

(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
2022 年 8 月 18 日 (18.08.2022)



(10) 国际公布号
WO 2022/170966 A1

(51) 国际专利分类号:
G06F 9/445 (2018.01)

(21) 国际申请号: PCT/CN2022/073725

(22) 国际申请日: 2022 年 1 月 25 日 (25.01.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110176522.7 2021 年 2 月 9 日 (09.02.2021) CN

(71) 申请人: 支付宝 (杭州) 信息技术有限公司 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(72) 发明人: 张煜龙 (ZHANG, Yulong); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。 韦韬 (WEI, Tao); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,

(54) Title: METHOD AND APPARATUS FOR LAUNCHING APPLICATION PROGRAM ON TARGET PLATFORM

(54) 发明名称: 在目标平台上启动应用程序的方法及装置

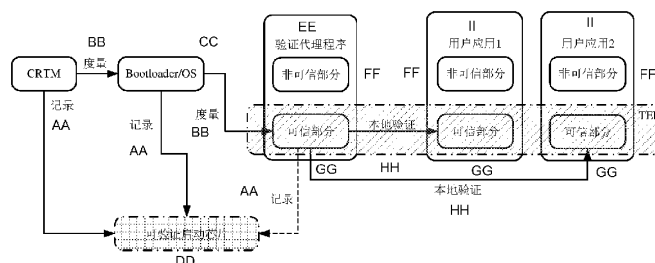


图 1

AA Record
BB Measure
CC Bootloader/OS
DD Attestable launching chip
EE Attestation agent program
FF Untrusted logic
GG Trusted logic
HH Local attestation
II User application

(57) Abstract: The embodiments of the description provide a method and an apparatus for launching an application program on a target platform. The target platform at least comprises an attestable launching chip and a trusted execution environment. Said method comprises: launching a plurality of system launching items in sequence according to a preset launching sequence, wherein the launching of a first launching item included in the plurality of system launching items comprises measuring a next launching item thereof, and recording the measurement result in an attestable launching chip; launching an attestation agent program on the basis of a trusted execution environment; and launching a first user application program on the basis of the trusted execution environment, and the attestation agent program determining first attestation information corresponding to the first user application program on the basis of local attestation in the trusted execution environment.

[见续页]

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,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, WS, 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))。

(57) 摘要: 说明书实施例提供了一种在目标平台上启动应用程序的方法及装置, 目标平台至少包含可验证启动芯片和可信执行环境, 该方法包括: 按预设的启动次序依次启动多个系统启动项, 其中, 对于多个系统启动项中包含的第一启动项的启动包括, 对于其下一个启动项进行度量, 并将度量结果记录到可验证启动芯片中; 基于可信执行环境启动验证代理程序; 基于可信执行环境启动第一用户应用程序, 并由验证代理程序基于可信执行环境中的本地验证, 确定第一用户应用程序对应的第一验证信息。