡实例，第一类通用卡实例包括第一类通用卡标识和第一类通用个人化数据，第二类通用卡实例包括第二类通用卡标识和第二类通用个人化数据，第一类通用卡实例用于用户终端进行卡类型为第一类型的卡的交易验证，第二类通用卡实例用于用户终端进行卡类型为第二类型的卡的交易验证；

[0010] 用户终端包括：发送模块，用于向服务器发送卡绑定消息，卡绑定消息包括安全元件标识和绑定卡认证信息，绑定卡认证信息包括绑定卡的卡认证信息，以使服务器为绑定卡分配卡交易标识，并建立第一映射关系，第一映射关系包括安全元件标识、第一匹配通用卡标识和绑定卡的卡交易标识的映射关系，第一匹配通用卡标识为与绑定卡的卡类型匹配的第一类通用卡标识或第二类通用卡标识，第一匹配通用卡实例用于绑定卡的交易验证，第一匹配通用卡实例包括第一匹配通用卡标识，第一匹配通用卡实例为与绑定卡的卡类型匹配的第一类通用卡实例或第二类通用卡实例；接收模块，用于接收服务器发送的绑定卡的卡交易标识；处理模块，用于将绑定卡的卡交易标识存储至安全元件。

[0011] 第四方面，本申请实施例提供一种服务器，其特征在于，服务器存储有用户终端的第一类通用卡实例和第二类通用卡实例，第一类通用卡实例包括第一类通用卡标识和第一类通用个人化数据，第二类通用卡实例包括第二类通用卡标识和第二类通用个人化数据，第一类通用卡实例用于用户终端进行卡类型为第一类型的卡的交易验证，第二类通用卡实例用于用户终端进行卡类型为第二类型的卡的交易验证；

[0012] 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，卡绑定消息包括安全元件标识和绑定卡认证信息，绑定卡认证信息包括绑定卡的卡认证信息；处理模块，用于响应于卡绑定消息，为绑定卡分配卡交易标识，并建立第一映射关系，第一映射关系包括安全元件标识、第一匹配通用卡标识和绑定卡的卡交易标识的映射关系，第一匹配通用卡标识为与绑定卡的卡类型匹配的第一类通用卡标识或第二类通用卡标识，第一匹配通用卡实例用于绑定卡的交易验证，第一匹配通用卡实例包括第一匹配通用卡标识，第一匹配通用卡实例为与绑定卡的卡类型匹配的第一类通用卡实例或第二类通用卡实例；发送模块，用于向用户终端发送绑定卡的卡交易标识。

[0013] 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。

[0014] 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。

[0015] 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。

[0016] 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。

[0017] 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卡实例和第二类通用卡实例。用户终端通过向服务器发送卡绑定消息，使服务器为绑定卡分配卡交易标识，并建立安全元件标识、第一匹配通用卡标识和分配的卡交易标识的映射关系。用户终端自身可利用绑定卡对应的第一匹配通用卡实例进行交易验证，服务器利用确定的第一匹配通用卡实例进行交易验证。第一匹配通用卡实例为与绑定卡的卡类型匹配的第一类通用卡实例或第二类通用卡实例。即利用第一类通用卡实例或第二类通用卡实例即可完成交易验证。在绑定卡的过程中，服务器并不需要为每张卡分配对应的个人化数据，因此不需要在每次绑卡的过程中下载个人化数据，从而避免频繁地进行个人化数据的下载和存储，降低了卡管理流程的繁琐程度。

附图说明

[0018] 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。

[0019] 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；

[0020] 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；

[0021] 图3为本申请实施例提供的服务器中存储的映射关系的一示例的示意图；

[0022] 图4为本申请第一方面提供的卡管理方法的一示例的流程图；

[0023] 图5为本申请第一方面提供卡管理方法的另一实施例的流程图；

[0024] 图6为本申请第一方案提供的卡管理方法的又一实施例的流程图；

[0025] 图7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；

[0026] 图8为本申请第一方案提供的卡管理方法的又再一实施例的流程图；

[0027] 图9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；

[0028] 图10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；

[0029] 图11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；

[0030] 图12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；

[0031] 图13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；

[0032] 图14为本申请实施例提供的初始化流程的一示例的流程图；

[0033] 图15为本申请实施例提供的卡绑定流程的一示例的流程图；

[0034] 图16为本申请实施例提供的卡删除流程的一示例的流程图；

[0035] 图17为本申请实施例提供的卡删除流程的另一示例的流程图；

[0036] 图18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；

[0037] 图19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；

[0038] 图20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；

[0039] 图21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；

[0040] 图22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；

[0041] 图23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

[0042] 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。

[0043] 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，会为每张卡分配对应的程序数据包和个人化数据，并存储在用户终端。每绑定一张卡，用户终端都需要下载和存储为这一张卡分配的程序数据包和个人化数据。在应用程序绑定多张卡的情况下，用户终端需要多次下载和存储卡对应的程序数据包和个人化数据。在应用程序删除卡的情况下，用户终端需要将该卡对应的程序数据包和个人化数据删除。程序数据包和个人化数据频繁的下载、删除，使得卡管理流程更加繁琐。尤其是在用户将删除的卡重新绑定的情况下，用户终端需要将该卡对应的程序数据包和个人化数据重新下载，卡管理流程的繁琐程度更加严重。

[0044] 本申请实施例提供一种卡管理方法、终端设备、服务器、系统及存储介质，能够避免个人化数据频繁的下载和删除，从而简化卡管理流程，降低卡管理流程的繁琐程度。

[0045] 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。

[0046] 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。用户可通过应用程序实现支付交易。

[0047] 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卡实例和第二类通用卡实例。具体的，可在初次进行卡绑定的过程中，通过初始化操作将第一类通用卡实例和第二类通用卡实例下载至安全元件中；也可在用户终端出厂前将第一类通用卡实例和第二类通用卡实例预置在安全元件中，在此并不限定。

[0048] 第一类通用卡实例包括第一类通用卡标识和第一类通用个人化数据。第一类通用卡实例用于用户终端进行卡类型为第一类型的卡的交易验证。第一类通用卡标识包括卡类型为第一类型的卡的通用标识。第一类通用个人化数据包括卡类型为第一类型的卡的通用的个人化数据。在卡类型为第一类型的卡进行支付交易的情况下，可利用第一类通用卡实例进行交易验证计算。

[0049] 第二类通用卡实例包括第二类通用卡标识和第二类通用个人化数据。第二类通用卡实例用于用户终端进行卡类型为第二类型的卡的交易验证。第二类通用卡标识包括卡类型为第二类型的卡的通用标识。第二类通用个人化数据包括卡类型为第二类型的卡的通用

的个人化数据。在卡类型为第二类型的卡进行支付交易的情况下，可利用第二类通用卡实例进行交易验证计算。

[0050] 安全元件中还可存储应用程序中绑定的卡的卡交易标识。不同的卡的卡交易标识不同。卡的卡交易标识可在绑定卡的过程中由管理服务器分配，用户终端接收卡的卡交易标识并存储于安全元件。通过不同的卡交易标识可在卡中资源转移、清算等过程中，区分进行支付交易的具体卡。

[0051] 第一类通用卡标识与第二类通用卡标识的格式可以不同。例如，第一类通用卡标识为借记通用卡标识，借记通用卡标识可为19位标识；第二类通用卡标识为贷记通用卡标识，贷记通用卡标识可为16为标识。卡类型不同的卡的卡交易标识的格式也可以不同。例如，借记卡的卡交易标识可为19位标识，贷记卡的卡交易标识可为16位标识。

[0052] 在一些示例中，安全元件中还可存储有一个程序数据包。该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、第一类通用卡实例和第二类通用卡实例等的内部操作可共用这一个程序数据包，且该程序数据包存储至安全元件后，不再删除，避免程序数据包的频繁下载和删除。具体地，该程序数据包可在初次进行卡绑定的过程中通过初始化操作下载至安全元件中；也可在用户终端出厂前将该程序数据包预置在安全元件中，在此并不限定。

[0053] 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Cap包、第一类通用卡实例、第二类通用卡实例和绑定的各个银行卡的卡交易标识。第一类型的卡为银行卡中的借记卡，第一类通用卡标识可作为与应用程序绑定的卡中的所有借记卡通用的卡标识，第一类通用卡标识记为Token A，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，第二类通用卡标识可作为与应用程序绑定的卡中的所有贷记卡通用的卡标识，第二类通用卡标识记为TokenB，第二类通用个人化数据记为DataB。设应用程序绑定有银行卡C1、C2、C3和C4。其中，银行卡C1和C2为借记卡，银行卡C1和C2各自的卡交易标识分别为Token1和Token 2。银行卡C3和C4为贷记卡，银行卡C3和C4各自的卡交易标识分别为Token 3和Token 4。

[0054] 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卡实例、第四类通用卡实例等，第三类通用卡实例、第四类通用卡实例等与第一通用卡实例、第二通用卡实例类似，作用和在卡管理流程中的使用可参考第一通用卡实例、第二通用卡实例，在此不再赘述。

[0055] 用户终端存储通用卡实例，并不需要下载、存储每张卡对应的实例，可减小用户终端中存储资源的占用率，减少下载所占用的运行资源，优化存储资源和运行资源。

[0056] 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(TrustedService 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。

[0057] 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卡实例和第二类通用卡实例。用户终端的安全元件中的第一类通用卡实例和第二类通用卡实例与服务器中存储的第一类通用卡实例和第二类通用卡实例相同。需要说明的是，不同用

户终端对应的第一类通用卡实例和第二类通用卡实例不同，可由服务器统一分配。

[0058] 服务器12中可存储与该服务器12进行交互的各个终端设备的绑定卡的安全元件标识、匹配通用卡标识和绑定卡的卡交易标识的映射关系。匹配通用卡标识为与绑定卡的卡类型匹配的第一类通用卡标识或第二类通用卡标识。在一些示例中，该映射关系中涉及的元素还可包括与安全元件标识对应的CPLC中的其他信息，在此并不限定。

[0059] 例如，设服务器12与三个不同的用户终端UE1、UE2和UE3分别进行交互。用户终端UE1中安全元件的安全元件标识为SEID1。用户终端UE1对应的借记类通用卡标识为Token A，贷记类通用卡标识为Token B。用户终端UE1对应绑定有两张银行卡，两张银行卡包括一张借记卡和一张贷记卡，借记卡的卡交易标识为Token1，贷记卡的卡交易标识为Token 2。用户终端UE2中安全元件的安全元件标识为SEID 2。用户终端UE2对应的借记类通用卡标识为TokenC，贷记类通用卡标识为Token D。用户终端UE2对应绑定有一张银行卡，该银行卡为借记卡，该借记卡的卡交易标识为Token 3。用户终端UE3中安全元件的安全元件标识为SEID 3。用户终端UE3对应的借记类通用卡标识为TokenE，贷记类通用卡标识为Token F。用户终端UE3对应绑定有三张银行卡，三张银行卡包括两张借记卡和一张贷记卡，借记卡的卡交易标识分别为Token4和Token 5，贷记卡的卡交易标识为Token 6。图3为本申请实施例提供的服务器中存储的映射关系的一示例的示意图，示出了上述各个终端设备的绑定卡的安全元件标识、匹配通用卡标识和绑定卡的卡交易标识的映射关系。

[0060] 在一些示例中，为了便于用户终端与管理服务器之间的交互，可在用户终端安装管理服务器的功能控件，用户终端可通过该功能控件与管理服务器进行交互。例如，用户终端可通过该功能控件与TSM服务器进行交互。

[0061] 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。

[0062] 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4为本申请第一方面提供的卡管理方法的一示例的流程图。如图4所示，该卡管理方法可包括步骤S201至步骤S203。

[0063] 在步骤S201中，向服务器发送卡绑定消息。

[0064] 具体地，用户终端设备可响应于用户对用户终端的应用程序的输入触发卡绑定消息的发送，在此并不限定。

[0065] 卡绑定消息包括安全元件标识和绑定卡认证信息。安全元件标识用于标识安全元件。不同的用户终端中的安全元件的安全元件标识不同。安全元件标识可在初次进行卡绑定的过程中通过初始化操作写入安全元件；也可在用户终端出厂前将安全元件标识预置入安全元件。

[0066] 绑定卡认证信息包括绑定卡的卡认证信息。卡绑定消息请求绑定的卡即为绑定卡。卡认证信息可用于标识卡。例如，在卡为银行卡的情况下，卡认证信息具体可包括银行卡的卡号，还可包括密码、卡所属人手机号、卡有效期、信用卡鉴别密码等，在此并不限定。不同的卡的卡认证信息不同。卡认证信息可通过用户输入或扫描得到，在此并不限定。

[0067] 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为绑定卡分配卡交易标识。卡交易标识用于标识卡，与卡认证信息不同。同一张卡的卡交易标识和卡认证信息均可标识该卡，但由于卡认证信息为敏感信息，在进行支付交易的过程中，通过卡交易标识来进行交易，以避免用户隐私泄露。

[0068] 在服务器接收到卡绑定消息的情况下，服务器还可建立第一映射关系。第一映射关系包括安全元件标识、第一匹配通用卡标识和绑定卡的卡交易标识的映射关系。第一匹配通用卡标识为与绑定卡的卡类型匹配的第一类通用卡标识或第二类通用卡标识。在绑定卡的卡类型为第一类型的情况下，绑定卡的第一匹配通用卡标识为第一类通用卡标识。在绑定卡的卡类型为第二类型的情况下，绑定卡的第一匹配通用卡标识为第二类通用卡标识。

[0069] 在步骤S202中，接收服务器发送的绑定卡的卡交易标识。

[0070] 卡交易标识可用于该绑定卡进行交易。

[0071] 在步骤S203中，将绑定卡的卡交易标识存储至安全元件。

[0072] 为了保证卡交易标识的安全性，将绑定卡的卡交易标识存储至安全元件中。安全元件中存储有绑定的各个卡对应的卡交易标识。

[0073] 用户终端的安全元件中存储的第一匹配通用卡实例可用于该绑定卡的交易验证。第一匹配通用卡实例包括第一匹配通用卡标识。即第一匹配通用卡实例为与绑定卡的卡类型匹配的第一类通用卡实例或第二类通用卡实例。

[0074] 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卡实例和第二类通用卡实例。用户终端通过向服务器发送卡绑定消息，使服务器为绑定卡分配卡交易标识，并建立安全元件标识、第一匹配通用卡标识和分配的卡交易标识的映射关系。用户终端自身可利用绑定卡对应的第一匹配通用卡实例进行交易验证，服务器利用确定的第一匹配通用卡实例进行交易验证。第一匹配通用卡实例为与绑定卡的卡类型匹配的第一类通用卡实例或第二类通用卡实例。即利用第一类通用卡实例或第二类通用卡实例即可完成交易验证。在绑定卡的过程中，服务器并不需要为每张卡分配对应的个人化数据，因此不需要在每次绑卡的过程中下载个人化数据，从而避免频繁地进行个人化数据的下载和存储，降低了卡管理流程的繁琐程度，简化卡管理流程，还可提高卡绑定的速度，减少卡绑定所花费的时间。

[0075] 在用户终端将绑定卡的卡交易标识存储至安全元件后，完成了卡绑定的申请阶段，还需要将绑定卡激活。图5为本申请第一方面提供卡管理方法的另一实施例的流程图。图5与图4的不同之处在于，图5所示的卡管理流程还可包括步骤S204至步骤S207。

[0076] 在步骤S204中，向服务器发送验证码获取请求消息。

[0077] 用户终端在存储绑定卡的卡交易标识后，可通过向服务器发送验证码获取请求，触发绑定卡激活流程。验证码获取请求消息用于请求动态验证码。

[0078] 在步骤S205中，接收服务器响应于验证码获取请求消息反馈的第一动态验证码。

[0079] 服务器响应于验证码获取请求消息，向用户终端发送第一动态验证码。第一动态验证码用于绑定卡激活。第一动态验证码可通过短信、即时通信消息、通话等反馈至用户终端，在此并不限定。用户终端可通过显示文字图像或发出声音以向用户展示第一动态验证码，在此并不限定。

[0080] 在步骤S206中，接收输入的第二动态验证码。

[0081] 第二动态验证码可为用户输入的动态验证码，也可为通过应用程序根据第一动态验证码获取并输入的动态验证码，在此并不限定。

[0082] 在步骤S207中，向服务器发送验证码请求消息，以使服务器在第二动态验证码验

证成功的情况下激活第一映射关系。

[0083] 验证码请求消息包括第二动态验证码。在第一动态验证码与第二动态验证码相同的情况下，确定第二动态验证码验证成功。服务器在第二动态验证码验证成功的情况下，激活第一映射关系。在第一映射关系未激活的情况下，第一映射关系中卡交易标识对应的绑定卡处于不可用状态。在第一映射关系激活的情况下，第一映射关系中卡交易标识对应的绑定卡处于可用状态。

[0084] 在一些示例中，在第一映射关系激活的情况下，用户终端可将第一映射关系中卡交易标识对应的绑定卡的生命状态设置为可用状态。

[0085] 在用户终端初次进行卡绑定的情况下，用户终端需要进行卡管理的初始化流程。图6为本申请第一方案提供的卡管理方法的又一实施例的流程图。图6与图4的不同之处在于，图6所示的卡管理方法还可包括步骤S208至步骤S210。

[0086] 在步骤S208中，向服务器发送初始化请求消息。

[0087] 初始化请求消息用于触发卡管理的初始化流程。

[0088] 在用户终端还安装有与服务器的功能控件的情况下，在用户终端向服务器发送初始化请求消息之前，用户终端还可通过应用程序调用功能控件进行初始化。为了保证初始化的合法性，在用户终端向服务器发送初始化请求信息前，用户终端可与服务器之间先进行用户终端进行卡绑定的应用程序的合法性。

[0089] 在步骤S209中，与服务器建立安全元件与服务器之间的安全通道。

[0090] 安全通道具体可为GP通道，在此并不限定。用户终端中安全元件还可与服务器相互进行认证，在认证成功后，服务器即可通过安全通道与安全元件进行交互。安全通道能够提高用户终端与服务器之间交互的安全性。

[0091] 在步骤S210中，通过安全通道接收服务器下发的初始化信息，并将初始化信息存储至安全元件。

[0092] 在本示例中，在未进行初始化流程的情况下，用户终端中安全元件处于原始状态，无安全元件标识，也未存储第一类通用卡实例和第二类通用卡实例等信息。在进行初始化流程的过程中，通过安全通道传输的初始化信息可包括但不限于安全元件标识、加密公钥、第一类通用卡实例和第二类通用卡实例。加密公钥可在后续的卡绑定流程中，对用户终端与服务器之间传输的数据进行加密。

[0093] 在一些示例中，初始化信息还可包括安全元件中用于存储与卡管理流程相关数据的交易功能区域的区域初始密钥。

[0094] 在一些示例中，程序数据包可在用户终端出厂前预置于用户终端的安全元件中。

[0095] 在另一些示例中，在安全元件未存储有程序数据包的情况下，初始化信息还可包括程序数据包。即在卡管理的初始化过程中，将程序数据包下载至用户终端的安全元件中。在后续过程中，若不需更新，则不需要重复下载程序数据包。

[0096] 在又一些示例中，在安全元件中存储的程序数据包需要更新的情况下，初始化信息还包括更新后的程序数据包。即在卡管理的初始化过程中，可对安全元件中的程序数据包进行更新，如利用更新后的程序数据包替换更新前的程序数据包。

[0097] 需要说明的是，安全元件中存储的程序数据包的更新也可在除初始化过程外的其他过程中进行，在此并不限定。在安全元件中存储的程序数据包需要更新的情况下，用户终

端可向服务器发送更新请求消息。更新请求消息用于请求更新后的程序数据包。该更新请求消息可以是服务器检测到安全元件中存储的程序数据包需要更新，通知用户终端发起更新请求消息，请求更新后的程序数据包。该更新请求消息也可以是用户终端接收用户更新输入操作，向服务器发起更新请求消息，请求更新后的程序数据包。

[0098] 在安全元件中存储的程序数据包的版本低于服务器中存储的程序数据包的最新版本的情况下，可认为安全元件中存储的程序数据包需要更新。或者，在安全元件中存储的程序数据包的版本低于服务器中存储的程序数据包的最新版本，且得到用户终端的用户授权的情况下，可认为安全元件中存储的程序数据包需要更新。

[0099] 在一些示例中，在用户终端非初次进行卡绑定的情况下，服务器可利用与上述初始化过程存储入安全元件中的加密公钥成对的加密私钥对绑定的卡交易标识进行加密。即用户终端接收到的绑定卡的卡交易标识可为利用与加密公钥成对的加密私钥加密的卡交易标识。加密公钥和加密私钥为成对的非对称密钥。在用户终端与服务器之间传输加密的卡交易标识，可在未建立安全通道的基础上保证数据传输的安全性，不需要建立安全通道，从而节省了建立安全通道所需占用的资源及花费的时间。

[0100] 对应地，用户终端接收到加密的卡交易标识，可在安全元件内利用加密公钥对绑定卡的卡交易标识解密，在安全元件中存储解密后的绑定卡的卡交易标识。

[0101] 在绑定卡绑定成功后，可利用绑定卡进行交易支付。交易可分为联网交易和脱机交易两种。联网交易即为交易设备如POS机、刷卡机等具有交易功能的设备处于联网状态下的交易。脱机交易即为交易设备处于脱机状态下的交易。图7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与图4的不同之处在于，图7所示的卡管理方法还可包括步骤S211、步骤S212。

[0102] 在步骤S211中，在利用绑定卡进行联网交易的情况下，利用第一匹配通用卡实例进行交易验证计算，向交易设备提供第一交易验证信息，以通过交易设备使服务器根据第一映射关系，利用与绑定卡的卡交易标识对应的第一匹配通用卡实例进行交易验证计算。

[0103] 在利用绑定卡进行支付交易的情况下，第一交易验证信息包括绑定卡的卡交易标识。

[0104] 用户终端和交易设备在联网状态下进行交易，用户终端和服务器需要进行交易验证。具体地，用户终端利用第一匹配通用卡实例进行交易验证计算。交易设备可将接收到的第一交易验证信息向服务器发送。服务器根据存储的第一映射关系，可确定与绑定卡的卡交易标识对应的第一匹配通用卡标识。服务器基于第一匹配通用卡标识，可确定与绑定卡的卡交易标识对应的第一匹配通用卡实例，并利用该第一匹配通用卡实例进行交易验证计算。第一匹配通用卡实例包括第一匹配通用卡标识，即第一匹配通用卡实例为与绑定卡的卡类型匹配的第一类通用卡实例或第二类通用卡实例。交易验证计算具体可由TSP服务器执行。在用户终端的交易验证计算结果与服务器的交易验证计算结果一致的情况下，确定交易验证成功。例如，用户终端和服务器之间进行的交易验证具体可包括但不限于授权请求报文(Authenticate Request cryptogram,ARQC)验证。

[0105] 用户终端与交易设备在联网支付交易的情况下，用户终端提供的第一交易验证信息包括用于交易的绑定卡的卡交易标识。第一交易验证信息可通过交易设备传输至服务器，服务器能够根据卡交易标识识别出本次支付交易所使用的卡，使得收单方能够区分不

同的卡进行的支付交易。

[0106] 在步骤S212中，在利用绑定卡进行脱机交易的情况下，利用第一匹配通用卡实例进行交易验证计算，向交易设备提供第二交易验证信息，以使交易设备利用第一匹配通用卡实例进行交易验证计算。

[0107] 第二交易验证信息包括第一匹配通用卡实例。在脱机交易情况下，用户终端与交易设备需要进行脱机数据认证(Offline Data Authentication，ODA)。具体地，用户终端可利用第一匹配通用卡实例进行交易验证计算，交易设备可利用第二交易验证信息中的第一匹配通用卡实例进行交易验证计算，在用户终端的交易验证计算结果与服务器的交易验证计算结果一致的情况下，确定脱机数据认证成功。例如，用户终端和交易设备进行的交易验证具体可为交易证书(Transaction Certificate，TC)验证，在此并不限定。

[0108] 需要说明的是，在交易设备再次联网的情况下，交易设备会将本次脱机交易的数据向服务器发送。脱机交易的数据可包括交易时间、第一匹配通用卡标识等，在此并不限定。

[0109] 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，使用该默认卡进行支付交易。默认卡可更改。图8为本申请第一方案提供的卡管理方法的又再一实施例的流程图。图8与图5的不同之处在于，图8所示的卡管理方法还可包括步骤S213至步骤S216。

[0110] 在步骤S213中，接收默认卡设置输入。

[0111] 默认卡设置输入用于选定默认卡。默认卡设置输入可为用户对用户终端的输入，在此并不限定。默认卡为默认进行交易支付的卡。

[0112] 在步骤S214中，在联网的情况下，向服务器发送默认卡设置消息，以使服务器将第二映射关系的使用状态设置为默认使用状态。

[0113] 默认卡设置消息包括默认卡的卡交易标识。第二映射关系包括安全元件标识、第二匹配通用卡标识和默认卡的卡交易标识的映射关系。第二匹配通用卡标识为与默认卡的卡类型匹配的第一类通用卡标识或第二类通用卡标识。在默认卡的卡类型为第一类型的情况下，默认卡的第二匹配通用卡标识为第一类通用卡标识。在默认卡的卡类型为第二类型的情况下，默认卡的第二匹配通用卡标识为第二类通用卡标识。

[0114] 服务器可根据默认卡的卡交易标识，查找到包括默认卡的卡交易标识的第二映射关系。服务器将第二映射关系的使用状态设置为默认使用状态，对应地，在进行支付交易的过程中，服务器会默认利用第二映射关系包括的安全元件标识、第二匹配通用卡标识和默认卡的卡交易标识进行支付交易流程。

[0115] 在步骤S215中，接收服务器发送的默认卡应答消息。

[0116] 在将第二映射关系的使用状态设置为默认使用状态的情况下，服务器向用户终端发送默认卡应答消息，以通知用户终端。默认卡应答消息用于表征第二映射关系的使用状态已设置为默认使用状态。

[0117] 在步骤S216中，响应于默认卡应答消息，通过默认卡设置指令，将安全元件中默认卡的卡交易标识的使用状态设置为默认使用状态，将安全元件中与默认卡的卡交易标识对应的第二匹配通用卡实例的生命状态设置为生效状态。

[0118] 第二匹配通用卡实例为与默认卡的卡类型匹配的第一类通用卡实例或第二类通

用卡实例。在默认卡的卡类型为第一类型的情况下，默认卡的第二匹配通用卡实例为第一类通用卡实例。在默认卡的卡类型为第二类型的情况下，默认卡的第二匹配通用卡实例为第二类通用卡实例。

[0119] 用户终端接收到默认卡应答消息，可确定服务器中第二映射关系的使用状态已设置为默认使用状态，可对应设置安全元件中的默认卡的卡交易标识的使用状态，以及设置第二匹配通用卡实例的生命状态，从而保证用户终端中默认卡的设置与服务器中默认卡的设置的一致。

[0120] 默认卡设置指令为用户终端向安全元件发送的控制指令。在此并不限定默认卡设置指令的具体形式，例如，默认卡设置指令可为应用协议数据单元(Application Protocol Data Unit，APDU)指令，在此并不限定。

[0121] 需要说明的是，安全元件可识别的默认卡设置指令可包括不同版本模式下的指令。安全元件接收到默认卡设置指令，可优先执行新版本模式的指令，若指令无效，再执行旧版本的指令。新、旧版本模式下的指令相互独立，保证新、旧版本模式下的指令的执行具有兼容性。

[0122] 在一些示例中，在进行支付交易所使用的卡即为默认卡。在进行支付交易的过程中需要利用与默认卡的卡类型相同的第一类通用卡实例或第二类通用卡实例进行交易验证。可将与默认卡的卡类型相同的第一类通用卡实例或第二类通用卡实例即第二匹配通用卡实例的生命状态设置为生效状态，在进行支付交易的过程中，会默认利用生命状态设置为生效状态的第二匹配通用卡实例进行交易验证。

[0123] 在使用上述实施例中某张绑定卡进行交易支付的情况下，该绑定卡即为默认卡。在利用某绑定卡进行脱机交易后，在交易设备再次联网的情况下，交易设备会将本次脱机交易的数据向服务器发送。脱机交易的数据可包括交易时间、第一匹配通用卡标识等。在这种情况下，第一匹配通用卡标识与第二匹配通用卡标识相同，即第一匹配通用卡实例与第二匹配通用卡实例相同。

[0124] 服务器可通过交易时间，查询在交易时间使用状态为默认使用状态的映射关系中的卡交易标识，利用卡交易标识进行结算等流程，即本次交易的金额从该卡交易标识对应的卡中转出，从而保证脱机交易的结算的准确性。

[0125] 在再一些实施例中，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。用户终端可接收卡删除消息，响应于卡删除消息，在安全元件中删除卡删除消息指示的待删除卡的卡交易标识，或者，将卡删除消息指示的待删除卡的卡交易标识的生命状态设置为失效状态。

[0126] 卡交易标识的生命状态为失效状态，表示该卡交易标识处于不可用状态，无法被调用。在该卡被删除又再次需要绑定的情况下，可将该卡的卡交易标识的生命状态设置为有效状态，从而快速实现再次绑卡。

[0127] 需要注意的是，在这种情况下，安全元件中删除了待删除卡的卡交易标识，或者并不删除待删除卡的卡交易标识，只将待删除卡的卡交易标识的生命状态设置为失效状态。不会删除第一类通用卡实例和第二类通用卡实例，也不会删除程序数据包。第一类通用卡实例和第二类通用卡实例还可用于其他未删除的卡的交易验证。

[0128] 在一些示例中，卡删除流程可由用户通过用户终端发起。具体地，用户可通过对用

户终端的应用程序的操作，发起卡删除流程。用户终端向服务器发送卡删除申请消息，通知服务器请求删除待删除卡。响应于卡删除申请消息，服务器可生成卡删除消息，向用户终端发送卡删除消息。用户终端响应于卡删除消息，在安全元件中删除待删除卡的卡交易标识，或者，将待删除卡的卡交易标识的生命状态设置为失效状态。卡删除消息可指示待删除卡，例如，卡删除消息包括待删除卡的卡交易标识。用户终端可向服务器发送卡删除请求消息，卡删除请求消息可包括待删除卡的卡交易标识。服务器响应于卡删除请求消息，将包括待删除卡的卡交易标识的映射关系删除。服务器还可向用户终端发送删除卡应答消息，删除卡应答消息用于表征服务器中已删除包括待删除卡的卡交易标识的映射关系。用户终端可发出卡删除成功提示信息，以提示用户待删除卡删除成功。

[0129] 在另一些示例中，卡删除流程可由卡组织通过服务器发起，例如，由银行发起。服务器接收卡组织发出的卡删除请求消息。卡删除请求消息用于指示待删除卡，例如，卡删除请求消息可包括待删除卡的卡交易标识。响应于卡删除请求消息，服务器删除包括待删除卡的卡交易标识的映射关系，并向用户终端发送卡删除消息。卡删除消息用于指示待删除卡，例如，卡删除消息可包括待删除卡的卡交易标识。用户终端响应于卡删除消息，在安全元件中删除待删除卡的卡交易标识，或者，将待删除卡的卡交易标识的生命状态设置为失效状态。用户终端可向服务器发送卡删除应答消息，以通知服务器安全元件中待删除卡删除成功。

[0130] 需要说明的是，在待删除卡为默认卡的情况下，需要指定绑定的另外一张卡为默认卡后，再进行待删除卡的删除。

[0131] 本申请实施例中，在删除卡的情况下，应用终端并不删除第一类通用卡实例和第二类通用卡实例，也不删除程序数据包，避免了个人化数据和程序数据包的频繁删除。尤其是在再次绑定之前删除过的卡的情况下，可避免再次绑定的过程中个人化数据和程序数据包的再次下载，从而进一步降低绑定卡过程、删除卡过程的繁琐程度。

[0132] 本申请第二方面还提供一种卡管理方法，可应用于服务器。图9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9所示，该卡管理方法可包括步骤S301至步骤S303。

[0133] 在步骤S301中，接收用户终端发送的卡绑定消息。

[0134] 卡绑定消息包括安全元件标识和绑定卡认证信息。安全元件标识用于标识用户终端中的安全元件。绑定卡认证信息包括绑定卡的卡认证信息。绑定卡为需要与用户终端中的应用程序绑定的卡。

[0135] 在步骤S302中，响应于卡绑定消息，为绑定卡分配卡交易标识，并建立第一映射关系。

[0136] 服务器为不同的卡分配不同的卡交易标识。具体地，服务器可根据卡绑定消息中的绑定卡认证信息，为绑定卡分配卡交易标识。

[0137] 第一映射关系包括安全元件标识、第一匹配通用卡标识和绑定卡的卡交易标识的映射关系。第一匹配通用卡标识为与绑定卡的卡类型匹配的第一类通用卡标识或第二类通用卡标识。第一匹配通用卡实例用于绑定卡的交易验证。第一匹配通用卡实例包括第一匹配通用卡标识。

[0138] 在步骤S303中，向用户终端发送绑定卡的卡交易标识。

[0139] 上述步骤S301至步骤S303中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。

[0140] 在本申请实施例中，服务器响应于用户终端发送的卡绑定消息，为绑定卡分配卡交易标识，并建立安全元件标识、第一匹配通用卡标识和分配的该卡交易标识的第一映射关系。服务器将为绑定卡分配的卡交易标识向用户终端发送，以使用户终端获取该卡交易标识。第一匹配通用卡实例用于进行绑定卡的交易验证计算。对于用户终端的应用程序绑定的卡类型相同的卡，用户终端与服务器利用相同的匹配通用卡实例进行交易验证，因此服务器不需要为每张卡单独配置用于交易验证的个人化数据，避免了每次卡绑定服务器都需要将该卡对应的个人化数据传输给用户终端的情况，降低了卡管理流程的繁琐程度，简化卡管理流程，还可提高卡绑定的速度，减少卡绑定所花费的时间。

[0141] 在用户终端将绑定卡的卡交易标识存储至安全元件后，完成了卡绑定的申请阶段，还需要将绑定卡激活。图10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与图9的不同之处在于，图10所示的卡管理方法还可包括步骤S304至步骤S307。

[0142] 在步骤S304中，接收用户终端发送的验证码获取请求消息。

[0143] 在步骤S305中，响应验证码获取请求消息，向用户终端反馈第一动态验证码。

[0144] 在步骤S306中，接收用户终端发送的验证码请求消息，验证码请求消息包括第二动态验证码。

[0145] 在步骤S307中，在第二动态验证码验证成功的情况下激活第一映射关系。

[0146] 步骤S304至步骤S307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。

[0147] 在用户终端初次进行卡绑定的情况下，用户终端需要进行卡管理的初始化流程。图11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与图9的不同之处在于，图11所示的卡管理方法还可包括步骤S308至步骤S310。

[0148] 在步骤S308中，接收用户终端发送的初始化请求消息。

[0149] 初始化请求消息用于触发卡管理的初始化流程。

[0150] 在步骤S309中，响应于初始化请求消息，与用户终端建立用户终端中安全元件与服务器之间的安全通道。

[0151] 在步骤S310中，通过安全通道向安全元件下发初始化信息。

[0152] 初始化信息包括安全元件标识、加密公钥、第一类通用卡实例和第二类通用卡实例。

[0153] 服务器还可记录第一类通用个人化数据和第二类通用个人化数据的版本，在第一类通用个人化数据和第二类通用个人化数据出现新版本的情况下，可更新用户终端的安全元件存储的第一类通用个人化数据和第二类通用个人化数据。

[0154] 上述步骤S308至步骤S310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。

[0155] 在一些示例中，初始化信息还可包括安全元件中用于存储与卡管理流程相关数据的区域的区域初始密钥。

[0156] 在一些示例中，程序数据包可在用户终端出厂前预置于用户终端的安全元件中。

[0157] 在另一些示例中，在安全元件未存储有程序数据包的情况下，初始化信息还包括

程序数据包。

[0158] 在又一些示例中，在安全元件中存储的程序数据包需要升级的情况下，初始化信息还包括升级后的程序数据包。

[0159] 在一些示例中，不限于初始化过程，在其他过程中，在安全元件中存储的程序数据包需要更新的情况下，服务器可接收用户终端发送的更新请求消息。服务器响应更新请求消息，向用户终端下发更新后的程序数据包，以实现安全元件中程序数据包的更新。程序数据包更新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。

[0160] 在一些示例中，在服务器非初次接收到卡绑定消息的情况下，服务器可利用与加密公钥成对的加密私钥对绑定卡的卡交易标识加密；向用户终端发送加密后的绑定卡的卡交易标识。

[0161] 在绑定卡绑定成功后，可利用绑定卡进行交易支付。交易可分为联网交易和脱机交易两种。联网交易即为交易设备如POS机、刷卡机等具有交易功能的设备处于联网状态下的交易。脱机交易即为交易设备处于脱机状态下的交易。图12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与图9的不同之处在于，图12所示的卡管理方法还可包括步骤S311、步骤S312。

[0162] 在步骤S311中，在利用绑定卡进行联网交易的情况下，通过交易设备接收用户终端提供的第一交易验证信息，根据第一映射关系，利用与绑定卡的卡交易标识对应的第一匹配通用卡实例进行交易验证计算。

[0163] 第一交易验证信息包括绑定卡的卡交易标识。根据第一映射关系，可确定与绑定卡的卡交易标识对应的第一匹配通用卡实例，进而利用第一匹配通用卡实例进行交易验证计算。第一匹配通用卡实例包括第一匹配通用卡标识，即第一匹配通用卡实例为与绑定卡的卡类型匹配的第一类通用卡实例或第二类通用卡实例。在用户终端的交易验证计算结果与服务器的交易验证计算结果一致的情况下，确定交易验证成功。

[0164] 用户终端与交易设备在联网支付交易的情况下，服务器通过交易设备从用户终端获取的第一交易验证信息包括用于交易的绑定卡的卡交易标识。服务器能够根据该卡交易标识识别出本次支付交易所使用的卡，使得收单方能够区分不同的卡进行的支付交易。

[0165] 在步骤S312中，在用户终端利用绑定卡与交易设备进行脱机交易后，在联网的情况下，获取第一匹配通用卡实例，根据第一匹配通用卡实例进行交易验证计算。

[0166] 具体地，在发生脱机交易后，若交易设备再次联网，服务器可获取到与该绑定卡对应的第一匹配通用卡实例，利用第一匹配通用卡实例进行交易验证计算。

[0167] 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，使用该默认卡进行支付交易。默认卡可更改。图13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S313至步骤S315。

[0168] 在步骤S313中，在联网的情况下，接收用户终端发送的默认卡设置消息。

[0169] 默认卡设置消息包括选定的默认卡的卡交易标识。

[0170] 在步骤S314中，响应于默认卡设置消息，将第二映射关系的使用状态设置为默认使用状态。

[0171] 第二映射关系包括安全元件标识、第二匹配通用卡标识和默认卡的卡交易标识的

映射关系。

[0172] 在步骤S315中,向用户终端发送默认卡应答消息。

[0173] 默认卡应答消息用于表征第二映射关系的使用状态已设置为默认使用状态。

[0174] 在使用上述实施例中某张绑定卡进行交易支付的情况下,该绑定卡即为默认卡。在利用某绑定卡进行脱机交易后,在交易设备在此联网的情况下,服务器会接收到交易设备发送的脱机交易的相关信息,该相关信息可包括交易时间。服务器可根据交易时间,确定在交易时间使用状态为默认使用状态的第二映射关系。利用该第二映射关系中默认卡的卡交易标识进行结算,即从该默认卡的账户中将交易金额转出,能够避免利用错误的账户进行结算,提高了脱机交易的准确性。

[0175] 在交易支付过程的结算流程中,可利用第二映射关系中默认卡的卡交易标识进行结算。服务器与用户终端的默认卡的设置只能在联网状态下进行,从而使得能够通过交易时间,来确定交易时间对应的默认卡。

[0176] 步骤S313至步骤S315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。

[0177] 在再一些实施例中,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。服务器可接收卡删除请求消息,响应于卡删除请求消息,删除第三映射关系,或者,将第三映射关系的生命状态设置为失效状态。

[0178] 卡删除请求消息用于指示待删除卡。第三映射关系包括安全元件标识、第三匹配通用卡标识与待删除卡的卡交易标识的对应关系。第三匹配通用卡标识为与待删除卡的卡类型匹配的第一类通用卡标识或第二类通用卡标识。在绑定卡的卡类型为第一类型的情况下,待删除卡的第三匹配通用卡标识为第一类通用卡标识。在待删除卡的卡类型为第二类型的情况下,绑定卡的第三匹配通用卡标识为第二类通用卡标识。

[0179] 第三映射关系的生命状态为失效状态,表示第三映射关系处于不可用状态,无法被调用。在该卡被删除又再次需要绑定的情况下,可将第三映射关系的生命状态设置为有效状态,从而快速实现再次绑卡。

[0180] 卡删除流程可由用户通过用户终端的应用程序发起,也可由卡组织发起,在此并不限定,具体内容可参见上述实施例中的相关说明,在此不再赘述。

[0181] 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以及功能控件,服务器包括应用程序的后台服务器、TSM服务器和TSP服务器,以及卡类型包括借记卡和贷记卡为例进行说明。应用程序具体可为电子钱包应用程序。功能控件为TSM服务器对应的控件。

[0182] 图14为本申请实施例提供的初始化流程的一示例的流程图。图14省略了一些交互的流程文字说明,但在图14中以箭头示出这些交互。如图14所示,初始化流程可包括步骤S401至步骤S420。

[0183] 在步骤S401中,应用程序向功能控件发起初始化请求。

[0184] 在步骤S402中,功能控件将初始化请求向TSM服务器发送。

[0185] 在步骤S403中,TSM服务器验证应用程序的合法性。

[0186] TSM服务器向功能控件返回应答消息,以通知功能控件建立安全通道。

[0187] 在步骤S404中,在合法性验证结果表征应用程序的合法性验证成功的情况下,建

立功能控件与安全元件之间的安全通道，相当于建立TSM服务器与安全元件之间的安全通道。

[0188] 安全元件向功能控件返回应答消息，以通知功能控件安全通道建立成功。功能控件向TSM服务器发送验证请求，以使TSM服务器验证安全元件中交易功能区域的合法性。

[0189] 在步骤S405中，TSM服务器验证安全元件中交易功能区域的合法性。

[0190] 在步骤S406中，在合法性验证结果表征交易功能区域的合法性验证成功的情况下，将交易功能区域的区域初始密钥和为安全元件分配的安全元件标识向功能控件发送。

[0191] 在步骤S407中，功能控件将区域初始密钥和安全元件标识写入安全元件。

[0192] 安全元件向功能控件返回应答消息，功能控件向TSM返回该应答消息，以通知TSM服务器区域初始密钥和安全元件标识写入成功。

[0193] TSM服务器向功能控件发送第一触发消息，功能控件向应用程序发送第一触发消息，以通知应用程序可进行程序数据包的下载。

[0194] 应用程序向功能控件发送下载触发消息，功能控件向TSM服务器发送下载触发消息。该下载触发下次用于触发下载程序数据包和通用卡标识。通用卡标识可包括通用借记卡标识和通用贷记卡标识。可选的，该下载触发还可触发下载通用个人化数据。通用个人化数据可包括借记卡通用个人化数据和贷记卡通用个人化数据。

[0195] 在步骤S408中，TSM服务器将程序数据包向功能控件发送。

[0196] 在步骤S409中，功能控件将程序数据包写入安全元件。

[0197] 安全元件向功能控件返回应答消息，功能控件向TSM服务器返回应答消息，以通知TSM服务器程序数据包写入成功。

[0198] TSM服务器向功能控件发送第二触发消息，以触发功能控件触发下载通用卡标识，或者触发下载通用卡标识和通用个人化数据。本示例中以触发下载通用卡标识、通用个人化数据和加密公钥为例。功能控件向TSM服务器发送下载请求，以请求下载通用卡标识、通用个人化数据和加密公钥。

[0199] 在步骤S410中，TSM服务器向功能控件发送通用卡标识、通用个人化数据和加密公钥。

[0200] 在步骤S411中，功能控件向安全元件发送通用卡标识、通用个人化数据和加密公钥。

[0201] 安全元件向功能控件返回应答消息，功能控件向TSM服务器返回应答消息，以通知TSM服务器通用卡标识、通用个人化数据和加密公钥写入成功。

[0202] 在步骤S412中，TSM服务器建立安全元件标识、通用卡标识、通用个人化数据的映射关系。

[0203] TSM服务器与TSP服务器进行交互，以使TSP服务器建立安全元件标识、通用卡标识、通用个人化数据的映射关系。

[0204] 在步骤S413中，TSP服务器建立安全元件标识、通用卡标识、通用个人化数据的映射关系。

[0205] TSP服务器向TSM服务器返回应答消息，TSM服务器向功能控件返回应答消息，功能控件向应用程序返回应答消息，以通知用户终端映射关系建立完毕。

[0206] 在步骤S414中，应用程序获取银行卡的卡号。

[0207] 在步骤S415中，应用程序将卡号向功能控件发送。

[0208] 功能控件对卡号进行加密，将加密的卡号返回应用程序。应用程序将加密的卡号向后台服务器发送。后台服务器将加密的卡号向TSM服务器发送。TSM服务器根据卡号，确定卡的类型和发卡行，将卡类型和发卡行反馈给后台服务器。后台服务器将卡的类型和发卡行向应用程序发送。

[0209] 在步骤S416中，应用程序根据卡类型，获取卡认证信息，如贷记卡的有效期、信用卡鉴别密码(即CVN2)、所属人手机号，或者，如借记卡的卡密码、所属人手机号等。

[0210] 应用程序将卡认证信息传输至功能控件。功能控件对卡认证信息加密，将加密的卡认证信息返回应用程序。应用程序将加密的卡认证信息向后台服务器发送。

[0211] 在步骤S417中，后台服务器向TSM服务器发送卡认证信息。

[0212] 在步骤S418中，TSM服务器向卡组织发送卡认证信息，以使卡组织对该卡进行认证。

[0213] 在步骤S419中，TSM服务器接收卡组织发送的认证结果。

[0214] 在步骤S420中，在认证结果表征认证成功的情况下，TSM服务器向后台服务器发送通知信息，以通知后台服务器可开始卡绑定流程。

[0215] 图15为本申请实施例提供的卡绑定流程的一示例的流程图。图15省略了一些交互的流程文字说明，但在图15中以箭头示出这些交互。如图15所示，卡绑定流程可包括步骤S501至步骤S518。

[0216] 在步骤S501中，后台服务器向应用程序发送卡绑定消息。

[0217] 在步骤S502中，应用程序向功能控件发送卡绑定消息。

[0218] 在步骤S503中，功能控件向TSM服务器发送卡绑定消息。

[0219] 在步骤S504中，TSM服务器响应于卡绑定消息，向功能控件发送利用加密私钥加密的卡交易标识。

[0220] 在步骤S505中，功能控件向安全元件发送加密的卡交易标识。

[0221] 在步骤S506中，利用加密公钥对加密的卡交易标识解密，并存储。

[0222] 安全元件向功能控件发送应答消息，功能控件向TSM服务器发送应答消息，以通知TSM服务器已将卡交易标识写入安全元件。

[0223] 在步骤S507中，TSM服务器建立安全元件标识、第一匹配通用卡标识和卡交易标识的映射关系。

[0224] TSM服务器与TSP服务器交互，以使TSP服务器建立安全元件标识、第一匹配通用卡标识和卡交易标识的映射关系。

[0225] 在步骤S508中，TSP服务器建立安全元件标识、第一匹配通用卡标识和卡交易标识的映射关系。

[0226] TSP服务器向TSM服务器发送应答消息，TSM服务器向功能控件发送应答消息，功能控件向应用程序发送应答消息，以通知应用程序映射关系建立完毕。

[0227] 在步骤S509中，应用程序向后台服务器发送验证码获取请求消息。

[0228] 在步骤S510中，后台服务器向TSM服务器发送验证码获取请求消息。

[0229] 在步骤S511中，TSM服务器向卡组织发送验证码获取请求消息。

[0230] 在步骤S512中，卡组织向TSM服务器发送第一动态验证码。

[0231] 在步骤S513中,TSM服务器向后台服务器发送第一动态验证码。

[0232] 在步骤S514中,后台服务器向应用程序发送第一动态验证码。

[0233] 在步骤S515中,应用程序向后台服务器发送第二动态验证码。

[0234] 在步骤S516中,后台服务器向TSM服务器发送第二动态验证码。

[0235] 在步骤S517中,TSM服务器向卡组织发送第二动态验证码,以使卡组织进行动态验证码验证。

[0236] 卡组织向TSM服务器发送验证应答消息。

[0237] 在步骤S518中,在验证应答消息表征验证成功的情况下,TSM服务器根据验证结果激活映射关系。

[0238] TSM服务器向后台服务器发送验证应答消息,后台服务器向应用程序发送验证应答消息。

[0239] 图16为本申请实施例提供的卡删除流程的一示例的流程图。图16省略了一些交互的流程文字说明,但在图16中以箭头示出这些交互。如图16所示,卡删除流程可包括步骤S601至步骤S608。

[0240] 在步骤S601中,应用程序响应于用户输入,向后台服务器发送卡删除申请消息。

[0241] 在步骤S602中,后台服务器向TSM服务器发送卡删除申请消息。

[0242] 在步骤S603中,TSM服务器向后台服务器发送卡删除消息。

[0243] 在步骤S604中,后台服务器向功能控件发送卡删除消息。

[0244] 在步骤S605中,功能控件向安全元件发送卡删除消息。

[0245] 在步骤S606中,安全元件删除卡的卡交易标识。

[0246] 安全元件向功能控件发送应答消息,功能控件向TSM服务器发送应答消息,以通知TSM服务器安全元件已删除卡的卡交易标识。

[0247] 在步骤S607中,TSM服务器删除包括该卡的卡交易标识的映射关系。

[0248] TSM服务器与TSP服务器交互,以使TSP服务器删除包括该卡的卡交易标识的映射关系。

[0249] 在步骤S608中,TSP服务器删除包括该卡的卡交易标识的映射关系。

[0250] TSP服务器向TSM服务器发送应答消息,以通知TSM服务器TSP服务器已删除该映射关系。TSM服务器与卡组织交互,以使卡组织删除包括该卡的卡交易标识的映射关系。卡组织删除包括该卡的卡交易标识的映射关系后向TSM服务器发送应答消息,TSM服务器向后台服务器发送应答消息,后台服务器向应用程序发送应答消息,以通知用户删卡成功。

[0251] 图17为本申请实施例提供的卡删除流程的另一示例的流程图。图17省略了一些交互的流程文字说明,但在图17中以箭头示出这些交互。如图17所示,卡删除流程可包括步骤S701至步骤S705。

[0252] 在步骤S701中,TSM服务器响应于卡组织的卡删除请求消息,删除包括卡删除请求消息指示删除的卡的卡交易标识的映射关系。

[0253] TSM服务器与TSP服务器交互,以使TSP服务器删除包括该卡的卡交易标识的映射关系。

[0254] 在步骤S702中,TSP服务器删除包括该卡的卡交易标识的映射关系。

[0255] TSP服务器向TSM服务器发送应答消息,以通知TSM服务器TSP服务器已删除包括该

卡的卡交易标识的映射关系。TSM服务器向卡组织发送应答消息，以通知卡组织TSM服务器和TSP服务器均已删除包括该卡的卡交易标识的映射关系。

[0256] 在步骤S703中，TSM服务器向功能控件发送卡删除消息。

[0257] 在步骤S704中，功能控件向安全元件发送卡删除消息。

[0258] 在步骤S705中，响应于卡删除消息，安全元件删除该卡的卡交易标识。

[0259] 安全元件向功能控件发送应答消息，功能控件向TSM服务器发送应答消息，以通知TSM服务器安全元件已删除该卡的卡交易标识。

[0260] 本申请第三方面提供一种用户终端。该用户终端具有安全元件。安全元件存储有第一类通用卡实例和第二类通用卡实例。第一类通用卡实例包括第一类通用卡标识和第一类通用个人化数据。第二类通用卡实例包括第二类通用卡标识和第二类通用个人化数据。第一类通用卡实例用于用户终端进行卡类型为第一类型的卡的交易验证。第二类通用卡实例用于用户终端进行卡类型为第二类型的卡的交易验证。

[0261] 图18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18所示，该用户终端800可包括发送模块801、接收模块802和处理模块803。

[0262] 发送模块801可用于向服务器发送卡绑定消息，以使服务器为绑定卡分配卡交易标识，并建立第一映射关系。

[0263] 卡绑定消息包括安全元件标识和绑定卡认证信息。绑定卡认证信息包括绑定卡的卡认证信息。第一映射关系包括安全元件标识、第一匹配通用卡标识和绑定卡的卡交易标识的映射关系。第一匹配通用卡标识为与绑定卡的卡类型匹配的第一类通用卡标识或第二类通用卡标识。

[0264] 接收模块802可用于接收服务器发送的绑定卡的卡交易标识。

[0265] 处理模块803可用于将绑定卡的卡交易标识存储至安全元件。

[0266] 第一匹配通用卡实例用于绑定卡的交易验证。第一匹配通用卡实例包括第一匹配通用卡标识。

[0267] 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卡实例和第二类通用卡实例。用户终端通过向服务器发送卡绑定消息，使服务器为绑定卡分配卡交易标识，并建立安全元件标识、第一匹配通用卡标识和分配的卡交易标识的映射关系。用户终端自身可利用绑定卡对应的第一匹配通用卡实例进行交易验证，服务器利用确定的第一匹配通用卡实例进行交易验证。第一匹配通用卡实例为与绑定卡的卡类型匹配的第一类通用卡实例或第二类通用卡实例。即利用第一类通用卡实例或第二类通用卡实例即可完成交易验证。在绑定卡的过程中，服务器并不需要为每张卡分配对应的个人化数据，因此不需要在每次绑卡的过程中下载个人化数据，从而避免频繁地进行个人化数据的下载和存储，降低了卡管理流程的繁琐程度，简化卡管理流程，还可提高卡绑定的速度，减少卡绑定所花费的时间。

[0268] 在一些示例中，在用户终端初次进行卡绑定的情况下，上述发送模块801还可用于向服务器发送初始化请求消息。

[0269] 上述接收模块802还可用于与服务器建立安全元件与服务器之间的安全通道；以及用于通过安全通道接收服务器下发的初始化信息。初始化信息包括安全元件标识、加密公钥、第一类通用卡实例和第二类通用卡实例。

[0270] 处理模块803还可用于将初始化信息存储至安全元件。

[0271] 在一些示例中，在用户终端非初次进行卡绑定的情况下，接收的绑定卡的卡交易标识为利用与加密公钥成对的加密私钥加密的卡交易标识。

[0272] 处理模块803可用于利用加密公钥对绑定卡的卡交易标识解密，将解密后的绑定卡的卡交易标识存储至安全元件内。

[0273] 在一些示例中，在安全元件未存储有程序数据包的情况下，初始化信息还包括程序数据包。

[0274] 在另一些示例中，在安全元件中存储的程序数据包需要更新的情况下，初始化信息还包括更新后的程序数据包。

[0275] 在一些示例中，不限于初始化过程，在安全元件中存储的程序数据包需要更新的情况下，上述发送模块801还可用于向服务器发送更新请求消息。更新请求消息用于请求更新后的程序数据包。

[0276] 在一些示例中，发送模块801还可用于向服务器发送验证码获取请求消息。

[0277] 接收模块802还可用于接收服务器响应于验证码获取请求消息反馈的第一动态验证码。

[0278] 接收模块802还可用于接收输入的第二动态验证码。

[0279] 发送模块801还可用于向服务器发送验证码请求消息，以使服务器在第二动态验证码验证成功的情况下激活第一映射关系。

[0280] 验证码请求消息包括第二动态验证码。

[0281] 图19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19与图18的不同之处在于，图19所示的用户终端800还可包括验证模块804和输出模块805。

[0282] 验证模块804可用于在利用绑定卡进行联网交易的情况下，利用第一匹配通用卡实例进行交易验证计算。

[0283] 输出模块805可用于在利用绑定卡进行联网交易的情况下，向交易设备提供第一交易验证信息，以通过交易设备使服务器根据第一映射关系，利用与绑定卡的卡交易标识对应的第一匹配通用卡实例进行交易验证计算。

[0284] 第一交易验证信息包括绑定卡的卡交易标识。第一匹配通用卡实例包括第一匹配通用卡标识。

[0285] 在用户终端进行支付交易的情况下，用户终端向交易设备提供第一交易验证信息，以使服务器从交易设备获取进行交易的绑定卡的卡交易标识，通过卡交易标识确定第一匹配通用卡实例。

[0286] 用户终端与交易设备在联网支付交易的情况下，用户终端提供的第一交易验证信息包括用于交易的绑定卡的卡交易标识。第一交易验证信息可通过交易设备传输至服务器，服务器能够根据卡交易标识识别出本次支付交易所使用的卡，使得收单方能够区分不同的卡进行的支付交易。

[0287] 在另一些示例中，验证模块804还可用于在利用绑定卡进行脱机交易的情况下，利用第一匹配通用卡实例进行交易验证计算。

[0288] 输出模块805还可用于向交易设备提供第二交易验证信息，以使交易设备利用第一匹配通用卡实例进行交易验证计算。

[0289] 第二交易验证信息包括第一匹配通用卡实例。

[0290] 在一些示例中，接收模块802还可用于接收默认卡设置输入。

[0291] 默认卡设置输入用于选定默认卡。

[0292] 发送模块801还可用于在联网的情况下，向服务器发送默认卡设置消息，以使服务器将第二映射关系的使用状态设置为默认使用状态。

[0293] 默认卡设置消息包括默认卡的卡交易标识。第二映射关系包括安全元件标识、第二匹配通用卡标识和默认卡的卡交易标识的映射关系。第二匹配通用卡标识为与默认卡的卡类型匹配的第一类通用卡标识或第二类通用卡标识。

[0294] 接收模块802还可用于接收服务器发送的默认卡应答消息。

[0295] 默认卡应答消息用于表征第二映射关系的使用状态已设置为默认使用状态。

[0296] 处理模块803还可用于响应于默认卡应答消息，通过默认卡设置指令，将安全元件中默认卡的卡交易标识的使用状态设置为默认使用状态，将安全元件中与默认卡的卡交易标识对应的第二匹配通用卡实例的生命状态设置为生效状态。

[0297] 第二匹配通用卡实例为与默认卡的卡类型匹配的第一类通用卡实例或第二类通用卡实例。

[0298] 需要说明的是，在利用某张绑定卡进行交易支付的情况下，该绑定卡即为默认卡。

[0299] 在一些示例中，处理模块803还可用于响应于接收的卡删除消息，在安全元件中删除待删除卡的卡交易标识，或将待删除卡的卡交易标识的生命状态设置为失效状态。

[0300] 卡删除消息用于指示待删除卡。

[0301] 本申请第四方面提供一种服务器。该服务器存储有用户终端的第一类通用卡实例和第二类通用卡实例。第一类通用卡实例包括第一类通用卡标识和第一类通用个人化数据。第二类通用卡实例包括第二类通用卡标识和第二类通用个人化数据。第一类通用卡实例用于用户终端进行卡类型为第一类型的卡的交易验证。第二类通用卡实例用于用户终端进行卡类型为第二类型的卡的交易验证。

[0302] 图20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20所示，该服务器900可包括接收模块901、处理模块902和发送模块903。

[0303] 接收模块901可用于接收用户终端发送的卡绑定消息。

[0304] 卡绑定消息包括安全元件标识和绑定卡认证信息。绑定卡认证信息包括绑定卡的卡认证信息。

[0305] 处理模块902可用于响应于卡绑定消息，为绑定卡分配卡交易标识，并建立第一映射关系。

[0306] 第一映射关系包括安全元件标识、第一匹配通用卡标识和绑定卡的卡交易标识的映射关系。第一匹配通用卡标识为与绑定卡的卡类型匹配的第一类通用卡标识或第二类通用卡标识。

[0307] 发送模块903可用于向用户终端发送绑定卡的卡交易标识。

[0308] 第一匹配通用卡实例用于绑定卡的交易验证。第一匹配通用卡实例包括第一匹配通用卡标识。

[0309] 在本申请实施例中，服务器响应于用户终端发送的卡绑定消息，为绑定卡分配卡交易标识，并建立安全元件标识、第一匹配通用卡标识和分配的该卡交易标识的第一映射

关系。服务器将为绑定卡分配的卡交易标识向用户终端发送，以使用户终端获取该卡交易标识。服务器利用第一匹配通用卡实例进行交易验证计算，第一匹配通用卡实例包括第一匹配通用卡标识。对于用户终端的应用程序绑定的卡类型相同的卡，用户终端与服务器利用相同的匹配通用卡实例进行交易验证，因此服务器不需要为每张卡单独配置用于交易验证的个人化数据，避免了每次卡绑定服务器都需要将该卡对应的个人化数据传输给用户终端的情况，降低了卡管理流程的繁琐程度，简化卡管理流程，还可提高卡绑定的速度，减少卡绑定所花费的时间。

[0310] 在一些示例中，接收模块901还可用于接收用户终端发送的初始化请求消息。

[0311] 发送模块903还可用于响应于初始化请求消息，与用户终端建立用户终端中安全元件与服务器之间的安全通道。

[0312] 发送模块903还可用于通过安全通道向安全元件下发初始化信息。

[0313] 初始化信息包括安全元件标识、加密公钥、第一类通用卡实例和第二类通用卡实例。

[0314] 在一些示例中，在服务器非初次接收到卡绑定消息的情况下，处理模块902还可用于利用与加密公钥成对的加密私钥对绑定卡的卡交易标识加密。

[0315] 发送模块903还可用于向用户终端发送加密后的绑定卡的卡交易标识。

[0316] 在一些示例中，在安全元件未存储有程序数据包的情况下，初始化信息还包括程序数据包；

[0317] 在另一些示例中，在安全元件中存储的程序数据包需要升级的情况下，初始化信息还包括升级后的程序数据包。

[0318] 在一些示例中，不限于初始化过程，在安全元件中存储的程序数据包需要更新的情况下，上述接收模块还可用于接收用户终端发送的更新请求消息。

[0319] 上述发送模块903还可用于响应更新请求消息，向用户终端下发更新后的程序数据包。

[0320] 在一些示例中，接收模块901还可用于接收用户终端发送的验证码获取请求消息。

[0321] 发送模块903还可用于响应验证码获取请求消息，向用户终端反馈第一动态验证码。

[0322] 接收模块901还可用于接收用户终端发送的验证码请求消息。

[0323] 验证码请求消息包括第二动态验证码。

[0324] 处理模块902还可用于在第二动态验证码验证成功的情况下激活第一映射关系。

[0325] 图21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21与图20的不同之处在于，图21所示的服务器900还可包括验证模块904。

[0326] 上述接收模块901还可用于在利用绑定卡进行联网交易的情况下，通过交易设备接收用户终端提供的第一交易验证信息。

[0327] 第一交易验证信息包括绑定卡的卡交易标识。

[0328] 验证模块904可用于根据第一映射关系，利用与绑定卡的卡交易标识对应的第一匹配通用卡实例进行交易验证计算。

[0329] 在联网交易的情况下，服务器可通过交易设备接收到用户终端设备提供的第一交易验证信息。第一验证信息包括绑定卡的卡交易标识。服务器可根据该卡交易标识，确定第

一映射关系中的第一匹配通用卡实例，从而利用第一匹配通用卡实例进行交易验证计算。

[0330] 而且，用户终端与交易设备在联网支付交易的情况下，服务器通过交易设备从用户终端获取的第一交易验证信息包括用于交易的绑定卡的卡交易标识。服务器能够根据该卡交易标识识别出本次支付交易所使用的卡，使得收单方能够区分不同的卡进行的支付交易。

[0331] 在另一些示例中，处理模块902还可用于在用户终端利用绑定卡与交易设备进行脱机交易后，在联网的情况下，获取第一匹配通用卡实例，利用第一匹配通用卡示例进行交易验证计算。

[0332] 在一些示例中，接收模块901还可用于在联网的情况下，接收用户终端发送的默认卡设置消息。

[0333] 默认卡设置消息包括选定的默认卡的卡交易标识；

[0334] 处理模块902还可用于响应于默认卡设置消息，将第二映射关系的使用状态设置为默认使用状态。

[0335] 第二映射关系包括安全元件标识、第二匹配通用卡标识和默认卡的卡交易标识的映射关系；

[0336] 发送模块903还可用于向用户终端发送默认卡应答消息，默认卡应答消息用于表征第二映射关系的使用状态已设置为默认使用状态。

[0337] 在一些示例中，验证模块904还可用于在用户终端与交易设备进行脱机交易后，在联网的情况下，根据第二匹配通用卡实例进行交易验证计算。

[0338] 第二匹配通用卡实例为与默认卡的卡类型匹配的第一类通用卡实例或第二类通用卡实例。

[0339] 在一些示例中，在利用某张绑定卡进行交易支付的情况下，该绑定卡即为默认卡。处理模块902还可用于在用户终端与交易设备进行脱机交易后，在联网的情况下，确定使用状态为默认使用状态的第二映射关系；以及，用于利用第二映射关系中默认卡的卡交易标识进行结算。

[0340] 在一些示例中，接收模块901还可用于接收卡删除请求消息。

[0341] 卡删除请求消息用于指示待删除卡。

[0342] 处理模块902还可用于响应于卡删除请求消息，删除第三映射关系，或者，将第三映射关系的生命状态设置为失效状态。

[0343] 第三映射关系包括安全元件标识、第三匹配通用卡标识与待删除卡的卡交易标识的对应关系。第三匹配通用卡标识为与待删除卡的卡类型匹配的第一类通用卡标识或第二类通用卡标识。

[0344] 本申请第五方面提供了一种用户终端。图22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22所示，用户终端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。

[0345] 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。

[0346] 存储器可包括只读存储器(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。

[0347] 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一方面的卡管理方法。

[0348] 在一个示例中,用户终端1000还可包括通信接口1003和总线1004。其中,如图22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。

[0349] 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。

[0350] 总线1004包括硬件、软件或两者,将用户终端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。

[0351] 本申请第六方面提供了一种服务器。图23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23所示,服务器1100包括存储器1101、处理器1102及存储在存储器1101上并可在处理器1102上运行的计算机程序。

[0352] 在一个示例中,上述处理器1102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。

[0353] 存储器可包括只读存储器(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。

[0354] 处理器1102通过读取存储器1101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。

[0355] 在一个示例中,服务器1100还可包括通信接口1103和总线1104。其中,如图23所示,存储器1101、处理器1102、通信接口1103通过总线1104连接并完成相互间的通信。

[0356] 通信接口1103,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1103接入输入设备和/或输出设备。

[0357] 总线1104包括硬件、软件或两者，将服务器1100的部件彼此耦接在一起。举例来说而非限制，总线1104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1104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。

[0358] 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。

[0359] 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。

[0360] 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。对于交换设备实施例、服务器实施例、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。

[0361] 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。

[0362] 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。

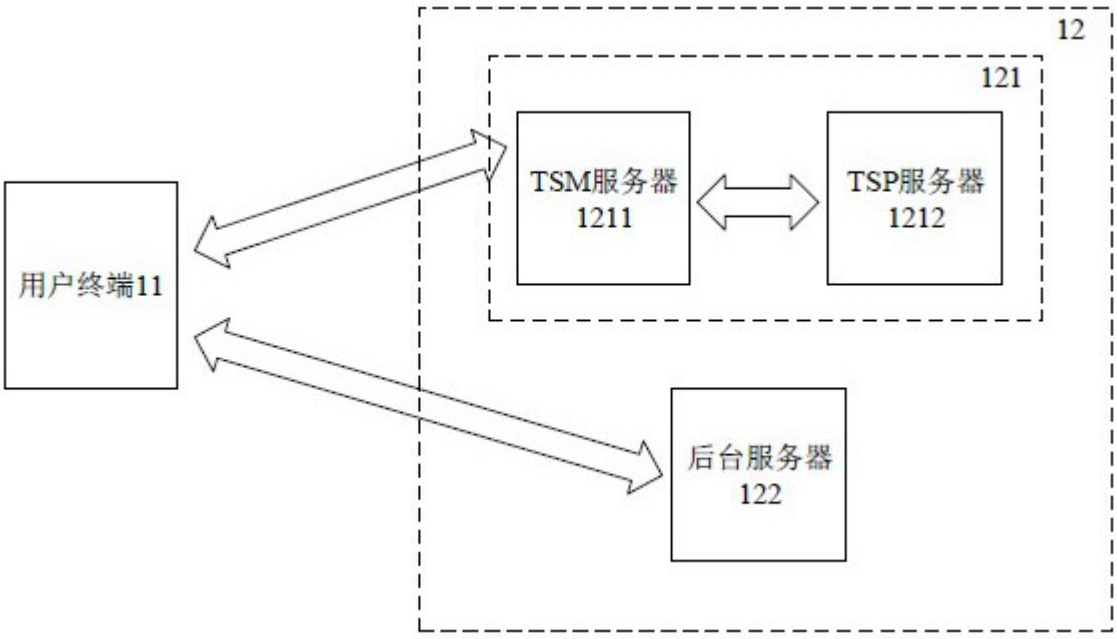
12
121
TSM服务器
1211
TSP服务器
1212
用户终端11
后台服务器
122

图1

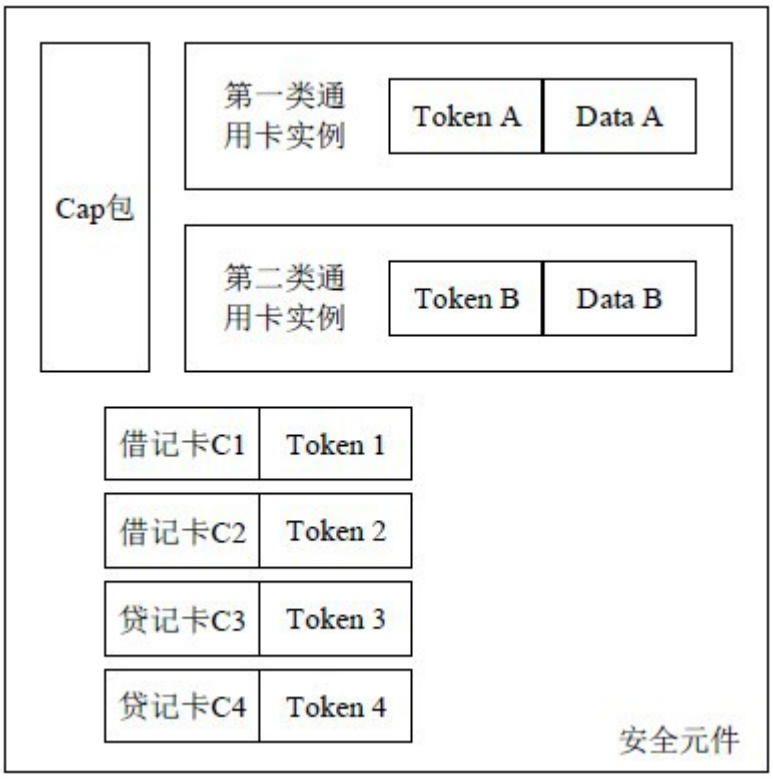
Cap包
第一类通
用卡实例
Token A
Data A
第二类通
用卡实例
Token B
Data B
借记卡C1
Token 1
借记卡C2
Token 2
贷记卡C3
Token 3
贷记卡C4
Token 4
安全元件

图2

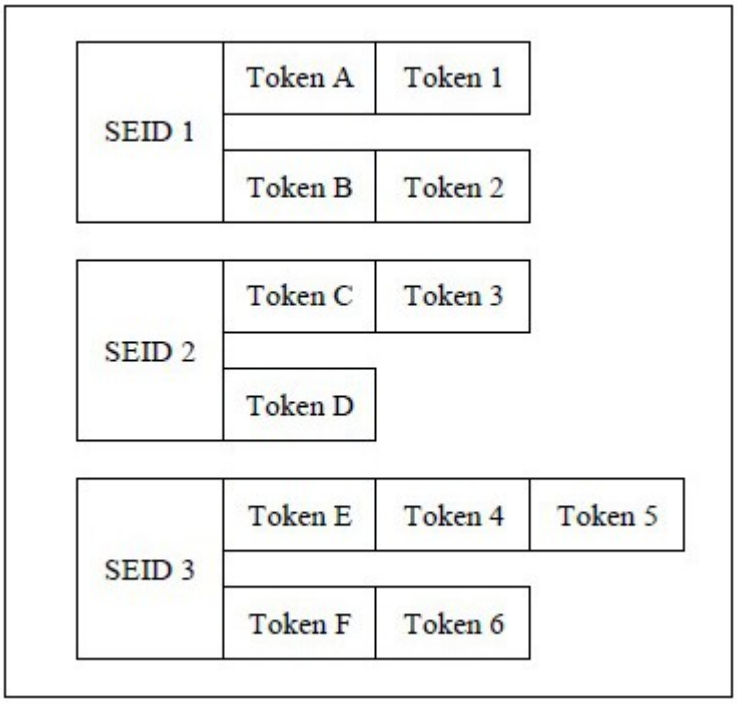
SEID 1
Token A
Token 1
Token B
Token 2
SEID 2
Token C
Token 3
Token D
SEID 3
Token E
Token 4
Token 5
Token F
Token 6

图3

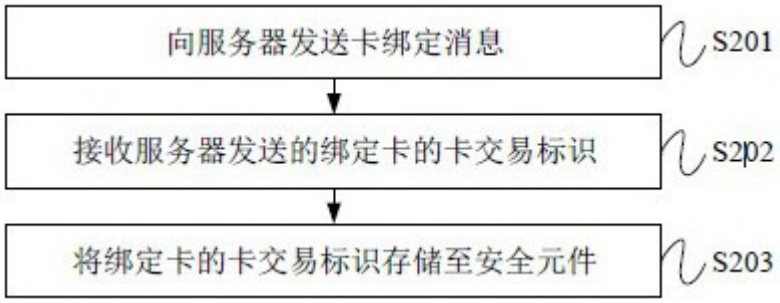
向服务器发送卡绑定消息
S201
接收服务器发送的绑定卡的卡交易标识
S202
将绑定卡的卡交易标识存储至安全元件
S203

图4

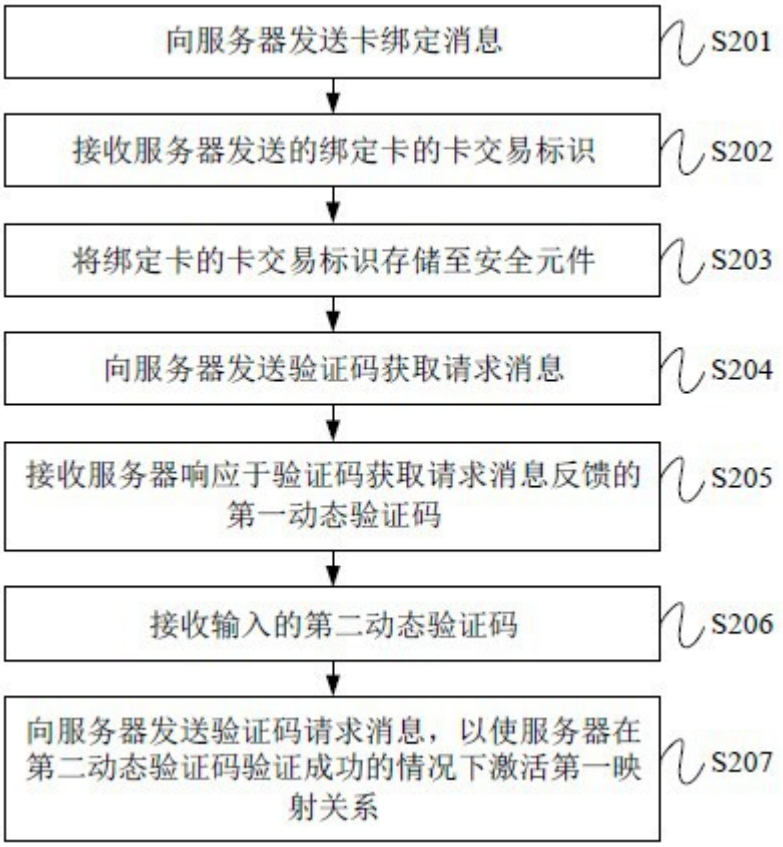
向服务器发送卡绑定消息
S201
接收服务器发送的绑定卡的卡交易标识
S202
将绑定卡的卡交易标识存储至安全元件
S203
向服务器发送验证码获取请求消息
S204
接收服务器响应于验证码获取请求消息反馈的第一动态验证码
S205
接收输入的第二动态验证码
S206
向服务器发送验证码请求消息，以使服务器在第二动态验证码验证成功的情况下激活第一映射关系
S207

图5


向服务器发送初始化请求消息
S208
与服务器建立安全元件与服务器之间的安全通道
S209
通过安全通道接收服务器下发的初始化信息，并将初始化信息存储至安全元件
S210
向服务器发送卡绑定消息
S201
接收服务器发送的绑定卡的卡交易标识
S202
将绑定卡的卡交易标识存储至安全元件
S203

图6

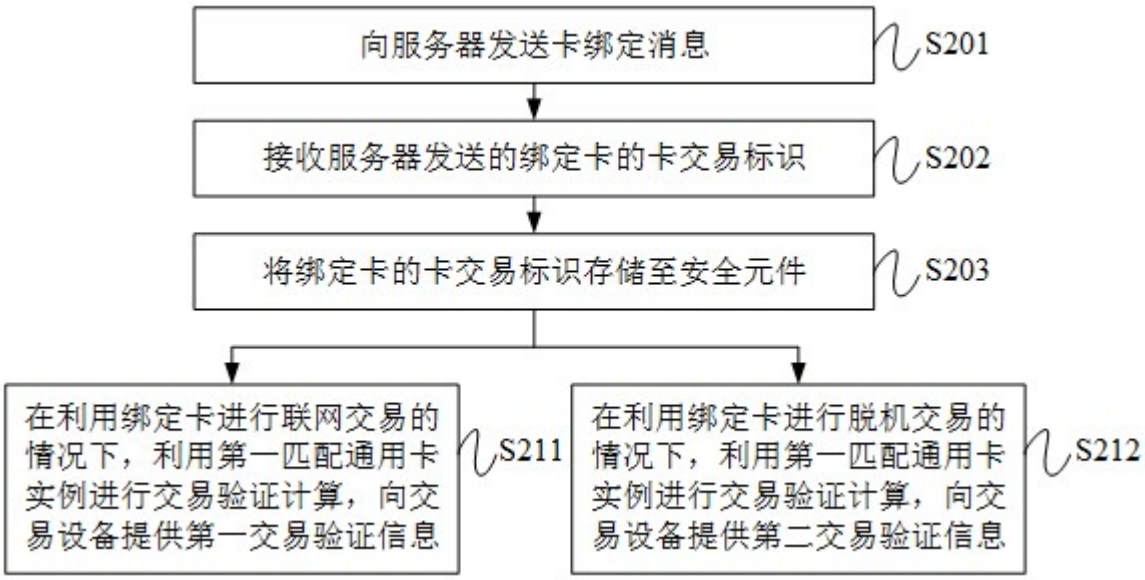
向服务器发送卡绑定消息
S201
接收服务器发送的绑定卡的卡交易标识
S202
将绑定卡的卡交易标识存储至安全元件
S203
在利用绑定卡进行联网交易的情况下，利用第一匹配通用卡实例进行交易验证计算，向交易设备提供第一交易验证信息
S211
在利用绑定卡进行脱机交易的情况下，利用第一匹配通用卡实例进行交易验证计算，向交易设备提供第二交易验证信息
S212

图7

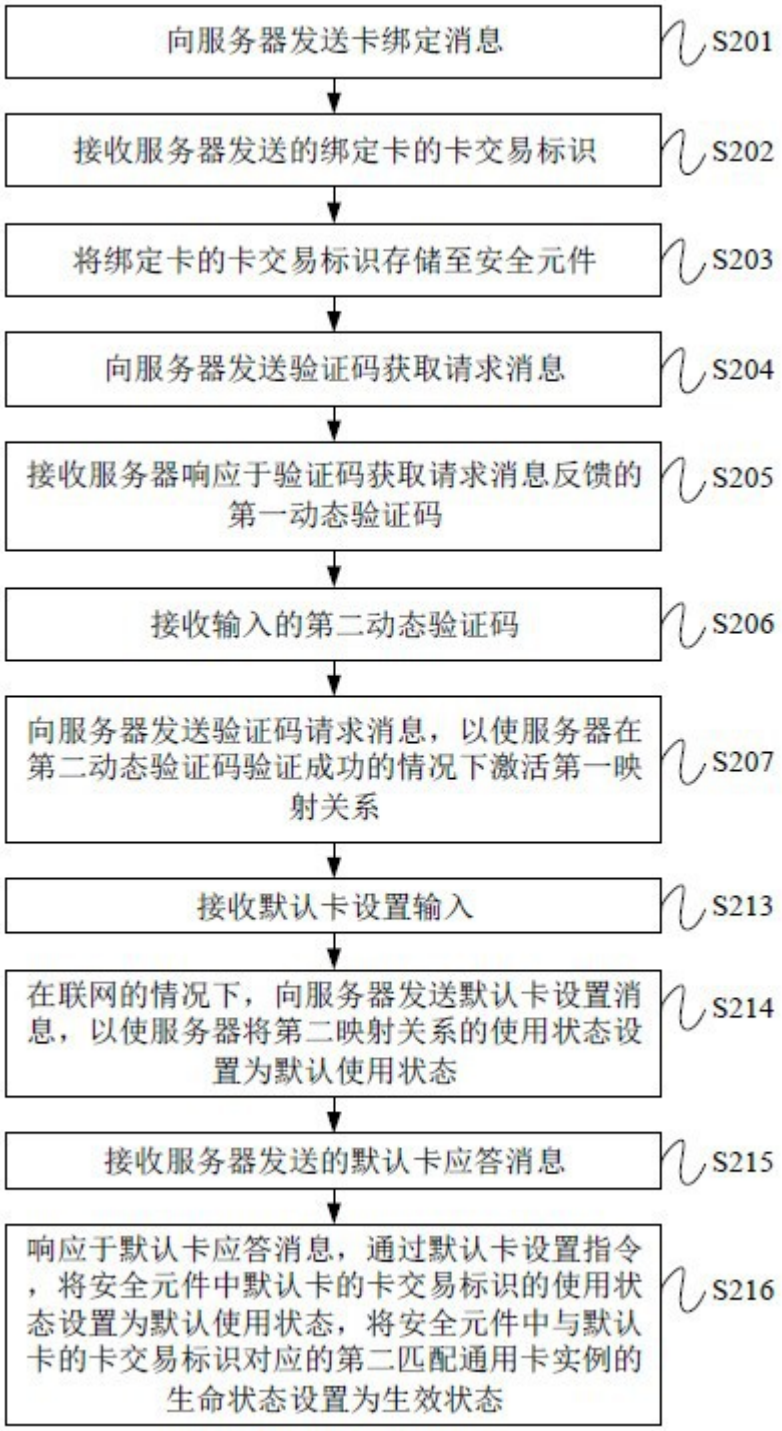
向服务器发送卡绑定消息
S201
接收服务器发送的绑定卡的卡交易标识
S202
将绑定卡的卡交易标识存储至安全元件
S203
向服务器发送验证码获取请求消息
S204
接收服务器响应于验证码获取请求消息反馈的第一动态验证码
S205
接收输入的第二动态验证码
S206
向服务器发送验证码请求消息，以使服务器在第二动态验证码验证成功的情况下激活第一映射关系
S207
接收默认卡设置输入
S213
在联网的情况下，向服务器发送默认卡设置消息，以使服务器将第二映射关系的使用状态设置为默认使用状态
S214
接收服务器发送的默认卡应答消息
S215
响应于默认卡应答消息，通过默认卡设置指令，将安全元件中默认卡的卡交易标识的使用状态设置为默认使用状态，将安全元件中与默认卡的卡交易标识对应的第二匹配通用卡实例的生命状态设置为生效状态
S216

图8

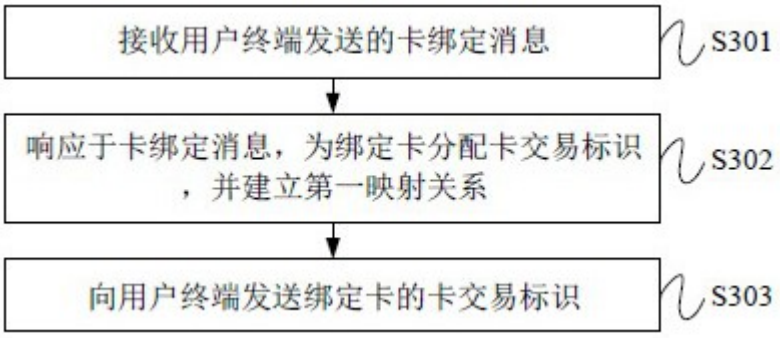
接收用户终端发送的卡绑定消息
S301
响应于卡绑定消息，为绑定卡分配卡交易标识，并建立第一映射关系
S302
向用户终端发送绑定卡的卡交易标识
S303

图9

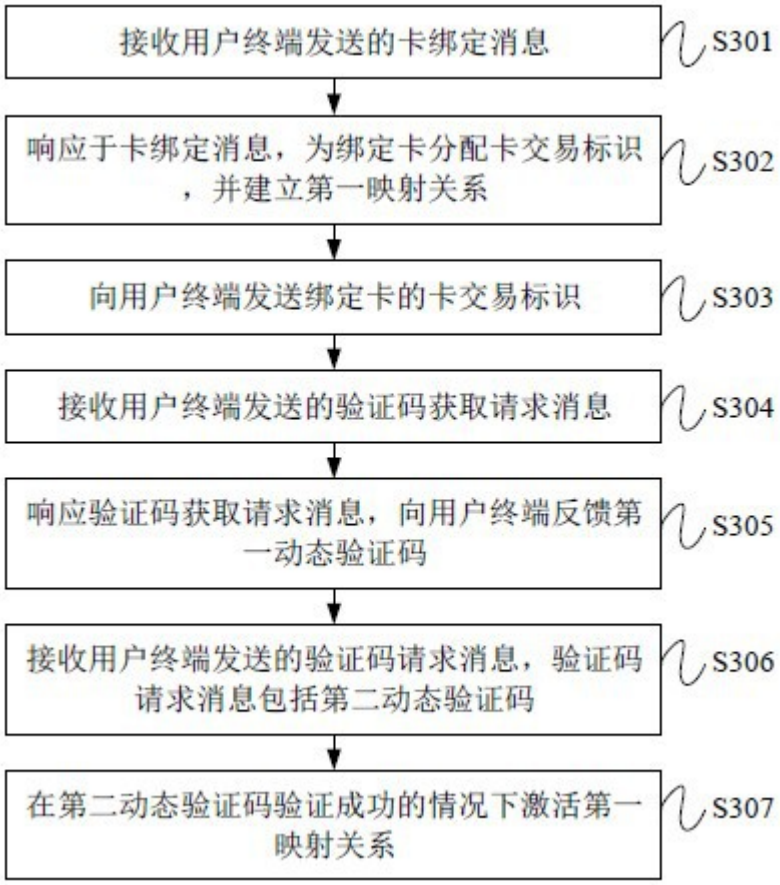
接收用户终端发送的卡绑定消息
S301
响应于卡绑定消息，为绑定卡分配卡交易标识，并建立第一映射关系
S302
向用户终端发送绑定卡的卡交易标识
S303
接收用户终端发送的验证码获取请求消息
S304
响应验证码获取请求消息，向用户终端反馈第一动态验证码
S305
接收用户终端发送的验证码请求消息，验证码请求消息包括第二动态验证码
S306
在第二动态验证码验证成功的情况下激活第一映射关系
S307

图10

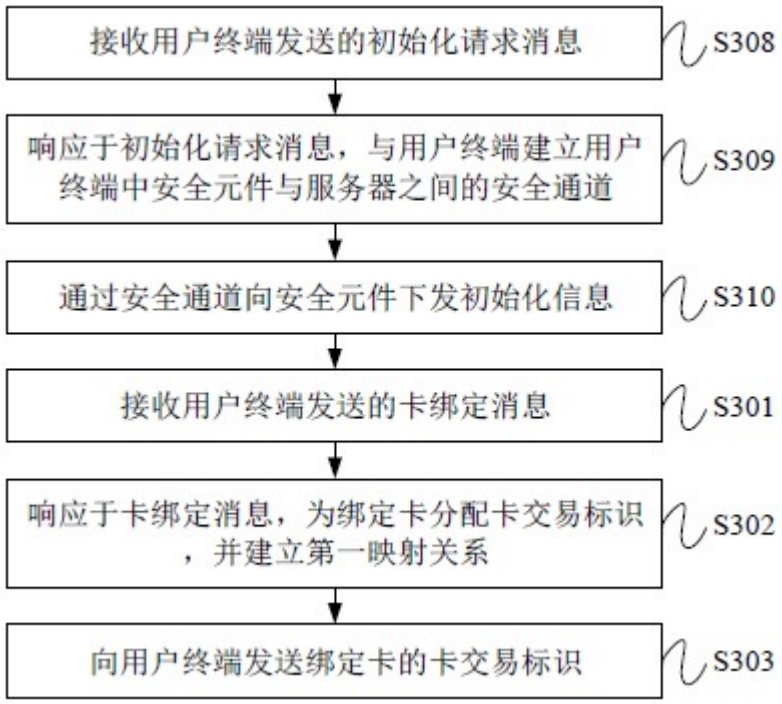
接收用户终端发送的初始化请求消息
S308
响应于初始化请求消息，与用户终端建立用户终端中安全元件与服务器之间的安全通道
S309
通过安全通道向安全元件下发初始化信息
S310
接收用户终端发送的卡绑定消息
S301
响应于卡绑定消息，为绑定卡分配卡交易标识，并建立第一映射关系
S302
向用户终端发送绑定卡的卡交易标识
S303

图11

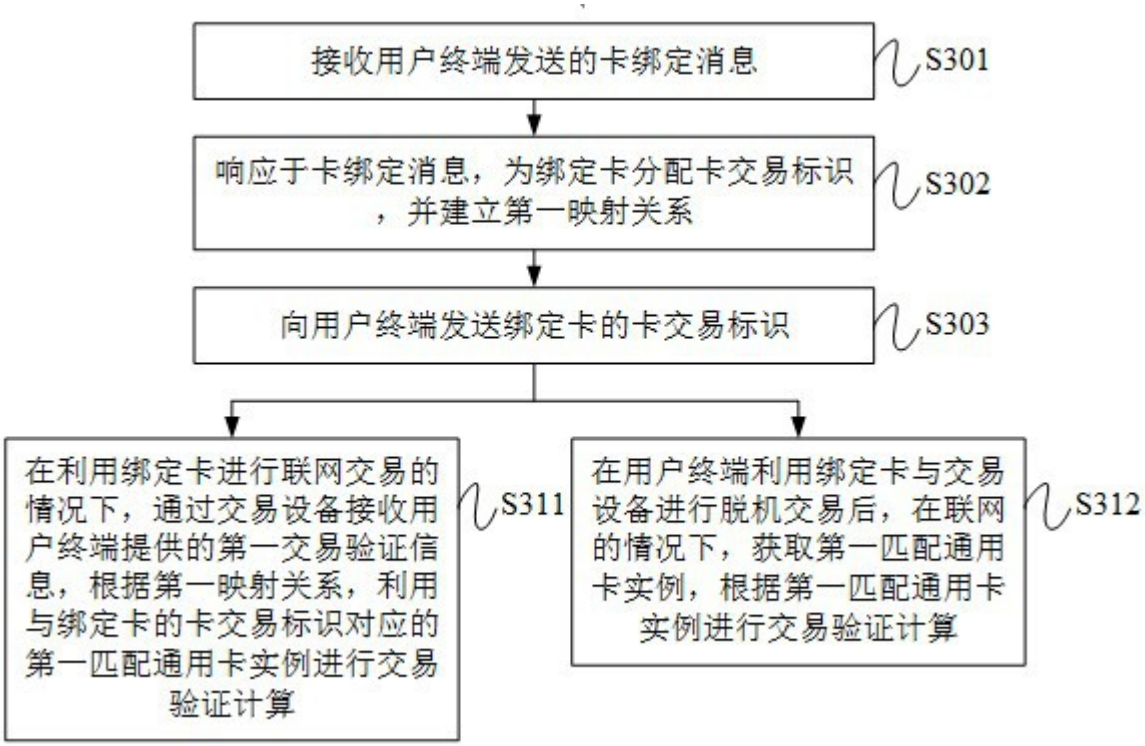
接收用户终端发送的卡绑定消息
S301
响应于卡绑定消息，为绑定卡分配卡交易标识，并建立第一映射关系
S302
向用户终端发送绑定卡的卡交易标识
S303
在利用绑定卡进行联网交易的情况下，通过交易设备接收用户终端提供的第一交易验证信息，根据第一映射关系，利用与绑定卡的卡交易标识对应的第一匹配通用卡实例进行交易验证计算
S311
在用户终端利用绑定卡与交易设备进行脱机交易后，在联网的情况下，获取第一匹配通用卡实例，根据第一匹配通用卡实例进行交易验证计算
S312

图12

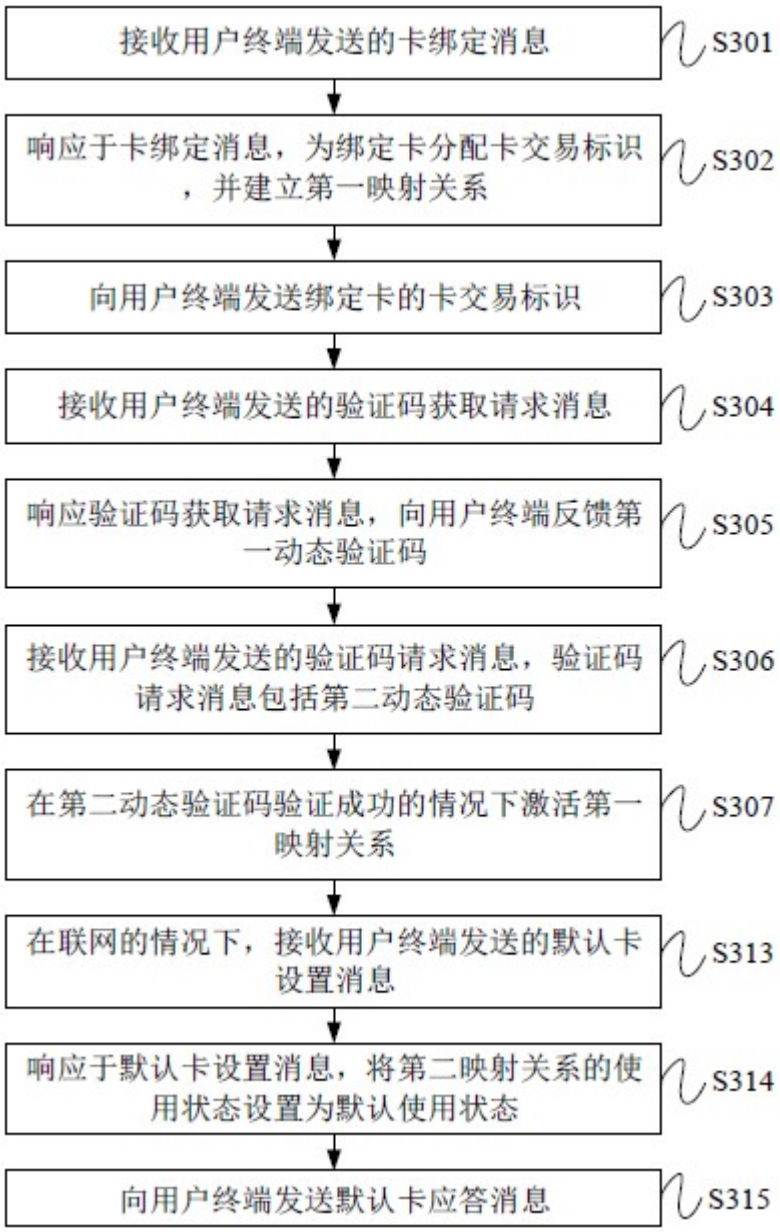
接收用户终端发送的卡绑定消息
S301
响应于卡绑定消息，为绑定卡分配卡交易标识，并建立第一映射关系
S302
向用户终端发送绑定卡的卡交易标识
S303
接收用户终端发送的验证码获取请求消息
S304
响应验证码获取请求消息，向用户终端反馈第一动态验证码
S305
接收用户终端发送的验证码请求消息，验证码请求消息包括第二动态验证码
S306
在第二动态验证码验证成功的情况下激活第一映射关系
S307
在联网的情况下，接收用户终端发送的默认卡设置消息
S313
响应于默认卡设置消息，将第二映射关系的使用状态设置为默认使用状态
S314
向用户终端发送默认卡应答消息
S315

图13

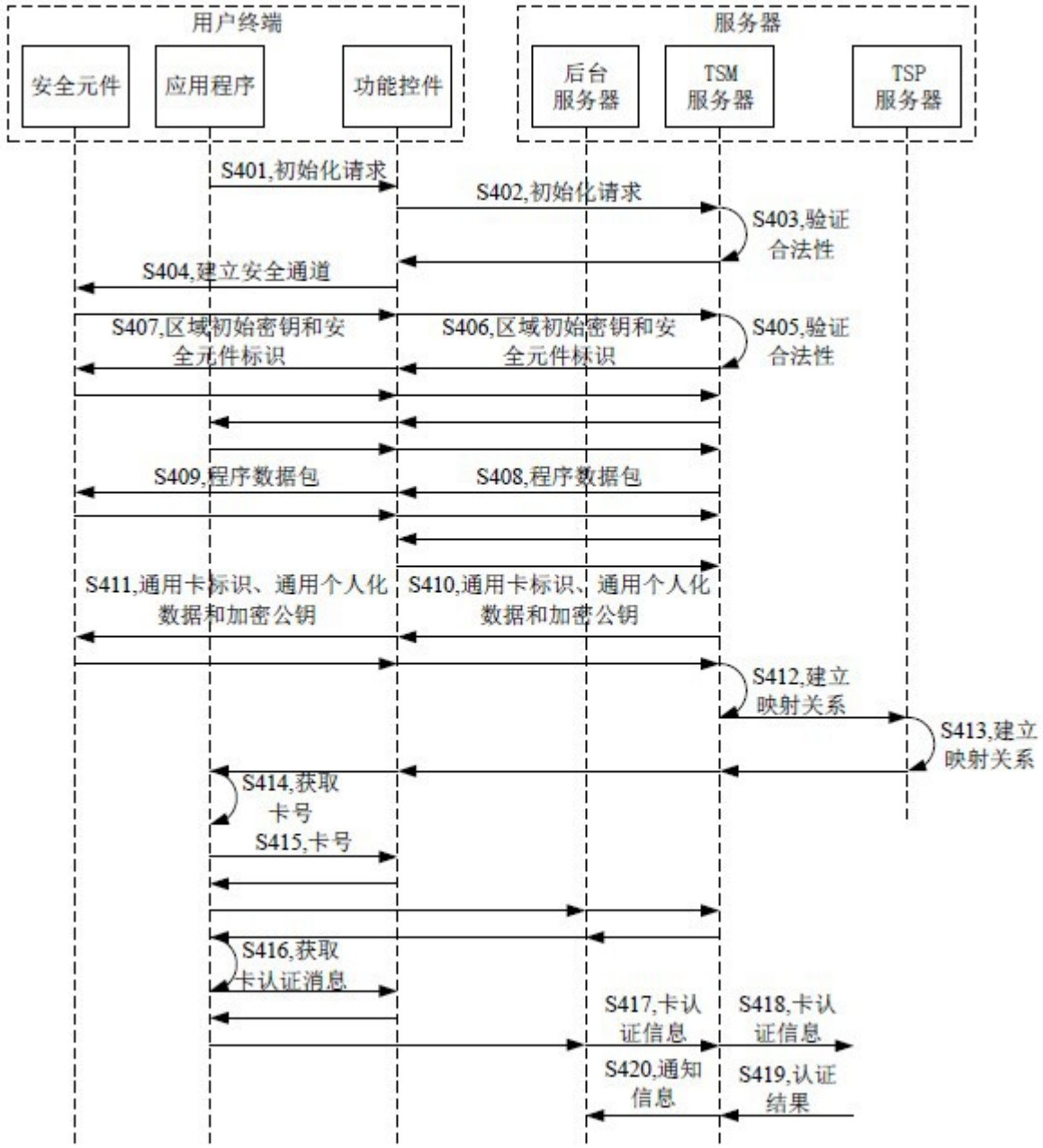
用户终端
安全元件
应用程序
功能控件
服务器
后台服务器
TSM服务器
TSP服务器
S401,初始化请求
S402,初始化请求
S403,验证合法性
S404,建立安全通道
S407,区域初始密钥和安全元件标识
S406,区域初始密钥和安全元件标识
S405,验证合法性
S409,程序数据包
S408,程序数据包
S411,通用卡标识、通用个人化数据和加密公钥
S410,通用卡标识、通用个人化数据和加密公钥
S412,建立映射关系
S413,建立映射关系
S414,获取卡号
S415,卡号
S416,获取卡认证消息
S417,卡认证信息
S418,卡认证信息
S420,通知信息
S419,认证结果

图14

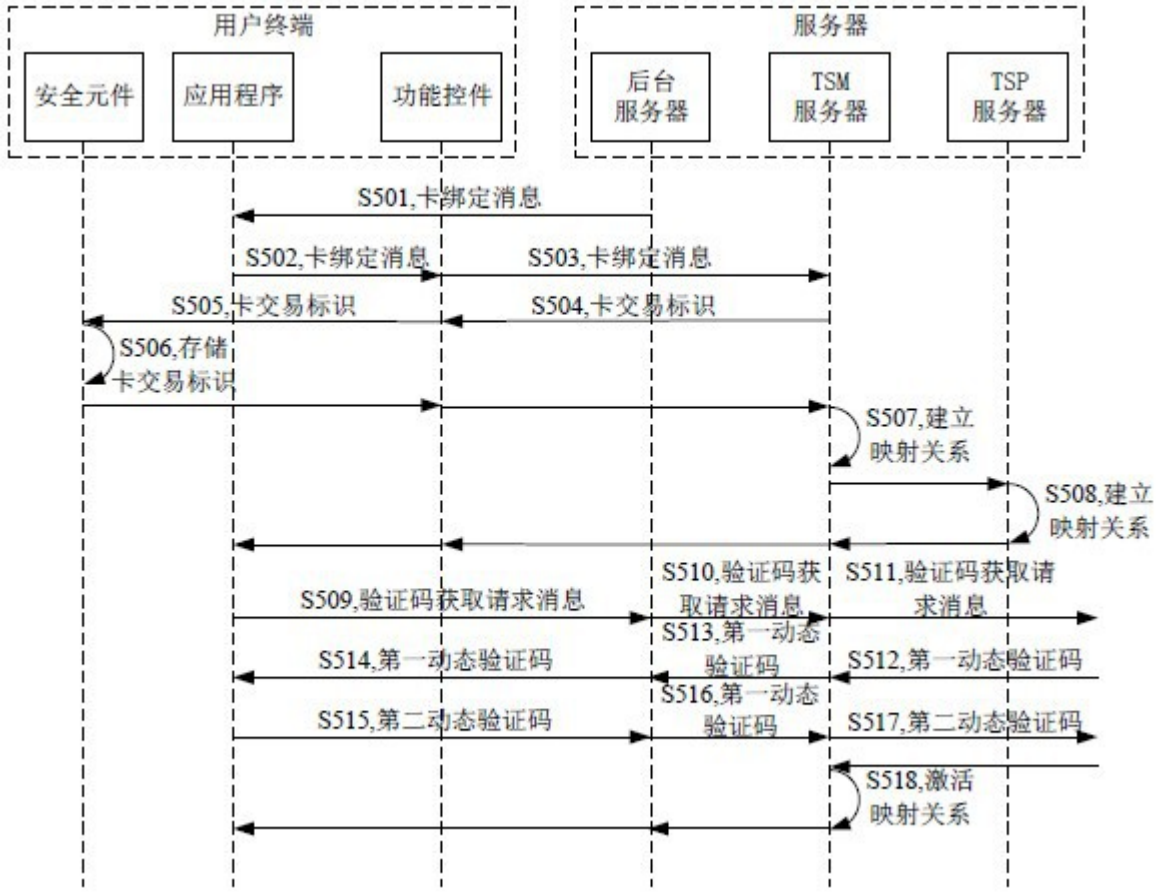
用户终端
安全元件
应用程序
功能控件
服务器
后台服务器
TSM服务器
TSP服务器
S501,卡绑定消息
S502,卡绑定消息
S503,卡绑定消息
S505,卡交易标识
S504,卡交易标识
S506,存储卡交易标识
S507,建立映射关系
S508,建立映射关系
S509,验证码获取请求消息
S510,验证码获取请求消息
S511,验证码获取请求消息
S514,第一动态验证码
S513,第一动态验证码
S512,第一动态验证码
S515,第二动态验证码
S516,第一动态验证码
S517,第二动态验证码
S518,激活映射关系

图15

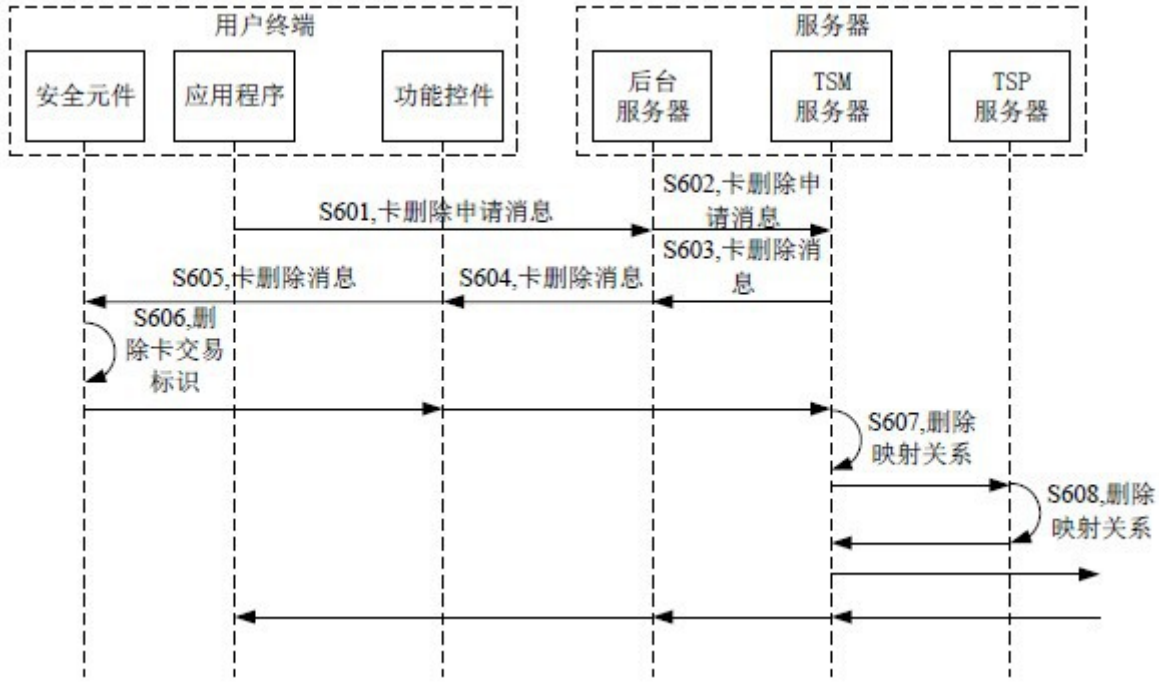
用户终端
安全元件
应用程序
功能控件
服务器
后台服务器
TSM服务器
TSP服务器
S601,卡删除申请消息
S602,卡删除申请消息
S603,卡删除消息
S605,卡删除消息
S604,卡删除消息
S606,删除卡交易标识
S607,删除映射关系
S608,删除映射关系

图16

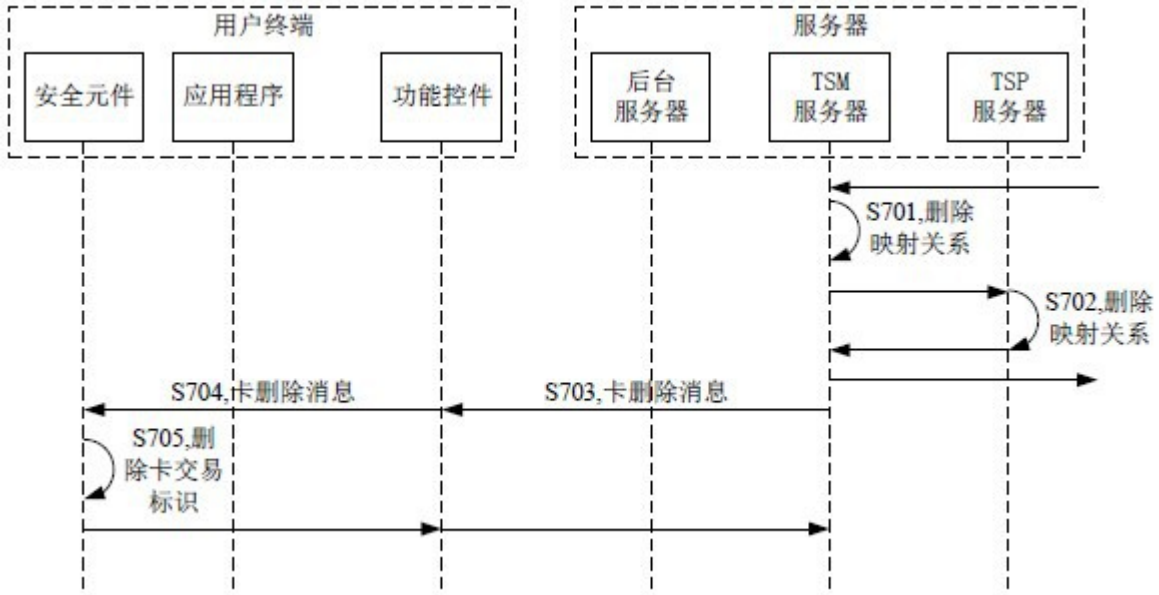
用户终端
安全元件
应用程序
功能控件
服务器
后台
服务器
TSM
服务器
TSP
服务器
S701,删除
映射关系
S702,删除
映射关系
S704,卡删除消息
S703,卡删除消息
S705,删
除卡交易
标识

图17


800
发送模块801
接收模块802
处理模块803

图18

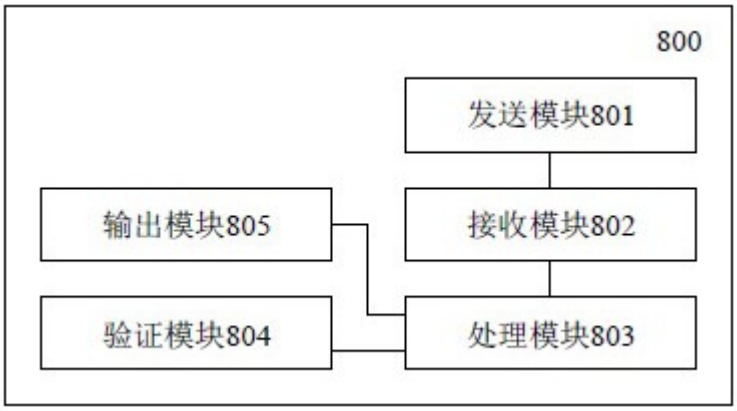
800
发送模块801
输出模块805
接收模块802
验证模块804
处理模块803

图19


900
接收模块901
处理模块902
发送模块903

图20

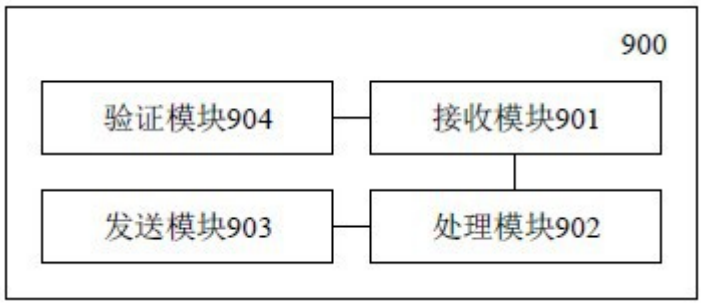
900
验证模块904
接收模块901
发送模块903
处理模块902

图21

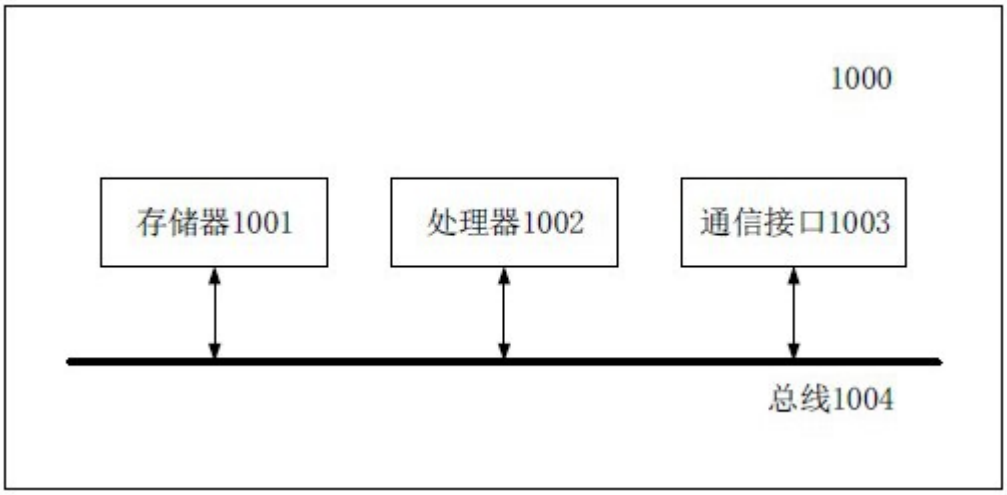
1000
存储器1001
处理器1002
通信接口1003
总线1004

图22

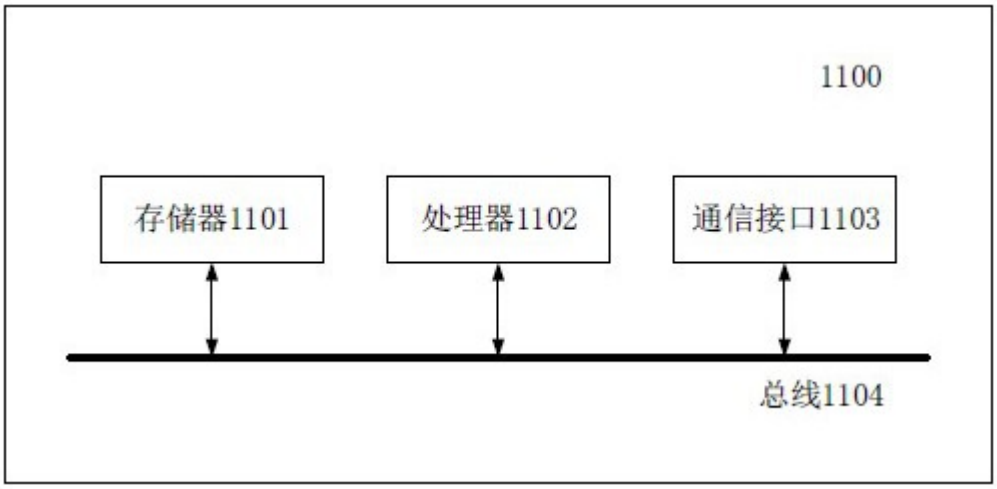
1100
存储器1101
处理器1102
通信接口1103
总线1104

图23