(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 11 月 20 日 (20.11.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/183392 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01) *H04L 9/14* (2006.01)

(21) 国际申请号: PCT/CN2013/086753

(22) 国际申请日: 2013 年 11 月 8 日 (08.11.2013)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310177428.9 2013 年 5 月 14 日 (14.05.2013) CN

(71) 申请人: **北大方正集团有限公司 (PEKING UNIVERSITY FOUNDER GROUP CO., LTD.)** [CN/CN]; 中国北京市海淀区成府路 298 号, Beijing 100871 (CN)。 **北京大学 (PEKING UNIVERSITY)** [CN/CN]; 中国北京市海淀区颐和园路 5 号, Beijing 100871 (CN)。 **北京北大方正电子有限公司 (BEIJING FOUNDER ELECTRONICS CO., LTD.)** [CN/CN]; 中国北京市海淀区上地五街 9 号方正大厦, Beijing 100085 (CN)。

(72) 发明人: **荆艳影 (JING, Yanying)**; 中国北京市海淀区上地五街 9 号方正大厦, Beijing 100085 (CN)。 **杨建武 (YANG, Jianwu)**; 中国北京市海淀区上地五街 9 号方正大厦, Beijing 100085 (CN)。 **于晓明 (YU, Xiaoming)**; 中国北京市海淀区上地五街 9 号方正大厦, Beijing 100085 (CN)。 **张丹 (ZHANG, Dan)**; 中国北京市海淀区上地五街 9 号方正大厦, Beijing 100085 (CN)。

(74) 代理人: **中国国际贸易促进委员会专利商标事务所 (CCPIT PATENT AND TRADEMARK LAW OFFICE)**; 中国北京市西城区阜成门外大街 2 号万通新世界广场 8 层, Beijing 100037 (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, 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,

[见续页]

(54) Title: SECURE COMMUNICATION AUTHENTICATION METHOD AND SYSTEM IN DISTRIBUTED ENVIRONMENT

(54) 发明名称 : 分布式环境下的安全通信认证方法及系统

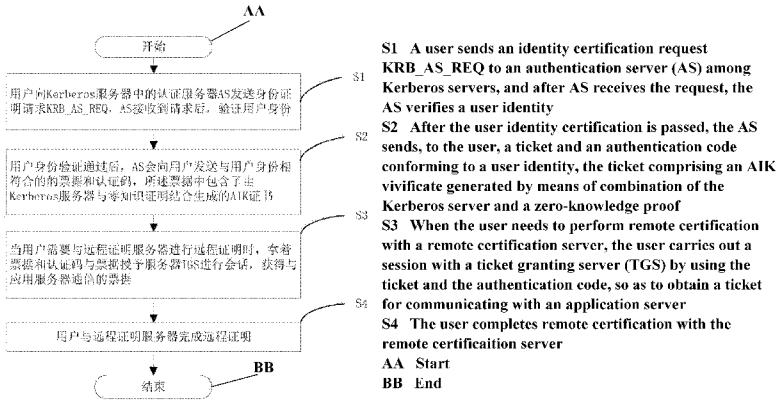


图 3 /FIG. 3

(57) **Abstract**: The present invention relates to a secure communication authentication method and system in a distributed environment. By using the method and the system of the present invention, disadvantages in a platform identity certification process in TCG remote certification are alleviated, a method for platform identity certification is expanded, and by combining three technologies, that are, zero-knowledge proof, a Kerberos framework and a virtual TPM, a new verification method is designed, which is mainly intended to make improvement in the aspects in the existing method such as platform information exposure, a trusted third-party bottleneck and complexity avoidance. By using the method and the system of the present invention, the problems of privacy exposure and efficiency in mutual verification between remote servers in the existing distributed system.

(57) **摘要**: 本发明涉及一种分布式环境下的安全通信认证方法及系统。本发明所述的方法及系统改进了 TCG 远程证明中平台身份证明过程中的各方面不足之处，扩展了平台身份证明方法，将零知识证明、Kerberos 框架和虚拟 TPM 三种技术结合起来，设计了一种新的认证方法，主要针对现有方法中平台信息暴露、可信第三方瓶颈和避免复杂度等方面进行改进。采用本发明所述的方法及系统，解决了现有分布式系统中远程服务器之间相互证明时所面临的隐私暴露与效率问题。

WO 2014/183392 A1

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))。

分布式环境下的安全通信认证方法及系统

技术领域

本发明涉及计算机信息安全技术领域，具体涉及一种分布式环境下的安全通信认证方法及系统。

背景技术

随着大数据时代的到来，单个服务器的处理速度与功能已经无法满足人们对信息处理的时效性的要求，分布式并行运算势在必行。但当我们使用未知服务器提供的服务和资源，并且无法得知其安全状态时，将不能与其进行安全的通信互联。所以两个服务器之间通信前进行有效的安全认证对全面保证分布式系统的安全稳定运行具有重要意义。

在现有的安全协议中，对终端平台操作系统的安全性考虑都不是很多，一般都没有考虑终端平台在启动和加载操作系统时是否满足终端平台的要求，通常都假设其是安全的。如果没有可靠的终端平台，就不可能谈到可信网络和可信网络连接。

TCG（Trusted Computing Group，可信计算组织）提出的远程证明过程中的身份认证技术为这个问题提供了技术支持。TCG 是 1999 年由 Compaq、HP、IBM、Intel 和 Microsoft 牵头组织 TCPA(Trusted Computing Platform Alliance)，目前已发展成员 190 家，遍布全球各大洲主力厂商。TCPA 专注于从计算平台体系结构上增强其安全性，并于 2001 年 1 月发布了可信计算平台标准规范。2003 年 3 月 TCPA 改组为 TCG(Trusted Computing Group)，其目的是在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台，以提高整体的安全性。

TCG 组织制定了 TPM（Trusted Platform Moudle）的标准，目前很多安全芯片都是符合这个规范的。而且由于其硬件实现安全防护，正逐渐成为 PC，尤其是便携式 PC 的标准配置。

“零知识证明”－zero-knowledge proof，是由 Goldwasser 等人在 20 世纪 80 年代初提出的。它指的是证明者能够在不向验证者提供任何有用的信

息的情况下，使验证者相信某个论断是正确的。零知识证明实质上是一种涉及两方或更多方的协议，即两方或更多方完成一项任务所需采取的一系列步骤。证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。大量事实证明，零知识证明在密码学中非常有用。如果能够将零知识证明用于验证，将可以有效解决许多问题。

Kerberos 是一种网络认证协议，其设计目标是通过密钥系统为客户机 / 服务器应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证，无需基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地读取、修改和插入数据。在以上情况下， Kerberos 作为一种可信任的第三方认证服务，是通过传统的密码技术（如：共享密钥）执行认证服务的。认证过程具体如下：客户机向认证服务器（AS）发送请求，要求得到某服务器的证书，然后 AS 的响应包含这些用客户端密钥加密的证书。证书的构成为：1)服务器“ticket”；2) 一个临时加密密钥（又称为会话密钥“session key”）。客户机将 ticket（包括用服务器密钥加密的客户机身份和一份会话密钥的拷贝）传送到服务器上。会话密钥可以（现已经由客户机和服务器共享）用来认证客户机或认证服务器，也可用来为通信双方以后的通讯提供加密服务，或通过交换独立子会话密钥为通信双方提供进一步的通信加密服务。

本说明书中对于任何现有技术的描述不应被看做是承认或者暗示：其中的内容在申请日或任何权利要求的优先权日之前是众所周知的或者是本领域的公知常识。

发明内容

针对现有技术中存在的一个或多个缺陷，本发明的目的是提供一种分布式环境下的安全通信认证方法及系统。该方法及系统改进了 TCG 远程证明中平台身份证明过程中的各方面不足之处,扩展了平台身份证明方法，将零知识证明、Kerberos 框架和虚拟 TPM 三种技术结合起来，设计了一种新的认证方法。该方法主要针对以上方法中平台信息暴露、可信第三方瓶颈和避免复杂度等方面进行改进。

为达到以上目的，本发明采用的技术方案是：一种分布式环境下的安全通信认证方法，用户采用零知识证明方法进行身份认证，包括以下步骤：

(1)用户向 Kerberos 服务器中的认证服务器 AS 发送身份证明请求 KRB_AS_REQ，AS 接收到请求后，验证用户身份；

(2)用户身份验证通过后，AS 会向用户发送与用户身份相符合的的票据和认证码，所述票据中包含了由 Kerberos 服务器与零知识证明结合生成的 AIK 证书；

(3)当用户需要与远程证明服务器进行远程证明时，拿着票据和认证码与票据授予服务器 TGS 进行会话，获得与应用服务器通信的票据；

(4)用户与远程证明服务器完成远程证明。

一种分布式环境下的安全通信认证系统，包括以下装置：

用户平台，所述用户平台是指需要进行 AIK 证书认证的客户端；

Kerberos 服务器，包括认证服务器 AS 和票据授予服务器 TGS，所述的认证服务器 AS 用于检验用户平台提供的属性信息是否在安全阀中，并对处于安全阀中的用户平台签发 TGS 票据和与之关联的 AIK 证书，所述的票据授予服务器 TGS 检测用户平台所持的 TGS 票据是否过期，对合法的用户平台发放可通信的应用服务票据；

远程证明服务器，用于当持有应用服务票据的用户平台与远程证明服务器进行通信时，对 AIK 证书和应用服务票据进行检查，合法后再与之进行应用服务；

所述的用户平台、Kerberos 服务器和远程证明服务器通过互联网互相连接。

本发明的效果在于： 采用本发明所述的方法和系统，可以解决了现有分布式系统中远程服务器之间相互证明时所面临的隐私暴露与效率问题。本方法将零知识证明、Kerberos 技术和虚拟 TPM 技术相结合，在平台申请 AIK 证书时，使用零知识的证明方式，使用 Kerberos 作为 TTP，Kerberos 中分为 AS 和 TGS，AS 进行 AIK 认证，那么一个 TPM 只需要

进行一次 AS 认证，当需要接入网络时，到 TGS 处申请应用服务器票据，即可进行远程证明，分工合作减少 TTP 的负载，vTPM 架构作为平台的体系结构，虚拟技术实现按功能模块的安全隔离，形成新的身份证明模式，达到防止平台信息暴露、避免可信第三方瓶颈和降低远程证明复杂度的目的。

附图说明

图 1 是本发明所述系统的结构图；

图 2 是本发明所述方法远程证明过程中 AIK 证书体系结构示意图；

图 3 是本发明所述方法的流程图；

图 4 是本发明所述方法 AIK 证书生成协议的流程图。

具体实施方式

下面结合附图和具体实施方式对本发明作进一步描述。应注意到：除非另外具体说明，否则在这些实施例中阐述的部件和步骤的相对布置、数字表达式和数值不限制本发明的范围。

以下对至少一个示例性实施例的描述实际上仅仅是说明性的，决不作为对本发明及其应用或使用的任何限制。

对于相关领域普通技术人员已知的技术、方法和设备可能不作详细讨论，但在适当情况下，所述技术、方法和设备应当被视为授权说明书的一部分。

在这里示出和讨论的所有示例中，任何具体值应被解释为仅仅是示例性的，而不是作为限制。因此，示例性实施例的其它示例可以具有不同的值。

如图 1 所示，一种分布式环境下的安全通信认证系统，包括以下装置：

用户平台，所述用户平台是指需要进行 AIK 证书认证的客户端；

Kerberos 服务器，包括认证服务器 AS 和票据授予服务器 TGS，所述的认证服务器 AS 用于检验用户平台提供的属性信息是否在安全阀中，并

对处于安全阀中的用户平台签发 TGS 票据和与之关联的 AIK 证书，所述的票据授予服务器 TGS 检测用户平台所持的 TGS 票据是否过期，对合法的用户平台发放可通信的应用服务票据;

远程证明服务器，用于当持有应用服务票据的用户平台与远程证明服务器进行通信时，对 AIK 证书和应用服务票据进行检查，合法后再与之进行应用服务。

所述的用户平台、Kerberos 服务器和远程证明服务器通过互联网互相连接。

本实施例中，所述的用户平台包括以下模块:

安全芯片 TPM/TCM，用于记录所在用户平台系统属性信息的度量值;

XEN 虚拟机，用于为证明过程提供安全可靠的实施平台。共享同一平台上的工作负载因多种原因经常需要保持独立。利益不同决定了竞争性业务的网站需要访问彼此的数据，会存在很多不安全的因素存在。此外，恶意软件破坏了正常运作这些软件的共享硬件环境。虚拟化越来越多地用于生产，使得在软件方面的安全，就更加的需要严格要求完整性和工作量隔离性。

如图 2 所示，图 2 为用户平台的体系结构示意图，构建 vTPM 体系结构，需要用户平台配有安全芯片 TPM/TCM,本文以 TPM 为例; CPU 要具有 Intel-VT 或者 AMD-V 虚拟技术; BIOS 支持 TCG 规范和高级配置和电源管理接口（Advanced Configuration and Power Management Interface，ACPI）; 同时需要具有 IMA 度量功能的 Linux 系统启动加载器(GRUB-IMA)来加载操作系统。

XEN 虚拟机上主要包括三个虚拟域，用户平台开机后 TPM 以自身的可信度量根为起点，首先对 BIOS 的其它部件进行完整性度量，并将度量值存储于可信密码模块的 PCR 中，按照选择的判断机制判断 BIOS 的完整性，若完整性未破坏，则运行 BIOS; 并度量初始化程序加载器(Initial Program Loader-IPL)/主引导分区(Master Boot Record-MBR)的完整性，基于判断机制判断 IPL/MBR 完整性，若 IPL/MBR 完整性没有破坏，则运行 MBR; 然后由 IPL/MBR 度量操作系统(Operation System，OS)内核度

量与加载部件 GRUB-IMA(GNU GRand Unified Bootloader-IMA，GRUB-IMA)的完整性，若该部件完整性未被破坏则由该部件度量 OS 内核的完整性，若未被篡改，则运行 OS 内核。OS 内核启动后进入 Domain 0，基于同样的机制检测 OS 服务完整性，通过信任关系传递，形成可信根，可以确保所启动的系统是可信的。

Domain 0 中涉及到四部分内容：安装了 XEN 补丁(XEN patch)的 Linux 操作系统；OS 和 TPM 进行通信的驱动程序 tpm_tis；TPM 模拟器；XEN 中的 vTPM 管理功能模块 vTPMManager，负责 XEN 中 vTPM 功能模块与 TPM Emulator 的通信。

Domain U 是半虚拟化虚拟域，它中主要涉及到以下几个部分：XEN 中的功能模块 vTPM，由于 XEN 虚拟域本身无法与 TPM 进行交互，所以采用 vTPM 的方式，vTPM 与 TPM Emulator 进行交互，TPM Emulator 调用底层 TPM 硬件的数据，并充当 TPM 硬件的角色，对外进行数据交互；XEN 与 TPM Emulator 之间的通信驱动程序 xen_tpmu，此驱动是在编译内核时需要额外添加的；IAIK jTSS 是由格拉茨工业大学应用信息过程和计算机研究所(Institut fuer AngewandteInformationsverarbeitung und Kommunikation, IAIK)使用 Java 语言开发的，是对 TCG 软件栈(TCG Software Stack，TSS)的实现，为上层的应用程序提供了访问 TPM 和 TPM Emulator 的接口。vTPM 位于 XEN 虚拟机中,即在 Domain 0 中，但在功能上是 Domain U 程序与 Domain 0 中 TPM Emulator 进行信息交互接口，是 Domain U 中功能模块执行的关键，所以在图 2 中用虚线圈到了 Domain U 的区域下。

HVM-Domain 是全虚拟化的虚拟域，主要涉及到以下部分：支持 TCG 规范的 BIOS；具有度量功能的 OS 加载器，形成可信根；虚拟域与 TPM Emulator 进行数据交互的 vTPM 部件；同时 OS 在内核编译时要将 IBM 发明的 IMA 部件编译到内核(Linux-IMA)，用于查看整个系统的度量结果和对 OS 中运行的软件进行度量；Linux-IMA 查看 TPM 数据需要与 TPM 硬件进行交互，需要 OS 加载 TPM 驱动 tpm_tis；用户对 TPM 和 TPM Emulator 进行编程的接口软件 IAIK jTSS；开源平台可信服务(Open Platform Trust Services，OpenPTS)是由 TCG 提出的，对概念验证

(Proof-of-Concept，PoC)和平台可信服务(Platform Trust Services ，PTS)的相关实现，与其它可信计算相关开源软件一起工作，用于与远程挑战者进行可信计算。

Domain 0 负责协调管理各个计算域间的通信。启动 TPM Emulator 后，处于等待状态，等待对方与自身进行通信。启动 vTPMManager 管理 TPM Emulator 与 vTPM 间的通信。当需要进行身份认证时，在 Domain U 中，用户通过使用 IAIK jTSS 发布 TPM 命令，准备身份认证所需要的 TPM 身份相关数据，vTPM 接到命令后，会与 Domain 0 中的 vTPMManager 进行通信，通知其想通 TPM Emulator 进行数据交互，vTPMManager 会将命令发送给 TPM Emulator，TPM Emulator 接到命令后会调底层的 TPM 数据，准备好数据后会将数据再按照相反的顺序反馈给 IAIK jTSS。IAIK jTSS 接收到所有所需数据后会给 AS 发送身份认证请求，认证结束后 AS 会给 IAIK jTSS 发送 AIK 证书。IAIK jTSS 收到证书后，IAIK jTSS 会将其传送到 Domain 0 处保存。HVM-Domain 会到 Domain 0 处提取 AIK 证书，然后到 TCG 处申请应用程序票据，拿到票据后会向远程证明服务器发送远程证明请求，将 AIK 证书和度量列表同时发送给远程证明服务器进行远程证明。这种执行方法要求各个虚拟域各司其职，相互隔离，提高了安全性。

如图 3 所示，一种分布式环境下的安全通信认证方法，用户采用零知识证明方法进行身份认证，包括以下步骤：

步骤 S1，用户向 Kerberos 服务器中的认证服务器 AS 发送身份证明请求 KRB_AS_REQ，AS 接收到请求后，验证用户身份；

步骤 S2，用户身份验证通过后，AS 会向用户发送与用户身份相符合的的票据和认证码，所述票据中包含了由 Kerberos 服务器与零知识证明结合生成的 AIK 证书；

步骤 S3，当用户需要与远程证明服务器进行远程证明时，拿着票据和认证码与票据授予服务器 TGS 进行会话，获得与应用服务器通信的票据；

步骤 S4，用户与远程证明服务器完成远程证明。

本实施例中，Kerberos 与零知识证明结合生成 AIK 证书过程如图 4 所示，证书生成过程如下：

（1）用户封装 KRB_AS_REQ 消息

用户像原 Kerberos 协议那样封装 KRB_AS_REQ 消息，只是预定义块由以下消息代替：E(PUAS,KC,AS)||pk||vk , KC,AS 是由用户产生的和 AS 的会话密钥，使用 AS 的公钥 PUAS 加密，消息格式：

Option||IDC||Realmc||IDTGS||Times||Nounce1||E(PUAS,KC,AS)||pk||vk

其中，pk=E(AIKpub，EKpub),e1,e2,…,ek 是由系统选择的一个哈希函数的输出，其输入为：

Option||IDC||Realmc||IDTGS||Times||Nounce1||E(PUAS,KC,AS)||pk

这样可以有效的防止中间人攻击。

（2）Kerberos 接收到 KRB_AS_REQ 消息

AS 收到 KRB_AS_REQ 消息后，在发放 TGS 票据前，AS 必须要对用户的身份进行认证。可信平台与可信第三方进行零知识协议认证。首先，使用和用户同样的算法产生 e1,e2,…,ek ；其次，AS 在自己的数据库中提取相应的用户的身份验证信息 v1,v2,…,vk；第三，AS 检查发送来的 KRB_AS_REQ 的消息是否满足下式：

$$pk = \pm vk^2 \prod_{e_j=1} v_j (\mathrm{mod}\, n)$$

认证通过后，可信平台使用 zk= E(AIKpub，ω)来表示证书，其中 ω 是背书证书、平台证书、确认证书和验证证书的集合，且背书证书中不包含背书公钥。并把 zk||vk’发送给 Kerberos，其中 vk’是输入为：

Option||IDC||Realmc||IDTGS||Times||Nounce1||E(PUAS,KC,AS)||zk(公式 1)的输出结果，即第二次使用 Feige-Fiat-Shamir 协议。如果证明证书有效，那么解密 KRB_AS_REQ 消息，获得会话密钥 KC,AS，用 KC,AS 加密 AIK 公钥，产生 AIK 证书 AIKcert，使用 pk 加密证书，生成 KRB_AS_REP 发送给可信平台。Kerberos 产生 KRB_AS_REP 消息消息的密文部分使用解密 KRB_AS_REQ 消息的密文部分获得的会话密钥 KC,AS 来加密，而不是使用用户的口令加密。消息格式：

RealmC||IDC||TicketTGS||E(KC,AS,[AIK||KC,TGS||Times||IDTGS]) (公

式 2)

将其发送给用户。其中，AIK=E(pk,AIKcert)。

(3) 用户收到AS的消息后，就可以向TGS发送消息即KRB_TGS_REQ。消息中包含申请到的 TGS 票据和所申请服务的标识 ID。另外，用户还发送一条认证吗 Authenticatorc，此消息包含有用户的标识 ID、网络地址和时间戳，并且用和 TGS 的会话密钥来加密，此会话密钥即 AS 信息交换阶段的所得到的 Kc,tgs。和 TGS 票据的生命期相比，此认证码的生命期很短，并且只能使用一次。Nounce2、Options 和 Times 的作用同消息上。将消息按如下格式发送给 Kerberos 服务器的 TGS 模块:

Options||IDv||Times||Nounce2||Tickettgs||Authenticatorc (公式 3)

其中，Authenticatorc=E(Kc,tgs,[IDc||Realmc||TS1])

(4)成功地验证了消息 KRB_TGS_REQ 的合法性后，TGS 开始组装消息 KRB_TGS_REP。这个消息的格式同消息（公式 2）KRB_AS_REP。首先 Kerberos 服务器根据消息（公式 3）和收到的 TGS 票据来决定发送给用户的应用服务器票据的性质，然后从用户口令数据库中提取出相应的应用服务器密钥，将该票据加密，产生应用服务器的票据。KRB_TGS_REP 消息的密文部分用会话密钥 Kc,tgs。同 AS 消息交换一样，和应用服务器的消息交换时使用的会话密钥 Kc,v 也在 TGS 信息交换阶段分发，用户和应用服务器均可从相应的域中获得此会话密钥。消息的格式如下:

realmc||IDc||Ticketv||E(Kc,tgs,[Kc,v||Times||Nounce2||Realmv||IDv]) (公式 4)其中，Ticketv=E(Kv,[Flags||Kc,v||Realmc||IDc||ADc||Times])

使用得到的 Ticket 和认证码，就能连接到 Remote Attestation (RA)服务器，客户机发送 IMA 度量列表和当前使用 AIK 签名的 PCR10 值给服务器。RA 服务器检查 Ticket 和认证码的有效性，是否由可信的 Kerberos 颁发。

本公开还提供一种或多种具有计算机可执行指令的计算机可读介质，所述指令在由计算机执行时，执行分布式环境下的安全通信认证方法，用户采用零知识证明方法进行身份认证，该方法包括以下步骤：(1)用户向 Kerberos 服务器中的认证服务器 AS 发送身份证明请求 KRB_AS_REQ，AS 接收到请求后，验证用户身份；(2)用户身份验证通过后，AS 会向用户

发送与用户身份相符合的的票据和认证码，所述票据中包含了由 Kerberos 服务器与零知识证明结合生成的 AIK 证书；(3)当用户需要与远程证明服务器进行远程证明时，拿着票据和认证码与票据授予服务器 TGS 进行会话，获得与应用服务器通信的票据；(4)用户与远程证明服务器完成远程证明。

本公开还提供一台包括带有计算机可执行指令的一个或多个计算机可读介质的计算机，所述指令在由计算机执行时执行上述分布式环境下的安全通信认证方法。

示例性操作环境

诸如此处所描述的计算设备具有硬件，包括一个或多个处理器或处理单元、系统存储器和某种形式的计算机可读介质。作为示例而非限制，计算机可读介质包括计算机存储介质和通信介质。计算机存储介质包括以用于存储诸如计算机可读指令、数据结构、程序模块或其它数据的信息的任何方法或技术实现的易失性与非易失性、可移动与不可移动介质。通信介质一般以诸如载波或其它传输机制等已调制数据信号来体现计算机可读指令、数据结构、程序模块或其它数据，并且包括任何信息传递介质。以上的任一种的组合也包括在计算机可读介质的范围之内。

计算机可使用至一个或多个远程计算机，如远程计算机的逻辑连接在网络化环境中操作。尽管结合示例性计算系统环境进行了描述，但本发明的各实施例可用于众多其它通用或专用计算系统环境或配置。计算系统环境并非旨在对本发明的任何方面的使用范围或功能提出任何限制。此外，计算机环境也不应被解释成对于示例性操作环境中所示出的任一组件或其组合有任何依赖或要求。适用于本发明的各方面的公知的计算系统、环境和/ 或配置的示例包括，但不仅限于：个人计算机、服务器计算机、手持式或膝上型设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费电子产品、移动电话、网络 PC、小型计算机、大型计算机、包括上面的系统或设备的中的任何一种的分布式计算环境等等。

可以在由一台或多台计算设备执行的诸如程序模块之类的计算机可执行的指令的一般上下文中来描述本发明的各实施例。计算机可执行指令可作为软件被组织成一个或多个计算机可执行组件或模块。一般而言，程序

模块包括，但不限于，执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件，以及数据结构。可以利用任何数量的这样的组件或模块及其组织来实现本发明的各方面。例如，本发明的各方面不仅限于附图中所示出并且在此处所描述的特定计算机可执行指令或特定组件或模块。本发明的其他实施例可以包括具有比此处所示出和描述的功能更多或更少功能的不同的计算机可执行指令或组件。本发明的各方面也可以在其中任务由通过通信网络链接的远程处理设备执行的分布式计算环境中实现。在分布式计算环境中，程序模块可以位于包括存储器存储设备在内的本地和远程计算机存储介质中。

本领域技术人员应该明白，本发明所述的方法和系统并不限于具体实施方式中所述的实施例，上面的具体描述只是为了解释本发明的目的，并非用于限制本发明。本领域技术人员根据本发明的技术方案得出其他的实施方式，同样属于本发明的技术创新范围，本发明的保护范围由权利要求及其等同物限定。

权 利 要 求

1. 一种分布式环境下的安全通信认证方法，用户采用零知识证明方法进行身份认证，包括以下步骤:

(1)用户向 Kerberos 服务器中的认证服务器 AS 发送身份证明请求 KRB_AS_REQ，AS 接收到请求后，验证用户身份;

(2)用户身份验证通过后，AS 会向用户发送与用户身份相符合的的票据和认证码,所述票据中包含了由 Kerberos 服务器与零知识证明结合生成的 AIK 证书;

(3)当用户需要与远程证明服务器进行远程证明时，拿着票据和认证码与票据授予服务器 TGS 进行会话，获得与应用服务器通信的票据;

(4)用户与远程证明服务器完成远程证明。

2. 如权利要求 1 所述的一种分布式环境下的安全通信认证方法，其特征是，步骤(2)中， 由 Kerberos 服务器与零知识证明结合生成 AIK 证书的方法包括以下步骤:

1） 用户封装 KRB_AS_REQ 消息;

2） Kerberos 服务器中的 AS 收到 KRB_AS_REQ 消息后，在发放 TGS 票据前，AS 对用户的身份进行认证，可信平台与可信第三方进行零知识协议认证;

3） 用户收到 AS 的消息后，向 TGS 发送消息 KRB_TGS_REQ;

4） 成功地验证了消息 KRB_TGS_REQ 的合法性后，TGS 开始组装消息 KRB_TGS_REP。

3. 如权利要求 2 所述的一种分布式环境下的安全通信认证方法，其特征是：步骤 1)中，用户封装 KRB_AS_REQ 消息过程中，预定义块由以下消息代替：E(PUAS,KC,AS)||pk||vk，其中，KC,AS 是由用户产生的和 AS 的会话密钥，使用 AS 的公钥 PUAS 加密，消息格式:

Option||IDC||Realmc||IDTGS||Times||Nounce1||E(PUAS,KC,AS)||pk||vk

其中，pk=E(AIKpub，EKpub),e1,e2,…,ek 是由系统选择的一个哈希函

数的输出，其输入为：

Option||IDC||Realmc||IDTGS||Times||Nounce1||E(PUAS,KC,AS)||pk。

4. 如权利要求 2 所述的一种分布式环境下的安全通信认证方法，其特征是，步骤 2)中，AS 对用户的身份进行认证的方法是：首先，使用和用户同样的算法产生 e1,e2,...,ek ；其次，AS 在自己的数据库中提取相应的用户的身份验证信息 v1,v2,...,vk；第三，AS 检查发送来的 KRB_AS_REQ 的消息是否满足下式：

$$pk = \pm vk^2 \prod_{e_j=1} v_j (\mathrm{mod}\, n)$$

用户的身份认证通过后，可信平台使用 zk= E(AIKpub，ω)来表示证书，其中 ω 是背书证书、平台证书、确认证书和验证证书的集合，且背书证书中不包含背书公钥 。

5. 如权利要求 2 或 3 或 4 所述的一种分布式环境下的安全通信认证方法，其特征是，步骤 3)中，用户还发送一条认证码 Authenticatorc，此消息包含有用户的标识 ID、网络地址和时间戳，并且用和 TGS 的会话密钥来加密，此会话密钥即 AS 信息交换阶段的所得到的 Kc,tgs 和 TGS 票据的生命期相比，此认证码的生命期很短，并且只能使用一次。

6. 如权利要求 5 所述的一种分布式环境下的安全通信认证方法，其特征是，步骤 4)中，TGS 组装消息 KRB_TGS_REP 的方法包括：

首先，Kerberos 服务器根据消息和收到的 TGS 票据来决定发送给用户的应用服务器票据的性质；

然后，从用户口令数据库中提取出相应的应用服务器密钥，将该票据加密，产生应用服务器的票据；

KRB_TGS_REP 消息的密文部分用会话密钥 Kc,tgs 同 AS 消息交换一样，和应用服务器的消息交换时使用的会话密钥 Kc,v 也在 TGS 信息交换阶段分发，用户和应用服务器均可从相应的域中获得此会话密钥；

KRB_TGS_REP 消息的格式如下：

realmc||IDc||Ticketv||E(Kc,tgs,[Kc,v||Times||Nounce2||Realmv||IDv])

其中，Ticketv=E(Kv,[Flags||Kc,v||Realmc||IDc||ADc||Times])。

7. 一种分布式环境下的安全通信认证系统，包括以下装置：

用户平台，所述用户平台是指需要进行 AIK 证书认证的客户端；

Kerberos 服务器，包括认证服务器 AS 和票据授予服务器 TGS，所述的认证服务器 AS 用于检验用户平台提供的属性信息是否在安全阀中，并对处于安全阀中的用户平台签发 TGS 票据和与之关联的 AIK 证书，所述的票据授予服务器 TGS 检测用户平台所持的 TGS 票据是否过期，对合法的用户平台发放可通信的应用服务票据；

远程证明服务器，用于当持有应用服务票据的用户平台与远程证明服务器进行通信时，对 AIK 证书和应用服务票据进行检查，合法后再与之进行应用服务；

所述的用户平台、Kerberos 服务器和远程证明服务器通过互联网互相连接。

8. 如权利要求 7 所述的一种分布式环境下的安全通信认证系统，其特征在于，所述的用户平台包括以下模块：

安全芯片 TPM/TCM，用于记录所在用户平台系统属性信息的度量值；

XEN 虚拟机，用于为证明过程提供安全可靠的实施平台。

9. 如权利要求 8 所述的一种分布式环境下的安全通信认证系统，其特征在于： 所述安全芯片 TPM 的 CPU 要具有 Intel-VT 或者 AMD-V 虚拟技术； BIOS 支持 TCG 规范和高级配置和电源管理接口； 同时需要具有 IMA 度量功能的 Linux 系统启动加载器(GRUB-IMA)来加载操作系统。

10. 如权利要求 7 或 8 或 9 所述的一种分布式环境下的安全通信认证系统，其特征在于：所述的 XEN 虚拟机包括 Domain 0、Domain U 和 HVM-Domain 三个虚拟域，用户平台开机后 TPM 以自身的可信度量根为

起点，首先对 BIOS 的其它部件进行完整性度量，并将度量值存储于可信密码模块的 PCR 中，按照选择的判断机制判断 BIOS 的完整性，若完整性未破坏，则运行 BIOS；并度量 IPL/MBR 的完整性，基于判断机制判断 IPL/MBR 完整性，若 IPL/MBR 完整性没有破坏，则运行 MBR；然后由 IPL/MBR 度量操作系统内核度量与加载部件 GRUB-IMA 的完整性，若该部件完整性未被破坏则由该部件度量 OS 内核的完整性，若未被篡改，则运行 OS 内核；OS 内核启动后进入 Domain 0，基于同样的机制检测 OS 服务完整性，通过信任关系传递，形成可信根，可以确保所启动的系统是可信的。

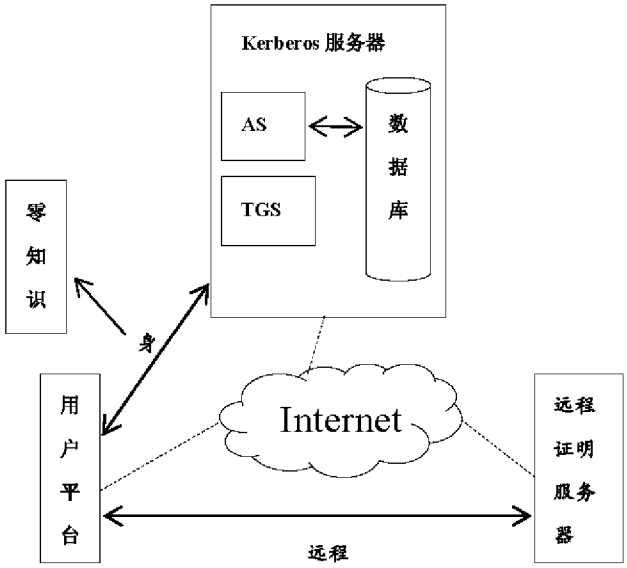

Kerberos 服务器
AS
TGS
数据库
零知识
身
用户平台
Internet
远程证明服务器
远程

图 1

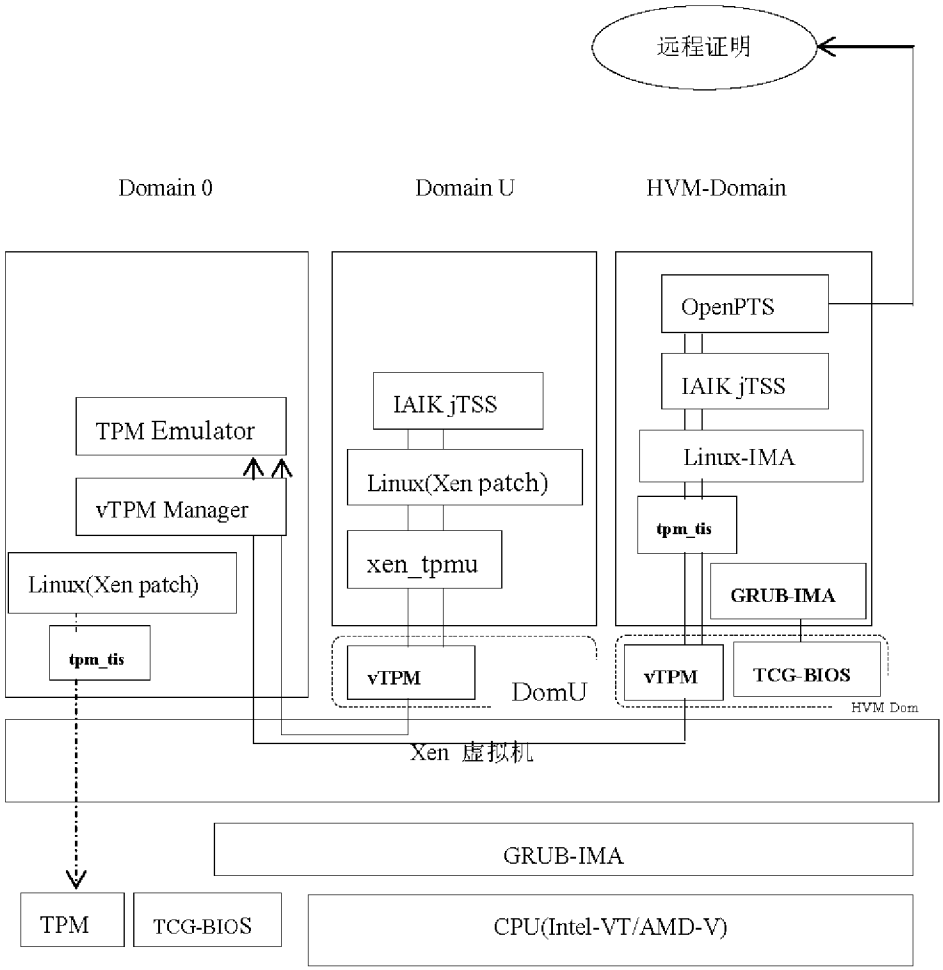

远程证明
Domain 0
Domain U
HVM-Domain
TPM Emulator
vTPM Manager
Linux(Xen patch)
tpm_tis
IAIK jTSS
Linux(Xen patch)
xen_tpmu
vTPM
DomU
OpenPTS
IAIK jTSS
Linux-IMA
tpm_tis
GRUB-IMA
vTPM
TCG-BIOS
HVM Dom
Xen 虚拟机
GRUB-IMA
TPM
TCG-BIOS
CPU(Intel-VT/AMD-V)

图 2

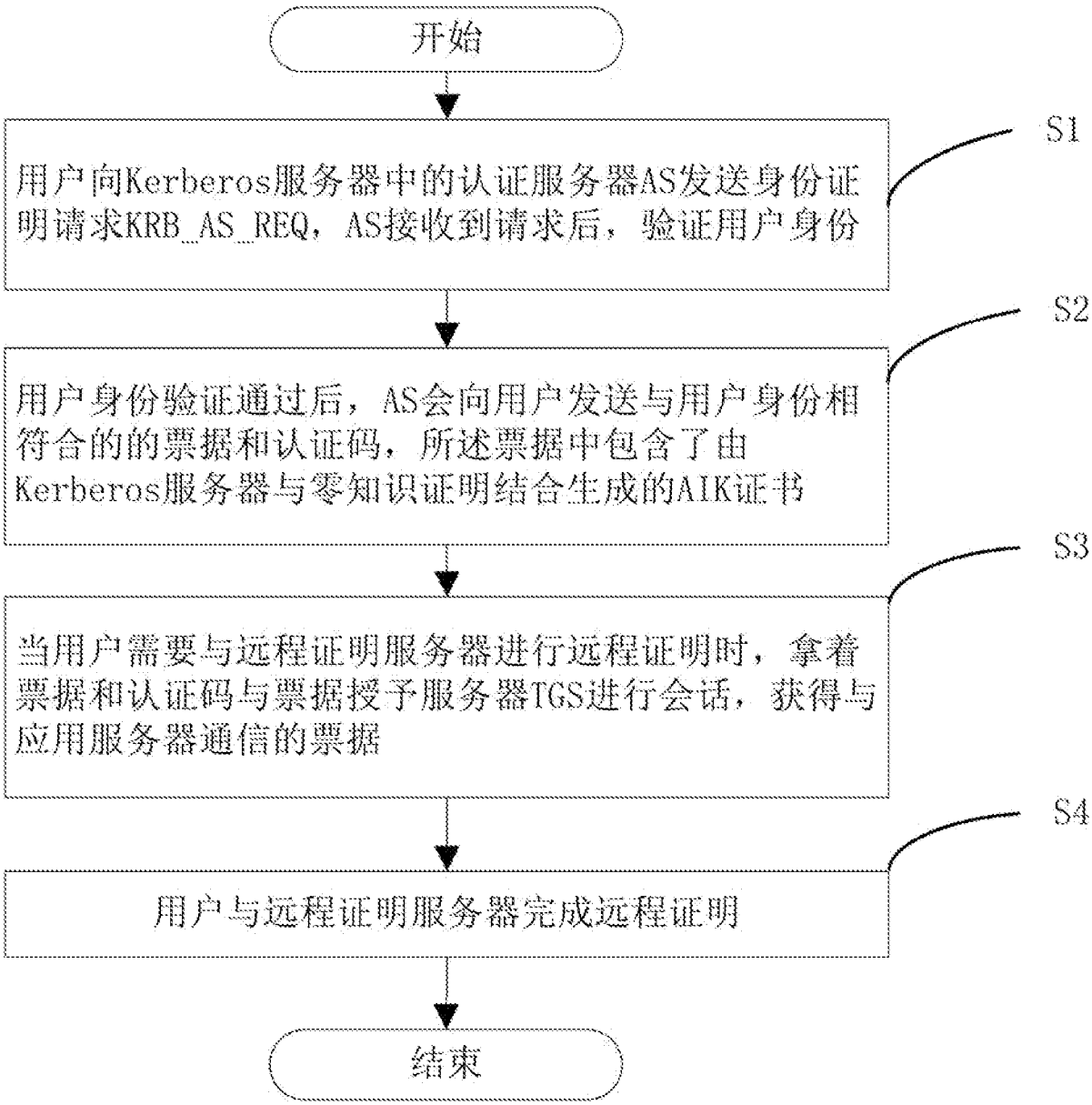

开始
用户向Kerberos服务器中的认证服务器AS发送身份证明请求KRB_AS_REQ，AS接收到请求后，验证用户身份
S1
用户身份验证通过后，AS会向用户发送与用户身份相符合的的票据和认证码，所述票据中包含了由Kerberos服务器与零知识证明结合生成的AIK证书
S2
当用户需要与远程证明服务器进行远程证明时，拿着票据和认证码与票据授予服务器TGS进行会话，获得与应用服务器通信的票据
S3
用户与远程证明服务器完成远程证明
S4
结束

图 3

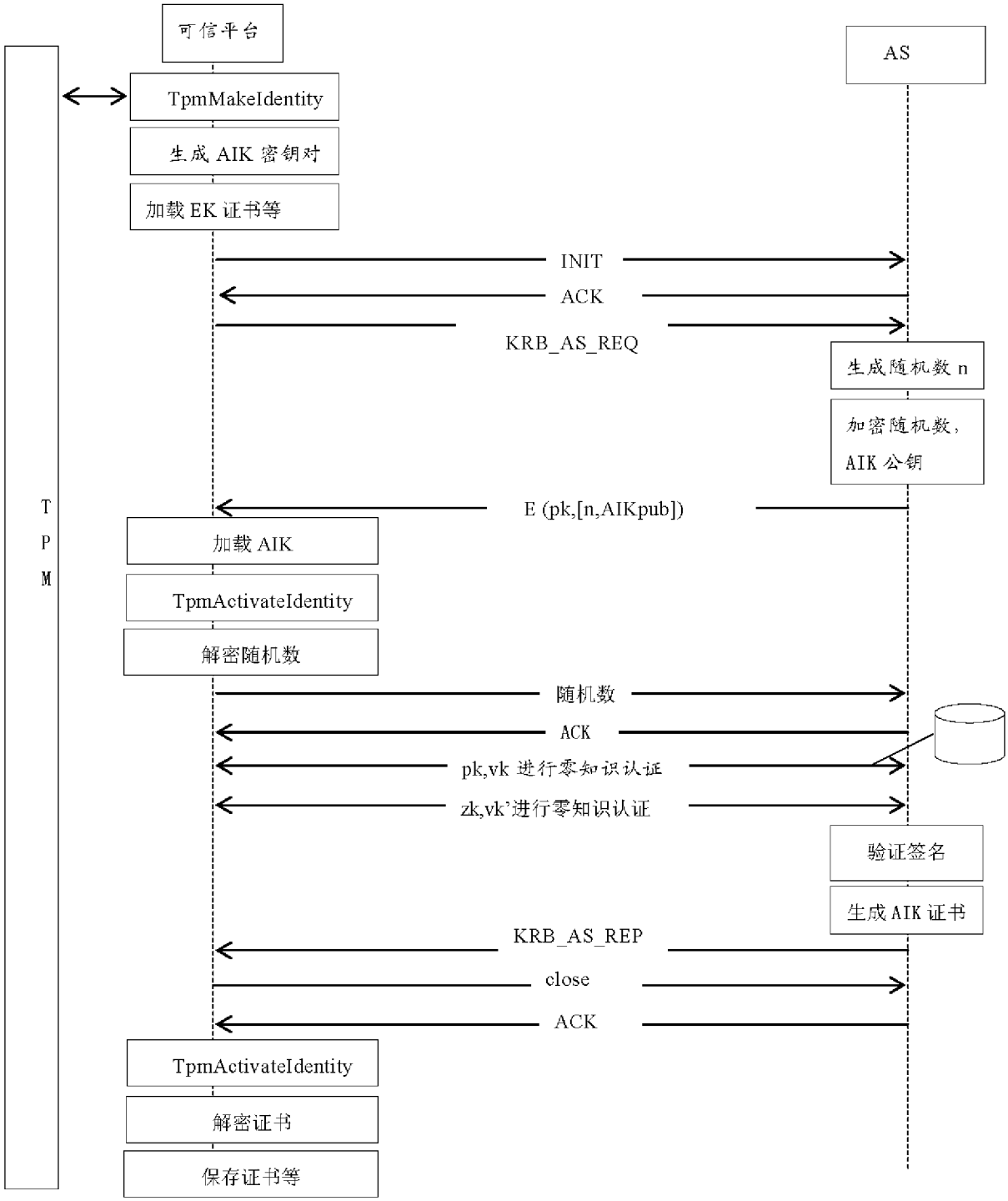

可信平台
AS
TpmMakeIdentity
生成 AIK 密钥对
加载 EK 证书等
INIT
ACK
KRB_AS_REQ
生成随机数 n
加密随机数，
AIK 公钥
T
P
M
E (pk,[n,AIKpub])
加载 AIK
TpmActivateIdentity
解密随机数
随机数
ACK
pk,vk 进行零知识认证
zk,vk'进行零知识认证
验证签名
生成 AIK 证书
KRB_AS_REP
close
ACK
TpmActivateIdentity
解密证书
保存证书等

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/086753

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, CNTXT, CNKI: distributed, kerberos, authentication server, AS, Ticket Grant Server, TGS, KRB_AS_REQ, KRB_TGS_REQ, zero knowledge, Trusted Platform, TPM, Trusted Third Party, TTP, AIK; VEN: zero knowledge proof, ZKP

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101479987 A (MICROSOFT CORP.) 08 July 2009 (08.07.2009), the whole document	1-10
A	CN 101051898 A (HUAWEI TECHNOLOGIES CO., LTD.) 10 October 2007 (10.10.2007), the whole document	1-10
A	CN 1625105 A (IBM CORP.) 08 June 2005 (08.06.2005), the whole document	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 February 2014 (11.02.2014)	27 February 2014 (27.02.2014)
Name and mailing address of the ISA/CN State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer NIE, Jincheng Telephone No. (86-10) 62412155

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/086753

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101479987 A	08.07.2009	CA 2653615 A1	31.07.2008
		US 2010242102 A1	23.09.2010
		AU 2007345313 B2	16.12.2010
		IN 200807105 P4	21.08.2009
		WO 2008091277 A3	18.12.2008
		NO 20085023 A	12.12.2008
		MX 2008015958 A	31.03.2009
		RU 2008152118 A	10.07.2010
		AU 2007345313 A1	31.07.2008
		JP 2010505286 A	18.02.2010
		RU 2434340 C2	20.11.2011
		EP 2033359 A2	11.03.2009
		WO 2008091277 A2	31.07.2008
		KR 20090041365 A	28.04.2009
CN 101051898 A	10.10.2007	CN 101051898 B	21.04.2010
CN 1625105 A	08.06.2005	JP 4064914 B2	19.03.2008
		US 8171295 B2	01.05.2012
		US 2005120219 A1	02.06.2005
		JP 2005167589 A	23.06.2005
		CN 100594692 C	17.03.2010

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/086753

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i

H04L 9/14 (2006.01) n

国际检索报告

国际申请号
PCT/CN2013/086753

A. 主题的分类

参见附加页

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC：H04L，G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNABS，CNTXT，CNKI：分布式, kerberos, 认证服务器, AS, 票据授予服务器, 票证授予服务器, TGS, KRB_AS_REQ, KRB_TGS_REQ, 零知识, 可信平台, TPM, 可信第三方, TTP, AIK; VEN：distributed, kerberos, authentication server, AS, Ticket Grant Server, TGS, KRB_AS_REQ, KRB_TGS_REQ, zero knowledge proof, ZKP, Trusted Platform, TPM, Trusted Third Party, TTP, AIK

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN101479987A (微软公司), 08.7 月 2009 (08.07.2009), 全文	1-10
A	CN101051898A (华为技术有限公司), 10.10 月 2007 (10.10.2007), 全文	1-10
A	CN1625105A (国际商业机器公司),08.6 月 2005 (08.06.2005), 全文	1-10

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
11.2 月 2014 (11.02.2014)	**27.2 月 2014 (27.02.2014)**

ISA/CN 的名称和邮寄地址：
中华人民共和国国家知识产权局
中国北京市海淀区蓟门桥西土城路 6 号 100088
传真号：(86-10)62019451

受权官员
聂锦程
电话号码：(86-10) **62412155**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2013/086753

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101479987A	08.07.2009	CA2653615A1	31.07.2008
		US2010242102A1	23.09.2010
		AU2007345313B2	16.12.2010
		IN200807105P4	21.08.2009
		WO2008091277A3	18.12.2008
		NO20085023A	12.12.2008
		MX2008015958A	31.03.2009
		RU2008152118A	10.07.2010
		AU2007345313A1	31.07.2008
		JP2010505286A	18.02.2010
		RU2434340C2	20.11.2011
		EP2033359A2	11.03.2009
		WO2008091277A2	31.07.2008
		KR20090041365A	28.04.2009
CN101051898 A	**10.10.2007**	**CN101051898B**	**21.04.2010**
CN1625105A	08.06.2005	JP4064914B2	19.03.2008
		US8171295B2	01.05.2012
		US2005120219A1	02.06.2005
		JP2005167589A	23.06.2005
		CN100594692C	17.03.2010

A. 主题的分类

H04L 9/32 (2006.01) i

H04L 9/14 (2006.01) n