(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103856477 A
(43)申请公布日 2014.06.11

(21)申请号 201310050808.6

(22)申请日 2013.02.08

(66)本国优先权数据
201210520930.0 2012.12.06 CN

(71)申请人 阿里巴巴集团控股有限公司
地址 英国英属开曼群岛大开曼资本大厦一座四层 847 号邮箱

(72)发明人 付颖芳

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 栗若木

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

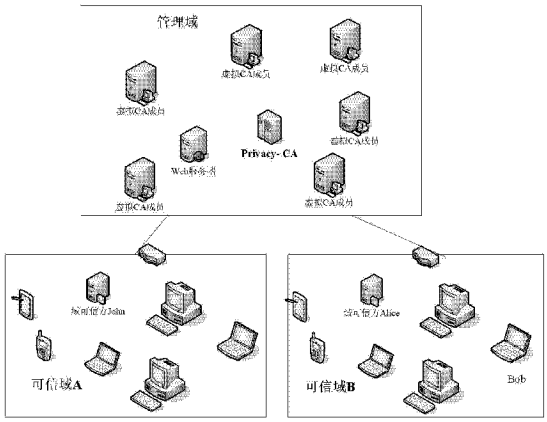
权利要求书6页 说明书18页 附图6页

(54)发明名称

一种可信计算系统及相应的认证方法和设备

(57)摘要

一种可信计算系统及相应的认证方法和设备，所述可信计算系统包括管理域和多个可信域，所述可信域的成员包括域可信方(DT)和域终端，所述方法包括：DT 以其平台身份证书为证明到管理域注册，管理域认证通过后，将管理域对所述 DT 的签名证书授予所述 DT；域终端以其平台身份证书为证明到所在可信域的 DT 注册，所述 DT 认证通过后，将终端身份证书授予所述域终端，所述终端身份证书包含管理域对所述 DT 的签名和所述 DT 对所述域终端的签名；不同可信域的域终端之间交互时，基于远程端的终端身份证书实现对远程端身份的远程认证。本申请便于扩展来应对不同规模可信域的集成，减少了网络流量、计算负载和存储空间，提高了跨域认证的效率。



CN 103856477 A

1. 一种可信计算系统的认证方法，所述可信计算系统包括管理域和多个可信域，所述可信域的成员包括域可信方 (DT) 和域终端，所述方法包括 ：

DT 以其平台身份证书为证明到管理域注册，管理域认证通过后，将管理域对所述 DT 的签名证书授予所述 DT ；

域终端以其平台身份证书为证明到所在可信域的 DT 注册，所述 DT 认证通过后，将终端身份证书授予所述域终端，所述终端身份证书包含管理域对所述 DT 的签名和所述 DT 对所述域终端的签名 ；

不同可信域的域终端之间交互时，基于远程端的终端身份证书实现对远程端身份的远程认证。

2. 如权利要求 1 所述的认证方法，其特征在于 ：

所述管理域的成员包括隐私证书权威 (PrivacyCA) ；

所述管理域认证通过后，将管理域对所述 DT 的签名证书授予所述 DT，包括 ：所述 PrivacyCA 认证通过后，将 DT 身份证书授予所述 DT，所述 DT 身份证书包含所述 PrivacyCA 对所述 DT 的签名。

3. 如权利要求 1 所述的认证方法，其特征在于 ：

所述管理域的成员包括隐私证书权威 (PrivacyCA) 和多个虚拟 CA 成员，所述认证方法还包括以下虚拟 CA 的建立过程 ：

所述 PrivacyCA 产生一对系统公私钥，公布门限签名和验证所需的公共参数，并将系统私钥秘密分发给虚拟 CA 成员 ；

各虚拟 CA 成员基于 (t,n) 门限体制秘密共享所述系统私钥，构成虚拟 CA，每一虚拟 CA 成员保存一份系统子私钥 ；

所述 DT 以其平台身份证书为证明到管理域注册是分别到 t 个虚拟 CA 成员注册 ；所述管理域认证通过后，将管理域对所述 DT 的签名证书授予所述 DT，包括 ：所述 t 个虚拟 CA 成员分别认证通过后，根据门限签名算法用各自保存的系统子私钥对所述 DT 签名得到 t 个子 DT 身份子证书并授予所述 DT，所述 DT 对所述 t 个 DT 身份子证书中系统子私钥对所述 DT 的签名的合法性认证通过后，根据所述 t 个 DT 身份子证书合成 DT 身份证书，所述 DT 身份证书包含用门限签名算法合成的虚拟 CA 对所述 DT 的签名。

4. 如权利要求 3 所述的认证方法，其特征在于 ：

所述 t 个虚拟 CA 成员用各自保存的系统子私钥对所述 DT 签名得到 t 个 DT 身份子证书并授予所述 DT 时，还将自己的 CA 成员身份证书作为身份证明提供给所述 DT ；

所述 DT 收到所述 DT 身份子证书和 CA 成员身份证书后，先基于所述 CA 成员身份证书对相应虚拟 CA 成员进行身份认证，认证通过后，再对所述 DT 身份子证书中的签名进行合法性认证。

5. 如权利要求 4 所述的认证方法，其特征在于 ：

所述 CA 成员身份证书是虚拟 CA 成员通过以下过程得到的 ：

一虚拟 CA 成员以其平台身份证书为证明到其他 t 个或 t-1 个虚拟 CA 成员注册，所述其他 t 个或 t-1 个虚拟 CA 成员验证通过后，用各自保存的系统子私钥对该虚拟 CA 成员签名，得到的 t 个或 t-1 个 CA 成员子身份证书授予该虚拟 CA 成员，该虚拟 CA 成员对所述 t 个或 t-1 个 CA 成员身份子证书中系统子私钥对该虚拟 CA 成员的签名进行合法性认证通过

后，合成 CA 成员 t 身份证书，所述 CA 成员身份证书包含用门限签名算法合成的虚拟 CA 对所述 DT 的签名；

所述 CA 成员身份证书中签名的主体部分包括该虚拟 CA 成员的平台标识，或者同时包含该虚拟 CA 成员的平台标识和系统管理员标识。

6. 如权利要求 2 或 3 或 4 或 5 所述的认证方法，其特征在于：

所述 DT 将终端身份证书授予域终端时，还将自己的 DT 身份证书作为身份证明提供给所述域终端；

所述域终端收到所述终端身份证书和 DT 身份证书后，先基于所述 DT 身份证书对所述 DT 进行认证，认证通过后，再保存所述终端身份证书。

7. 如权利要求 3 所述的认证方法，其特征在于：

所述 DT 身份证书中签名的主体部分包括所述 DT 的域管理员标识和平台标识。

8. 如权利要求 1 或 2 或 3 或 4 或 5 或 7 所述的认证方法，其特征在于：

所述管理域的成员包括 PrivacyCA，所述可信计算系统除 PrivacyCA 外的其他成员均通过以下过程到所述 PrivacyCA 注册以获取平台身份证书：

所述其他成员以其可信计算平台中可信模块的签署证书为证明到所述 PrivacyCA 注册，保存所述 PrivacyCA 授予的平台身份证书；

所述 PrivacyCA 认证通过后，向所述其他成员授予平台身份证书，所述平台身份证书包含所述 PrivacyCA 对所述其他成员的签名。

9. 如权利要求 8 所述的认证方法，其特征在于：

所述其他成员到所述 PrivacyCA 注册的过程是在所述其他成员加入所述可信计算系统之前进行的；

在该过程中，所述 PrivacyCA 认证通过后，还为所述其他成员分配一个系统内唯一的平台标识，所述 PrivacyCA 授予所述其他成员的平台身份证书中签名的主体部分包含所述平台标识。

10. 如权利要求 1-5,7,9 中任一权利要求所述的认证方法，其特征在于：

所述终端身份证书中 DT 对所述域终端的签名的主体部分包括所述域终端的终端用户标识和平台标识。

11. 一种基于分布式网络环境的可信计算系统，该可信计算系统包括管理域和可信域，所述可信域的成员包括域可信方 (DT) 和域终端，其特征在于：

所述管理域用于接受 DT 的注册，对所述 DT 认证通过后，将管理域对所述 DT 的签名证书授予所述 DT；

所述域终端包括：

终端证书申请模块，用于以本域终端的平台身份证书为证明到所在可信域的 DT 注册，保存所述 DT 授予的终端身份证书；

远程认证模块，用于在与其他可信域的域终端交互时，向远程端提供终端身份证书，并基于远程端的终端身份证书对远程端进行身份认证；

所述 DT 包括：

DT 证书申请模块，用于以本 DT 的平台身份证书为证明到管理域注册，并保存管理域授予的签名证书；

终端证书颁发模块，用于接受域终端的注册，对所述域终端认证通过后，将终端身份证书授予所述域终端，所述终端身份证书包含管理域对本 DT 的签名和本 DT 对所述域终端的签名。

12. 如权利要求 11 所述的可信计算系统，其特征在于：

所述管理域的成员包括隐私证书权威 (PrivacyCA)；

所述 PrivacyCA 包括：

DT 证书颁发模块，用于接受 DT 的注册，对所述 DT 认证通过后，将 DT 身份证书授予所述 DT，所述 DT 身份证书包含所述 PrivacyCA 对所述 DT 的签名。

13. 如权利要求 11 所述的可信计算系统，其特征在于：

所述管理域的成员包括 PrivacyCA 和多个虚拟 CA 成员，其中：

所述 PrivacyCA 包括：

系统密钥管理模块，用于产生一对系统公私钥，公布门限签名和验证所需的公共参数，并将系统私钥秘密分发给虚拟 CA 成员；

所述多个虚拟 CA 成员基于 (t,n) 门限体制秘密共享所述系统私钥，共同构成虚拟 CA，其中，每一虚拟 CA 成员包括：

DT 证书颁发模块，用于接受 DT 的注册，对所述 DT 认证通过后，根据门限签名算法，用本虚拟 CA 成员保存的系统子私钥对所述 DT 签名，得到的 DT 身份子证书授予所述 DT；

所述 DT 的 DT 证书申请模块是分别到 t 个虚拟 CA 成员注册，得到 t 个 DT 身份子证书，对所述 t 个 DT 身份子证书中系统子私钥对所述 DT 的签名的合法性认证通过后，根据所述 t 个 DT 身份子证书合成 DT 身份证书，所述 DT 身份证书中包含用门限签名算法合成的虚拟 CA 对所述 DT 的签名。

14. 如权利要求 13 所述的可信计算系统，其特征在于：

所述虚拟 CA 成员的 DT 证书颁发模块将 DT 身份子证书授予所述 DT 时，还将自己的 CA 成员身份证书作为身份证明提供给所述 DT；

所述 DT 的 DT 证书申请模块收到所述 t 个 DT 身份子证书和相应的 CA 成员身份证书后，先基于所述 CA 成员身份证书对相应虚拟 CA 成员进行身份认证，认证通过后，再对所述 DT 身份子证书中的签名进行合法性认证。

15. 如权利要求 14 所述的可信计算系统，其特征在于：

每一虚拟 CA 成员还包括：

CA 成员证书申请模块，用于以其平台身份证书为证明到其他 t 个或 t-1 个虚拟 CA 成员注册，收到授予的 t 个或 t-1 个 CA 成员子证书后，对其中系统子私钥对本虚拟 CA 成员的签名进行合法性认证，认证通过后合成自己的 CA 成员身份证书，所述 CA 成员身份证书包含用门限签名算法合成的虚拟 CA 对所述 DT 的签名，该签名的主体部分包括该虚拟 CA 成员的平台标识，或者同时包含该虚拟 CA 成员的平台标识和系统管理员标识；

CA 成员证书颁发模块，用于接收另一虚拟 CA 成员的注册，对该另一虚拟 CA 成员认证通过后，用自己保存的系统子私钥对该另一虚拟 CA 成员签名，得到的 CA 成员身份子证书授予该另一虚拟 CA 成员。

16. 如权利要求 12 或 13 或 14 或 15 所述的可信计算系统，其特征在于：

所述 DT 的终端证书颁发模块将终端身份证书授予所述域终端时，还将自己的 DT 身份

证书作为身份证明提供给所述域终端；

所述域终端的终端证书申请模块收到所述终端身份证书和 DT 身份证书后，先基于所述 DT 身份证书对所述 DT 进行认证，认证通过后，再保存所述终端身份证书。

17. 如权利要求 13 所述的可信计算系统，其特征在于：

所述 DT 的 DT 证书申请模块合成的 DT 身份证书中签名的主体部分包括所述 DT 的域管理员标识和平台标识。

18. 如权利要求 11-15，17 中任一权利要求所述的可信计算系统，其特征在于：

所述管理域的成员包括隐私证书权威 (PrivacyCA)；

所述 PrivacyCA 包括：

平台证书颁发模块，用于接受系统其他成员的注册，认证通过后，向所述其他成员授予平台身份证书，所述平台身份证书包含所述 PrivacyCA 对所述其他成员的签名；

所述可信计算系统的其他成员还包括：

平台证书申请模块，用于以其可信计算平台中可信模块的签署证书为证明到所述 PrivacyCA 注册，保存所述 PrivacyCA 授予的平台身份证书。

19. 如权利要求 18 所述的可信计算系统，其特征在于：

所述系统其他成员的平台证书申请模块是在加入所述可信计算系统之前到所述 PrivacyCA 注册；

所述 PrivacyCA 的平台证书颁发模块在认证通过后，还为所述其他成员分配一个系统内唯一的平台标识，所述 PrivacyCA 授予所述其他成员的平台身份证书中签名的主体部分包含所述平台标识。

20. 如权利要求 11-15，17，19 中任一权利要求所述的可信计算系统，其特征在于：

所述 DT 的终端证书颁发模块授予域终端的终端身份证书中所述 DT 对域终端的签名的主体部分包括所述域终端的终端用户标识和平台标识。

21. 一种基于分布式网络环境的可信计算系统中的隐私证书权威 (PrivacyCA)，其特征在于：所述 PrivacyCA 包括：

平台证书颁发模块，用于接受系统其他成员的注册，认证通过后，向所述其他成员授予平台身份证书，所述平台身份证书包含所述 PrivacyCA 对所述其他成员的签名；

系统密钥管理模块，用于产生一对系统公私钥，公布门限签名和验证所需的公共参数，并将系统私钥秘密分发给虚拟 CA 成员。

22. 如权利要求 21 所述的 PrivacyCA，其特征在于：

所述平台证书颁发模块在认证通过后，还为所述其他成员分配一个系统内唯一的平台标识，所述 PrivacyCA 授予所述其他成员的平台身份证书中签名的主体部分包含所述平台标识。

23. 一种基于分布式网络环境的可信计算系统中的虚拟证书权威 (CA) 成员，其特征在于：

多个虚拟 CA 成员基于 (t，n) 门限体制秘密共享系统私钥，共同构成虚拟 CA，其中，每一虚拟 CA 成员包括：

平台证书申请模块，用于以其可信计算平台中可信模块的签署证书为证明到所述 PrivacyCA 注册，保存所述 PrivacyCA 授予的平台身份证书；

DT 证书颁发模块，用于接受 DT 的注册，对所述 DT 认证通过后，根据门限签名算法，用本虚拟 CA 成员保存的系统子私钥对所述 DT 签名，得到的 DT 身份子证书授予所述 DT。

24. 如权利要求 23 所述的虚拟证书 CA 成员，其特征在于，还包括：

CA 成员证书申请模块，用于以其平台身份证书为证明到其他 t 个或 t-1 个虚拟 CA 成员注册，收到授予的 t 个或 t-1 个 CA 成员子证书后，对其中系统子私钥对本虚拟 CA 成员的签名进行合法性认证，认证通过后合成自己的 CA 成员身份证书，所述 CA 成员身份证书包含用门限签名算法合成的虚拟 CA 对所述 DT 的签名，该签名的主体部分包括该虚拟 CA 成员的平台标识，或者同时包含该虚拟 CA 成员的平台标识和系统管理员标识；

CA 成员证书颁发模块，用于接收另一虚拟 CA 成员的注册，对该另一虚拟 CA 成员认证通过后，用自己保存的系统子私钥对该另一虚拟 CA 成员签名，得到的 CA 成员身份子证书授予该另一虚拟 CA 成员；

所述 DT 证书颁发模块将 DT 身份子证书授予所述 DT 时，还将自己的 CA 成员身份证书作为身份证明提供给所述 DT。

25. 一种基于分布式网络环境的可信计算系统中的域可信方 (DT)，其特征在于，所述 DT 包括：

平台证书申请模块，用于以其可信计算平台中可信模块的签署证书为证明到所述 PrivacyCA 注册，保存所述 PrivacyCA 授予的平台身份证书；

DT 证书申请模块，用于以本 DT 的平台身份证书为证明到管理域注册，并保存管理域授予的签名证书；

终端证书颁发模块，用于接受域终端的注册，对所述域终端认证通过后，将终端身份证书授予所述域终端，同时将自己的 DT 身份证书作为身份证明提供给所述域终端，所述终端身份证书包含管理域对本 DT 的签名和本 DT 对所述域终端的签名。

26. 如权利要求 25 所述的域可信方，其特征在于：

所述 DT 证书申请模块是分别到 t 个虚拟 CA 成员注册，得到 t 个 DT 身份子证书，对所述 t 个 DT 身份子证书中系统子私钥对所述 DT 的签名的合法性认证通过后，根据所述 t 个 DT 身份子证书合成 DT 身份证书，所述 DT 身份证书中包含用门限签名算法合成的虚拟 CA 对所述 DT 的签名。

27. 如权利要求 26 所述的域可信方，其特征在于：

所述 DT 证书申请模块收到所述 t 个 DT 身份子证书时还收到相应的 CA 成员身份证书，先基于所述 CA 成员身份证书对相应虚拟 CA 成员进行身份认证，认证通过后，再对所述 DT 身份子证书中的签名进行合法性认证。

28. 如权利要求 25 或 26 或 27 所述的域可信方，其特征在于：

所述终端证书颁发模块授予域终端的终端身份证书中所述 DT 对域终端的签名的主体部分包括所述域终端的终端用户标识和平台标识。

29. 如权利要求 26 或 27 所述的域可信方，其特征在于：

所述 DT 证书申请模块合成的 DT 身份证书中签名的主体部分包括所述 DT 的域管理员标识和平台标识。

30. 一种基于分布式网络环境的可信计算系统中的域终端，其特征在于：所述域终端包括：

平台证书申请模块，用于以其可信计算平台中可信模块的签署证书为证明到所述 PrivacyCA 注册，保存所述 PrivacyCA 授予的平台身份证书；

终端证书申请模块，用于以本域终端的平台身份证书为证明到所在可信域的 DT 注册，保存所述 DT 授予的终端身份证书；

远程认证模块，用于在与其他可信域的域终端交互时，向远程端提供终端身份证书，并基于远程端的终端身份证书对远程端进行身份认证。

31. 如权利要求 30 所述的域终端，其特征在于：

所述终端证书申请模块收到所述终端身份证书的同时还收到 DT 身份证书后，先基于所述 DT 身份证书对所述 DT 进行认证，认证通过后，再保存所述终端身份证书。

一种可信计算系统及相应的认证方法和设备

技术领域

[0001] 本申请涉及可信计算，更具体地，涉及一种具有分布式网络拓扑的可信计算系统及相应的认证方法和设备。

背景技术

[0002] 随着 Internet 的不断发展，分布式计算能力的不断加强，使得大范围的资源共享成为一种趋势。然而，由于分布式网络环境的开放性、不可控性及其资源的自治性，资源聚合与协同环境存在的不完整性、不一致性和不确定性等问题，传统的基于集中管理的安全机制已经不再适用。人们提出新的思路来保障终端安全，即可信计算技术。可信计算技术核心思想是在包括台式机、笔记本及智能手机等多种设备中，以所嵌入的可信平台模块 (Trusted Platform Module，TPM) 为核心为用户和平台（包括 TPM 和主机）提供安全保障。TPM 具有远程证明的能力，能够响应远程认证方的请求，证明平台身份和平台完整性等可信属性。可信计算组织 (Trusted Computing Group，TCG) 要求在远程证明过程中，有效的保护平台身份信息的隐私性，即 TPM 向认证方进行远程证明时不能暴露身份信息。

[0003] 为了解决远程证明时平台隐私信息的保护问题，TCG 先后采用 PCA 方法和 DAA 方法。

[0004] TCG 在其 TPM v1.1b 规范中提出了隐私证书权威 (Privacy Certificate Authority，PrivacyCA) 匿名认证系统，它采用 PrivacyCA 作为可信第三方为客户平台的 EK 证书签发别名证书来保证匿名性，并通过一次一密的方法保证平台的多次认证间的不可关联。

[0005] 针对密钥的不同用途，TCG 定义了七种类型的密钥，，其中与平台身份认证有关的主要密钥有：

[0006] 签署密钥 (EK，Endorsement Key)：用于唯一标识平台身份的密钥，一般由 TPM 生产商在制造 TPM 时生成。EK 影响到整个系统的安全性，它只用于两个操作：一是在确定平台属主时，解密属主的授权数据；二是生成 AIK 密钥并创建平台身份的别名证书。

[0007] 身份证明密钥 (AIK，Attestation Identity Key)：专用于对 TPM 产生的数据（如 PCRs 值等）进行签名，证明平台身份的合法性及平台环境的可信性。

[0008] 为了实现密钥的应用、管理及平台的可信证明，TCG 定义了五类证书，每类都被用于为特定操作提供必要的信息，包括：

[0009] 签署证书 (Endorsement Credential)：又称 EK 证书，一般由生成 EK 的厂商发布，包含 TPM 制造者名、TPM 型号、TPM 版本号和 EK 公钥等信息。EK 公钥虽然是公开的，但它是鉴别 TPM 身份的唯一证据，因此也具有秘密性和敏感性。

[0010] 身份证明证书 (AIK Credential)：又称 AIK 证书，用于鉴定对 PCR 值进行签名的 AIK 私钥，它包括 AIK 公钥和其它签发者认为有用的信息。AIK 证书是由一个可信的、能够校验各种证书和保护用户隐私的服务方签发。通过签发证书，服务方可以证明提供 TPM 信息的 TPM 是真实的。

[0011] 其他的还有一致性证书(Conformance Credential)、平台证书(Platform Endorsement Credential)和确认证书(Validation Credential)。

[0012] PrivacyCA系统简单易行,能实现平台的匿名认证,但PrivacyCA需要为平台的每次认证签发新的AIK证书,要求其高度可用,导致PrivacyCA可能成为整个认证系统的性能瓶颈,可能遭受DoS攻击而导致系统单点失效。

[0013] 2007年12月,中国国家密码管理局颁布了《可信计算密码支撑平台功能与接口规范》,该规范描述了可信计算密码支撑平台的功能原理与要求,并定义了可信计算密码支撑平台为应用层提供服务的接口规范,用以指导我国相关可信计算产品开发和应用。为实现远程证明过程中对平台身份匿名的保护,该规范定义了一个以可信第三方为中心的平台身份认证系统,以可信密码模块(TCM,Trusted Cryptographic Module)替代TPM作为可信根,其工作原理及签发证书的协议流程基本与TCG PrivacyCA系统相同,但为适应我国的国情,采用了双证书体系和不同的密码算法。其中的双证书包括平台身份证书和平台加密证书,其中,平台身份证书是为平台身份密钥(PIK,Platform Identity Key)的公钥签发的证书,也称为PIK证书。PIK是在TCM内部生成的一个SM2密钥对,用于对TCM内部的信息进行签名,实现平台身份认证和完整性报告;平台加密证书是为平台加密密钥(PEK,Platform Encryption Key)的公钥签发的证书,也称为PEK证书,它是TCM中与PIK证书相关联的数据加密证书。但该规范定义的认证系统存在与PrivacyCA系统相同的缺陷。

[0014] 为克服PrivacyCA系统的缺陷,TCG在TPM v1.2标准中提出了直接匿名认证(direct anonymous attestation,DAA)系统。DAA认证系统以C-L签名方案和基于离散对数的零知识证明为基础,并使用Fiat-Shamir启发式方法将知识证明转换为非交互式知识签名。DAA认证系统的主要参与方有签名方(Signer)、可信发布方(Issuer)和认证方(Verifier)。其工作时,首先,TPM基于EK公钥向可信发布方申请获得对于秘密数据(f_0,f_1)的C-L签名,也即获得关于(f_0,f_1)的DAA证书(A,e,v),之后的每次认证TPM与其相绑定的平台主机一起向认证方零知识证明其拥有秘密数据(f_0,f_1)及相关DAA证书(A,e,v),并用(f_0,f_1)计算了假名N_v,证明通过则该TPM对应平台的身份是可信的。由于认证采用的是零知识证明,认证方不能获知(f_0,f_1)及其证书(A,e,v),也就不能判断出证明平台的真实身份,实现了认证的匿名性。DAA认证系统在实现身份合法性认证的同时,也对AIK公钥进行签名,使得AIK成为EK的别名。

[0015] DAA使用DAA证书来代替原有的AIK证书,只需要申请一次并可以多次使用来保证可信平台的匿名性,且无需Privacy-CA的帮助。但DAA认证系统主要是面向范围较小、边界确定的网络环境,尤其适用于一个内部网络,只有在TPM与认证方信任共同的可信发布方的情况下才是适用的,其无法提供分属不同DAA域(向不同发布者申请DAA证明)的TPM与认证方或TPM与TPM之间的身份认证,也即目前的DAA认证系统仅适用于单信任域,对于跨域的认证不能提供信任关系。尽管可考虑采用允许一个TPM向多个不同DAA发布者申请不同DAA证明的方式来构建不同的TPM信任关系集合,但这种穷举所有信任关系的方法过于复杂冗余,而TPM能够保存的信息又十分有限,因而这种方法不可能在Internet环境中真正使用。

[0016] 对于这种跨域认证所存在的局限性,现有技术提出了一些解决方案。

[0017] 《计算机工程》第36卷第11期(2010年6月)公开的蒋李等所著的《基于动态信

任值的DAA跨域认证机制》中，提出一种通过建立域间信任关系来实现TPM用户跨域认证的方案，该方案将域间的信任值量化为一个[0,1]之间的实数，并和信任阈值比较，如果大于等于信任阈值，则两域之间建立暂时的信任关系，认可经本地域认证过的TPM用户，使其依据访问控制策略来访问远程域中的资源。现有DAA方案无法提供向分属不同DAA域的TPM的身份认证，为此该方案引入了信任值中心(TA)来计算并保存各域之间的信任值。在跨域认证时，TPM先向本域（域A）认证服务器提交对远程域B的访问请求，本域认证服务器认证通过后向远程域（域B）认证服务器发送该跨域访问请求，域B认证服务器认证通过后，计算对TPM的信任值并请求TA计算对域B对域A的信任值，如果该信任值大于阈值则向域A认证服务器返回允许消息，域A认证服务器认证是允许时，将票据(Ticket)发送给TPM，TPM持该票据访问远程域资源。

[0018] 《计算机应用》第30卷第8期(2010年8月）公开的周彦伟等所著的《分布式网络环境下的跨域匿名认证机制》中，提出的跨域认证框架包含可信第三方证书仲裁中心(Arbitration Center of Certificate，CAC)和多个可信域，每个可信域包括TCP和DAA证书颁发者(IS)，CAC对不同厂商DAA证书颁发者所签发AIK证书的真实性进行险证。可信域DO_A的可信计算平台TCP_A向另一可信域DO_B的服务提供商申请服务时，TCP_A首先通过本域DAA证书颁发者IS_A的DAA认证，获得其签发的AIK证书，然后向CAC发送跨域证书请求，TCP_A使用本地域AIK证书和自身的完整性度量值向CAC证明其身份，CAC通过与IS_A间的消息交互认证TCP_A的真实性和完整性，对持有合法AIK证书且平台完整的TCP_A颁发跨域认证证书，TCP_A使用跨域认证证书向可信域DO_B中的服务提供商证明其身份的真实性及平台的完整性。

[0019] 《计算机学报》第31卷第7期(2008年7月）公开的陈小峰等人所著的《一种多信任域内的直接匿名证明方案》中，提出一种跨域的DAA方案，该方案在DAA方案的基础上，在每一可信域增加了两个参与方：护照颁发者和签证颁发者。其跨域的基本思想是：如果信任域DO_A的可信计算平台HT_A(Host/TPM A)要向信任域DO_B的认证者V_B证明自己的身份，同时不暴露自己的隐私，那么首先HT_A向本地域的护照颁发者申请一个护照证书，该护照证书证明了HT_A在信任域DO_A中的身份，然后HT_A用该护照证书向信任域DO_B的签证颁发者申请签证证书，最后，HT_A用该护照证书和签证证书向信任域DO_B中的认证者V_B匿名地证明自己的身份。

[0020] 《计算机应用》第30卷第12期(2010年12)公开的李子臣等人所著的《改进的跨域直接匿名认证方案》中，将不同信任域内的DAA颁发者作为本域的一个代理成员，由其代理成员先对本域的可信平台进行身份认证，在确认合法的情况下颁发其信任域内的直接匿名证书，并将其身份、证书有效日期与直接匿名证书进行绑定。

[0021] 以上这些跨域认证方案都需要各个可信域的证书颁发者或者可信第三方（如第三方证书仲裁中心、信任值中心）参与颁发跨域认证所需的证书，其过程仍然过于复杂，有待研究更好的方案。

[0022] 申请内容

[0023] 有鉴于此，本申请要解决的技术问题是提供一种可信计算系统及相应的认证方法及设备。

[0024] 为了解决上述技术问题，本申请提出一种可信计算系统的认证方法，所述可信计

算系统包括管理域和多个可信域，所述可信域的成员包括域可信方 (DT) 和域终端，所述方法包括 ：

[0025] DT 以其平台身份证书为证明到管理域注册，管理域认证通过后，将管理域对所述 DT 的签名证书授予所述 DT ；

[0026] 域终端以其平台身份证书为证明到所在可信域的 DT 注册，所述 DT 认证通过后，将终端身份证书授予所述域终端，所述终端身份证书包含管理域对所述 DT 的签名和所述 DT 对所述域终端的签名 ；

[0027] 不同可信域的域终端之间交互时，基于远程端的终端身份证书实现对远程端身份的远程认证。

[0028] 较佳地，上述认证方法中，

[0029] 所述管理域的成员包括隐私证书权威 (PrivacyCA) ；

[0030] 所述管理域认证通过后，将管理域对所述 DT 的签名证书授予所述 DT，包括 ：所述 PrivacyCA 认证通过后，将 DT 身份证书授予所述 DT，所述 DT 身份证书包含所述 PrivacyCA 对所述 DT 的签名。

[0031] 较佳地，上述认证方法中，

[0032] 所述管理域的成员包括隐私证书权威 (PrivacyCA) 和多个虚拟 CA 成员，所述认证方法还包括以下虚拟 CA 的建立过程 ：

[0033] 所述 PrivacyCA 产生一对系统公私钥，公布门限签名和验证所需的公共参数，并将系统私钥秘密分发给虚拟 CA 成员 ；

[0034] 各虚拟 CA 成员基于 (t,n) 门限体制秘密共享所述系统私钥，构成虚拟 CA，每一虚拟 CA 成员保存一份系统子私钥 ；

[0035] 所述 DT 以其平台身份证书为证明到管理域注册是分别到 t 个虚拟 CA 成员注册 ；所述管理域认证通过后，将管理域对所述 DT 的签名证书授予所述 DT，包括 ：所述 t 个虚拟 CA 成员分别认证通过后，根据门限签名算法用各自保存的系统子私钥对所述 DT 签名得到 t 个子 DT 身份子证书并授予所述 DT，所述 DT 对所述 t 个 DT 身份子证书中系统子私钥对所述 DT 的签名的合法性认证通过后，根据所述 t 个 DT 身份子证书合成 DT 身份证书，所述 DT 身份证书包含用门限签名算法合成的虚拟 CA 对所述 DT 的签名。

[0036] 较佳地，上述认证方法中，

[0037] 所述 t 个虚拟 CA 成员用各自保存的系统子私钥对所述 DT 签名得到 t 个 DT 身份子证书并授予所述 DT 时，还将自己的 CA 成员身份证书作为身份证明提供给所述 DT ；

[0038] 所述 DT 收到所述 DT 身份子证书和 CA 成员身份证书后，先基于所述 CA 成员身份证书对相应虚拟 CA 成员进行身份认证，认证通过后，再对所述 DT 身份子证书中的签名进行合法性认证。

[0039] 较佳地，上述认证方法中，

[0040] 所述 CA 成员身份证书是虚拟 CA 成员通过以下过程得到的 ：

[0041] 一虚拟 CA 成员以其平台身份证书为证明到其他 t 个或 t-1 个虚拟 CA 成员注册，所述其他 t 个或 t-1 个虚拟 CA 成员验证通过后，用各自保存的系统子私钥对该虚拟 CA 成员签名，得到的 t 个或 t-1 个 CA 成员子身份证书授予该虚拟 CA 成员，该虚拟 CA 成员对所述 t 个或 t-1 个 CA 成员身份子证书中系统子私钥对该虚拟 CA 成员的签名进行合法性认证

通过后，合成 CA 成员 t 身份证书，所述 CA 成员身份证书包含用门限签名算法合成的虚拟 CA 对所述 DT 的签名；

[0042] 所述 CA 成员身份证书中签名的主体部分包括该虚拟 CA 成员的平台标识，或者同时包含该虚拟 CA 成员的平台标识和系统管理员标识。

[0043] 较佳地，上述认证方法中，

[0044] 所述 DT 将终端身份证书授予域终端时，还将自己的 DT 身份证书作为身份证明提供给所述域终端；

[0045] 所述域终端收到所述终端身份证书和 DT 身份证书后，先基于所述 DT 身份证书对所述 DT 进行认证，认证通过后，再保存所述终端身份证书。

[0046] 较佳地，上述认证方法中，

[0047] 所述 DT 身份证书中签名的主体部分包括所述 DT 的域管理员标识和平台标识。

[0048] 较佳地，上述认证方法中，

[0049] 所述管理域的成员包括 PrivacyCA，所述可信计算系统除 PrivacyCA 外的其他成员均通过以下过程到所述 PrivacyCA 注册以获取平台身份证书：

[0050] 所述其他成员以其可信计算平台中可信模块的签署证书为证明到所述 PrivacyCA 注册，保存所述 PrivacyCA 授予的平台身份证书；

[0051] 所述 PrivacyCA 认证通过后，向所述其他成员授予平台身份证书，所述平台身份证书包含所述 PrivacyCA 对所述其他成员的签名。

[0052] 较佳地，上述认证方法中，

[0053] 所述其他成员到所述 PrivacyCA 注册的过程是在所述其他成员加入所述可信计算系统之前进行的；

[0054] 在该过程中，所述 PrivacyCA 认证通过后，还为所述其他成员分配一个系统内唯一的平台标识，所述 PrivacyCA 授予所述其他成员的平台身份证书中签名的主体部分包含所述平台标识。

[0055] 较佳地，上述认证方法中，

[0056] 所述终端身份证书中 DT 对所述域终端的签名的主体部分包括所述域终端的终端用户标识和平台标识。

[0057] 相应地，本申请还提供了一种基于分布式网络环境的可信计算系统，该可信计算系统包括管理域和可信域，所述可信域的成员包括域可信方 (DT) 和域终端，其特征在于：

[0058] 所述管理域用于接受 DT 的注册，对所述 DT 认证通过后，将管理域对所述 DT 的签名证书授予所述 DT；

[0059] 所述域终端包括：

[0060] 终端证书申请模块，用于以本域终端的平台身份证书为证明到所在可信域的 DT 注册，保存所述 DT 授予的终端身份证书；

[0061] 远程认证模块，用于在与其他可信域的域终端交互时，向远程端提供终端身份证书，并基于远程端的终端身份证书对远程端进行身份认证；

[0062] 所述 DT 包括：

[0063] DT 证书申请模块，用于以本 DT 的平台身份证书为证明到管理域注册，并保存管理域授予的签名证书；

[0064] 终端证书颁发模块，用于接受域终端的注册，对所述域终端认证通过后，将终端身份证书授予所述域终端，所述终端身份证书包含管理域对本 DT 的签名和本 DT 对所述域终端的签名。

[0065] 较佳地，上述可信计算系统中，

[0066] 所述管理域的成员包括隐私证书权威 (PrivacyCA)；

[0067] 所述 PrivacyCA 包括：

[0068] DT 证书颁发模块，用于接受 DT 的注册，对所述 DT 认证通过后，将 DT 身份证书授予所述 DT，所述 DT 身份证书包含所述 PrivacyCA 对所述 DT 的签名。

[0069] 较佳地，上述可信计算系统中，

[0070] 所述管理域的成员包括 PrivacyCA 和多个虚拟 CA 成员，其中：

[0071] 所述 PrivacyCA 包括：

[0072] 系统密钥管理模块，用于产生一对系统公私钥，公布门限签名和验证所需的公共参数，并将系统私钥秘密分发给虚拟 CA 成员；

[0073] 所述多个虚拟 CA 成员基于 (t,n) 门限体制秘密共享所述系统私钥，共同构成虚拟 CA，其中，每一虚拟 CA 成员包括：

[0074] DT 证书颁发模块，用于接受 DT 的注册，对所述 DT 认证通过后，根据门限签名算法，用本虚拟 CA 成员保存的系统子私钥对所述 DT 签名，得到的 DT 身份子证书授予所述 DT；

[0075] 所述 DT 的 DT 证书申请模块是分别到 t 个虚拟 CA 成员注册，得到 t 个 DT 身份子证书，对所述 t 个 DT 身份子证书中系统子私钥对所述 DT 的签名的合法性认证通过后，根据所述 t 个 DT 身份子证书合成 DT 身份证书，所述 DT 身份证书中包含用门限签名算法合成的虚拟 CA 对所述 DT 的签名。

[0076] 较佳地，上述可信计算系统中，

[0077] 所述虚拟 CA 成员的 DT 证书颁发模块将 DT 身份子证书授予所述 DT 时，还将自己的 CA 成员身份证书作为身份证明提供给所述 DT；

[0078] 所述 DT 的 DT 证书申请模块收到所述 t 个 DT 身份子证书和相应的 CA 成员身份证书后，先基于所述 CA 成员身份证书对相应虚拟 CA 成员进行身份认证，认证通过后，再对所述 DT 身份子证书中的签名进行合法性认证。

[0079] 较佳地，上述可信计算系统中，

[0080] 每一虚拟 CA 成员还包括：

[0081] CA 成员证书申请模块，用于以其平台身份证书为证明到其他 t 个或 t-1 个虚拟 CA 成员注册，收到授予的 t 个或 t-1 个 CA 成员子证书后，对其中系统子私钥对本虚拟 CA 成员的签名进行合法性认证，认证通过后合成自己的 CA 成员身份证书，所述 CA 成员身份证书包含用门限签名算法合成的虚拟 CA 对所述 DT 的签名，该签名的主体部分包括该虚拟 CA 成员的平台标识，或者同时包含该虚拟 CA 成员的平台标识和系统管理员标识；

[0082] CA 成员证书颁发模块，用于接收另一虚拟 CA 成员的注册，对该另一虚拟 CA 成员认证通过后，用自己保存的系统子私钥对该另一虚拟 CA 成员签名，得到的 CA 成员身份子证书授予该另一虚拟 CA 成员。

[0083] 较佳地，上述可信计算系统中，

[0084] 所述 DT 的终端证书颁发模块将终端身份证书授予所述域终端时，还将自己的 DT

身份证书作为身份证明提供给所述域终端；

[0085] 所述域终端的终端证书申请模块收到所述终端身份证书和 DT 身份证书后，先基于所述 DT 身份证书对所述 DT 进行认证，认证通过后，再保存所述终端身份证书。

[0086] 较佳地，上述可信计算系统中，

[0087] 所述 DT 的 DT 证书申请模块合成的 DT 身份证书中签名的主体部分包括所述 DT 的域管理员标识和平台标识。

[0088] 较佳地，上述可信计算系统中，

[0089] 所述管理域的成员包括隐私证书权威 (PrivacyCA)；

[0090] 所述 PrivacyCA 包括：

[0091] 平台证书颁发模块，用于接受系统其他成员的注册，认证通过后，向所述其他成员授予平台身份证书，所述平台身份证书包含所述 PrivacyCA 对所述其他成员的签名；

[0092] 所述可信计算系统的其他成员还包括：

[0093] 平台证书申请模块，用于以其可信计算平台中可信模块的签署证书为证明到所述 PrivacyCA 注册，保存所述 PrivacyCA 授予的平台身份证书。

[0094] 较佳地，上述可信计算系统中，

[0095] 所述系统其他成员的平台证书申请模块是在加入所述可信计算系统之前到所述 PrivacyCA 注册；

[0096] 所述 PrivacyCA 的平台证书颁发模块在认证通过后，还为所述其他成员分配一个系统内唯一的平台标识，所述 PrivacyCA 授予所述其他成员的平台身份证书中签名的主体部分包含所述平台标识。

[0097] 较佳地，上述可信计算系统中，

[0098] 所述 DT 的终端证书颁发模块授予域终端的终端身份证书中所述 DT 对域终端的签名的主体部分包括所述域终端的终端用户标识和平台标识。

[0099] 相应地，本申请还提供了一种上述可信计算系统中的隐私证书权威 (PrivacyCA)，其特征在于：所述 PrivacyCA 包括：

[0100] 平台证书颁发模块，用于接受系统其他成员的注册，认证通过后，向所述其他成员授予平台身份证书，所述平台身份证书包含所述 PrivacyCA 对所述其他成员的签名；

[0101] 系统密钥管理模块，用于产生一对系统公私钥，公布门限签名和验证所需的公共参数，并将系统私钥秘密分发给虚拟 CA 成员。

[0102] 较佳地，所述平台证书颁发模块在认证通过后，还为所述其他成员分配一个系统内唯一的平台标识，所述 PrivacyCA 授予所述其他成员的平台身份证书中签名的主体部分包含所述平台标识。

[0103] 相应地，本申请还提供了一种上述可信计算系统中的虚拟证书权威 (CA) 成员，其特征在于：

[0104] 多个虚拟 CA 成员基于 (t,n) 门限体制秘密共享系统私钥，共同构成虚拟 CA，其中，每一虚拟 CA 成员包括：

[0105] 平台证书申请模块，用于以其可信计算平台中可信模块的签署证书为证明到所述 PrivacyCA 注册，保存所述 PrivacyCA 授予的平台身份证书；

[0106] DT 证书颁发模块，用于接受 DT 的注册，对所述 DT 认证通过后，根据门限签名算法，

用本虚拟 CA 成员保存的系统子私钥对所述 DT 签名，得到的 DT 身份子证书授予所述 DT。

[0107] 较佳地，上述虚拟证书 CA 成员还包括：

[0108] CA 成员证书申请模块，用于以其平台身份证书为证明到其他 t 个或 t-1 个虚拟 CA 成员注册，收到授予的 t 个或 t-1 个 CA 成员子证书后，对其中系统子私钥对本虚拟 CA 成员的签名进行合法性认证，认证通过后合成自己的 CA 成员身份证书，所述 CA 成员身份证书包含用门限签名算法合成的虚拟 CA 对所述 DT 的签名，该签名的主体部分包括该虚拟 CA 成员的平台标识，或者同时包含该虚拟 CA 成员的平台标识和系统管理员标识；

[0109] CA 成员证书颁发模块，用于接收另一虚拟 CA 成员的注册，对该另一虚拟 CA 成员认证通过后，用自己保存的系统子私钥对该另一虚拟 CA 成员签名，得到的 CA 成员身份子证书授予该另一虚拟 CA 成员。

[0110] 所述 DT 证书颁发模块将 DT 身份子证书授予所述 DT 时，还将自己的 CA 成员身份证书作为身份证明提供给所述 DT。

[0111] 相应地，本申请还提供了一种上述可信计算系统中的域可信方 (DT)，所述 DT 包括：

[0112] 平台证书申请模块，用于以其可信计算平台中可信模块的签署证书为证明到所述 PrivacyCA 注册，保存所述 PrivacyCA 授予的平台身份证书；

[0113] DT 证书申请模块，用于以本 DT 的平台身份证书为证明到管理域注册，并保存管理域授予的签名证书；

[0114] 终端证书颁发模块，用于接受域终端的注册，对所述域终端认证通过后，将终端身份证书授予所述域终端，同时将自己的 DT 身份证书作为身份证明提供给所述域终端，所述终端身份证书包含管理域对本 DT 的签名和本 DT 对所述域终端的签名。

[0115] 较佳地，所述 DT 证书申请模块是分别到 t 个虚拟 CA 成员注册，得到 t 个 DT 身份子证书，对所述 t 个 DT 身份子证书中系统子私钥对所述 DT 的签名的合法性认证通过后，根据所述 t 个 DT 身份子证书合成 DT 身份证书，所述 DT 身份证书中包含用门限签名算法合成的虚拟 CA 对所述 DT 的签名。

[0116] 较佳地，所述 DT 证书申请模块收到所述 t 个 DT 身份子证书时还收到相应的 CA 成员身份证书，先基于所述 CA 成员身份证书对相应虚拟 CA 成员进行身份认证，认证通过后，再对所述 DT 身份子证书中的签名进行合法性认证。

[0117] 较佳地，所述终端证书颁发模块授予域终端的终端身份证书中所述 DT 对域终端的签名的主体部分包括所述域终端的终端用户标识和平台标识。

[0118] 较佳地，所述 DT 证书申请模块合成的 DT 身份证书中签名的主体部分包括所述 DT 的域管理员标识和平台标识。

[0119] 相应地，本申请还提供了一种上述可信计算系统中的域终端，所述域终端包括：

[0120] 平台证书申请模块，用于以其可信计算平台中可信模块的签署证书为证明到所述 PrivacyCA 注册，保存所述 PrivacyCA 授予的平台身份证书；

[0121] 终端证书申请模块，用于以本域终端的平台身份证书为证明到所在可信域的 DT 注册，保存所述 DT 授予的终端身份证书；

[0122] 远程认证模块，用于在与其他可信域的域终端交互时，向远程端提供终端身份证书，并基于远程端的终端身份证书对远程端进行身份认证。

[0123] 较佳地，所述终端证书申请模块收到所述终端身份证书的同时还收到 DT 身份证书后，先基于所述 DT 身份证书对所述 DT 进行认证，认证通过后，再保存所述终端身份证书。

[0124] 本申请的实施方式中，可信计算系统的认证方法及相应系统采用基于可信域的分布式网络拓扑，便于扩展来应对不同规模可信域的集成。

[0125] 本申请的实施方式中，域终端使用从所在可信域的 DT 得到终端身份证书就可以实现跨域认证，不用针对每个可信域去申请证书，这减少了网络流量、计算负载和存储空间，提高了分布式网络跨域认证的效率。

[0126] 本申请的实施方式中，采用虚拟 CA 代替 PrivacyCA 向 DT 颁发 DT 身份证书，多个虚拟 CA 成员按 (t,n) 门限体制来共享系统私钥，可以避免伪冒攻击、单点 DOS 攻击和失效，也使得 PrivacyCA 只在系统其他成员注册时授予这些成员平台身份证书，之后的认证过程无需 PrivacyCA 参与，可以有效地保护 PrivacyCA，提高系统的保密性能。

[0127] 本申请的实施方式中，在授予系统成员的证书中将该成员的使用者标识和平台标识绑定，可以有效地防止平台替换攻击。

附图说明

[0128] 图 1 为本申请实施例的可信计算系统的架构示意图；

[0129] 图 2 为本申请实施例各系统成员的模块图；

[0130] 图 3 为本申请实施例认证方法的总体流程图；

[0131] 图 4 是本申请实施例认证方法中，可信域的成员到 PrivacyCA 注册以申请平台身份证书的流程图；

[0132] 图 5 是本申请实施例认证方法中，虚拟 CA 的建立过程的流程图；

[0133] 图 6 是本申请实施例认证方法中，DT 到管理域虚拟 CA 注册的流程图；

[0134] 图 7 是本申请实施例认证方法中，域终端到所在可信域的 DT 注册的流程图；

[0135] 图 8 是本申请实施例认证方法中，虚拟 CA 成员到其他虚拟 CA 成员注册的流程图；

[0136] 图 9 为本申请一个应用示例的架构及流程示意图。

具体实施方式

[0137] 为使本申请的目的、技术方案和优点更加清楚明白，下文中将结合附图对本申请的实施例进行详细说明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

[0138] 如图 1 所示，本实施例的可信计算系统包括管理域和多个可信域，管理域和可信域均包含若干成员。作为可信计算系统的成员，所有成员的可信计算平台都具有嵌入在硬件平台上的可信模块（如 TPM、TCM 等），每个可信模块内保存有一对能唯一标识自己的签署密钥 (EK，Endorsement Key) 和相应的 EK 证书。

[0139] 管理域用于接受域可信方 (DT) 的注册，对 DT 认证通过后，将管理域对所述 DT 的签名证书授予 DT。

[0140] 可信域的成员包括域可信方 (DT) 和域终端，DT 也可称为可信域服务器，DT 的使用者称为域管理员。域终端即可信域中的普通成员，域终端的使用者称为终端用户。DT 用于以其平台身份证书为证明到管理域获取管理域授予的签名证书，及接受域终端的注册，

将终端身份证书授予认证通过的域终端，所述终端身份证书包含管理域对本 DT 的签名和本 DT 对域终端的签名。域终端用于以其平台身份证书为证明到所在可信域的 DT 注册，获取 DT 授予的终端身份证书，及在与其他可信域的域终端交互时，基于远程端的终端身份证书实现对远程端的远程身份认证。

[0141] 本实施例中，管理域的成员包括隐私证书权威 (PrivacyCA)10 和多个虚拟 CA 成员 20，其中虚拟 CA 成员也可称为管理域服务器，其使用者称为系统管理员。请参照图 2（仅画出一可信域 A 作为示例），其中：

[0142] Privacy CA10 包括：

[0143] 系统密钥管理模块 102，用于产生一对系统公私钥，公布门限签名和验证所需的公共参数，并将系统私钥秘密分发给虚拟 CA 成员。

[0144] 平台证书颁发模块 104，用于接受系统其他成员的注册，认证通过后，向所述其他成员授予平台身份证书，所述平台身份证书包含所述 PrivacyCA 对所述其他成员的签名。这里的其他成员包括可信域的所有成员如 DT、域终端以及管理域除 Privacy CA 之外的其他成员如虚拟 CA 成员。

[0145] 所述多个虚拟 CA 成员基于 (t,n) 门限体制秘密共享系统私钥，共同构成虚拟 CA，这些虚拟 CA 成员可由 Privacy CA 指定，也可由系统中的终端申请，经 Privacy CA 批准后成为虚拟 CA 成员。

[0146] 其中，每一虚拟 CA 成员 20 包括：

[0147] DT 证书颁发模块 202，用于接受 DT 的注册，对所述 DT 认证通过后，根据门限签名算法，用本虚拟 CA 成员保存的系统子私钥对所述 DT 签名，得到的 DT 身份子证书授予所述 DT。此外，DT 证书颁发模块将 DT 身份子证书授予所述 DT 时，还可以将自己的 CA 成员身份证书作为身份证明提供给所述 DT。

[0148] CA 成员证书申请模块 204，用于以其平台身份证书为证明到其他 t 个或 t-1 个虚拟 CA 成员注册，收到授予的 t 个或 t-1 个 CA 成员子证书后，对其中系统子私钥对本虚拟 CA 成员的签名进行合法性认证，认证通过后合成自己的 CA 成员身份证书，所述 CA 成员身份证书包含用门限签名算法合成的虚拟 CA 对所述 DT 的签名，该签名的主体部分可以包括该虚拟 CA 成员的平台标识，也可以同时包含该虚拟 CA 成员的平台标识和系统管理员标识，以使验证方如 DT 实现对该虚拟 CA 成员的平台身份和使用者身份的同时认证。

[0149] CA 成员证书颁发模块 206，用于接收另一虚拟 CA 成员的注册，基于密钥交换协议对该另一虚拟 CA 成员认证通过后，用自己保存的系统子私钥对该另一虚拟 CA 成员签名，得到的 CA 成员子证书授予该另一虚拟 CA 成员。

[0150] 平台证书申请模块 208，用于以其可信计算平台中可信模块的签署证书为证明到所述 PrivacyCA 注册，并保存所述 PrivacyCA 授予的平台身份证书。

[0151] 管理域还可以包括相应的数据库，如 PrivacyCA 管理的用户信息及平台身份证书库，虚拟 CA 管理的 DT 身份证书库和 CA 成员身份证书库等。在一示例中，系统成员可通过如图 1 所示的 Web 服务器访问相应的数据库。

[0152] 可信域的成员中，域可信方 30 包括：

[0153] 平台证书申请模块 302，用于以其可信计算平台中可信模块的签署证书为证明到所述 PrivacyCA 注册，保存所述 PrivacyCA 授予的平台身份证书。

[0154] DT 证书申请模块 304，用于以本 DT 的平台身份证书为证明到管理域注册，并保存管理域授予的签名证书。本实施例中，DT 证书申请模块是分别到 t 个虚拟 CA 成员注册，得到 t 个 DT 身份子证书，对所述 t 个 DT 身份子证书中系统子私钥对所述 DT 的签名的合法性认证通过后，根据所述 t 个 DT 身份子证书合成 DT 身份证书，所述 DT 身份证书中包含用门限签名算法合成的虚拟 CA 对所述 DT 的签名，该签名的主体部分可以同时包括所述 DT 的域管理员标识和平台标识，以使验证方如域终端实现对 DT 的平台身份和使用者身份的同时认证。在虚拟 CA 成员提供自己的 CA 成员身份证书时，DT 证书申请模块收到所述 t 个 DT 身份子证书和相应的 CA 成员身份证书后，先基于所述 CA 成员身份证书对相应的虚拟 CA 成员进行认证，认证通过后，再对所述 DT 的签名的合法性进行认证。

[0155] 终端证书颁发模块 306，用于接受域终端的注册，对所述域终端认证通过后，将终端身份证书授予所述域终端，所述终端身份证书包含管理域对本 DT 的签名和本 DT 对所述域终端的签名，其中本 DT 对所述域终端的签名的主体部分可以同时包括域终端的终端用户标识和平台标识，以使验证方如另一域终端可以实现对该域终端的平台身份和使用者身份的同时认证。本实施例的终端证书颁发模块将终端身份证书授予所述域终端时，还可以将自己的 DT 身份证书作为身份证明提供给所述域终端。

[0156] 域终端 40 包括：

[0157] 平台证书申请模块 402，用于以其可信计算平台中可信模块的签署证书为证明到所述 PrivacyCA 注册，保存所述 PrivacyCA 授予的平台身份证书。

[0158] 终端证书申请模块 404，用于以本域终端的平台身份证书为证明到所在可信域的 DT 注册，保存所述 DT 授予的终端身份证书。在 DT 同时提供 DT 身份证书时，先基于所述 DT 身份证书对所述 DT 进行认证，认证通过后，再保存所述终端身份证书。

[0159] 远程认证模块 406，用于在与其他可信域的域终端交互时，向远程端提供终端身份证书，并基于远程端的终端身份证书对远程端进行身份认证。

[0160] 本实施例的认证方法如图 3 所示，其总体流程包括：

[0161] 步骤 1，DT 以其平台身份证书为证明到管理域注册，管理域认证通过后，将 DT 身份证书授予该 DT，该 DT 身份证书包含管理域对该 DT 的签名；

[0162] 本实施例的各种证书可以遵循 X.509 标准（但不局限于此），证书中包括主体部分 (tbsCertificate)、签名算法标识部分 (signature Algorithm) 和签名值部分 (signature Value)，signature Value 是使用 signature Algorithm 部分指定的签名算法对 tbsCertificate 证书主题部分签名后的值。文中，将证书中的主体部分和签名值部分统称为签名。其中主体部分中包括证书版本号、证书序列号、证书主体名称、证书公钥、证书发行者名称、证书有效期等字段，还可以包括证书发行者 ID、证书主体 ID 和证书扩展段等字段，其中证书公钥可用于加密和 / 或身份证明，不再详细说明。

[0163] 较佳地，本实施例的 DT 身份证书中签名的主体部分，除了包括 DT 的可信计算平台的平台标识外，还包括 DT 的合法使用者的 ID 即域管理员 ID。也就是说，在授予 DT 的 DT 身份证书中将该 DT 的平台 ID 和域管理员 ID 绑定在一起，验证方如域终端基于 DT 身份证书对该 DT 认证时，可以实现对该 DT 的平台和使用者的同时认证，避免非法使用者使用合法的 DT 平台进行的平台替换攻击。

[0164] 步骤 2，域终端以其平台身份证书为证明到所在可信域的 DT 注册，所述 DT 认证通

过后，将终端身份证书授予所述域终端，所述终端身份证书包含管理域对所述 DT 的签名和所述 DT 对所述域终端的签名；

[0165] 本步中，DT 将终端身份证书授予域终端时，可将自己的 DT 身份证书作为身份证明提供给所述域终端；域终端收到授予的所述终端身份证书和所述 DT 的 DT 身份证书后，先基于所述 DT 身份证书对所述 DT 进行认证，认证通过后，再保存所述终端身份证书。

[0166] 较佳地，终端身份证书中 DT 对域终端的签名的主体部分，包括域终端的平台标识和终端用户标识。将该域终端的用户 ID 和平台 ID 绑定在一起。这样可以避免非法用户利用合法平台进行平台替换攻击。

[0167] 步骤 3，不同可信域的域终端之间交互时，基于远程端的终端身份证书实现对远程端的身份认证。

[0168] 例如，可信域 A 的域终端 A 与可信域 B 的域终端 B 交互时，域终端 A 基于域终端 B 的终端身份证书实现对域终端 B 身份的远程认证，域终端 B 基于域终端 A 的终端身份证书实现对域终端 A 身份的远程认证。

[0169] 由于 DT 身份证书包含管理域对 DT 的签名，信任链由管理域传递到该 DT。而终端身份证书同时包含管理域对 DT 的签名和 DT 对该域终端的签名，信任链就由管理域传递到该域终端。其他可信域的域终端得到所在可信域 DT 授予的终端身份证书后，通过对管理域对 DT 签名的校验和对该 DT 对域终端的签名的校验，就可以信任该域终端，实现跨域认证，不需要到每个可信域去申请证书，这便于可信域管理的独立性，减少了网络流量、计算负载和存储空间从而提高了分布式网络跨域认证的效率。

[0170] 本实施例的认证方法可以包括以下可信计算系统除 PrivacyCA 外的其他成员到 PrivacyCA 注册以申请平台身份证书的过程，该过程可以在所述其他成员加入可信计算系统之前完成，如图 4 所示，该过程包括：

[0171] 步骤 110，所述其他成员的可信计算平台在所有者的授权下，其内部的可信模块生成一对平台身份公私钥，平台身份私钥保存在可信模块内部；

[0172] 此处的可信模块可以是不同标准的可信模块如 TPM 或者 TCM，可信模块嵌入于所在可信计算平台中。

[0173] 步骤 120，所述其他成员的可信计算平台以 EK 证书为身份证明，向 PrivacyCA 申请注册，携带 EK 证书和生成的平台身份公钥；

[0174] 步骤 130，PrivacyCA 认证通过后，向所述其他成员授予平台身份证书，该平台身份证书包含 PrivacyCA 对所述其他成员的签名。

[0175] 较佳地，PrivacyCA 认证通过后，还为所述其他成员分配一个系统内唯一的平台标识以标识所述成员的可信计算平台，所述 PrivacyCA 对所述其他成员的签名的主体部分包含所述平台标识。为不同可信域的成员建立系统内的统一标识，方便对系统的可信计算平台的统一管理及跨域认证的实现。

[0176] 上述申请平台身份证书的过程可以采用 PCA 系统中 TPM 获取 AIK 证书或中国规范中 TPM 获取 PIK 证书的方式，但不局限于此，这里不再赘述。Privacy-CA 签发的平台身份证书作为 EK 在系统内的别名证书，可以向系统的其他成员证明该平台身份的合法性。

[0177] 秘密共享是现代密码学领域中一个非常重要的分支，也是信息安全方向一个重要的研究内容。第一个秘密共享方案是 (t，n) 门限体制方案，该方案是 Shamir[1] 和

Blakley[2] 在 1979 年分别基于 Lagrange 插值法和多维空间点的性质提出的，秘密共享概念被提出后，许多研究人员对其做了大量的研究，并取得了不少成果。所述 (t,n) 门限体制是将秘密 s，分成 n 份，由每一个参与者保存一份秘密份额，为了重构秘密 s，，需要至少 t 个参与者合作。

[0178] 本申请将 (t,n) 门限体制运用于可信计算系统的虚拟 CA 的建立，由 PrivacyCA 作为秘密分发者，其生成的系统私钥作为秘密 s，n 个虚拟 CA 成员作为参与者，每一个虚拟 CA 成员保存一份秘密份额（称为系统子私钥）。重构者需要得到至少 t 个虚拟 CA 成员保存的系统子私钥或用系统子私钥计算出的伪份额，才能恢复出系统私钥。

[0179] 本实施例中，虚拟 CA 的建立过程如图 5 所示，包括：

[0180] 步骤 210，所述 PrivacyCA 产生一对系统公私钥，公布门限签名和验证所需的公共参数，并将系统私钥秘密分发给虚拟 CA 成员；

[0181] Privacy-CA 可以采用 RSA 算法、SM2 等密钥生成算法来生成上述系统公私钥。产生的一对系统公私钥可以存放在系统的密钥池中。

[0182] 步骤 220，各虚拟 CA 成员基于 (t,n) 门限体制秘密共享所述系统私钥。

[0183] 构造的虚拟 CA 可以代替 PrivacyCA 来为可信域的 DT 颁发 DT 身份证书。可信域成员从 PrivacyCA 取得平台身份证书后，之后的证书获取和认证的过程都不需要 PrivacyCA 参与，避免了由 PrivacyCA 一个节点进行身份证书颁发时带来的单点 DOS 攻击和失效的问题，而多个虚拟 CA 成员共同来颁发 DT 身份证书，也提高了隐私性。

[0184] 本实施例中，DT 到管理域注册的过程如图 6 所示，包括：

[0185] 步骤 310，DT 以其平台身份证书为身份证明，向 t 个虚拟 CA 成员提交注册申请，同时携带本 DT 的平台 ID；

[0186] 可信域的 DT 可以由 Privacy CA 指定，也可由可信域的域终端申请，由 Privacv CA 批准成为 DT。

[0187] 步骤 320，各虚拟 CA 成员对所述 DT 进行认证，认证通过后，分别向该 DT 授予 DT 身份子证书，每一 DT 身份子证书中包含相应虚拟 CA 成员用其保存的系统子私钥对该 DT 的签名；

[0188] 步骤 330，DT 根据得到的 t 个 DT 身份子证书合成 DT 身份证书，所述 DT 身份证书中包含用门限签名算法合成的虚拟 CA 对所述 DT 的签名。

[0189] 基于门限体制的签名和验证方案目前已提出很多，如文献 [1]R Gennaro，S Jarecki，HKrawczyk，TRabin.Robust threshold DSS signatures.In:Eurocrypt'96，LNCS1070.Berlin:Springer-Verlag,1996.354-371；文献 [2]Ronald Cramer，Ivan Damgard，Ueli Maurer.General secure multi-party computation from any linear secret sharing scheme.In:Procceedings of Eurocrypt'2000.LNCS1807.Berlin:Springer-Verlag,2000.316-334；文献 [3] 许春香，董庆宽，肖国镇．矢量空间的秘密共享 --- 多重签名方案．电子学报，2003,31(1):48-50。文献 [4] 张兴兰．带容错性的门限签名方案．中国科学院研究生院学报．第 21 卷第 3 期．2004 年 7 月．398-401。其中，文献 [1]，[2] 给出的门限签名方案中，一个子秘密 (secret share) 持有者，首先需要做出自己的子签名。文献 [2] 给出一个门限签名方案，每一个子秘密持有者所做的签名皆可验证。文献 [4] 是针对文献 [3] 给出的改进方案，利用多方计算的原理，给出一个有效的、带有容

错性的门限签名和验证方案。

[0190] 本实施例中采用文献 [4] 的门限签名和验证方案但本申请不局限于此，本实施例中的 Privacy CA 作为文献 [4] 中选择并计算公开参数的可信赖的中心，n 个虚拟 CA 成员构成 n 个参与者的集合，而任意 t 个虚拟 CA 成员构成一个授权子集，系统私钥作为要共享的秘密，系统子私钥作为子秘密，而包含 DT 身份信息、相关公钥等信息的 DT 身份子证书中的主体部分作为消息 m。根据门限签名算法的子签名算法（计算 $sig_i(m)$），每一虚拟 CA 成员对消息 m 的子签名即为 DT 身份子证书中用系统子私钥对 DT 所做的签名，DT 可以根据对子签名的验证算法来验证 DT 身份子证书中的签名。而 DT 收到 t 个身份子证书后，根据门限签名算法中的合成算法（文献 [4] 中计算门限签名 (R, S) 的算法）可以合成得到 DT 身份证书中管理域对 DT 的签名。而域终端门限签名算法中对合成的签名的验证算法，用相应的公共参数即可对 DT 身份证书中的签名进行验证。

[0191] 较佳地，DT 身份证书中管理域对 DT 的签名的主体部分同时包括 DT 的平台 ID 和域管理员 ID，域管理员 ID 可以在系统中唯一标识该域管理员，其中可以包含域 ID。该域管理员 ID 可以在到 Privacy CA 注册获取平台身份证书时由 Privacy CA 分配，也可以按照预定的规则生成，如已有可信域的 DT 加入本系统时，在原标识的基础上加上域标识得到域管理员 ID。下文的虚拟 CA 成员的系统管理员标识和域终端的终端用户标识也是如此。

[0192] 在本步骤中，t 个虚拟 CA 成员在将 DT 身份子证书授予 DT 时可以同时提供自己的 CA 成员身份证书作为身份证明。DT 可以基于所述 CA 成员身份证书对相应虚拟 CA 成员的身份进行认证，对所有 t 个虚拟 CA 认证通过后，再对 t 个 DT 身份子证书中的签名进行认证。虚拟 CA 成员到虚拟 CA 注册以获取 CA 成员身份证书的过程在下文将详细说明，但在其他实施例中，DT 也可以根据虚拟 CA 成员的公钥或者虚拟 CA 成员提供的平台身份证书等方式来认证其身份，虚拟 CA 成员获取 CA 成员身份证书的过程是可选的。

[0193] 本实施例中，域终端到所在可信域的 DT 注册的过程如图 7 所示，包括：

[0194] 步骤 410，域终端的可信计算平台 (TCP) 以平台身份证书为身份证明，到所在可信域的 DT 注册，同时携带 TCP ID；

[0195] 步骤 420，所述 DT 对所述域终端认证通过后，生成所述域终端的终端身份证书，所述终端身份证书包含所述 DT 对所述域终端的签名；

[0196] 终端身份证书可以遵循 X.509 标准，其签名的主体部分包括域终端的相关信息如同时包含域终端的平台 ID 和终端用户 ID 等信息，该终端用户 ID 可以在系统中唯一标识该终端用户，其中可以包含域 ID。本实施例中，该终端身份证书中还包括证书颁发者即 DT 的相关信息如该 DT 的平台 ID 和域管理员 ID。其签名值部分包含了管理域对该 DT 的相关信息的签名值和该 DT 对所述域终端的相关信息的签名值。这样，域终端的终端身份证书可以用于另一可信域对该域终端的远程认证。

[0197] 步骤 430，所述 DT 将所述终端身份证书发送给所述域终端。

[0198] 上述域终端基于平台身份证书从 DT 申请终端身份证书的过程，可以采用 PCA 系统中证明方基于 EK 证书从 Privacy CA 申请 AIK 证书的方式来实现，此时本申请中的域终端相当于 PCA 系统中的证明方，DT 相当于 PCA 系统中的 Privacy CA，而本申请的终端身份证书相对 AIK 证书，增加了管理域对 DT 的签名。在另一实施方式中，上述域终端基于平台身份证书从 DT 申请终端身份证书的过程也可以采用 DAA 系统中证明方基于 EK 公钥向可信发

布方申请获得对于秘密数据 (f_0, f_1) 的 C-L 签名即 DAA 证书 (A,e,v) 的方式来实现，此时，本申请中的域终端相当于 DAA 系统中的该证明方，DT 相当于 DAA 系统中的可信发布方，而本申请的终端身份证书相对 DAA 证书，增加了管理域对 DT 的签名。

[0199] 终端身份证书及相应的用户信息可以保存在可信域相应的数据库中。

[0200] 本实施例中，可以包括虚拟 CA 成员到虚拟 CA 注册以获取 CA 成员身份证书的过程，如图 8 所示，该过程和 DT 到虚拟 CA 注册以获取 DT 身份证书的过程类似，包括：

[0201] 步骤 510，一虚拟 CA 成员以其平台身份证书为证明到其他 t 个或 t-1 个虚拟 CA 成员注册申请 CA 成员身份证书；

[0202] 因为虚拟 CA 成员本身是 (t,n) 门限体制中共享秘密的参与者，只要获取其他 t-1 个虚拟 CA 成员的秘密份额或其伪份额就可以恢复出秘密，但本申请虚拟 CA 成员到虚拟 CA 注册以获取 CA 成员身份证书时，可以规定将注册的该虚拟 CA 成员排除在 t 个虚拟 CA 成员之外，此时，该虚拟 CA 成员仍应到 t 个虚拟 CA 成员注册。

[0203] 步骤 520，所述其他 t 个或 t-1 个虚拟 CA 成员对该虚拟 CA 成员认证通过后，根据门限签名算法用各自保存的系统子私钥对该虚拟 CA 成员签名，将得到的 t 个或 t-1 个 CA 成员身份子证书授予该虚拟 CA 成员；

[0204] 步骤 530，该虚拟 CA 成员对所述其他 t 个或 t-1 个虚拟 CA 成员身份子证书中系统子私钥对该虚拟 CA 成员的签名的合法性验证通过后，根据所述 t 个或 t-1 个 CA 成员身份子证书合成自己的 CA 成员身份证书，所述 CA 成员身份证书包含用门限签名算法合成的管理域（这里是虚拟 CA）对本虚拟 CA 成员的签名。

[0205] 所述 CA 成员身份证书中签名的主体部分可以包括该虚拟 CA 成员的平台标识，或者同时包含该虚拟 CA 成员的平台标识和系统管理员标识。

[0206] 上述实施例主要描述了通过证书实现身份认证的过程，关于平台的完整性等认证可参照相关标准，此处不再赘述。

[0207] 上述实施方式中，可信计算系统的认证方法及相应系统采用基于可信域的分布式网络拓扑，便于扩展来应对不同规模可信域的集成。

[0208] 上述实施方式中，域终端使用从所在可信域的 DT 得到终端身份证书就可以实现跨域认证，不用针对每个可信域去申请证书，这减少了网络流量、计算负载和存储空间，提高了分布式网络跨域认证的效率。

[0209] 上述实施方式中，采用虚拟 CA 代替 PrivacyCA 向 DT 颁发 DT 身份子证书，多个虚拟 CA 成员按 (t,n) 门限体制来共享系统私钥，可以避免伪冒攻击、单点 DOS 攻击和失效，也使得 PrivacyCA 只在系统其他成员注册时授予这些成员平台身份证书，之后的认证过程无需 PrivacyCA 参与，可以有效地保护 PrivacyCA，提高系统的保密性能。

[0210] 上述实施方式中，在授予系统成员的证书中可以将该成员的使用者标识和平台标识绑定，可以有效地防止平台替换攻击。

[0211] 上述实施例可以有一些变例。在一个变例中，管理域由 PrivacyCA 构成，不包括虚拟 CA。相应地的认证书中不包括虚拟 CA 的建立过程。而可信计算系统除 PrivacyCA 外的其他成员到 PrivacyCA 注册以申请平台身份证书的过程可以保留，也可以取消。在 DT 到 PrivacyCA 注册过程中，DT 可以用其可信模块的 EK 证书或者其别名证书作为平台身份证书来证明其身份。相应地，PrivacyCA 认证通过后，直接将 DT 身份证书授予所述 DT，该 DT 身

份证书包含PrivacyCA对所述DT的签名，PrivacyCA在此处签名使用的一对密钥中的私钥，可以与平台身份证书中签名使用的相同或不同。

[0212] 可信计算系统中，与虚拟CA相关的成员及其模块可以取消。相应地，PrivacyCA包括：

[0213] DT证书颁发模块，用于接受DT的注册，对所述DT认证通过后，将DT身份证书授予所述DT，所述DT身份证书包含所述PrivacyCA对所述DT的签名。

[0214] 而DT中的DT证书申请模块只需要以本DT的平台身份证书为证明到管理域注册，并保存PrivacyCA授予的DT身份证书，不再需要根据DT身份子证书来合成DT身份证书。

[0215] 由于可信域的域终端只需从所在域的DT申请得到终端身份证书即可与其他可信域交互，同样也可以避免PrivacyCA成为整个认证系统的性能瓶颈，遭受DoS攻击而导致系统单点失效；且也不用针对每个可信域去申请证书，这减少了网络流量、计算负载和存储空间，提高了分布式网络跨域认证的效率。本变例的DT身份证书和终端身份证书的结构可以与上述实施例相同。

[0216] 下面用一个应用示例对上述实施例进行说明。请参照图1，本应用示例的分布式可信计算系统包括1个管理域和2个可信域（可信域A和可信域B），管理域包括6个虚拟CA成员（1个虚拟CA成员对应一台服务器）和1个Privacy-CA，管理域中还可以设置1个Web服务器。该6个虚拟CA成员按(3,6)门限体制构成虚拟CA。每一可信域中有1个域可信方(DT)和多个域终端，域终端可以是PDA、手机、笔记本电脑等移动终端和台式机等固定终端等等。

[0217] 请同时参照图9，相应的认证方法包括：

[0218] 步骤①，Privacy-CA产生用于平台身份证书签名的自己的一对公私钥及用于秘密分发的一对系统公私钥，并公开相应的系统参数；

[0219] 上述两对密钥都可以用RSA算法生成但不局限于此，生成的密钥可以保存的密钥池中。

[0220] 步骤②，系统其他成员的可信计算平台中的可信模块产生一对平台身份密钥，到Privacy-CA注册，携带EK证书和平台身份公钥；

[0221] 步骤③，Privacy-CA收到注册申请，认证所述其他成员平台的合法性后，授予所述其他成员平台ID和平台身份证书。

[0222] 在步骤②和③的过程中，除Privacy-CA之外的系统成员如域终端、DT、虚拟CA成员以自己的EK证书为证明从Privacy-CA申请获取其平台身份证书，作为其可信计算平台在本系统中的身份证明。这个过程可以类似于PCA系统中证明方以EK证书获取AIK证书的过程，但在本示例中，Privacy-CA在颁发平台身份证书时同时为系统成员分配一个平台标识。例如，域终端Bob到Privacy-CA注册，Privacy-CA认证通过后，分配给Bob一个平台ID，和平台身份证书一起发送给他。这些成员的平台身份证书可以存放在管理域相应的证书库，该证书库可通过Web服务器来访问。各成员的使用者标识也可以在此时一并分配。

[0223] 步骤④，多个虚拟CA成员根据(t，n)门限体制秘密共享系统私钥，构成虚拟CA，Privacy CA在虚拟CA成员中秘密分发系统私钥；

[0224] 在实体上，Privacy CA可以包括一个或两个实体，如一个实体用于颁发平台身份证书，一个实体用于生成和秘密分发系统私钥。虚拟CA成员可以由Privacy CA指定，也可

以由终端申请，Privacy CA 来选定。系统密钥采用分布式管理方式，可提高系统密钥保管的安全性。

[0225] 基于 (t，n) 门限体制共享秘密和秘密分发的方式有很多，下面给出一个示例但不用于限制本申请，上述步骤④中，n 个虚拟 CA 成员组成的虚拟 CA，用 B_i 表示其中第 i 个虚拟 CA 成员，s_i 表示第 i 个虚拟 CA 成员分得的系统子私钥，i ＝ 1，…，n

[0226] Privacy CA 根据以下公式得到 S_i 并分发给相应的虚拟 CA 成员：

[0227] $h(x) = \alpha_{t-1}x^{t-1}+\cdots+\alpha_1 x+\alpha_0 \bmod \Phi$ (4-1)

[0228] $S_i = h(x_i) \bmod \Phi \; x_i = i, i = 1,\ldots,n$ (4-2)

[0229] 其中，素数 Φ 大于最大可能的系统私钥 S 和虚拟 CA 成员总数 n，并且 $\alpha_0 \bmod \Phi = h(0) = S$，$\alpha_{t-1},\ldots,\alpha_1$ 为随机系数且这些系数保密；x_i 是第 i 个子私钥 s_i 对应的变量，本示例中，x_i 的值等于 i。

[0230] 令 A 为 n 个虚拟 CA 成员中的任一子集且 A 中包括 t 个虚拟 CA 成员即 A ≥ t，将子集 A 中的第 r 个虚拟 CA 成员的系统子私钥记为 s_{i_r}，r ＝ 1…t，$x_{i_r} = i_r$。

[0231] 根据式 (4-2)，有：

[0232] $$s_{i_r} = h(x_{i_r}) \bmod \phi \quad (4\text{-}3)$$

[0233] t 个虚拟 CA 成员保存的系统子私钥 s_{i_r} 与系统私钥 S 之间满足：

[0234] $$s = \sum_{B_i \in A, r=1}^{t} c_{i_r} s_{i_r} \quad (4\text{-}4)$$

[0235] $$c_{i_r} = \prod_{1 \le j,r \le t, j \ne r} \frac{x_{i_j}}{x_{i_j} - x_{i_r}} \left(x_{i_r} = i_r\right) \quad (4\text{-}5)$$

[0236] 其中，

[0237] x_{i_r} 是 n 个子私钥对应的变量集中的 t 个变量组成的子集中的第 r 个变量；x_{i_j} 是 n 个子私钥对应的变量集中的 t 个变量组成的子集中的第 j 个变量。

[0238] 步骤⑤，DT 以其平台身份证书为证明，至少向 n 个虚拟 CA 成员中的 t 个成员注册以获取 DT 身份子证书；

[0239] 假定，n ＝ 6，t ＝ 3，以域可信方 John 为例，John 至少向 6 个可信虚拟 CA 成员的 3 个成员提交申请。

[0240] 步骤⑥，t 个虚拟 CA 成员认证该 DT 平台合法后，分别将一 DT 身份子证书授予该 DT，每一 DT 身份子证书包含一个虚拟 CA 成员基于门限签名算法用其保存的系统子私钥对该 DT 的签名，该 DT 对 DT 身份子证书中签名的合法性验证通过后，根据 t 个 DT 身份子证书合成 DT 身份证书，该 DT 身份证书中包含用门限签名算法合成的虚拟 CA 对本 DT 的签名。

[0241] 虚拟 CA 成员可以用类似的方式到其他虚拟 CA 成员注册获取 CA 成员身份证书并在 DT 注册过程中提供给 DT，此时 DT 先基于 CA 成员身份证书对虚拟 CA 成员的身份进行认证，通过后再对 DT 身份子证书中签名进行合法性验证。使用 CA 成员身份证书验证可以提高对虚拟 CA 成员身份验证的可信度。

[0242] 步骤⑦，域终端想访问可信域的网络资源，到所在可信域的 DT 注册申请终端身份

证书，域终端与 DT 互相认证对方证书的合法性，DT 将终端身份证书授予该域终端，域终端保存该终端身份证书；

[0243] 终端身份证书中签名的主体部分可以同时包括域终端的平台标识和终端用户标识。

[0244] 步骤⑧，域终端访问非本地可信域的另一域终端时，提交终端身份证书，远程端（即另一域终端）认证合法后，也提交自己的终端身份证书，该域终端认证通过后，便可接入该可信域网络获得资源服务。

[0245] 域终端在上述认证过程中可以共同协商授权密钥以加密交互的数据。

[0246] 现有分布式网络用户在接入不同的可信域时，需要重新进行接入认证，该过程不仅要求扩展性强、认证可信且延迟小。本申请的分布式网络跨域认证方法可以有效防止未授权用户进入网络，使授权用户能被快速认证从而获得异地域中的资源服务。

[0247] 本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现，相应地，上述实施例中的各模块 / 单元可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本申请不限制于任何特定形式的硬件和软件的结合。

[0248] 以上所述仅为本申请的优选实施例而已，并不用于限制本申请，对于本领域的技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

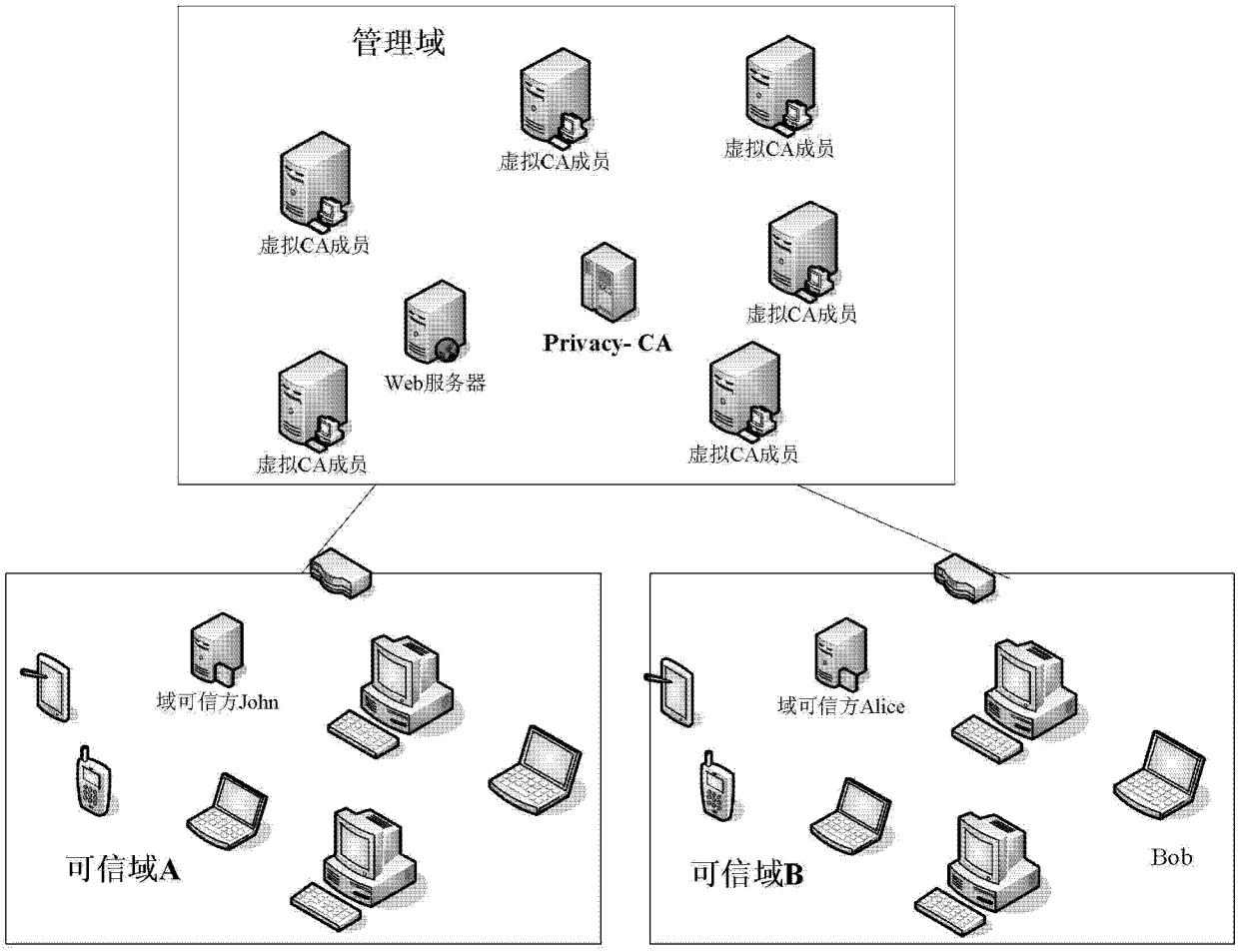

管理域
虚拟CA成员
虚拟CA成员
虚拟CA成员
虚拟CA成员
Privacy- CA
虚拟CA成员
Web服务器
虚拟CA成员
虚拟CA成员
域可信方John
可信域A
域可信方Alice
可信域B
Bob

图 1

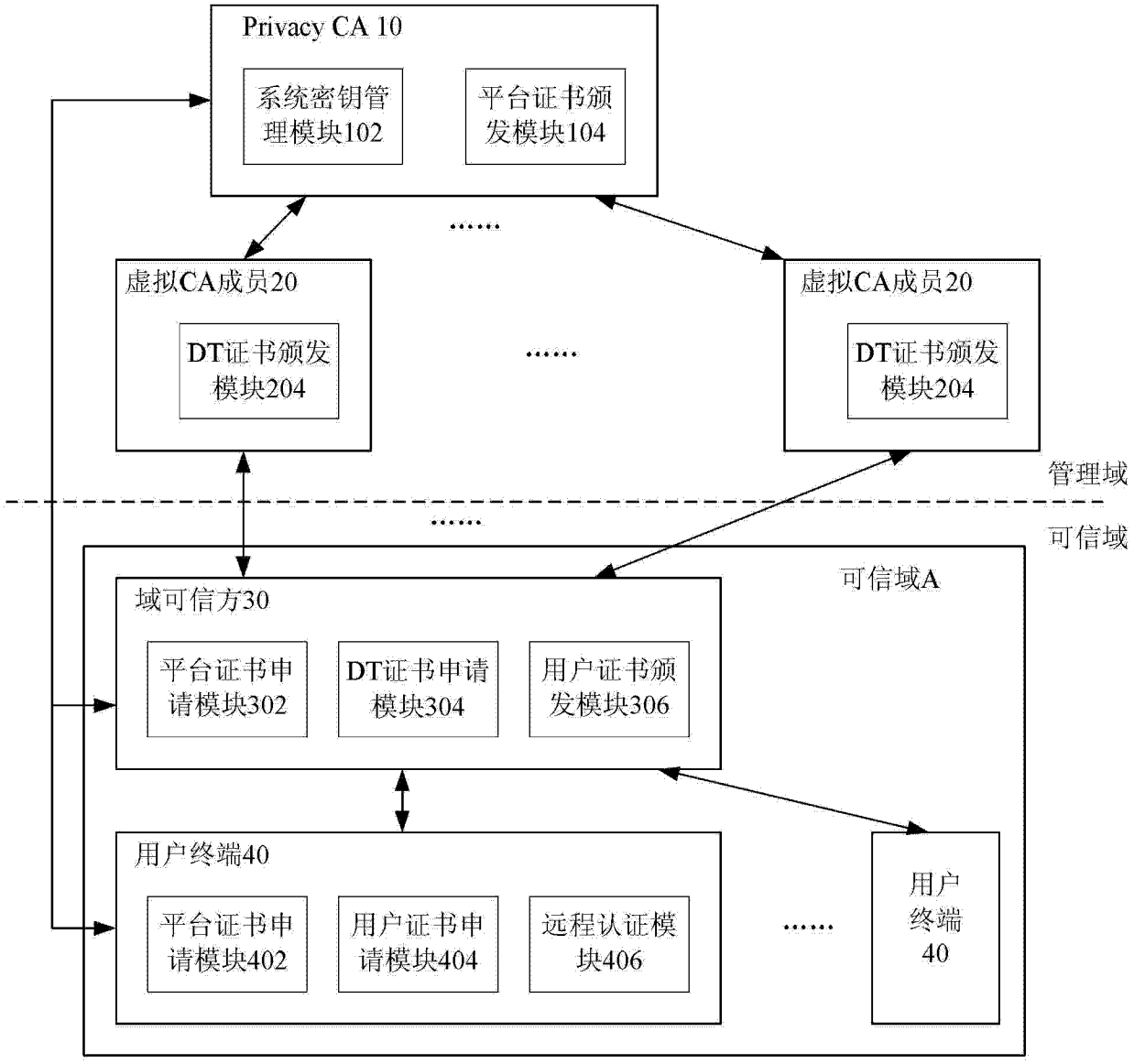

Privacy CA 10
系统密钥管理模块102
平台证书颁发模块104
虚拟CA成员20
DT证书颁发模块204
虚拟CA成员20
DT证书颁发模块204
管理域
可信域
可信域A
域可信方30
平台证书申请模块302
DT证书申请模块304
用户证书颁发模块306
用户终端40
平台证书申请模块402
用户证书申请模块404
远程认证模块406
用户终端40

图 2

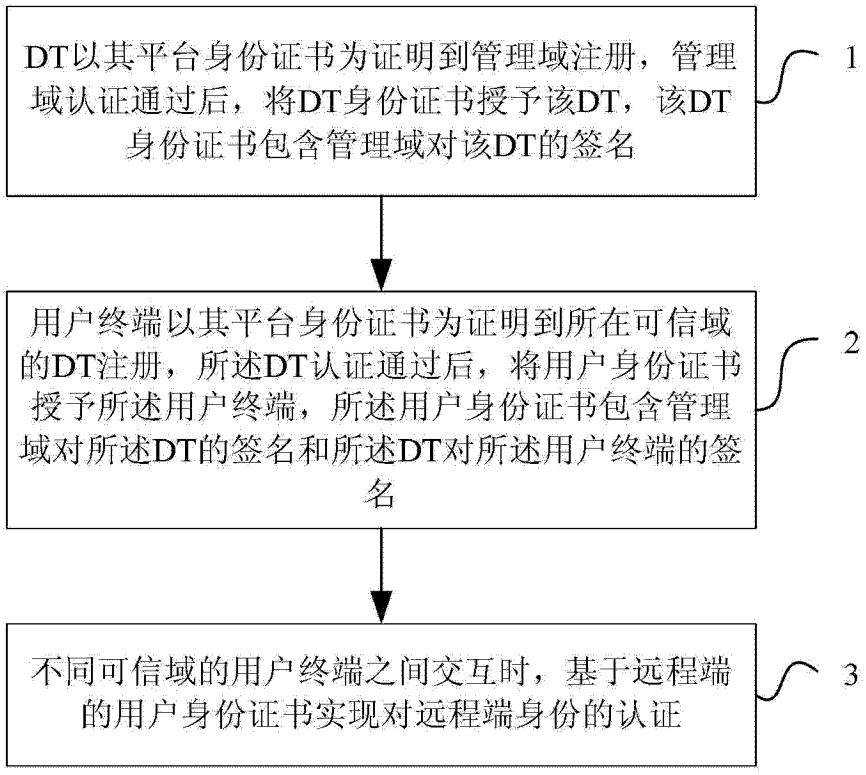

DT以其平台身份证书为证明到管理域注册，管理域认证通过后，将DT身份证书授予该DT，该DT身份证书包含管理域对该DT的签名
1
用户终端以其平台身份证书为证明到所在可信域的DT注册，所述DT认证通过后，将用户身份证书授予所述用户终端，所述用户身份证书包含管理域对所述DT的签名和所述DT对所述用户终端的签名
2
不同可信域的用户终端之间交互时，基于远程端的用户身份证书实现对远程端身份的认证
3

图 3

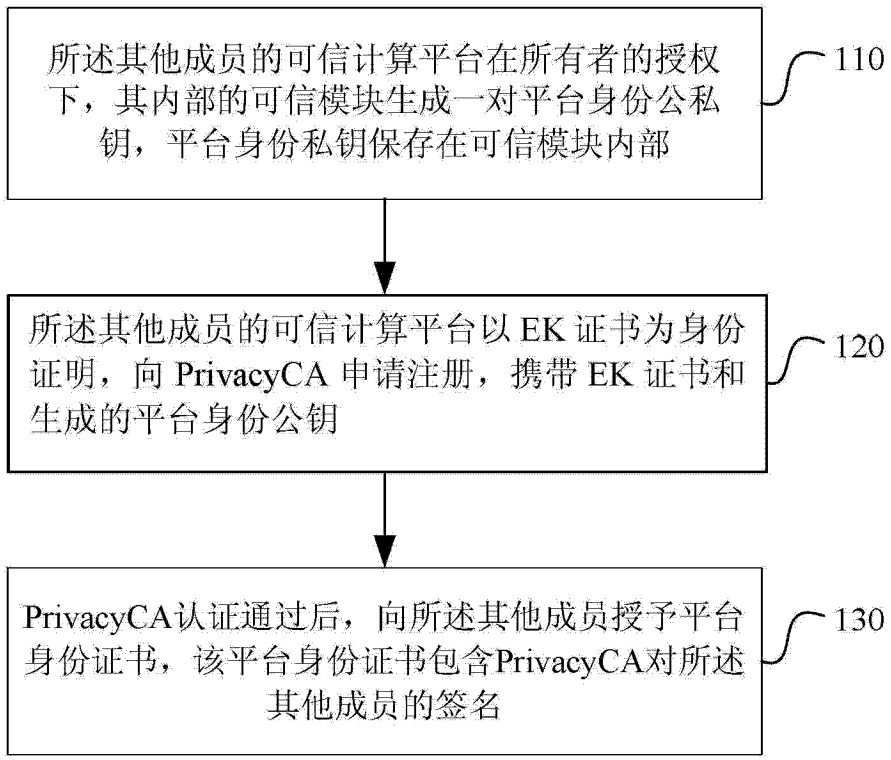

所述其他成员的可信计算平台在所有者的授权下，其内部的可信模块生成一对平台身份公私钥，平台身份私钥保存在可信模块内部
110
所述其他成员的可信计算平台以 EK 证书为身份证明，向 PrivacyCA 申请注册，携带 EK 证书和生成的平台身份公钥
120
PrivacyCA认证通过后，向所述其他成员授予平台身份证书，该平台身份证书包含PrivacyCA对所述其他成员的签名
130

图 4

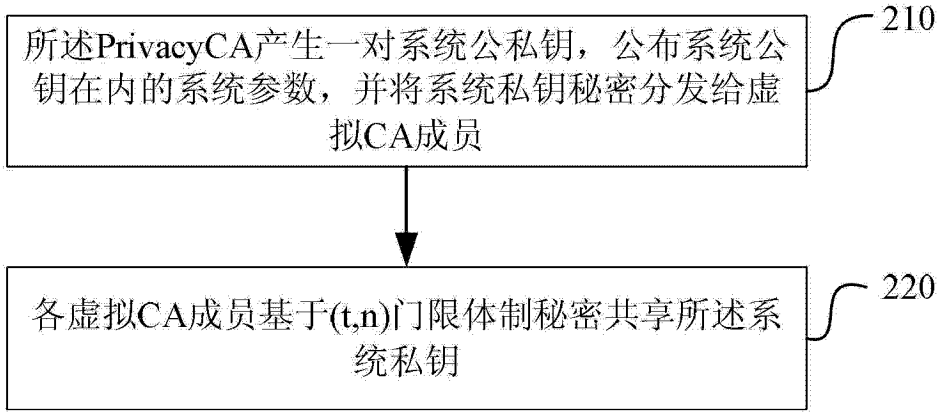

所述PrivacyCA产生一对系统公私钥，公布系统公钥在内的系统参数，并将系统私钥秘密分发给虚拟CA成员
210
各虚拟CA成员基于(t,n)门限体制秘密共享所述系统私钥
220

图 5

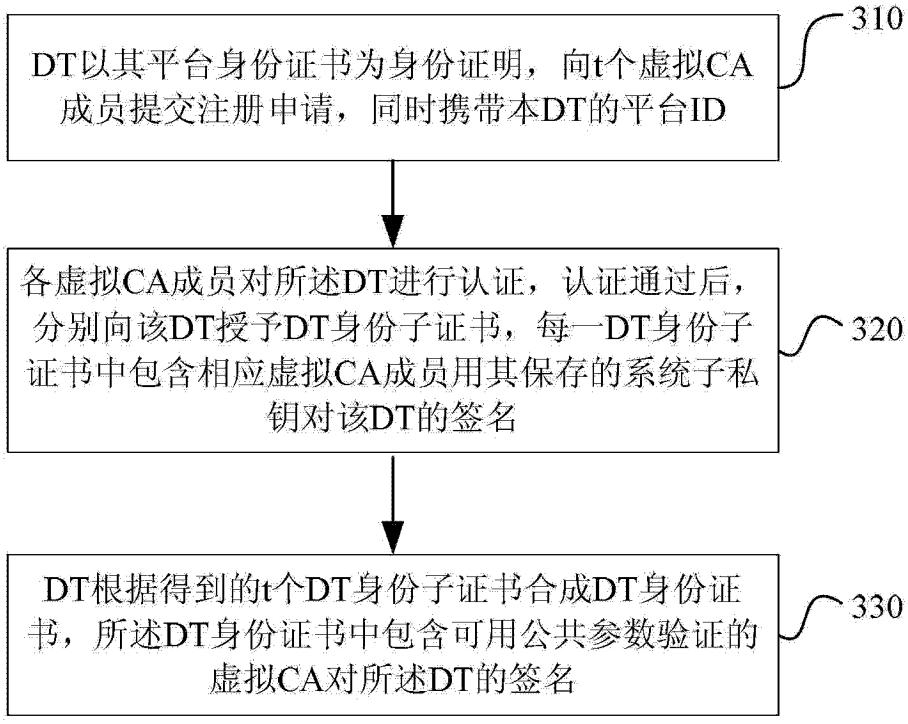

DT以其平台身份证书为身份证明，向t个虚拟CA成员提交注册申请，同时携带本DT的平台ID
310
各虚拟CA成员对所述DT进行认证，认证通过后，分别向该DT授予DT身份子证书，每一DT身份子证书中包含相应虚拟CA成员用其保存的系统子私钥对该DT的签名
320
DT根据得到的t个DT身份子证书合成DT身份证书，所述DT身份证书中包含可用公共参数验证的虚拟CA对所述DT的签名
330

图 6

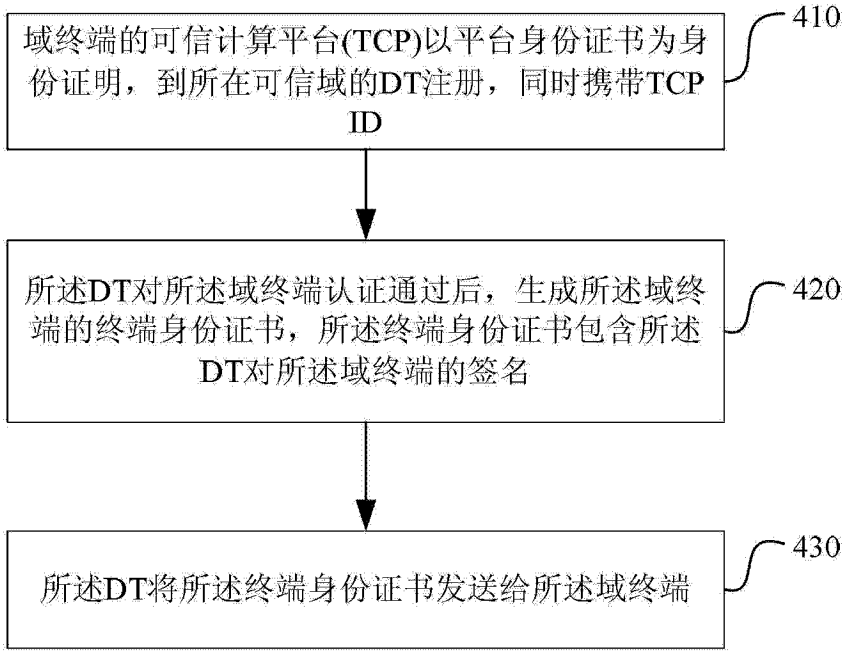

域终端的可信计算平台(TCP)以平台身份证书为身份证明，到所在可信域的DT注册，同时携带TCP ID
410
所述DT对所述域终端认证通过后，生成所述域终端的终端身份证书，所述终端身份证书包含所述DT对所述域终端的签名
420
所述DT将所述终端身份证书发送给所述域终端
430

图 7

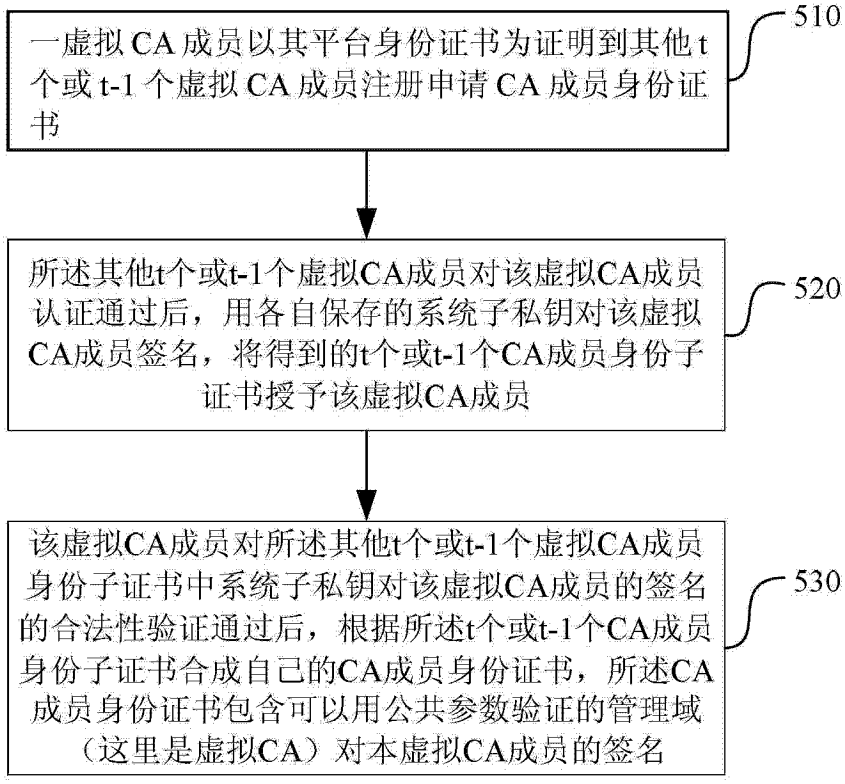

一虚拟 CA 成员以其平台身份证书为证明到其他 t 个或 t-1 个虚拟 CA 成员注册申请 CA 成员身份证书
510
所述其他t个或t-1个虚拟CA成员对该虚拟CA成员认证通过后，用各自保存的系统子私钥对该虚拟CA成员签名，将得到的t个或t-1个CA成员身份子证书授予该虚拟CA成员
520
该虚拟CA成员对所述其他t个或t-1个虚拟CA成员身份子证书中系统子私钥对该虚拟CA成员的签名的合法性验证通过后，根据所述t个或t-1个CA成员身份子证书合成自己的CA成员身份证书，所述CA成员身份证书包含可以用公共参数验证的管理域（这里是虚拟CA）对本虚拟CA成员的签名
530

图 8

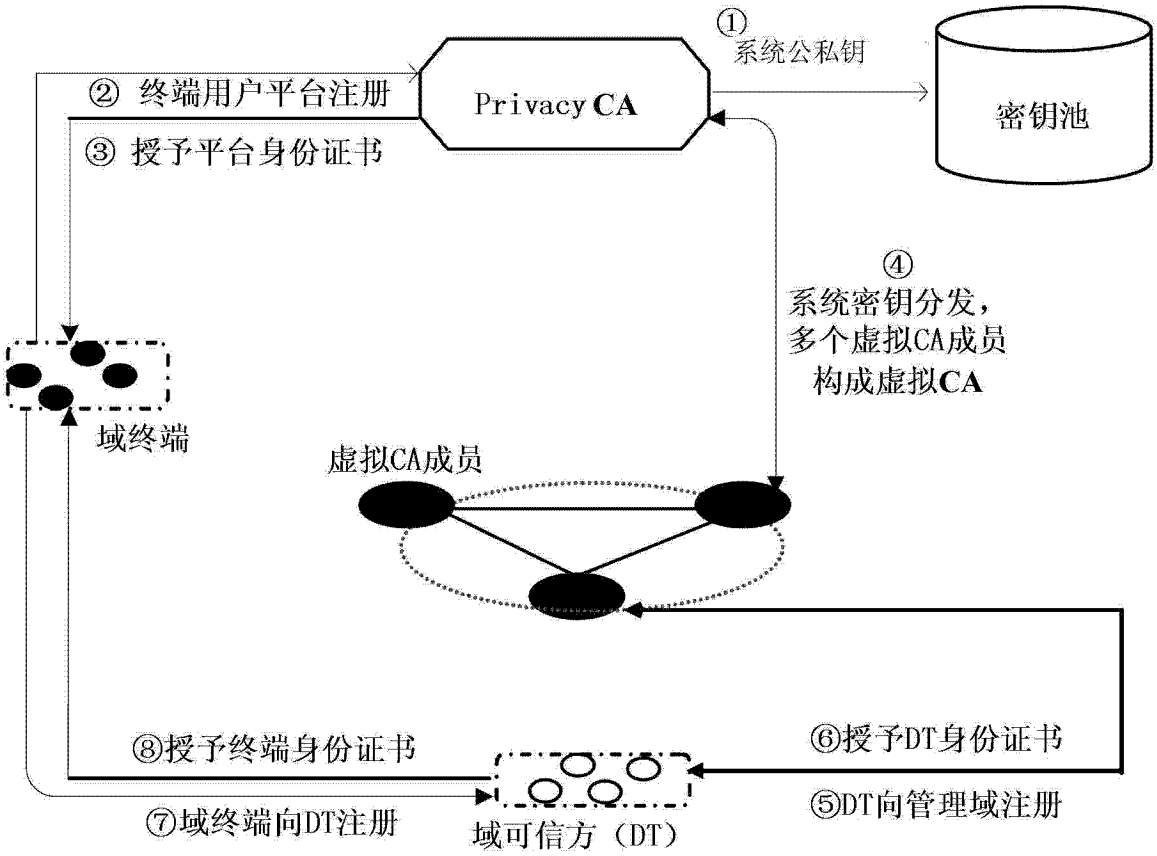

①
系统公私钥
② 终端用户平台注册
Privacy CA
密钥池
③ 授予平台身份证书
④
系统密钥分发，
多个虚拟CA成员
构成虚拟CA
域终端
虚拟CA成员
⑧授予终端身份证书
⑥授予DT身份证书
⑦域终端向DT注册
⑤DT向管理域注册
域可信方（DT）

图 9