

(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
2015 年 10 月 29 日 (29.10.2015)



(10) 国际公布号
WO 2015/161699 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2015/072057
- (22) 国际申请日: 2015 年 1 月 30 日 (30.01.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410172028.3 2014 年 4 月 25 日 (25.04.2014) CN
201410171785.9 2014 年 4 月 25 日 (25.04.2014) 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)。

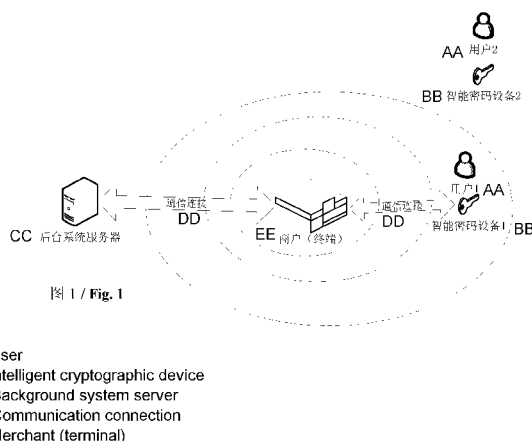
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, 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, ST, 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: SECURE DATA INTERACTION METHOD AND SYSTEM

(54) 发明名称: 数据安全交互方法和系统



(57) Abstract: Provided are a secure data interaction method and system, the method comprising: a terminal scans an intelligent cryptographic device within signal coverage, and acquires the identifier information of the scanned intelligent cryptographic device; the terminal and a background system server authenticate each other, and/or the terminal and the intelligent cryptographic device authenticate each other; the terminal acquires user information corresponding to the intelligent cryptographic device according to the identifier information of the scanned intelligent cryptographic device; and the terminal stores the user information in a pre-established current user list. Thus, the present invention constructs a method system of mutually authenticating the background system server, the terminal and the intelligent cryptographic device, and establishes security channels therebetween to prevent phishing risks and transaction risks such as transaction information tampering, remote hijacking and middle-man attacks, thus effectively ensuring fund security of a user possessing the intelligent cryptographic device and a merchant possessing the terminal.

(57) 摘要:

[见续页]

WO 2015/161699 A1



本发明提供一种数据安全交互方法和系统，其中所述方法包括：终端在信号覆盖范围内扫描智能密码设备，并获得扫描到的智能密码设备的标识信息；终端与后台系统服务器进行相互认证，和/或终端与智能密码设备进行相互认证；终端根据扫描到的智能密码设备的标识信息获取智能密码设备对应的用户信息；终端将用户信息存储到预先建立的当前用户列表中。由此，可以构建后台系统服务器、终端、智能密码设备三者之间进行相互认证的方法体系，建立三者之间的安全通道，防范钓鱼风险，防止交易信息篡改、远程劫持和中间人攻击等交易风险，从而有效保障持有智能密码设备的用户与持有终端的商户的账户资金安全。