

图形码信息提供、获取方法、装置及终端

技术领域

本申请涉及信息处理技术领域，尤其涉及图形码信息提供、获取方法、装置及终端。

5 背景技术

随着移动通信技术和终端技术的快速发展，终端可以通过安装多种应用，使得终端可以为用户提供越来越丰富的功能。相关技术中，大多数应用出于安全考虑，通常不会将本应用所涉及的较为敏感的图形码信息提供给其他应用。

- 10 例如，在购物等支付应用场景中，用户可以通过支付宝应用所提供的离线付款码快速方便地进行付款操作。目前支付宝在离线付款码支付技术上以及使用人群数量上与其他互联网公司相比都有着极大的优势，因此，各个移动终端厂商都希望能够接入支付宝离线付款码功能，然而向移动终端厂商提供支付宝离线付款码的过程中，有可能存在第三方盗刷离线付款码，或者是
- 15 截获支付宝离线付款码生成的关键数据从而仿制成类似的图形码等情况。

发明内容

为克服相关技术中存在的问题，本申请提供了图形码信息提供、获取方法、装置及终端。

- 根据本申请实施例的第一方面，提供一种图形码信息提供方法，所述方法应用于包括有第一模块、第二模块和接口模块的装置中，所述接口模块与
- 20 所述第二模块对应，所述方法包括：

第二模块通过所述接口模块验证第一模块是否为可信模块；

第二模块接收目标用户信息，并验证所述目标用户信息是否在第二模块

上处于登录状态, 所述目标用户信息与所述接口模块预先关联;

第二模块在验证第一模块为可信模块, 并且所述目标用户信息在第二模块上处于登录状态后, 生成图形码信息并通过所述接口模块传给所述第一模块。

- 5 根据本申请实施例的第二方面, 提供一种图形码信息提供方法, 所述方法应用于第二模块中, 所述方法包括:

通过接口模块验证第一模块是否为可信模块;

通过接口模块接收目标用户信息, 并验证所述目标用户信息是否在第二模块上处于登录状态, 所述目标用户信息与所述接口模块预先关联;

- 10 在验证第一模块为可信模块, 并且所述目标用户信息在第二模块上处于登录状态后, 生成图形码信息并通过所述接口模块传给所述第一模块。

根据本申请实施例的第三方面, 提供一种图形码信息提供方法, 所述方法应用于接口模块中, 所述方法包括:

接收第二模块发送的加密的会话信息并传给第一模块;

- 15 将第一模块对所述加密的会话信息进行解密的解密结果传给第二模块, 以供第二模块根据所述解密结果验证第一模块是否为可信模块;

将预先关联的目标用户信息发送给第二模块, 以供第二模块验证所述目标用户信息是否在第二模块上处于登录状态;

- 接收第二模块在验证第一模块为可信模块, 并且所述目标用户信息在第二模块上处于登录状态后所生成的图形码信息, 并将图形码信息传给所述第一模块。

根据本申请实施例的第四方面, 提供一种图形码信息获取方法, 所述方法应用于第一模块, 所述方法包括:

通过接口模块接收第二模块发送的加密的会话信息;

- 25 对所述加密的会话信息进行解密, 将解密结果通过接口模块传给第二模块, 以供第二模块根据所述解密结果验证所述第一模块是否为可信模块;

通过接口模块接收第二模块提供的图形码信息; 所述图形码信息由第二

模块在验证所述第一模块为可信模块，并且验证接口模块预先关联的目标用户信息在第二模块上处于登录状态后所提供。

根据本申请实施例的第五方面，提供一种图形码信息提供方法，所述方法应用于包括有终端支付应用、第三方支付应用和接口模块的终端中，所述接口模块与所述第三方支付应用对应，所述方法包括：

第三方支付应用通过所述接口模块验证终端支付应用是否为可信应用；

第三方支付应用接收目标用户信息，并验证所述目标用户信息是否在第三方支付应用上处于登录状态，所述目标用户信息与所述接口模块预先关联；

第三方支付应用在验证终端支付应用为可信应用，并且所述目标用户信息在第三方支付应用上处于登录状态后，生成图形码信息并通过所述接口模块传给所述终端支付应用。

根据本申请实施例的第六方面，提供一种图形码信息提供装置，所述装置应用于包括有接口装置和第一装置的终端中，所述装置包括：

可信验证模块，用于通过所述接口装置验证第一装置是否为可信装置；

用户信息验证模块，用于通过接口装置接收目标用户信息，并验证所述目标用户信息是否在第二装置上处于登录状态，所述目标用户信息与所述接口装置预先关联；

信息传输模块，用于在验证第一装置为可信装置，并且所述目标用户信息在第二装置上处于登录状态后，生成图形码信息并通过所述接口装置传给所述第一装置。

根据本申请实施例的第六方面，提供一种图形码信息提供装置，所述装置应用于包括有第一装置和第二装置的终端中，所述装置包括：

加密会话信息接收模块，用于接收第二装置发送的加密的会话信息并传给第一装置；

解密结果传输模块，用于将第一装置对所述加密的会话信息进行解密的解密结果传给第二装置，以供第二装置根据所述解密结果验证第一装置是否为可信装置；

用户信息发送模块，用于将预先关联的目标用户信息发送给第二装置，以供第二装置验证所述目标用户信息是否在第二装置上处于登录状态；

- 图形码信息接收模块，用于接收第二装置在验证第一装置为可信装置，并且所述目标用户信息在第二装置上处于登录状态后所生成的图形码信息，
- 5 并将图形码信息传给所述第一装置。

根据本申请实施例的第七方面，提供一种图形码信息获取装置，所述装置应用于包括有接口装置和第二装置的终端中，所述装置包括：

加密会话信息接收模块，用于通过接口装置接收第二装置发送的加密的会话信息；

- 10 解密模块，用于对所述加密的会话信息进行解密，将解密结果通过接口装置传给第二装置，以供第二装置根据所述解密结果验证所述第一装置是否为可信装置；

- 图形码信息接收模块，用于通过接口装置接收第二装置提供的图形码信息；所述图形码信息由第二装置在验证所述第一模块为可信装置，并且验证
- 15 接口装置预先关联的目标用户信息在第二装置上处于登录状态后所提供

根据本申请实施例的第八方面，提供一种终端，所述终端包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

- 20 第二模块通过接口模块验证第一模块是否为可信模块；

第二模块接收目标用户信息，并验证所述目标用户信息是否在第二模块上处于登录状态，所述目标用户信息与所述接口模块预先关联；

- 第二模块在验证第一模块为可信模块，并且所述目标用户信息在第二模块上处于登录状态后，生成图形码信息并通过所述接口模块传给所述第一模
- 25 块。

本申请的实施例提供的技术方案可以包括以下有益效果：

本申请实施例的方案，第一模块可以在用户需要接入第二模块的图形码

功能时，第二模块对第一模块进行安全验证，同时对第一模块已关联的第二模块的用户进行安全验证，在两者都通过安全验证后，再将图形码信息提供给第一模块，因此保证图形码信息提供过程的安全性能，从而能防止图形码被盗刷或者被截获等情况。

- 5 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本申请。

附图说明

此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本申请的实施例，并与说明书一起用于解释本申请的原理。

- 10 图 1 是本申请一个实施例中图形码信息提供方法的流程示意图。
- 图 2A 是本申请另一个实施例中图形码信息提供方法的流程示意图。
- 图 2B 是本申请一个实施例中图形码信息提供方法的应用场景图。
- 图 2C 是本申请另一个实施例中图形码信息提供方法的流程示意图。
- 图 2D 是本申请另一个实施例中图形码信息提供方法的流程示意图。
- 15 图 2E 是本申请另一个实施例中图形码信息提供方法的流程示意图。
- 图 3 是本申请图形码信息提供装置/图形码信息获取装置所在终端设备的一种硬件结构图。
- 图 4 是本申请一个实施例中图形码信息提供装置的框图。
- 图 5 是本申请另一个实施例中图形码信息提供装置的框图。
- 20 图 6 是本申请一个实施例中图形码信息获取装置的框图。

具体实施方式

- 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。
- 以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。
- 25 相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一

致的装置和方法的例子。

在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

应当理解，尽管在本申请可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本申请范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

本申请实施例所提供的方案可应用于智能终端，例如智能手机、智能手表、智能眼镜、平板电脑或随身听设备等。终端可以通过安装多种应用，使得终端可以为用户提供越来越丰富的功能。相关技术中，大多数应用出于安全考虑，通常不会将本应用所涉及的较为敏感的图形码信息提供给其他应用。本申请实施例所提供的方案，可以使数据提供方安全传输图形码信息给数据接收方。

参见图 1，是本申请一个实施例中图形码信息提供方法的流程示意图，所述方法应用于包括有第一模块、第二模块和接口模块的装置中，所述接口模块与所述第二模块对应，所述方法包括如下步骤 101 至 103:

在步骤 101 中，第二模块通过所述接口模块验证第一模块是否为可信模块。

在步骤 102 中，第二模块接收目标用户信息，并验证所述目标用户信息是否在第二模块上处于登录状态。所述目标用户信息与所述接口模块预先关联。

在步骤 103 中，第二模块在验证第一模块为可信模块，并且所述目标用户信息在第二模块上处于登录状态后，生成图形码信息并通过所述接口模块传给所述第一模块。

本申请实施例中的装置可运行于如智能手机、平板电脑、随身听设备、个人计算机或便携设备等智能终端，第一模块可以是指图形码信息接收方，第二

模块可以是指图形码信息提供方。第一模块和第二模块可以是独立运行于所述装置中的两个不同应用，由于图形码信息是由第二模块提供给第一模块，接口模块可与第二模块对应，用于第二模块与第一模块之间的安全通信。

由于第二模块向第一模块提供图形码信息，第一模块和第二模块需要进行数据交互。假设第一模块和第二模块由不同厂商所生产，且两者直接进行数据交互，则双方需相互向对方公开信息传输协议，以实现图形码信息提供处理过程。然而，公开信息传输协议将降低安全性能，因此，本实施例通过接口模块实现第一模块和第二模块的交互过程，接口模块可以是由生产第二模块的厂商提供给第一模块，接口模块的具体功能由生产第二模块的厂商提供，则生产第二模块的厂商无须向第一模块公开较多的数据传输协议。接口模块提供给第一模块后，可以由第一模块整合，作为第一模块的子模块与第二模块进行交互，从而减少第一模块对应厂商的开发成本和难度。

当第二模块向第一模块发送图形码信息之前，第二模块可通过接口模块对第一模块，以及第一模块所关联的用户信息进行安全验证。在验证第一模块为可信模块，并且所述目标用户信息在第二模块上处于登录状态后，生成图形码信息并通过所述接口模块传给所述第一模块。

其中，第二模块验证第二第一模块为可信模块，是为了确定第一模块是第二模块预先设定的可信的模块，以防止其他不可信模块向第二模块发起图形码信息获取请求，而将图形码信息提供给不可信模块。由于图形码信息涉及用户敏感信息，因此还可验证第二模块所关联的用户信息是否当前在第二模块上处于登录状态。其中，该目标用户信息可以为能够唯一区分用户的信息，例如用户账号或用户标识等，用户信息的具体形式在实际应用中可以灵活配置，本实施例对此不作限定。若第二模块上处于登录状态的用户信息与第二模块所关联的用户信息不匹配，表示当前使用第一模块和第二模块的用户可能不是同一个，则安全验证不通过，从而防止将图形码信息提供给其他用户，保证图形码信息的安全。

在实际应用中，验证第一模块是否为可信模块，可以有多种方式实现，例

如第一模块和第二模块可以预先约定某些自定义的标识信息（比如某些密码串、第一模块的唯一标识或某些自定义的字符串等），第二模块在验证时，接口模块可以获取第一模块所保存的标识信息，并提供给第二模块进行核对，第二模块根据核对结果确定第一模块是否为可信模块。另外，接口模块在提供给第二模块时还可对标识信息进行加密等安全处理，以进一步提高数据传输安全性。

在其他可选的实现方式中，还可以是第一模块和第二模块预先约定密钥，接口模块可以将第一模块加密的数据提供给第二模块进行解密，若成功解密，则可以确定第一模块为可信模块；或者，还可以是第二模块将加密的数据提供给第一模块进行解密，若成功解密，则可以确定第二模块为可信模块。

10 在一个可选的实现方式中，所述第二模块通过所述接口模块验证第一模块是否为可信模块，包括：

第二模块将加密的会话信息通过接口模块传给第一模块。

第一模块对所述加密的会话信息进行解密，并将解密结果通过接口模块传给第二模块。

15 第二模块根据所述解密结果验证第一模块是否为可信模块。

通过上述对会话信息加密的方式，可以提高数据传输安全性。其中，当第一模块为智能终端的厂商所生产，所述第一模块对所述加密的会话信息进行解密所采用的密钥可以为预置在安全存储区的私钥，所述第二模块加密所述会话信息所采用的密钥为第一模块预先分发的公钥。本实施例的终端可以是预先配置有安全存储区域（TEE，Trusted Execution Environment）的终端。TEE是指终端厂商定制的客户安全存储数据和执行程序的区域，其提供了一个与设备操作系统并行运行的独立执行环境，能用于存储密钥，认证和证书；执行设备上重要的内容保护软件；执行核心内容保护功能等。本实施例的终端厂商可以在安全存储区域为第一模块预置有非对称密钥（公钥和私钥），第一模块可以在与第二模块的用户信息进行关联的时候，将公钥分发给第二模块。公钥和私钥预置在终端 TEE 的方式，其破解难度较大，能保证密钥的安全存储。

20

25

本实施例采用公钥和私钥进行数据加密，也即是采用非对称密钥加密的方式，该方式的安全性较高。非对称密钥加密是指加密和解密使用不同密钥的加密方式，其需要两个密钥：公钥（publickey）和私钥（privatekey）。如果用公钥对数据进行加密，只有用对应的私钥才能解密。例如，甲方生成一
5 对密钥并将其中的一把作为公钥向乙方公开；得到该公钥的乙方使用该密钥对机密信息进行加密后再发送给甲方；甲方再用自己保存的另一把私钥对加密后的信息进行解密。

由于第一模块持有私钥，第二模块持有公钥，该公钥可以由第一模块预先分发给第二模块。当第三方支付应用发送采用公钥加密的会话信息，若终
10 端支付应用的私钥可以解开，则可以确定终端支付应用为可信应用。

在一个可选的实现方式中，所述会话信息包括随机生成的会话密钥。

所述第一模块对所述加密的会话信息进行解密，并将解密结果通过接口模块传给第二模块，包括：

第一模块对所述加密的会话信息进行解密，若第一模块成功解密，得到
15 解密的会话密钥，并将解密得到的会话密钥传给接口模块。

接口模块加密一验证信息，并传给第二模块；其中，接口模块加密所述验证信息所采用的密钥为所述第一模块解密得到的会话密钥。

所述第二模块根据所述解密结果验证第一模块是否为可信模块，包括：

第二模块接收加密的验证信息，并利用所述随机生成的会话密钥进行解
20 密；若成功解密，确定第一模块为可信模块。

第二模块采用公钥加密的数据传输至第一模块，第二模块需要知道第一模块采用私钥进行解密的解密结果，而解密结果通过接口模块传输给第二模块的过程，也需要保证其安全性，以防止被恶意软件破解。本实施例中，第二模块采用公钥加密的会话信息时，可以是随机生成会话密钥，将会话密钥
25 作为会话信息，利用公钥加密该会话密钥。会话密钥（session key）是指保证会话双方之间安全通信会话而随机产生的具有时效性的加密和解密密钥。若第一模块成功解密，将得到解密的会话密钥，接口模块可以利用该会话密

钥加密一验证信息并传输给第二模块。其中，该验证信息的具体形式可以根据实际需要而灵活配置，该步骤的目的是利用第一模块解密得到的会话密钥加密一信息即可，则第二模块可以接收接口模块所发送的加密的验证信息，并利用其事先随机生成的会话密钥进行解密。若成功解密，可以确定第一模块为可信模块。通过上述会话密钥，可以准确地检验出第一模块是否能利用预先约定的密钥成功解密，也可以保证解密结果传输的安全性。

由前述描述可知，第二模块对第一模块进行安全验证的过程，包括有验证第一模块预先关联的用户信息是否在第二模块处于安全登录状态的过程。在进行此验证的过程中，可以是由第一模块将预先关联的用户信息传输给第二模块，为了保证该过程用户信息传输的安全性，可以是接口模块将用户信息加密后传输给第二模块。

在一个可选的实现方式中，为了减少处理流程，加快第二模块的验证速度，所述接口模块加密一验证信息，并传给第二模块，可以包括：

所述接口模块加密所述目标用户信息后，将加密的目标用户信息作为所述加密的验证信息传给第二模块。

本实施例中，接口模块可以在向第二模块发送第一模块的解密结果时，将目标用户信息作为验证信息并采用会话密钥加密后传输给第二模块，一方面实现了在传输目标用户信息时对目标用户信息进行加密，另一方面也减少了处理流程。对于第二模块而言，第二模块能够同时验证第一模块是否成功解密以及验证目标用户信息。

第二模块在验证第一模块为可信模块，并且所述目标用户信息在第二模块上处于登录状态后，可以生成图形码信息并通过所述接口模块传给所述第一模块。在传输图形码信息的过程中，可以将图形码信息进行加密后传输。

在一个可选的实现方式中，所述会话信息还可包括随机码。所述第二模块可以随机生成随机码，并利用公钥将会话密钥和随机码发送给接口模块。第一模块成功解密后，得到会话密钥和随机码。接口模块在利用会话密钥加密目标用户信息时，可以是利用会话密码加密目标用户信息和随机码。本申请实施例

中，会话信息还可以包括随机生成的随机码，第二模块可以验证接口模块所回传的随机码与随机生成的随机码是否一致，从而可以防止请求重入，以进一步保证数据传输安全。

其中，所述生成图形码信息并通过所述接口模块传给所述第一模块，可以
5 包括：

所述第二模块生成图形码信息后，利用所述随机生成的会话密钥加密图形码信息并传给接口模块。

所述接口模块接收所述加密图形码信息，对所述加密图形码信息解密后传给所述第一模块；其中，接口模块解密所述加密图形码信息时所采用的密钥为
10 所述第一模块解密得到的会话密钥。

本实施例中，在传输图形码信息的过程中可以利用前述的会话密钥进行加密，以保证图形码信息传输过程的安全。

在实际应用中，所述生成图形码信息，可以是：通过预分发的动态口令种子生成所述图形码信息。其中，动态口令（One-time Password）种子可以根据专
15 门的算法每隔 60 秒生成一个与时间相关的、不可预测的随机数字组合，每个口令只能使用一次，因此能保证图形码信息只能使用一次，并且能限制图形码信息的使用时效，从而有效保护图形码信息的安全使用。

至此，实施本申请实施例所提供的方案，第一模块可以在用户需要接入第二模块的图形码功能时，利用接口模块安全地接入第二模块的图形码信息并快速
20 地提供给第一模块，使得第一模块可以快速获取到图形码信息。

上述实施例具体描述了第一模块获取第二模块所提供的图形码信息过程，在一个可选的实现方式中，在第二模块向第一模块提供图形码前，第一模块可以向第二模块请求接入图形码信息，以实现与目标用户信息的关联。接下来对第一模块预先关联目标用户信息的过程进行描述。

25 本实施例中，所述目标用户信息与所述接口模块可以预先通过如下方式关联：

第一模块通过接口模块向第二模块发起关联请求。

第二模块将处于登录状态的用户身份授权信息通过接口模块发送给第一模块。

第一模块将所述用户身份授权信息、预置在安全存储区中的公钥和预置的设备唯一标识通过第一模块对应的服务端发送给第二模块对应的服务端。

- 5 第一模块接收目标用户信息，并将所述目标用户信息传给接口模块，所述目标用户信息为第二模块对应的服务端在验证用户身份授权信息正确后通过第一模块对应的服务端所发送。

本申请实施例中，OAuth（Open Authorization，开放授权）是为用户资源的授权定义的一个安全、开放及简单的标准，第三方无需知道用户的账号及密码，
10 就可获取到用户的授权信息，也即是上述的用户身份授权信息。该用户身份授权信息可以是第二模块对应的服务端在验证用户通过第二模块输入的用户账户和账户密码正确后所生成。

终端支付应用请求第二模块的用户身份授权信息，从而可以采用安全方式将用户身份授权信息、公钥和终端唯一标识发送给第二模块对应的服务端，第二模块对应的服务端可以在将第二模块所发送的用户身份授权信息与之前生成的用户身份授权信息核对一致后，将用户身份授权信息、公钥和设备唯一标识三者进行存储，从而建立第一模块、公钥和第二模块用户的三者关联。

第一模块可以将携带有设备唯一标识的图形码开通授权请求发送给第二模块，第二模块根据该请求，可以向第二模块对应的服务端请求获得第一模块所分发的公钥，第二模块对应的服务端接收到开通授权请求，在验证用户身份授权信息正确后利用所存储的用户身份授权信息、公钥和设备唯一标识，将与设备唯一标识对应的公钥分发给第二模块，同时还可以发送用于生成图形码信息的动态口令种子，从而为当前登录用户在第一模块开通接入第二模块的图形码的功能。

25

本申请实施例的方案可以应用在大多数需要提供涉及用户敏感信息的图形码的场景中，例如，在支付应用场景下，第三方支付应用可以将付款码提供给

终端支付应用，通过终端支付应用可以快速便捷地调出付款码，以使用户快速地进行付款操作；或者，在社交等应用场景下，社交应用将用户信息的图形码提供其他应用，通过其他应用可以快速便捷地调出付款码，以使用户快速地进行添加好友等操作。

- 5 接下来将以本申请方案应用于支付场景为例进行详细描述。其中，图 1 所示实施例中的第一模块可以是本实施例的终端支付应用，第二模块可以是本实施例的第三方支付应用。

10 目前，越来越多的智能终端厂商推出了支付应用，例如苹果公司的苹果支付、三星公司的三星支付或华为公司的华为支付等。此类终端厂商的终端支付应用，可以预先绑定用户的银行卡，用户在支付时，无论是终端处于锁屏、黑屏或主屏幕等状态下，用户无需查找并启动应用，只需按照预设操作，例如在屏幕下方输入向上滑动的轨迹，即可调出终端支付应用的支付功能，通过与 POS 机进行近场通信的方式实现付款操作。

15 传统技术中，智能终端也可以安装第三方支付应用，利用第三方支付应用进行交易支付操作。以支付宝为例，当用户在向商户付款时，可以利用支付宝提供的付款码功能，在应用界面中显示付款二维码，该付款二维码通常携带有加密后的用户信息，商户可以通过扫码机扫描该付款二维码，从而实现付款操作。

20 由于第三方支付应用庞大的用户群以及付款码支付的操作便利性，越来越多的终端厂商希望能接入支付宝的离线付款码功能。然而向移动终端厂商提供支付宝离线付款码的过程中，有可能存在第三方盗刷离线付款码，或者是截获支付宝离线付款码生成的关键数据从而仿制成类似的图形码等情况。

25 本申请实施例提供的图形码信息提供方案，第三方支付应用可以对发起付款码请求的终端厂商应用进行安全验证，同时对终端厂商应用已关联的第三方支付应用用户进行安全验证，在两者都通过安全验证后，再将图形码信息提供给终端厂商应用，因此能保证图形码提供过程的安全性能，从而能防止付款码被盗刷或者被截获。

本实施例的终端可以安装有终端支付应用和第三方支付应用。用户可以通过终端支付应用基于第一账户登录终端服务器，在通过输入账户和密码并成功登录终端服务器后，可以通过终端支付应用获得终端服务器所提供的功能。用户还可以通过第三方支付应用基于第二账户登录第三方支付服务器，在通过输入账户名和密码成功登录第三方支付服务器后，可以通过第三方支付应用获得第三方支付服务器所提供的功能。

其中，本申请实施例的终端为预先配置有安全存储区域（TEE，Trusted Execution Environment）的终端。本实施例的终端厂商可以在安全存储区域为终端支付应用预置有非对称密钥（公钥和私钥），以用于数据加密。

结合图 2A 和图 2B 对本实施例的图形码信息提供方案进行详细描述。图 2A 是本申请一个实施例中图形码信息提供方法的流程示意图，图 2B 是本申请一个实施例中图形码信息提供方法的应用场景图，图 2B 中包括一作为终端的智能手机，第三方支付应用和终端厂商所生产的支付应用。智能手机中设置有安全存储区域，该手机厂商在安全存储区域中预置有公钥和私钥。第三方支付应用的服务厂商可以预先进行相关程序开发，并打包为软件开发工具包 SDK 提供给终端厂商，终端厂商可以将该 SDK 以子模块的方式集成在终端支付应用中，并作为终端支付应用的一个子模块与第三方支付应用进行交互，本实施例将该子模块称为接口模块。可以理解，在其他可选的实现方式中，终端还可以是平板电脑、智能手环或智能眼镜等设备，第三方支付应用可以具体为包括常见的微信支付或百度钱包等应用。该方法包括如下步骤 201 至 203：

在步骤 201 中，第三方支付应用通过所述接口模块验证终端支付应用是否为可信应用。

在步骤 202 中，第三方支付应用接收目标用户信息，并验证所述目标用户信息是否在第三方支付应用上处于登录状态，所述目标用户信息与所述接口模块预先关联。

在步骤 203 中，第三方支付应用在验证终端支付应用为可信应用，并且所述目标用户信息在第三方支付应用上处于登录状态后，生成图形码信息并通过

所述接口模块传给所述终端支付应用。

本实施例中，终端可以安装有终端支付应用和第三方支付应用。用户可以通过终端支付应用基于第一账户登录终端服务器，在通过输入账户和密码并成功登录终端服务器后，可以通过终端支付应用获得终端服务器所提供的功能。

- 5 用户还可以通过第三方支付应用基于第二账户登录第三方支付服务器，在通过输入账户名和密码成功登录第三方支付服务器后，可以通过第三方支付应用获得第三方支付服务器所提供的功能。

其中，本申请实施例的终端为预先配置有安全存储区域（TEE，Trusted Execution Environment）的终端。终端厂商可以在安全存储区域为终端支付应用
10 预置有非对称密钥（公钥和私钥），以用于在支付过程中进行数据加密。

本实施例中，终端厂商应用可以在用户指示下，调用接口模块向第三方支付应用发起付款码生成请求。终端厂商应用可以预先绑定第三方支付应用的用户账户，当该用户需要通过终端厂商应用获取第三方支付应用的付款码时，可以按照预设操作，例如，参见图 2B 所示，用户可以在屏幕下方输入向上滑动的
15 轨迹，即可调出终端支付应用的支付功能，并由用户选择第三方支付应用进行支付。

本实施例中，第三方支付应用可以通过接口模块对终端支付应用进行安全验证，以确认终端支付应用是第三方支付应用的可信应用。在具体实施时，可以采用非对称密钥加密的方式，由终端支付应用持有私钥，第三方支付应用持有公钥，第三方支付应用采用公钥加密的会话信息并通过接口模块发送给终端
20 支付应用，若终端支付应用的私钥可以解开，则可以确定终端支付应用为可信应用。其中，终端支付应用可以预先与第三方支付应用的用户进行关联，并在成功关联后将安全存储区的公钥分发给第三方支付应用。

采用终端支付应用持有私钥，第三方支付应用持有公钥的方式，是由于公
25 钥和私钥预置在终端的 TEE 区域中，能保证公钥和私钥的安全存储。本实施例中，不同终端所预置的公钥和私钥不同，并且由于终端支付应用为终端厂商所开发，因此终端支付应用可以拥有在 TEE 中读取公钥或私钥等的权限。

第三方支付应用通常是由第三方支付服务厂商提供第三方支付应用 APP 供用户下载，用户可以将下载的 APP 安装于终端中。假设由第三方支付应用提供公钥和私钥，若是在 APP 中预置算法以用于生成公钥和私钥，但由于 APP 安装在终端的公共存储区域，所生成的公钥和私钥无法安全存储，且容易被其他恶意应用所攻击或破解。因此，公钥和私钥存储在终端的 TEE 中，公钥由终端支付应用提供给第三方支付应用，可以保证密钥的安全存储。

公钥可以是终端支付应用预先分发给第三方支付应用，当第三方支付应用发送采用公钥加密的会话信息给终端支付应用，若终端支付应用的私钥可以解开，则可以确定终端支付应用为可信应用。

终端支付应用可以在安全存储区中，通过预置在安全存储区私钥解密该加密的会话信息。由于私钥是终端支付应用所持有，终端支付应用利用私钥对第三方支付应用发送的采用公钥加密的会话信息的解密结果需提供给第三方支付应用，以使第三方支付应用确认终端支付应用是否为可信应用。而解密结果在告知第三方支付应用的过程，也需要采用加密的方式进行传输。

本实施例中，第三方支付应用采用公钥加密的会话信息中，可以包括有随机生成的会话密钥。若终端支付应用利用私钥成功解密会话信息，则可获得会话密钥，接口模块可以利用该会话密钥加密终端支付应用预先关联的目标用户信息并回传给第三方支付应用。

第三方支付应用接收到该会话密钥加密的目标用户信息，一方面，若第三方支付应用利用之前随机生成的会话密钥成功解开，则说明终端支付应用利用私钥成功解开其采用公钥加密的会话信息，因此可以确定终端支付应用为可信应用；另一方面，会话密钥保证了双方此次会话的安全；并且，会话密钥加密了终端支付应用已关联的目标用户信息，则第三方支付应用可以利用该目标用户信息，确认其是否在第三方支付应用处于登录状态，进而可以对终端支付应用已绑定的用户账户进行安全验证。

第三方支付应用可以在对终端支付应用和终端支付应用所绑定的用户的安全验证都通过后，生成付款码，并采用会话密钥进行加密传输给接口模块，以

保证付款码传输过程的安全。接口模块可以接收该会话密钥加密的付款码，利用会话密钥进行解密，将得到的付款码提供给终端支付应用进行显示。

至此，实施本申请实施例所提供的方案，终端支付应用可以在用户需要接入第三方支付应用的付款码功能时，接口模块可以安全地接入第三方支付应用的付款码并快速地提供给终端支付应用，使得终端支付应用可以在应用界面中快速显示如图 2B 所示的付款码，以供用户快速地完成付款操作。

接下来在图 2B 所示实施例的基础上，再提供一具体实施例对本申请的方案进行说明。如图 2C 和图 2D 所示，是本实施例图形码提供方法的流程示意图，本实施例中，第三方支付应用采用支付宝钱包为例进行说明，包括：

步骤 230、终端支付应用调用支付宝付款码 SDK 的生成条码接口，SDK 向支付宝钱包发起付款码生成请求。

步骤 231、支付宝钱包收到付款码生成请求。根据当前登录用户的用户账户获取与用户账户对应的公钥。

其中，该公钥由终端服务端提供给第三方支付端，并由第三方支付服务端分发给支付宝钱包进行安全存储。在实际应用中，第三方支付服务端在分发时基于与支付宝钱包预先协商的加密方式进行加密，支付宝钱包可以存储加密后的公钥，当需要获取时，基于预先协商的解密方式进行解密。

步骤 232、支付宝钱包随机生成会话密钥 sessionKey 和随机码 challenge，并使用步骤 231 中所获取的公钥进行加密后，传给 SDK。

其中，采用公钥加密是为了保证数据传输安全，并用于对终端支付应用进行安全验证。会话密钥用于在本次请求时提供给 SDK，还可用于后续对付款码的解密，保证付款码的安全。

步骤 233、SDK 将加密的 sessionKey 和 challenge 传给终端支付应用。

步骤 234、终端支付应用将接收到的加密的 sessionKey 和 challenge，在安全存储区域 TEE 中，采用预置在 TEE 中的私钥进行解密；若解密成功，将解密后的 sessionKey、challenge 和预存的用户账户（userID）回传给 SDK。

其中，该预存的用户账户是开通终端厂商应用的付款码接入功能的用户账户。

步骤 235、SDK 使用 sessionKey 对 userID 和 challenge 加密后传到支付宝钱包。

5 其中，对 userID 进行加密并传到支付宝钱包，是为了验证支付宝钱包当前的用户账户是否是在终端支付应用预先开通付款码支付的用户。

步骤 236、支付宝钱包用 sessionKey 解密后，得到 userID 和 challenge，对两者进行校验。

步骤 237、两者都校验成功，支付宝钱包根据当前的 userID 获取 Otp 种子，
10 生成付款码，并用 sessionkey 加密付款码回传给 SDK。

步骤 238、SDK 用 sessionKey 解密出付款码给终端支付应用。

步骤 239、终端支付应用在屏幕中展示付款码。

参考图 2E，是本申请实施例的图形码提供方法的流程示意图，该示意图示出了终端支付应用关联第三方支付应用用户的过程，也即是付款码开通授权流
15 程，本实施例中，第三方支付应用采用支付宝钱包为例进行说明，包括：

步骤 251、终端支付应用通过 SDK 向支付宝钱包请求身份授权码 AuthCode。
如果支付宝钱包中已有登录账户，可直接进入步骤 254，否则进入步骤 252。

步骤 252、支付宝钱包弹出用户登录界面，用户输入帐号和登陆密码向支付宝服务端请求登录。

20 步骤 253、假设用户帐号和密码正确，则登录成功，支付宝服务端生成 AuthCode 并返回给支付宝。

步骤 254、支付宝钱包将 AuthCode 通过 SDK 传给终端支付应用。

步骤 255、终端支付应用从安全存储区 TEE 中获取预置的公钥。

步骤 256、终端支付应用使用厂商相关安全隧道将公钥、终端唯一标识和
25 AuthCode 上传至终端服务端，同时以 Authcode 请求用户信息。

步骤 257、终端服务端将公钥、设备唯一标识和 AuthCode 发送给支付宝服务端。

步骤 258、支付宝服务端接收公钥、设备唯一标识和 AuthCode，验证 AuthCode 正确后，将三者进行关联安全存储，并通过终端服务端返回用户信息给终端支付应用，用户信息中包括用户账户 userID。

步骤 259、终端支付应用通过支付宝付款码 SDK 向支付宝钱包发起付款码
5 开通请求，该请求中携带有终端唯一标识。

步骤 260、支付宝钱包将请求传给支付宝服务端。

步骤 261、支付宝服务端根据上传的设备唯一标识和用户账户，将对应的公钥以及用于生成付款码的动态口令种子下发给支付宝钱包。

步骤 262、支付宝钱包以当前登录的用户 ID 为索引，对加密的公钥和动态
10 口令种子进行安全存储。

接下来从第二模块侧对本申请所提供的图形码信息提供方案进行描述，本实施例的图形码信息提供方法可应用于如图 2A 所示的第二模块中，包括如下步骤 301 至 303:

15 在步骤 301 中，通过接口模块验证第一模块是否为可信模块。

在步骤 302 中，通过接口模块接收目标用户信息，并验证所述目标用户信息是否在第二模块上处于登录状态，所述目标用户信息与所述接口模块预先关联。

在步骤 303 中，在验证第一模块为可信模块，并且所述目标用户信息在第二模块上处于登录状态后，生成图形码信息并通过所述接口模块传给所述第一模块。
20 模块。

在一个可选的实现方式中，所述通过所述接口模块验证第一模块是否为可信模块，包括：

生成会话信息并加密，将加密的会话信息通过接口模块传给第一模块；

25 通过接口模块接收第一模块返回的对所述加密的会话信息进行解密的解密结果；

根据所述解密结果验证第一模块是否为可信模块。

在一个可选的实现方式中，在加密所述会话信息时所采用的密钥为所述第一模块预先分发的公钥。

在一个可选的实现方式中，所述生成会话信息包括：随机生成会话密钥作为所述会话信息；

5 所述根据所述解密结果验证第一模块是否为可信模块，包括；

接收接口模块发送的加密的验证信息，并利用所述随机生成的会话密钥进行解密；若成功解密，确定第一模块为可信模块。

在一个可选的实现方式中，所述生成图形码信息并通过所述接口模块传给所述第一模块，包括：

10 生成图形码信息后，利用所述随机生成的会话密钥加密所述图形码信息，并将加密的图形码信息通过所述接口模块传给第一模块。

本实施例的详细描述可参考前述实施例，在此不做赘述。

接下来从接口模块侧对本申请所提供的方案进行描述，本实施例的图形码信息提供方法可应用于如图 2A 所示的接口模块中，所述方法包括 401 至 404：

15 在步骤 401 中，接收第二模块发送的加密的会话信息并传给第一模块。

在步骤 402 中，将第一模块对所述加密的会话信息进行解密的解密结果传给第二模块，以供第二模块根据所述解密结果验证第一模块是否为可信模块。

20 在步骤 403 中，将预先关联的目标用户信息发送给第二模块，以供第二模块验证所述目标用户信息是否在第二模块上处于登录状态。

在步骤 404 中，接收第二模块在验证第一模块为可信模块，并且所述目标用户信息在第二模块上处于登录状态后所生成的图形码信息，并将图形码信息传给所述第一模块。

25 在一个可选的实现方式中，所述会话信息包括随机生成的会话密钥；

所述将第一模块对所述加密的会话信息进行解密的解密结果传给第二模块，包括：

接收第一模块发送的解密得到的会话密钥，所述解密的会话密钥由第一模块在对所述加密的会话信息成功解密后所获得；

利用所述解密得到的会话密钥加密一验证信息，并将加密的验证信息传给第二模块。

5 在一个可选的实现方式中，所述利用所述解密得到的会话加密一验证信息，并将加密的验证信息传给第二模块，包括：

利用所述解密得到的会话密钥加密所述目标用户信息，并将加密后的目标用户信息作为所述加密的验证信息传给第二模块。

10 在一个可选的实现方式中，所述第二模块所生成的图形码信息为第二模块利用随机生成的会话密钥加密的图形码信息；

所述将图形码信息传给所述第一模块，包括：

接收所述加密的图形码信息，对所述加密的图形码信息解密后传给所述第一模块；其中，解密所述加密的图形码信息时所采用的密钥为所述第一模块解密得到的会话密钥。

15 本实施例的详细描述可参考前述实施例，在此不做赘述。

接下来从第一模块侧对本申请所提供的方案进行描述，本实施例的图形码信息提供方法可应用于如图 2A 所示的第一模块中，所述方法包括 501 至 503：

在步骤 501 中，通过接口模块接收第二模块发送的加密的会话信息。

20 在步骤 502 中，对所述加密的会话信息进行解密，将解密结果通过接口模块传给第二模块，以供第二模块根据所述解密结果验证所述第一模块是否为可信模块。

25 在步骤 503 中，通过接口模块接收第二模块提供的图形码信息；所述图形码信息由第二模块在验证所述第一模块为可信模块，并且验证接口模块预先关联的目标用户信息在第二模块上处于登录状态后所提供。

在一个可选的实现方式中，所述目标用户信息与所述接口模块预先通过如下方式关联：

通过接口模块向第二模块发起关联请求；

通过接口模块接收第二模块根据所述关联请求所发送的用户身份授权信息，所述用户身份授权信息在第二模块上处于登录状态；

将所述用户身份授权信息、预置在安全存储区中的公钥和预置的设备唯一标识通过所述第一模块对应的服务端发送给第二模块对应的服务端；

接收目标用户信息，并将所述目标用户信息传给接口模块，所述目标用户信息为第二模块对应的服务端在验证用户身份授权信息正确后通过第一模块对应的服务端所发送。

本实施例的详细描述可参考前述实施例，在此不做赘述。

10

与前述方法的实施例相对应，本申请还提供了图形码信息提供、图形码信息获取装置及其所应用的终端的实施例。

本申请图形码信息提供装置/图形码信息获取装置的实施例可以应用在终端设备上。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过其所在电子设备的处理器 310 将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，如图 3 所示，为本申请图形码信息提供装置/图形码信息获取装置所在终端设备的一种硬件结构图，除了图 3 所示的处理器 310、内存 330、网络接口 320、以及非易失性存储器 340 之外，实施例中装置 331 所在的终端设备通常根据该终端设备的实际功能，还可以包括其他硬件，对此不再赘述。

15

20

如图 4 所示，图 4 是本申请根据一示例性实施例示出的一种图形码信息提供装置的框图，所述图形码信息提供装置应用于包括有接口装置和第一装置的终端中，所述图形码信息提供装置包括：

25

可信验证模块 41，用于通过所述接口装置验证第一装置是否为可信装置。

用户信息验证模块 42，用于通过接口装置接收目标用户信息，并验证所

述目标用户信息是否在第二装置上处于登录状态，所述目标用户信息与所述接口装置预先关联。

信息传输模块 43，用于在验证第一装置为可信装置，并且所述目标用户信息在第二装置上处于登录状态后，生成图形码信息并通过所述接口装置传
5 给所述第一装置。

在一个可选的实现方式中，所述可信验证模块 41，包括：

会话信息加密子模块，用于生成会话信息并加密，将加密的会话信息通过接口模块传给第一模块。

解密子模块，用于通过接口模块接收第一模块返回的对所述加密的会话
10 信息进行解密的解密结果。

验证子模块，用于根据所述解密结果验证第一模块是否为可信模块。

在一个可选的实现方式中，所述会话信息加密子模块在加密所述会话信息时所采用的密钥为所述第一装置预先分发的公钥。

在一个可选的实现方式中，所述生成会话信息包括：随机生成会话密钥
15 作为所述会话信息。

所述验证子模块，还用于：接收接口模块发送的加密的验证信息，并利用所述随机生成的会话密钥进行解密；若成功解密，确定第一模块为可信模块。

在一个可选的实现方式中，所述信息传输模块 43，还用于：

20 生成图形码信息后，利用所述随机生成的会话密钥加密所述图形码信息，并将加密的图形码信息通过所述接口模块传给第一模块。

如图 5 所示，图 5 是本申请根据一示例性实施例示出的一种图形码信息提供装置的框图，所述图形码信息提供装置应用于包括有第一装置和第二装置
25 的终端中，所述图形码信息提供装置包括：

加密会话信息接收模块 51，用于接收第二装置发送的加密的会话信息并传给第一装置。

解密结果传输模块 52, 用于将第一装置对所述加密的会话信息进行解密的解密结果传给第二装置, 以供第二装置根据所述解密结果验证第一装置是否为可信装置。

5 用户信息发送模块 53, 用于将预先关联的目标用户信息发送给第二装置, 以供第二装置验证所述目标用户信息是否在第二装置上处于登录状态。

图形码信息接收模块 54, 用于接收第二装置在验证第一装置为可信装置, 并且所述目标用户信息在第二装置上处于登录状态后所生成的图形码信息, 并将图形码信息传给所述第一装置。

在一个可选的实现方式中, 所述会话信息包括随机生成的会话密钥。

10 所述解密结果传输模块 52, 包括:

会话密钥接收子模块, 用于接收第一模块发送的解密得到的会话密钥, 所述解密的会话密钥由第一模块在对所述加密的会话信息成功解密后所获得。

15 验证信息加密发送模块, 用于利用所述解密得到的会话密钥加密一验证信息, 并将加密的验证信息传给第二模块。

在一个可选的实现方式中, 所述验证信息加密发送模块, 还用于:

利用所述解密得到的会话密钥加密所述目标用户信息, 并将加密后的目标用户信息作为所述加密的验证信息传给第二模块。

20 验证信息加密发送模块, 所述第二模块所生成的图形码信息为第二模块利用随机生成的会话密钥加密的图形码信息。

所述图形码信息接收模块 54, 还用于:

接收所述加密的图形码信息, 对所述加密的图形码信息解密后传给所述第一模块; 其中, 解密所述加密的图形码信息时所采用的密钥为所述第一模块解密得到的会话密钥。

25

如图 6 所示, 图 6 是本申请根据一示例性实施例示出的一种图形码信息获取装置的框图, 所述图形码信息获取装置应用于包括有接口装置和第二装

置的终端中，所述图形码信息获取装置包括：

加密会话信息接收模块 61，用于通过接口装置接收第二装置发送的加密的会话信息。

解密模块 62，用于对所述加密的会话信息进行解密，将解密结果通过接口装置传给第二装置，以供第二装置根据所述解密结果验证所述第一装置是否为可信装置。

图形码信息接收模块 63，用于通过接口装置接收第二装置提供的图形码信息；所述图形码信息由第二装置在验证所述第一模块为可信装置，并且验证接口装置预先关联的目标用户信息在第二装置上处于登录状态后所提供。

10 在一个可选的实现方式中，所述装置还包括关联模块，所述关联模块用于：通过接口模块向第二模块发起关联请求；通过接口模块接收第二模块根据所述关联请求所发送的用户身份授权信息，所述身份信息授权信息在第二模块上处于登录状态；将所述身份信息授权信息、预置在安全存储区中的公钥和预置的设备唯一标识通过所述第一模块对应的服务端发送给第二模块对应的

15 服务端；接收目标用户信息，并将所述目标用户信息传给接口模块，所述目标用户信息为第二模块对应的服务端在验证身份信息授权信息正确后通过第一模块对应的服务端所发送。

相应的，本申请实施例还提供一种终端，所述终端包括：处理器；用于

20 存储处理器可执行指令的存储器；其中，所述处理器被配置为：

第二模块通过接口模块验证第一模块是否为可信模块。

第二模块接收目标用户信息，并验证所述目标用户信息是否在第二模块上处于登录状态，所述目标用户信息与所述接口模块预先关联。

第二模块在验证第一模块为可信模块，并且所述目标用户信息在第二模块上处于登录状态后，生成图形码信息并通过所述接口模块传给所述第一模块。

25 块。

上述装置中各个模块的功能和作用的实现过程具体详见上述方法中对应

步骤的实现过程，在此不再赘述。

对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理模块，即可以位于一个地方，或者也可以分布到多个网络模块上。可以根据实际的需要选择其中的部分或者全部模块来实现本申请方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

本领域技术人员在考虑说明书及实践这里申请的发明后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未申请的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本申请的真正范围和精神由下面的权利要求指出。

应当理解的是，本申请并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。