



(12) 发明专利申请

(10) 申请公布号 CN 104580250 A

(43) 申请公布日 2015. 04. 29

(21) 申请号 201510044405. X

(22) 申请日 2015. 01. 29

(71) 申请人 成都卫士通信息产业股份有限公司
地址 610041 四川省成都市高新区云华路
333 号

(72) 发明人 刘强

(74) 专利代理机构 成都九鼎天元知识产权代理
有限公司 51214

代理人 韩雪

(51) Int. Cl.

H04L 29/06(2006. 01)

H04L 9/32(2006. 01)

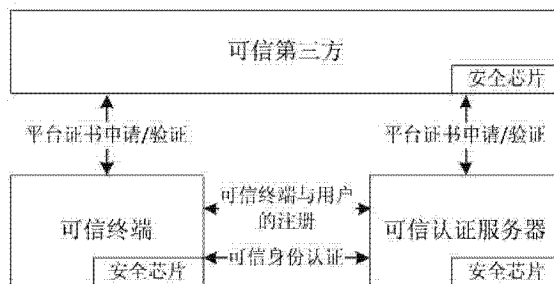
权利要求书2页 说明书5页 附图1页

(54) 发明名称

一种基于安全芯片进行可信身份认证的系统
和方法

(57) 摘要

本发明提供了一种基于安全芯片进行可信身份认证的系统和方法。可信认证服务器和可信终端向同一可信第三方申请平台证书；所述平台证书申请成功后，所述可信认证服务器将所述可信终端加入到自己的已注册终端列表，存储可信终端相应的证书，同时可信认证服务器添加新用户到注册用户列表；用户在可信终端，通过平台可信性认证和用户身份认证后访问相应服务器；所述平台可信性认证是可信认证服务器与可信终端之间的双向认证；所述用户身份认证用于验证用户身份的真实性；所述平台证书包括平台身份证书和平台加密证书。利用安全芯片进行平台的可信性认证，使得认证服务器与终端能够互相确认对方身份的真实性以及平台的安全性，确保用户身份认证过程的安全。



1. 一种基于安全芯片进行可信身份认证的系统,其特征在於,包括分别装载有安全芯片的可信认证服务器、可信终端和可信第三方;所述可信第三方用于平台证书的签发、验证和撤销;所述可信认证服务器用于管理可信终端和用户信息,提供可信终端与用户的添加、认证和删除;用户通过所述可信终端访问相应服务。

2. 一种基于权利要求 1 所述的进行可信身份认证系统的可信身份认证方法,其方法步骤为:

步骤一、可信认证服务器和可信终端向同一可信第三方申请平台证书;

步骤二、所述平台证书申请成功后,所述可信认证服务器将所述可信终端加入到自己的已注册终端列表,存储可信终端相应的证书,同时可信认证服务器添加新用户到注册用户列表;

步骤三、用户在可信终端,通过平台可信性认证和用户身份认证后访问相应服务器;所述平台可信性认证是可信认证服务器与可信终端之间的双向认证;所述用户身份认证用于验证用户身份的真实性;

所述平台证书包括平台身份证书和平台加密证书。

3. 根据权利要求 2 所述的进行可信身份认证方法,所述平台身份证书的申请方法步骤为:

A1、申请端创建平台身份密钥,生成证书请求;所述证书请求包括对称密钥对证书请求内容的加密和可信第三方的公钥对所述对称密钥的加密;所述证书请求内容包括用户身份标识信息和平台身份密钥的公钥;

A2、可信第三方收到证书请求后使用其私钥解密获得所述对称密钥,再利用获得的对称密钥解密得到证书的请求内容;可信第三方对证书请求内容进行审核,审核通过后利用其私钥对申请端签发平台身份证书;

A3、可信第三方生成对称密钥对申请端平台身份证书进行加密,再利用申请端 EK 密钥的公钥对该对称密钥进行加密后发送给申请端;

A4、申请端收到可信第三方发回的步骤 A3 所述的两个加密数据,利用 EK 密钥的私钥解密其中的对称密钥,并利用该对称密钥解密已加密的证书得到平台身份证书。

4. 根据权利要求 2 或 3 所述的进行可信身份认证方法,所述平台加密证书的申请方法步骤为:

B1、申请端生成平台加密证书请求,证书请求包括对称密钥对结构 TCM_PEK_PROOF 加密的结果和可信第三方的公钥对该对称密钥进行加密的数据;

B2、可信第三方收到证书请求后,用其私钥解密获得对称密钥,再利用该对称密钥得到证书请求的明文;可信第三方按照 TCM_PEK_PROOF 结构中的身份标识创建一个非对称密钥作为申请端的平台加密密钥;

B3、可信第三方创建一个对称密钥,用这个创建的对称密钥加密平台加密密钥,再利用申请端的 EK 密钥的公钥加密该创建的对称密钥,并将加密后的平台密钥和加密后的该所述创建的对称密钥发送给申请端;

B4、可信第三方用其私钥签发平台加密证书,并产生对称密钥对该平台加密证书进行加密,再利用申请端 EK 密钥的公钥加密该对称密钥,将所述对称密钥加密后的证书和加密后的对称密钥数据发送给申请端;

B5、申请端利用 EK 密钥的私钥解密步骤 B3 中所述的对称密钥,利用该对称密钥解密平

台加密密钥,并用存储主密钥对平台加密密钥的私钥进行加密保护;

B6、申请端利用 EK 密钥的私钥解密步骤 B4 中所述的对称密钥,利用该对称密钥解密加密过的证书得到平台加密证书。

5. 根据权利要求 2 所述的可信身份认证方法,所述步骤二还包括,有新的可信终端向同一可信第三方申请平台证书成功后,所述可信认证服务器将所述新的可信终端添加到已注册终端列表,存储可信终端相应的证书,同时可信认证服务器添加新用户到注册用户列表。

6. 根据权利要求 2 所述的可信身份认证方法,所述可信身份认证的具体方法步骤为:

C1、可信终端选择一个随机数 A 发送给可信认证服务器;

C2、可信认证服务器选择一个随机数 B,可信认证服务器对自身组件进行度量得到度量结果和度量事件日志,将随机数 B、度量结果和度量事件日志,以及利用其自身平台身份密钥的私钥进行签名后的结果,连同平台身份证书和平台加密证书一起发送给可信终端;

C3、可信终端通过可信第三方验证可信认证服务器的平台身份证书和平台加密证书的有效性,并对数据的完整性进行验证,验证成功则认为可信认证服务器的身份是真实的;可信终端根据可信认证服务器提供的度量事件日志重新进行计算,将计算结果与收到的度量结果相比较以确定认证服务器的可信状态;当可信认证服务器证明其平台可信之后,可信终端对自身组件进行度量得到度量结果和度量事件日志,将随机数、度量结果和度量事件日志,以及利用其自身平台身份密钥的私钥进行签名后的结果,连同平台身份证书、平台加密证书一起发送给可信认证服务器;

C4、可信认证服务器通过可信第三方验证可信终端平台身份证书和平台加密证书的有效性,并对数据的完整性进行验证,验证成功则认为可信终端身份是真实的;可信认证服务器根据可信终端提供的事件度量日志重新进行计算,将计算结果与收到的度量结果相比较以确定可信终端的可信状态;当可信终端证明其平台可信之后,此时则认为可信终端和可信认证服务器彼此相信对方身份的真实性和平台的安全性;可信认证服务器向可信终端发送平台可信认证成功结果;

C5、用户在可信终端上进行身份认证,产生随机数,并用可信认证服务器平台加密密钥的公钥对用户名和密码进行加密,自身平台身份密钥的私钥对加密结果进行签名,将加密和签名后的结果发送给可信认证服务器;

C6、可信认证服务器解密并验证签收到的数据,最后验证用户名和密码的正确性。

一种基于安全芯片进行可信身份认证的系统和方法

技术领域

[0001] 本发明涉及一种基于安全芯片进行可信身份认证的系统和方法,特别是涉及一种适用于信息安全领域的基于安全芯片进行可信身份认证的系统和方法。

背景技术

[0002] 随着计算机技术的不断发展及相关应用需求的不断变化,计算机安全以及信息安全方面的问题越来越突出。常见的身份认证往往是与平台无关的,用户可在任意终端上进行身份认证,由于未对终端安全性进行验证,这就给在终端上进行操作的用户带来了安全隐患。可信计算技术和安全芯片技术的不断进步为解决信息安全问题提出了新思路。

[0003] 可信计算是一种信息系统安全新技术,包括可信硬件、可信软件、可信网络和可信计算应用等诸多方面。可信计算主要内涵是强调实体行为的可预期,以及系统的安全与可靠。可信计算的基本思想是,在计算机系统中,首先建立一个信任根,信任根的可信性由物理安全、技术安全与管理安全共同确保;之后建立一条信任链,从信任根开始到硬件平台,到操作系统,再到应用,一级测量认证一级,一级信任一级,把这种信任扩展到整个计算机系统,从而确保整个计算机系统的可信。

[0004] 安全芯片采用可信计算技术、SOC 技术,内部结构主要包括微处理器、易失性存储器、非易失性存储器、硬件密码算法引擎等;安全芯片内部存储出厂发行时下发的 EK 证书和相关身份证书;EK 密钥、存储主密钥等核心密钥永不出芯片,保证了密钥与机密数据的安全存储;密钥生成、加密解密、数字签名与验证等核心操作在芯片内部安全高效地完成。安全存储是采用可信技术对密钥和敏感数据进行保护存储;通过报告机制完成平台和用户身份证明,建立可信的身份体系;安全芯片的密钥管理功能包括密钥的生成、存储、更新、销毁等。此外,安全芯片的功能还包括可信度量、随机数生成、数据加解密等。

发明内容

[0005] 本发明要解决的技术问题是提供一种用户在任意终端进行身份认证操作时能够进行可信身份认证的系统和方法。

[0006] 本发明采用的技术方案如下:一种基于安全芯片进行可信身份认证的系统,其特征在于,包括分别装载有安全芯片的可信认证服务器、可信终端和可信第三方;所述可信第三方用于平台证书的签发、验证和撤销;所述可信认证服务器用于管理可信终端和用户信息,提供可信终端与用户的添加、认证和删除;用户通过所述可信终端访问相应服务;所述平台证书包括平台身份证书和平台加密证书。

[0007] 一种基于上述进行可信身份认证系统的可信身份认证方法,其方法步骤为:

步骤一、可信认证服务器和可信终端向同一可信第三方申请平台证书;

步骤二、所述平台证书申请成功后,所述可信认证服务器将所述可信终端加入到自己的已注册终端列表,存储可信终端相应的证书,同时可信认证服务器添加新用户到注册用户列表;

步骤三、用户在可信终端,通过平台可信性认证和用户身份认证后访问相应服务器;所述平台可信性认证是可信认证服务器与可信终端之间的双向认证;所述用户身份认证用于验证用户身份的真实性。

[0008] 作为优选,所述平台身份证书的申请方法步骤为:

A1、申请端创建平台身份密钥,生成证书请求;所述证书请求包括对称密钥对证书请求内容的加密和可信第三方的公钥对所述对称密钥的加密;所述证书请求内容包括用户身份标识信息和平台身份密钥的公钥;

A2、可信第三方收到证书请求后使用其私钥解密获得所述对称密钥,再利用获得的对称密钥解密得到证书的请求内容;可信第三方对证书请求内容进行审核,审核通过后利用其私钥对申请端签发平台身份证书;

A3、可信第三方生成对称密钥对申请端平台身份证书进行加密,再利用申请端 EK 密钥的公钥对该对称密钥进行加密后发送给申请端;

A4、申请端收到可信第三方发回的步骤 A3 所述的两个加密数据,利用 EK 密钥的私钥解密其中的对称密钥,并利用该对称密钥解密已加密的证书得到平台身份证书。

[0009] 作为优选,所述平台加密证书的申请方法步骤为:

B1、申请端生成平台加密证书请求,证书请求包括对称密钥对结构 TCM_PEK_PROOF 加密的结果和可信第三方的公钥对该对称密钥进行加密的数据;

B2、可信第三方收到证书请求后,用其私钥解密获得对称密钥,再利用该对称密钥得到证书请求的明文;可信第三方按照 TCM_PEK_PROOF 结构中的身份标识创建一个非对称密钥作为申请端的平台加密密钥;

B3、可信第三方创建一个对称密钥,用这个创建的对称密钥加密平台加密密钥,再利用申请端的 EK 密钥的公钥加密该创建的对称密钥,并将加密后的平台密钥和加密后的该所述创建的对称密钥发送给申请端;

B4、可信第三方用其私钥签发平台加密证书,并产生对称密钥对该平台加密证书进行加密,再利用申请端 EK 密钥的公钥加密该对称密钥,将所述对称密钥加密后的证书和加密后的对称密钥数据发送给申请端;

B5、申请端利用 EK 密钥的私钥解密步骤 B3 中所述的对称密钥,利用该对称密钥解密平台加密密钥,并用存储主密钥对平台加密密钥的私钥进行加密保护;

B6、申请端利用 EK 密钥的私钥解密步骤 B4 中所述的对称密钥,利用该对称密钥解密加密过的证书得到平台加密证书。

[0010] 作为优选,所述步骤二还包括,有新的可信终端向同一可信第三方申请平台证书成功后,所述可信认证服务器将所述新的可信终端添加到已注册终端列表,存储可信终端相应的证书,同时可信认证服务器添加新用户到注册用户列表。

[0011] 作为优选,所述可信身份认证的具体方法步骤为:

C1、可信终端选择一个随机数 A 发送给可信认证服务器;

C2、可信认证服务器选择一个随机数 B,可信认证服务器对自身组件进行度量得到度量结果和度量事件日志,将随机数 B、度量结果和度量事件日志,以及利用其自身平台身份密钥的私钥进行签名后的结果,连同平台身份证书和平台加密证书一起发送给可信终端;

C3、可信终端通过可信第三方验证可信认证服务器的平台身份证书和平台加密证书的

有效性,并对数据的完整性进行验证,验证成功则认为可信认证服务器的身份是真实的;可信终端根据可信认证服务器提供的度量事件日志重新进行计算,将计算结果与收到的度量结果相比较以确定认证服务器的可信状态;当可信认证服务器证明其平台可信之后,可信终端对自身组件进行度量得到度量结果和度量事件日志,将随机数、度量结果和度量事件日志,以及利用其自身平台身份密钥的私钥进行签名后的结果,连同平台身份证书、平台加密证书一起发送给可信认证服务器;

C4、可信认证服务器通过可信第三方验证可信终端平台身份证书和平台加密证书的有效性,并对数据的完整性进行验证,验证成功则认为可信终端身份是真实的;可信认证服务器根据可信终端提供的事件度量日志重新进行计算,将计算结果与收到的度量结果相比较以确定可信终端的可信状态;当可信终端证明其平台可信之后,此时则认为可信终端和可信认证服务器彼此相信对方身份的真实性和平台的安全性;可信认证服务器向可信终端发送平台可信认证成功结果;

C5、用户在可信终端上进行身份认证,产生随机数,并用可信认证服务器平台加密密钥的公钥对用户名和密码进行加密,自身平台身份密钥的私钥对加密结果进行签名,将加密和签名后的结果发送给可信认证服务器;

C6、可信认证服务器解密并验证签收到的数据,最后验证用户名和密码的正确性。

[0012] 与现有技术相比,本发明的有益效果是:利用安全芯片进行平台的可信性认证,使得认证服务器与终端能够互相确认对方身份的真实性以及平台的安全性,确保用户身份认证过程的安全。

附图说明

[0013] 图1为本发明其中一实施例的原理示意图。

具体实施方式

[0014] 为了使本发明的目的、技术方案及优点更加清楚明白,以下结合附图及实施例,对本发明进行进一步详细说明。应当理解,此处所描述的具体实施例仅用以解释本发明,并不用于限定本发明。

[0015] 本说明书(包括任何附加权利要求、摘要和附图)中公开的任一特征,除非特别叙述,均能够被其他等效或者具有类似目的的替代特征加以替换。即,除非特别叙述,每个特征只是一系列等效或类似特征中的一个例子而已。

[0016] 如图1所示,一种基于安全芯片进行可信身份认证的系统,包括分别装载有安全芯片的可信认证服务器、可信终端和可信第三方三个功能实体;所述可信第三方用于平台证书的签发、验证和撤销;所述可信认证服务器用于管理可信终端和用户信息,提供可信终端与用户的添加、认证和删除;用户通过所述可信终端访问相应服务。

[0017] 一种基于上述进行可信身份认证系统的可信身份认证方法,其方法步骤为:

步骤一、可信认证服务器和可信终端向同一可信第三方申请平台证书;在本具体实施例中,所述平台证书包括平台身份证书和平台加密证书。

[0018] 步骤二、所述平台证书申请成功后,所述可信认证服务器将所述可信终端加入到自己的已注册终端列表,存储可信终端相应的证书,并添加用户到已注册用户列表;有新的

可信终端向同一可信第三方申请平台证书成功后,所述可信认证服务器将所述新的可信终端添加到已注册终端列表,存储可信终端相应的证书,同时可信认证服务器添加新用户到注册用户列表。

[0019] 步骤三、用户在可信终端,通过平台可信性认证和用户身份认证后访问相应服务器;所述平台可信性认证是可信认证服务器与可信终端之间的双向认证;所述用户身份认证用于验证用户身份的真实性。

[0020] 在本具体实施例的认证方法中,可信认证服务器和可信终端必须向可信第三方提交平台证书申请,由可信第三方对其申请进行审核后签发平台身份证书和平台加密证书,在同一个可信第三方下注册的平台表示在同一个可信域中,只有在同一个可信域中的可信认证服务器和可信终端才能完成平台的身份认证;在可信认证服务器和可信终端分别获取到各自的平台证书后,可信认证服务器将可信终端加入到自己的已注册终端列表中;用户使用相应的服务必须在可信终端上进行,只有在终端与可信认证服务器完成平台可信性认证后才能够继续进行用户的身份认证,用户身份认证成功才能够访问相应的服务。可信认证服务器与可信终端之间的平台可信性认证包括了平台身份认证以及平台安全性认证,只有通过了平台可信性认证的设备才能保证用户使用平台的安全可信。

[0021] 利用安全芯片进行平台的可信性认证,使得认证服务器与终端能够互相确认对方身份的真实性以及平台的安全性,确保用户身份认证过程的安全。

[0022] 在本具体实施例中,可信第三方、可信认证服务器和可信终端都内置的安全芯片为可信密码模块 TCM 安全芯片。TCM 安全芯片采用了双证书机制,包括平台身份证书和平台加密证书,平台身份证书用于证明平台身份,平台加密证书用于加解密数据,因此平台注册时需要同时申请平台身份证书和平台加密证书。在此阶段,可信认证服务器和可信终端都作为申请端向可信第三方申请平台证书。

[0023] 在本具体实施例中,平台身份证书的申请方法步骤为:

A1、申请端创建平台身份密钥,生成证书请求;所述证书请求包括两部分,对称密钥对证书请求内容的加密和可信第三方的公钥对所述对称密钥的加密;所述证书请求内容中包括用户身份标识信息和平台身份密钥的公钥;

A2、可信第三方收到证书请求后使用其私钥解密获得所述对称密钥,再利用获得的对称密钥解密得到证书的请求内容;可信第三方对证书请求内容进行审核,审核通过后利用其私钥对申请端签发平台身份证书;

A3、可信第三方生成对称密钥对申请端平台身份证书进行加密,再利用申请端 EK 密钥的公钥对该对称密钥进行加密后发送给申请端;

A4、申请端收到可信第三方发回的步骤 A3 所述的两个加密数据,首先利用 EK 密钥的私钥解密其中的对称密钥,再利用该对称密钥解密已加密的证书得到平台身份证书。

[0024] 平台加密证书的申请方法步骤为:

B1、申请端生成平台加密证书请求,证书请求包括两部分内容,对称密钥对结构 TCM_PEK_PROOF 加密的结果和可信第三方的公钥对该对称密钥进行加密的数据;

B2、可信第三方收到证书请求后,用其私钥解密获得对称密钥,再利用该对称密钥得到证书请求的明文;可信第三方按照 TCM_PEK_PROOF 结构中的身份标识创建一个非对称密钥作为申请端的平台加密密钥;

B3、可信第三方创建一个对称密钥,用这个创建的对称密钥加密平台加密密钥,再利用申请端的 EK 密钥的公钥加密该创建的对称密钥,并将加密后的平台密钥和加密后的该所述创建的对称密钥发送给申请端;

B4、可信第三方用其私钥签发平台加密证书,并产生对称密钥对该平台加密证书进行加密,再利用申请端 EK 密钥的公钥加密该对称密钥,将所述对称密钥加密后的证书和加密后的对称密钥数据发送给申请端;

B5、申请端利用 EK 密钥的私钥解密步骤 B3 中所述的对称密钥,利用该对称密钥解密平台加密密钥,并用存储主密钥对平台加密密钥的私钥进行加密保护;

B6、申请端利用 EK 密钥的私钥解密步骤 B4 中所述的对称密钥,利用该对称密钥解密加密过的证书得到平台加密证书。

[0025] 可信身份认证分为平台可信性认证和用户身份认证两部分。平台可信性认证是可信认证服务器与可信终端之间的双向认证,用于确保双方身份的真实性和平台的安全性,用户身份认证用于验证用户身份的真实性。

[0026] 在本具体实施例中,可信身份认证的具体方法步骤为:

C1、可信终端选择一个随机数 A 发送给可信认证服务器;

C2、可信认证服务器选择一个随机数 B,可信认证服务器对自身组件进行度量得到度量结果和度量事件日志,将随机数 B、度量结果和度量事件日志,以及利用其自身平台身份密钥的私钥进行签名后的结果,连同平台身份证书和平台加密证书一起发送给可信终端;

C3、可信终端通过可信第三方验证可信认证服务器的平台身份证书和平台加密证书的有效性,并对数据的完整性进行验证,验证成功则认为可信认证服务器的身份是真实的;可信终端根据可信认证服务器提供的度量事件日志重新进行计算,将计算结果与收到的度量结果相比较以确定认证服务器的可信状态;当可信认证服务器证明其平台可信之后,可信终端对自身组件进行度量得到度量结果和度量事件日志,将随机数、度量结果和度量事件日志,以及利用其自身平台身份密钥的私钥进行签名后的结果,连同平台身份证书、平台加密证书一起发送给可信认证服务器;

C4、可信认证服务器通过可信第三方验证可信终端平台身份证书和平台加密证书的有效性,并对数据的完整性进行验证,验证成功则认为可信终端身份是真实的;可信认证服务器根据可信终端提供的事件度量日志重新进行计算,将计算结果与收到的度量结果相比较以确定可信终端的可信状态;当可信终端证明其平台可信之后,此时则认为可信终端和可信认证服务器彼此相信对方身份的真实性和平台的安全性;可信认证服务器向可信终端发送平台可信认证成功结果;

C5、用户在可信终端上进行身份认证,产生随机数,并用可信认证服务器平台加密密钥的公钥对用户名和密码进行加密,自身平台身份密钥的私钥对加密结果进行签名,将加密和签名后的结果发送给可信认证服务器;

C6、可信认证服务器解密并验证签收到的数据,最后验证用户名和密码的正确性。

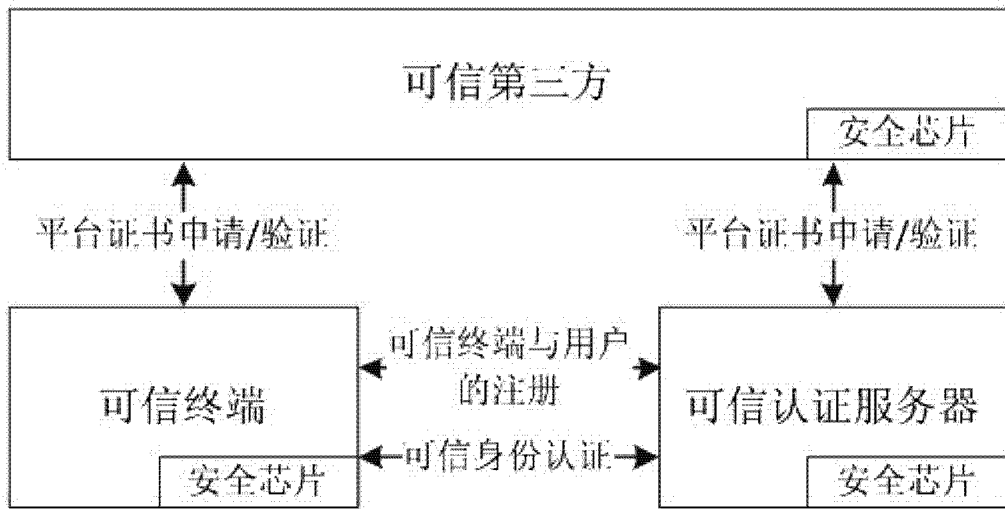


图 1