(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 110460609 B
(45)授权公告日 2021.12.14

(21)申请号 201910759345.8

(22)申请日 2019.08.16

(65)同一申请的已公布的文献号
申请公布号 CN 110460609 A

(43)申请公布日 2019.11.15

(73)专利权人 江苏恒宝智能系统技术有限公司
地址 210019 江苏省南京市建邺区奥体大街68号国际研发总部园4A幢8层801

(72)发明人 许传勋 李勇

(74)专利代理机构 北京卓特专利代理事务所(普通合伙) 11572
代理人 陈变花

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)

(56)对比文件
CN 105187450 A,2015.12.23
CN 109728909 A,2019.05.07
CN 105162785 A,2015.12.16
CN 106127016 A,2016.11.16
CN 102315934 A,2012.01.11

审查员 肖丽金

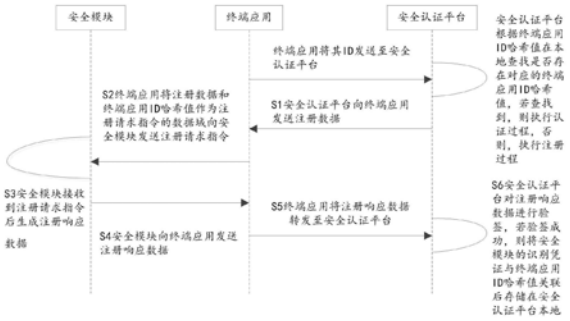
权利要求书2页 说明书6页 附图1页

(54)发明名称

终端应用与安全认证平台的双向认证方法及系统

(57)摘要

本申请提供一种终端应用与安全认证平台的双向认证方法及系统，该方法包括：判断终端应用是否已在安全认证平台注册，若是，则执行认证过程，若否，则执行注册过程；所述认证过程包括：T1，安全认证平台向终端应用发送认证数据；T2，终端应用将认证数据作为认证请求指令的数据域向安全模块发送认证请求指令；T3，安全模块接收到认证请求指令后对认证数据进行验证，验证成功后，则执行下一步；否则，验证失败；T4，安全模块向终端应用发送认证响应指令；T5，终端应用将认证响应指令的数据发送给安全认证平台，T6，安全认证平台对该数据进行验证。本申请提高了交易的安全性，实现了免密登录，交易更加方便快捷。



CN 110460609 B

1.一种终端应用与安全认证平台的双向认证方法,其特征在于,该方法包括:

判断终端应用是否已在安全认证平台注册,若是,则执行认证过程,若否,则执行注册过程;

其中,判断终端应用是否已在安全认证平台注册的方法为:终端应用向安全认证平台发送终端应用ID哈希值,安全认证平台根据终端应用ID哈希值在本地查找是否存在对应的终端应用ID哈希值,若存在,则已经注册;若否,则未注册;

所述认证过程包括:

T1,安全认证平台向终端应用发送认证数据;

所述认证数据包括安全认证平台的信息数据、终端应用ID哈希值和安全模块的识别凭证;

T2,终端应用将认证数据作为认证请求指令的数据域向安全模块发送认证请求指令;

T3,安全模块接收到认证请求指令后对认证数据进行验证,验证成功后,执行下一步;否则,验证失败;

T4,安全模块向终端应用发送认证响应指令;

T5,终端应用将认证响应指令的数据发送给安全认证平台;

T6,安全认证平台对认证响应指令的数据进行验证,若验证通过,则终端应用与安全认证平台之间相互认证通过;否则,验证失败;

其中,安全模块向终端应用发送认证响应指令包括:安全模块根据认证计数器Counter_A、终端设备的ID识别数据哈希后的结果和安全认证平台的信息数据作为ECC签名的明文数据M,生成认证响应数据域的签名,将签名和认证计数器发生至终端应用;

其中,签名(R,S)的生成方法如下:

任意选取一个随机数K=(x1,y1),R的计算公式为:R=x1 mod n,该公式表示为R的值为x1的值对n的取余运算,n表示椭圆曲线的可倍积阶数,若R=0,则重新选取一个随机数K再计算R的值;

S的计算公式为:$S=K^{-1}(E+d\cdot R)\bmod n$,其中,E表示摘要数据,E=HASH(M),即E等于M哈希运算后的结果;d为私钥,若S=0,则重新选取一个随机数K再计算S的值。

2.根据权利要求1所述的终端应用与安全认证平台的双向认证方法,其特征在于,所述注册过程包括:

S1,安全认证平台向终端应用发送注册数据;

S2,终端应用将注册数据与终端应用ID哈希值作为注册请求指令的数据域向安全模块发送注册请求指令;

S3,安全模块接收到注册请求指令后生成注册响应数据;

S4,安全模块向终端应用发送注册响应数据;

S5,终端应用将注册响应数据转发至安全认证平台;

S6,安全认证平台对注册响应数据进行验签,若验签成功,则将安全模块的识别凭证与终端应用ID哈希值关联后存储在安全认证平台本地。

3.根据权利要求2所述的终端应用与安全认证平台的双向认证方法,其特征在于,步骤T3中,安全模块接收到认证请求指令后对认证数据进行验证的方法为:将认证请求指令中的识别凭证与安全模块本地保存的安全模块识别凭证进行匹配,若匹配成功,则验证通过,

否则,验证失败。

4.根据权利要求3所述的终端应用与安全认证平台的双向认证方法,其特征在于,步骤T4中,

安全模块生成认证响应数据域的签名,其中,安全模块本地保存的且与安全模块识别凭证相关联的私钥作为认证响应数据域签名的密钥;

安全模块将其保存的认证计数器和生成的签名作为认证响应指令的数据域发送给终端应用。

5.根据权利要求4所述的终端应用与安全认证平台的双向认证方法,其特征在于,步骤T5中,终端应用将签名发送给安全认证平台;

步骤T6中,安全认证平台对签名进行验签。

6.根据权利要求2所述的终端应用与安全认证平台的双向认证方法,其特征在于,步骤S1中,注册数据为终端应用获取的随机数数据。

7.根据权利要求6所述的终端应用与安全认证平台的双向认证方法,其特征在于,步骤S3中,安全模块接收到注册请求后,采用ECC算法生成公私密钥对,根据新生成的私钥和安全认证平台的信息数据生成安全模块的识别凭证,并在本地创建认证计数器,其中,安全模块对新生成的安全模块的识别凭证、认证计数器与公私密钥对中的私钥进行关联并保存。

8.一种终端应用与安全认证平台的双向认证系统,其特征在于,包括:

安全认证平台和终端设备,所述终端设备包括终端应用和安全模块,所述终端应用分别与所述安全认证平台和所述安全模块通讯连接,

其中,终端应用向安全认证平台发送终端应用ID哈希值,安全认证平台根据终端应用ID哈希值在本地查找是否存在对应的终端应用ID哈希值,若存在,则已经注册;若否,则未注册;

所述安全认证平台用于向终端应用发送认证数据,所述认证数据包括安全认证平台的信息数据、终端应用ID哈希值和安全模块的识别凭证;

所述终端应用用于向所述安全模块发送注册请求指令或认证请求指令;

所述安全模块用于向所述终端应用发送注册请求响应数据或认证请求响应数据;

所述终端应用还用于将其接收的注册请求响应数据或认证请求响应数据转发给安全认证平台;

所述安全认证平台用于对注册请求响应数据或认证请求响应数据进行验签;

其中,安全模块向终端应用发送认证响应指令包括:安全模块根据认证计数器Counter_A、终端设备的ID识别数据哈希后的结果和安全认证平台的信息数据作为ECC签名的明文数据M,生成认证响应数据域的签名,将签名和认证计数器发生至终端应用;

其中,签名(R,S)的生成方法如下:

任意选取一个随机数K=(x1,y1),R的计算公式为:R=x1 mod n,该公式表示为R的值为x1的值对n的取余运算,n表示椭圆曲线的可倍积阶数,若R=0,则重新选取一个随机数K再计算R的值;

S的计算公式为:$S=K^{-1}(E+d\cdot R)\bmod n$,其中,E表示摘要数据,E=HASH(M),即E等于M哈希运算后的结果;d为私钥,若S=0,则重新选取一个随机数K再计算S的值。

终端应用与安全认证平台的双向认证方法及系统

技术领域

[0001] 本申请涉及安全认证技术领域，尤其涉及一种终端应用与安全认证平台的双向认证方法及系统。

背景技术

[0002] 目前，随着网络金融的普及，各种联网支付终端应用层出不穷。交易终端与安全认证平台之间的通信很多是通过公共网络进行数据传输；终端上运行的应用获取使用者私密信息，同时绑定了借记/贷记卡。因此安全模块、终端应用与安全认证平台三者之间的安全及合法性尤为重要。

[0003] 现有安全模块、终端应用与安全认证平台三方认证方式为安全认证平台对接入安全认证平台的终端应用进行身份认证，安全认证平台对通过终端应用登录的使用者验证。

[0004] 终端应用却未对安全认证平台身份的合法性进行认证；终端应用的使用者(交易的发起者)也未对安全认证平台身份的合法性进行认证。

[0005] 交易终端与安全认证平台，使用者与安全认证平台的认证关系是单向的；需要从技术上来确保安全认证平台、终端应用和使用者这三方的合法性；无法确保三方的合法性就无法实现免密登陆。

[0006] U盾等硬件认证机制过于繁琐，用户需要记忆多个密码，且密码设置较长，无法满足当前对安全快捷登录的要求。

发明内容

[0007] 本申请的目的在于提供一种终端应用与安全认证平台的双向认证方法及系统，实现了运行终端应用与安全认证平台的相互认证和免密登录终端应用的特点，使得交易更加方便快捷。

[0008] 为达到上述目的，本申请提供一种终端应用与安全认证平台的双向认证方法，该方法包括：

[0009] 判断终端应用是否已在安全认证平台注册，若是，则执行认证过程，若否，则执行注册过程；

[0010] 如上的，其中，所述认证过程包括：

[0011] T1，安全认证平台向终端应用发送认证数据；

[0012] T2，终端应用将认证数据作为认证请求指令的数据域向安全模块发送认证请求指令；

[0013] T3，安全模块接收到认证请求指令后对认证数据进行验证，验证成功后，执行下一步；否则，验证失败；

[0014] T4，安全模块向终端应用发送认证响应指令；

[0015] T5，终端应用将认证响应指令的数据发送给安全认证平台。

[0016] T6，安全认证平台对认证响应指令的数据进行验证，若验证通过，则终端应用与安

全认证平台之间相互认证通过;否则,验证失败。

[0017] 如上的,其中,所述注册过程包括:

[0018] S1,安全认证平台向终端应用发送注册数据;

[0019] S2,终端应用将注册数据和终端应用ID哈希值作为注册请求指令的数据域向安全模块发送注册请求指令;

[0020] S3,安全模块接收到注册请求指令后生成注册响应数据;

[0021] S4,安全模块向终端应用发送注册响应数据;

[0022] S5,终端应用将注册响应数据转发至安全认证平台;

[0023] S6,安全认证平台对注册响应数据进行验签,若验签成功,则将安全模块的识别凭证与终端应用I D哈希值关联后存储在安全认证平台本地。

[0024] 如上的,其中,判断终端应用是否已在安全认证平台注册的方法为:终端应用向安全认证平台发送终端应用ID,安全认证平台根据终端应用ID哈希值在本地查找是否存在对应的终端应用I D哈希值,若存在,则已经注册;若否,则未注册。

[0025] 如上的,其中,所述认证数据包括安全认证平台的信息数据、终端应用ID哈希值和安全模块的识别凭证。

[0026] 如上的,其中,步骤T3中,安全模块接收到认证请求指令后对认证数据进行验证的方法为:将认证请求指令中的识别凭证与安全模块本地保存的安全模块的识别凭证进行匹配,若匹配成功,则验证通过,否则,验证失败。

[0027] 如上的,其中,步骤T4中,安全模块生成认证响应数据域的签名,其中,安全模块本地保存的且与安全模块识别凭证相关联的私钥作为认证响应数据域签名的密钥;安全模块将其保存的认证计数器和生成的签名作为认证响应指令的数据域发送给终端应用。

[0028] 如上的,其中,步骤T5中,终端应用将签名发送给安全认证平台;步骤T6中,安全认证平台对签名进行验签。

[0029] 如上的,其中,步骤S1中,注册数据为终端应用获取的随机数数据。

[0030] 如上的,其中,步骤S3中,安全模块接收到注册请求后,采用ECC算法生成公私密钥对,根据新生成的私钥和安全认证平台的信息数据生成安全模块的识别凭证,并在本地创建认证计数器,其中,安全模块对新生成的安全模块的识别凭证、认证计数器与公私密钥对中的私钥进行关联并保存于安全模块中。

[0031] 本申请还提供一种终端应用与安全认证平台的双向认证系统,包括:

[0032] 安全认证平台和终端设备,所述终端设备包括终端应用和安全模块,所述终端应用分别与所述安全认证平台和所述安全模块通讯连接,

[0033] 所述终端应用用于向所述安全模块发送注册请求指令或认证请求指令;

[0034] 所述安全模块用于向所述终端应用发送注册请求响应数据或认证请求响应数据;

[0035] 所述终端应用还用于将其接收的注册请求响应数据或认证请求响应数据转发给安全认证平台;

[0036] 所述安全认证平台用于对注册请求响应数据或认证请求响应数据进行验签。

[0037] 本申请实现的有益效果如下:

[0038] (1)用户通过终端应用登录安全认证平台进行交易时,使运行终端应用的硬件设备与安全认证平台实现相互认证,提高交易的安全性。

[0039] (2)用户不需要记忆复杂密码,用户密码用于登录使用,弱化了交易安全对用户密码的依赖,实现用户直接免密登录终端应用。

[0040] (3)安全模块本地保存keyhandle(安全模块的识别凭证)与密钥对的私钥,安全认证平台本地保存终端应用的ID与密钥对的公钥,节省了两者的物理空间。

附图说明

[0041] 为了更清楚地说明本申请实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本申请中记载的一些实施例,对于本领域技术人员来讲,还可以根据这些附图获得其他的附图。

[0042] 图1为本发明一种终端应用与安全认证平台的双向认证方法的注册过程流程图。

[0043] 图2为本发明一种终端应用与安全认证平台的双向认证方法的认证过程流程图。

具体实施方式

[0044] 下面结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

[0045] 实施例一

[0046] 一种终端应用与安全认证平台的相互认证方法包括:判断终端应用是否已在安全认证平台注册,若是,则执行认证过程,若否,则执行注册过程。

[0047] 具体的,判断终端应用是否已在安全认证平台注册的方法为:终端应用与安全认证平台链接,并且终端应用向安全认证平台发送终端应用ID哈希值,安全认证平台根据终端应用ID哈希值在本地查找是否存在对应的终端应用ID哈希值,若存在,则已经注册,执行认证过程;若否,则未注册,安全认证平台向运行终端应用的终端设备发送注册数据(challenge注册数据),执行注册过程。

[0048] 注册过程包括如下步骤:

[0049] S1:安全认证平台向终端应用发送注册数据。

[0050] 其中,注册数据为安全认证平台生成的随机数数据(也就是challenge数据)。Challenge数据是一个数据集合,其生成方法为:安全认证平台生成随机数,安全认证平台将该随机数和安全认证平台的信数据息进行哈希后的值即为challenge数据。

[0051] 进一步的,challenge数据可以是安全认证平台生成的随机数与安全认证平台的信息数据SHA256哈希运算后的结果,哈希运算为一种加密算法,提高了信息的安全性。

[0052] S2:终端应用将注册数据和终端应用ID哈希值(application数据)作为注册请求指令的数据域向安全模块发送注册请求指令。

[0053] 注册请求的指令数据域包含安全认证平台发送到终端应用的challenge数据和终端应用的application数据(终端应用ID哈希值)。

[0054] S3,安全模块接收到注册请求后生成注册响应数据。安全模块的注册响应数据包括keyhandle(安全模块的识别凭证)、公钥和签名。

[0055] 具体的，安全模块采用ECC算法(椭圆曲线加密算法)生成公私密钥对，根据新生成密钥对私钥和安全认证平台的信息数据生成keyhandle(安全模块的识别凭证)；并且，安全模块在本地创建认证计数器Counter_A，keyhandle(安全模块的识别凭证)、认证计数器Counter_A与公私密钥对中的私钥进行关联并保存在安全模块中。

[0056] 其中，认证计数器Counter_A是一个保存于安全模块本地用于记录安全模块的识别凭证(keyhandle)认证次数的计数器，当keyhandle每用于认证一次，认证计数器的值就加1。

[0057] 其中，签名(R,S)的生成方法如下：

[0058] 安全模块用新生成公私密钥对中的私钥作为签名密钥。

[0059] application数据(终端应用ID哈希值)、challenge数据、keyhandle(安全模块的识别凭证)和密钥对的公钥作为待签名的明文数据M。其中明文数据可以为所述数据拼接后形成的待签名数据。任意选取一个随机数$K=(x_1,y_1)$，其中，R和S均为正整数。

[0060] R的计算公式为：$R=x_1 \bmod n$，该公式表示为R的值为x_1的值对n的取余运算，n表示椭圆曲线的可倍积阶数，mod表示取余运算，若R＝0，则重新选取一个随机数K再计算R的值；

[0061] S的计算公式为：$S=K^{-1}(E+d\cdot R) \bmod n$，其中，E表示摘要数据，E＝HASH(M)，即E等于M哈希运算后的结果；K^{-1}表示K的逆运算；d为ECC椭圆曲线算法生成的私钥，若S＝0，则重新选取一个随机数K再计算S的值。ECC存在的理论基础点倍积，私钥d几乎不可能被破解。

[0062] S4，安全模块向终端应用发送注册响应数据。具体的，安全模块将keyhandle(安全模块的识别凭证)、公钥和签名作为安全模块的注册响应数据发送给终端应用。

[0063] S5：终端应用将注册响应数据转发给安全认证平台。

[0064] S6：安全认证平台对注册响应数据进行验签，验签成功后，将安全模块的识别凭证与终端应用ID哈希值关联后存储在安全认证平台本地。

[0065] 具体的，将注册响应数据中的签名作为待验签数据(R,S)，(R,S)为签名的原始数据，注册响应数据中的公钥记作P_b；判断(R,S)是否属于[1,n-1]，若是，则验签成功，若否，则验签失败。

[0066] 具体的，验签过程如下：

[0067] 计算参数$w=S^{-1} \bmod n$，其中，S^{-1}表示S的逆运算；

[0068] 计算两个参数u_1和u_2：

[0069] $u_1=(E\cdot w) \bmod n$，其中，“·”表示点积运算；

[0070] $u_2=(R\cdot w) \bmod n$，其中，“·”表示点积运算；

[0071] 计算点$X=u_1\cdot G+u_2\cdot P_b=(x_1',y_1')$，其中，$P_b$为ECC椭圆曲线算法生成的公钥，$P_b$和d之间的关系为：$P_b=d\cdot G$，其中，G表示椭圆曲线生成的基点，也即所有点倍积运算的基点；如果(x_1',y_1')不是椭圆曲线上的点，则验证失败，

[0072] 若X＝0，则签名无效，计算$v=x_1' \bmod n$；若v＝R，则签名有效；否则，无效。

[0073] 安全认证平台密钥验签通过后，安全认证平台在本地创建认证请求计数器Counter_B，将安全模块的识别凭证keyhandle、认证请求计数器、公钥和终端应用ID哈希值关联并存储于安全认证平台本地。

[0074] 其中，Counter_B是一个保存于安全认证平台本地用于记录认证请求次数的计数器，每认证成功一次后，认证请求计数器加1，正常情况下，与keyhandle认证计数器的值相

等。

[0075] 认证过程包括如下步骤：

[0076] T1:安全认证平台向终端应用发送认证数据。

[0077] 认证数据包括:challenge数据、application数据(终端应用ID哈希值,也就是终端应用ID哈希运算后的结果)和keyhandle数据(安全模块的识别凭证)。

[0078] T2:终端应用向安全模块发送认证请求指令,该指令的指令数据域包含keyhandle(安全模块的识别凭证)、application数据(终端设备的ID识别数据哈希后的结果)和challenge数据;

[0079] T3:安全模块接收到认证请求指令后对认证数据进行验证,验证成功后,执行下一步,否则,验证失败。

[0080] 具体的,对认证数据进行验证包括:将认证请求指令中的keyhandle(安全模块的识别凭证)与安全保存模块本地保存的keyhandle(安全模块的识别凭证)进行匹配,若匹配成功,则验证通过,否则,验证失败。

[0081] T4,安全模块向终端应用发送认证响应指令。

[0082] 安全模块生成认证响应数据域的签名,其中,安全模块本地保存的且与安全模块识别凭证相关联的私钥作为认证响应数据域签名的密钥。具体的,将认证计数器Counter_A、application数据(终端设备的ID识别数据哈希后的结果)和challenge数据作为ECC签名的明文数据M,用与注册过程中相同的方法生成签名,安全模块将认证计数器Counter_A和签名作为认证响应指令的数据域发送至终端应用。

[0083] T5:终端应用将认证响应指令的数据发送给安全认证平台。

[0084] T6,安全认证平台对认证响应指令的数据进行验证,若验证通过,则终端应用与安全认证平台之间相互认证通过;否则,验证失败。

[0085] 具体的,终端应用将签名发送给安全认证平台;安全认证平台对签名进行验签。

[0086] 具体的,安全认证平台用与注册过程中相同的方法进行签名的验签,验签通过后将认证响应指令中的认证计数器Counter_A和与keyhandle(安全模块的识别凭证)相关联的认证请求计数器Counter_B大小进行比较,两者相同,则安全认证平台验证成功,终端应用与安全认证平台之间相互认证通过,实现终端应用安全登录和登录后两者的安全通信的功能。

[0087] KeyHandle表示:ECC算法新生成的私钥与注册请求指令数据域中的安全认证平台的challenge数据和终端应用的application数据进行SHA256哈希后的结果数据。

[0088] Application数据表示:终端ID数据SHA256哈希运算后的结果。

[0089] 实施例二

[0090] 一种终端应用与安全认证平台的双向认证系统,包括:

[0091] 安全认证平台和终端设备,所述终端设备包括终端应用和安全模块,终端应用分别与安全认证平台和安全模块通讯连接,

[0092] 终端设备为运行终端应用的硬件设备。

[0093] 终端应用用于向安全模块发送注册请求指令或认证请求指令;

[0094] 安全模块用于向终端应用发送注册请求响应数据或认证请求响应数据;安全模块具有注册、注册响应功能;安全模块根据注册信息使用SHA256哈希算法生成安全模块的识

别凭证(keyhandle),并将识别凭证与注册信息之间关联后的数据存储在安全模块本地的功能;安全模块具有根据识别凭证与待认证数据进行匹配认证的功能;安全模块具有认证响应的功能。

[0095] 安全模块支持ECC椭圆曲线算法生成公私密钥对和签名。公私密钥对包括公开密钥和私有密钥,即公钥和私钥,私钥用于签名,公钥用于验签,如果用公钥对数据进行加密,则只有用对应的私钥才能解密,如果用私钥对数据进行加密,则只有用对应的公钥才能解密。

[0096] 终端应用还用于将其接收的注册请求响应数据或认证请求响应数据转发给安全认证平台;

[0097] 安全认证平台用于对注册请求响应数据或认证请求响应数据进行验签。

[0098] 运行终端应用的硬件设备登陆安全认证平台时,安全认证平台向硬件设备发送注册信息;硬件设备生成公私密钥对,用新生成的私钥对注册信息进行签名处理,将签名后的数据发送至安全认证平台,安全认证平台获得新生成的公钥和签名,并用公钥对签名进行验签;当终端应用再次登录时,终端应用向安全认证平台发送终端应用ID等识别数据,安全认证平台根据终端应用ID查找对应安全模块的识别凭证(keyhandle),并向终端硬件设备发送验证请求,硬件设备对请求数据进行匹配,并作签名响应;安全认证平台用本地保存的公钥对响应中的签名进行验签,验签成功后,安全模块、终端应用与安全认证平台三者认证完成。

[0099] 本申请实现的有益效果如下:

[0100] (1)用户通过终端应用登录安全认证平台进行交易时,使运行终端应用的硬件设备与安全认证平台实现相互认证,提高交易的安全性。

[0101] (2)用户不需要记忆复杂密码,用户密码用于登录使用,弱化了交易安全对用户密码的依赖,实现用户直接免密登录终端应用。

[0102] (3)安全模块本地保存keyhandle(安全模块的识别凭证)与密钥对的私钥,安全认证平台本地保存终端应用的ID与密钥对的公钥,节省了两者的物理空间。

[0103] 以上对本发明的一个实施例进行了详细说明,但内容仅为本发明的较佳实施例,不能被认为用于限定本发明的实施范围。凡依本发明申请范围所作的均等变化与改进等,均应归属于本发明的专利涵盖范围之内。

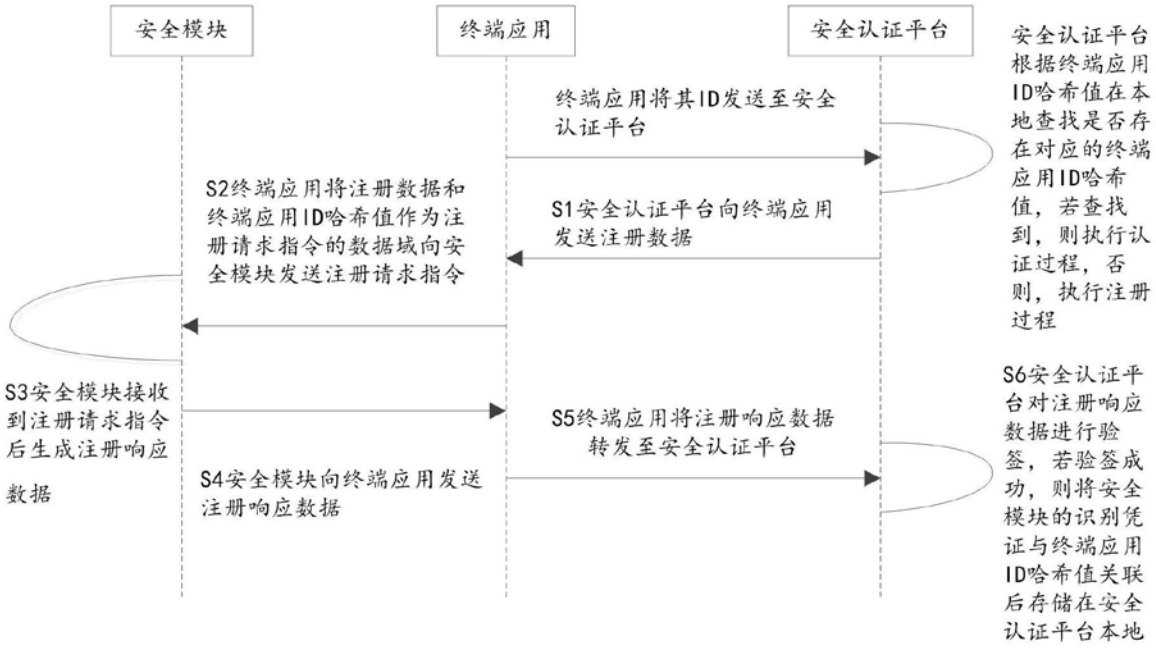

安全模块
终端应用
安全认证平台
终端应用将其ID发送至安全认证平台
安全认证平台根据终端应用ID哈希值在本地查找是否存在对应的终端应用ID哈希值，若查找到，则执行认证过程，否则，执行注册过程
S2终端应用将注册数据和终端应用ID哈希值作为注册请求指令的数据域向安全模块发送注册请求指令
S1安全认证平台向终端应用发送注册数据
S3安全模块接收到注册请求指令后生成注册响应数据
S5终端应用将注册响应数据转发至安全认证平台
S6安全认证平台对注册响应数据进行验签，若验签成功，则将安全模块的识别凭证与终端应用ID哈希值关联后存储在安全认证平台本地
S4安全模块向终端应用发送注册响应数据

图1

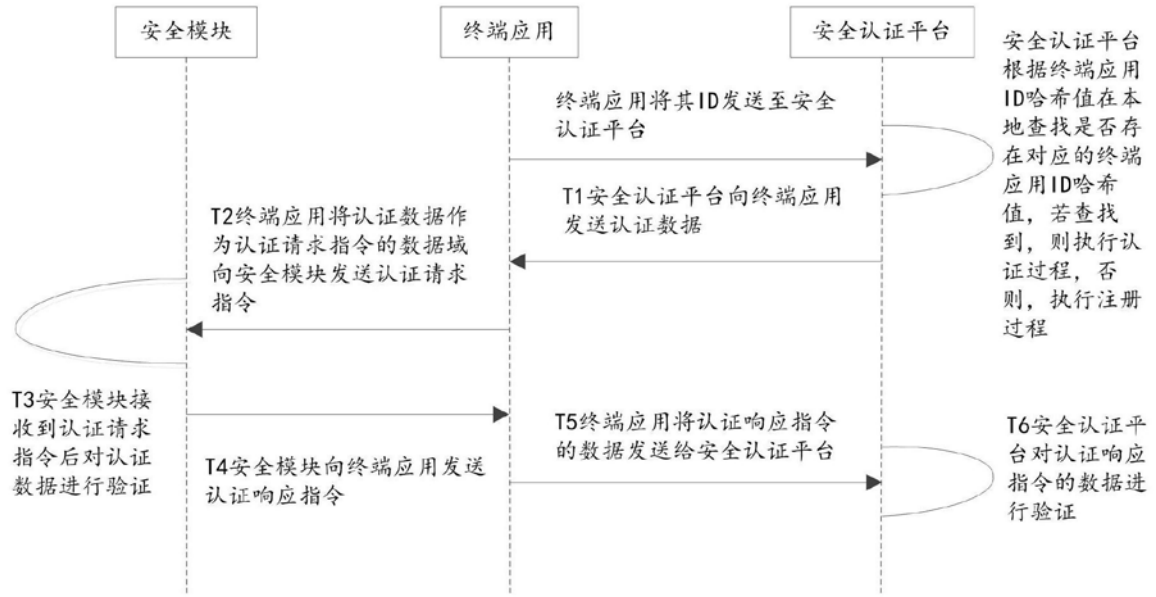

安全模块
终端应用
安全认证平台
终端应用将其ID发送至安全认证平台
安全认证平台根据终端应用ID哈希值在本地查找是否存在对应的终端应用ID哈希值，若查找到，则执行认证过程，否则，执行注册过程
T1安全认证平台向终端应用发送认证数据
T2终端应用将认证数据作为认证请求指令的数据域向安全模块发送认证请求指令
T3安全模块接收到认证请求指令后对认证数据进行验证
T5终端应用将认证响应指令的数据发送给安全认证平台
T6安全认证平台对认证响应指令的数据进行验证
T4安全模块向终端应用发送认证响应指令

图2