

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(43) 国际公布日
2014 年 7 月 17 日 (17.07.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/107977 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2013/084117
- (22) 国际申请日: 2013 年 9 月 24 日 (24.09.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201310009435.8 2013 年 1 月 10 日 (10.01.2013) CN
- (71) 申请人: 天地融科技股份有限公司 (TENDYRON CORPORATION) [CN/CN]; 中国北京市海淀区学清路 38 号 B 座 1810, Beijing 100083 (CN)。
- (72) 发明人: 李东声 (LI, Dongsheng); 中国北京市海淀区学清路 38 号 B 座 1810, Beijing 100083 (CN)。
- (74) 代理人: 北京清亦华知识产权代理事务所 (普通合伙) (TSINGYIHUA INTELLECTUAL PROPERTY LLC); 中国北京市海淀区清华园清华大学照澜院商业楼 301 室, Beijing 100084 (CN)。

- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(54) Title: KEY PROTECTION METHOD AND SYSTEM

(54) 发明名称: 密钥保护方法和系统

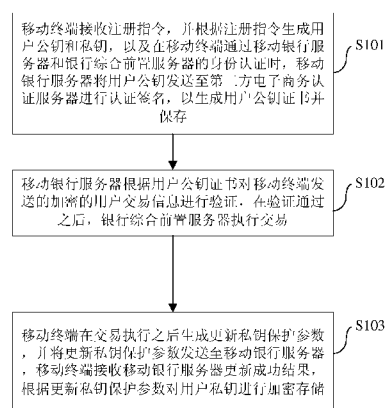


图 1 / FIG.1

S101 A mobile terminal receiving a registration instruction and generating a user public key and private key according to the registration instruction, and when the mobile terminal passes identity authentication of a mobile bank server and a bank integration front server, the mobile bank server sending the user public key to a third-party electronic commerce authentication server to perform an authentication signature so as to generate a user public key certificate, and storing same

S102 The mobile bank server verifying encrypted user transaction information sent by the mobile terminal according to the user public key certificate, and after the verification is passed, the bank integration front server executing a transaction

S103 The mobile terminal generating an updating private key protection parameter after the transaction is executed, and sending the updating private key protection parameter to the mobile bank server, and the mobile terminal receiving an updating success result of the mobile bank server, and encrypting and storing the user private key according to the updating private key protection parameter

(57) Abstract: Proposed are a key protection method and system. The method comprises: a mobile terminal receiving a registration instruction and generating a user public key and private key according to the registration instruction, and when the mobile terminal passes identity authentication of a mobile bank server and a bank integration front server, the mobile bank server sending the user public key to a third-party electronic commerce authentication server to perform an authentication signature so as to generate a user public key certificate, and storing same; the mobile bank server verifying encrypted user transaction information sent by the mobile terminal according to the user public key certificate, and after the verification is passed, the bank integration front server executing a transaction; and the mobile terminal generating an updating private key protection parameter after the transaction is executed, and sending the updating private key protection parameter to the mobile bank server, and the mobile terminal receiving an updating success result of the mobile bank server, and encrypting and storing the user private key according to the updating private key protection parameter. The present invention can increase the difficulty of an attack, and improve security.

(57) 摘要:

[见续页]

WO 2014/107977 A1

本发明提出一种密钥保护方法和系统，该方法包括：移动终端接收注册指令，并根据注册指令生成用户公钥和私钥，以及在移动终端通过移动银行服务器和银行综合前置服务器的身份认证时，移动银行服务器将用户公钥发送至第三方电子商务认证服务器进行认证签名，以生成用户公钥证书并保存；移动银行服务器根据用户公钥证书对移动终端发送的加密的用户交易信息进行验证，在验证通过之后，银行综合前置服务器执行交易；移动终端在交易执行之后生成更新私钥保护参数，并将更新私钥保护参数发送至移动银行服务器，移动终端接收移动银行服务器更新成功结果，根据更新私钥保护参数对用户私钥进行加密存储。根据本发明可增加攻击的难度，提高安全性。