(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 103281186 B
(45)授权公告日 2016.02.03

(21)申请号 201310168241.2
(22)申请日 2013.05.08
(73)专利权人 上海众人网络安全技术有限公司
地址 201821 上海市嘉定区叶城路1411号4幢211室
(72)发明人 谈剑锋 丁震宇 李海宏
(74)专利代理机构 上海硕力知识产权代理事务所 31251
代理人 王建国
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)
G06F 21/31(2013.01)

审查员 汪三骏

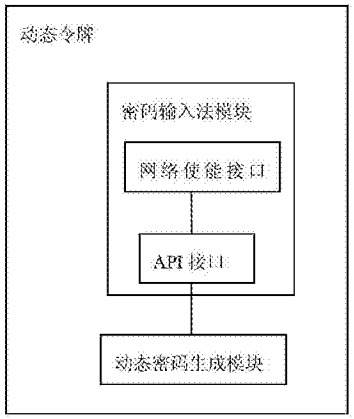
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种基于android系统的动态令牌、交易系统及方法

(57)摘要

本发明实施例提供了一种基于android系统的动态令牌，用圆圈技术领域，包括：密码输入法模块，安装于所述android系统中，包含认证服务器中唯一的ID号，当用户需要调用动态密码生成模块时，所述密码输入法模块被选择调用；动态密码生成模块，用来接收用户通过所述密码输入法模块输入的挑战摘要信息，生成动态密码。本发明实施例通过将动态密码技术集成到系统输入法之中，用户可以利用手上的终端直接在当前APP界面下调出动态密码界面，极大的方便了用户，使用户不必要调用多个界面，另外，终端直接与应用服务器通信，降低了认证服务器和终端的复杂度，输入法ID号与动态令牌唯一绑定，为认证服务器所识别，因而安全性很高。



CN 103281186 B

1.一种基于 android 系统的动态令牌,其特征在于,所述动态令牌包括 :

密码输入法模块 , 安装于所述 android 系统中 , 包含认证服务器中唯一的 ID 号 , 当用户需要调用动态密码生成模块时 , 所述密码输入法模块被选择调用 ;

动态密码生成模块,用来接收用户通过所述密码输入法模块输入的挑战摘要信息,根据输入法内置的唯一密钥生成动态密码 ;

所述密码输入法模块具体包括 :

网络使能接口,用来初始化密码输入法 , 生成唯一密钥,并当用户需要调用动态密码生成模块时,使能与应用服务器的网络连接,所述 ID 号用来唯一识别所述动态令牌的密码输入 ;

API 接口,用来提供输入法的系统调用接口,并提供输入法界面。

2.如权利要求 1 所述的基于 android 系统的动态令牌,其特征在于,

所述输入法界面包含一按键或内置输入法选择识别码,当所述按键被选择或输入法选择识别码被匹配时,提供用来生成动态密码的挑战摘要信息的输入框。

3.一种交易系统,其特征在于,所述交易系统包括 :

动态令牌,所述动态令牌集成于基于 android 系统的终端中,用来提供密码输入法模块,使用户输入挑战摘要信息,生成动态密码一,其中所述动态密码一连同帐户信息、密码输入法模块的 ID 号和交易信息被所述终端发送至应用服务器 ;

所述应用服务器,用来对所述帐户信息进行常规认证,若通过,则将所述交易信息、ID 号和所述动态密码一转发至认证服务器中 ;

所述认证服务器,用来根据所述交易信息提取挑战摘要信息,并根据所述密码输入法模块的 ID 号查找对应密钥,计算得到动态密码二,并将动态密码一和动态密码二进行对比认证,返回认证结果到应用服务器 ;

所述应用服务器接收所述认证结果,进行交易并返回交易结果给所述终端。

4.如权利要求 3 所述的交易系统,其特征在于,所述动态令牌具体包括 :

密码输入法模块 , 安装于所述 android 系统中 , 包含认证服务器中唯一的 ID 号 , 当用户需要调用动态密码生成模块时 , 所述密码输入法模块被选择调用 ;

动态密码生成模块,用来接收用户通过所述密码输入法模块输入的挑战摘要信息,生成动态密码。

5.如权利要求 4 所述的交易系统,其特征在于,所述密码输入法模块具体包括 :

网络使能接口,用来初始化密码输入法 , 生成唯一密钥,并当用户需要调用动态密码生成模块时,使能与应用服务器的网络连接,所述 ID 号用来唯一识别所述动态令牌的密码输入 ;

API 接口,用来提供输入法的系统调用接口,并提供输入法界面。

6.一种交易方法,其特征在于,所述交易方法包括如下步骤 :

用户利用密码输入法模块输入挑战摘要信息,动态密码生成模块根据所述挑战摘要信息生成动态密码一,其中所述动态密码一连同帐户信息、密码输入法模块的 ID 号和交易信息被终端发送至应用服务器 ;

所述应用服务器对所述帐户信息进行常规认证,若通过,则将所述交易信息、ID 号和所述动态密码一转发至认证服务器中 ;

所述认证服务器根据所述交易信息提取挑战摘要信息，并根据所述密码输入法模块的ID号查找对应密钥，计算得到动态密码二；

将动态密码一和动态密码二进行对比认证，返回认证结果到应用服务器；

所述应用服务器接收所述认证结果，进行交易并返回交易结果给所述终端。

一种基于 android 系统的动态令牌、交易系统及方法

技术领域

[0001] 本发明涉及安全技术领域，尤其涉及一种基于 android 系统的动态令牌、交易系统及方法。

背景技术

[0002] 动态口令，即根据特定的算法生成一个不可预测和难以破解的随机认证字符串密码，且每个生成的密码只能一次使用有效，并被限定认证的有效时间区间，因而可以用来确认用户身份的合法性，从而使得在用户身份合法的基础上保障业务使用的合法性，被广泛应用于应用、证券以及第三方支付、大型企业的 OA 系统中。用来生成所述动态口令的动态令牌又即动态令牌通常为用户终端、应用系统终端或企业终端。

[0003] 特别地，个人用户在其日常生活中，通过个人电脑或手机完成水电煤缴费、购物等支付行为已不再是新鲜事儿。各大应用为保障支付过程的安全，纷纷推出了动态令牌等产品。通常，用户在动态令牌上输入交易信息（如交易金额、交易账号等）后，获得一组动态口令，再将该组口令提交至应用服务器及认证后台，完成对此次交易真伪的认证。由于动态口令与传统的口令登录方式几乎无异，故在网上应用、手机应用、电话应用等多种交易渠道得到了广泛应用。

[0004] 目前，android 系统在终端中得到非常广泛的应用，动态密码技术也应用到了手机终端等 APP 领域。这样，很多 APP 开始使用动态密码来加强自身的安全性；另一方面，各厂商也推出了自己对应的 APP 动态密码令牌。但是 Android 系统特性约定了其当前界面只可显示一个 APP 应用界面，当使用手机等移动终端上的动态令牌时，需要关闭当前 APP 应用界面，再开启动态密码 APP，然后回到初始 APP，输入动态密码，这就导致了基于 android 系统的移动终端使用动态密码 APP 很不方便。

发明内容

[0005] 为了保证交易的安全性，又尽可能地提高用户使用基于 android 系统的终端动态令牌的便利性，本发明实施例提供了一种基于 android 系统的动态令牌、交易系统及方法。

[0006] 为了实现前述发明目的，本发明实施例提供了一种基于 android 系统的动态令牌，所述动态令牌包括：

[0007] 密码输入法模块，安装于所述 android 系统中，包含认证服务器中唯一的 ID 号，当用户需要调用动态密码生成模块时，所述密码输入法模块被选择调用；

[0008] 动态密码生成模块，用来接收用户通过所述密码输入法模块输入的挑战摘要信息，生成动态密码。

[0009] 进一步地，所述密码输入法模块包括：

[0010] 网络使能接口，用来初始化输入法，生成唯一密钥，并当用户需要调用动态密码生成模块时，使能与应用服务器的网络连接，所述 ID 号用来唯一识别所述动态令牌的密码输入；

[0011] API 接口，用来提供输入法的系统调用接口，并提供输入法界面。

[0012] 进一步地，所述输入法的界面包含一按键或内置输入法选择识别码 (android 系统层的 inputmethod() 方法)，当所述按键被选择或输入法选择识别码被匹配时，提供用来生成动态密码的挑战摘要信息的输入框。

[0013] 为了实现前述发明目的，本发明实施例还提供了一种交易系统，所述交易系统是通过以下的技术方案实现的：

[0014] 动态令牌，所述动态令牌集成于基于 android 系统的终端中，用来提供密码输入法模块，使用户输入挑战摘要信息，生成动态密码一，其中所述动态密码一连同帐户信息、密码输入法模块的 ID 号和交易信息被所述终端发送至应用服务器；

[0015] 所述应用服务器，用来对所述帐户信息进行常规认证，若通过，则将所述交易信息、ID 号和所述动态密码一转发至认证服务器中；

[0016] 所述认证服务器，用来根据所述交易信息提取挑战摘要信息，并根据所述密码输入法模块的 ID 号查找对应密钥，计算得到动态密码二，并将动态密码一和动态密码二进行对比认证，返回认证结果到应用服务器；

[0017] 所述应用服务器接收所述认证结果，进行交易并返回交易结果给所述终端。

[0018] 为了实现前述发明目的，本发明实施例还提供了一种交易方法，所述交易方法是通过以下的技术方案实现的：

[0019] 用户利用密码输入法模块输入挑战摘要信息，动态密码生成模块根据所述挑战摘要信息生成动态密码一，其中所述动态密码一连同帐户信息、密码输入法模块的 ID 号和交易信息被所述终端发送至应用服务器；

[0020] 所述应用服务器对所述帐户信息进行常规认证，若通过，则将所述交易信息、ID 号和所述动态密码一转发至认证服务器中；

[0021] 所述认证服务器根据所述交易信息提取挑战摘要信息，并根据所述密码输入法模块的 ID 号查找对应密钥，计算得到动态密码二；

[0022] 将动态密码一和动态密码二进行对比认证，返回认证结果到应用服务器；

[0023] 所述应用服务器接收所述认证结果，进行交易并返回交易结果给所述终端。

[0024] 本发明实施例提供一种新的基于 android 系统的动态令牌、交易系统和方法，通过将动态密码技术集成到系统输入法之中，用户可以利用手上的终端直接在当前 APP 界面下调出动态密码界面，极大的方便了用户，使用户不必要调用多个界面，也可推动动态口令技术的进一步推广。其中，在动态密码认证系统中，终端直接与应用服务器通信，无须与认证服务器通信，降低了认证服务器和终端的复杂度，且动态密码的输入法 ID 号与动态令牌唯一绑定，由应用服务器传递到认证服务器，为认证服务器所识别，因而安全性很高。

附图说明

[0025] 下面结合附图和实施例对本发明进一步说明：

[0026] 图 1 为本发明实施例 1 动态令牌的组成示意图；

[0027] 图 2 为本发明实施例 2 交易系统的组成示意图；

[0028] 图 3 为本发明实施例 3 交易方法的流程示意图。

具体实施方式

[0029] 在传统基于 android 系统的动态令牌的使用过程中，用户在输入交易信息及动态挑战码时，需要调用多个 APP 界面，导致使用的不便利，本发明实施例提供一种新的基于 android 系统的动态令牌。如图 1 所示，本发明实施例 1 提供了一种基于 android 系统的动态令牌，所述动态令牌包括：

[0030] 密码输入法模块，安装于所述 android 系统中，包含认证服务器中唯一的 ID 号，当用户需要调用动态密码生成模块时，所述密码输入法模块被选择调用；

[0031] 动态密码生成模块，用来接收用户通过所述密码输入法模块输入的挑战摘要信息，生成动态密码。

[0032] 其中，所述密码输入法模块包括：

[0033] 网络使能接口，用来初始化输入法，生成唯一密钥，并当用户需要调用动态密码生成模块时，使能与应用服务器的网络连接，所述 ID 号用来唯一识别所述动态令牌的密码输入；

[0034] API 接口，用来提供输入法的系统调用接口，并提供输入法的界面。

[0035] 进一步地，所述输入法的界面包含一按键或内置输入法选择识别码 (ANDROID 系统层的 inputmethod() 方法)，当所述按键被选择或输入法选择识别码匹配时，提供用来生成动态密码的挑战摘要信息的输入框。

[0036] 其中，用户手持终端，终端包含有动态令牌，所述动态令牌的密码输入法模块和动态密码生成模块一起集成于终端中，密码输入法模块用来接收用户输入的挑战摘要信息，并不需要特定的应用界面，而直接以输入法集成的形式提供输入法界面，供用户输入，当用户输入并确认输入完成后，动态密码生成模块被调用，生成需要认证的动态密码一。

[0037] 本发明实施例通过将动态密码技术集成到系统输入法之中，用户可以直接在当前 APP 界面下调出动态密码界面，极大的方便了用户，使用户不必要调用多个界面，也可推动动态口令技术的进一步推广。其中，动态密码界面的输入与动态令牌唯一绑定，为认证服务器所识别，因而安全性很高。

[0038] 为了实现本发明的发明目的，本发明实施例还提供了一种交易系统，所述系统包括：

[0039] 动态令牌，所述动态令牌集成于基于 android 系统的终端中，用来提供密码输入法模块，使用户输入挑战摘要信息，生成动态密码一，其中所述动态密码一连同帐户信息、密码输入法模块的 ID 号和交易信息被所述终端发送至应用服务器；

[0040] 所述应用服务器，用来对所述帐户信息进行常规认证，若通过，则将所述交易信息、ID 号和所述动态密码一转发至认证服务器中；

[0041] 所述认证服务器，用来根据所述交易信息提取挑战摘要信息，并根据所述密码输入法模块的 ID 号查找对应密钥，计算得到动态密码二，并将动态密码一和动态密码二进行对比认证，返回认证结果到应用服务器；

[0042] 所述应用服务器接收所述认证结果，进行交易并返回交易结果给所述终端。

[0043] 如图 2 所示，为本发明实施例基于动态密码的交易系统的组成及交易数据流程，其中，IKEY 服务器为动态密码认证服务器，数据 1、2、3、4 分别可示例如下：

[0044] 数据 1：交易信息 + 信用卡帐户信息 + 动态密码 + 输入法 ID 串号；

[0045] 数据 2 :交易信息 + 动态密码 + 输入法 ID 串号 ;

[0046] 数据 3 :交易签名认证结果 ;

[0047] 数据 4 :用户交易结果。

[0048] 本发明实施例通过将动态密码技术集成到系统输入法之中,用户可以利用手上的终端直接在当前 APP 界面下调出动态密码界面,极大的方便了用户,使用户不必要调用多个界面,也可推动动态口令技术的进一步推广。其中,在动态密码认证系统中,终端直接与应用服务器通信,无须与认证服务器通信,降低了认证服务器和终端的复杂度,且动态密码界面的输入 ID 号与动态令牌唯一绑定,由应用服务器传递到认证服务器,为认证服务器所识别,因而安全性很高。

[0049] 如图 3 所示,为了实现本发明的发明目的,本发明实施例还提供了一种交易方法,所述方法包括 :

[0050] S101. 用户利用密码输入法模块输入挑战摘要信息,动态密码生成模块根据所述挑战摘要信息生成动态密码一,其中所述动态密码一连同帐户信息、密码输入法模块的 ID 号和交易信息被所述终端发送至应用服务器 ;

[0051] S102. 所述应用服务器对所述帐户信息进行常规认证,若通过,则将所述交易信息、ID 号和所述动态密码一转发至认证服务器中 ;

[0052] S103. 所述认证服务器根据所述交易信息提取挑战摘要信息,并根据所述密码输入法模块的 ID 号查找对应密钥,计算得到动态密码二 ;

[0053] S104. 将动态密码一和动态密码二进行对比认证,返回认证结果到应用服务器 ;

[0054] S105. 所述应用服务器接收所述认证结果,进行交易并返回交易结果给所述终端。

[0055] 其中,用户手持终端,终端包含有动态令牌,所述动态令牌的密码输入法模块和动态密码生成模块一起集成于终端中,密码输入法模块用来接收用户输入的挑战摘要信息,并不需要特定的应用界面,而直接以输入法集成的形式提供输入法界面,供用户输入,当用户输入后确认书输入完成后,动态密码生成模块被调用,生成需要认证的动态密码一。

[0056] 本发明实施例通过将动态密码技术集成到系统输入法之中,用户可以利用手上的终端直接在当前 APP 界面下调出动态密码界面,极大的方便了用户,使用户不必要调用多个界面,也可推动动态口令技术的进一步推广。其中,在动态密码认证系统中,终端直接与应用服务器通信,无须与认证服务器通信,降低了认证服务器和终端的复杂度,且动态密码界面的输入 ID 号与动态令牌唯一绑定,由应用服务器传递到认证服务器,为认证服务器所识别,因而安全性很高。

[0057] 本领域技术人员应该认识到,上述的具体实施方式只是示例性的,是为了使本领域技术人员能够更好的理解本专利内容,不应理解为是对本专利保护范围的限制,只要是根据本专利所揭示精神所作的任何等同变更或修饰,均落入本专利保护范围。

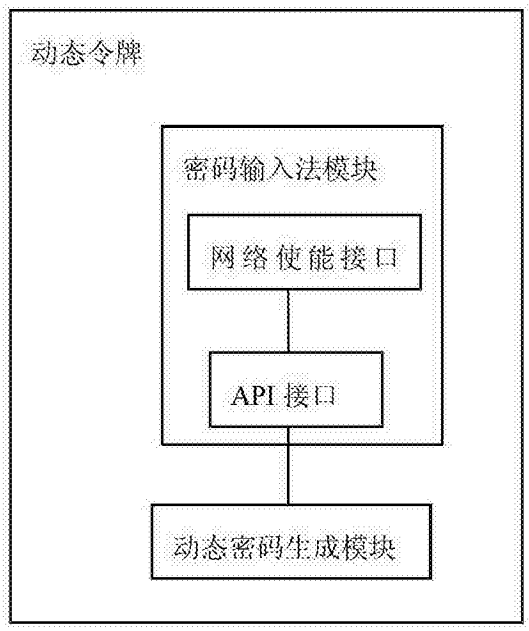

动态令牌
密码输入法模块
网络使能接口
API 接口
动态密码生成模块

图 1

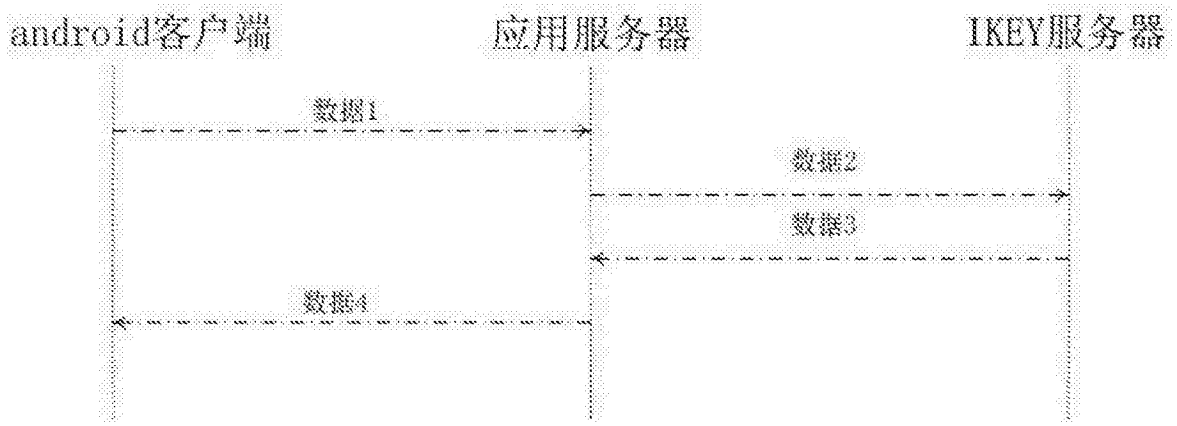

android客户端
应用服务器
IKEY服务器
数据1
数据2
数据3
数据4

图 2

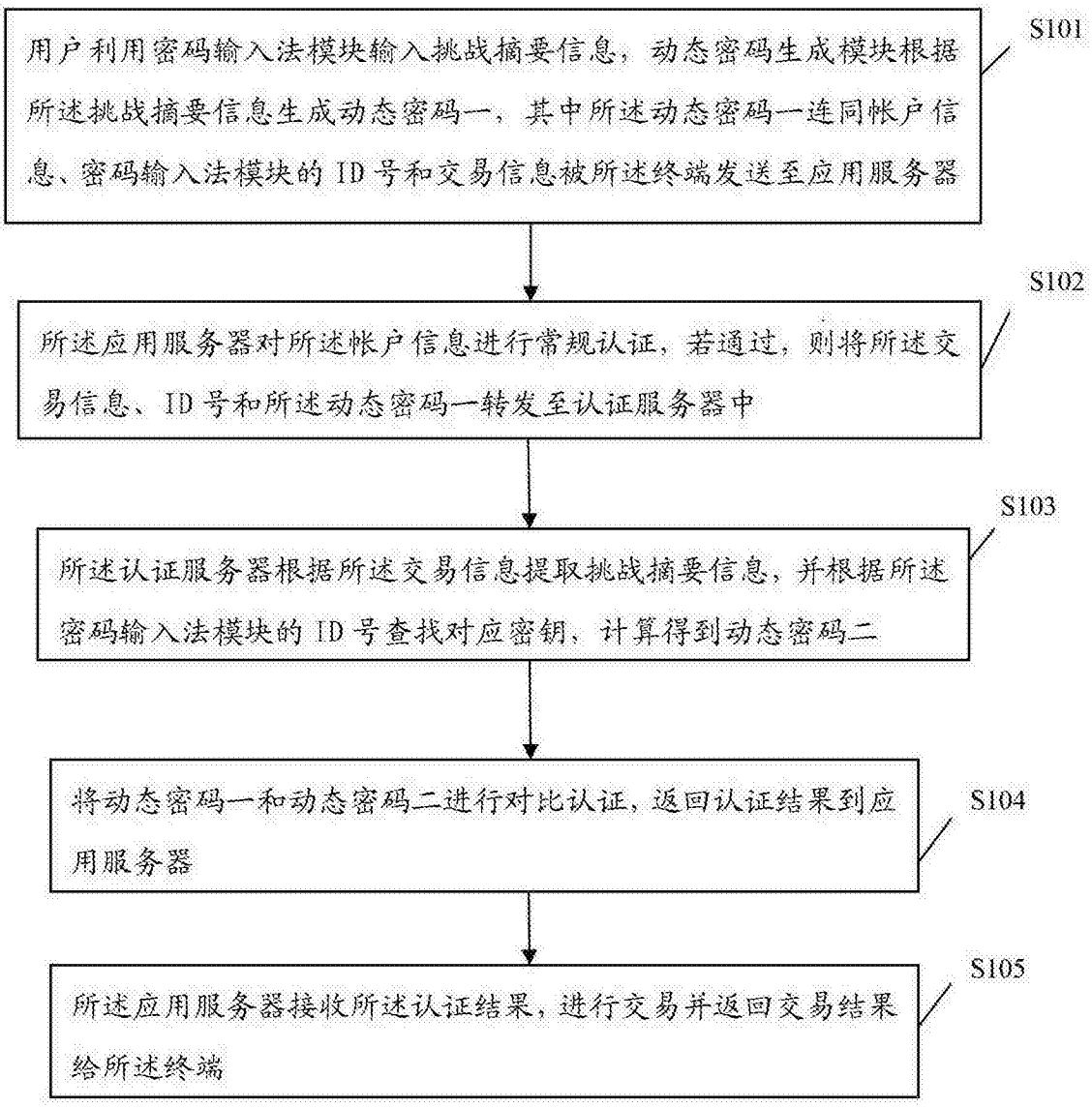

用户利用密码输入法模块输入挑战摘要信息，动态密码生成模块根据所述挑战摘要信息生成动态密码一，其中所述动态密码一连同帐户信息、密码输入法模块的 ID 号和交易信息被所述终端发送至应用服务器
S101
所述应用服务器对所述帐户信息进行常规认证，若通过，则将所述交易信息、ID 号和所述动态密码一转发至认证服务器中
S102
所述认证服务器根据所述交易信息提取挑战摘要信息，并根据所述密码输入法模块的 ID 号查找对应密钥，计算得到动态密码二
S103
将动态密码一和动态密码二进行对比认证，返回认证结果到应用服务器
S104
所述应用服务器接收所述认证结果，进行交易并返回交易结果给所述终端
S105

图 3