(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 105743930 A
(43)申请公布日 2016.07.06

(21)申请号 201610283655.3

(22)申请日 2006.11.20

(30)优先权数据
60/738,231 2005.11.18 US

(62)分案原申请数据
200680051080.7 2006.11.20

(71)申请人 安全第一公司
地址 美国加利福尼亚

(72)发明人 里克·L·奥尔西尼
马克·S·奥黑尔
罗杰·达文波特 史蒂文·威尼克

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 郑宗玉

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 9/08(2006.01)

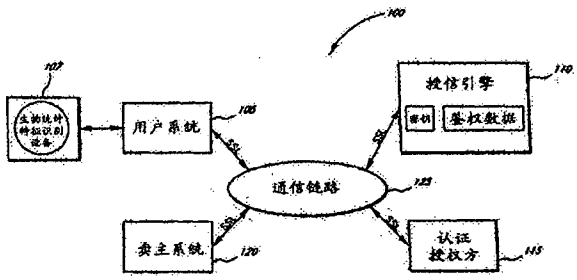
权利要求书2页 说明书62页 附图35页

(54)发明名称

安全数据解析方法和系统

(57)摘要

安全数据解析方法和系统。本发明提供了安全数据解析器，其可集成到任何安全存储和通信数据的合适系统。安全数据解析器解析数据并分割数据为不同存储和通信的多个部分。可为额外的安全性加密原始数据，数据部分，或这两者。安全数据解析器可通过分割原始数据为数据部分保护移动数据，这些数据部分可用多个通信路径传输。



CN 105743930 A

1.一种用于保护数据的方法，所述方法包括：

生成原始保密信息；

从唯一认证授权方获得多个公共密钥；

将所述保密信息分散到共享体中；以及

至少部分地基于多个加密密钥来加密所述共享体，所述多个加密密钥中的至少一个来自于所述多个公共密钥，其中，能够通过重新组合至少阈值数量的共享体而从所述共享体的至少一个子集恢复所述共享体。

2.如权利要求1所述的方法，还包括：

重新组合所述至少阈值数量的共享体；以及

传输基于经重新组合的共享体的数据。

3.如权利要求1所述的方法，其中，加密所述共享体包括使用所述多个公共密钥中的不同公共密钥来加密每个所述共享体。

4.如权利要求1所述的方法，还包括基于密钥包裹来加密保密信息的所述共享体中的每一个共享体。

5.如权利要求4所述的方法，其中，所述密钥包裹基于工作组密钥。

6.如权利要求1所述的方法，其中，将所述保密信息分散到共享体中包括对所述保密信息执行密码操作并且将所述保密信息分布到所述共享体中。

7.如权利要求1所述的方法，其中，所述共享体包括所述保密信息的基本上随机的分布。

8.如权利要求1所述的方法，其中，所述共享体包括来自所述保密信息的已被扰乱的数据单元。

9.如权利要求1所述的方法，还包括将所述共享体存储在两个或更多个不同位置处。

10.如权利要求1所述的方法，还包括将所述共享体存储在两个或更多个不同设备上。

11.一种用于保护数据的系统，所述系统包括处理电路，所述处理电路被配置为：

生成原始保密信息；

从唯一认证授权方获得多个公共密钥；

将所述保密信息分散到共享体中；以及

至少部分地基于多个加密密钥来加密所述共享体，所述多个加密密钥中的至少一个来自于所述多个公共密钥，其中，能够通过重新组合至少阈值数量的共享体而从所述共享体的至少一个子集恢复所述共享体。

12.如权利要求11所述的系统，还包括第二设备，所述第二设备包括第二处理电路，所述第二处理电路被配置为：

重新组合所述至少阈值数量的共享体；以及

传输基于经重新组合的共享体的数据。

13.如权利要求11所述的系统，其中，所述处理电路被配置为通过使用所述多个公共密钥中的不同公共密钥加密每个所述共享体来加密所述共享体。

14.如权利要求11所述的系统，其中，所述处理电路还被配置为基于密钥包裹来加密保密信息的所述共享体中的每一个共享体。

15.如权利要求14所述的系统，其中，所述密钥包裹基于工作组密钥。

16.如权利要求11所述的系统，其中，所述处理电路被配置为通过对所述保密信息执行密码操作并且将所述保密信息分布到所述共享体中而将所述保密信息分散到共享体中。

17.如权利要求11所述的系统，其中，所述共享体包括所述保密信息的基本上随机的分布。

18.如权利要求11所述的系统，其中，其中，所述共享体包括来自所述保密信息的已被扰乱的数据单元。

19.如权利要求11所述的系统，其中，所述处理电路还被配置为将所述共享体存储在两个或更多个不同位置处。

20.如权利要求11所述的系统，其中，所述处理电路还被配置为将所述共享体存储在两个或更多个不同设备上。

安全数据解析方法和系统

[0001] 本申请是申请号为200680051080.7、发明名称为“安全数据解析方法和系统”、国际申请日为2006年11月20日的专利申请的分案申请，其全部内容通过引用合并于此。

[0002] 相关申请的交叉参考

[0003] 本申请要求2005年11月18日申请的美国临时申请No.60/738231的权益，该申请全文包括在此以供参考。

技术领域

[0004] 本发明一般涉及用于保护数据免受未经授权的访问或使用的系统。

背景技术

[0005] 当今社会中，个人和商业经计算机系统进行活动的量日益增加。这些计算机系统，包括私有和非私有计算机网络，通常存储，存档和传输所有类型的敏感信息。因此对确保经这些系统存储和传输的数据不被读取或危害的需要日益增加。

[0006] 一种确保计算机系统安全的普通做法是提供登录和口令功能。然而，口令管理被证明成本很高，因为大部分服务台请求(help desk calls)都涉及口令问题。而且，口令提供的安全性小，因为口令通常都存储在易被不适当访问，例如暴力袭击的文件中。

[0007] 确保计算机系统安全的另一个解决方案是提供密码基础结构。一般地，密码术是指通过变换或加密数据为不可读的格式来保护数据。只有拥有密钥的人才可解密数据为可用格式。密码术用于识别用户，例如鉴定，用于允许访问特权，例如授权，以及用于产生数字证书和签名等。一个流行的密码术系统是使用两个密钥的公钥系统，公钥是每个人已知的，而私钥仅个体或商业所有人知道。通常以一个密钥加密的数据是以另一个密钥解密的，且任一密钥均不可从另一个密钥重新创建。

[0008] 不幸的是，即使是前面典型的公钥加密系统，在安全性方面仍高度依赖于用户。例如密码系统通过例如用户浏览器发出私钥给用户。没有经验的用户通常将私钥存储在其他人可经开放计算机系统，如因特网来访问的硬盘上。另一方面，用户可能为包含他们私钥的文件选择差名字，如“key.”。前述和其他动作的结果是使密钥安全易受危害。

[0009] 除了前述安全危害，用户可能在配置有归档或备份系统的计算机系统上保存他或她私钥，这可能会导致私钥副本在多个计算机存储装置或其他系统上传播。该安全破坏通常称为“密钥迁移(key migration)”。类似于密钥迁移，许多应用程序顶多通过简单登录和口令访问提供对用户私钥的访问。如上所述，登录和口令访问通常不提供足够的安全。

[0010] 一种增加前述密码系统安全性的解决方案是把生物统计特征(biometrics)包括进来，作为鉴定或授权的。生物统计特征通常包括可测量的物理特征，如可由诸如(指纹图案或语音样式(speech pattern)的模式匹配或识别)等自动化系统检验的指纹或语音。在这类系统中，用户生物统计特征和/或密钥可存储在移动计算机装置中，如智能卡、膝上型计算机、个人数字助理或移动电话，从而允许生物统计特征或密钥可用在移动环境中。

[0011] 前述移动生物统计特征密码系统尚有多种缺点。例如，移动用户可能丢失或损坏

智能卡或便携式计算装置，因而使得他或她不再能够访问可能重要的数据。可替换地，有恶意的人可能窃取移动用户智能卡或便携式计算装置，并将其用来有效地窃取移动用户的数字证件(credential)。另一方面，便携式计算装置可连接到开放系统，如因特网，且与口令类似，存储生物统计特征的文件可能由于用户对安全保护的疏忽或恶意入侵者易受危害。

发明内容

[0012] 基于前面所述，存在提供密码系统的需要，该密码系统的安全保护是用户无关的并支持移动用户。

[0013] 因此，本发明的一个方面是提供一种方法，用于安全保护几乎任何类型的数据，防止未授权的访问或使用。该方法包括一个或多个解析、分割和/或分离待保护数据为两个或多个分部或部分的步骤。该方法也包括加密待保护数据。数据加密可在数据第一次解析，分割和/或分离之前或之后执行。此外，加密步骤可为一个或多个数据部分重复。类似地，解析，分割和/或分离步骤可为一个或多个数据部分重复。该方法也可选包括在一个或多个位置存储解析的，分割的和/或分离的已经加密的数据。该方法也可选包括为授权访问或使用重构或重组安全保护的数据为原始形式。该方法可合并到任何能够执行本方法所需步骤的计算机，服务器，引擎等操作中。

[0014] 本发明的另一方面是提供一种系统，用于安全保护几乎任何类型的数据，防止未授权访问或使用。该系统包括数据分割模块，密码处理模块，以及可选的数据组装模块(data assembling module)。在一个实施例中，该系统进一步包括存储安全数据的一个或多个数据存储设施。

[0015] 因此，本发明一个方面提供安全保护服务器(secure server)，或授信引擎(trust engine)，其具有服务器中心式密钥(server-centric key)，或换句话说在服务器上存储密钥和用户鉴定数据。按照该实施例，用户访问授信引擎以便执行鉴定和密码功能，例如但不限于鉴定、授权、数字签名和证书、密码、公证书和委托书类动作的生成，存储和检索。

[0016] 本发明的另一个方面是提供可靠或授信的鉴定过程。而且，在可信肯定鉴定后，可采取大量不同动作，从提供密码技术，到系统或装置授权和访问，以及允许一个或大量电子装置的使用或控制。

[0017] 本发明另一个方面是在密钥和鉴定数据不会丢失，被窃取或危害的环境中提供密钥和鉴定数据，因而有利地避免了持续再发出和管理新密钥和鉴定数据的需要。按照本发明另一个方面，授信引擎允许用户为多个活动，卖主，和/或鉴定请求使用一个密钥对。按照本发明另一个方面，授信引擎执行至少一步密码处理，例如但不限于，在服务器侧加密、鉴定或签名，因而允许客户或用户只拥有最小的计算资源。

[0018] 按照本发明另一个方面，授信引擎包括一个或多个用于存储每个密钥和鉴定数据部分的存储仓库(depository)。这些部分是通过数据分割过程产生的，数据分割过程在没有来自存储仓库中一个以上位置或来自多个存储仓库的预定部分时阻止重构。按照另一个实施例，多个存储仓库可以是地理上远程的，因此欺诈性雇员或一个存储仓库受危害的系统不会提供对用户密钥或鉴定数据的访问。

[0019] 按照又一个实施例，鉴定过程有利地允许授信引擎并行处理多种鉴定活动。按照另一个实施例，授信引擎可有利地跟踪失败的访问企图，并因而限制恶意入侵者试图破坏

系统的次数。

[0020] 按照另一个实施例，授信引擎可包括多个实例，其中每个授信引擎可预测并与其他授信引擎共享处理负载。按照另一个实施例，授信引擎可包括冗余模块供调检(polling)多个鉴定结果，从而确保一个以上的系统鉴定用户。

[0021] 因此，本发明一个方面包括可远程访问的安全保护密码系统，其用于存储任何类型的数据，包括但不限于多个要与多个用户关联的私人密钥。密码系统将多个用户中的每一个与多个私人密钥中的一个或多个不同密钥相关联，并为每个使用关联的一个或多个不同密钥的用户执行密码功能，而不用向用户发布多个私人密钥。密码系统包括具有至少一个服务器的存储仓库系统，该服务器存储待安全保护的数据，如多个私人密钥和多个登记鉴定数据(enroll authentication data)。每个登记鉴定数据识别多个用户中的一个，且多个用户中的每个都与多个私人密钥中的一个或多个不同密钥关联。密码系统也包括鉴定引擎，鉴定引擎比较多个用户中一个用户接收的鉴定数据和对应于多个用户中该一个用户并从存储仓库系统接收的登记鉴定数据，因而产生鉴定结果。密码系统也可包括密码引擎，在鉴定结果指示多个用户中的一个用户身份适当时，密码引擎代表该多个用户中的该一个用户以关联的一个或多个从存储仓库系统接收的不同密钥执行密码功能。密码系统也包括交易引擎，鉴定引擎，和密码引擎，其中，交易引擎连接到从多个用户到存储仓库服务器系统的路由数据。

[0022] 本发明另一个方面包括密码系统，其可选能远程访问。密码系统包括存储仓库系统，其具有至少一个存储至少一个私钥和任何其他数据的服务器，其他数据例如，但不限于多个登记鉴定数据，其中每个登记鉴定数据识别可能的多个用户中的一个。密码系统也可选包括鉴定引擎，该鉴定引擎比较由用户接收的鉴定数据和相应于该用户并从存储仓库系统接收的登记鉴定数据，因而产生鉴定结果。密码系统也包括密码引擎，当鉴定结果指示用户身份适当时，该密码引擎代表用户至少使用可从存储仓库系统接收的所述私钥执行密码功能。密码系统也可选交易引擎，鉴定引擎，和密码引擎。其中，交易引擎连接到从用户到其他引擎或系统的路由数据，其他引擎或系统例如，但不限于存储仓库系统。

[0023] 本发明另一个方面包括促进密码功能的方法。该方法包括关联多个用户中的一个用户和多个存储在安全位置的私人密钥中的一个或一个以上的密钥，该安全位置如安全服务器。该方法也包括从用户接收鉴定数据，并比较该鉴定数据和相应于用户的鉴定数据，因而验证用户的身份。该方法也包括利用一个或多个密钥执行密码功能而不发布一个或多个密钥给用户。

[0024] 本发明另一个方面包括鉴定系统，用于通过用户登记鉴定数据的安全存储来唯一识别用户。鉴定系统包括一个或多个数据存储设施，其中每个数据存储设施包括存储至少一部分登记鉴定数据的计算机可访问存储介质。鉴定系统也包括与一个或多个数据存储设施通信的鉴定引擎。鉴定引擎包括对登记鉴定数据操作从而建立多个部分的数据分割模块，处理来自至少一个数据存储设施多个数据部分从而组合登记鉴定数据的数据组装模块，以及从用户接收当前鉴定数据并与组合的登记鉴定数据比较当前鉴定数据从而判断用户是否已经被唯一识别的数据比较器模块。

[0025] 本发明另一个方面包括密码系统。密码系统包括一个或多个数据存储设施，其中每个数据存储设施包括计算机可访问存储介质，该存储介质存储一个或多个密钥的至少一

部分。密码系统也包括与数据存储设施通信的密码引擎。密码引擎也包括对密钥操作从而建立多个数据部分的数据分割模块，处理来自至少一个数据存储设施多个数据部分从而组合密钥的数据组装模块，以及接收组合的密钥并执行密码功能的密码操纵模块。

[0026] 本发明另一个方面包括存储任何类型数据的方法，包括但不限于地理上远程安全数据存储设施中的鉴定数据，因而依靠任何个人数据存储设施的组合来保护数据。该方法包括在授信引擎接收数据，在授信引擎组合数据与第一基本为随机的值形成第一组合值，并组合该数据与第二基本为随机的值从而形成第二组合值。该方法包括建立第一对第一基本随机值和第二组合值，建立第二对第一基本随机值和第二基本随机值，和在第一安全数据存储设施中存储第一对。该方法包括在与第一安全数据存储设施远距离的第二安全数据存储设施中存储第二对。

[0027] 本发明另一个方面包括存储任何类型数据的方法，包括但不限于，包括接收数据的鉴定数据，组合数据和第一比特集合从而形成第二比特集合，和组合该数据与第三比特集合从而形成第四比特集合。该方法也包括建立第一对第一比特集合和第三比特集合。该方法还包括建立第二对第一比特集合和第四比特集合，并在第一计算机可访问介质中存储第一和第二对中的一对。该方法还包括在第二计算机可访问存储介质中存储第一和第二对中的另一对。

[0028] 本发明另一个方面包括在地理上远距离的安全数据存储设施中存储密码数据的方法，从而靠任何个人数据存储设施的组合来保护密码数据。该方法包括在授信引擎接收密码数据，在授信引擎组合密码数据与第一基本随机值从而形成第一组合值，并组合密码数据与第二基本随机值从而形成第二组合值。该方法也包括建立第一对第一基本随机值与第二组合值，建立第二对第一基本随机值和第二基本随机值，并在第一安全数据存储设施中存储第一对。该方法还包括在与第一安全数据存储设施远程的第二数据存储设施中存储第二对。

[0029] 本发明另一个方面包括存储密码数据的方法，该方法包括接收鉴定数据，并组合该密码数据和第一比特集合从而形成第二比特集合。该方法还包括组合该密码数据与第三比特集合从而形成第四比特集合，建立第一对第一比特集合和第三比特集合，并建立第二对第一比特集合和第四比特集合。该方法也包括在第一计算机可访问介质中存储第一和第二对中的一对。该方法还包括在第二计算机可访问存储介质中存储第一和第二对中的另一对。

[0030] 本发明另一个方面包括在密码系统中处理任何类型或形式敏感数据和采用该敏感数据的方法，其中该敏感数据仅在授权用户动作其间以可用形式存在。该方法也包括在软件模块中接收来自第一计算机可访问存储介质中的基本随机化或加密的敏感数据，并在软件模块中接收来自一个或多个其他的计算机可访问存储介质的基本随机化或加密的数据，该数据可以是也可以不是敏感数据。该方法也包括在软件模块中处理基本随机化的预加密敏感数据和可以是也可不是敏感数据的基本随机化的或加密的数据，从而合并该敏感数据，还包括在软件引擎中采用该敏感数据从而执行动作。该动作包括但不限于鉴定用户和执行密码功能中的一个。

[0031] 本发明另一个方面包括安全鉴定系统。该安全鉴定系统包括多个鉴定引擎。每个鉴定引擎接收用于一定程度上唯一识别用户的登记鉴定数据。每个鉴定引擎接收当前鉴定

数据从而与登记鉴定数据比较，且每个鉴定引擎判断鉴定结果。安全鉴定系统也包括接收至少两个鉴定引擎的鉴定结果，并判断是否用户已被唯一识别的冗余系统。

[0032] 本发明另一个方面包括移动系统(motion system)中的安全数据，因而数据可以以按照本发明被安全保护的不同部分传输，以便被危害的任一部分不能提供足够的数据来恢复原始数据。这可应用到任何数据传输，无论是有线，无线，还是物理传输。

[0033] 本发明另一个方面包括将本发明的安全数据解析器集成到任何合适的系统上，数据在这里存储或通信。例如，电子邮件系统，RAID系统，视频广播系统，数据库系统，或任何其他合适系统可具有以任何合适水平集成的安全数据解析器。

[0034] 本发明另一个方面包括使用任何合适的解析和分割算法从而生成数据共享。要么随机，伪随机，确定性，或他们的任何组合均可用于解析和分割数据。

附图说明

[0035] 下面更详细地联系附图说明本发明，附图仅是为了示出本发明而非限制本发明，其中：

[0036] 图1示出按照本发明一个实施例的密码系统的方框图；

[0037] 图2示出按照本发明一个实施例的图1中授信引擎的方框图；

[0038] 图3示出按照本发明一个实施例的图2中交易引擎的方框图；

[0039] 图4示出按照本发明一个实施例的图2中存储仓库的方框图；

[0040] 图5示出按照本发明一个实施例的图2中鉴定引擎的方框图；

[0041] 图6示出按照本发明一个实施例的图2中密码引擎的方框图；

[0042] 图7示出按照本发明另一个实施例的存储仓库系统的方框图；

[0043] 图8示出按照本发明一个实施例的数据分割过程的流程图；

[0044] 图9中面A示出按照本发明一个实施例的登记过程的数据流；

[0045] 图9中面B示出按照本发明一个实施例的互操作过程(interoperability process)的流程图；

[0046] 图10示出按照本发明一个实施例的鉴定过程的数据流；

[0047] 图11示出按照本发明一个实施例的签名过程的数据流；

[0048] 图12示出按照本发明另一个实施例的加密/解密过程的数据流；

[0049] 图13示出按照本发明另一个实施例的授信引擎系统的简化方框图；

[0050] 图14示出按照本发明另一个实施例的授信引擎系统的简化方框图；

[0051] 图15示出按照本发明一个实施例的图14中冗余模块的方框图；

[0052] 图16示出按照本发明一个方面的评价鉴定的过程；

[0053] 图17示出按照本发明图16所示一个方面的分配值给鉴定的过程；

[0054] 图18示出按照图17所示一个方面的执行授信仲裁(trust arbitrage)过程；以及

[0055] 图19示出按照本发明一个实施例的用户和卖主间简单交易，其中初始基于web的合同导致双方签署的销售合同。

[0056] 图20示出具有密码服务提供商模块的简单用户系统，该密码服务提供商模块为用户系统提供安全功能。

[0057] 图21示出解析，分割和/或分离数据的过程，其中有加密主钥(encryption master

key)随数据的加密和存储。

[0058] 图22示出解析，分割和/或分离数据的过程，其中加密主钥与数据独立加密和存储。

[0059] 图23示出用于解析，分割和/或分离数据的中间密钥(intermediary key)过程，其中有加密主钥随数据的加密和存储。

[0060] 图24示出用于解析，分割和/或分离数据的中间密钥过程，其中加密主钥与数据独立加密和存储。

[0061] 图25示出本发明密码方法和系统在小工作组中的利用。

[0062] 图26是说明性物理标记安全系统的方框图，其采用按照本发明实施例的安全数据解析器。

[0063] 图27是按照本发明一个实施例的说明性组织的方框图，其中安全数据解析器集成到系统中。

[0064] 图28是按照本发明一个实施例，在移动系统中说明性数据的方框图。

[0065] 图29是按照本发明一个实施例，另一个在移动系统中说明性数据的方框图。

[0066] 图30－32是按照本发明一个实施例，具有集成的安全数据解析器的说明性系统的方框图。

[0067] 图33是按照本发明一个实施例，解析和分割数据的说明性过程的流程图。

[0068] 图34是按照本发明一个实施例将数据部分恢复为原始数据的说明性过程的流程图。

[0069] 图35是按照本发明一个实施例在比特级分割数据的说明性过程的流程图。

[0070] 图36是按照本发明一个实施例的说明性步骤和特征的流程图，这些步骤和特征可以按照任何适当的组合使用，并可有任何合适的添加，删除或修改。

[0071] 图37是按照本发明一个实施例的说明性步骤和特征的流程图，这些步骤和特征可以按照任何适当的组合使用，并可有任何合适的添加，删除或修改。

[0072] 图38是按照本发明一个实施例的共享体内密钥和数据构件存储的简化方框图，该共享体可以按照任何适当的组合使用，并可有任何合适的添加，删除或修改。

[0073] 图39是按照本发明一个实施例的使用工作组密钥的共享体内密钥和数据构件存储的简化方框图，该共享体可以按照任何适当的组合使用，并可有任何合适的添加，删除或修改。

[0074] 图40A和40B是按照本发明一个实施例，移动数据的头文件生成和数据分割的简化的说明性流程图，该过程可以按照任何适当的组合使用，并可有任何合适的添加，删除或修改。

[0075] 图41是按照本发明一个实施例的说明性共享格式的简化方框图，其可以按照任何适当的组合使用，并可有任何合适的添加，删除或修改。

具体实施方式

[0076] 本发明的一个方面是提供一种密码系统，其中一个或多个安全服务器或授信引擎(trust engine)存储密码密钥和用户鉴权数据。用户通过对授信引擎的网络访问来访问传统密码系统的功能，然而，授信引擎不发出实际密钥和其他鉴权数据，因此密钥和数据保持

安全。密钥和鉴权数据的这种服务器中心式存储提供了用户无关安全性，便携性，可用性，和直接性。

[0077] 由于用户可确信或信任密码系统来执行用户和文档鉴权及其他密码功能，所以多种功能可被包括在该系统中。例如，授信引擎提供器可例如通过鉴权协议参与方、代表或为参与方对协议进行数字签名、和存储由每个参与方数字签名的协议的记录，来确保防止协议否认。此外，密码系统可监视协议，并例如基于价格、用户、卖主、地理位置、使用地点等来确定应用变化的鉴权度。

[0078] 为了促进对本发明完整的理解，以下详细说明参考附图说明本发明，其中相似的元素以相似的标识号表示。

[0079] 图1示出按照本发明一个实施例的密码系统100的方框图。如图1所示，密码系统100包括通过通信链路125通信的用户系统105、授信引擎110、认证授权方115、和卖主系统120。

[0080] 按照本发明一个实施例，用户系统105包括传统的通用计算机，其具有一个或多个微处理器，诸如基于英特尔的处理器。并且，用户系统105包括适当的操作系统，诸如能够包括图形或窗口的操作系统，诸如Windows，Unix，Linux等。如图1所示，用户系统105可包括生物统计特征识别装置107。生物统计特征社别装置107有利地可以捕获用户的生物统计特征，并将所捕获的生物统计特征传递到授信引擎110。按照本发明的一个实施例，生物统计特征识别装置有利地可以包括具有与以下专利文献中所公开的那些类似的属性和特征的装置，1997年9月5日申请的美国专利申请No.08/926277，该美国专利申请标题为“RELIEF OBJECT IMAGE GENERATOR”，2000年4月6日申请的美国专利申请No.09/558634，其标题为“IMAGING DEVICE FOR A RELIEF OBJECT AND SYSTEM AND METHOD OF USING THE IMAGE DEVICE”，1999年11月5日申请的美国专利申请No.09/435011，其标题为“RELIEF OBJECT SENSOR ADAPTOR”，和2000年1月5日申请的美国专利申请No.09/477943，其标题为“PLANAR OPTICAL IMAGE SENSOR AND SYSTEM FOR GENERATING IN ELECTRONIC IMAGE OF A RELIEF OBJECT FOR FINGERPRINT READING”，所有这些专利申请都为本申请受让人所有，且都包括在此以供参考。

[0081] 此外，用户系统105可通过传统的服务提供商被连接到通信链路125，诸如拨号上网，数字用户线(DSL)，线缆调制解调器，光纤连接，等等。按照另一个实施例，用户系统105通过网络连接，诸如局域网或广域网来连接通信链路125。按照一个实施例，操作系统包括处理在通信链路125上传递的所有入局和出局消息业务的TCP/IP协议栈。

[0082] 虽然用户系统105是参考前面的实施例公开的，但本发明不限于前面的实施例。相反，本领域技术人员可从这里的公开认识到用户系统105有大量可替换的实施例，几乎包括任何能够向/从另一个计算机系统发送/接收信息的计算装置。例如，用户系统105可包括，但不限于计算机工作站，互动电视，交互查询系统(interactive kiosk)，个人移动计算装置，如数字助理，移动电话，膝上型计算机，等等，无线通信装置，智能卡，嵌入式计算装置等等，这些都可以与通信链路125互动。在这类替换系统中，操作系统可能彼此不同并为特定装置调整。然而，按照一个实施例，操作系统有利地继续为在通信链路125上建立通信所需提供适当的通信协议。

[0083] 图1示出了授信引擎110。按照一个实施例，授信引擎110包括一个或多个安全服务

器，用于访问和存储敏感信息，其中敏感信息可以是任何类型或形式的数据，例如文本、音频、视频、用户鉴权数据和公共密钥和私人密钥，但不限于这些。按照一个实施例，鉴权数据包括被设计用于唯一地识别密码系统100的用户的数据。例如，鉴权数据可包括用户标识号，一个或多个生物统计特征，和一系列由授信引擎110或用户生成的问题和回答，但最初由用户在登记时回答。前面的问题可包括人口统计数据，如出生地、地址、周年纪念日等，个人信息，如母亲的娘家姓、喜欢的冰激凌等，或其他唯一识别用户的数据。授信引擎110将与当前交易相关联的用户鉴权数据与以前提供-诸如在登记时提供-的鉴权数据进行比较。授信引擎110有利地可以要求用户在每次交易时生成鉴权数据，或授信引擎110有利地可以允许用户周期性地生成鉴权数据，诸如在开始一系列交易时或在登录到特定卖主网址时。

[0084] 按照其中用户生成生物统计特征数据的一个实施例，用户提供物理特征，诸如面部扫描，手扫描，耳朵扫描，虹膜扫描，视网膜扫描，血管图案，DNA，指纹，笔迹或语音给生物统计特征装置107，但不局限于这些特征。生物统计特征装置有利地产生物理特征的电子图案、或生物统计特征。电子图案通过用户系统105被传递到授信引擎110，用于登记或鉴权。

[0085] 一旦用户生成适当的鉴权数据且授信引擎110确定该鉴权数据(当前鉴权数据)与登记时所提供的鉴权数据(登记鉴权数据)正面(positive)匹配，则授信引擎110向用户提供完整的密码功能。例如，被适当鉴权的用户有利地可以采用授信引擎110来执行散列处理、数字签名、加密和解密(通常一起被称为加密)、创建或分布数字证书等。然而，用作密码功能中的私人密钥不能在授信引擎110外得到，因而确保密码密钥的完整性。

[0086] 按照一个实施例，授信引擎110生成并存储密码密钥。按照另一个实施例，至少一个密码密钥与每个用户相关联。而且，当密码密钥包括公钥技术时，与用户相关联的每个私钥在授信引擎110内被生成且不被发出(release)。因此，只要用户有权访问授信引擎110，用户就可利用他或她的私钥或公钥来执行密码功能。这样的远程访问有利地允许用户完全保持移动性，并通过实际上任何因特网连接来访问密码功能，诸如蜂窝和卫星电话，信息亭，膝上型计算机，宾馆房间等。

[0087] 按照另一个实施例，授信引擎110利用为授信引擎110所生成的密钥对来执行密码功能。按照该实施例，授信引擎110首先鉴权用户，并且在用户已经适当地生成与登记鉴权数据匹配的鉴权数据后，授信引擎110代表被鉴权用户而使用其自身的密码密钥对来执行密码功能。

[0088] 本领域技术人员将从这里公开的内容认识到密码密钥可有利地包括某些或所有对称密钥，公钥，私钥。此外，本领域技术人员将从这里的公开认识到前面的密钥可以用大量算法执行，这些算法可从商业技术获得，如RSA，ELGAMAL等。

[0089] 图1也示出了认证授权方(certificate authority)115。按照一个实施例，认证授权方115有利地可以包括可信的第三方组织或公司，其发出数字证书，诸如VeriSign，Baltimore，Entrust等。授信引擎110有利地可以通过一个或多个传统的数字证书协议、诸如PKCS10发送对数字证书的请求至认证授权方115。作为响应，认证授权方115将以大量不同协议中的一种或多种，诸如PKCS7发出数字证书。按照本发明的一个实施例，授信引擎110向几个或所有知名认证授权方(prominent certificate authority)115请求数字证书，使得授信引擎110有权访问对应于任何请求方的证书标准的数字证书。

[0090] 按照另一个实施例，授信引擎110内部地执行证书发布。在该实施例中，在请求证

书时，例如在密钥生成时或在请求时刻所请求的证书标准中，授信引擎110可访问证书系统以生成证书和/或可以内部地生成证书。授信引擎110将在下面更详细地公开。

[0091] 图1还示出了卖主系统120。按照一个实施例，卖主系统120有利地包括网络服务器。典型的网络(Web)服务器通常利用多种因特网标记语言或文档格式标准、诸如超文本标记语言(HTML)或可扩展标记语言(XML)之一经因特网提供内容。网络服务器接受来自诸如Netscape和Internet Explorer这样的浏览器的请求，然后返回适当的电子文档。大量服务器或客户端技术可被用来增加Web服务器的功能使其超出其传送标准电子文档的能力。例如，这些技术包括通用网关接口(CGI)脚本，安全套接层(SSL)安全性，和动态服务器页(ASP)。卖主系统120有利地可以提供关于商业，个人，教育或其他交易的电子内容。

[0092] 虽然卖主系统120是参考前面的实施例公开的，本发明不限于此。本领域技术人员可以这里的公开内容认识到，卖主系统120可有利地包括参考用户系统105说明的任何装置或其组合。

[0093] 图1也示出了连接用户系统105、授信引擎110、认证授权方115、和卖主系统120的通信链路125。按照一个实施例，通信链路125优选地包括因特网。本公开所用的因特网是计算机环球网络。因特网的结构对本领域技术人员是公知的，其包括网络主干及其分支。这些分支进而也包括分支，如此类推。路由器在网络层间移动信息包，然后从一个网络到另一个网络，直到分组到达其目的地区域内。目的地网络主机将信息包从该目的地发送到适当的终端或节点。在一个有利的实施例中，因特网路由集线器包括域名系统(DNS)服务器，该域名系统服务器使用传输控制协议/因特网协议(TCP/IP)，这是本领域公知的。路由集线器经高速通信线路连接到一个或多个其他路由集线器。

[0094] 因特网一个流行的部分是万维网。万维网含不同类型的计算机，这些计算机存储能够显示图形和文本信息的文件。提供关于万维网信息的计算机通常称为“网址”。网址由具有相关电子页面的因特网地址定义。电子页面可由统一资源定位器(URL)识别。通常电子页面是组织文本、图形图像、音频、视频等呈现的文档。

[0095] 虽然通信链路125是以其优选实施例公开的，本领域技术人员可从这里公开中认识到通信链路125可包括宽范围的交互通信链路。例如，通信链路125可包括交互电视网络，电话网络，无线数据传输系统，双向缆线系统，定制的私人或公共计算机网络，交互查询网络，自动柜员机网络，直接链路(direct link)，卫星或蜂窝网络等等。

[0096] 图2示出了按照本发明一个实施例的方面的图1中授信引擎110的方框图。如图2所示，授信引擎110包括交易引擎205、存储库210、鉴权引擎215、密码引擎220。按照本发明一个实施例，授信引擎110还包括海量存储装置225。如图2所示，交易引擎205与存储库210、鉴权引擎215和密码引擎220以及海量存储装置225通信。此外，存储库210与鉴权引擎215、密码引擎220、海量存储装置225通信。而且，鉴权引擎215与密码引擎220通信。按照本发明一个实施例，部分或所有前述通信有利地可以包括将XML文档传输到对应于接收装置的IP地址。如前面所述，XML文档有利地允许设计人员创建他们自己定制的文档标签(tag)，使得数据能够在应用程序之间和组织之间定义，传输，确认和编译。而且，部分或所有前述通信可包括传统SSL技术。

[0097] 按照一个实施例，交易引擎205包括数据路由装置，诸如可从Netscape，Microsoft，Apache等得到的传统Web服务器。例如，Web服务器有利地可以从通信链路125接

收进入数据。按照本发明的一个实施例，进入数据被寻址到用于授信引擎110的前端安全系统。例如，前端安全系统有利地可以包括防火墙、搜索已知攻击模式(attack profile)的入侵检测系统和/或病毒扫描器。在清理(clear)前端安全系统后，数据被交易引擎205接收并被路由到存储库210、鉴权引擎215、密码引擎220、和海量存储装置225之一。此外，交易引擎205监视来自鉴权引擎215和密码引擎220的进入数据，并通过通信链路125将该数据路由到特定系统。例如，交易引擎205有利地可以将数据路由到用户系统105、认证授权方115、或卖主系统120。

[0098] 按照一个实施例，数据是用传统HTTP路由技术路由的，如采用URL或统一资源指示器(RUL)。URI类似于URL，然而，URI通常指示文件或动作的资源，如，可执行文件，脚本文件等。因此，按照一个实施例，用户系统105，认证授权方115，卖主系统120，和授信引擎210的组件，有利地包括通信URL或URI内足够的数据以便交易引擎205适当地在整个密码系统内路由数据。

[0099] 虽然数据路由是参考优选实施例公开的，本领域技术人员可认识到有大量可能的数据路由解决方案或策略。例如，XML或其他数据分组可有利地通过他们的格式，内容等解包和识别，因此交易引擎205可适当地在整个授信引擎110中路由数据。而且本领域技术人员可认识到数据路由可有利地适应符合特定网络系统，例如在通信链路125包括局域网时的数据传输协议。

[0100] 按照本发明另一个实施例，交易引擎205包括传统的SSL加密技术，从而在特定通信过程中，前述系统可借助交易引擎205鉴定其自身，反之亦然。如本说明书中所用的那样，术语“1/2SSL”指其中服务器被SSL鉴定，但客户端不必被SSL鉴权的通信，术语“全SSL”指客户端和服务器都被SSL鉴权的通信。当本说明书使用术语“SSL”时，通信可以包括1/2或全SSL。

[0101] 因为交易引擎205路由数据到密码系统100的多个组件，所以交易引擎205有利地可以创建审计跟踪(audit trail)。按照一个实施例，审计跟踪包括交易引擎205所路由的至少该类型和格式的数据在整个密码系统100中的记录。这样的审计数据有利地可以被存储在海量存储装置225中。

[0102] 图2还示出存储库210。按照一个实施例，存储库210包括一个或多个数据存储设施，诸如目录服务器、数据库服务器等。如图2所示，存储库210存储密码密钥和登记鉴权数据。密码密钥有利地可以对应于授信引擎110或对应于密码系统100的用户，诸如用户或卖主。登记鉴权数据有利地可以包括用于唯一识别用户身份的数据，如用户ID，口令，问题答案，生物统计特征数据等等。该登记鉴权数据有利地可以在用户登记时或在另一可选的时间被采集。例如，授信引擎110可包括登记鉴权数据的周期性或其他更新或再发出。

[0103] 按照一个实施例，交易引擎205与鉴权引擎215和密码引擎220之间的通信包括安全通信，诸如传统的SSL技术。此外，如前面所述，传输到存储仓库210及从其发出的数据可用URL，URI，HTTP或XML文档传输，且其中有利地嵌入有前述的数据请求和格式。

[0104] 如上所述，存储仓库210可有利地包括多个安全数据存储设施。在这样的实施例中，安全数据存储设施可配置以便单个数据存储设施中安全上的让步不会危害其中存储的密钥或鉴定数据。例如，按照该实施例，密钥和鉴定数据可数学运算，以便统计地并充分地随机化存储在每个数据存储设施内的数据。按照一个实施例，单个数据存储设施数据的随

机化使得该数据不可判读。因此，单个数据存储设施的妥协仅产生随机化的不可判读的数字，且不会危及任何作为整体的密钥或鉴定数据的安全性。

[0105] 图2还示出授信引擎110，其包括鉴权引擎215。按照一个实施例，鉴权引擎215包括数据比较器，该比较器被配置为比较来自交易引擎205的数据与来自存储库210的数据。例如，在鉴权过程中，用户提供当前鉴权数据给授信引擎110，从而交易引擎205接收当前鉴权数据。如前面所述，交易引擎205识别数据请求，优选在URL或URI中，并将鉴权数据路由到鉴权引擎215。而且，一旦请求，存储库210将对应于用户的登记鉴权数据转发到鉴权引擎215。因此，鉴权引擎215既有当前鉴权数据，也有登记鉴权数据以便比较。

[0106] 按照一个实施例，对鉴权引擎的通信包括安全通信，诸如SSL技术。此外，安全性可被提供在授信引擎110组件内，诸如使用公钥技术的超级加密(super-encryption)。例如，按照一个实施例，用户以鉴权引擎215的公钥加密当前鉴权数据。此外，存储库210也以鉴权引擎215的公钥加密登记鉴权数据。以该方式，仅鉴权引擎的私钥可被用来解密传输。

[0107] 如图2所示，授信引擎110还包括密码引擎220。按照一个实施例，密码引擎包括密码操纵模块(cryptographic handling module)，其被配置为有利地提供传统的密码功能，诸如公钥基础设施(PKI:public-key infrastructure)功能。例如，密码引擎220有利地可以为密码系统100的用户发出公钥和私钥。以该方式，密码钥匙在密码引擎220处被生成并被转发给存储库210，从而至少私有密码密钥不能在授信引擎110外部得到。按照另一个实施例，密码引擎220至少将私有密码密钥随机化并分割，因而仅存储随机化的分割数据。类似于登记鉴权数据的分割，分割过程确保所存储的密钥不能在密码引擎220外部得到。按照另一个实施例，密码引擎的功能可与鉴权引擎215组合并由该鉴权引擎执行。

[0108] 按照一个实施例，与密码引擎的通信包括安全通信，如SSL技术。此外，XML文档可有利地用来传输数据和/或进行密码功能请求。

[0109] 图2还示出了具有海量存储装置225的授信引擎110。如前面所述，交易引擎205保持对应于审计跟踪的数据，并在海量存储装置225中存储这样的数据。类似地，按照本发明一个实施例，存储库210保持对应于审计跟踪的数据，并在海量存储装置225中存储这样的数据。存储库审计跟踪数据与交易引擎205的类似之处在于审计跟踪数据包括存储库210所接收的请求记录及其响应。此外，海量存储装置225可被用来存储其中包含有用户的公钥的数字证书。

[0110] 虽然授信引擎110是相对于其优选和可替换的实施例公开的，但本发明不限于这些实施例。本领域技术人员将从本公开中认识到有授信引擎110的大量可替代物。例如，授信引擎110可有利地只执行鉴定，或者，可替换地，仅执行某些或所有密码功能，如数据加密和解密。按照该实施例，鉴定引擎215和密码引擎220之一可有利地被除去，因而产生更直接的授信引擎110的设计。此外，密码引擎220也可与认证授权方通信，以便认证授权方嵌入到授信引擎110内。按照另一个实施例，授信引擎110可有利地执行鉴定和一个或多个密码功能，如数字签名。

[0111] 图3示出按照本发明一个实施例的方面的图2中交易引擎205的方框图。按照该实施例，交易引擎205包括具有处理线程和监听线程的操作系统305。操作系统305有利地可以类似于传统高容量服务器中的那些，诸如Apache公司所提供的Web服务器的操作系统。监听线程监视来自通信链路125、鉴权引擎215、和密码引擎220之一的进入进入通信用于进入数

据流。处理线程辨别进入数据流的特定数据结构，诸如前述数据结构，因而将进入数据路由到通信链路125、存储库210、鉴权引擎215、密码引擎220、或海量存储装置225之一。如图3所示，进入和发出数据可有利地例如通过SSL技术而被保护。

[0112] 图4示出了按照本发明一个实施例的方面的图2中存储库210的方框图。按照该实施例，存储库210包括一个或多个轻量级目录访问协议(LDAP:lightweight directory access protocol)服务器。LDAP目录服务器可从许多制造商得到，诸如Netsacpe，ISO和其他制造商。图4也示出了目录服务器优选地存储对应于密码密钥的数据405和对应于登记鉴权数据的数据410。按照一个实施例，存储库210包括将鉴权数据和密码密钥数据索引到唯一用户ID的单逻辑存储结构。单逻辑存储结构优选地包括确保存储在其中的数据的高可信度或安全性的机制。例如，存储库210的物理位置有利地可以包括大量传统的安全措施，诸如受限雇员访问，现代监视系统等。作为物理安全性的补充或替代，计算机系统或服务器有利地可以包括软件解决方案来保护所存储的数据。例如，存储库210有利地可以创建和存储对应于所采取的动作的审计跟踪的数据415。此外，入局和出局通信可有利地以与传统SSL技术耦合的公钥加密而被加密。

[0113] 按照另一个实施例，存储库210可包括不同的且物理分开的数据存储设施，如下面参考图7的描述。

[0114] 图5示出按照本发明实施例的方面的图2中鉴权引擎215的方框图。类似于图3中的交易引擎205，鉴权引擎215包括操作系统505，该操作系统至少具有改进形式的传统Web服务器的监听和处理线程，如Apache公司的Web服务器。如图5所示，鉴权引擎215包括对至少一个私钥510的访问。私钥510可有利地被用来例如解密来自交易引擎205或存储库210的数据，这些数据是用鉴权引擎215的相应公钥加密的。

[0115] 图5也示出了包括比较器515、数据分割模块520、和数据组装模块525的鉴权引擎215。按照本发明的优选实施例，比较器515包括能够比较与前述生物统计特征鉴定数据相关的潜在复杂图案的技术。该技术可包括硬件，软件，或组合解决方案用于图案比较，如表示指纹图案或语音图案的那些。此外，按照一个实施例，鉴权引擎215的比较器515可有利地比较文档的传统散列，以便提供比较结果。按照本发明的一个实施例，比较器515包括将探试过程(heuristics)530应用于比较。探试过程530可有利地涉及鉴权尝试周围的环境，诸如时间，IP地址或子网掩码，采购概况(purchasing profile)，电子邮件地址，处理器序列号或ID，等等。

[0116] 而且，生物统计特征数据比较的特性可导致当前生物统计特征鉴定数据与登记数据匹配产生的可信度变化。例如，与传统口令不同，传统口令可能仅返回正或负匹配，而指纹可判断为部分匹配，如90％匹配，75％匹配，10％匹配，而非简单的正确或不正确。其他生物统计特征识别，如声纹分析或面容识别也可有概率鉴定的这种特性，而非绝对鉴定。

[0117] 在概率鉴定或在鉴定不是当作绝对可靠的其他情形中，有必要应用探试过程530判断所提供的鉴定可信度是否足够高，从而鉴定正在进行的交易。

[0118] 有时是这样的情形，讨论中的交易是相对低值的交易，这样的交易被鉴定为较低的可信度是可以接受的。这可包括具有与其相关的低美元值的交易(如10美元的采购)或低风险的交易(如进入会员专用网站)。

[0119] 相反，对于鉴定其他交易，有必要在允许交易进行之前，要求高可信度的鉴定。这

样的交易可包括大美元值交易(如签署几百万美元供应合同)或如果鉴定不当具有高风险的交易(如远程登录到政府计算机)。

[0120] 使用结合可信度和交易值的探试过程530可如下所述那样使用,从而允许比较器提供动态的、内容敏感的鉴定系统。

[0121] 按照本发明另一个实施例,比较器515可有利地为特定交易跟踪鉴定尝试。例如,当交易失败时,授信引擎110可请求用户再次输入他或她的当前鉴定数据。鉴定引擎215的比较器515可有利地采用尝试限制器(attempt limiter)535限制鉴定尝试的次数,因而阻止暴力尝试模仿(impersonate)用户鉴定数据。按照一个实施例,尝试限制器535包括软件模块用于监视重复鉴定尝试的交易,以及例如对于给定的交易限制鉴定尝试次数为3次。因此,尝试限制器535限制自动尝试模仿个人鉴定数据,例如仅限制为3次"猜测"。在三次失败后,尝试限制器535可有利地拒绝额外的鉴定尝试。这样的拒绝可有利地通过下面的方式执行,例如比较器515返回负结果,而无论当前鉴定数据发出与否。另一方面,交易引擎205可有利地为三次尝试已经失败的交易阻挡任何额外的鉴定尝试。

[0122] 鉴定引擎215也包括数据分割模块520和数据组装模块525。数据分割模块520有利地包括软件,硬件,或能够数学运算不同数据以便充分随机化并分割数据为多个部分的组合模块。按照一个实施例,原始数据不能再从单个部分重新建立。数据组装模块525有利地包括软件,硬件,或组合模块,该组合模块经配置对前面基本随机化的部分进行数学运算,因此其组合提供原始可判读数据。按照一个实施例,鉴定引擎215采用数据分割模块520随机化和分割登记鉴定数据为多个部分,并采用数据组装模块525来将这些部分重新组装为不可用登记鉴定数据。

[0123] 图6示出按照本发明一个实施例的图2中授信引擎200的密码引擎220的方框图。类似于图3的交易引擎205,密码引擎220包括操作系统605,其至少具有改进形式的传统Web服务器的监听和处理线程,如可从Apache得到的Web服务器。如图6所示,密码引擎220包括功能类似于图5中相应模块的数据分割模块610和数据组装模块620。然而,按照一个实施例,数据分割模块610和数据组装模块620处理密钥数据,与前面登记鉴定数据相反。尽管如此,本领域技术人员可从这里的公开内容认识到,数据分割模块910和数据分割模块620可与鉴定引擎215的相应模块组合。

[0124] 密码引擎220也包括密码处理模块625,其经配置用于执行一个、部分或所有大量密码功能。按照一个实施例,密码处理模块625可包括软件模块或程序,硬件,或两者都有。按照另一个实施例,密码处理模块625可执行数据比较,数据解析,数据分割,数据分离,数据散列运算,数据加密或解密,数字签名、验证或创建,数字证书生成,存储或请求,密钥发生等。而且,本领域技术人员可从这里的描述认识到,密码处理模块825可有利地包括公钥基础设施,如Pretty Good Privacy(PGP),基于RSA的公钥系统,或大量可替换的密钥管理系统。此外,密码处理模块625可执行公钥加密,对称密钥加密,或这两种加密。除了前面的说明,密码处理模块625可包括一个或多个计算机程序或模块,硬件,或这两者供执行无缝透明的互操作功能。

[0125] 本领域技术人员可从这里的公开内容认识到密码功能可包括大量不同的通常涉及密钥管理系统的功能。

[0126] 图7示出按照本发明实施例存储仓库系统700的简化方框图。如图7所示,存储仓库

系统700有利地包括多个数据存储设施，例如数据存储设施D1，D2，D3，和D4。然而，本领域技术人员易于理解，存储仓库系统可仅有一个数据存储设施。按照本发明一个实施例，每个数据存储设施D1到D4可有利地包括参考图4中存储仓库210所述的部分或所有要素。类似于存储仓库210，数据存储设施D1到D4优选经传统SSL与交易引擎205，鉴定引擎215，密码引擎220通信。通信链路传输例如XML文档。与交易引擎205的通信可有利地包括对数据的请求，其中该请求有利地广播给每个数据存储设施D1到D4的IP地址。另一方面，基于大量标准，如响应时间，服务器负载，维护周期等，交易引擎205可广播请求给特定数据存储设施。

[0127] 响应来自交易引擎205的请求，存储仓库系统700有利地将存储的数据转送到鉴定引擎215和密码引擎220。各数据组装模块接收转送的数据并将这些数据组装为可用形式。另一方面，从鉴定引擎215和密码引擎220到数据存储设施D1到D4的通信可包括待存储敏感数据的传输。例如，按照一个实施例，鉴定引擎215和密码引擎220可有利地采用他们各自数据分割模块，从而将敏感数据分割为多个不可判读部分，且然后将敏感数据的一个或多个不可判读部分传输给特定数据存储设施。

[0128] 按照一个实施例，每个数据存储设施D1到D4包括分开并独立的存储系统，如目录服务器。按照本发明另一个实施例，存储仓库700包括多个地理上分开的独立数据存储系统。通过分布所述敏感数据到不同并独立的存储设施D1到D4中，其中存储设施的某些或全部可有利地地理分离，存储仓库系统700提供冗余和额外的安全措施。例如，按照一个实施例，多个数据存储设施D1到D4中仅两个存储设施的数据需要解读并重组敏感数据。因此，四个数据存储设施D1到D4中两个可能由于维护，系统故障，电源故障等而不起作用，但不会影响授信引擎110的功能。此外，按照一个实施例，因为存储在每个数据存储设施中的数据是随机化并且是不可判读的，对任何单个数据存储设施的危害不必危害该敏感数据。而且，在数据存储设施具有地理分离的实施例中，危害多个地理远程设施变得更困难。实际上，甚至欺诈性雇员在扰乱所需的多个独立的地理远程数据存储设施时也面临极大的挑战。

[0129] 虽然存储仓库系统700是参考优选的可替换实施例公开的，本发明不局限于这些。本领域技术人员将从这里的公开认识到存储仓库系统700有大量的可替换者。例如，存储仓库系统700可包括一个，两个或更多数据存储设施。此外，敏感数据可数学运算以便两个或更多数据存储设施的多个部分需要重组并判读敏感数据。

[0130] 如前面所述，鉴定引擎215和密码引擎220分别包括数据分割模块520和610，以便分割任何类型或形式的敏感数据，如文本，音频，视频，鉴定数据和密钥数据。图8示出按照本发明一个实施例的数据分割模块执行的数据分割过程800的流程图。如图8所示，当敏感数据“S”被鉴定引擎215或密码引擎220的数据分割模块接收到时，数据分割过程800从步骤805开始。优选在步骤810，数据分割模块随后生成基本随机的数字，值，或字符串或比特集合“A.”。例如，随机数A可以用大量本领域技术人员可用的不同传统技术生成，以便产生高质量的适用于密码应用的随机数字。此外，按照一个实施例，随机数A包括任何合适长度的比特长度，如较短的，较长的或等于敏感数据S比特长度的比特长度。

[0131] 此外，在步骤820中，数据分割过程800生成另一个统计随机数“C”。按照优选实施例，统计上随机数字A和C可有利地平行生成。数据分割模块组合数字A和C与敏感数据S，因而生成新数字“B”和“D”。例如，数字B可包括A XOR S的二元组合(binary combination)，且数字D可包括C XOR S的二元组合。XOR函数，或“exclusive-or”“异或”函数是本领域技术人

员公知的。前面的组合分别优选出现在步骤825和830中，并且按照一个实施例，前面的组合也可平行出现。然后数据分割过程800进入到步骤835，这里随机数字A和C以及数字B和D成对，因此没有哪一对自身含足够再组和判断原始敏感数据S的数据。例如，下面这些数字可成对：AC，AD，BC，和BD。按照一个实施例，每个前述对分布到图7中存储仓库D1到D4之一。按照另一个实施例，每个前述对随机分布到存储仓库D1到D4之一。例如，在第一数据分割过程800中，数字对AC可发送到存储仓库D2，例如通过随机选择D2的IP地址。然后，在第二数据分割过程800中，数字对AC可发送到存储仓库D4，例如通过随机选择D4的IP地址。此外，数字对可都存储在一个存储仓库上，并可存储在所述存储仓库上分开的位置。

[0132] 基于前面所述，数据分割过程800有利地将敏感数据的组成部分存放在四个数据存储设施D1到D4的每个设施中，因此数据存储设施D1到D4中没有一个包括足够的加密数据来重建原始敏感数据S。如上所述，这类将数据随机化为各个不可用加密部分增加了安全性并为所述数据中保持的信任作准备，即使D1到D4中一个数据存储设施被危害。

[0133] 虽然数据分割过程800是参考优选实施例公开的，但本发明不限于此。本领域技术人员可从这里的公开内容认识到数据分割过程800有大量可替换过程。例如，数据分割过程可有利地分割数据为两个数字，例如随机数字A和数字B，并在两个数据存储设施中随机分布A和B。而且，数据分割过程800可有利地通过生成额外随机数字在大量数据存储设施中分割数据。数据可分割为任何所需的，选择的，预定的，或随机分配大小的单元，包括但不限于，一个比特，多个比特，字节，千字节，兆字节或更大，或多个大小的组合或序列。此外，改变源自分割过程的数据单元大小可使数据更难于恢复到可用形式，因而增加敏感数据的安全性。对本领域技术人员来说，显然所述分割数据单元大小可以是多种数据单元大小或大小花样方式或大小组合。例如，数据单元大小可选择或预定为所有相同大小，不同大小的固定集合，多个大小组合，或随机发生大小。类似地，按照固定或预定数据单元大小，数据单元大小的花样方式或组合，或随机生成的每个共享体的数据单元大小或多个大小，数据单元可分布到一个或多个共享体。

[0134] 如前面所述，为了再建敏感数据S，数据部分需要去随机化并再组。该过程可有利地分别出现在鉴定引擎215和密码引擎220的数据组装模块525和620中。数据组装模块，例如数据组装模块525从数据存储设施D1到D4接收数据部分，并再组数据为不可用的形式。例如，按照数据分割模块520采用了图8中数据分割过程800的一个实施例，数据组装模块525使用来自数据存储设施D1到D4中至少两个数据存储设施的数据部分，从而再建敏感数据S。例如，分布数字对AC，AD，BC，和BD，以便任意两个数字对提供A和B，或C和D中的一个。注意S＝A XOR B或S＝C XOR D指示当数据组装模块接收A和B，或C和D中的一个时，数据组装模块525可有利地再组敏感数据S。因此，例如数据组装模块525在接收来自数据存储设施D1到D4中至少两个数据存储设施的数据部分时，数据组装模块525可组装敏感数据S，从而响应授信引擎110的组装请求。

[0135] 基于上面的数据分割和组装过程，敏感数据S仅以可用形式存在于授信引擎110的有限区域中。例如，当敏感数据S包括登记鉴定数据时，可用的非随机化登记鉴定数据仅可在鉴定引擎215中得到。相似地，当敏感数据S包括私人密钥数据时，可用的非随机化私人密钥数据仅可在鉴定引擎220中得到。

[0136] 虽然数据分割和组装过程是参考他们的优选实施例公开的，本发明不限于此。本

领域技术人员可从这里的公开认识到，分割和重组敏感数据S有大量可替换方式。例如，公钥加密可用于进一步安全保护数据存储设施D1到D4的数据。此外，本领域技术人员易于理解，这里所述的数据分割模块也是本发明分开的独立实施例，其可包括到任何现有计算机系统，软件套件(software suite)，数据库，或其组合，或者本发明其他实施例，如这里公开并描述的授信引擎，鉴定引擎，和交易引擎中，或与它们结合或构成它们的一部分。

[0137] 图9A示出按照本发明实施例的登记过程900的数据流。如图9A所示，当用户希望登录密码系统100的授信引擎110时，登记过程900从步骤905开始。按照该实施例，用户系统105有利地包括客户端小应用程序(applet)，如Java基的小应用程序，其询问用户输入登记数据，如人口数据和登记鉴定数据。按照一个实施例，登记鉴定数据包括用户ID，口令，生物统计特征，等等。按照一个实施例，在询问过程中，客户端小应用程序优选与授信引擎110通信，以确保所选用户ID是唯一的。当用户ID不是唯一的时，授信引擎110可有利地建议唯一用户ID。客户端小应用程序收集登记数据并传输登记数据，例如通过XML文档传输到授信引擎110，具体而言，传输到交易引擎205。按照一个实施例，传输是以鉴定引擎215的公钥编码的。

[0138] 按照一个实施例，用户在登记过程900的步骤905中执行单个登记。例如，用户将其自己登记为特定人，如Joe用户。当Joe用户需要登记为Joe用户，Mega公司的CEO时，那么按照该实施例，Joe用户登记第二次，接收第二唯一用户ID，且授信引擎110不关联这两个身份。按照本发明另一个实施例，登记过程900为单个用户ID提供多次用户识别。因此，在上面的例子中，授信引擎110将有利地关联Joe用户的两个身份。如本领域技术人员从本公开理解的那样，一个用户可以有多个身份，例如Joe用户为户主，Joe用户为慈善基金会员等等。按照该实施例，即使用户可具有多种身份，授信引擎110优选仅存储一组登记数据。而且，当需要时，用户可有利地按需要添加，编辑/更新，或删除身份。

[0139] 虽然登记过程900是参考优选实施例公开的，本发明不限于此。本领域技术人员将从这里的描述认识到有大量替换方式收集登记数据，特别是登记鉴定数据。例如，小应用程序可以是公用对象模型(COM)基的小应用程序等等。

[0140] 另一方面，登记过程可包括分级登记。例如，在最低登记级别，用户可经通信链路125登记，而无需产生关于他或她身份的文档。按照登记级别的增加，用户用授信的第三方，如数字公证人登记。例如，用户可亲自到授信的第三方处建立证件，如出生证明，驾驶执照，军方ID等，且授信第三方可有利地包括例如登记提交文件中他们的数字签名。授信第三方可包括实际公证人，政府机构，如邮政局或机动车部门，招募雇员的大公司中人力资源人员。本领域技术人员可从这里的公开理解大量不同级别的登记可在登记过程900中出现。

[0141] 在步骤915接收登记鉴定数据后，交易引擎205使用传统FULL SSL技术转发该登记鉴定数据给鉴定引擎215。在步骤920，鉴定引擎215用鉴定引擎215的私钥解密登记鉴定数据。此外，鉴定引擎215采用数据分割模块对登记鉴定数据执行数学运算，以便将数据分割为至少两个独立不可判读的随机化数字。如前面所述，至少两个数字可包括统计上的随机数字和二元XOR数字。在步骤925中，鉴定引擎215将随机化数字的每个部分转发给数据存储设施D1到D4之一。如前面所述，鉴定引擎215传输到存储仓库的部分。

[0142] 通常在登记过程900中，用户也会需要发出数字证书以便他或她可从密码系统100外部接收加密的文档。如前面所述，认证授权方115通常按照数个传统标准中的一个或多个

来发出数字证书。一般地，该数字证书包括人人都知道的用户或系统的公钥。

[0143] 无论用户是否在登记时或其他时间请求数字证书，该请求都经授信引擎110传输到鉴定引擎215。按照一个实施例，请求包括XML文档，其具有例如正确的用户名称。根据步骤935，鉴定引擎215传输请求到密码引擎220，指示密码引擎220，从而生成密钥或密钥对。

[0144] 在步骤935，在收到请求后，密码引擎220生成至少一个密钥。按照一个实施例，密码处理模块625生成密钥对，这里一个密钥用作私钥，另一个用作公钥。按照一个实施例，密码引擎220存储公钥的副本和私钥。在步骤945，密码引擎220发送数字证书的请求给交易引擎205。按照一个实施例，该请求有利地包括标准化的请求，如XML文档中嵌入的PKCS10。数字证书的请求可有利地相应于一个或多个认证授权方，以及认证授权方要求的一种或多种标准格式。

[0145] 在步骤950中，交易引擎205将该请求转交给认证授权方115，在步骤955中，认证授权方115返回数字证书。返回的数字证书可有利地采用标准化的格式，如PKCS7，或采用一个或多个认证授权方115专有的格式。在步骤960中，数字证书是通过交易引擎205接收的，且一个副本被转交给用户，一个副本由授信引擎110存储。授信引擎110存储证书副本，以便授信引擎110不必依赖于认证授权方115的可用性。例如，当用户需要发送数字证书，或第三方请求用户数字证书时，对数字证书的请求通常被发送到认证授权方115。然而，如果认证授权方115在执行维护或具有故障或安全危害，可能得不到数字证书。

[0146] 在发出密钥后的任何时间，密码引擎220可有利地采用上面要求的数据分割过程800，以便密钥被分成独立不可判读的随机化数字。类似于鉴定数据，在步骤965，密码引擎220传输随机化的数字给数据存储设施D1到D4。

[0147] 本领域技术人员将从这里的公开认识到，用户可在登记后的任意时间请求数字证书。而且，系统间通信可有利地包括FULL SSL或公钥加密技术。而且，登记过程可从多个认证授权方发出多个数字证书，包括授信引擎110内部或外部的一个或多个专有认证授权方。

[0148] 如步骤935到960中的公开，本发明一个实施例包括对最后存储在授信引擎110中证书的请求。因为按照一个实施例，密码处理模块625发出授信引擎110使用的密钥，每个证书相应于一个私钥。因此，授信引擎110可有利地通过监视用户所拥有或关联的证书而提供互操作性。例如，当密码引擎220接收密码功能的请求时，密码处理模块625可调查请求用户所拥有的证书，并判断是否该用户拥有与请求属性相匹配的私钥。当这样的证书存在时，密码处理模块625可使用该证书或与其关联的公钥或私钥来执行所请求的功能。当这样的证书不存在时，密码处理模块625可有利并透明地执行大量动作从而试图对缺失适当的密钥进行补救。例如，图9B示出互操作性过程970的流程图，按照本发明实施例，该过程公开了前述步骤从而确保密码处理模块625使用适当密钥执行密码功能。

[0149] 如图9B所示，互操作性过程970从步骤972开始，这里密码处理模块925判断所需证书的类型。按照本发明一个实施例，证书类型可有利地规定在对密码功能的请求中，或规定在请求者提供的其他数据中。按照另一个实施例，证书类型可由请求的数据格式确定。例如，密码处理模块925可有利地识别相应于特殊类型的请求。

[0150] 按照一个实施例，证书类型可包括一个或多个算法标准，例如RSA，ELGAMAL等。此外，证书类型可包括一个或多个密钥类型，如对称密钥，公钥，强加密密钥，如256比特密钥，较低安全密钥等等。而且，证书类型可包括一个或多个前述算法标准或密钥，一个或多个消

息或数据格式，一个或多个数据封装或编码方案，如Base 32或Base 64，的升级或取代。证书类型也可包括与一个或多个第三方密码应用程序或接口，一个或多个通信协议，或一个或多个证书标准或协议的兼容性。本领域技术人员可从这里的公开认识到其他差别可存在于证书类型中，并且这些差别间的转化可按这里的公开执行。

[0151] 一旦密码处理模块625判断了证书类型，则互操作性过程970进入到步骤974，并判断是否用户拥有与步骤974中判断的类型匹配的证书。当用户拥有匹配证书时，例如授信引擎110有权通过其之前的存储访问匹配的证书，密码处理模块825知道匹配私钥也存储在授信引擎110内。例如，匹配私钥可以存储在存储仓库210内或存储仓库系统700中。密码处理模块625可有利地请求在存储仓库210组装匹配私钥，然后在步骤976，使用该匹配私钥执行密码动作或功能。例如，如前面所述，密码处理模块625可有利地执行散列运算，散列比较，数据加密或解密，数字签名验证或创建等。

[0152] 当用户没有匹配证书时，互操作过程970进入步骤978，这里密码处理模块625判断用户是否拥有交叉认证证书(cross-certified certificate)。按照一个实施例，当第一认证授权方决定信任第二认证授权方的证书时发生认证授权方之间的交叉认证。换句话说，第一认证授权方确定第二认证授权方的证书满足某些质量标准时，并因此可“证明”为等价于第一认证授权方自己的证书。在认证授权方发出，例如具有多个信任级别的证书时，交叉认证变得更复杂。例如，第一认证授权方通常基于登记过程的可靠程度，可为特定证书提供三个信任级别，同时第二认证授权方可提供七个信任级别。交叉认证可有利地跟踪第二认证授权方的哪个级别和哪个证书可替换第一认证授权方的哪个级别和哪个证书。当前面的交叉认证是官方并公开地在两个证书授权方间进行的时，一个到另一个证书和级别的映射通常别称为“链接(chaining)”。

[0153] 按照本发明另一个实施例，密码处理模块625可有利地开发在认证授权方同意的交叉认证之外的交叉认证。例如密码处理模块625可访问第一认证授权方的认证执行声明(CPS)，或其他公布的政策陈述，并使用例如特定信任级别要求的鉴定标记，匹配第一认证授权方的证书和另一个认证授权方的证书。

[0154] 在步骤978中，当密码处理模块625判断用户拥有交叉认证证书，互操作过程970进入步骤976，并用交叉认证公钥，私钥或这两者执行密码动作或功能。可替换地，当密码处理模块625判断用户没有交叉认证证书时，互操作过程970进入步骤980，这里密码处理模块625选择认证授权方，该认证授权方发出所请求的证书类型，或证书交叉认证。在步骤982，密码处理模块625判断前面讨论的用户登记鉴定数据是否满足所选认证授权方的鉴定要求。例如，如果用户经网络通过回答人口和其他问题而登记，则所提供的鉴定数据可建立低于用户提供生物统计特征数据和第三方，如公证人见证的信任级别。按照一个实施例，前面的鉴定要求可有利地提供在所选的鉴定授权方的CPS中。

[0155] 当用户向授信引擎110提供了符合所选认证授权方要求的登记鉴定数据后，互操作过程970进入步骤984，这里密码处理模块825采集来自所选认证授权方的证书。按照一个实施例，密码处理模块625通过登记过程900的随后步骤945到960采集证书。例如，密码处理模块625可有利地采用密码引擎220可用的一个或多个密钥对的一个或多个公钥，从而要求认证授权方的证书。按照另一个实施例，密码处理模块625可有利地生成一个或多个新密钥对，并使用相应公钥请求认证授权方的证书。

[0156] 按照另一个实施例，授信引擎110可有利地包括一个或多个能够发出一种或多种证书类型的证书发出模块。按照该实施例，证书发出模块可提供前述证书。当密码处理模块625获得证书时，互操作过程970进入步骤976，并用相应于采集证书的公钥，私钥，或这两者执行密码动作或功能。

[0157] 在步骤982中，当用户没有向授信引擎110提供符合所选认证授权方要求的登记鉴定数据时，在步骤986中，密码处理模块625判断是否有具有不同鉴定要求的其他认证授权方。例如，密码处理模块625可查找具有较低鉴定要求的认证授权方，但仍然发出所选证书或交叉认证。

[0158] 当存在前述具有较低要求的认证授权方时，互操作过程970进入步骤980并选择该认证授权方。可替换地，当不存在这类认证授权方时，在步骤988，授信引擎110可从用户请求额外的鉴定标记。例如，授信引擎110可请求包括例如生物统计特征数据的新登记鉴定数据。而且，授信引擎110可请求用户由可信的第三方见证，并向公证人提供适当的鉴定证明，如驾驶执照，社会安全卡，银行卡，出生证明，军人ID，等等。当授信引擎110接收更新的鉴定数据时，互操作过程970进入步骤984并获取前述所选证书。

[0159] 通过前述互操作过程970，密码处理模块625有利地提供不同密码系统间无缝、透明的翻译和转换。本领域技术人员可从这里的公开认识到前述互操作系统大量的优点和实现方法。例如，互操作过程970的前述步骤986可有利地包括下面进一步详细讨论的授信仲裁，这里认证授权方可在特定环境中接受较低级别的交叉认证。此外，互操作过程970可包括确保标准证书撤销的操作及各操作之间的互操作性，例如采用证书撤销列表(CRL)，在线证书状态协议(OCSP)等。

[0160] 图10示出按照本发明实施例的鉴定过程1000的数据流。按照一个实施例，鉴定过程1000包括从用户收集当前鉴定数据并将其与用户的登记鉴定数据比较。例如，鉴定过程1000在步骤1005开始，这里用户希望执行交易，譬如与卖主的交易。这样的交易可包括例如选择采购选项，请求访问受限制的区域或卖主系统120的装置等。在步骤1010，卖主向用户提供交易ID和鉴定请求。交易ID可有利地包括与128位随机量连接、具有32位时间信息的192位量，或与卖主特有的32位常数连接的“临时值(nonce)”。这样的交易ID唯一地识别交易，因此授信引擎110可拒绝模仿的交易。

[0161] 鉴定请求可有利地包括，对于特定交易需要何种鉴定级别。例如，卖主可规定讨论中交易所要求的特定信任级别。如果不能对该信任级别做出鉴定，如下面的讨论，如果用户没有进一步的鉴定以提升信任级别，或如果卖主与服务器间的鉴定条款没有改变，则交易将不会发生。这些问题将在下面更完整地讨论。

[0162] 按照一个实施例，交易ID和鉴定请求可有利地由卖主端的Java程序或其他软件程序生成。此外，交易ID和鉴定数据的传输可包括一个或多个用传统SSL技术，如1/2SSL加密的XML文档，1/2SSL换句话说就是卖主端鉴定的SSL。

[0163] 在用户系统105接收交易ID和鉴定请求后，用户系统105从用户收集当前鉴定数据，有可能包括当前生物统计特征信息。在步骤1015，用户系统105用鉴定引擎215的公钥加密至少当前鉴定数据“B”和交易ID，并将该数据转移到授信引擎110。该传输优选包括至少以传统1/2SSL技术加密的XML文档。在步骤1020中，交易引擎205接收传输，优选识别数据格式或URL或URI中的请求，并将该传输转发给鉴定引擎215。

[0164] 在步骤1015和1020中，卖主系统120在步骤1025用优选的FULL SSL技术将交易ID和鉴定请求转发给授信引擎110。该通信也可包括卖主ID，但卖主身份也可以通过交易ID的非随机部分来通信。在步骤1030和1035，交易引擎205接收通信，在审计跟踪中建立记录，并生成请求，用于请求从数据存储设施D1到D4组装的用户登记鉴定数据。在步骤1040，存储仓库系统700将相应于用户的登记鉴定数据的各部分转移到鉴定引擎215。在步骤1045，鉴定引擎215用其私钥解密传输，并比较登记鉴定数据和用户提供的当前鉴定数据。

[0165] 步骤1045的比较可有利地应用试探性内容敏感鉴定，如前面提到并在下面进一步详细讨论的那样。例如，如果所接收的生物统计特征信息不完美匹配，则匹配的信任级别较低。在特定实施例中，鉴定的信任级别是由交易的性质和用户与卖主双方的期望来平衡的。同样，这将在下面更详细地讨论。

[0166] 在步骤1050，鉴定引擎215将步骤1045的比较结果填入鉴定请求中。按照本发明一个实施例，鉴定过程1000的结果YES/NO或TRUE/FALSE被填入鉴定请求中。在步骤1055，填写的鉴定请求被返回给卖主供卖主采取动作，如允许发起鉴定请求的用户完成交易。按照一个实施例，确认消息被传递给用户。

[0167] 基于前面所述，鉴定过程1000有利地保持敏感数据安全并产生经配置以保持敏感数据完整性的结果。例如，敏感数据仅在鉴定引擎215内组装。例如，登记鉴定数据在被数据组装模块在鉴定引擎215中组装之前都是不可判读的，且当前鉴定数据在被传统SSL技术和鉴定引擎215的私钥解包(unwrapped)之前都是不可判读的。而且，传输给卖主的鉴定结果不包括敏感数据，且用户甚至不知道他或她是否产生了有效的鉴定数据。

[0168] 虽然鉴定过程1000是参考优选和可替换的实施例公开的，本发明不局限于这些实施例。本领域技术人员将从这里的公开认识到鉴定过程1000有大量的替换过程。例如，卖主可有利地由几乎任意请求应用程序取代，甚至是驻存在用户系统105中的应用程序。例如，客户端应用程序，如Microsoft Word，可在解锁文档之前使用应用程序接口(API)或密码API(CAPI)请求鉴定。可替换地，邮件服务器、网络、蜂窝电话、个人或移动计算装置、工作站等都可以作出鉴定请求，这些鉴定请求可由鉴定过程1000填写。实际上，在提供前面的可信鉴定过程1000后，请求应用程序或装置可提供对大量电子或计算机装置或系统的访问或使用。

[0169] 而且，鉴定失败时，鉴定过程1000可采用大量可替换过程。例如，鉴定失败后，可以保持同样的交易ID，并请求用户再次输入他或她的当前鉴定数据。如上所述，对于特定的交易，相同交易ID的使用允许鉴定引擎215的比较器监视和限制鉴定尝试的次数，因而产生更安全的密码系统100。

[0170] 此外，鉴定过程1000可有利地被用来开发简练的单个注册解决方案，如解锁敏感数据保险库(vault)。例如，成功的或正的鉴定可为已被鉴定的用户提供自动访问几乎无限数目的系统和应用程序的任意数目口令的能力。例如，用户的鉴定可提供与多个在线卖主、局域网、不同个人计算装置、因特网服务提供商、拍卖提供商、投资经纪人等关联的对口令、登录、经济证明(financial credential)等的用户访问。通过采用敏感数据保险库，用户可选择很大并且随机的口令，因为用户不再需要通过关联而记住这些口令。鉴定过程1000提供对敏感数据保险库的访问。例如，用户可选择长度为20多位的随机字母串，而非与可记忆的数据、名称等关联的口令。

[0171] 按照一个实施例，与给定用户关联的敏感数据保险库可有利地存储在存储仓库210的数据存储设施中，或分割并存储在存储仓库系统700中。按照该实施例，在正用户鉴定后，授信引擎110提供被请求的敏感数据，如适当的口令给请求应用程序。按照另一个实施例，授信引擎110可包括分开的系统，用于存储敏感数据保险库。例如，授信引擎110可包括执行数据保险库功能并象征性地驻存在授信引擎110的前述前端安全系统“后面”的独立软件引擎。按照该实施例，软件引擎在从授信引擎110接收到指示正用户鉴定的信号之后提供被请求的敏感数据。

[0172] 在另一个实施例中，数据保险库可通过第三方系统执行。类似于软件引擎实施例，第三方系统可有利地在从授信引擎110接收到指示正用户鉴定的信号之后提供被请求的敏感数据。按照另一个实施例，数据保险库可在用户系统105上执行。用户端软件引擎可有利地在从授信引擎110接收到指示正用户鉴定的信号之后提供前述数据。

[0173] 虽然前述数据保险库是参考可替换实施例说明的，本领域技术人员将从这里的公开认识到可有大量额外的执行方式。例如特定数据保险库可包括部分或所有前述实施例的多个方面。此外，任何前述数据保险库可在不同时间采用一个或多个鉴定请求。例如任何数据保险库可要求每个交易或多个交易、周期性地、每一次或多次会话、每次访问一个或多个网页或网址，在一个或多个规定的间隔，等等进行鉴定。

[0174] 图11示出按照本发明实施例签名过程1100的数据流。如图11所示，签名过程1100包括类似于前面参考图10说明的鉴定过程1000的步骤。按照本发明一个实施例，签名过程1100首先鉴定用户，然后执行几个数字签名功能中的一个或多个，如下面的详细说明。按照另一个实施例，签名过程1100可有利地存储与其相关的数据，如消息或文档的散列值等。该数据可有利地用在审计或任何其他事件中，例如当参与方试图否认交易时。

[0175] 如图11所示，在鉴定步骤的过程中，用户和卖主可有利地同意诸如合同之类的消息。在签名过程中，签名过程1100有利地确保用户签署的合同与卖主提供的合同相同。因此，按照一个实施例，在鉴定过程中，在传输到鉴定引擎215的数据中，卖主和用户包括他们各自的消息或合同副本的散列。仅仅通过采用消息或合同的散列，授信引擎110可有利地存储显著减少的数据量，提供更有效且更划算的密码系统。此外，存储的散列可有利地与被讨论的文档散列相比较从而判断被讨论的文档是否与任一方签署的文档匹配。判断该文档是否与涉及交易的文档相同的这一能力，为反驳交易一方要求的否认提供了额外的证据。

[0176] 在步骤1103中，鉴定引擎215组装登记鉴定数据并将其与用户提供的当前鉴定数据比较。当鉴定引擎215的比较器指示登记鉴定数据与当前鉴定数据相匹配时，鉴定引擎215的比较器也比较由卖主提供的消息散列和用户提供的消息散列。因此，鉴定引擎215有利地确保该用户同意的消息与卖主同意的消息相同。

[0177] 在步骤1105中，鉴定引擎215发送数字签名请求给密码引擎220。按照本发明一个实施例，请求包括消息或合同的散列。然而，本领域技术人员将从这里的公开认识到密码引擎220实际上可加密任意类型的数据，包括但不限于视频、音频、生物统计特征、图像或文本，从而形成所需的数字签名。返回到步骤1105，数字签名请求优选包括通过传统SSL技术通信的XML文档。

[0178] 在步骤110中，鉴定引擎215发送请求给每个数据存储设施D1到D4，因此每个数据存储设施D1到D4发送相应于签名方的各部分密钥。按照另一个实施例，密码引擎220采用前

面讨论的互操作过程970的部分或全部步骤，因此密码引擎220首先为签名方从存储仓库210或存储仓库系统700请求经密码引擎判断认为合适的密钥，并采取动作提供适当的匹配密钥。按照另一个实施例，鉴定引擎215或密码引擎220可有利地请求一个或多个与签名方关联并存储在存储仓库210或存储仓库系统700中的密钥。

[0179] 按照一个实施例，签名方包括用户和卖主之一或两者。在这样的情形中，鉴定引擎215有利地请求相应于用户和/或卖主的密钥。按照另一个实施例，签名方包括授信引擎110。在该实施例中，授信引擎110证明鉴定过程1000适当地鉴定了用户、卖主或两者。因此，鉴定引擎215请求授信引擎110的密钥，如属于密码引擎220的密钥，从而执行数字签名。按照另一个实施例，授信引擎110执行类似数字公证人的功能。在该实施例中，签名方包括用户、卖主或这两者以及授信引擎110。因此，授信引擎110提供用户和/或卖主的数字签名，然后以其自身数字签名指示用户和/或卖主已被适当鉴定。在该实施例中，鉴定引擎215可有利地请求相应于用户、卖主或这两者的密钥组件。按照另一个实施例，鉴定引擎215可有利地请求相应于授信引擎110的密钥组件。

[0180] 按照另一个实施例，授信引擎110执行类似委任书的功能。例如，授信引擎110可代表第三方对消息进行数字签名。在这样的情形中，鉴定引擎215请求与第三方关联的密钥。按照该实施例，在允许类似委托书功能之前，签名过程1100可有利地包括第三方的鉴定。此外，鉴定过程1000可包括对第三方约束(constraint)的检查，如商务逻辑等，该第三方约束指示在何时以及在何种环境中，特定第三方的签名可以使用。

[0181] 基于前面所述，在步骤1110中，鉴定引擎从数据存储设施D1到D4请求相应于签名方的密钥。在步骤1115中，数据存储设施D1到D4发送相应于签名方的密钥各部分给密钥引擎220。按照一个实施例，前述传输包括SSL技术。按照另一个实施例，前述传输可有利地用密码引擎220的公钥超级加密。

[0182] 在步骤1120，密码引擎220组装签名方的前述密钥并加密其中的消息，因而形成数字签名。在签名过程1100的步骤1125中，密码引擎220发送数字签名给鉴定引擎215。在步骤1130中，鉴定引擎215将填写好的鉴定请求，与散列消息和数字签名的副本一起发送给交易引擎205。在步骤1135中，交易引擎205发送收据(receipt)给卖主，该收据包括交易ID、鉴定是否成功的指示，和数字签名。按照一个实施例，前述传输可有利地包括授信引擎110的数字签名。例如，授信引擎110可以用其私钥加密收据散列，因而形成附加到对卖主的传输上的数字签名。

[0183] 按照一个实施例，交易引擎205也发送确认消息给用户。虽然签名过程1100是参考优选可替换实施例公开的，但本发明不限于这些实施例。本领域技术人员将从这里的公开内容中认识到，签名过程1100有大量可替换过程。例如，卖主可以由用户申请，如电子邮件申请来替代。例如，用户可能希望用他或她的数字签名来对特定的电子邮件进行数字签名。在这样的实施例中，签名过程1100的传输可有利地仅包括该消息散列的一个副本。而且，本领域技术人员可从这里的公开认识到大量客户端应用程序可请求数字签名。例如，客户端应用程序可包括字处理器、电子制表软件、电子邮件、语音电子邮件、对受限系统区域的访问，等等。

[0184] 此外，本领域技术人员将从这里的公开认识到签名过程1100的步骤1105到步骤1120可有利地采用图9B中互操作过程970的部分或所有步骤，因而提供不同密码系统间的

互操作性，这些系统，举例而言，可能需要处理不同签名类型的数字签名。

[0185] 图12示出按照本发明实施例的加密/解密过程1200的数据流。如图12所示，解密过程1200从用鉴定过程1000来鉴定用户开始。按照一个实施例，鉴定过程1000包括鉴定请求中的同步会话密钥(session key)。例如，在传统PKI技术中，本领域技术人员可以理解，用公钥和私钥加密或解密数据，数学强度高并可能要求可观的系统资源。然而，在对称密钥密码系统中，或在消息发送方和接收方共享一个用于加密和解密消息的公共密钥(common key)的系统中，数学运算明显更简单并更快。因此，在传统PKI技术中，消息发送方将生成同步会话密钥，并用更简单更快的对称密钥系统加密消息。然后，发送方将用接收方的公钥加密会话密钥。加密的会话密钥将被附加到同步加密的消息上，且这两个数据都被发送给接收方。接收方使用他或她的私钥解密会话密钥，然后用该会话密钥解密消息。基于以上所述，更简单更快的对称密钥系统被用于大多数加密/解密处理。因此，在解密过程1200中，解密有利地假定同步密钥已经以用户的公钥加密。因此，上面的说明中，加密的会话密钥包括在鉴定请求中。

[0186] 回到解密过程1200，在步骤1205中，用户得到鉴定后，鉴定引擎215将加密的会话密钥转发至密码引擎220。在步骤1210，鉴定引擎215将请求转发至每个数据存储设施D1到D4，从而请求用户的密钥数据。在步骤1215，每个数据存储设施D1到D4发送它们的各部分密钥到密码引擎220。按照一个实施例，前面的传输是以密码引擎220的公钥加密的。

[0187] 在解密过程1200的步骤1200中，密码引擎220组装密钥并解密会话密钥。在步骤1225，密码引擎转发会话密钥至鉴定引擎215。在步骤1227，鉴定引擎215填写包括解密的会话密钥的鉴定请求，并发送填写的鉴定请求至交易引擎205。在步骤1230，交易引擎205转发鉴定请求和会话密钥至请求应用程序或卖主。然后，按照一个实施例，请求应用程序或卖主使用会话密钥从而解密加密的消息。

[0188] 虽然解密的过程1200是参考优选的可替换实施例说明的，本领域技术人员可从这里的公开内容认识到解密过程1200有大量可替换过程。例如，解密过程1200可先于同步密钥加密并依靠全部公钥技术。在这样的实施例中，请求应用程序可发送整个消息给密码引擎220，或可采用某些类型的压缩或可逆散列(reversible hash)，以便发送信息给密码引擎220。本领域技术人员也将从这里的公开内容认识到，前述通信可有利地包括以SSL技术包裹(wrapped)的XML文档。

[0189] 加密/解密过程1200也提供文档或其他数据的加密。因此，在步骤1235，请求应用程序或卖主可有利地发送对用户公钥的请求到授信引擎110的交易引擎205。请求应用程序或卖主作出该请求是因为请求应用程序或卖主使用该用户公钥来加密将用于加密文件或消息的会话密钥。如登记过程900中提到的那样，交易引擎205在例如海量存储装置225中存储用户数字证书的副本。因此，在加密过程1200的步骤1240中，交易引擎205从海量存储装置225请求用户的数字证书。在步骤1245中，海量存储装置225发送相应于用户的数字证书给交易引擎205。在步骤1250中，交易引擎205发送数字证书至请求应用程序或卖主。按照一个实施例，加密过程1200的加密部分不包括用户的鉴定。这是因为发出请求的卖主只需要该用户的公钥，而非请求任何敏感数据。

[0190] 本领域技术人员可从这里的公开内容认识到如果特定用户没有数字证书，则授信引擎110可采用部分或全部登记过程900从而为该特定用户生成数字证书。然后，授信引擎

110可启动加密/解密过程1200并因此提供适当的数字证书。此外，本领域技术人员将从这里的公开内容认识到，该加密/解密过程1200的步骤1220和1235到1250可有利地采用图9B的互操作过程的部分或所有步骤，因而提供不同密码系统间的互操作性，这些系统，举例而言，可能需要处理加密。

[0191] 图13示出按照本发明另一个实施例的授信引擎系统1300简化的方框图。如图13所示，授信引擎系统1300包括多个不同的授信引擎1305，1310，1315，和1320。为了促进对本发明更完整的理解，图13示出每个授信引擎1305，1310，1315，和1320都具有交易引擎、存储仓库，和鉴定引擎。然而，本领域技术人员将认识到每个交易引擎可有利地包括部分图1－8公开的元素和通信信道，或者其组合或全部。例如，一个实施例可有利地包括具有一个或多个交易引擎、存储仓库，密码服务器，或它们的任何组合的授信引擎。

[0192] 按照本发明一个实施例，每个授信引擎1305，1310，1315和1320是地理分开的，以便授信引擎1305可驻存在第一位置，授信引擎1310可驻存在第二位置，授信引擎1315可驻存在第三位置，而授信引擎1320可驻存在第四位置。前述地理分离有利地减小系统响应时间，同时增加整个授信系统1300的安全。

[0193] 例如，当用户登录到密码系统100上时，用户可能最接近第一位置并需要被鉴定。如参考图10的说明，为了鉴定，用户提供当前鉴定数据，如生物统计特征等，且当前鉴定数据与该用户的登记鉴定数据作比较。因此，按照一个例子，用户有利地提供当前鉴定数据给地理上最近的授信引擎1305。然后授信引擎1305的交易引擎1321转发当前的鉴定数据至同样驻存在第一位置的鉴定引擎1322。按照另一个实施例，交易引擎1321转发当前鉴定数据至授信引擎1310、1315、或1320中一个或多个鉴定引擎。

[0194] 交易引擎1321也请求组装每个授信引擎，例如1305到1320的存储仓库的登记鉴定数据。按照该实施例，每个存储仓库提供部分登记数据给授信引擎1305的鉴定引擎1322。鉴定引擎1322然后采用例如前两个存储仓库的加密的数据部分从而响应并组装登记鉴定数据为可判读的形式。鉴定引擎1322比较登记鉴定数据和当前鉴定数据，并返回鉴定结果给授信引擎1305的交易引擎1321。

[0195] 基于以上所述，授信引擎系统1300采用多个地理分开的授信引擎1305到1320中最近的一个执行鉴定过程。按照本发明一个实施例，信息到最近交易引擎的路由选择可有利地由客户端java程序完成，该java程序在用户系统105、卖主系统120，或认证授权方115中的一个或多个上执行。按照可替换实施例，更复杂的决策过程可用来选择授信引擎1305到1320。例如，决策可基于给定授信引擎的可用性、可操作性、连接速度、负载、性能、地理上接近度，或它们的组合。

[0196] 以该方式，授信引擎1300降低其响应时间，同时保持与地理上的远程数据存储设施关联的安全优势，如参考图7的讨论，其中每个数据存储设施存储敏感数据随机化的部分。例如，授信引擎1315的存储仓库1325处的安全危害不必危及授信引擎1300的敏感数据。这是因为存储仓库1325仅含有不可判读的随机化的数据，缺乏其他数据时，这些不可判读的随机化的数据是完全无用的。

[0197] 按照另一个实施例，授信引擎系统1300可有利地包括多个与鉴定引擎排列类似的密码引擎。密码引擎可有利地执行密码功能，如参考图1－8公开的密码功能。按照又一个实施例，授信引擎系统1300可有利地取代具有多个密码引擎的多个鉴定引擎，因而执行密码

功能，如参考图1－8公开的密码功能。按照本发明又一个实施例，授信引擎系统1300可以用具有鉴定引擎、密码引擎或这两者的部分或所有功能的引擎，来取代多个鉴定引擎中的每一个，如前面的公开。

[0198] 虽然授信引擎1300是参考优选的可替换实施例公开的，本领域技术人员将认识到授信引擎系统1300可包括授信引擎1305到1320中的多个部分。例如，授信引擎系统1300可包括一个或多个交易引擎，一个或多个存储仓库，一个或多个鉴定引擎，或一个或多个密码引擎或它们的组合。

[0199] 图14示出按照本发明又一实施例的授信引擎系统1400的简化方框图。如图14所示，授信引擎系统1400包括多个授信引擎1405、1410、1415和1420。按照一个实施例，每个授信引擎1405、1410、1415和1420包括参考图1－8公开的授信引擎110的部分或全部组件。按照该实施例，当用户系统105、卖主系统120、或认证授权方115的客户端java程序与授信引擎系统1400通信时，这些通信被发送到每个授信引擎1405到1420的IP地址。进一步地，每个授信引擎1405、1410、1415和1420的每个交易引擎的行为与参考图13公开的授信引擎1305的交易引擎1321类似。例如，在鉴定过程中，每个授信引擎1405、1410、1415和1420的每个交易引擎传输当前的鉴定数据给他们各自的鉴定引擎，并传输请求来组装存储在每个授信引擎1405到1420的每个存储仓库中的随机化的数据。图14没有示出所有这些通信，因为示出这些通信将变得过度复杂。继续鉴定过程，每个存储仓库然后将其部分随机化的数据传输到每个授信引擎1405到1420的每个鉴定引擎。每个授信引擎的每个鉴定引擎采用其比较器来判断是否当前鉴定数据是否与由每个授信引擎1405到1420的存储仓库提供的登记鉴定数据匹配。按照该实施例，每个鉴定引擎的比较结果然后被发送到其他三个授信引擎的冗余模块。例如，授信引擎1405的鉴定引擎的结果被发送给授信引擎1410、1415和1420的冗余模块。因此，授信引擎1405的冗余模块类似地接收来自授信引擎1410，1415，和1420的鉴定引擎的结果。

[0200] 图15示出图14中冗余模块的方框图。冗余模块包括比较器，该比较器经配置用于接收三个鉴定引擎的鉴定结果并将该结果发送到第四个授信引擎的交易引擎。比较器比较三个鉴定引擎的鉴定结果，如果有两个结果相符，则比较器断定，鉴定结果应与这两个相符的鉴定引擎匹配。然后该结果被发回给相应于与三个鉴定引擎不相关的授信引擎的交易引擎。

[0201] 基于上面所述，冗余模块根据接收到的来自鉴定引擎的数据来判断鉴定结果，该鉴定引擎优选与该冗余模块的授信引擎地理上远距离隔开。通过提供这样的冗余功能，授信引擎系统1400确保授信引擎1405到1420之一的鉴定引擎的危害不足以危及特定授信引擎的冗余模块的鉴定结果。本领域技术人员可以认识到授信引擎系统1400的冗余模块功能也可应用到每个授信引擎1405到1420的密码引擎。然而，这样的密码引擎通信没有在图14中示出以便避免复杂化。而且，本领域技术人员将认识到，用于图15中比较器的大量可替换的鉴定结果冲突解决算法适用于本发明。

[0202] 按照本发明又一个实施例，授信引擎系统1400可有利地在密码比较步骤中采用冗余模块。例如，参考图14和15公开的部分或所有前述冗余模块可有利地在特定交易过程中由一方或多方提供的文档散列比较过程中执行。

[0203] 尽管前面以某些优选的可替换实施例来说明本发明，但对阅读了本公开内容的本

领域技术人员来说，其他实施例也显然是可行的。例如授信引擎110可发布短期证书，这里私钥发布给用户在预定的时间段内使用。例如，当前证书标准包括有效性字段，该字段在预定的时间量后可设定为过期。因此授信引擎110可发布私钥给用户，该私钥可以在例如24小时内是有效的。按照这样的实施例，授信引擎110可有利地发出要与特定用户关联的新密钥对，然后发布新密钥对的私钥。然后，一旦发布了私钥，则授信引擎110立即使这类私钥的内部有效使用过期，因为授信引擎110不再能获得它。

[0204] 此外，本领域技术人员将认识到密码系统100或授信引擎110可包括识别任何类型装置的能力，包括但不限于膝上型计算机、蜂窝电话、网络、生物统计特征识别装置等。按照一个实施例，这类识别可源自对特定服务的请求，如对鉴定导致的访问或使用的请求、对密码功能的请求等提供的数据。按照一个实施例，前述请求可包括唯一装置识别符，如处理器ID。可替换地，请求可包括特定可识别数据格式的数据。例如，移动和卫星电话通常没有全X509.v3重加密证书(full X509.v3heavy encryption certificate)的处理能力，且因此不会请求全X509.v3重加密证书。按照该实施例，授信引擎110可识别所呈现的数据格式的类型，并按数据格式类型做出响应。

[0205] 在上述系统的额外方面中，内容敏感鉴定可用下面说明的多种技术提供。如图16所示的内容敏感鉴定提供了评估实际数据和该数据生成、交付环境的可能性，该实际数据是用户在试图鉴定自身时发送的。这类技术也可支持用户与授信引擎110间或卖主与授信引擎110间的交易特定授信仲裁，如下面所述。

[0206] 如上所述，鉴定是证明用户正是其自称的人的过程。通常，鉴定要求向认证授权方证明某些事实。本发明的授信引擎110代表用户必须向其证明自身的授权方。用户必须通过以下方式之一向授信引擎110证明他就是其自称的人：知道某些仅用户知道的事情(基于知识的鉴定)，具有某些仅用户拥有的物品(基于令牌的鉴定)，或通过作为某些仅用户才具有的特征(基于生物统计特征的鉴定)。

[0207] 基于知识鉴定的例子包括但不限于口令、PIN号，或锁组合(lock combination)。基于令牌鉴定的例子包括但不限于房屋钥匙、物理信用卡、驾驶执照，或特定电话号码。基于生物统计特征鉴定的例子包括但不限于指纹、笔迹分析、面部扫描、手扫描、耳朵扫描、虹膜扫描、血管图案、DNA、语音分析，或视网膜扫描。

[0208] 每种类型的鉴定都具有特定的优点和缺点，且每种都提供不同级别的安全性。例如，创建与其他人指纹匹配的假指纹通常要比偷听某人口令并重复该口令要困难。每种类型的鉴定也要求鉴定授权方知道不同类型的数据，以便用该鉴定形式验证某些人。

[0209] 这里所用的“鉴定”将泛指验证某人身份就是其自称的人的整个过程。“鉴定技术”指基于特定知识、物理标记，或生物统计特征读取的特定鉴定类型。“鉴定数据”指被发送给或被证明给认证授权方，以建立身份的信息。“登记数据”指初始被提交给鉴定授权方，以建立与鉴定数据比较基线的数据。“鉴定事件”指与试图用鉴定技术鉴定相关联的数据。

[0210] 鉴定用户过程中涉及的内部协议和通信是参考上面图10说明的。该过程中发生内容敏感鉴定的部分出现在图10的步骤1045所示的比较步骤中。该步骤在鉴定引擎215中发生，并涉及到组装从存储仓库210中检索的登记数据410和将其与用户提供的鉴定数据比较。该过程的一个特定实施例在图16中示出并在下面说明。

[0211] 由用户提供的当前鉴定数据和从存储仓库210中检索的登记数据是由鉴定引擎

215在图16中步骤1600接收的。这些数据集合均可含涉及鉴定分离技术的数据。鉴定引擎215在步骤1605中分离与每个单独的鉴定事件相关联的鉴定数据。这是必须的，从而鉴定数据与用户登记数据的适当子集比较(如，指纹鉴定数据应与指纹登记数据，而非口令登记数据作比较)。

[0212] 通常，根据哪些鉴定技术对于用户可用，鉴定用户涉及一个或多个单独的鉴定事件。这些方法受用户在其登记过程中提供的登记数据的限制(如果用户在登记时没有提供视网膜扫描，则不能用视网膜扫描鉴定自己)，也受用户当前可用的方法限制(如，如果用户在当前位置没有指纹读取器，则不能执行指纹鉴定)。在某些情形中，单个鉴定事件足以鉴定用户；然而，在某些环境下，可使用多种鉴定事件的组合以便为特定交易更可靠地鉴定用户。

[0213] 每个鉴定事件由涉及到特定鉴定技术(如指纹，口令，智能卡等)的数据和该特定技术的数据捕获和交付环境组成。例如，试图经口令鉴定的特定事件不仅将生成涉及口令自身的数据，还将生成涉及口令尝试的环境数据，所谓的“元数据”。环境数据包括这样的信息，如特定鉴定事件发生的时间，发出已交付鉴定信息的网络地址，以及本领域技术人员已知的其鉴定数据的起源(连接的类型，处理器序列号等)可判断的任何其他信息。

[0214] 在许多情形中，仅少量的环境元数据可用。例如，如果用户位于使用代理、网络地址转换或其他掩蔽源端计算机地址技术的网络上，则仅代理或路由器的地址可判断。类似地，由于所用的硬件或操作系统的限制，或这类特征被系统操作员禁用，或用户系统与授信引擎110间连接的其他限制，在许多情形中得不到诸如处理器序列号的信息。

[0215] 如图16所示，一旦在鉴定数据内表达的各鉴定事件在步骤1605中被提取并分离，则鉴定引擎215评估每个指示用户就是其自称的人的事件的可靠度。单个鉴定事件的可靠度通常是基于几个因子判断的。这些因子可被分组，一组为涉及到与鉴定技术相关的可靠度的因子，在步骤1610中被评估；还有一组为涉及到所述提供的特定鉴定数据的可靠度的因子，在步骤1815中被评估。第一组包括但不限于所用鉴定技术的固有可靠度，和该方法所用登记数据的可靠度。第二组包括但不限于登记数据和鉴定事件提供的数据之间的匹配度，和与鉴定事件关联的元数据。这些因子的每一个均可独立于其他因子而变化。

[0216] 鉴定技术的固有可靠度基于冒名者提供其他人正确数据的困难程度，以及鉴定技术的总错误率。对于基于口令和知识的鉴定方法，该可靠度通常相当低，因为没有措施防止某些人向别人透露其口令以及别人使用该口令。即使是更复杂的基于知识的系统，也可能仅具有中等可靠度，因为知识可相当容易地从一个人转移到另一个人。基于令牌的鉴定，如具有适当的智能卡或使用特定终端执行鉴定，也类似地具有低可靠度，因为不能保证拥有适当令牌的是正确的人。

[0217] 然而，生物统计特征技术具有更高的固有可靠度，因为使其他人能够便利地使用你的指纹，即使是有意，通常也很困难。因为扰乱生物统计特征的技术更困难，生物统计特征方法的固有可靠度通常高于纯粹基于知识或令牌的鉴定技术。然而，即使生物统计特征技术也可在某些情形下发生误接受或误拒绝。这些事件的发生可由同一生物统计特征技术的不同实施的不同可靠度反映。例如，由一个公司提供的指纹匹配系统可比由别的公司提供的系统具有更高可靠度，因为该公司提供的系统使用较高质量的光学器件或更好的扫描分辨率或某些其他改进，减少了误接受或误拒绝的发生。

[0218] 注意，该可靠度可用不同方式表达。该可靠度希望以某种度量表达，该度量可由鉴定引擎215的试探过程530和算法使用从而计算每次鉴定的信任级别。表达这些可靠度的一种优选模式是百分数或分数。例如，可能分配97％的固有可靠度给指纹，而仅分配50％的固有可靠度给口令。本领域技术人员可认识到这些特定值仅是示例性的并可随特定的实施改变。

[0219] 评价可靠度必需的第二个因子是登记可靠度。这是上面提到的“分级登记”的一部分。该可靠度因子反映出在初始登记过程中提供的身份的可靠度。例如，如果个人初始以这样的方式登记，即个人产生实体的身份证明并提供给公证人或其他公共官方机构，且登记数据是在该时间记录并公证，则该数据将比在登记时经网络提供，或者仅通过数字签名或不是真正与个人联系的其他信息担保的数据更加可靠。

[0220] 其他可靠度级别可变的登记技术包括但不限于：在授信引擎110操作员的实体办公室登记；在用户雇用地点登记；在邮局或护照办公室登记；通过授信引擎110操作员的委任方或授信方登记；匿名或假名登记，其中登记的身份还没有与特定的真实个体确认；以及本领域已知的其他方式。

[0221] 这些因子反映授信引擎110与登记过程中提供的身份源之间的信任。例如，如果登记是在提供身份证明的初始过程中与雇主联合执行的，则可认为该信息在公司内是极其可靠的，但政府机构或竞争者可认为该信息不那么可靠。因此，由每个其他组织操作的授信引擎可给该登记指定不同的可靠度级别。

[0222] 类似地，经网络提交、但是经过在之前登记过程中由同一授信引擎110提供的其它授信数据鉴定的额外数据，可认为与原始登记数据一样可靠，即使后面的数据是经公开网络提交的。在这样的情形中，随后的公证将有效地增加与原始登记数据相关的可靠度级别。例如，以该方式，匿名或假名登记可通过向某些登记官方机构展示与登记数据匹配的个人身份而提升为完整登记。

[0223] 上面讨论的可靠度因子通常是可在特定鉴定事件之前判断的值。这是因为他们基于登记和技术而非实际鉴定。在一个实施例中，基于这些因子生成可靠度的步骤涉及查找之前为该特定鉴定技术判断的值和该用户的登记数据。在本发明进一步有利的实施例中，这类可靠度可与登记数据自身一起被包括在内。以该方式，这些因子与从存储仓库210发出的登记数据一起自动交付给鉴定引擎215。

[0224] 虽然这些因子通常可在任何个人鉴定事件之前判断，但它们还是对为鉴定该用户使用了特定技术的每次鉴定事件有影响。而且，虽然其值可随时间变化(如用户以更可靠的方式重新登记)，但它们不依赖于鉴定数据自身。与之对照，与单个特定事件的数据关联的可靠度因子可随每个情形改变。如下面的讨论，这些因子必须为每次新鉴定评估，以便在步骤1815中生成可靠度分值(score)。

[0225] 鉴定数据的可靠度反映出由用户在特定鉴定事件中提供的数据和在鉴定登记过程中提供的数据之间的匹配。对于用户声称自己就是该个体的个人，这是鉴定数据是否与登记数据匹配的根本问题。通常，当数据不匹配时，则认为该用户没有被成功鉴定，鉴定失败。该结果的评估方式可随所用的鉴定技术改变。这类数据的比较是通过如图5所示的鉴定引擎215的比较器515的功能执行的。

[0226] 例如，口令的匹配通常是以二元方式评估的。换句话说，口令要么完美匹配，要么

匹配失败。如果口令并非绝对正确，即使是接近于正确口令的部分匹配的口令，通常也不予接受。因此，当评估口令鉴定时，比较器515返回的鉴定的可靠度通常是100％(正确)或0％(错误)，没有中间值。

[0227] 与口令相似的规则也通常应用到基于令牌的鉴定方法，如智能卡。这是因为拥有具备类似识别符或类似正确的识别符的智能卡与拥有具有其他不正确令牌一样是错误的。因此，令牌也倾向于是二元鉴定者(authenticator)：用户要么具有正确的令牌，要么没有正确令牌。

[0228] 然而，某些类型的鉴定数据，如问卷和生物统计特征通常不是二元鉴定者。例如，指纹可与参考指纹具有不同程度的匹配。某种程度上，这可能是由于在初始登记或随后的鉴定中，捕获的数据质量的偏差。(指纹可能被弄脏，或某人有尚未愈合的伤疤，或特定手指被烧伤。)在其他情形中，数据可能不能完美匹配，因为信息自身在一定程度上可变并且是基于图案匹配的。(语音分析看起来接近完美匹配，但由于背景噪声或语音记录的环境声音，或者这个人患感冒，因此并非很正确。)最后，在大量数据被比较的情况下，可以简化为这样的情形：多数数据匹配良好，但某些不匹配。(10个问题的问卷可能得到8个个人问题的正确答案，但还有2个不正确。)对于这些原因中的任意一个，需要用比较器515给登记数据和特定鉴定事件的数据之间的匹配指定一个部分匹配值。例如，以该方式，指纹可以说成是85％匹配，语音图案可以说成是65％匹配，而问卷是80％匹配。

[0229] 由比较器515产生的该度量(匹配度)是表示鉴定是否正确的基本问题的因子。然而，如上所述，这仅是可用来判断给定鉴定事件可靠度的因子之一。同样要注意，即使可判断部分程度的匹配，最终，可能需要提供基于部分匹配的二元结果。在可替换操作模式中，也可能把部分匹配当作二元匹配，即根据匹配程度是否超过特定的匹配度阈值，决定匹配为完美(100％)或失败(0％)匹配。这样的过程可用来为系统提供简单的通过/失败的匹配值，否则系统会产生部分匹配。

[0230] 评估给定鉴定事件可靠度中要考虑的另一个因子考虑到提供该特定事件的鉴定数据的环境。如上所述，环境指与特定鉴定事件关联的元数据。这可包括但不限于如下信息：鉴定者的网络地址，可判断的程度；鉴定时间；鉴定数据的传输模式(电话线，蜂窝电话，网络等)；和鉴定者的系统的序列号。

[0231] 这些因子可用来产生通常由用户请求的鉴定类型的概况(profile)。然后，通过至少两种方式，该信息可被用于评估可靠度。一种方式是考虑用户是否以与该用户鉴定的正常概况一致的方式请求鉴定。如果用户通常在工作日(用户在工作时)中从一个网络地址发出鉴定请求，而在晚间或周末(用户在家里时)从另一个网络地址发出鉴定请求，那么在工作日来自家中网络地址的鉴定可靠度较低，因为该情形在正常鉴定概况之外。类似地，如果用户通常使用指纹生物统计特征并在晚间鉴定，则在白天仅使用口令的鉴定可靠度较低。

[0232] 环境元数据可用来评估鉴定事件可靠度的另外一种方式是判断在鉴定者就是其声称的个体时，环境提供多大的确证。例如，如果鉴定来自已知系列号与用户关联的系统，这是好的环境指示符，即用户就是其所自称的人。相反，如果鉴定来自已知位于Los Angeles的网络地址，而已知该用户位于London，这表明基于该环境，该鉴定可靠度较低。

[0233] 当用户系统与卖主系统或授信引擎110互动时，cookie或其他电子数据也可置于用户所用的系统上。该数据被写入到用户系统存储装置上，并可含用户系统上Web浏览器或

其他软件可读取的身份。如果该数据被允许在两次会话之间驻存在用户系统上(“持久cookie”),则该数据可随鉴定数据发送,作为该系统在特定用户鉴定中使用过的进一步证据。给定事件的元数据,特别是持久cookie,可有效地形成一类基于令牌的鉴定者。

[0234] 一旦基于鉴定事件技术和数据的适当可靠度因子分别如上述步骤1610和1615的描述而生成,则这些因子被用于产生步骤1620提供的鉴定事件的总体可靠度。一种实现方法是简单地将每个可靠度表达为百分数然后将他们相乘。

[0235] 例如,假定鉴定数据是从与用户过去鉴定概况(100%)一致的已知的用户家中计算机网络地址发送的,且所用技术是指纹识别(97%),且初始指纹数据是通过用户雇主以授信引擎110获得的(90%),且鉴定数据和登记数据中原始指纹模板间的匹配非常好(99%)。然后这一鉴定事件总的可靠度可由这些可靠度的乘积来计算:可靠度为100%*97%*90%*99%=86.4%。

[0236] 该计算的可靠度表示单个鉴定事件的可靠度。单个鉴定事件的总可靠度也可用如下的技术计算,即对不同的可靠度因子做不同处理,例如利用公式,给每个可靠度因子指定不同的权重。而且,本领域技术人员将认识到所使用的实际值可表示为百分数之外的值,并可使用非算术系统。一个实施例可包括鉴定请求者用来为每个因子设定权重的模块和用来建立鉴定事件总可靠度的算法。

[0237] 鉴定引擎215可使用上述技术及其变化来判断单个鉴定事件的可靠度,如步骤1620所示。然而,在许多鉴定情形中,同时提供多个鉴定事件是有用的。例如,在试图用本发明系统鉴定自身时,用户可提供用户身份、指纹鉴定数据、智能卡,和口令。在这样的情形中,三个独立鉴定事件被提供给授信引擎110供评估。进入步骤1625,如果鉴定引擎215判断用户提供的数据包括一个以上的鉴定事件,则每个事件将依次如步骤1630所示那样被选择,并如上述步骤1610、1615和1620那样被评估。

[0238] 注意所讨论的许多可靠度因子可随事件改变。例如,这些技术的固有可靠度可能是不同的,鉴定数据与登记数据间的匹配度也是不同的。而且,用户可能在不同时间和不同环境为每个这类技术提供了登记数据,并为每个这类事件提供不同的登记可靠度。最后,即使每个这类事件的数据被提交的环境相同,使用这类技术可都不同地适合用户概况,且因此可以指定以不同的环境可靠度。(例如,用户可正常使用他们的口令和指纹,而非他们的智能卡。)

[0239] 结果,每个这类鉴定事件的最终可靠度可能彼此不同。然而,通过将多个事件一起使用,鉴定的总信任度趋向于增加。

[0240] 一旦鉴定引擎为鉴定数据中提供的所有鉴定事件执行了步骤1610到1620,每个事件的可靠度用在步骤1635中从而评估总鉴定信任度。该组合单个鉴定事件可靠度为鉴定信任度的过程可通过涉及产生各个可靠度的不同方法模拟,并可解决这些鉴定技术中某些之间的特定互动。(例如,多个基于知识的系统,如口令系统,可产生比单个口令,甚至相当弱的生物统计特征,如基本语音分析还要低的信任度。)

[0241] 鉴定引擎215可组合多个同时鉴定事件的可靠度从而生成最终信任度的一个方法是将每个事件的不可靠度相乘从而得到总不可靠度。不可靠度通常是可靠度的互补百分数。例如,具有84%的可靠度的技术,具有16%的不可靠度。上述三个产生86%,75%和72%可靠度的鉴定事件(指纹、智能卡、口令)分别具有相应的(100-86)%,(100-75)%,和(100-

72)%的不可靠度。通过将这些不可靠度相乘，我们得到14%*25%*28%＝0.98%的累积不可靠度，这相应于99.02%的可靠度。

[0242] 在额外的操作模式中，额外的因子和试探过程530可应用在鉴定引擎215中从而解决不同鉴定技术间的相互依赖。例如，如果某些人未授权访问特定家庭计算机，他们也可能在该地址接入电话线。因此，基于发端电话号码和鉴定系统序列号的鉴定不会向鉴定总信任度添加太多。然而，基于知识的鉴定基本独立于基于令牌的鉴定(即，如果某人窃取你的蜂窝电话或密钥，但如果他们没有你的PIN号或口令，则不太可能知道)。

[0243] 而且，不同卖主或其他鉴定请求者可能希望不同程度地加权鉴定的不同方面。这可包括在计算各个事件可靠性时使用独立加权因子或算法，以及使用不同方法来评估具有多个事件的鉴定事件。

[0244] 例如，某些类型交易的卖主，例如公司电子邮件系统，可能希望主要基于试探过程和其他缺省的环境数据来鉴定。因此，他们可对涉及元数据和其他概况相关的信息的因子应用高权重，该信息与鉴定事件的周围环境相关。这样的安排对用户的要求不比当用户在工作时间登录到正确的机器时更多，从而可用来在正常操作时间里减轻用户负担。然而，另一个卖主可能对来自特定技术的鉴定加权最重，例如指纹匹配，这是根据这样的决策，即这样的技术最适于特定卖主目的的鉴定。

[0245] 在一个操作模式中，这样的权重改变可由鉴定请求者在生成鉴定请求中定义，并随鉴定请求发送给授信引擎110。在另一个操作模式中，这类选项也可在初始登记过程中为鉴定请求者设定为优选项并存储在鉴定引擎中。

[0246] 一旦鉴定引擎215为所提供的鉴定数据产生鉴定信任度，该信任度用于完成步骤1640中的鉴定请求，且该信息从鉴定引擎215转发到交易引擎205以便包括在给鉴定请求者的消息中。

[0247] 上述过程仅是示例性的，且本领域技术人员将认识到这些步骤不必以所示顺序执行，或仅某些步骤需要执行，或需要多种步骤组合。而且，如果环境允许，某些步骤，如每个提供的鉴定事件的可靠度的评估，可彼此平行执行。

[0248] 在本发明进一步的方面中，当上述过程产生的鉴定信任度不能满足卖主或要求鉴定的其他方所要求的信任度时，提供了一种方法来适应条件。在诸如在所提供的信任度和所需信任度之间存在差距的环境中，授信引擎110的操作员要为一方或双方提供机会从而提供备用的数据或要求以缩小该信任差距。该过程在这里将被称为“授信仲裁”。

[0249] 授信仲裁可发生在上面参考图10和11所述的密码鉴定框架内。如图所示，卖主或其他方将请求鉴定与特定交易关联的特定用户。在一个环境中，卖主仅请求鉴定，要么是正结果要么是负结果，并且在接收来自用户的适当数据后，授信引擎110将提供这样的二元鉴定。在诸如这样的环境中，为了保证正鉴定所要求的信任度是基于信任引擎110内优选项设定来判断的。

[0250] 然而，卖主请求特定信任度以便完成特定交易也是可能的。所要求的信任度可包括在鉴定请求(如鉴定该用户信任度为98%)中，或可基于其他与交易关联的因子，由授信引擎110判断(即鉴定该用户对于该交易是适当的)。一个这类因子可以是交易的经济价值。对于具有较大经济值的交易，可能要求较高的信任度。类似地，对于高度风险的交易，要求高的信任度。相反，对于低风险或低价值交易，卖主或其他鉴定请求者则要求较低的信任

度。

[0251] 授信仲裁的过程出现在图10中授信引擎110在步骤1050接收鉴定数据的步骤和在图10的步骤1055中鉴定结果返回给卖主的步骤之间。这些步骤之间，导致授信水平的评估和潜在授信仲裁的过程如图17所示那样发生。在执行简单二元鉴定的环境中，图17所示的过程简化为使交易引擎205直接比较所提供的鉴定数据和上面参考图10讨论的被识别用户的登记数据，并将任何差别标记为负鉴定。

[0252] 如图17所示，在步骤1050中接收数据后第一步是为交易引擎205判断信任度，该信任度是步骤1710中特定交易的正鉴定必需的。该步骤可通过几种不同方法中的一种执行。所要求的信任度可以是在作出鉴定请求时鉴定请求者为授信引擎110指定的。鉴定请求者也可事先设定优选项，该优选项存储在存储仓库210中或交易引擎205可访问的其他存储装置中。然后该鉴定请求者每次请求鉴定时，该优选项可读取和使用。该优选项也可与特定用户关联作为安全措施，使得总是要求特定授信度以便鉴定该用户，该用户优选项存储在存储仓库210或交易引擎205可访问的其他存储介质中。基于鉴定请求提供的信息，如要鉴定的交易值和风险水平，所要求的级别也可通过交易引擎205或鉴定引擎215获得。

[0253] 在一种操作模式中，在生成鉴权请求时所使用的策略管理模块或其他软件被用来指定对于交易的鉴权所要求的信任度。这可被用于提供在基于策略管理模块内所指定的策略分配所要求的信任度时要遵守的一系列规则。一个有利的操作模式是这样的模式与卖主的网络服务器结合，以便适当地确定对于由卖主网络服务器所发起的交易所要求的信任度。以该方式，按照卖主的策略，来自用户的交易请求可被分配以所要求的信任度，且这样的信息可与鉴权请求一起被转发到授信引擎110。

[0254] 这个所要求的信任度与卖主想要的关于鉴权的个人实际上就是其将他自己标识为那个个人的确定度相关。例如，如果因为商品在不断改变掌管权，所以交易是卖主想要相当确定度的交易，则卖主可要求85％的信任度。对于卖主仅鉴权用户以允许其察看仅会员可看的内容或在聊天室行使特权的情形，则不利的风险可能足够小，以至于卖主仅要求60％的信任度。然而，为了进入价值几万美元的生产合同，卖主可能要求90％或更高的信任度

[0255] 这个被要求的信任度表示用户必须鉴权其自身以完成交易的度量。如果所需的信任度例如是85％，则用户必须提供足以使授信引擎110以85％的置信度说该用户是其所自称的人的鉴权给授信引擎110。该所要求的信任度和鉴权信任度之间的平衡产生正面鉴定(卖主满意)或授信仲裁的可能性。

[0256] 如图17所示，在交易引擎205接收到所要求的可信度后，在步骤1720中，交易引擎205比较所要求的可信度和鉴权引擎215为当前鉴权所计算的鉴权信任度(如参考图16的讨论)。如果在步骤1730中，鉴权信任度高于交易所要求的可信度，则过程进入到步骤1740，其中交易引擎205为该交易产生正面鉴定。然后，关于该效果的信息将被插入到鉴权结果中，并通过交易引擎205返回给卖主，如步骤1055所示(参看图10)。

[0257] 然而，如果在步骤1730中，鉴权信任度不满足所要求的可信度，则对于当前鉴权存在信任差距，且在步骤1750中描述授信仲裁(trust arbitrage)。授信仲裁更完全地参考下面图18被说明。如下所述的过程发生在授信引擎110的交易引擎205内。由于不需要鉴权或其他密码操作来执行授信仲裁(非交易引擎205和其他元件间的SSL通信所要求的那些授信

仲裁)，该过程可在鉴权引擎215外部被执行。然而，如下面的讨论，鉴权数据或其他密码或鉴权事件的任何再评估将要求交易引擎205重新提交适当的数据给鉴权引擎215。本领域技术人员将认识到，授信仲裁过程可以替换地被结构化为部分或全部地发生在鉴权引擎215内。

[0258] 如上所述，授信仲裁是授信引擎110调停卖主和用户间谈判以试图在适当的情况下确保正面鉴定的过程。如步骤1805所示，交易引擎205首先判断当前情形对于授信仲裁是否适当。这可基于鉴权环境被判断，例如该鉴权是否已经通过多个仲裁循环，以及基于卖主或用户的优先选择，这将在下面进一步讨论。

[0259] 在仲裁不可能的情形中，过程进入到步骤1810，其中交易引擎205生成负面鉴定，然后将其插入到鉴权结果中，该鉴权结果在步骤1055中被发送给卖主(参看图10)。可能有利地被用于防止鉴权不确定地悬而未决的一个限制是设定从初始鉴权请求开始的超时时间段。以该方式，在时间限内没有被正面鉴定的任何交易被拒绝进一步的仲裁并被负面地鉴权。本领域技术人员将认识到，这样的时间限可根据交易的环境和用户及卖主的期望而改变。也可对在提供成功鉴权时可以进行的尝试的次数做出限制。这样的限制可通过尝试限制器535来处理，如图5所示

[0260] 如果在步骤1805中没有禁止仲裁，则交易引擎205将与交易一方或双方谈判。交易引擎205可发送信息给用户，请求某种形式的额外鉴权，以便提升如步骤1820所示地生成的鉴权信任度。在最简单的形式中，这可仅仅指示鉴定不充分。也可发送请求产生一个或多个附加鉴权利实例以提高鉴权的总信任度的请求。

[0261] 如果用户在步骤1825中提供某些附加鉴权利实例，则交易引擎205将这些鉴权利实例添加到交易的鉴权数据，并在步骤1015中将其转发到鉴权引擎215(参看图10)，且基于该交易的预先存在的鉴权利实例和新提供的鉴权实例重新评估鉴权。

[0262] 附加类型的鉴权可以授信引擎110请求在授信引擎110操作员(或授信机构)与用户之间建立某种形式的人对人联系，例如通过电话的请求。该电话呼叫或其他非计算机鉴权可被用来提供与个体的人员联系，并且还基于鉴权进行某种形式的问卷。这也可以提供在用户呼入时验证发端电话号码并潜在地验证用户的语音分析的机会。即使没有额外的鉴权数据可被提供，与用户的电话号码相关联的额外内容可提高鉴权上下文(context)的可靠性。考虑到鉴权请求，任何基于该电话呼叫的修订的数据或环境被馈入授信引擎110中供使用。

[0263] 此外，在步骤1820中，授信引擎110可为用户提供购买保险的机会，从而有效地购买更可信的鉴权。授信引擎110的操作员有时可能仅希望在鉴权的信任度在某个阈值以上的情况下才开始使这样的选项可用。实际上，这个用户侧保险是授信引擎110在鉴权符合授信引擎110对鉴权所正常要求的可信度、但不满足该交易的卖主所要求的信任度时为用户担保的一种方式。以该方式，用户虽然可以卖主可能要求的非常高的程度成功地鉴权，即使用户仅具有产生对于授信引擎110足够的信任度的鉴权利实例。

[0264] 授信引擎110的该功能允许授信引擎110为被鉴权为满足授信引擎110而不满足卖主的人担保。这类似于公证人在将其签名添加到文档中以便向以后读取该文档的某人指示签名出现在文档上的人实际上就是签名的人的功能。公证人的签名证明用户签名的动作。以同样的方式，授信引擎提供关于交易的人员就是他们自称的人的指示。

[0265] 然而，因为授信引擎110人工地提升用户所提供的信任度，所以对于授信引擎110操作员存在更大的风险，因为用户实际不符合卖主所要求的可信度。保险的成本被设计以补偿假的正面鉴定对授信引擎110的风险(授信引擎110可以有效地公证用户的鉴权)。用户向授信引擎110操作员支付费用以提升鉴权风险至比实际提供的信任度更高的信任度。

[0266] 因为这样的保险系统允许某人从授信引擎110有效地购买更高信任评级，所以卖主和用户可能希望在某些交易中防止使用用户侧保险。卖主可能希望将正面鉴定限定到以下情形中，即其中卖主知道实际鉴权数据支持他们所要求的信任度，且因此可指示授信引擎110用户侧保险是不允许的。类似地，为了保护他的在线身份，用户可能希望防止为自己使用用户侧保险，或者可能希望将其使用限制到以下情形，即其中无保险的鉴权信任度高于一定限度。这可被用作安全措施，以防止某人偷听口令或窃取智能卡并使用其以在低信任度上不实地鉴权，并然后购买保险以产生非常高的(假)信任度。在判断是否允许用户侧保险时，这些因素可被评估。

[0267] 如果在步骤1840中用户购买保险，则在步骤1845，鉴权信任度可基于所购买的保险被调整，且在步骤1730中，再次比较鉴权信任度和所要求的可信度(参看图17)。该过程从此处开始，并可在步骤1740中导致正面鉴定(参看图17)，或在步骤1750中返回到授信仲裁过程，以进一步的仲裁(如果允许)或如果禁止进一步仲裁，则在步骤1810中导致负面鉴定。

[0268] 除了在步骤1820中发送消息给用户，交易引擎205也可在步骤1830中发送消息给卖主，其表示未决鉴权当前低于所要求的可信度。消息也可提供关于如何前进到卖主的各种选项。这些选项中的一个选项是仅仅通知卖主当前鉴权信任水平是什么，并询问卖主是否希望保持他们当前未满足的所需可信度。这可能是有益的，因为在某些情形中，卖主可能有独立的方式用于鉴权交易，或可能已经使用缺省的要求设置，这些要求通常导致初始指定比对于即将发生的特定交易实际所需要的更高的所要求的信任度。

[0269] 例如，标准做法是卖主的所有进入的购买订单交易被预期为满足98%的可信度。然而，如果订单是卖主与长期客户近期通过电话讨论的，并且此后立即鉴权交易，但信任度仅为93%，则卖主可能希望仅仅为该交易降低接受阈值，因为电话呼叫有效地为卖主提供了额外的鉴权。在某些环境中，卖主可能愿意降低他们所要求的可信度，但不是自始至终都是当前鉴权信任度。例如，上面例子中的卖主可能考虑订单之前的电话呼叫可能值所需可信度的4%的减小；然而，这仍然比用户所产生的93%的信任度高。

[0270] 如果卖主在步骤1835中确实调整他们所要求的可信度，则在步骤1730中，比较鉴权所产生的鉴权信任度和所要求的可信度(参看图17)。如果信任度现在超过所要求的信任度，则可在步骤1740中在交易引擎205中生成正面鉴定(参看图17)。如果不是，则在允许的情况下如上面讨论的那样尝试进一步仲裁。

[0271] 除了请求调整所要求的可任度之外，交易引擎205也可提供卖主侧保险给请求鉴权的卖主。该保险用于与上述用户侧保险相似的目的。然而，这里不是成本对应于授信引擎110在鉴权高于所产生的实际鉴权信任度中所遭受的风险，而是保险成本对应于卖主在鉴权中接收较低可任度中所遭受的风险。

[0272] 不是仅降低其实际要求的可信度，卖主可选择购买保险以保护自身免受与用户鉴权中较低信任度相关的额外风险。如上所述，对于卖主，可能有利的是仅考虑购买这样的保险以覆盖在现有鉴权已经在一定阈值以上的情形中的信任缺口。

[0273] 这样的卖主侧保险的可用性允许卖主选择:对其无额外成本地直接降低其信任要求,但承担误鉴权自身的风险(基于所要求的较低可信度);或为鉴权信任度与其要求间的信任缺口购买保险,其中信任引擎110操作员承担已经被提供的较低信任度的风险。通过购买该保险,卖主有效地保持其高可信度要求;因为误鉴权的风险转移到授信引擎110操作员

[0274] 如果在步骤1840中,卖主购买保险,则鉴权信任度和所要求的可信度在步骤1730中被比较(参看图17),并且如上所述过程继续。

[0275] 注意,用户和卖主二者也可能对来自授信引擎110的消息做出响应。本领域技术人员将认识到有多种方式可以用来处理这类情形。处理多个响应可能性的一种有利模式是以先到先处理的方式处理响应。例如,如果卖主以降低后的所要求的可信度响应,且然后用户立即购买保险以提升其鉴权水平,则首先基于来自卖主的降低的信任要求再次评估鉴权。如果鉴权现在是正面鉴定,则忽略用户的保险采购。在另一种有利的操作模式中,可能仅向用户收取对于满足卖主的新的降低的信任要求所要求的保险水平收费(如果即使以降低的卖主信任要求,仍然存在信任缺口)。

[0276] 如果在步骤1850的授信仲裁过程中,没有为鉴权所设置的时间限内接收到来自任一方的响应,则在步骤1805中重新评估仲裁。这有效地再次起动仲裁过程。如果在步骤1805中时间限是最终的,或其他环境阻止进一步仲裁,则交易引擎110在步骤1810中生成负面鉴定,并在步骤1055中将其返回到卖主(参看图10)。如果不是,则新消息可被发送给用户和卖主,且过程可按需要被重复。

[0277] 注意,对于某些类型的交易,例如对不是交易部分的文档进行数字签名,可以不需要卖主或其他第三方;因此,交易主要在用户和授信引擎110之间。在该类环境中,授信引擎110将具有自身所要求的可信度,该可信度必须被满足以生成正面鉴定。然而,在这样的环境中,授信引擎110经常不期望为用户提供保险以为其提升其自己的签名的信任度。

[0278] 上面所述并在图16—18中示出的过程可利用上面参考授信引擎110所说明的各种通信模式而被执行。例如,消息可以是基于网络的,并利用授信引擎110和实时下载的小程序之间的SSL连接而被发送给用户或卖主系统上运行的浏览器。在可替换的操作模式中,某些专用应用程序可由用户和卖主使用,这些专用应用程序可促进这样的仲裁和保险交易。在另一种可替换的操作模式中,安全电子邮件操作可被用来调停上述仲裁,因而允许推迟鉴权的评估和批处理。本领域技术人员将认识到不同通信模式可使用,透明对于卖主的环境和鉴定要求是适当的。

[0279] 下面参考图19的说明描述一个示例交易,该示例交易集成了本发明的上述各个方面。该例子示出了由授信引擎(trust engine)110调停(mediate)的用户和卖主之间的整个过程。虽然上面详细说明的各个步骤和部件可被用来执行下面的交易,但是所示过程集中在授信引擎110、用户和卖主间的交互。

[0280] 在步骤1900中,当用户在在线浏览网页的同时填写卖主网站上的订单表格时,交易开始。用户希望提交以其数字签名签名的该订单表格给卖主。为了实现这一点,在步骤1905中,用户提交带有其对签名的请求的订单表格给授信引擎110。用户也将提供鉴权数据,该鉴权数据将如上所述被用来鉴定其身份。

[0281] 在步骤1910,如上所述,授信引擎110比较鉴权数据与登记数据,且如果产生正面鉴定结果,则用用户私钥签名的订单表格的散列被与订单表格自身一起转发给卖主。

[0282] 卖主在步骤1915中接收到签名后的表格，然后卖主将在步骤1920中生成与要执行的购买相关的发票或其他合同。在步骤1925中，该合同被送回给用户并请求签名。在步骤1930中，卖主还将对该合同交易的鉴权请求发送给授信引擎110，其中包括将由双方签名的合同的散列。为了允许合同由双方数字签名，卖主也包括其自身的鉴权数据，从而如果需要，卖主在合同上的签名可随后被验证。

[0283] 如上所述，授信引擎110然后验证卖主所提供的鉴权数据，以确认卖主的身份，且如果在步骤1935中，数据产生正面鉴定结果，则当从用户接收到数据时继续步骤1955。如果卖主的鉴权数据没有在期望的程度上与卖主的登记数据匹配，则消息被返回到请求进一步鉴权的卖主。如上所述，如果需要，这里可以执行授信仲裁(turst arbitrage)，以便卖主向授信引擎110成功地鉴权其自身。

[0284] 当用户在步骤1940中接收到合同时，用户检查合同，在步骤1945中如果合同是可接受的则生成鉴权数据以对其签名，且然后在步骤1950中发送合同的散列及用户的鉴权数据给授信引擎110。授信引擎110在步骤1955中验证鉴权数据，且如果鉴权结果好，则如上所述继续处理合同。如上面参考图17和18所讨论的那样，授信仲裁可被适当地执行，以缩小鉴权信任度(confidence level)和交易所要求的鉴权水平之间的信任差距。

[0285] 在步骤1960中，授信引擎110以用户的私钥对合同的散列进行签名，并发送该签名后的散列给卖主，从而代表其自身对完整消息进行签名，即包括以授信引擎110的私钥加密的完整消息的散列(包括用户的签名)。在步骤1965中，该消息被卖主接收。该消息表示签名后的合同(利用用户的私钥加密的合同的散列)和来自授信引擎110的收条(receipt)(消息的散列包括签名后的合同，以授信引擎110的私钥加密)。

[0286] 在步骤1970中，授信引擎110类似地准备带有卖主私钥的合同散列，并将其转发给用户，其由授信引擎110签名。在步骤1975中，以该方式，用户也接收由卖主签名的合同的副本，以及由授信引擎110签名的收条，以交付签名后的合同。

[0287] 除了前面所述，本发明的附加方面提供了密码服务提供商模块(SPM:Service Provider Module)，该模块可用于客户端应用，作为访问上述授信引擎110所提供的功能的方式。一种提供这类服务的有利方式为密码SPM调停第三方应用编程接口(API)和授信引擎110之间的通信，其中授信引擎110可经由网络或其他远程连接被访问。示例性密码SPM在下面参考图20说明。

[0288] 例如，在典型的系统上，程序员可使用大量API。每个API提供一组可由在系统上运行的应用2000进行的功能调用。提供适于密码功能、鉴权功能、和其他安全功能的编程接口的API的例子包括由微软公司以其Windows操作系统所提供的密码API(CAPI)2010、和由开放组(Open Group)的IBM、英特尔和其他成员发起的通用数据安全架构(CDSA)。在下面的讨论中，CAPI将用作示例性安全API。然而，所述的密码SPM可与CDSA或本领域公知的其他安全API一起使用。

[0289] API在对密码功能进行调用时被用户系统105或卖主系统120使用。这些功能包括与执行各种密码操作相关联的请求，这些密码操作诸如是以特定密钥加密文档，对文档进行签名，请求数字证书，验证签名后文档上的签名，以及在这里说明或本领域技术人员公知的其他这类密码功能。

[0290] 这类密码功能通常对于CAPI 2010位于其上的系统本地地执行。这是因为，通常，

被调用的功能要求使用本地用户系统105的资源，诸如指纹读取器，或利用在本地机器上执行的库编程的软件功能。对这些本地资源的访问通常由一个或多个上面提到的提供资源的服务提供商模块(SPM)2015、2020提供，密码功能由这些资源执行的。这类SPM可包括软件库2015，以执行加密或解密操作，或能够访问专用硬件2025，诸如生物统计特征扫描设备的驱动程序和应用程序2020。以该方式，CAPI 2010提供可由系统105的应用程序2000使用的功能，SPM 2015、2020为CAPI提供对与系统上可用服务相关联的较低级别的功能和资源的访问。

[0291] 按照本发明，可以提供密码SPM 2030，其能够访问授信引擎110所提供的密码功能并使应用程序2000可通过CAPI 2010使用这些功能。与CAPI 2010仅能够访问通过SPM 2015，2020本地可用的资源的实施例不同，这里所述的密码SPM 2030能够将对于密码操作的请求提交给远程位置的网络可访问的授信引擎110，以便执行所期望的操作。

[0292] 例如，如果应用程序2000需要密码操作，诸如对文档进行签名，则应用程序2000对适当的CAPI 2010功能进行功能调用。CAPI 2010进而将执行该功能，利用通过SPM 2015，2020和密码SPM 2030使其可用的资源。在数字签名功能的情形中，密码SPM 2030将生成适当的请求，该请求将通过通信链路125被发送给授信引擎110。

[0293] 出现在密码SPM 2030和授信引擎110间的操作是与在任何其他系统与授信引擎110间可能的操作相同的操作。然而，通过CAPI 2010有效地使这些功能可由用户系统105使用，使得它们看起来在用户系统105自身上本地地可用。然而，不同于普通SPM 2015，2020，这些功能在远程授信引擎110上被执行，且响应经通信链路125的适当请求，结果被中继到密码SPM 2030。

[0294] 该密码SPM 2030使大量操作可由用户系统105或卖主系统120使用，否则这些操作可能不可用。这些功能包括但不限于：文档的加密和解密；数字证书的发布；文档的数字签名；数字签名的验证；和对本领域技术人员来说明显的其他操作。

[0295] 在单独的实施例中，本发明包括用于对任何数据集执行本发明的数据保护方法的完整系统。该实施例的计算机系统包括数据分割模块，其包括图8中所示并在此说明的功能。在本发明一个实施例中，有时被称为安全数据解析器的数据分割模块包括解析器程序或软件套件，其中解析器或软件套件包括数据分割，加密和解密，重构或重组装功能。该实施例可进一步包括数据存储设施或多个数据存储设施。数据分割模块或安全数据解析器包括集成在电子基础设施内或作为要求其数据元素的最终安全性(ultimate security)的任何应用程序的添加件的跨平台软件模块套件(cross-platform software module suite)。该解析过程对任何类型的数据集，和任何和所有文件类型，或在数据库中对该数据库的任一行，列或数据单元进行操作。

[0296] 在一个实施例中，本发明的解析过程以模块分层方式(modular tiered fashion)被设计，且任何加密过程都适用在本发明的过程中。本发明的解析和分割过程的模块分层可包括但不限于，1)密码分割，分散和安全地存储在多个位置中；2)加密，密码分割，分散和安全地存储在多个位置中；3)加密，密码分割，加密每个共享体，然后分散和安全地存储在多个位置中；和4)加密，密码分割，以与在第一步中所使用的加密不同类型的加密来加密每个共享体，然后分散和安全地存储在多个位置中。

[0297] 在一个实施例中，该过程包括按照所生成的随机数或密钥的内容的数据分割，和

执行用于数据分割的加密的密钥的相同密码分割，该数据被保护为解析并分割后的数据的两个或更多部分或共享体，并且在一个实施例中，优选被保护为解析并分割后的数据的四个或更多部分，以及加密所有部分，然后将这些部分分散并存储会数据库中，或根据请求人对私密性和安全性的需要，将他们重新放置到任何固定或可拆卸的命名的设备中。可替换地，在另一个实施例中，加密可在数据集被分割模块或安全数据解析器分割之前发生。按该实施例所述处理的原始数据被加密并扰乱(obfuscate)，并被保护。如果需要，加密后元素的分散实际上可在任何地方，包括但不限于单个服务器或数据存储设备，或在多个独立的数据存储设施或设备中。在一个实施例中，加密密钥管理可被包括在软件套件中，或在另一个实施例中可被集成到现有基础设施或任何其他期望的位置中。

[0298] 密码分割(cryptosplit)将数据分成N个共享体。划分可以任意大小的数据单位进行，包括单个比特，多个比特，字节，千字节，兆字节，或更大的单位，以及数据单位大小的任何模式或组合，无论是预定的还是随机生成的。基于随机或预定的数值集，这些单元也可以是不同大小的。这意味着数据可被看作这些单元的序列。以该方式，数据单元自身的大小可使数据更安全，例如通过使用数据单元大小的一个或多个预定或随机生成的模式、序列或组合。这些单元然后被分布到N个共享体内(随机地，或者通过预定的数值集)。该分布也可涉及打乱共享体中单元的顺序。本领域技术人员易于理解，数据单元分布到共享体中可按照多种可能的选择来执行，包括但不限于尺寸固定的，预定尺寸的，或预定或随机生成的数据单元尺寸的一个或多个组合、方式或序列。

[0299] 该密码分割过程的一个例子将考虑数据大小为23字节，其中数据单元大小被选择为1字节，共享体的数目被选择为4个。每个字节将被分布到4个共享体中的一个中。采用随机分布，将获得密钥以创建23个随机数字的序列(r1，r2，r3直到r23)，其中每个都有对应于4个共享体的1和4之间的值。每个数据单元(在该例子中，23个单独数据字节)与对应于四个共享体中一个的23个随机数中的一个相关联。数据字节分布到四个共享体中是通过以下方式实现的，即将数据的第一字节放置到共享数r1，第二字节放置到共享r2，第三字节放置到共享r3，直到数据的第23字节放置到共享r23。本领域技术人员易于理解，多种其他可能的步骤或步骤组合或序列，包括数据单元的大小，可被用在本发明的密码分割过程中，且上面的例子是密码分割数据的一个过程的非限制性说明。为了重新创建原始数据，要执行逆向操作。

[0300] 在本发明密码分割过程的另一个实施例中，密码分割过程的选项是在共享体中提供充分的冗余，使得只需要这些共享体的一个子集来将数据重组或恢复为其原始或可用形式。作为非限制性例子，密码分割可以“四中三”密码分割的形式实现，使得只有四个共享体中的三个共享体对于将数据重组或恢复为其原始或可用形式是必需的。这也可称为“N中M密码分割”，其中N是总的共享体数目，M至少比N小1。本领域技术人员可以理解，有很多可能的方法来在本发明的密码分割过程中创建该冗余。

[0301] 在本发明的密码分割的一个实施例中，每个数据单元被存储在两个共享体中，即主共享体和备份共享体。使用上述“四中三”密码分割过程，任意一个共享体可被丢失，且因为仅要求四个共享体中的三个，所以这足以重组或恢复原始数据，而不丢失数据单元。如这里所述，生成相应于其中一个共享体的随机数。基于密钥，随机数与数据单元相关联，并被存储在相应共享体内。在该实施例中，使用一个密钥以生成主和备份共享体随机数。如这里

为本发明的密码分割过程所述，生成等于数据单元数量的一组从0到3的随机数(也被称为主共享体数)。然后，生成等于数据单元数量的从1到3的另一组随机数(也被称为备份共享体数)。每个数据单元于是与主共享体数和备份共享体数相关联。可替换地，可生成一组少于数据单元数目的随机数，并重复随机数组，但这可减少敏感数据的安全性。主共享体数被用于确定数据单元被存储到哪个共享体中。备份共享体数与主共享体数结合以形成在0到3之间的第三共享体数，且该数字被用来确定数据单元被存储到哪个共享体中。在该例子中，确定第三共享体数的等式为：

[0302] (主共享体数+备份共享体数)MOD 4＝第三共享体数

[0303] 在上述实施例中，其中主共享体数在0到3之间，且备份共享体数在1到3之间，其确保了第三共享体数与主共享体数不同。数据单元中的该结果被存储在两个不同共享体中。本领域技术人员易于理解，除了这里公开的实施例之外，还有许多方式来执行冗余密码分割和非冗余密码分割。例如，每个共享体中的数据单元可利用不同算法被扰乱。该数据单元扰乱例如可在原始数据被分割为数据单元时，或在数据单元被放置到共享体中后，或在共享体充满后被执行。

[0304] 可对任意大小的数据单位执行这里所述的各种密码分割过程和数据扰乱过程，以及本发明的密码分割和数据扰乱方法的其他实施例，包括但不限于单个比特，多个比特，字节，千字节，兆字节或更大。

[0305] 执行这里所述的密码分割过程的源代码的一个实施例的例子是：

[0306]

```
DATA [1:24] – 具有待分割数据的字节的阵列
SHARES [0:3; 1:24] – 2 维阵列，其中每一行表示其中一个共享
体
RANDOM [1:24] – 0...3 范围中的阵列随机数
S1 = 1;
S2 = 1;
S3 = 1;
S4 = 1;
For J = 1 to 24 do
Begin
IF RANDOM[J[ ==0 then
      Begin
      SHARES[1,S1] = DATA [J];
      S1 = S1 + 1;
      End
ELSE IF RANDOM[J[ ==1 then
      Begin
      SHARES[2,S2] = DATA [J];
      S2 = S2 + 1;
      END
ELSE IF RANDOM[J[ ==2 then
      Begin
      SHARES[3,S3] = DATA [J];
      S3 = S3 + 1;
      End
```

[0307]

```
Else begin
      Share[4,S4] = data [J];
      S4 = S4 + 1;
      End;
END;
```

[0308] 执行这里所述的密码分割RAID过程的源代码的一个实施例的例子是：

[0309] 生成两组数，PrimaryShare是0到3，BackupShare是1到3。然后将每个数据单元放置到share[primaryshare[1]]和share([primaryshare[1]+backupshare[1])mod 4中，通过与上述密码分割中相同的过程。该方法将被缩放(scale)到任意大小N，其中仅N-1个共享体对于恢复数据是必需的。

[0310] 检索，重组，再组装或重构加密后数据元素可利用任意数目的鉴权技术，包括但不限于生物统计特征，诸如指纹识别，面部扫描，手扫描，虹膜扫描，视网膜扫描，耳朵扫描，血管图案识别，或DNA分析。本发明的数据分割和/或解析器模块可根据需要被集成到多种基础设施产品或应用中。

[0311] 本领域公知的传统加密技术依靠一个或多个用来加密数据并使其在无密钥时不可用的密钥。然而，数据保持完整并受到攻击。在一个实施例中，本发明的安全数据解析器通过以下方法解决该问题，即执行密码解析和将加密文件分割为两个或多个部分或共享体，且在另一个实施例中，优选为4个或更多共享体，对每个数据共享体添加另一层加密，然后在不同物理和/或逻辑位置存储共享体。当一个或多个数据共享体被从系统中物理地除去-通过使用可移动设备，诸如数据存储设备，或通过使共享体在另一方的控制下-时，任何危害被保护数据的可能性都得以有效地消除。

[0312] 本发明的安全数据解析器的一个实施例的例子及其可以如何被利用的例子在图21中示出并在下面说明。然而，对本领域技术人员来说显然，除了下面的非限制性例子之外，本发明的安全数据解析器可以多种方式被利用。作为一种部署选择，并且在一个实施例中，安全数据解析器可以外部会话密钥管理或会话密钥的安全内部存储而被实现。在实现时，将生成将被用于保护应用和用于加密目的的解析器主密钥。应该指出，在所得到的被保护数据中包括解析器主密钥就允许工作组、企业或扩展的受众中的个体灵活地共享被保护的数据。

[0313] 如图21所示，本发明的该实施例示出了安全数据解析器对数据所执行的处理步骤，以存储带被解析数据的会话主密钥：

[0314] 1.生成会话主密钥并利用RS1流密码加密数据。

[0315] 2.按照会话主密钥的图案将所得到的加密后的数据划分为被解析数据的四个共享体或部分。

[0316] 3.在方法的该实施例中，会话主密钥将与被保护的数据共享体一起被存储在数据存储库中。按照解析器主密钥的图案分离会话主密钥，并将密钥数据附加到加密后的解码数据。

[0317] 4.所得到的数据的四个共享体将包含原始数据的被加密部分和会话主密钥的部分。为四个数据共享体中每个共享体生成流密码密钥。

[0318] 5.加密每个共享体，然后在与被加密的数据部分或共享体不同的位置存储加密密钥：共享体1得到密钥4，共享体2得到密钥1，共享体3得到密钥2，共享体4得到密钥3。

[0319] 反转步骤以恢复原始数据格式。

[0320] 本领域技术人员易于理解，这里所述的方法的某些步骤按照需要可以不同顺序被执行或被重复多次。本领域技术人员也易于理解，数据的多个部分可彼此不同地被操纵。例如，多个解析步骤可仅对被解析数据的一个部分执行。被解析数据的每个部分可以任意期

望的方式被唯一地保护，仅如果数据可被重新组装，重新构建，重新形成，解密或恢复到其原始或其他可用形式。

[0321] 如图22所示和这里所述，本发明的另一实施例包括安全数据解析器对数据所执行的过程步骤，以在一个或多个分离的密钥管理表中存储会话主密钥数据：

[0322] 1.生成会话主密钥并用RS1流密码加密数据。

[0323] 2.按照会话主密钥的图案，将所得到的加密后的数据划分为被解析数据的四个共享体或部分。

[0324] 3.在本发明方法的该实施例中，会话主密钥将被存储在数据存储库的独立密钥管理表中。为该交易生成唯一交易ID。在独立的密钥管理表中存储交易ID和会话主密钥。按照解析器主密钥的图案分离交易ID，并将数据附加到加密后的被解析或被分离数据。

[0325] 4.所得到的数据的四个共享体将包含原始数据的被加密部分和交易ID的部分。

[0326] 5.为四个数据共享体中每个共享体生成流密钥。

[0327] 6.加密每个共享体，然后在与被加密数据部分或共享体不同的位置中存储加密密钥：共享体1得到密钥4，共享体2得到密钥1，共享体3得到密钥2，共享体4得到密钥3。

[0328] 颠倒步骤以恢复原始数据格式。

[0329] 本领域技术人员易于理解，这里所述方法的某些步骤可以按需要以不同的顺序被执行，或被重复多次。本领域技术人员也易于理解，数据部分可彼此不同地被操纵。例如，多个分离或解析步骤可仅对被解析数据的一个部分执行。解析数据的每个部分可以任意所需的方式被唯一地保护，仅如果数据可被重新组装，重新构建，重新形成，解密或恢复到其原始或其他可用形式。

[0330] 如图23所示，本发明的该实施例示出由安全数据解析器对数据所执行的过程步骤，以存储带被解析数据的会话主密钥：

[0331] 1.访问与被鉴权用户相关联的解析器主密钥

[0332] 2.生成唯一的会话主密钥

[0333] 3.从解析器主密钥和会话主密钥的异或函数获得中间密钥(intermediary key)

[0334] 4.利用以中间密钥键入(key)的现有或新加密算法选择性地加密数据。

[0335] 5.按照中间密钥的图案，将所得到的被选择性加密的数据划分为四个共享体或部分。

[0336] 6.在方法的该实施例中，会话主密钥将与被保护的数据共享体一起被存储在数据存储库中。按照解析器主密钥的图案分离会话主密钥，并将密钥数据附加到被选择性加密的被解析数据共享体。

[0337] 7.所得到的多个数据共享体将包含原始数据的被选择性加密的部分和会话主密钥的部分。

[0338] 8.为四个数据共享体中的每个共享体选择性地生成加密密钥。

[0339] 9.以现有的或新的加密算法选择性地加密每个共享体，然后在与被加密数据部分或共享体不同的位置存储加密密钥：例如共享体1得到密钥4，共享体2得到密钥1，共享体3得到密钥2，共享体4得到密钥3。

[0340] 颠倒步骤以恢复原始数据格式。

[0341] 本领域技术人员易于理解，这里所述方法的某些步骤可根据需要以不同的顺序被

执行，或被重复多次。本领域技术人员还易于理解多个数据部分可以彼此不同的方式被操纵。例如多个解析步骤可仅对被解析数据的一个部分执行。解析数据的每个部分可以任意期望的方式被唯一地保护，仅如果数据可被重新组装，重新构建，重新形成，解密或恢复到其原始或其他可用形式。

[0342] 如图24和这里所示，本发明另一个实施例包括安全数据解析器对数据执行的过程步骤，以在一个或多个独立的密钥管理表中存储会话主密钥：

[0343] 1.访问与被鉴权用户相关联的解析器主密钥

[0344] 2.生成唯一的会话主密钥

[0345] 3.从解析器主密钥和会话主密钥的异或函数获得中间密钥

[0346] 4.用以中间密钥键入的现有或新加密算法选择性地加密数据。

[0347] 5.按照中间密钥的图案，将所得到的被选择性加密的数据划分为四个共享体或部分。

[0348] 6.在本发明方法的该实施例中，会话主密钥将被存储在数据存储库中独立的密钥管理表中。为该交易生成唯一交易ID。在独立的密钥管理表中存储交易ID和会话主密钥，或将会话主密钥和交易ID回传给调用程序用于外部管理。按照解析器主密钥的图案分离交易ID，并将数据附加到被选择性加密的被解析或分离数据上。

[0349] 7.所得到的数据的四个共享体将包含原始数据的选择性加密的部分和交易ID的部分。

[0350] 8.为四个数据共享体中每个共享体选择性地生成加密密钥。

[0351] 9.选择性地加密每个共享体，然后在与被加密数据部分或共享体不同的位置中存储加密密钥。例如，共享体1得到密钥4，共享体2得到密钥1，共享体3得到密钥2，共享体4得到密钥3。

[0352] 颠倒步骤从而恢复原始数据格式。

[0353] 本领域技术人员易于理解，这里所述方法的某些步骤可按需要以不同顺序被执行，或被重复多次。本领域技术人员还易于理解，数据的多个部分可以彼此不同的方式执行。例如，多个分离或解析步骤可仅对被解析数据的一部分执行。解析数据的每个部分可以任意所需的方式被唯一地保护，仅如果数据可被重新组装，重新构建，重新组成，解密或恢复到其原始或其他可用形式时提供。

[0354] 本领域技术人员易于理解多种加密方法适用于本发明的方法。一次一密算法通常被被认为是最安全的加密方法，并适用于本发明的方法。使用一次一密算法要求生成与待保护数据一样长的密钥。在某些环境中使用该方法较不理想，诸如那些由于待保护的数据集的大小而导致生成和管理非常长密钥的情形。在一次一密(OTP)算法中，使用简单的异或函数XOR。对于同样长度的两个二进制流x和y，x XOR y表示x和y的逐位异或操作。

[0355] 在位级别上，XOR操作得到：

[0356] 0 XOR 0＝0

[0357] 0 XOR 1＝1

[0358] 1 XOR 0＝1

[0359] 1 XOR 1＝0

[0360] 这里该过程的例子是为要分割的n字节秘密(secret)s(或数据集)说明的。该过程

将生成n字节随机值a，然后设定：

[0361] b＝a XOR s。

[0362] 注意，可经下面的等式获得“s”：

[0363] s＝a XOR b。

[0364] 值a和b被称为共享体或部分，并被放置在分离的存储库中。一旦秘密s被分割成两个或多个共享体，则其以安全方式被丢弃。

[0365] 本发明的安全数据解析器可利用该功能，执行多次包括多个不同保密键值：K1，K2，K3，Kn，K5的XOR函数。在操作开始时，待保护数据经过第一加密操作，安全数据＝数据XOR秘密键值5：

[0366] S＝D XOR K5

[0367] 为了安全地在例如四个共享体S1，S2，S3，Sn中存储所得到的被加密数据，按照K5的值，数据被解析并被分割为“n”个段或共享体。该操作导致原始加密数据的“n”个伪随机共享体。然后可以以剩余的秘密键值对对每个共享体执行后续XOR函数，例如：安全数据段1＝加密数据共享体1XOR秘密键1：

[0368] SD1＝S1 XOR K1

[0369] SD2＝S2 XOR K2

[0370] SD3＝S3 XOR K3

[0371] SDn＝Sn XOR Kn。

[0372] 在一个实施例中，可能不期望有任一存储库包含有足够的信息来解密保存在其中的信息，从而解密共享体所需要的密钥被存储在不同数据存储库中：

[0373] 存储库1：SD1，Kn

[0374] 存储库2：SD2，K1

[0375] 存储库3：SD3，K3

[0376] 存储库n：SDn，K3。

[0377] 此外，附加到每个共享体的可以是恢复原始会话加密密钥K5所要求的信息。因此，在这里所述的密钥管理例子中，按照安装相关解析器主密钥(TID1，TID2，TID3，TIDn)的内容，原始会话主密钥被分割成“n”个共享体的交易ID引用：

[0378] 存储库1：SD1，Kn，TID1

[0379] 存储库2：SD2，K1，TID2

[0380] 存储库3：SD3，K2，TID3

[0381] 存储库n：SDn，K3，TIDn。

[0382] 在这里所述的包含的会话密钥例子中，按照安装相关解析器主密钥(SK1，SK2，SK3，SKn)的内容，会话主密钥被分成“n”个共享体：

[0383] 存储库1：SD1，Kn，SK1

[0384] 存储库2：SD2，K1，SK 2

[0385] 存储库3：SD3，K2，SK 3

[0386] 存储库n：SDn，K3，SK n。

[0387] 除非所有四个共享体被检索，否则数据不能按照该例子被重新组装。即使所有四个共享体都被捕获，也不可能在不访问会话主密钥和解析器主密钥的情况下重新组装或恢

复原始信息。

[0388] 该例子说明了本发明的方法的一个实施例，并且还在另一个实施例中说明了用来将共享体放置到存储库的算法，使得来自所有存储库的共享体可被组合以形成保密鉴权材料。所需的计算非常简单和快速。然而，对于一次一密(OTP)算法，可能有使其不太期望的情形，诸如大数据集要被保护，因为密钥大小与待存储的数据的大小相同。因此，需要存储和传输约为原始数据的量的两倍，这在某些情形中是不太期望的。

[0389] 流密码RS1

[0390] 流密码RS1分割技术非常类似于这里所述的OTP分割技术。不是n字节随机值，而是生成n'=min(n,16)字节随机值，并且其被用于键入(key)RS1流密码算法。RS1流密码算法的优点是从小得多的种子数生成伪随机密钥。RS1流密码加密的执行速度也被认定为约为本领域公知的三重DES加密的速度的10倍，而不削弱安全性。RS1流密码算法是本领域公知的，并可被用于生成用在异或(XOR)函数中的密钥。RSI流密码算法可与其他商业上可获得的流密码算法，诸如RSA安全公司的RC4™流密码算法协同操作，并适用于本发明的方法。

[0391] 使用上面提到的密钥，K1到K5现在是n'字节随机值，我们设定：

[0392] SD1=S1 XOR E(K1)

[0393] SD2=S2 XOR E(K2)

[0394] SD3=S3 XOR E(K3)

[0395] SDn=Sn XOR E(Kn)。

[0396] 其中E(K1)到E(Kn)是由K1到Kn键入的RS1流密码算法输出的前n'个字节。如这里所述，共享体现在被放置在数据存储库中。

[0397] 在该流密码RS1算法中，所要求的计算与OTP算法一样简单快速。该例子中使用RS1流密码的益处是，每个共享体，系统平均只需要存储和传输比待保护的原始数据的大小多大约16个字节。当原始数据的大小超过16个字节时，该RS1算法因为其更短而比OTP算法更高效。本领域技术人员易于理解，多种加密方法或算法适用于本发明，包括但不限于RS1，OTP，RC4™，三重DES和AES。

[0398] 本发明的数据安全方法和计算机系统相对于传统加密方法提供了显著的优点。一个优点是从将数据共享体移动到一个或多个数据存储库或存储设备上的不同位置而获得的安全性，这些数据存储库或存储设备可位于不同的逻辑，物理或地理位置。当数据共享体在不同人员的控制下被物理地分割时，例如显著地减小危及数据的可能性。

[0399] 本发明的方法和系统所提供的另一个优点是组合本发明的保护数据方法以提供保持敏感数据安全性的完整过程。数据以安全密钥被加密，并被分割成一个或多个共享体，且在一个实施例中，按照安全密钥被分割为四个共享体。安全密钥安全地以引用指针被存储，该引用指针按照安全密钥被固定到四个共享体。然后，数据共享体被单独加密，且密钥安全地以不同加密共享体被存储。当组合时，按照这里公开的方法保护数据的整个过程成为用于数据安全性的完整方案。

[0400] 按照本发明方法保护的数据可以易于重新检索和恢复，重新构建，重新组装，解密，或以其他方式被返回到其原始或其他合适形式供使用。为了恢复原始数据，可利用下面的项：

[0401] 1.数据集的所有共享体或部分。

[0402] 2.再现用于保护数据的方法的流程的知识和能力。

[0403] 3.访问会话主密钥。

[0404] 4.访问解析器主密钥。

[0405] 因此，可能期望规划安全安装，其中至少一个上述元素可与系统的剩余元件物理地分开(例如在不同系统管理员的控制下)。

[0406] 可利用解析器主密钥而加强对防止流氓应用程序调用数据保护方法应用的保护。本发明的该实施例中可能要求在采取任何动作之前安全数据解析器和应用之间相互鉴权握手。

[0407] 系统的安全性指示没有“后门”方法用于再创建原始数据。对于可能产生数据恢复问题的安装，安全数据解析器可被增强以提供四个共享体和会话主密钥存储库的镜像。硬件选项，诸如RAID(廉价磁盘冗余阵列，用于在几个磁盘上传播信息)和软件选项，诸如复制也可辅助数据恢复规划。

[0408] 密钥管理

[0409] 在本发明的一个实施例中，数据保护方法使用三组密钥用于加密操作。基于安装，每组密钥可具有单独密钥存储，检索，安全性和恢复选项。可使用的密钥包括但不限于：

[0410] 解析器主密钥

[0411] 该密钥是与安全数据解析器的安装相关联的单独密钥。其被安装在其上已经部署了安全数据解析器的服务器上。有多种选项适于保护该密钥，例如包括但不限于智能卡，独立的硬件密钥存储，标准密钥存储，定制密钥存储(custom key store)或在被保护的数据库表内。

[0412] 会话主密钥

[0413] 会话主密钥可在每次数据被保护时被生成。会话主密钥被用来在解析和分割操作之前加密数据。其也可以被包含(如果会话主密钥不被集成到被解析数据中)作为解析加密数据的方法。会话主密钥可以多种方式被保护，例如包括但不限于标准密钥存储，定制密钥存储，独立数据库表，或在被加密的共享体内被保护。

[0414] 共享体加密密钥

[0415] 对于被创建的数据集的每个共享体或部分，可生成单独共享体加密密钥以进一步加密共享体。共享体加密密钥可被存储在与被加密的共享体不同的共享体中。

[0416] 本领域技术人员易于理解，本发明的数据保护方法和计算机系统可在任何设置或环境中被广泛应用于任何类型的数据。除了经因特网或在客户与卖主之间执行的商业应用之外，本发明的数据保护方法和计算机系统高度地可用于非商业或私人设置或环境。任何期望被保护防止任何未授权用户访问的数据集可利用这里所述的方法和系统而被保护。例如，对公司或组织内特定数据库的访问权限可有利地利用本发明的保护数据的方法和系统而只被限制到选定的用户。另一个例子是发生，修改或访问文件，其中期望限制访问或防止未授权或意外访问或防止向选定的个体，计算机或工作站组之外公开。本发明数据的数据保护方法和系统可被应用于任意非商业或商业情景或设置的这些和其他例子，包括但不限于任何组织，政府机构或公司。

[0417] 在本发明的另一个例子中，数据保护方法使用三组密钥用于加密操作。基于安装，每组密钥可具有单独密钥存储，检索，安全性和恢复选项。可使用的密钥包括但不限于：

[0418] 1.解析器主密钥

[0419] 该密钥是与安全数据解析器的安装相关联的单独密钥。其被安装在其上已经部署了安全数据解析器的服务器上。有多种选项适于保护该密钥，例如包括但不限于智能卡，单独的硬件密钥存储，标准密钥存储，定制密钥存储或在被保护的数据库表内。

[0420] 2.会话主密钥

[0421] 每次数据被保护时生成会话主密钥。会话主密钥与解析器主密钥结合使用，以获得中间密钥。会话主密钥可以多种方式被保护，例如包括但不限于标准密钥存储，定制密钥存储，单独数据库表，或在被加密共享体内被保护。

[0422] 3.中间密钥

[0423] 每次数据被保护时生成中间密钥。中间密钥被用于在解析和分割操作之前加密数据。其也可以被包含作为解析加密数据的方法。

[0424] 4.共享体加密密钥

[0425] 对于被创建的数据集的每个共享体或部分，可生成单独共享体加密密钥以进一步加密共享体。共享体密钥可被存储在与被加密的共享体不同的共享体中。

[0426] 本领域技术人员易于理解，在任何设置或环境中，本发明的数据保护方法和计算机系统可广泛地用于任何类型的数据。除了经因特网或在客户与卖主间执行的商业应用之外，本发明的数据保护方法和计算机系统高度地可用于非商业或私人设置或环境中。期望被保护以防止任何未授权用户的数据集可利用这里公开的方法和系统而被保护。例如，对公司或组织内特定数据库的访问权限可以有利地利用本发明的保护数据的方法和系统而被限制在选定的用户。另一个例子是生成，修改或访问文档，其中期望限制访问或防止未授权或意外访问或向选定的个体，计算机或工作站之外公开。本发明的数据保护方法和系统可应用于任意非商业或商业情景或设置的方式的这些和其他例子，包括但不限于任何组织，政府机构或公司。

[0427] 工作组，项目，单个PC/膝上型计算机或跨平台数据安全性

[0428] 本发明的数据保护方法和计算机系统也可用于通过工作组，项目，单人PC/膝上型计算机和任何其他例如用在商业，办公室，政府机构或任何创建，操纵或存储敏感数据的设置中的平台保护数据。本发明提供了方法和计算机系统来保护数据，该数据是组织，诸如美国政府搜索以便跨整个政府组织或在州或联邦政府间执行的数据。

[0429] 本发明的数据保护方法和计算机系统提供了解析和分割文件以及任何类型的数据字段，集合和/或表格的能力。此外，所有形式的数据能够在该过程中被保护，包括但不限于文本，视频，图像，生物统计特征和语音数据。本发明的保护数据方法的可缩放性，速度和数据通吐量仅限于用户操纵的硬件。

[0430] 在本发明一个实施例中，数据保护方法如下所述在工作组环境中被使用。在一个实施例中，如图23中所示和下面所述，本发明的工作组等级(Workgroup Scale)数据保护方法使用授信引擎的私钥管理功能，从而存储用户/工作组关系和用户组共享安全数据所必须的相关私钥(解析器组主密钥)。本发明的方法能够根据解析器主密钥如何被部署而为企业，工作组，或个人用户保护数据。

[0431] 在一个实施例中，可提供额外的密钥管理和用户/工作组管理程序，使得能够以单点管理和密钥管理实现宽比例工作组实现。密钥生成，管理和撤销是由单个维护程序操纵

的，这些随着用户数目的增加都变得特别重要。在另一个实施例中，密钥管理也可跨一个或几个不同系统管理员而被设置，这可能不允许任意一个人员或组按需要控制数据。这允许以组织所定义的角色，责任，成员资格，权限等获得被保护数据的管理，且对被保护数据的访问可被仅仅限制到那些被允许或要求只有权访问他们在其上进行工作的部分，而其他人，诸如经理或执行人员可有权访问所有被保护的数据。该实施例允许在公司或组织内的不同组之间被保护数据的共享，同时仅允许某些选择的个体，诸如具有被授权和预定角色，责任的人察看整个数据。此外，本发明的方法和系统的该实施例也允许例如在独立的公司或独立的部分或公司部门，或其中要求某些共享的任何政府或组织的任何独立组织部门，组，机构，或办公室等之间共享数据，但不是任何一方都可被允许有权访问所有数据。对本发明的这样的方法和系统的需要和使用的特别明显的例子是允许在政府区域，机构和办公室之间，和在大公司，或任何其他组织的不同分部，部门或办公室之间共享但保持安全性。

[0432] 本发明的方法的小规模可应用性例子如下：解析器主密钥被用作安全数据解析器对组织的串行化(serialization)或印记(branding)。随着解析器主密钥的使用规模从整个企业减小到较小的工作组，这里所述的数据保护方法被用来在用户组内共享文件。

[0433] 在图25所示且在下面所述的例子中，有六个与其在组织内的头衔或角色一起定义的用户。侧条表示用户按照其角色可以属于其中的5个可能的组。箭头表示用户在一个或多个组中的成员资格。

[0434] 当为该例子中用途而配置安全数据解析器时，系统管理员从操作系统通过维护程序访问用户和用户组信息。该维护程序基于用户在组内的成员资格生成并分配解析器组主密钥给用户。

[0435] 在该例子中，有三个成员在高级职员组中。对于该组，动作如下：

[0436] 1.访问用于高级职员组的解析器组主密钥(如果不存在，则生成一个密钥)；

[0437] 2.生成将CEO与高级职员组相关联的数字证书；

[0438] 3.生成将CFO与高级职员组相关联的数字证书；

[0439] 4.生成将副总裁、市场部与高级职员组相关联的数字证书；

[0440] 对每个组和每组内的每个成员执行同一组动作。当维护程序完成时，解析器组主密钥成为该组每个成员的共享凭证。可在通过维护程序从组中移除用户时自动实现被分配的数字证书的撤回，而不影响组的剩余成员。

[0441] 一旦共享凭证已经被定义，则解析和分割过程保持相同。当文件、文档或数据元素要被保护时，在保护数据时为要使用的目标组提示用户。所得到的被保护数据仅可由目标组的其他成员访问。本发明的方法和系统的功能可与任何其他计算机系统或软件平台一起使用，例如可以被集成到现有应用程序中或为文件安全性而单独使用。

[0442] 本领域技术人员易于理解，任何一个加密算法或任何加密算法的组合适用于本发明的方法和系统。例如，在一个实施例中，加密步骤被重复，以产生多层加密方案。此外，不同加密算法或加密算法的组合可被用在重复加密步骤中，使得不同加密算法被应用到多层加密方案的不同层中。同样地，加密方案自身可成为用于保护敏感数据免遭未授权使用或访问的本发明方法的组件。

[0443] 安全数据解析器可包括作为内部组件、外部组件、或也作为错误检测组件。例如，在一种合适的方法中，由于利用按照本发明的安全数据解析器创建数据是的多个部分，以

确保一部分内数据的完整性，所以在该部分内以预定间隔取散列值并将其附加到间隔的尾部。散列值是数据的可预测和可复制的数值表示。如果数据中任意位改变，则散列值会不同。扫描模块(要么作为安全数据解析器外部的独立元件，要么作为内部元件)然后可扫描安全数据解析器所生成的数据的部分。将数据的每个部分(或可替换地，按照某间隔或通过随机或伪随机取样，少于数据的所有部分)与附加的散列值进行比较，并可以采取动作。该动作可包括匹配和不匹配的值的报告，不匹配的值的警告，或调用某外部或内部程序以触发数据的恢复。例如，基于按照本发明的为了生成原始数据可能需要少于所有的部分的的理念，可以通过调用恢复模块执行数据的恢复。

[0444] 任何其他合适的完整性检查可以利用附加在所有数据部分或数据部分的子集中任何地方的任何合适的完整性信息来实现，该信息。完整性信息可包括任何可用来判断数据部分的完整性的合适信息。完整性信息的例子可包括基于任何合适参数(例如基于相应数据部分)所计算的散列值，数字签名信息，消息鉴定码(MAC)信息，任何其他合适信息或它们的组合。

[0445] 本发明的安全数据解析器可被用在任何合适的应用中。也就是，这里所述的安全数据解析器在不同计算和技术领域中具有多种应用。几个这样的领域在下面讨论。可以理解，这本质上仅是说明性的，且任何其他合适的应用可利用安全数据解析器。进一步可以理解，这里所述的例子仅是说明实施例，这些实施例可以任何合适的方式被修改以便满足任何合适的需要。例如，解析和分割可基于任何合适的单位，诸如以比特，字节，千字节，兆字节，以及其任何组合，或任何其他合适的单位进行。

[0446] 本发明的安全数据解析器可被用来实现安全物理权标，因而可能要求存储在物理权标中的数据以便访问存储在另一存储区中的额外数据。按照本发明，在一个合适的方法中，物理权标，诸如紧凑USB闪存驱动器，软盘，光盘，智能卡，或任何其他合适的物理权标可被用来存储被解析数据的至少两个部分中的一个。为了访问原始数据，需要访问USB闪存驱动器。因此，保存被解析数据的一个部分的个人计算机在原始数据能被访问之前需要将具有被解析数据的其他部分的USB闪存驱动器连接。图26示出该应用。存储区2500包括被解析数据的部分2502。具有被解析数据的部分2506的物理权标2504需要用任何合适的通信接口2508(例如USB，串行，并行，蓝牙，IR，IEEE1394，以太网，或任何其他合适的通信接口)被耦接到存储区2500，以便访问原始数据。这在下面的情形中是有用的，例如其中计算机上的敏感数据不被管理并受到未授权访问尝试。通过除去物理权标(例如USB闪存驱动器)，敏感数据是不可访问的。可以理解，可以采用使用物理权标的任何其他合适方法。

[0447] 本发明的安全数据解析器可被用于实现安全鉴定系统，其中利用安全数据解析器解析和分割用户登记数据(例如，口令，私用加密密钥，指纹模板，生物统计特征数据或任何其他合适的用户登记数据)。用户登记数据可被解析和分割，其中一个或多个部分被存储在智能卡、政府公共访问卡、任何合适的物理存储设备(例如，磁盘或光盘，USB密钥驱动器，等)，或任何其他合适的设备上。被解析的用户登记数据的一个或多个其他部分可被存储在执行鉴定的系统中。这为鉴定过程提供了外加的安全度(例如，除了从生物统计特征源所获得的生物统计特征鉴权信息外，用户登记数据也必须经适当的被解析和分割的数据部分而被获得)。

[0448] 本发明的安全数据解析器可被集成到任何合适的现有系统中，以便在每个系统各

自的环境中提供其功能的使用。图27示出了说明性系统2600的方框图，其可包括软件，硬件，或两者用于执行任何合适应用。系统2600可以是现有系统，其中安全数据解析器2602可以被改进为集成组件。可替换地，安全数据解析器2602可以例如从其最早设计阶段被集成到任何合适的系统2600中。安全数据解析器2600可以在系统2600的任何合适级上被集成。例如，安全数据解析器2602可以在充分的后端级被集成到系统2600中，使得安全数据解析器2602的存在可对系统2600的最终用户是充分透明的。按照本发明，安全数据解析器2602可被用于在一个或多个存储设备2604中解析和分割数据。其中集成有安全数据解析器的系统的某些示例性例子在下面讨论。

[0449] 本发明的安全数据解析器可被集成到操作系统内核(例如，Linux，Unix，或任何其他合适的商业或专有操作系统)中。该集成可被用于在设备级保护数据，其中例如通常会被存储在一个或多个设备中的数据被集成到操作系统中的安全数据解析器划分成一定数量的部分并被存储在这一个或多个设备中。当试图访问原始数据时，也被集成到操作系统中的适当软件可以可能对于最终用户而言透明的方式将被解析的数据部分重新组合为原始数据。

[0450] 本发明的安全数据解析器可被集成到卷管理器或存储系统的任何其他合适的组件中，以跨任意或所有被支持平台保护本地和联网的数据存储。例如，通过集成安全数据解析器，存储系统可利用安全数据解析器所提供的冗余(即，其被用于实现需要少于全部被划分的数据部分以重构原始数据的特征)，以放置数据损失。安全数据解析器也允许所有被写到存储设备的数据的形式为按照本发明的解析所生成的多个部分，而无论是否使用冗余。当试图访问原始数据时，也被集成到卷管理器或存储系统的其他合适组件中的适当软件可以可能对最终用户透明的方式将被解析的数据部分重新组合为原始数据。

[0451] 在一个合适的方法中，本发明的安全数据解析器可被集成到RAID控制器中(作为硬件或软件)。这允许数据安全地存储到多个驱动器，同时在驱动器故障中保持容错能力。

[0452] 本发明的安全数据解析器可被集成到数据库中以便例如保护敏感表信息。例如，按照本发明，在一个合适的方法中，与数据库表格的特定单元(例如各个单元，一个或多个特定列，一个或多个特定行，其任意组合，或整个数据库表格)相关联的数据可被解析并划分(例如，不同部分被存储在一个或多个位置处的一个或多个存储设备上，或被存储在单个存储设备上)。传统鉴权方法(例如，用户名和口令查询)可授权访问以重组这些部分以便察看原始数据。

[0453] 本发明的安全解析器可被集成到涉及数据移动(即数据从一个位置转移到另一个位置)的任何合适的系统中。这类系统例如包括电子邮件、流式数据广播、和无线(例如，WiFi)通信。对于电子邮件，在一种合适的方法中，安全解析器可被用来解析出局信息(即，包含文本，二进制数据，或这两者(例如附加到电子邮件消息的文件)，和沿不同路径发送被解析数据的不同部分，因此创建多个数据流。如果这些数据流中的任意一个受损，则原始消息保持安全，因为按照本发明，系统可要求组合一个以上的这些部分，以便生成原始数据。在另一个合适的方法中，数据的不同部分可沿一条路径相继地被通信，从而如果获得一个部分，则可能不足以生成原始数据。按照本发明，不同部分到达期望的接收方的位置，并可被组合以生成原始数据。

[0454] 图28和29是这类电子邮件系统的示例性方框图。图28示出发送方系统2700，其可

包括任何合适的硬件，诸如计算机终端，个人计算机，手持设备(例如PDA，Blackberry)，蜂窝电话，计算机网络，任何其他合适的硬件，或其任意组合。发送方系统2700被用于生成和/或存储消息2704，其例如可以是电子邮件消息，二进制数据文件(例如图形，语音，视频，等)，或两者。按照本发明，消息2704被安全数据解析器2702解析并分割。所得到的数据部分可跨一个或多个分离的通信路径2706经网络2708(例如因特网，内联网，LAN，WiFi，蓝牙，任何其他合适的硬布线或无线通信方式，或其任意组合)被传输到接收方系统2710。数据部分可被实时地或可替换地按照不同数据部分的通信之间任何合适的时间延迟被并行传输。接收方系统2710可以是如上针对发送方系统2700所述的任何合适的硬件。按照本发明，沿通信路径2706传输的分离的数据部分在接收方系统2710处被重组，以生成原始消息或数据。

[0455] 图29示出发送方系统2800，其可包括任意合适的硬件，诸如计算机终端，个人计算机，手持设备(如PDA)，蜂窝电话，计算机网络，任何其他合适硬件，或其任何组合。发送方系统2800被用于生成和/或存储消息2804，其例如可以是电子邮件消息，二进制数据文件(例如，图形，语音，音频等)，或这两者。按照本发明，消息2804被安全数据解析器2802解析和分割。所得到的数据部分可经网络2808(例如，因特网，内联网，LAN，WiFi，蓝牙，任何其他合适的通信方式，或其任何组合)跨单个通信路径2806被通信到接收方系统2810。数据部分可相互串行地通过通信路径2806被传输。接收方系统2810可以是以上针对发送方系统2800所述的任何合适的硬件。按照本发明，沿通信路径2806传输的分离的数据部分在接收方系统2810处被重组，以生成原始消息或数据。

[0456] 可以理解，图28和29的结构仅是示例性的。任何其他合适的结构都可使用。例如，在其他合适的方法中，图28和29的系统的特征可被组合，其中使用图28的多径方法，通信路径2706中一个或多个被用来携带数据的一个以上的部分，如同通信路径2806在图29的情形中那样。

[0457] 安全数据解析器可以在数据移动系统的任何合适级被集成。例如，在电子邮件系统的情形中，安全解析器可以在用户接口级被集成(例如，集成到Microsoft® Outlook)中，在该情形中，在使用电子邮件时，用户可控制安全数据解析器特征的使用。可替换地，按照本发明，安全解析器可在后端组件中被实现，诸如在交换服务器处，在该情形中，消息可被自动解析、分割，并沿不同路径被传输，而无需任何用户干预。

[0458] 类似地，在数据的流式广播的情形中(例如音频，视频)，出局数据可被解析并划分成多个流，其中每个流都含有被解析数据的部分。按照本发明，多个流可沿着一个或多个路径被传输并在接收方位置处被重组。该方法的一个优点是其避免了在加密数据经单个通信信道传输之前与传统的数据加密相关联的相对大的额外开销。本发明的安全解析器允许运动数据在多个并行流中被发送，从而增加速度和效率。

[0459] 可以理解，安全数据解析器可被集成以用于任何类型的通过任何传输介质移动的数据的保护和容错，传输介质例如包括有线，无线，或物理介质。例如，网络语音通信(VoIP)应用可利用本发明的安全数据解析器。可利用本发明的安全数据解析器来保护与任何合适的个人数字助理(PDA)设备，诸如Blackberry和SmartPhone的无线或有线数据传输。按照本发明，利用用于对等和基于hub的无线网络的无线802.11协议的通信，卫星通信，点对点无线通信，因特网客户机/服务器通信，或任何其他合适的通信可涉及根据本发明的安全数据解析器的移动数据能力。计算机和计算机外围设备之间，计算机外围设备与任何其他合适

的设备之间，或其任何组合的计算机外围设备(例如打印机，扫描仪，监视器，键盘，网络路由器，生物统计特征识别设备(例如指纹扫描仪)，或任何其他合适的外围设备)的数据通信可以利用本发明的移动数据特征。

[0460] 本发明的移动数据(data in motion)特征也可应用到安全共享体的物理传输，例如使用分离的路由，载体，方法，任何其他合适的物理传输，或其任何组合。例如，数据的物理传输可在数字/磁带，软盘，光盘，物理权标，USB驱动器，可拆卸硬驱，带有闪存的消费电子设备(例如Apple IPOD或其他MP3播放器)，闪存，任何用于传输数据的其他合适介质，或其任何组合上发生。

[0461] 本发明的安全数据解析器可提供安全性，并具有灾难恢复能力。按照本发明，为了找回原始数据，少于由安全数据解析器所生成的分离数据的所有部分可能是必需的。也就是说，m个存储的部分中，n可能是这些m个部分中对于恢复原始数据所必须的最小数目，其中n<=m。例如，如果四个部分中的每个都相对于其他三个部分被存储在不同的物理位置，那么在该例子中如果n=2，则两个位置可能受危害，因而数据被破坏或不可访问，且原始数据仍可从其他两个位置中的部分恢复。可使用n和m的任何合适的值。

[0462] 此外，本发明的m个中n个的特征可被用来建立“两人规则”，因而为了避免向单个个体或任何其他实体委托对可能是敏感数据的对象的完全访问权，分别具有由本发明的安全解析器所解析的分离数据的部分的两个或多个不同实体可能需要同意将他们的部分放在一起，以恢复原始数据。

[0463] 本发明的安全数据解析器可被用于提供一组具有组内密钥(group-wide key)的实体，该组内密钥允许组成员访问被授权由该特定组访问的特定信息。组密钥可以是由按照本发明的安全解析器所生成的数据部分之一，该数据部分被要求与中央存储的另一部分组合，例如以便恢复想要的信息。该特征例如允许组内的安全合作。例如，该特征可被应用到专用网络，虚拟私人网络，内联网，或任何其他合适的网络。

[0464] 安全解析器的这个使用的具体例子例如包括联合信息共享(coalition information sharing)，其中例如为多国友好政府力量提供经单个网络或双网络(即，与许多涉及当前使用的基本手动的过程的网络相比)在被授权给各国的安全级上传输操作的和敏感的数据的能力。该能力也可应用于公司和其他组织，其中一个或多个特定个体(在组织内或组织外)需要知道的信息可经单个网络传输，而无需担心未授权的个体察看该信息。

[0465] 另一个特定应用包括用于政府系统的多级安全性分层结构。也就是，本发明的安全解析器可提供使用单个网络来在分类信息的不同级(例如未分类的，分类的，机密的，绝密的)操作政府系统的能力。如果需要，可使用更多网络(例如用于绝密信息的单独网络)，但本发明允许比当前结构显著更少，其中在当前结构中，分离网络被用于分类的每级。

[0466] 可以理解，本发明的安全解析器的上述应用的任何组合都可被使用。例如，组密钥应用可与移动数据安全应用一起被使用(即，其中经网络传输的数据仅可被相应组的成员访问，且在数据移动时，根据本发明在多个路径间分割(或以连续的部分被发送))。

[0467] 本发明的安全数据解析器可被集成到任何中间件应用中，从而使得应用能够将数据安全地存储到不同数据库产品或不同设备，而不修改应用或数据库。中间件是允许两个分离的已经存在的程序通信的任何产品的一般术语。例如，在一个合适的方法中，集成有安全数据解析器的中间件可被用来允许为特定数据库写的程序与其他数据库通信，而无需定

制编码。

[0468] 本发明的安全数据解析器可以被实现为任何合适能力、诸如这里所讨论的那些能力的任何组合。在本发明的某些实施例中，例如，安全数据解析器可被实现为仅具有某些能力，而其他能力可通过使用直接或间接地与安全数据解析器对接的外部软件，硬件，或其二者而被获得。

[0469] 例如图30示出安全数据解析器的示例性实现为安全数据解析器3000。安全数据解析器3000可以被实现为具有非常少的内置能力。如这里所示，按照本发明，安全数据解析器3000可包括用于使用模块3002将数据解析和分割为数据的部分(这里也称为共享体)的内置能力。安全数据解析器3000也可包括用于执行冗余的内置能力，以便能够用模块3004实现上述n中m特征(即用少于被解析和分割数据的所有共享体来重新建立原始数据)。按照本发明，安全数据解析器3000也可包括使用模块3006的共享分布能力，用于将数据的共享体放置到缓存中，共享体从这些缓存被发送用于传输到远程位置、用于存储等。可以理解，任何其他合适的能力可被内置到安全数据解析器3000中。

[0470] 组装的数据缓存3008可以是用于存储原始数据(虽然不必以其原始形式)的任何合适的存储器，该原始数据将由安全数据解析器3000解析和分割。在分割操作中，组装的数据缓存3008提供输入给安全数据解析器3008。在恢复操作中，组装的数据缓存3008可被用于存储安全数据解析器3000的输出。

[0471] 分割共享体缓存3010可以是一个或多个存储器模块，其可被用于存储源自原始数据的解析和分割的数据的多个共享体。在分割操作中，分割共享体缓存3010保存安全数据解析器的输出。在恢复操作中，分割共享体缓存保存安全数据解析器3000的输入。

[0472] 可以理解，能力的其他合适结构可被内置用于安全数据解析器3000。任何额外的特征可以被内置，所示的任何特征可被除去，使其更健壮，使其更不健壮，或可以以任何合适的方式被修改。缓存3008和3010同样只是说明性的，并可以任何合适的方式被修改，除去，或添加。

[0473] 以软件，硬件，或这两者实现的任何合适的模块可由安全数据解析器3000调用或调用安全数据解析器3000。如果需要，甚至内置到安全数据解析器3000中的能力可由一个或多个外部模块取代。如图所示，某些外部模块包括随机数发生器3012，密码反馈密钥发生器3014，散列算法3016，任何一种或多种类型的加密3018，和密钥管理3020。可以理解，这些仅是说明性的外部模块。作为对所示的这些的附加或替代，可以使用任何其他的合适模块。

[0474] 密码反馈密钥发生器3014可在安全数据解析器3000外部为每个安全数据解析器操作生成唯一的密钥或随机数(例如使用随机数发生器3012)，以被用作用于将原始会话密钥大小(例如128，256，512，或1024位的值)扩展到等于待解析和分割的数据的长度的值的操作的种子值。任何合适的算法可被用于密码反馈密钥发生，包括例如AES密码反馈密钥发生算法。

[0475] 为了促进将安全数据解析器3000及其外部模块(即安全数据解析器层3026)集成到应用层3024(例如电子邮件应用，数据库应用，等)中，可使用例如可以利用API功能调用的包裹层(wrapping layer)。可使用任何其他用于促进将安全数据解析器层3026集成到应用层3024中的合适结构。

[0476] 图31示出在写入(例如向存储设备写入)，插入(例如在数据库字段中)，或传输(例

如跨网络)命令在应用层3024中被发出时，图30的结构如何被使用。在步骤3100，待保护的数据被识别，并调用安全数据解析器。调用被传递通过包裹器层3022，其中在步骤3102中，包裹器层3022将在步骤3100所识别的输入数据流式传输到组装的数据缓存3008中。而且在步骤3102，任何合适的共享信息，文件名称，任何其他合适的信息，或其任何组合可被存储(例如，作为包裹器层3022的信息3106)。按照本发明，安全数据处理器3000然后解析并分割作为来自组装的数据缓存3008的输入的数据。其输出数据共享体到分割共享体缓冲器3010中。在步骤3104，包裹器层3022从所存储的信息3106获得任何合适的共享信息(即，在步骤3102由包裹器3022存储的)和共享位置(例如，来自一个或多个配置文件)。包裹器层3022然后适当地写入(例如写到一个或多个存储设备，传输到网络上等)输出共享体(从分割共享体缓存3010获得)。

[0477] 图32说明性地示出当发生读取(例如从存储设备)，选择(例如从数据库字段)，或接收(例如从网络)时，图30的结构可以如何被使用。在步骤3200，待恢复的数据被识别，且从应用层3024调用安全数据解析器3000。在步骤3202，从包裹器层3022获得任何合适的共享信息，并确定共享位置。包裹器层3022加载在步骤3200所识别的数据部分至分割共享体缓存3010。安全数据解析器3000然后按照本发明处理这些共享体(例如，如果四个共享体中仅三个共享体可用，则安全数据解析器3000的冗余能力可被用于只使用这三个共享体来恢复原始数据)。恢复的数据然后被存储在组装的数据缓存3008中。在步骤3204，应用层3022将存储在组装的数据缓存3008中的数据转换为其原始数据格式(如果需要)，并以其原始格式提供原始数据到应用层3024。

[0478] 可以理解，在图31中示出的原始数据的解析和分割以及图32中示出的将数据部分恢复为原始数据仅是说明性的。任何其他合适的过程，组件，或这两者都可被使用以作为所示的这些的补充或替换。

[0479] 图33是按照本发明一个实施例将原始数据解析和分割为两个或更多数据部分的说明性过程的方框图。如图所示，想要被解析并分割的原始数据是纯文本3306(即，使用单词“SUMMIT”作为例子)。可以理解，任何其他类型的数据可按照本发明被解析和分割。生成会话密钥3300。如果会话密钥3300的长度与原始数据3306的长度不兼容，则可生成密码反馈会话密钥3304。

[0480] 在一个合适的方法中，原始数据3306可在解析，分割，或这两者之前被加密。例如，如图33所示，原始数据3306可以与任何合适的值进行异或(XOR)操作(例如与密码反馈会话密钥3304，或与任何其他合适值)。可以理解，任何其他合适的加密技术可被用来取代所示的XOR技术或作为其的补充。还可以理解，虽然图33是以逐字节操作示出的，但是操作也可以在位级别或在任何其他合适的级别执行。进一步可以理解，如果希望，不需要原始数据3306的无论什么任何加密。

[0481] 所得到的加密数据(或如果没用加密则为原始数据)然后被散列化，以确定如何在输出桶(bucket)(例如，在所示例子中有四个)间分割加密(或原始)数据。在所示例子中，散列是按字节发生的，并且是密码反馈会话密钥3304的函数。可以理解这仅是说明性的。如果需要，散列可在位级别执行。散列可以是除了密码反馈会话密钥3304外的任何其他合适值的函数。在另一个合适方法中，不需要使用散列化。相反，可以使用任何其他合适的技术用于分割数据。

[0482] 图34是按照本发明一个实施例的示例性过程流程的方框图，其用于从原始数据3306的两个或多个被解析和分割的部分恢复原始数据3306。该过程涉及根据密码反馈会话密钥3304逆向地对数据部分散列化(即与图33中过程相反)，从而恢复加密的原始数据(或如果在解析和分割之前没有加密则为原始数据)。然后，加密密钥可被用来恢复原始数据(即，在所示的例子中，密码反馈会话密钥3304被用于通过将其与加密数据进行XOR而解密XOR加密)。这样就恢复了原始数据3306。

[0483] 图35示出在图33和34的例子中可以如何执行位分割。散列可被用来确定分割数据的每个字节的位值(例如根据密码反馈会话密钥，根据任何其他合适的值)。可以理解，这仅是一个在位级别实现分割的说明性的方法。任何其他合适的技术都可被使用。

[0484] 可以理解，可以相对于任何合适的散列算法进行这里对散列功能的任何引用。这些例如包括MD5和SHA-1。不同散列算法可被使用不同次数，以及由本发明的不同组件使用。

[0485] 在已经按照上述过程或通过任何其他过程或算法确定了分割点之后，确定哪个数据部分附加每个左段和右段。任何合适的算法可被用于进行该确定。例如，在一个合适的方法中，可建立所有可能的分布的表(例如以用于左段和用于右段的目的地的配对的形式)，其中可通过对会话密钥，密码反馈会话密钥，或任何其他合适的随机或伪随机值中的相应数据使用任何合适的散列函数而确定用于左段和右段中每一个的目的地共享值，这些密钥或值可被生成并扩展到原始数据的大小。例如，可进行随机或伪随机值中相应字节的散列函数。散列函数的输出被用来确定从所有目的地组合的表中选择目的地的哪个配对(即一个用于左段，一个用于右段)。基于该结果，分割数据单元的每个段被附加到由作为散列函数的结果所选择的表值所指示的相应两个共享体。

[0486] 按照本发明，冗余信息可被附加到数据部分，从而允许用少于所有数据部分来恢复原始数据。例如，如果期望四个部分中的两个部分足以恢复数据，则来自共享体的额外数据可相应地被附加到每个共享体中，例如以循环(round-robin)方式(例如，原始数据的大小为4MB，那么共享体1得到其自身的共享以及共享体2和3的共享；共享体2得到其自身的共享和共享体3和4的共享；共享体3得到其自身的共享和共享体4和1的共享；共享体4得到其自身的共享和共享体1和2的共享)。按照本发明，任何这类合适的冗余都可被使用。

[0487] 可以理解，按照本发明，任何其他合适的解析和分割方法可被用于从原始数据集生成数据部分。例如，解析和分割可逐位随机或伪随机地被处理。随机或伪随机值可被使用(例如会话密钥，密码反馈会话密钥，等)，因而对于原始数据中的每个位，对随机或伪随机值中相应数据的散列函数结果可指示哪个共享体附加相应位。在一个合适的方法中，随机或伪随机值可被生成为，或被扩展到原始数据的大小的8倍，从而相对于原始数据的每个位，散列函数可对随机或伪随机值的相应字节执行。按照本发明，可使用任何其他合适的逐位解析和分割数据的算法。进一步可以理解，按照本发明，冗余数据可以例如前面所述的方式被附加到数据共享体。

[0488] 在一种合适方法中，解析和分割不必是随机或伪随机的。相反，可使用用于解析和分割数据的任何合适的判断算法。例如，可以使用将原始数据分解为连续共享体作为解析和分割算法。另一个例子是逐位解析和分割原始数据，相续地以循环方式将每个相应位附加到数据共享体。可以进一步理解，按照本发明，冗余数据可以上述方式被附加到数据共享体。

[0489] 在本发明的一个实施例中，在安全数据解析器生成原始数据的多个部分之后，为了恢复原始数据，某一个或多个所生成的部分是强制性的。例如，如果其中一个部分被用作鉴权共享体(例如在物理权标设备上保存)，以及如果安全数据解析器的容错特征正被使用(即，少于所有部分是恢复原始数据所必须的)，则即使安全数据解析器可能有权访问原始数据的足够数目的部分以恢复原始数据，这也可能在恢复原始数据之前要求存储在物理权标设备上的鉴权共享体。可以理解，例如基于应用，数据类型，用户，任何其他合适的因子，或其任何组合，任何数目和类型的特定共享体可能被要求。

[0490] 在一个合适的方法中，安全数据解析器或安全数据解析器的某外部组件可加密原始数据的一个或多个部分。可能要求提供和解密加密的部分，以便恢复原始数据。不同的加密部分可以不同的加密密钥被加密。例如，该特征可被用于实现更安全的“两人规则”，因而第一用户需要具有利用第一加密密钥加密的特定共享体，而第二用户需要具有利用第二加密密钥加密的特定共享体。为了访问原始数据，这两个用户需要具有它们各自的加密密钥，并提供他们各自的原始数据的部分。在一个合适方法中，公钥可被用来加密一个或多个数据部分，这些数据部分可能是恢复原始数据所要求的强制共享体。然后，私钥可被用来解密共享体，以便被用于恢复原始数据。

[0491] 可使用任何这样的利用强制共享体的合适模式，其中少于所有共享体被需要以恢复原始数据。

[0492] 在本发明一个合适实施例中，可以随机或伪随机地处理将数据分布到有限数目的数据共享体中，使得从统计的角度看，任何特定数据共享体接收特定数据单元的概率等于任一其余共享体接收该数据单元的概率。结果，每个数据共享体具有近似相等量的数据位。

[0493] 按照本发明的另一个实施例，有限数目的数据共享体中每一个不必具有接收来自原始数据的解析和分割的数据单元的相同概率。相反，某一个或多个共享体可具有较剩余共享体更高或更低的概率。结果，在位大小方面，某些共享体可相对其他共享体更大或更小。例如，在两个共享体的情形中，一个共享体可具有1％的概率接收数据单元，而第二共享体具有99％的概率。因此，一旦安全数据解析器已经在这两个共享体间分布数据单元，则第一共享体应具有约1％的数据，而第二共享体具有约99％的数据。按照本发明，可使用任何合适的概率。

[0494] 可以理解，安全数据解析器可被编程为还按照精确(或近似精确的)百分数来将数据分布到共享体。例如，安全数据解析器可被编程为将80％的数据分布到第一共享体，而将剩余20％的数据分布到第二共享体。

[0495] 按照本发明的另一个实施例，安全数据解析器可生成数据共享体，其中一个或多个数据共享体具有预定的大小。例如，安全数据解析器可将原始数据分割为数据部分，其中一个部分精确为256位。在一个合适方法中，如果不能生成具有必须的大小的数据部分，则安全数据解析器可对该部分进行填充以使其为正确的尺寸。任何合适的尺寸都可被使用。

[0496] 在一个合适的方法中，数据部分的大小可以是加密密钥，分割密钥，任何其他合适密钥，或任何其他合适的数据元素的大小。

[0497] 如前面所讨论的那样，安全数据解析器可在数据解析和分割中使用密钥。为了简单明了，这些密钥在这里应被称为“分割密钥”。例如，前面介绍的会话主密钥是一种分割密钥。而且，如前面所讨论的，分割密钥可在安全数据解析器所生成的数据共享体内被保护。

用于保护分割密钥的任何合适的算法可被用来在数据共享体间保护它们。例如，Shamir算法可被用于保护分割密钥，因而可被用于重构分割密钥的信息被生成并被附加到数据共享体上。按照本发明，可使用任何其他的这样的合适算法。

[0498] 类似地，按照任何合适的算法，诸如Shamir算法，任何合适的加密密钥可在一个或多个数据共享体内被保护。例如，可例如使用Shamir算法或任何其他合适算法保护用来在解析和分割之前加密数据集的加密密钥，用来在解析和分割之后加密数据部分的加密密钥，或这两者。

[0499] 按照本发明一个实施例，全有或全无变换(AoNT:All or Nothing Transform)，诸如全封包变换(Full Package Transform)可被用于通过变换分割密钥，加密密钥，任何其他合适的数据元素，或其任意组合来进一步保护数据。例如，按照本发明，用于在解析和分割之前加密数据集的加密密钥可由AoNT算法被变换。变换后的加密密钥然后可例如按照Shamir算法或任何其他合适的算法被分布在数据共享体间。为了重构加密密钥，加密后的数据集必须被恢复(例如，按照本发明，如果使用冗余，则不必使用所有数据共享体)，以便按照AoNT访问关于变换的必要信息，如本领域技术人员公知的那样。当原始加密密钥被恢复时，其可被用来解密加密后的数据集，以恢复原始数据集。可以理解，本发明的容错特征可与AoNT特征结合使用。也就是，冗余数据可被包括在数据部分中，从而少于所有数据部分对于恢复加密后数据集是必须的。

[0500] 可以理解，AoNT可被应用到用于在解析和分割后加密数据部分的加密密钥，作为解析和分割之前对应于数据集的相应加密密钥的加密和AoNT的替换或补充。类似地，AoNT可被应用于分割密钥。

[0501] 在本发明的一个实施例中，按照本发明所用的加密密钥，分割密钥，或这两者可进一步例如利用工作组密钥被加密，以便为保护的数据集提供额外的安全度。

[0502] 在本发明的一个实施例中，可提供审计模块，其只要安全数据解析器被调用来分割数据就跟踪。

[0503] 图36示出按照本发明使用安全数据解析器组件的可能选择3600。每个选项组合在下面被概述的并以图36中的适当的步骤号被标记。安全数据解析器本质上可以是模块化的，从而允许在图36所示的每个功能块内使用任何已知的算法。例如，其他密钥分割(例如，保密共享)算法，诸如Blakely可被用来取代Shamir，或AES加密可由其他已知的加密算法取代，诸如三重DES。图36的例子中所示的标签仅描述用在本发明一个实施例中的算法的一种可能的组合。可以理解，任何合适算法或算法组合可被用来取代标记的算法。

[0504] 1)3610，3612，3614，3615，3616，3617，3618，3619

[0505] 在步骤3610使用先前加密的数据，数据可最终被分割为预定数目的共享体。如果分割算法要求密钥，则分割加密密钥可在步骤3612处用密码安全伪随机数发生器生成。分割加密密码可以可选地当在步骤3615被密钥分割成具有容错的预定数目的共享体之前，在步骤3614利用全有或全无变换(AoNT)被变换为变换分割密钥。然后，在步骤3616，数据可被分割为预定数目的共享体。在步骤3617处可以使用容错方案，以允许从少于全部共享体重新生成数据。一旦创建了共享体，则在步骤3618处，鉴权/完整性信息可被嵌入到共享体中。每个共享体可以可选地在步骤3619处被后加密。

[0506] 2)3111，3612，3614，3615，3616，3617，3618，3619

[0507] 在某些实施例中，可利用用户或外部系统所提供的加密密钥加密输入数据。外部密钥在步骤3611被提供。例如，密钥可从外部密钥存储装置提供。如果分割算法要求密钥，则可在步骤3612处利用密码安全伪随机数发生器生成分割加密密钥。分割密码可以可选地当在步骤3615处被密钥分割成预定数目的具有容错的共享体之前，在步骤3614处利用全有或全无变换(AoNT)被变换为变换分割密钥。然后，在步骤3616，数据被分割为预定数目的共享体。在步骤3617，可以使用容错方案，以允许从少于全部共享体重新生成数据。一旦创建了共享体，则在步骤3618，鉴权/完整性信息可被嵌入到共享体中。每个共享体可以可选地在步骤3619处被后加密。

[0508] 3)3612,3613,3614,3615,3612,3614,3615,3616,3617,3618,3619

[0509] 在某些实施例中，可在步骤3612处利用密码安全伪随机数发生器生成加密密钥，以变换数据。利用所生成的密钥加密数据可发生在步骤3613。加密密钥可以可选地在步骤3614利用全有或全无变换(AoNT)被转换为变换加密密钥。然后在步骤3615，变换加密密钥和/或所生成的加密密钥可被分割成预定数目的具有容错的共享体。如果分割算法要求密钥，则利用密码安全伪随机数发生器生成分割加密密钥可在步骤3612发生。在步骤3615被密钥分割为预定数目的具有容错的共享体之前，分割密钥可以可选地在步骤3614利用全有或全无变换(AoNT)被变换为变换分割加密密钥。然后在步骤3616，数据可被分割为预定数目的共享体。在步骤3617可以使用容错方案，以允许从少于全部共享体重新生成数据。一旦创建了共享体，则在步骤3618，鉴权/完整性信息可被嵌入到共享体中。每个共享体然后可以可选地在步骤3619处被后加密。

[0510] 4)3612,3614,3615,3616,3617,3618,3619

[0511] 在某些实施例中，数据可被分割为预定数目的共享体。如果分割算法要求密钥，则可在步骤3162发生利用密码保护伪随机数发生器生成分割加密密钥。在步骤3615中被密钥分割为预定数目的具有容错的共享体之前，分割密钥可以可选地在步骤3614处利用全有或全无变换(AoNT)被转换为变换分割密钥。然后，数据可在步骤3616处被分割。可以在步骤3617处使用容错方案，以允许从少于全部共享体重新生成数据。一旦创建了共享体，则在步骤3618处，鉴权/完整性信息可被嵌入到共享体中。每个共享体可以可选地在步骤3619处被后加密。

[0512] 虽然在本发明的一些实施例中优选使用上面四个选项组合，但特征，步骤，或选项的任何其他合适的组合可在其他实施例中与安全数据解析器一起被使用。

[0513] 安全数据解析器可通过促进物理分离而提供灵活的数据保护。数据可首先被加密，然后被分割为具有“n中m”容错的共享体。这允许在少于全部共享体可用时再生原始信息。例如，某些共享体可能在传输中被丢失或破坏。丢失或破坏的共享体可通过容错或附加到共享体的完整性信息而被再创建，如下面更详细的讨论。

[0514] 为了创建共享体，安全数据解析器可选地利用大量密钥。这些密钥可包括一个或多个以下项：

[0515] 预加密密钥：当选择共享体的预加密时，外部密钥可被传输到安全数据解析器。该密钥可被生成并被外部地存储在密钥存储器中(或其他位置)，并可被用于可选地在数据分割之前加密数据。

[0516] 分割加密密钥：该密钥可被内部地生成并由安全数据解析器用来在分割之前加密

数据。该密钥然后可利用密钥分割算法而被安全地存储在共享体内。

[0517] 分割会话密钥：该密钥不与加密算法一起使用；相反，其可被用于在选择随机分割时键入(key)数据分区算法(data partitioning algorithm)。在使用随机分割时，分割会话密钥可被内部地生成并由安全数据解析器用来将数据划分为共享体。该密钥可利用密钥分割算法而被安全地存储在共享体内。

[0518] 后加密密钥：当共享体的后加密被选择时，外部密钥可被传输到安全数据解析器并被用来后加密各个共享体。该密钥可被生成并外部地存储在密钥存储器或其他合适位置中。

[0519] 在某些实施例中，当利用安全数据解析器以该方式保护数据时，信息仅可在所有要求的共享体和外部加密密钥存在的情况下被重组。

[0520] 图37示出某些实施例中使用本发明的安全数据解析器的总过程3700。如上所述，安全数据解析器3706的两个非常合适的功能可以包括加密3702和备份3704。类似地，在某些实施例中，安全数据解析器3706可与RAID或备份系统或硬件或软件加密引擎集成。

[0521] 与安全数据解析器3706相关联的主要密钥过程可包括预加密过程3708，加密/变换过程3710，密钥保护过程3712，解析/分布过程3714，容错过程3716，共享鉴权过程3716，和后加密过程3720中的一个或多个。这些过程可以几种合适的顺序或组合被执行，如图36详细示出。所用过程的组合和顺序可取决于特定的应用或使用，所期望的安全级别，是否期望可选的预加密，后加密或两者，期望的冗余，下层或集成系统的能力或性能，或任何其他合适的因子或因子组合。

[0522] 说明性过程3700的输出可以是两个或多个共享体3722。如上所述，在某些实施例中，数据可被随机(或伪随机)地分布到这些共享体的每个中。在其他实施例中，可使用确定性算法(或随机，伪随机和确定性算法的某种合适的组合)。

[0523] 除了信息资产的单独保护，有时还要求在不同用户组或利益体之间共享信息。于是可能需要在该用户组内控制对各共享体的访问或在那些用户之间共享仅允许组成员重组共享体的凭证。为了该目的，在本发明的某些实施例中，工作组密钥可被部署给组成员。工作组密钥应被保护并保持机密，因为危及工作组密钥可能潜在地允许组外人员访问信息。用于工作组密钥部署和保护的某些系统和方法在下面讨论。

[0524] 工作组密钥概念允许通过加密存储在共享体内的密钥信息而增强信息资产的保护。一旦执行该操作，即使所有要求的共享体和外部密钥被公开，袭击者也不能在不访问工作组密钥的情况下重新建立信息。

[0525] 图38示出在共享体内存储密钥和数据成分的方框图3800。在图3800的例子中，略去可选的预加密和后加密步骤，虽然这些步骤可被包括在其他实施例中。

[0526] 分割数据的简化过程包括在加密步骤3802利用加密密钥3804加密数据。然后，按照本发明，加密密钥3804的部分可被分割和存储在共享体3810内。分割加密密钥3806的部分也可被存储在共享体3810内。使用分割加密密钥，数据3808然后被分割并被存储在共享体3810内。

[0527] 为了恢复数据，按照本发明，可检索和恢复分割加密密钥3806。然后分割操作可以被反向处理以恢复密文。加密密钥3804也可被检索和恢复，且密文然后可利用加密密钥被解密。

[0528] 当利用工作组密钥时，上面的过程可稍微改变，从而以工作组密钥保护加密密钥。加密密钥于是可在被存储在共享体内之前以工作组密钥被加密。修改的步骤在图39所示的方框图3900中示出。

[0529] 简化的用工作组密钥分割数据的过程包括首先在步骤3902用加密密钥加密数据。加密密钥然后可在步骤3904以工作组密钥被加密。以工作组密钥加密的加密密钥然后可被分割为部分并以共享体3912被存储。分割密钥3908也可被分割并存储在共享体3912中。最后，数据3910的部分利用分割密钥3908而被分割并存储在共享体3912中。

[0530] 为了恢复数据，按照本发明，分割密钥可被检索和恢复。按照本发明，然后分割操作可以被反转以恢复密文。加密密钥(其以工作组密钥被加密)可被检索和恢复。然后，加密密钥可利用工作组密钥被解密。最后，密文可以利加密密钥被解密。

[0531] 有几种安全方法用于部署和保护工作组密钥。选择哪种方法来用于特定的应用取决于大量因子。这些因子可包括所要求的安全级别，成本，便利，和工作组内用户的数目。某些实施例中的某些通用的技术如下：

[0532] 基于硬件的密钥存储

[0533] 基于硬件的解决方案通常为加密系统中加密/解密密钥的安全性提供最强的保证。基于硬件的存储解决方案的例子包括抗窜改密钥权标设备，其在便携式设备(例如智能卡/软件狗)，或非便携式密钥存储外设中存储密钥。这些设备被设计来防止密钥材料被未授权方容易地复制。密钥可由授信方生成并被分配给用户，或在硬件内被生成。此外，许多密钥存储系统提供多因子鉴权，其中密钥的使用要求访问物理对象(权标)和通关语(passphrase)或生物统计特征。

[0534] 基于软件的密钥存储

[0535] 虽然专用的基于硬件的存储对于高安全性部署或应用是理想的，但可选择其他部署来直接在本地硬件(例如，磁盘，RAM或非易失性RAM存储装置，诸如USB设备)上存储密钥。这对于内部人攻击，或攻击者能够直接访问加密机器的情形提供了较低的保护水平。

[0536] 为了保护磁盘上的密钥，基于软件的密钥管理通常通过将密钥以从其他鉴权度量的组合所获得的密钥加密形式存储而保护密钥，这些鉴权度量包括：口令和通关语，其他密钥的提供(例如来自基于硬件的解决方案)，生物统计特征，或前述的任何合适组合。这样的技术所提供的安全水平可以从某些操作系统(例如MS Windows和Linux)所提供的相对弱的密钥保护机理到利用多因子鉴权所实现的更健壮的解决方案。

[0537] 本发明的安全数据解析器可有利地被用在大量应用和技术中。例如，电子邮件系统，RAID系统，视频广播系统，数据库系统，或任何其他合适的系统可在任何合适的级集成安全数据解析器。如前面的讨论，可以理解，也可集成安全数据解析器用于任何类型的通过任何传输介质移动的数据的保护和容错，这些传输介质例如包括有线，无线，或物理传输介质。作为一个例子，IP语音通信(VoIP)应用可利用本发明的安全数据解析器来解决涉及IP语音通信中常见的回声和延迟的问题。使用容错可消除网络对再尝试被丢失的分组的需求，这保证了分组交付，即使存在预定数目的共享体丢失。也可有效地以最小的延迟和缓存“在处理中”分割和恢复数据分组(例如网络分组)，从而得到对不同类型的移动中数据的全面解决方案。安全数据解析器可作用于网络数据分组、网络语音分组、文件系统数据块、或任何其他合适的信息单元。除了与IP语音通信应用集成之外，安全数据解析器也可与文件

共享应用(例如对等文件共享应用),视频广播应用,电子表决或轮询应用(这可执行电子表决协议和盲签名,诸如Sensus协议),电子邮件应用,或任何其他可能要求或需要安全通信的网络应用集成。

[0538] 在某些实施例中,移动网络数据的支持可由本发明的安全数据解析器以两个不同阶段提供:头文件生成阶段和数据划分阶段。简化的头文件生成过程4000和简化的数据划分过程4010分别在图40A和图40B中示出。这两个过程中的一个或二者可在网络分组,文件系统块,或任何其他合适的信息上执行。

[0539] 在某些实施例中,头文件生成过程4000可在网络分组流启动时被执行一次。在步骤4002,可生成随机(或伪随机)分割加密密钥K。然后,在AES密钥包裹(wrap)步骤4004,分割加密密钥K被可选地加密(例如利用上述工作组密钥)。虽然AES密钥包裹可被用在某些实施例中,但是在其他实施例中可使用任何合适的密钥加密或密钥包裹算法。AES密钥包裹步骤4004可对整个分割加密密钥K进行操作,或分割加密密钥可被解析为几个块(例如64位块)。如果需要,AES密钥包裹步骤4004然后可对分割加密密钥的块进行操作。

[0540] 在步骤4006,保密共享算法(例如Shamir)可被用来将加密密钥K分割为密钥共享体。每个密钥共享体然后可被嵌入到其中一个输出共享体(例如在共享头文件中)。最后,共享完整块和(可选的)后鉴权标签(例如MAC)可被附加到每个共享体的头文件块。每个头文件块可被设计为匹配在单个数据分组中。

[0541] 在头文件生成完成(例如利用简化的头文件生成过程4000)后,安全数据解析器可利用简化的数据分割过程4010进入数据划分阶段。在步骤4012,流中每个流入的数据分组或数据块利用分割加密密钥K被加密。在步骤4014,共享完整性信息(例如散列值H)可在从步骤4012所得到的密文上被计算。例如,可计算SHA—256散列值。在步骤4106,按照本发明,数据分组或数据块然后可利用上述数据分割算法中的一个而被划分为两个或多个数据共享体。在某些实施例中,数据分组或数据块可被分割,因此每个数据共享体包含加密数据分组或数据块的基本上随机分布。完整性信息(例如散列值H)然后可被附加到每个数据共享体。在某些实施例中,可选的后鉴权标签(例如MAC)也可被计算并被附加到每个数据共享体。

[0542] 每个数据共享体可包括可能对于正确重构数据块或数据分组必须的元数据。该信息可被包括在共享头文件中。元数据可包括诸如密码密钥共享体,密钥标识,共享体现时(nonce),签名/MAC值,和完整性块这样的信息。为了最大化带宽效率,元数据可以紧凑二进制格式被存储。

[0543] 例如,在某些实施例中,共享头文件包括明文头文件组块(header chunk),其不被加密并且可包括诸如Shamir密钥共享体,每会话现时(per-session nonce),每共享体现时(per-share nonce),密钥识别符(例如工作组密钥识别符和后鉴权密钥识别符)。共享头文件也可包括以分割加密密钥加密的加密后头文件组块。可包括用于任意数目的先前块(例如前两块)的完整性检验的完整性头文件组块也可被包括在头文件中。任何其他合适的值或信息也可被包括在共享头文件中。

[0544] 如图41的说明性共享格式4100所示,头文件块4102可与两个或更多输出块4104关联。每个头文件块,诸如头文件块4102可被设计成适配在单个网络数据分组中。在某些实施例中,在头文件块4102从第一位置传输到第二位置后,然后可传输输出块。可替换地,头文

件块4102和输出块4104可同时并行地被传输。传输可发生在一个或多个类似或不同的通信路径上。

[0545] 每个输出块可包括数据部分4106和完整性/真实性部分4108。如上所述，每个数据共享体可利用包括被加密的预划分数据的共享完整性信息(例如SHA-256散列值)的共享完整性部分而被保护。为了在恢复时验证输出块的完整性，安全数据解析器可比较每个共享体的共享完整性块，然后反转分割算法。然后可以相对于共享散列值验证被恢复数据的散列值。

[0546] 虽然上面说明了安全数据解析器的某些普通应用，应该理解，本发明可预任何网络应用程序集成以便增加安全性，容错性，匿名性，或前述任何合适组合。

[0547] 另外，本领域技术人员可显然看出其他组合，添加，替代和修改。因此，本发明不是要限制在优选实施例中，而是由权利要求界定。

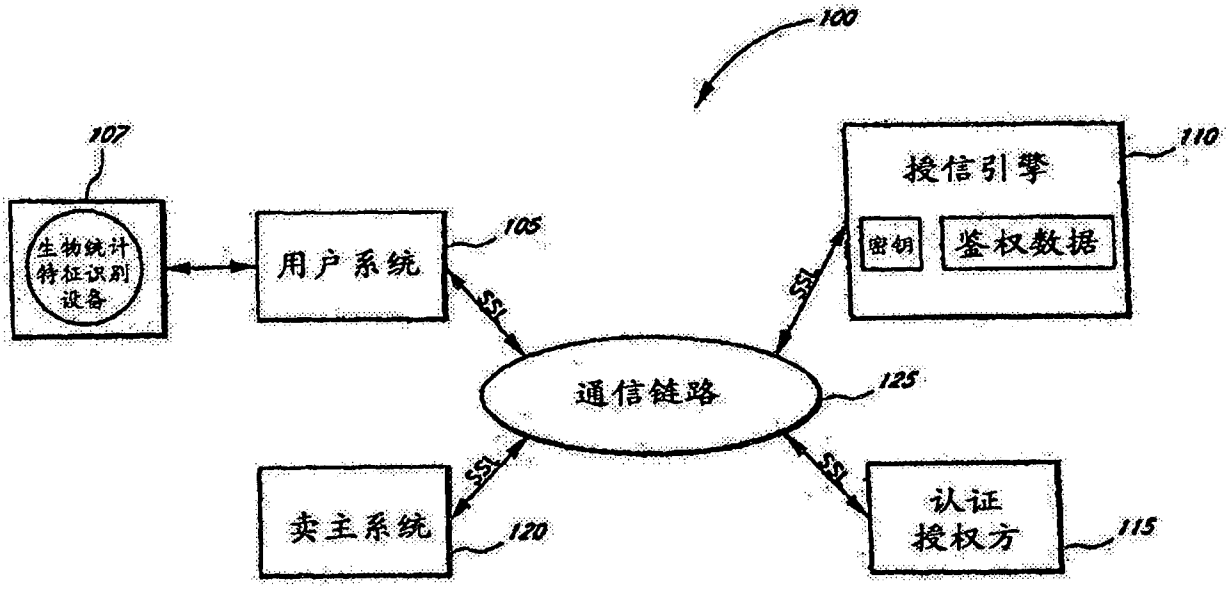

100
107
生物统计特征识别设备
用户系统
105
SSL
授信引擎
110
密钥
鉴权数据
通信链路
125
卖主系统
120
认证授权方
115

图1

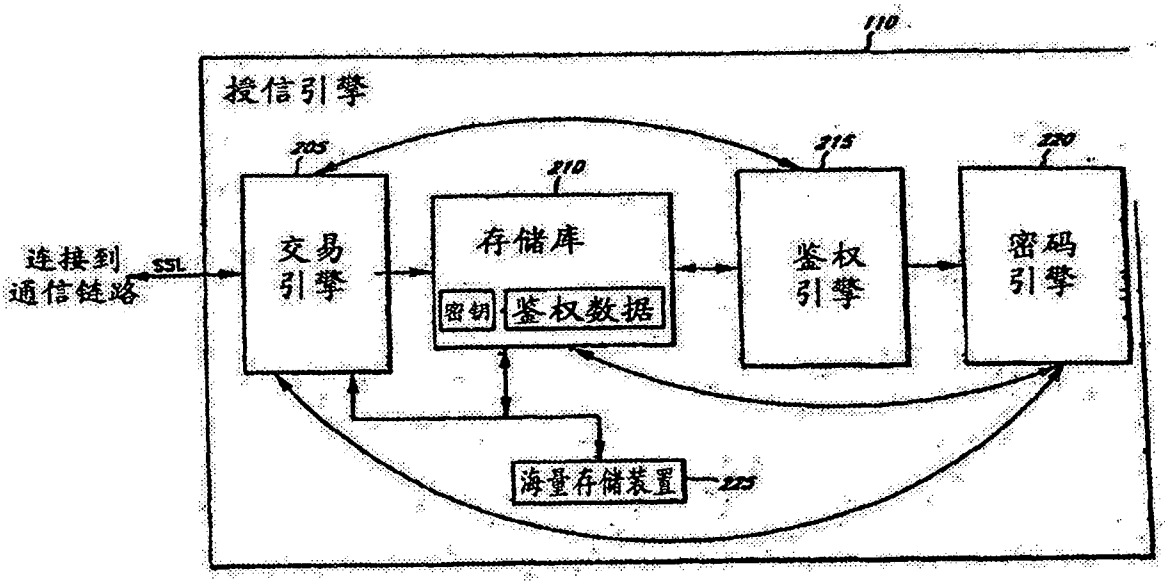

110
授信引擎
205
210
215
220
连接到通信链路
SSL
交易引擎
存储库
密钥
鉴权数据
鉴权引擎
密码引擎
海量存储装置
225

图2

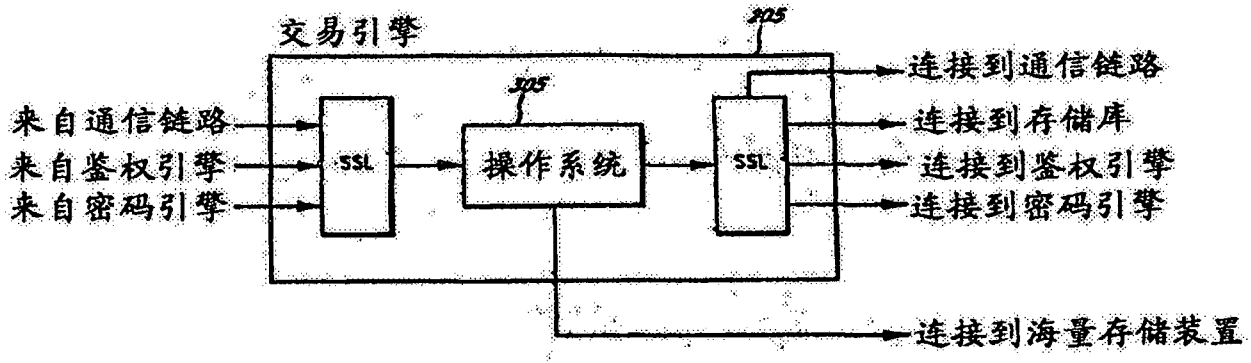

交易引擎
305
305
来自通信链路
来自鉴权引擎
来自密码引擎
SSL
操作系统
SSL
连接到通信链路
连接到存储库
连接到鉴权引擎
连接到密码引擎
连接到海量存储装置

图3

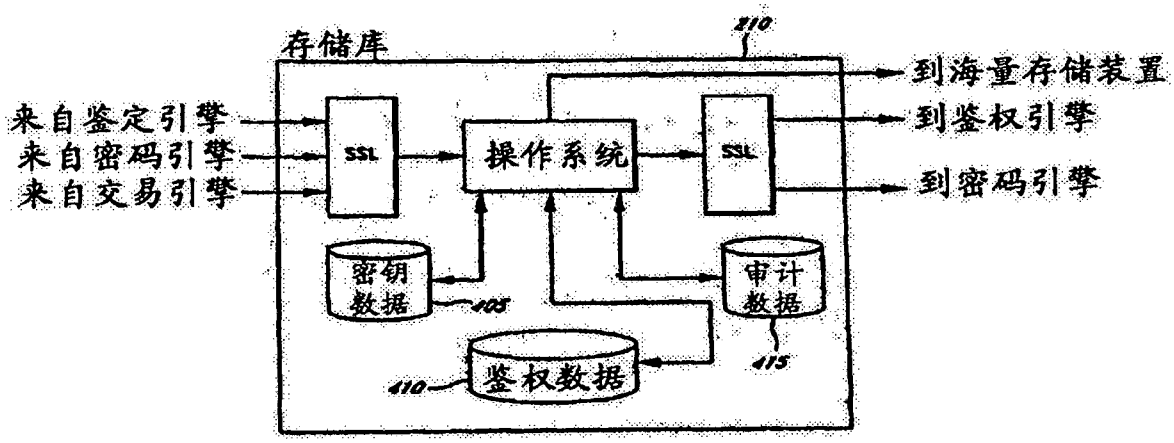

存储库
210
来自鉴定引擎
来自密码引擎
来自交易引擎
SSL
操作系统
SSL
到海量存储装置
到鉴权引擎
到密码引擎
密钥数据
405
审计数据
415
410
鉴权数据

图4

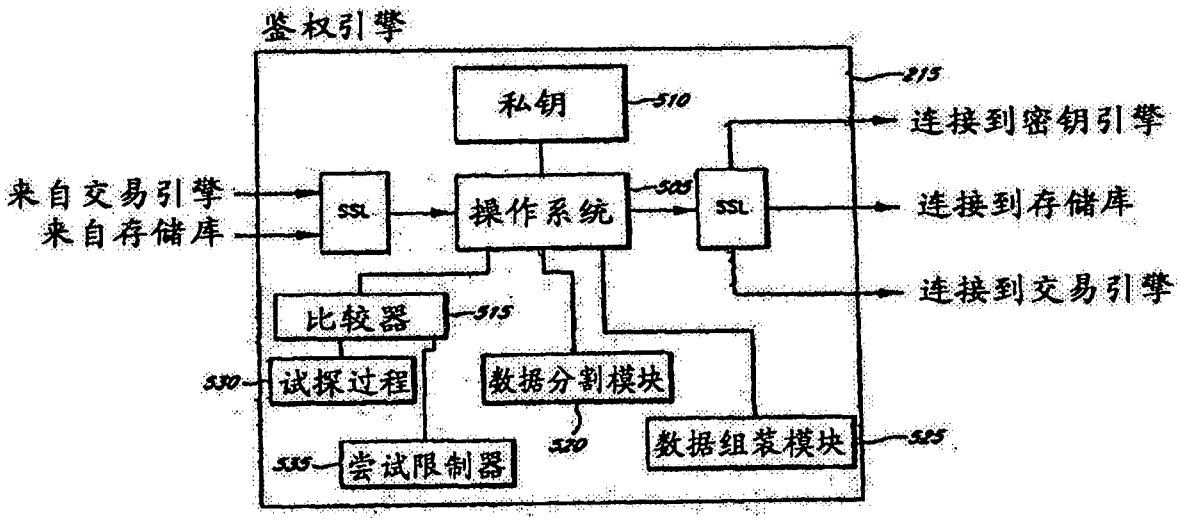

鉴权引擎
215
私钥
510
来自交易引擎
来自存储库
SSL
操作系统
505
SSL
连接到密钥引擎
连接到存储库
连接到交易引擎
比较器
515
530
试探过程
数据分割模块
520
数据组装模块
525
535
尝试限制器

图5

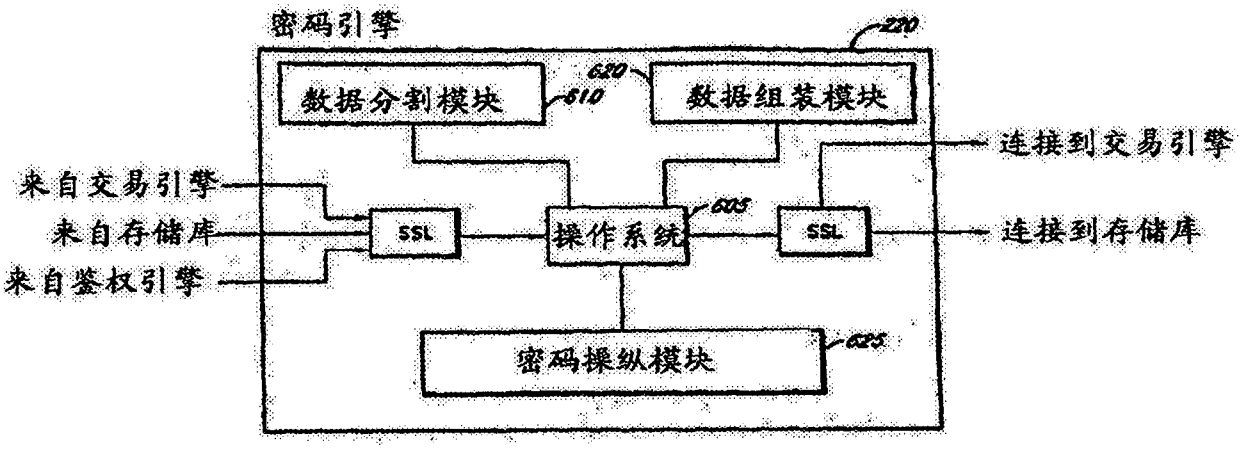

密码引擎
220
数据分割模块
610
620
数据组装模块
连接到交易引擎
来自交易引擎
来自存储库
来自鉴权引擎
SSL
操作系统
605
SSL
连接到存储库
密码操纵模块
625

图6

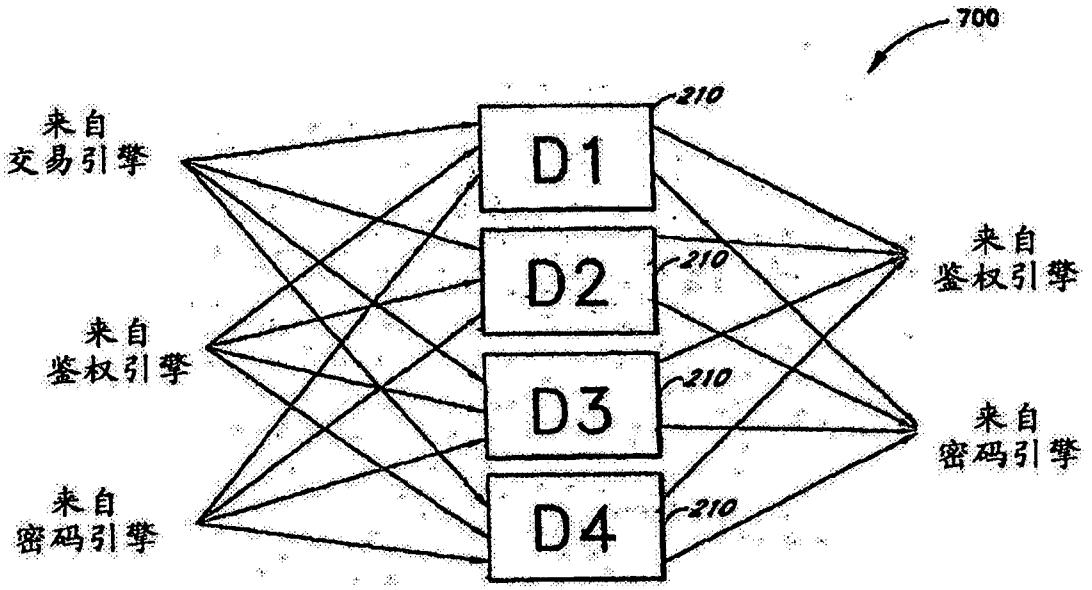

700
来自
交易引擎
来自
鉴权引擎
来自
密码引擎
D1
D2
D3
D4
210
210
210
210
来自
鉴权引擎
来自
密码引擎

图7

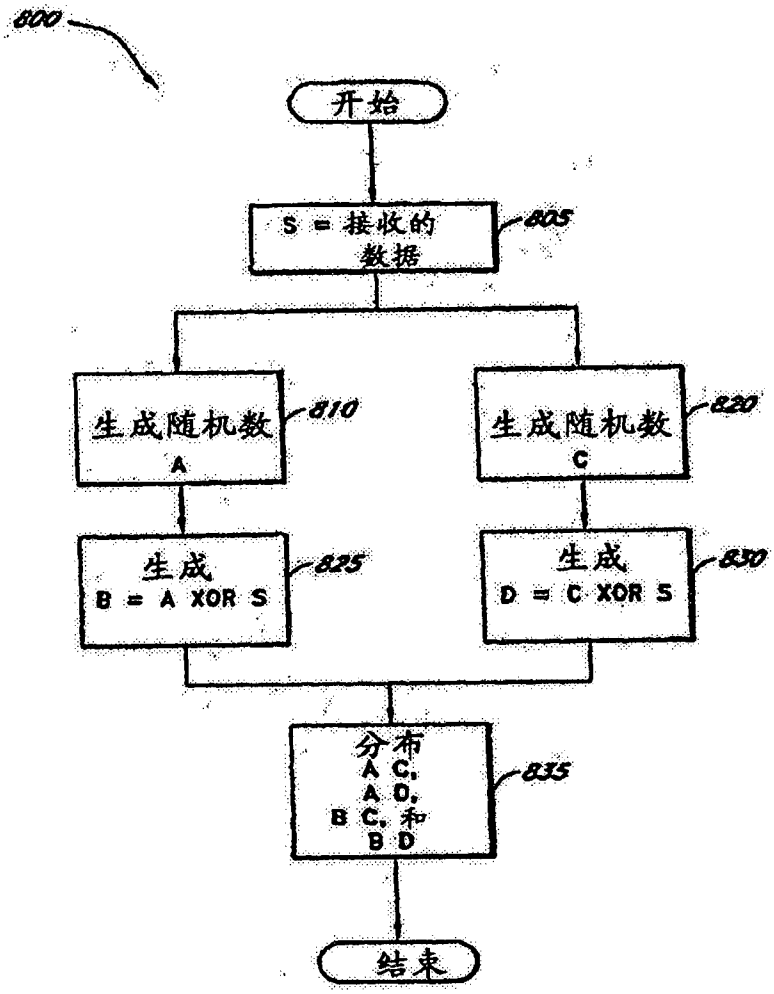

600
开始
S = 接收的数据
805
生成随机数 A
810
生成随机数 C
820
生成 B = A XOR S
825
生成 D = C XOR S
830
分布 A C, A D, B C, B D 和
835
结束

图8

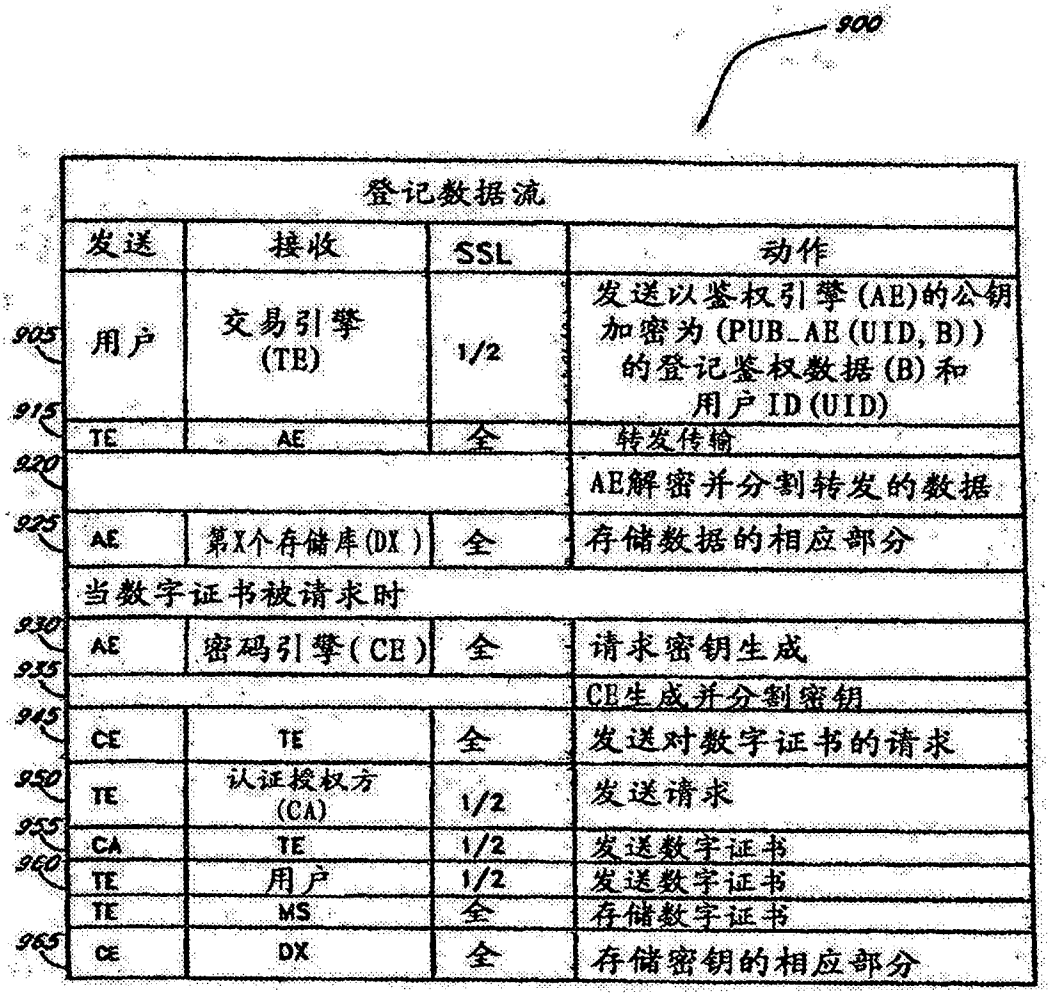

900
登记数据流
发送
接收
SSL
动作
905
用户
交易引擎(TE)
1/2
发送以鉴权引擎(AE)的公钥加密为(PUB_AE(UID,B))的登记鉴权数据(B)和用户ID(UID)
915
TE
AE
全
转发传输
920
AE解密并分割转发的数据
925
AE
第X个存储库(DX)
全
存储数据的相应部分
当数字证书被请求时
930
AE
密码引擎(CE)
全
请求密钥生成
935
CE生成并分割密钥
945
CE
TE
全
发送对数字证书的请求
950
TE
认证授权方(CA)
1/2
发送请求
955
CA
TE
1/2
发送数字证书
960
TE
用户
1/2
发送数字证书
TE
MS
全
存储数字证书
965
CE
DX
全
存储密钥的相应部分

图9(面A)

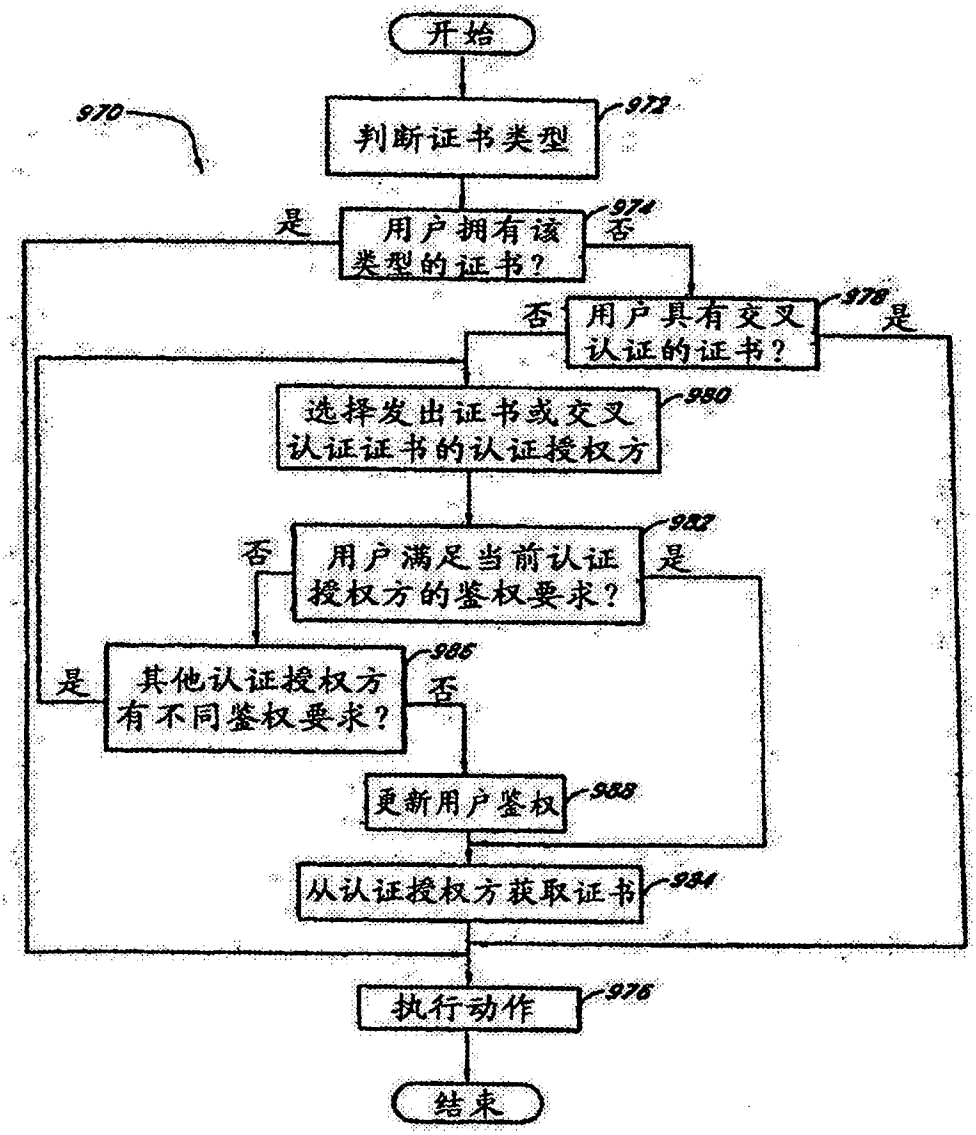
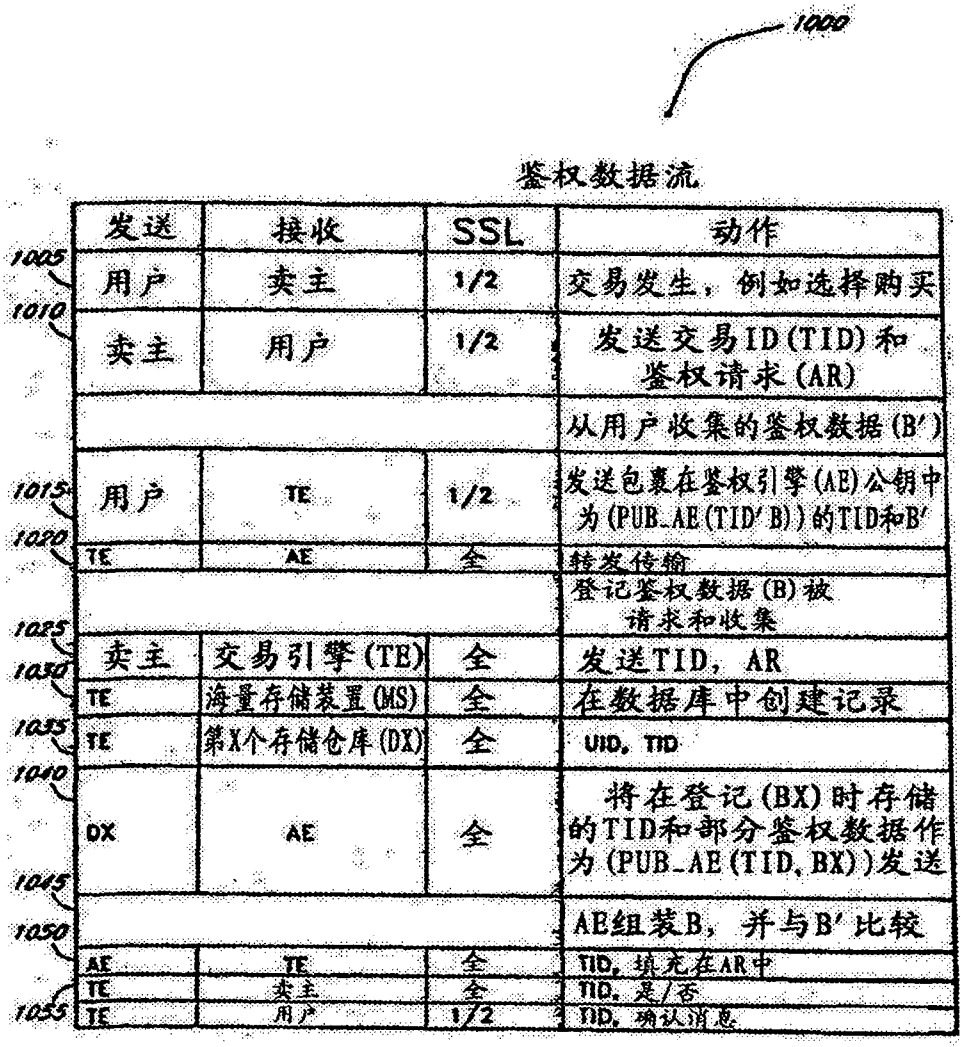

开始
970
判断证书类型
972
是
用户拥有该类型的证书？
974
否
否
用户具有交叉认证的证书？
978
是
选择发出证书或交叉认证证书的认证授权方
980
否
用户满足当前认证授权方的鉴权要求？
982
是
是
其他认证授权方有不同鉴权要求？
986
否
更新用户鉴权
988
从认证授权方获取证书
984
执行动作
976
结束

图9(面B)



发送	接收	SSL	动作
用户	卖主	1/2	交易发生，例如选择购买
卖主	用户	1/2	发送交易ID(TID)和鉴权请求(AR)
			从用户收集的鉴权数据(B′)
用户	TE	1/2	发送包裹在鉴权引擎(AE)公钥中为(PUB_AE(TID′B))的TID和B′
TE	AE	全	转发传输
			登记鉴权数据(B)被请求和收集
卖主	交易引擎(TE)	全	发送TID，AR
TE	海量存储装置(MS)	全	在数据库中创建记录
TE	第X个存储仓库(DX)	全	UID，TID
DX	AE	全	将在登记(BX)时存储的TID和部分鉴权数据作为(PUB_AE(TID,BX))发送
			AE组装B，并与B′比较
AE	TE	全	TID，填充在AR中
TE	卖主	全	TID，是/否
TE	用户	1/2	TID，确认消息

图10

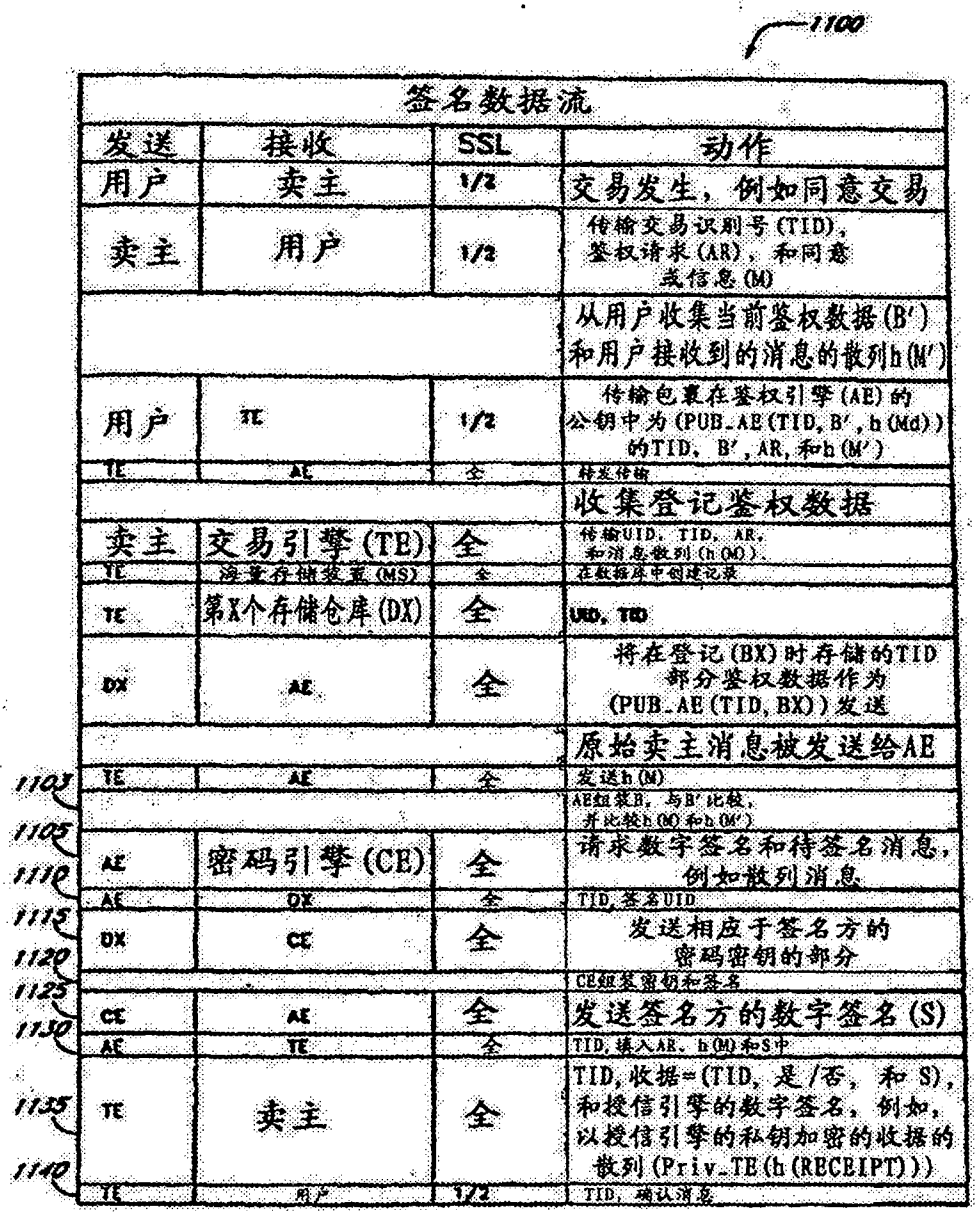

1100
签名数据流
发送 接收 SSL 动作
用户 卖主 1/2 交易发生，例如同意交易
卖主 用户 1/2 传输交易识别号(TID)，鉴权请求(AR)，和同意或信息(M)
从用户收集当前鉴权数据(B')和用户接收到的消息的散列h(M')
用户 TE 1/2 传输包裹在鉴权引擎(AE)的公钥中为(PUB_AE(TID, B', h(Md))的TID, B', AR, 和h(M')
TE AE 全 转发传输
收集登记鉴权数据
卖主 交易引擎(TE) 全 传输UID, TID, AR, 和消息散列(h(M))
TE 海量存储装置(MS) 全 在数据库中创建记录
TE 第X个存储仓库(DX) 全 UID, TID
DX AE 全 将在登记(BX)时存储的TID部分鉴权数据作为(PUB_AE(TID, BX))发送
原始卖主消息被发送给AE
1103 TE AE 全 发送h(M)
AE组装B, 与B'比较, 并比较h(M)和h(M')
1105 AE 密码引擎(CE) 全 请求数字签名和待签名消息，例如散列消息
1110 AE DX 全 TID, 签名UID
1115 DX CE 全 发送相应于签名方的密码密钥的部分
1120 CE组装密钥和签名
1125 CE AE 全 发送签名方的数字签名(S)
1130 AE TE 全 TID, 插入AR, h(M)和S中
1135 TE 卖主 全 TID, 收据=(TID, 是/否, 和S), 和授信引擎的数字签名，例如，以授信引擎的私钥加密的收据的散列(Priv_TE(h(RECEIPT)))
1140 TE 用户 1/2 TID, 确认消息

图11

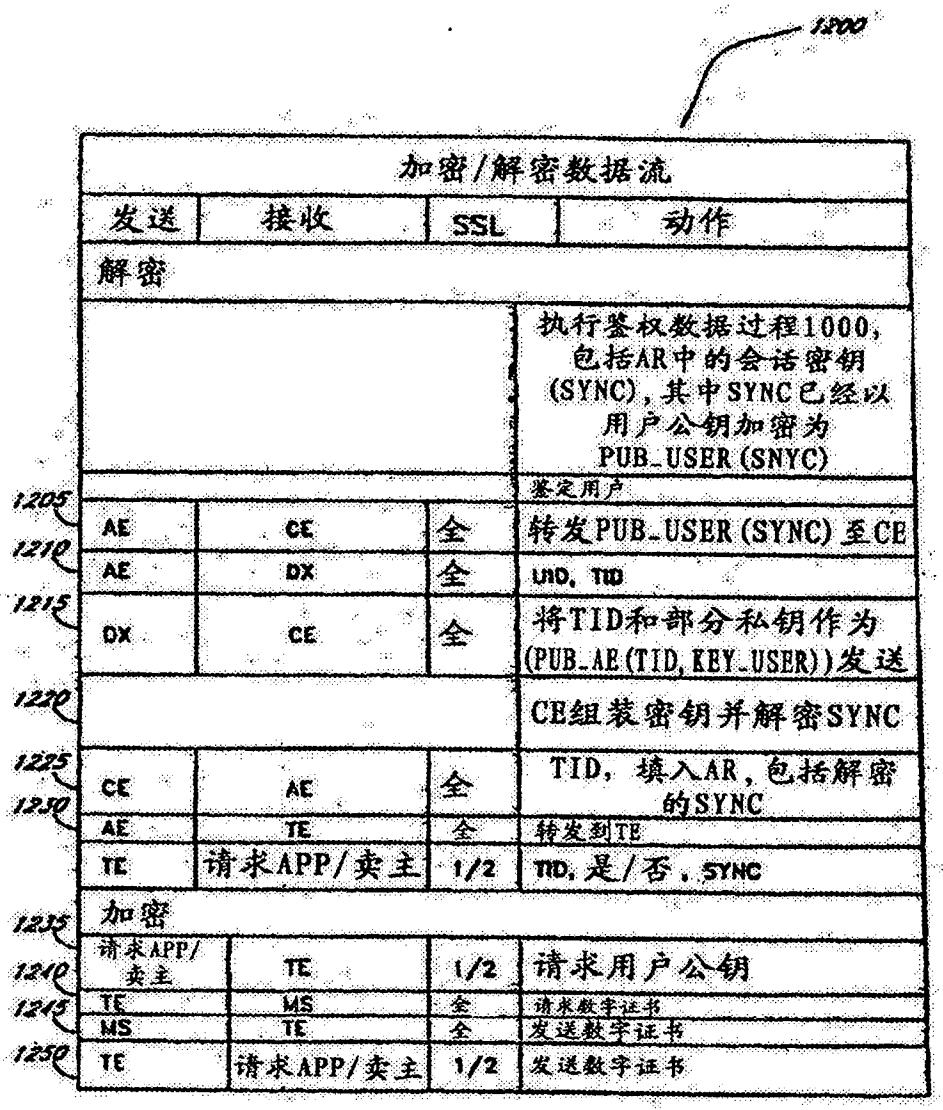

1000
加密/解密数据流
发送
接收
SSL
动作
解密
执行鉴权数据过程1000，包括AR中的会话密钥(SYNC)，其中SYNC已经以用户公钥加密为PUB_USER(SNYC)
鉴定用户
1205
AE
CE
全
转发PUB_USER(SYNC)至CE
1210
AE
DX
全
UID，TID
1215
DX
CE
全
将TID和部分私钥作为(PUB_AE(TID,KEY_USER))发送
1220
CE组装密钥并解密SYNC
1225
CE
AE
全
TID，填入AR，包括解密的SYNC
1230
AE
TE
全
转发到TE
TE
请求APP/卖主
1/2
TID，是/否，SYNC
1235
加密
1240
请求APP/卖主
TE
1/2
请求用户公钥
1245
TE
MS
全
请求数字证书
MS
TE
全
发送数字证书
1250
TE
请求APP/卖主
1/2
发送数字证书

图12

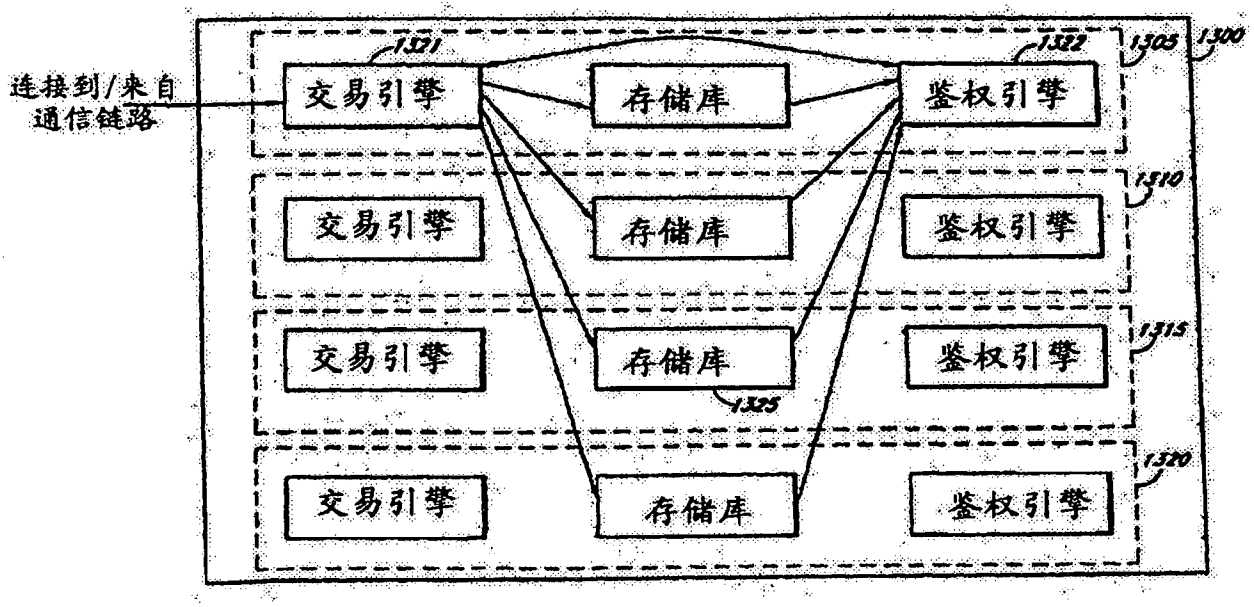

连接到/来自
通信链路
交易引擎
存储库
鉴权引擎
1321
1322
1305
1300
1310
1315
1325
1320

图13

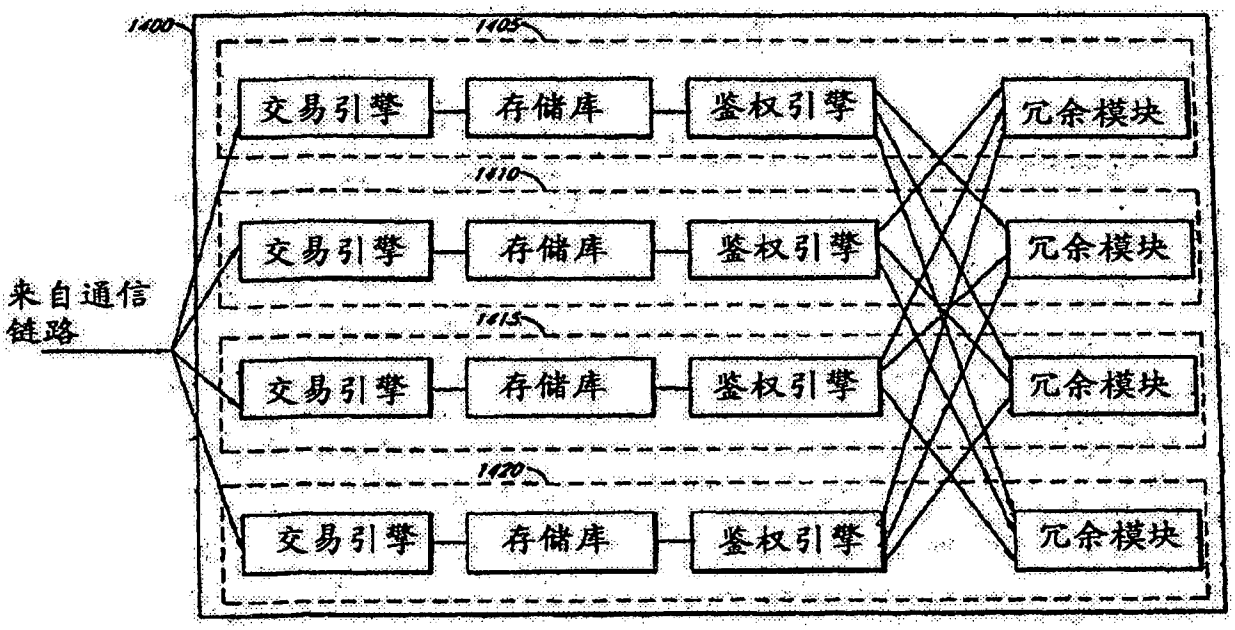

1400
1405
交易引擎
存储库
鉴权引擎
冗余模块
1410
1415
1420
来自通信
链路

图14

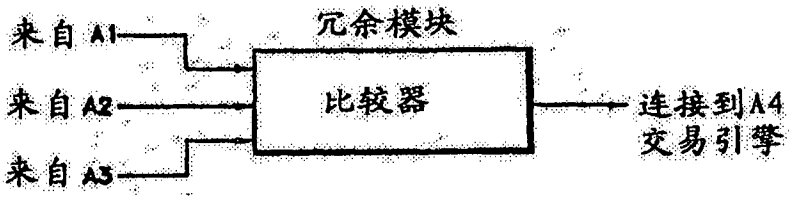

冗余模块
来自 A1
来自 A2
来自 A3
比较器
连接到A4
交易引擎

图15

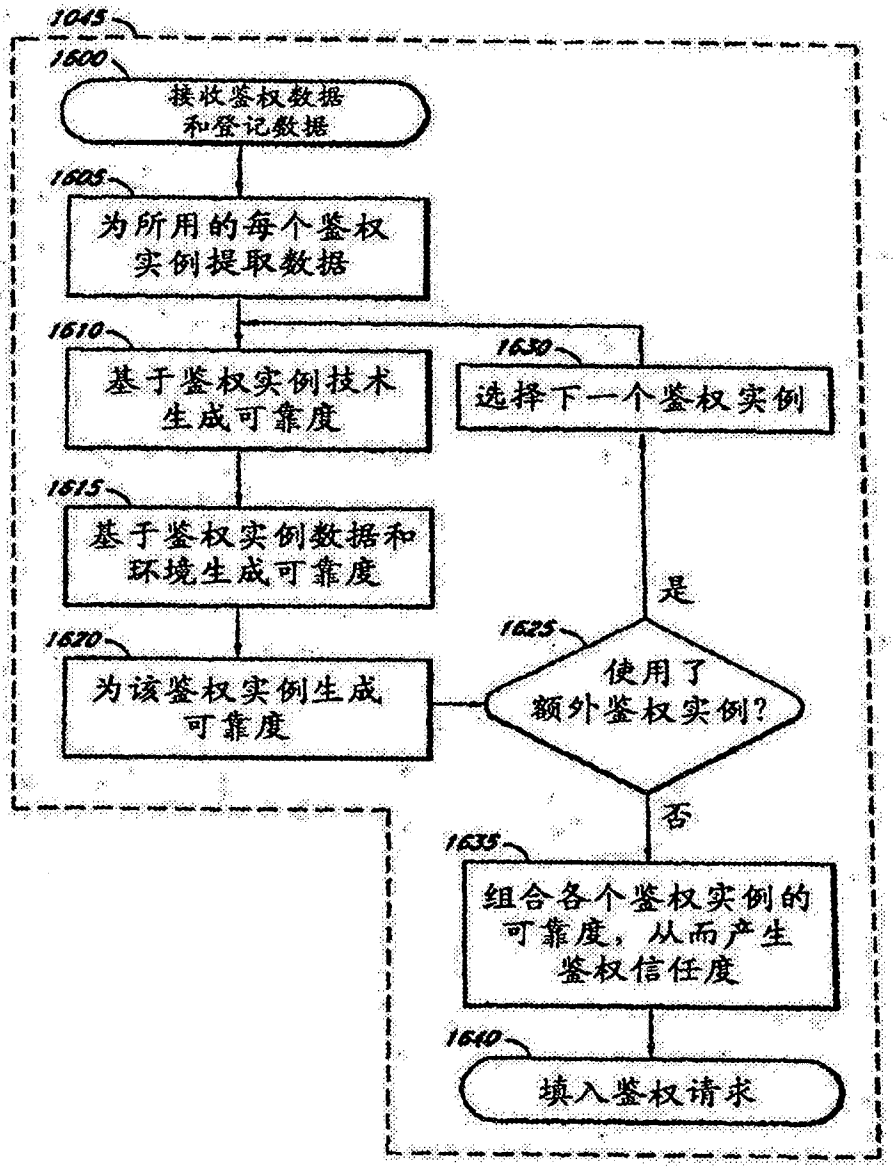

1045
1600
接收鉴权数据和登记数据
1605
为所用的每个鉴权实例提取数据
1610
基于鉴权实例技术生成可靠度
1615
基于鉴权实例数据和环境生成可靠度
1620
为该鉴权实例生成可靠度
1630
选择下一个鉴权实例
是
1625
使用了额外鉴权实例?
否
1635
组合各个鉴权实例的可靠度，从而产生鉴权信任度
1640
填入鉴权请求

图16

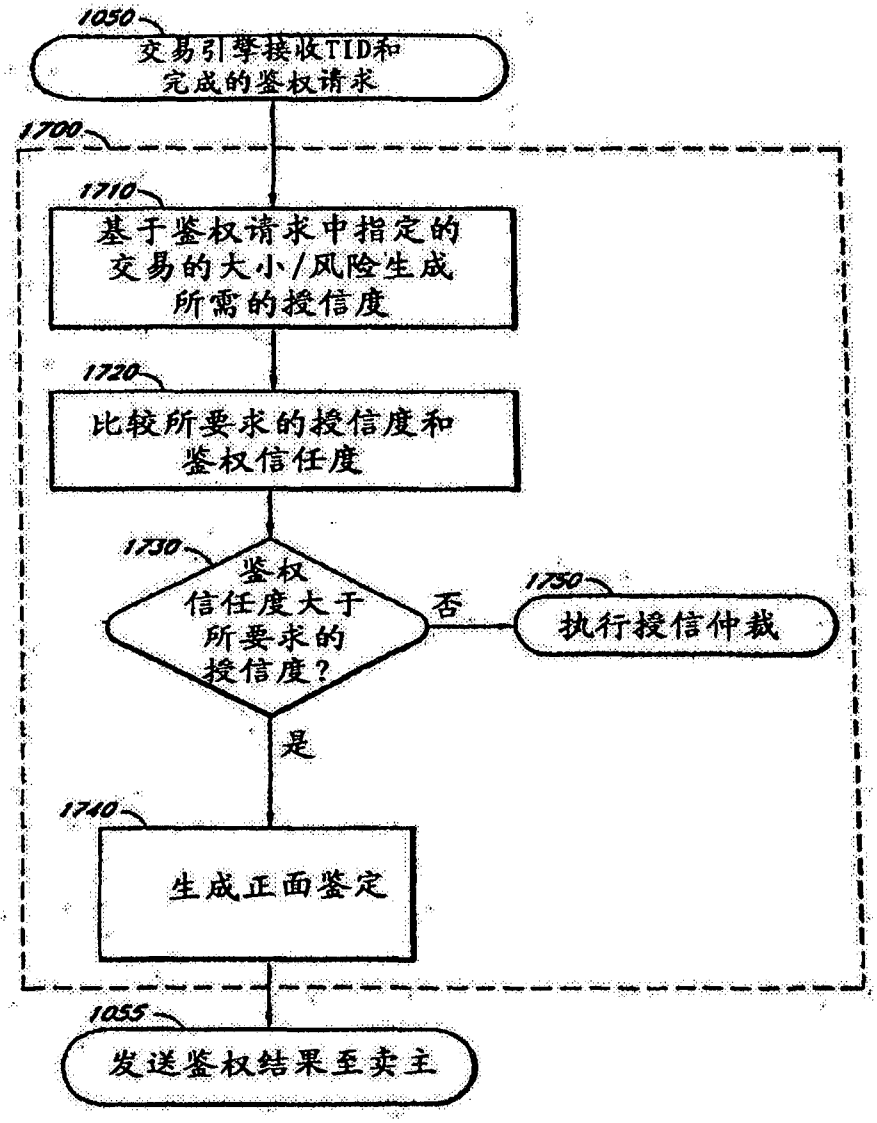

1050
交易引擎接收TID和完成的鉴权请求
1700
1710
基于鉴权请求中指定的交易的大小/风险生成所需的授信度
1720
比较所要求的授信度和鉴权信任度
1730
鉴权信任度大于所要求的授信度？
否
1750
执行授信仲裁
是
1740
生成正面鉴定
1055
发送鉴权结果至卖主

图17

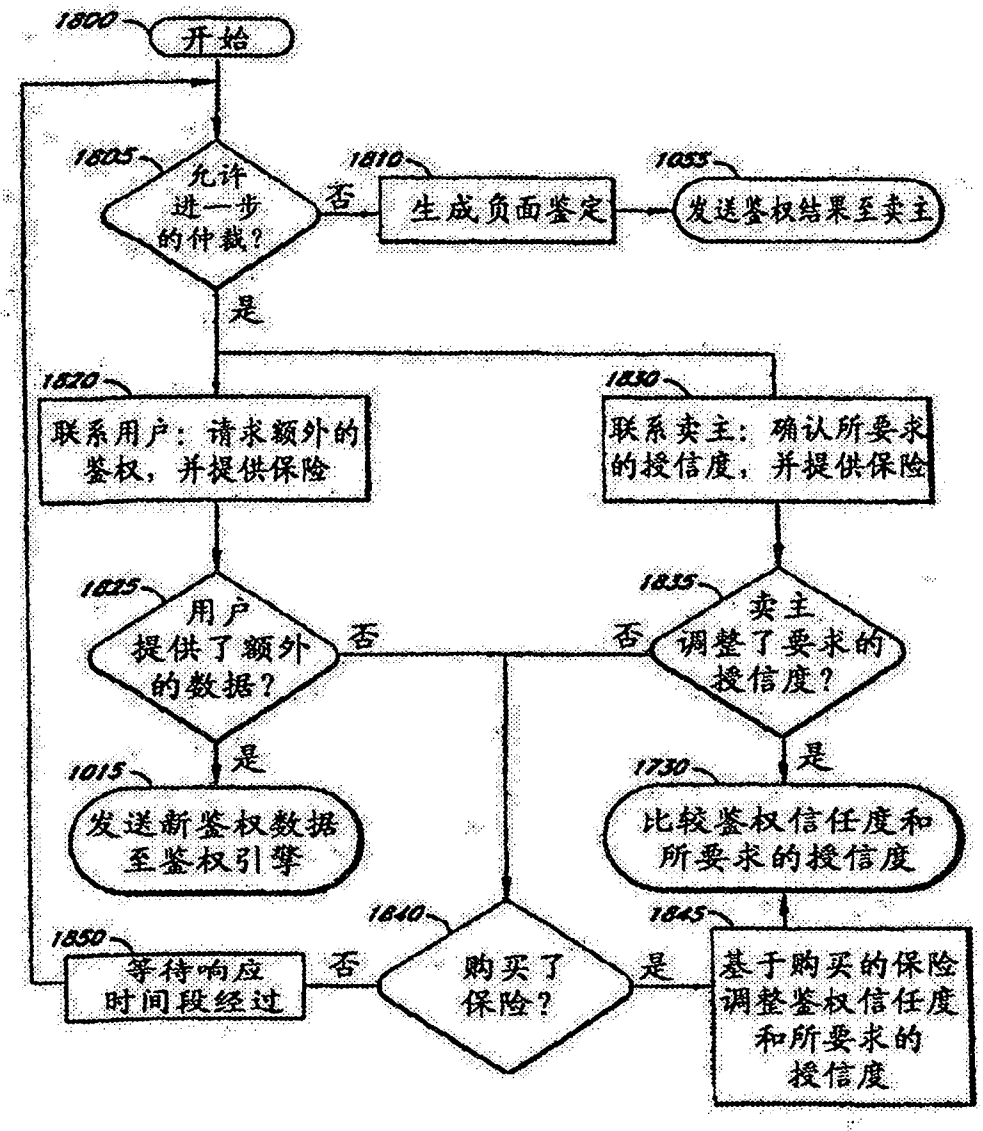

1800
开始
1805
允许进一步的仲裁？
否
1810
生成负面鉴定
1035
发送鉴权结果至卖主
是
1820
联系用户：请求额外的鉴权，并提供保险
1830
联系卖主：确认所要求的授信度，并提供保险
1825
用户提供了额外的数据？
否
否
1835
卖主调整了要求的授信度？
是
1015
发送新鉴权数据至鉴权引擎
是
1730
比较鉴权信任度和所要求的授信度
1840
购买了保险？
1845
基于购买的保险调整鉴权信任度和所要求的授信度
是
1850
等待响应时间段经过
否

图18

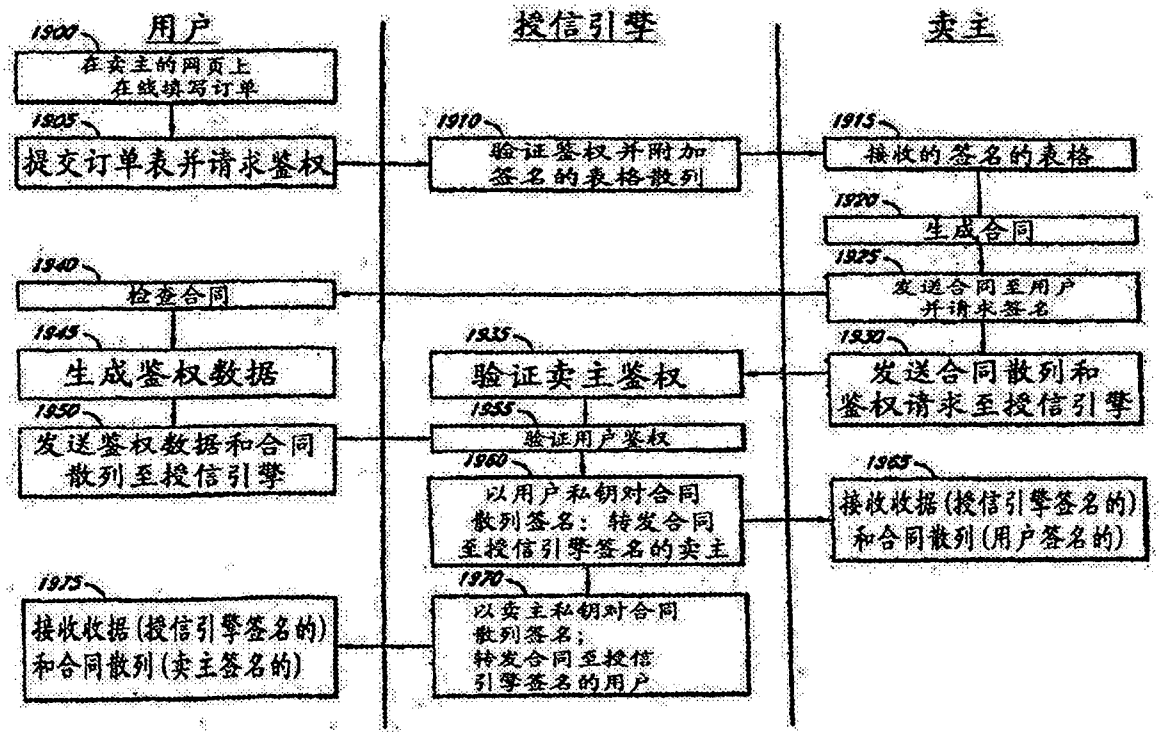

用户
授信引擎
卖主
1900
在卖主的网页上在线填写订单
1905
提交订单表并请求鉴权
1910
验证鉴权并附加签名的表格散列
1915
接收的签名的表格
1920
生成合同
1925
发送合同至用户并请求签名
1930
发送合同散列和鉴权请求至授信引擎
1935
验证卖主鉴权
1940
检查合同
1945
生成鉴权数据
1950
发送鉴权数据和合同散列至授信引擎
1955
验证用户鉴权
1960
以用户私钥对合同散列签名：转发合同至授信引擎签名的卖主
1963
接收收据(授信引擎签名的)和合同散列(用户签名的)
1970
以卖主私钥对合同散列签名；转发合同至授信引擎签名的用户
1975
接收收据(授信引擎签名的)和合同散列(卖主签名的)

图19

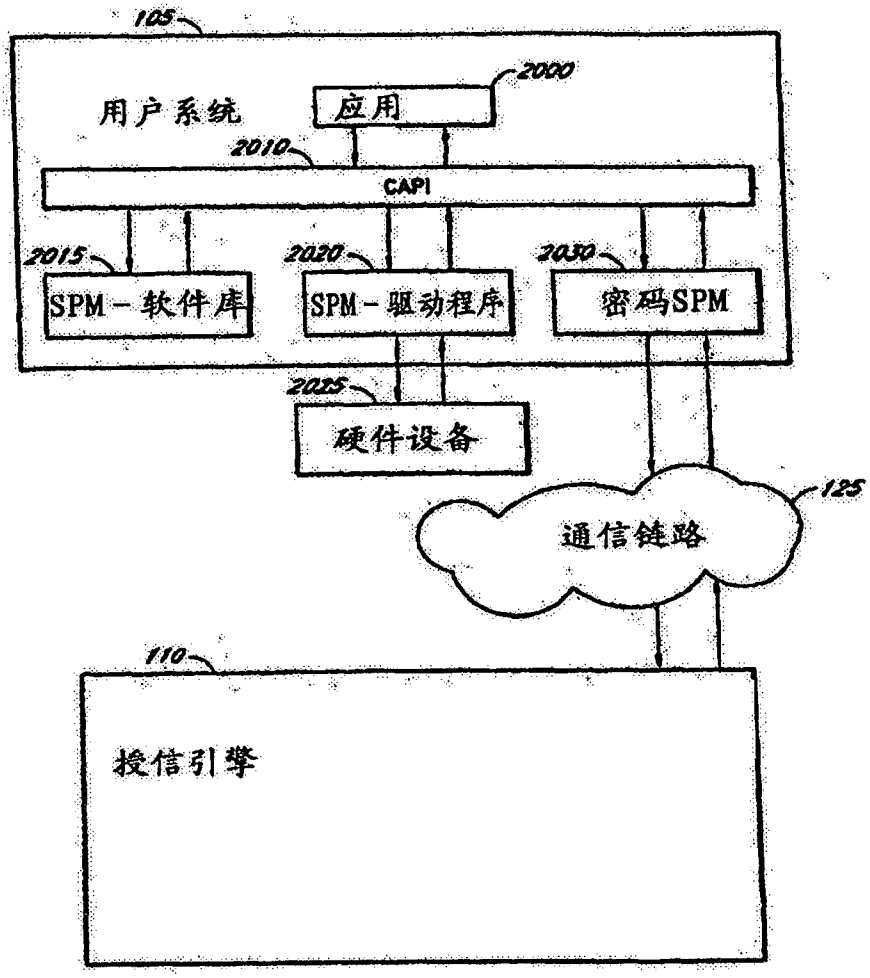

105
用户系统
2000
应用
2010
CAPI
2015
SPM－软件库
2020
SPM－驱动程序
2030
密码SPM
2025
硬件设备
125
通信链路
110
授信引擎

图20

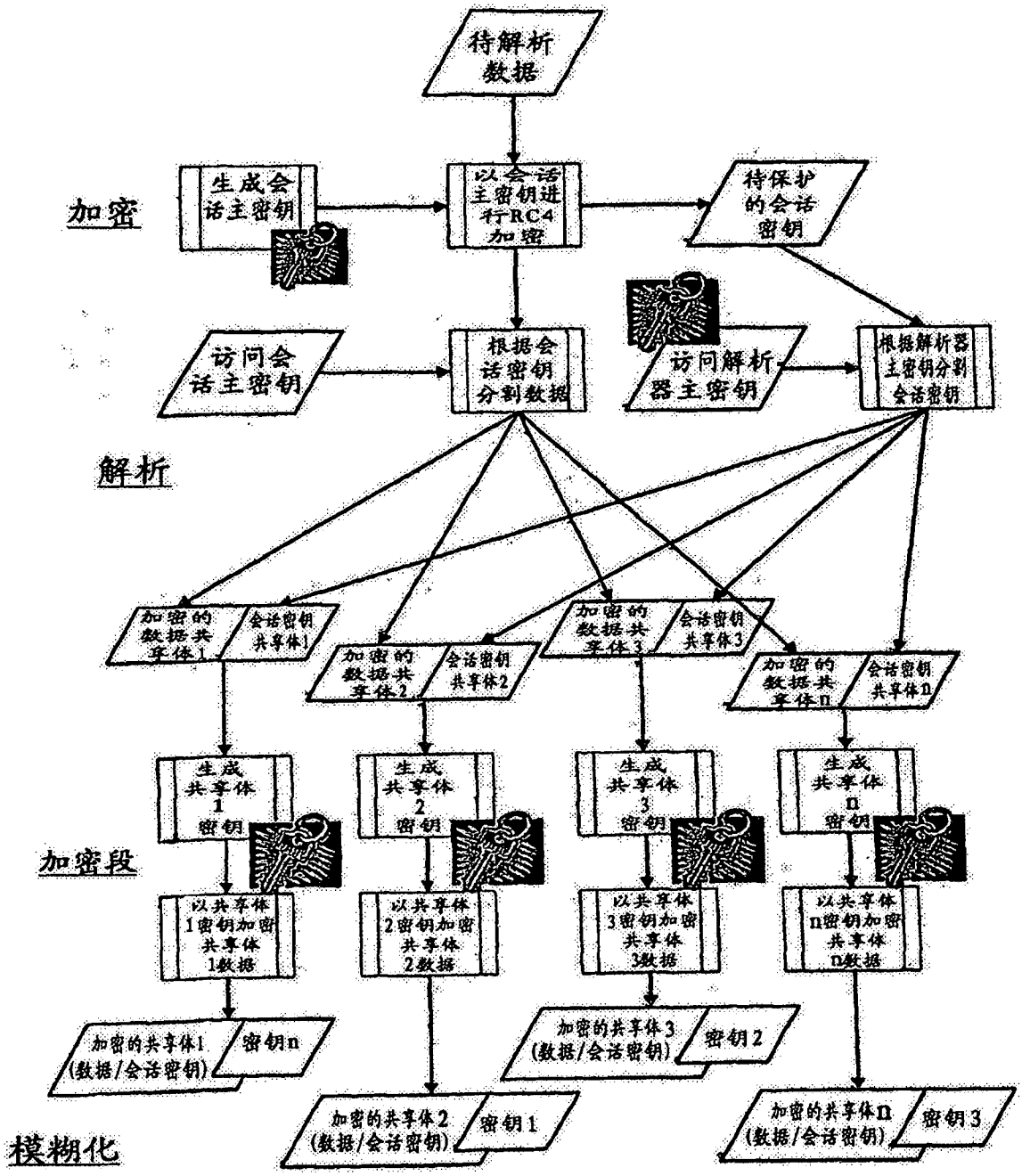

待解析数据
加密
生成会话主密钥
以会话主密钥进行RC4加密
待保护的会话密钥
访问会话主密钥
根据会话密钥分割数据
访问解析器主密钥
根据解析器主密钥分割会话密钥
解析
加密的数据共享体1
会话密钥共享体1
加密的数据共享体2
会话密钥共享体2
加密的数据共享体3
会话密钥共享体3
加密的数据共享体n
会话密钥共享体n
生成共享体1密钥
生成共享体2密钥
生成共享体3密钥
生成共享体n密钥
加密段
以共享体1密钥加密共享体1数据
以共享体2密钥加密共享体2数据
以共享体3密钥加密共享体3数据
以共享体n密钥加密共享体n数据
加密的共享体1(数据/会话密钥)
密钥n
加密的共享体2(数据/会话密钥)
密钥1
加密的共享体3(数据/会话密钥)
密钥2
加密的共享体n(数据/会话密钥)
密钥3
模糊化

图21

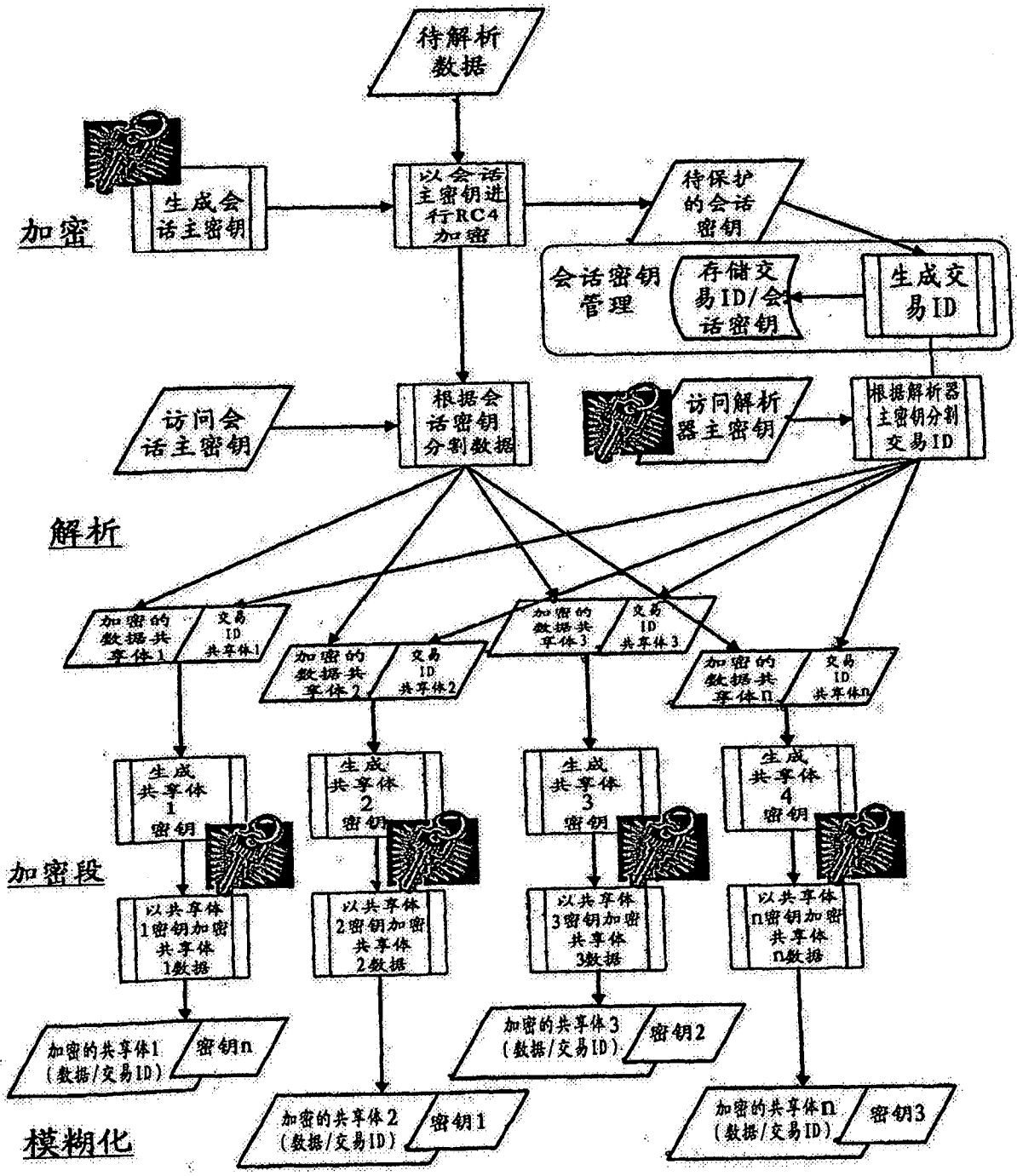

待解析数据
加密
生成会话主密钥
以会话主密钥进行RC4加密
待保护的会话密钥
会话密钥管理
存储交易ID/会话密钥
生成交易ID
访问会话主密钥
根据会话密钥分割数据
访问解析器主密钥
根据解析器主密钥分割交易ID
解析
加密的数据共享体1
交易ID 共享体1
加密的数据共享体2
交易ID 共享体2
加密的数据共享体3
交易ID 共享体3
加密的数据共享体n
交易ID 共享体n
生成共享体1密钥
生成共享体2密钥
生成共享体3密钥
生成共享体4密钥
加密段
以共享体1密钥加密共享体1数据
以共享体2密钥加密共享体2数据
以共享体3密钥加密共享体3数据
以共享体n密钥加密共享体n数据
加密的共享体1(数据/交易ID)
密钥n
加密的共享体2(数据/交易ID)
密钥1
加密的共享体3(数据/交易ID)
密钥2
加密的共享体n(数据/交易ID)
密钥3
模糊化

图22

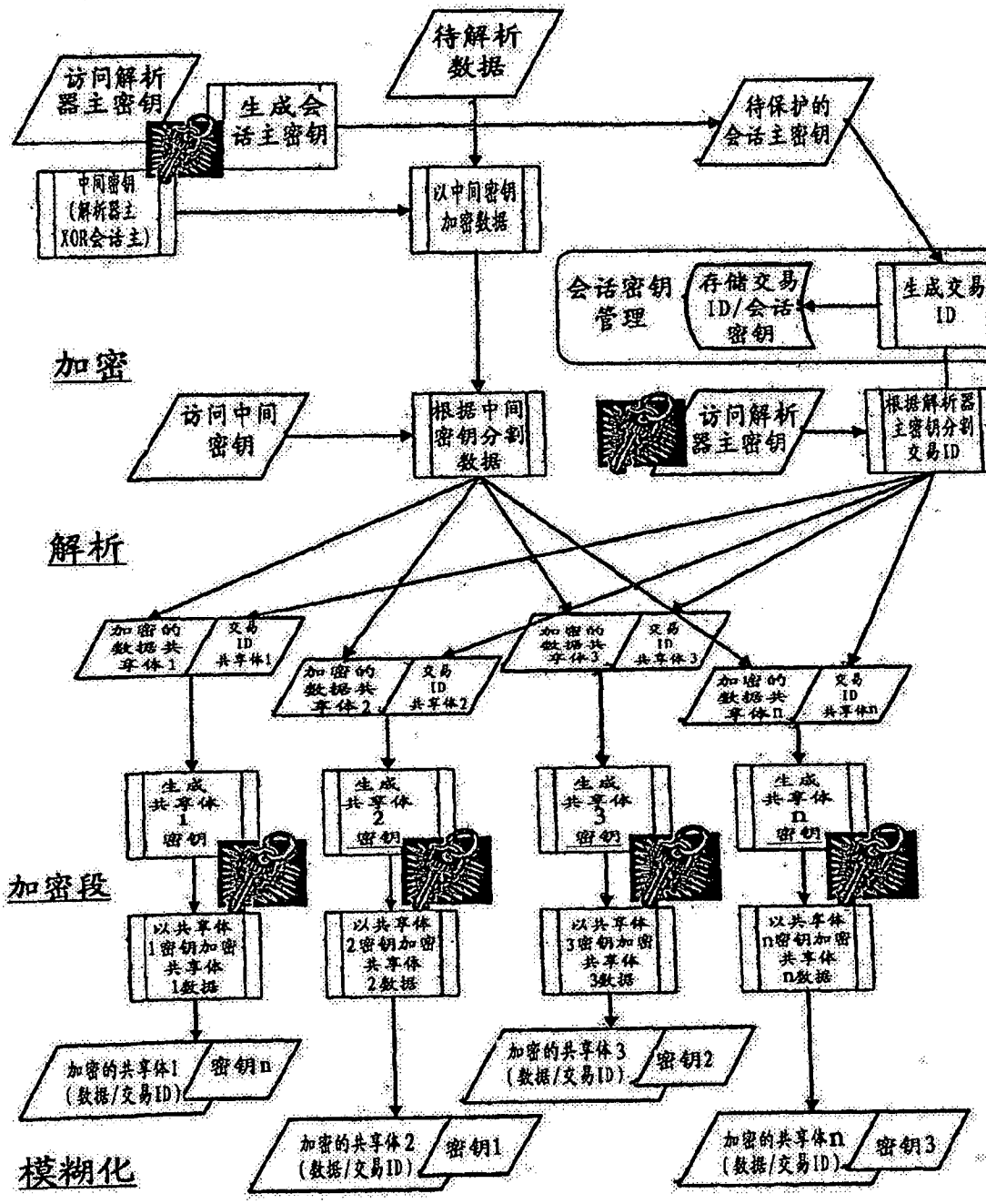

待解析数据
访问解析器主密钥
生成会话主密钥
待保护的会话主密钥
中间密钥(解析器主XOR会话主)
以中间密钥加密数据
会话密钥管理
存储交易ID/会话密钥
生成交易ID
加密
访问中间密钥
根据中间密钥分割数据
访问解析器主密钥
根据解析器主密钥分割交易ID
解析
加密的数据共享体1
交易ID共享体1
加密的数据共享体2
交易ID共享体2
加密的数据共享体3
交易ID共享体3
加密的数据共享体n
交易ID共享体n
生成共享体1密钥
生成共享体2密钥
生成共享体3密钥
生成共享体n密钥
加密段
以共享体1密钥加密共享体1数据
以共享体2密钥加密共享体2数据
以共享体3密钥加密共享体3数据
以共享体n密钥加密共享体n数据
加密的共享体1(数据/交易ID)
密钥n
加密的共享体3(数据/交易ID)
密钥2
加密的共享体2(数据/交易ID)
密钥1
加密的共享体n(数据/交易ID)
密钥3
模糊化

图23

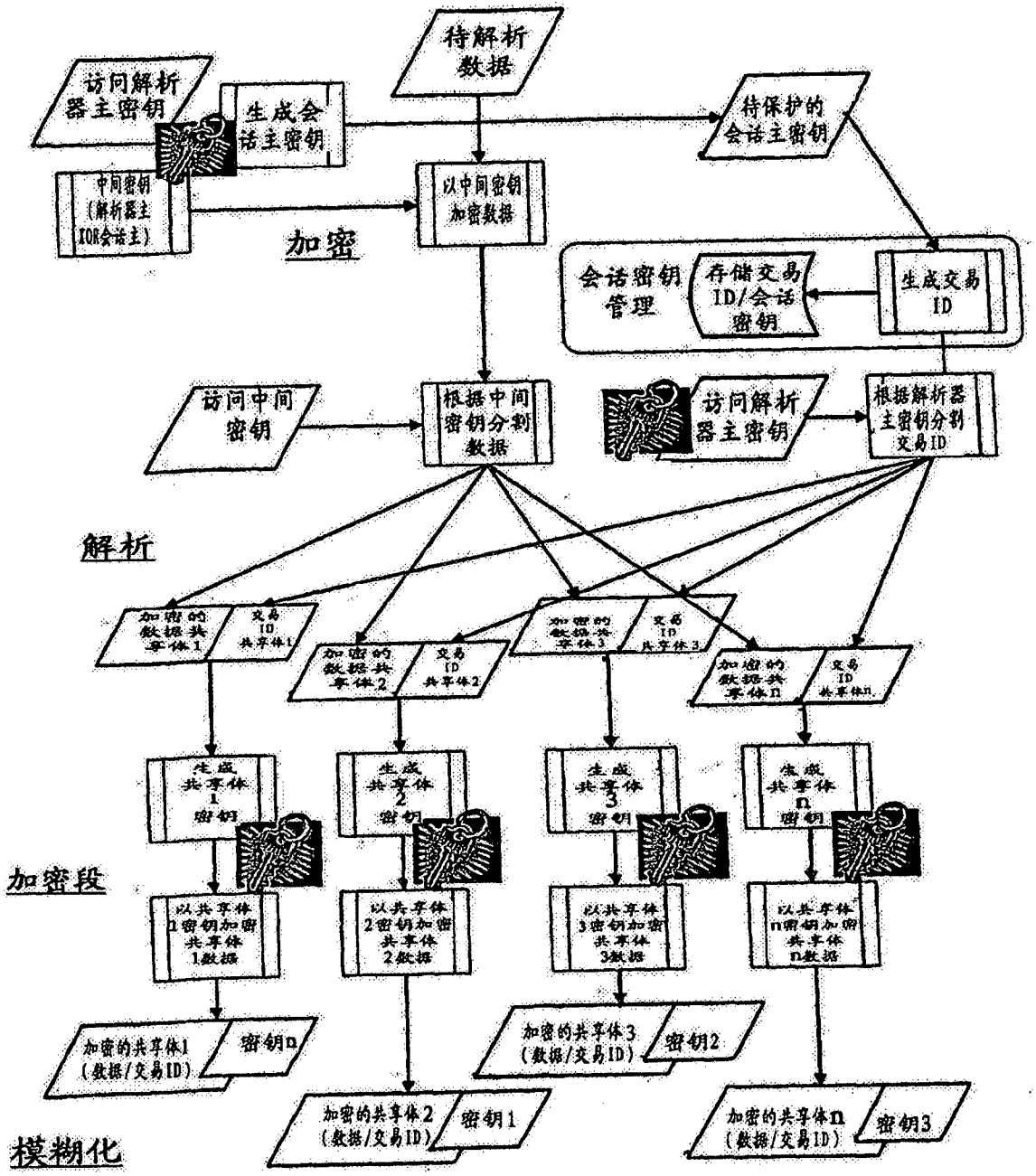

待解析数据
访问解析器主密钥
生成会话主密钥
待保护的会话主密钥
中间密钥(解析器主IOR会话主)
以中间密钥加密数据
加密
会话密钥管理
存储交易ID/会话密钥
生成交易ID
访问中间密钥
根据中间密钥分割数据
访问解析器主密钥
根据解析器主密钥分割交易ID
解析
加密的数据共享体1
交易ID共享体1
加密的数据共享体2
交易ID共享体2
加密的数据共享体3
交易ID共享体3
加密的数据共享体n
交易ID共享体n
生成共享体1密钥
生成共享体2密钥
生成共享体3密钥
生成共享体n密钥
加密段
以共享体1密钥加密共享体1数据
以共享体2密钥加密共享体2数据
以共享体3密钥加密共享体3数据
以共享体n密钥加密共享体n数据
加密的共享体1(数据/交易ID)
密钥n
加密的共享体2(数据/交易ID)
密钥1
加密的共享体3(数据/交易ID)
密钥2
加密的共享体n(数据/交易ID)
密钥3
模糊化

图24

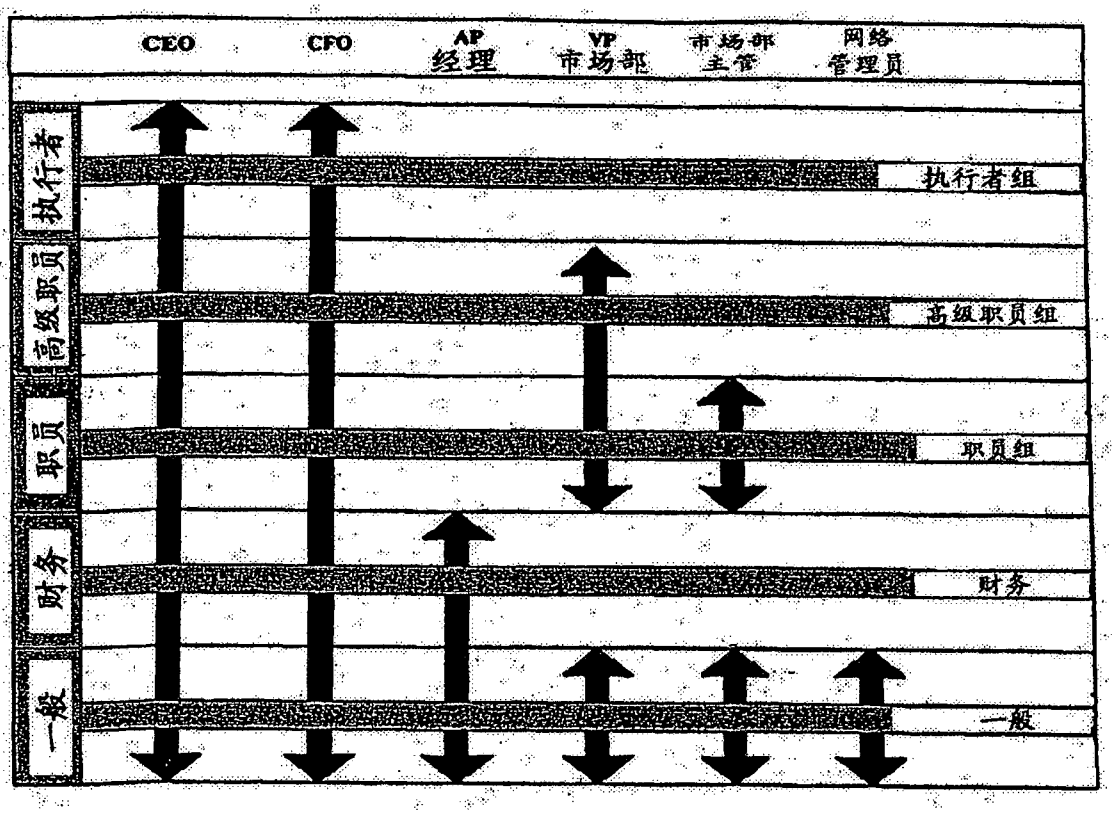

CEO
CFO
AP
经理
VP
市场部
市场部
主管
网络
管理员
执行者
高级职员
职员
财务
一般
执行者组
高级职员组
职员组
财务
一般

图25

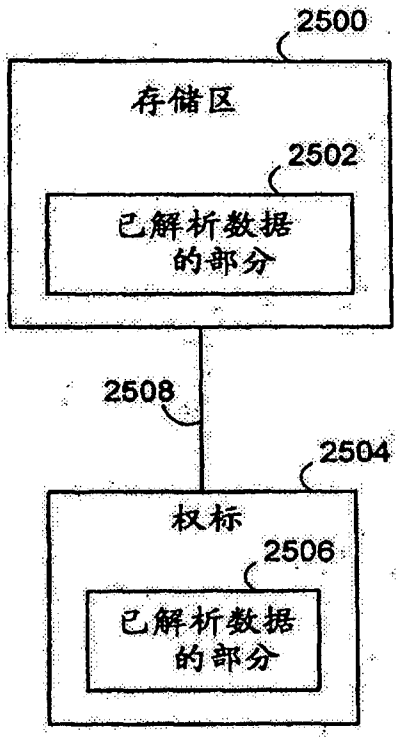

2500
存储区
2502
已解析数据的部分
2508
2504
权标
2506
已解析数据的部分

图26

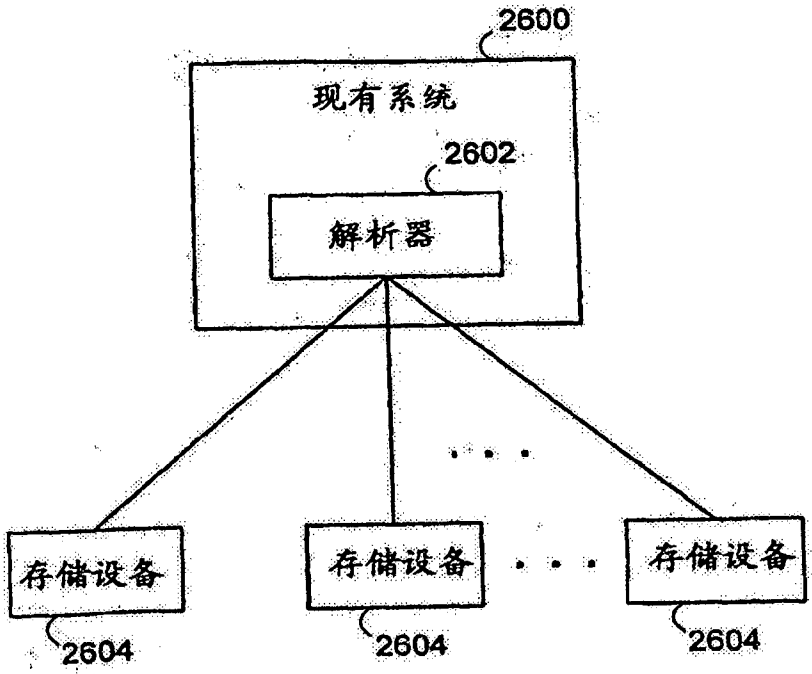

2600
现有系统
2602
解析器
存储设备
2604
存储设备
2604
存储设备
2604

图27

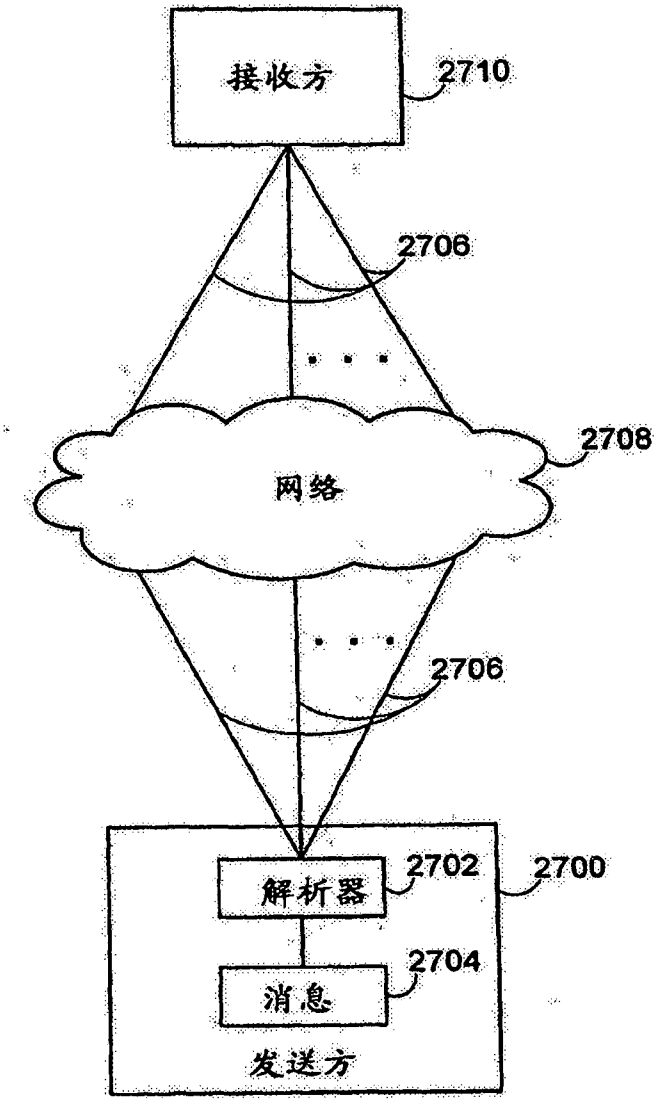


图28

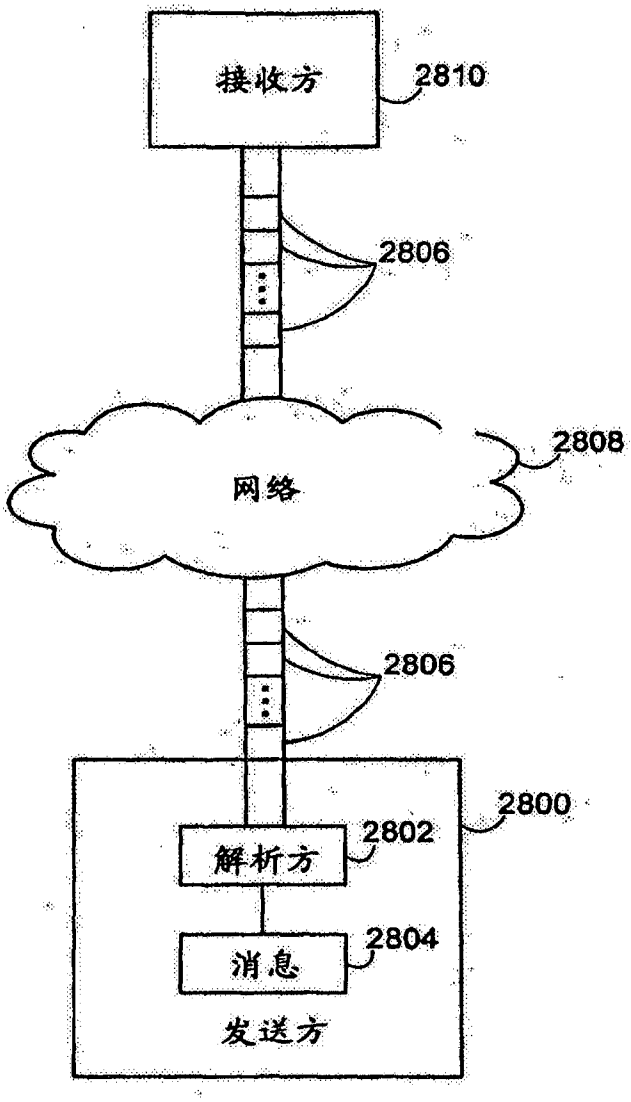


图29

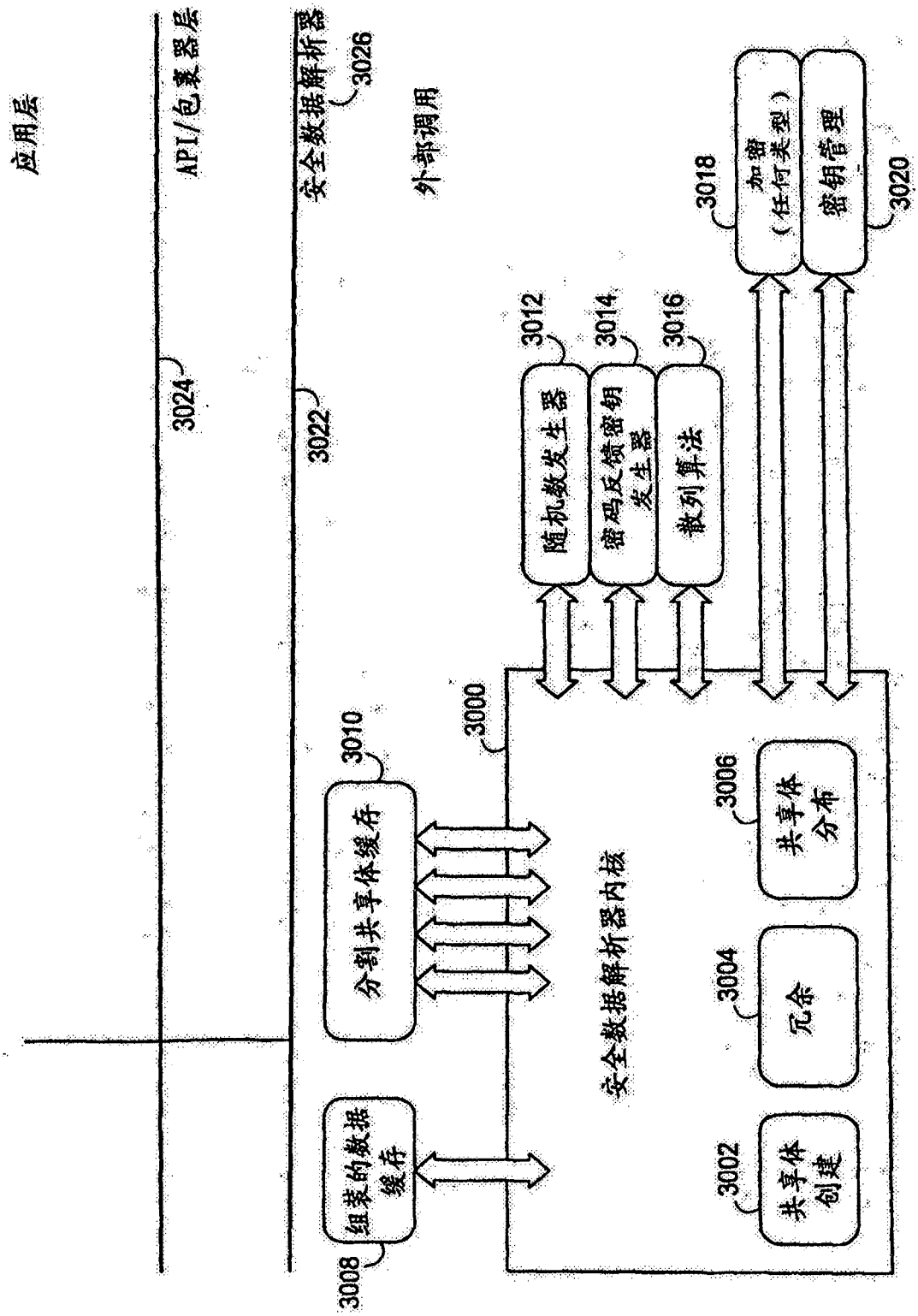

应用层
API/包装器层
安全数据解析器
3026
外部调用
3024
3022
3012
3014
3016
3018
3020
随机数发生器
密码反馈密钥发生器
散列算法
加密（任何类型）
密钥管理
3000
3010
分割共享体缓存
3006
共享体分布
安全数据解析器内核
3004
冗余
3002
共享体创建
组装的数据缓存
3008

图30

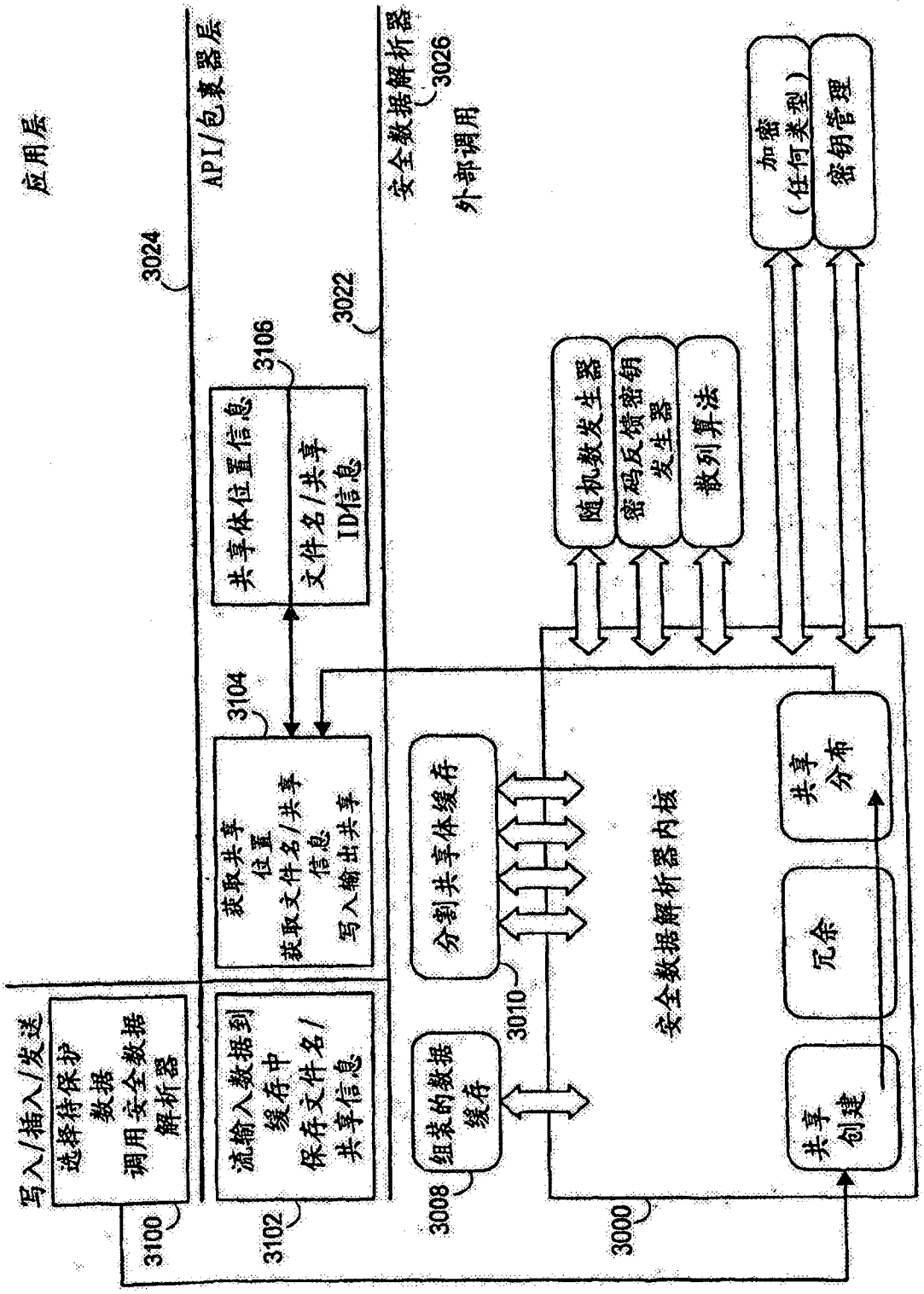

应用层
API/包装器层
安全数据解析器
外部调用
3024
3022
3026
3106
3104
3100
3102
3008
3010
3000
写入/插入/发送
选择待保护数据调用安全数据解析器
流输入数据到缓存中保存文件名/共享信息
获取共享位置获取文件名/共享信息写入输出共享
共享体位置信息
文件名/共享ID信息
组装的数据缓存
分割共享体缓存
安全数据解析器内核
随机数发生器
密码反馈密钥发生器
散列算法
加密（任何类型）
密钥管理
冗余
共享分布
共享创建

图31

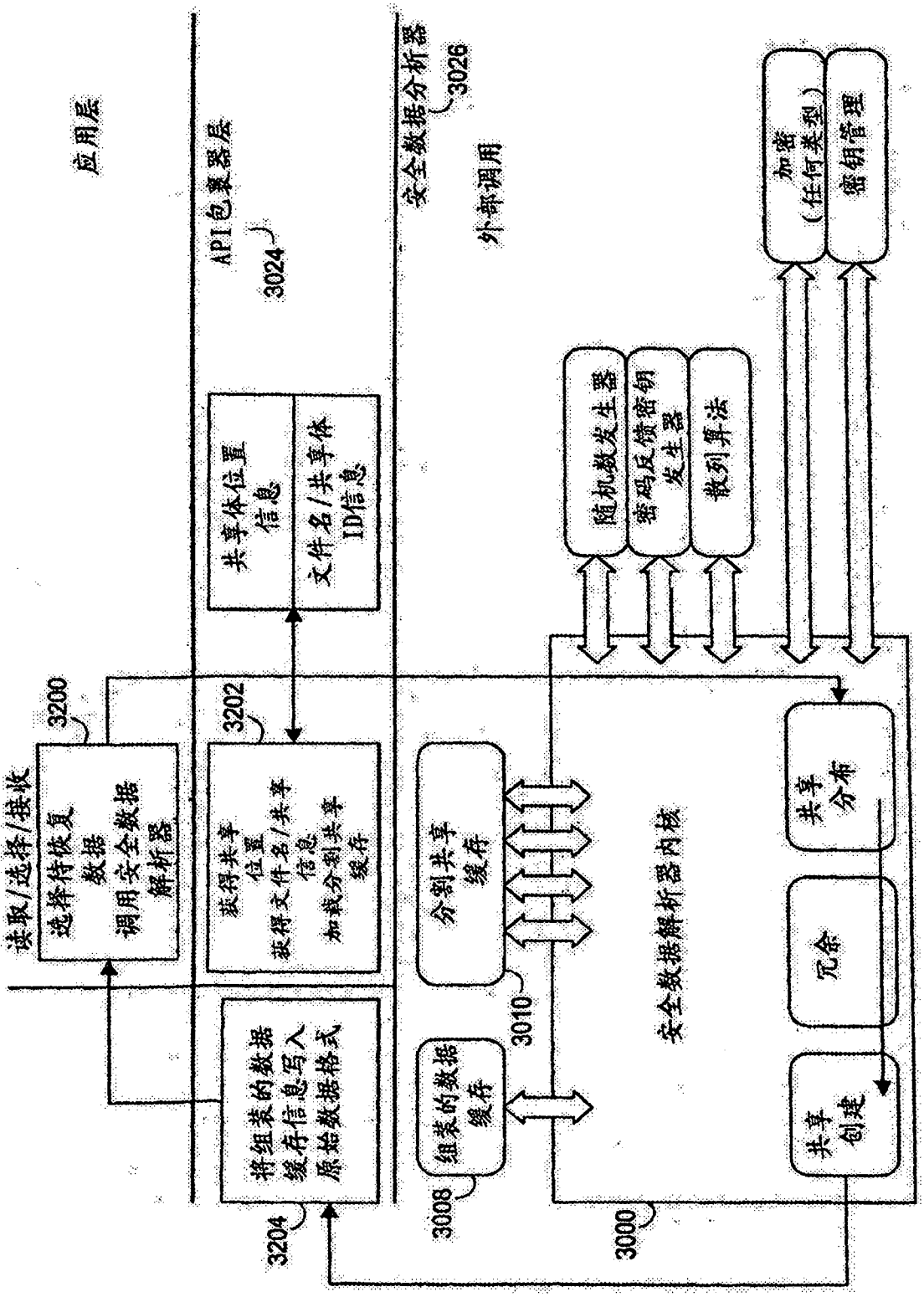

应用层
API包装器层
3024
安全数据分析器
3026
外部调用
读取/选择/接收
选择待恢复数据
调用安全数据解析器
3200
获得共享位置
获得文件名/共享信息
加载分割共享缓存
3202
共享体位置信息
文件名/共享体ID信息
将组装的数据缓存信息写入原始数据格式
3204
分割共享缓存
3010
组装的数据缓存
3008
安全数据解析器内核
3000
随机数发生器
密码反馈密钥发生器
散列算法
加密（任何类型）
密钥管理
共享分布
冗余
共享创建

图32

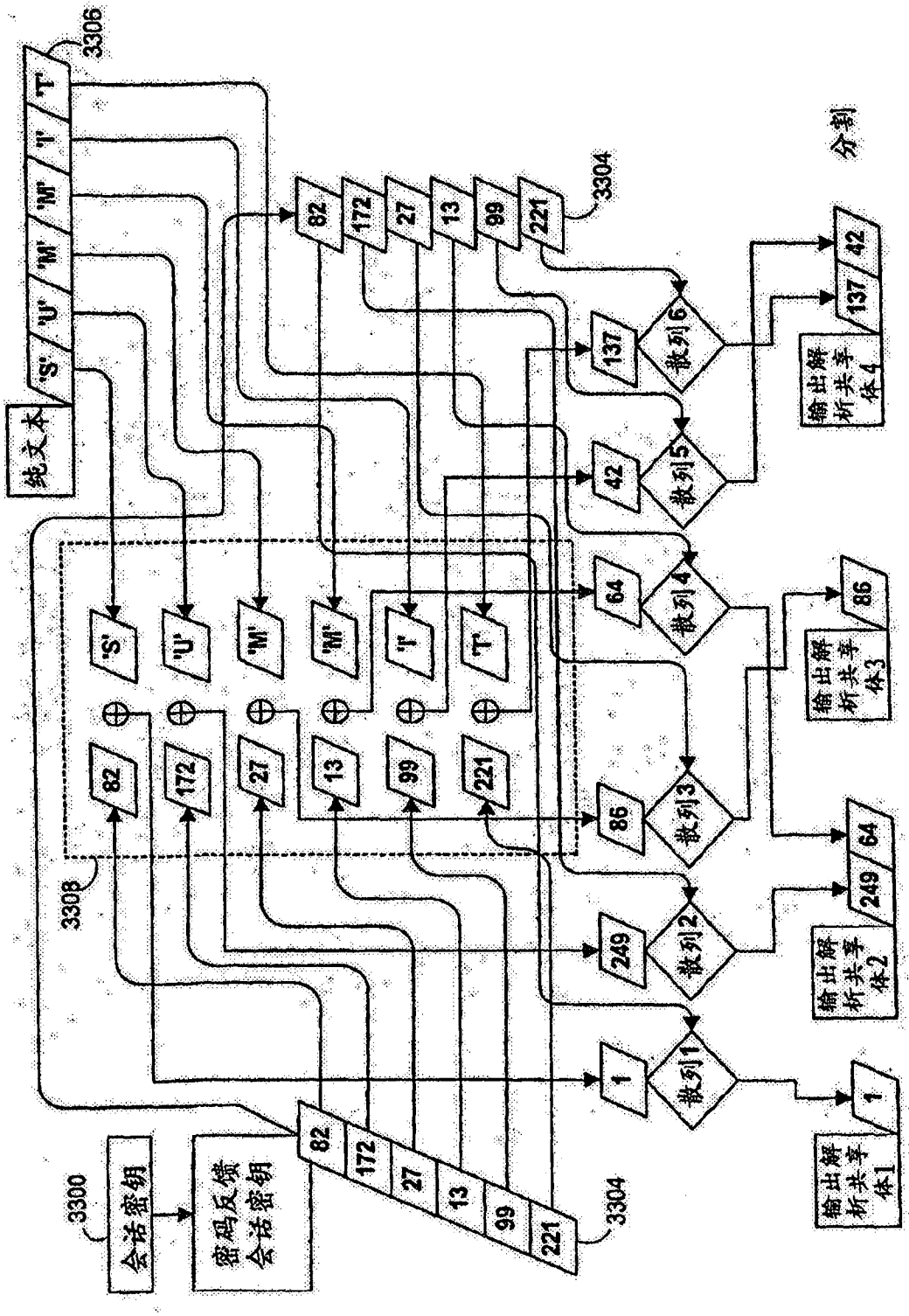

3306
'T'
'I'
'M'
'M'
'U'
'S'
纯文本
82
172
27
13
99
221
3304
分割
137
散列6
42
散列5
64
散列4
86
散列3
249
散列2
1
散列1
输出解析共享体4
输出解析共享体3
输出解析共享体2
输出解析共享体1
3308
3300
会话密钥
密码反馈会话密钥

图33

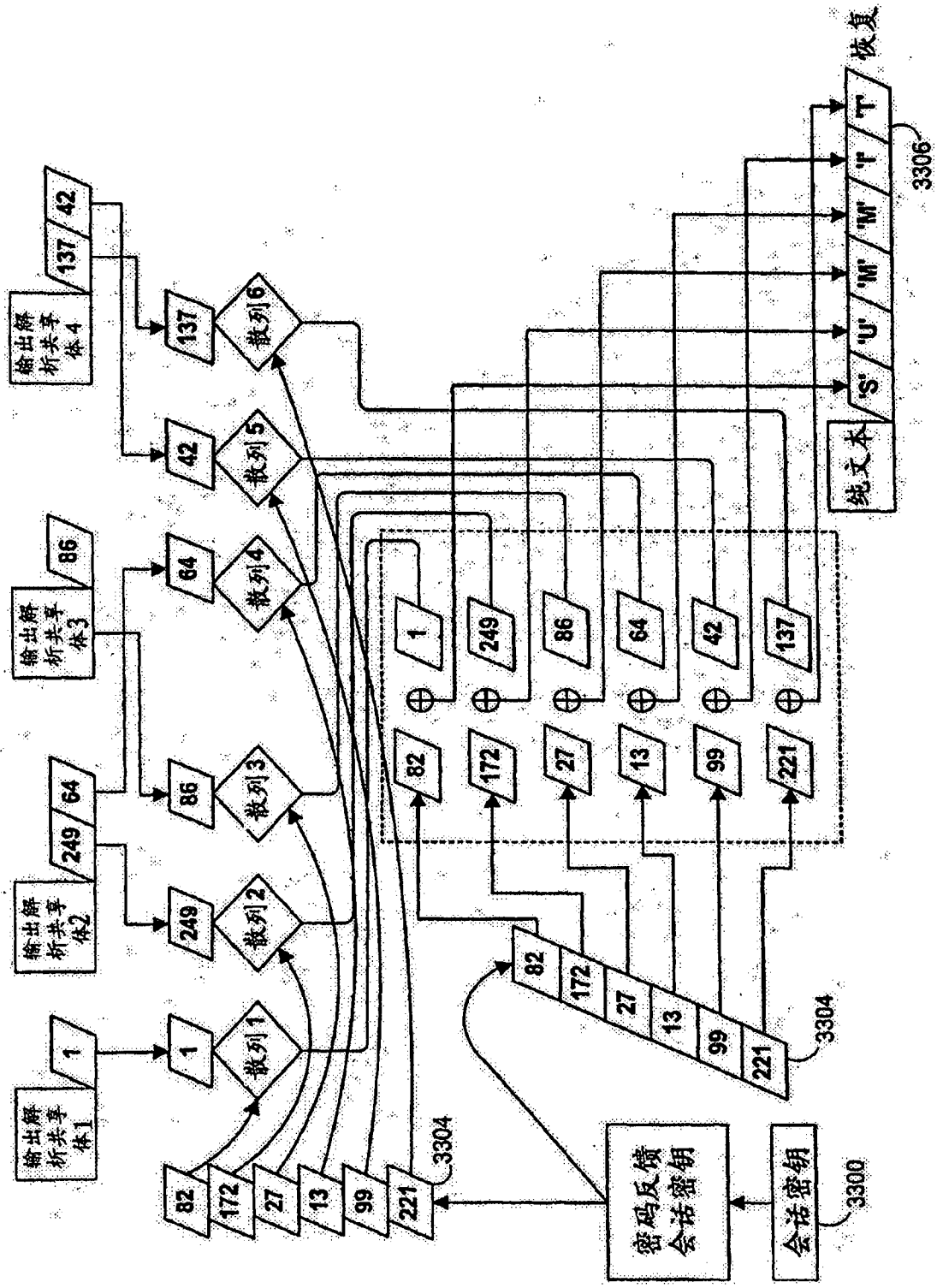

输出解析共享体1
输出解析共享体2
输出解析共享体3
输出解析共享体4
1
249
86
137
42
64
82
172
27
13
99
221
3304
3300
3306
密码反馈会话密钥
会话密钥
明文本
恢复
'S'
'U'
'M'
'M'
'F'
'T'

图34

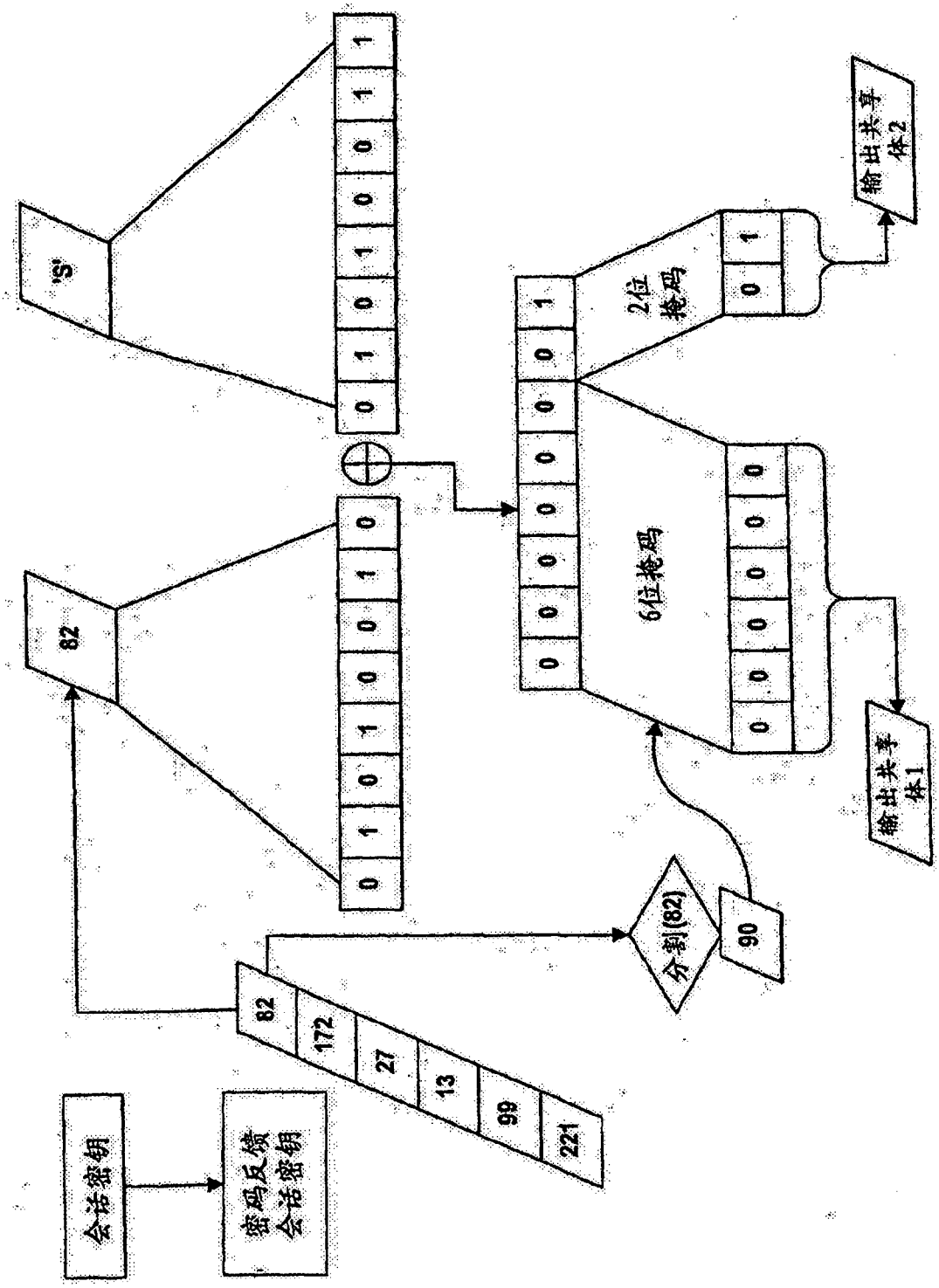

'S'
82
会话密钥
密码反馈
会话密钥
82
172
27
13
99
221
分割(82)
90
2位
换码
6位换码
输出共享
体2
输出共享
体1

图35

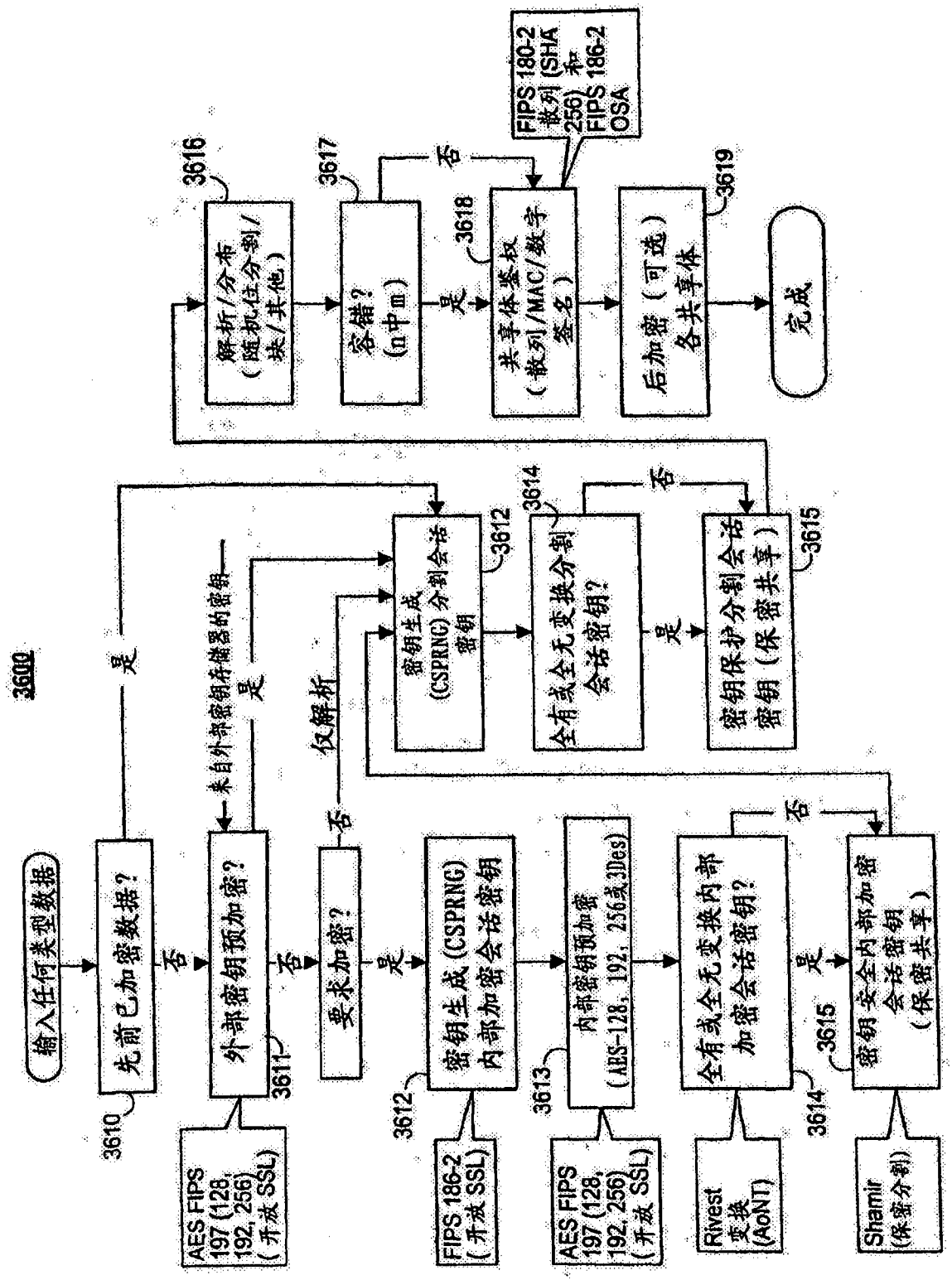

3600
输入任何类型数据
先前已加密数据?
否
是
3610
外部密钥预加密?
否
是
来自外部密钥存储器的密钥
3611
AES FIPS 197 (128, 192, 256) (开放 SSL)
要求加密?
否
是
仅解析
密钥生成 (CSPRNG)
内部加密会话密钥
3612
FIPS 186-2 (开放 SSL)
密钥生成 (CSPRNG) 分割会话密钥
3612
内部密钥预加密 (ABS-128, 192, 256或3Des)
3613
AES FIPS 197 (128, 192, 256) (开放 SSL)
全有或全无变换分割会话密钥?
3614
是
否
密钥保护分割会话密钥 (保密共享)
3615
全有或全无变换内部加密会话密钥?
否
是
3614
Rivest 变换 (AoNT)
密钥安全内部加密会话密钥 (保密共享)
3615
Shamir (保密分割)
解析/分布 (随机位分割/块/其他)
3616
容错? (n中m)
3617
否
是
FIPS 180-2 散列 (SHA 256) 和 FIPS 186-2 OSA
3618
共享体鉴权 (散列/MAC/数字签名)
后加密 (可选) 各共享体
3619
完成

图36

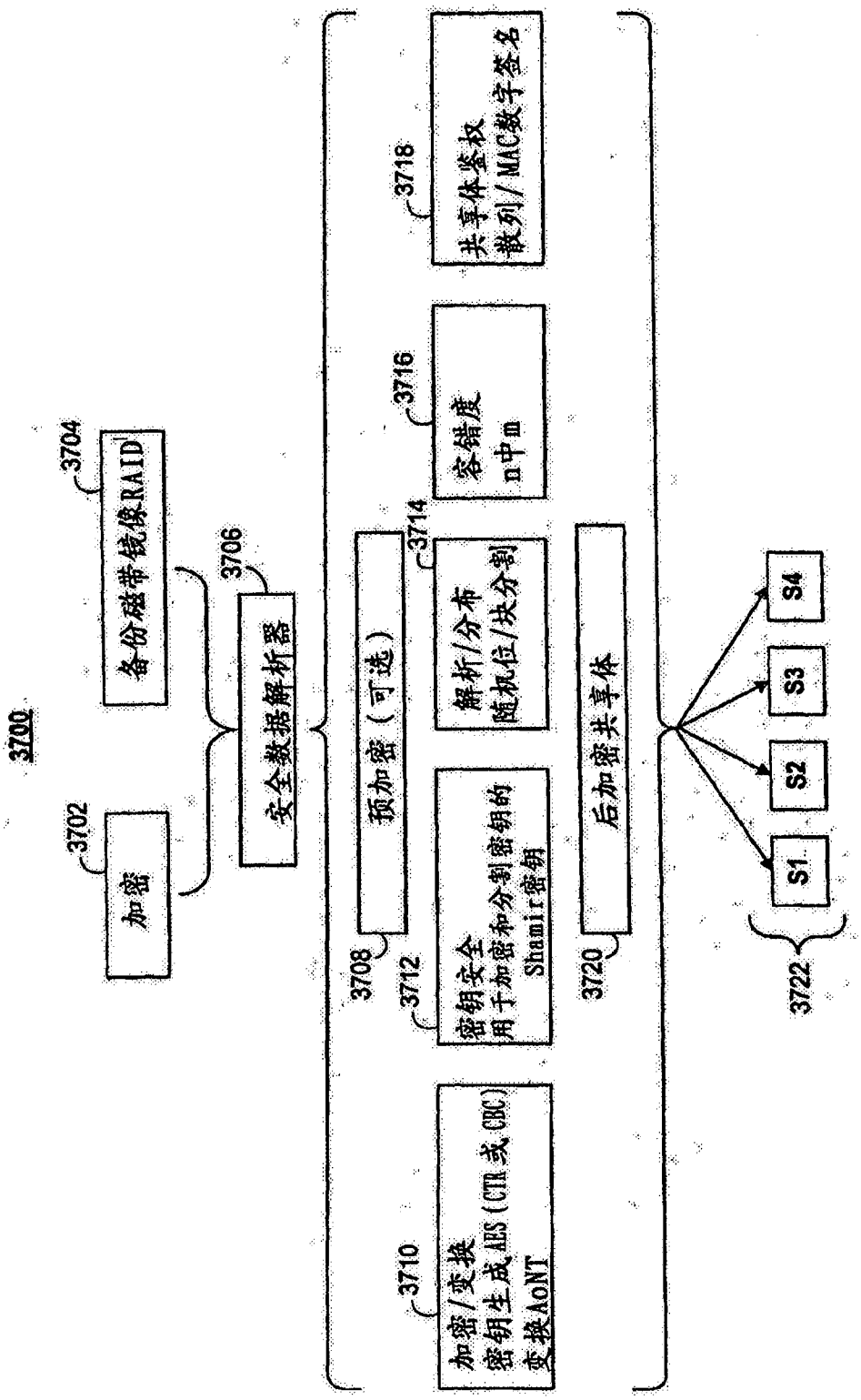

3700
3702
加密
3704
备份磁带镜像RAID
3706
安全数据解析器
3708
预加密（可选）
3710
加密/变换
密钥生成AES（CTR或CBC）
变换AoNT
3712
密钥安全
用于加密和分割密钥的
Shamir密钥
3714
解析/分布
随机位/块分割
3716
容错度
n中m
3718
共享体鉴权
散列/MAC数字签名
3720
后加密共享体
S1
S2
S3
S4
3722

图37

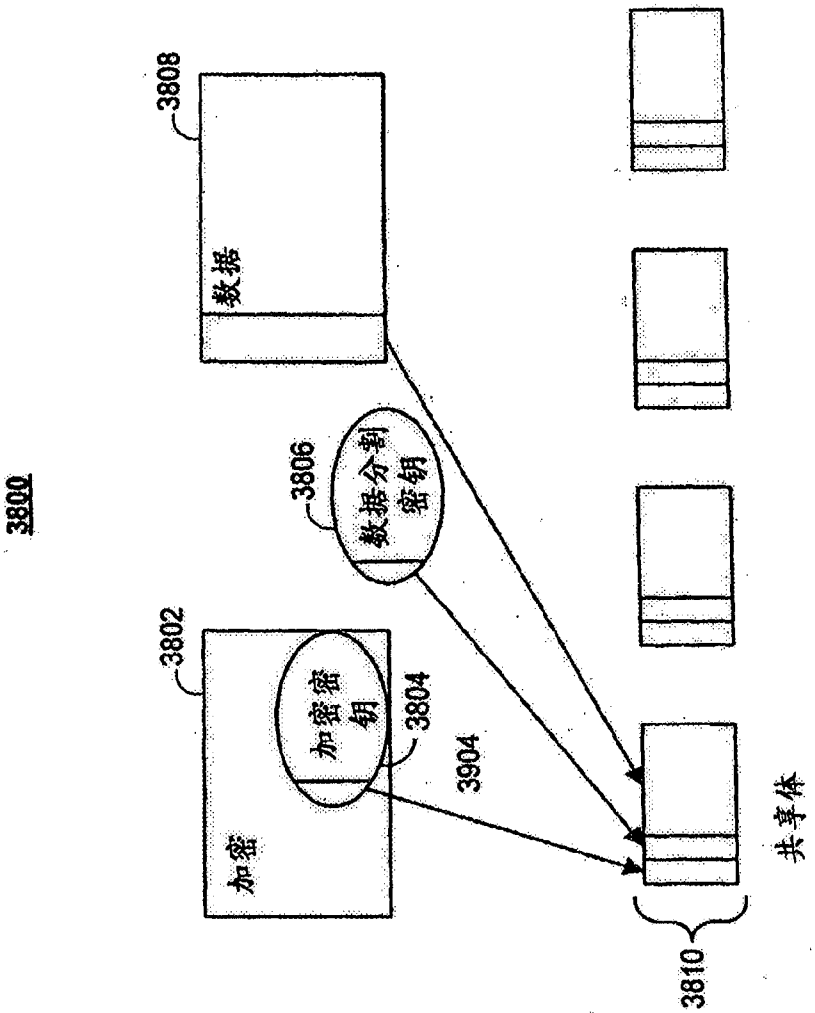


图38

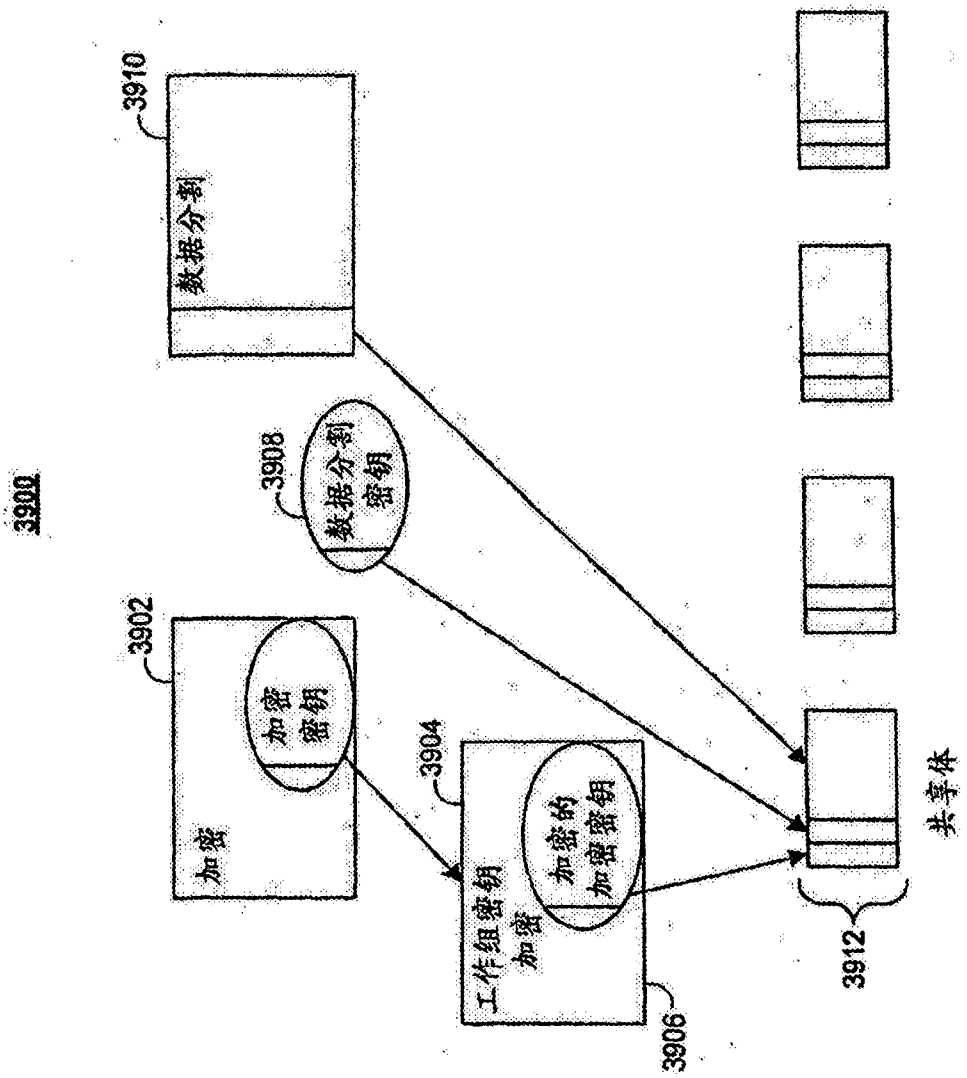

3900
3910
数据分割
3908
数据分割密钥
3902
加密密钥
加密
3904
加密的加密密钥
工作组密钥加密
3906
3912
共享体

图39

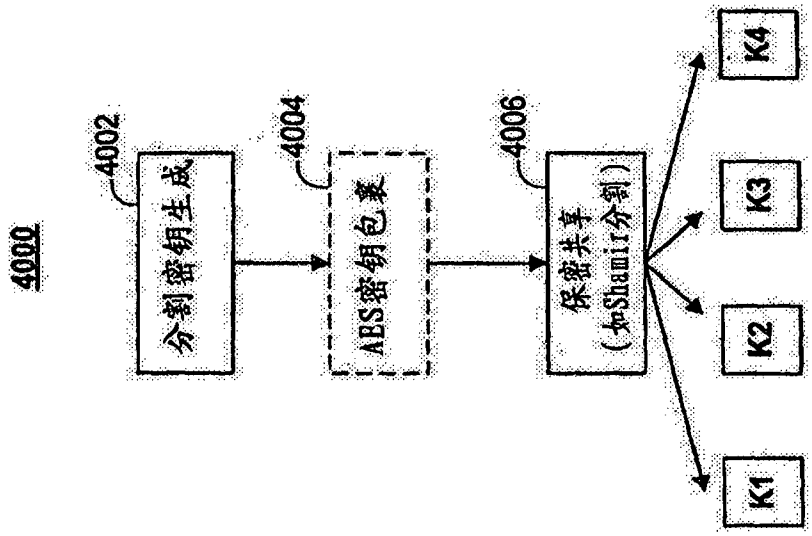

4000
4002
分割密钥生成
4004
ABS密钥包裹
4006
保密共享
(如Shamir分割)
K4
K3
K2
K1

图40A

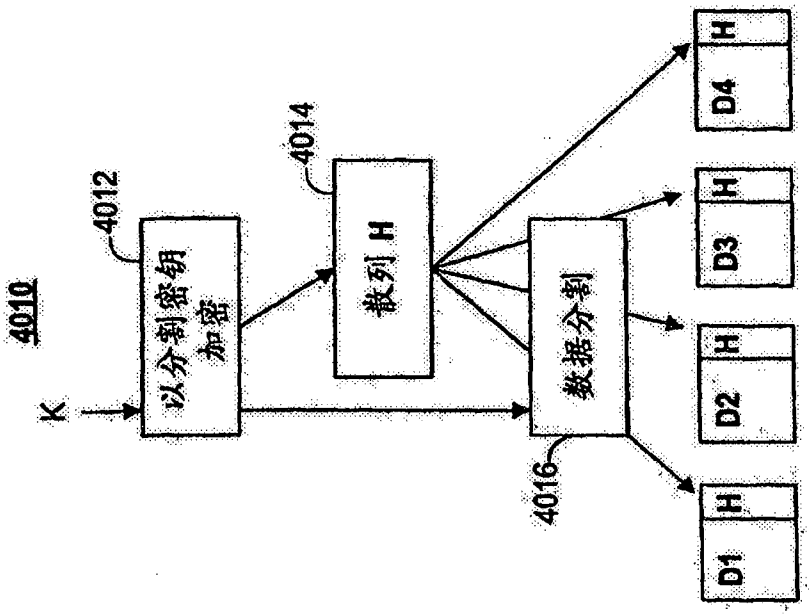

4010
K
4012
以分割密钥
加密
4014
数列 H
数据分割
4016
H
D4
H
D3
H
D2
H
D1

图40B

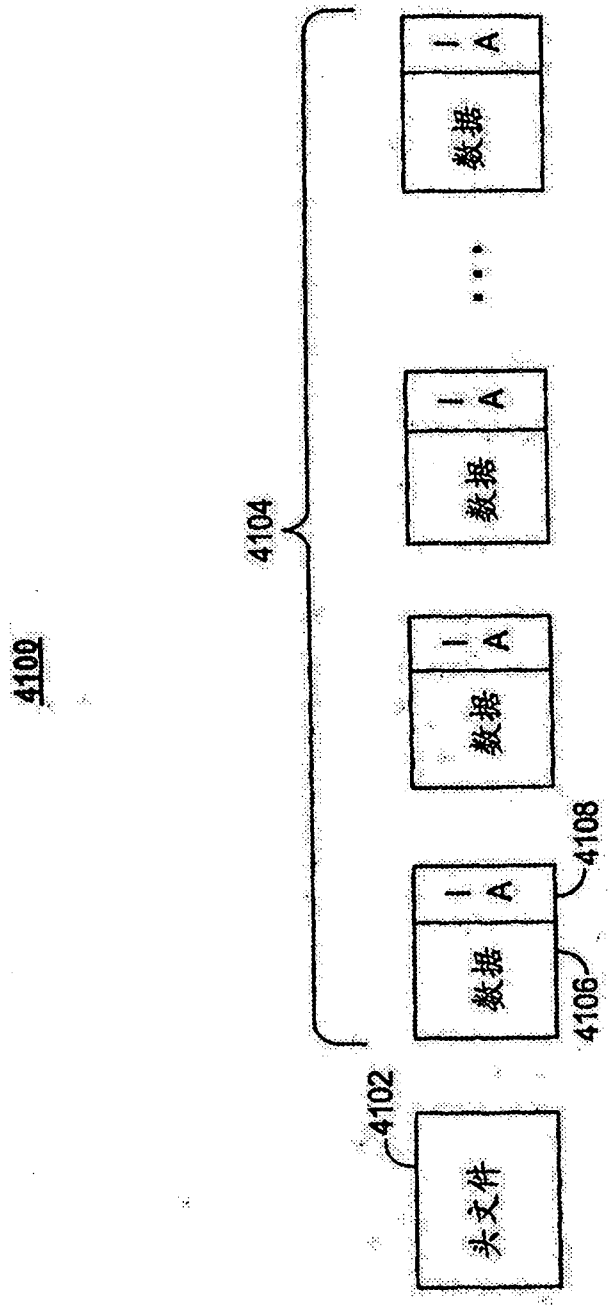


图41

IHC160497 ABSTRACT

A secure data parser is provided that may be integrated into any suitable system for securely storing and communicating data. The secure data parser parses data and then splits the data into multiple portions that are stored or communicated distinctly. Encryption of the original data, the portions of data, or both may be employed for additional security. The secure data parser may be used to protect data in motion by splitting original data into portions of data, that may be communicated using multiple communications paths.